# Administration Guide for Labris UTM

Unified Threat Management Appliances and Software Version 3.4.2

http://labrisnetworks.com/support-training/ Tel: +90 850 455 4555





# 1. Copyright

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission in writing of the author/publisher.

## 2. Disclaimer

Neither the author nor the publisher makes any representation or warranty of any kind with regard to the information contained in the book. No liability shall be accepted for any actions caused, or alleged to have been caused, directly or indirectly from using the information contained in this book.

© Copyright 2013-2014. All rights reserved.

## 3. Document Revision History

#	Document modified by	Description	Authorized by
1			
2			
3			
4			

# **Table of Contents**

Copyright1
Disclaimer1
Document Revision History1
About Labris Networks Inc12
About LABRIS UTM13
How to Purchase LABRIS UTM ?13
LABRIS UTM Appliance deployment Architecture14
Connecting Appliance14
Accessing the Web Admin Console15
LRMS into the LABRIS UTM Appliance15
Wizard Installation19
How to use Wizard Installation?20
A – Gateway Mode Network Configuration This is the section where the hostname and working mode settings of the device can be made22
B - DNS Configuration This is the section where DNS IP address settings can be made
C - DHCP Configuration This is the section where we can activate or deactivate DHCP server in which the interface and IP settings of the IP addresses to be distributed to our DHCP Local users, are made
Accessing LABRIS UTM through LMC27
LMC Interface27
Menu28
File Menu29
Edit Menu31
View Menu
Device Menu
Add Modules from Server Menu36
User Management
Users
Adding User
Deleting User42
Changing password / Editing User43
Groups44
Adding Group44
Deleting Group48

Editing Group	
WAUTH	56
Deleting WAUTH policy	60
Editing WAUTH Policy	61
Adding WAUTH Authentication and User	62
Login	82
Change User Password	
Obtain Password	
Registering with SMS	
GSM number and common key	
System	
System LMC Module	
Users	
Adding User	
Deleting User	
Change Password / Editing User	
DHCP	
DNS	
HA - High Availability Appliance Deployment Architecture	
Configuration Backup / Restore	
Update	
Automatic Update	
Record	
Date / Time Settings	
Console Access Settings	
General Settings	
Trusted Time Stamp	
Restart	
Shutdown	
Network Settings	
IP Configuration	
IP Alias (ADD, Edit, Delete, Status, Enable/disable)	
ADSL (Add, Edit, Delete, Status, Enable/Disable)	
Bridge(Add ,Edit, Delete, Status , Enable/disable)	

3G (ADD, Edit, Delete, Status, Enable/disable)	
Vlan (Add , Edit, Delete, Status , Enable/disable)	
Routes	
Default Gateway	
Static Route	
Add (Static Route)	
Delete (Static Route)	
Load Balance	
Add (Load Balance Route)	
Edit (Load Balance Route)	200
Delete (Load Balance Route)	201
Advanced/ Policy Based Routing	201
Link Configuration	202
Decision Table	203
WAN failover (WAN Backup)	207
Firewall	214
Make a new firewall object	215
Objects	220
Network Objects	221
Hosts	222
Networks	227
Address Ranges	229
Object Groups	232
Users	235
Services	237
ICMP	238
IP	240
ТСР	244
UDP	247
Service Groups	249
DoS/DDoS	253
General	254
SYN Flood	254
UDP Flood	255

CONN Flood	256
ICMP Flood	256
ICMPv6 Flood	256
Notes	257
QoS/Bandwidth	259
General	259
Notes	260
Schedule	261
Standard	262
User Defined	263
General	263
Start	264
Stop	265
Notes	265
Application Control	267
User Defined	267
Firewall	270
Labris Firewall Management	270
Labris Firewall Management Install, Save (create a new policy object for first setup), Install Policy	270
Labris Firewall Management Install, Save (create a new policy object for first setup), Install Policy Add Next Generation Firewall	270 270 272
Labris Firewall Management Install, Save (create a new policy object for first setup), Install Policy Add Next Generation Firewall Firewall Properties	
Labris Firewall Management Install, Save (create a new policy object for first setup), Install Policy Add Next Generation Firewall Firewall Properties Global Policy table	
Labris Firewall Management Install, Save (create a new policy object for first setup), Install Policy Add Next Generation Firewall Firewall Properties Global Policy table NAT (Network Address Translate) Policy table	
Labris Firewall Management. Install, Save (create a new policy object for first setup), Install Policy Add Next Generation Firewall. Firewall Properties. Global Policy table. NAT (Network Address Translate) Policy table. Interfaces	
Labris Firewall Management. Install, Save (create a new policy object for first setup), Install Policy Add Next Generation Firewall. Firewall Properties. Global Policy table. NAT (Network Address Translate) Policy table. Interfaces. Firewall Application.	
Labris Firewall Management Install, Save (create a new policy object for first setup), Install Policy Add Next Generation Firewall Firewall Properties Global Policy table NAT (Network Address Translate) Policy table Interfaces Firewall Application SSH Inspection	
Labris Firewall Management Install, Save (create a new policy object for first setup), Install Policy Add Next Generation Firewall Firewall Properties Global Policy table NAT (Network Address Translate) Policy table Interfaces Firewall Application SSH Inspection Network Address Translate (NAT)	
Labris Firewall Management. Install, Save (create a new policy object for first setup), Install Policy. Add Next Generation Firewall. Firewall Properties . Global Policy table. NAT (Network Address Translate) Policy table . Interfaces . Firewall Application. SSH Inspection. Network Address Translate (NAT) What is the NAT?	
Labris Firewall Management Install, Save (create a new policy object for first setup), Install Policy Add Next Generation Firewall Firewall Properties Global Policy table NAT (Network Address Translate) Policy table Interfaces Firewall Application SSH Inspection Network Address Translate (NAT) What is the NAT? Why it is made?	
Labris Firewall Management Install, Save (create a new policy object for first setup), Install Policy Add Next Generation Firewall Firewall Properties Global Policy table NAT (Network Address Translate) Policy table Interfaces Firewall Application SSH Inspection Network Address Translate (NAT) What is the NAT? Why it is made? NAT Types	
Labris Firewall Management Install, Save (create a new policy object for first setup), Install Policy Add Next Generation Firewall Firewall Properties Global Policy table NAT (Network Address Translate) Policy table Interfaces Firewall Application SSH Inspection Network Address Translate (NAT) What is the NAT? Why it is made? NAT Types SNAT	
Labris Firewall Management Install, Save (create a new policy object for first setup), Install Policy Add Next Generation Firewall Firewall Properties Global Policy table NAT (Network Address Translate) Policy table Interfaces Firewall Application SSH Inspection Network Address Translate (NAT) What is the NAT? What is the NAT? Why it is made? NAT Types SNAT DNAT	
Labris Firewall Management Install, Save (create a new policy object for first setup), Install Policy Add Next Generation Firewall Firewall Properties Global Policy table NAT (Network Address Translate) Policy table Interfaces Firewall Application SSH Inspection Network Address Translate (NAT) What is the NAT? Why it is made? NAT Types SNAT DNAT PAT	

Reverse Proxy engine	92
Sample configuration:	94
VPN	95
IPSEC VPN Configuration	96
Profile Administration;	96
Add Profile29	96
Identity Confirmation RSA; RSA (Rivest Shamir Adleman) It is the section where common security key used in the stage of establishing connection with the remote network with which IPSEC VPN will be made is defined. RSA is an internet encryption and authentication system	y, 07
Add Local Networks (Manuel):	22
Add Remote Networks:	20
Policy:	20
Add Policy	00
Add PHASE-1	00
Add PHASE-2.	)U
Add Clobal Dalicy For Romata Natwork access permissions in cases where Congrate Eirowall Pula	71
Automatically option is not selected, Step 3 and Step 4 must be applied.	03
Add NAT policy	03
Delete Profile	03
Connection Tracking;	34
SSL VPN Configuration using CLI	34
Create a new global policy	35
Create a new NAT Policy	36
Add a user on policy	70
SSL VPN CLIENT - User Administration	70
SSLVPN Client	38
Add	38
Edit	10
Delete	11
Settings	12
L2TP	13
Add32	15
Edit3:	16
Delete	18
Service Management	18

ILTER	
Filter Groups	
Add/Edit Filter Group	
Delete Filter Group	
Time limit	
Add Time	
Delete Time	
Add Users	
Add Groups	
Add IP/ IP Range	
Delete	
Banned Filters	
Domain/ Category Filtering	
Add	
Add More	
Delete	
URL/Category Filtering	
Add	
Add More	
Delete	
Regex URL Filtering	
Add	
Add More	
Delete	
Phrases	
Add	
Delete	
Content Change	
Add	
Delete	
Extension Filter	
Add	
Delete	
Application Types Filter (MIME)	

Add
Add More
Delete
Exception Filters
Domain
Add
Add Multiple
Delete
URL
Add
Delete
Phrases
Add
Delete
Grey Site
Add
Add Multiple
Delete
Grey URL
Add
Add More
Delete
Settings
Reporting Options
Authentication
NTLM Authentication
NTLM Authentication AD Configuration
General View
Prerequisite
Scenario416
Configuration
Logging Options
Network Settings
Weighted Phrase Settings

Cache Settings
Fork Pool Settings425
Log Monitoring426
Show427
Filter
Start
Clear
ANTISPAM/ANTIVIRUS429
Spam Mail Box429
Search Criterions
Virus Mail Box430
Search Criterions430
Antispam-Antivirus Options431
Domain Control431
Settings434
Antispam Options436
Check Options
Report Options
Whitelist Blacklist
Enable White List
Enable black List
Antivirus Options
Antivirus Options
Report Options451
IDS/IPS452
Sensor Settings452
Intrusion Detection System452
Settings453
Network Settings453
Interface458
Rule sets
Alert Settings469
Mail Alert Settings469
Report Mails470

Alerts	470
MESSAGING	470
Domains	471
Domain	471
All Users	474
Aliases	479
Groups	482
Services	484
Configuration	486
Load Balancer	488
Configuration	489
Externally Advertised Services	489
Internal Servers for Selected External Service	493
Internal Address	493
Service	495
Global	496
Global Settings	496
Monitor	497
Service Monitor	497
License	498
New License	498
Install License	500
Glossary	500
Labris Firewall Messages	501
1. Labris Logview User Guide	505
1. Introduction	505
2. Parts & Tools	507
3. Instructions	511
4. Records Table	511
4.1. Real-time Monitoring	514
5. Utilities	517
5.1. Settings	517
5.2. Save Screen	518
5.3. Load Screen	518

6. Regional Settings	520
7. Service Monitoring	521
8. Layout Options	522
8.1. Single Widget View	522
8.2. Column View	523
8.3. List View	523
8.4. Grid View	523

## 4. About Labris Networks Inc.

Since 2002, Labris Networks Inc. has been an R&D focused and rapidly-growing provider of network security solutions through its globally-proven products. Labris ensures ultimate network security through its extensive product line including Firewall/VPN, Web Security, E-Mail Security, Lawful Interception and Availability Protection solutions on LABRIS UTM, Labris LOG and Harpp DDoS Mitigator appliances. Next-generation solutions are developed to detect, identify all kinds of real-time threats, applications providing a smart shield against intrusions, viruses, spam, malware and availability attacks.

Labris products protect networks of all sizes with a variety of topologies and deployment scenarios. Through Labris FLEX firmware options, the customers have privileges to get the security software they need as well as extra modules such as Wireless Guest Authentication, Detailed Internet Reporting, Lawful Interception and Logging. Having a customer-focused, future-oriented and flexible approach, Labris also offers its state-of-the-art security software as a Cloud Service.

Having operations in a rapidly growing global network of more than 20 countries, Labris products protect enterprises, brands, government entities, service providers and mission-critical infrastructures.

Labris with its worldwide partners is committed to the highest levels of customer satisfaction and loyalty, providing the best after-sales support by the multilingual Global Support Center. Being one of the Common Criteria EAL4+ certified security gateway brands in the world and rapidly growing global player, Labris provides its customers the top-level security with optimum cost. Labris, headquartered in Ankara, Turkey, has offices serving Europe, Middle East, North Africa, Caucasus and Southeast Asia.

## 5. About LABRIS UTM

Labris UTM is an Identity-based UTM Appliance. Labris UTM's solution is purpose-built to meet the security needs of corporates, government organizations, and educational institutions. Labris UTM's perfect blend of best-of-breed solutions includes Identity based Firewall, Content filtering, Anti Virus, Anti Spam, Intrusion Detection and Prevention (IDP), and VPN.

Labris UTM provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server etc. hosted in DMZ which are visible to the external world and still have firewall protection. It also provides assistance in improving bandwidth management, increasing employee productivity and reducing legal liability associated with undesirable Internet content access.

Labris UTM is available for Small Enterprises , Medium Enterprises as well as Large Enterprises

Labris UTM Web Security provides further control to block inappropriate and illegal web sites as well as instant messaging and peer-to-peer applications while Labris UTM Application Intelligence and Control broadens control over inefficient web applications such as social media platforms (Facebook, twitter, etc.), online trading, IM/chat, peer-to-peer sharing and streaming video sites. Labris Email Security completes the offering with effective protection against spam and phishing attacks so employees only read legitimate emails and are not exposed to fake emails. Labris UTM's intelligent solutions simplify the centralized management of local and remote network services while protecting your precious information and communications resources with low TCO.

## 6. How to Purchase LABRIS UTM ?

To purchase LABRIS UTM, Visit - <u>http://labrisnetworks.com/products/product/lbrutm-series-appliances/</u>

You can purchase through authorized distributors <u>http://labrisnetworks.com/authorized-distributors/</u>

# 7. LABRIS UTM Appliance deployment Architecture

This section provides information about the logical and physical design for the prescribed deployment architecture. LABRIS UTM Appliance deployment architecture consists of software processes called servers, topological units referenced as nodes and the security device known as Labris UTM. In the below deployment architecture, all the Servers and LAN users are connected to the Labris UTM through L2 switches. Labris UTM Appliance is connected to external network through Router.



# 8. Connecting Appliance

Connect appliance to a management computer's Ethernet interface. You can use a cross-over Ethernet cable to connect directly or use straight-through Ethernet cable to connect through the hub or switch. Both the cables are provided along with the appliance. Connect Ethernet cable one end to Labris UTM device in eth0 and other end to computer.

Note

•Labris UTM Device will provide default IP address

## 9. Accessing the Web Admin Console

Labris Default Management Port = eth0/Port1/Net0/Mgt (first port to device)

Labris Default IP Address: 169.254.1.1 Labris Default Username: admin Labris Default Password: labris

Connect your computer to the first port on the Labris and then open computer's network settings section and assign IP address **169.254.1.2** and subnet **255.255.0.0**. Open your browser and browse <u>https://169.254.1.1:81</u>(Here IP address is the IP address of your device) to access **LABRIS UTM** Web Console (GUI). Login page is displayed and you are prompted to enter login credentials. Use default username and password to log on.

Note

•Latest versions of Browsers like Internet Explorer or Mozilla Firefox are required to access web Admin Console

# **10.LRMS into the LABRIS UTM Appliance**

LRMS – Labris Report and Monitoring Service

Once you set and install LABRIS UTM Appliance properly this is how you will login in to the LABRIS UTM Appliance

It has a login screen as well as languages selection screen

These are the inputs for LABRIS UTM Login screen

1	Username	Type in your valid Default username.This username is the one which you have given during the installation
2	Password	Type in your valid Default password. This password is the one which you have given during the installation. A good password is a mix of alphabets , numericals, special characters with a minimum length of 8
3	Warm Me	Warm Me before logging me into other sites.
4	Clear	Clear all Input
5	Login	Click on "Login" button to login to your appliance
6	Languages	Select your prefered language before logging into your appliance .Currently available languages are English and Turkish

Labris Central Authentication Service
Username: 1 Password: 2
Warn me before logging me into other sites. 3 CLEAR 5 Login For security reasons, please Log Out and Exit your web browser when you are done accessing services that require authentication
6 English   Turkish

Note

•You can also change your prefered language even after you login to the appliance as shown in following image



# Understanding your landing page or home screen

In this section you will understand various sections of **LABRIS UTM** appliance's home screen after the initial login.



1	Page Header	In this section, you will find links to LMC, Logview, Visibility, Wizard, Authentication and Settings
	Section	toggle, Help and Logout. Notice the right hand top corner for Help and Logout.
2	Main	After the initial login, you will be landed on to your Labris Security Gateway Software Dashboard.
	Dashboard	Main dashboard will show you System Information and various historical & real time statistics.
3	Navigation	You can navigate to various sections such as. In addition to these you will also find options to change
		your preferred language.

On Dashboard, You will find widgets such as **System Information**, **Network Interfaces**, **Resources**, **Protection Information**, **Application Data** and **Signature Databases**.



1	System	System Information field in the dashboard displays information on the <b>No.of users</b> ,
	Information	Host Name , Labris Version , System Time and Uptime
2	Resources	Resources field displays information on resources(Processors , Memory , Disk) and
		their utilization levels with diagrams which makes us to understand easily.
3	Signature	Signature Databases displays information which is related to the UTM device
	Databases	
4	Network Interfaces	Network Interfaces field displays information like Ip Address, NetMask, Status and
		Error Information. We can also find a chart which gives pictorical representation of
		the Ethernet utilization.
5	Accept-Deny Data	Accept-Deny Data witget summarizes Accepted and Denied traffics count by a single
		date from Firewall(Network) and Webfilter(Access) data.
6	Protection	Protection field displays information related to the virus / spams caught and also the
	Information	No.of websites blocked and Attacks prevented.
7	Application Data	Application Data widget shows a treemap graph for most used application along the
		whole network.

# How to Pop-in/out and Maximize/Minimize widgets on the Main Dashboard

You can pop-out/in and maximize/minimize these widgets on the main dashboard by clicking icons which, are shown as below based on your need.



# **Wizard Installation**

Installation wizard enables simple configuration of Labris UTM products by users in just a few steps. Installation wizard can be accessed via product's web interface. The wizard is fixed at the top right corner of the web interface.



#### **11.** How to use Wizard Installation?

The product configuration can be started by clicking the Wizard icon on the web interface. The product configuration can be made in five steps in total.

- 1. Hostname and Gateway Mode Configuration
  - a. Gateway Mode Network Configuration
    - i. Network Configuration for LAN or DMZ
      - 1. Network Configuration for HotSpot and Web Filter on the LAN or DMZ interface
    - ii. Network Configuration for IP Type DHCP
    - iii. Network Configuration for IP Type Static
    - iv. Network Configuration for IP Type PPPoE
  - b. DNS Configuration
  - c. DHCP Server Configuration
- 2. Hostname and Bridge Mode Configuration
  - a. Bridge Mode Network Configuration

#### 1. Hostname and Gateway Mode Configuration

Configure as Gateway if you want to use Labris UTM as

- A firewall or replace an existing Firewall
- A gateway for routing traffic
- Link load balancer and implement gateway failover functionality

Apart from configuration Gateway IP address (IP address through which all the traffic will be routed), you must also configure LAN and WAN IP addresses.

Internet		192.168.168.1	LAN Ne	twork
External Router 85.88.82.81	85-88-82-82 Datively Mode policies controlling traffic between LAN and WAN Network	Labris in Gateway Mode	197.168.168.100	Gateway Mt de polities controlling tat#fc between LAN and DNC Networks
		- 10.20.30.1	->r	z
			Web Server 10 20 30 3	MallServer 10.20.30.3

# Hostname and Working Mode;

Labris	Installation Wizard
Hostname and	Working Mode Configuration (1/4)
1 Hostname	2 Working Mode
slave	Gateway
6 jump to selected section Hostname Configuration Network Configuration Bridge Configuration DNS Configuration	3 K Back Next > Apply & Next 5
DHCP Server Configuration jump to selected section	

1	Hostname	Device Hostname
2	Working Mode	Select a Working Mode. Gateway or Bridge
3	Back	The Back Step Now
4	Next	The Next Step Now
5	Apply & Next	Apply Changes and goto Next Step
6	Jump to Selected Section	Connect The Desired Step

#### 12. A – Gateway Mode Network Configuration

This is the section where the hostname and working mode settings of the device can be made.

#### i - Network Configuration for LAN or DMZ;

#### Network Configuration - (eth2) (2/4)

1	Interfac	æ	2	Interface Ty	pe	3	Interface Name	4	NAT	
	eth:	۲		LAN	•		INSIDE			OFF

1	Interface	Select Interface
2	Interface Type	Select Network Type for WAN,LAN or DMZ
3	Interface Name	Name for Network
4	NAT	Network Address Translate ON or OFF

#### ii - Network Configuration for IP Type DHCP;

6 IP Type	7 IP Address	8 Netmask	9 Default Gateway
Dynamic (DH)	•		

6	IP Туре	Select IP Type for DHCP, Static or PPPoE
7	IP Address	IP Address for Network LAN,WAN or DMZ
8	Netmask	Netmask for Network LAN, WAN or DMZ
9	Default Gateway	Gateway for Network WAN

#### iii - Network Configuration for IP Type Static

Static <b>V</b> 192.168.168.1 255.255.0

6	IP Туре	Select IP Type for DHCP, Static or PPPoE
7	IP Address	IP Address for Network LAN,WAN or DMZ
8	Netmask	Netmask for Network LAN, WAN or DMZ
9	Default Gateway	Gateway for Network WAN

VLAN ID

11

10 vL	AN 11	VLAN ID		
10	VLAN		VLAN ON or OFF for Network	

# iv - Network Configuration for IP Type PPPoE

IP Type	7 IP Address	8 Netmask	🧕 Default Gateway
PPPoE T	<b>,</b>		
DSL Username	11 DSL Pas	ssword	12 Verify DSL Password

ID for VLAN

6	ІР Туре	Select IP Type for DHCP, Static or PPPoE	
7	IP Address	IP Address for Network LAN,WAN or DMZ	
8	Netmask	Netmask for Network LAN, WAN or DMZ	
9	Default Gateway	Gateway for Network WAN	
10	DSL Username	Username for DSL Authentication	
11	DSL Password	Password for DSL Authentication	
12	Verify DSL Password	Again Password for DSL Authentication	

# 1 - Network Configuration for HotSpot and Web Filter on the LAN or DMZ interface;

	14 WAUTH SSL Connection	ON
15 HTTP Filtering ON	16 HTTPS Filtering	ON

13	WAUTH	Wireless Authentication enable or disable for Network LAN or DMZ	
14	WAUTH SSL Connection	Connect with SSL on the WAUTH Management Page	
15	HTTP Filtering	Web Filtering enable or disable HTTP Protocol for Network LAN or	
10		Mah Filtering enable or dischle LITTPC Dretegel for Network LAN	
10	HTTPS Filtering	web Filtering enable of disable HTTPS Protocol for Network LAN	
		or DIVIZ	

#### **13. B - DNS Configuration**

This is the section where DNS IP address settings can be made.

	DNS Configurat	ion (3/4)
1 DNS 1 IP	DNS 2 IP	3 DNS 3 IP
192.168.168.10	8.8.8	4.4.2.2
1 Internal DNS Domain	Name <mark>5</mark> Tir	ne Zone

1	DNS 1 IP	First DNS Server for IP Address
2	DNS 2 IP	Second DNS Server for IP Address
3	DNS 3 IP	Third DNS Server for IP Address
4	Internal DNS Domain Name	Internal DNS Server Domain Name
5	Time Zone	Select a Time Zone

## 14. C - DHCP Configuration

This is the section where we can activate or deactivate DHCP server in which the interface and IP settings of the IP addresses to be distributed to our DHCP Local users, are made.

#### DHCP OFF

	DHCP Configuration (4/4)	
1 DHCP Server for LAN	2 DHCP Interface eth0	Y

1	DHCP Server for LAN	Select DHCP Server Active or Passive
2	DHCP Interface	Interface list for DHCP Server or Relay

#### DHCP ON

	DHCP C	onfiguration (4/4)	
DHCP Server for	LAN	2 DHCP Interface	
DHCP IP Start	4 DHCP IP End	5 DHCP Netmask	6 DHCP Gateway
192.168.168.50	192.168.168.254	255.255.255.0	192.168.168.1
DNS 1 IP		8 DNS 2 IP	

1	DHCP Server for LAN	Select DHCP Server Active or Passive
2	DHCP Interface	Select DHCP Interface
3	DHCP IP Start	DHCP IP Start Address
4	DHCP IP End	DHCP IP End Address
5	DHCP Netmask	Netmask for IP Address
6	DHCP Gateway	Gateway IP Address for Client s
7	DNS 1 IP	First DNS IP Address for Clients
8	DNS 2 IP	Second DNS IP Address for Clients

## 2. Hostname and Bridge Mode Configuration

Configure as Bridge if

- You have a private network behind an existing firewall or behind a router and you do not want to replace the firewall.
- You are already masquerading outgoing traffic.

Internet				
10.20.30.2			LAN Net	work
Controlling traffic between LAN and WAN set social	Labris	4LAN>	2	2
10.20.30.1	Labris in Bridge Mode		10.70.30.3	20.20.30.4

A - Bridge Mode Network Configuration

🔂 Labris	Installation Wizard
Hostname	e and Working Mode Configuration (1/4)
1 Hostname	2 Working Mode
slave	Bridge 🗸
	3 K Back Next > Apply & Next 5

1	Hostname	Device Hostname
2	Working Mode	Select a Working Mode. Gateway or Bridge
3	Back	The Back Step Now
4	Next	The Next Step Now
5	Apply & Next	Apply Changes and goto Next Step

Bridge Configuration (2/4)				
Bridge Name 1				
br0				
2 Left Bridge Interface	3 Right Bridge Interface			
etn2	▼ em3 ▼			
4 Bridge IP	5 Bridge Netmask			
192.168.168.2	255.255.255.0			
	6 Submit			

1	Bridge Name	Name for Bridge
2	Left Bridge Interface	Select Bridge Interface for Left
3	Right Bridge	Select Bridge Interface for Right
4	Bridge IP	Bridge IP for Management
5	Bridge Netmask	Bridge IP Netmask for Management
6	Submit	Apply Changes

# Accessing LABRIS UTM through LMC

Click on LMC tab (Labris Management Console) from the Dashboard.

≡	👤 Management Console	🎽 LOGVIEW	VISIBILITY	
	System Information			Signature Database
	Hostname:	yssyk		Appcontrol Signature Co
Note	•LMC requires JAVA addon. While and security related information appropriate	e opening the LMC, yo n. Please accept the inj	u will be offered certi formation and procee	fcate d as

After all the validation and verification, the following LMC screen appears.



Now, we are ready to get connected to our appliance for further activities.

## **LMC Interface**

This is the default LMC interface we get when we connect to the Labris Management Console



In Labris Management Console we will find three sections.

Section 1	Menu Tab	Menu Tab is a horizontal strip that contains lists of available menus
Section 2	Module	<b>Module Tab</b> consists of three short cut icons for Change view, Add module, Delete Module
Section 3	Server List	Server List consists of list of servers added to LMC

#### Menu

A **Menu Tab** is a region of a screen or application interface where drop down menus are displayed. A **Menu tab** is an integral graphical user interface (GUI) component in LMC.

In Menu Tab we will find Device, File Menu, Edit Menu, View Menu and About Menu.



#### Brief Summary about each of the parameters in Menu tab:

1	Device	<b>Device</b> helps to manage the server with different options
2	File Menu	<b>File Menu</b> offers commands for closing windows and exiting the current program. It contains commands relating to the handling of files, such as New, open, save, exit
3	Edit Menu	<b>Edit Menu</b> consists of LMC options and Certificates. We can manage Certificates by using this Menu
4	View Menu	<b>View Menu</b> provides two different options like Sort and GUI templates to view the content in different modes
5	About	About Menu gives information about LMC

#### File Menu

File Menu enables us to connect to new LMC, Open a file, save a file and Exit from the LMC

Under File Menu we find the following options

1	New	This option enables to connect to the New LMC
2	Open	This option enables to open an existing document which is located in the local machine
3	Save	This option enables to save the contents of a Files
4	Exit	This option enables to close and exit from the LMC

#### To open New Labris management console

- 1. Go to File>New
- 2. **New** Options helps us to connect to the **New** Labris Management Console (LMC). When we click on New the following screen appears.

Lab	ris Manag	ement	Con	sole
Device	File Edi	t Vie	-w	About
	Now Al	-N		
688	Open Al	-0	Ŀ	
🖃 🔡 D	Save Al			
<u> </u>	Save A	- 4	000	
	EXIT AI	ны а	gem	ent
	🎽 Syste	em		

## Opening an existing file using LMC

- 1. Go to File>Open
- 2. Using **Open** option we can open an existing file in LMC



3. Browse the path of the file, Select the File and click Ok



#### Saving the files in LMC

1. Go to File>Save



2. Using Save option we can save the files in LMC

#### **Exiting from LMC console**

- 1. Go to File>Exit
- 2. When we click on Exit it prompts us with a message "Do you really want to exit?"
- 3. Click on "Yes" to exit, or click on "No" to remain in the same LMC



#### **Edit Menu**

**Edit Menu** helps us to manage LMC options like change of Language (English & Turkish), settings etc. Certificate details can also be viewed and managed from Edit Menu

Under Edit Menu we find the following options

1	Options	This option helps us manage LMC options
2	Certificates	This option helps us to View details and manage certificates in LMC

#### **Editing options in LMC**

1. Go to Edit>Options

2. Using **Options** we can view settings and select interface language in LMC and click **"Ok"** to apply settings.

1	View settings	View Settings consists of show button bar and open module list on start. Choose appropriate option	
2	Language	This option enables us to choose preferred	
	options	language either English or Turkish	
3	ОК	Select <b>OK</b> to apply the settings	
4	Cancel	Select Cancel if we don't want to apply these	
		settings	
5	Help	Help options gives the related information	
		about LMC options. It provides online help.	



LMC Options	×
View Settings	
Open recent module list on start	
Language Options	
Interface Language English	-
Türkçe	
Ok K Cancel	elp 🕑

#### **Certificates details in LMC**

- 1. Go to Edit>Certificates
- 2. When we click on **"Certificates"** the Certificate manager console gets opened, where we can manage the Certificate using options like Delete, View Details, Close, Help

🛒 Labris Management Console								
<u>D</u> evice <u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>A</u> bout					
	Options Alt-O							
9 <b>00</b>	Certificates Alt-C							
🖃 📲 🕻 Device l	ist							
ē- 📃 10.11.12.221:4000								
🎂 User Management								
	System							

Certificate Manager			
You have trusted to the following of	certificates:		
Certificate Name	Subject (CN)	Exp	pires on
78.188.50.48.static.ttnet.com.tr	labris.security.gateway	Tue Nov 20 17:1	12:23 IST 2018

3. If we want to view the certificate details click on "**View Details**". A screen appears as below with all necessary details of the certificate

1	Delete	Delete options helps us to delete the				
		selected certificate from LMC				
2	Close	Close option helps us to close the				
		Certificate manager window				
3	Help	Help Options gives information about the				
		certificates and its related options				

Certificate Details	×
Certificate: 78.188.	50.48.static.ttnet.com.tr
Subject	
Name:	labris.security.gateway
Organization:	Labris Teknoloji
Organization Unit:	RaD
Country:	TR
State:	ANK
Issuer	
Name:	labris.security.gateway
Organization:	Labris Teknoloji
Organization Unit:	RaD
Country:	TR
State:	ANK
Serial:	d96e87f2b466f601
View Public Key	Cancel

1	View public Key	This option helps us to view the public key
2	Cancel	This option helps us to close the Certificate details window

#### View Menu

**View Menu** is one of the option in Menu Tab. **View Menu** helps us to view the contents in different modes depending on the options available in LMC.

#### Under View Menu we find the following options

1	Sort	This option helps to sort by server or
		module
2	<b>GUI Templates</b>	This option helps to change the view of
		LMC to Aero mode or MacWin mode

#### Sorting Labris management console

1. Go to View>Sort> By Server

Labris Management Console								
<u>D</u> evice <u>F</u> ile <u>E</u> dit	<u>V</u> iew <u>A</u>	bout						
	Sort	Þ	By Server	Alt-S				
4 <b>66</b> 🚞	GUI Tem	GUI Templates  By Module Alt-M						
🖃 🔠 Module								
🗄 🆄 User Management								
🗄 🚔 System								

2. When we sort **By Module** the view of the LMC appears as below



- 1. Go to View>Sort> BY Module
- 2. When we sort by module the view of the LMC changes as below

🔣 Labris Management Console									
Device	e <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>A</u> bout								
	•	Sort 🕨			By Server Alt-S				
4 <b>86</b>	GUI Templates 🕨 By Module Alt-M								
🖻 – 🎫 Mo	🖃 🍔 Module								
÷ *									

View using GUI Templates option in Aero Mode

- 1. Go to View>GUI Templates> Aero
- 2. When we click on Aero the view of the LMC appears as below

🔢 Labris Management Console							
Device File	<u>E</u> dit	<u>V</u> iew	<u>A</u> bou	t	_		
<b>1</b> 5		Sort		- ▶	]		
9 <b>00</b>	GUI Templates 🕨 Aero						
					MacWin		

#### View using GUI Templates option in MacWin Mode

- 1. Go to View>GUI Templates>MacWin
- 2. When we click on MacWin the view of the LMC appears as below

🙀 Labris Management Console								
<u>D</u> evice	<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>A</u> bo	ut		_	
<b>1</b>			Sort			١,		
9 <b>00</b>	GUI Templates 🕨 Aero							
	odule						MacWin	

#### **Device Menu**

**Device Menu** provides us with different options like Add, Remove, Connect, Disconnect server from LMC. We can manage the server using the options in **Device Menu**
# Under Device Menu we find the following options

1	Add Server	This option helps to Add server to the LMC
2	Remove Server	This option helps us to <b>Remove server</b> from the LMC
3	Connect	This option helps to <b>Connect</b> the server to the LMC
4	Disconnect	This option helps to <b>Disconnect</b> the server from LMC

# Add Modules from Server Menu

To manage and configure the appliances we will add Server to the LMC.

1. Go to Device>Add server



#### Note

•We can even choose a short cut icon under Module to **Add server** 

After clicking on the "Add Server", you will see the "Add Devices from Server" menu. . Type in the appropriate Default Username and Default Password and click on "Authenticate" button.

Notice & verify your appliance's IP address in the **"Add Devices from Server"** menu and click on the **"Login"** button as shown below

E Labris Management Console		- @ ×
<u>D</u> evice <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>A</u> bout		<u>H</u> elp
Labris Management Console Device File Edit View About  Device List	Labris Management Console       ×         Please fill in the fields according to the device you want to connect.       IP       10.11.12.221         User Name admin       Password	- G X Help

2. After successful authentication process, you will notice your new appliance appearing on LMC's Server list as shown in the following images.



# **User Management**

User Management system providing administrators with the ability to effectively manage users on the network. It is an authentication feature that provides administrators with the ability to identify and control the state of users logged into the network.

It is not limited to, the ability to query and filter users that are currently logged into the network, but also manually log out users, and control users login counts and login times.



## Viewing Options in User Management

When we Right click on "User Management Tab" we find following options

1	Connect	It enables Users, Groups & WAUTH to connect to the LMC
2	Disconnect	It enables Users, Groups & WAUTH to disconnect from LMC
3	Properties	It helps us to view properties of User Management in LMC

## 15. Users

**Users Tab** in LMC enables us to **Add** new User, **Edit** existing Users, **Delete** User in User Management Section in LMC.

When we click on Users tab all the existing Users are displayed with fields User Name, Name Surname, Source, Domain, Global and Note

## **Adding User**

Add tab in user management helps us to Add a new user to the LMC Appliance

Click on Add tab to add a New User

Upers	Users Groups Identity Integration WAUTH Quota					
Select A	ll 🛛 🗶 Delete 🔒	ne Edit 🛛 🖗 Add				🔍 Filter
	User Name	Name Surname	Source	Domain	Global	Note
	testuser2745	testuser2745	ad	labristeknoloji.com	✓	<b></b>
	testuser7610	testuser7610	ad	labristeknoloji.com	✓	1
	testuser486	testuser486	ad	labristeknoloji.com	✓	
	testuser4500	testuser4500	ad	labristeknoloji.com	✓	
	testuser3983	testuser3983	ad	labristeknoloji.com	✓	
	testuser9446	testuser9446	ad	labristeknoloji.com	✓	
	testuser2633	testuser2633	ad	labristeknoloji.com	✓	
	testuser7236	testuser7236	ad	labristeknoloji.com	✓	
	testuser9795	testuser9795	ad	labristeknoloji.com	✓	
	testuser8720	testuser8720	ad	labristeknoloji.com	✓	
	testuser3928	testuser3928	ad	labristeknoloji.com	✓	
	testuser7577	testuser7577	ad	labristeknoloji.com	~	



These are the inputs for adding New User

1	User Name	Type the name of the new User
2	Name	Type the Surname of the new User
	Surname	
3	Password	Type Password of the new User s
4	Password	Re type the same Password for confirmation
	Again	
5	Domain	By default Slave is being selected in <b>Domain</b>
6	Global	It is deemed central management. In the case of the device is the same as the firm's global projects marking more than one user is deemed to be used every time a user was created in the location is achievable UTM device.
7	Comment	Type reason for the User creation (Optional)
8	Select Group	You can make a user, member of a group
9	Select Quota	You can choose a quota policy for user
	Policy	

Global, Comment and Select Group fields can be selected according to the User requirement and click on **OK** to apply these settings.

Labris Networks	×
Applying Changes	

Type the name of the User in the **Filter Tab** to check whether the user is added to the list or not. If the user is not added click on **Refresh Tab** 

ct All 📃 🔀 Delete 🛛	🥖 Edit 🛛 🍄 Add		Sample		🔍 Filter
User Name	Name Surname	Source	Domain	Global	Note
testuser9719	testuser9719	ad	labristeknoloji.com	✓	
testuser7551	testuser7551	ad	labristeknoloji.com	~	
testuser6672	testuser6672	ad	labristeknoloji.com	~	
testuser5467	testuser5467	ad	labristeknoloji.com	~	
testuser1557	testuser1557	ad	labristeknoloji.com	~	
testuser1603	testuser1603	ad	labristeknoloji.com	✓	
testuser3517	testuser3517	ad	labristeknoloji.com	~	
testuser8747	testuser8747	ad	labristeknoloji.com	✓	
testuser9532	testuser9532	ad	labristeknoloji.com	✓	
testuser3366	testuser3366	ad	labristeknoloji.com	✓	
testuser4218	testuser4218	ad	labristeknoloji.com	~	
testuser6691	testuser6691	ad	labristeknoloji.com	✓	
testuser5784	testuser5784	ad	labristeknoloji.com	✓	
testuser8734	testuser8734	ad	labristeknoloji.com	~	
testuser6082	testuser6082	ad	labristeknoloji.com	✓	
testuser8488	testuser8488	ad	labristeknoloji.com	~	
testuser495	testuser495	ad	labristeknoloji.com	~	
testuser9253	testuser9253	ad	labristeknoloji.com	✓	
testuser784	testuser784	ad	labristeknoloji.com	~	
testuser798	testuser798	ad	labristeknoloji.com	~	
testuser8208	testuser8208	ad	labristeknoloji.com	~	
testuser3693	testuser3693	ad	labristeknoloji.com	~	
testuser9527	testuser9527	ad	labristeknoloji.com	✓	
testuser9953	testuser9953	ad	labristeknoloji.com	~	
testuser8040	testuser8040	ad	labristeknoloji.com	✓	
testuser9778	testuser9778	ad	labristeknoloji.com	✓	
testuser4783	testuser4783	ad	labristeknoloji.com	✓	
testuser9494	testuser9494	ad	labristeknoloji.com	✓	
tt0040	tt0040		lele viete lue ele il e e es		

Below screen appears stating that it takes some time to Refresh, click **OK** to continue the **Refresh** process

Refresh	×
This will take some time depending on your user and group count, so it will run as a background process. Do you want to proce	ed ?

After completing Refresh process type the name of the User in the **Filter tab**, then you can notice the **New User** displaying in the User's list

U	sers	Groups Identity	Integration WAUT	H Quota			
Sele	ect Al	📃 🄀 Delete 🍃	🖊 Edit 🛛 🔮 Add	s	ample		🔍 Filter
		User Name	Name Surname 🔺	Source	Domain	Global	Note
		user2	labris	labris	localhost.localdom	~	sample
		Sample	Sample	labris	localhost.localdom	~	Sample note
		user3	labris	labris	localhost.localdom	✓	sample user
		userl	labris	labris	localhost.localdom	~	sample note

## **Deleting User**

**Delete** Tab in user management helps us to **delete** the **user** permanently from the LMC Appliance

Type the name of the User which you want to delete in the Filter tab, Select the User and click on **Delete Tab** 

Users	Groups Identit	y Integration 🏾 WAL	JTH Quota			
Select Al	l 📃 🔀 Delete	🥒 Edit 🛛 🍄 Add		Sample		🔍 Filter
	User Name 🔺	Name Surname	Source	Domain	Global	Note
~	Sample	Sample	labris	localhost.localdom	~	Sample note

Then the below screen appears, Click **OK** to delete a User in User Management in LMC



It takes some time to Delete an User from User's list



Below screen gives information that the selected User is deleted successfully. Click OK



Changing password / Editing User

Select a User from the User's list and click on

## Edit Tab

User	Groups Identit	ty Integration WA	UTH Quota				
Select A	All 📃 🔀 Delete	🧪 Edit 🛛 🍄 Add				🔍 Filter	
	User Name 🔻	Name Surname	Source	Domain	Global	Note	
	user3	labris	labris	localhost.localdo	✓	sample user	
	user2	labris	labris	localhost.localdo	✓	sample	
~	userl	labris	labris	localhost.localdo	~	sample note	
	testuser9999	testuser9999	ad	labristeknoloji.com	✓		
	testuser9998	testuser9998	ad	labristeknoloji.com	✓		
	testuser9997	testuser9997	ad	labristeknoloji.com	~		

Edit option helps us to change the password of the existing User and edit the comment.

Edit User	×
User Name	userl
Name Surname	labris
	4
Password	*****
Password Again	***** 2
Domain	localhost.localdomain 🔻
	✓ Global
Comment	sample note 3
<b>Q</b> uota Policy	sample_quota
	OK Cancel

1	Password	Type new Password of the User
2	Password Again	Re Type new Password again for confirmation
3	Comment	Type reason for the User creation (Optional)

Click **OK** to apply these settings.

Labris Networks	×
Applying Changes	

## 16. Groups

Groups permit us to easily assign to all members of a group abilities in a space that are specified to that Group. After creating a Group we are able to manage its membership by adding or deleting Users to that Group. All the created Users may be a member of any Group with Guest abilities. We can have same Users in multiple Groups.

**Groups Tab** in LMC enables us to **Add New Group**, **Edit existing Groups**, **Delete Groups** in User Management Section in LMC.

When we click on **Groups Tab** all the existing groups are displayed with the fields **Group Name**, **Source**, **Domain**.

Users Groups Identity Integration WAU	ITH Quota		
Select All 📃 🔀 Delete 🥒 Edit 🔮 Add		Silter	
Group Name	Source	Domain 🔻	
sample_group	labris	localhost.localdomain	
testgroup45	ad	labristeknoloji.com	
testgroup33	ad	labristeknoloji.com	
ras and ias servers	ad	labristeknoloji.com	

## **Adding Group**

Users Groups Identity Integration WA	UTH Quota		
Select All 📃 🔀 Delete 🥒 Edit 🙀 Add		🔍 Filter	
Group Name	Source	Domain 🔻	
sample_group	labris	localhost.localdomain	
testgroup45	ad	labristeknoloji.com	
testgroup33	ad	labristeknoloji.com	
ras and ias servers	ad	labristeknoloji.com	
incoming forest trust builders	ad	labristeknoloji.com	
testgroup46	ad	labristeknoloji.com	
enterprise admins	ad	labristeknoloji.com	
testgroup43	ad	labristeknoloji.com	

Click on Add Tab to add New Group to the Groups in User Management

Below screen appears with Group Name & Group Configuration.

Id Group Group Name	ars	omain · localho	st localdomain			Ousta Balia		
Group Configuration All Users and Group	s <mark>1</mark>	Grilte	r		Group Componer	nts <sup>1</sup> 2	sample_quota	
Name testuser2745 testuser7610 testuser486 testuser4500 testuser3983 testuser9446 testuser2633 testuser7236 testuser9795	Type user user user user user user user use	Source ad ad ad ad ad ad ad ad ad ad	Domain labristeknoloji labristeknoloji labristeknoloji labristeknoloji labristeknoloji labristeknoloji labristeknoloji labristeknoloji	3 > 4	Name	Туре	Source	Domain
testuser8720	user	ad	labristeknoloji 🔽	Ca	ncel			

# Group Name consists of two fields Group Name & Domain.

1	Group Name	Type name of the New Group
2	Domain	In this field <b>slave</b> is selected by default

# Group Configuration consists of two fields All Users and Groups and Group Components.

1	All Users and	All the users and groups are displayed in this
	Groups	field
2	Group	Users in specific Group are displayed in this
	Components	field
3	8	Click this icon to add Users in to Group
		Components

4

Click this icon to delete Users from the Group Components

Click **OK** to add New Group to the Group's list.

# It takes some time to apply changes.

Labris Networks	×
Applying Changes	

Type the **New Group name** in the **Filter tab** and click **Refresh** to find out the **New Group** in the **Group's** list is added or not.

lect All 📃 🔀 Delete 🥒 Edit 🔮 Add	sample_group	🔍 Filter
Group Name	Source	Domain 🔻
testgroup11	ad	labristeknoloji.com
testgroup12	ad	labristeknoloji.com
testgroup13	ad	labristeknoloji.com
testgroup14	ad	labristeknoloji.com
testgroup15	ad	labristeknoloji.com
testgroup16	ad	labristeknoloji.com
testgroup17	ad	labristeknoloji.com
testgroup18	ad	labristeknoloji.com
testgroup19	ad	labristeknoloji.com
testgroup2	ad	labristeknoloji.com
testgroup20	ad	labristeknoloji.com
testgroup21	ad	labristeknoloji.com
testgroup22	ad	labristeknoloji.com
testgroup23	ad	labristeknoloji.com
testgroup24	ad	labristeknoloji.com
testgroup25	ad	labristeknoloji.com
testgroup26	ad	labristeknoloji.com
testgroup27	ad	labristeknoloji.com
testgroup28	ad	labristeknoloji.com
testgroup29	ad	labristeknoloji.com
testgroup3	ad	labristeknoloji.com
testgroup30	ad	labristeknoloji.com
testgroup31	ad	labristeknoloji.com
testgroup32	ad	labristeknoloji.com
testgroup33	ad	labristeknoloji.com
testgroup34	ad	labristeknoloji.com
testgroup35	ad	labristeknoloji.com
testgroup36	ad	labristeknoloji.com

Now you can notice the **newly added Group** in the **Group's** list. Right click on the **Group** and select **Show Group**.

User	Users Groups Identity Integration WAUTH Quota							
Select /	All 📃 🔀 Delete 🥒 Edit 🛛 👙 Add				🔍 Fi	lter		
	Group Name		Source		Domain 🔻			
	sample_group		labris		localhost.localdomain			
	windows authorization access group	Show Group	ad		labristeknoloji.com			
	users testgroup99		ad		labristeknoloji.com			
			ad		labristeknoloji.com			
	testgroup98		ad		labristeknoloji.com			

When you click on **Show Group**, Users in that **group** are displayed. Click **OK** to close the current tab.

sample_group			×			
Name	Туре	Source	Domain			
testuser2745	user	ad	labristeknoloji			
testuser486	user	ad	labristeknoloji			
testuser7610	user	ad	labristeknoloji			
testuser4500	user	ad	labristeknoloji			
Sample	user	labris	localhost.local			
userl	user	labris	localhost.local			
user2	user	labris	localhost.local			
OK						

### **Deleting Group**

Select the Group from the Group's list and click on **Delete** Tab.

Users	Groups Identity Integration WAU	ITH Quota		
Select A	All 📃 🔀 Delete 🧪 Edit 🔮 Add		A Filter	
	Group Name	Source	Domain 🔻	
✓	test_group	labris	localhost.localdomain	•
	sample_group	labris	localhost.localdomain	
	testgroup45	ad	labristeknoloji.com	
	testgroup33	ad	labristeknoloji.com	

Warning screen is displayed; Click **OK** to delete a Group from the LMC.



Deleting process is in progress.

Labris Networks	×
Selected groups are being deleted	

Below screen appears stating that the selected Group is **Deleted** successfully & click **OK** to close the current tab



# **Editing Group**

Select the Group which you want to edit from the list and click on Edit Tab.

User	s Groups Identity Integration WAU	TH Quota							
Select A	Select All 📃 🔀 Delete 🥜 Edit 🔮 Add								
	Group Name	Source	Domain 🔻						
~	sample_group	labris	localhost.localdomain						
	windows authorization access group	ad	labristeknoloji.com						
	users	ad	labristeknoloji.com						
	testgroup99	ad	labristeknoloji.com						
	testgroup98	ad	labristeknoloji.com						
	testgroup97	ad	labristeknoloji.com						

Select the User from the **Group** components list and click on the **icon 1**to remove User from the **Group** Components and click **OK** 

Select the **User** from All Users and **Groups** field and click on the **icon 2** to add Users in to Group Components list and click **OK** 

roup Name : samp	le_group	Domain :	localhost.localdomair	n	-	📃 Quota Pol	icy sample_qu	ota
oup Configuration								
Users and Groups	5				Group Components			
		🔍 Filter					🔍 Filter	
Name	Type	Source	Domain	4	Name	Type	Source	Domain
testuser2745	user	ad	labristeknoloji 🔺	2	testuser2745	user	ad	labristeknoloji
testuser7610	user	ad	labristeknoloji		testuser486	user	ad	labristeknoloji.
testuser486	user	ad	labristeknoloji	>	testuser7610	user	ad	labristeknoloji.
testuser4500	user	ad	labristeknoloji		testuser4500	user	ad	labristeknoloji.
testuser3983	user	ad	labristeknoloji		Sample	user	labris	localhost.local
testuser9446	user	ad	labristeknoloji	_	userl	user	labris	localhost.local
testuser2633	user	ad	labristeknoloji	<	user2	user	labris	localhost.local
testuser7236	user	ad	labristeknoloji					
testuser9795	user	ad	labristeknoloji	1				
testuser8720	user	ad	labristeknoloji 🔻					

It takes some time to apply the changes.



# To notice changes made to the Group right click on the User and select Show Group

Users Groups Identity Integration WAUTH Quota							
Select A	Select All 📃 🔀 Delete 🥜 Edit 🔮 Add 🖉 🖓 Filter						
	Group Name		Source	Domain 🔻			
	sample_group		labris	localhost.localdomain			
	windows authorization access group		ad	labristeknoloji.com			
	users		ad	labristeknoloji.com			
	testgroup99		ad	labristeknoloji.com			
	testgroup98		ad	labristeknoloji.com			

Then information about **Group** Components are displayed and click **OK** to close the current tab.

5	sample_group 🗙								
	Name	Туре	Source	Domain					
	testuser2745	user	ad	labristeknoloji					
	testuser486	user	ad	labristeknoloji					
	testuser7610	user	ad	labristeknoloji					
	testuser4500	user	ad	labristeknoloji					
	Sample	user	labris	localhost.local					
	userl	user	labris	localhost.local					
	user2	user	labris	localhost.local					
	OK								

# **17. Identity Integration**

**Identity Integration Tab** in LMC enables us to **Add** new Identity, **Edit** existing Identities, **Delete** Identity in User Management Section in LMC.

When we click on Identity Integration tab all the existing Identity Integrations are displayed with fields **Name, Domain Name, Hostname, Server IP, Type.** 

Users	Groups	Identity Inte	gration	WAUTH	Quota			
[Identity Inte	egration							
👙 Add	🥖 Edit	🔀 Delete						 
	Name	E	Domain Na	me	Hostname		Server IP	Туре
a	d_name_4	e	example.co	m	host.example.com	n	192.168.0.1	AD_LDAP
a	d_name_3	e	example.co	m	host.example.com	n	192.168.0.1	AD_LDAP
a	d_name_2	e	example.co	m	host.example.com	n	192.168.0.1	AD_LDAP
a	d_name_1	e	example.co	m	host.example.com	n	192.168.0.1	AD_LDAP
	labris	labr	risteknoloj	i.com	develad.labristeknolo	oji.c	192.168.0.89	AD_LDAP

# **Adding Identity**

Add tab in identity integration helps us to Add a new integration to the LMC Appliance

Click on **Add tab** to add a New Identity Integration.

Users Groups Ideni	iliy Integration WAUTI	H Quota						
Identity Integration								
🚰 Add 🥒 Edit 🛛 🗶 D	elete							
Name	Domain Name	Hostname	Server IP	Туре				
ad_name_4	example.com	host.example.com	192.168.0.1	AD_LDAP				
ad_name_3	example.com	host.example.com	192.168.0.1	AD_LDAP				
ad_name_2	example.com	host.example.com	192.168.0.1	AD_LDAP				
ad_name_1	example.com	host.example.com	192.168.0.1	AD_LDAP				
labris	labristeknoloji.com	develad.labristeknoloji.c	192.168.0.89	AD_LDAP				

You can type credentials and test without integration using **Test** button below.

Integration - Add 🗙
1 Name*: example_name
2 Type*: AD_LDAP ▼
Configuration
Domain Name*: example.com 3
Hostname*: test.example.com 4
Server IP*: 192.168.0.1 5
Workgroup*: EXAMPLE 6
Authentication
User*: Administrator 7
Password*: 8
Advanced
Search Base : OU=Unit 10
Filter: CN=testaroup
"*" areas must be filled. 🦉 Test 🗳 Add 🗶 Cancel

These are the inputs for New Integration:

1	Name	Unique name for integration			
2	Туре	Server configuration type			
3	Domain Name	Domain Name			
4	Hostname	Hostname of Server			
5	Server IP	IP Address of Server			
6	Workgroup	Workgroup of User			
7	User	Username			
8	Password	Password			
9	Port	Connection port			
10	Search Base	Starting point for the search instead of the default			
11	Filter	Conditions for entries			

If credentials are correct, you can see queried users. Using **Filter** button, you can filter queried users.

Authentication is successful		×
	Filte	r
Name	Туре	
testuser3542	user	•
testuser6031	user	
testuser1565	user	
testuser1564	user	
testuser1567	user	
testuser1566	user	
testuser1561	user	
testuser1560	user	
testuser1563	user	
testuser1562	user	•
	ΟΚ	

After writing necessary configurations, you can add integration with the **Add** button below.

Integration - Add	×
Name*:	example_name
Type*:	AD_LDAP
Configuration	
Domain Name* :	example.com
Hostname* :	test.example.com
Server IP* :	192.168.0.1
Workgroup*:	EXAMPLE
Authentication	
User* :	Administrator
Password*:	••••••
Advanced	
Port :	389
Search Base :	OU=Unit
Filter :	CN=testgroup
"*" areas must be	filled. 🦉 Test 🚰 Add 🔀 Cancel

# **Editing Identity**

A previously added Integration can be edited by choosing it and clicking the Edit Button.

	Users Crews a lide att		Quete							
	Osers Groups Identi	y integration WAUTH	Quota							
Ē	Identity Integration									
	A									
	🖓 Add 🧹 Edit 💢 De	ete								
	Name	Domain Name	Hostname	Server IP	Type					
	Nume	Domain Name	Hostifulie	Screet II	Type					
	ad_name_4	example.com	host.example.com	192.168.0.1	AD_LDAP					
	example name	example.com	test.example.com	192.168.0.1	AD LDAP					
	ad name 2	ovemple.com	hast overnle com	102169.01						
	au_name_z	example.com	noscexample.com	192.100.0.1	AD_LDAF					
	ad_name_1	example.com	host.example.com	192.168.0.1	AD_LDAP					
	labris	labristeknoloji.com	develad.labristeknoloji.com	192.168.0.89	AD LDAP					

## **Deleting Identity**

Select the Integration from the Integrations list and click on **Delete** Tab.

Users Groups Identity Integration WAUTH Quota										
Identity Integration										
🖆 Add 🥜 Edit 🔀 Delete										
Name	Domain Name	Hostname	Server IP	Туре						
ad_name_4	ad_name_4 example.com		192.168.0.1	AD_LDAP						
example_name	example.com	test.example.com	192.168.0.1	AD_LDAP						
ad_name_2	example.com	host.example.com	192.168.0.1	AD_LDAP						
ad_name_1	example.com	host.example.com	192.168.0.1	AD_LDAP						
labris	labristeknoloji.com	develad.labristeknoloji.com	192.168.0.89	AD_LDAP						

Warning will be shown after clicking delete button.



If you press **OK** progress bar will be shown. This might take some time.



# **Advanced Options for Identity Integration**

Advanced	
Port :	ol
Search Base :	OU=Ankara, OU=İstanbul
Filter :	memberOf=CN=testgroup,OU=test,DC=domain,DC=com

**Port:** Port number between 0-65535 which will be used to connect to the server. Default value is 0 which is actually translated into default port of Server.

**Search base:** The starting point for the search of the users and groups. If it is empty, default search base which consists of domain name will be used. If not, it is concatenated to the default search base.

For example if "OU=Ankara" is written on the search base and domain name is "example.com", it will be translated into "OU=Ankara, DC=example, DC=com".

**Filter:** Conditions for searching users and groups which should conform to the string representation for search filters as defined in RFC 4515.

For example: "&(objectClass=Person)(primaryGroupId=513)".

## **Other Options in User Management**

Right click on the User Management and select Properties.



All the properties of the module are displayed in this screen. Click **Close** to move out of this tab.

Give right click on the **User Management** Tab and select **Disconnect** to disconnect from the **User Management**.

🗽 Labris Management Console								
<u>D</u> evice	<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>A</u> bout				
5 <b>8</b> 🖻 💻								
🖃 🍔 Mo	dule							
🛨 ··· 🌺	Use	r Mana	gement	Connect				
💷 🗄 🖓 🎽	Syst	em		Disconnect				
🕀 🛄 Network Settings			Disconnect					
🕀 😫 Firewall				Properties				
i <u>i</u>	VPN							

M	Module Properties					
	Propertie	5	1			
	Server:	8.static.ttnet.com.tr:4000				
	Module:	users				
	Status:	<ul> <li>Connected</li> </ul>				
		Close	3			

# WAUTH

WAuth is the module used for user authentication and guest authentication. WAuth is enabled by interface and supports specific exceptions.

WAuth (Wireless Authentication) in LMC enables us to Add New WAuth Interface, Edit existing WAuth Interface, and Delete WAuth Interface in User Management Section in LMC.

Your device configuration for WAUTH

# First Step:

Add a separate Network for WAuth in the Network settings module. Select Network settings for selected interface.

Choose the interface you want to choose for enabling WAuth.

🔢 Labris Management Console						
<u>File E</u> dit <u>V</u> iew <u>M</u> odule <u>A</u> bout	:					
Par 💼 💼	IP Configurat	ion Routing				
Server	Interfaces					
78,188.50.48;4000	Active	Device	Name	Туре	IP	
🚽 🖄 User Management	~	tun0		Tunnel	10.8.3.1	
System	<b>~</b>	eth0		Ethernet	169.254.1.1	
Eirowall	~	eth1	OUTSIDE	Ethernet	10.11.14.221	
VPN	~	eth2	INSIDE	Ethernet	192.168.20.1	
- AL Filter	~	eth3	WAUTH	Ethernet	10.1.0.1	
Antispam/Antivirus		eth4	OUTSIDE2	Ethernet	10.11.12.231	
IDS/IPS	~	eth5	INSIDE2	Ethernet	192.168.168.1	
Server						
Load Balancer						
- & License						

• Edit Interface IP address or Name;

Ethernet Properties 🗙 🗙							
📃 Use dynamic IP	configuration						
Static IP Configuratio	n	_					
Name	Name WAUTH						
IP Address	10.1.0.1						
Mask	255.255.255.0						
Save Apply Cancel							

### Second Step:

Create a DHCP Server for WAUTH;

Click for DHCP configuration.

# Third Step:

Create a **Network object** in firewall for WAUTH host and **Network** WAUTH\_Net. (For Creating Network Object, please refer to **Hosts** under Network Objects section in Make a new Firewall object)

😸 🗶 🖉	Policy	🛃 Obje	ct	Insert Rule		Install		Connections	14	IP-MAC	Matcher	E:
Server	onfiguration	NenFiremalOb	ect						-			-
Islave:4000 Ser Management	Objects	No.	Source	Destination	S	ervice	Action	Schedule	QoS/Ban.	. Applications	Securi	Optio
System	Hosts	0		🗅 Any	🗅 Алу		O Accept	🗅 Any	🗅 Any	🗅 Any	🗅 Any	80
Firewall     Filter     Antispam/Antivirus     DiSIPS     Messaging     Server     Load Balancer	NewHostsObject     NewHostsObject     Survey     WaldTH     WebServer     Networks     Standard     User Defined	1		🗅 Any	https http pop3 smtp WewServi	iceGroup_DNS	Accept	🗅 Any	🗅 Any	🗅 Any	🗅 Any	Bđ
→ Server Load Balancer → Ucense	Address Ranges Address Ranges Object Groups Services Services ObS & DoS QoS/Bandwidth Schedule Application Control Schedule											

# Fourth Step:

Add a policy (For Creating a **new policy** firewall object please refer to **Labris Firewall Management**)



## Fifth Step:

Enable Wauth for the selected interface by configuring in interface WAUTH tab in Firewall module.



## Sixth Step:

Add a user for WAUTH.

Click for User Management.

# Configuring WAUTH policy

Click on Add Tab to add Interface to the WAUTH in User Management.

Users Groups WAUTH									
Select All 📃 🔀 Delete 🥜 Edit 🙀 Add 🗲									
	Name	IP/IP - Range / MAC ad	Interface	Policy	Statement	State			
	Wa	10.0.0.1	eth0	Require Authentication		Active			
	Wauthinterface1	169.254.1.2	eth0	Require Authentication	new Wauth interface to	Active			
	WAUTH Interface	10.1.0.1	eth3	Require Authentication		Active			

Below screen appears.

Authentication Policy	×
Active 1	
Policy   Require Authentication  Doesn't Require Authentication	
Interface eth0(169.254.1.1)	
Name Wauthinterface1 4	
Type IP Adress 5	
IP Adress 169.254.1.2 6	
Statement new Wauth interface to the LMC 7	כ
OK Cancel	

These are the inputs for the **Authentication Policy**.

1	Active	Enable this option to activate the interface
2	Policy	Choose required Policy
3	Interface	Choose interface from the drop down list
4	Name	Type name of the Interface
5	Туре	Choose type of Interface from drop down list
6	IP Address	Give the IP Address
7	Statement	Type the Statement if any required (Optional)

Click Ok.

Notice Interface added to the **WAUTH** in the below screen.

	Users Groups WAUTH									
Select All 📃 🔀 Delete 🥜 Edit 🍦 Add							🔍 Filter			
		Name	IP/IP - Range / MAC ad	Interface	Policy	Statement	State			
		Wa	10.0.0.1	eth0	Require Authentication		Active			
		Wauthinterface1	169.254.1.2	eth0	Require Authentication	new Wauth interface to	Active			
		Wauthinterface2	169.254.1.1	eth0	Require Authentication		Active			
		WAUTH Interface	10.1.0.1	eth3	Require Authentication		Active			

# **Deleting WAUTH policy**

Select the Interface from the WAUTH list and click on Delete Tab

	Users Groups WAUTH									
Select All 📃 🔀 Delete 🥒 Edit 🔮 Add										
		Name 🔺	IP/IP - Range / MAC ad	Interface	Policy	Statement	State			
		Wa	10.0.0.1	eth0	Require Authentication		Active			
		WAUTH Interface	10.1.0.1	eth3	Require Authentication		Active			
		Wauthinterface1	169.254.1.2	eth0	Require Authentication	new Wauth interface to	Active			
	<ul> <li>Image: A second s</li></ul>	Wauthinterface2	169.254.1.1	eth0	Require Authentication		Active			

Warning screen is displayed, Click **OK** to delete the Interface

	×
2	Selected rules will be deleted. Are you sure?

Deleting process is in progress.

Labris Networks	×
Selected users are being deleted	

Below screen appears stating that **Deleted** successfully & click **OK** to close the current tab.



## **Editing WAUTH Policy**

Select the **Group** which you want to edit from the list and click on **Edit Tab**.

Users	Users Groups WAUTH					
Select All	I 📃 🔀 Delete 🍃	🖻 Edit 🛛 😤 Add				🔍 Filter
	Name	IP/IP - Range / MAC ad	Interface	Policy	Statement	State
	W	192.168.0.1	eth0	Require Authentication		Active
-	Wauthinterface1	169.254.0.1	eth0	Require Authentication	new WAuth interface in	Active
	WAUTH Interface	10.1.0.1	eth3	Require Authentication		Active

We can edit any of the fields in the Authentication policy.

Authentication Policy	×
Active	
Policy   Require Authentication  Doesn't Require Authentication	
Interface eth3(10.1.0.1)	
Name Wauthinterface1	
Type IP Adress	
IP Adress 169.254.0.1	
Statement new WAuth interface in User management section	
OK Cancel	

Click Ok.

## Adding WAUTH Authentication and User

Click on WAUTH tab from the dashboard and select Settings

#### **Subnet Rules**

Select **Subnet Rules** tab to view and change Subnet Rule specific settings. You can use subnet rules to enable/disable specific settings for specific networks. To illustrate, your internal network may not offer any sign up methods in Wauth Welcome screen but your guest network may offer TCKN Sign Up method. You can also set how the login screen should look using for different networks (different Company Logo's etc.). Combined with Access Control List (ACL) you can allow only specific users/groups to login from your internal network.

**Note:** Subnet independent configurations (like Hotel and AD configuration). Should be made on **Default** subnet rule.

Subnet Rules - Adding New Subnet Rule

Settings - Default					
Setting Rule:	Default 🔺				
	۹				
Subnet Rules	Default	ACL	TCKN Wauth		
	Add new rule				
Subnet list: 0.0.0/0.0.0					
Save					

# Subnet Rules - Editing Subnet Rule

Settings - subnet-b	based-rule 2
Setting Rule:	subnet-based-rule 2
Subnet Rules	General UI ACL
	Rule name: subnet-based-rule 2 2
	Subnet list: 192.168.0.0/255.255.255. 3
	0
	Save 4 Delete 5

1	Setting Rule	Current subnet rule choice. This affects all configuration data in
		all tabs (General, UI, ACL)
2	Rule Name	Name of this subnet rule
3	Subnet List	Comma separated list of networks that this subnet rule should
		apply to.
4	Save	Save changes to subnet rule.
5	Delete	Delete this subnet rule.
		Warning: This also deletes all configuration choices for this rule
		on other tabs (General, UI, TCKN, SMS, ACL etc.)

# Subnet Rules - Default

Default subnet rule can't be deleted and its networks can't be edited. This ensures that if no other subnet rules matches the user, **Default** subnet rule will be applied for user.

Settings - Default					
Setting Rule:	Default	w			
Subnet Rules	General	UI	ACL	TCKN Wauth	
	Rule name: Defa	ault			
	Subnet list: 0.0	.0.0/0.0.0.0			
	Save				
					)

# **General Settings**

Select General tab to view and change the General settings.

Authentication methods in WAUTH is configured in General tab.

# Common Key:

Common key provides an effective mechanism to prevent unauthorized users from registering. During registration, user must provide the common key if authentication method requires it.

Example scenario:

TCKN Wauth with common key (Assuming TCKN Wauth is already configured)

- In General tab;
  - $\circ$   $\;$  Set CK Option to Manual.
  - Set Common Key to the desired value.
  - $\circ \quad \text{Click Save.}$
- In TCKN Wauth tab:
  - o Activate common key

You can also set CK Option to Automatic and provide a CK period. If you do this, common key will be changed at the end of this period automatically.

If you want unauthorized users (users who cannot login to web admin panel) to view common key, you can set a username and password for this.

• Set CK Username and CK Password values.

- For wauth listening ip 192.168.0.1, as unauthorized user go to: 192.168.0.1:85/wauth/show\_ck/
- Enter values from CK Username and CK Password.
- Current common key will be shown.

**Important Note:** Common keys are different for each subnet rule. If you have multiple subnet rules, you should provide matching subnet rule's CK Username and CK Password. Otherwise you will get an error.

#### **Network Authentication System**





These are the inputs for the General Settings.

1	Welcome message	Welcome message is displayed in Turkish	
2	Welcome message (EN)	Welcome message is displayed in English	
3	Local Authent format	Choose Authentication format from the drop down list	
4	SMS Wauth	We can enable or disable this option	
5	Active Directory Authent	We can enable or disable this option	
6	Hotel Integration	We can enable or disable this option	
7	TC Identity NVI	We can enable or disable option	
	Confirmation		
8	Passport Wauth	We can enable or disable option	
9	Agreement	We can enable or disable this option	
10	Agreement [TR]	This option displays information regarding agreement in Turkish.	
11	Agreement (EN)	This option displays information regarding agreement in english	
12	Time out	We can enable or disable this option	
13	Time period	Mention time period in minutes	
14	Authentication Type	Choose Authentication type from the drop down list	
15	Ingress session	We can enable or disable this option	
16	Reference Emails/Domains	We can add or delete reference emails/domains from this field	
17	Reference Timeout	We can set reference email timeout (seconds)	
18	Smtp Server Address	We can set smtp server address	
19	Smtp Mode	We can choose smtp mode (TLS, SSL, Normal)	
20	Smtp Port	We can set port number for smtp protocol	
21	Smtp Username	We can set username for smtp server	

22	Smtp Password	We can set password for smtp server	
23	Smtp Mail From	We can set mail from field in sent mail	
24	CK Option	Common key will be set manually or generated automatically.	
25	CK Period	Common key regeneration period when common key is	
		generated automatically.	
26	Common Key	Current common key (will be regenerated on save if it's	
		automatically generated)	
27	CK Username	Username to get current common key for unprivileged user	
28	CK Password	Password to get current common key for unprivileged user	
29	CK Instructions	Instructions to show user on sign-up screen.	
30	CK Instructions (EN)	Instructions to show user on sign-up screen (english)	

## Click on Save to save the changes

## **Settings of Hotel Authentication**

### Select Hotel tab



These are the inputs for the Hotel Authentication.

1	Default	Select User Group
2	Hotel Name	Type the Name of the Hotel
3	Product type	Choose product type
4	MAC Address	Type MAC Address (optional)

-		
5	Machine Port	Type Machine port (optional)
6	Real Name	Type the name of the Database
7	Real Name	Type the name of the table (optional)
8	User Name	Type the Username
9	Password	Type the password
10	User Name Field Name	Type Username Field Name (optional)
11	Password Field Name	Type Password Field Name (optional)
12	Name Field Name	Type Name of the Field Name (optional)
13	Surname Field Name	Type Surname of the Field Name (optional)
14	Departure Date	Mention Departure Date (optional)
15	Timeout	Mention Timeout in minutes
16	Infinite timeout	We can enable or disable this option
17	Multiple Login	We can enable or disable this option

Click on Test to test the details and then select **save** to save the changes

# **Settings of SMS Authentication**

# Select SMS Authentication

These are the inputs for the SMS Authentication.

Subnet Rules	General	SMSWauth	UI	ACL	TCKN Wauth	Passport
	Default Group:	Default 🔹 📘				
	Multiple Login:	2				
	Account Quota:	1440	(mins)			
Accou	nt Expiration Date:	24	(hours)			
	Timeout:	1440	(mins) 5			
	Cust. Serv. Tel:	111111111	6			
	Comp. Mobile*** :	1111111111	7			
[	Cust. Serv. Email:	example@labrisnetwor	ks.coi			
Help page for SI	IS authentication:	9				
Title of SMS authen	ication help page:	Labris Networks	10			
Subtitle of SMS a	uthentication help page:	Wauth Ağ Yetkilendirm	e Sist			
Message of SMS a	uthentication help page:	Giriş için Kullanıcı adı <b>Şifrem Var</b> bu girip internette gezinm  cliriş bilgileriniz y butonuna basarak cep SMS ile giriş bilgilerini 	ve sifreniz var ise tonuna basıp bilgiler eye başlayabilirsiniz ok ise <b>Şifrem Yo telefonu numaranız alabilir ve bu bilgiler neye başlayabilirsini</b>	inizi k ı girip, le giriş z.		
Ena	ble Common Key: 📱	<mark>∕</mark> 13				
SMS sending will	be afforded by the company*:	14				
Use	Custom SMS Api:	15				
R	emaneu roken**: 50		iguration 17			
	Buv	tokens 18				
	Sho	w Common Key	9			
	Save	20				

1	Default Group	Users authenticated with SMS will be a member of
		this group.
2	Multiple Login	SMS users will be allowed to login from different
		devices simultaneously.
3	Account Quota	Account Quota
4	Account Expr. Date	Users authenticated with SMS will be expired after
		this period of time.
5	Timeout	Mention Timeout Period
6	Cust. Serv. Tel	Type Customer Service Telephone number
7	Comp. Mobile	Type Company Mobile Name
8	Cust. Serv. Email	Type Customer Service Email address
9	Help page for SMS	Show a help page to user for SMS authentication.
	authentication	
10	Title of SMS auth. help	Title of SMS authentication help page
	page	
11	Subtitle of SMS auth.	Subtitle of SMS authentication help page
	help page	
12	Message of SMS auth.	Message to show in SMS authentication help page
	help page	
13	Enable Common Key	Require common key for new user sign-up.

