Administration Guide for Labris UTM

Unified Threat Management Appliances
and Software

http://labrisnetworks.com/support-training/

Tel: +90 850 455 4555

Labris NETWORKS

1. Copyright

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.

3. Document Revision History

#	Document modified by	Description	Authorized By
1			
2			
3			
4			
5			

1. COPYRIGHT 1
2. DISCLAIMER 1
3. DOCUMENT REVISION HISTORY 1
4. ABOUT LABRIS NETWORKS INC. 7
5. ABOUT LABRIS UTM 7
6. HOW TO PURCHASE LABRIS UTM? 8
7. LABRIS UTM APPLIANCE DEPOLYMENT ARCIHTECTURE 8
8. CONNECTING TO THE DEVICE 9
9. ACCESSING THE WEB ADMIN CONSOLE 9
9.1 Understanding the landing page or home screen 10
9.1.1 System Information 11
9.1.2 Signature Database 11
9.1.3 System Status 12
9.1.4 Application Usage 12
9.1.5 Network Interfaces 13
9.1.6 Action Statistics 15
10. SYSTEM 16
10.1 General Settings 17
10.1.1 General Settings 17
10.1.2 Date / Time Settings 18
10.1.3 SMTP Settings 21
10.2 Administration 22
10.2.1 Users 23
10.2.2 Profiles 25
10.3 Certificate Manage 27
10.3.1 Certificates 27
10.3.2 Certificate Authority 31
10.4 High Availability 34
10.4.1 High Availability Settings 35
10.4.2 Control Settings 36
10.4.3 Load Transfer Settings 38
10.4.4 Status 39
10.5 Backup & Restore 40
10.5.1 Settings 40
10.5.2 Backup and Restore Configuration 41
10.5.3 Factory Default 41
10.5.4 Backups 42
10.6 Firmware 42
10.7 Console Access 42
10.8 License 44
10.8.1 License Overview 45
10.8.2 Install License 45
10.8.3 License Details 46
11. NETWORK 47
11.1 Interface 47
11.1.1 Interface Editing 48
11.1.2 Adding an Interface 50
11.1.2.1 Alias 50
11.1.2.2 Bridge Interface 52
11.1.2.3 VLAN Interface 53
11.1.2.4 Bond Interface 54
11.1.2.5 PPPoE 58
11.1.2.5 3G/4G 60

11.2 Static Routes 61
11.3 SD-WAN 63
11.3.1 Gateway 64
11.3.2 Gateway Groups 65
11.4 DHCP 66
11.4.1 Scope 68
11.4.2 Lease 73
11.4.3 Relay 74
11.4.4 Global Settings 75
11.5 DNS 76
12. VPN 78
12.1 L2TP 79
12.2 PPTP 80
12.3 SSL VPN 81
12.3.1 Tunnel 83
12.3.1.1 Network Settings 83
12.3.1.2 Security Settings 84
12.3.1.3 Client Settings 85
12.3.1.4 Other Settings 86
12.3.2 Bookmarks 86
12.3.3 Portal 88
12.4 IPSec 92
12.4.1 Tunnel 92
12.4.2 IKE Profiles 95
12.4.3 IPsec Profiles 98
13. POLICIES 103
13.1 Firewall 103
13.1.1Rules 104
13.1.2 Settings 110
13.1.2.1 Implicit Policies 111
13.1.2.2 Protection Port Scanner 113
13.1.2.3 Flood Control 114
13.2 NAT(Network Address Translation) 115
13.3 SD-WAN Policy 120
13.4 Web Filter 124
13.4.1Policies 125
13.4.2 Exception 132
13.5 Wauth 133
13.5.1 Policy 134
13.5.1.1 Add New Rule 134
13.5.1.2 Subnet Rules 135
13.5.1.3 General 136
13.5.2 Reference Records 149
13.5.2.1 Pending Reference Records 149
13.5.2.2 Reference Records History 150
13.5.3 Exception 150
13.5.4 Interface Settings 153
13.6 IP/MAC Binding 155
14. E-MAIL SECURITY 158
14.1 Settings 158
14.1.1 General 158
14.1.2 Domain Control 159
14.1.3 Authentication 161
14.1.4 Antispam 162
14.1.5 Antivirus 165
14.1.6 Digest 166

14.1.7 Policy 168
14.1.8 Spam Learn 171
14.1.9 RBL Server 172
14.1.10 RBL Exception 173
14.1.11 Allow/Deny List 174
14.2 Antispam 176
14.2.1 Malware Site Filter 177
14.2.2 Malware Exceptions 178
14.2.3 Content Filter 180
14.2.4 ByPass 189
14.2.5 Bayes 191
14.3 Antivirus 192
14.3.1 Banned File Type 193
14.3.2 Bypass 194
14.4 Quarantine 195
14.4.1 Spam 196
14.4.2 Virus 196
15. IDS&IPS 198
15.1 Sensor 198
15.1.1 Address Settings 201
15.1.2 Port Settings 203
15.2 Signature Profile 204
15.3 DLP Profile 210
15.4 Exception IPs 215
15.5 Settings 217
16. OBJECTS & IDENTITY 218
16.1 Network Objects 218
16.1.1 Address 219
16.1.2 Address Group 223
16.1.3 Country 224
16.1.4 Service 225
16.1.5 Service Group 228
16.2 Policy Objects 229
16.2.1 Schedule 230
16.2.2 Bandwidth 232
16.2.3 DoS&DDoS 234
16.3 Quota Objects 236
16.3.1 Quota 237
16.3.2 Quota Exception 239
16.4 Application 241
16.4.1 List 241
16.4.2 Group 242
16.5 Identity 244
16.5.1 Users 244
16.5.2 Groups 248
16.5.3 Domains 250
16.5.4 User Templates 251
16.5.5 L2TP/PPTP Users 254
16.5.6 Authentication 256
16.5.7 MFA Provider 258
16.5.8 Settings 262
16.6 Receiver Profiles 262
16.6.1 Syslog 263
16.6.2 SNMP Trap 265
16.6.3 HTTP 267
16.6.4 E-Mail 269