14	SMS sending will be	Cost of SMS sending will be afforded by the host.
	afforded by the company	
15	Use Custom SMS Api	Use another SMS sending API. You need to configure
		this API via "Custom SMS Service Configuration"
		button
16	Remained Token	If SMS sending cost will be afforded by company and
		custom SMS API isn't used, these tokens will be used
		for new registrations.
17	Custom SMS Service	Configure custom (third-part) SMS service API.
	Configuration	
18	Buy Tokens	Open token purchase page.
19	Show Common Key	Show common key query webpage.
20	Save	Save changes

Click on **Buy tokens** and select **Save** to save the changes.

# **Active Directory Authentication**

Select AD (Active Directory tab)

Domain name and authenticating account information configuration is done in this tab.

Settings				
General	Hotel	SMSWauth	AD	UI
	AD Domain Name:		1	
[	Disable Group Name:	2		
	AD Workgroup:		3	
	AD Group Name:		4	
	Timeout: Unlin	nited (f	nours) <mark>5</mark>	
	Infinite timeout: 🔽	6		
	AD Quota: Unlin	nited ()	nours) 7	
	Infinite quota: 🔽	8		
	AD Expire After: Unlin	nited (P	nours) 🧕	
	Infinite Expr Time: 🔽	10		
	Test Save			

These are the inputs for Active directory Authentication.

1	AD Domain Name	Type Active Directory Domain Name
2	Disable Group Name	Choose this option to Disable Group Name
3	AD Work Group	Type Active Directory Work Group Name
4	AD Group Name	Type Active Directory Group Name
----	--------------------	---
5	AD Timeout	Mention Active Directory Timeout period
6	Infinite Timeout	We can enable or disable this option
7	AD Quota	Mention time period of Active Directory Quota
8	Infinite Quota	We can enable or disable this option
9	AD Expire Date	Mention time period of Active Directory Expire Date
10	Infinite Expr time	We can enable or disable this option

# **User Interface Customization**

Select UI (Active Directory tab)

UI tab is used for customization of guest and user welcome screens.

Logic Choose File No file chosen 1   Detete Logic 2   Logi URL: 3   Background image 5   Background image Position: Detault   Page Title: 8   Page Title: 8   Page Title: 10   Login Page Header: 11   Login Page Footer: 12   Login Page Footer: 13   Username Caption: 14   Username Caption: 16   Password Caption: 16   Password Caption: 16   Password Caption: 18   Login Button Caption: 19   Login Button Caption: 20   Login Button Caption: 21   Background Cotto: 23   aage Title Background Cotto: 23   Page Title: 24   Page Title: 25	et Rules	General	U	A	CL			
Delete Logo: 2   Logo URL: 3   Background image: 5   Background image Position: Default •   Page Title: 8   Page Title: 8   Page Title: 9   Login Page Header: 10   Login Page Footer: 12   Login Page Footer: 13   Username Caption: 14   Username Caption: 16   Password Caption: 16   Password Caption: 16   Password Caption: 16   Password Caption: 18   Login Button Caption: 19   Login Button Caption: 20   Login Button Caption: 21   Background Cotor: 23   aage Title Background Cotor: 23   aage Title Background Cotor: 25		Logo:	Choose File	No file chosen			1	
Logu URL: 3   Background Image: 5   Background Image Position: 0   Defete Background Image Position: 0   Default 6   ackground Image Repetition: 0   Page Title: 7   Page Title: 0   Ugin Page Header: 10   Login Page Header: 10   Login Page Footer: 12   Login Page Footer: 12   Username Caption: 14   Username Caption: 16   Password Caption: 16   Password Caption: 18   Login Button Caption: 18   Login Button Caption: 20   Login Button Caption: 21   Background Colir: 22   Headeer: 22   Headeer: 23		Delete Logo:	2					
Background Image: Choose File   Background Image 5   Background Image Position: Default   Cargonal mage Repetition: Default   Page Titte: 6   Page Titte: 0   Page Titte: 0   Cogin Page Header: 10   Login Page Header: 11   Login Page Footer: 12   Login Page Footer: 12   Username Caption: 14   Username Caption: 16   Password Caption: 16   Password Caption: 18   Login Buton Caption: 20   Login Buton Caption: 20   Login Buton Caption: 20   Login Buton Caption: 20   Login Buton Caption: 23   aad ground Coli: FFFFFF   22 Headerrotoric Tori Coli:   Wange Title Background Coli: EEEEE   24 25		Logo URL:			3			
Defete Background Image 5   Background Image Repetition: Default v   Page Tite: 8   Page Tite: (eng)   Login Page Header: 10   Login Page Header: 11   Login Page Header: 12   Login Page Footer: 12   Login Page Footer: 13   Username Caption: 14   Username Caption: 16   Password Caption: 18   Login Button Caption: 19   Login Button Caption: 20   Login Button Caption: 21	Ba	ackground Image:	Choose File	No file chosen			4	
Background Image Position: Default v 6   ackground Image Repetition: Default v 7   Page Title: (eng) 9   Login Page Header: 10   Login Page Header: 11   Login Page Header: 12   Login Page Footer: 12   Login Page Footer: 13   Username Caption: 14   Username Caption: 16   Password Caption: 18   Login Button Caption: 19   Login Button Caption: 20   Background Color: EEEEE   22 Header:   Page Title Background Color: EEEEE   23 24	Delete Ba	ackground Image:	5					
ackground Image Repetition: Page Title: Page Title: Pa	Backgroun	d Image Position:	Default 🔻	6				
Page Title: 8   Page Title: 9   Login Page Header: 10   Login Page Header: 11   Login Page Header: 12   Login Page Footer: 12   Login Page Footer: 13   Username Caption: 14   Username Caption: 16   Password Caption: 16   Password Caption: 18   Login Button Caption: 18   Login Button Caption: 19   Login Button Caption: 19   Login Button Caption: 20   Loguin Button Caption: 21   Background Color: 22   Header/Footer Font Color: 23   Page Title Font Color: 25	Background	Image Repetition:	Default v	7				
Page Title:   Page Title:   Login Page Header:   Login Page Header:   Login Page Header:   Login Page Footer:   12   Login Page Footer:   12   Login Page Footer:   13   Username Caption:   14   Username Caption:   16   Password Caption:   18   Login Button Caption:   19   Login Button Caption:   20   Login Button Caption:   21   Backgroud Color:   FFFFF   22   Header/Footer Font Color:   205		Page Title:			0			
Login Page Header:       10         Login Page Header:       11         Login Page Header:       11         Login Page Footer:       12         Login Page Footer:       12         Login Page Footer:       13         Username Caption:       14         Username Caption:       16         Password Caption:       18         Login Button Caption:       20         Logint Button Caption:       20         Logint Button Caption:       20         Lagout Button Caption:       20         Lagout Button Caption:       21         Backgroud Color:       FFFFFF       22         Header/Footer Font Color:       00000       23         'age Title Background Color:       EEEEEE       24         Page Title Font Color:       BED128 </td <td></td> <td>Page Title:</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>		Page Title:						
Image: Control of the second secon	Lo	gin Page Header:			eng) 9			
Login Page Header:       11         Login Page Footer:       12         Login Page Footer:       12         Login Page Footer:       13         Username Caption:       14         Username Caption:       16         Password Caption:       18         Login Button Caption:       18         Login Button Caption:       18         Login Button Caption:       19         Login Button Caption:       20         Loguin Button Caption:       21         Backgroud Color:       FFFFFF       22         Header/Footer Font Color:       200         Page Title Background Color:       EEEEEE       24         Page Title Font Color:       BED12B       25		5			1.	10		
Login Page Header:   Login Page Footer:   12   Login Page Footer:   12   Login Page Footer:   13   Username Caption:   14   Username Caption:   16   Password Caption:   16   Password Caption:   18   Login Button Caption:   19   Logut Button Caption:   19   Logut Button Caption:   19   Logut Button Caption:   20   Logut Button Caption:   21   Backgroud Color:   FFFFFF   22   Header/Footer Font Color:   23   'age Title Background Color:   EEEEE   24   Page Title Font Color:   BELIZE						10		
Login Page Header:       11         Login Page Footer:       12         Login Page Footer:       12         Login Page Footer:       13         Username Caption:       14         Username Caption:       16         Password Caption:       18         Login Button Caption:       18         Login Button Caption:       18         Login Button Caption:       18         Login Button Caption:       20         Logout Button Caption:       20         Logout Button Caption:       21         Backgroud Color:       FFFFFF       22         Header/Footer Fort Color:       00000       23 <sup>3</sup> age Title Background Color:       BEELEEE       24         Page Title Fort Color:       BED12B       25								
Login Page Footer:       12         Login Page Footer:       12         Login Page Footer:       13         Username Caption:       14         Username Caption:       16         Password Caption:       16         Password Caption:       18         Login Button Caption:       18         Login Button Caption:       20         Logout Button Caption:       20         Logout Button Caption:       20         Logout Button Caption:       21         Backgroud Color:       FFFFFF       22         Header/Footer Font Color:       00000       23         'age Title Background Color:       EEEEE       24         Page Title Font Color:       00000       23	Lo	gin Page Header:						
Login Page Footer:       12         Login Page Footer:       13         Login Page Footer:       13         Username Caption:       14         Username Caption:       16         Password Caption:       16         Password Caption:       18         Login Button Caption:       19         Logout Button Caption:       20         Page Title Backgroud Color:       FFFFFF         22       Header/Footer Font Color:       00000         Page Title Backgroud Color:       FEFEFF       22         Page Title Backgroud Color:       FEFEFE       24         Page Title Font Color:       00000       23         Page Title Font Color:       00000       23						1	1	
Login Page Footer:   Login Page Footer:   Login Page Footer:   Login Page Footer:   Username Caption:   14   Username Caption:   16   Password Caption:   16   Password Caption:   17   Login Button Caption:   18   Login Button Caption:   19   Logout Button Caption:   20   Logout Button Caption:   21   Backgroud Color:   FFFFFF   22   Header/Footer Font Color:   20   23   Page Title Background Color:   EEEEE   24   Page Title Font Color:   Botton:   25								
Login Page Footer:       12         Login Page Footer:       13         Login Page Footer:       13         Username Caption:       14         Username Caption:       14         Username Caption:       16         Password Caption:       18         Login Button Caption:       19         Logout Button Caption:       20         Logout Button Caption:       21         Backgroud Color:       FFFFFF       22         Header/Footer Font Color:       00000       23         Page Title Background Color:       BED12B       25					🧷 (eng	)		
Login Page Footer:       13         Login Page Footer:       13         Username Caption:       14         Username Caption:       16         Password Caption:       16         Password Caption:       18         Login Button Caption:       18         Login Button Caption:       20         Logut Button Caption:       20         Lagut Button Caption:       21         Backgroud Color:       FFFFFF       22         Header/Footer Font Color:       30000       23         'age Title Background Color:       BED12B       25	L	ogin Page Footer:				_		
Login Page Footer:       13         Username Caption:       14         Username Caption:       14         Username Caption:       16         Password Caption:       16         Password Caption:       18         Login Button Caption:       18         Login Button Caption:       20         Logout Button Caption:       20         Logout Button Caption:       20         Logout Button Caption:       20         Backgroud Color:       FFFFFF       22         Header/Footer Font Color:       00000       23         Page Title Background Color:       EEEEE       24         Page Title Font Color:       BED12B       25						12		
Login Page Footer:   Username Caption:   14   Username Caption:   (eng)   15   Password Caption:   16   Password Caption:   16   Password Caption:   17   Login Button Caption:   (eng)   17   Login Button Caption:   (eng)   19   Logout Button Caption:   (eng)   19   Logout Button Caption:   (eng)   20   Logout Button Caption:   (eng)   21   Backgroud Color:   FFFFF   22   Header/Footer Font Color:   20000   23   Page Title Background Color:   EEEEEE   24   Page Title Font Color:   BED12B   25								
Login Page Footer: 13   Username Caption: 14   Username Caption: 14   Username Caption: 15   Password Caption: 16   Password Caption: 16   Password Caption: 18   Login Button Caption: 18   Login Button Caption: 20   Logout Button Caption: 21   Backgroud Color: FEFFFF   22 23   Page Title Background Color: EEEEEE   24 25					4			
Image:	Lo	ogin Page Footer:				7		
Username Caption:       14         Username Caption:       14         Username Caption:       16         Password Caption:       16         Password Caption:       16         Login Button Caption:       18         Login Button Caption:       19         Logout Button Caption:       20         Page Title Background Color:       FFFFFF       22         Header/Footer Font Color:       000000       23         Page Title Font Color:       BED12B       25						1	<mark>3</mark>	
Username Caption: 14   Username Caption: 16   Password Caption: 16   Password Caption: 16   Password Caption: 17   Login Button Caption: 18   Login Button Caption: 19   Logout Button Caption: 20   Page Title Background Color: FEFFFF   24 25								
Username Caption: 14   Username Caption: (eng)   Password Caption: 16   Password Caption: (eng)   Login Button Caption: 18   Login Button Caption: (eng)   Logout Button Caption: 20   Logout Button Caption: (eng)   Backgroud Color: FFFFFF   22   Header/Footer Font Color: 00000   23   Page Title Background Color: EEEEEE   24 25					🧷 (eng	)		
Username Caption: (eng) 15   Password Caption: 16   Password Caption: (eng) 17   Login Button Caption: 18   Logout Button Caption: (eng) 19   Logout Button Caption: 20   Logout Button Caption: (eng) 21   Backgroud Color: FFFFFF 22   Header/Footer Font Color: 00000 23   Page Title Background Color: EEEEE 24   Page Title Font Color: BED12B 25	U	sername Caption:			14			
Password Caption:       16         Password Caption:       (eng)         Login Button Caption:       18         Login Button Caption:       (eng)         Logout Button Caption:       20         Logout Button Caption:       (eng)         Backgroud Color:       FFFFFF         Backgroud Color:       FFFFFF         Page Title Background Color:       EEEEEE         Page Title Font Color:       BED12B         Description:       25	U	sername Caption:			eng) <mark>1</mark>	5		
Password Caption:       (eng)       17         Login Button Caption:       18         Login Button Caption:       (eng)       19         Logout Button Caption:       20         Logout Button Caption:       (eng)       21         Backgroud Color:       FFFFFF       22         Header/Footer Font Color:       000000       23         Page Title Background Color:       EEEEEE       24         Page Title Font Color:       BED12B       25	P	assword Caption:			16			
Login Button Caption:       18         Login Button Caption:       (eng)         Logout Button Caption:       20         Logout Button Caption:       (eng)         Backgroud Color:       FFFFFF         Backgroud Color:       FFFFFF         Page Title Background Color:       EEEEEE         Page Title Font Color:       BED12B         Description       25	Р	assword Caption:		(	eng) <mark>1</mark>	.7		
Login Button Caption:       (eng)       19         Logout Button Caption:       20         Logout Button Caption:       (eng)       21         Backgroud Color:       FFFFFF       22         Header/Footer Font Color:       000000       23         Page Title Background Color:       EEEEEE       24         Page Title Font Color:       BED12B       25	Logi	n Button Caption:			18			
Logout Button Caption:       20         Logout Button Caption:       (eng)       21         Backgroud Color:       FFFFFF       22         Header/Footer Font Color:       000000       23         Page Title Background Color:       EEEEEE       24         Page Title Font Color:       BED12B       25	Logi	n Button Caption:		(	eng)	19		
Logout Button Caption:       (eng)       21         Backgroud Color:       FFFFFF       22         Header/Footer Font Color:       000000       23         Page Title Background Color:       EEEEEE       24         Page Title Font Color:       BED12B       25	Logou	It Button Caption:			20	<u>- 1</u>		
Backgroud Color: FFFFF       22         Header/Footer Font Color: 000000       23         Page Title Background Color: EEEEE       24         Page Title Font Color: BED12B       25	Logou	It Button Caption:			eng)	21		
Header/Footer Font Color:       000000       23         Page Title Background Color:       EEEEEE       24         Page Title Font Color:       BED12B       25		Backgroud Color:	FFFFF		22			
Page Title Background Color: EEEEEE 24 Page Title Font Color: BED128 25	Header/F	ooter Font Color:	000000		23			
Page Title Font Color: BED12B	Page Title B	ackground Color:	EEEEE		24			
	Page	e Title Font Color:	BED12B		25			

٢S

1	Logo	Add a company logo
2	Delete Logo	Delete default logo
3	Logo URL	Add a company logo on the web
4	Background Image	Add a image for background
5	Delete Background Image	Delete default background image
6	Background Image Position	Select position for background image
7	Background Image Repetition	Select repetition for background image
8	Page Title	Page Title Instructions is displayed in Turkish
9	Page Title-Eng	Page Title Instructions is displayed in English
10	Login Page Header	Login Page Header Instructions is displayed in Turkish
11	Login Page Header-Eng	Login Page Header Instructions is displayed in English
12	Login Page Footer	Login Page Footer Instructions is displayed in Turkish
13	Login Page Footer-Eng	Login Page Footer Instructions is displayed in English
14	Username Caption	Username Instructions is displayed in Turkish
15	Username Caption-Eng	Username Instructions is displayed in English
16	Password Caption	Password Instructions is displayed in Turkish
17	Password Caption-Eng	Password Instructions is displayed in English
18	Login Button Caption	Login Button Caption Instructions is displayed in Turkish
19	Login Button Caption-Eng	Login Button Caption Instructions is displayed in English
20	Logout Button Caption	Logout Button Caption Instructions is displayed in Turkish
21	Logout Button Caption- Eng	Logout Button Caption Instructions is displayed in English
22	Background Color	Select Background
23	Header/Footer Font Color	Select Header/Footer font color
24	Page Title Background Color	Select Page Title background color
25	Page Title Font Color	Select Page Title font color
26	Default Domain Choice	Select default domain choice for login screen

# **Turkish Citizen ID Number Authentication**

Select TCKN Wauth tab (Turkish Citizen ID Number Tab)

You can set configuration options for Turkish Citizen ID Number authentication method in this tab.

Subnet Rules	General	SMSWauth	UI	ACL	TCKN Wauth	Passport
	Default Group: Def	fault 🔻 📘				
	Multiple Login:	2				
	Infinite Quota:	3				
	Account Quota: 144	40	(mins) 4			
	Infinite Account:	5				
	Timeout: 144	40	(mins) 6			
Accourt	t Expiration Date: 24		(hours) 7			
	Cust. Serv. Tel: 111	1111111	8			
(	Cust. Serv. Email: exa	ample@labrisnetworks	.coi <mark>9</mark>			
Re	ference Approval: 📃	10				
Reque	est Mobil Number: 📃	11				
Use GSM Numb	per for Username: 📃	12				
Send Pas	sword With SMS:	13				
Enal	ble Common Key: 🕑	14				
	Show C Save	Common Key 15				

1	Default Group	Users signed up with this method will be a member of this group			
2	Multiple Login	TCKN users will be allowed to login from different devices			
		simultaneously.			
3	Infinite Quota	We can set enable or disable infinite quota			
4	Account Quota	We can set time quota for user			
5	Infinite Account	We can set enable or disable infinite account time			
6	Timeout	We can set time for login time			
7	Account Expiration Date	Users authenticated with SMS will be expired after this period of			
		time.			
8	Cust. Serv. Tel	Type customer service telephone number			
9	Cust. Serv. Mail	Type customer service mail			
10	Reference Approval	We can enable or disable reference approval			
11	Request Mobile Number	We can require user's gsm no with this field.			
12	Use GSM Number for	Checking this option will generate username from gsm no			
	Username	(instead of TCKN)			
13	Send Password With SMS	Activating this will generate a random password for user and			
		send it to user's mobile phone.			
14	Enable Common Key	Require Common Key for new users.			
15	Show Common Key	Show common key query webpage.			
16	Save	Save changes.			

# Passport Number Authentication

Select Passport Wauth tab (Turkish Citizen ID Number Tab)

You can set configuration options for Passport Number authentication method in this tab.

Subnet Rules	General	SMSWauth	UI	ACL	TCKN Wauth	Passport
	Default Group: Def	efault 👻 <mark>1</mark>				
	Multiple Login:	2				
	Infinite Quota: 📃	<mark>.</mark> 3				
	Account Quota: 14	140	(mins) 4			
	Infinite Account:	5				
	Timeout: 14	140	(mins) 6			
Accou	nt Expiration Date: 24	ļ	(hours) 7			
	Cust. Serv. Tel: 11	11111111	8			
[	Cust. Serv. Email: ex	ample@labrisnetworks	.coi <b>9</b>			
Re	eference Approval: 📃	10				
Requ	est Mobil Number: 📃	11				
Use GSM Num	ber for Username: 📃	12				
Send Pa	ssword With SMS:	13				
Ena	able Common Key: 🕑	14				
	Show Save	 Сотто Кеу 15 16	-			

1	Default Group	Users signed up with this method will be a member of this group.			
2	Multiple Login	Passport users will be allowed to login from different devices			
		simultaneously.			
3	Infinite Quota	We can enable or disable infinite quota			
4	Account Quota	We can set time quota for user			
5	Infinite Account	We can set enable or disable infinite account time			
6	Timeout	We can set time for login time			
7	Account Expiration Date	Users authenticated with SMS will be expired after this period of			
		time.			
8	Cust. Serv. Tel	Type customer service telephone number			
9	Cust. Serv. Mail	Type customer service mail			
10	Reference Approval	We can enable or disable reference approval			
11	Request Mobile Number	We can require user's gsm no with this field.			
12	Use GSM Number for	Checking this option will generate username from GSM No			
	Username	(instead of Passport No)			
13	Send Password With SMS	Activating this will generate a random password for user and			
		send it to user's mobile phone.			
14	Enable Common Key	Require Common Key for new users.			
20	Show Common Key	Show common key query webpage.			
21	Save	Save changes.			

# **Access Control List**

Subnet Rules	General	UI	ACL	
	IP Addresses:			
	1			
	<b>–</b>			
	Rule choice:			
	2	<ul> <li>Only allow given</li> <li>Deny given IPs,u</li> </ul>	IPs,users and groups sers and groups	
	Select Members:	N	lembers	All Users
		Filter		Filter
				* testuser3129@labristeknoloji.com
				testuser2754@labristeknoloji.com
	3			testuser7327@labristeknoloji.com
				testuser5861@labristeknoloji.com
				testuser7071@labristeknoloji.com
				testuser2547@labristeknoloji.com
				testuser9728@labristeknoloji.com
				↓ testuser7669@labristeknoloji.com
			Remove Member	rs Add Members «Prev Next»
	Select Groups:	Mem	ber Groups	All Groups
		Filter		Filter
				testgroup98@labristeknoloji.com
	4			testgroup78@labristeknoloji.com
				testgroup66@labristeknoloji.com
				testgroup70@labristeknoloji.com
				testgroup51@labristeknoloji.com
				testgroup29@labristeknoloji.com
				hasanlar@u9
				✓ enterprise admins@labristeknoloji.com
			Remove Group	ps Add Groups «Prev Next»

1	Ip Addresses Comma separated list of ips	
2	2 Rule choice Allow or deny these ip's, users and groups	
3	3 Select Members Choose users to apply this rule	
4	Select Member Groups	Choose groups to apply this rule

## **Creating WAUTH User**

User for WAUTH may be created in two ways. First is LMC. Local users can be created in LMC User Management module and directly be used in Wauth. Second is Wauth web based simple management screens. By Wauth web screen, one can create Wauth users.

Create User
Username: TestUser
Domain: slave V
Group: Default V
Real Name: Labris Test User 4
Expiration Date: Date: 2014-04-30 Today
Time: 12:00:00 Now
Quota (min): 6
Infinite quota: 🔽 🔽
MAC Address(Optional): 112233445566 × 8
Allow Multiple Logins: 🔽 9
Notes: Labris Test User
10
Password: •••••• 11
Create User

Select WAUTH tab from the dashboard and click on Create User tab

These are the inputs to Create User.

1	User Name	Type name of the User		
2	Domain	Choose Domain Name		
3	Group	Select Group for User		
4	Real Name	Type Real Name of the User		
5	Expiration Date	Select Expiration Date and Time of the User		
6	Quota	Mention Quota		
7	Infinite Quota	We can enable or disable this option		
8	MAC Address	Type MAC Address (optional)		
	(optional)			
9	Allow multiple Logins	We can enable or disable this option		
10	Notes	Type any notes regarding User (optional)		
11	Password	Type Password of the User		

#### **Online Users**

IP/MAC addresses and login time information is shown in Online Users screen. Also, this screen provides a function to disconnect the user.

0	nline Users	8					
l	Username	Name Surname	IP	MAC	Login Time	Quota (min)	Action
3	salih@slave	Salih Ucpinar	10.1.0.110	b8:6b:23:93:94:13	April 22, 2014, 10:52 a.m.	Unlimited	Disconnect

# All Users (User editing)

It is the screen that showing all users and information of users. Editing is easily done by clicking and opening Edit User window.

Note: If a user is online and his account is deleted, the user will be disconnected.

All Users Search Results										
User Name	Real Name	Account Expiration Date	Expired In	Creation Time	MAC Address	Multiple Login	Quota (min)	Notes	User Name	Transaction
Salih@slave	Salih Ucpinar	Unlimited	Unlimited	April 9, 2014, 6:41 p.m.		Active	Unlimited minutes		Local	Delete Edit

This edit window can also be used for just password changing without any account information editing. If you do not touch any field other than password, no other information will be changed except for password. In the same way, this editing window may be used for prolonging account lifetime.



1	User Name	Show Username
2	Real Name	Edit Real Name
3	Expiration DateEdit Expiration Date and Time of the User	
4	MAC Address	Edit MAC Address
5	Allow Multiple Login	We can enable or disable this option
6	Quota Edit Mention Quota	
7	Infinite Quota	We can enable or disable this option
8	Notes	Type any notes regarding User (optional)
9	Password	Change User Password

### WAUTH Welcome Screen

The guest or user is expected to authenticate him/herself to the system with given credential information, credential information they get through SMS messages, TCKN, Passport authentication.

Also, the system provides function for authenticating users of Active Directory with their AD credentials.

After account creation, user is expected to open an internet browser and will be welcomed with a welcome screen. Guest or user should enter the credentials on this stage.

This welcome screen can be shown in different languages according to internet browser's language settings.

For obtaining passwords, please follow next parts of the document.

Lapris Wauth Network Authentication System		n
	Sign In	1
1	Usemanie	-
1	Password	ĺ
L Domair u81	Password :	i 
L Dmair u81	Password Password v Password Login	

1	User Name	Username Input
2	Password	Password Input
3	Domain Select Domain Local or Domain Control	
4	Login	Login Button
5	Sign Up	Alternative Sign-up Methods
6	Reset Password	Reset forgot password

Alternative Sign Up Methods



1	SMS Sign Up	Sign up using mobile number	
2	TCKN Sign Up	Sign up using your TC Identity Number	
3	Passport Sign Up	Sign Up using passport number	

### 18. Login

Post-entry Screen



1	Logout	Logout Button
2	Change Password	Change Password Button

# **19. Change User Password**

User can change his password with "Change Password" button and Change Password window shown.

Change Password	
Current password	1
New password	2
Verify password	3
Confirmation	
Back	

1	Current Password	User Old Password
2	New Password	User New Password
3	Verify Password	New Password Again

### 20. Reset Password

Users who signed up with TCKN or Passport Number may reset their forgot passport.

### **Reset Password - Personal Info Validation Step**

In this step, user provides the same information during sign up. This fields will be checked against the previous information of user and if they match, user will be allowed to reset their password.



1	Name	First Name
2	Surname	Last Name
3	Year of Birth	Year of birth
4	E-Mail	E-Mail
5	TC Identity Code	TC Identity Number

Reset Password - Set new password step



1	New Password	New password for user
2	Confirm Password	Confirm new password for user

### **Reset Password - Password Changed Screen**

After completing all steps user will see the screen below.



# 21.

# SMS Sign Up

### 22. Registering with SMS

Click to "Obtain Password" button. If SMS authentication is disabled, obtain password choice will not be shown. For enabling SMS authentication, enable SMS Wauth in Wauth General Settings tab.

### GSM number and common key

Common key is a security solution for preventing unwanted guests to use the corporation's wifi guest internet access. This common key is enabled and set in SMSWauth screen. If CK is enabled, guest is wanted to enter it.



1	Mobile Number	Mobile Telephone Number
2	Common Key	Company Common Key

# 23. TCKN Sign Up

Users may sign up using their TC Identity Number. Validity of user-provided information (TC Identity Code, Name, Surname, Year of Birth) is checked against the records.

Net	Labris Wauth work Authentication S	<b>System</b>
1	TC Identity Code	1
0	Name	2
0	Surname	3
©	Year of Birth	4
۵	Mobile Number	5
1	Reference Mail	6
	Common Key	7
	Sign Up	
	Back	
	Customer Services Phone: 3122101490 E-Mail: support@labrisnetworks.com	

1	TC Identity Code	TC Identity Number of user
2	Name	Name of new user
3	Surname	Surname of new user
4	Year of Birth	Year of birth
5	Mobile Number	Only visible if <b>Request Mobile Number</b> is activated. Will be used for
		sending password via sms if <b>Send Password with Sms</b> is activated.
6	Reference Mail	Mail of the person who will approve this new user. This fields is visible
		if <b>Reference Approval</b> is activated. Reference mail should be one of
		the mails or member of a domain configured in General Settings-
		>Reference Emails/Domains.
7	Common Key	We can fill common key

# 24. Passport Sign Up

Users may sign up using their Passport Number.

Labris Wauth Network Authentication System									
1	Passport Number	1							
0	Name	2							
0	Surname	3							
©	Year of Birth	4							
۵	Mobile Number	5							
1	Reference Mail	6							
۵	Common Key	7							
	Sign Up								
	Back								
	Customer Services Phone: E-Mail:								

1	Passport Number	Passport number of new user.
2	Name	Name of new user
3	Surname	Surname of new user
4	Year of Birth	Year of birth
5	Mobile Number	Only visible if <b>Request Mobile Number</b> is activated. Will be used for
		sending password via sms if Send Password with Sms is activated.
6	Reference Mail	Mail of the person who will approve this new user. This fields is visible
		if <b>Reference Approval</b> is activated. Reference mail should be one of
		the mails or member of a domain configured in General Settings-
		>Reference Emails/Domains.
7	Common Key	We can fill common key

# 25.Quota

Labris UTM can measure internet usage of users in terms of byte count and elapsed time. This functionality is provided by Quota module. In this section, all information required to configure quota settings and monitor quota usage of users is provided. Quota module measures all the traffic which passes over Labris UTM. This means if you have multiple internal networks, you can measure and limit traffic between internal networks also.

#### Terminology

In order to simplify configuration and enable advanced configuration options, administrator can define Quota Policies and Quota Exceptions and use any combination of them for different users or groups.

### **Quota Policy**

A Quota Policy is a set of rules which defines how much a user or members of a group can use the internet in a period.

**Period:** Defines when the usages will be cleared. In other words, it defines when the quota will be renewed. It's useful if you want to set the limits daily, weekly, monthly, yearly. If you don't want quota to reset and define final limits in the policy, you can choose non-periodic.

Note: Periods are completed at the end of specified unit. For example, if a new policy is created with 1 Month period on 15<sup>th</sup> November, usage will be reset on 30<sup>th</sup> November, not on 15<sup>th</sup> December.

**Surfing Time:** It allows limiting the quota by time. Time limit allows measuring surfing time of user and set limit for them. Surfing time is not measured directly, instead calculated by counting transferred bytes in the last minute. If user transferred at least 100 KB in the last minute, it is passed for a minute usage. This means minimum unit for surfing time is minute and for example ten seconds of usage may be calculated as one-minute usage.

If period is set, this usage will be reset at the end of period.

Data Quota: Download and upload limits can be defined here.

Quota Exception: Multiple Quota Exceptions can be attached to the policy. Order is important.

#### **Quota Exception**

A Quota Exception is a rule to measure a specific usage pattern and define limit for this pattern. For example, you may have a generic quota policy with 5 GB download limit. If you have an ftp server outside of your internal network or in a separate network (e.g. DMZ) you may want to set a separate limit for transfers between users and ftp server. In this case you need to define an exception an attach this exception to your quota policy.

**Destination IP:** Set the destination IP address for this exception. You may also specify a network in the CIDR form (e.g. 10.0.0.0/16).

**Destination Port:** Set the destination port for this exception. You may specify a single port here. Different use cases are possible here. For example, you may skip defining destination IP and set

destination port as 22. This allows all SSH traffic to match this exception regardless of the destination IP address.

Day of Week Range: Set a filter for week range.

**Time Range:** Set when the exception will match during day. Again, different use cases are possible here. For example, you may want that FTP exception match only during work hours. In this case, you can set Day of Week Range to Monday-Friday and Time Range to 08:00:00-17:00:00.

### Creating a Simple Quota Policy with Single Quota Exception

This is a simple scenario with general 5 GB download limit, 20 GB download exception for SSH and 20 GB upload exception for SSH. SSH exception is defined for work hours. Both policy period and SSH exception period are set to one month.

#### **Quota Policy Creation**

This is the main screen of quota. By default, Quota Policies screen is open. You can add new policy, edit or delete existing policies here. Right sidebar allows hopping to other screens: Quota Exceptions, Quota Monitoring.

Note: Do not forget pressing Save after adding/editing/deleting. Otherwise your changes will be lost.

🔢 Labris Management Con	sole						- 🗆 🗙
<u>D</u> evice <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>A</u> bou	t						<u>H</u> elp
	Users Groups	Identity Integrat	ion WAUTH	juota			
🖃 📳 Device List	Quota Policy Object 2	3					Queta 🌣
· ■ 10.100.0.3:4000		Delete	Tuno	Deried	Data Quata	Time Quete	4 <u> </u>
System		Name	Туре	Penod	Data Quota		Quota Policies
Network Settings	A	B	C	D	E	F	Quota Monitoring
VPN							0
🐴 Filter							
IDS/IPS							
Server							
Load Balancer							
on License							
					<mark>7</mark>		
						🔊 Refresh	
Lmc server address you are	connected to is: 1	10.100.0.3					Labris Teknoloji

No	Name	Description				
1	Add Policy	Create a new quota policy				
2	Edit Policy	Edit an existing quota policy				
3	Delete Policies	Delete existing quota policy				
4	4 Quota Policies Open Quota Policies screen					
5	5 Quota Exceptions Open Quota Exceptions screen					
6	6 Quota Monitoring Open Quota Monitoring screen					
7	Refresh	Refresh policies exceptions and monitoring data (unsaved changes will be lost)				
8	Save	Save Quota Policies to UTM. Omitting save step will cause changes to be lost				
А	Rule No	Number of quota policy				
В	Name	Name of quota policy				
С	Туре	Periodic or non-periodic				
D	Period	Show if policy is periodic				
Е	Data Quota	Show data quota of policy				
F	Time Quota	Show time quota of policy				

🛃 Labris Management Console	- 🗆 X
Device <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>A</u> bout	Help
📲 📄 💽 Us Add Quota Policy 🗙	
Image: Second	Save       Quota *         Ie Quota       Quota Policies         Quota Exceptions       Quota Monitoring
Lmc server address you are connected to is: 10.100.0.3	Labris Teknoloji

No	Name	Description
1	Policy Name	Name of the policy. This name will be used when assigning to
		users/groups.
2	Periodic	Usage will be zeroed at the end of period.
3	Non-periodic	Usage will not be reset. Limits are final.
4	Period count	Period count.
5	Period unit	Possible values are: Day, Week, Month, Year
6	Unlimited surfing time	Don't set a limit for surfing time. Disables Hours and Minutes fields.
7	Surfing Time Hour Limit	Set how many hours a user is allowed to surf. Combination with minutes field is possible.
8	Surfing Time Minute Limit	Set how many minutes a user is allowed to surf. Combination with hours field is possible.
9	Quota Download Limit	Set how many megabytes a user is allowed to download.
10	Unlimited Quota Download	Don't set a limit for download.
11	Quota Upload Limit	Set how many megabytes a user is allowed to upload.
12	Unlimited Quota Upload	Don't set a limit for upload.
13	Attach New Exception	Attach an existing quota exception to this policy.
14	Remove an Exception	Remove an already attached quota exception from this policy.
15	Move chosen exception up	Move attached exception up in the order.
16	Move chosen exception down	Move attached exception down in the order.
17	Add	Complete policy creation
18	Cancel	Cancel policy creation

### **Quota Exception Creation**

This is Quota Exceptions screen. Don't forget pressing save after exception create/edit/delete.



🛃 Labris Management Console	- 🗆 X
Device Eile Edit View About	Help
📲 🖻 JAdd Quota Object 🗙	
Image: Status Control Status Contrel Status Contrel Status Contrel Status Contro	Save me Quota     Quota Policies Quota Exceptions Quota Monitoring     Save     Refresh
Lmc server address you are connected to is: 10.100.0.3	Labris Teknoloji

No	Name	Description
1	Exception Name	Name of the exception. This name will be used when attaching
		exception to a policy.
2	Periodic	Usage will be zeroed at the end of period.
3	Non-periodic	Usage will not be reset. Limits are final.
4	Period count	Period count.
5	Period unit	Possible values are: Day, Week, Month, Year.
6	Destination IP/Net	Destination IP Address or Network (CIDR) for this exception.
7	Destination Port	Destination port for this exception (only one port).
8	Day of Week Range	Which days this exception will match.
9	Time Range	Which hours this exception will match.
10	Surfing time	Set time limits for this exception.
11	Download Limit	Set download limit for this exception.
12	Upload Limit	Set upload limit for this exception.
13	Add	Complete exception creation.
14	Cancel	Cancel exception creation.



🔢 Labris Management Cons	ole	_	-				- 🗆 ×
<u>D</u> evice <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>A</u> bout							<u>H</u> elp
	Users Groups	Identity Integra	ation WAUTH	Quota			
🖃 📳 Device List	Quota Policy Object	📽 Delete					Quota 🌼
10.100.0.3:4000	Rule No	Name	Type	Period	Data Ouota	Time Ouota	Queta Relicion
System	1	5GB_Limit	Periodic	1 month	DL: 5120MB, UL:	Unlimited	Quota Exceptions
Firewall							Quota Monitoring
VPN							
Antispam/Antivirus							
Messaging							
Load Balancer							
® License							
4							
×							
						Refresh	
Lmc server address you are	connected to is: 1	0.100.0.3					Labris Teknoloji
📴 Labris Management Cons	sole						- 🗆 X
Device <u>File</u> <u>E</u> dit <u>V</u> iew <u>A</u> bout						_	<u>H</u> elp
		olicy				×	
Device List     Device List	General Setting	js D. I. Jacob				📙 Save	Quota 🕆
Southanagement	Name : 5G	B_LIMIt				ne Quota	Quota Policies
Network Settings	Type: •	Periodic 🔘 Non	periodic			hlimited	Quota Exceptions
Firewall	Period : 1	Month	-				quota rioniconing
Filter	Time Quota			Data Quota			
IDS/IPS	Surfing Time	· Vinlimited		Download : 5120	MB Unlimiter		
Server :	Suming mile			Download . Direc		<b>'</b>	
Load Balancer		Hours :		Upload :	MB 🔽 Unlimited	ł	
:		Minutes :					
<	Quota Exceptio	n					
D	Attach	Remove		Mov     Mov	ve up 🕴 Move Down		
		Rule No		ſ	vame		
					<b>a</b>		
					🖓 Add 🛛 💥 Cance	!	
						Refresh	
Lmc server address you are	connected to is: 1	0.100.0.3					Labris Teknoloii

# Attaching a Quota Exception to a Quota Policy





## Assigning a Quota Policy to User

After defining a policy (and exceptions), you need to assign users to this policy. This is possible in both LMC and WAUTH.

L <b>MC</b>							
🚾 Tabris Management Co	nsole						- <b>T</b> X
Device File Edit View Abo	ut						Help
	Users	Groups Identity	v Integration WAUT	H Quota			Terb
9 <b>80</b> and a second seco	Select All	🗙 Delete 🛛	ne Add				🔍 Filter
= 10.100.0.3:4000		User Name	Name Surname	Source	Domain	Global	Note
👋 User Management		ali2	ali	labris	u3		
🗳 System		veli2	veli	labris	u3		
Network Settings		alil		labris	u3		
VPN		kaan1	kaan	labris	u3		
e Filter		velil	veli	labris	u3		
	🤌 Chang	je Local Domain Na	me				🧬 Refresh
Lmc server address you are	e connected	d to is: 10.100.0.3	3				Labris Teknoloji
🔀 Labris Management Co	nsole						- 🗆 X
<u>D</u> evice <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>A</u> bo	ut						<u>H</u> elp
	Users	Groups Identit	y Integration WAUT	H Quota			
E Device List	Select All	🔀 Delete	🥜 Edit 🛛 🔮 Add				🔍 Filter
▣ 📃 10.100.0.3:4000		User Name	Name Surname	Source	Domain	Global	Note
👋 User Managemen		ali2	ali	labris	u3		
System		voli2	voli	lobrio			

	User	S Groups Id	entity	Integration WAU	TH Quota				
E Device List	Select /	All 📃 🔀 Dele	te 🖌	🖊 Edit 🛛 😤 Add					🔍 Filter
■ 📃 10.100.0.3:4000		User Nam	e	Name Surname	Source	Don	nain	Global	Note
🐴 User Management		ali2		ali	labris	u	3		
System	~	veli2		veli	labris	u	3		
Eirewall		ali1	-		labrie	u u	3		
VPN		kaanl	Edici	leer		×u	3		
61 Filter		veli1				u	3		
Antispam/Antivirus				User Name veli2					
Messaging				-					
Server			Na	me Surname veli					
Load Balancer				Password					
License									
			Pas	sword Again					
-				<b>n</b> i [n					
				Domain U3					
					Slobal				
				Comment					
				Quota Policy 5GB_Lim	it	•			
				016	- Constant				
				OK	Cancel				
	/ Cha	ange Local Dom	ain Na	me					🔊 Refresh
	CODDOC	tod to ic: 10 1	00.0.2						
Increase address you are connected to is: 10.100.0.3									

#### **WAUTH**

$[i]$ Labris $\equiv$	🛓 Yönetim Arabirimi	S LOGVIEW	A 0	ど admin 🗸
📲 İstatistikler 🛛 💌	Network A	uthentication System		
🖲 Kayıt Dosyalarını İndir 🛛 💌	Network A	differite attorn System		
🕲 Raporlar 🛛 💌	Create User	Edit User		7
🛡 Saldırı Uyanları	Online Users	Setting Rule:	Default :	
18 WAUTH	All Users	Username:	- akteus	
≭ SSLVPN	Settings	Password:		
🖂 AVAS		Generate Password:		
		Send Password:		
		Send with SMS:		
		Send with Mail:		
		GSM Number:		
		Mail Address:		
		Quota Policy:	5GB_Limit ;	
		Real Name:		
		Expiration Date:	Date: 3000-01-29 Tatar C	
		MAC Address:	: (Optional)	
		Multiple Login Limit:	1 :	
		Notes:		
			di Oser	

#### Assigning a Quota Policy to Group

Assignment to groups are only possible in LMC. When you assign a policy to group, all users not having a quota policy before are associated with new quota policy. If a user is specifically assigned a quota policy before, policy of this user will not be changed with group quota assignment.

🛃 Labris Management Co	nsole									- 🗆 X
Device <u>File</u> Edit <u>V</u> iew Abo	ut									<u>H</u> elp
	Users	Groups Identity Int	egration WAU	TH Quota						
E Device List	Select All	🔀 Delete 📝 E	dit 🔮 Add							🔍 Filter
■ 💻 10.100.0.3:4000		Group Name			Source				Domain	
User Management		veliler			labris				u3	
Network Settings	~		aliler			labris			u3	
Firewall     VPN     Fiter     Antispan/Antivirus     Dis/IPS     Govern     Code Balancer     Governee		Edit group Group Name Group Name : alii - Group Configuration All Users and Grou Name ali2 veli2 ali1	er Jps User User User User	Domain : C Filter Source Iabris Iabris	U3 Domain U3 U3 U3		Group Componer Name ali1 ali2	Quota Polic  ts  Type user user user	y SGB_Limit Q Filter Source labris labris	Domain U3 U3
		kaani	user	labris	U3					
		veliler	aroup	labris	u3					
		aliler	group	labris	u3	<				
						DK Car	ncel			
Lmc server address you are	connected	to is: 10.100.0.3								Labris Teknoloii

#### **Monitoring Quota Usage**

Usages of all users can be monitored in LMC. Additionally, a single user can see own usage in WAUTH Welcome screen. Monitoring in LMC is more detailed since you can examine by policy and see all exception usages also. On the other hand, a user can only see only policy usage in welcome screen. Exceptions and usages belong to them are not listed.

#### *LMC*

Double clicking on a usage shows exception usage.







### WAUTH Welcome Screen

La	oris Nauth	La	oris Wauth		
Ağ Yetkil	endirme Sistemi	Ağ Yetkil	endirme Sistemi		
Sisteme erişiminiz adres çubuğunu kı başlayabilirsiniz.	kabul edildi. Tarayıcınızın ullanarak gezintinize	Sisteme erişiminiz adres çubuğunu ku başlayabilirsiniz.	Sisteme erişiminiz kabul edildi. Tarayıcınızın adres çubuğunu kullanarak gezintinize başlayabilirsiniz.		
Bu pencereyi kapa	tmayınız	Bu pencereyi kapa	tmayınız		
Kullanıcı Adı Ad Soyad Silinme tarihi	veli2 veli Silinme Yok	Kullanıcı Adı Ad Soyad Silinme tarihi	veli2 veli Silinme Yok		
İndirme Kotası Gönderme Kotası Zaman Kotası	0 MB / 5120 MB 0 MB / Sınırsız Kullanım Yok / Sınırsız	İndirme Kotası Gönderme Kotası Zaman Kotası	214 MB / 5120 MB 5 MB / Sınırsız 1 dakika / Sınırsız		
	Çıkış		Çıkış		
5	Şifre Değiştir	Ş	Şifre Değiştir		

# **System**

System Tab in the LMC provides us with different options like DHCP, DNS, Date / Time settings, Configuring backup's, update, automatic updates, logs and general settings.

All the above mentioned options can be **configured** under **System Module**. When we are connected to **System Module** below screen appears.



### **Viewing Options in System**

When we Right click on "System Tab" we find following options.

1	Connect	ect It enables us to Connect to the System Module			
2	Disconnect	It enables us to Disconnect from System Module			
3	Properties	It helps us to view properties of System Module in			
		LMC			

### 26. System LMC Module

🖑 Labr	s Manag	ement Con	sole
<u>F</u> ile <u>E</u> di	t <u>V</u> iew	<u>M</u> odule	<u>A</u> bo
<b>4</b> 4			
erver 78.188.3 Use Syst Netw Fire VPN Antis IDS/ Mes Server	50 48.stat r Manage er Vo Conn va Disco Propo spam/Anti IPS saging er d Balance	ic.ttnet.con ment ect onnect erties virus	n.tr:4(

#### Users

In **System Module** on the right pane you can find **Users** tab in that click on **Users** 

# **Adding User**

Click on Add Tab to add a New User in System Module.

🔮 Labris Management Console					- 🗆 🗙
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>M</u> odule <u>A</u> bout					<u>H</u> elp
91 📑 📑 U	sers			lleore	~
	Login	Name	Comment	Users	^
□ □ □ □ Server □ □ □ □ 78 188 50 48:4000	admin	Administrator	administration account	Users	
👋 <u>User Ma</u> nagement 🛛 2	2 deneme	deneme wauth	deneme wauth		
System 3	3 SystemUse	User1	TestUser	Services	*
Eirewall	Testadmin	Testing	For Demo	DHCP	
VPN				Cached DNS	Server
Antionom/Antivirus					
IDS/IPS				System	*
🔁 Messaging					
Server					
Si License					
· · · ·					
			9 Add 9 Damana 92 Edit		
			Add C Remove V Edit		
Lmc server address you are connected to is: 78.188.50.48 Labris Teknoloji					knoloji

Add User	×
Username:	SystemUser1
Password:	2
Re-type:	••••••• 3
Name:	User1 4
Comment:	TestUser
	Add Cancel

These are the inputs for adding a New User

1	Username	Type the name of the Username of the new User		
2	Password	Type the <b>Password</b> of the new User		
3	Re-type	Re-Type Password of the new User for		
		confirmation		
4	Name	Type the Name of the new User		
5	Comment	Type reason for the User creation (Optional)		

Below screen appears stating that User added successfully, click OK to close the current tab



We can notice new User added in the User's list of System Module
	Login	Name	Comment	
1	admin	Administrator	administration account	
2	deneme	deneme wauth	deneme wauth	
2	System Iser1	Licor1	Teetlleer	

# **Deleting User**

Select User and click on **Remove Tab** to delete an User.

Login	Name	Comment
admin	Administrator	administration account
deneme	deneme wauth	deneme wauth
SystemUser1	User1	TestUser
SampleUser	User	test
		×
		<b>N</b>
		•

When the below screen appears, click **Yes** to remove User.



Alert screen appears displaying User removed successfully; click **Ok** to close the current tab.



**Change Password / Editing User** 

Select the user from the list and click on  $\ensuremath{\textit{Edit}}$ 

		<b>A A</b>	
Login	Name	Comment	
admin	Administrator	administration account	
deneme	deneme wauth	deneme wauth	
SystemUser1	User1	TestUser	

## Viewing options in Edit User

1	Module	Displays all the Modules in LMC
2	Access level	Displays access level of each Module
3 Set Password This option help		This option helps to Set Password to the User

Select the Module and choose Access level from the drop down menu as shown below

Edit User					×
Username:	ser1				
Name:	Name: User1				
Comment:	r				
1					2
Modu	le	· · ·	Access	Level	2
users		read			<b>V</b>
system		none		-	
iproute		read			
firewall		write			
vpn		none			
filter		none			
spam		none			
Lida		0000			
Set Passwo	rd 3			Save	Close

When we click on **Set Password**, below screen appears.

Set Password		×
New Password:		
Re-type password:	••••••	
	Set	Cancel

1	New Password	Type password of the User
2	Re-type	Re-type Password of the User for
	Password	confirmation

Click on Set Tab to set New Password

Below screen appears stating that password is changed successfully, Click **Ok** to close the current tab.



Click on **Save Tab** to save changes.

Edit User					×			
Username:	Username: SystemU							
Name:	Name: User1							
Comment:	TestUser	r						
Modu	lle		Access	Level				
users	users							
system		read						
iproute		none						
firewall		none						
vpn		none						
filter	filter							
spam		none						
lida		0000	•					
Set Passwo	Set Password Save Close							

When the below screen appears, click Ok.

info		×
1	Successful!	

Click on Close Tab

Edit User					×
Username:	Username: SystemU				
Name:	User1				
Comment:	TestUse	r			
Madu	ula.		A	a Laval	
Modu	Module			SLevel	_
users		read			
system		read			
iproute		none			
firewall		none			
vpn		none			
filter		none			
spam		none			-
lida		0000			
Set Passwo	rd			Save	Close

## **27. DHCP**

## DHCP: DHCP stands for Dynamic Host Configuration Protocol

DHCP server provides IP address and other related configuration information like subnet mask and default gateway to the host systems within a LAN network. For every computer it will provide unique IP to identify the system.

By our configuration settings IP address will change certain period of time for the host systems

DHCP is useful in extremely larger networks where we want to centralize the IP management to reduce human errors.

## **ISP (Internet Service Provider)**

Usually ISP's implement DHCP servers

DHCP is a server which assigns IPs automatically to the clients requested from a range of IPs.

## IP leasing process:

1. **DHCP discover**: The client machine when turned on, broadcasts the network id, broadcast id and MAC address on Network for discovering **DHCP** server.

2. Offer: The DHCP server listening to the request made by the client offers a pool of IP addresses to the client machine.

3. **Selection**: The client machine on receiving the pool of IP address selects an IP and requests the **DHCP** server to offer that IP.

4. **Acknowledgement**: The **DHCP** sends a confirmation about the allotment of the IP assigned to the client as an acknowledgement.

5. **IP lease**: If the client machine is not restarted for 8 days, exactly after 4days the client machine requests the **DHCP** server to extend the IP lease duration, on listening to this the **DHCP** server adds 8 more days for existing 4 days which is 12 days

If the client machine is restarted again the **DHCP** lease process takes place and again the client gets an IP for 8 days.



Select System option from the Labris Management console

Right click on the System tab and click on Connect to get connected

## Select **DHCP** option under services.

C Pl Server			Login	Name	Comment			
- 78,188,50,48;4000	н	1	admin	Administrator	administration account		Users	
👋 User Management		2	deneme	deneme wauth	deneme wauth			
System		3	SystemUser1	User1	TestUser		Services	*
Network Settings		4	Testadmin	Testing	For Demo			
Firewall						-	DHCP	
					Select DHCP	1	Cached DNS Server	
Antispam/Antivirus								

Select Server tab to view the DHCP server details like Name , Subnet , Router , Type and Status.

Server Leases List DHCP R	elay Global Settings				Users	*
Server Select All 📃 🔀 Delete 🥖 Edit	t 😤 Add			🔍 Filter	Users	
Name	Subnet/Netmask	Router	Туре	Status		
WAUTH_DHCP	10.1.0.0/255.255.255.0	10.1.0.1	Dynamic	Active	Services	~
labtest	192.168.20.0/255.255.255.0	192.168.20.1	Dynamic	Active	DHCP Cached DNS Se	rver

Click on **Add** to Add the New DHCP Server details.

👶 Labris Management Console			
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>M</u> odule <u>A</u> bo	ut		
	Server Leases List DHCP F	Relay Global Settings	
Server	Select All 📃 🔀 Delete 🥖 Ec	iit 🔮 Add	
🐴 User Management	Name	Subnet/Netmask	Router
System	WAUTH_DHCP	10.1.0.0/255.255.255.0	10.1.0.1
E Firewall	labtest	192.168.20.0/255.255.255.0	192.168.20.1
VPN			
Al Filter			
Antispam/Antivirus			
Server	:		
Load Balancer			
License	:		

Make **DHCP** scope **Active** by enabling the **Active** checkbox. Select the **type** of the scope from the options mentioned here. In this screen we selected **Dynamic** option. Also Enable Use interface's IP address as router check box.

1	Scope Name	Type Scope name
2	Interface	Select Interface from drop down menu
3	IP Range	Mention Scope

Click on Add Tab to add an IP Range

Add Dhep Scope	
Settings	
Active Typ	e Dynamic Static Ipsec
Scope Name *	TestScope
Interface *	tun0 - 10.8.3.1
IP Address *	Use interface's IP address as subnet
Netmask *	/24 (255.255.255.0)
Ip Range * 10.8.3.	10 - 10.8.3.80 🗳 Add
10.8.3.	10-10.8.3.80 Zelit
	2 Delete
Router * *	Use interface's IP address as router
	· · · · · · · · · · · · · · · · · · ·

Continuation to the above screen, choose Lease Time & Maximum Lease Time from the scope and type Domain Name, Click on Save Tab.

Lease Time * 1440 Maximum Lease Time * 2880		5-144000 Minutes (100 Days) 5-144000 Minutes (100 Days)
Domain Name DNS * Primary DNS	loak.com Vse router's IP address as DNS	
Secondary DNS		
Advanced Settings		Save

Saving changes is in progress.

Labris Teknoloji	×
Saving	

Below screen appears stating that **Changes are saved and applied**, click **Ok** to close the current tab.



We can notice from the list that the Server is added

Sei	ver Leases List DHCP R	elay Global Settings					
Server							
Select All 📃 🗶 Delete 🥜 Edit 👙 Add					🔍 Filter		
	Name	Subnet/Netmask	Router	Туре	Status		
	WAUTH_DHCP	10.1.0.0/255.255.255.0	10.1.0.1	Dynamic	Active		
	labtest	192.168.20.0/255.255.255.0	192.168.20.1	Dynamic	Active		
	TestScope	10.8.3.0/255.255.255.0	10.8.3.1	Dynamic	Active		

If we want to **Edit** the **IP Range**, Select IP Range and click on **Edit Tab**, modify the contents and Click **Ok** to apply changes

Add Dhcp Scope		
Settings		
Active Type	● Dynamic   ○ Static   ○ Ipsec	
Scope Name * T Interface * tu	estScope	
IP Address *	Use interface's IP address as subnet	
Netmask * /2	24 (255.255.255.0)	
lp Range * 10.8.3.10	- 10.8.3.80 - Add	
Edit	× Delete	
10.8.3.10	OK Cancel	
Router * *	Use interface's IP address as router	•

Select the Server from the list and click on Edit Tab.

Sei	rver Leases List DHCP R	elay Global Settings					
Selec							
	Name	Subnet/Netmask	Router	Туре	Status		
	WAUTH_DHCP	10.1.0.0/255.255.255.0	10.1.0.1	Dynamic	Active		
	labtest	192.168.20.0/255.255.255.0	192.168.20.1	Dynamic	Active		
>	TestScope	10.8.3.0/255.255.255.0	10.8.3.1	Dynamic	Active		

We can Edit **Scope Name, Interface and IP Range** in **Edit DHCP Scope**. At the same time we can even **Add, Edit, Delete IP Range** from the same tab.Select IP Range and click on **Delete** to delete the entire range.

Edit Dhop Scope	
Settings	
Active Typ	e 💿 Dynamic 💿 Static 💿 Ipsec
Scope Name * Interface * IP Address * Netmask *	TestScope tun0 - 10.8.3.1 ▼ ✓ Use interface's IP address as subnet /24 (255.255.255.0) ▼
Ip Range * 10.8.3.1 10.8.3.1	0 - 10.8.3.80
Router **	Use interface's IP address as router

Adding IP Reservation to DHCP scope



These are the inputs for adding IP Reservation

1	Active	We can enable or disable this option
2	Mac Address	Give Mac Address of the Host
3	IP Address	Give the IP Address within the scope of DHCP server
4	Hostname	Type the name of the Host

Click on Ok

In the below screen we can notice IP Reservation added to the DHCP Server

Edit Dhep Scope						×
Settings		IP Reservations				
Active Tune Dunamic Static Incoc		Select All 📃 🖇	🕇 Delete 🥜 Edit 🔮	Add		🔍 Filter
Active Type O Dynamic O Static O Ipsec			Mac Address	IP Address 🔺	Hostname	Status
			09:2c:a3:4d:13:a9	192.168.20.111	Testhost	Active
Scope Name * labtest			4d:6c:3c:12:c3:a0	192.168.20.112	loakhost	Active
Interface #			08:00:27:97:0e:4b	192.168.20.117	labtest_1	Active
Interface * ein2 - 192, 108,20,1			d4:be:d9:58:d9:a5	192.168.20.118	labtest_2	Active
IP Address * 🗸 Use interface's IP address as subnet						
	=					
Netmask* (24 (255.255.25.0)						
lo Range *						
192.168.20.110-192.168.20.120						
ZDelete						
Router ** 🔽 Use interface's IP address as router						
						E Savo
	-					Save
	Clos	e				

## **Editing IP Reservation**

Select IP and click on Edit tab

We can edit all the fields in the Edit tab and click **Ok** 

Edit Dhcp Scope								×
Settings		<u>.</u>		IP Reservations	🕻 Delete 🥜 Edit 🔮	Add		Filter
Active I)	/pe	U Ipsec			Mac Address	IP Address 🔺	Hostname	Status
Scone Name 1	lablast			~	09:2c:a3:4d:13:a9 4d:6c:3c:12:c3:a0	192.168.20.111 192.168.20.112	Testhost Ioakhost	Active Active
Scope Name *	lablest				08:00:27:97:0e:4b	192.168.20.117	labtest 1	Active
Interface *	eth2 - 192.168.20.1	•			d4:be:d9:58:d9:a5	192.168.20.118	labtest 2	Active
IP Address *	Use interface's IP address as subne	t						
Netmask *	/24 (255.255.255.0)	IP Reservation - Edit			×			
Ip Range * 192.16i Router * *		Active Mac Address 4d:6c:3c:12 IP Address 192:168.20 Hostname loakhost	2:c3:a0 .112 K	Cancel				
		]	¥					📕 Save
			Clo	se				

# **Deleting IP Reservation**

Select the IP and click on **Delete tab**, Click **Ok** to delete.

IP Reservations         Select All         Mac Address         IP IP Address         IP IP Address         IP IP IP Address         IP IP IP IP IP IP IP IP IP IP IP IP IP I	Hostname Status thost Active chost Active est_1 Active est_2 Active
Select All       Celete       Edit       Add         Mac Address       IP Address       F         09:2c:a3:4d:13:a9       192:168:20:111       Tes         4d:6c:3c:12:c3:a0       192:168:20:112       Ioal         08:00:27:97:0e:4b       192:168:20:117       Iabl         d4:be:d9:58:d9:a5       192:168:20:112       Ioal         will be deleted. Are you sure ?       Cancel       Cancel	Hostname Status thost Active drost Active est_1 Active est_2 Active
Mac Address         IP Address         IP Address           ✓         09:2c:a3:4d:13:a9         192:168:20:111         Tes           △         4d:6c:3c:12:c3:a0         192:168:20:112         loai           ○         68:00:27:97:0e:4b         192:168:20:117         labi           ○         d4:be:d9:58:d9:a5         192:168:20:118         labi	Hostname         Status           ithost         Active           dost         Active           est_1         Active           est_2         Active
•         09:2c:a3:4d:13:a9         192:168:20:111         Tes           •         4d:6c:3c:12:c3:a0         192:168:20:112         toal           •         08:00:27:97:0e:4b         192:168:20:117         labt           •         d4:be:d9:58:d9:a5         192:168:20:118         labt	thost         Active <host< td="">         Active           est_1         Active           est_2         Active</host<>
4466.3c.12.c2:a0       192.188.20.112       loai         08:00.27.97:0e.4b       192.168.20.117       labt         d4:be.d9:58:d9:a5       192.168.20.118       labt         will be deleted. Are you sure ?       Cancel	khost Active lest_1 Active est_2 Active
08:00:27:97:0e:4b         192:168:20.117         labt           d4:be:d9:58:d9:a5         192:168:20.118         labt	lest_1 Active lest_2 Active
vill be deleted. Are you sure ?	lest_2 Active
X       will be deleted. Are you sure ?       Cancel	
Will be deleted. Are you sure ? Cancel	
will be deleted. Are you sure ?	
X       will be deleted. Are you sure ?       Cancel	

Below screen appears stating that selected records have been deleted. Click **Ok** to close the current tab.

Info	×
1	Selected records have been deleted
	OK

Select the Server from the list and click on Delete Tab to delete the DHCP Server.

	Server Leases List DHCP Relay Global Settings							
Г	Server							
	Selec	t All 📃 🔀 Delete 🥖 Edi	t 🔮 Add			🔍 Filter		
		Name	Subnet/Netmask	Router	Туре	Status		
		WAUTH_DHCP	10.1.0.0/255.255.255.0	10.1.0.1	Dynamic	Active		
		labtest	192.168.20.0/255.255.255.0	192.168.20.1	Dynamic	Active		
	~	TestScope	10.8.3.0/255.255.255.0	10.8.3.1	Dynamic	Active		

Deleting process is in progress.

Labris Teknoloji	×
Deleting	

When the below screen appears, click Ok.



We can notice that the selected **Server** is **deleted** from the Servers list.

Ser	Server Leases List DHCP Relay Global Settings						
Server							
Selec	Select All 📃 🔀 Delete 🥒 Edit 🖗 Add 🔍 🤇 Filter						
	Name	Subnet/Netmask	Router	Туре	Status		
	WAUTH_DHCP	10.1.0.0/255.255.255.0	10.1.0.1	Dynamic	Active		
	labtest	192.168.20.0/255.255.255.0	192.168.20.1	Dynamic	Active		

## Lease list options

Select Lease List to display the details of DHCP Lease List.

Ser	Server Leases List DHCP Relay Global Settings						
DHCF	DHCP Leases						
Selec	t All 📃 🛛 🔀 Del	ete 🛛 👙 Add Re	servation All	-			🔍 Filter
	IP Address 🔺	Physical Address	Start Date	End Date	Hostname	Lease	Status
	10.1.0.110	18:67:b0:34:0e:	2013/11/28-18:	2013/11/29-18:	Unknown	Free	Off
	192.168.20.117	08:00:27:97:0e:	2013/12/13-17:	2013/12/14-17:	Unknown	Free	Off
	192.168.20.118	d4:be:d9:58:d9:	2013/12/05-13:	2013/12/06-13:	Unknown	Free	Off
	192.168.20.119	08:00:27:db:94:	2013/11/25-19:	2013/11/26-19:	Unknown	Free	Off
	192.168.20.120	08:00:27:f1:df:4c	2013/12/13-17:	2013/12/14-17:	Unknown	Free	Off

Choose IP Address and click on Add Reservation Tab.

Se	Server Leases List DHCP Relay Global Settings						
	DHCP Leases						
Sele	ct All 📃 🛛 🔀 De	lete 🛛 😤 Add Re:	servation All	-			🔍 Filter
	IP Address 🔺	Physical Address	Start Date	End Date	Hostname	Lease	Status
	10.1.0.110	18:67:b0:34:0e:	2013/11/28-18:	2013/11/29-18:	Unknown	Free	Off
	192.168.20.117	08:00:27:97:0e:	2013/12/13-17:	2013/12/14-17:	Unknown	Free	Off
	192.168.20.118	d4:be:d9:58:d9:	2013/12/05-13:	2013/12/06-13:	Unknown	Free	Off
	192.168.20.119	08:00:27:db:94:	2013/11/25-19:	2013/11/26-19:	Unknown	Free	Off
~	192.168.20.120	08:00:27:f1:df:4c	2013/12/13-17:	2013/12/14-17:	Unknown	Free	Off

Click Ok to Add reservation for the selected IP Address.

	×
2	Selected records will be reserved. Are you sure ?
	OK Cancel

Select the IP Address and click on delete tab to delete the selected lease list.

Sei	rver Leases Li	ist DHCP Rela	y Global Setti	ngs			
DHCP Leases Select All  All Filter							
	IP Address 🔺	Physical Address	Start Date	End Date	Hostname	Lease	Status
	10.1.0.110	18:67:b0:34:0e:	2013/11/28-18:	2013/11/29-18:	Unknown	Free	Off
	192.168.20.117	08:00:27:97:0e:	2013/12/13-17:	2013/12/14-17:	Unknown	Free	Off
	192.168.20.118	d4:be:d9:58:d9:	2013/12/05-13:	2013/12/06-13:	Unknown	Free	Off
	192.168.20.119	08:00:27:db:94:	2013/11/25-19:	2013/11/26-19:	Unknown	Free	Off
~	192.168.20.120	08:00:27:f1:df:4c	2013/12/13-17:	2013/12/14-17:	Unknown	Free	Off

Click Ok to delete the selected lease list



## **DHCP Relay options**

Select DHCP Relay and click on Add Tab.

Server	Leases List	DHCP Relay	<b>Global Settings</b>	
DHCP Relay			÷	
Select All	🔀 Delete	e 🥖 Edit 🥞	Add	
			Interfece	

## Give the server IP Address and click **OK**.

DHCP R	elay - Edit	×		
2	Arabirim *	tun0 - 10.8.3.1		
	Sunucu IP Adresi *	192.168.0.10		
OK Cancel				

We can notice that **Server** is added in the **DHCP Relay**.

To set up the DHCP Relay with one Server and more than one interfaces, each interface should

be added separately with Server .

After add operation, a route which is from **DHCP Server** to **DHCP Relay** should be added.

Server Leases List DHCP Relay Global Settings				
DHCP Relay				
Select All 🗌 🄀 Delete 🥜 Edit 👙 Add 🔍 🔍 Filter				
Interface Server				
	tun0	192.168.0.10		

Select the Server and click on Edit Tab.

L	Server Leases List DHO	P Relay Global Settings
	DHCP Relay	
	Select All 📃 🔀 Delete 🗾	Edit 🔮 Add
		Interface Server
	<ul><li>✓</li></ul>	tun0 192.168.0.10

Edit the Server IP Address and click OK.

DHCP Re	əlay - Edit		x
$\bigcirc$	Arabirim *	tun0 - 10.8.3.1	1
	Sunucu IP Adresi *	192.168.0.11	1
	,	OK Cancel	

Select the **Server** and click on **Delete Tab** to delete server from the DHCP Relay.

Server Leases List DHC	P Relay Global Settings
DHCP Relay	
Select All 📃 🔀 Delete 🥖	Edit 🔮 Add
	Interface Server
✓	tun0 192.168.0.11

Click **OK** to delete the server from DHCP Relay.

	×
0	Selected records will be deleted. Are you sure ?

Below screen appears stating that Selected **Records** have been deleted, click **Ok** to close the current tab.



## **Global Settings options**

When we click on **Global Settings**, below screen appears.

From the **IPSec VPN Interface** drop down list select the Ethernet adapter.

Server	Leases List	DHCP Relay	Global Settings		
IPSec Settin	ngs				
Activat	te IPSec Server				
IPSec	VPN Interface	eth3 - 10.1.0	.1/255.255.255.0	-	
Activation	te Advanced Par	amet eth0 - 10.8.3 eth0 - 169.2 eth1 - 10.11	0.1/255.255.255.0 54.1.1/255.255.0.0 .12.221/255.255.255	.0	
192.168	3.0.10	eth2 - /		🗗 Add	
		eth3 - 10.1.0	).1/255.255.255.0	✓ Edit ★ Delete	]

Enable Activate Advanced Parameters, give the IP Address and click on Add and then Save.

Server Leases List DHCP Relay Clobal Settings
IPSec Settings
Activate IPSec Server
IPSec VPN Interface eth3 - 10.1.0.1/255.255.255.0
Activate Advanced Parameters
192.168.0.10
192.168.0.10
× Delete
Save

Select the IP Address and click on Edit tab to edit IP Address.

Server Leases List	DHCP Relay Global Settings
IPSec Settings	
Activate IPSec Server	
IPSec VPN Interface	eth3 - 10.1.0.1/255.255.255.0
Activate Advanced Par	ameters
192.168.0.10	👙 Add
192.168.0.10	Edit
	🔀 Delete

Edit the IP Address and click OK.

Edit	×
192.168.0.11	2
OK Cancel	

Select the IP Address and click on Delete button to delete the IP Address.

Server Leases List D	ICP Relay Global Settings
IPSec Settings	
Activate IPSec Server	
IPSec VPN Interface	eth3 - 10.1.0.1/255.255.255.0
Activate Advanced Parame	ters
192.168.0.10	👙 Add
192.168.0.11	Edit
	🔀 Delete
1	

We can notice that IP Address is deleted, click on **Save Tab** to save the changes.

Server Leases List DHCP Re	elay Global Settings		
IPSec Settings			
Activate IPSec Server			
IPSec VPN Interface eth3 -	10.1.0.1/255.255.255.0	▼	
Activate Advanced Parameters			
192.168.0.10		🚽 Add	
		🥟 Edit	
		× Delete	
			Save

Below screen appears stating that Changes are Saved. Click OK to close the current tab.



## 28. DNS

Domain Name System (DNS) is the name resolution protocol for TCP/IP networks, such as the Interne. DNS translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites.

DNS is that it serves as the "phone book" for the Internet by translating human-friendly computer hostnames into IP addresses.

In System Module, right pane click on Services tab and select Cached DNS Server to manage DNS Server.



In the **DNS Server Management** tab we find different options like Local Subnet, Real DNS Servers. In the Real DNS Servers give the **IP Address** of the **DNS server** and click on **Add**.

DNS Server Management		
Add Real DNS Servers	Delete 2	
DNS Server:	121.1.2.31	
8.8.8.8 Add Service Managem Start Restar	Delete Undate ent 3 rt Stop Status:RUNNING	

## Viewing fields in DNS

1	DNS Server Management	In this we can Add, Delete, Update Local Domain	
2	Real DNS Server	In this we can Add, Delete, Update DNS server	
3	Service	In this we can Start, Restart, Stop DNS Server and it also displays status of the	
	Management	DNS Server	

In the below screen we can notice **DNS Server** is added.

Real DNS Servers		
DNS Server:	121.1.2.31	
8.8.8.8		
121.1.2.31		
	1	
Add	D <u>e</u> lete	Update
Service Managemer	nt	
Start Restart Ston Status PUNNING		
Start Restart Stop Status:RUNNING		

Select the server and click on Start tab to start the services of DNS Server.

Real DNS Servers		
DNS Server:	121.1.2.31	
8.8.8.8		
121.1.2.31		
Add	D <u>e</u> lete	U <u>p</u> date
Service Management		
Start Restart Stop Status:RUNNING		

Below screen appears stating that DNS Service Started, click Ok to close the current tab.

	×
DNS Service Started!	
	DNS Service Started!

In the below screen we can notice the **Status** of the **DNS Server** is shown as **Started**.

Real DNS Serve	rs	
DNS Server:	121.1.2.31	
8.8.8.8		
121.1.2.31		
A <u>d</u> d	D <u>e</u> lete	U <u>p</u> date
Service Manage	ment	
<u>S</u> tart <u>R</u> e	start S <u>t</u> op	Status: Started

Select the Server and click on Stop button to stop the services of DNS Server.

DNS Server:	121.1.2.31	
8.8.8.8		
121.1.2.31		
A <u>d</u> d	D <u>e</u> lete	U <u>p</u> date
A <u>d</u> d Service Manage	D <u>e</u> lete	U <u>p</u> date

Below screen appears stating that **DNS Service Stopped**, click **OK** to close the current tab.



In the below screen we can notice the status of the DNS Server is shown as Stopped.

Real DNS Servers	
DNS Server:	121.1.2.31
8.8.8.8	
121.1.2.31	
A <u>d</u> d Service Managemen Start Restart	D <u>e</u> lete U <u>p</u> date nt Stop Status: Stopped

Select the Server and click on Restart button to Restart the Services of DNS Server.

Real DNS Server	5	
DNS Server:	121.1.2.31	
8.8.8.8		
121.1.2.31		
A <u>d</u> d	D <u>e</u> lete	U <u>p</u> date
A <u>d</u> d Service Manage	D <u>e</u> lete	U <u>p</u> date

Below screen appears stating that **DNS Service Restarted**, click **OK** to close the current tab.

lnfo		×
1	DNS Service Restarted!	

Select the Server and click on **Delete** button to delete a **DNS Server**.

Real DNS Servers		
DNS Server: 121.1.2.31		
8.8.8.8		
121.1.2.31		
Add Delete Update		
Service Management		
Start Restart Stop Status:RUNNING		

In the below screen we can notice newly added **DNS Sever** got deleted.

Real DNS Servers DNS Server:		
8.8.8.8		
A <u>d</u> d	D <u>e</u> lete	U <u>p</u> date
Service Management Start Restart Stop Status: Started		

# 29. HA - High Availability Appliance Deployment Architecture

High Availability service is designed for Labris UTM devices to run in a redundant (activepassive) mode. With this service, you can configure two Labris UTM devices in a redundant way and ensure non stop service.

•You can also change your prefered language even after you login to the appliance as shown in following image					
🔢 Labris Managem	ent Console				- 🗆 🗙
Device <u>F</u> ile <u>E</u> dit <u>V</u> iew	w <u>A</u> bout				<u>H</u> elp
	High Availability				Users 🌣
Device List     fw:4000	High Availability	Enable		Save	Users
System	gement Synchronize Pe	riod 120	Minutes ( Min: 10, Max: 1440 )		Services
Firewall	HA Shared Key	sharedkey			DHCP Sached DNS Server
🔒 Filter 🖄 Antispam/A	ntivirus				High Availability

## Steps;

By following the steps below and with the information in the document, Labris High Availability system can be setup.

Active Device (Master)	Passive Device (Slave)
	1 - Device hostname is configured
	2 - IP configuration is done. Here, High Availability
	port and dummy IP settings are configured. (Alias IP
	address configuration is done on the active device on
	first configuration)
	3 - Console access settings are configured.
4 - Device hostname is configured.	
5 - IP configuration is done. High Availability port,	
dummy IP and alias IP settings are configured.	
6 - Console access settings are configured.	
7 - High Availability service is configured.	
8- All the other configurations are done. Firewall,	
webfilter etc.	
High Availability	system is tested.

## Topology

For the redundant setup of Labris UTM devices, the following topology can be used as a reference.

The basic logic while setting the topology is to connect both of the Labris devices via ethernet cable to the other devices that they are connected and connect the two Labris UTM devices to each other, for health checking.



For the High Availability system, first of all hostname, IP settings (except alias IP addresses) and console access settings are configured on the second device.

All other configurations are done on the first device. When high availability is started all the configurations will be synchronized between the two devices.

After setting the above topology, you can continue following the configuration steps.

### Hostname Settings

Devices used in High Availability should have different hostnames. High Availability service checks access control between each other using this hostname.

To configure the hostname, enter the system module from LMC. After clicking *General Settings* you can edit the hostname.



Hostname	
Hostname	labrisl
	Save

1	Hostname	Labris UTM Device Name
2	Save	Configuration Save

The same setting is also configured on the second Labris UTM device. On the second device another hostname should be given.

### **IP Configuration**

When setting up the High Availability system an unused IP address from the internal network is given from the *Network Settings* module.

Active and passive devices are configured to have different IP adresses.

The IP adresses that will actually be used should be defined as an alias IP on the related ethernet. (Only defined on the active device on first configuration.)

For IP configuration, enter the *netwok settings* module from LMC.

IP settings are configured according to your network topology.



### **Dummy IP Address**

For ethernet interfaces to be active, an unused IP address which will not normally be used should be set on an ethernet. The IP adresses which will be actually used will be defined as an alias IP on the ethernets. The alias IP adresses are automatically run on the current active device by High Availability service.

Dummy IP addresses, which are not used in the network, are given to the related ethernets via the IP Configuration menu. For this, after selecting the related ethernet, right click and press edit. After the configurations press apply button.

IP Configuration	Routing				
_ Interfaces					
Active	Device	Name	Туре	IP	
✓	eth0		Ethernet	169.254.1.1	Add
✓	ethl	Ethernet Properties		×	
✓	eth2		£	^	
✓	eth3	Use dynamic IP cor	nfiguration		Delete
✓	tun0	Static IP Configuration			
		Name Lan			
		IP Address 192.	168.55.11		Deactivate
		Mask 255	255 255 0		
		MdSK 200.	200.200.0		
		Advanced Ethernet Setting	15		C Status
		Ethernet Speed	Auto-Negotiation	-	
		мти	1500	(576-1500)	
		MAC Address	00:90:0B:2A:76:7E		
		Finde Address	00.00.00.00.00.00		
		Restore Settings			
		S	ave Apply Canc	el	

1	Name	A name defining the ethernet interface	
2	IP Address	The IP address used for the selected interface. In this scenario, a unused IP address should be given. Also on the second device a unused IP address should be given.	
3	Mask	Mask of the network address.	
4	Apply	Applies the configurations.	
5	Other Parameters	For other parameters, please refer to the Ethernet Settings section	
		in the admin guide.	

This procedure is done for all the used ethernets.

### Alias IP

More than one IP address can be defined on a physical ethernet interface. For this, alias IP addresses are added to the system. When using Labris High Availability service, IP settings are done using alias IPs. Press on the *Add* button in *IP Configuration* menu and select *Alias IP*. Define the IP addresses which will actually be used.

🖑 Labris IPRo	uie – 🗆 🗙			
Labris Security	Gateway Widget			
Labris IpRoute cr aliases and PPPo interface type tha	eate wizard allows you create IP E connections.Please select the at you want to create			
Types				
	as			
ADSL	-			
🔵 Bridg	le			
🔘 3G				
	1			
<u>Previous</u>	lext ▶ Last Einish Cancel			
🖑 Labris IPRo	ute – 🗖			
IP aliases gives IP address and	s you the ability to assign another 🛛 🕅			
Alias Confi	guration			
Name	Name lan_1			
IP Address 192.168.55.1				
Netmask 255.255.255.0				
Interface	Lan (eth2) 💌			

1	Name	A name defining the alias ethernet interface.	
2	IP Address	The IP address used for the selected interface. In this scenario, an unused IP address should be given. Also on the second device an unused IP address should be given.	
3	Mask	Mask of the network address	
4	Interface	The ethernet interface which the alias IP will be configured on	
5	Next	After the settings are configured click on the <i>Next</i> button and the alias interface will be defined.	

This way, all IP addresses which will actually be used are added as an alias ethernet interface. After the definitions are made, the alias ethernet interfaces which have been defined are selected and activated.

eth2:	0 lan_1	IP Alias	192.168.55.1
X Activate			

This procedure is done for all alias ethernets.

Alias IP addresses are only configured on the active device. There is no need to do this configuration for the passive device.

### HA Port

It is the ethernet interface which will be used to communicate between Labris UTM devices. HA ethernet interface is defined on both the active and passive devices. The two devices are connected via an ethernet cable using these ports configured for HA.

The ethernet interfaces used for HA should be the same on both devices. In other words, if the active device is using eth3 for HA, the passive device should also use eth3.

An IP address is given to the ethernet interface configured as HA port. Any unused IP address having a minimum mask of /30(255.255.255.252) in the local network can be given. The IP adresses given to the HA ports of the active and passive device should be in the same subnet.

IP Configuration	Routing					
Interfaces						
Active	Device	N	ame	Туре	IP	
~	eth0			Ethernet	169.254.1.1	Add 💦
~	ethl	Ethernet Prop	perties		×	
	eth2 eth2:0	📃 Use dynam	ic IP configu	uration		Pelete Delete
✓	eth3	Static IP Configu	ation			
~	tun0	Name	HA1			×1
		IP Address	10.20.30	).1		Deactivate
		Mask	255.255	.255.252		
						Edit
		Advanced Ethern Ethernet Sp	et Settings eed Aut	o-Negotiation	′	C Status
		MTU	150	0	(576-1500)	
		MAC Addres	s 00:	90:0B:2A:76:7F		
		Restore Se	ettings			
			Save	ApplyCancel		

1	Name	A name defining the ethernet interface.	
2 IP Address		The IP address used for the selected interface. The IP adress given	
		to the HA port for the access of two Labris devices.	
3	Mask	Mask of the network address.	
4	Apply	Applies the changes.	

5	Other Parameters	For other parameters, please refer to the Ethernet Settings section
		in the admin guide.

The same configuration is done for the second device.

### Console Access (Access Between Devices)

For allowing connection between active and passive devices, the IP addresses given to the HA ports should be written to the console access configuration of the active and passive devices.

Just for the first time this setting should be done on both devices. After HA starts running, it is enough to configure the console access on active device.

Under the system module in LMC you will see the *console access settings*. The IP addresses defined for the HA ports of both devices should be added here.



#### Console Access Blocking-

#### Block remote console access

Console connection is allowed only via eth0 interface.IP address of eth0 is set to 169.254.1.1Client PC should have an IP adress in network 169.254.0.0/255.255.0.0such as 169.254.1.2

#### Console Access Addresses

IP/Network Address	Netmask
169.254.1.10	255.255.255.255
0.0.0.0	0.0.0.0
169.254.1.9	255.255.255.255
192.168.1.100	255.255.255.255
10.0.2.15	255.255.255.255
10.11.12.155	255.255.255.255
10.11.12.10	255,255,255,255

Add Access Address 🗙
IP/Network Address
Netmask
Add Cancel
📃 Add 🕎 Edit 🔄 Remova

1	IP/Network	The IP or network addess which will be allowed for accessing the
		device. In this scenario, the IP/network address defined for the HA
		ports are written.
2	Netmask	The netmask of the IP/network addess which is allowed to access
		is written.
3	Add	After clicking this button, it will also be applied. There is no need
		to click the save button additionally.

#### High Availability Service Settings

HA service settings are located under the services menu in system module of LMC.

It is sufficient to make the configurations from the active device. The configuration of the passive device is done by the active device automatically.
High Availability	Enable		🔡 Save
Synchronize Period	120	Minutes ( Min: 10, Max: 1440 )	
HA Shared Key	sharedkey		

1	High Availability	Enable. Activation of the service
2	Synchronize Period	The time period of the synchronization between Active and Passive devices.
3	HA Shared Key	The shared key of the HA service between the two device.
4	Save	The button to save and apply the configurations.

_ This No	de Settings	
Node	e	Master 💌
Inter	face	eth3 (10.20.30.1 / 255.255.255.0)

1	Node	This is used to determine if the device being configured is the first (master) device or the second (slave) device. Master device is the active device whereas the slave device is the device on stand by mode
2	Interface	The HA ethernet port configured for this device.

Peer Node Settings-		
IP Address	10.20.30.2	

ddress The IP address given to the HA port of the other device.	IP Address	1
---	------------	---

Reliable Host Settings		
Interface	eth2 (192.168.116.186 / 255.255.255.0)	<b>•</b>
Reliable Ping IP	192.168.116.100	

1	Interface	This is used to determine the ethernet which has the address which is used to control the life status of the devices by sending ping packets. It is advised to select the ethernet which is on the LAN.
2	Reliable Ping IP	The IP address of a device which is behind the selected IP address, which will be always up and sent ping packets to.

### Saving and Applying Configurations

After pressing the save button the configurations are saved.

Process	Status
Saving Configuration	0
Check Authentication	0
Authenticate Peers	0
Saving Configuration on Peer Node	0
Synchronizing Nodes	0
Checking Reliable Host	0
Restarting Service	0

Access to the second device is started over SSH protocol. The key of the second device is seen. Click *yes* if the key is correct.

ligh Availability		>
First time connect Peer host's host I Do you want to pr	ting to peer host. key : "1C:48:7E:5E:FC:E0:5B:A4:39:78:] roceed?	LD:4D:D5:F2:68:A1*

Enter the root password of the other device. This procedure is done only once. It will not appear on consecutive configurations.

1.4	Process	Status
Savin	High Availability	×
Check		
Authe	Please enter peer host's password :	
Savin		
Synch	OK Cancel	
Check		
Resta	rting Service	0

After establishing the connection, the configuration of the other device is saved and the synchronization between devices start.

After the procedure completes successfully High Availability system will be established.

	Process	Status
Saving C	High Availability	×
Check A		
Authenti	High Availability configuration is saved su	uccessfully.
Saving C		
Synchron	OK	
Checking	<u>vi</u>	
Restartin	a Service	

The status of the High Availabilty service can be seen below the page.

## **30. Configuration Backup / Restore**

## In System module, right pane select Configuration Backup

System 🌣
Configuration Backup
Click to manage configuration
Automatic Update
Logs
Date/Time Settings
Console Access Settings
General Settings
Trusted Timestamping
💥 Reboot
0 Shutdown

According to user requirement choose any one of the radio button in the below screen and click on **Backup Tab** to start the Backup process.

Choose Configuration radio button and click on Backup button.

Backup	
Choose backup type:	
Configuration	
O User Settings	
Permanent Logs	
Operational Logs	
Network Logs	
Delete logs after backups	<b>A</b>
a	Backup

Click on **Save tab** to save the file with **file name.bak** extension in your local machine as in the below screenshot.

Save Backup	×
Save In: Documents 💌	🔹 🙆 🐸 🏢 🏢
<ul> <li>Bluetooth Exchange Folder</li> <li>Camtasia Studio</li> <li>My Shapes</li> <li>New Folder</li> <li>Snagit</li> <li>78.188.50.48.static.ttnet.com.tr_2013-12-27_1125.bak</li> <li>78.188.50.48.static.ttnet.com.tr_auditlog_2013-12-27_1110.tar.gz</li> <li>78.188.50.48.static.ttnet.com.tr_networklog_2013-12-27_1118.tar.gz</li> </ul>	78.188.50.48.static.ttnet.com.tr_oper     78.188.50.48.static.ttnet.com.tr_user     Image: Comparison of the state of the st
	Þ
Enter file name: 78.188.50.48.static.ttnet.com.tr_2013-12-27_1143.ba	ak
Files: *	•
	Save Cancel

Creating **Backup** process for **Configuration** is in progress.

Creating Backup	×
Please wait	

Below screen appears stating that **Backup** saved at the chosen location in your hard drive, click **OK** to close the current tab.



According to user requirement choose any one of the radio button in the below screen and click on **Restore** to start restore process

## Choose Configuration and click on Restore button.

<sup>D</sup> Restore ───	
; Choose b	ckup type:
: Onfi	uration
User	Settings
0.000	
	Restore

Choose the backup file from the local machine and click OK to Restore Backup

Restore Backup	×
Look In: Documents	- 🔒 🙆 📽 🏢
Bluetooth Exchange Folder	78.188.50.48.static.ttnet.com.tr_oper
🎉 Camtasia Studio	78.188.50.48.static.ttnet.com.tr_user
🛗 My Shapes	
New Folder	
🥼 Snagit	LABRIS 1.doc
78.188.50.48.static.ttnet.com.tr_2013-12-27_1125.bak	🖾 Labris.xlsx
78.188.50.48.static.ttnet.com.tr_auditlog_2013-12-27_1110.tar	r.gz
78.188.50.48.static.ttnet.com.tr_networklog_2013-12-27_1118	8.tar.gz
Enter file name: 78.188.50.48.static.ttnet.com.tr_2013-12-27_1	125.bak
Files: *	<b>•</b>
	OK Cancel

Restoring Backup process for Configuration is in progress.

Restoring Backup	×
Please wait	

Below screen appears stating that **Backup restored**, click **OK** to close the current tab.



Choose User Settings and click on Backup Tab

Backup	
	Choose backup type:
	Configuration
	User Settings
	O Permanent Logs
	Operational Logs
	O Network Logs
Delete log	gs after backups

Click on **Save tab** to save the file with **file name.bak** extension in your local machine as shown in the below screen.

Save Backup	×
Save In: 👔 Doc	uments 💌 🖬 🏠 🎬 🏢
Bluetooth Excha	ange Folder
🔒 Camtasia Studio	
🛗 My Shapes	
🌗 New Folder	
🌗 Snagit	
LABRIS 1.doc	
🕙 Labris.xlsx	
Enter file name:	78.188.50.48.static.ttnet.com.tr_user-settings_2013-12-27_1053.bak
Files:	*
1165.	
	Save Cancel

Creating **Backup** process for **User Settings** is in progress.

Creating Backup	×
Please wait	

Below screen appears stating that **Backup Saved**, click **OK** to close the current tab.



Choose User Settings and click on Restore button.

Restore		
Choose backup type:		
Configuration		
User Settings	Restore	

Choose the backup file from the local machine and click Ok to Restore Backup

Restore Backup X
Look In: Documents 🔹 🔝 🏠 🔡 🏢
Bluetooth Exchange Folder   Camtasia Studio   My Shapes   New Folder   Snagit   78.188.50.48.static.ttnet.com.tr_user-settings_2013-12-27_1053.bat
Enter file name: 78.188.50.48.static.ttnet.com.tr_user-settings_2013-12-27_1053.bak Files: OK Cancel

Restoring Backup process for User Settings is in progress.

Restoring Backup	×
Please wait	

Below screen appears stating that **Backup restored**, click **OK** to close the current tab.



## Choose Permanent Logs and click on Backup button.

	Backup
	Choose backup type:
	Configuration
	User Settings
	Permanent Logs
	Operational Logs
	Network Logs
	Delete logs after backups Backup
- 11	

Click on **Save tab** to save the file with **file name. tar.gz** extension in your local machine at your chosen location as shown below.

Save Backup		×
Save In: 👔 Do	ocuments 💌 🗈 🖄 🔛 🏢	
Bluetooth Exch Camtasia Studi My Shapes New Folder Snagit 78.188.50.48.s	hange Folder  Jio  LABRIS 1.doc  Labris.xlsx  static.ttnet.com.tr_user-settings_2013-12-27_1053.bak	
•		1
Enter file name:	78.188.50.48.static.ttnet.com.tr_auditlog_2013-12-27_1110.tar.gz	3
Files:	* Save Cancel	3

Creating **Backup** process for **Permanent logs** is in progress.

Creating Backup	×
Please wait	

Below screen appears stating that **Backup Saved**, click **OK** to close the current tab.



Choose Operational Logs and click on Backup Tab

Backup	
Choose backup type:	
Configuration	
User Settings	
Permanent Logs	
Operational Logs	
O Network Logs	× .
Delete logs after backups	Backup

Click on **Save tab** to save the file with **file name .tar.gz** extension in your local machine to save the operational logs as shown below.

Save Backup	×	
Save In: Documents	۵ 🗳 🖽 🖿	
Bluetooth Exchange Folder		
🍌 Camtasia Studio	LABRIS 1.doc	
🛗 My Shapes	🖾 Labris.xlsx	
🕌 New Folder		
🔒 Snagit		
78.188.50.48.static.ttnet.com.tr_auditlog_2013-12-27_1110.tar.gz		
78.188.50.48.static.ttnet.com.tr_user-settings_2013-12-27_1053.ba	k	
-		
Enter file name: 78.188.50.48.static.ttnet.com.tr_operlog_2013-12-27	7_1114.tar.gz	
Filme		
riles.	<b>`</b>	
	Save Cancel	

Creating **Backup** process for **Operational logs** is in progress.

Creating Backup	×
Please wait	

Below screen appears stating that **Backup Saved**, click **OK** to close the current tab.



Choose Network Logs and click on Backup Tab.

If we want to delete logs after completion of Backups process for each log, Check the **Delete** logs after backups check box.

Backup	
Choose backup type:	
Configuration	
<ul> <li>User Settings</li> </ul>	
Permanent Logs	
<ul> <li>Operational Logs</li> </ul>	
Network Logs	
Delete logs after backups	Backup

Click on **Save tab** to save the file with **file name .tar. gz** extension in your local machine as shown below.

Save Backup	×
Save In: Documents	. 🗈 🙆 😤 🏥 🏢
Bluetooth Exchange Folder	
🐌 Camtasia Studio	
🔛 My Shapes	LABRIS 1.doc
🐌 New Folder	🖼 Labris.xlsx
🐌 Snagit	
78.188.50.48.static.ttnet.com.tr_auditlog_2013-12-27_1110.tar.gz	
78.188.50.48.static.ttnet.com.tr_operlog_2013-12-27_1114.tar.gz	
78.188.50.48.static.ttnet.com.tr_user-settings_2013-12-27_1053.b	ak
Enter file name: 78.188.50.48.static.ttnet.com.tr networklog 2013-	12-27 1118.tar.oz
Files:	•
	Sava Cancel
	Save

Creating **Backup** process for **Network logs** is in progress.

Creating Backup	×
Please wait	

Below screen appears stating that **Backup Saved**, click **OK** to close the current tab.



# **Factory settings**

Click on Factory to roll back Labris UTM the default settings.



### 31. Update

In System module, Right Pane under system tab click on **update** tab

One formation Dealers
Automatic LIndate Automatic LIndate Logs Date/Time Settings Console Access Settings General Settings Trusted Timestamping Reboot Shutdown

Note – In the below screen if any package is pending for upgrade, please request from the service provider using the mail id or call.

When we click on **Update Tab**, below screen appears, **Package** of the Server version and **Signature** has to browsed from local machine and click **Install** 

LUM packet Manager	
Server Version 2.2.0	
	$\sim$
Package	Browse
🥜 Signature	Browse
	Install

### 32. Automatic Update

In **System Module**, right pane under **System Tab** click on **Automatic Update Tab** to get Updated automatically



### 33. Record

In **System Module**, right pane under **System Tab** click on **Logs** to view Logs of LMC



Below screen appears displaying all the Log Types in LMC.

Select any required log from the **Log Types** then the related information is displayed in the right pane.

😤 LMC Log Viewer					- 🗆 🗙
Log Types	Vie	w 30 🔻 per page			Search
	#	Date	User Name	Source Ip	Url
Accessiog	1	2013.12.19-16:24:48	-	10.11.12.28	http://safebrowsing.clients.google.com/safebrowsing/dow
Administrative	2	2013.12.19-16:22:37	<u> -</u>	10.11.12.28	http://www.milliyet.com.tr/d/handler/MilliyetHandler.ashx?ht
	3	2013.12.19-16:22:37	-	10.11.12.28	http://www.milliyet.com.tr/d/handler/MilliyetHandler.ashx?h(
Dhcp	4	2013.12.19-16:22:37	-	10.11.12.28	http://www.milliyet.com.tr/d/handler/MilliyetHandler.ashx?h
	5	2013.12.19-16:22:37	-	10.11.12.28	http://www.milliyet.com.tr/d/handler/MilliyetHandler.ashx?h(
Ipmac.log	6	2013.12.19-16:22:36	-	10.11.12.28	http://www.milliyet.com.tr/d/advert/emlAnasayfaV2_2.html
	7	2013.12.19-16:22:36	-	10.11.12.28	http://www.milliyet.com.tr/ashx/GoogleBanner.ashx?a=Ant 📃
L2tp	8	2013.12.19-16:22:36		10.11.12.28	http://www.milliyet.com.tr/ashx/GoogleBanner.ashx?a=An
	9	2013.12.19-16:22:36		10.11.12.28	http://rtax.criteo.com/delivery/rta/rta.js?netId=2196&cookieN
Maillog	10	2013.12.19-16:22:36	-	10.11.12.28	http://pubads.g.doubleclick.net/gampad/ads?gdfp_req=1&c
	11	2013.12.19-16:22:36	-	10.11.12.28	http://live.sporx.com/banners/milliyet.php
Network	12	2013.12.19-16:22:36	-	10.11.12.28	http://ads.milliyet.cubecdn.net/iframe/milliyet/300x150_4.htm
	13	2013.12.19-16:22:35	-	10.11.12.28	http://www.milliyet.com.tr
Operational	14	2013.12.19-16:22:18		10.11.12.28	http://app.pubserver.adhood.com/6961
	15	2013.12.19-16:22:17	-	10.11.12.28	http://app.pubserver.adhood.com/6967
Sslvpn	<u>16</u>	2013.12.19-16:22:17	-	10.11.12.28	http://app.pubserver.adhood.com/6961
	17	2013.12.19-16:22:17	-	10.11.12.28	http://app.pubserver.adhood.com/6919
Wauth-access.log	18	2013.12.19-16:22:16	-	10.11.12.28	http://www.milliyet.com.tr/subs/fotogaleri_csuv.asp?DOL_
	19	2013.12.19-16:22:16	-	10.11.12.28	http://www.milliyet.com.tr/fotogaleri/49083-yasam-reza-za
	20	2013.12.19-16:22:16	-	10.11.12.28	http://secure.milliyet.com.tr/redirect/Default.aspx?z=145&I=
		Go t	o Page		Prev 1 / 111 Next

### Different types of Logs in LMC.

1	Access.log	Log messages related to Access can be viewed
2	Administrative	Log messages related to Administrative can be viewed
3	Dhcp	Log messages related to Dhcp can be viewed
4	Lpmac.log	Log messages related to Lpmac can be viewed
5	L2tp	Log messages related to L2tp can be viewed
6	Maillog	Log messages related to Maillog can be viewed
7	Network log	Log messages related to Network log can be viewed
8	Operational	Log messages related to Operational can be viewed
9	Ssslvpn	Log messages related to Ssslvpn can be viewed
10	Wauth-	Log messages related to Wauth-access can be viewed
	access.log	

### 34. Date / Time Settings

In System Module, right pane under System Tab click on Date/Time Settings.



Below screen appears, set the date and time and click **Save** to save the **Current Date/Time**.



## **35. Console Access Settings**

In System Module, right pane under System Tab click on Console Access Settings.

System 🕆
Configuration Backup Update Automatic Update Logs Date/Time Settings
Console Access Settings General Settings Console Access Mosed Access Mping Reboot Shutdown

Enable **Block remote console access** check box to block remote access for other users or desktops.

Console Access Blocking	1
Block remote console access	
Console connection is allowed only via eth0 interface.IP address of eth0 is set to 169.254.1.1Client PC should have an IP adress in network 169.254.0.0/255.255.0.0such as 169.254.1.2	

Click on Add Tab to add an IP/Network Address to Console Access Address.

IP/Network Address	Netmask
169.254.1.2	255.255.255.255
0.0.0.0	0.0.0.0
10.11.12.10	255.255.255.255
10.11.12.28	255.255.255.255
10.1.0.110	255.255.255.255
169.254.1.10	255.255.255.255
192,168.0.100	255 255 255 255

Below screen appears

Add Access Address	4	×
IP/Network Address	192.168.0.20	
Netmask	255.255.255.0	2
	Add	Cancel

1	IP/Network Address	Type IP/Network Address
2	Netmask	Type Sub Netmask

We can notice the IP/Network address in the Console Access Address

Netmask
255.255.255.255
0.0.0.0
255.255.255.255
255.255.255.255
255.255.255.255
255.255.255.255
255.255.255.255
255.255.255.0

Select the IP/Network Address and click on Edit button.

IP/Network Address	Netmask
169.254.1.2	255.255.255.255
0.0.0.0	0.0.0.0
10.11.12.10	255.255.255.255
10.11.12.28	255.255.255.255
10.1.0.110	255.255.255.255
169.254.1.10	255.255.255.255
192.168.0.100	255.255.255.255
192.168.0.20	255.255.255.0

We can Edit the IP/Network Address and click Apply.

Edit Access Address	×
IP/Network Address	192.168.0.21
Netmask	255.255.255.0
	Apply Cancel

We can notice the applied changes

IP/Network Address	Netmask
169.254.1.2	255.255.255.255
0.0.0.0	0.0.0.0
10.11.12.10	255.255.255.255
10.11.12.28	255.255.255.255
10.1.0.110	255.255.255.255
169.254.1.10	255.255.255.255
192.168.0.100	255.255.255.255
192.168.0.21	255.255.255.0

Select the **IP/Network Address** and click on **Remove** button, then it will be removed from the **Console Access Address**.

IP/Network Address	Netmask
169.254.1.2	255.255.255.255
.0.0.0	0.0.0.0
0.11.12.10	255.255.255.255
0.11.12.28	255.255.255.255
0.1.0.110	255.255.255.255
69.254.1.10	255.255.255.255
92.168.0.100	255.255.255.255
92.168.0.21	255.255.255.0

## **36. General Settings**

In System Module, right pane under System Tab click on General Settings.



Below screen will appear displaying Hostname, Internal network hostname/IP address, and Notification mail address.

Hostname							
Hostname	slav	e					
					Save		
Web Access Address							
Internal network host	name/IP ad	dress	localhost.localdomain				
					Save		
System Monitor Settings	System Monitor Settings						
Notification mail addr	resses	noreply	/@labristeknoloji.com				
					Save		

### **37. Trusted Time Stamp**

In System Module, rightpane under System tab select Trusted Time stamping



Below screen appears displaying settings and Previous Time Stamped Log Packages, select log/date/hash row click on Save Tab.

Turkey is valid within the boundaries of the "Law No. 5651" requirement;

content provider, provider, access provider and public liability and responsibilities of providers of certain crimes committed on the internet with the content relating to the fight over the location and access providers and procedures.

The item is provided on behalf of the meet.

Must be held according to law, and the mandatory or hits just set **cvars labris** UTM equipment that meets the requirement of the law in any way.

In the case of certain specified property on every day or **istenillmesiperiyorlarda** for the protection of the State against the log file, which consists of modified authorized the signing of the "TURK TRUST" side of the premises.

Select the Log file and click on Save

Date	Hash
2013/12/19 03:31:14	dd15edd089aa027db85798fc69a32d8b
2013/12/17 03:31:14	2e8db4c6e7e7c0bb19f62a0c180d1546
2013/12/14 03:31:33	b4a4c86d08b97d6ce8808fbbc31f7035
2013/12/13 03:31:32	f2040007556816e44067321fbc1b0126
2013/12/12 03:31:31	b30f65657d6bb4d2bf93f6dfa562a93a
2013/12/11 03:31:31	dc19a2d1042b4ad8ca4426e494951966
2013/11/28 03:31:29	22653e0793d95a6a745c13839f6e3722
2013/11/27 03:31:36	1a776447b0672bea97f188ea2b5ca541
2013/11/26 03:31:36	42f30a85986d2c1c13e491e678628cff

#### 38. Restart

In System Module, under **System Tab** click on **Reboot** to Reboot the System.

#### **39. Shutdown**

In System Module, under **System Tab** click on **Shutdown** to shutdown the System.



## **Network Settings**

In Network settings IP Configuration and Routing can be done for Labris UTM appliance.

In this section we can Add, Delete, Edit and View the Status of the Interface.

## **40.IP Configuration**

Labris Secure Gateway is a capable router, and it has many Ethernet interfaces both used for security and also routing, load balancing and many other network tasks. IP Routing is used to Configure Ethernet interfaces and routing configuration of Labris Security Gateway.

Right click on Network Settings and select Connect.

### IP Alias (Add, Edit, Delete, Status, Enable/disable)

Below screen appears select IP Configuration, click on Add button.



IP Configuration	Routing				
Interfaces					
Active	Device	Name	Туре	IP	
~	eth0		Ethernet	169.254.1.1	Add 💦
✓	eth1	OUTSIDE	Ethernet	10.11.12.221	
	eth2		Ethernet		- Darlah
✓	eth3	WAUTH	Ethernet	10.1.0.1	Delete
	eth4		Ethernet		
	eth5		Ethernet		Activate
					~~
					Edit
					Status

Choose **IP Alias** radio button from the types of **Interfaces**, Click on **Next** button to continue the process.

🛎 Labris IPRoute	- 🗆 🗙				
Labris Security Gateway Widget					
Labris lpRoute create wizard allows you create IP aliases and PPPol connections.Please select the interface type that you want to create	E				
Types IP Alias ADSL Bridge 3G Vlan					
Previous Next Last Einish	<u>C</u> ancel				

Configuration of the Alias connection.

营 Labris IPRoute	<u>- 🗆 ×</u>					
IP aliases gives you the ability to assign another IP address and netmask to an interface						
Alias Configu	ration					
Name	test 1					
IP Address	169.254.1.10 2					
Netmask	255.255.255.0 3					
Interface	eth0 4					
Interface eth0 4						

These are the inputs for the Configuration of Interface.

1	Name	Type the Name	
2	2 IP Give the IP Address		
	Address		
3	Netmask	Type the Netmask	
4	Interface	Select Interface from the drop down Menu	

Installation is finished, Click on Finish button.

😤 Labris IPRoute	- 🗆 🗙
Congratulations, it should be all setup	
Installation finished	
▲ Previous Next Last Finish	<u>C</u> ancel

Below screen appears, click on **close** button.



IP Configuratio	a Routing				
Interfaces					1
Active	Device	Name	Туре	IP	
✓	eth0		Ethernet	169.254.1.1	Add 🔧
[	eth0:0	test	IP Alias	169.254.1.10	
~	eth1	OUTSIDE	Ethernet	10.11.12.221	
<ul> <li>Image: A set of the</li></ul>	eth2	INSIDE	Ethernet	192.168.20.1	Delete
	eth2:9		IP Alias		
	eth2:10		IP Alias		Activate
	eth2:11		IP Alias		
	eth2:12		IP Alias		
	eth2:13		IP Alias		Edit
	eth2:14		IP Alias		
	eth2:15		IP Alias		-
	eth2:16		IP Alias		Status
	eth2:17		IP Alias		
<ul> <li>Image: A start of the start of</li></ul>	eth3	WAUTH	Ethernet	10.1.0.1	
	eth4		Ethernet		
	eth5		Ethernet		

We can notice the New interface added to the Interfaces list with **IP Alias connection**.

# Select the Interface and click on Activate button.

Active	Device	Name	Туре	IP	
~	eth0		Ethernet	169.254.1.1	Add 🎺
_	eth0:0	test	IP Alias	169.254.1.10	
~	eth1	OUTSIDE	Ethernet	10.11.12.221	
✓	eth2	INSIDE	Ethernet	192.168.20.1	
	eth2:9		IP Alias		6
	eth2:10		IP Alias		🔨 Activat
	eth2:11		IP Alias		
	eth2:12		IP Alias		
	eth2:13		IP Alias		Edit
	eth2:14		IP Alias		
	eth2:15		IP Alias		
	eth2:16		IP Alias		Status
	eth2:17		IP Alias		
✓	eth3	WAUTH	Ethernet	10.1.0.1	
	eth4		Ethernet		

Activation process is in progress.

Activate	×
Interface is beig activated	

Now we can notice that the newly added Interface is Active.

IP Configuration Routing							
Interfaces							
Active	Device	Name	Туре	IP			
	eth0		Ethernet	169.254.1.1			
	eth0:0	test	IP Alias	169.254.1.10			
~	eth1	OUTSIDE	Ethernet	10.11.12.221			
✓	eth2	INSIDE	Ethernet	192.168.20.1			
			ID All				

## **Editing IP Alias**

Select the Interface and click on **Edit** button to Edit the Interface.

IP Configuration	Routing				
Interfaces				1	1
Active	Device	Name	Туре	IP	
✓	eth0		Ethernet	169.254.1.1	Add 🔬
Image: A state of the state	eth0:0	test	IP Alias	169.254.1.10	
✓	eth1	OUTSIDE	Ethernet	10.11.12.221	
✓	eth2	INSIDE	Ethernet	192.168.20.1	Delete
	eth2:9		IP Alias		
	eth2:10		IP Alias		V Deactivate
	eth2:11		IP Alias	×	
	eth2:12		IP Alias		
	eth2:13		IP Alias	4	Edit
	eth2:14		IP Alias		-
	eth2:15		IP Alias		
	eth2:16		IP Alias		Status
	eth2:17		IP Alias		
✓	eth3	WAUTH	Ethernet	10.1.0.1	
	eth4		Ethernet		
	eth5		Ethernet		

Editing the **Alias configuration**, give the inputs and click on **Apply tab** to apply the changes.

Note

•Click on Save tab to save the changes in Configuration

Note: Click on Save tab to save the changes in configuration.



These are the inputs for **Editing** the Interface

1	Name	We can Edit the existing Name
2	IP Address	We can Edit the existing IP Address
3	Netmask	Give the Netmask for the given IP Address

After applying the changes, Interface will restart.

Restart process is in progress.

Restart	×
Restarting Interface	

We can notice the changes in the Interface in the Interfaces list.

IP Configuration	Routing			
Interfaces				
Active	Device	Name	Туре	IP
✓	eth0		Ethernet	169.254.1.1
Image: A state of the state	eth0:0	testsample	IP Alias	169.254.1.11
~	eth1	OUTSIDE	Ethernet	10.11.12.221
✓	eth2	INSIDE	Ethernet	192.168.20.1
	eth2:9		IP Alias	
	eth2:10		IP Alias	
	eth2:11		IP Alias	
	eth2:12		IP Alias	
	eth2:13		IP Alias	
	eth2:14		IP Alias	
	eth2:15		IP Alias	
	eth2:16		IP Alias	
	eth2:17		IP Alias	
✓	eth3	WAUTH	Ethernet	10.1.0.1
	eth4		Ethernet	
	eth5		Ethernet	

# Enable / Disable

Select the Interface and click on Deactivate button to deactivate the Interface.

25			1		
Active	Device	Name	Туре	IP	
✓	eth0		Ethernet	169.254.1.1	🛛 🕹 Add
~	eth0:0	testsample	IP Alias	169.254.1.11	
~	eth1	OUTSIDE	Ethernet	10.11.12.221	
~	eth2	INSIDE	Ethernet	192.168.20.1	
	eth2:9		IP Alias		
	eth2:10		IP Alias		V. Deactivat
	eth2:11		IP Alias		
	eth2:12		IP Alias		
	eth2:13		IP Alias		🔣 Edit
	eth2:14		IP Alias		
	eth2:15		IP Alias		0
	eth2:16		IP Alias		Status
	eth2:17		IP Alias		
✓	eth3	WAUTH	Ethernet	10.1.0.1	

## Status

### Select the Interface and Click on Status button to check the status of the Interface

IP Configuration Routing					
terfaces					
Active	Device	Name	Туре	IP	<b>"</b>
~	eth0		Ethernet	169.254.1.1	Add 💉
~	eth0:0	testsample	IP Alias	169.254.1.11	
~	eth1	OUTSIDE	Ethernet	10.11.12.221	
~	eth2	INSIDE	Ethernet	192.168.20.1	Delete
	eth2:9		IP Alias		
	eth2:10		IP Alias		Z Deactivate
	eth2:11		IP Alias		
	eth2:12		IP Alias		
	eth2:13		IP Alias		🔣 Edit
	eth2:14		IP Alias		
	eth2:15		IP Alias		- <u>~</u>
	eth2:16		IP Alias		Status
	eth2:17		IP Alias		
~	eth3	WAUTH	Ethernet	10.1.0.1	
	eth4		Ethernet		
	eth5		Ethernet		

Below screen gives the status of the Interface

Ethernet Stat	US				
RECIEVED	2.04 M	2045867	TRANSMITT Packets	ed 971.34 K	971342
Bytes	273.32 MB	286602294	Bytes	445.43 MB	467067233
Error	0		Error	0	
Dropped	244		Dropped	0	
Overruns	0		Overruns	0	
Frame	0		Carrier	0	

Right click on the Interface, to perform Edit, Activate, Deactivate, status, Delete, Edit groups, Activate groups, Deactivate groups actions.

IP Configuration	Routing			
Interfaces				
Active	Device	Name	Туре	IP
<ul> <li>Image: A start of the start of</li></ul>	eth0		Ethernet	169.254.1.1
✓	eth0:0	testsample	IP Alias	169.254.1.11
~	eth1	OUTSIDE	Ethernet	10.11.12.221
~	eth2	INSIDE	Edit	192.168.20.1
	eth2:9		Activate	
	eth2:10		Deactivate	
	eth2:11		Status	
	eth2:12		Delete	
	eth2:13		Edit Groups	
	eth2:14		Activate Group	
	eth2:15		Deactivate Group	
	eth2:16	l		
	eth2:17		IP Alias	
~	eth3	WAUTH	Ethernet	10.1.0.1
	eth4		Ethernet	
	eth5		Ethernet	

## ADSL (Add, Edit, Delete, Status, Enable/Disable)

Select IP Configuration and click on Add button

IP Configuration	Routing				<u> </u>
Interfaces					
Active	Device	Name	Туре	IP	
✓	eth0		Ethernet	169.254.1.1	Add 💦
✓	eth1	OUTSIDE	Ethernet	10.11.12.221	
	eth2		Ethernet		
✓	eth3	WAUTH	Ethernet	10.1.0.1	Delete
	eth4		Ethernet		
	eth5		Ethernet		Activate
					~*
					Edit
					Status

Choose **ADSL** from the types of Interfaces and click on **Next** button to continue.

🛎 Labris IPRoute	- 🗆 🗙				
Labris Security Gateway Widget 🧕					
Labris IpRoute create wizard allows you create IP aliases and PPPo connections.Please select the interface type that you want to create	E				
Types ○ IP Alias ○ ADSL ○ Bridge ○ 3G ○ Vlan Previous Next ► Last Einish	Cancel				

Choose the Ethernet Interface to the ADSL from the drop down list, check mark the default Gateway and click on **Next** button.

🛎 Labris IPRoute 📃 🗖 🗙					
Select the interface connected to your ADSL device					
Interface List					
Please choose the Ethernet interface connected to the ADSL mod.					
OUTSIDE (eth1) ▼ Select as default gateway ▼					
OUTSIDE (eth1)					
WAUTH (eth3) eth4					
leth5					
▲ Previous Next ▲ Last Einish Cancel					

User Information should be provided

💩 Labris IPRoute		- 🗆 🗙
User information is used connection	d for authenticating your ADSL	9
Authentication		
Login Te	estUser1	
Password •	•••••• 2	
Password (again) •	••••••	
▲ Previous Next	Last Einish	<u>C</u> ancel

These are the inputs for the User

1	Login	Type Login name of the User	
2	Password	Type the Password of the User	
3	Password (again)	Type the Password of the User again for	
		confirmation	

## ADSL

Configuration of ADSL connection.

😤 Labris IPRou	te	- 🗆 X	
Make sure all the information is correct			
ADSL conf	iguration vice will be created.		
Login	TestUser		
Interface	OUTSIDE (eth1) 2		
Device	ppp0 3		
▲ Previous	<u>Next</u> ▶ Last Einish	Cancel	

1	Login	It displays Login name of the User
2	Interface	It displays the Interface type

3 Device

It displays device name

Click on Next button to continue.

Once the installation is finished, Click on **Finish** button.



Below screen appears, click on close button.



We can notice Interface added in the Interfaces list with ADSL type of connection

IP Configuration	Routing			
Interfaces				
Active	Device	Name	Туре	IP
✓	eth0		Ethernet	169.254.1.1
✓	eth0:0	testsample	IP Alias	169.254.1.11
✓	eth1	OUTSIDE	Ethernet	10.11.12.221
	ррр0		ADSL	
~	eth2	INSIDE	Ethernet	192.168.20.1
	eth2:9		IP Alias	
	eth2:10		IP Alias	
	eth2:11		IP Alias	
	eth2:12		IP Alias	
	eth2:13		IP Alias	
	eth2:14		IP Alias	
	eth2:15		IP Alias	
	eth2:16		IP Alias	
	eth2:17		IP Alias	
✓	eth3	WAUTH	Ethernet	10.1.0.1
	eth4		Ethernet	
	eth5		Ethernet	

P Configuration Routing					
Active	Device	Name	Туре	IP	
~	eth0		Ethernet	169.254.1.1	Add 🌄
✓	eth0:0	testsample	IP Alias	169.254.1.11	
✓	eth1	OUTSIDE	Ethernet	10.11.12.221	
	ррр0		ADSL		Delete
~	eth2	INSIDE	Ethernet	192.168.20.1	
	eth2:9		IP Alias		Activate
	eth2:10		IP Alias		
	eth2:11		IP Alias		
	eth2:12		IP Alias		🛃 Edit
	eth2:13		IP Alias		
	eth2:14		IP Alias		
	eth2:15		IP Alias		Status
	eth2:16		IP Alias		
	eth2:17		IP Alias		
✓	eth3	WAUTH	Ethernet	10.1.0.1	
	eth4		Ethernet		
	eth5		Ethernet		

Select the Interface and click on **Activate** button to activate the **Interface**.

# Activation process is in progress

Activate	×
Interface is beig activated	

## Bridge(Add ,Edit, Delete, Status , Enable/disable)

🔹 Labris IPRoute	- 
Labris Security Gateway Widget	1
Labris IpRoute create wizard allows you create IP aliases and PPPo connections.Please select the interface type that you want to creat	e e
Types O IP Alias	
ADSL	
Bridge     3G	
🔿 Vlan	
Previous Next Last Einish	<u>C</u> ancel

To configure Bridge connection for the Interface select **Bridge radio button** from the types of connection.

Configuration of Bridge Connection screen.

🔮 Labris IPRoute	- 🗆 ×	
IP aliases gives you the ability to assign another IP address and netmask to an interface		
Bridge		
Bridge Interface	br0	
Bridge Name	TestBridge 1	
IP	192.168.0.110 2	
Netmask	255.255.255.0 3	
First Interface	OUTSIDE (eth1)	
Second Interface	eth4	
▲ Previous Next	Last <u>F</u> inish <u>C</u> ancel	

These are the inputs for Bridge connection

1	Bridge Name	Type the Bridge connection	
2	IP	Type the IP Address	
3	Netmask	Type the Netmask	
4	First Interface	Select the First Interface from the drop down list	
5	Second Interface	Select the Second Interface from the drop down	
		list	
# Interface Configuration process is in progress



Once the installation finished click on **Finish** button.

🖑 Labris IPRoute	×
Congratulations, it should be all setup	<b>1</b>
Installation finished	
▲ Previous Next Last Finish	<u>C</u> ancel

We can notice that the Interface is added in the Interfaces list with **Bridge** type of connection.

IP Configuration	Routing			
Interfaces				
Active	Device	Name	Туре	IP
✓	eth0		Ethernet	169.254.1.1
✓	eth0:0	testsample	IP Alias	169.254.1.11
✓	eth1	OUTSIDE	Ethernet	10.11.12.221
	ppp0		ADSL	
✓	eth2	INSIDE	Ethernet	192.168.20.1
✓	eth2:9	sampleuser1	IP Alias	192.168.0.201
	eth2:0		IP Alias	
	eth2:1		IP Alias	
	eth2:2		IP Alias	
	eth2:3		IP Alias	
	eth2:4		IP Alias	
	eth2:5		IP Alias	
	eth2:6		IP Alias	
	eth2:7		IP Alias	
	eth2:8		IP Alias	
	eth2:10		IP Alias	
	eth2:11		IP Alias	
	eth2:12		IP Alias	
	eth2:13		IP Alias	
	eth2:14		IP Alias	
	eth2:15		IP Alias	
	eth2:16		IP Alias	
	eth2:17		IP Alias	
✓ <b>、</b>	eth3	WAUTH	Ethernet	10.1.0.1
	eth4		Ethernet	
	eth5		Ethernet	
	br0	TestBridge	Bridge	192.168.0.110

Activation process is in progress.

Activate	×
Interface is beig activated	

Click on **Add** button to add an interface.

IP Configuration	Routing				
Interfaces					
Active	Device	Name	Туре	IP	
~	eth0		Ethernet	169.254.1.1	Add 🏹
~	eth1	OUTSIDE	Ethernet	10.11.12.221	
	eth2		Ethernet		
✓	eth3	WAUTH	Ethernet	10.1.0.1	Delete
	eth4		Ethernet		
	eth5		Ethernet		V. Deactivate
					Edit
					<u></u>
					Status

3G (Add, Edit, Delete, Status, Enable/disable)

To configure 3G connection for the Interface

Select **3Gbutton** from the types of connection.

🔹 Labris IPRoute	- 🗆 🗙
Labris Security Gateway Widget	1
Labris lpRoute create wizard allows you create IP aliases and PPPoE connections.Please select the interface type that you want to create	
Types O IP Alias	
ADSL	
Bridge	
◯ Vlan	
<u>Previous</u> <u>Next</u> <u>L</u> ast <u>Einish</u> <u>C</u>	ancel

Choose the service provider of the 3G modem from the drop down list, check the default gateway.



Scanning of 3G Modems process is in progress.

Modems List	×
Scannig Modems	

Then the below screen appears stating that, User information is used for authentication. Choose the **"Modem"** from the drop down list and enter the **"pin"** of the modem and click on **"Next"** to proceed further.

🖑 Labris IPRoute		- 🗆 X
User information is us connection	ed for authenticating your ADSL	1
Modem		
Modem	<b>v</b>	
Pin		No PIN
-		
	1	_
▲ <u>P</u> revious <u>N</u> ext ►	Last Einish	

Note – Since we don't have connection to the 3G modem, in the below screen message is displayed as "There is no plugged modem on the Labris device Please check your modem". Click on Cancel tab.

🖑 Labris IPRoute	- 🗆 🗙
User information is used for authenticating your ADSL connection	1
Modem	
Modem	
Pin	No PIN
There is no plugged modem on the Labris device. Please check your modem.	
▲ Previous Next Last Einish	Cancel

### **3G Release Note;**

- 1 Configuration of old generation 3G Modem
- Plug the modem into the USB port on the device.
- Labris Management Console is opened and accessed to the system with an authorized user name and password.
- By clicking on the add button on the right in the IP Configuration tab from the Network Settings Module the Labris Interface Wizard opens.
- The forward button is clicked by selecting the 3G on the opened screen.
- The service provider is selected on the next screen, and in case the added 3G shall be used as the default gateway the related box is selected and clicked on next button.
- In the next screen are the 3G modems listed on the modem line. The appropriate modem is selected and , if available, the pin entered, if no pin available then the" no pin" box is selected and clicked on the next button.
- On the next screen are the features of the configured modem listed, the PPP interface is created

by clicking on the next button.

- By clicking on end button on the next screen the interface wizard is closed.
- The created PPP interface is listed under interfaces.
- The related PPP interface is selected and enabled with the help of the "Activate" button on the right or right-clicking on the interface. Activation may last up to 1-2 minutes..
- The type, IP address, connection status, referrals status, signal status will be shown on the enabled interface.
- In case the added modem shall not be used as the default gateway and will be used as additional line it has to be saved as an additional line. For this, it can be added as a line by clicking on the advanced button on the Network Settings> Routing screen.
- The permission rule of the created interface is added to the firewall general policy.
- According to the usage status of the created interface in the firewall NAT policy the NAT rule is added and the modem is made available to use.

### 2. Configuration of new generation 3G modem

- The modem is plugged into the USB port on the device.
- The Labris Management Console is opened and accessed to the system with an authorized user name and password.
- Network settings module is opened. The new generation of devices plugged on the device is seen as ether interface. The latest added interface on the interface list is the interface of the modem.
- The IP address of the modem is usually example:192.168.1.1 or 192.168.2.1. We can give the IP address of the modem interface on the device in the same subnet with the modem interface by clicking on create on the right side, for example:192.168.1.2 or 192.168.2.2
- If the modem is selected as the default gateway the IP address of the modem is entered by selecting the related interface in the pre-defined network gateway from the Network Settings> Routing section and saved with the button in the bottom right.
- In case the added modem shall not be used as the default gateway and will be used as additional line it has to be saved as an additional line. For this, it can be added as a line by clicking on the advanced button on the Network Settings> Routing screen.
- The permission rule of the created interface is added to the firewall general policy.
- According to the usage status of the created interface in the firewall NAT policy the NAT rule is added and the modem is made available to use.

### Vlan (Add , Edit, Delete, Status , Enable/disable)

To configure VLAN for the Interface.

Select VLAN button from the types of connection.

🛎 Labris IPRoute	- 🗆 X
Labris Security Gateway Widget	<b>B</b>
Labris IpRoute create wizard allows you create IP aliases and PPPc connections.Please select the interface type that you want to creat	)E ;e
Types O IP Alias	
◯ ADSL	
O Bridge	
) 3G	
● Vian	
Previous Next Last Einish	<u>C</u> ancel

# Configuration of VLAN

👙 Labris IPRoute		- 🗆 🗙		
Virtual LANs (Vlans) networks to an inter	Virtual LANs (Vlans) give you the ability to assign multiple networks to an interface			
Vlan Configu	ration			
Name	VLAN11			
IP Address	10.1.13.1 2			
Netmask	255.255.255.255 3			
Vlan Tag	11 4			
Interface	eth5 5			
▲ Previous Nex	t▶ Last Einish	<u>C</u> ancel		

# These are inputs for configuration of VLAN

1	Name	Type the Name
2	IP Address	Give the IP Address
3	Netmask	Give the Netmask of the IP Address
4	Vlan Tag	Give the Tag of the Vlan
5	Interface	Choose the Interface from the drop down list

Click on Next tab to continue

# Interface Configuration process is in progress

Interface Configuration	×
Configuring Interface	

Installation finished click on Finish button.

🛎 Labris IPRoute	- 🗆 🗙
Congratulations, it should be all setup	<b>@</b>
Installation finished	
▲ <u>Previous</u> <u>N</u> ext <u>Last</u>	<u>C</u> ancel

Below screen appears, click on close button.

🔮 Labris IPRoute	- 🗆 🗙
Congratulations, it should be all setup	<b>B</b>
Installation finished	
	Close

In the below screen we can notice Interface, click on Activate tab to activate the Interface.

terfaces Rout	ing				
Active	Device	Name	Туре	IP	
~	tun0		Tunnel	10.8.3.1	Add 🌭
✓	eth0		Ethernet	169.254.1.1	
✓	eth1	OUTSIDE	Ethernet	10.11.14.221	Dalata
~	eth2	INSIDE	Ethernet	192.168.20.1	
~	eth3	WAUTH	Ethernet	10.1.0.1	
~	eth4		Ethernet		🔀 Activate
~	eth4.10	VLAN10	Vlan	10.1.13.1	× *
	eth5		Ethernet		
	eth5.11	VLAN11	Vian	10.1.13.1	📕 🥳 Edit
					Refresh

Activation process is in progress.

Activate	×
Interface is beig activated	

We can notice Interface is Activated in the below screen.

ing			
Device	Name	Туре	IP
tun0		Tunnel	10.8.3.1
eth0		Ethernet	169.254.1.1
eth1	OUTSIDE	Ethernet	10.11.14.221
eth2	INSIDE	Ethernet	192.168.20.1
eth3	WAUTH	Ethernet	10.1.0.1
eth4		Ethernet	
eth4.10	VLAN10	Vlan	10.1.13.1
eth5		Ethernet	
eth5.11	VLAN11	Vlan	10.1.13.1
	ing Device tun0 eth0 eth1 eth2 eth3 eth4 eth4.10 eth5 eth5.11	Device         Name           tun0         eth0           eth1         OUTSIDE           eth2         INSIDE           eth3         WAUTH           eth4         eth4           eth5         VLAN10	ing Device Name Type tun0 Tunnel eth0 Ethernet eth1 OUTSIDE Ethernet eth2 INSIDE Ethernet eth3 WAUTH Ethernet eth4 Ethernet eth4 Ethernet eth4 Ethernet eth4 Ethernet eth5 Ethernet

### 41. Routes

In **Routing tab** the touting table of Labris Secure Gateway is displayed. In this table you can see the

Destination, Mask, Default Gateway, Interface and Metric properties of each route. Destination is the destination IP or network; mask defines the destination host or network's Netmask, default gateway is next way point of the package. Interface is the interface which will be used for routing operation.

IP Configuration Rout	ing			
Destination	Mask	Default Gateway	Interface	Metric
10.1.0.0	255.255.255.0	0.0.0	WAUTH (eth3)	0
10.8.3.0	255.255.255.0	0.0.0		0
10.11.12.0	255.255.255.0	0.0.0.0	OUTSIDE (eth1)	0
169.254.0.0	255.255.0.0	0.0.0	eth0	0
Advanced				See Add
Coteway 10.11.12.1				
	1			
Interface OUTSIDE (eth1)				
Load Balancing Disabled	🤣 Enable			
				Save 🧖 Refresh

### **Default Gateway**

The Default gateway is the default next hop for every packet, when there is no explicitly specified gateway for destination of that packet. In order to change the default gateway firstly enter an IP address of the default gateway and choose an interface from which Packets are sent to the gateway.

r Default Gateway
Gateway 10.11.12.1
Interface OUTSIDE (eth1)
eth0
OUTSIDE (eth1)
Load Bala WAUTH (eth3) Enable

### **Static Route**

A static route is a manually configured mapping of an IP address to a next-hop destination.

A static route causes packets to be forwarded to a different next hop other than the configured default gateway. By specifying through which interface/gateway the packet will leave and to which device the packet should be routed, static routes control the traffic exiting Labris UTM.

### Add (Static Route)

**Add** static routes when you want to route traffic destined for specific network/host via a different next hope instead of a default route.

Click on Add button to add static route.

IP Configuration Routi	ng			
Destination	Mask	Default Gateway	Interface	Metric
10.1.0.0	255.255.255.0	0.0.0.0	WAUTH (eth3)	0
10.8.3.0	255.255.255.0	0.0.0.0		0
10.11.12.0	255.255.255.0	0.0.0.0	OUTSIDE (eth1)	0
169.254.0.0	255.255.0.0	0.0.0.0	eth0	0

Below screen appears.

R	loute Add		-		×
	Route				
	Destination	192.168.0.10	1		
	Mask	255.255.255.0	2	2	
	Gateway	192.168.0.1		3	
	Device	eth0	<b>▼</b> 4	_	
	Metric	• 🗘 5			
	,	Add	Cancel		

# These are the inputs to Add route

1	Destination	Give the Destination IP Address
2	Mask	Give the Netmask of the Destination IP Address
З	Gateway	Give the Gateway IP Address
4	Device	Choose Device from drop down list
5	Metric	Choose Metric value

Click on Add button.

We can notice Static route in the Routing list.

IP Configuration Routing					
Destination	Mask	Default Gateway	Interface	Metric	
10.1.0.0	255.255.255.0	0.0.0.0	WAUTH (eth3)	0	
10.8.3.0	255.255.255.0	0.0.0.0		0	
10.11.12.0	255.255.255.0	0.0.0.0	OUTSIDE (eth1)	0	
192.168.0.10	255.255.255.0	192.168.0.1	eth0	0	
169.254.0.0	255.255.0.0	0.0.0.0	eth0	0	

### **Delete (Static Route)**

Select the Static Route from the list and click on **Delete** button, to delete Static route.

IP Configuration	uting				
Destination	Mask	Default Gateway	Interface		Metric
10.1.0.0	255.255.255.0	0.0.0.0	WAUTH (eth3)	0	
10.8.3.0	255.255.255.0	0.0.0.0		0	
10.11.12.0	255.255.255.0	0.0.0.0	OUTSIDE (eth1)	0	
192.168.0.10	255.255.255.0	192.168.0.1	eth0	0	
169.254.0.0	255.255.0.0	0.0.0.0	eth0	0	
Advanced				1	Add Kalender

Load Balance (OLD)

Load Balance (NEW)

### 42. Load Balance

-----BEGIN NEW STUFF------BEGIN NEW STUFF------

Load balance module allows administrators to create Policy Based Rules using links and/or link groups. PBR allows administrators to write advanced route rules. User, group, ip based rules can be written to specific destinations over chosen links or link groups. Also for network stability administrators can add backup links and link groups. To load balance traffic between links administrators can create link groups.

### MAIN SCREEN



No	Name	Description
1	Link and Link Groups	Manage all links and link groups
2	Policy Based Routing	Manage all policy based routing rules (PBR)
3	Add Link	Create a new link to use in a link group or in a PBR.
4	Add Link Group	Create a new link group to use in a PBR.
5	Edit Link/Link Group	Edit an existing link or link group.
6	Delete Link/Link Group	Delete an existing link or link group.
7	Link Groups	Link groups section.
8	Links	Links section.
9	Add PBR	Create a new policy based routing rule.
10	Edit PBR	Edit an existing policy based routing rule.
11	Delete PBR	Delete an existing policy based routing rule.
12	Default Route	Default gateway written in Route tab is automatically written as last rule of PBR.
13	Load Balance Service Status	Service status. PBR rules only work when service status is "Running".
14	Start Service	Start service.
15	Stop Service	Stop service.
16	Restart Service	Restart service.
17	Save Changes	Save changes.
18	Refresh Screen	Refresh everything in the screen.

### Add Link Screen



No	Name	Description
1	Link Name	Name of the new link.
2	Gateway	Gateway IP address of new link.
3	Interface	Interface of new link.
4	Ping Address Input	Use this field to add a new ping ip address.
5	Add Ping Address	Add the value in Ping Address Input.
6	Edit Ping Address	Edit selected ping address.
7	Delete Ping Address	Delete selected ping address
8	Ping Addresses	Show all ping addresses. To edit/delete, select one.
9	Add Link	Save new link
10	Cancel	Cancel.

### Add Link Group Screen

oup Name				
ks			Links in this group with weight (You	can edit the weight value in the tal
Link Name	Gateway	Interface	Link Name	Weight
eth3	10.101.0.201	eth3	5	
ethl	10.100.0.201	eth1		

No	Name	Description
1	Group Name	Name of the new link group.
2	All Links	Available links for adding to this link group.
3	Add link to group	Add selected link to link group (left -> right)
4	Remove link from group	Remove selected link from group. (left <- right)
5	Links in this group	Selected links in this link group.
6	Create Link Group	Create this link group.
7	Cancel	Cancel.

Network traffic going through link group is load balanced between links in the link group according to links' weights. Also links in a link group are failovered, network traffic is not redirected to down links.

# Add Policy Based Route Screen

Add Policy Based Route	×
Add Policy Based Route - 1	
Sources	
Add IP or Network	K Delete
4 Source J Type	
Destination	
Add IP or Network 🚔 Add Users or Groups	& Delete
Destination Type	
<b>)</b>	
3 Link and Link Backup	
Link / Link Group	<b>_</b>
Link / Link Group Backup 8 eth3	-
🗳 Add	💥 Cancel
9	10

No	Name	Description
1	Sources	Sources for this policy based routing rule.(PBR)
2	Destinations	Destinations for this policy based routing rule.
3	Link and Link Backup	Link and link backup choice for this PBR.
4	Add IP or Network	Add a new IP or network to this PBR. Examples: 192.168.0.5, 192.168.0.0/24, 10.0.20.0/255.0.255.0
5	Add Users or Groups	Add User or Group
6	Delete	Delete selected IP/Network/User/Group.
7	Link/Link Group	Configure link choice for this PBR.
8	Backup Link / Backup Link Group	Enable/Disable backup link choice for this PBR.
9	Add Policy Based Route	Save changes.
10	Cancel	Cancel.

Backup links/link groups are activated if main link is down or if all links in the main link group are down. Backup links/link groups are active until main link is up or one of links in main link group's is up again.

Policy Based	d Routing			
🌵 🖶	🥒 Edit 🛛 🗶 Delete			
Id	Source	Destination		Link
1	aliler@u20	0.0.0/0		eth3 (link)
2	0.0.0/0	0.0.0.0/0	la	bris_group (link_group)
3	0.0.0/0.0.0.0	Move this rule to top	_1	eth3 (link)
		or Move this rule to end	2	
		🔷 Insert Rule at the top	3	
		🕲 Insert Rule above this ru	ıle <mark>4</mark>	
		🍭 Insert Rule below this ru	le <mark>5</mark>	
		Move this rule up	_ <mark>6</mark>	
	N	Ø Move this rule down	7	
	14			1

### Policy Based Route Right Click

No	Name	Description
	Move to top	
1		Move selected rule to the top.
	Move to end	Move selected rule to the end.
2		
	Insert at top	
3		Insert a rule at top.
	Insert above	
4		Insert a rule above the selected rule.
	Insert below	
5		
	Move up	
6		
	Move down	
7		

### -----END NEW STUFF-----

-----BEGIN OLD STUFF-----

Load balance can be configured based on following types

- Configuring a virtual web server with three real web servers
- Adding a server load balance port forwarding virtual IP
- Weighted load balancing configuration
- HTTP and HTTPS persistence configuration
- Packet load balance or destination load balance

By default Load Balance is in disable mode, click on Enable button.

Default Gateway
Gateway 10.11.12.1
Interface OUTSIDE (eth1)
Load Balancing Disabled 🧹 Enable

When Load Balance is enabled Gateways section with the fields **Gateway**, **Interface**, **Weight**, **Reachable**, **Router** are seen

Gateways					
Gateway	Interface	Weight	Reachable	Router	🔮 Add 🛛 🗶 Remove
10.11.12.1	OUTSIDE (eth1)	1	2	٢	🖉 Edit 🧠 Settings
Load Balancing Enabled 🏼 🎉 I	Disable				

# Add (Load Balance Route)

Click on Add tab to add Gateway

	Gateways						
	Gateway	Interface	Weight	Reachable	Router	🖨 Add	🔀 Remove
	10.11.12.1	OUTSIDE (eth1)	1	3	3	A Edit	Cottings
						J Eun	- Settings
L	and Polonging Enchlad	aabla					
Ľ		sable					

### Below screen appears

	×
Gateway Edi	t
IP Address 19	2.168.0.10
Interface et	10 2 🔻
Weight	1 🗘 🔒
$\sim$	
	OK Cancel

These are the inputs to add Gateway.

1	IP Address	Type IP Address
2	Interface	Choose the Interface from the drop down list
3	Weight	Choose Weight value

# Click **Ok** to add Gateway

### We can notice Gateway added in the below screen

Gateways							
Gateway	Interface	Weight	Reachable	Router	👍 Add 🛛 🗶 Remove		
10.11.12.1	OUTSIDE (eth1)	1	٢	٨			
192,168.0,10	eth0	1	2	3	Settings		
Load Balancing Enabled	💥 Disable						

# Edit (Load Balance Route)

Select the Gateway and click on Edit tab to Edit the Gateway

Gateways						
Gateway	Interface	Weight	Reachable	Router	🔪	
10.11.12.1	OUTSIDE (eth1)	1	2	2		
192.168.0.10	ethO	1	3	3	Settings	
Load Balancing Enabled 🔀 Disable						

### Below screen appears

		×
Gateway E	dit	1
IP Address	192.168.0.1	
Interface	eth0 2	•
Weight	1 +	3
	OK Cancel	_

These are the inputs to edit gateway

1	IP Address	We can Edit the existing IP Address
2	Interface	We can Edit Interface (Optional)
3	Weight	We can Edit Weight value (Optional)

Click Ok to apply changes

### **Delete (Load Balance Route)**

Select the Gateway and click on Remove tab to remove gateway

Gateways						
Gateway	Interface	Weight	Reachable	Router	🔮 Add	🔀 Remove
10.11.12.1	OUTSIDE (eth1)	1	2	٢	A = 11	0.0.11
192.168.0.1	eth0	1	3	3	JE Edit	Settings
Load Balancing Enabled 🎽	Disable					

# We can notice Gateway removed from the list in the below screen

Gateways					
Gateway	Interface	Weight	Reachable	Router	🔮 Add 🛛 🗶 Remove
10.11.12.1	OUTSIDE (eth1)	1	٨	٨	📝 Edit 🐁 Settings
Load Balancing Enabled	💥 Disable				

# 43. Advanced/ Policy Based Routing

# Click on Advanced Tab

Destination	Mask 255.255.255.0	Default Gateway	Interface	Metric
10.1.0.0 2	255.255.255.0	0.0.0.0		
10.0.2.0			WAUTH (eth3)	0
10.0.3.0 2	255.255.255.0	0.0.0.0		0
10.11.12.0 2	255.255.255.0	0.0.0.0	OUTSIDE (eth1)	0
169.254.0.0 2	255.255.0.0	0.0.0.0	eth0	0
				••••••••••••••••••••••••••••••••••••••

Advanced Routing Table × Links Configuration Link Name Gateway Interface 👍 🐣 nain 10.11.12.1 eth1 🗶 Remove Decision Table 🐥 Add Source Destination Link 🗶 Remove

Save 🔄 Refresh 🗙 Cancel

There are two sections in the Advanced Routing table:

Upper section is for link configuration and the other one is for decision configuration. A Link is a virtual "link" for packets to a specific interface and a gateway. By defining decisions, one can redirect a package to a link based on the package's source and destination IP or network addresses.

Down

### **Link Configuration**

A Link is represented by a name, a default gateway and an interface.

To create an Interface, click on **Add** button in the Link Configuration table.

Links Configuration						
Link Name	Gateway	Interface	🖓 Add			
main	10.11.12.1	eth1	X Remove			

Below screen appears to create a New Gateway

Link Edit	×
Link Name Testlink 1	
Default Gateway 192.168.0.1 2	
Interface eth0 🔽 3	
add cancel	

These are the inputs to add Link

1	Link Name	Type the Name of the Link
2	Default Gateway	Give the Default Gateway
3	Interface	Choose the Interface from the drop down list

Click on Add tab

We can notice New  ${\bf Link}$  added in the Link Configuration in the below screen

Links Configuration —			
Link Name	Gateway	Interface	🔗 Add
main	10.11.12.1	eth1	2 Remove
Testlink	192.168.0.1	eth0	

### **Decision Table**

A Decision is represented by source IP/network, destination IP/network and the link name to which the packages are redirected.

To add new decision, click on Add tab

Source	Destination	Link	🚽 🖓 Add
			🗶 Remov
			🔺 Up
			Down

Below screen appears

Decision Add	×
Please type an ip address or select a user or group	$\mathbf{X}$
From salih	Add User or Group
To testgroup1768 2	Add User or Group
Link main (10.11.12.1)	
Add Cancel	

(OR)

Decision Add	×
Please type an ip address or select a user or o	group
From 192.168.20.0/24	Add User or Group
To 0.0.0.0	Add User or Group
Link Testlink (192.168.0.1) 💌	
Add Cancel	

These are the inputs to add **Decision** 

1	From	Click on Add User or Group and browse User or Group as
		Source or we can give the IP address
2	То	Click on Add User or Group and browse User or Group as
		Destination or provide the IP address
3	Link	Choose Link from the drop down list

### Click on Add tab

•Source IP can also be mentioned in the **From tab** instead of browsing User or Group.

•Destination IP can also be mentioned in the **To tab** instead of browsing User or Group

### We can notice **Decision** added in the **Decision table** in the below screen

Decision Table			
Source Destination Link		Link	Add
salih	testgroup1768	main	X Remove
			M Up
			Down

Click on Save button to save newly added Link and Decision to the Advanced Routing Table.

main	10.11.12.1	eth1	Add 🖓 =
Testlink	192.168.0.1	eth0	Remove
Decision Table			
Source	Destination	Link	🚔 Add
-		and a loss	
salih	testgroup1/68	main	🛛 🄀 Remove
salih	testgroup1768	main	Remove

1	Save	It enables us to Save changes made to the
		Advanced Routing Table
2	Refresh	It enables us to Refresh Advanced Routing Table
3	Cancel	It enables us to Cancel and close the tab

Saving and Applying Links and Decisions is in progress.



Select the Link and click on Remove tab to remove Link from Link Configuration.

main 10.11.12.1 eth1
Testlink 192.168.0.1 eth0

We can notice Link is removed from the Link Configuration.

Links Configuration -			
Link Name	Gateway	Interface	🖨 Add
main	10.11.12.1	eth1	Remove

Select the Decision and click on **Remove** tab to remove Decision from the Decision table.

Decision Table			
Source	Destination	Link	Add 🍄
salih	testgroup1768	main	Remove
			N Remove
			📥 Up
			Down

Click on Save tab to save the changes made to the Routing.