16.6.5 FTP 271
17. VISIBILITY 274
17.1 Interface Selection 275
17.2 Dashboard 276
17.2.1 Traffic Dashboard 276
17.2.1.1 Talkers 277
17.2.1.2 Hosts 277
17.2.1.3 Ports 277
17.2.1.4 Applications 278
17.2.2 Network Discovery 278
17.3 Alerts 278
17.3.1 Engaged Alerts 278
17.3.2 Past Alerts 279
17.3.3 Flow Alerts 280
17.4 Flow 281
17.5 Hosts 283
17.5.1 Hosts 284
17.5.2 Mac Address 285
17.5.3 Networks 287
17.5.4 Host Pools 288
17.5.5 Operating System 290
17.5.6 HTTP Server 291
17.5.7 Top Hosts 292
17.6 Interface 293
17.6.1 Networks 294
17.6.2 Packets 294
17.6.3 DSCP 295
17.6.4 Applications 295
17.6.5 ICMP 296
17.6.6 ARP 296
17.6.7 Graphic 296
18. MONITOR 297
18.1 Firewall Statistics 297
18.2 Attacks 298
18.3 Interfaces 298
18.4 Link/Target 299
18.5 E-Mail Security 300
18.6 Online Users 300
18.7 Quota Usage 301
18.8 IPSec 303
18.9 SSL VPN Client 304
18.10 L2TP 305
18.11 PPTP 305
18.13 Connections 307
18.14 Arp Cache 308
18.15 Services 309
19. LOGS&REPORTS 311
19.1 Logs 311
19.1.1 Live Monitoring 312
19.1.1.1 Firewall 312
19.1.1.2 Web Filter 314
19.1.1.3 Service 316
19.1.1.4 Administrative 318
19.1.1.5 WAUTH 320
19.1.1.6 Mail 321
19.1.1.7 IP/MAC 322

19.1.1.8 DHCP 323
19.1.1.9 SSLVPN 325
19.1.1.10 IPSec 327
19.1.1.11 Connections 329
19.1.2Archive 330
19.2 Reports 332
19.2.1 Recent Reports 332
19.3 Time Stamp Logs 340

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.

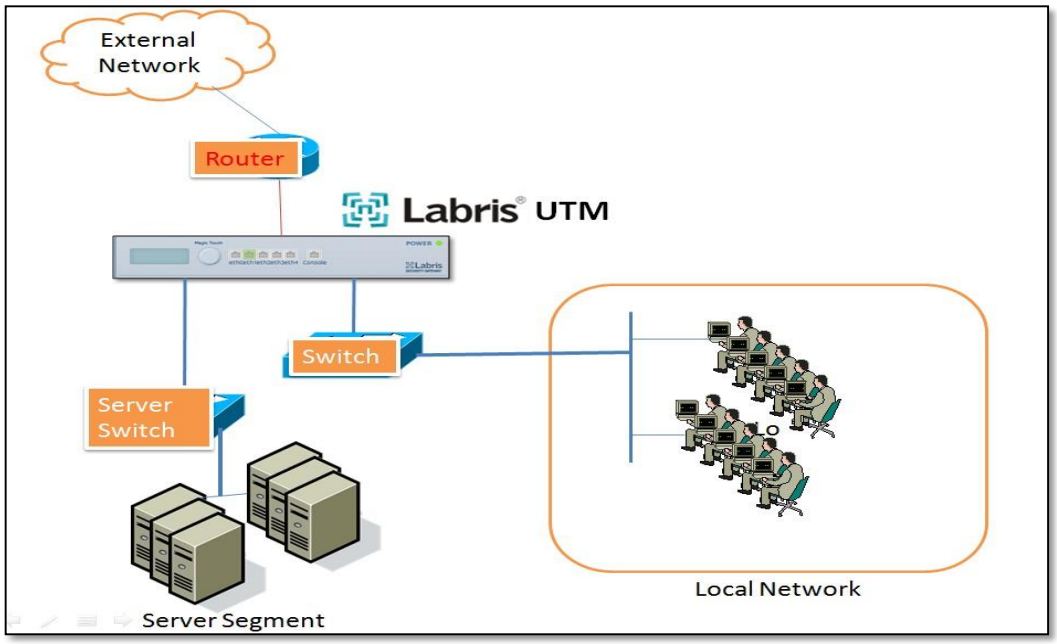
6. How to Purchase Labris UTM?

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

You can purchase througauthorized distributors http://labrisnetworks.com/authorized-distributors/

7. Labris UTM Appliance Depolyment Archtecture

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 to the Device

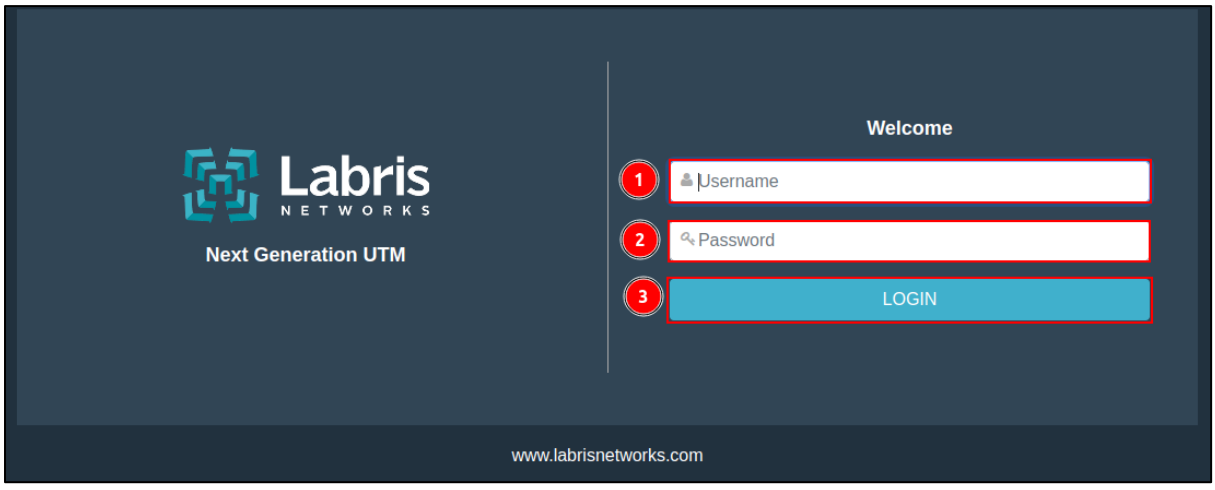
Connect the device to a management computer using an Ethernet cable. You can use a Crossover Ethernet cable for a direct connection, or a straight Ethernet cable if connecting via a hub or switch. Both types of cables are provided with the device. Connect one end of the Ethernet cable to the Labris UTM device (eth0) and the other end to the computer's Ethernet interface.

9. Accessing the Web Admin Console

To access the Labris Web Admin Console, follow these steps:

1. Identify the Default Management Port: Labris Default Management Port: eth0/Port1/Net0/Mgt (the first port of the device).
2. Default IP Address: The default IP address for eth0/Port 1/Net0/Mgt (the first port) is 169.254.1.1/16 (subnet mask 255.255.0.0).
3. Default Credentials:
   Username: admin
   Password: labris
4. Configure Your Computer: Connect your computer to the first port of the Labris device. Open the network settings on your computer. Assign the IP address 169.254.1.10 and the subnet mask 255.255.0.0 to your computer.
5. Access the Web Console: Open a web browser and navigate to https://169.254.1.1:81. This IP address corresponds to the Labris device's management interface.
6. Log In: The login page for the LABRIS UTM Web Console will be displayed. Enter the default username and password to log in.

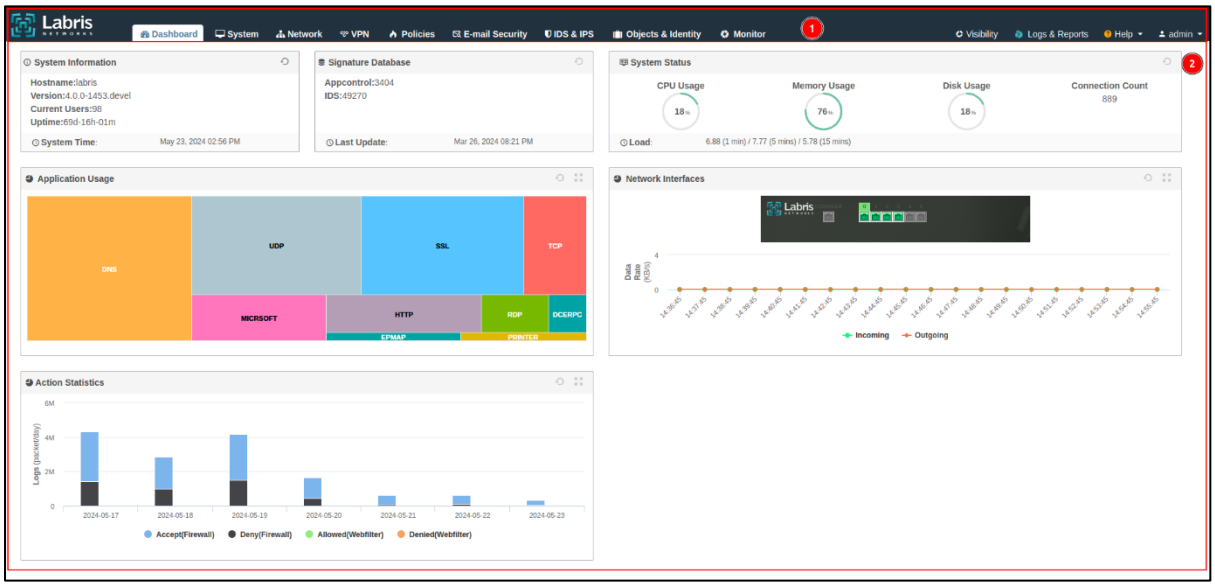
You should now have access to the Labris Web Admin Console where you can configure and manage your device.



1	**Username**	Type your current Default username. This username is provided during setup.
2	**Password**	Type your current default password. This password is the one you give during installation. A good password is a mix of letters, numbers, and special characters together that is at least 8 characters long.
3	**Login**	Click on the "Login" button to log in to your device

9.1 Understanding the landing page or home screen

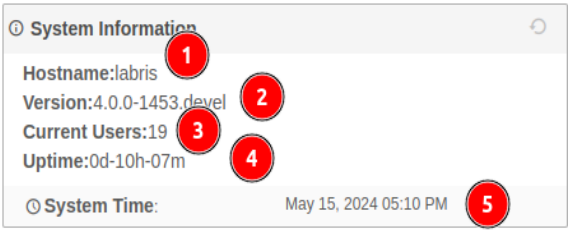
After logging in with the username and password, you will understand the various parts of the main screen of the Labris UTM device.



1	**Tab Section**	You can navigate through various sections such as Control Panel, System, Network, VPN, Policies, E-mail Security, Object & Identity, Monitor, Visibility, Logs & Reports, Help, and Logged-in User.
2	**Control Panel**	After the first login, you will see the Labris Security Dashboard. On the Dashboard, you can see the system, signature database, system status, application usage, interfaces, and transaction statistics.

9.1.1 System Information

In the System Information area on the control panel, you can view the device's name, version, number of users, runtime, and system time information.



1	**Hostname**	Indicates the name of the device.
2	**Version**	Shows device version information.
3	**Current Users**	Shows the instantaneous number of users connected to the device.
4	**Runtime**	Displays the operating time of the device in days, hours, and minutes.
5	**System Time**	Shows the time and date of the device.