Click on Refresh tab to refresh Routing.

IP Configuration Ro	uting							
Destination	Mask	Defau	It Gateway	Interface	Metric			
10.1.0.0	255.255.255.0	0.0.0.0	WA	JTH (eth3)	0			
10.8.3.0	255.255.255.0	0.0.0.0			0			
10.11.12.0	255.255.255.0	0.0.0.0	OU	TSIDE (eth1)	0			
169.254.0.0	255.255.0.0	0.0.0.0	eth	)	0			
Advanced					Add Selet			
Gateways	Interface	Weight	Reachable	Router	🐥 Add 🛛 🗶 Remove			
10.11.12.1	OUTSIDE (eth1)	1	3	٨	<b>Edit</b> Settings			
Load Balancing Enabled	ad Balancing Enabled 🔀 Disable							

### Saving process is in progress

Labris IProute	х
Saving static routes	

# WAN failover (WAN Backup)

By default load balance is disabled, Click on **enable tab**, to make Load balance Enable.

In the below screen we can notice Load Balance Enabled

terfa	ace		Weight	Reachable	Router	🗳 Add 🛛 🗶 Remove
E (et	th1)	1		×	¥	
E2 (	eth4)	1		×	×	Settings
						Equa Defeada

### Click on Add tab

the second	Midah	Default Gateway	Interface	Metho
95.175.1.0	255 255 255 252	0.0.0.0	OUTSIDE2 (eth4)	0
0.1.0.0	255.255.255.0	0.0.0.0	WAUTH (eth3)	0
0.1.13.0	255.255.255.0	0.0.0.0	INSIDE2 (eth5)	0
0.8.3.0	255 255 255 0	0.0.0	tun0	0
0.11.12.0	255.255.255.0	0.0.0.0	OUTSIDE (eth1)	0
92 168 20 0	255.255.255.0	0.0.0.0	INSIDE (eth2)	0
69.254.0.0	255.255.0.0	0.0.0.0	eth0	0
	Gatewo IP Add Interfa Weigh	ay Edit ress ce INSIDE (eth2) 👻	x ] 1 ]2	
Advanced	Gatew IP Add Interfa Weigh	ay Edit ress ce INSIDE (eth2) • t 1 • 3 OK Cancel	x ] 1 ]2	Add 🔀 D
Advanced Sateways Gateway	Gatew IP Add Interfa Weigh	ay Edit ress ce INSIDE (eth2) t 1 OK Cancel Weight Reach	x 1 2 able Router	Add 🏾 🎉 Di
Advanced Sateways Gateway 10.11.12.1	Interface OUTSIDE (eth1)	ay Edit ress ce INSIDE (eth2) t 1 OK Cancel Weight Reach: 1	x 1 2 able Router	Add Solar Poly Add Rem

These are the inputs for the Gateway Edit.

2       Interface       Choose Interface from the drop down lis         3       Weight       Select Weight. Weight of the distribution ratio between each of the two represent default gateway	1	IP Address	Type IP Address
3 Weight Select Weight. Weight of the distribution ratio between each of the two represent default gateway	2	Interface	Choose Interface from the drop down list
deladit Satemay.	3	Weight	Select Weight. Weight of the distribution ratio between each of the two represents default gateway.

Click on Ok tab.

We can notice one interface in active mode.

Gateway	Interface	Weight	Reachable	Router		🔮 Add	🔀 Remove
10.11.12.1	OUTSIDE (eth1)	1	¥	¥		A	A
195.175.1.2	OUTSIDE2 (eth4)	1	×	×	-	🖉 Edit	Settings
oad Balancing, Enabled	💥 Disable						

# WAN Failover using CLI

When more than one internet line is used for active-passive in-line redundancy then in that case truncation of the preferred line is the second line, in the second line of the first line again when auto and auto disable.

This process is carried out via the CLI.

These are the following command lines.

### Information

WAN1 IP Address:10.10.10.2/30

WAN1 Gateway: 10.10.10.1

WAN2 IP Address:20.20.20.2/30

WAN2 Getaway: 20.20.20.1

LAN IP Address: 192.168.168.0/24

DMZ IP Address: 10.0.0/24

### **WAN Failover Configuration**

### Step 1:

The configuration file patch

NOTE: Open CLI and Open conf file for editing using the below command

vim /opt/labris/etc/sysconfig/labris-trigger.conf

The following is the configuration file, you can use your own network ip addresses contained in the update according to the requirement.

### #It's starting

#NOTE : Default GW for WAN1 (Active)
route1 = "10.10.10.1"

#NOTE : WAN1 up Interface
route1.iface = "eth1"

#NOTE : WAN1 live checkup the line will make the control of the external environment, ip addresses. route1.ping = "144.122.166.1 195.175.39.40"

#NOTE : WAN1 in the absence of the line to the following line in this line.
route1.action.NOT\_ROUTER = "\
echo ---METRO ETHERNET1DOWN--- | logger \
route del default gw10.10.10.1 \

#NOTE : Add a new route for backup link WAN2
route add default gw20.20.20.1 \

#NOTE: Users are added to the Internet through a NAT policy to WAN2.The IP address of the LAN. If more than one of the same row is copied only ip addresses are changed. iptables -t nat -I POSTROUTING -o eth2 -s 192.168.168.0/24 -j SNAT --to-source 20.20.20.2 \ iptables -t nat -I POSTROUTING -o eth2 -s 10.0.0.0/24 -j SNAT --to-source 20.20.20.2 \

#NOTE : updates the settings for the web filter
/etc/init.d/labris-webfilter reload \

echo "---SNAT changed to METROETHERNET1" | logger"

#NOTE: Check the status of the line would last WAN1 3 second route1.action.ROUTER = " \ echo ---METRO ETHERNET 1 UP--- | logger \

#NOTE : If the WAN1 WAN2 to stand up for the route will be deleted. route del default gw20.20.20.1 \

#NOTE :WAN1 to route again.
routeadd default gw10.10.10.1 \

//NOTE: Delete old rule for WAN2 iptables -t nat -D POSTROUTING -o eth2 -s 192.168.168.0/24 -j SNAT --to-source 20.20.20.2 iptables -t nat -D POSTROUTING -o eth2 -s 10.0.0.0/24 -j SNAT --to-source 20.20.20.2

//NOTE: updates the settings for the web filter
/etc/init.d/labris-webfilter reload \

echo "---SNAT changed to METRO ETHERNET1" | logger" route2 = "20.20.20.1" route2.iface = "eth2" route2.ping = "144.122.166.1 195.175.39.40" route2.action.UNREACHABLE = "echo ---METRO ETHERNET 2DOWN--- | logger" route2.action.REACHABLE = "echo ---ADSLMODEMUP--- | logger" route2.action.ROUTER = "echo ---ADSL-LINE-UP--- | logger"

route2.action.NOT\_ROUTER = "echo ---ADSL-LINE-DOWN--- | logger"

/etc/init.d/labris-trigger restart

#It's finished

Step 2:

Add Advance routing on the new gateway for wan2.

Click on Advanced option under Routing in Network Settings tab.

Click on **Add** tab to add a link.

IP Configuration Routing	ע			
Destination	Mask	Default Gateway	Interface	Metric
10.1.0.0	255.255.255.0	0.0.0.0	WAUTH (eth3)	0
10.8.3.0	25 Advanced Routing Table		×	0
10.11.12.0	25			0
192.168.20.0	25 Links Configuration			0
169.254.0.0	25 Link Name C	Gateway Interface	🔂 🔂	0
	main 10.11.	.12.1 eth1	Remove	
	Decision Table			
	Source De	estination Link	🔮 Add	
a			X Remove	
			Down	
	<b>m</b> . <b>m</b>			
	🔁 Save 🤤	Refresh X Cancel		
Advanced				Mdd X Delete

Give the **Link Name**, mention **Default Gateway** and choose **interface** from the drop down list and click on **Add** tab.

Links Config	uration -				
Link Na	ame	Gatewa	ay	Interface	💮 💮 Add
main		10 11 12 1		oth1	
	Link	Edit			×
	Link				
	Link	Name	WAN2	2	
Decision Ta	bl Defa	ault Gateway	20.20	.20.1	
Sour	ce Inte	face	INSIE	DE (eth2) 🔻	t
				add cance	JVe
		E Dofra	ah	V Canaal	n

We can notice new Link added to the Link Configuration table.

Under Decision Table click on Add tab.

Links Configuration			
Link Name	Gateway	Interface	🖶 Add
main	10.11.12.1	eth1	Remove
WAN2	20.20.20.1	eth2	
Decision Table			
Decision Table Source	Destination	Link	- Add
Decision Table Source	Destination	Link	Add
Decision Table Source	Destination	Link	Add Remove
Decision Table Source	Destination	Link	Add Remove

# Step 3:

Add a source/policy base route on the decision table for DMZ and LAN network.

Mention Source and Destination IP address and choose Link from the drop down list.

Click on Add tab.

Advanced Routing Table	×
Links Configuration	
Decision Add	×
Please type an ip address or select a user or group	
From 10.0.0/24	Add User or Group
То 0.0.0.0	Add User or Group
Link WAN2 (20.20.20.1)	
Add Cancel	
	Down -
💾 Save  😫 Refresh 🗶 Cancel	

In the below screen, we can notice Decision added in the Decision table.

navan ssa n saang i	able		×
Links Configuration			
Link Name	Gateway	Interface	🗳 Add
main	10.11.12.1	eth1	2 Remove
WAN2	20.20.20.1	eth2	~ remove
Decision Table			
Source	Destination	Link	🔗 Add
Source 10.0.0/24	Destination all	Link WAN2	🔮 Add 🔀 🧩 Remove
Source 10.0.0.0/24	Destination all	Link WAN2	Add Remove
Source 10.0.0.0/24	Destination all	Link WAN2	Add Remove

# **Firewall**

Firewall is software which controls the traffic of incoming and outgoing by analyzing the data packets which is allowable or not in a network. It serves as a gate keeper between severs and outside of the world.

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet.



Right click on Firewall and select Connect.



# 44. Make a new firewall object

A firewall is a rule that describes us what all the incoming connections that are accepted by which instances. Each firewall contains one rule, which specifies a permitted incoming connection request, defined by source, destination, ports, and protocol.

By default, all incoming traffic from outside a network is blocked and without an appropriate firewall rule, no packet is allowed into an instance. You need to set up firewalls to allow incoming network traffic to permit these connections. Each firewall represents a single rule that determines what traffic is permitted into the network. It is possible to have many firewall rules and to be as general or specific as we would like.

When we get connected to Firewall, below screen appears.

By default Labris Demo is displayed.
Policy	Object	Insert Rule	▶ Install	Connections	IP-MAC Matcher
Policys	Compile, save and Ins	tall the rules of Labris_Demo			J
Cobjects Cob	Opened Policy Save Date :30 Dec Current Active Policy Save Date :30 Dec Previous Active Polic Save Date :30 Dec	Compile, save and Install the rules of Labris_Demo Opened Policy :Policys Save Date :30 Dec 2013, 10:25:05 Current Active Policy :Policys Save Date :30 Dec 2013, 10:25:05 Previous Active Policy:Policys Save Date :30 Dec 2013, 10:21:44			
Labris_Demo	Save		Install Policy		Sollback
Image: Constraint of the second s	Properties of Labris_D Ciemeral Opt Name Labris_Demo	emo (Firewall)	ecting		
	Apply				<table-cell-rows> Cancel</table-cell-rows>
ected to is: 78.188.50.48					Labris Teknoloji

Right click on Policy, Select New Policy



It consists of two fields, Name and Network Interfaces.

In the Name tab, name of the new firewall object should be mentioned.

### Network Interfaces with Name, IP , Mask are selected by default.

Click on **Add** tab.

	×
Make a new Firewall object	
NewsampleObject	
Mask: 255 . 255 . 0 . 0	
Network Interface	
Name eth1	
IP: 10.11.12.221	
Mask: 255 . 255 . 255 . 0	
Network Interface	▼
Add	<b>5</b> Cancel

We can notice new firewall object under firewall.

It consists of two fields.

**Compile, Save and Install the rules of new firewall object** field displays information regarding newly added object to the firewall.

Properties of new firewall object displaying General, Options, Notes, SSH Inspecting.

Under General tab, the name of the new firewall object is displayed

Policy	Object	Insert Rule	▶ Install	Connections	IP-MAC Matcher
Default	-Compile, save and Ins	stall the rules of NewsampleObject			
Objects     Objects     Services     OoS & DDoS     OoS & DDoS     OoS/Bandwidth     Schedule     Application Control     Firewall     OoS & NAT Policy     OoS & tun0     ened Policy Save Date : Current Active Policy Save Date :30 Dec Previous Active Polic Save Date :30 Dec	:Default 2013, 10:25:05 9:Policys 2013, 10:21:44				
tin tin tin tin tin tin tin tin tin tin	: 📃 <u>S</u> ave		Install Policy		<table-cell-rows></table-cell-rows>
	Properties of Newsam General Opt Name NewsampleObject	pleObject (Firewall)	ecting		

Under Options tab, we can checkmark options like Firewall is part of "ANY", Accept TCP sessions opened prior to firewall installation, Accept ESTABLISHED and RELATED packets before and click on Apply tab to apply these rules to the firewall object.

Properties of NewsampleObject (Firewall)	
Ceneral Outions Notes SSH Inspecting	
delierur Synams Notes San Inspecting	
Firewall is part of "Any"	
Accent TCP sessions opened prior to firewall installation	
Accept ESTABLISHED and RELATED packets before first rule	
Apply	Cancel
• орру	• Cancer

Under **Notes tab**, we can describe any points regarding new firewall Object and click on **Apply tab**.

Properties of N	ewsampleObje	ct (Firewall	()	
General	Options	Notes	SSH Inspecting	
Notes		·		
New firewal	lobject			
Apply			4	Cancel

#### SSH inspecting

SSH inspecting is a unique security solution which enables both real-time inspection, and full replay of SSH, SFTP, Telnet, and RDP traffic and sessions to meet compliance, governance, auditing, and forensics requirements in enterprises and government entities.

In SSH Inspecting tab, we can check mark options like Allow HTTP request through ssh port forwarding, Allow scp, Allow shell login, Allow sftp and click on Apply tab to apply them to the firewall object.

<ul> <li>Properties of NewsampleObject (Firewall)</li> </ul>		
General Options Notes	SSH Inspecting	
Allow HTTP request through ssh	) port forwarding	
Allow scp		
Allow shell login		
Allow sftp		
Apply		숙 Cancel

Click on Save tab to save changes.

Policy	Object	Insert Rule	▶ Install	Connections	IP-MAC Matcher
Default	Compile, save and Ins	tall the rules of NewsampleObjec	t		
Objects Network Objects Services DoS & DDoS QoS/Bandwidth Schedule Application Control Firewall Firewall Schedule HowsampleObjection Schedule HowsampleObjection	Opened Policy Save Date : Current Active Policy Save Date :30 Dec Previous Active Polic Save Date :30 Dec	:Default :Policys 2013, 10:25:05 y:Policys 2013, 10:21:44			
tin4 . tin4 . tin4 . tin4 .	Save		Install Policy		<b>S</b> Rollback

Input tab appears, Give the name of the **New file** (new firewall object name) and click on **Ok** to close the current tab.

Input		×
$\bigcirc$	New filename:	
NewsampleObject		
	OK Cancel	

Below screen appears stating that "New sample Object have been saved successfully" click Ok to close the current tab



# 45.Objects

Firewall rules can be created in an object-oriented design. A firewall object is a named collection that represents specific networks, services, or connections. Using firewall objects gives you the following advantages:

• Each object has a unique name that is more easily referenced than an IP address or a network range.

• Maintenance of the firewall rules is simplified. When you update a firewall object, the change is automatically updated in every rule that uses the object.

The Firewall objects are a prime example of those building blocks. They are something that can be configured once and then used over and over again to build what you need. They can assist in making the administration of the LABRIS UTM unit easier and more intuitive as well as easier to change. By configuring these objects with their future use in mind as well as building in accurate descriptions the firewall will become almost self-documenting. That way, months later when a situation changes, you can take a look at a policy that needs to change and use a different firewall object to adapt to the new situation rather than build everything new from the ground up to accommodate the change.

Objects folder consists of Network Objects, Services, Dos &DDOS, QoS/Bandwidth, Schedule, Application Control, Firewall.



### **Network Objects**

Network objects are used to categorize IP addresses into different types of network entities. These network entities are then used to represent sources and destinations in the access rules, publishing rules, cache rules, traffic chaining rules, and HTTP compression settings that make up your firewall policy.

Expand Network Objects.

It consists of Hosts, Networks, Address Ranges, Object Groups, Users.



### Brief Summary about each of the parameters in Network Objects:

1	Hosts	It enables us to Add new Host
2	Networks	It enables us to Add new Networks
3	Address Ranges	It enables us to Create new Address
		Range
4	Objects Groups	It enables us to Add new Object Groups

#### Hosts



Expand Hosts, by default it consists of three Hosts.

# They are INSIDE, OUTSIDE, WAUTH



Right click on Hosts to Add new Host.



Below screen appears, Select General tab.

It consists of two fields, Name and Interfaces.

In the Name tab, name of the new Host Object should be mentioned.

These are the inputs for the Interfaces:

1	Name	Type the name of the Interface
2	IP	Give the IP Address of the Interface
3	MAC(Optional)	Give the MAC Address (Optional)

Make a new Host object General Notes	
Name	
Interface	
Name intertace1	
MAC(optional):00:00:00:	00:00:00
Add Cancel	X Delete:

Click on Add tab to Add new Host.

Select Notes tab to provide information about the newly added Host and click on Apply tab.

**Cancel** tab helps to cancel the Notes.

General Notes	
New Host is added to the Network objects Interface of Newhost is 1 IP Address:10.0.0.1	
Apply Sca	incel

We can notice newly added Host under the Hosts list with selected type of the Interface.



Right click on added Host, to perform actions like viewing **Properties** of the Host, to find out where it is used, **copying** Host, **Deleting** Host and **Adding new Interface** to the Host.



To Add new Interface to the Host, Right click on the Host select Add new Interface tab.



Below screen appears, Select General tab.

It consists of two fields, Name and Interfaces.

In the Name tab, name of the new Interface should be mentioned.

These are the inputs for the Interfaces:

1	IP	Give the IP Address of the Interface
2	MAC(Optional)	Give the MAC Address (Optional)

Make a new Host Interface Object
General Notes
Name
New531
Interface
IP:10.0.21
MAC(optional):00:00:00:00:00:00
Add Cancel Cancel

Click on Add tab.

We can notice the newly added Interface under the New Host.

Right click on the Interface to perform actions like viewing **Properties** of the Interface, to find out where it is used, **copying** Interface, **Adding new IP address** to the Interface, **Adding new MAC address** to the Interface and **Deleting** Interface.



We can notice Interfaces for the newly added Host in the below screen.



#### Networks



Expand Networks, by default it consists of two Network

They are Standard and User Defined networks



# Right click on Networks, to Add new Network



Below screen appears, Select General tab.

It consists of two fields, Name and Interfaces.

In the Name tab, name of the new Network object should be mentioned.

These are the inputs for the Interfaces:

1	IP	Give the IP Address of the Interface
2	MAC(Optional)	Give the MAC Address (Optional)

Make a new Network object		
Name		
IP and Mask IP 10 . 0 . 0 . 3 Mask 255 . 255 . 255 . 0 2		
Add Cancel	I Duplicate	X Delete:

Click on Add tab.

We can notice Newly added Network under the **User Defined Network** with selected type of the Interface.



Right click on added Network, to perform actions like viewing **Properties** of the Network, to find out where it is used, **copying** Network, **Duplicating** Network and **Deleting** Network.



### **Address Ranges**



Expand Address Ranges, User Defined is displayed



Right click on User Defined, to Create New Address Range



Below screen appears, Select General tab.

It consists of two fields, Name and Address Range.

In the Name tab, name of the new Address Range should be mentioned.

These are the inputs for the Address Range:

1	Start IP	Give the IP Address of the Interface
2	End IP	Give the MAC Address (Optional)

Create New Address Range		
General Notes		
Name		
NewAddressRange		
Start IP 10 , 0 , 0 , 1		
End IP 10 . 0 . 0 . 2 2		
Add Sancel	I Duplicate	Delete:

Click on Add tab.

We can notice the new Address Range in the below screen.

Right click on added Address Range, to perform actions like viewing **Properties** of the New Address Range, to find out where it is used, **copying** New Address Range, **Duplicating** New Address Range and **Deleting** New Address Range.



When we click on Duplicate New Address Range, below screen appears.

In which it displays **Name** of the Duplicate Address Range and **Address Range**.

Properties of Dup908 (Address Range)		
General Notes		
_ Name		
Dup908		
-		
Address Range		
Start IP 10 . 0 . 0 . 1		
Apply Scancel	X Duplicate	X Delete:

We can notice Duplicate Address Range under User Defined list.



### **Object Groups**



Expand Object Groups, by default Standard and User Defined Object Groups are displayed.



Right click on Object Groups, to add new object Group.



Below screen appears.

Select **General tab**, give the name of the new Object Group.

We can copy and paste new Objects in this Object Group.

Iake a new Object Group object Ceneral Notes	
Name New7209 Objects in this Group. Copy and Paste new Objects	
	•
Add Cancel I Duplicate Collete:	

## Click on Add tab.

We can notice new **Object Group** in the **User Defined.** 



Right click on the **Object Group**, to perform actions like viewing **Properties** of the Object Group, to find out where it is used, **copying** Object Group, **Duplicating** Object Group and **Deleting** Object Group.



Right click on the object Group and select Properties.



We can notice name of the **Object Group** and list of objects in the Group.

Properties of rfc1918-nets (Object Group)
General Notes
Name
rfc1918-nets
Objects in this Group. Copy and Paste new Objects
1. 🚰 net-10.0.0.0
2. 🚰 net-192.168.0.0
3. 🚰 net-172.16.0.0
Apply Cancel K Duplicate Colete:

### Users

Expand Users.



By default User Defined is displayed.



Right click on the User Defined to Add new User Group.



Below screen appears.

(Create a new	User Group)-			_					
Name									
loakUser	Users I	n Database	2	ter	4		Users In C	urrent Group	3 Q Filter
Name	Туре	Domain	Source			Name	Туре	Domain	Source
Sales	group	slave	labris		ك	sam	user	slave	labris
Marketing	group	slave	labris			loakUsers	group	slave	labris
loakUsers	group	slave	labris	T					
4	Add 🖌		<b>b</b> Cancel		5	X Dupl	icate	XD	elete:

These are the inputs two add new User Group:

1	Name	Type Name of the new User Group
2	Users in Data base	Displays Users in Data base
3	Users in Current Group	Displays Users in Current Group
4	>	It enables to add Users from Database to Current Group
5	«	It enables to remove Users from Current Group

Click on Add tab.

We can notice new User Group under the User Defined list.



Right click on the User Group, to perform actions like viewing **Properties** of the User Group, to find out where it is used, **copying** User Group, **Duplicating** User Group and **Deleting** User Group.



### 46. Services

In Firewall Builder, service objects are represented by IP, ICMP, TCP, and UDP services such as "host unreachable" in ICMP, HTTP in TCP, GRE in IP, and DNS in UDP. Firewall Builder plays a crucial role in providing necessary service objects for hundreds of well-known and frequently-used services in ICMP (IP protocol number 1), TCP (IP protocol number 6), and UDP (IP protocol number 17).



Expand Services, service Objects ICMP, IP, TCP, UDP, Custom, Service Groups are displayed



### ICMP

Expand ICMP, by default Standard and User Defined.



Right click on Standard, to add new ICMP service



Select **General tab,** to give he name of the **ICMP** object and choose the type of object from the drop down list in the **Type tab** 

	0 · Echo reniv
Make a new ICMP object	3 : Destination unreachable
General Notes	4 : Source quench
	5 : Redirect
Name	8 : Echo request
NewUser	9 : Router advertisiment
	10: Router solicitation
Type And Code	11: Time exceeded
Any kind	Type 0 : Echo reply
	Code 0
Add Cance	I Duplicate Delete:

Enable Any kind option and click on Add tab

Male a secolOMD able of	·····	
Make a new ICMP object		
General Notes		
Name		
NewUser		
Type And Code		
Any kind 🖌	Type 0 : Echo reply	-
	Code	<b>_</b>
Add Sancel	el 🗈 Duplicate 🗶 Delete:	

We can notice new Object under User Defined.



Right click on the new ICMP Service object, to perform actions like viewing **Properties** of the ICMP Service object, to find out where it is used, **copying** ICMP Service object, **Duplicating** and **Deleting** ICMP Service object.



# IP

Expand IP, by default Standard and User Defined.



Right click on IP, to add new IP service



Select **General tab**, give the name of the **IP** object and choose Protocol Number.

### Click on Add tab.

Make a new IP object			
General Option	s Notes		
Name			
Newlpobject			
Protocol Number			
Protocol Number, 1-2	55, 0 for Any		
Add	Cancel	X Duplicate	Delete:

We can notice new IP object under User Defined.



Right click on the new IP Service object, to perform actions like viewing **Properties** of the IP Service object, to find out where it is used, **copying** IP Service object, **Duplicating** and **Deleting** IP Service object.



## ТСР

Expand TCP ,by default Standard and User Defined are displayed.



Right click on **TCP**, to add new **TCP** service.



Select General tab, give the Name of the TCP object and choose Source port range, Destination port range.

## Click on Add tab.

Make a new TCP object	······	
General Flags Notes		
Name		
NewTcpobject		
Source port range	Destination port	range
Start: 0 🗘		Start: 0 🗘
End: 4 🜩		End: 4
🕂 Add 🥠 Cancel	I Duplicate	🗙 Delete:

Select Flags tab, to enable Flags which need to be examined by the firewall.

Click on Apply tab.

Properties of NewTopobject (TCP)	
General Flags Notes	
TCP Flags	
Match when the TCP flags are as specified.	
Flags that firewall should examine:	
URG ACK PSH RST SYN FIN	
Flags that must be set:	
URG ACK PSH RST SYN FIN	
Apply Scancel Cancel	X Delete:

We can notice new **TCP** object in the **User Defined** option.



Right click on the new TCP Service object, to perform actions like viewing **Properties** of the TCP Service object, to find out where it is used, **copying** TCP Service object, **Duplicating** and **Deleting** TCP Service object.



### UDP

Expand UDP ,by default Standard and User Defined are displayed.



Right click on **UCP**, to add new **UCP** service.



Select General tab, give the Name of the UDP object and choose Source port range, Destination port range.

## Click on Add tab.

make a new UDP ob	ject		
General No	ites		
NewUDPobject			
Source port range	h	Destination port ra	nae
	Start: 2 🗘		Start: 2 🔹
	End: 4 🜩		End: 4
Add	<b>5</b> Cancel	I Duplicate	X Delete:

We can notice new **UDP** object under **User Defined**.



Right click on the new UDP Service object, to perform actions like viewing **Properties** of the UDP Service object, to find out where it is used, **copying** UDP Service object, **Duplicating** and **Deleting** UDP Service object.



### **Service Groups**

Expand Service Groups, by default Standard and User Defined are displayed.



Right click on Service Groups, to add new Service Group.



Below screen appears.

Select General tab, give the name of the new Service object Group.

We can copy and paste new Objects in this Service Object Group.

#### Click on Add tab.

Make a new Service Group	object	··· Δ V ·······	
General Notes			
· · · · · · · · · · · · · · · · · · ·			
Name			
NewServiceGroup			
- Service Objects in this G	roup. Coopy and Posts new	Objects	
Service Objects in this G	oup. Copy and Paste new	Objects	
			<b>•</b>
<u>.</u>			
📌 Add	<b>5</b> Cancel	I Duplicate	X Delete:

We can notice new Service Group under User Defined.



Right click on the new Service Group, to perform actions like viewing **Properties** of the New Service Group, to find out where it is used, **copying** New Service Group, **Duplicating** and **Deleting** New Service Group.


Right click on the Service Group and select Properties.



Below screen appears, name of the **Service Group** and list of Objects in this **Service Group** is displayed.

Properties of Useful_ICMP (Service Group)  General Notes
Name
Service Objects in this Group. Copy and Paste new Objects
1 of 4 👪 time exceeded
3 of 4 M ping reply
4 of 4 📓 all ICMP unreachables 🔹
Apply Sancel Cancel Collecte:

# 47.DoS/DDoS

A Denial of Service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.

The most common type of Denial of Service attack involves flooding the target resource with external communication requests. This overloaded prevents the resources from responding to legitimate traffic, or slows its responses so significantly that it is rendered effectively unavailable.

A Distributed Denial-of-Service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

In a typical DDoS attack, the assailant begins by exploiting a vulnerability in one computer system and making it the DDoS master. The attack master, also known as the boot master, identifies and identifies and infects other vulnerable systems with malware. Eventually, the assailant instructs the controlled machines to launch an attack against a specified target.

\*Source - www.searchsecurity.com



Expand DoS & DDoS, by default User Defined is displayed.



Right click on **Dos &DDoS**, to add new DoS



#### General

Below screen appears. Select **General tab** it consists of two fields, Name & General Settings.

In the Name field, name of the Dos object should be mentioned.

In General Setting's field, we can enable or disable Before Dnat, Log, Drop.

Create a new DoS object					
General SYN Floo	d UDP Flood	CONN Flood	ICMP Flood	ICMPv6 Flood	Notes
News					
NewDosObject					
-					
General Settings					
Before Dnat		V Log			
					9
	<b>4</b> 0		WID Duralitanta		Deleter
Add	Cancel		Nii Duplicate		Lelete:

## **SYN Flood**

SYN Flood helps us to view and change the SYN Flood Settings.

We can enable or disable SYN Flood, Per Source, Per Destination, and Total.

Give the appropriate Count and Burst values.

Create a new DoS object				
General SYN Floor	UDP Flood CONN Floo	d ICMP Flood	ICMPv6 Flood Notes	
SYN Flood Settings				
SYN Flood				
Per Source	Count 1		Burst (1-10000) 400	
Per Destination	Count 40		Burst (1-10000) 55	
🗸 Total	Count 699		Burst (1-10000) <mark>800</mark>	
💠 Add	Sancel	I Duplicate	X Dele	ete:

#### **UDP Flood**

UDP Flood helps us to view and change the UDP Flood Settings.

We can enable or disable UDP Flood, Per Source, Per Destination, and Total.

Give the appropriate Count and Burst values.

Create a new DoS object-					
General SYN Flo	Dood UDP Flood	CONN Flood	ICMP Flood	ICMPv6 Flood	Notes
UDP Flood Settings					
UDP Flood					
Per Source	Coun	30		Burst (1-10000)	60
Per Destination	Coun	60		Burst (1-10000)	900
✓ Total	Coun	800		Burst (1-10000)	1000
1	J	S			s
🕂 Add	Sancel		I Duplicate	]	X Delete:

# **CONN Flood**

CONN Flood helps us to view and change the UDP Flood Settings.

We can enable or disable CONN Flood, Per Source, Per Destination, Total.

Give the appropriate Count and Burst values.

Create a new D	oS object					
General	SYN Flood	UDP Flood	CONN Flood	ICMP Flood	ICMPv6 Flood	Notes
CONN Flood	Settings			1		
	Flood					
Per So	urce	Coun	t50		Burst (1-10000)	599
✓ Per De	stination	Coun	t <mark>300</mark>		Burst (1-10000)	3000
✓ Total		Coun	500		Burst (1-10000)	378
🕂 Add		<b>5</b> Cancel		I Duplicate		X Delete:

## **ICMP Flood**

ICMP Flood helps us to view and change the UDP Flood Settings.

We can enable or disable ICMP Flood, Per Source, Per Destination, Total.

Give the appropriate Count and Burst values.

Create a new DoS o	bject						
General SY	/N Flood	UDP Flood	CONN Flood	ICMP Flood	ICMPv6 Flood	Notes	
ICMP Flood Settin	igs				e		
	1						
Per Source		Coun	70		Burst (1-10000)	299	
Per Destina	ation	Coun	67		Burst (1-10000)	387	
✓ Total		Coun	t200		Burst (1-10000)	300	
	_						

#### **ICMPv6 Flood**

ICMPv6 Flood helps us to view and change the UDP Flood Settings.

We can enable or disable ICMPv6 Flood, Per Source, Per Destination, and Total.

Give the appropriate Count and Burst values.

General STN FIC	od UDP Flood	CONN Flood	ICMP Flood	ICMPv6 Flood	Notes
MPv6 Flood Settings				-	1
ICMPv6 Flood				_	
Per Source	Cour	nt 220		Burst (1-10000)	330
<ul> <li>Per Source</li> <li>Per Destination</li> </ul>	Cour	nt 220 nt 680		Burst (1-10000) Burst (1-10000)	1500

## **Notes**

In Notes column, we can write information regarding new DOS Object.

Create a new D	oS object						
General	SYN Flood	UDP Flood	CONN Flood	ICMP Flood	ICMPv6 Flood	Notes	
_ Notes						_	
NewDosObje	ect						
💠 Add		<table-cell-rows> Cancel</table-cell-rows>		C Duplicate		X Delete	

After providing all the inputs to the New Dos Object, click on **Apply tab**.

Properties of NewDosObject (Do	S)				
General SYN Flood	UDP Flood	CONN Flood	ICMP Flood	ICMPv6 Flood	Notes
Name NewDosObject					
General Settings					
Before Dnat		✓ Log		✓ Drop	
Apply	🕈 Cancel		🕮 Duplicate	X	Delete:

Click on Add tab.

Create a new DoS o	bject						
General S	YN Flood	UDP Flood	CONN Flood	ICMP Flood	ICMPv6 Flood	Notes	
- Name							
NewDosObject							
- General Settings -							
- General Settings -							
Before Dna	at		✓ Log		Drop	)	
📌 Add		🕈 Cancel		I Duplicate		X Dele	te:

In the below screen, we can notice New Dos Object under User Defined.

Policy	*	Object	🌑 Insert Rule	▶ Install	Connections	IP-MAC Matcher
Policys		Compile, save a	and Install the rules of Labris_D	emo		
💐 Objects		Opened Policy	:Policys			
🖻 💼 Network Objects		Save Date :0	7 Jan 2014, 14:34:13			
🖻 🛄 Services						
🖨 🖏 DoS & DDoS		Current Active	Policy :Policys			
🖻 💐 User Defined	_ []]	Save Date :0	)7 Jan 2014, 14:34:13			
🔤 🔼 NewDosObject						

Right click on the New Dos object, to perform actions like viewing **Properties** of the Dos object, to find out where it is used, **copying** object, **Duplicating** and **Deleting** Dos object.



## 48.QoS/Bandwidth

QoS (Quality of Service) plays a crucial role in ensuring high-quality performance to latency and bandwidth sensitive applications. Differential treatment of traffic based on rules are accepted and prioritized. Necessary protocols and performance of the network is effectively improved by QoS.



Expand QoS/Bandwidth, by default User Defined is displayed.



Right click on User Defined under QoS/Bandwidth, to add new QoS/Bandwidth.



#### General

To make a new QoS/Bandwidth, select General tab.

Give the name of the QoS/Bandwidth object.

Give appropriate values for Rate (Mbit/s), Ceil (Mbit/s), Burst (Byte) and Priority in **QoS/Bandwidth Settings.** 

Choose Interface for the New QoS/Bandwidth object from the list of Interfaces.

Properties of gostest (0oS)	······	
Topenies of dostest (005)		
General Notes		
Name		
nostest		
QoS/Bandwidth Settings		Interfaces
Type 🔘 Shared 💿 Per IP		eth0
Download		
Rate 1.0 Mbit/s 🔻	2.0 Mbit/s 🔻	
Burst 2.0 Mbyte 🔻	4.0 Mbyte 🔻	
- Annely - Conce	VIII Duplicate	M Deleter
Cance	Duplicate	A Delete:
- Properties of charact and (0.05)	······	
Properties of shared_qos(QoS)	△ ▽	
Properties of shared_qos (QoS)	Δ 🗸	
Properties of shared_qos (QoS)	Δ	
Properties of shared_gos (QoS)	······· Δ ∇ ······	
Properties of shared_gos (QoS)		
Properties of shared_qos (QoS) General Notes Name shared_qos QoS/Bandwidth Settings		r Interfaces
Properties of shared_gos (QoS) General Notes Name shared_gos QoS/Bandwidth Settings Type • Shared O Per IP		Interfaces eth0
Properties of shared_gos (QoS) Cerreral Notes Name shared_gos QoS/Bandwidth Settings Type • Shared • Per IP Bate	1000.0 Mbit/s ▼	Interfaces
Properties of shared_gos (QoS) Cerreral Notes Name shared_gos QoS/Bandwidth Settings Type  Shared Per IP Rate Coil	1000.0 Mbit/s ▼	r Interfaces eth0
Properties of shared_qos (QoS) Cerreral Notes Name shared_qos QoS/Bandwidth Settings Type • Shared • Per IP Rate Ceil	1000.0 Mbit/s V 1000.0 Mbit/s V	Interfaces eth0
Properties of shared_qos (QoS) Cerreral Notes Name shared_qos QoS/Bandwidth Settings Type O Shared O Per IP Rate Ceil Burst	1000.0 Mbit/s V 1000.0 Mbit/s V 15360.0 byte V	Interfaces eth0
Properties of shared_qos (QoS) Cerrenzi Notes Name shared_qos QoS/Bandwidth Settings Type  Shared Per IP Rate Ceil Burst Priority	1000.0 Mbit/s ▼ 1000.0 Mbit/s ▼ 15360.0 byte ▼ 3	Interfaces
Properties of shared_qos (QoS) Cerrenzi Notes Name shared_qos QoS/Bandwidth Settings Type Shared Per IP Rate Ceil Burst Priority	1000.0 Mbit/s ▼ 1000.0 Mbit/s ▼ 15360.0 byte ▼ 3	Interfaces eth0

Choose between per ip or shared, for your rule's purpose. Then press apply to save changes.

#### Notes

Select Notes tab to write notes regarding new object creation.

Properties of NewQoSobject (QoS)		
General Notes		
Notes		
New QoS bandwidth is created with the interface eth 4 v	with appropriate bandwith settings	
L		
Apply 5 Cancel	X Duplicate	Delete:

Click on Apply tab.

In the below screen we can notice **QoS/Bandwidth** object.



Right click on the new QoS/Bandwidth object, to perform actions like viewing **Properties** of the QoS/Bandwidth object, to find out where it is used, **copying** object, **Duplicating** and **Deleting** QoS/Bandwidth object.



## 49. Schedule

Firewall rules are scheduled in such a way that they must be Active only at certain times of the day or particular days or particular hours and minutes.

Firstly schedule should be created under Firewall and then apply a schedule to the rule or while creating a rule pick up appropriate defined schedule to the rule.

We can create one time schedule or recurring time schedule. One time schedule is applied only once for the specified period in the schedule, recurring time schedule are applied repeatedly at specified times.



## Standard

Expand schedule, Standard and User Defined is displayed.



Expand standard, by default some schedule objects are displayed under Standard Schedule.



Right click on the schedule object, to perform actions like viewing **Properties** of the Schedule object, to find out where it is used, **copying** object, **Duplicating** and **Deleting** Schedule object.



# **50. User Defined**

Right click on **User Defined** to Add new Time Definition.



## General

Select General tab, Give the name of new time Object in the Name field.

Make a new Time obje	ct	Δ 🔍	
General Star	t Stop Notes		
Name			
Newtimeobject			
,			
💠 Add	Cancel	I Duplicate	X Delete:

#### Click on Add tab.

### Start

Schedule object start time should be mentioned in this section, select **Start** tab.

Properties of Newtimeobject (T	'ime)				
General Start Sto	p Notes			calender	
1		Doto: Jap 7, 2014			
Activate date		Hour:	72	Minute:	20
Activate day	Day of	Week: Tuesday	-		
Apply	<b>S</b> Cancel	K Duplicate	3	K Delete:	

# These are the inputs for Start

1	Active date	Enable Active date to choose start date from the calendar
2	Active hour	Enable Active hour to choose starting hours and minutes
3	Active day	Enable Active day to choose starting day from drop down list

After choosing appropriate date, hour and day disable Active mode of date, hour, day and click on **Apply tab** 

Properties of Newtimeobject (T	ime)			
General Start Sto	p Notes			
Terran Market				
Activate date	Date	e: Jan 7, 2014		
Activte hour	Hou	r:	0 🔶 Minute:	20
Activate day	Day of Weel	c Tuesday	-	
Apply	<table-cell-rows> Cancel</table-cell-rows>	I Duplicate	X Delete:	

## Stop

Schedule object stop time should be mentioned in this section, select **Stop** tab.

General Start	Notes		 calender	
Activate date Activte hour 2 Activate day 3	Da Ho Day of Wee	te: Jan 16, 2014 un: ek: Wednesday	Minute:	0+
Apply	<b>4</b> Cancel	X Duplicate	X Delete:	

1	Active date	Enable Active date to choose stop date from calendar
2	Active hour	Disable Active hour for not mentioning stop hour and minutes
3	Active day	Enable Active day to choose week day

### Notes

Select **Notes tab**, to write necessary information regarding time Object.

General Star	t Stop Notes		
new time object is c	reated with start time and stop time		
✓ Apply	<b>5</b> Cancel	XIII: Duplicate	X Delete:

Click on Apply tab.

We can notice new time Object in the below screen.



Right click on the schedule object, to perform actions like viewing **Properties** of the Schedule object, to find out where it is used, **copying** object, **Duplicating** and **Deleting** Schedule object.



# **51. Application Control**

Using Application Control in firewall enables us to block applications based on Users or User Groups. So, that you can control risky port and protocol hopping applications before they get in.You can also reduce your attacks surface by enforcing mobile applications and social media application policies. You can even control bandwidth



#### **User Defined**

Expand Application Control, by default User Defined is displayed.



Right click on User Defined to add new Application Group.



# Creating new application group

Create a new Name NewAppG	Create a new Application Group Name Name Applications In Database Filter							
Name	Category	Risk	Productivity		Name	Category	Risk	Productivity
050Plus	Messaging	2	2	▲	12306.cn	Web Services	4	1
12306.cn	Web Servi	4	1		126.com	Mail	4	2
126.com	Mail	4	2	- L				
4	Add Cancel 5 Duplicate Celete:							

These are the inputs for new Application Group.

1	Name	Type the name of the Application Group
2	Application in	It displays list of Application in Database
	Database	
3	Application in Current	It displays list of Applications in Current Group
	Group	
4	8	This symbol enables to add Applications in to Current Group from Database
5	<	This symbol enables to remove Applications from Current Group to Database

In the below screen we can notice new Application Group.



Right click on the Application Group, to perform actions like viewing **Properties** of the Application Group, to find out where it is used, **copying** Application Group, **Duplicating** and **Deleting** Application Group.



# 52.Firewall

Firewall is a concept which blocks unwanted traffic and passes desirable traffic to and from both sides of the network.

A firewall is a system (either software or hardware or both) that enforces an access control policy between two networks.

Example:

- Allows: http, mails etc
- Keeps out : Intruders ,Denial of services attacks, spam etc.

## **53. Labris Firewall Management**

Install, Save (create a new policy object for first setup), Install Policy



## Creating new policy firewall object

Give the **Name** of the Object in the Name tab, by default Network Interfaces have been selected for the new firewall object and click on **Add** tab.



Below screen appears stating Welcome to Labris Firewall Policy Maker.

Policy	😹 Object	Insert Rule	Install	Connections	IP-MAC Matcher
Default  Coljects  Network Objects  Services  DoS & DDOS  Collect  Application Control  Firewall	N Welcome to Labris I	Frewall Policy Maker			
	Labri	Firew Policy Make	all / r		

Now we have created a new firewall object and we will configure it now.

Default	Compile, save and Install the rules of Newfirewallobject	
Objects     Network Objects     Services     DoS & DDOS     OoS/Bandwidth     Schedule     Application Control     Firewall     Global Policy     Globa	Opened Policy     :Default       Save Date     :       Current Active Policy     :Policys       Save Date     :20 Jan 2014, 12:35:00       Previous Active Policy:Policys       Save Date     :20 Jan 2014, 12:23:52	
<ul> <li></li></ul>	Properties of Newfirewallobject (Firewall)	back
	Selferal Options Notes SSH Inspecting	ancel

### **Add Next Generation Firewall**

First step:

**Create Global policies** 

### **Global policy**

Global policies in one logical system are in a separate context than other security policies. According to the source from the target set on the way to the Objects or forbids. In addition, these rules can be imported from the previously created Network Objects(Hosts, Networks, Addresses, Address Ranges, Object Groups and Users), Services (ICMP,IP,TCP,UDP, Custom, Service Group), DoS/DDoS Objects, QoS(Bandwidth Management) Objects can be added to the schedule Objects for controlling application profiles.

#### Second step:

#### **Create NAT Policies**

#### **NAT Policy**

NAT: It is a service of routing provides network address translation from private to public

When we have 2 networks public & private in order to protect private network from public network (intruders) we need NAT.

NAT enables one way communication. i.e. private network can communicate with public network but not vice versa.

### NAT policies

It allows you to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services.

For example, a lot of the IP subnet address from internal network will route to outside network with single IP address.

#### Third step:

#### **Physical interfaces**

The physical interface that are supported by the device and subsequently added to the interface listed in the area.

This field contains the interfaces for the WAUTH interface, Dynamic source address translation interface, and the external network interface definitions.

Default	Compile, save and Install the rules of Newfirewallobject	
Colored Color	Opened Policy       :Default         Save Date       :         Current Active Policy       :Policys         Save Date       :20 Jan 2014, 12:35:00         Previous Active Policy:Policys       :20 Jan 2014, 12:23:52	
tarian eth3 : arian eth4 : arian eth5 :	Save Install Policy	ollback
	Properties of Newfirewallobject (Firewall)  General Options Notes SSH Inspecting  Name New firewallobject	
	✓ Apply	Cancel

#### **Firewall Properties**

- Interface Use this property to match which network port or data link packet is traversing such as "eth0" for Ethernet built-in.
- **Source MAC Address** Use this property to specify an Ethernet Hardware Address that matches the source MAC (Media Access Control) address in the link layer frame header.
- Destination MAC Address Use this property to specify an Ethernet Hardware Address that matches the destination MAC (Media Access Control) address in the link layer frame header.
- **Source Net** Use this property to specify a single IP address or network range that matches the source IP address of a packets IP header.
- **Destination Net** use this property to specify a single IP address or network range that matches the destination IP address of a packets IP header Network ranges can be specified as address1-address2.
- **Protocol** Use this property to specify the protocol number that appears in a packets IP header.
- **IP Options** Use this property to specify the IP option numbers that appear in a packets IP header.
- **ICMP Type** Use this property to specify the ICMP type that appears in a packets ICMP header.
- ICMP Code Use this property to specify the ICMP code that appears in a packets ICMP header.

- **TCP Header Flags** Use this property to specify the TCP header flags that appear in a packets of TCP header.
- **TCP Options** Use this property to specify the TCP option numbers that appear in a packetsof TCP header.
- **Destination Port** Use this property to specify a single protocol port or range of protocol ports that matches the destination port of a packets TCP or UDP header. Port ranges can be specified as port1-port2.
- URL Keyword Use this property to search for keywords that appear within a HTTP (web site) URL.
- **Parent Match Count** Use this property to notify you if the parent rule has been matched a specified number of times.
- **Parent Byte Count** Use this property to notify you if the parent rule has been matched by network traffic containing a specified number of bytes.

Right click on Firewall object to view Properties of firewall object.

Select General tabto view details about Name of the Firewall object.

We can change name and click on Apply tab to change the name.

Policy	Object	Insert Rule	Install	Connections	IP-MAC Matcher
Policys	Compile, save and Inst	all the rules of Labris_Demo			
🐧 Objects	Opened Policy	:Policys			
🗉 📋 Network Objects	Save Date :07 Jan 2	2014, 14:34:13			
E Services	Current Active Policy	:Policys			
Dos & DDos	Save Date :07 Jan 2	2014, 14:34:13			
Bondula	Previous Active Policy	r:Policys			
Application Control	Save Date :07 Jan 2	2014, 10:25:42			
🖻 🐧 Firewall					
E Labris_Demo			In stall Dalian		4 Dellhaut
Global Polic	Save		Install Policy		> Rollback
🕀 💶 eth0	Properties of Labris_De	emo (Firewall)	· · · · · · · · · · · · · · · · · · ·		
eth1	General Onti	ions Notes SSH Inst	ecting		
eth3	Contrast open				
🕀 💶 eth4					
eth5					
	Name				
	Labris_Demo				
	Apply				Sancel

Select Options tab.

We can Enable or Disable Options Firewall is part of "ANY", Accept TCP sessions opened prior to firewall installation, Accept ESTABLISHED and RELATED packets before first rule.

Policy	尉 Object	Insert Rule	▶ Install	Connections	IP-MAC Matcher
Policys	Compile, save and Inst	all the rules of Labris_Demo			
💐 Objects	Opened Policy	:Policys			
🗈 🛅 Network Objects	Save Date :07 Jan :	2014, 14:34:13			
Services	Current Active Policy	:Policys			
DOS & DDOS	Save Date :07 Jan :	2014, 14:34:13			
€ Schedule	Previous Active Policy	/:Policys			
Application Control	Save Date :07 Jan :	2014, 10:25:42			
🖻 💐 Firewall					
E Labris_Demo	Covo.		Install Policy		Sellback
MAT Policy	<u>Dave</u>				Rollback
🕀 💶 eth0	Properties of Labris_D	emo (Firewall)			
eth1	General Opt	ions Notes SSH Insp	ecting		
eth3	Eirowell is nor	t of "Any"			
eth4	I newants par				
tun0	Accept TCP se	ssions opened prior to firew	all installation		
	Accept ESTAB	LISHED and RELATED pack	ets before first rule		
	-				
	🗸 Apply				<table-cell-rows> Cancel</table-cell-rows>

Click on **Apply** tab to apply changes to the firewall object.

Select Notes tab to write information regarding firewall object (Optional).

Policy	Object	Insert Rule	Install	Connections	IP-MAC Matcher
Policys	Compile, save and Inst	all the rules of Labris_Demo			
Objects     Metwork Objects     Services     DoS & DDoS     OS/Bandwidth     Schedule     Application Control     Firewall	Opened Policy Save Date :07 Jan 2 Current Active Policy Save Date :07 Jan 2 Previous Active Policy Save Date :07 Jan 2	:Policys 014, 14:34:13 :Policys 014, 14:34:13 :Policys 014, 10:25:42			
Global Polic Global Polic Com NAT Policy Com NAT Po	Properties of Labris_De General Opti	mo (Firewall)	ecting		Rollback
	🗸 Apply				<table-cell-rows> Cancel</table-cell-rows>

Click on Apply tab to apply changes.

### Select SSH Inspecting tab

We can Enable or Disable Allow HTTP request through SSH port forwarding, Allow SCP, Allow shell login, Allow sftp.



Click on Apply tab to apply changes

#### **Global Policy table**

Global policy table is displayed with the fields **Source, Destination, Service, Action, Schedule, QoS/Bandwidth, Application, Security policy, Options**.

How to add new Global policy? And what can be done?

Example1: My host objects for policy

🐞 🗏 📕	Policy	Object		Insert Ru	ile.	Ins	itall	Connectio	ns	IP-MAC Match	her
Server Slave:4000 User Management System Network Settings Firewall WPN ali Filter Antispam/Antivirus USS/IPS Messaging Server	Configuration Configuration Network Objects Notors	NewFir	evalobject Source	Destination	Service	Action Accept	Schedule Any	QoS/Bandwidth	Applications Any	Security Policy	Options ⇒⊡

My global policy

In the above screen we can notice columns such as Source, Destination, Service, Action, Schedule, QoS/Bandwidth, Application, Security Policy, Options.

Application is allowed if the created Source with interfaces INSIDE & OUTSIDE is accessed, and when the Destination, Service, Schedule, QoS/Bandwidth, Application, Security Policy options are Selected as ANY. We can even drag-and-drop the desired objects created earlier, or copy and paste can be added with it.

Example 2: My network objects for policy.



All of the destinations on the IP addresses of the source of the rule INSIDE\_Net with access to only the specified services. This rule also holds at their outer radio marker internal IP addresses on the policy.

Example 3: How do we add a rule for users and My.applicaiton.info.stacktrace users with QoS, control, DDOS and schedule how do we apply.

Ele Edit View Module Abo	sole ut									-	€ × Help
5a 🗶 🗶	> Policy	Dbject	Inse	rt Rule	I		install	Connections	[	IP-MAC Matcher	
Server     Save: 4000     Sorver     Save: 4000     Sorver     System     Sorver     Sorver     Sorver     Sorver     Load Balancer     Sorver	Conformation     Collects     Mosts     Mosts     Mosts     Address Ranges     Object Groups     Object Groups     Object Groups     User Defined     My IT_Department     Service Groups     UpP     OUP     Outrom     Object Defined     operties of New	Source E DB Department_Users	Destin	Service	Action Accept Accept	Schedule Any ScheduleOb.	QoS/Bandwidth Any NewQoS_Objec	Applicati.	Security Policy Any NewDD05_0bjec	0p	

The rule previously created users ((For creating users please refer to **users section** in **User Management**) in the same way as the example demonstrates how to use the drop-down with the yerede rule, let's link the current field) and user network appeal (For adding users in Network objects please refer to **users field** in **Network Objects Section**)owed as the source, and again before our Schedule-appeal (Please refer to **Schedule section** in **Network Objects** and the link in the same was the example demonstrates how to use the drop-down with the yerede rule, let's link the current field),QoS-appeal (Please refer to **Qos/Bandwidth section** in **Network Objects** here's the link and the link in the same way as the example demonstrates how to use the rule drop down yerede with the current field link), and DoS/DDoS previously created object located at the source by placing the user in the appropriate fields in the rule or the rope according to the specified criteria.

How to add an application control rule for users?

W.	Labris Man	agement Con	sole										- @ X
Eile	Edit View	Module Abou	ıt										Help
	1		> Policy	Dbjec	ct	🔘 Insert P	ule		👂 Insta	r [	Connection	s IP-MA	C Matcher
8-	Server		Configuration	NenFren	vallObject								
1	a 📓 slave: 4	000	C Objects	No.	S	ource	Destin	Service	Action	Schedule	QoS/Band	. Applications	Secu Optio
	System		Os & DDoS	0	INSIDE OUTSIDE		🗅 Any	🗅 Any	🔗 Accept	Any	Any	🗅 Any	🗅 Any 📴
	VPN	wall	QoS/Bandwidth     Schedule	1	My_IT_Dep	artment_Users	Any	🗅 Any	Deny	🗅 Any	🗅 Any	My_IT_Department	
	Filte	er spam/Antivirus IPS saging ver d Balancer	O Application Control     O User Defined     Wy IT Department Ap     Firewall     NewFirewallObject     Global Policy	-									

The rule previously created users ((For creating users please refer to **users section** in **User Management**) and here is the link in the same way as the example demonstrates how to use the drop-down with the yerede rule, let's link the current field) and Application control profile (Please refer to **Application control section** in **Network Objects** and here is the link in the same way as the example demonstrates how to use the drop-down with the yerede rule, let's link the current field).

Read all the rules in the table. Buy why you must be careful when writing the canonical ordering Application control. If the source specified in the rule is a rule used in the queues and objects in higher action has been ruling on the accept or deny rule.

Example 4: The outside should be accessed with specific protocols for access to the web or other services to the rule writing. And create a new NAT policy (NAT policy Please refer Example2)

	> Policy	1	Dbject	1000	Convert Male		👂 install		Connections	6 i i	IP-MAC Ma	tcher
Server .	Configuration		NenfrenalOb	the state								
🗟 🔚 slave:4000	O Objects		No.	Source	Destination	Service	Action	Schedule	QoS/Bandwi	dth Application	ns Security P.	Options
System Network Settings	Hosts		0		🗅 Any	🗅 Any	Accept	🗅 Any	🗅 Any	🗅 Any	🗅 Any	ъØ
Artispani(Antivirus	A NewHostsoby     A OUTSIDE     A WebServer	OUTSIDE     WebServer     Networks	1	🗅 Any	G WebServer	http https	Accept	🗅 Any	🗅 Any	🗅 Any	C Any	-
Server Load Balancer E License Users Load Salancer Users Services Services Standard Altop Altop Altop Resh video Trp Standard domain Finger Resh video Trp Stata passiv												

For example, one in which each web server and outside a place gave over to access http and https protocols. The source column of the address will be "any", which is the target column because the target to a specific server to be accepted through the "host object" (for creating **hosts object** Please refer to **Hosts field** in **Network object** section here is the link to give the host object will be created in the same manner as the host and the creation stage of the policy section and use the example currently in the link).

Policy	Object		🕘 Insert Ru	le	Insta	all	Connecti	ons	IP-MAG	C Matcher	
Policys	Labris_Demo										
💐 Objects	No.	Source	Destination	Service	Action	Schedule	QoS/Band.	Applicatio.	. Security P.	. Options	
Metwork Objects     Services     DoS & DDoS     QoS/Bandwidth	0	🚊 suleym. 🚊 win_for_ 🚊 win_for_	Any	🖻 Any	Accept	🗅 Any	🗅 Any	🗅 Any	🗅 Any	₽₽	
Schedule     Application Control     Firewall     Apris Demo	1	A INSIDE OUTSI WAUTH	Any Any	🗅 Any	Accept	🗅 Any	🗅 Any	🗅 Any	🗅 Any	┣╋	=
The state of the s	2	🗅 Any	📇 kalilinux	🔄 t8090 💽 http	Accept	🗅 Any	🗅 Any	🗅 Any	🗅 Any	⊵₁₽	
eth2	3	F INSIDE.	🕒 Any	🗅 Any	🥥 Deny	🗅 Any	🗅 Any	🔒 Applica	ti 🗋 Any	₽₽	
⊕ eth3 ⊕ eth4 ⊕ eth5	4	🗅 Any		🖸 rdp	Accept	🗅 Any	🗅 Any	🗅 Any	🗅 Any	<mark>₽</mark> t₽	
🖻 🛄 tun0		P INSIDE		_	_	_	_	_	_		-
	٦٦ لك La	bris"	Fi Po Ma	rewa olicy akei	all						

### NAT (Network Address Translate) Policy table

NAT Policy table is displayed with the fields **Original Src**, **Original Dst**, **Original Srv**, **Translated Src**, **Translated Dst**, **Translated Srv**, **Comment**.

In this section, in accordance with the global policy also created the device permissions, changing the status of the source, destination, and services will write the rules.

# Example1: Internet NAT policy



For example, a lot of the IP subnet address my device contains and leave all our internet users out of their IP addresses through a single IP address we need over. So we have to translate the network address.

IP subnet is 255.255.255.0 and your default gateway is 192.168.168.1 and 192.168.168.0 considering the need to build rule my IP Address; a of range IP address and target the source 192.168.168.0 255.255.255.0 on the Internet as a place to which "any" and all the services in the same way that any change in the subverted will be converted to the destination address in the above policy, such as changing to run assuming the IP address. In our example, changing IP address is 192.168.168.1

Example2: Web server access from Wide Area Network.

🖌 🗶 🗶	C Policy	Cbject	0	insert Rule	Insti	all la	Connections	IP-MA	C Matcher
Server	Configuration	NewFirewallObject							
🗟 🗮 slave:4000	C Objects	No.	Original Src	Original Dst	Original Srv	Translated Src	Translated Dst	Translated Srv	Commen
2 System	B Network Objects	0	P INSIDE_Net	Any Any	Any Any	D Original	A INSIDE	Driginal	<sup>D</sup>
Vetwork Settings	B INSIDE     B NewHostsObje     D Outrops	( <b>1</b> )	🗅 Any		http https	C Original	A WebServer	🗅 Original	t₽
Messagng     were     Load Balancer     we ucense     Ucense     were     rse Cooper Gerse Services Gerse Properties of WebS	ierver (Host)								

Any source outside web server "any" http and https access to the supplier global policy is written as (For **global policy** please refer to **ADD Next generation firewall** section) and later to the server on specific ports from outside should identify which requests inside.

Example 3: Web Filter service enables.

Internet web filter service requests that returning web filtering. The following rule is written to the NAT policy.

	Policy	<ul> <li>Object</li> </ul>	0	Insert Rule	Insta	Million (	Connections	IP-MAC MI	tcher.
Server	Configuration	NewFrenalObject							
Illier Machanner	C Objects	No.	Original Src	Original Dst	Original Srv	Translated Src	Translated Dst	Translated Srv	Comme
System	B C Hosts	0	# INSIDE_Net	Any Any	C Any	Criginal	A INSIDE	Criginal Original	P
Network Settings Network Setting Network Settings Network Setting Network Setti	B NSIDE     NewHostsObje	1	Any Any		http https	Criginal	A WebServer	Criginal	e .
	2	- INSIDE Net	C Any	M http	C Original	S INSOE	Labris Webfilter	-	
	Standard Standard All TCP Auth daytime								

The resources specified in the rule, the user/user group, IP addresses/IP range, in the case of http service running on the device to web subnet, IP filter rule is required to be sent to the service. This rule should be written to all devices with web filtering. (For web filter please refer

to **Filters section** here is the link to the web filter also web filter configuration screens to give the link).



#### Interfaces

By default seven Interfaces are present in the firewall object.

They are eth0, eth1, eth2, eth 3, eth4, eth5, tun0.

Select **General tab**, Name of the interface is displayed.

Policy		🛃 Object	Insert Rule	▶ Install	Connections	IP-MAC Matcher
Policys		Compile, save and	Install the rules of Labris_Demo			
💐 Objects		Opened Policy	:Policys			
🗄 🛅 Network Objects		Save Date :07 Ja	an 2014, 14:34:13			
🖻 🛅 Services		Current Active Poli	icv :Policvs			
🕀 🛅 DoS & DDoS		Save Date :07 Ja	an 2014, 14:34:13			
E CoS/Bandwidth		Dravieve Active De	lieur Delieure			
Schedule	.	Save Date :07 Ja	an 2014, 10:25:42			
Application Contro						
E Rirewall						
😳 🚯 Global Poli	icy					
MAT Policy						
eth0						
eth2						
🕀 💶 eth3	-					
E eth4						
tun0	-	Save		Install Policy		Sollback
				· · · · · · · · · · · · · · · · · · ·		
		Properties of eth0 (	(Firewall Interface)			
		General Se	ettings Notes WAU	ГН		
		Name				
		leth0				
		Apply				👆 Cancel
cted to is: 78.188.50.48.st	atic.t	tnet.com.tr				Labris Teknoloji

Select **Settings tab**, we can Enable or Disable **Dynamical source Address Translation**, This interface is an external network interface.




Select Notes tab, to write information regarding Interface (Optional).

Select WAUTH tab, we can enable or disable options like Active, Use SSL Connection, Use Default Gateway IP



### **Firewall Application**

- The Web Application Firewall (WAF) protects applications from current and future security threats by combining multiple security engines into a cohesive Web defense.
- Not like a "normal" firewall- Applies rules to HTTP conversations
- Allow or deny based on expected input Unexpected input is a common method of exploiting an application.
- SQL injection Add your own commands to an application's SQL query.
- A major focus of payment card industry, Data Security Standard (PCI DSS).

### **SSH Inspection**

Labris SSH Inspector provides an easy and effective way to limit actions allowed over ssh. Its engine detects the internals of ssh traffic and allows administators to manage and log ssh traffic in depth. Administators can allow/block/log shell login, sftp, scp or HTTP request through ssh port forwarding.

### **Enabling SSH Inspection**

SSH Inspection configuration is done in firewall object settings under **Firewall** module.



In firewall object properties administrators can choose which actions will be enabled in ssh traffic.

Properties of slave (Firewall)	7
General Options Notes SSH Inspecting	
Allow HTTP request through ssh port forwarding	
Allow scp	
Allow shell login	
Allow sftp	
✓ Apply	

### **Restricting SSH Activities**

In **Firewall** module under **NAT Policy** administrators decide which users will be redirected to SSH Inspector.

Administrators add users/hosts/networks to be restricted to Original Src of NAT rule, port number of SSH service to **Original Srv**, internal interface IP of restricted network to **Translated Dst** and port number of SSH Inspector to **Translated Srv**.



After installing NAT rule SSH traffic of users will be inspected by Labris SSH Inspector and unauthorized actions will be blocked.

### Monitoring SSH Activities

SSH activities of users are logged under **/var/log/labris/sshinspection** and can be monitored by accessing Labris UTM over ssh.



#### Usage Notes About Labris SSH Inspector

- When using Labris SSH Inspector clients should accept Labris SSH Inspector's SSH key as their remote SSH server key.
- When using Labris SSH Inspector remote SSH key changes are not visible to clients behind Labris SSH Inspector.

### **Network Address Translate (NAT)**

Network Address Translation is used to communicate the internal network to internet. It will be configured in the Router.

### What is the NAT?

Network Address Translation is nothing but converting a group of computers IP Address to communicate or to send the packets to the outside of the world through the internet. Whenever the host computer in a Network need to send packets to the other internet user it will be possible through the Router. In the router it must be configured for the communication between outside of the internet user and host computer in a company LAN Network. The router only will take care the changes in IP address whenever sending and receiving the packets to and from outside of the network and internal LAN. It will be configured in Router in a table.

### Why it is made?

In the whole world there are billions of computers. For communication between them they need unique IP Address like our street numbers and door numbers .NAT is a network protocol used in IPv4 networks that allows multiple devices to connect to a public network using the same public IPv4 address. NAT was originally designed in an attempt to help conserve IPv4 addresses. NAT has become a common, indispensable feature in routers for home and small-office Internet connections.

#### **NAT Types**

There are three types of NAT

#### **SNAT**

**Static NAT**: In this type, host computer will have particular IP Address to communicate with outside network. It is used for one device to communicate with outside network.

#### DNAT

**Dynamic NAT**: In this type, Router will assign the IP Address to communicate with outside network. It is used for communication of group of computers with outside network.

#### PAT

**PAT (Port Address Translation)**: This is the type of dynamic, but it will map multiple unregistered IP Addresses to registered single IP Address using port numbers called Port Address Translation.

#### **Port Forwarding/Port Mapping**

Port Forwarding is also known as Port Mapping is the process that a router uses to sort the right kind of network data to the right port. Computers and routers use ports as a way to organize network data. Different types of data, like web sites, file downloads, and online games, each are assigned a port number. The router or firewall uses forwarding to send the correct data to the correct place.

A firewall protects a computer by blocking unauthorized information, but if a firewall blocked all the incoming and outgoing data, the computer would be unable to access the Internet. When a computer user wants some data to go through the firewall and to send it to a specific location, he can set up port forwarding. This gives the firewall instructions about which types of data are allowed and how they should be directed.

Information on the Internet is associated with a port. Web pages, for example, are typically assigned port 80. File transfer protocol (FTP), often used for downloading and uploading files, typically uses port 21. Online games may use a number of different port numbers, but often choose numbers in the thousands.

Port forwarding also serves as another way to protect computers. People outside the network will only have access to the router or firewall, which will, in turn, control which types of data reach the computers. Any data that does not come to the router with the correct port will not be passed through to the computers inside the network.

## **Reverse Proxy engine**

Reverse proxy engine is the feature for proxying web sites hosted on different real server with different internal IPs through a single public IP address. Engine welcomes any incoming web connection to your web sites. Then, fetch the web site data from the real server in your LAN or DMZ and gives to the client.

For example, any incoming web connection to your public IP (for example 85.10.10.10) will be welcomed by the engine. There may be several web sites be hosted on this IP address. These web sites may be hosted in different real/virtual machines inside your network. The engine will bring web sites from where they are located and give to the client.

The engine is configured through a configuration file on current version. (/etc/sysconfig/Labris-reverseproxy.conf). Configuration options and remarks are explained in the following table.

[options] listen_port=2480 listen_port_ssl=2443	"listen_port" and "listen_port_ssl" attributes are used for configuring listen ports for http ad https, respectively. Default value should be used, if there are not any special conditions.
default_certificate_file=/etc/httpd/certs/server1.crt default_certificate_key_file=/etc/httpd/certs/privkey.pem	These attributes used for setting SSL certificates which are used for terminating SSL connections.
[revproxy1] original_website_name=www.labrisnetworks.com incoming_conn_type=nonssl realserver_conn_type=nonssl realserver_conn_url=http://www.labrisnetworks.com/	A block of variables are defined for each web site served through this reverse proxy engine. Each block has a name which is enclosed between "[]" and should include 4 attributes.
	"original_website_name" attribute is the web site name that the end user uses in his/her web browser to request your web site.
	"incoming_conn_type" attribute defines incoming connection type. Options are "ssl" and "nonssl".
	"realserver_conn_type" attribute defines protocol with the real server hosting the web site. Options are "ssl" and "nonssl".
	"incoming_conn_type" and "realserver_conn_type" attributes are also used for terminating a SSL connection and fetching data from a nonssl web server.
	"realserver_conn_url" attribute defines the address for the real web server inside your networks. Each definition should end with a "/". Internal IP addresses for the real servers are defined in hosts file (etc/hosts) or in first DNS forwarder server.

After configuring the engine itself, traffic should be redirected to the engine.

1. First of all traffic should be allowed. Traffic coming into YourPublicIP:2480 and YourPublicIP:2443 should be allowed.

Example Global Policy;

No.	Source	Destination	Service	Action	Schedule	QoS/Bandw	Applications	Security Po	Options
0	🗅 Any		▶ P_2443 ▶ P_2480	🔿 Accept	🗅 Any	🗅 Any	🗅 Any	🗅 Any	₽₽

 HTTP/HTTPS traffic should be redirected into the engine. Traffic coming into YourPublicIP:80 (or other http port) should be redirected to UTM\_IP:2480 (or configured listen\_port). Traffic coming into YourPublicIP:443 (or other https port) should be redirected to UTM\_IP:2443 (or configured listen\_port\_ssl).

Example NAT Policy;

No.	Original Src	Original Dst	Original Srv	Translated Src	Translated Dst	Translated Srv	Comment
0	🗅 Any		🔄 http	🗅 Original	🚊 WebServerl	S P_2480	<b>₽</b>
1	🗅 Any		🔄 https	🗅 Original	📇 WebServer2	P_2443	₽

## 54. Sample configuration:

/etc/sysconfig/labris-reverseproxy.conf:

;options must be set [options] listen\_port=2480 listen\_port\_ssl=2443 ; default certificate will be using on a ssl connection if any ; certificate for VirtualServer defined ; default\_certificate\_file=/opt/labris/etc/labris-lmc/certs/server.crt ; default\_certificate\_key\_file=/opt/labris/etc/labris-lmc/certs/server.key default\_certificate\_file=/etc/httpd/certs/server1.crt default\_certificate\_key\_file=/etc/httpd/certs/privkey.pem

- ; Configuration parameters for VirtualServer setup
- ; numbers at the end of section names (revproxy\*)
- ; must be increased sequentially
- ; (but writing order can be random)
- ; following configuration examples demonstrate connection types
- ; (incoming\_conn\_type realserver\_conn\_type)
- ; non-ssl non-ssl
- ; ssl non-ssl
- ; non-ssl ssl
- ; ssl ssl

```
[revproxy1]
original_website_name=www.labrisnetworks.com
```

Administration Guide for Labris UTM Version 3.4.2

incoming\_conn\_type=nonssl
realserver\_conn\_type=nonssl
realserver\_conn\_url=http://www.labrisnetworks.com/

[revproxy2]
original\_website\_name=www.labrisnetworks.com
incoming\_conn\_type=ssl
realserver\_conn\_type=nonssl
realserver\_conn\_url=http://www.labrisnetworks.com/

## VPN

VPN stands for Virtual Private Network. It is a Private Network which allows us to connect to public network remotely in a secured way.

Personal VPN's allow you to encrypt your data from being sent from your computer to a VPN Server. This prevents hackers from stealing your information when you access the Internet from a public Wi-Fi. VPN's can be used for several other things, than just getting passed blocked sites, use Windows Firewall to block non-VPN traffic for selected applications, e.g. your torrent client, a browser, download manager, etc. When using a VPN to secure a public Wi-Fi spot.

From using your ISP connection, permit it to connect the the Internet using only the VPN connection. Unfortunately, this will not work with the built-in firewall in Windows XP or Vista.

Right click on the VPN tab and select Connect.



# **IPSEC VPN Configuration**

## 55. Profile Administration;

It is the section where IPSEC Profile definitions are made.

IPSec SSL VPN CLIE	ENT L2TP Servis Yönetimi				
👙 Add Profile 🥒 Edit P	Profile 🔀 Delete Profile 4				IDSec 🌣
2 3	Server Name	Remote Wan IP	Firewall Rule	Status [1]	Profile Administration Policy

1	Profile Administration	Manage IPSEC Profile
2	Add Profile	Create a New IPSEC Profile
3	Edit Profile	Edit Selection IPSEC Profile
4	Delete Profile	Delete Selection IPSEC Profile

#### Step 1:

## 56. Add Profile

It is used to create a new IPSEC Profile.