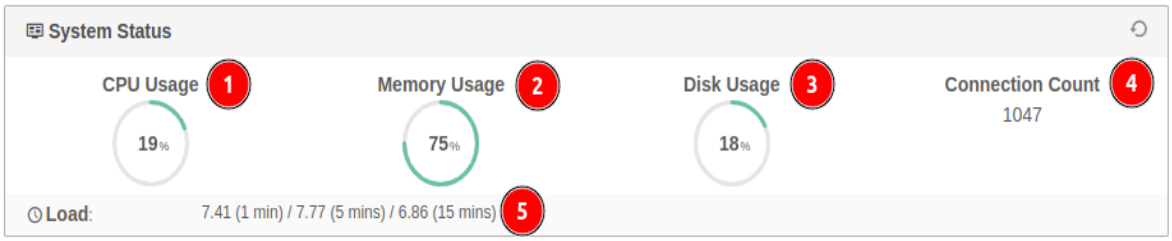
9.1.2 Signature Database

Shows the IDS and application control numbers on the Labris UTM device.

1	**Appcontrol**	Shows the number of application check signatures.
2	**IDS**	Shows the number of intrusion detection system signatures.
3	**Last Update**	Indicates the date and time when the application control and intrusion detection systems were updated.

9.1.3 System Status

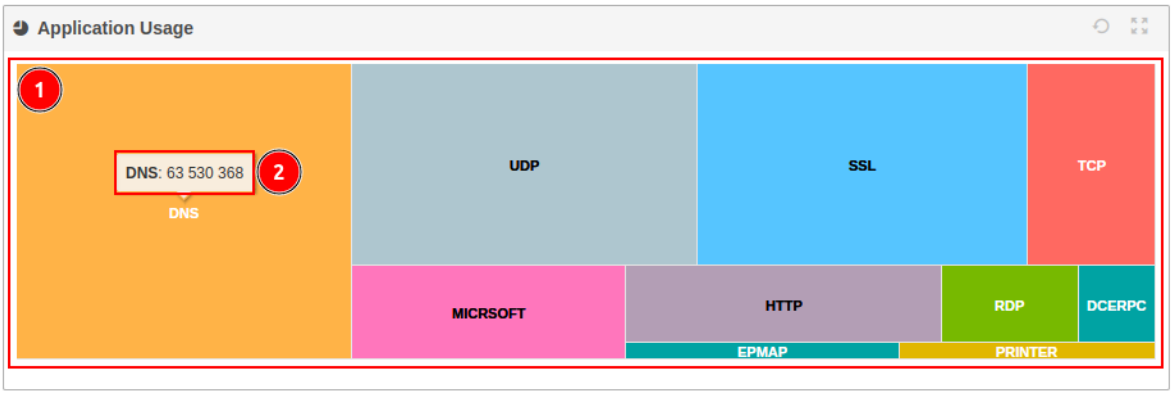
The system status displays the device's processor usage, memory usage, disk usage, number of connections, and load statuses, and shows information with diagrams that allow us to easily understand the use cases of the processor, memory, disk, and number of connections.



1	**Cpu Usage**	Shows the device’s processor usage numerically.
2	**Memory Usage**	Shows the device's memory usage numerically.
3	**Disk Usage**	Shows the disk usage of the device numerically.
4	**Connection Count**	Shows the number of devices that are connected to the device.
5	**Load**	Shows the load status of services running on the device. The values here show the average load values of 1, 5, and 15 minutes.

9.1.4 Application Usage

The names of the protocols present in the application layer and the number of their uses.



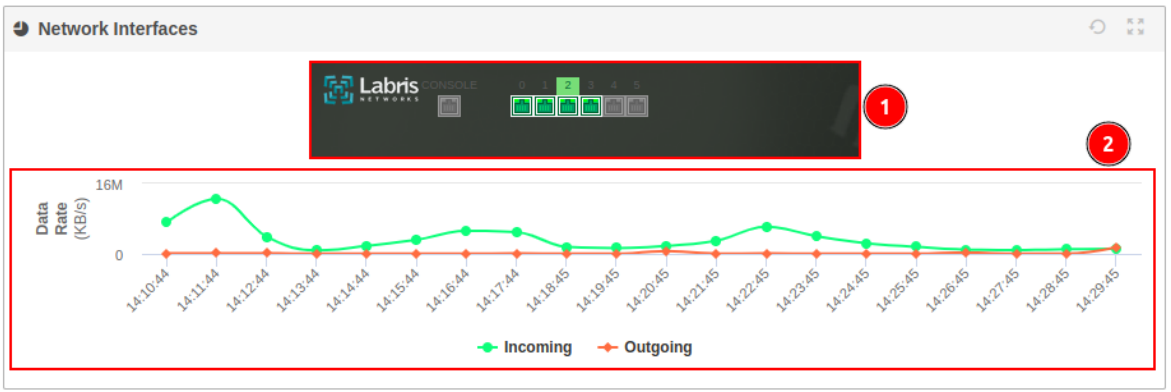
1	**Application Names**	Shows the names of the most used protocols in the application layer.
2	**Number of Applications**	Shows the number of uses of the most used protocols in the application layer.

Note

To see the number of applications, you must first hover the cursor over the application name you want to see the number of.

9.1.5 Network Interfaces

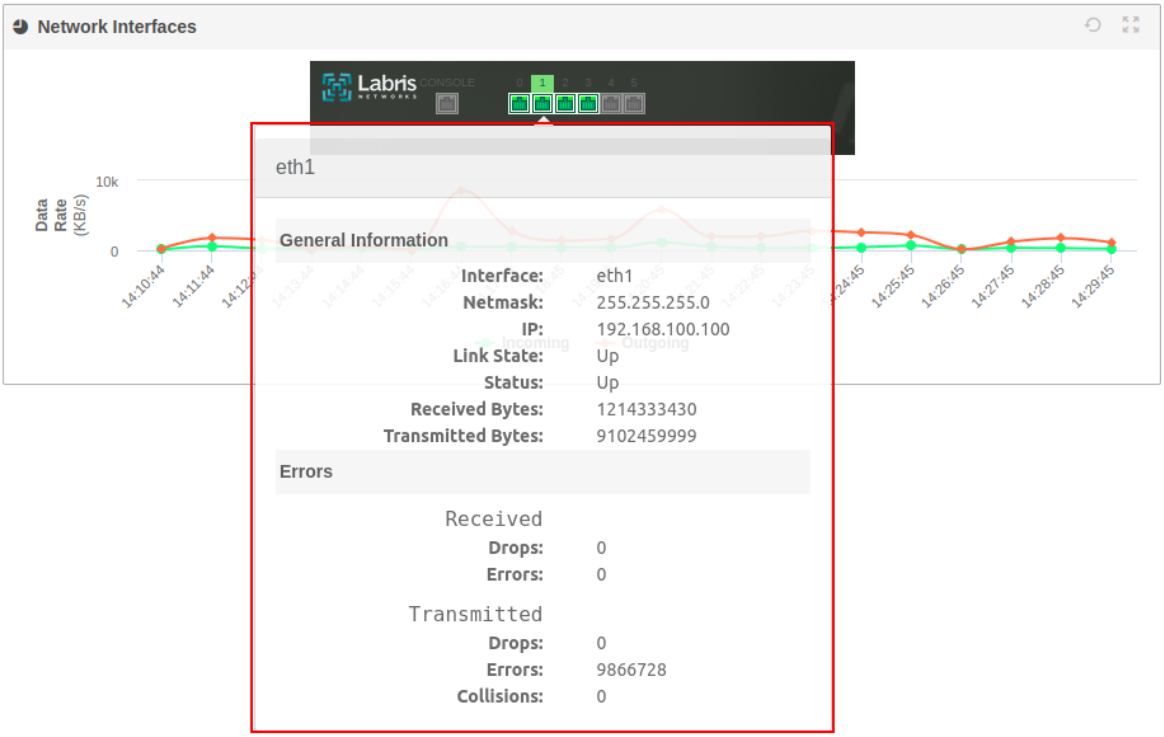
It shows the interfaces defined on the device and gives detailed information about the defined interfaces. If a cable is plugged in on the ports of the Labris device, it is green. If the cable is unplugged or the port is not in use, it will be grayed out. In this way, information about the cables connected to the device is obtained.



1	**Interfaces**	The port information of the interfaces and the port to which the cable is connected are displayed. If there is a cable connected to the port, it appears in green, and if the cable is not connected, it appears in gray.
2	**Incoming/Outgoing Packets**	The time interval of inbound/outbound packets is displayed in KB/s. A green chart shows incoming packets, while an orange chart shows outgoing packets.

Note

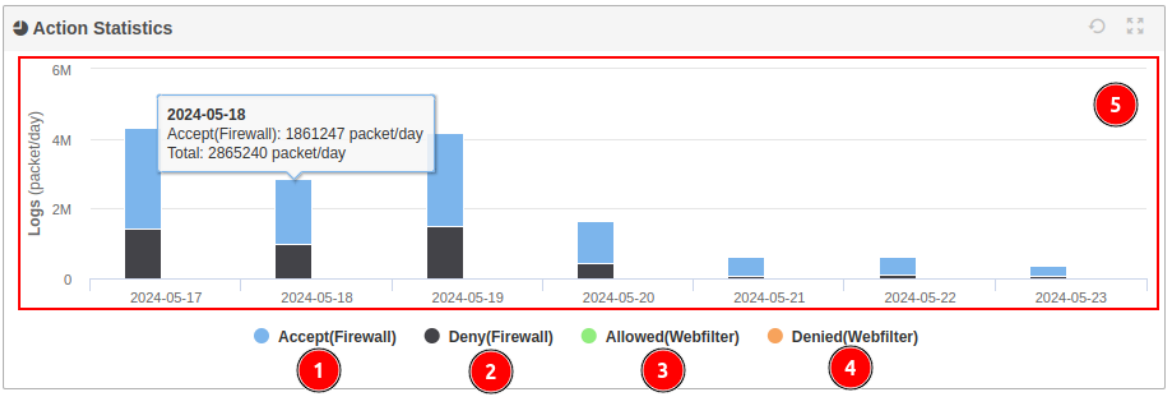
To see the number of allowed or blocked traffic on the graph, the first cursor must be on the column to which you want to check the number.



When the cursor above is moved to Port1, it shows detailed information about Port1. It shows interface information, IP and network mask, link status, received and sent data, and incoming information. In the Errors section, it shows the errors in the received and sent packets.

9.1.6 Action Statistics

Action statistics graphically show the number of traffic that passes through the firewall and web filter rules in the policies module, whether it is allowed or blocked. The data kept in Action Statistics is 7 days of data.