Add Profil	e								×
1	Profile Name	Merkez to Ankara	Active 2	Local Networks					
-	r rome ryame	monitor_to_vintara	· / / cuve	Local Wan IP	eth1 (10.	11.12.221)		-	10
3	Description	IPSEC VPN Ankara							6 a)
(-)				Local Networks	Rou	te Remote Netv	vork Traffic From	This Site	11
4	Select Policy	Default	T 🔁 🖸		lan_net - 1	192.168.20.0/24 (	255.255.255.0)	12	#
	6		[7]					13	
Identity (	Confirmation	Shared Key RS	GA A						
								14	×
Shared K	.ey								
*****	****	8	15	Local IP				-	17
			Ī						-
	Show Passwor	rd 9	16	Local Id					18
				L					
Remote 1	Networks 20	21 22							
19 Sel	ect All 🛛 👘 Ad	id 🥖 Edit 🔀 Dele	te 2	3				٩,	Filter
ld	Name	Remote Wan IP	Remote Networks	Remote	e Lan IP	Remote Id	Process	NAT_T S	tatus
1	Ankara	88.10.10.12	10.0.0/8				Start	No A	ctive
G A	dvanced Setting	as 26					24 🔡 Sa	ave 🛛 💥 C	ancel 25

1	Profile Name	IPSEC Profile Name
2	Active	Status Active / Passive
3	Description	Description for IPSEC Profile
4	Select Policy	Select Policy for FAZ1 and FAZ2

5	Add Policy	Add New Policy Profile. Click for Details or Example
6	Identity Confimation	Shared Key
7	Identity Confimation	RSA. Click for Details or Example
8	Shared Key	Shared Key Input
9	Show Password	Show Shared Key
10	Local WAN IP	Select Local WAN Interface
11	Local Networks (Automatic)	All Local Networks Route Remote Network
12	Add Local Networks (Manuel)	Add Local Networks or IP Address Manuel
13	Edit Local Networks (Manuel)	Edit Local Networks or IP Address Manuel
14	Delete Local Networks (Manuel)	Delete Local Networks or IP Address Manuel
15	Local IP	Local IP Active / Passive
16	Local ID	Lacal ID Active / Passive
17	Local IP	Select Local IP from List
18	Local ID	Local ID Input
19	Select All	Remote Networks Select All
20	Add Remote Networks	Create a Remote Networks Button Click for Details or Example
21	Edit Remote Networks	Edit Remote Networks
22	Delete Remote Networks	Delete Remote Networks
23	Filter	Filter Remote Networks Input
24	Save	Save IPSEC Profile
25	Cancel	Cancel IPSEC Profile
26	Advanced Settings	Advanced Settings Button

## 57. Identity Confirmation RSA;

RSA (Rivest Shamir Adleman)

It is the section where common security key, used in the stage of establishing connection with the remote network with which IPSEC VPN will be made, is defined. RSA is an internet encryption and authentication system.

Identity Co	nfirmation	Shared Key 💽 RSA 1
RSA		Create RSA Key
Local	3	
Remote	4	

1	RSA	Identity Confirmation for RSA
2	Create RSA Key	RSA Key Execute Button
3	Local	Local RSA Key Input
4	Remote	Remote RSA Key Input

## 58. Add Local Networks (Manuel);

It is the section where local network or IP addresses which can communicate with the remote network with which IPSEC VPN will be made, are defined.

Add Network		x
1 Select I	2 New	
3 🔿 IP 🖲 Netw	rork 4	
Name	5	
Network Address	6	
Netmask	7 /24 (255.255.255.0)	
		9
	Save 🔀 Cance	

1	Select	Select Network or IP Address from Database	
2	New	Create a New Network or IP Adress	
3	IP	Create a New IP Address	
4	Network	Create a New Network	
5	Name	Network Name	
6	Network or IP Address Network or IP Address Input		
7	Netmask Netmask for Network		
8	Save	Save Configuration	
9	Cancel	Cancel Configuration	

## 59. Add Remote Networks;

It is the section where local network or IP addresses in the remote network with which IPSEC VPN will be made, are defined.

Edit Remote Network
1     2     3       Active     Auto Start     Image: NAT Traversal
Remote Name 4 Ankara_Local_Network
Remote Wan IP 5 88.1.1.2 Route all network traffic from this site 6
Remote Networks Ankara_Net - 192.168.2.0/24 (255.255.255.0) 7
10
Remote IP 11
Remote Id 13
12 14 Generate Firewall Rule Automatically
15 Save Cancel

1	Active	Remote Network Projile Active/Passive
2	Auto Start	Connection Auro Start When Disabled
3	NAT Traversal	NAT Traversal Active/Passive
4	Remote Name	Name for Remote Network
5	Remote WAN IP	Remote Static WAN IP Address
6	Local Networks (Automatic)	All Local Networks Route Remote Network
7	Add Local Networks (Manuel)	Add Local Networks or IP Address Manuel
8	Edit Local Networks (Manuel)	Edit Local Networks or IP Address Manuel
9	Delete Local Networks (Manuel)	Delete Local Networks or IP Address Manuel
10	Remote IP	Remote IP Active / Passive
11	Remote IP Input	Remote IP Input
12	Remote ID	Remote ID Active / Passive
13	Remote ID Input	Remote ID Input
14	Genarate Firewall Rule Autimatically	Add Firewall Rule Automatically for Remote Network Access

# 60. Policy;

It is the section where IPSEC PHASE1 and PHASE2 definitions are assigned to created profile.

IPS	IPSec SSL VPN CLIENT L2TP Servis Yönetimi						
S	📃 Select All 🖆 Add 🥒 Edit 🄀 Delete					Filter	IDSoo A
Id	2 3 Name 4	5 Mod	Compact	PFS	Phase 1	Phase 2	IP SEC ^
1	Default	main	No	No	3des-md5	3des-md5	Profile Administration
							Policy     Connection Tracking

1	Policy	Manage IPSEC Profile
2	Select All	Select All Policy
3	Add	Create a New Policy

4	Edit	Edit Selection Policy
5	Delete	Delete Selection Policy

#### Step 2:

## 61. Add Policy

It is the section where connection method and policy general definitions before IPSEC PHASE1 and PHASE2 are made.

Edit Policy	×
1       Policy Name       Default         2       Description       Default_Profile         Mod       • Main       Aggressive       ikev2         3       4       5	6 8 Compact Data Transfer Re-keying Enable Fragmented Packet Handling Key tries 7 9 0 0 = Unlimited

1	Policy Name	Policy Name Input
2	Description	Description for Policy
3	Main Mod	Connection Mod is Main
4	Aggressive Mod	Connection Mod is Aggressive
5	lkev2 Mod	Connection Mod is Ikev2
6	Compact Data Transfer	Compact Data Transfer Active / Passive
7	Fragmented Packet Handing	Fragmented Packet Handing Active / Passive
8	Re-keying Enable	Re-keying Enable / Disable
9	Key Tries	Key Tries Value Input

#### 62. Add PHASE-1;

It is the section where settings such as Encryption, Authentication, Connection times, The method to follow in case of disconnection, are defined. It is required that the configuration made here is mutually equal with the settings in the second place with which IPSEC VPN connection will be made.

PHASE 1 PHASE 2				
1       Encryption       3des       2       Authentication       md5         3       Encryption       none       4       Authentication       none         5       Encryption       none       6       Authentication       none	Diffie Hellman Groups(DH):         10       1 (DH-768)         12       14 (DH-2048)         13       15 (DH-3072)         14       5 (DH-1536)			
7       Key Life Time       28800       Sec          8       Rekey Margin       3600       Sec          9       Randomize Re-keying Margin       100       %	16   Dead Peer Detection     17   Action     18   Delay     30   Sn			
	20 Save Cancel			

1	Encryption	Encryption Metod
2	Authentication	Authentication Metod
3	Encryption-More	Encryption Metod
4	Authentication-More	Authentication Metod
5	Encryption-More	Encryption Metod
6	Authentication-More	Authentication Metod
7	Key Life Time	Key Life Time / Sec
8	Rekey Margin	Rekey Margin / Sec
9	Randomize Re-keying Margin	Randomize Re-keying Margin / %
10	Diffie Hellman Groups-1	Dh Groups -1 / 768 bit
11	Diffie Hellman Groups-2	Dh Groups -2 / 1024 bit
12	Diffie Hellman Groups-14	Dh Groups -14 / 2048 bit
13	Diffie Hellman Groups-15	Dh Groups -15 / 3072 bit
14	Diffie Hellman Groups-5	Dh Groups -5 / 1536 bit
15	Diffie Hellman Groups-16	Dh Groups -16 / 4096 bit
16	Dead Peer Detection	Dead Peer Detection Active / Passive
17	Action	Action : Restart / Clear / Hold
18	Delay	Delay Time / Sec
19	Timeout	Connection Timeout / Sec
20	Save	Save Configuration
21	Cancel	Cancel Configuration

### 63. Add PHASE-2;

It is the section where the second PHASE settings such as Encryption, Authentication, Connection times, are defined. It is required that the configuration made here is mutually equal with the settings in the second place with which IPSEC VPN connection will be made.

PHASE 1 PHAS	5E 2			
1 Encryption	3des 🔻	2 Authentication	md5 🔻	
3 Encryption	none 🔻	4 Authentication	none	
5 Encryption	none 🔻	6 Authentication	none 🔻	
Key Life Time 3600 Sec -				
▼ Pro Gloups (DH).         ■         1 (DH-768)         ▼ 2 (DH-1024)         5 (DH-1536)         14 (DH-2048)         15 (DH-3072)         16 (DH-4096)         10         11         12         13         14				
	-	-		
			15	16 Save X Cancel

1	Encryption	Encryption Metod
2	Authentication	Authentication Metod
3	Encryption-More	Encryption Metod
4	Authentication-More	Authentication Metod
5	Encryption-More	Encryption Metod
6	Authentication-More	Authentication Metod
7	Key Life Time	Key Life Time / Sec
8	PFS Groups (DH)	PFS Groups Active / Passive
9	Diffie Hellman Groups-1	Dh Groups -1 / 768 bit
10	Diffie Hellman Groups-2	Dh Groups -2 / 1024 bit
11	Diffie Hellman Groups-14	Dh Groups -14 / 2048 bit
12	Diffie Hellman Groups-15	Dh Groups -15 / 3072 bit
13	Diffie Hellman Groups-5	Dh Groups -5 / 1536 bit
14	Diffie Hellman Groups-16	Dh Groups -16 / 4096 bit
15	Save	Save Configuration
16	Cancel	Cancel Configuration

#### Step 3:

## 64. Add Global Policy

For Remote Network access permissions in cases where Generate Firewall Rule Automatically option is not selected, Step 3 and Step 4 must be applied.



#### Step 4:

## 65. Add NAT policy



### 66. Delete Profile

Select **Delete profile** to delete Connection.



Then a screen appears prompting **Are you sure you want to delete connection Test VPN**, click on **Yes** tab to delete connection.

Delete C	connection 🗙
2	Are you sure you want to delete connection TestVPN ?
	Yes No

Below screen appears stating Changes saved, click on Ok.



**67. Connection Tracking;** 

IPSEC Connection Monitoring / Status, Send and Recive Bytes/Package, Phase-1/Phase-2 ReAuthentication Status.

IPSec	IPSec SSL VPN CLIENT L2TP Servis Yönetimi										
🚙 Conne	🐼 Connect 🖉 Disconnect										
	Connection Name	Phase 1 Reauthentication	Received Bytes/Package	Send Bytes/Package	Remote IP	Status	IPSEC ^				
<b>-</b>	TEST (main-10.11.12.221-PSK)						Profile Administration				
0	test	-	-	-	1.1.1.2	<u> </u>	Policy				
	Merkez_to_Ankara (main-10.11.12.221-PSK)						Connection Tracking				
0	Ankara	-	-	-	88.10.10.12	<u> </u>					
	Merkez_to_lzmir (main-10.11.12.221-PSK)										
0	Ankara	-	-	-	88.1.1.2	<u> </u>					

# SSL VPN Configuration using CLI.

Open CLI using root user

### Step 1:

For SSL VPN, sample Configuration file is copied to relevant folder. labris-ssl-vpn.conf file is edited taking the following sample as base.

```
# cd /etc/openvpn/
# ls
```

#### samples

```
# cp -a samples/labris-ssl-vpn/* .
# ls -ltr
labris-ssl-vpn labris-ssl-vpn.conf up-down.sh samples
```

# vim labris-ssl-vpn.conf

And edit labris-ssl-vpn.conf;

#SSL VPN client using ip address (SSLVPN Network) server 172.16.0.0 255.255.255.0

# Change Maximum online client count max-clients 100

# access to Local Area Network address (INSIDE Network) push "route 192.168.2.0 255.255.255.0"

#### Step 2:

#### 68. Create a new global policy

INSIDE Network access to SSLVPN Network and SSLVPN Network access to INSIDE Network.



Step3:

69. Create a new NAT Policy



#### Step4:

Select a SSL VPN User (Please refer User Management section to **add user**) and add/Select VPN user (Please refer SSI VPN Client section for VPN  $\rightarrow$  User Administration  $\rightarrow$  Add)

🔢 Labris Management Console	1						- 6 ×
<u>File Edit View M</u> odule About							Help
Sa 🖹 🖹	DOL VHU CL	JENJI L2TP					😂 VPN Main 🛛 🖇
🖃 🚼 Server	Select All	🔀 Delete 🍃	🖊 Edit 🛛 🍄 Add 🖉 🖉 Se	ettings		🔍 Filter	Configuration
slave:4000		User Name	Name Surname	IP Address	Source	Domain	Connection
User Management		salih	Salih Ucpinar	10.8.3.2	labris	slave	So User Administration
System		sam	sam	10.8.3.3	labris	slave	
Eirowoll		administrator		10.8.3.4	ad	labtest.local	
VPN							🙁 System 🛛 🕆
Antispam/Antivirus							8 Service
- DS/IPS							Connection Viewer
Messaging							
Load Balancer							Save Changes 🔗
- 0m License							Apply 8
							Discard
							il .

### Step5:

## 70. Add a user on policy.

(Please refer to Users in Object Group section for Create Network Object  $\rightarrow$  Users)

Le For Tien Hoope Hoop											
🍓 🖹 🖹	Policy	Dbject	O Ins	ert Rule	In:	stall	Cor	nections	010	IP-MAC Ma	atcher
Server	Configuration	NenFrenal	Object								
slave: 4000	Objects	No.	Source	Destination	Service	Action	Schedule	QoS/Ban	. Applicati.	. Security P	. Options
System	Hosts	0	INSIDE OUTSIDE	🗅 Any	🗅 Any	Accept	🗅 Апу	🗅 Any	🗅 Any	🗅 Any	₽¢
REFINE VPN	RewHostsObject	1	P INSIDE Net	SSLVPN Net	Any	Accept	Any	Any	Any Any	Any Any	Pod P
Antispam/Antivirus	B WebServer     WebServer     Standard	2	SSLVPN_Net		🗅 Any	📿 Accept	🗋 Any	🗋 Any	🗅 Any	🗅 Any	÷¢₽
1	Address Ranges     Address Ranges     Deloct Groupe     Users     User Defined     My IT Departmen     MSSLVPNUsers     Setures										
1	Address Ranges     Address Ranges     Dest Component     Users     Users     Dest Defined     Dest Defined     Dest Debos     Dos & DDos     Ossendwidth     Schedule     Application Control     Firewall     NewFirewallObject	3	f SSLVPNUsers User Grou	p		40					
1	Address kanges     Address kanges     Address kanges     Users     Users     Users     Serves     My IT Departmen     Serves     Oos & DDos     Schedule     Schedule     Firewall     Firewall     Schedule	3 Properties of Name	FSLVPNUsers User Group	9							_
1	Address kanges     Address kanges     Address kanges     Users     Users     Users     Oss kupser     Oos	3 Properties of Name SSLVPNU	f SSLVPNUsers User Grou Sers	•							
1	Address kanges     Address kanges     Address kanges     Users     Users     Users     Oss k Deos     Oss k Dos     Oss     Oss k Dos     Oss k Dos     Oss k Dos     Oss     Oss k Dos     Oss     Oss k Dos     Oss	3 Properties of Name SSLVPNU	f SSLVPNUsers User Grou sers Users In D	atabase				Users In	n Current (	Group	
1	Address Ranges     Address Ranges     Users     Users     Users     Stures     Stur	3 Properties o Name SSLVPNU	f SSLVPNUsers User Grou sers Users In D	atabase	Q Filter			Users in	n Current (	Group	<u>Q</u> , Fi (e
1	Address Ranges     Address Ranges     Users     Users     Users     Stures     Stur	3 Properties of SSLVPNU	f SSLVPNUsers User Grou sers Users In D e Type	Patabase Domain S	Q. Filter		Name	Users in Type	n Current (	Group	Source
1	Address Ranges     Address Ranges     Address Ranges     Users     Users     Users     Oss G DOs     Oss     Os	3 Properties C Name SSLVPNU	f SSLVPHUsers User Grou sers Users In D e Type Ia user Ia	atabase Domain S btest.local ad	Q, Filter	saih	Name	Users Ir Type user	n Current ( slave	Group omain lab	Source

## 71.SSL VPN CLIENT - User Administration

The management part deals with adding user names and passwords to electronic directories along with the assignment of rights to data and network resources such as files, databases, printers, Internet. Maintenance includes updating the directories when employees change their job classifications or departments or leave the company.

In the right pane under VPN Main, select SSL VPN CLIENT - User Administration.

IPSec	SSL VPN CLIENT	L2TP	Servis Yör	etimi			
Selec	t All 🔀 Delete	🥖 Edit	🐥 Add	🥒 Settings 🧕			🔍 Filter
1	2 User Nam	e <mark>3</mark>	4	Name Surname	IP Address	Source	Domain
		_	-				
1	Select Al	I			Select All User	S	

1	Select All	Select All Users	
2	Delete	Delete Selection User/Users	
3 Edit Edit Selection User			
4	Add	Add User	
5	Settings	Setting SSL VPN CLIENT	

#### **SSLVPN Client**

SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. In contrast to the traditional Internet Protocol Security (IPsec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer. It is used to give remote users with access to Web applications, client or server applications and internal network connections.

An SSL VPN consists of one or more VPN devices to which the user connects by using his Web browser. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol or its successor, the Transport Layer Security (TLS) protocol. An SSL VPN offers versatility, ease of use and granular control for a range of users on a variety of computers, accessing resources from many locations

SSL VPN CLIENT L2TP									
Sele	ect All 🔀 Delete	🥖 Edit 🛛 🍄 Add 🥖	Settings		🔍 Filter				
	User Name	Name Surname	IP Address	Source	Domain				
	salih	Salih Ucpinar	10.8.3.2	labris	slave				
	sam	sam	10.8.3.8	labris	slave				
	administrator		10.8.3.4	ad	labtest.local				

## Add Click on Add tab

SSL V	IPN CLIENT L2TP				
Sele	ect All 🛛 🗶 Delete 🌽 Edit	👙 Add 🥒 Settings			Filter
	User Name	Name Surname	IP Address	Source	Domain
	salih	Salih Ucpinar	10.8.3.2	labris	slave
	sam	sam	10.8.3.3	labris	slave
	administrator		10.8.3.4	ad	labtest.local

## Below screen appears.

Selecting Users		Filter				Selected Users	2	<b>G</b> Filter	
Name	Туре	Source	Domain			Name	Туре	Source	Domain
salihucpinar	user	ad	labtest.local		. 3	guest	user	ad	labtest.local
guest	user	ad	labtest.local		>	5			
sm_949f021062d	user	ad	labtest.local						
labris	user	ad	labtest.local						
sam	user	labris	slave		4				
administrator	user	ad	labtest.local						
sucpinar	user	ad	labtest.local		<				
sm_34ac2b83b80	user	ad	labtest.local		_				
salih.ucpinar	user	ad	labtest.local						
sm_55ae4f2645a	user	ad	labtest.local	-	•				
				ОК	Car	cel			

## These are the inputs adding User to SSLVPN Client

1	All Users All the Users are displayed in this field				
2	Selected Users Selected Users are only displayed in this field				
3	>	This symbol helps us to add Users to Selected Users from All Users			
4	~	This symbol helps us to remove User from Selected Users list			

Click on **Ok** to add User.

## Adding User is in Progress

Applying changes	Labris Teknoloji	×
, ppy ing energeen.	Applying changes	

In the below screen we can notice Selected User added to the SSLVPN Client.

SSL V	SSL VPN CLIENT L2TP									
Sele	ect All 🔀 Delete	🥒 Edit 🛛 🍄 Add 🥖	Settings		Filter					
	User Name	Name Surname	IP Address	Source	Domain					
	guest		10.8.3.3	ad	labtest.local					
S	salih	Salih Ucpinar	10.8.3.2	labris	slave					
	sam	sam	10.8.3.8	labris	slave					
	administrator		10.8.3.4	ad	labtest.local					

## Edit

## Select User and click on Edit tab

SSL V	PN CLIENT L2TP				
Sele	ect All 🛛 🗶 Delete 📝 Edit	Add 🥜 Settings	labris		🔍 Filter
	User Name	Name Surname	IP Address	Source	Domain
	salih	Salih Ucpinar	10.8.3.2	labris	slave
~	sam	sam	10.8.3.3	labris	slave

Edit User tab appears, we can only edit IP Address and click on **Ok** tab.

Edit User	>	<
User Name	sam	
Domain	slave	
IP Address	10.8.3.8 Automatic	
	OK Cancel	

## Editing User is in Progress.

Labris Teknoloji	×
Applying changes	

In the below screen, we can notice IP Address has been changed.

SSL VPN CLIENT L2TP						
Sele	ect All 🛛 🗶 Delete 📝 Edit	🛉 Add 🥜 Settings	labris		🔍 Filter	
	User Name	Name Surname	IP Address	Source	Domain	
	salih	Salih Ucpinar	10.8.3.2	labris	slave	
	sam	sam	10.8.3.8	labris	slave	

#### Delete

Select User and click on **Delete** tab.

SSL VPN CLIENT L2TP						
Select All 🗶 Delete 🥒 Edit 🔮 Add 🥒 Settings 🛛 🕼 labris				🔍 Filter		
User Name	Name Surname	IP Address	Source	Domain		
salih	Salih Ucpinar	10.8.3.2	labris	slave		
✓ sam	sam	10.8.3.8	labris	slave		

Then below screen appears, Click **Ok** to delete.



Deleting Process is in progress.

Labris Teknoloji	×
Deleting	

Below screen appears displaying information, Selected records have been deleted. Click on **Ok** to close the current tab.



## Settings

Click on **Settings tab** to view and change the Settings of SSL VPN Client.

SSL V	SSL VPN CLIENT L2TP					
Sele	ect All 🔀 Delete	🥒 Edit 🛛 🍄 Add 🗾	Settings		🔍 Filter	
	User Name	Name Surname	IP Address	Source	Domain	
	salih	Salih Ucpinar	10.8.3.2	labris	slave	
	administrator		10.8.3.4	ad	labtest.local	

## AD Settings tab appears.

AD Settings X					
Group Authorising					
Domain Name 🛛 🗛	BTEST.LOCAL 2				
Work Group	BTEST 3	-		- í	
AD Group it	4			3	
🔍 Filter	_				
	Please select the	group from the table	1		
Name	Туре	Source	Domain		
sales	group	ad	labtest.local		
management	group	ad	labtest.local		
pazarlama	group	ad	labtest.local		
it	group	ad	labtest.local		
domain guests	group	ad	labtest.local	-	
domain users	group	ad	labtest.local		
accounting	group	ad	labtest.local		
unfiltered	group	ad	labtest.local		
winrmremotewmi	group	ad	labtest.local		
domain admins	group	ad	labtest.local	-	
OK Cancel					

1	Group Authorizing	Ve can enable or disable this option	
2	Domain Name	omain Name is selected by default	
3	Work Group	Work Group is selected by default	
4	4 AD Group Select AD Group from the group table.		

Click on Ok.

### L2TP

L2TP uses packet-switched network connections to make it possible for the endpoints to be located on different machines. Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.

The two main components that make up L2TP are the L2TP Access Concentrator (LAC), which is the device that physically terminates a call and the L2TP Network Server (LNS), which is the device that terminates and possibly authenticates the PPP stream.

SSL VPN CLI	ENT L2TP		
Enable L2TP	connection		
Settings			
Server IP:			
Pre-shared Key:			
IP Range:	192.168.1.128-192.168.1.254		
Local IP:	192.168.1.99		
Router:			
Other:			
Users	llear	ID.	Add
	USer	IP	Add
			Edit
			Delete

### Add

Enable L2TP connection to view and change settings of L2TP and to Add, Edit, Delete Users to L2TP.

## Click on Add tab

SSL VPN CLI	SSL VPN CLIENT 1277				
Enable L2TP	Enable L2TP connection				
Settings					
Server IP:	192.168.1.120				
Pre-shared Key:					
IP Range:	192.168.1.128-192.168.1.254				
Local IP:	192.168.1.99				
Router:					
Other:					
Users					
	User	IP Add Edit Delete	2		

Add User tab is appeared.

Add/Update User
Name: Jhon 1
Password: •••••••
IP: IP aralığından bir adresi otomatik ata 192.168.1.131
OK Cancel

These are the inputs to add an User.

1	Name	Type the name of the User
2	Password	Type the Password for the User
3	IP	We can enable default IP or give an IP within the IP range

Click on **Ok** to add User.

In the below screen, we can notice new **User** added to the Users list of **L2TP** within the IP Range.

SSL V	PN CLI	ENT L2TP				
🗸 Ena	ble L2TP	connection				
Settings						
Server	IP:	192.168.1.120				
Pre-sha	ared Key:					
IP Ran	ge:	192.168.1.128-192.168.1.254	1			
Local IF	₽:	192.168.1.99				
Router:						
Other:						
>						
Users						
		User			P	Add
Jhon				192.168.1.131		Edit
						Delete
						Delete

## Edit

Select the User and click on Edit tab.

Users		
User	IP	Add
Williams	*	Edit
Jhon	192.168.1.131	Luit
		Delete

Below screen appears.

We can edit Name, Password and the IP of the User.

Add/Update	User X
Name	Williams
Password	
IP:	IP aralığından bir adresi otomatik ata 192.168.1.140
	OK Cancel

Click on Ok.

We can notice the changes made to the **User** in the below screen.

SSL VPN CLIENT L2TP	
✓ Enable L2TP connection	
Settings	
Server IP: 192.168.1.120	
Pre-shared Key:	
IP Range: 192.168.1.128-192.168.1.254	
Local IP: 192.168.1.99	
Router:	
Other:	
Users	
User IP	Add
Williams 192.168.1.140	Edit
192, 106, 1, 151	Delete

#### Delete

Select the User and click on Delete tab.

ŀr	Users		
	User	IP	Add
	Williams	192.168.1.140	Edit
	Jhon	192.168.1.131	
			Delete
l			
L			

Delete User tab appears with User name, click on Yes tab to delete the User.



We can notice the selected User deleted.

ſ	Users		
1	User	IP	Add
	Jhon	192.168.1.131	Edit
			Delete
l			

## 72. Service Management

In the right pane under VPN tab, select Service Management.

IPSec SSL VPN CLIENT L2TP Servis Yönetimi							
VPN Bağlantı Türü	DURUM		İşlem				
IPSec VPN	2	Start	3	😔 Restart			
L2TP VPN	at a second second second second second second second second second second second second second second second s	Start	🚀 Stop	😔 Restart			
PPTP VPN	ű.	Start	🚀 Stop	😔 Restart			
SSL VPN	ø	Start	🖉 Stop	estart			

	1	VPN Connection Type	VPN Connection Type List
--	---	---------------------	--------------------------

2	Status	Connection Status
3	Action	Connection Start / Stop / Restart

## **FILTER**

Filters are rule sets that control the flow of traffic into and out of a device. it consists of a series of from-then statements

You cannot apply more than one firewall filter per port, VLAN or router interface per direction input and output. For example, for a given port you can apply at most one filter in the input direction and one filter in the output direction. You should try to be conservative in the number of terms that you include in each filter, because a large number of terms require longer processing time during a commit operation and can make testing and troubleshooting more difficult.



The purpose of the filter is system can drop packets based on header information, rate-limit traffic, classify packets into forwarding classes, log and count packets or prevent denial of service attacks.



Right click on Filter and select Connect.

## 73. Filter Groups



#### Add New Filter Policy

These options will be exposed to the web filter.

	Policy	Dbject	O Insert Rule	▶ in	stall	Connec	tions	IP-MAC Matcher
Server	Configuration	Nenfrenalities						
slave:4000	Objects	No.	Original Src	Original Dst	Original Srv	Translated	Translated Ds	Translated Srv Co
System	* Distances	0	MSIDE_Net	🗅 Any	Minttp	Conginal		🔀 Labris Webfilter 😭
© IDSIPS Messaging Server Load Balancer ⊕ Ucense	Crewall     Firewall     Global Policy     NAT Policy     NAT Policy     Startho	100110						

## Add/Edit Filter Group

Click on Add icon to add a filter group.

	🍓 Filter Groups 🚱 Ban	ned Filte	rs 💿 I	Exception Filters	👷 Configuration	💿 Log Monitorin	g
	Default WF-Demo WF-Sales WF-Accounting WF-Marketing WF-Management WF-Unfiltered	Name: D Default Gro Mode: Filtering Le Anti-virus S Time Limit Start	efault oup: evel: Scanning: t End	Default  Filtered High	Days	🚳 Ac	d Time
		08:30	17:30	Mon,Tue,Thur,Wed,Fr	ri 		elete
		You can	manage	users of this filtering g	roup.		
						Ado	User
						Add	IP
						× Del	ete
ι	JRL/Content Filter Service Status	: Running					

Add Group tab appears, Give the Name of the Group and click on **Ok.** 



In the below screen we can notice new Filter Group added in the list.

🍓 Filter Groups 🛛 🚱 Ba	Banned Filters 🕜 Exception Filters 🚏 Configuration 🕜 Log Moni	itoring	
💠 🛥 🔮 🖊 🔎	Name: Joseph		
Image: Constraint of the second se	Name: Joseph Default Group: Default  Mode: Filtered  Filtering Level: High  Anti-virus Scanning:  Start End Days Users You can manage users of this filtering group	& Add Time X Delete	
		Add User Add Group Add IP Delete	
JRL/Content Filter Service Status: Running			

## Editing Filter Group

🔌 Filter Groups 🔞	Banned Filters @ Exception Filters 🏋 Configuration @ Log Monitorin	g
Image: Constraint of the second se	Name: Joseph 1 Default Group: WF-Unfiltered 2 Mode: Filtered 3 Filtering Level: Medium 4 Anti-virus Scanning: 5 Time Limit	
Joseph	Start End Days	Add Time
	You can manage users of this filtering group.	<ul> <li>Add User</li> <li>Add Group</li> <li>Add IP</li> <li>X Delete</li> </ul>

# These are the inputs for Filter Groups

1	Name	We can edit name of the filter group
2	Default Group	Choose Default Group from the drop down list
3	Mode	Choose Mode type from the drop down list
4	Filtering Level	Choose Filtering level form the drop down list
5	Anti-virus Scanning	We can Enable/Disable this option
🍓 Filter Groups 🛛 🚱	Banned Filters 🔞 Exception Filters 🚏 Configuration 🔞 Log Monitoring	J
--	---	------------------------
🔮 🛥 🔮 🦊 📔	Name: Joseph	
WF-Demo WF-Sales WF-Accounting	Mode: Filtered  Filtering Level: Medium	
WF-Marketing WF-Management WF-Unfiltered	Anti-virus Scanning: 🔽	
Joseph	Start End Days	& Add Time 🔀 Delete
a P	Users You can manage users of this filtering group.	
5 5 6		Add User
5 7 7		🍇 Add Group
		🦪 Add IP
		🔀 Delete

# Click on Save icon to save the Group configuration

# **Delete Filter Group**

Click on the Remove icon to Delete Group.

🍓 Filter Groups 🏼 🚱	Banned Filters @ Exception Filters 🚏 Configuration @ Log Monitoring
Default Remove group WF-Demo WF-Sales WF-Accounting WF-Marketing WF-Management	Name: Joseph Default Group: WF-Unfiltered ▼ Mode: Filtered ▼ Filtering Level: Medium ▼ Anti-virus Scanning: ▼ _ Time Limit
Joseph	Start End Days
	2 You can manage users of this filtering group.

Delete Group tab appears, click on **Yes** to Delete Group.



In the below screen we can notice Filter Group deleted.



### **Time limit**

Time limit enables us to set up Starting time and ending time of the Filter Groups.

	🍓 Filter Groups 🔞 I	Banned Filters 💿 Exception Filters 🊏 Configuration 💿 Log Monitoring	
	💠 🛥 🔺 🏺 🦓	Name: WF-Demo	
	Default	Default Group: Default 🔻	
	WF-Demo	Mode: Filtered	
	WF-Sales		
	WF-Accounting	Filtering Level: High 💌	
	WF-Marketing	Anti-virus Scanning:	
	WF-Management		
	WF-Unfiltered	Time Limit	
		Start End Days	d Time
		Z De	lete
<1			

Add Time Click on Add time tab

🍓 Filter Groups 🚳	Banned Filters 🔞 Exception Filters 🎇 Configuration 🔞 Log Monitoring
💠 🛥 🔹 🖊 📖	Name: WF-Demo
Default	Default Group: Default 🔻
WF-Demo WF-Sales	Mode: Filtered -
WF-Accounting	Filtering Level: High 🔻
WF-Marketing WF-Management WF-Unfiltered	Anti-virus Scanning: 🔽
	Start End Days

Time Limits tab appears.

Time Limits 🗙
Edit time limits of this filter group.
<ul> <li>Monday</li> <li>Tuesday</li> <li>Wednesday</li> <li>Friday</li> <li>Saturday</li> <li>Sunday</li> </ul>
All Days 🔽 Weekdays 🗌 Weekend
OK Cancel

These are the inputs for adding Time Limit.

1	Start Time	Choose the starting time
2	End Time	Choose the ending time
3	Days	We can enable specific days

Click on Ok.

In the below screen, we can notice Time Limit

👌 Filter Groups 🚳 I	Banned Filt	ters 🥝	Exception Filters 🛛 🎀 Configuration 🤇 🚱 Log Monitoring	,
Image: second se	Name: W Default Gro Mode: Filtering Le Anti-virus S	/F-Demo oup: evel: Scanning:	Default  Filtered High	
WF-Unfiltered	Time Limit	l		
	Start	End	Days	Add Time
	09:30	14:30	Mon,Tue,Thur,Wed,Fri	🔀 Delete

### **Delete Time**

Select the Time Limit and click on **Delete tab.** 

🍓 Filter Groups 🚱	Banned Filters 💿 Exception Filters 🚏 Configuration 💿 Log Monitoring	
	Name: WF-Demo   Default Group: Default   Mode: Filtered   Filtering Level: High   Anti-virus Scanning: Image: Comparison of the second secon	
	Start     End     Days       09:30     14:30     Mon,Tue,Thur,Wed,Fri	Add Time Delete

In the below screen we can notice Time Limit deleted.

🝇 Filter Groups 🚱	Banned Filters	Exception Filters	<b>Configuration</b>	💿 Log Monitoring	
	Name: WF-Demo Default Group: Mode: Filtering Level: Anti-virus Scanning:	Default  Filtered High			
	Start End		Days		🐁 Add Time Ҟ Delete

### Add Users

.

Click on Add Users tab

🍓 Filier Groups 🌀	Banned Filters 🕜 Exception Filters 🍿 Configuration 🚱 Log Monitorin	g
	Name: WF-Demo Default  Mode:  Filtered  Filtering Level: High  Anti-virus Scanning:	
Wi -Officied	Start End Days	Add Time
	You can manage users of this filtering group.	Add User Add Group Add IP
		X Delete

Add Members tab appears, in which we can choose Members and click on Ok.

A	ld Members 🗙 🗙
	Search:
	Name
	sm_6dccb10b4bad42f98@labtest.local
	salihucpinar@labtest.local
	guest@labtest.local
	sm_949f021062dd4c10a@labtest.local
	labris@labtest.local
ļĮ	✓ sam@slave
	administrator@labtest.local
	sucpinar@labtest.local
	sm_34ac2b83b806403c9@labtest.local
	salih.ucpinar@labtest.local
!	sm_55ae4f2645a049f69@labtest.local 🔹
	Ok Cancel Help

In the below screen, we can notice selected Members added to the Filter Group.

🍓 Filter Groups 🌀	Banned Filters 💿 Exception Filters 🎇 Configuration 💿 Log Monitoring
<b>⇔</b> = ↑ <del>♥</del> 🖰	Name: WF-Demo
Default	Default Group: Default
WF-Demo	Mode: Filtered 🔻
WF-Sales WF-Accounting	Filtering Level: High 💌
WF-Marketing	Anti-virus Scanning: 🗸
WF-Management WF-Unfiltered	Time Limit-
	Start End Days 🔕 Add Time
	2 Delete
	; []
	Users
	You can manage users of this filtering group.
	salih.ucpinar@labtest.local
	seven@labtest.local
	👼 Add IP
	🔀 Delete

Add Groups

Click on Add Groups tab.

🍓 Filter Groups 🌀	Banned Filters 🔞 Exception Filters 💡 Configuration	🚱 Log Monitoring
Cefault WF-Demo WF-Sales WF-Accounting WF-Management WF-Unfiltered	Name: WF-Demo Default Group: Default Mode: Filtered Filtering Level: High Anti-virus Scanning: ✓ Time Limit Start End Days Users You can manage users of this filtering group. seven@labtest.local salih.ucpinar@labtest.local sam@slave	Add Time Add Time Add User Add User Add Group Add IP Celete

Add Members tab appears, select the Groups and click on Ok.

Add M Sea	lembers arch:	×			
	Name				
	@Management@slave				
	@Sales@slave				
	@Marketing@slave				
✓ (	@loakUsers@slave				
	@sales@labtest.local				
	@management@labtest.local				
	@pazarlama@labtest.local				
	@it@labtest.local				
	@domain guests@labtest.local				
	@domain users@labtest.local				
	@accounting@labtest.local	•			
	Ok Cancel Help				

In the below screen, we can notice **Group** added in the Users list.

🍓 Filter Groups 🌀	Banned Filters 🕜 Exception Filters 🍿 Configuration	Log Monitoring
Image: Constraint of the second se	Name: WF-Demo Default Group: Default Mode: Filtered Filtering Level: High Anti-virus Scanning: Time Limit Start End Days Users You can manage users of this filtering group. @loakUsers@slave salih.ucpinar@labtest.local sam@slave seven@labtest.local	Add Time Celete  Add User  Add Group  Add IP  Celete

# Add IP/ IP Range

Click on Add IP tab.

🍓 Filter Groups 🚳	Banned Filters	Exception Filters	<b>Configuration</b>	💿 Log Monitoring
Default     WF-Demo     WF-Sales     WF-Accounting     WF-Marketing     WF-Marketing     WF-Unfiltered	Name: WF-Demo Default Group: Mode: Filtering Level: Anti-virus Scanning: Time Limit Start End Users You can manage u @loakUsers@slave salih.ucpinar@labtes saw@slave seven@labtest.loca	Default	Days	Add Time Add User Add Group Add IP Colored Add IP Delete

Add IP tab appears, type valid IP Address within the range mentioned in the below tab and click on **Ok**.

Add IP
Enter below IP address definitions each on a new line.
You can use any valid IP address (172.16.0.5), network (192.168.1.0/24) or address range (10.0.0.115-10.0.0.120).
IP Addresses           10.0.0.118           172.16.0.6
OK Cancel Help

In the below screen, we can notice IP Address in the Users tab.

🍓 Filter Groups 🌀	Banned Filters	Exception Filters	<b>Configuration</b>	💿 Log Monitoring
🌵 🛥 🔺 🤣 💾	Name: WF-Demo			
Default	Default Group:	Default 💌		
WF-Demo	Mode:	Filtered 🔻		
WF-Sales	Filtering Level:	High		
WF-Accounting	Fillering Level.			
WF-Management	Anti-virus Scanning	<ul> <li>✓</li> </ul>		
WF-Unfittered	Time Limit			
	Start End	D	ays	Add Time
				Z Delete
	Hener			
	You can manage	uppers of this filtering group		
	Fou can manage	users of this intering group	<b>y</b> .	
	10.0.0.118			Add User
	172.16.0.6			🍇 Add Group
				Add IP
				🔀 Delete
	L			

### Delete

Select the IP Address or User or Group and click on **Delete** tab.

🔌 Filter Groups 🌀	Banned Filters	Exception Filters	<b>Configuration</b>	Log Monitoring
Cefault WF-Demo WF-Sales WF-Accounting WF-Marketing WF-Management WF-Unfiltered	Name: WF-Demo Default Group: Mode: Filtering Level: Anti-virus Scanning	Default  Filtered High		
	Start End	D users of this filtering group	ays	Add Time
	10.0.0.118 172.16.0.6			Add User

In the below screen, we can notice selected Group deleted.

🍓 Filier Groups 🌀	Banned Filters 💿 Exception Filters 🍿 Configuration	on 🕜 Log Monitoring
Cefault WF-Demo WF-Sales WF-Accounting WF-Marketing WF-Management WF-Unfiltered	Name: WF-Demo Default Group: Default Mode: Filtered Filtering Level: High Anti-virus Scanning: Time Limit	
	Start End Days	Add Time
	10.0.0.118	Add User

### 74. Banned Filters

🍇 Filter Groups	🕟 Banned Filters	Exception Filters	<b>P</b> Configuration	Log Monitoring
Default 👻				
Domain				
Regex URL				
Phrases				
Extension				
🎯 Mime				
Content				

Select the profile from the drop-down menu and below shown settings (Domain, URL, Regex URL, Phrases, Extensions, Mime, and Content) can be done separately for each profile.

In the below screen we have selected default profile.

🍇 Filter Groups	👒 Banned Filters	Exception Filters	<b>Configuration</b>	Log Monitoring
Default				
Default				
WF-Demo				
WF-Sales				
WF-Accounting				
WF-Marketing				
WF-Management				
WF-Unfiltered				
Phrases				
A Extension				
<b>8 Mime</b>				
Content				

## 75. Domain/ Category Filtering

Domain filter is the firewall function to help you block the specified domain. When we click on Domain tab, all the categories in the Domain are displayed. Exceptional sites from banning are being selected in the Categories list.

Section 2017	🕞 Banned Filters 💿 Exception Filters	<mark> </mark> Cor	figuration	💿 Log Monitoring
Default	Banned Site Banned Sites lists. This filters block all of a site.			
Domain	Categories	_	Custo	m Si 🔗 Add
	Military		V badbo	ys.c
Regex URL	Music     News			🛥 Delete
Nrases	Social Networking			
A Extension	Portal Sites Search Engines			
🍪 Mime	Online Ads     Job Search			
Content	Real Estate			
	Miscellaneous Parked			
	Block all (except for Exception Site list)	-		

### Add

Click on Add tab.

lefter Groups	🔞 Banned Filters	ed Filters 💿 Exception Filters 🚏 Configuration		🔞 Banned Filters 💿 Exception Filters 🛛 🎌 Configuration 💿 Log Moni		n 💿 Log Monitoring
Default	Banned Site Banned Sites lists. This	filters block all of a site.				
Domain	Military	Categories	Cus	tom Si 🔗 Add		
Regex URL	Humor Music News			😅 Delete		
Phrases	Veb-based Em	ng ail				
Sea Mime	Search Engines     Online Ads     Job Search	3				
Content	Spam Miscellaneous Parked					
	Block all (except f	or Exception Site list)	<b>•</b>			

Add site tab appears, type domain name to be banned and click **Ok.** 



Message tab appears stating that This site is already in banned list, Click Ok.



# Add More

Click on Add More tab.

lefter Groups	Banned Filters 🕜 Exception Filters 🏼 🎀 Co	onfiguration 🕜 Log Monitoring
Default 👻	anned Site anned Sites lists. This filters block all of a site.	
Domain	Categories	Custom Si 👙 Add
	Torrent Repository	✓ badboys.c
URL	✓ Toys	🚰 Add More
	Unreachable	😑 Delete
Regex URL	Web Hosting, ISP & Telco	
	Web-based Greeting Cards	
Mases Phrases	Wikis	
	Image Search	
A Extension	Community Forums	
	Remote Access	
🏙 Mime	Marketing Services	
	Motorized Vehicles	
Q Content	<ul> <li>Food &amp; Restaurants</li> </ul>	
	Legislation, Politics & Law	
	<ul> <li>Personal Pages &amp; Blogs</li> </ul>	
	Sport Fighting	
	Text Messaging & SMS	
	Block all (except for Exception Site list)	

Add Bulk Site tab appears type name of the domain as one in each line and click **Ok.** 

Please enter dom:	ain names as one in ea	ch line	
Adds.com			
Games.com			

Message tab appears stating that This site is already in banned list, Click Ok.

Messag	e	×
1	Adds.com This site is already in banned list.	
	OK	

Message tab appears stating that This site is already in banned list, Click Ok.



Message tab appears stating that This site is already in banned list, Click Ok.



### Delete

Select the site and click on **Delete** tab.

🍇 Filter Groups	3	anned Filters 💿 Exception Filters	) y	Со	nfiguration	<b>@</b> 1	Log Monitoring
Default	Banne Bann	ed Site ed Sites lists. This filters block all of a site.					
Domain		Categories			Custo	m Si	🔗 Add
- Sup		Abortion - Pro Choice			🗸 badbo	ys.c	
URL		Abortion - Pro Life			-		Add More
		Agriculture					💷 Delete
Regex URL		Architecture & Construction					· · · · · ·
		Arts					
Phrases		Astrology & Horoscopes					
8		Atheism & Agnosticism					
- Extension		Auctions & Marketplaces					
		Banking					
🥂 Mime		Biotechnology					
	-	Botnet					
Content		Businesses & Services (General)					
		Cartoons, Anime & Comic Books					
		Catalogs					
		Chat					
		Child Abuse Images		Υ.			
		Block all (except for Exception Site list)					

# 76. URL/Category Filtering

URL categories help us ensure real-time protection against today's targeted and advanced threats.

& Filter Groups	Banned Filters 🚱 Exception Filters 🎇 Configuration 🙆 Log Monitoring	
Default	Banned URL Banned URLs lists filters only a part of a site.	
Domain	Categories Custom URL List 👙 Ad	bi
- Jun	Compromised	
ORL	Hate Speech	More
	📃 Illegal Drugs 🔤 Dele	ete
Regex URL	Phishing/Fraud	
	Nudity	
Mases Phrases	Violence	
Bu	Weapons	
A A Extension	Anonymizer	
	Translator	
🌌 Mime	Alcohol	
	Pharmacy	
🔍 Content	Tobacco	
	Gambling	
	Games	
	Dating & Relationships	
	Travel	
	Military	
	Humor	
	Music	
	News Views	

# Add

Click on Add tab

Silter Groups	9	Banned Filters	Exception Filt	ers	1	Configuration	💿 Log Monitoring	
Default	- Bann Bann	ed URL ned URLs lists filters o	nly a part of a site.					
Domain		Cate	egories			Custo	m URL List	🖗 Add
🗗 URL		Compromised Hate Speech		•		members.home.r	net/uporn	🖗 Add More
		Illegal Drugs						💴 Delete
Regex URL	~	Phishing/Fraud						
Phrases		Violence						
A Extension		Weapons Anonymizer						
		Translator						
Mime		Pharmacy						
Sontent		Tobacco						
	~	Games						
	~	Dating & Relation	ships					
		Military						
		Humor						
		News						
				•				

Add Site tab appears type domain name to be banned and click **Ok.** 

Add Site		×
	Please enter an domain name:	_
-	Games.com/default.asp	
	OK Cancel	

In the below screen, we can notice domain name added in the Banned list.

🍇 Filter Groups	Banned Filters 🕜 Exception Filters 🕅 💏 Configuration 🧑 Log Monitoring	
Default 🔻	Banned URL-	
_	Banned URLs lists filters only a part of a site.	
Domain	Categories Custom URL List	👍 Add
-	Compromised 🔺 🗸 yahoo.com/index	
URL	Hate Speech Games.com/default.asp	🛛 🖓 Add More
-	Illegal Drugs	Delete
Regex URL	Phishing/Fraud	
-	Nudity	
Phrases	Violence	
	Weapons	
A Extension	Anonymizer	
-	Translator	
🏙 Mime	Alcohol	
	Pharmacy	
Content	Tobacco	
	Gambling	
	Games	
	✓ Dating & Relationships	
	Travel	
	Military	
	Humor	
	Music	
	News	
	Social Networking	
	Web-based Email	
	Portal Sites	
	Search Engines	
RL/Content Filter Ser	mice Status: Running	

#### Add More

Click on Add More tab.

lage Filter Groups	Banned Filters 💿 Exception Filters 🎇 Configuration 💿 Log Monitoring	
Default 👻	Banned URL Banned URLs lists filters only a part of a site.	
Domain	Categories Custom URL List 🔮 Add	
	Compromised	
URL	Hate Speech	e
	📃 Illegal Drugs	
Regex URL	Phishing/Fraud	
	Nudity	
Phrases	Violence	
8	Weapons	
<ul> <li>A Extension</li> </ul>	Anonymizer	
	Translator	
Mime Mime	Alcohol	
	Pharmacy	
Content	Tobacco	
	Gambling	
	Games	
	Dating & Relationships	
	Military	
	Humor	
	Music	
	News V	

Add Bulk URL tab appears, type name of the domain as one in each line and click Ok.

Add Bulk URL	×
Cartoon.com/index.html	7
Fashion.com/index.html	
OK Cancel Help	

#### Delete

Select the URL and click on **Delete** tab.

Sector 2015	Banned Filters @ Exception Filters 🎇 Configuration @ Log Monitoring
Default	Banned URL Banned URLs lists filters only a part of a site.
Domain	Categories Custom URL List Architecture & Construction Arts
Regex URL	Astrology & Horoscopes         Atheism & Agnosticism         Auctions & Marketplaces
Phrases	Banking Biotechnology
Extension	Botnet Businesses & Services (General)
Mime	Cartoons, Anime & Comic Books
Q Content	Child Abuse Images
	Control Control Centers
	Coupons Criminal Skills
	Educational Institutions Educational Materials & Studies
	Entertainment News & Celebrity Sit

# 77. Regex URL Filtering

This is completed when parts of the HTTP request are matched with the use of a list of regex patterns. You can either block specific URL's or block all URL's except for a select few particular URL's.

🍇 Filter Groups	Banned Filters 💿 Exception Filters 🏾 🎀 Configuration 🛛 💿 Log Monitoring	
Default 💌	Banned URL Regexes Block URLs with the following URL regexes match.	
Domain	While adding new element, you can use (+,-) marks in front of words.(default :+) For example if "+ sex - esex" is specified, it means block uris those include "sex" but not "esex". Note that URLs can include dash mark, so "dont match" mark must be used seperated.	
URL	URL Regex	🐥 Add
Regex URL	(adultsight]adultsite]adultsonly adultweb blowjob bondage centerfold cumshot cyberlust cybercore hardcor	
Phrases	(/\[/?+=&/])(girls babes)([?+=&/][\$) (/\[/?+=&/])(girls babes)([?+=&/][\$)	😅 Delete
A Extension	(nl/1+2+24)(anal(babe)bharath)boob(breas(busen(busk)(cliftum)cunt)dick(fetish)fuck(giri(hooter)lez(lust)na (nlutrism(naturist)nude)nudistinudism(nekkid)nakt(naakt)	
Mime	(adlog.php/cnt.cgilcount.cgilcount.dal/count.jsp/count.php/count.php/counter.cgilcounter.js/counter.pl/countlin           (*/[[?+=&/])(.*\_google\.*/.*?.*safe=off)([?+=&/]\$)	
Content	(*(!c?+=&/)).*(.alltheweb.com/customize)?.*copt_offensive=off)(!c?+=&/](\$) (yahoo.com/imageV)	
	(vimg.comvimagev) (altavista.comVimageV)	
	(altavista.comWideoV)	
	(cecid.php nph-proxy nph-prol/dmirror cgiproxy)	
	(anonymizer(proxity)megaproxy)	
	Variants/AVTest)	

# Add

# Click on Add tab

🍇 Filter Groups	Banned Filters @ Exception Filters 🎇 Configuration @ Log Monitoring	
Default 🔻	Banned URL Regexes	
	Block URLs with the following URL regexes match. While adding new element, you can use (+,-) marks in front of words.(default : +) For example if "+ sex - esex" is specified, it means block uris those include "sex" but not "esex". Note that URLs can include dash mark, so "dont match" mark must be used seperated.	
	URL Regex	🔗 Add
Regex URL	(adultsight adultsite adultsonly adultweb blowjob bondage centerfold cumshot cyberlust cybercore hardcor	
Phrases	(/[/?+=&/])(girls babes)([/?+=&/])\$) (/[/2+2+=&/]/biplcyberlbard bupe menalsmallisoff(supertiny bare naked bude anal gral topn?les seyV1.3*	😑 Delete
🚚 Extension	<pre>("['\'-\'+-&amp;_])(anal babe bharath boob breast busen busty clit cum cunt dick fetish fuck girl hooter lez lust na (naturism naturist nude nudist nudism nekkid nakt nakt )</pre>	
🎯 Mime	(adlog.php]cnt.cgi[count.cgi]count.dat[count.jsp]count.php]counter.cgi]counter.js]counter.pl[countlin	
Q Content	(\[[?+=&/]](*\alltheweb.com/customize\?.*copt_offensive=off)([!?+=&/]]\$) (yahoo.comVimageV)	
	(ving.comVimageV)	
	(altavista.comVimageV)	
	(anonymizer/proxify/megaproxy)	
	(proxy)	
	(Variants/AVTest)	

# Add URL Regex tab appears, type regex to be banned and click **Ok.**

Add URL	Regex	×
	Please enter a regex: rediff.com	-
	OK Cancel	_

In the below screen, we can notice Regex URL added to list



#### Add More

Click on Add Multiple tab.

Section 2010 Secti	Banned Filters @ Exception Filters   💏 Configuration   @ Log Monitor	ring
Default	Banned URL Regexes Block URLs with the following URL regexes match. While adding new element, you can use (+,-) marks in front of words.(default : +) For example if "+ sex - esex" is specified, it means block uris those include "sex" but not "esex". Note that URLs can include dash mark, so "dont match" mark must be used seperated.	
	URL Regex	🗳 Add
Regex URL	(^[-\?+=&/_))(big]cyber hard huge mega small soft super tiny bare naked nude anal  (^[-\?+=&/_))(anal babe bharath boob breast busen busty clit cum cunt dick fetish fu	Add Multiple
Phrases	(naturism naturist nude nudist nudism nekkid nakt naakt)       (adlog.php cnt.cgi count.cgi count.dat count.jsp count.pl count.php counter.cgi count	📟 Delete
A Extension	(^[\?+=&/])(.*\_google\*/.*\?.*safe=off)([\?+=&/]\$)           (^[\?+=&/])(.*\_alltheweb.com/customize\?.*copt_offensive=off)([\?+=&/]\$)	
🍪 Mime	(yahoo.comVimageV) (yimg.comVimageV)	
Q Content	(altavista.comVimageV) (altavista.comVvideoV)	. =
	(cecid.php nph-proxy nph-pro /dmirror cgiproxy)     (anonymizerlproxif/Imegaproxy)	
	(proxy)	
	(Variants/AVTest) (((?=(.*rediff))(?=(.*com)).*)	•

Add URL Regex tab appears, type regex as one in each line and click Ok.

Add URL Regex	×
_ Please enter a regex:	
facebook.com whatsapp	
OK Cancel Help	

In the below screen, we can notice Regex URL added in the list.

🍇 Filter Groups	💿 Banned Filters 🕜 Exception Filters 🍿 Configuration 💿 Log Monitor	ring	
Default 💌	Banned URL Regexes Block URLs with the following URL regexes match. While adding new element, you can use (+,-) marks in front of words.(default : +) For example if "+ sex - esex" is specified, it means block urls those include "sex" but not "esex". Note that URLs can include dash mark, so "dont match" mark must be used seperated.		
URL	URL Regex		🗳 Add
Regex URL	(naturism naturist nude nudist nudism nekkid nakt naakt) (adlog.php cnt.cgi count.cgi count.dat count.jsp count.pl count.php counter.cgi count		Add Multiple
Phrases	<pre>(^[(?+=&amp;/])(.*\.google\*/.*\?.*safe=off)([\?+=&amp;/] \$) (^[(?+=&amp;/])(.*\.alltheweb.com/customize\?.*copt_offensive=off)([\?+=&amp;/] \$)</pre>		😅 Delete
Extension	(yahoo.comVimageV) (yimg.comVimageV)		
🎯 Mime	(altavista.comVimageV) (altavista.comVvideoV)		
Content	Image: Construction of the second		
	(proxy)		
	((?=(.*rediff))(?=(.*com)).*)		
	((?=(.*facebook))(?=(.*com)).*) ((?=(.*upotcom)).*)		
	((/=(."wnaisapp)).")	-	

# Delete

Select Regex URL and click on **Delete** tab.

🍓 Filter Groups	👒 Banned Filters 💿 Exception Filters  🎌 Configuration 💿 Log Monitor	ing
Default	Banned URL Regexes Block URLs with the following URL regexes match. While adding new element, you can use (+,-) marks in front of words.(default : +) For example if "+ sex - esex" is specified, it means block urls those include "sex" but not "esex". Note that URLs can include dash mark, so "dont match" mark must be used seperated.	
URL	URL Regex	👙 Add
Pagey LIPI	(naturism naturist nude nudist nudism nekkid nakt naakt)	Add Multiple
INEGEN OIL	(adlog.php cnt.cgi count.cgi count.dat count.jsp count.pl count.php counter.cgi count	- Add Multiple
Phrases	(^[[\?+=&/])(.*\.google\*/.*\?.*safe=off)([\?+=&/] \$)	📟 Delete
	(^[[?+=&/])(.*\.alltheweb.com/customize\?.*copt_offensive=off)([\?+=&/] \$)	
Extension	(yahoo.comVimageV)	
-	(vimg.comvimagev)	
🦓 Mime	(altavista.com/vinagev)	
	(and visital continue ov) (cecid phplnph-prox/lpph-prol/dmirrorlcgiproxy)	
Content	✓ (anonymizer proxify megaproxy)	
	(proxy)	
	✓ (Variants/AVTest)	
	((?=(.*rediff))(?=(.*com)).*)	
	((?=(.*facebook))(?=(.*com)).*)	
	✓ ((?=(.*whatsapp)).*)	•

Delete URL Regex tab appears, click on Yes.



In the below screen, we can notice Regex URL deleted.

lacktrian Sector	Banned Filters @ Exception Filters 💏 Configuration @ Log Monitoring
Default	Banned URL Regexes Block URLs with the following URL regexes match. While adding new element, you can use (+,-) marks in front of words.(default : +) For example if "+ sex - esex" is specified, it means block urls those include "sex" but not "esex". Note that URLs can include dash mark, so "dont match" mark must be used seperated.
DURL	URL Regex 👙 Add
🔀 Regex URL	(^I?+=&/_)(anal babe bharath boob breast busen busty clit cum cunt dick fetish fu (naturism naturist nude nudist nudism nekkid nakt naakt)
Phrases	(adlog.phplcnt.cgi count.cgi count.dat count.jsp count.phplcounter.cgi count
A Extension	(^[[?+=&/])(.*\alltheweb.com/customize\?.*copt_offensive=off)([\?+=&/]]\$)         (yahoo.comVimageV)
🍪 Mime	(yimg.comVimageV) (altavista.comVimageV)
Content	(altavista.comWideoV) (cecid.php nph-proxy nph-pro /dmirror cgiproxy)
	(anonymizer proxify megaproxy)
	✓ (Variants/AVTest)
	((?=(.*rediff))(?=(.*com)).*)
	✓ ((?=(.*facebook))(?=(.*com)).*)

#### 78. Phrases

#### Add

In Banned filters, Select Phrases and Click on Add tab



### Add phrase tab appears.

Add Phrase	×
Please enter beginning word(s)(Eg. word1, 2)	
Please enter ending word(s)(Eg. word1,word2) Entertainment Sites 2	
Please enter a phrase for any position (Eg. word1,wd 2) Porn 3	
Please enter a phrase for exact match (Eg. v 4 1,word2) Pornografi	
OK Cance	

### These are the inputs to Add Phrase.

1	Beginning Words	Enter the Beginning words of the phrase	
2	Ending Words	Enter the Ending words of the phrase	
3	Phrase for any position	Enter a phrase	
4	Phrase for exact match	Enter a phrase for exact match	

Click on OK.

In the below we can notice that **Phrase** is added to the list.

lacktrian lacktri lacktrian lacktrian lacktrian lacktrian lacktrian lacktria	Banned Filters @ Exception	Filters 🛛 🎀 Config	juration 🕜 Log	g Monitoring		
Default 🔻	Banned Phrase List If a site content includes these, site will be ba	nned.				
Domain	Phrase Groups	at Begin	End	Any Point	Only	🖨 Add
-Sup	✓ User	Facebook Sites	Entertainment Sites	porn	pornografi	😅 Delete
OKL	Pornography Sites					
	Illegal Drug Sites	-				
Regex UKL	Gambling Sites					
Phrases	Google Searches					
A Extension						
🎯 Mime						
Content						

### Delete

Select the Phrase from the list and click on **delete** tab.

lage Filter Groups	G	) B	anned Filters 💿 Exception	or	n Filters 🛛 🎀 Co	onfiguration	😨 Log Monitor	ing	
Default 💌	Ba If	anne a sit	d Phrase List e content includes these, site will be	e b	anned.				
Domain			Phrase Groups		at Begin	End	Any Point	Only	🐥 Add
		✓	User		Facebook Sites	Entertainment Sites	porn	pornografi	- Delete
LP URL			Pornography Sites						Delete
			Illegal Drug Sites						
Regex URL			Gambling Sites						
Phrases			Google Searches						

Delete Phrase tab appears stating Are you sure? Click on Yes.



### **79. Content Change**

In this section, as seen in the places specified words or addresses to the new string to be replaced with the value entered into the field provided.

Content Filtering generally refers to the filtering of inappropriate content or messages, such as content containing objectionable materials, personal or sensitive information, in terms of information security. Content Filtering has different applications like for example, in internet the browsing, receiving mails accessing database, etc.

lage Filter Groups	Banned Filters @ Exception Filters	🚏 Configuration 🛛 💿 Log Monitoring	
Default	Banned Content Content modifying regular expressions. The format is: "extended regular expression"->"replacement straight stri case. Far more complicated matches are possible.	ng". E.g. "shit"->"censored" would replace all occurr	ences of shit in any
URL Regex URL Phrases	Regex	New String	Gerefeter Add G

Add Click on Add tab

lage Filter Groups	🔞 Banned Filters 🔞 Exc	eption Filters	Configuration	Log Monitoring
Default  Comain	Banned Content Content modifying regular expressio "extended regular expression"->"rep occurrences of shit in any case. Far more complicated matches are p	ns. The format is: placement straight s possible.	tring". E.g. "shit"->"censor	ed" would replace all
Regex URL	Regex		New String	🚽 Add
Phrases				
Extension				
Content				

Add New Regular Expression tab appears, type regex and click **Ok.** 

Add New Regular Expression				
	Please enter a regex:			
facebook.com				
	OK Cancel	_		

New string tab appears, type string and click **Ok.** 

New Str	ing	х
⚠	Please enter a string: acbd	
	OK Cancel	

In the below screen, we can notice Regex with new string.

🍇 Filter Groups	Banned Filters 💽 Exception F	ilters 🏾 🎀 Configuration 🗋 🚱 Log	Monitoring
Default	Banned Content Content modifying regular expressions. The for "extended regular expression"->"replacement s occurrences of shit in any case. Far more complicated matches are possible.	mat is: traight string". E.g. "shit"->"censored" would r	eplace all
	Regex	New String	🖨 Add
Regex URL	facebook.com	acbd	😑 Delete
Phrases			
A Extension			
🍪 Mime			
Content			

# Delete

Se Filter Groups	Banned Filters 💽 Exception F	ilters 🛛 🔐 Configuration	Log Monitoring
Default  Comain	Banned Content Content modifying regular expressions. The for "extended regular expression"->"replacement s occurrences of shit in any case. Far more complicated matches are possible.	mat is: traight string". E.g. "shit"->"censor	ed" would replace all
	Regex	New String	👙 Add
Regex URL	facebook.com	acbd	Delete
Phrases			
A Extension			
Mime			
Content			

Delete Content tab appear, click on Yes.



In the below screen, we can notice content is deleted.

liter Groups	Banned Filters @ Exception Filters	Configuration	Log Monitoring
Default 🔍	Banned Content Content modifying regular expressions. The format is: "extended regular expression"->"replacement straight occurrences of shit in any case. Far more complicated matches are possible.	string". E.g. "shit"->"censor	ed" would replace all
Regex URL	Regex	New String	
Extension			
Content			

### **80. Extension Filter**

🍓 Filter Groups	<b>B</b> 1	anned Filter	🛚 💿 Exception Filters 🛛 🎀 Configuration 🤇	🗿 Log	Monitoring
Default 🔻	Banne Block	ed Extension	hat can contain executable codes or which may decrease you	r netwo	rk efficiency.
Domain		Extension	Comment	-	
-57		.ade	Microsoft Access project extension	•	Delete
URL		.adp	Microsoft Access project		Delete
		.asf	this can also exploit a security hole allowing virus infec	:ti ≡	
Regex URL		.asx	Windows Media Audio / Video		
		.avi	Movie file		
Www.Phrases		.bas	Microsoft Visual Basic class module		
	~	.bat	Batch file		
A Extension		.bin	CD ISO image		
		.bz2	Unix compressed file		
🌌 Mime		.cab	Windows setup file		
		.cdr	Mac disk image		
Q Content		.chm	Compiled HTML Help file		
		.cmd	Microsoft Windows NT Command script		
		.com	Microsoft MS-DOS program		
		.cpl	Control Panel extension	_	
		crt	Security certificate		

### Add

Click on Add tab.

lacktrian Sector	🔞 Banned Filte	🕫 💿 Exception Filters 🏾 🎀 Configuration 🏾 💿	Log Monitoring
Default	Banned Extension Block file extensions	that can contain executable codes or which may decrease your n	etwork efficiency.
Domain	Extension	Comment	🐥 Add
	.ade	Microsoft Access project extension	A Delete
URL	.adp	Microsoft Access project	Delete
	.asf	this can also exploit a security hole allowing virus infecti.	🔳
Regex URL	.asx	Windows Media Audio / Video	_
	.avi	Movie file	
Mases Phrases	.bas	Microsoft Visual Basic class module	
	J.bat	Batch file	
A Extension	.bin	CD ISO image	
	.bz2	Unix compressed file	
🍪 Mime	.cab	Windows setup file	
	.cdr	Mac disk image	
Q Content	.chm	Compiled HTML Help file	
	.cmd	Microsoft Windows NT Command script	
	.com	Microsoft MS-DOS program	
	.cpl	Control Panel extension	
	Crt	Security certificate	

Add Extension tab, type extension and click **Ok**.

Add Ext	ension	×
⚠	Please enter an extension: .org	_
	OK Cancel	

Add Comment tab appears, type comment for the extension and click **Ok**.



🍇 Filter Groups	👒 Banned Fili	ers 💿 Exception Filters 🊏 Configuration	Log Monitoring
Default	Banned Extension	s that can contain executable codes or which may decrease yo	our network efficiency.
Domain	Extension	Comment	🗳 Add
, 🔂 URL	.tgz	Unix compressed file	Delete
-	.url	Internet shortcut	
Regex URL	✓ .vbe	VBScript Encoded script file	
	✓ .vbs	VBScript file	
Phrases	✓ .vb	VBScript file	
	.vxd	Windows system file	
A Extension	.wax	Windows Media AutoRedirector	
	.wmf	Movie file	
🔗 Mime	.wmv	Windows Media Video	
	.wsc	Windows Script Component	
Ountrat	.wsf	Windows Script file	
Content	.wsh	Windows Script Host Settings file	
	.xls	Excel document	
	zip	Windows compressed file	
	✓ .org	# nielsen	<b>T</b>
L			

In the below screen, we can notice extension added to list.

#### Delete

Select the extension and click on **Delete** tab.

🍓 Filter Groups	<b>G</b> 1	Janned Filter	🕫 💿 Exception Filters 🏾 🎀 Configuration 🗋 💿 I	Log Monitoring
Default 💌	Banne Block	ed Extension	hat can contain executable codes or which may decrease your ne	twork efficiency.
Domain		Extension	Comment	🔗 Add
🗗 URL		.tgz	Unix compressed file	Delete
		.url	Internet shortcut	
Regex URL	-	.vbe	VBScript Encoded script file	
	<ul> <li>Image: A start of the start of</li></ul>	.vbs	VBScript file	
🛛 🕠 Phrases	-	.vb	VBScript file	
		.vxd	Windows system file	
A Extension		.wax	Windows Media AutoRedirector	
		.wmf	Movie file	
🛞 Mime		.wmv	Windows Media Video	
		.WSC	Windows Script Component	
Content		.wsf	Windows Script file	
Content		.wsh	Windows Script Host Settings file	
		.xls	Excel document	
		.zip	Windows compressed file	
		.org	# nielsen	-

Delete Extension tab appears, click on Yes.



### In the below screen, we can notice extension deleted.

lage Filter Groups	3	Banned Filter	🕫 💿 Exception Filters 🛛 🎀 Configuration 🤇 🧟	Log Monitoring
Default	- Banne Block	ed Extension	hat can contain executable codes or which may decrease your	network efficiency.
Domain		Extension	Comment	🗳 Add
URL		.tar	Tape ARchive file	Delete
		.tgz	Unix compressed file	
Regex URL		.url	Internet shortcut	
	<ul> <li>Image: A start of the start of</li></ul>	.vbe	VBScript Encoded script file	
Phrases	<ul> <li>Image: A start of the start of</li></ul>	.vbs	VBScript file	
	<ul> <li>Image: A set of the</li></ul>	.vb	VBScript file	
Extension		.vxd	Windows system file	
		.wax	Windows Media AutoRedirector	
Mime		.wmf	Movie file	
		.wmv	Windows Media Video	
Contant		.WSC	Windows Script Component	
Content		.wsf	Windows Script file	
		.wsh	Windows Script Host Settings file	
		.xls	Excel document	
		.zip	Windows compressed file	•



#### Add

Click on Add tab.

& Filter Groups	Banned Filters     Generation Filters     Second State     Second Sta	Cog Monitoring
Default 💌	Banned Mime Types One may need to block HTTP requests with the following mime types.	
Domain	Mime Types in Banned List	🐥 Add
	application/astound	Add Multiple
	application/compress	
	application/fastman	드 Delete
Regex URL	application/gzip	
	application/java-archive	
Phrases	application/java-serialized-object	
	application/java-vm	
A Extension	application/mac-binhex40	
	application/mbedlet	
🌌 Mime	application/msword	
	application/octet-stream	
Sontent Content	application/oda	
	application/pdf	
	application/postscript	
	application/pre-encrypted	-
	annlication/studiom	

Add Mime tab appears, give Mime type and click Ok.

Add Min	ne	×
	Please enter a type:	
	lmage/snag	
	OK Cancel	

In the below screen, we can notice Mime type added in the list.

lacktrian Sector	Banned Filters @ Exception Filters 👫 Configuration	Q	Log Monitoring
Default 💌	Banned Mime Types One may need to block HTTP requests with the following mime types.		
Domain	Mime Types in Banned List		🗳 Add
URL URL	video/vnd.sealed.swf		👙 Add Multiple
Regex URL	video/vnd.vivo video/wavelet		📟 Delete
	video/x-flv		
Phrases	video/x-ra-asi		
A Extension	video/x-ms-asf	-	
Mime	video/x-ms-wx-plugin		
	video/x-sgi-movie x-conference/x-cooltalk	-	
Content	x-world/x-svr		
	x-world/x-vrml		
	image/snag	F	

# Add More

Click on Add Multiple tab.