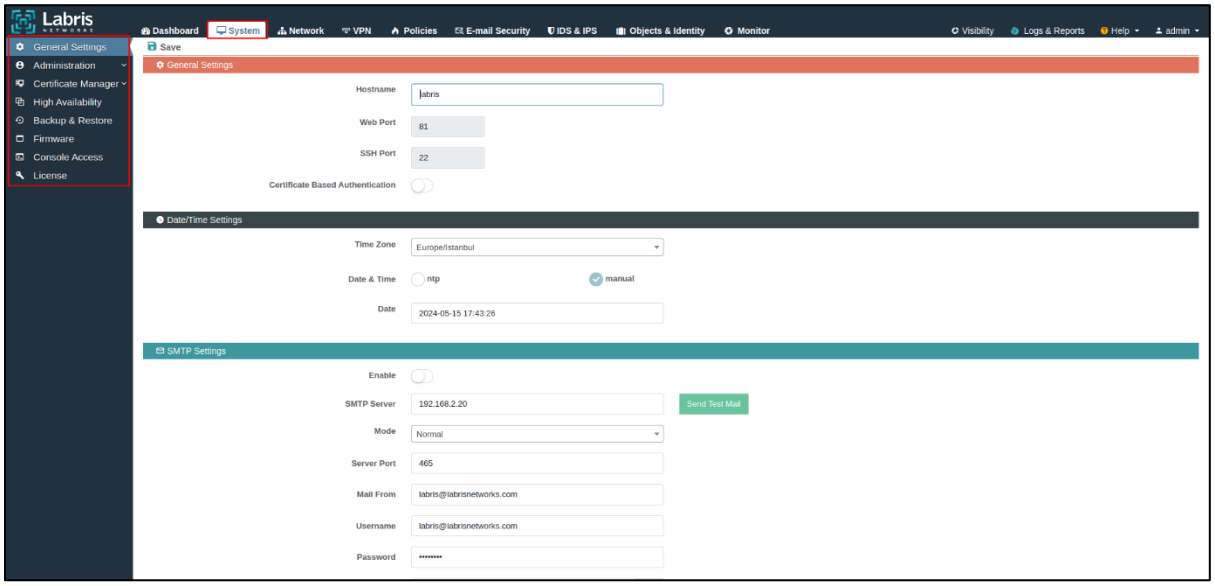


1	**Accept(Firewall)**	Shows a graph of the traffic that has passed through the firewall rules in the Policy module with permission. It is light blue in color.
2	**Deny(Firewall)**	Shows a graph of traffic that has been blocked by the firewall rules in the Policy module. It is black in color.
3	**Allowed(Webfilter)**	Shows a graph of the traffic that passes through the web filter users in the Policies module with permission. It is green in color.
4	**Denied(Webfilter)**	Shows a graph of the traffic that passes through the web filter used in the Policies module as blocked. It is orange in color.
5	**Graphic**	Graphically shows the traffic that passes through the firewall and web filter rules. It graphically shows 7 days of data.

10. System

In the system module, the name of the device is determined, and web and SSH port information is assigned. In addition, the users who will be authorized to access the device and their authorization settings are regulated. In this module, the certificate is created and the configuration settings of the devices are made for the redundancy structure (active/active or active/passive). Backups of the settings on the device are taken and software updates are performed. The IP address to be authorized to access the device is added, and finally, the license information is displayed.

All of the above-mentioned operations are performed in the System Module. When the System Module is clicked, the General Settings module appears as the welcome screen.

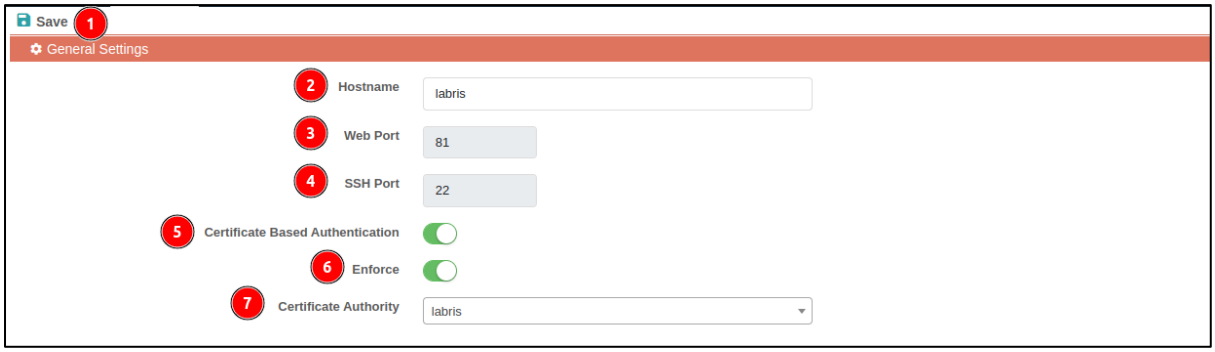


10.1 General Settings

The device's name, web port, SSH port, date and time settings, and SMTP settings are displayed, and the default settings are changed here. The General Settings tab is divided into three sections. These are General Settings, Date and Time Settings, and SMTP Settings.

10.1.1 General Settings

It shows the name, ssh, and web port of the device defined on the device. Using the General Settings module, the device name is changed, and the added certificate is added in the Certificate Management module.



1	**Save**	Saves the changes made in the incoming Settings module.
2	**Hostname**	Indicates the name of the device. To change the name of the device, the device name is changed by typing the server name you want and pressing the save button.
3	**Web Port**	Indicates the port that allows connecting to the web interface. (e.g. 192.168.1.1:81)
4	**SSH Port**	Indicates the port that allows connecting to SSH.
5	**Certificate-Based Authentication**	It is a button that allows you to connect to the web interface with a certificate. In this way, it can be connected to the device that has the certificate added in the Certificate Management module.
6	**Enforce**	It makes it mandatory to connect with a certificate when connecting to the web interface.

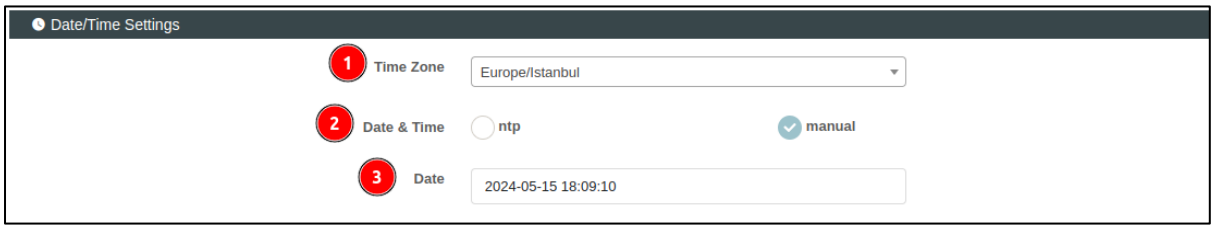
7	**Certificate Authority**	The certificate authority added in the Certificate Management module is selected.

Note

When you change the web and ssh ports, your connection may drop. For this reason, it is disabled for security reasons.

10.1.2 Date / Time Settings

The date and time of the device are set manually or via an NTP server in the Date/Time Settings section found in the General Settings tab.