🍇 Filter Groups	Banned Filters 🕜 Exception Filters 🎌 Configuration	0	Log Monitoring
Default 💌	Banned Mime Types One may need to block HTTP requests with the following mime types.		
Domain	Mime Types in Banned List		🗳 Add
D URL	video/vnd.sealed.swf		🖗 Add Multiple
🔀 Regex URL	video/wavelet		😅 Delete
Phrases	video/x-flv video/x-la-asf		
	video/x-mpeg2		
A Extension	video/x-ms-asi		
🎊 Mime	video/x-ms-wvx-plugin		
Content	x-conference/x-cooltalk		
	x-world/x-svr		
	x-world/x-vrt		
	image/snag	-	

When the below screen appears enter the Mime extensions of the applications which you want to ban and click on **Ok.** 

Add Mime			×
Please enter a type: application/pdf			
application/png			
	ОК	Cancel	Help

In the below screen, we can notice Mime types added in the list.

lefter Groups	🔞 Banned Filters 🕜 Exception Filters 🕅 👯 Configuration 🧐 Log Monitoring		
Default 💌	Banned Mime Types		
Delduit	One may need to block HTTP requests with the following mime types.		
Domain			
L OKL	Mime Types in Banned List		👙 Add
Degay LIDI	video/vnd.rn-realvideo		🝰 Add Multiple
Regex OKL	video/vnd.sealedmedia.softseal.mov		
Dhuran	video/vnd.sealed.mpeq1		📟 Delete
Phrases	video/vnd.sealed.mpeq4		
<b>Re</b> - 1 - 1	video/vnd.sealed.swf		
+ Extension	video/vnd.vivo		
<b>A</b>	video/wavelet		
Mime Mime	video/x-flv		
	video/x-la-asf		
Content	video/x-mpeg2		
	video/x-ms-asf		
	video/x-msvideo		
	video/x-ms-wvx-plugin		
	video/x-sgi-movie		
	x-conference/x-cooltalk		
	x-world/x-svr		
	x-world/x-vrml		
	x-world/x-vrt		
	Image/snag		
	application/pdf		
	application/png	-	

#### Delete

Select the Mime type and click on **Delete** tab.
lefter Groups	Banned Filters 💿 Exception Filters 🎇 Configuration	💿 Log Monitoring
Default	Banned Mime Types One may need to block HTTP requests with the following mime types.	
Domain	Mime Types in Banned List	Add
URL URL	video/vnd.sealed.swf	🖨 Add Multiple
Regex URL	video/wavelet	- Delete
Dhrasas	video/x-flv video/x-la-asf	
rillases	video/x-mpeg2	
A Extension	video/x-ms-asf video/x-msvideo	
🎊 Mime	video/x-ms-wvx-plugin	
	x-conference/x-cooltalk	
Content	x-world/x-svr	
	x-world/x-vrml x-world/x-vrt	
	image/snag	•

Delete Mine tab appears, Click on Yes.



😣 Filter Groups 🔯 Banned Filters 🚱 Exception Filters 🚏 Configuration 💿 Log Monitoring Banned Mime Type Default Ŧ One may need to block HTTP requests with the following mime types. Domain Mime Types in Banned List 🐥 Add video/vid.seared.mpeg 🗗 URL 🔮 Add Multiple video/vnd.sealed.mpeg4 video/vnd.sealed.swf 르 Delete Regex URL video/vnd vivo video/wavelet video/x-flv hrases 📐 video/x-la-asf video/x-mpeg2 A Extension video/x-ms-asf video/x-msvideo 🧞 Mime video/x-ms-wvx-plugin video/x-sgi-movie Q Content x-conference/x-cooltalk x-world/x-svr x-world/x-vrml x-world/x-vrt -

In the below screen, we can notice Mime type deleted.

# 82. Exception Filters

Section 2017 Secti	Banned Filters	Exception Filters	Configuration	Log Monitoring		
Default 🔻	Grey URL					
Domain	Domains in grey list. Don't The 'grey' lists override the is that the 'exception' lists	bother with the www. or the e 'banned' lists. The 'exceptior completely switch off *all* oth	http://. 'lists override the 'banned er filtering for the match. '	d' lists also. The difference 'grey' lists only stop the		
URL URL	An example of grey list us still filter as normal on their	URL filtering and allow the normal filtering to work. An example of grey list use is when in Blanket Block (whitelist) mode and you want to allow some sites but still filter as normal on their content.				
Phrases	Another example of grey list use is when you ban a site but want to allow part of it. The greyurllist is for partly unblocking PART of a site. The greysitelist is for partly unblocking ALL of a site.					
Grev Site		URL		🗳 Add		
				👙 Add Multiple		
Grey URL				🖴 Delete		

## 83. Domain

Click on Domain tab

Sector 2 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Banned Filters	Exception Filters	🚏 Configuration	🚱 Log Monitoring
Default 💌	Site Exception Sites in exception list. The You can also match IPs h	ese are specifically domains ar ere too. ist of Domain Names in Ex	nd are not URLs. For exam	nple; labristeknoloji.com . 😤 Add
	vindowsupdate.	microsoft.com		Add Multiple
Phrases				Delete
Grey Site				
Grey URL				

# Add

Click on Add tab.

& Filter Groups	🚱 Banned Filters	Exception Filters	<b>Configuration</b>	💿 Log Monitoring
Default 💌	Site Exception Sites in exception list. These You can also match IPs here	are specifically domains ar too.	nd are not URLs. For exam	ple; labristeknoloji.com .
	List windowsupdate.mic	of Domain Names in Ex crosoft.com	ception List	Add 👙 Add
Phrases				🛥 Delete
Grey Site				
Grey URL				

Add site tab appears type domain name and click Ok.



In the below screen, we can notice domain name added.

Silter Groups	🚱 Banned Filters 💽 Exception Filters 💱 Configuration 🦉	Log Monitoring
Default 💌	Site Exception — Sites in exception list. These are specifically domains and are not URLs. For example; You can also match IPs here too.	labristeknoloji.com .
URL Phrases	List of Domain Names in Exception List           image: windowsupdate.microsoft.com           image: Labris.com	🗳 Add
Grey URL		

# Add Multiple

Click on Add Multiple tab.

🍓 Filter Groups	Banned Filters	Exception Filters	🚏 Configuration	Cog Monitoring
Default 💌	Site Exception Sites in exception list. The You can also match IPs h	ese are specifically domains an ere too.	id are not URLs. For exam	ple; labristeknoloji.com .
	✓ windowsupdate. ✓ Labris.com	ist of Domain Names in Ex microsoft.com	ception List	🗳 Add
Phrases				르 Delete
Grey URL				

Add Bulk site tab appears, type domain name one in each line. Click **Ok**.

Add Bulk Site	×
r Please enter domain names as one in each line	_
Google.co.in Yahoo.co	
	_
OK Cancel Help	

In the below screen, we can notice Multiple domains added.

lefter Groups	🚱 Banned Filters 💽 Exception Filters 🎀 Configuration @	Log Monitoring
Default 💌	Site Exception Sites in exception list. These are specifically domains and are not URLs. For example; li You can also match IPs here too.	abristeknoloji.com .
	List of Domain Names in Exception List           Image: windowsupdate.microsoft.com           Image: Labris.com	Add Multiple
Phrases	<ul> <li>✓ Google.co.in</li> <li>✓ Yahoo.co</li> </ul>	😅 Delete
Grey Site		

# Delete

Select Domain and click on **Delete** tab.

& Filter Groups	🚱 Banned Filters 🦉	Exception Filters	<b>Configuration</b>	Log Monitoring	
Default         Site Exception           Sites in exception list. These are specifically domains and are not URLs. For example; labristeknoloji.com . You can also match IPs here too.					
	List	of Domain Names in Ex crosoft.com	ception List	🗳 Add	
Phrases	<ul><li>✓ Labris.com</li><li>✓ Google.co.in</li></ul>			- Delete	
Grey Site	Yahoo.co			-	
Grey URL					

# Delete Site tab appears, click on Yes.

Delete S	lite	×
2	Are you sure?	
	Yes No	

In the below screen, we can notice selected domain deleted.

Silter Groups	🚱 Banned Filters 💽 Exception Filters 💏 Configuration 💿	Log Monitoring			
Default 💌	Site Exception Sites in exception list. These are specifically domains and are not URLs. For example; labristeknoloji.com . You can also match IPs here too.				
	List of Domain Names in Exception List	🖨 Add			
	Windowsupdate.microsoft.com     Labris.com	Add Multiple			
Phrases	Vahoo.co	🖴 Delete			
Grey Site					
Grey URL					

# 84. URL

Click on URL tab

🍇 Filter Groups	🚱 Banned Filters 🔯	Exception Filters	💏 Configuration	💿 Log Monitoring
Default 💌	URL Exception URLs in exception list. These are domain with a path. For example	e parts of sites that filter ; labristeknoloji.com/sup	ing should be switched of port	f for. They should be a
	Li	st of URLs in Excepti	on List	🗳 Add
URL	generallybadsite.tld/pa	irtthatsok/		🗳 Add Multiple
<u>k</u> Phrases				🛥 Delete
Grey Site				
Grey URL				

# Add

Click on Add tab.

lefter Groups	🚱 Banned Filters 🔯 Exception Filters 💏 Configuration 🥝	Log Monitoring
Default 💌	URL Exception URLs in exception list. These are parts of sites that filtering should be switched off for domain with a path. For example; labristeknoloji.com/support	r. They should be a
	List of URLs in Exception List	谷 Add
URL	generallybadsite.tld/partthatsok/	👙 Add Multiple
Phrases		😑 Delete
Grey Site		
Grey URL		

Add URL tab appears, type URL and click Ok.



In the below screen, we can notice URL added.

🍇 Filter Groups	🔞 Banned Filters 💽 Exception Filters 💱 Configuration 🧟	Log Monitoring
Default 💌	URL Exception URLs in exception list. These are parts of sites that filtering should be switched off for domain with a path. For example; labristeknoloji.com/support	. They should be a
URL	List of URLs in Exception List generallybadsite.tld/partthatsok/ Labristeknoloji.com/support	Add 🗳 Add
Grey Site		

# Delete

Select URL and click on **Delete** tab.

Section 24 Section 24	🚱 Banned Filters	Exception Filters	🚏 Configuration	💿 Log Monitoring
Default 💌	URL Exception URLs in exception list. The domain with a path. For ex	ese are parts of sites that filter cample; labristeknoloji.com/sup	ing should be switched of port	f for. They should be a
URL	generallybadsite.	Add		
Grey Site				

Delete URL tab appears, click on Yes.



In the below we can notice URL deleted.

Sector Groups	Banned Filters     Exception Filters     P     Configuration     G	Log Monitoring
Default 💌	URL Exception URLs in exception list. These are parts of sites that filtering should be switched off for domain with a path. For example; labristeknoloji.com/support	. They should be a
URL	List of URLs in Exception List generallybadsite.tld/partthatsok/	Add 🖗 Add Multiple
Phrases		😑 Delete
Grey Site		

# 85. Phrases

# In the exceptions Filters, Select Phrases tab

Se Filter Groups	<b>G</b> E	Banned Filters	C Exception F	ilters 💡	Configuration	🕝 Log	Monitoring		
Default 💌	Excep If any	otion Phrase List	d below appear in a v	veb page the	en the page will be allo	wed.			
Domain		Phrase	Groups	Begin	nning End	ling	Any Point	Exact Match	🐥 Add
		User							Delete
URL	<ul> <li>Image: A start of the start of</li></ul>	goodphrases							Delete
<u> Phrases</u>									

# Add

# Click on $\boldsymbol{Add}$ to add the $\boldsymbol{Phrases}$ to the exception phrase list

Sector Groups	G B	anned Filters	Exception I	Filters	🎀 Configu	ration (	强 Log Monito	oring		
Default 💌	Excep If any	tion Phrase List	d below appear in a	web page	then the page v	vill be allowe	ed.			
Domain		Phrase	Groups	Be	ginning	Endin	g Any	Point	Exact Match	🗳 Add
5 URI	-	User								😑 Delete
L ONE	-	goodphrases								
<u>w</u> Phrases										

When the Add phrase screen appears , give the necessary inputs in the boxes



Options in Add phrase screen are

1	Beginning word	In the <b>beginning word</b> box , enter the benning word of the phrase
2	Ending word	In the Ending word box , enter the ending word of the phrase
3	Phrase for any	In the Phrase for any position box , enter a Phrase for any position
	position	
4	Phrase for exact	In the Phrase for exact match box , enter a Phrase whicg matches exactly
	match	

# You can notice that a phrase is added to the list

lacktrian Sector	<b>G</b> E	Banned Filters 💿 Excep	tion Fi	liers 🛛 🎀 Conf	iguration 🛛 💿 L	og Monitoring		
Default 💌	Excep If any	otion Phrase List r of the phrases listed below appe	ar in a w	eb page then the pa	ge will be allowed.			
Domain		Phrase Groups		Beginning	Ending	Any Point	Exact Match	🖨 Add
- Tun		User		Gmail	.com		google mail	🤤 Delete
URL	-	goodphrases						Delete
Phrases							1	

#### Delete

Select the phrase and click on **Delete** tab to delete the phrase from the list

lage Filter Groups	<b>(G</b> ) B	Banned Filters 💿 Exception	Filters 💡 Confi	iguration 🛛 💿 Lo	g Monitoring		
Default	Excep If any	otion Phrase List of the phrases listed below appear in a	a web page then the pa	ge will be allowed.			
Domain		Phrase Groups	Beginning	Ending	Any Point	Exact Match	🖨 Add
	<b>~</b>	User	Gmail	.com		google mail	C Delete
URL	✓	goodphrases					Delete
Nrases			-				

Below screen appears stating that Are you sure, click on Yes



# 86. Grey Site

Select Grey Site tab.

Section 2017 Secti	🚱 Banned Filters 💽	Exception Filters	<b>Configuration</b>	Log Monitoring					
Default 💌	Grey Site Domains in grey list. Don't bother with the www. or the http://. The 'grey' lists override the 'banned' lists. The 'exception' lists override the 'banned' lists also. The difference is that the 'exception' lists completely switch off *all* other filtering for the match. 'grey' lists only stop the								
URL	URL filtering and allow the normal filtering to work. An example of grey list use is when in Blanket Block (whitelist) mode and you want to allow some sites but still filter as normal on their content. Another example of grey list use is when you ban a site but want to allow part of it.								
Grey Site	Domain 🔮 Add								
Grey URL	www.bbc.co.uk			Add Multiple					

# Add

Click on Add tab.

lefter Groups	🚱 Banned Filters	Exception Filters	<b>Configuration</b>	🚱 Log Monitoring
Default	Grey Site Domains in grey list. Don't The 'grey' lists override the is that the 'exception' lists URL filtering and allow the An example of grey list us still filter as normal on their Another example of grey li The greyurllist is for partly	bother with the www. or the e 'banned' lists. The 'exception completely switch off *all* oth normal filtering to work. e is when in Blanket Block (w r content. ist use is when you ban a site unblocking PART of a site. Th	http://. ' lists override the 'banned er filtering for the match. hitelist) mode and you wa but want to allow part of e greysitelist is for partly	d' lists also. The difference 'grey' lists only stop the nt to allow some sites but it. unblocking ALL of a site.
Grey Site	www.bbc.co.uk	Domain		Add

Add Grey Site tab appears, type domain name and click **Ok.** 



In the below screen we can notice domain added.

Silter Groups	🚱 Banned Filters	💿 Exception Filters	Configuration	Log Monitoring			
Default  Default  Domain  URL  Phrases	Grey Site Domains in grey list. Don't The 'grey' lists override th is that the 'exception' lists URL filtering and allow the An example of grey list us still filter as normal on thei Another example of grey l The greyurllist is for partly	bother with the www. or the e 'banned' lists. The 'exception completely switch off *all* oth e normal filtering to work. e is when in Blanket Block (w r content. list use is when you ban a site r unblocking PART of a site. Th	http://. n' lists override the 'banned er filtering for the match. nhitelist) mode and you wa e but want to allow part of he greysitelist is for partly	d' lists also. The difference 'grey' lists only stop the nt to allow some sites but it. unblocking ALL of a site.			
Grey Site		Domain		🐴 Add			
	Add Mult						
Grey URL		•		Delete			

# Add Multiple

Click on Add Multiple tab.

lacktrian Sector	🚱 Banned Filters	💿 Exception Filters	<b>Configuration</b>	💿 Log Monitoring	
Default <ul> <li>Domain</li> <li>URL</li> <li>Phrases</li> </ul>	Grey Site Domains in grey list. Don't bother with the www. or the http://. The 'grey' lists override the 'banned' lists. The 'exception' lists override the 'banned' lists also is that the 'exception' lists completely switch off *all* other filtering for the match. 'grey' lists URL filtering and allow the normal filtering to work. An example of grey list use is when in Blanket Block (whitelist) mode and you want to allow still filter as normal on their content. Another example of grey list use is when you ban a site but want to allow part of it. The greyurllist is for partly unblocking PART of a site. The greysitelist is for partly unblocking				
Grev Site		Domain		🗳 Add	
<u>•</u>	www.bbc.co.uk			🖨 Add Multiple	
Grey URL	www.google.com			Delete	

Add Bulk Site tab appears, type domain name as one in each line and click **Ok**.

Add Bulk Site	×
Please enter domain names as one in each line	
www.gmail.com www.twitter.com	
OK Cancel Help	

In the below screen we can notice multiple domains added.

Sector 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Banned Filters     Exception Filters     Filters	Log Monitoring
Default	Grey Site Domains in grey list. Don't bother with the www. or the http://. The 'grey' lists override the 'banned' lists. The 'exception' lists override the 'banned' lists is that the 'exception' lists completely switch off *all* other filtering for the match. 'grey' URL filtering and allow the normal filtering to work. An example of grey list use is when in Blanket Block (whitelist) mode and you want to a still filter as normal on their content. Another example of grey list use is when you ban a site but want to allow part of it. The greyurllist is for partly unblocking PART of a site. The greysitelist is for partly unblock	also. The difference lists only stop the allow some sites but cking ALL of a site.
Grey Site	Domain	🐈 Add
	Www.bbc.co.uk	
Grey URL	www.gmai.com www.google.com	📟 Delete
	www.twitter.com	

# Delete

Select the domain and click on **delete** tab.

🍇 Filter Groups	🚱 Banned Filters	Exception Filters	🚏 Configuration	🚱 Log Monitoring
Default  Domain       URL       Phrases	Grey Site Domains in grey list. Don't The 'grey' lists override th is that the 'exception' lists URL filtering and allow the An example of grey list us still filter as normal on thei Another example of grey The greyurllist is for partly	bother with the www. or the e 'banned' lists. The 'exception completely switch off *all* oth e normal filtering to work. se is when in Blanket Block (w r content. list use is when you ban a site r unblocking PART of a site. Th	http://. ' lists override the 'banner er filtering for the match. hitelist) mode and you wa : but want to allow part of e greysitelist is for partly	d' lists also. The difference 'grey' lists only stop the Int to allow some sites but 'it. unblocking ALL of a site.
Grey Site	www.bbc.co.uk	Domain		Add

Delete Grey Site tab appears, Click on Yes.



In the below screen we can notice Domain deleted.

le Filter Groups	Banned Filters	Exception Filters	Configuration	Log Monitoring
Default  Default  Domain  URL  Phrases	Grey Site Domains in grey list. Don't The 'grey' lists override th is that the 'exception' lists URL filtering and allow the An example of grey list us still filter as normal on the Another example of grey The greyurllist is for parth	t bother with the www. or the ne 'banned' lists. The 'exceptior completely switch off *all* oth e normal filtering to work. se is when in Blanket Block (w ir content. list use is when you ban a site y unblocking PART of a site. Th	http://. ' lists override the 'banned er filtering for the match. hitelist) mode and you wa but want to allow part of e greysitelist is for partly i	d' lists also. The difference 'grey' lists only stop the nt to allow some sites but 'it. unblocking ALL of a site.
Grey Site	www.bbc.co.uk	Domain		Add

# 87. Grey URL

Select Grey URL tab.

Silter Groups	Banned Filters     Exception Filters     Provide Configuration	Log Monitoring
Default   Default  Domain  URL  Phrases	Grey URL Domains in grey list. Don't bother with the www. or the http://. The 'grey' lists override the 'banned' lists. The 'exception' lists override the 'banned' lists is that the 'exception' lists completely switch off *all* other filtering for the match. 'grey URL filtering and allow the normal filtering to work. An example of grey list use is when in Blanket Block (whitelist) mode and you want to still filter as normal on their content. Another example of grey list use is when you ban a site but want to allow part of it. The greyurllist is for partly unblocking PART of a site. The greysitelist is for partly unblocking	s also. The difference ' lists only stop the allow some sites but ocking ALL of a site.
Grey Site	URL VRL	🗳 Add
Grey URL		🛥 Delete

# Add

Click on Add tab.

& Filter Groups	Banned Filters	Exception Filters	<b>Representation</b>	Log Monitoring
Default  Default  Domain  URL  Phrases	Grey URL Domains in grey list. Don't The 'grey' lists override th is that the 'exception' lists URL filtering and allow the An example of grey list us still filter as normal on the Another example of grey The greyurllist is for party	bother with the www.or the le 'banned' lists. The 'exceptior completely switch off *all* oth e normal filtering to work. se is when in Blanket Block (w ir content. list use is when you ban a site y unblocking PART of a site. Th	http://. n' lists override the 'banned er filtering for the match. rhitelist) mode and you wa e but want to allow part of he greysitelist is for partly	d' lists also. The difference 'grey' lists only stop the nt to allow some sites but it. unblocking ALL of a site.
Grey Site	members.home	URL .net/nice		Add Add Multiple

Add Grey URL tab appears, type URL and click **Ok**.

Add Grey URL		×	
	Please enter an URL:		
labristecknoloji.com/support			
	OK Cancel		

In the below screen we can notice URL added.

🍇 Filter Groups	🚱 Banned Filters	Exception Filters	Configuration	🚱 Log Monitoring
Default	Grev URL		·	
	Domains in grey list. Don't	bother with the www.or the	http://.	
0 Domain	The 'grey' lists override th	e 'banned' lists. The 'exception	' lists override the 'banne	d' lists also. The difference
	is that the 'exception' lists URL filtering and allow the	completely switch off *all* oth e normal filtering to work.	er filtering for the match.	'grey' lists only stop the
🗇 URL	An example of grey list us	se is when in Blanket Block (w	hitelist) mode and you wa	nt to allow some sites but
	still filter as normal on the Another example of grey	ir content. list use is when you ban a site	but want to allow part of	it.
Phrases	The greyurllist is for partly	y unblocking PART of a site. Th	e greysitelist is for partly	unblocking ALL of a site.
		URI		Add 🗳
Grey Site	✓ labristeknloji.cpr	m/support		
				Add Multiple
Grey URL				📟 Delete
Domain URL Phrases Grey Site Grey URL	The 'grey' lists override th is that the 'exception' lists URL filtering and allow the An example of grey list us still filter as normal on the Another example of grey The greyurllist is for parth	ie 'banned' lists. The 'exception completely switch off *all* oth e normal filtering to work. se is when in Blanket Block (wi ir content. list use is when you ban a site y unblocking PART of a site. Th URL n/support	<ul> <li>Ists override the 'banned er filtering for the match.</li> <li>hitelist) mode and you wa</li> <li>but want to allow part of e greysitelist is for partly</li> </ul>	d' lists also. The dif 'grey' lists only stop nt to allow some si it. unblocking ALL of a Add M Add M

# Add More

Click on Add Multiple tab.

lefter Groups	🚱 Banned Filters 🦉	Exception Filters	Configuration	💿 Log Monitoring
Default 💌	Grey URL Domains in grey list. Don't bot The 'grey' lists override the 'b is that the 'exception' lists cor	ther with the www. or the anned' lists. The 'exception mpletely switch off *all* oth	http://. ' lists override the 'banned er filtering for the match.	d' lists also. The difference 'grey' lists only stop the
URL	URL filtering and allow the no An example of grey list use is still filter as normal on their co Another example of grey list The greyurllist is for partly un	rmal filtering to work. s when in Blanket Block (w ontent. use is when you ban a site blocking PART of a site. Th	hitelist) mode and you wa but want to allow part of e greysitelist is for partly	nt to allow some sites but it. unblocking ALL of a site.
Grey Site	Iabristeknloji.cpm/s	URL		🗳 Add
Grey URL				- Delete

In the below screen we can notice multiple URL added.

Silter Groups	🚱 Banned Filters 💽 Exception Filters 💱 Configuration @	Log Monitoring				
Default  Default  Domain  URL  Phrases	Grey URL Domains in grey list. Don't bother with the www. or the http://. The 'grey' lists override the 'banned' lists. The 'exception' lists override the 'banned' lists also. The difference is that the 'exception' lists completely switch off *all* other filtering for the match. 'grey' lists only stop the URL filtering and allow the normal filtering to work. An example of grey list use is when in Blanket Block (whitelist) mode and you want to allow some sites but still filter as normal on their content. Another example of grey list use is when you ban a site but want to allow part of it. The greyurllist is for partly unblocking PART of a site. The greysitelist is for partly unblocking ALL of a site.					
Grey Site	URL           URL	🗳 Add				
Grey URL	✓ labristeknoloji.com/test	- Delete				

Add Bulk URL tab appears, type domain name one in each line and click Ok.

Add Bulk URL	×
Please enter domain names as one in each line laristeknoloji.com/support labristeknoloji.com/test	~
OK Cancel Help	

# Delete

Select the URL and click on **Delete** tab.

& Filter Groups	Banned Filters	Exception Filters	<b>P</b> Configuration	💿 Log Monitoring
Default	Grey URL			
Domain	Domains in grey list. Don't The 'grey' lists override th is that the 'exception' lists	bother with the www. or the e 'banned' lists. The 'exception completely switch off *all* oth	http://. '' lists override the 'banne er filtering for the match.	d' lists also. The difference 'grey' lists only stop the
	URL filtering and allow the An example of grey list us still filter as normal on the	e normal filtering to work. se is when in Blanket Block (w ir content.	hitelist) mode and you wa	nt to allow some sites but
Phrases	Another example of grey The greyurllist is for partly	list use is when you ban a site y unblocking PART of a site. Th	e but want to allow part of ne greysitelist is for partly	it. unblocking ALL of a site.
Grev Site		URL		🗳 Add
<u></u>	members.home.	net/nice		Add Multiple
Grey URL				💴 Delete

Delete Grey URL tab appears, Click on Yes.



In the below screen we can notice Grey URL deleted.

le Filter Groups	Banned Filters	Exception Filters	Configuration	Log Monitoring
Default 💌	Grey URL Domains in grey list. Don't The 'grey' lists override the is that the 'exception' lists	bother with the www. or the e 'banned' lists. The 'exception completely switch off *all* oth	http://. n' lists override the 'banned	d' lists also. The difference 'grey' lists only stop the
URL	URL filtering and allow the An example of grey list us still filter as normal on their Another example of grey li The greyurllist is for partly	normal filtering to work. e is when in Blanket Block (w content. ist use is when you ban a site unblocking PART of a site. Th	hitelist) mode and you wa but want to allow part of re greysitelist is for partly	nt to allow some sites but it. unblocking ALL of a site.
Grey Site		URL		Add
Grey URL				Add Multiple

# 88. Settings

# **Reporting Options**

Choose use HTML template file radio button for Web Access Denied Reporting.

🍇 Filter Groups 🔞 Banned Filter	rs 💿 Exception Filters	🎌 Configuration	💿 Log Monitoring		
Reporting Options		1	<i>.</i>		
Web Access Denied Reporting					
🔘 log, but do not block - Stealth mode					
🔘 just say 'Access Denied'					
report why but not what denied phrase	se				
report fully					
<ul> <li>use HTML template file (accessdeni</li> </ul>	ied addressignored) - recomm	nended			
				Customize	
					1
Authentication					1
✓ NILM Authentication Configure					
Basic Authentication					
✓ IP Authentication					
- Loaging Options					
Log Level					
none					
🔘 just denied					
<ul> <li>all text based</li> </ul>					
<ul> <li>all requests</li> </ul>					
Log Exception Hits : Log if an exception (i	user, ip, URL, phrase) is matc	hed and so the page g	ets let through. Can be	useful for diagnosing why a site	-
				Save 🛃 Canc	cel
JRL/Content Filter Service Status: Running					9
ted to is: 78 188 50 48				Labris Teknolo	iii

In Reporting options click on **Customize** tab.

Reporting Options Web Access Denied Reporting	
Iog, but do not block - Stealth mode	
◯ just say 'Access Denied'	
report why but not what denied phrase	
report fully	
use HTML template file (accessdenied addressignored) - recommended	
·	Customize

Customize tab appears displaying HTML coding. Here we can modify the code if required

8	Customize	- 🗆 🗙
	<b>Sayfa adresi:</b> -URL-	
	<h3>Bağlantı detaylarınız:</h3> Subheader H3	
	<ul> <li><ul> <li>class="navigation"&gt;<!-- Start Navigation UL--></li> </ul> </li></ul>	
	<li><a href="#">» <b>Neden:</b> -REASONGIVEN-</a></li>	
	<li><a href="#">» <b>Kategori:</b> -CATEGORIES-</a></li>	
	<li><a href="#">» <b>Kullanıcı adınız:</b> -USER-</a></li>	
	<li><a href="#">» <b>IP:</b> -IP-</a></li>	
	>>	
	End Right Column D/V	
	 br class="clear" />	
	<div id="footer"><!-- Start Footer DIV--></div>	
	<div id="copyright">© 2013 Labris Networks. Tüm hakları saklıdır.</div> Copyright Notice	
	End Footer DIV	
	End Main DIV	
	End Wrapper DIV	
	😗 Help 🔄 Import	Save

# **Authentication**

Three types of Authentication are available.

They are NTLM Authentication, Basic Authentication, IP Authentication.

We can enable or disable above mentioned three Authentication types.



#### **Join Active Directory Domain**

Enable NTLM Authentication and click on Join AD Domain button.



# NTLM Authentication tab appears.

NTLM A	uthentication 🗙
	Domain LABTEST.LOCAL
Of the second	DC Hostname w2k12.labtest.local 2
	Domain Controller 192.168.20.254
	Password Server 192.168.20.254 4
	Try to find the workgroup automatically. Workgroup LABTEST 5
	OK Cancel Help

These are the inputs for NTLM Authentication.

1	Domain	Type domain name
2	DC Hostname	Type DC Hostname
3	Domain Controller	Give the Domain Controller IP
4	Password Server	Give the Server Password
5	Workgroup	Type Workgroup or enable Try to find work group automatically

# Click Ok.

NTLM A	uthentication		×
	Domain	LABTEST.LOCAL	
C.	DC Hostname	w2k12.labtest.local	
	Domain Controller	192.168.20.254	
	Password Server	192.168.20.254	
	Try to find the w	vorkgroup automatically.	
	Workgroup	LABTEST	
			_
	OK	Cancel Help	2

Join Domain tab appears.



### These are the inputs to join domain.

1	Username	Type Username to join Domain
2	Password	Type Password

#### Leave Active Directory Domain

#### Click Leave AD Domain button.



# **89. HTTPS Filtering**

#### **Introduction and Preliminary Information**

# What is SSL/TLS and HTTPS?

"SSL" means "Secure Sockets Layer". This was coined by the inventors of the first versions of the protocol, Netscape

"TLS" means "Transport Layer Security". The name was changed to avoid any legal issues with Netscape so that the protocol could be "open and free" (and published as a RFC). It also hints at the idea that the protocol works over any bidirectional stream of bytes, not just Internet-based sockets.

TLS is the new name for SSL. Namely, SSL protocol got to version 3.0; TLS 1.0 is "SSL 3.1". TLS versions currently defined include TLS 1.1 and 1.2. So it's generally called SSL/TLS.

HTTPS is a protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.

Note: Explanation and definitions are borrowed from StackExchange and Wikipedia.

# Certificate Authorities (CA), Chain of Trust and Certificate Chain

A certificate authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made by the private key that corresponds to the certified public key. In this model of trust relationships, a CA is a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate.

Digital certificates are verified using a chain of trust. The trust anchor for the digital certificate is the root certificate authority.

A certificate chain is a list of certificates (usually starting with an end-entity certificate) followed by one or more CA certificates (usually the last one being a self-signed certificate), with the following properties:

1 - The Issuer of each certificate (except the last one) matches the Subject of the next certificate in the list.

2 - Each certificate (except the last one) is supposed to be signed by the secret key corresponding to the next certificate in the chain (i.e. the signature of one certificate can be verified using the public key contained in the following certificate).

3 - The last certificate in the list is a trust anchor: a certificate that you trust because it was delivered to you by some trustworthy procedure.

Note: Explanations and definitions are borrowed from relevant Wikipedia pages.

# **Creation of Labris UTM CA**

Since HTTPS connection and chain of trust is unbreakable by definition, explicit permission needs to be granted by clients in order to inspect the content of HTTPS connections. This happens in the form of Root CA import in client machines.

Importing the Root CA of Labris UTM means that client trusts the UTM and promises to trust certificates issued by Labris UTM. When a client tries to establish a new HTTPS connection with a web server, Labris UTM intercepts the connection and redirects it to labris-webcache daemon. Labris-webcache analyses the connection request, extracts the destination domain and decides if this connection should be inspected or not. If the connection requires inspection, labris-webcache establishes a new HTTPS connection with the webserver, verifies its certificate chain and issues a new certificate for domain signed by Labris UTM CA. This whole process allows labris-webcache to maintain two HTTPS connections, first one between client and UTM, second one between UTM and webserver. This allows decryption and re-encryption of HTTPS connection on-the-fly and inspection of its content. This is also called Man-in-the-Middle (MitM) and makes labris-webcache man in the middle. Doing this on a public network (like ISP provided) and without explicit permission from clients may be illegal.

# Configuration

This tab allows tuning the configuration options of HTTPS Filtering.

🗽 Labris Management Cons	sole
Device Eile Edit View About	Help
	😫 Filter Groups 🔞 Banned Filters 🔞 Exception Filters 🙀 Configuration 💿 HTTH'S Filtering 💿 Log Monitoring
Device List Device List User Management Verw Network Settings Firewall Solver Antispam/Antivnus Doc/IPS Server Load Balancer CLicense	Elter Groups Characteristics Content Scanning) Perform Deep Inspection (Content Scanning) Deep Inspection Will not be performed for these websites Deep Inspection Will not be performed for these websites Deep Inspection Stating Despiration Stating Despiration Stating Despiration Stating Despiration Stating Despiration Will not be performed for these websites Despiration Stating Despiration Stating Despiration Stating Despiration Stating Despiration Stating Despiration Stating Despiration Stating Despiration Stating Domain Names to Bypass Deep Inspection Some websites and applications use Websocket technology to implement instant communication between client and server. Since these connections interfere with Deep Inspection. Labris UTH care recognize therm and add their domain names to exception domain names automatically: <ul> <li>On</li> <li>Off</li> </ul> Instant Requiring Deep Inspection Exception Domain Names Requiring Deep Inspection Exception Domain Names Requiring Deep Inspection Exception Instant Char State Area: Domain Names Requiring Deep Inspection Exception Instant Char State Area: Domain Names Requiring Deep Inspection Exception Instant Char State Following Instant Area: Domain Names Requiring Deep Inspection Exception Instant Char State Area: Domain Names Requiring Deep Inspection Exception Instant Char State Following Instant Area: Perform Char State Area: Domain Names Requiring Deep Inspection Exception Instant Char State Following Instant Area: Performed State Area: Following Instant Area: Perform: Solid State Solid Insecure Clipher Suites (Default
	Save Save
	URL/Content Filter Service Status: Running
Line server address you are	Labis Textiologi

# **HTTPS Filtering Settings**

# Deep Inspection (Default)

Perform man-in-the-middle inspection for HTTPS connection. Requires Labris UTM Root CA import in client machines.

#### **Domain-only Inspection**

Try to extract destination domains and apply domain-based rules if it's possible. This option doesn't require certificate import. On the other hand, labris-webcache can't perform deep analysis of packets and in some situations where domain name is not present during HTTPS connection, domain-based rules may not work.

# **HTTPS Filtering Exceptions**

#### **Domain Names to Bypass Deep Inspection**

Some applications and domains used by them can't be inspected for various reasons including but not limited to:

- Key pinning
- Deviation from SSL/TLS protocol
- Proprietary algorithms or cipher suites
- Using TCP port 443 for Non-HTTPS protocols.

Some of the problems above may be solved by adding relevant domains to exception. If adding an exception doesn't solve the problem, not redirecting connections to labris-webcache for known destination IP addresses should solve the problem.

Certain domains (or all subdomains of a domain) can be added to this list if it causes problem or it's not appropriate to decrypt and inspect its content on-the-fly.



# Bypass Websocket Domain Names Automatically

Some websites and applications use Websocket connection over HTTPS connections. Websocket connections start with HTTP handshake and uses 101 Upgrade response to upgrade the connection to Websocket protocol. Since they are not actually HTTP over TLS they cannot be effectively inspected and passed. So domains using Websocket needs exception to not break them. Labris UTM may inspection HTTP headers and recognize Websocket headers on-the-fly. This allows auto-adding Websocket domains to exception list. User may manage and examine these domains later in the "Domain Names to Bypass Deep Inspection" list.

Warning: Allowing Websocket domains may allow bypassing filter rules. Make it 'off' if you think your clients may act maliciously.

# **Domain Names Requiring Deep Inspection Exception**

Labris provides a list of known domains which require exception in order to make related applications to work. You can examine the list and add them directly to "Domain Names to Bypass Deep Inspection" list.



### **Insecure Cipher Suites**

Some algorithms are considered insecure and cipher suites using them are disabled by default. Allowing them solve connection problems with web servers using these cipher suites.

Insecure algorithms: DSS, 3DES, RC4, MD5, IDEA

Cipher suites using them: TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA TLS DHE DSS WITH AES 128 CBC SHA256 TLS DHE DSS WITH AES 128 GCM SHA256 TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA TLS DHE DSS WITH AES 256 CBC SHA256 TLS\_DHE\_DSS\_WITH\_AES\_256\_GCM\_SHA384 TLS DHE DSS WITH CAMELLIA 128 CBC SHA TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA TLS\_DHE\_DSS\_WITH\_SEED\_CBC\_SHA TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA TLS\_ECDH\_ECDSA\_WITH\_RC4\_128\_SHA TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA TLS ECDHE ECDSA WITH RC4 128 SHA TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA TLS ECDH RSA WITH 3DES EDE CBC SHA TLS ECDH RSA WITH RC4 128 SHA TLS RSA WITH 3DES EDE CBC SHA TLS\_RSA\_WITH\_IDEA\_CBC\_SHA TLS\_RSA\_WITH\_RC4\_128\_MD5 TLS\_RSA\_WITH\_RC4\_128\_SHA TLS\_RSA\_WITH\_SEED\_CBC\_SHA

#### **Insecure Protocols**

SSL version 2 and version 3 are considered insecure and disabled by default. Allowing them may solve connection problems with web servers which doesn't support TLS.

#### **Certificate Import (Desktop)**

#### Windows

#### System-wide Import (Internet Explorer, Chrome)

Importing certificate to system certificate store of windows allows Internet Explorer, Chrome and other applications trusting system store to work without certificate warning.

If root certificate is not imported to the system, browser shows a warning about certificate security.



Internet Explorer shows certificate warning before import



Click Yes.

9	User Account Control	×
•	Do you want to allow the following program to make changes to this computer?	
	Program name: Windows host process (Rundll32) Verified publisher: Microsoft Windows	
<mark>ی د</mark>	Show details Yes No	
	Change when these notifications appe	<u>ear</u>

Choose "Place all certificates in the following store" and click Browse.

Sertificate Import Wizard
Certificate Store Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
<ul> <li>Automatically select the certificate store based on the type of certificate</li> <li>Place all certificates in the following store</li> </ul>
Certificate store: Browse
Next Cancel

Choose Trusted Root Certification Authorities as store.



Click Next.

	×
📀 👙 Certificate Import Wizard	
Certificate Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for the certificate.	
$\bigcirc$ Automatically select the certificate store based on the type of certificate	
Place all certificates in the following store	
Certificate store:	
Trusted Root Certification Authorities Browse	
Next Car	ncel



Internet Explorer shows no warning after certificate import.

	Vebsite Identification				
1	Labris HTTPS Inspection Module, Certificate ID:679522415706				
	has identified this site as:				
	This connection to the server is encrypted.				
	Should I trust this site?				
	View certificates				
		· ·			
			Google'da Ara	Kendimi Şanslı Hissediyorum	

#### Firefox

Firefox doesn't use system store instead uses its own certificate store. Shows a warning before certificate import.



On the right click options.



In Advanced menu, choose Certificates tab and click View Certificates.

🚯 Untrusted Connection	×
Firefox about:prefe	rences#advanced C Q Search 🔂 🖨 🛡 🖡 🗭 🚍
<ul> <li>General</li> <li>General</li> <li>Search</li> <li>Content</li> </ul>	Advanced General Data Choices Network Update Certificates
<ul> <li>Applications</li> <li>Privacy</li> <li>Security</li> <li>Sync</li> </ul>	Requests         When a server requests my personal certificate:         Select one automatically         Ask me every time
<b>&amp;</b> Advanced	Query OCSP responder servers to confirm the current validity of certificates

On Authorities tab, click Import.





Choose Root UTM CA.

Click "Trust this CA to identify websites.



You can see Labris UTM CA is present in Certificate Store.

🔔 Untrusted	Certificate Manager			-		×
♦ € Firefox	Your Certificates People Servers Authorities Others	☆ 🖻	Ŧ	â	9	=
	You have certificates on file that identify these certificate authorities:					^
Gonoral	Certificate Name Security Device 🛱					
, M, General	SecureSign RootCA11 Builtin Object Token					
Q Search	▲Japanese Government					
	ApplicationCA - Japanese Government Builtin Object Token	tes				
Content	ALabris UTM CA, Certificate ID:679522415706					
A Applicat	Labris HTTPS Inspection Module, Certific Software Security Device					
Applicat	Microsec e-Sziano Root CA Builtin Object Token					
🗢 Privacy	Microsec e-Szigno Root CA 2009 Builtin Object Token					
	ANetLock Halozathiztonsani Kft					
Security 📾	View Edit Trust Import Export Delete or Distrust					
C) Sync						
• • • • • •	ок	cates				
🔬 Advance		Juico				
	View Cartificator	-				
	view <u>Certificates</u> Security <u>D</u> evices					

Firefox shows no warning after certificate import.



## **OS X**

## System-wide Import (Safari, Chrome)

Importing to system allows Safari and Chrome certificate problems.

## Open Keychain Access.

On the left sidebar ensure System keychain and Certificates are selected.

Click File -> Import Items

s File	Edit	View	Window	Help	
Net Net	w Passv w Secu w Keycl	vord Ite re Note nain	em Item	第N 合第N て第N	
Ne	w Certif	icate P	reference.		Cortif
Contractions of the second sec	<mark>port Iter</mark> port Iter	ns ns		<mark> </mark>	07 h 43 i
Ado me Del	<b>d Keych</b> lete Key	i <b>ain</b> 'chain '		<b>☆೫A</b> ∖⊂೫⊗	Kind
Clo	se			жw	certifica
Go Get	There t Info			۴I	certifica certifica
Uni Loc	lock Key ck All Ke	ychain eychain	"System" s	ЖL	certifica
Ма	ke Keyo	hain "S	System" D	efault	
	File Ne Ne Ne Exp Add Cloc Cloc Cloc Cloc Cloc Cloc Cloc Cloc	File Edit New Passw New Secur New Keych New Certif Import Iter Export Iter Add Keych Delete Key Close Go There Get Info Unlock Key Lock All Ke	File Edit View New Password Ite New Secure Note New Keychain New Certificate P Import Items Export Items Add Keychain Delete Keychain ' Close Go There Get Info Unlock Keychain Lock All Keychain Make Keychain ''S	<ul> <li>File Edit View Window</li> <li>New Password Item</li> <li>New Secure Note Item</li> <li>New Keychain</li> <li>New Certificate Preference.</li> <li>Import Items</li> <li>Export Items</li> <li>Add Keychain</li> <li>Delete Keychain "System"</li> <li>Close</li> <li>Go There</li> <li>Get Info</li> <li>Unlock Keychain "System"</li> <li>Lock All Keychains</li> <li>Make Keychain "System" Delete</li> </ul>	File       Edit       View       Window       Help         New       Password Item       第N         New       Secure Note Item       ①第N         New       Keychain       ①第N         New       Certificate Preference       ①第I         Import Items       ①第I         Export Items       ①第E         Add       Keychain         Delete       Keychain "System"         Go       There         Get       Info         Unlock       Keychains         Make       Keychains

Choose UTM Root CA certificate file click Open.

	a ca	٥	C	Search
Name	Date Modified	~	Size K	ind
sslfilter2-717662503678.crt	22 Dec 2015 14	1:59	2 KB c	ertificate
sslfilter	08 Dec 2015 14	4:55	2 KB P	lain Text
e				
•				
Options			Cancel	Open

Double click on the imported certificate. This will open certificate details.



#### Labris HTTPS Inspection Module, Certificate ID:717662503678

Root certificate authority

Expires: Saturday 13 December 2025 at 07 h 43 min 51 s Eastern European Standard Time This certificate has custom trust settings

Name	^	Kind	Expires	Keychain
20	Apple Worldwide Deveions Certification Authority	certificate	14 Feb 2016 20:56:35	System
27	com.apple.kerberos.kdc	certificate	02 Feb 2035 21:46:08	System
<b>1</b>	com.apple.systemdefault	certificate	02 Feb 2035 21:46:07	System
- 63	Labris HTTPS Inspectirtificate ID:717662503678	certificate	13 Dec 2025 07:43:51	System
20	VeriSign Class 3 Secure Server CA - G3	certificate	08 Feb 2020 01:59:59	System

# Expand the section Trust.

•••	Labris HTTPS Inspection Module, Certificate ID:717662503678
Certificate Ref E	abris HTTPS Inspection Module, Certificate ID:717662503678 oot certificate authority xpires: Saturday 13 December 2025 at 07 h 43 min 51 s Eastern European Standard Time This certificate has custom trust settings
▶ Trust	
Details	
Subject	Name
C	puntry TR
State/Pr	ovince ANK
Lo	ocality Ankara
Organi	zation Labris UTM CA, Certificate ID:717662503678
Organization	al Unit Labris HTTPS Inspection Module Unit, Certificate ID:717662503678
Common	Name Labris HTTPS Inspection Module, Certificate ID:717662503678
Email Ad	idress -
Issuer	Name
C	puntry TR
#### Choose Always Trust for Secure Sockets Layer.



#### Linux

#### Firefox

Steps are the same as Firefox on Windows.

#### Chromium

Click Settings on right and click Show advanced settings.

# Administration Guide for Labris UTM Version 3.4.2



Chromium Settings Sign in to Chromium History Extensions On startup Settings Open the New Tab page Continue where you left off About Open a specific page or set of pages. Set pages Appearance Get themes Use GTK+ theme Use Classic theme Show Home button Always show the bookmarks bar Use system title bar and borders Search Set which search engine is used when searching from the omnibox. Google 

Manage search engines... People Person 1 (current) 🕢 Enable Guest browsing Let anyone add a person to Chrome Add person... Edit... Remove... Import bookmarks and settings... Default browser Make Chromium the default browser Chromium is not currently your default browser. Show advanced settings...

Click Manage certificates.

Chromium	Settings
History	Languages
Extensions	Change how Chromium handles and displays languages. Learn more
Settings	Language and input settings
	Offer to translate pages that aren't in a language you read. Manage language
lbout	Downloads
	Download location: /home/labris/Downloads Change
	Ask where to save each file before downloading
	Manage certificates  Google Cloud Print Set up or manage printers in Google Cloud Print. Learn more Manage  Show notifications when new printers are detected on the network  Accessibility Add additional accessibility features
	System
	<ul> <li>Continue running background apps when Chromium is closed</li> <li>Use hardware acceleration when available</li> </ul>
	Reset settings Restore settings to their original defaults. Reset settings





#### **Labris Networks**

Click "Trust this certificate to identify websites".





Chromium shows no warning and certificate is signed by Labris UTM CA.



#### **Certificate Import (Mobile)**

#### iOS

Certificate can be transported to device via e-mail. Importing is simple. Use the steps below.





#### **Android**

#### System-wide Import

Certificate should be imported to Android Trusted Credentials. Sending the certificate via mail is the recommended way. Other possible options would be placing the certificate on a HTTP server or on a FTP server.



#### Give a name to certificate



#### Set-up screen lock

If device doesn't have a screen lock set up already, Android may require this prior to certificate import. Different vendors and different Android versions have implemented different policies about this issue. Some of them may enforce PIN lock while some others seems to accept also Pattern screen lock.

-	Ø	13:05	<b>•</b>	🛇 🎽 🎯 13:05			©	13:06
÷	C 1	🖼 :	Unlock selection		Choose yo	ur PIN		
ojects/weamoney/wik g_root_certificate_in_G	izinstanın Google_Chromi	e	None Disabled by administrator, encry credential storage	otion policy, or	Touc	h Continue w	/hen done	
Kolay gelsin. – Tarik Demirci			Swipe Disabled by administrator, encry credential storage					_
Attention			Pattern					
You need to set a l password before y credential storage.	lock screen F rou can use	PIN or	PIN					
	CANCEL	ок	Password					
					CANCE	L	CONTINUE	
ssifilter2-71750	3678.crt 👱					1	2	3
Reply Rep	ly all	Forward				4	5	6
						7	8	9
						×	0	-/ )





#### Network Monitoring Warning

After importing the certificate, Android System shows a warning with the title of 'Network Monitoring' even if cellular connection is used instead of Wi-Fi. Some vendors and some Android versions allow dismissing this warning while others don't. If system doesn't allow dismissing, there is no way to disable this warning.



#### **Checking trusted CAs**

Imported certificate can be examined under the Trusted Credentials menu.



Off

#### Testing certificate import

#### **Dolphin Browser**

Dolphin respects CAs trusted by system. HTTPS Filtering works with no issues after certificate is imported. Inspection of connection details shows that Labris UTM analyses the connection.





#### Chrome

Chrome respects CAs trusted by system. HTTPS Filtering works with no issues after certificate is imported. Inspection of connection details shows that Labris UTM analyses the connection.



#### **Opera**

No issues after importing certificate.



#### Clearing Trusted Credentials and Disabling Screen Lock

Android doesn't allow disabling screen lock when a third-party CA is imported. To clear the credentials store and disable screen lock, follow the steps below.

Warning: Clearing credentials will prevent establishing HTTPS connections. Do this only if the device will not be subject to HTTPS filtering anymore.



1

#### Firefox (Not Supported)

Firefox for Android doesn't use System CA Store for validation and doesn't provide a way to import third-party CAs. So it can't be used with HTTPS filtering.



#### Windows Phone

Windows phone doesn't recognize PEM encoded "\*.crt" certificates. Certificate needs to be converted to DER format and its extension must be ".cer". This can be accomplished in a Linux system with the following command:

openssl x509 -in sslfilter2.crt -outform der -out sslfilter2.cer



#### **Certificate Distribution via Active Directory**

You can use the steps below to distribute Labris UTM Root CA via Active Directory.

<u>.</u>		Group Policy Manager	nent		_ 0 X
Eile Action View Window Help					_ 8 ×
Group Policy Management	Group Policy Objects in labris.local				
A Morett: Jernsucci A Morett: Jernsucci A Morett: Jernsucci A Morett: Jernsucci A Morest Becking Security Groups A Morest Becking Security Groups A Morest Becking Security Groups A More that A More that A More that A More A More thatA More that A Mo	Corterio Debgaton	GPO Status Establid Establid Enablied	WMI Fiter None None	Монблед 7/7/2015 93-602 АМ 12/31/2015 93-446 АМ 12/31/2015 9-4003 АМ	Ower Dowin Admin (JABRIS2012,Dom Dowin Admine (JABRIS2012,Dom Dowan Admine (JABRIS2012,Dom
		Group Policy Manager	nent		3 Group Policy Object(s)
In the second s		Group Policy Manager	nent		3 Group Policy Object(3), a course
Ele Action View Window Help      Decomposition     Source Policy Management     A Forest labris.local     Source Policy Management     A Source Policy	Group Policy Objects in labris.local	Group Policy Manager	nent		3 Group Policy Object(s)
	Group Policy Objects in labris.local Corterts Delegation Name @ Default Domain Controlers Policy	Group Policy Manager GPO Setus Enabled	went WMI Fiter None	Modified 7/72015 935 02 AM	Group Policy Object(s)     Counter     Downer     Downer     Downer
File Action View Window Help	Corcup Policy Objects in labris.loca Contexts Designon Mane Default Doma Controlers Policy Default Doma Po	Group Policy Manager	while Reversion of the second se	Modified 7/7/2015 935 02 AM 1/2/10/10/3/2/4/2/M 1/2/31/2015 940 03 AM	Group Pelicy Object(s)     Course     Orner     Doman Adming (LABRIS2012:Dom     Doman Adming (LABRIS2012:Dom     Doman Adming (LABRIS2012:Dom



Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
<u>C</u> urrent User <u>L</u> ocal Machine
To continue, click Next.
Next

Lertificate Import Wiza	ra	
• to Import Specify the file you want to im	port.	
Eile name: C:\Users\Administrator.LABR Note: More than one certificat Personal Information Excha Cryptographic Message Sw	ISNETWORKS\Desktop\sslfilter2.crt te can be stored in a single file in the ange-PKCS #12 (.PFX,.P12)	Browse following formate
Microsoft Serialized Certific	ate Store (.SST)	(,P76)
		Next

Certificate	tore		
Certific	ate stores are system areas where ce	ertificates are kept.	
Windo the cer	us can automatically select a certificat tificate.	te store, or you can spec	ify a location fo
0	utomatically select the certificate sto	ore based on the type of	certificate
۲	lace all certificates in the following st	ore	
	Certificate store:		
	Trusted Root Certification Authoritie	'S	Browse

) 📀 🌛 Certificate Import Wiz	zard
Completing the Ce The certificate will be imported	e <b>rtificate Import Wizard</b> d after you click Finish.
You have specified the follow Certificate Store Selected b Content File Name	ing settings: y User Trusted Root Certification Authorities Certificate C:\Users\Administrator.LABRISNETWORKS\Desktop\;
<	III >
	<u>Finish</u> Cancel
Certificate Import Wizard	ı.
ОК	



#### **Customizing Root CA Details**

You can use the below command to regenerate the certificate with custom details: openssl req -new -key /opt/labris/etc/labris-webcache/certs/sslfilter2.key -x509 -days 3650 -out /opt/labris/etc/labris-webcache/certs/sslfilter2.crt

Openssl will ask for details. Fields and default values of Labris UTM CA are shown below:

Country Name (2 letter code) [GB]: **TR** State or Province Name (full name) [Berkshire]: **ANK** Locality Name (eg, city) [Newbury]: **Ankara** Organization Name (eg, company) [My Company Ltd]: Labris UTM CA, Certificate ID: <ID> Organizational Unit Name (eg, section) []: Labris HTTPS Inspection Module Unit, Certificate ID: <ID> Common Name (eg, your name or your server's hostname) []: Labris HTTPS Inspection Module, Certificate ID:<ID> Email Address []: -

#### **Firewall Configuration**

Connections to TCP Port 443 must be intercepted in order to make HTTPS Filtering work.



# **NTLM Authentication AD Configuration**

## **90.General View**

Active Directory users can be used in areas such as Firewall, Webfilter, VPN, Wauth by integrating Labris products with Active Directory. Authorization can be made with the user name or rules can be written.

Logon script must be set for all users with Group Policy on Active Directory for using simple authentication system. Logon script shares user information periodically with Labris. With this method, the correct settings can be made by making the necessary settings on structures which have more than one location and using the same active directory.

#### 91. Prerequisite

Active Directory Structure must be set and all computers must be included in Active Directory. Active Directory integration must be made with Labris.

#### 92. Scenario

Logon script settings will be made by using Group Policy on active directory integrated with Labris. How to make settings on structures which have more than one location and using the same active directory will be explained

This expression was performed on Windows Server 2012.

Although general method is same for Windows Server 2003/2008, the location of the menu on server can be different.

#### **93.**Configuration

Step 1: The attached files are downloaded and are copied to netlogon directory of Active Directory server.

**a. Run** opens by using "**Windows + R**" keys combination and netlogon directory is called as in the picture.



Attached files are copied to this area.



networksettings registry file is edited for the network settings.
 Right button + edit are clicked on networksettings file.

Appropriate definitions are made to your network settings in registry file opened.

If the regedit file is not set, the gateway of computer sends requests to the IP address by default. If the default gateway is Labris device, it works without any problems.



#### **Parameter Description**

No	Parameter	Value	Description
1	Location Name	Istanbul	The location name to be made network identification.
2	Network	192.168.20.0	Network address of the Labris device location is written.
	Address		
3	Subnet Mask	255.255.255.0	The subnet mask belongs to network address specified is defined.
4	Labris IP	192.168.20.1	Labris device's IP address in location is written.
	address		
5	Labris Port	9090	The port accepting requests on Labris. TCP 9090
6	requestsleep	3000000	It is set that it will make communicate with Labris device in how many
			milliseconds. It is set 5 minutes by default. It can be set so as to at least
			1 minute.

#### Step 2: Active Directory Group Policy settings are made.



It is entered in the **Group Policy** Management window.

**Default Domain Policy** is set. If desired, settings can also be made here by creating a different group policy.

墨	Group Policy Management
<ul> <li>File Action View Window H</li> <li></li></ul>	Default Domain Policy
<ul> <li>▲ Correst: Indeest.Incent</li> <li>▲ Domains</li> <li>▲ Indeest.Incent</li> <li>▶ Default Domain Policy</li> <li>▶ Domain Controllers</li> <li>▶ B Coroup Policy Objects</li> <li>▶ ⊕ WMI Filters</li> <li>▶ ⊕ Starter GPOs</li> <li>▶ ⊕ Sites</li> <li>₩ Group Policy Modeling</li> <li>♥ Group Policy Results</li> </ul>	Scope Details Settings Delegation Links Display links in this location: Iab Fdit Fdit Link Enabled Save Report View New Window from Here Delete Rename
	Refresh Help

Script Settings section opens.



a. **Logon** settings open. Add is clicked in the window appeared. regedit file displays, which we copied under netlogon directory with the Active Directory IP address.

	Logon Properties		?	x	
Scripts PowerShell Scrip	ts				
Logon Script	s for Default Domain Policy			_	
Name	Parameters				
			Up		
			Down		
			Add		
			E dit		
Add a Script 🛛 🗙					
Script Name:					
regedit.exe			Browse	9]	
Script Parameters:					
/s \\192.168.20.254\n	etlogon\networksettings.reg				
	ОК		Canc	el	

#### **Parameter Description**

No	Parameter	Value	Description
1	Script name	regedit.exe	Registry editing tool in which will run registry
			file that we set.

2	Script	/s	It will not be displayed while applying registry		
	Parameters 1		record in user computers.		
3	Script	\\192.168.20.254\netlogon\networksettings.reg	The path of networksettings.reg file is		
	Parameters 2		displayed, which we copied to netlogon		
			directory of active directory server.		

#### Labris User logon tracker settings are made.

Add Again and Browse is clicked on Logon script settings

\\SunucuIP\netlogon\ is written to the address line of window appeared and entered.

Labris-user-login-tracker-x86.exe is selected and opened

Browse		x
	Search netlogon	م
Organize 🔻 New folder	: :	- 🔲 🕜
Videos 🔷 Name	Date modified	Туре
Local Disk (C:) DVD Drive (D:) IR DVD Drive (D:) IR networksettings	1.5.2014 14:28	Applicatio Registratio
Image: Wetwork     Image: Wetwork       Image: Wetwork     Image: Wetwor		-
slave 🗸 kini 🖬		>
File name: Labris-user-login-tracker-x86 🗸 🗸	All Files Open	✓ Cancel

Operation mode and registry record are given as script parameters with path on the server.

Add a Script 🛛 🗙
Script Name: \\192.168.20.254\netlogon\Labris-user-login-tracker k Browse Script Parameters: logon \\192.168.20.254\netlogon\networksettings.reg
OK Cancel

## **Parameter Description**

No	Parameter	Value	Description	
1	Script name	\\192.168.20.254\netlogon\Labris-user-login-	File path definition is made for Labris user	
		tracker-x86.exe	logon tracker program.	
2	Script	logon	When the user logs on, the operating mode	
	Parameters 1		of the logon tracker is set as logon.	
3	Script	\\192.168.20.254\netlogon\networksettings.reg	In case of failure writing of the registry record	
	Parameters 2		to the user's computer, logon tracker tries to	
			perform settings by reading the registry file	

		here. It is written with a space after the value
		of Script parameters 1.

In the latter case, Logon Script settings should be as follows.

l	logo <mark>n Prope</mark> r	ties	? X
Scripts PowerShell Scripts			
Logon Scripts for Default Domain Policy			
Name	Parameters		
regedit.exe	/s \\192.168.2	0.254\n	Up
\\192.168.20.254\netlo.	logon \\192.16	8.20.25	Down
			Add Edit
	and in this Casue De	liau Obiant a	Remove
the button below.	ea in this Group Po	nicy Object, pi	ess
	ОК	Cancel	Apply

b. Logoff settings are clicked and then Add is clicked.

As in the setting of logon, **Labris-user-login-tracker-x86.exe** is selected and script parameters are written.

Logoff Properties ? X
Scripts PowerShell Scripts
Logoff Scripts for Default Domain Policy
Name Parameters
Edit Script 🛛 🗶
Script Name:   \\192.168.20.254\netlogon\Labris-user-login-tracker-   Script Parameters:   logoff \\192.168.20.254\netlogon\labris.reg     OK   Cancel
the button below.
OK Cancel Apply

# **Parameter Description**

No	Parameter	Value	Description
1	Script name	\\192.168.20.254\netlogon\Labris-user-login-	File path definition is made for Labris
		tracker-x86.exe	user logon tracker program.
2	Script	logoff	When the user logs off, the operating
	Parameters 1		mode of the logon tracker is set as logoff.
3	Script	\\192.168.20.254\netlogon\networksettings.reg	In case of failure writing of the registry
	Parameters 2		record to the user's computer, logon
			tracker tries to perform settings by
			reading the registry file here. It is written
			with a space after the value of Script
			parameters 1.

In the latter case, Logoff Script settings should be as follows.

Logoff Properties	? X
Scripts PowerShell Scripts	
Logoff Scripts for Default Domain Policy	
Name Parameters	
\\192.168.20.254\netlo logoff \\192.168.20.25	Up
	Down
	Add
	Edit
	Remove
To view the script files stored in this Group Policy Object, p the button below.	Dress
Show Files	
OK Cancel	Apply

c. Group Policy settings are applied.

For the changes to be valid, Group Policy settings will be updated for all users. **Run** opens by using "**Windows + R**" keys.

The settings are applied by giving **gpudate / force** command to this area.

	Run	
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
<u>O</u> pen:	gpupdate /force          This task will be created with administrative privileges.	
	OK Cancel <u>B</u> rowse	

d. Control of the settings is made.

The user computer is log off and logon again after settings successfully applied. It can be seen that **Labris-user-logon-tacker-x86.exe** is running in task manager (ctrl + shift + esc) application.

pplications Processes Services Pe	erformance Netv	vorking l	Jsers
Image Name	User Nar	me CPU	Memory
dtmng.exe *32	labris3	00	4.54
dtmngui.exe *32	labris3	00	2.90-
csrss.exe		00	4.268
dllhost.exe	labris3	00	2.288
dwm.exe	labris3	00	1.168
explorer.exe	labris3	00	10.33:
Labris-user-login-tracker-x86.exe *:	32 labris3	00	2.220
SearchProtocolHost.exe	labris3	00	1.508
taskhost.exe	labris3	00	1.97
taskmgr.exe	labris3	00	1.84
userinit.exe	labris3	00	84(
vmtoolsd.exe	labris3	00	3.208
winlogon.exe		00	1.916
wuaudt.exe	labris3	00	1.45:
۰ III III III III III III III III III I			۲
Show processes from all users		End P	rocess

To provide control over Labris;

"labrisdb\_user\_manager.py -getall-ip" command is written on the command line and it is seen that the IP addresses of users came.

# 94. Logging Options

Log Level and Log Exception Hills tabs are displayed.



#### **Network Settings**

Network settings consists of four fields. They are Filter IP, Filter Port, Proxy IP and Proxy Port. Give appropriate Filter IP, Filter Port, Proxy IP and Proxy Port.

Network Settings Filter IP : The IP that Labris Web Filter listens on. If left blank filter will listen on all IPs. That would include all NICs, loopback, modem, etc. Normally you would have your firewall protecting this, but if you want you can limit it to only 1 IP. Yes only one.
1
Filter Port : The port that filter listens to. 8080 2
Proxy IP : The ip of the proxy. (default is the loopback - i.e. this server)           127.0.0.1
Proxy Port : The port filter connects to proxy on

#### **Weighted Phrase Settings**

In the Weighted Phrases Settings we can choose Weighted Phrase Mode.

If it is on then the phrases found that made up the total which exceeds the naughtiness limit will be logged, if the level is high enough reported.



## **Cache Settings**

We can view and change Cache Settings.

Cache Settings Positive result caching for text URLs. Caches good pages so they don't need to be scanned again (0 = off (recommended for ISPs with users with dissimilar browsing), 1000 = recommended for most users, 5000 = suggested max upper limit)
5000
Age before they are stale and should be ignored in seconds. (0 = never, 900 = recommended = 15 mins)
900

#### **Fork Pool Settings**

We can view and change Fork Pool Settings.

Fork Pool Settings Sets the maximum number of processes to sporn to handle the incomming connections. Max value usually 250 depending on OS. On large sites you might want to try 180.
Sets the minimum number of processes to sporn to handle the incomming connections. On large sites you might want to try 32.
Sets the minimum number of processes to be kept ready to handle connections. On large sites you might want to try 8.
Sets the minimum number of processes to sporn when it runs out On large sites you might want to try.
Sets the maximum number of processes to have doing nothing. When this many are spare it will cull some of them. On large sites you might want to try 64.
Sets the maximum age of a child process before it croaks it. This is the number of connections they handle before exiting. On large sites you might want to try 10000.

Click on **Save tab** to save the changes.

🍇 Filter Groups 🕜 Banned Filters 🕜 Exception Filters 📝 Configuration 💿 Log Monitoring	
r Reporting Options	· · · · · · · · · · · · · · · · · · ·
Web Access Denied Reporting	
🔿 log, but do not block - Stealth mode	
🔿 just say 'Access Denied'	
report why but not what denied phrase	
report fully	
use HTML template file (accessdenied addressignored) - recommended	
Customi	ze
Authentication	
✓ NTLM Authentication Configure	
✓ Basic Authentication	
IP Authentication	
Logging Options	
Log Level	
○ none	
🔿 just denied	
Il text based	
◯ all requests	
<b>\</b>	
Log Exception Hits : Log if an exception (user, ip, URL, phrase) is matched and so the page gets let through. Can be useful for disgnost	sing why a site 💽 💌
	Save 🛃 Cancel
URL/Content Filter Service Status: Running	
cted to is: 78.188.50.48	Labris Teknoloji

# 95. Log Monitoring

When we click on **Log Monitoring tab**, Live traffic Monitoring tab appears.



#### 96.Show

Click on Show tab to see current traffic on Webfilter.



#### Filter

Below screen appears.

*					- 🗆 🗙
Filtrele       URL:       Client IP       Client User Name					
					Start Clear
Time	User Name	Client Address	Url	Result	Filter Group Name

#### Start

Filtrele URL: Client IP Client User Na	labristeknoloji.com 10.1.1.0 ame labris	1 2 3			Start Clear
Time	User Name	Client Address	Url	Result	Filter Group Name

#### These are the inputs to start

1	URL	Type URL
2	Client IP	Give the client IP Address
3	Client User Name	Type client User Name.

Click on Start tab.

In the below screen we can notice service has been started.

*				- 🗆 🗙
Filtrele				
URL:	labristeknoloji.com			
Client IP	10.1.1.0			
Client User Name	labris			
<u>.</u>			5	Stop Clear
Time User N.	Client Add	Url	Result	Filter Gro

#### Clear

When we select the log and click on clear button the logs can be cleared from the list. If there are too many rows in the table we can select each one of them and Click on the **Clear** button, to delete a log.

Filtrele		
URL:	labristeknoloji.com	
✓ Client IP	10.1.1.0	
✓ Client User Na	ame labris	

# **ANTISPAM/ANTIVIRUS**



# 97. Spam Mail Box

#### **Search Criterions**

Labris Management Console					- 🗆 X
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>M</u> odule <u>A</u> bou	t				<u>H</u> elp
	Spam Mail Box Virus Mail Box	AntiSpam-AntiVirus Options	5		
Server 78.188.50.48:4000 System Network Settings Firewall VPN Filter Antispam/Antivirus IDS/IPS Messaging Server Load Balancer Elicense	Search Criterions	<prev 0="" 1="" next="">&gt; Order</prev>	To From V Max	Date	Mail-Id er pa 20 💌
Lmc server address you are connec	cted to is: 78.188.50.48				Labris Teknoloji

These are the inputs for Spam Mail Box.

1	Sender	Enable Sender and type Sender name
2	Recipient	Enable Recipient and type Recipient name

3	Date and Time	Enable Date and Time, choose Start Date and End Date
4	Search	Click on Search tab to find out Mail.

Info tab appears stating No Mail, Since No mail has been sent. Click Ok



# **Virus Mail Box**

## **Search Criterions**

Labris Management Console		- 🗆 ×
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>M</u> odule <u>A</u> bou	t	<u>H</u> elp
	Spam Mail Box Virus Mail Box AntiSpam-AntiVirus Options	<u> </u>
Server 78.188.50.48:4000 Ver Management System Network Settings Firewall VPN Filter IDS/IPS Messaging Server Load Balancer Elicense	Search Criterions Search Criterions John Recipient 2 Bob Date and Time 3 Start Date 06/01/2014 End Date 22/01/2014 Search 4	From Max listed mail per pa
Lmc server address you are connec	cted to is: 78.188.50.48	Labris Teknoloji

These are the inputs for Virus Mail Box

1	Sender	Enable Sender and type Sender name
2	Recipient	Enable Recipient and type Recipient name
3	Date and Time	Enable Date and Time, choose Start Date and End Date
4	Search	Click on Search tab to find out Mail.

Info tab appears stating No Mail, Since No mail has been sent. Click Ok



# 98. Antispam-Antivirus Options

## **Domain Control**

Save
e 🔐 Edit

Domain Control tab appears with the fields Domain and Relay IP

Add New Domain tab appears.

Type Domain name and Give Relay ip address. Click Ok

Add New Domain			×
Domain:	kralsensin.com		
Relay ip address:	192.168.1.252		
		Ok	Cancel

It takes some time to Apply changes.
Applying Changes	×
Please wait	

In the below screen, we can notice New Domain added in the Domain Control tab.

Spam Mail Box Vir	us Mail Box AntiSpam-AntiVirus Options	
Domain Control	Ayarlar	
Antispam Options	Domain: kralsensin.com H	lostname: mail.kralsensin.com
Whitelist Blacklist		Save
Antivirus Options		
, , ,	Domain Conrtol	·
	Domain	Relay IP
4	kralsensin.com	192.168.1.252
· ·		
•		
		🚰 Add 🔤 Remove 🛛 🕎 Edit
ected to is: 78.188.50.48		Labris Teknoloji

Select the Domain and Click on Edit tab.

Spam Mail Box Vir	us Mail Box AntiSpam-AntiVirus Options	
Domain Control Antispam Options Whitelist Blacklist Antivirus Options	Ayarlar Domain: kralsensin.com H	ostname: mail.kralsensin.com Save
	Domain kralsensin.com	Relay IP 192.168.1.252
cted to is: 78.188.50.48		Labris Teknoloji

Edit tab appears.

We can edit Domain name and Relay IP address. Click Ok.

Edit			×
Domain:	kralsensin.com		
Relay ip address:	192.168.1.245		
		Ok	Cancel

It takes some time to apply changes.

Applying Changes	×
Please wait	
Please wait	

In the below screen, we can notice changes made in the new domain.

Spam Mail Box Vir	us Mail Box AntiSpam-AntiVirus Options	
Domain Control	Ayarlar	
Antispam Options	Domain: kralsensin.com H	ostname: mail.kralsensin.com
Whitelist Blacklist		Save
Antivirus Options		
	Domain Conrtol	
	Domain	Relay IP
]	kralsensin.com	192.168.1.245
>		
		n Add 😑 Remove 😗 Edit
cted to is: 78.188.50.48	I	Labris Teknoloji

Select the Domain and click on Remove tab.

Spam Mail Box Vir	us Mail Box AntiSpam-AntiVirus Options	
Domain Control Antispam Options Whitelist Blacklist Antivirus Options	Ayarlar Domain: kralsensin.com	Hostname: mail.kralsensin.com
	Domain kralsensin.com	Relay IP 192.168.1.245
		🔮 Add 🔤 Remove 💱 Edit
cted to is: 78.188.50.48		Labris Teknoloji

It takes some time to apply changes.

Applying Changes	×
Please wait	

In the below screen, we can notice **Domain** deleted in the Domain Control tab.

Spam Mail Box Vir	us Mail Box AntiSpam-AntiVirus Options	
Domain Control Antispam Options Whitelist Blacklist Antivirus Options	Ayarlar Domain: kralsensin.com H	lostname: mail.kralsensin.com
	Domain	Relay IP
cted to is: 78.188.50.48		Labris Teknoloji

# Settings

Add a Global policy.