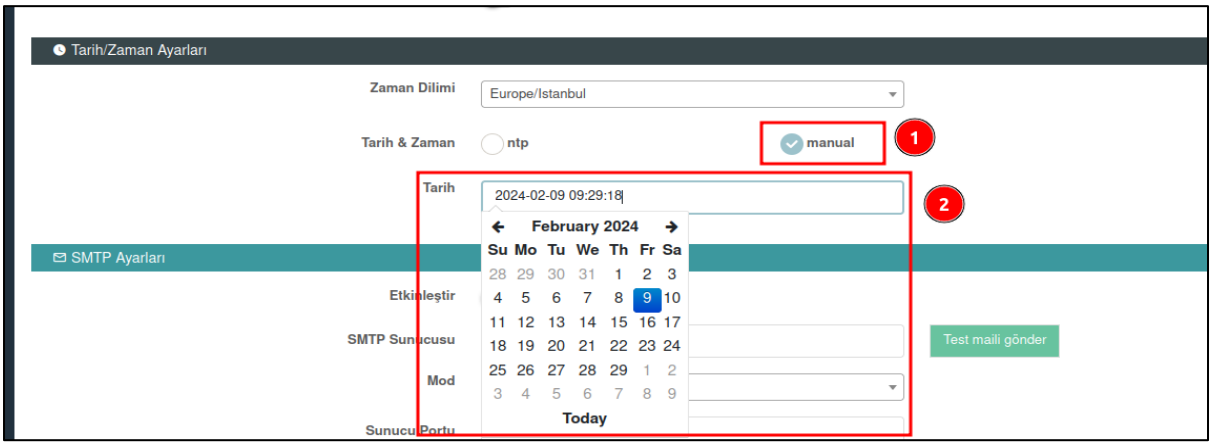


1	**Time Zone**	It is used to set the date and time of the device according to the time zone.
2	**Date &Time**	It is used to add the date and time of the device from the NTP server or manually.
3	**Date**	When the manual is selected, the date and time can be adjusted. When NTP is selected, date and time settings are made according to the added NTP server.

-If the manual is selected in the Date & Time Settings section, the following steps are followed:

1. The manual must be marked in the Date & Time section.

2. The date is set manually from the calendar.



Note

After any changes made in the Date/Time Settings section, you should save the transactions made by clicking the Save button in the General Settings tab.

-If NTP is selected in the Date & Time Settings section, the following steps are followed:

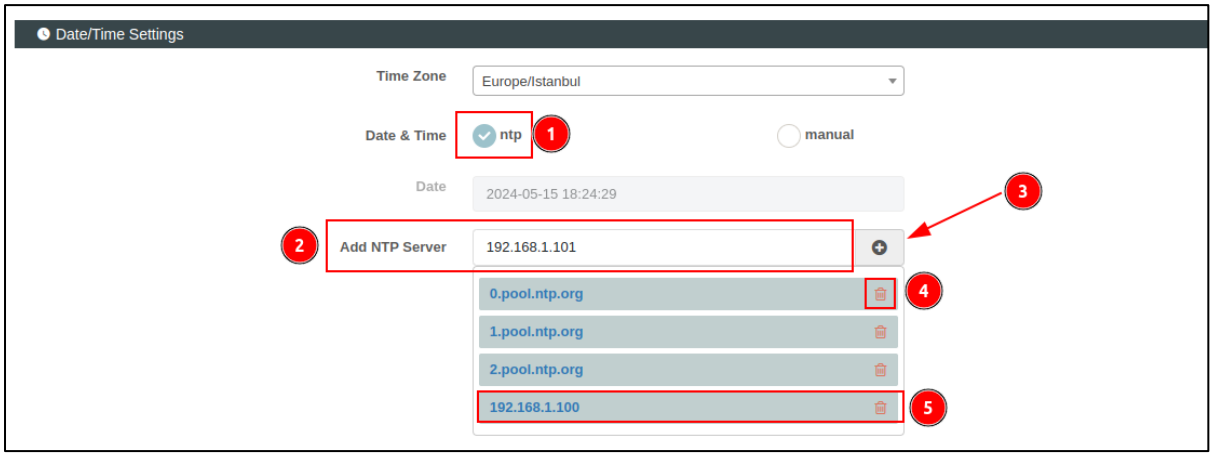
1. NTP must be marked in the Date & Time section.

2. By default, another IP or domain address is entered other than 0.pool.ntp.org, 1.pool.ntp.org, and 2.pool.ntp.org.

3. After entering the IP or domain address of the NTP server, the addition process is done by pressing the add button.

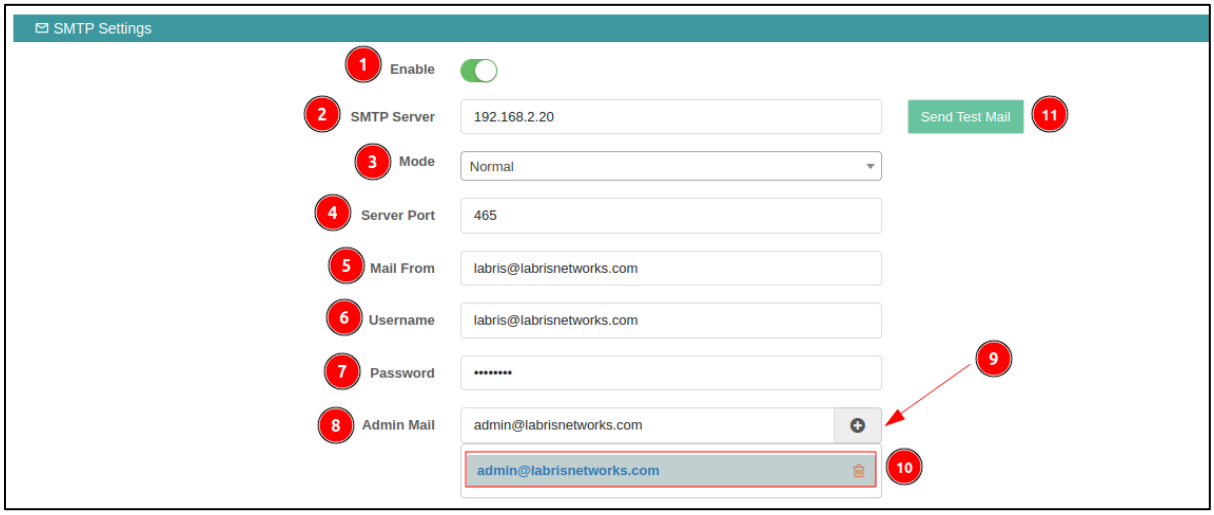
4. If you want to delete the NTP server you have added, you can delete it by pressing the delete button.