No.	Source	Destination	Service	Action	Schedule	QoS/Band	Applications	Security P	Options
0	🗅 Any	A EXCHANGE	smtp smtps	Accept	🗅 Any	🗅 Any	🗅 Any	🗅 Any	₽₽
		Contraction of the local distance of the loc	Contraction of the local distance of the loc		14-1 1-1		<u></u>		2.2

### 99. Antispam Options

Antispam consists of three fields.

They are Bypass spam check, By pass header check, spam mail receivers.

#### **Check Options**

It helps us to enable Bypass spam check, By pass header check, spam mail receivers and perform actions like Add, Delete on check options.

Spam Mail Box Vir	rus Mail Box AntiSpam-AntiVirus Options	
Domain Control Antispam Options Whitelist Blacklist	Antispam Options Check Options Enable "Bypass spam check" list	Cancel
Antivirus Options	Bypass spam check Add Delete	
	Enable "Bypass header check" list Bypass header check Add Delete	
	Enable "Spam mail receivers" list Spam mail receivers Add Delete	
	Report Options Modify spam mail subject Warn spam sender Spam subject tag Spam admin mail adress Spam mail policy Discard	
cted to is: 78.188.50.48	Advanced settings	pris Teknoloji

Enable Bypass spam check list and click on Add tab.

Spam Mail Box Vi	us Mail Box AntiSpam-AntiVirus Options
Domain Control Antispam Options Whitelist Blacklist	Antispam Options Check Options Enable "Bypass spam check" list
Antivirus Options	Bypass spam check Add Delete

Add Domain Name or Mail Address tab appears.

Type Domain name or e-mail address. Enable No include, check domain part and click on **Add** tab.



In the below screen, we can notice domain name added in the spam check list.

Check Options		
Enable "Bypass spam check" list		
Bypass spam check	Add	
1.\$mydomain	Delete	

Select domain and click on **Delete** tab.

ſ,	Antispam Options	
	Check Options	
	<ul> <li>Enable "Bypass spam check" list</li> </ul>	
	Bypass spam check	Add
	I.\$mydomain	Delete

Warning tab appears stating Are you sure? Click on Yes



Enable Bypass header check list and click on Add tab.

Enable "Bypass header check" list	
Bypass header check	Add
D	elete

Add Domain Name or Mail Address tab appears.

Type Domain name or e-mail address. Enable No include, check domain part and click on Add

#### tab.

Add Domain Name or Mail A	ddress		×
Enter a domain name or a	n e-mail address	\$mydomain	
EX	ample: ttnet.net.tr,	alper@ttnet.net.tr o	or \$mydomain
✓ No include			
Check domain part			
		Add	Cancel

In the below screen, we can notice domain name added in the header check list.

Enable "Bypass header check" list		
Bypass header check	Add	
I.\$mydomain	Delete	

Select domain and click on **Delete** tab.

✓ Enable "Bypass header check" list	
Bypass header check	Add
I.\$mydomain	Delete

Warning tab appears stating Are you sure? Click on Yes



Enable Spam mail receivers list and click on Add tab.

Enable "Spam mail receivers" list		
	Spam mail receivers	Add
		Delete

Add Domain Name or Mail Address tab appears.

Type Domain name or e-mail address. Enable No include, check domain part and click on **Add** tab.

Add Domain Name or Mail Ad	idress 🔰
Enter a domain name or an	e-mail address \$mydomain
Exa	mple: ttnet.net.tr, alper@ttnet.net.tr or \$mydomain
✓ No include	
Check domain part	
	Add Cancel

In the below screen, we can notice domain name added in the Spam mail receivers list.

Enable "Spam mail receivers" list		
Spam mail receivers	Add	
I.\$mydomain	Delete	

### Select domain and click on **Delete** tab.

Enable "Spam mail receivers" list	
Spam mail receivers	Add
I.\$mydomain	Delete

### Warning tab appears stating Are you sure? Click on Yes

WARNIN	G	X
2	Are you sure?	
	Yes No	

## **Report Options**

Report Options		1	-		
Modify spam mail subject			_		no 🔻
Warn spam sender					no 🔻
Spam subject tag 🦯				***SPAM***	
Spam admin mail adress	1	_		admin@labristeknoloji.com	
Spam mail policy		5		Pass	-
		-			

These are the inputs for the Report options.

1	Modify spam mail subject	To modify spam mail subject select yes or else no
2	Warn spam sender	To Warn spam sender select yes or else no
3	Spam subject tag	Type tag of Spam subject.
4	Spam admin mail address	Type spam admin mail address
5	Spam mail policy	Select policy from the drop down list.

Click on **Save** tab to save changes made to the AntiSpam-AntiVirus.

Domain Control	Antispam Options		
Antispam Options	Check Options		
Vhitelist Blacklist	Enable "Bypass spam check" list		×
Antivirus Options	Bypass spa	am check	Add
			Doloto
			Delete
	Enable "Bypass header check" list		
	Bypass hea	der check	Add
			Delete
	Enable "Spam mail receivers" list		
	Spam mail	receivers	Add
			Delete
	Report Options		
	Modify spam mail subject		no 🔻
	Warn spam sender		no 🔻
	Spam subject tag	***SPAM***	
	Spam admin mail adress	admin@labristeknolo	ji.com
	Spam mail policy	Pass	
			Advanced settings

## **100.** Whitelist Blacklist

#### **Enable White List**

Enable white list to perform action like Add, Edit, Delete, Delete All Whitelist.

Spam Mail Box Virus Mail Box AntiSpam-AntiVirus Options			
Domain Control Antispam Options Whitelist Blacklist	WhiteList WhiteList Enable white list		Cancel
Antivirus Options	White list	Add	]
	sorun@labristeknoloji.com	Edit Delete Delete All	

#### Click on Add tab.

WhiteList Carlos Enable white list	
White list	Add
sorun@labristeknoloji.com	Edit
	Delete
	Delete All

Add Domain Name or Mail Address tab appears.

Type Domain name or e-mail address, we can enable Check Domain part if necessary and click on **Add** tab.

Add Domain Name or Mail Address		×
Enter a domain name or an mail address	admin@labristek	noloji.com
Example: ttnet.net.t	tr, alper@ttnet.ne	et.tr or \$mydomain
Check domain part		
	Add	Cancel

In the below screen, we can notice mail address added in the White list.

WhiteList		
Enable white list		
White list	Add	
admin@labristeknoloji.com	Edit	
sorun@labristeknoloji.com	Delete	
	Delete	
	Delete All	

Select mail address and click on Edit tab.

[	WhiteList	
	✓ Enable white list	
	White list	Add
	admin@labristeknoloji.com	Edit
	sorun@labristeknoloji.com	Delete
		Doloto All
		Delete All

Edit List tab appears, we can edit URL and click on **Save** tab.

In the below screen, we can notice changes made to the mail address.

WhiteList	
Enable white list	
White list	Add
admin2@labristeknoloji.com	Edit
sorun@labristeknoloji.com	Delete
	Doloto All

Select mail address and click on **Delete** tab.

Add
Edit
elete
lete All
E

Warning tab appears stating Are you sure? Click on Yes

WARNIN	IG	×
3	Are you sure?	
	Yes No	

Below screen we can notice selected mail deleted from the white list.

Click on **Delete All** tab to delete all the mail addresses in White list.

[	WhiteList	
	<ul> <li>Enable white list</li> </ul>	
	White list	Add
	sorun@labristeknoloji.com	Edit
		Delete
		Delete All

Warning tab appears stating Are you sure? Click on Yes

WARNIN	IG	×
2	Are you sure?	
	Yes <u>N</u> o	

#### **Enable black List**

Enable Black List to perform actions like Add, Delete, Delete All in Black list.

BlackList		
Enable black list		
Black list	Add	
	Edit	
	Delete	
	Delete All	

Click on Add tab.

BlackList	
Black list	Add
	Edit
	Delete
	Delete All

Add Domain Name or Mail Address tab appears.

Type Domain name or e-mail address, We can enable Check Domain part if necessary and click on **Add** tab.

Add Domain Name or Mail Address		×
Enter a domain name or an mail address	test@labristekn	oloji.com
Example: ttnet.net.tr	, alper@ttnet.ne	et.tr or \$mydomain
Check domain part		
	Add	Cancel

In the below screen, we can notice mail address added to the Black list.

BlackList	
Enable black list	
Black list	Add
.\$mydomain	Edit
test@labristeknoloji.com	Datata
	Delete
	Delete All

Select mail address and click on Edit tab.

BlackList	
Enable black list	
Black list	Add
.\$mydomain	Edit
test@labristeknoloji.com	Delete
	Delete
	Delete All

Edit List tab appears, we can edit URL and click on Save tab.

Edit Lis	t	×
URL	test2@labristeknoloji.cr	om
	Save	Cancel

In the below screen, we can notice changes made to the mail address.

- BlackList	
Enable black list	
Black list	Add
.\$mydomain	Edit
test2@labristeknoloji.com	Delete
	Delete All

Select mail address and click on **Delete** tab.

BlackList	
Enable black list	
Black list	Add
.\$mydomain	Edit
test2@labristeknoloji.com	Delete
	Delete
	Delete All

Warning tab appears stating Are you sure? Click on Yes



In the below screen we can notice selected mail deleted from the Black list.

Click on **Delete All** tab to delete all the mail addresses in White list.

BlackList	
Enable black list	
Black list	Add
.\$mydomain	Edit
	Delete
	Delete All

Warning tab appears stating Are you sure? Click on Yes



# **101.** Antivirus Options

Antivirus consists of two fields.

They are Virus check bypass list and Virus mail receivers list.

Spam Mail Box Vir	rus Mail Box AnifSpam-AnifVirus Opifons	
Domain Control Antispam Options Whitelist Blacklist	Antivirus Options Antivirus Options Enable "Virus check bypass list"	Cancel
Antivirus Options	Virus check bypass list Add Delete	
	Enable virus mail receivers inst       Add         Virus mail receivers       Add         Delete	
	Warn virus sender     no     ▼       Warn virus recipient     no     ▼       Infected mail policy     Discard     ▼       Admin address     ×     ×       X_HEADER_TAG' value     ×     ×       X_HEADER_LINE' value     by Labris Messaging Suite Mail Security at Smydomain	
	Advanced Options	

# **Antivirus Options**

It helps us to enable Virus check bypass list and Virus mail receivers list and perform actions like Add, Delete on check options.

Enable "Virus check bypass list"	
Virus check bypass list	Add
	Delete
Enable "Virus mail receivers" list	Add
virus mail receivers	1.1100.0

Enable virus check bypass list and click on **Add** tab.

Antivirus Options	
Enable Virus check bypass list	
Virus check bypass list	Add
	Delete

Add URL or Mail Address tab appears.

Type **URL or e-mail address**. We can enable No include, check domain part only when we give domain and click on **Add** tab.

Add URL or Mail Address	×
Enter a URL or an e-mail address	bob@labristeknoloji.com
Example: ttnet.net.tr,	alper@ttnet.net.tr or \$mydomain
No include	
Check domain part	
	Add Cancel

In the below screen, we can notice mail address added in the Virus check bypass list.

Antivirus Options Antivirus Options Enable "Virus check byn	ass list"	
bob@labristeknoloji.com	Virus check bypass list	Add

Select mail address and click on Delete tab.

_A	Intivirus Options	
lг	Antivirus Options	
	Enable "Virus check bypass list"	
	Virus check bypass list	Add
	bob@labristeknoloji.com	Delete

#### Warning tab appears stating Are you sure? Click on Yes

WARNII	IG	×
2	Are you sure?	
	Yes No	

Enable Virus mail receivers list and click on Add tab.

Enable "Virus mail receivers" list	
Vi	rus mail receivers Add
	Delete

Add URL or Mail Address tab appears.

Type **URL or e-mail address**. We can enable No include, check domain part only when we give domain and click on **Add tab**.



In the below screen, we can notice mail address added in the Virus mail receivers.

Enable "Virus mail receivers" list	
Virus mail receivers	Add
sam@labristeknoloji.com	Delete

#### Select mail address and click on **Delete tab**.

Enable "Virus mail receivers" list	
Virus mail receivers	Add
sam@labristeknoloji.com	Delete

#### Warning tab appears stating Are you sure? Click on Yes



### **Report Options**



These are the inputs for **Report Options**.

1	Warn virus sender	To Warn virus sender select yes or else no	
2	Warn virus recipient	To Warn virus recipient select yes or else no	
3	Infected mail policy	Select policy from the drop down list	
4	Admin address	Type spam admin mail address	
5	'X_HEADER_TAG' value	Give header tag value	
6	'X_HEADER_line' value	Give header line value.	

Click on **Save** tab to save changes made to the Antivirus options.

Antivirus Options			💾 Save
Antivirus Options			
Enable "Virus check bypass list"			🔀 Cancel
Virus chec	k bypass list	Add	
		Delete	
Taskie Wine and a sector of the		-	
<ul> <li>Enable "Virus mail receivers" list</li> </ul>			
Virus mai	il receivers	Add	
		Delete	
		·	
Report Options			
Warn virus sender		no 🔻	
Warn virus recipient		no 🔻	
Infected mail policy	Discard	-	
Admin address	admin@labristeknoloji.com		
'X_HEADER_TAG' value			
X_HEADER_LINE value	by Labris Messaging Suite Mail Security at \$mydomain		

# **IDS/IPS**

Right Click on the IDS / IPS tab and click on Connect to get connected to the IDS/IPS tab



### **102.** Sensor Settings

Once you get connected you can find two options on the top i.e., Sensor settings and alert settings.

Click on Sensor settings , in that tab you can find Intrusion detection system

#### **Intrusion Detection System**

🔣 Labris Management Console	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>M</u> odule <u>A</u> bo	but
	Sensor Settings Alert Settings
Server	Sensor 1  Service  Running

## 103. Settings

# **Network Settings**

# Under Intrusion Detection System we find options like **Settings > Network settings**

Sensor Settings Alert Settin	ngs			
Sensor 1 🔻		Sensor 1 configu	uration: listening all interfaces	
Service 🕐 🕕 📇 Appl	у	Variable	Value	Control/Status
	HOME_NET	г	10.1.1.0/24	Disabled
Settings	HOME_NET	г	\$eth0_ADDRESS	Disabled
Network Settings	HOME_NET	г	10.1.1.0/24, 192.168.1.0/24	Disabled
Interface	HOME_NET	Г	any	Enabled
🗄 👹 Rulesets	EXTERNAL	_NET	any	Enabled
	DNS_SER\	/ERS	\$HOME_NET	Enabled
	SMTP_SER	VERS	\$HOME_NET	Enabled
	, HTTP_SER	VERS	\$HOME_NET	Enabled
	SQL_SERV	'ERS	\$HOME_NET	Enabled
	TELNET_S	ERVERS	\$HOME_NET	Enabled
0	SNMP_SEF	RVERS	\$HOME_NET	Enabled
>	dHTTP_POR	RTS	8081	Disabled
	D Variable Se	ettings		
	; Variable	HOME_NET		
	Value	10.1.1.0/24		
	Comment	Must change the following var You can specify it explicitly as HOME_NET 10.1.' or use global variable S-interfe initialized to IP address and net HOME_NET Seth0 You can specify lists of IP add the IPs with commas like this: HOME_NET 10.1.'	iables to reflect your local network. : 1.0/24 acename>_ADDRESS which will be always tmask of the network interface. _ADDRESS resses for HOME_NET by separating 1.0/24, 192.168.1.0/24	
			<b>⊡</b> ∱ Cha	nge 👔 Delete ⊘ Cancel

## **Changing variable**

Select one of the variable from the list in the right pane, below you can **edit** the contents of the variables in variable settings tab and click on **Change**.

Variable	Value	Control/Status	
HOME_NET	10.1.1.0/24	Disabled 🔺	
HOME_NET	\$eth0_ADDRESS	Disabled	
HOME_NET	10.1.1.0/24, 192.168.1.0/24	Disabled	
HOME_NET	any	Enabled	
EXTERNAL_NET	any	Enabled	
DNS_SERVERS	SHOME_NET	Enabled	
SMTP_SERVERS	SHOME_NET	Enabled	
HTTP_SERVERS	SHOME_NET	Enabled	
SQL_SERVERS	SHOME_NET	Enabled	
TELNET_SERVERS	SHOME_NET	Enabled	
SNMP_SERVERS	SHOME_NET	Enabled	
HTTP_PORTS	8081	Disabled	
Variable Settings         Variable Value         Value         10.1.1.1/24         Comment         Must change the following variables to reflect your local network.         You can specify it explicitly as:         HOME_NET 10.0.1.1.0/24         or use global variable S         Initialized to IP address and netmask of the network interface.         HOME_NET Seth0_ADDRESS         You can specify lists of IP addresses for HOME_NET by separating         the IPs with commas like this:         HOME_NET 10.1.1.0/24, 192.168.1.0/24			
	Chan	ge 🔂 Delete 🖉 Cancel	
		Labris Teknoloji	

Changes are applied to the variables immediately. We can notice in the below screen.

Select the variable and double click on Control/Status to make the Variable Enable.

ervice unning Intrusion Detection Syste Settings Rulesets	Apply tem HOME_NET HOME_NET HOME_NET HOME_NET EXTERNAL DNS_SERV SMTP_SERV HTTP_SERV	Variable	Value 10.1.1.0/24 \$eth0_ADDRESS 10.1.1.0/24, 192.168.1.0/24 any any	Control/Status Disabled Disabled Disabled Enabled
Intrusion Detection System Settings Interface	HOME_NET HOME_NET HOME_NET HOME_NET EXTERNAL DNS_SERV SMTP_SERV HTTP_SERV	NET	10.1.1.0/24 \$eth0_ADDRESS 10.1.1.0/24, 192.168.1.0/24 any any	Disabled Disabled Disabled Enabled
Intrusion Detection System     Settings     Settings     Interface     Rulesets	HOME_NET HOME_NET HOME_NET EXTERNAL DNS_SERV SMTP_SERV HTTP_SERV	NET	\$eth0_ADDRESS 10.1.1.0/24, 192.168.1.0/24 any any	Disabled Disabled Enabled
	HOME_NET HOME_NET EXTERNAL DNS_SERV SMTP_SERV HTTP_SERV	NET	10.1.1.0/24, 192.168.1.0/24 any any	Disabled Enabled
<ul> <li>Interface</li> <li>B Rulesets</li> </ul>	HOME_NET EXTERNAL_ DNS_SERV SMTP_SERV HTTP_SERV	NET	any	Enabled
⊞- 💕 Rulesets	EXTERNAL_ DNS_SERV SMTP_SERV HTTP_SERV	NET	anv	
	DNS_SERV SMTP_SERV HTTP_SERV		any	Enabled
	SMTP_SER	ERS	\$HOME_NET	Enabled
	HTTP SER	/ERS	\$HOME_NET	Enabled
	-	/ERS	\$HOME_NET	Enabled
	SQL_SERVE	ERS	\$HOME_NET	Enabled
	TELNET_SE	RVERS	\$HOME_NET	Enabled
	SNMP_SER	VERS	\$HOME_NET	Enabled
	dHTTP_POR	rs	8081	Disabled
	<ul> <li>Variable Se</li> <li>Variable</li> <li>Variable</li> <li>Value</li> <li>Comment</li> </ul>	ttings HOME_NET 10.1.1.0/24	ing unriching to onfloat your logal patronal.	
	Comment	You can specify it expl HOME_NE or use global variable \$ initialized to IP address : HOME_NE You can specify lists of the IPs with commas like HOME_NE	ing variables to reflect your local fletwork. city as: r 10.1.1.0/24 <interfacename>_ADDRESS which will be alw and netmask of the network interface. r \$eth0_ADDRESS iP addresses for HOME_NET by separating e this: r 10.1.1.0/24, 192.168.1.0/24</interfacename>	/ays

Changes are applied to the variables immediately. We can notice in the below screen.

Sensor Settings Alert Settings				
Sensor 1 🔻		Sensor 1 configur	ation: listening all interfaces	
Service D D Apply		Variable	Value	Control/Status
Running System	HOME_NET	•	10.1.1.0/24	Enabled
Settings	HOME_NET	•	\$eth0_ADDRESS	Disabled
Metwork Settings	HOME_NET		10.1.1.0/24, 192.168.1.0/24	Disabled
Interface	HOME_NET		any	Enabled
🗈 👹 Rulesets	EXTERNAL	_NET	any	Enabled
	DNS_SERV	ERS	\$HOME_NET	Enabled
	SMTP_SER	VERS	\$HOME_NET	Enabled
	HTTP_SER	VERS	\$HOME_NET	Enabled
	SQL_SERV	ERS	\$HOME_NET	Enabled
	TELNET_SE	ERVERS	\$HOME_NET	Enabled
4	SNMP_SER	VERS	\$HOME_NET	Enabled
D	HTTP_POR	TS	8081	Disabled
:	<sup>D</sup> Variable Se	ttings		
	Variable	HOME_NET		
	Value	10.1.1.0/24		
	Comment	Must change the following varia You can specify it explicitly as: HOME_NET 10.1.1. or use global variable \$-interfac initialized to IP address and netr HOME_NET \$=th0_ You can specify lists of IP addre the IPs with commas like this: HOME_NET 10.1.1.	bles to reflect your local network. 0/24 bename>_ADDRESS which will be always nask of the network interface. ADDRESS esses for HOME_NET by separating 0/24, 192.168.1.0/24	
			Chan	ge 🚮 Delete ⊘ Cancel

# **Deleting variable**

Select one of the variables from the list right pane and click on **Delete**.

Selected variables are deleted from the list immediately.

Sensor 1 configuration: listening all interfaces			
	Variable	Value	Control/Status
HOME_NET1	1	10.1.1.1/24	Disabled 🔺
HOME_NET		\$eth0_ADDRESS	Disabled
HOME_NET		10.1.1.0/24, 192.168.1.0/24	Disabled
HOME_NET		any	Enabled
EXTERNAL_	NET	any	Enabled
DNS_SERVE	ERS	\$HOME_NET	Enabled
SMTP_SERV	/ERS	\$HOME_NET	Enabled
HTTP_SERV	'ERS	\$HOME_NET	Enabled
SQL_SERVE	RS	\$HOME_NET	Enabled
TELNET_SE	RVERS	\$HOME_NET	Enabled
SNMP_SERV	/ERS	\$HOME_NET	Enabled
HTTP_PORT	S	8081	Disabled
Variable Set	tings		
Variable	SNMP_SERVERS		
Value	\$HOME_NET		
Comment	((/SNMP_SERVERS/(/		
		Change	e 🚺 Delete ⊘ Cancel

### Cancel

Click on **Cancel** tab to **revert back** to the same settings as before.

Sensor 1 configuration: listening all interfaces				
	Variable	Value	Control/Status	
HOME_NET	٢1	10.1.1.1/24	Disabled	-
HOME_NET	Г	\$eth0_ADDRESS	Disabled	
HOME_NET	Г	10.1.1.0/24, 192.168.1.0/24	Disabled	
HOME_NET	Г	any	Enabled	
EXTERNAL	_NET	any	Enabled	
DNS_SER\	/ERS	\$HOME_NET	Enabled	
SMTP_SER	VERS	\$HOME_NET	Enabled	
HTTP_SER	VERS	\$HOME_NET	Enabled	
SQL_SERV	ERS	\$HOME_NET	Enabled	
TELNET_S	ERVERS	\$HOME_NET	Enabled	
HTTP_POR	TS	8081	Disabled	
HTTP_POR	TS	80	Enabled	-
Variable Settings         Variable Value       TELNET_SERVERS         Value       SHOME_NET         Comment       List of telnet servers on your network. This allows only look for attacks to systems that have a service up. These configurations MUST follow the same configuration scheme as defined above for \$HOME_NET.				
			Change 🚡 Delete 🖉 C	Cancel
			Labris Tekr	noloji

Click on Apply tab to apply the modified settings in Network settings tab

Sensor 1 🔻	Sensor 1 c	onfiguration: listening all interfaces		
Service 🕦 🕕 📇 Apply	Variable	Value	Control/Status	
Distantian Data dia 2014 are	HOME_NET1	10.1.1/24	Disabled	-
Intrusion Detection System	HOME_NET	<pre>\$eth0_ADDRESS</pre>	Disabled	
W Network Settings	HOME_NET	10.1.1.0/24, 192.168.1.0/24	Disabled	
Interface	HOME_NET	any	Enabled	
🗉 🍘 Rulesets	EXTERNAL_NET	any	Enabled	
	DNS_SERVERS	\$HOME_NET	Enabled	
	SMTP_SERVERS	\$HOME_NET	Enabled	
	HTTP_SERVERS	\$HOME_NET	Enabled	
	SQL_SERVERS	\$HOME_NET	Enabled	
	TELNET_SERVERS	\$HOME_NET	Enabled	
	SNMP_SERVERS	\$HOME_NET	Enabled	
	HTTP_PORTS	8081	Disabled	

Click **Ok** to save the changes



#### Interface

# Select Interface tab from the left pane

Sensor 1 🔻	Sensor 1 configuration: listening all interfaces
Service 🕥 🕕 💾 Apply	Sniff packages on this interface:
Intrusion Detection System     Settings     Network Settings	Unblockables List
	IP Adresleri 127.0.0.1

### From the drop down list select any one of the required Ethernet type

Sensor 1 configuration: listening all interfaces		
Sniff packages on this interface:	any	•
- Unblockables List	any	-
Hosts's whichs IP adresses are in th	eth0	
	eth2	
107.0.0.1	eth3	
127.0.0.1	eth4	
	eth4.10	_
	eth5	

# Adding IP

Click on Add tab to Add the new IP Address to the unblockable list

Sensor 1	configuration: listening all interfaces
Sniff packages on this interface:	any
Unblockables List	
Hosts's whichs IP adresses are in	th's table, will not be blocked by IDS in any case.
	IP Adresleri
127.0.0.1	
0	
	Add Remove Refresh
	Labris Teknoloji

Enter the IP Address which you wanted to add to the list and click on "EKLE"

Yeni Adres Ekle	×
IP adresi: 10.01.1.0	3
Ekle	

Sniff packages on this interface:	any 💌			
Unblockables List				
Hosts's whichs IP adresses are in t	h's table, will not be blocked by IDS in any case.			
	IP Adresleri			
127.0.0.1	127.0.0.1			
10.01.1.0				

#### Delete

Select one of the IP Address which you want to remove from the list and click on Remove tab.

Sensor 1 d	configuration: listening all interfaces
Sniff packages on this interface:	any
- Lieblaskablas List	
Hosts's whichs IP adresses are in t	h's table, will not be blocked by IDS in any case
127.0.0.1	IP Adresieri
10.01.1.0	
	Add Remove Refresh
	Labris Teknoloji

Selected IP Address is removed from the list immediately, which you can notice from the below screen.

Sensor 1 configuration: listening all interfaces		
Sniff packages on this interface:	any 💌	
Unblockables List Hosts's whichs IP adresses are in t	h's table, will not be blocked by IDS in any case.	
IP Adresleri		
127.0.0.1		

### Refresh

Click on **Refresh** Tab to refresh the entire tab.

Sniff packages on this interface:	any	•
Unblockables List		_
Hosts's whichs IP adresses are in	th's table, will not be blocked by IDS in any case.	
	IP Adresleri	
127.0.0.1		-11
	χ.	
	Add Remove Refresh	
	Labris Teknolo	oii

#### **Rule sets**

Select Rulesets tab from the left pane.

Sensor Settings Alert Settings		-			
Sensor 1 💌	Sensor 1 configuration: listening all interfaces				
Service O O Apply	RuleSets				
Intrusion Detection System     Settings     Metwork Settings     Interface     Rulesets	Rule File	Control/Status			
	local.rules	Disabled			
	bad-traffic.rules	Disabled			
	exploit.rules	Disabled			
	scan.rules	Disabled			
	finger.rules	Disabled			
	ftp.rules	Disabled			
	teinet.rules	Disabled			
	rpc.rules	Disabled			
0	rservices.rules	Disabled			

Click on New File to create a new rule file.

Sensor Settings Alert Settings				
Sensor 1 🔻	Sensor 1 configuration: listening all interfaces			
Service Running	RuleSets			
Intrusion Detection System	Rule File	Control/Status		
- Settings	local.rules	Disabled		
Interface	bad-traffic.rules	Disabled		
🕀 🍘 Rulesets	exploit.rules	Disabled		
	scan.rules	Disabled		
	finger.rules	Disabled		
	ftp.rules	Disabled		
	telnet.rules	Disabled Disabled		
	rpc.rules			
4	rservices.rules	Disabled Enabled		
	dos.rules			
	ddos.rules	Enabled		
	dns.rules	Enabled		
	tftp.rules	Disabled		
	web-cgi.rules	Disabled		
	web-coldfusion.rules	Disabled		
	web-iis.rules	Disabled		
	web-frontpage.rules	Disabled		
	web-misc.rules	Disabled		
	web-client.rules	Disabled		
	web-php.rules	Disabled		
	sql.rules	Disabled		
	x11.rules	Disabled		
	iome rulao	Dischlad		
		New File Delete File		
cted to is: 78.188.50.48		Labris Teknoloji		

Give the **name** of the file without any extension and click **Ok.** 



You can notice that the new file with the name **test** is **added** to the list.

RuleSets		
Rule File	Control/Status	
in a second seco		-
inappropriate.rules	Disabled	
bleeding.rules	Disabled	
rbn.rules	Disabled	
deleted.rules	Disabled	
content-replace.rules	Disabled	
compromised-BLOCK.rules	Disabled	
attack_response.rules	Disabled	
drop.rules	Disabled	
web-activex.rules	Disabled	
dshield.rules	Disabled	
rbn-BLOCK.rules	Disabled	
dshield-BLOCK.rules	Disabled	
malware.rules	Enabled	
botcc-BLOCK.rules	Disabled	
web_sql_injection.rules	Disabled	
botcc.rules	Disabled	
web.rules	Disabled	
game.rules	Disabled	
ddos-BLOCK.rules	Disabled	
geo-BLOCK.rules	Disabled	
ciarmy.rules	Disabled	
test.rules	Enabled	-

Select the required file form the list and click on **delete file** tab to remove the file form the list.

Rule File	Control/Status
inappropriate.rules	Disabled
bleeding.rules	Disabled
rbn.rules	Disabled
deleted.rules	Disabled
content-replace.rules	Disabled
compromised-BLOCK.rules	Disabled
attack_response.rules	Disabled
drop.rules	Disabled
web-activex.rules	Disabled
dshield.rules	Disabled
rbn-BLOCK.rules	Disabled
dshield-BLOCK.rules	Disabled
malware.rules	Enabled
botcc-BLOCK.rules	Disabled
web_sql_injection.rules	Disabled
botcc.rules	Disabled
web.rules	Disabled
game.rules	Disabled
ddos-BLOCK.rules	Disabled
geo-BLOCK.rules	Disabled
ciarmy.rules	Disabled
test.rules	Enabled

#### **Rulesets List**

Expand **Rulesets** from the Leftpane.

We can find different list of Rulesets.

Expand any one of the Rulesets as shown in the below figure.



Select any one of the Rule from the RuleList.

Sensor Settings Alert Settings					
Sensor 1  Sensor					
Service DO	Rule L	ist Search			
E Rulesets	SID	Message	Reference	Action	
eral local a bad-traffic bad-traffic tcp port 0 traffic	524	BAD-TRAFFIC tcp port 0 traffic		0	
data in TCP SYN packe	525	BAD-TRAFFIC udp port 0 traffic	bugtraq, cve, nessus		
<ul> <li>ip reserved bit set</li> <li>0 ttl</li> <li>bad frag bits</li> </ul>	526	BAD-TRAFFIC data in TCP SYN packet	url	() 🔋 🖂	
syn to multicast addres	528	BAD-TRAFFIC loopback traffic	uri		

Click on Rule.



the icon from the Action Tab to **Block , UnBlock or cancel** the selected

Sensor Settings Alert Settings					
Sensor 1 💌 Sensor 1 configuration: listening all interfaces					
Service Nunning	Rule L	ist Search			
🖹 😭 Rulesets 🔺	SID	Message	Reference	Action	
<ul> <li> <i>∂</i> local     </li> <li> <i>∂</i> bad-traffic     </li> <li> <i>d</i> port 0 traffic     </li> </ul>	524	BAD-TRAFFIC tcp port 0 traffic		l 🔋 🔤 🗖	
data in TCP SYN packe	525	BAD-TRAFFIC udp port 0 traffic	bugtraq, cve, nessus		
o ttl bad frag bits	526	BAD-TRAFFIC data in TCP SYN packet	url		
syn to multicast addres	528	BAD-TRAFFIC loopback traffic	url		
P Proto 77 Sun ND P Proto 103 PIM ⊕ 2 exploit	523	BAD-TRAFFIC ip reserved bit set			
⊞⊸a scan ⊞⊸a finger ⊞⊸a ftp	1321	BAD-TRAFFIC 0 ttl	uri, uri		
⊕…a telnet ⊕…a rpc ⊕…a rservices	1322	BAD-TRAFFIC bad frag bits			
terra dos terra dos terra dos terra dos	Rule B	lock			
web-cai	Rule a	pply to src		•	
	How a	pply(optional)		•	
⊕ a web-iis	Time(o	day:hr:min:sec) 00:00:00:00			
			🔘 Block 🚫 U	nblock 🚫 Cancel	

Click on the highlighted icon to **Start / Stop** the Rule.

### Red Light – Stop

**Green Light - Start** 

Sensor Settings Alert Settings							
Sensor 1  Sensor							
Service 🕥 🕕 📇 Apply	Service O O Rule List Search						
🖹 📲 🚱 Rulesets	SID	Message	Reference	Action			
<ul> <li>a local</li> <li>a bad-traffic</li> <li>a top port 0 traffic</li> </ul>	524	BAD-TRAFFIC tcp port 0 traffic					
data in TCP SYN packe	525	BAD-TRAFFIC udp port 0 traffic	bugtraq, cve, nessus				
<ul> <li>Ip reserved bit set</li> <li>0 tti</li> <li>bad frag bits</li> </ul>	526	BAD-TRAFFIC data in TCP SYN packet	url				
syn to multicast addres	528	BAD-TRAFFIC loopback traffic	url				
IP Proto 77 Sun ND IP Proto 77 Sun ND IP Proto 103 PIM	523	BAD-TRAFFIC ip reserved bit set					
er a scan er a finger er a fip	1321	BAD-TRAFFIC 0 tti	uri, uri				
e a telnet e a rpc e a rservices	1322	BAD-TRAFFIC bad frag bits					
i dos							

Click on the highlighted icon to redirect to the reference URL which is specified in the list.

Sensor Settings Alert Settings							
Sensor 1  Sensor							
Service Running	Rule L	ist Search					
🖮 💼 Rulesets 💽	SID	Message	Reference	Action			
a local a dotal a dotal a dotal bad-traffic bad-traffic	524	BAD-TRAFFIC tcp port 0 traffic		l 🔋 🖻 🗖			
data in TCP SYN packe	525	BAD-TRAFFIC udp port 0 traffic	bugtraq, cve, nessus				
0 ttl	526	BAD-TRAFFIC data in TCP SYN packet	url				
syn to multicast addres	528	BAD-TRAFFIC loopback traffic	url				
IP Proto 77 Sun ND IP Proto 103 PIM	523	BAD-TRAFFIC ip reserved bit set					
era scan era finger era finger	1321	BAD-TRAFFIC 0 tti	url, url				
e a telnet e a rpc e a rservices	1322	BAD-TRAFFIC bad frag bits					
i dos				<b>\</b>			

Click on Apply tab to apply the modified settings in Rulesets tab.


Click on **Ok** to save the changes.



Click on the Start tab as shown in the screen to start the IDS Service for chosen sensor

Service	RuleSets	
Intrusion Detection System	Rule File	Control/Status
Network Settings	local.rules	Disabled 🔺
Interface	bad-traffic.rules	Disabled
🗄 🎯 Rulesets	exploit.rules	Disabled
	scan.rules	Disabled
	finger.rules	Disabled
	ftp.rules	Disabled

Below screen appears stating that Starting IDS service is in progress.

Labris IDS	×
Starting IDS service for chosen sensor.	

Click on the **Stop** tab as shown in the screen to stop the IDS Service for chosen sensor.

Service Running	RuleSets		
Intrusion Detection System     Settings	Rule File	Control/Status	
Network Settings	local.rules	Disabled	
lnterface	bad-traffic.rules	Disabled	
🗄 👹 Rulesets	exploit.rules	Disabled	
	scan.rules	Disabled	
	finger.rules	Disabled	
	An autor		

Below screen appears stating that Stopping IDS service is in progress.



# **104.** Alert Settings

In the Alert tab we can find options like Mail Alert Settings ,Report Mails and Alerts.

Sensor Settings Aleri	Settings	
Mail Alert Settings		
Sender mail address: The mail a Administrator Mail: Alert mails v SMTP server: IP address of the	address that is used to post alerts by the ids mail alert service. vill be sent to this address. · SMTP server in the network.	
Sender mail adress	ids@labristeknoloji.com	
Administrator mail adress	admin@labristeknoloji.com	
SMTP host	smtp.example.com	
Mail Alert Service Status: F	Running	
Report Mails		
To: admin@labristekr	noloji.com	
Schedule: Every Day	00:00	
Alerts		
IDS alert duration on databas	e (Day)	15 🔹
		Save

## **Mail Alert Settings**

Give the inputs in the below fields.

Mail Alert Settings Sender mail address: The mail address that is used to post alerts by the ids mail alert service. Administrator Mail: Alert mails will be sent to this address. SMTP server: IP address of the SMTP server in the network.			
Sender mail adress	Sender mail adress ids@labristeknoloji.com 1		
Administrator mail adress	Administrator mail adress admin@labristeknoloji.com		
SMTP host smtp.example.com 3			
Mail Alert Service Status: Running			

1	Sender mail address	In this field give the sender mail address
2	Administrator mail address	In this field give the administrator mail address
3	SMTP host	In this field give the details of the SMTP server

### **Report Mails**

In the Report mails tab specify the **To address** and **Schedule time** to send mails.

Report Mails	1	
To:	admin@labristeknoloji.com	
Schedule:	Every Day 0100 🜩	

#### Alerts

In the Alerts tab, we can change the IDS Alert Duration depending on the requirement.

ID:	S alert duration on database (Dav)

## Click on save tab to save the modified settings

Sensor Settings Alert	Settings	
Mail Alert Settings		
Sender mail address: The mail a Administrator Mail: Alert mails w SMTP server: IP address of the	address that is used to post alerts by the ids mail alert service. vill be sent to this address. sMTP server in the network.	
Sender mail adress	ids@labristeknoloji.com	
Administrator mail adress	admin@labristeknoloji.com	
SMTP host	smtp.example.com	
Mail Alert Service Status: R	Mail Alert Service Status: Running	
Report Mails		_
To: admin@labristekr	noloji. com	
Schedule: Every Day	þ1:00 🗘	
Alerts		
IDS alert duration on databas	e (Day)	5 🗘
		Save

## MESSAGING

Right click on Messaging, Select Connect.

15 🗘



### 105. Domains

When we get connected to Messaging, we can notice **Domains** in the right pane.



### Domain

Click on Add tab to add new Domain to Messaging.

🔁 Mesg2	Domain	De	scription 🛛 📌 🦨 Add
Services	Labris.com	Testing	
🗄 🚭 Configuration	kralsensin.com		- Delete
		· · · · · · · · · · · · · · · · · · ·	🥟 Modify

Domain Add tab appears.

Type the **name of domain** and give information regarding Domain in the **Description** column.

Click on Add tab.

Domain Add	>	<
Name:	labristeknoloji.com	1
	Sample	1
Description:		
	Add Cancel	

Below screen appears stating that Adding Domain process is in progress.

Add Domain	×
Please wait	

In the below screen, we can notice new Domain added.

Mesg2	Domain	Description	🛟 Add
	Labris.com	Testing	😢 Delete
🗄 🖓 Configuration	kralsensin.com		~ Delete
	labristeknoloji.com	Sample	🥖 Modify
			·

Click on **Modify** tab to make any changes to the Domain.

Image: Configuration	Domain Labris.com kralsensin.com labristeknoloji.com	Description Testing Sample	🗳 Add 🗶 Delete 📝 Modify

Domain Edit tab appears, we can modify Description of the Domain and click on Add tab.

Domain Edit		×
Name:	labristeknoloji.com	]
	test domain	1
Description:		
		1
	Add Cancel	

In the below screen, we can notice changes made to the Domain.

Description	🔮 Add
Testing	Selete
	A Delete
test domain	🧪 Modify
	Description Testing test domain

Select the Domain and click on **Delete** tab.

Domain	Description	🗳 Add
Labris.com	Testing	😤 Delete
kralsensin.com		- Delete
labristeknoloji.com	test domain	🥖 Modify
	·	

Delete Domain tab appears stating Are you sure to delete the domain? Click on Delete tab.



Below screen appears stating that Deleting Domain process is in progress.

Delete Domain	×
Please wait	

When we click on Domain in the right pane, details of that particular domain is displayed.



#### **All Users**

When we expand domain, we can find options like All Users, Aliases, Groups



Select All Users, Click on Add tab to add new User.

When we click on Add tab, Message is displayed stating **Please create a group before adding new users!** 

Click Ok.

Before adding new user, we must create a Group in the domain.

Mesg2	User Na
All Users	Username First Name Last Name 🍇 List
Groups	Add
All Users	Z Delete
✓ Aliases Groups ✓ Services Configuration	Please create a group before adding new users!

Select Groups and click on Add tab.

🔁 Mesg2	🖨 Add
A labristeknoloji.com	🗶 Delete
All Users	Modify
All Users	
→ Y Aliases → S Groups	
Services	
term 🕤 Configuration	

Group Add tab appears, Type the name of the Group and give the information regarding Group in the Description column.

Click on Add tab.

Group Add		
Name: Smith		
new group in the domain labristeknoloji.com Description:		
Add Cancel		

In the below screen, we can notice new Group added to the Domain.



Now select All Users and click on Add tab.

₩esg2 = Domains	User Na 🔻 🔍 Search	
All Users	Username First Name Last Name	🍇 List
Haliases Haliases Groups		🖓 Add
All Users		🔀 Delete
In Aliases In Sector 1 and a sector 1 an		🥖 Modify
<ul> <li>✓ Services</li> <li>I → S Configuration</li> </ul>		

Add New User tab appears.

Add New User	×
User Name:	James 1
First Name:	William 2
Last Name:	James 3
Title:	SmithGroupUser 4
Group:	Smith 🔻 5
Description:	testuser 6
Employee Number:	030 7
Telefon Number:	9959496730 8
Alternative E-mail:	James.William@rediff.com 9
Quota:	Total Size: 30 10 B 🔻
Quota.	Number of emails: 2 11
Forwarding:	12
Password:	•••••• 13
Re-type Password:	••••••• 14
	Ok Cancel

These are the inputs to add New User.

1	User Name	Type the User Name
2	First Name	Type the First Name
3	Last Name	Type the Last Name
4	Title	Give the Title of the User
5	Group	Choose Group from the drop down list
6	Description	Give the Description of the User
7	Employee Number	Type Employee Number
8	Telephone Number	Type the Telephone Number
9	Alternative E-mail	Give the Alternate E-mail Address
10	Total Size	Choose the required Size
11	Number of emails	Type the Number of emails
12	Forwarding	Give the Forwarding E-mail Address if necessary
13	Password	Give the Password for the User
14	Re-type Password	Re-type Password for Confirmation.

Adding User process is in progress.

Add User	×
Please wait	

In the below screen we can notice New User added to All Users.

Mesg2	User Na 🔻		🔍 Search
All Users	Username	First Name	Last Name
Aliases	James	William	James
E Groups			

Select the User and click on **Modify** tab to make any changes to the User.

₩esg2 → → Domains	User Na 🔻		Search	
All Users	Username	First Name	Last Name	🍇 List
Aliases	James	William	James	👍 Add
A kralsensin.com				🔀 Delete
Aliases				🥖 Modify

Modify User tab appears.

Except User Name all the remaining fields can be modified.

Click Ok.

Modify User	_				×
User Name:	James				
First Name:	William				
Last Name:	James				
Title:	SmithGroupUser				
Group:	Smith 💌				
Description:	testuser				
Employee Number:	030				
Telefon Number:	9959496730				
Alternative E-mail:	James.William@rediff	.com			
Quality	Total Size:	30000			в 🔻
Quota.	Number of emails:	2			]
Forwarding:	Williams.lieo@gamil.co	om			
Password:					
Re-type Password:					
			Ok	Ca	ancel

Select User and click on Delete tab to delete an User.



Delete User tab appears stating Are you sure to delete the Users below? Click on Delete tab.

Delete User	×
Are you sure to delete the users below?:	
William James <james@labristeknoloji.com></james@labristeknoloji.com>	
Delete Cancel	

Deleting User process is in progress.

Delete User	×
Please wait	

## Aliases

Select Aliases and click on Add tab.



Add Aliases tab appears.

Type the Address and Aliases.

Click on Add tab.

Add Alias		×
Address:	Asmith	@labristeknoloji.com
Aliases:	Asmith@labristeknoloji.com	
	C.	Add Cancel

Adding Alias process is in progress.

×

In the below screen, we can notice New Alias added.

Mesg2	Address	Aliases
ang Domains	Christina@labristeknoloji.com	Christina@labristeknoloji.com
All Users	Asmith@labristeknoloji.com	Asmith@labristeknoloji.com
- T Aliases	T	
Groups		

Select the Alias and click on **Modify tab** to make any changes t the Alias.

Mesg2	Address	Aliases	
A labristeknoloji.com	Asmith@labristeknoloji.com	Asmith@labristeknoloji.com	🎔 Delete
All Users Aliases Croups A kralsensin.com Services Configuration	Christina@labristeknoloji.com	Christina@labristeknoloji.com	Modify

Modify Alias tab appears, we can modify Aliases column and click on Modify

Modify Alias	3	×
Address:	Asmith@labristeknoloji.com Asmith@labristeknoloji.com	
Aliases:		
	Modify Cancel	

Select the Alias and click on **Delete tab** to delete an Alias.



Delete Alias tab appears, click on Delete.



Deleting Alias process is in progress.

Delete Alias	×
Please wait	

In the below screen, we can notice Aliases deleted.

Mesg2  Domains  Domains  Albristeknoloji.com  Aliases  Groups  Akralsensin.com  Services  Configuration	Address asmith@labristeknoloji.com	Aliases asmith@labristeknoloji.com	Add Relete
---	---------------------------------------	---------------------------------------	------------

### Groups

Select Groups and click on Add tab.



Group Add tab appears.

Type the Name of the Group and give information regarding Group in the Description column.

Click on Add t	ab.	
Group Add		X
Group Add		
Name:	labris	
Description:	This is belong to labris users	
	Add Cance	

In the below screen, we can notice New Group added.



Select the Group and click on Modify tab.



Modify Group tab appears ;we can modify Description of the Group and click **Ok**.

Modify Group		×
Modify Group		
Group:	labris	
Description:	This is belong to labris teknoloji users	1
	OK Cancel	

Select the Group and click on **Delete tab**.



Delete Group tab appears stating Are you sure to delete the group below? Click on Delete tab.

Delete Group	×						
Are you sure to delete the group below?							
labris@labristeknoloji.com							
Delete							
Delete	Cancer						

### 106. Services

Services help us to know the status of the Messaging. It also enables us to start, stop the Service.



Select Services and click on the highlighted icon to the stop Service.



Mesg2 tab appears stating Stopping service, Please wait...

Stopping services process is in progress.

mesg2	×
Stopping service, please wait	

In the below screen, we can notice mes2 Service Status: Stopped.



Select Services and click on the highlighted icon to the start the Service.



Mesg2 tab appears stating Starting service, Please wait...

Starting Services process is in progress.

mesg2	×
Starting service, please wait	

In the below screen, we can notice mes2 Service Status: Running.



Select Services and click on the highlighted icon to the Reload Service.



Mesg2 tab appears stating Reload settings, please wait...

Reload settings process is in progress.



In the below screen, we can notice mes2 Service Status: Reloaded.





When we expand Configuration tab only General is displayed.

Click on General tab, Host Name and Domain Name are appeared.

Click on Save tab.

🔁 Mesg2	Host Name: mail.kralsensin.com
Services	Domain Name: kralsensin.com
General	Save

Saving General Configuration process is in progress.

Г



Below screen appears stating General configuration settings saved, Click Ok.



## **Load Balancer**

Right click on Server Load Balancer, select connect.



When we get connected to Server Load Balancer below screen appears.

Confi	Configuration Global Monitor								
Externa	Externally advertised services								
Add	External Address Port Scheduling Method Protocol								
Del	20.20.10.1	80	Weighted lea	ast connectio	n	TCP			
Upd	Upd								
	External IP address       Port       Connection scheduling method         20.20.10.1       80 <ul> <li>Weighted least connection</li> <li>Weighted round robin</li> <li>Round robin</li> <li>Least connection</li> </ul>								
Internal	I servers for selected external se	ervice							
<u>A</u> dd	Internal address	Port	Weight	Check Ti	meout	Che	eck Port		
<u>D</u> el	13.13.1.90	81	2	19	8	0			
Upd         Port         Weight         Check Timeout         Check Port           13.13.1.90         81         2         19         80									
	Server status 🌒 💶 🖸								

## **108.** Configuration

Load balance service open to outside servers, outside-in line with the demands of a specified weight values is used to send the request packets to servers.

For example, there is a web site, and you experience performance issues on the server because of the intense traffic. In such cases, you can use the same web resources can come in a second web server and load balance property between the two servers can share a server densities according to the packages.

In the below screen, we can notice external source Address.

In the internal servers field we can find two piece of the same source files in the background using the server providing the same background via request packets on port 443, respectively one among them, is the intensity of the request packet weight.

Labris Management Console							- 🗆 🗙
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>M</u> odule <u>A</u> bo	out						Help
	Con	figuration Global Monitor					
🖃 聞 Server	Exter	nally advertised services					
■ 78.188.50.48:4000	Add	d External Address			Port	Scheduling Method	Protocol
System	Del	0.0.0.0		443	3	Weighted least connection	TCP
Network Settings	Upo	d					
Firewall							
Filter							
Antispam/Antivirus							
St Messading		Estamol ID address				Ded. G	
Server		0.0.0.0				443	Weighted least connection
& License		Failback IP address				Port	Weighted reast connection
							weighted round robin
		Persiste					Round robin
						C	) Least connection
	- Interr	al servers for selected external service					
	Ado	i Internal address	Port	Weight		Check Timeout	Check Port
	: Del	192.168.168.11	443	1	15	443	
	Upo	d 192.168.168.12	443	1	15	443	
			Deat			Check Timesud	Charl Part
	192	2.168.168.11	443		1	15	443
	Servi	ce					
							Server status 🔮 💶 ڬ

### **Externally Advertised Services**

It enables us to Add, Delete and Update Externally advertised services

Confi	iguration Global Monitor				
Externa	ally advertised services				
Add	External Address	Port	Sched	uling Method	Protocol
Del	0.0.0.0	80	Weighted round r	obin	TCP
Upd	-				
	External IP address		- Port -	- Connection scheduling	method
	0.0.0.0		80	Weighted least c	onnection
	Failback IP address		Port	Weighted round	robin
				Reund robin	
[	Persiste			Round robin	
				<ul> <li>Least connection</li> </ul>	1

To add new service.

Mention External IP address and its Port number.

Mention Failback IP address and its Port number.

Choose the type of the Connection scheduling method and enter Persiste value.

After providing all the inputs, click on **Add** tab.

Coni	iguration Global Monitor				
Extern	ally advertised services				
Add	External Address	Port	Schedu	iling Method	Protocol
Del	0.0.0.0	80	Weighted round ro	obin	TCP
Upd					
<u> </u>	-				
	External IP address		Port	Connection scheduling	method
	11.11.11.1		80	Weighted least of	connection
	Failback IP address		Port	Weighted round	robin
~	10.10.10.1			Round robin	
	Persiste			Least connection	
	2			Cease connection	

### **Connection scheduling methods**

These are four types of server load balancing methods which are also known as "scheduling methods" or "algorithms".



## **Round Robin**

Round Robin is one of load balancing algorithm. It maintains a list of servers and forwards a new connection to the next server in the member list. Round robin is simple and effective method of distribution. This method functions best if all the servers have similar resource capacity.

## Weighted Round Robin

The weighted Round robin algorithm maintains a weighted list of servers and forwards new connections in proportion to the weight of each server.

#### Least connection

Least Connection is one of load balancing algorithm. This Algorithm maintains a record of active server connections and forwards a new connection to the server with least number of active connections. Least connection method functions best in environments where the servers have similar capabilities.

#### Weighted Least connection

The weighted least connection algorithm maintains a weighted list of application servers with their number of active connections and forwards a new connection to an application server based on a combination of its proportion to the weight and number of active connections. Like the least connections methods, these load balancing methods select pool members or nodes based on the number of active connections. This method work best in environments where the servers have different capacities.

In the below screen, we can notice New service added.

Externally advertised services							
Add	External Address	Port	Scheduling Method	Protocol			
Del	0.0.0.0	80	Weighted round robin	TCP			
Upd	11.11.11.1	80	Weighted least connection	TCP			

### Select the service and click on **Delete tab**.

ſ	Confi	iguration Global Monitor				
Γ	Externa	ally advertised services				
	Add	External Address	Port	Schedu	uling Method	Protocol
	Del	0.0.0.0	80	Weighted round r	obin	TCP
	Upd	11.11.11.1	80	Weighted least co	onnection	TCP
	[	External IP address		Port	Connection scheduling	method
		0.0.0.0		80	Weighted least of	connection
	_ [	Failback IP address	Port     Weighted rour		robin	
		- Persiste			Round robin	
		5			Least connection	n

To Update the service, Select the service.

We can modify External IP address and its port number, Connection scheduling method type. After making necessary changes, Click on **Update tab**.

dd	External Address	Port	Scheo	luling Method	Protoco
el 11.11	.11.1	80	Weighted least o	connection	TCP
pd					
-					
-					
Externa	al IP address		Port	Connection schedulir	ng method
Externa 20.20.1	al IP address		Port 80	Connection schedulir	ng method
Externa 20.20.1	al IP address 10.1 ck IP address		Port 80 Port	Connection schedulin Weighted leas	ng method

In the below screen, we can notice Updated server.

Externally advertised services							
Add	External Address	Port	Scheduling Method	Protocol			
Del	20.20.10.1	80	Weighted least connection	TCP			
Upd	2						

## **Internal Servers for Selected External Service**

## **Internal Address**

It enables us to Add, Delete and Update Inter server for selected external service.

Internal	ternal servers for selected external service							
<u>A</u> dd	Internal address	Port	Weight	Check Timeout	Check Port			
<u>D</u> el								
Upd								
- Intern	al address	Port		Veight Check Timeou	ut Check Port			

To add Internal server.

Mention Internal address, port number, weight, Check timeout and Check port. After providing all inputs click on **Add tab**.

Internal ser	vers for selected external serv	ice				 
Add	Internal address	Port	Weight	Check 1	Fimeout	Check Port
Del						
Und						
- laternal /	ddrore	Bort		Voiabt	- Chack Timory	 - Chook Port
102 168	10 5	80		2	12	 80
192.100.	10.5	00		2	12	00

In the below screen, we can notice Internal server added.

Interna	Internal servers for selected external service						
<u>A</u> dd	Internal address	Port	Weight	Check Timeout	Check Port		
Del	192.168.10.5	80	22	12	80		
Upd							

Select the server and click on **Delete** tab.

dd	Internal address	Port	Weight	Check Timeout	Check Port
)el	192.168.10.5	80	22	12	80
nd	10.10.0.1	81	1	20	81
20					
ntern	al address	Port		Weight Check Tim	eout Check Port

To Update the server, Select the server.

We can modify internal IP address, Port, Weight, Check Timeout and Check Port.

After making necessary changes, Click on **Update** tab.

Internal	servers for selected external servi	ce					
<u>A</u> dd	Internal address	Port	Weight	Check	Timeout		Check Port
<u>D</u> el	192.168.10.5	80	22	12		80	
Upd							
- Intern		Bort	- 1	Voiabt	- Chack Timoo	.+	- Chook Port
13.13	3.1.90	81	2	veign	19		80
						<u> </u>	

In the below screen, we can notice Updated server.

Interna	ernal servers for selected external service					
<u>A</u> dd	Internal address	Port	Weight	Check Timeout	Check Port	
<u>D</u> el	13.13.1.90	81	2	19	80	
Upd						
	1					

### Service

Service tab enables us to know the status of the service.

Service	Server status 🔵	

Click on the highlighted icon to stop the service.

- Service	
	Server status 🔵 🔲 匞

In the below screen, we can notice Red color status which indicates Server stopped.

- Service		
	Server status 🌒 💶 🖻	

Click on the highlighted icon to start the service.

- Service		
	Server status 🔴	

In the below screen, we can notice Green color status which indicates Server stopped.

- Service	
Service	Server status 🌒 💶 ව

## 109. Global

## **Global Settings**

Click on Global tab.

🔢 Labris Management Console	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>M</u> odule <u>A</u> bout	
	Configuration Global Monitor
Server 78.188.50.48:4000 Ver Management System Network Settings Firewall VPN Filter Matispam/Antivirus IDS/IPS Messaging Server	Global Settings Notification Email admin@server.com Notification Email From root@server.com SMTP Server mail.iliskisel.idealteknoloji.com Update
Server Load Balancer Conse	

It enables us to view and change the Global Settings.

Configuration Clobal Monitor
Global Settings
Notification Email admin@server.com
Notification Email From root@server.com 2
SMTP Server mail.iliskisel.ideatteknoloji.com
Update

These are the inputs for **Global**.

1	Notification Email	Give the Notification Email address
2	Notification Email From	Give the From address Notification Email
3	SMTO Server	Give the SMTO Server address

Click on Update tab.

Configuration Global Monitor
Global Settings
Notification Email admin@server.com
Notification Email From root@server.com
SMTP Server mail.iliskisel.idealteknoloji.com
Update

## 110. Monitor

### **Service Monitor**

## Select Monitor tab

🔡 Labris Management Console		- 🗆 🗙
<u>File Edit View M</u> odule <u>A</u> bout		<u>H</u> elp
File Edit View Module About	Configuration Global Monitor	<u>H</u> elp
BDS/IPS Berver Load Balancer Iccense		

Click on Update tab to update the information

Configuration Global Monitor	
Service Monitor	Update

You can notice that information is updated in this tab

Configuration Global Monitor	
C Service Monitor	
IP Virtual Server version 1.2.1 (size=1048576)	Update
Prot LocalAddress:Port Scheduler Flags	
-> RemoteAddress:Port Forward Weight ActiveConn InActConn	
TCP 20.20.10.1:80 wic	
*********	
IPVS connection entries	
pro expire state source virtual destination	

## License

Right click on License and select **connect**.



## **New License**

Click on **New License**, Information regarding License is being displayed.



Click on Get Hardware Information button.

🕎 Labris Management Console	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>M</u> odule <u>A</u> bo	ut
	🔁 New License 🚸 Install License
Server T 78.188.50.48:4000 User Management System Network Settings Firewall VPN Filter Sticspom/Aptivirus	Click on the "Get Hardware Information" button. The hardware information will be gathered from the server. Copy this information and send it to <b>license@labristeknoloji.com</b> .
IDS/IPS Messaging Server	Hardware Info = Not known yet
License	Copy in clipboard
	Remaining license time (days): 39 License expire date: 24/02/2014 Update license expire date: 24/02/2014 DB update license expire date: 24/02/2014 Support expire date: 24/02/2014

In the below screen, we can notice Hardware Information gathered from server is displayed.

😢 New License 🕪 Install License
Click on the "Get Hardware Information" button. The hardware information will be gathered from the server. Copy this information and send it to <b>license@labristeknoloji.com</b> .
Hardware Info = c7c12aa3dab750d5cf45de0dda0dd9a590af7fe6
Copy in clipboard
Remaining license time (days): 39 License expire date: 24/02/2014 Update license expire date: 24/02/2014
DB update license expire date: 24/02/2014 Support expire date: 24/02/2014

### **Install License**

Enter file name or choose **Open file** if we have a license file.

Signature of the file should be mentioned or choose **Open file** if we have a Signature and click on **Send the file to the server**.

Labris Management Console	- 🗆 X
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>M</u> odule <u>A</u> bout	<u>H</u> elp
New License 🔶 Install License	
Server	
WPN     > Open File       Antispam/Antivirus     File:       DS/IPS     > Open File       Messaging     > Signature	
Load Balancer    Send the file to the server	
Note For License file, please request from the service provider.	
111. Glossary	

DHCP	Dynamic Host Configuration Protocol
DNAT	Destination Network Address Translation
DNS	Domain Name System
DOS	Denial of service
DDOS	Distributed Denial of service
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
LMC	Labris Management Console
L2TP	Layer 2 Tunneling Protocol
MIME	Multi Purpose Internet Mail Extensions
NAT	Network Address Translation
PAT	Port Address Translation
QOS	Quality of service
SNAT	Secure Network Address Translation
SSL VPN	Secure Socket Layer Virtual Private Network
ТСР	Transmission Control Protocol
UDP	User Datagram Protocol
UTM	Unified Threat Management
VPN	Virtual Private Network
WAN	Wide Area Network
WAUTH	Wireless Authentication

# 112. Labris Firewall Messages

_lfp_ DROP IN ethN OTHER SRC	Blocking occurred because the source address of the packets incoming from an interface which is defined as external interface overlaps with either the network address of an internal interface or the internal networks defined under this internal interface.
_lfp_ DROP IN ethN 127.x SRC	Blocking occurred because the source address of a packet incoming from external interface belongs to 127.0.0.0/8 network.
_lfp_ DROP IN ethN BCAST SRC	Blocking occurred because the source address of a packet incoming from external interface belongs to Broadcast type.
_lfp_ DROP IN ethN BCAST PKT	Blocking occurred because the packet type of a packet incoming from external interface is Broadcast.
_lfp_ DROP IN MNG FWD	The packet forwarding process is blocked because the relevant interface has been defined as management interface.
_lfp_ DROP OUT MNG FWD	The packet forwarding process is blocked because the relevant interface has been defined as management interface.
_Ifp_ DROP IN MNG LMCS	Access to LMCS service port numbered 4000 from an interface except Management Interface is blocked.

	towards an interface except Management Interface is blocked.
_lfp_ DROP IN MNG WEB	Access to LRMS service port numbered 81 from an interface except Management Interface is blocked.
_lfp_ DROP OUT MNG WEB	Response access from LRMS service port numbered 81 towards an interface except Management Interface is blocked.
_lfp_ DROP IN MNG SSH	Access to SSH service port numbered 22 from an interface except Management Interface is blocked.
_lfp_ DROP OUT MNG SSH	Response access from SSH service port numbered 22 towards an interface except Management Interface is blocked.
_lfp_ DROP IN MNG IF	A management request connection which does not have management permission is blocked.
_lfp_ DROP OUT MNG IF	Response to a management request connection which does not have management permission is blocked.
_lfp_ DROP IN CONSOLE	Access to management ports is blocked.
_lfp_ DROP OUT CONSOLE	Access response from management ports is blocked.
_lfp_ DROP IN IF BAD SRCIP	Blocking occurred because the source address of the packets incoming from the relevant internal interface does not overlap with neither the network address of the internal interface nor the internal networks defined under this internal interface.
_lfp_ DROP IN ethN OWN SRCIP	B locking is done because the source address of the packet incoming from any overlaps with the IP address of one of the interfaces defined on the device.
_lfp_ DROP ICMP DoS	ICMP: Blocking occurred due to fragment or invalid session state.
_lfp_ DROP TCP DoS	TCP: Blocking occurred due to fragment or invalid session state.
_lfp_ DROP UDP DoS	UDP: Blocking occurred due to fragment or invalid session state.
_lfp_ DROP TCP Scan	TCP: Packets which are coming with scanning purpose and have packet flags which are expected to be absent normally, are blocked. FIN,URG,PSH / ALL SYN,RST,ACK,FIN,URG / ALL NONE / ALL ALL / ALL FIN / ALL SYN,RST / SYN,RST SYN,RST / SYN,RST tcp-option 64 tcp-option 128

_lfp_ DROP FRAG Scan	TCP Fragment Scan: Packets which are coming with scanning purpose and have packet flags which are expected to be absent normally, are blocked. FIN,URG,PSH / ALL SYN,RST,ACK,FIN,URG / ALL NONE / ALL ALL / ALL FIN / ALL SYN,RST / SYN,RST SYN,RST / SYN,RST tcp-option 64 tcp-option 128
_lfp_ drop sessionless pkt	Communication packets coming with a purpose other than opening session although there's no session are blocked.
_lfp_ DROP PKT Too small	UDP, TCP, ICMP packets which are smaller than they should be are blocked.
_lfp_ DROP LRMS Abuse	Extremely fast connection request to LRMS management service port is blocked.
_lfp_ DROP SSH Abuse	Extremely fast connection request to SSH management service port is blocked.
_lfp_ drop wauth input	Packets belonging to an unauthorized IP although WAUTH is active are blocked.
_lfp_ drop wauth forward	Packets belonging to an unauthorized IP although WAUTH is active are blocked.
_lfp_ DROP Default	Packets are blocked with the predefined blocking rule running after all the rules added by the user.
_lfp_ DefaultDENY	Packets are blocked with the predefined blocking rule running after all the rules added by the user.
_lfp_ Default_ ethN DENY	Packets are blocked with the predefined blocking rule running after all the rules added by the user.
_lfp_ Rule NNN ACCEPT	Permitted with the rule numbered NNN defined through LMC.
_lfp_Rule NNN DROP	Blocked with the rule numbered NNN defined through LMC.
_lfp_ Rule NNN REJECT	Actively rejected with the rule numbered NNN defined through LMC.
_lfp_ Rule NNN LOG	Only logged with the rule numbered NNN defined through LMC, no other process is performed.
_lfp_USER DEFINED PREFIX:	Logged with "USER DEFINED PREFIX" name specified by system administrator in a rule defined through LMC. ACCEPT, DROP state shall be specified by user.
_lfp_ IPMAC_MAXCONN:	Blocking occurred because the maximum number of connections assigned per IP is exceeded.
---	---
_lfp_ IPMAC_ABUSE	Blocking occurred because of contrary situation to IP-MAC mapping rules.
_lfp_i PROXYCONNLIMIT_DROP	Blocking occurred because number of sessions limit from internal clients to proxy system on the device is exceeded.
_lfp_ i FLOODCONTROL_DROP: _lfp_ f FLOODCONTROL_DROP	Temporary blocking occurred because an internal client exceeded the connection limits to a single destination.
_lfp_ i CLIENTFLOOD_DROP: _lfp_ f CLIENTFLOOD_DROP:	Temporary blocking occurred because an internal client exceeded the defined packet speed limits.
_lfp_ i CONNLIMIT_DROP: _lfp_ f CONNLIMIT_DROP:	Temporary blocking occurred because an internal client exceeded the defined number of sessions limits.

2013.7.31-3:33:12 USER IP <u>URL</u> *EXCEPTION* You_have_ privileged_username. GET 0 0 - 2 304 - GRUP - TCP_MISS/304 13 DEFAULT_PARENT/127.0.0.1	URL is permitted.
*SCANNED* POST	A sent web POST request is scanned and permitted. Blocking occurred because the source address of a packet incoming from external interface belongs to 127.0.0.0/8 network.
CONTENTMOD GET	The incoming content is replaced with regular expressions.
URLMOD GET	The outgoing request URL is replaced with regular expressions. For example with the purpose of forcing to Safe Search
*DENIED* Banned_file_extension:exe GET 0 0 Banned extension	Access is blocked due to a banned file extension (exe)
*DENIED*Banned_Site:_facebook.com GET	Access is blocked due to a banned site.
*DENIED* Banned_URL:_adfarm.mediaplex.com/ad GET	Access is blocked due to a banned URL.

*DENIED* Banned_MIME_Type:_video/mp4 GET 0 0 Banned MIME Type	Video (mp4) content is blocked due to a banned MIME Type.
*EXCEPTION*You_have_accessed_to_a_priviliged_site. GET	Access permission is given to a site that is added to exceptions.
*DENIED*Banned_irregular_expression_(URL)	Blocking occurred because URL matched with a blocked pattern.
*SCANNED**DENIED*Limit_of_blocked_expressions_is_exceeded:_50 -	Blocking occurred because web page content contains blocked expressions above the limit.
*SCANNED**DENIED*Banned_words_are_found	Blocking occurred because banned words are found in the web page content.

# **1. Labris Logview User Guide**

# **1. Introduction**

Labris Logview is a project which aims to make monitoring the system wide logs easier to system admins. User can see all logs for entire:

1	Firewall	Firewall Network Logs View
2	Access	Access Logs View
3	Operational	Operational Logs View
4	Administrative	Administrative Logs View
5	Wirelass Authentication	Wireless Authentication Logs View
6	IPMAC	IPMAC Logs View
7	DHCP	DHCP Logs View

8	Mail	Mail Logs View

system sources.

Logview allows user to define different log sources and regarding columns. Users can easily access new logs via "Live Monitoring" and reach older records for a given date range.

EWALL LOGS Cre	ate Time: 2014-06-03	08:12 Begin: 2014-06-03 00:00										٩
Date / Time	Source	Source User	Source Port	Destination	Destination User	Destinatio	Rule	Action	Protocol	Application	Mac Address	
014-06-03 08:12:31	192 168.0.165		45054	192 168.0.1		53	Ito Rule	ACCEPT	UDP	DNS DNS	08:00:27:80:1e:e0	
014-06-03 08:12:31	192 168.0 165		44804	192 168.0 1		53	Ifp Rule	ACCEPT	UDP	DNS DNS	08:00:27:80:1e:e0	
014-06-03 08:12:31	1.55.158.138		48917	192.168.1.2		25	Ifp Default	DROP	TCP	MARK=0x35	00:90:0b:2b:a0:94	
014-06-03 08:12:31	1.55.158.138		48917	192.168.1.2		25	Ifp Default	DROP	TCP	MARK=0x35	00:90:0b:2b:a0:94	
014-06-03 08:12:31	108.160.166.30		80	192.168.1.2		54867	Ito Rule	DENY	TCP		00:90:0b:2b:a0:94	
014-06-03 08:12:31	108.160.166.30		80	192.168.1.2		54867	Ifp Default	DROP	TCP	-	00:90:0b:2b:a0:94	
014-06-03 08:12:30	192 168 2 144	pelin@vssvk	137	192,168,2,255		137	Ifp Rule	ACCEPT	UDP	MARK=0x43	5c:19:dd:41:23:d8	
014-06-03 08:12:30	192 168 2 167	-	58472	192.168.0.1		53	Ifp Rule	ACCEPT	UDP	DNS DNS	00:15:65:5a:75:7b	
014-06-03 08:12:30	192.168.2.167		43040	194.27.44.55		123	Ifp_WAUTH_FORWARD	DROP	UDP	NTP_NTP	00:15:65:5a:75:7b	
014-06-03 08:12:30	192.168.1.2		33138	108.160.166.30		80	_lfp_ Rule	ACCEPT	TCP	-	-	
014-06-03 08:12:30	192.168.0.165		53930	192.168.0.1		53	_lfp_ Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:e0	
014-06-03 08:12:30	192.168.0.165		39453	192.168.0.1		53	_lfp_ Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:e0	
014-06-03 08:12:30	192.168.2.247		59078	192.168.2.1		3127	_lfp_Rule	ACCEPT	TCP	TCP_TCP	00:1e:8c:56:be:1c	
014-06-03 08:12:30	192.168.1.2		60609	5.9.147.90		80	_lfp_ Rule	ACCEPT	TCP			
014-06-03 08:12:30	192.168.2.149	-	1752	194.27.44.56		123	Ifp_WAUTH_FORWARD	DROP	UDP	NTP_NTP	00:15:65:52:23:db	
014-06-03 08:12:29	192.168.1.2		33138	108.160.166.30		80	_ttp_ Rule	ACCEPT	TCP	-		
014-06-03 08:12:29	192.168.2.144	pein@yssyk	137	192.168.2.255		137	_lfp_Rule	ACCEPT	UDP	MARK=0x43	5c:19:dd:41:23:d8	
014-06-03 08:12:29	95.6.72.25		34766	172.16.1.2		25	_ttp_ Rule	ACCEPT	TCP	SMTP_SMTP	00:90:0b:2b:a0:94	
014-06-03 08:12:29	192.168.0.165	-	37770	192.168.0.1		53	_lfp_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:e0	
014-06-03 08:12:29	192 168.0.165		48209	192 168.0.1		53	_ttp_ Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:e0	
014-06-03 08:12:29	192.168.2.144	pein@yssyk	55280	192.168.0.1		53	_lfp_Rule	ACCEPT	UDP	DNS_DNS	5c:19:dd:41:23:d8	
014-06-03 08:12:29	192.168.1.2		45547	195.175.39.39		53	_ttp_ Rule	ACCEPT	UDP			
014-06-03 08:12:29	192 168 2 144	pein@yssyk	1739	192 168 2 1		3127	_lfp_ Rule	ACCEPT	TCP	TCP_TCP	5c:19:dd:41:23:d8	
014-06-03 08:12:29	192 168 2 144	pelin@yssyk	1741	192 168 2 1		3127	_ttp_ Rule	ACCEPT	TCP	TCP_TCP	5c:19:dd:41:23:d8	
014-06-03 08:12:29	192.168.1.2	-	33086	173.194.70.102		80	_lfp_ Rule	ACCEPT	TCP	-	-	
014-06-03 08:12:29	192.168.0.139		51754	213.180.204.124		993	_lfp_WAUTH_FORWARD	DROP	TCP	IMAP_IMAP	e0:69:95:eb:e4:36	
014-06-03 08:12:28	93.186.122.9	-	45572	172.16.1.2		25	_lfp_ Rule	ACCEPT	TCP	SMTP_SMTP	00:90:0b:2b:a0.94	
014-06-03 08:12:28	192.168.0.190		43322	8.8.8.8		53	_lfp_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:5b:28:08	
014-06-03 08:12:28	192.168.2.144	pelin@yssyk	64835	192.168.0.1	-	53	_lfp_ Rule	ACCEPT	UDP	DNS_DNS	5c:19:dd:41:23:d8	
014-06-03 08:12:28	192.168.1.2		13314	195.175.39.39		53	_lfp_ Rule	ACCEPT	UDP	-		
014-06-03 08:12:28	192 168 2 144	pelin@yssyk	1735	173.194.70.113	-	443	_lfp_ Rule	ACCEPT	TCP	SSL_SSL	5c:19:dd:41:23:d8	
014-06-03 08:12:28	192.168.0.165	+	46489	192.168.0.1		53	_lfp_ Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:e0	
014-06-03 08:12:28	192.168.0.165		36701	192.168.0.1		53	_lfp_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:e0	
014-06-03 08:12:28	192.168.0.165	+	44055	192.168.0.1		53	_lfp_ Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:e0	
014-06-03 08:12:28	192.168.0.165		35754	192.168.0.1		53	_lfp_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:e0	
014-06-03 08:12:28	192.168.0.165	+	54602	192.168.0.1		53	_lfp_ Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:e0	
014-06-03 08:12:28	192.168.0.165		33736	192.168.0.1		53	_ttp_ Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:e0	
014-06-03 08:12:28	192.168.0.165	+	40605	192.168.0.1		53	_lfp_ Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:e0	
014-06-03 08:12:28	192.168.0.165		49518	192.168.0.1		53	_ttp_ Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:e0	
014.00.00.00.10.00	100 100 0 100		C7005	100 100 0 1		F 2	No. 19.44	ACCOUNT.	100	DNC DNC	00.00.77.00.10	

Logview Records table while streaming with some sample logs

Date / Time	Here	P	Mar Address	Destination	100	Desision	LITTLESS.	Contractor	
Date / Time	User	source	Mac Address	Destination	URL.	Decision	HIIIMISS	Category	
2014-06-03 08:23:33		192.168.0.166			http://192.168.0.1.85/login	"SCANNED"	TCP_DENIEDH03		
2014-06-03 08:23:33		192.168.0.166			http://192.168.0.1.85/logn	"SCANNED"	TCP_DENIEDI403		
2014-05-03 08:23:33		192.168.0.166			http://192.168.0.1.85.00gin	"SLANNED"	TCP_DENIEDI403		
2014-06-03 06:23:28		192.100.0.100			http://102.100.0.1.05/00/	-SCANNED	TCP_DENIEDH03		
2014-06-03 08:23:26		192.100.0.100			http://102.106.0.1.05/0001	"SCANNED"	TCP_DENIEDH03		
2014-06-03 08:23:28		192.168.0.166			http://102.166.0.1.85/login	"SCANNED"	TCP_DENIEDH03		
2014-06-03 08:23:23		192.168.0.166			http://192.168.0.1255kgin	"SLANNED"	TCP_DENIEDI403		
2014-06-03 08:23:22		192.168.0.166			http://192.168.0.1.85.logn	"SCANNED"	TCP_DENIED403		
2014-06-03 06:23:22		192.100.0.100		-	http://192.100.0.1.05k0gh	"SCANNED"	TCP_DENIEDH03		
2014-05-03 08:23:17		192.168.0.166			-mp://192.168.0.1255rogn	SCANNED.	TCP_DENIEDH03		
2014-05-03 08:23:17	-	192.168.0.166			- 100/192.168.0.1785/000	"SCANNED"	TCP_DENIED/403		
2014-06-03 08:23:17		192.168.0.166			ntp://192.168.0.1.85/logn	"SCANNED"	TCP_DENIED/403		
2014-06-03 08:23:12		192.168.0.166			http://192.168.0.1.85/logn	"SCANNED"	TCP_DENIEDH03		
2014-06-03 08:23:12		192.168.0.166			http://142.168.0.1.8540gn	"SCANNED"	TCP_DENIEDH03		
2014-06-03 08:23:07		192.168.0.166			http://192.168.0.125.http:/	"SCANNED"	TCP_DENIEDI403		
2014-06-03 08:23:07		192.168.0.166			http://192.168.0.1.85/logn	"SCANNED"	TCP_DENIED403		
2014-06-03 06:23:06		192.100.0.100			http://142.106.0.1.05/kg/h	"SCANNED"	TCP_DENIEDH03		
2014-05-03 08:23:01		192.168.0.166			http://142.168.0.1385/login	"SCANNED"	TCP_DENIEDI403		
2014-06-03 08:23:01		192.168.0.166			http://192.168.0.1365/login	"SCANNED"	TCP_DENIEDI403		
2014-06-03 06:23:01		192.100.0.100			http://192.100.0.1.05/kgm	"SLANNED"	TCP_DENIEDH03		
2014-06-03 08:22:56		192.108.0.100			http://142.166.0.1.65/kg/h	"SCANNED"	TCP_DENIEDH03		
2014-06-03 08:22:56		192.168.0.166			http://192.168.0.1.85/login	"SCANNED"	TCP_DENIEDH03		
2014-06-03 08:22:56		192.168.0.166			http://192.168.0.1.85.logn	"SCANNED"	TCP_DENIEDH03		
2014-06-03 06:22:51		192.100.0.100			http://192.106.0.1.05/kgin	"SLANNED"	TCP_DENIEDH03		
2014-06-03 08:22:51		192.168.0.166			http://142.166.0.1.85/login	"SCANNED"	TCP_DENIEDH03		
2014-06-03 08:22:46		192.168.0.166			http://142.168.0.1365/00jn	"SCANNED"	TCP_DENIEDI403		
2014-06-03 08:22:46		192.168.0.166			http://192.168.0.1.85.logn	"SCANNED"	TCP_DENIEDH03		
2014-06-03 06:22:41		192.100.0.100			http://192.106.0.1.05/kgin	"SLANNEL"	TCP_DENIEDH403		
2014-06-03 08:22:41		192.168.0.166			http://142.168.0.1.85nogn	"SCANNED"	TCP_DENIEDH03		
2014-06-03 08:22:36		192.168.0.166			http://142.168.0.1.85/login	"SCANNED"	TCP_DENIEDI403		
2014-06-03 08:22:36		192.168.0.166			http://192.168.0.1.85/logn	"SCANNED"	TCP_DENIEDI403		
2014-06-03 06:22:31		192.168.0.166			http://192.100.0.1/00/00/h	"SCANNED"	TCP_DENIED/403		
2014-05-03 08:22:31		192.168.0.166			Http://142.168.0.1785/ngin	"SCANNED"	TCP_DENIED/403		
2014-05-03 06:22:26		192.168.0.166			http://102.100.0.1.000000	-SCANNED*	TCP_DENIEDH03		
2014-06-03 06:22:21		192.168.0.166			http://192.168.0.1/85/kgin	"SCANNED"	TCP_DENIED/403		
2014-06-03 07/22/21		192.108.0.106			http://192.106.0.1.05/kgin	"SCANNEL"	TCP_DENIEDH03		
		192.168.0.166			http://192.168.0.1:85/login	"SCANNED"	TCP_DENIED/403		



# 2. Parts & Tools

Logview has some easy-to-use parts and useful tools:

5	Cabris						6					(d) Setting	* 🕤 Language *	6 Server Status.
							Firewall Logs	Access Logs	of Service	Logs 🔮 Ad	dministrative Logs 🖬 Wauth Logs	Mail Logs III IPMAC Lo	B XDHCP Logs	
Ì	FIREWALL LOGS	Create Time: 2014-06-03 16	52 Begin: 2014-06-03 00:00	1										<u>م</u> ۵ ×
<u> </u>	Date / Time	Source	Source User	Source Port	Destination	Destination User	Destinatio	Rule	Action	Protocol	Application	Mac Address		
(7)	2014-06-03 06:45:32	192.168.0.166		60728	192.168.0.187		8080	_lfp_Default	DROP	TCP		00:1e:8c:f4:47:11		A
$\sim$	2014-06-03 06:45:32	192.168.0.166		60729	192.168.0.187	100 C	8080	_ifp_Default	DROP	TCP		00:1e:8c:f4:47:11		
	2014-06-03 06:45:32	192.168.0.163		17500	255.255.255.255	-	17500	_ifp_Default	DROP	UDP		4c:72:b9:7c:55:11		
	2014-06-03 06:45:32	192.168.0.163		17500	192.168.0.255		17500	_fp_ Default	DROP	UDP		4c:72:b9:7c:55:11		
	2014-06-03 06:45:30	0.0.0.0	100 C	68	255.255.255.255	-	67	_fp_ Default	DROP	UDP		6a:1b:#:0b:69:61		
	2014-06-03 06:45:30	0.0.0.0		68	255.255.255.255		67 _	fp_IN_MNG_IF	DROP	UDP	DHCP_DHCP	6a:1b:#:0b:69:61		
	2014-06-03 06:45:30	0.0.0.0		68	255.255.255.255	-	67	_tp_Detault	DROP	UDP	-	6a:1b:#:0b:69:61		
	2014-06-03 06:45:30	0.0.0.0		68	255.255.255.255		67	Ip_IN_MNG_IF	DROP	UDP	DHCP_DHCP	6a:1b:#:0b:69:61		
	2014-06-03 06:45:29	192.168.0.163		57621	192.168.0.255	100 C	57621	_ifp_Default	DROP	UDP	100 C	4c:72:b9:7c:55:11		
	2014-06-03 06:45:28	0.0.0.0		68	255.255.255.255		67	_lfp_ Default	DROP	UDP		6a:1b:ff:0b:69:61		
	2014-06-03 06:45:28	0.0.0.0	1 C C C C C C C C C C C C C C C C C C C	68	255.255.255.255	-	67	Ifp_IN_MNG_IF	DROP	UDP	DHCP_DHCP	6a:1b:ff:0b:69:61		
	2014-06-03 06:45:28	192.168.0.23		17500	255.255.255.255		17500	_lfp_Default	DROP	UDP		10:60:4b:7e:81:87		
	2014-06-03 06:45:28	192.168.0.23		17500	192.168.0.255	-	17500	_tp_Detault	DROP	UDP		10:50:4b:7e:81:87		
	2014-06-03 06:45:27	0.0.0.0		68	255.255.255.255		67	_fp_Default	DROP	UDP		6a:1b:#:0b:69:61		
	2014-06-03 06:45:27	0.0.0.0		68	255.255.255.255	-	67	ID_IN_MNG_IF	DROP	UDP	DHCP_DHCP	68.10.0.00.69.61		
	2014-06-03 06:45:26	192.168.0.166		60/30	192.168.0.187		8080	_fp_Detaut	DROP	TCP		00:1e:8c:14.47:11		
	2014-06-03 06:45:26	192.168.0.166		60731	192.168.0.187	-	8080	_tp_Detaut	DROP	TCP		00:1e:8c:14:47:11		
	2014-06-03 06:45:24	192.168.0.166		60728	192.168.0.187		8080	_tp_Detaut	DROP	TCP		00:1e:8c:14:47:11		
	2014-06-03 06:45:24	192.168.0.166		60729	192.168.0.187	-	8080	_tp_Detaut	DROP	TCP		00:1e:8c:14:47:11		
	2014-06-03 06:45:22	192.168.0.166		60731	192.168.0.187		8080	_tp_Detault	DROP	TCP		00.16/80/14/47/11		
	2014-06-03 06:45:22	192.168.0.166		60/30	192.168.0.187		6060	_tp_ Detault	DROP	ICP		00:18:00:14:047:11		
	2014-06-03 06:45:20	192.168.0.158		5/621	192.168.0.255		5/621	_tp_ Detaut	DROP	UDP		e8:40:12.ec.ba:25		
	2014-06-03 06:45:20	192.168.0.166		60728	192.168.0.187		8080	_ifp_Default	DROP	TCP		00:1e:80:14:47:11		
	2014-06-03 06:45:20	192.168.0.166		60730	192.168.0.187		8080	_rp_Detaut	DROP	TCP		00/16/80/14/4/11		
	2014-06-03 06:45:20	192.168.0.166	1	60729	192.168.0.187		8080	_inp_ Default	DROP	TOP		00:16:00:14:47:11		
	2014-06-03 06:45:20	192.168.0.166		60731	192.100.0.107		8080	_inp_ Default	DROP	TCP		00.18:00:14:47:11		
	2014-06-03 06:45:19	102.100.0.100		00730	102 168 0 187		9090	_np_ Default	DROP	TCD		00.1=00.04/11		
	2014-06-03 06:45:19	192 168 0 166		60731	102 168 0 187	-	8080	_ip_Detauk	DROP	TCB		00.1e.0c.14.47.11		
	2014-06-03 06-46-18	192 168 0 166		60725	192 168 0 197		8080	to Default	DROP	TCP		00-14-94-14-17-11		
	2014-05-03-06-45-18	192 168 0 166		60728	192 168 0 187		8080	To Default	DROP	TCP		0014/8/16/2/11		
	2014-06-03 06-45-18	192 168 0 166		60720	192 168 0 187		8080	Ifo Default	DROP	TCP		00-1a-8e-14-47-11		
	2014-06-03 06-45-18	192 168 0 166		60728	192 168 0 187		8080	If Default	DROP	TCP		00-1a-8c-14-47-11		
	2014-05-03-06:45:18	192 168 0 166		60729	192 168 0 187		8080	Ifn Default	DROP	TCP		00-1e-8c-14-47-11		
	2014-05-03 05:44:04	0000		68	255,255,255,255		67	to IN MNG IF	DROP	UDP	DHCP DHCP	6x1b#0b5951		
	2014-06-03 06:44:02	00.00		68	255 255 255 255		67	to IN MNG IF	DROP	UDP	DHCP DHCP	6a 1b # 0b 69 61		
	2014-06-03 06:44:01	0.0.0		68	255,255,255,255		67	to IN MNG IF	DROP	UDP	DHCP DHCP	6a:1b:#0b:69:61		
	2014-06-03 06:43:36	0.0.0.0		68	224.0.0.1		67	to IN MNG IF	DROP	1 2	IGMP IGMP	76.37.66.23.33.87		
	2014-06-03 06:42:38	0000		68	255,255,255,255		67	to IN MNG IF	DROP	UDP	DHCP DHCP	6x1b#0b6961		
		0000		<b>C</b> 0	NET NET NET NET		17	-	0000	100	NUCE NUCE	A. 16406-2021		*
	¥ 4 4	Page 1 of 5 🕨 🖡	Streaming: ON										Displa	ying 1 to 50 of 203 items
Label	Lenvine vt 0.0.446												2013 © Labris N	marks. All rights reserved

Figure Parts & Tools on main display

# 1. Records tables

1	Show / Hide Column Fitering	Select Show or Hide Column Filtering
2	Export Filtered Records	Select Export Filtered Records
3	Remove Table	Select Remove Table



4	Table Length	Select Table Length
5	Backward Pages by 10	Select Backward Pages
6	Previous Page	Select Previous Page
7	Go to Page Number	Write Go to Page Number
8	Next Page	Go to Next Page
9	Forward Pages by 10	Select Forward Pages
10	Refresh The Table	Refresh The Table Button
11	Switch on/off	Switch on/off Live Monitoring



# 2. Live monitoring shortcuts

📥 Firewall Logs	🇰 Access Logs	o: Service Logs	😁 Administrative Logs	📑 Wauth Logs	🖂 Mail Logs	📰 IPMAC Logs	X DHCP Logs
1	2	3	4	5	6	7	8

1	Firewall	Firewall Network Logs View
2	Access	Access Logs View
3	Operational	Operational Logs View
4	Administrative	Administrative Logs View
5	Wirelass Authentication	Wireless Authentication Logs View
6	IPMAC	IPMAC Logs View
7	DHCP	DHCP Logs View
8	Mail	Mail Logs View

# 3 .Layout options

8			88
	1	23	4

1	Single View	Select Single View
2	Column View	Select Column View
3	List View	Select List View
4	Grid View	Select Grid View

# 4. Settings



1	Change Settings	Select Change Settings
2	Save Screen	Save Screen
3	Load Screen	Load Screen

5. Language selector



1	English	Select English Language
2	Turkish	Select Turkish Language

# 6 . Server status & service controller



1	Restart Services	Restart all Services

# 7. Sidebar



1	Dashboard	Select Dashboard for Dashboard Screen
2	All Logs	Select All Logs
3	CPU Usage	CPU Usage Info
4	RAM Usage	RAM Usage Info
5	Disk Usage	Disk Usage Info

#### **3. Instructions**

Logview is a web-based application and the only thing you could run it is a Web browser. We advice you to mostly use Chrome, Safari or Firefox. Logview does not support IE versions before 8.0.

Logview uses Websocket and most of near future Web technologies; therefore the browser you would use must support all these technologies.

## 4. Records Table

Records table shows records from your UTM device that is gathers all logs from defined sources. You can see any log data, which is gathered from given date range and given, source. You can access column filter feature just by clicking 1.1 Show / Hide column filtering button and you can make a search by typing any keyword regarding column data.

The picture shows a table that its column filter is not enabled yet:

ACCESS LOGS	Create Time: 2014-06-05 13:12 Begin:	2014-06-05 00:00						Q 🖺 🗙
Date / Time	User	Source	Mac Address	Destination	URL	Decision	HIT/MISS	Category Filter G
2014-06-05 13:13:	52	192.168.2.156				*EXCEPTION*Ayricalikli_bir_siteye_girdiniz.	TCP_MISS/200	kula
2014-06-05 13:13:	52	192.168.2.156				*SCANNED*	TCP_MISS/200	kula
2014-06-05 13:13:	52	192.168.2.156			The second second second second second second second second second second second second second second second se		TCP_MISS/304	kula
2014-06-05 13:13:	52	192.168.0.153			A A CONTRACTOR OF A REAL PROPERTY AND A REAL P	*EXCEPTION*Ayricaliki_bir_siteye_girdiniz.	TCP_MISS/206	kulla
2014-06-05 13:13:	52	192.168.2.161				*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13:	52	192.168.2.156					TCP_MISS/200	kulla
2014-06-05 13:13:	51	192.168.0.153			The statistic of a long decision has	*EXCEPTION*Ayricaliki_bir_siteye_girdiniz.	TCP_MISS/206	kulla
2014-06-05 13:13:	51	192.168.2.156				*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13:	50	192.168.2.156			and the second se	*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13:	50	192.168.2.156			and the state of the second second second second second second second second second second second second second	*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13:	50	192.168.2.156				*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13:	50	192.168.2.156			a second of the	*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13:	50	192.168.2.156			the second second second second second second second second second second second second second second second se		TCP_MISS/200	kulla
2014-06-05 13:13:	50	192.168.0.153		-	And shakes an even strategy and the	*EXCEPTION*Ayricaliki_bir_siteye_girdiniz.	TCP_MISS/206	kulla
2014-06-05 13:13:	50	192.168.2.156		-		*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13)	19	192.168.0.153	-	-		*EXCEPTION*Ayricaliki_bir_siteye_girdiniz.	TCP_MISS/206	kulla
2014-06-05 13:13:	19	192.168.2.156	-	-	THE R. H. R. Rolls in Long Street, 1		TCP_MISS/200	kulla
2014-06-05 13:13:	48	192.168.2.161	-	-	the last possible without the part of parts in the	*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13:	48	192.168.2.161			the second s		TCP_MISS/200	kulla
2014-06-05 13:13:	47	192.168.2.156	-	-	A REAL PROPERTY OF A REAL PROPERTY.		TCP_MISS/200	kulla
2014-06-05 13:13:	47	192.168.0.153			AND ADDRESS OF THE OWNER OWNER	*EXCEPTION*Ayricalikli_bir_siteye_girdiniz.	TCP_MISS/206	kulla
2014-06-05 13:13:	47	192.168.2.156	-	-	a service of the second of the second s	*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13:	47	192.168.2.156			And a second sec	*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13:	46	192.168.2.156		-	and the second se	*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13:	46	192.168.2.156			and the second second second	*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13:	46	192.168.2.156			the set of the set of	*SCANNED*	TCP_MISS/302	kulla
2014-06-05 13:13)	46	192.168.2.156			CONTRACTOR AND ADDRESS OF ADDRESS OF		TCP_MISS/200	kulla
2014-06-05 13:13)	16	192.168.2.156			the second second second second second second second second second second second second second second second se	*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13:	46	192.168.2.156			The second second in the state state of the		TCP_MISS/200	kulla
2014-06-05 13:13)	46	192.168.0.153				*EXCEPTION*Ayricaliki_bir_siteye_girdiniz.	TCP_MISS/206	kulla
2014-06-05 13:13)	46	192.168.2.156			the recence of the second seco	*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13)	46	192.168.0.198				*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13)	46	192.168.2.156			and the second se		TCP_MISS/200	kulla
2014-06-05 13:13)	16	192.168.2.156			the second second second second second second		TCP_MISS/200	kulla
2014-06-05 13:13)	46	192.168.0.163				*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13)	46	192.168.2.132			Contraction and the statement of	*SCANNED*	TCP_MISS/200	kulla
2014-06-05 13:13)	45	192.168.2.156			the start of the second start of the start o		TCP_MISS/200	kulla
2014-06-05 13:13)	45	192.168.2.156			the second statistics where it is an extension		TCP_MISS/200	kulla 🔻
								÷
🔻 📢 🍕	Page 1 of 990 🕨 🖗 🧐	Streaming: ON						Displaying 1 to 50 of 49457 items

And by clicking 1.1 Show / Hide Column Filtering button you will see the filters, even they are already filtered:

ACCESS LOGS Create Time: 2014-06-05 13:12 Begin: 2014-06-05 00:00						
Date / Time 🔻	User	Source	Mac Address	Destination	URL	Decision
🛗 Set Date Range	User	!=192.168.0.42	Mac Address	Destination	URL	scanne
2014-06-05 13:21:45		192.168.0.155			the second second second second	*SCANNED*
2014-06-05 13:21:44		192.168.6.173				*SCANNED*
2014-06-05 13:21:43		192.168.6.173			the state of the state of the state of the	*SCANNED*
2014-06-05 13:21:43		192.168.6.173			the same of the state of the second state of	*SCANNED*
2014-06-05 13:21:43		192.168.6.173	-		the second state of the se	*SCANNED*
2014-06-05 13:21:43		192.168.6.173				*SCANNED*
2014-06-05 13:21:43		192.168.6.173	-	-	A REAL PROPERTY AND A REAL PROPERTY.	*SCANNED*
2014-06-05 13:21:42		192.168.6.173			A service of the property of the service of	*SCANNED*
2014-06-05 13:21:41		192.168.6.173			And the second se	*SCANNED*
2014-06-05 13:21:41		192.168.6.173				*SCANNED*
2014-06-05 13:21:41		192.168.6.173			And the Construction of the second states	*SCANNED*
2014-06-05 13:21:41	hákan@vssvk	192.168.6.173			n haberturk.com/daler/2014/06/05/488693/daleri 200x200.pd?1401961075	*SCANNED*

It can be search by using some operators:

- "=" use it for define an equation such as for User column use like "user@domain" or type "=username@domain"
- "!=" use it for User column use like "user@domain" or type "=username@domain"
- "&&" use it for "and" keywords such as for User column use like "=user@domain && !=anotheruser@domain"
- "||" use it for "or" keywords such as for User column use like "=user@domain || !=anotheruser@domain"

In records table you can export your filtered data by clicking 1.2 Export filtered records as CSV

# or TXT file formatted.

-		http://techlaboratorv.net/ser	vice/notification	
Expo	ort			
	Export Type:		U CSV	
	File Name:	write a file name		
Evport				
Export				
-		http://techlaboratory.net/ser	vice/notification	
-	http://realti	me.services.disgus.com/api/2/t	thread/823237460?bust=4760	

And you can remove the table by clicking 1.3 Remove table button.

Records table also has a footer, which includes:

• record length: use it to set content length of a table by page 10, 15, 20, 30 and 50

	v
•	backward- forward buttons: use it to shift pages by 10 forward Por backward
•	previous- next buttons: use it to shift pages one by one
•	reload buttons: use it to reload the page if you think something goes wrong about the table

streaming on/off button: enable or disable stream, it is better to stop stream when filtering data.

Records tables also have nice user-friendly features. You can resize columns by pulling the next line to the column and leave it when you reach the size you want. Initially records tables have own predefined size to provide best-fit size for the data inside the column. You can also order historical records table just by clicking the header of the column you would like to sort by; and also you can show or hide columns by clicking the down-arrow on the column heading as show

# in figure.

Another feature tables have is "replacing columns". You can replace columns by drag and drop. Drag a column you want to move then drop to put where you want.

# 4.1. Real-time Monitoring

Logview provides a real-time monitoring for streaming logs. You can just click the shortcut buttons and it fires an event to create real-time logs monitoring tables.

14-06-05 00:00		
Source -		
=192.168.0.42    =192.16		
192.168.2.176		



1	Firewall Log	View All Firewall Logs
2	Access Logs	Internet Access Logs
3	Service Logs	Device Service Logs
4	Administrative Logs	Administrative Logs for This Device
5	Wireless Authentication Logs	Wireless Authentication Logs
6	Mail Logs	Mail Logs for SMTP, IMAP and POP3
7	IP-MAC Logs	IP AND MAC Address Logs
8	DHCP Logs	DHCP Logs

Real-time monitoring tables allow you to track real time logs. Even if you want to filter them then it still keeps streaming

# **Historical Logs**

🚳 Dashboard	>
🎫 All Logs	
😔 yssyk 🍾	
CPU Usage 6%	
RAM Usage 37%	
DISK Usage 8%	

Historical logs are all logs that are retrieved from older logs. You can create a historical records table from sidebar.

After you click the domain name you will see a window like below:

As we see in the figure, there are log sources and regarding fields which will be defined as columns when the table is created. We can select which column will be shown or hidden. In date range selection section, there are predefined date ranges 1 day, 3 days, 1 week. In another case, you can also select date range by manually.

Table			
Select Log Source	Firewall Logs Service Logs Wauth Logs IPMAC Logs	Access Logs     Administrative     Mail Logs     DHCP Logs	e Logs
Select Log Fields	<ul> <li>✓ Date / Time</li> <li>✓ Mac Address</li> <li>✓ Decision</li> <li>Host</li> <li>Response Code</li> <li>Client Host</li> <li>Method</li> </ul>	<ul> <li>✓ User</li> <li>✓ Destination</li> <li>✓ Undefined</li> <li>Domain</li> <li>User Agent</li> <li>Duration</li> </ul>	<ul> <li>✓ Source</li> <li>✓ URL</li> <li>✓ Category</li> <li>✓ Filter Group</li> <li>Size</li> <li>Mime Type</li> </ul>
Default Ranges:	1 day 3 days 1 w	veek	
From:	2014-05-29 16:09		
To:	2014-06-05 16:09		
CREATE TABLE			

Figure: Create Historical Log Table

Select Log Source	O Fi	Firewall Logs						Access Logs     Administrative Logs
	Su	Мо	Tu	We	Th 1	Fr 2	Sa 3	Mail Logs DHCP Logs
Select Log Fields	4 11 18 25 Time Hour Minu	5 12 19 26	6 13 20 27 16:09	7 14 21 28	8 15 22 29	9 16 23 30	10 17 24 31	er  v Source stination v URL sefined v Category nain v Fiter Group er Agent Size ration Mime Type
Default Ranges:	No	w				Do	one	
From:	2014-05-29 16:09							
To:	то: 2014-06-05 16:09							
CREATE TABLE								· · · · ·

Figure: Create Historical Log Table - Pick Date Range

## 5. Utilities

## 5.1. Settings

Settings section lets you change settings along Logview. By clicking 4.1 Change Settings you will able to set default behavior of columns to be shown or hidden.

If you check any field on this window, it will be shown in records table as shown column. If you uncheck a field, it will be hidden on the table.

urce	Settings Server Settings	Smtp Settings		
Q;	Please select default columns t	to be shown in table:		
Selec	t Log Source			
#	Firewall Logs	✓ Date / Time	Source	✓ Source User
		Source Port	Destination	Ø Destination User
	Access Logs	Destination Port	✓ Rule	✓ Action
		Protocol	Application	Mac Address
00	Service Logs	Host	Message	Sequence Number
		🗌 Туре	Code	TTL
쌸	Administrative Logs	Packet ID	Urgent Pointer	Outbound Interface
		Ack Number	Type of Service	Inbound Interface
	Wauth Logs	Precision	Window Size	TCP Flag
_	14-31	Packet Length		
Μ	Mail Logs			
:=	IPMAC Logs			
×	DHCP Logs			Save Exit

Choosing Default Log Fields which, are shown as predefined column in the table

Settings	
Source Settings	Server Settings Smtp Settings
Current serve	IP: <b>127.0.0.1</b>
	Connect to: <ul> <li>Local Host</li> <li>Remote Host</li> </ul>
	Server IP: 127.0.0.1
Check Con	nection Repair Save Exit

Settings Data Store to retrieve data from localhost or remote host

## 5.2. Save Screen

Logview allows you to save different views depending on your needs. You can create different widgets for different log sources, you can resize columns, set filters, change layouts and then you can click on "Save Screen" and give it a name. The page automatically saves the view after some critical events.

	137 103.234.233.233 -							
Save Pa	Save Page							
	View Name:							
CREATE	SAVE TO DASHBOARD							

#### 5.3. Load Screen

Logview stores your saved screen with any parameters and settings you asdf, as mentioned above. You can make a search then you fill find all saved screens and select which one you would like to load.

FIND A VIEW	
NAME:	
P. FROM:	
TO:	
View name	Table count
FIND	*
	2014-00-00 10.00.00 100.204.1.1

	FIND A VIEW			
	NAI	ME:		
€.	FRC	DM:		
	-	го:		
	View name	Table count		
D-1	view 2	4	Load	Delete
dis	dashboard	4	Load	Delete
	FIND			

# 5.4. SMTP Settings

It can be set SMTP settings by new version of Logview. You can either provide your own SMTP server settings or set any other SMTP server provider settings to send email(s) from Labris appliances. As it is shown in the figure below, there are mandatory fields you have to set and you have a "Test Connection"

### button to correct your settings before save it.

Settings
Source Settings Server Settings Smtp Settings
SMTP Server Address*: smtp.gmail.com
SMTP Mode: tis
SMTP Port*: 587
SMTP Username <sup>*</sup> :
SMTP Password': ++++++++++++++++++++++++++++++++++++
SMTP Mail From*:
Test SMTP Settings Save Exit

# 6. Regional Settings

Logview supports multilingual operations. Basically, it comes with English and Turkish. If clients require it, it is easy to add more languages to be supported.

<b>En Labri</b> s	s							🔅 Settings 👻 📁 Langua		Server State	us:O
E Z NETWORK			🛦 Firewall Logs 🗰 Access Logs	og Service Logs	🖌 😁 Administrative Log	s 📑 Wauth Logs	🖂 Mail Logs	IPMAC Logs X DHCP	Logs		= ::
>											
Dashboard	FIREWALL LOGS Cre	ate Time: 2014-06-06	14:04 Begin: 2014-06-06 00:00							۹	🖹 🗙
	Date / Time	Source	Source User	Source Port	Destination	Destination User	Destinatio.	. Rule	Action	Protocol	
III Logs	2014-06-06 10:53:07	169.254.1.1		138	169.254.255.255	-	138	Ifp OUT MNG IF	DROP	UDP	
	2014-06-06 10:53:06	169.254.1.1		137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
Q ino5	2014-06-06 10:53:05	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
1500 1500	2014-06-06 10:53:04	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
CDILLIange	2014-06-06 10:53:02	169.254.1.1		137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
CFO Usage	2014-06-06 10:53:01	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:53:00	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
RAMUsaga	2014-06-06 10:52:59	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
26%	2014-06-06 10:52:57	169.254.1.1	-	138	169.254.255.255		138	Ifp OUT MNG IF	DROP	UDP	
	2014-06-06 10:52:57	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
DISK Usage	2014-06-06 10:52:55	169.254.1.1	-	138	169.254.255.255		138	Ifp OUT MNG IF	DROP	UDP	
4%	2014-06-06 10:52:53	169.254.1.1	-	138	169.254.255.255		138	Ifp OUT MNG IF	DROP	UDP	
	2014-06-06 10:52:51	169.254.1.1	-	138	169.254.255.255		138	Ifp OUT MNG IF	DROP	UDP	
	2014-06-06 10:52:50	169.254.1.1	-	138	169.254.255.255		138	Ifp OUT MNG IF	DROP	UDP	
	2014-06-06 10:52:39	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:52:36	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	2014-06-06 10:52:36	169.254.1.1		137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTE
	🔻 📢 🧳 Pag	e 1 of1 🕨	Streaming: ON						Displa	aying 1 to 38 of 3	38 items

Main display in English

aons	5							🔅 Ayarlar 👻 🗎	≝Dil <del>v</del> ⊚	Veritabanı Duru	imu:🤍
RKS	s		🛔 Güvenlik Duvarı Kayıtları	🇰 Erişim Kayıtları	og işlem Kayıtları	😁 Yönetim Kayıtları	🛙 Wauth Kayıtları 🖂 N	lail Kayıtları 🔡 IPMA	C Kayıtları		= 87
>				0044 00 00 00:0						0	
6		ti Oluşturulma	Zamani: 2014-06-06 14:30 Başlan	giç: 2014-06-06 00:0						ų	<b>a x</b>
1	Tarih / Zaman	Kaynak	Kaynak Kullanıcı	Kaynak Portu	Hedef Adresi	Hedef Kullanıcı	Hedef Portu	Kural	Karar	Protokol	
	2014-06-06 10:53:07	169.254.1.1	-	138	169.254.255.255	· · · ·	138	Ifp OUT MNG I	DROP	UDP	
	2014-06-06 10:53:06	169.254.1.1	-	137	69.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:53:05	169.254.1.1	-	137	69.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:53:04	169.254.1.1	-	137	169.254.255.255	· · · ·	137	Ifp OUT MNG II	DROP	UDP	N
	2014-06-06 10:53:02	169.254.1.1	-	137	169.254.255.255	· · · ·	137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:53:01	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:53:00	169.254.1.1	-	137 *	169.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:52:59	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:52:57	169.254.1.1	-	138	169.254.255.255		138	Ifp OUT MNG I	DROP	UDP	
	2014-06-06 10:52:57	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:52:55	169.254.1.1	-	138	69.254.255.255		138	Ifp OUT MNG I	DROP	UDP	
	2014-06-06 10:52:53	169.254.1.1		138	69.254.255.255		138	Ifp OUT MNG I	DROP	UDP	
	2014-06-06 10:52:51	169.254.1.1	-	138	69.254.255.255		138	Ifp OUT MNG I	DROP	UDP	
	2014-06-06 10:52:50	169.254.1.1	-	138	69.254.255.255		138	Ifp OUT MNG I	DROP	UDP	
	2014-06-06 10:52:39	169.254.1.1		137	69.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:52:38	169.254.1.1	-	137	69.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	· · · ·	137	Ifp OUT MNG II	DROP	UDP	N
	2014-06-06 10:52:38	169.254.1.1	-	137	69.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:52:38	169.254.1.1	-	137	69.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:52:38	169.254.1.1	-	137	69.254.255.255		137	Ifp OUT MNG II	DROP	UDP	N
	2014-06-06 10:52:38	169.254.1.1	-	137	69.254.255.255	· · ·	137	Ifp OUT MNG II	DROP	UDP	N
	2014-06-06 10:52:37	169.254.1.1	-	137	69.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG II	DROP	UDP	N
	2014-06-06 10:52:37	169.254.1.1	-	137	69.254.255.255	-	137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:52:37	169.254.1.1	-	137 .	169.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N
	2014-06-06 10:52:36	169.254.1.1	-	137	69.254.255.255	-	137	Ifp OUT MNG II	DROP	UDP	N
	2014-06-06 10:52:36	169.254.1.1	-	137	69.254.255.255		137	Ifp OUT MNG I	DROP	UDP	N

Main display in Turkish

# 7. Service Monitoring

You can monitor background service's status of Logview. The status indicator will be green if all background services work fine, but the indicator will be yellow if some of services are ok but some have problem. If you see yellow indicator you should see system logs. If the indicator is red you should talk with the technical support.



There is also a service controlling option under the Server Status menu to restart services. If you see yellow indicator you may go through to try restarting services. If it may keep staying in the yellow status please contact the technical support.



# 8. Layout Options

Logview is a single page application that supports widgetizing the layout. You can monitor 4 different log sources in different records table. There are 4 layout option to placed widgets in the page:



1	Single Widget View	Single Widget View Button
2	Column View	Select Column View
3	List View	Select List View
4	Grid View	Select Grid View

Logview starts with a single widget if there is no dashboard saved and if the dashboard has no widget on it. So, Logview loads a firewall records table in single widget view. You can change the widgets, view option, columns, filters and then save the dashboard or save it with a different name.

# 8.1. Single Widget View

In single widget view layout you can see only one widget at a time. If you pick a streaming records table or create a historical records table it will replace the previous widget with itself. In another case, if you have more than one widget in a different view then you select the single view, the layout option will remove all widget except the one that added last.

FIREWALL LOGS C	Create Time: 2014-06-06 14	:59 Begin: 2014-06-06 00:00								Q 🖺 🗙
Date / Time	Source	Source User	Source Port	Destination	Destination User	Destinatio	Rule	Action	Protocol	Application
2014-06-06 10:53:07	169.254.1.1	-	138	169.254.255.255	-	138	Ifp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:53:06	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:53:05	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nat
2014-06-06 10:53:04	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:53:02	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:53:01	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:53:00	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:59	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:57	169.254.1.1	-	138	169.254.255.255	-	138	Ifp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:52:57	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:55	169.254.1.1	-	138	169.254.255.255		138	Ifp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:52:53	169.254.1.1	-	138	169.254.255.255	-	138	Ifp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:52:51	169.254.1.1	-	138	169.254.255.255		138	Ifp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:52:50	169.254.1.1	-	138	169.254.255.255		138	Ifp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:52:39	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:36	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
2014-06-06 10:52:36	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Na
v 📢 🍕 Pa	age 1 of 1 🕨	Streaming: ON								Displaying 1 to 38 of 38 items

## 8.2. Column View

In column view you can put widgets in columns and vertically display them.

FIREWALL LOGS	Create Time: 2014-06-06 15	5:16 Begin: 2014-06-0		Q 🖺 🗙	SERVICE LOGS Cro	eate Time: 2014-06-06 15:16 Begin: 2014-06-06	Q 🗈 🗙
Date / Time	Source	Source User	Source Port	Destination	Date / Time	Host Message	
2014-06-06 10:53:07	169.254.1.1	-	138	169.254.255.255	2014-06-06 12:16:40	localhost [2014/06/06 12:16:40.055664, 0] printing/print standard.c:6	8(std pcap cache reload)
2014-06-06 10:53:06	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:14:20	localhost Id "T0" respawning too fast: disabled for 5 minutes	
2014-06-06 10:53:05	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:14:15	localhost ttyS0: not a tty	
2014-06-06 10:53:04	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:14:10	localhost ttyS0: not a tty	
2014-06-06 10:53:02	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:14:05	localhost ttyS0: not a tty	
2014-06-06 10:53:01	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:14:00	localhost ttyS0: not a tty	
2014-06-06 10:53:00	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:13:55	localhost ttyS0: not a tty	
2014-06-06 10:52:59	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:13:49	localhost ttyS0: not a tty	
2014-06-06 10:52:57	169.254.1.1	-	138	169.254.255.255	2014-06-06 12:13:44	localhost ttyS0: not a tty	
2014-06-06 10:52:57	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:13:39	localhost ttyS0: not a tty	
2014-06-06 10:52:55	169.254.1.1	-	138	169.254.255.255	2014-06-06 12:13:34	localhost ttyS0: not a tty	
2014-06-06 10:52:53	169.254.1.1	-	138	169.254.255.255	2014-06-06 12:13:29	localhost ttyS0: not a tty	
2014-06-06 10:52:51	169.254.1.1	-	138	169.254.255.255	2014-06-06 12:08:28	localhost Id "T0" respawning too fast: disabled for 5 minutes	
2014-06-06 10:52:50	169.254.1.1	-	138	169.254.255.255	2014-06-06 12:08:23	localhost ttyS0: not a tty	
2014-06-06 10:52:39	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:08:18	localhost ttyS0: not a tty	
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:08:13	localhost ttyS0: not a tty	
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:08:08	localhost ttyS0: not a tty	
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:08:02	localhost ttyS0: not a tty	
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:07:57	localhost ttyS0: not a tty	
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:07:52	localhost ttyS0: not a tty	
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:07:47	localhost ttyS0: not a tty	
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:07:42	localhost ttyS0: not a tty	
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:07:37	localhost ttyS0: not a tty	
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:03:39	localhost [2014/06/06 12:03:39.266449, 0] printing/print standard.c:6	8(std pcap cache reload)
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:02:36	localhost Id "T0" respawning too fast: disabled for 5 minutes	
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:02:31	localhost ttyS0: not a tty	
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:02:26	localhost ttyS0: not a tty	
2014-06-06 10:52:36	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:02:21	localhost ttyS0: not a tty	
2014-06-06 10:52:36	169.254.1.1	-	137	169.254.255.255	2014-06-06 12:02:15	localhost ttvS0: not a ttv	
···· ▼ 41 4 I	Page 1 of 1 🕨	Streaming: ON	Display	ing 1 to 38 of 38 items	🔻 📢 Pa	age 1 of 7 🕨 🆗 🍜 Streaming: 💽 Dis	playing 1 to 50 of 321 items

### 8.3. List View

In list view you can put widgets in an horizontal order.

Date / Time	Source	Source User	Source Port	Destination	Destination User	Destinatio	Rule	Action	Protocol	Applicatio
2014-06-06 10:53:07	169.254.1.1	-	138	169.254.255.255	-	138	Ifp OUT MNG IF	DROP	UDP	CIFS CIF
2014-06-06 10:53:06	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS
2014-06-06 10:53:05	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS
2014-06-06 10:53:04	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS
2014-06-06 10:53:02	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS
2014-06-06 10:53:01	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS
2014-06-06 10:53:00	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS
2014-06-06 10:52:59	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS
2014-06-06 10:52:57	169.254.1.1	-	138	169.254.255.255		138	Ifp OUT MNG IF	DROP	UDP	CIFS CIF
2014-06-06 10:52:57	169.254.1.1	-	137	169.254.255.255		137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS
2014-06-06 10:52:55	169.254.1.1	-	138	169.254.255.255		138	Ifp OUT MNG IF	DROP	UDP	CIFS CIF
2014-06-06 10:52:53	169.254.1.1	-	138	169.254.255.255		138	Ifp OUT MNG IF	DROP	UDP	CIFS CIF
						***				0150 015
		W - Suballing. ON								
ERVICE LOGS Cre	eate Time: 2014-06-06 1	5:16 Begin: 2014-06-06 00:00								Q 🖻
ERVICE LOGS Cre Date / Time	eate Time: 2014-06-06 11 Host Messa	5:16 Begin: 2014-06-06 00:00								Q 🗈
RVICE LOGS Cre Date / Time 2014-06-06 12:16:40	eate Time: 2014-06-06 11 Host Messa localhost [2014/	6:16 Begin: 2014-06-06 00:00 90 906/06 12:16:40.055664, 0] printing/p	int standard.c:68(std	pcap cache reload)						Q 🖻
ERVICE LOGS Cre Date / Time 2014-06-06 12:16:40 2014-06-06 12:14:20	eate Time: 2014-06-06 11 Host Messa localhost [2014/ localhost Id "TO"	Constanting on     Constanting     Cons     Co	rint standard.c:68(std minutes	pcap cache reload)						Q B
ERVICE LOGS Cre Date / Time 2014-06-06 12:16:40 2014-06-06 12:14:20 2014-06-06 12:14:15	eate Time: 2014-06-06 11 Host Messa localhost [2014/ localhost [d Tf0" localhost ttvS0:	Country ON      Country ON     Country ON	int standard.c:68(std minutes	pcap cache reload)						Q B
ERVICE LOGS Crr Date / Time 2014-06-06 12:16:40 2014-06-06 12:14:20 2014-06-06 12:14:12 2014-06-06 12:14:13	eate Time: 2014-06-06 11 Host Messa localhost 12014// localhost 12014// localhost ttyS0: localhost ttyS0:	5:16 Begin: 2014-06-06 00:00 ge 9606 12:16:40.055664, 01 printina/p respanying too fast: disabled for 5 in toot a thy	int standard.c:68(std minutes	pcap cache reload)						Q B
ERVICE LOGS Cre Date / Time 2014-06-06 12:16:40 2014-06-06 12:14:15 2014-06-06 12:14:15 2014-06-06 12:14:10 2014-06-06 12:14:10	eate Time: 2014-06-06 11 Host Messa localhost I2014/N localhost ttyS0: localhost ttyS0:	Counting on     Counting	int standard.c:68(std minutes	pcap cache reload)						Q B
ERVICE LOGS Crr Date / Time 2014-06-06 12:16:40 2014-06-06 12:14:20 2014-06-06 12:14:15 2014-06-06 12:14:15 2014-06-06 12:14:05 2014-06-06 12:14:00	eate Time: 2014-06-06 11 Host Messa localhost (2014) localhost (2014) localhost (1701) localhost ttyS0; localhost ttyS0; localhost ttyS0;	Begin: 2014-06-06 00:00      Begin: 2014-06-06 00:00      Bogin: 2014	int standard.c:68(std	pcap cache reload)						Q B
ERVICE LOGS Cre Date / Time 2014-06-06 12:16:40 2014-06-06 12:14:20 2014-06-06 12:14:05 2014-06-06 12:14:05 2014-06-06 12:14:05 2014-06-06 12:13:55	eate Time: 2014-06-06 11 Host Messa localhost [2014// localhost Id T07 localhost thyS0: loc	Country of a ty	int standard.c:68(std	pcap cache reload)						Q B
CRVICE LOGS Cree Date/Time 2014-06-06 12:14:00 2014-06-06 12:14:20 2014-06-06 12:14:20 2014-06-06 12:14:05 2014-06-06 12:14:05 2014-06-06 12:13:34	age         1         0.1         p           eate Time:         2014-06-06 11         Host         Messa           localhost         1/2014/life         1/2014/life         I/2014/life           localhost         ttyS0:         localhost         ttyS0:         localhost         ttyS0:           localhost         ttyS0:         localhost         ttyS0:         localhost         ttyS0:           localhost         ttyS0:         localhost         ttyS0:         localhost         ttyS0:	Counting on      C	int standard.c:68(std	pcap cache reload)						Q 🖻 :
ERVICE LOGS Crr Date / Time 2014-06-06 12:16-40 2014-06-06 12:14:20 2014-06-06 12:14:15 2014-06-06 12:14:15 2014-06-06 12:14:05 2014-06-06 12:13:45 2014-06-06 12:13:49	age         1         0.1         p           eate Time:         2014-06-06 19         1         1           Host         Messa         localhost         1014 14         1	Begin: 2014-06-06 00:00      Begin: 2014	int standard.c:68(std	i pcap cache reload)						Q B
RVICE LOGS Crr Date / Time 2014-06-06 12:16:40 2014-06-06 12:14:20 2014-06-06 12:14:20 2014-06-06 12:14:15 2014-06-06 12:14:00 2014-06-06 12:13:49 2014-06-06 12:13:44 2014-06-06 12:13:49	eate Time: 2014-06-06 11 Host Messa localhost [2014// localhost thyS0: localhost	Country of a ty	int standard.c:68(std	pcap cache reicad)						Q B :
Carl Ce LOGS Cree Date / Time 2014-06-06 12:16:40 2014-06-06 12:14:20 2014-06-06 12:14:20 2014-06-06 12:14:05 2014-06-06 12:14:05 2014-06-06 12:13:49 2014-06-06 12:13:49 2014-06-06 12:13:39	age         1         0.1         p           eate Time: 2014-06-06 11         Host         Messa           localhost         1/2014/life         1/2014/life           localhost         th/S0:         localhost         th/S0:	Counting on      C	int standard.c:88(std	pcap cache reload)						Q B

It is easy to track log records while you have two streaming records table to compare some data. You can select columns and watch logs while the records table streams.

# 8.4. Grid View

Grid view has a wide gallery-like view and puts widgets in a 4 piece grid layout.

IREWALL LOGO CR	eate Time: 2014-06-06 15:17	Begin: 2014-06-0		Q 🖾 🗙	ADMINISTRATIVE LO	IGS Cr	eate Time: 2014-06-06 15:17 Begin: 20 Q
Date / Time	Source	Source User	Source Port	Destination	Date / Time	Host	Message
2014-06-06 10:53:07	169.254.1.1		138	169.254.255.255	2014-06-06 11:01:37	localhost	Accepted password for root from 10.7.100.102 port 58930 ssh2
2014-06-06 10:53:06	169.254.1.1		137	169.254.255.255	2014-06-06 11:01:37	localhost	pam unix(sshd:session): session opened for user root by (uid=0)
2014-06-06 10:53:05	169.254.1.1	-	137	169.254.255.255	2014-06-06 10:53:00	localhost	pam unix(login:session): session opened for user root by LOGIN(uid=0)
2014-06-06 10:53:04	169.254.1.1		137	169.254.255.255	2014-06-06 10:53:00	localhost	ROOT LOGIN ON tty1
2014-06-06 10:53:02	169.254.1.1	-	137	169.254.255.255			
2014-06-06 10:53:01	169.254.1.1		137	169.254.255.255			
2014-06-06 10:53:00	169.254.1.1	-	137	169.254.255.255			
2014-06-06 10:52:59	169.254.1.1		137	169.254.255.255			
2014-06-06 10:52:57	169.254.1.1		138	169.254.255.255			
2014-06-06 10:52:57	169.254.1.1		137	169.254.255.255			
2014-06-06 10:52:55	169.254.1.1		138	169.254.255.255			
	160 254 1 1		138	169.254.255.255			
2014-06-06 10:52:53	pe 1 of 1 + +	Streaming: ON	Display	ring 1 to 38 of 38 items	• 4 4	Page 1	1 of 1 ) ) (Streaming: ON Displaying 1 to 4 of 4 it
2014-06-06 10:52:53           Y         41         Pag           IREWALL LOGS         Cree	pe 1 of 1 ) ) )	Begin: 2014-06-0	) Display	Q B X	SERVICE LOGS	Page 1	1 of 1 ) ) ) Streaming: on Displaying 1 to 4 of 4 it e: 2014-06-06 15:16 Begin: 2014-06-06 Q
IREWALL LOGS Cree	eate Time: 2014-06-06 15:16	Streaming: ON Begin: 2014-06-0 Source User	Display	ning 1 to 38 of 38 items Q 🗈 🗙 Destination	SERVICE LOGS	Page 1 Create Time	1 of 1 ) ) (Streaming: ON Displaying 1 to 4 of 4 if e: 2014-06-06 15:16 Begin: 2014-06-06 Q
2014-06-06 10:52:53 	ate Time: 2014-06-06 15:16 Source 169.254.1.1	Streaming: ON Begin: 2014-06-0 Source User	Display	Q D X	• 44 4 SERVICE LOGS Date / Time 2014-06-06 12:16:4	Page 1 Create Time H 0 loca	1         of 1         )         )         Streaming:         ON         Displaying 1 to 4 of 4 it           e: 2014-06-06 15:16         Begin: 2014-06-06         Q         )           fost         Message         )<
2014-06-06 10:52:53	eate Time: 2014-06-06 15:16 Source 169.254.1.1 169.254.1.1 169.254.1.1	Streaming: ON Begin: 2014-06-0 Source User	Display Source Port 138 137	Q Destination 169.254.255.255 199.254.255.255	• • • • • • • • • • • • • • • • •	Page 1 Create Time 0 loca 0 loca	1 of 1 b b Streaming: on Displaying 1 to 4 of 4 it e: 2014-06-06 15:16 Begin: 2014-06-06 Q S iost Message allotet I2014/06/06 12:16:40.055664, 01 printing/brint standard c:68(sid pcap cache relations) diverse the OP responsioning too fast: disabled for 5 minutes
2014-06-06 10:52:53 <b>REWALL LOGS</b> Croc Date / Time 2014-06-06 10:53:07 2014-06-06 10:53:05 2014-06-06 10:53:05	I         of1         I         I           eate Time: 2014-06-06 15:16         Source         169-254.11         169-254.1	Streaming: ON Begin: 2014-06-0 Source User	Display	Q D × Destination 169.254.255.255 169.254.255.255 169.254.255.255	SERVICE LOGS Date / Time 2014-06-06 12:164 2014-06-06 12:164 2014-06-06 12:141	Page 1 Create Time 0 loca 5 loca 0 loca	1 of 1 b b Streaming: on Displaying 1 to 4 of 4 i et: 2014-06-06 15:16 Begin: 2014-06-06 Q S lost Message alhost [2014/06/06 12:16:40:0556664, 0] printing/print standard.c:68(std pcap cache rel alhost [2014/06/06 12:16:40:055664, 0] printing/print standard.c:68(std pcap cache rel alhost tyS0: not a try close the S00 or of a try
2014-06-06 10:52:53 	I         of1         I         I           eate Time: 2014-06-06         15:16         Source         169:254.1.1 </td <td>Streaming: OX Begin: 2014-06-0 Source User</td> <td>Display</td> <td>Q 🖻 🗙 Dostination 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255</td> <td>SERVICE LOGS Date / Time 2014-06-06 12:164 2014-06-06 12:14:1 2014-06-06 2014-06-06-06-06-06-06-06-06-06-06-06-06-06-</td> <td>Page 1 Create Time 0 loca 5 loca 0 loca 5 loca</td> <td>I of 1 b b C Streaming: ON Displaying 1 to 4 of 4 it e: 2014-06-06 15:16 Begin: 2014-06-06 Q S     Streaming: ON Displaying 1 to 4 of 4 it I 2014-06-06 15:16 Begin: 2014-06-06 Q S     Streaming: ON Displaying 1 to 4 of 4 it I 2014-06-06 15:16 Begin: 2014-06-06 Q S     Streaming: ON Displaying 1 to 4 of 4 it I 2014-06-06 15:16 Begin: 2014-06-06 Q S</td>	Streaming: OX Begin: 2014-06-0 Source User	Display	Q 🖻 🗙 Dostination 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255	SERVICE LOGS Date / Time 2014-06-06 12:164 2014-06-06 12:14:1 2014-06-06 2014-06-06-06-06-06-06-06-06-06-06-06-06-06-	Page 1 Create Time 0 loca 5 loca 0 loca 5 loca	I of 1 b b C Streaming: ON Displaying 1 to 4 of 4 it e: 2014-06-06 15:16 Begin: 2014-06-06 Q S     Streaming: ON Displaying 1 to 4 of 4 it I 2014-06-06 15:16 Begin: 2014-06-06 Q S     Streaming: ON Displaying 1 to 4 of 4 it I 2014-06-06 15:16 Begin: 2014-06-06 Q S     Streaming: ON Displaying 1 to 4 of 4 it I 2014-06-06 15:16 Begin: 2014-06-06 Q S
Date / Time           2014-06-06         0:52:53                IREWALL LOGS         Crrc           Date / Time            2014-06-06         10:53:07           2014-06-06         10:53:05           2014-06-06         10:53:05           2014-06-06         10:53:04           2014-06-06         10:53:04           2014-06-06         10:53:04	I         of1         I         I           ge         1         of1         I         I         I           ge         1         0         254.11         1         0         254.11         1         0         254.11         1         0         254.11         1         0         254.11         1         0         254.11         1         0         254.11         1         0         254.11         1         0         254.11         1         0         254.11         1         0         254.11         1         0         254.11         1         0         1         0         1         1         1         1         1         0         1         1         1         1         1         1         1         1         1         1         1         1         1         1 <td>Streaming: OX Begin: 2014-06-0 Source User</td> <td>Display Source Port 138 137</td> <td>Q E ★ Destination 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255</td> <td>Comparison of the second</td> <td>Page 1 Create Time 0 loca 5 loca 0 loca 55 loca 0 loca</td> <td>1 of 1 b b C Streaming: on Displaying 1 to 4 of 4 it e: 2014-06-06 15:16 Begin: 2014-06-06 Q S iost Message allost 1/21406/06 12:16:40.055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele 1/21406, 01 printing/pr</td>	Streaming: OX Begin: 2014-06-0 Source User	Display Source Port 138 137	Q E ★ Destination 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255	Comparison of the second	Page 1 Create Time 0 loca 5 loca 0 loca 55 loca 0 loca	1 of 1 b b C Streaming: on Displaying 1 to 4 of 4 it e: 2014-06-06 15:16 Begin: 2014-06-06 Q S iost Message allost 1/21406/06 12:16:40.055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 055664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele allost 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele 1/21406/06 12:16:40 05664, 01 printing/print standard c:68(std pcap cache rele 1/21406, 01 printing/pr
2014-06-06 10:52:53 	I         of1         I         I           eate Time: 2014-06-06         15:16         Source         169:254.11           169:254.1.1         169:254.1.1         169:254.1.1         169:254.1.1           169:254.1.1         169:254.1.1         169:254.1.1         169:254.1.1	Streaming: ON Begin: 2014-06-0 Source Usor	Display	Q Destination 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255	SERVICE LOGS     Date / Time     2014-06-06 12:16-4     2014-06-06 12:14-1     2014-06-06 12:14-1     2014-06-06 12:14-1     2014-06-06 12:14-0     2014-06-06     2014-00-06      2014-00-06      2014-00-06     2014-00-06     201	Page         1           Create Time         H           0         loca           5         loca           5         loca           15         loca           15         loca	1 of 1 ▶ ₩ Streaming: ox Displaying 1 to 4 of 4 i e: 2014-06-06 15:16 Begin: 2014-06-06 Q ≧ alhost [2014/06/06 12:16:40 055664, 0] printing/print standard.c:68(std pcap cache rel alhost [2014/06/06 12:16:40 055664, 0] printing/print standard.c:68(std pcap cache rel alhost tyS0: not a try alhost tyS0: not a try
2014-06-06 10:52:53 Participation of the second se	I         of1         I         I           ge         1         of1         I         I         I           eate Time: 2014-06-06         15:16         Source         I	Streaming: OX Begin: 2014-06-0 Source User - - - - - - - - -	Display Source Port 138 137	Q Destination 169.254.255.255 169.255.255 169.2	SERVICE LOGS Date / Time 2014-06-06 12:164 2014-06-06 12:145 2014-06-06 12:145 2014-06-06 12:145 2014-06-06 12:145 2014-06-06 12:145 2014-06-06 12:145 2014-06-06 12:145 2014-06-06 12:155 2014-06-06 2014-06 2014-06 2014 2014-06 2014 2014-06 2014 2014 2014-06 2014 2014 2014 2014 2014-06 2014 2014 2014 2014 2014 2014 2014 2014	Page         1           Create Time           0         locc           00         locc	1 of 1 ▶ ₩ Streaming: on Displaying 1 to 4 of 4 i a: 2014-06-06 15:16 Begin: 2014-06-06 Q tost Message alhost 1/2014/06/06 12:1640.055664.01 printing/print standard.c:68(std pcap cache rel alhost tySC: not a try alhost tySC: not a try
Date / Time           2014-06-06         00:52:53           IREWALL LOGS         Crr           Date / Time         2014-06-06           2014-06-06         10:53:07           2014-06-06         10:53:05           2014-06-06         10:53:05           2014-06-06         10:53:05           2014-06-06         10:53:01           2014-06-06         10:53:01           2014-06-06         10:53:01           2014-06-06         10:53:02           2014-06-06         10:53:02           2014-06-06         10:52:57	Image: 1         of 1         Image: 1           eate Time: 2014-08-06 15:16           Source           169.254.1.1           169.254.1.1           169.254.1.1           169.254.1.1           169.254.1.1           169.254.1.1           169.254.1.1           169.254.1.1           169.254.1.1           169.254.1.1           169.254.1.1           169.254.1.1	Streaming: ON Begin: 2014-06-0 Source User	Display  Source Port  38  137  137  137  137  137  137  137	Q Defination 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255 169.254.255.255		Page         1           Create Time         H           0         locci           5         locci           00         locci           15         locci           9         locci	1 of 1 b b C Streaming: on Displaying 1 to 4 of 4 i e: 2014-06-06 15:16 Begin: 2014-06-06 Q Displaying 1 to 4 of 4 i lost Message alhost I2014/06/06 12:16:40 055664, 01 printing/print standard c.68(std pcap cache rel alhost Id 'TO' respawning too fast: disabled for 5 minutes tids' root a try alhost titySC: not a try alhost titySC: not a try alhost titySC: not a try alhost titySC: not a try alhost titySC: not a try alhost titySC: not a try alhost titySC: not a try alhost titySC: not a try alhost titySC: not a try alhost titySC: not a try alhost titySC: not a try alhost titySC: not a try alhost titySC: not a try
2014-06-06 10:52:53 2014-06-06 10:52:53 2014-06-06 10:53:07 2014-06-06 10:53:07 2014-06-06 10:53:04 2014-06-06 10:53:04 2014-06-06 10:53:04 2014-06-06 10:53:04 2014-06-06 10:53:02 2014-06-06 10:53:02 2014-06-06 10:52:57 2014-06-06 10:52:57	I         of1         I         i           ge         1         of1         I         i           eate Time: 2014-06-06         15:16         Source         I           169.254.11         169.254.1.1         169.254.1.1         169.254.1.1         I	Streaming: ON Begin: 2014-06-0 Source Usor - - - - - - - - - - - - - - - - - - -	Display Source Port 138 137 137 137 137 137 137 137 137 137 137	Q Detailon 169.254.255.255 169.255 169	•         •         •         •           SERVICE LOGS         Date / Time         2014-06-06         12:16:4           2014-06-06         12:16:4         2014-06-06         12:14:1           2014-06-06         12:14:1         2014-06-06         12:14:1           2014-06-06         12:14:0         2014-06-06         12:13:1           2014-06-06         12:13:4         2014-06-06         12:13:4           2014-06-06         12:13:4         2014-06-06         12:13:4	Page         1           Create Time         H           0         locci           5         locci           5         locci           00         locci           5         locci           00         locci           15         locci           165         locci           175         locci           19         locci           19         locci	1 of 1 ▶ ▶ ∞ Streaming: on Displaying 1 to 4 of 4 i e: 2014-06-06 15:16 Begin: 2014-06-06 Q e: 2014-06-06 12:16:40 055664, 0) printing/print standard.c:68(std pcap cache rel alhost 1/2014/06/06 12:16:40 055664, 0) printing/print standard.c:68(std pcap cache rel alhost tySC: not a try alhost tySC: not a try
Z014-36-06         0:52:53            ¥         4         ¥         Pag           IREWALL LOGS         Crrc         Dato / Time         Z014-06-06         0:53:07           2014-06-06         10:53:07         Z014-06-06         10:53:02         Z014-06-06         10:53:02           2014-06-06         10:53:02         Z014-06-06         10:53:02         Z014-06-06         10:53:02           2014-06-06         10:53:02         Z014-06-06         10:53:02         Z014-06-06         10:53:02           2014-06-06         10:53:02         Z014-06-06         10:53:02         Z014-06-06         10:52:57           2014-06-06         10:52:57         Z014-06-06         10:52:57         Z014-06:06         10:52:57           2014-06-06         10:52:57         Z014-06:06         10:52:57         Z014-06:06         10:52:57	I         of1         I         I           ge         1         of1         I         I           eate Time: 2014-06-06         15:16         Source         169.254.1.1           169.254.1.1         169.254.1.1         169.254.1.1         169.254.1.1           169.254.1.1         169.254.1.1         169.254.1.1         169.254.1.1           169.254.1.1         169.254.1.1         169.254.1.1         169.254.1.1           169.254.1.1         169.254.1.1         169.254.1.1         169.254.1.1	Streaming: OX Begin: 2014-06-0 Source User - - - - - - - - - - - - - - - - - - -	Display Source Port 138 137 137 137 137 137 137 137 137 137 138 137 138	Q         Destination           169.254.255.255         169.254.255.255           169.254.255.255         169.254.255.255           169.254.255.255         169.254.255.255           169.254.255.255         169.254.255.255           169.254.255.255         169.254.255.255           169.254.255.255         169.254.255.255           169.254.255.255         169.254.255.255           169.254.255.255         169.254.255.255           169.254.255.255         169.254.255.255           169.254.255.255         169.254.255.255           169.254.255.255         169.254.255.255           169.254.255.255         169.254.255.255	SERVICE LOGS     Date / Time     2014-06-06 12:164     2014-06-06 12:164     2014-06-06 12:14:1     2014-06-06 12:14:1     2014-06-06 12:14:0     2014-06-06 12:134     2014-06-06     2014     2014-06-06     2014-06     2014-06-06     2014-06     2014-06     2014-06     2014-06     2014-06     2014-06     2014-06     2014-06     2014-06     2014-06     2014-06     2014-06     2014-06     2014-06     2014     2014-06     2014-06     2014     2014-06     2	Page         1           Create Time         H           0         loca           00         loca           00         loca           00         loca           00         loca           01         loca           02         loca           03         loca           04         loca	1 of 1 ▶ ▶ ∞ Streaming: on Displaying 1 to 4 of 4 i e: 2014-06-06 15:16 Begin: 2014-06-06 Q e: 2014-06-06 15:16 Begin: 2014-06-06 Q Message alhost 12014/06/06 12:16:40:055664,01 printing/print standard.c.68(sd pcap cache rel alhost twS0: not a try alhost twS0: not a try

This view helps you to compare or watch 4 different log sources in tables.

#### 9. Reports

By a new version 1.2.0-84 of Logview, we provide a brand new reporting module. Since, our products have already reporting module ERM, by this new module we add improving features listed below:

- Enables custom query writing,
- PDF report generation,
- Table and chart(PIE chart only for recent version) displaying in PDF,
- Report template add/edit/remove features,
- Schedule report generation by user,
- Email and FTP upload feature,
- Manually upload or email generated report to given destination,

## 9.1. Create Template

The figure shown below helps you create a "Report Template" which, defines "Report" fields, data set, chart set, schedule settings, email settings and FTP settings. In this view you can use **All** records in a log table or write your own custom query based on SQL syntax. See details in the figure below:

Create New	v Report Template	
Report N	Firewall Weekly Application Report	
Descrip	This report contains weekly application filter regarding provided query Max. 500 character	
Output Fo	ormat PDF	
Report Lang	uage English +	
Data Set	Table Settings         Chart Settings         Schedule Settings         Email Settings	Upload Settings
Data So	urce' Firewall v	
Р	eriod This Week 👻	
Report C	Query O All O Custom	
Report C	Query application = "HTTP_HTTP"	
	Please write a valid query	
		Create Depart
		Create Report Exit
		-
Create New Rep	port Template	
Report Name*	Firewall Weekly Application Report	
Description	This report contains weekly application filter regarding provided query	
Output Format	Max. 500 character	
Peport Language	Foolich	
Data Set I ab	e Settings Chart Settings Schedule Settings Email Settings Upload Settings	
Period	This Week v	
Report Query	⊖ All ⊛ Custom	
Report Query	date	
	Plea source source_user	
	source_port destination	
	destination_user Save Report Exit	
	destination_port rule	
	action	
	protocol	

Write custom SQL query and Logview suggest column names and basic SQL keywords.

Report Name*	Firewall Weekly Applic	ation Report		
Description	This report contains w application filter regard query Max. 500 character	eekly ding provided		
Output Format	PDF			
Report Language	English			
Data Set Table S	Settings Chart Setti	ngs Schedule Settings	Email Settings Upload S	ettings
Table Columns	Jate / Time	✓ Source	Source User	
	Source Port	Destination	Destination User	
	Destination Port	✓ Rule	✓ Action	
	Protocol	✓ Application	Mac Address	
	Host	Message	Sequence Number	
	Туре	Code	ΠL	
	Packet ID	Urgent Pointer	Outbound Interface	
	Ack Number	Inbound Interface	Precision	
	Window Size	TCP Flag	Packet Length	
Show in Table	Тор 30	Ψ		

Select columns which, are will be shown in the report table.

Create New Repor	rt Template
Report Name	Firewall Weekly Application Report
Description	This report contains weekly application filter regarding provided query Max. 500 character
Output Format	PDF
Report Language	English
Data Set Table	Settings Chart Settings Schedule Settings Email Settings Upload Settings
Chart Type	Pie Chart v
Chart Field	Source
Show in Chart	Тор 5 у
	Create Report Exit

Select chart field to be shown in Pie chart

Create New Report	t Template
Report Name <sup>*</sup>	Firewall Weekly Application Report
Description	This report contains weekly application filter regarding provided query Max. 500 character
Output Format	PDF
Report Language	English v Settings Chart Settings Schedule Settings Email Settings Upload Settings
Enable	
Generate Report Every	1 Weeks v
Schedule Start	2015-12-14 09:44
Schedule End	
	Create Report Exit

Schedule settings tab

Create New Repor	rt Template
Report Name*	Firewall Weekly Application Report
Description	This report contains weekly application filter regarding provided query Max. 500 character
Output Format	PDF
Report Language	English
Data Set Table	Settings Chart Settings Schedule Settings Email Settings Upload Settings
Enable	
Subject	Firewall Weekly Application Repc
Recipients	murat.bulbul@labrisnetworks.co m. <u>cem.yapalak@labrisnetworks.co</u> m Write email addresses with comma between them.
Message	This report contains weekly application filter regarding provided query
	Create Report Exit

# Email Settings Tab

Create New Report	tTemplate
Report Name*	Firewall Weekly Application Report
Description	This report contains weekly application filter regarding provided query Max. 500 character
Output Format	PDF
Report Language	English
Enable	Ø
Server	ftp.myserver.com
User	anonymous
Password	*****
Directory	home/reports/firewall
	Create Report Exit

FTP Settings Tab

						+ Create
Rep	port Templates					
	Name	Description	Period	Created Date	Reports	Manage
1	Firewall Weekly Application Report	This report contains weekly application filter regarding provi	This Week	Monday, 14 December 2015, 09:47		C 🛱
н -	← Page of 1 1 → M Records	per page: 20 • C Displaying 1 to 1 of 1 items.				

The figure above, contains all report templates which, are created by user or pre-defined by Labris regarding most required report enquiries. Some buttons and details can be seen in a template row: name, description, period, created date, show reports grid and generate a new report, edit and remove template.

Reports	Manage
	C m

There are helper tooltips on every single buttons placed in a row. It helps you about what its click event.

Show Report Table: Open a popup and show reports listed in a table that belong to the template.

**Generate New:** Generates a new report depending provided details such as data set, table settings, chart settings, schedule settings, emails settings and FTP settings.

Edit: Helps you edit the template details.

**Remove:** Delete the template and all reports generated previously by the template details.

Report List						
Reports						
	Name	Hostname	Output	Created Date	Manage	
1	Firewall Weekly Application Report - 2	localhost	🛓 📩 🐸	Monday, 14 December 2015, 09:55	Ē	
( (	← Page of 1 1 → N Reco	rds per page: 20 🔻	C Displaying 1 to 1 of 1 if	lems.		
					Ex	

Reports Grid shows all generated reports

F	Report List						
	Repo	Reports					
ł		Name	Hostname	Output	Created Date	Manage	
n	1	Firewall Weekly Application Report - 2	localhost	🛓 🕁 🔤	Monday, 14 December 2015, 09:55	â	

In reports table you can download, upload or send email manually. You can leave FTP and email settings as given previously or write new settings to deliver the report seperately to different email addresses or FTP destinations.

Server	ttp.myserver.com
User	anonymous
Password	
Directory	home/reports/firewall
	Upload Cancel

# FigureFTP Upload popup

i Subject	Firewall Weekly Application Repc
Recipients	murat.bulbul@labrisnetworks.co m, cem.yapalak@labrisnetworks.co m
Message	This report contains weekly application filter regarding provided query
	Send Cancel

#### Send email popup



Pie Chart result which, is shown in the report