5. The added NTP server is added to the end of the list.



10.1.3 SMTP Settings

It is the section where SMTP server settings are made on the Labris UTM device. When this section is configured, an information e-mail is received about the operating status of the device. Within the scope of the incoming mail, it sends an information e-mail in cases such as services that do not work on the device, disk status, etc. In addition to these, when SMTP is enabled, it sends an e-mail to the administrator e-mail address attached in the cases where the backup is taken in the Setting Backup tab.



1	**Enable**	It is the button where the STMP settings are enabled.
2	**SMTP Server**	It is where the domain address of the SMTP server is entered.
3	**Mode**	This is where the encryption mode of the SMTP server is selected.
4	**Server Port**	This is where the port of the SMTP server is entered. Ex. 465
5	**Mail From**	This is the section where the sender address of the incoming mail is entered. The mail will be sent to the e-mail address written here. Ex. labris@labrisnetworks.com
6	**Username**	SMTP is where the user name of the mail address opened on the server is written. Ex. labris@labrisnetworks.com

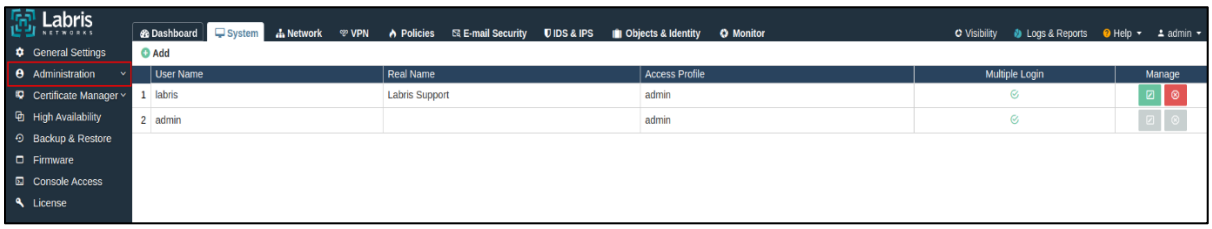
7	**Password**	SMTP is the place where the password of the mail address opened on the server is written.
8	**Admin Mail**	This is where the administrator address to which the mail will be sent is entered. Ex. yonetim@labrisnetworks.com
9	**Add an Admin Mail Address**	This is where the e-mail address of the administrator you want to add is written. Ex. destek@labrisnetworks.com
10	**Admin Mail Address List**	Shows the list of added admin mail addresses.
11	**Send Test Mail**	After the SMTP settings are made, a test email is sent for testing purposes, and the SMTP settings are tested.

Note

After any changes made in the SMTP Settings, you should save the transactions made by clicking the Save button in the General Settings tab.

10.2 Administration

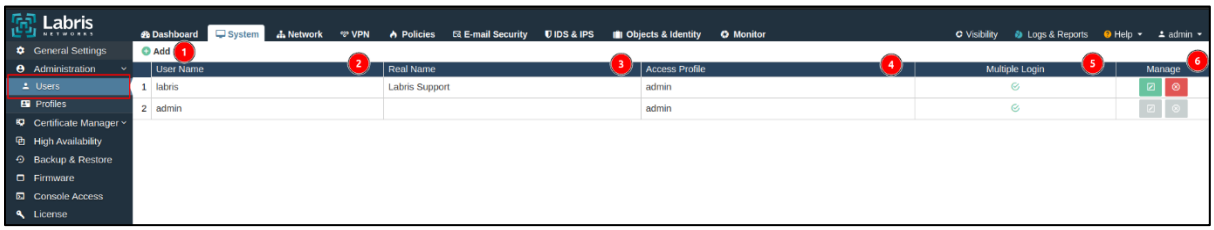
It is the tab where the users who will be authorized to access the web interface of the Labris UTM device are added and the profiles (authorizations) specific to the added users are set. It has two sub-tabs for users and profiles.



By default, the admin user comes. The password of the admin user comes as a Labris after the first installation.

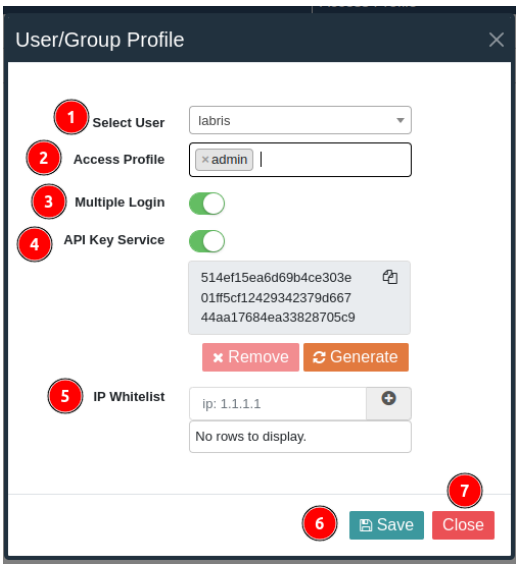
10.2.1 Users

It is the tab where users who will access the web interface are added. In order to add a user, it is first necessary to add a user from the Identity tab in the Objects and Identity module.



1	**Add**	It is the button to which the user who will access the device is added.
2	**Username**	This is the section where the name of the user who is authorized to log in to the Labris UTM device is displayed.
3	**Real Name**	This is the section where display real name of added admin user.
4	**Access Profile**	This is the section where the access authorization of the admin user is displayed.
5	**Multiple Login**	This is the section where the multiple login permission of the added admin user is displayed. A user who has been granted multiple entries can log on to more than one computer.
6	**Manage**	The added admin is the section where the user is deleted or the information about the user is changed.

-It is necessary to press the add button to add users. Once pressed, we must select the added user in the Objects and Identities module. After pressing the Add button, the following screen appears.

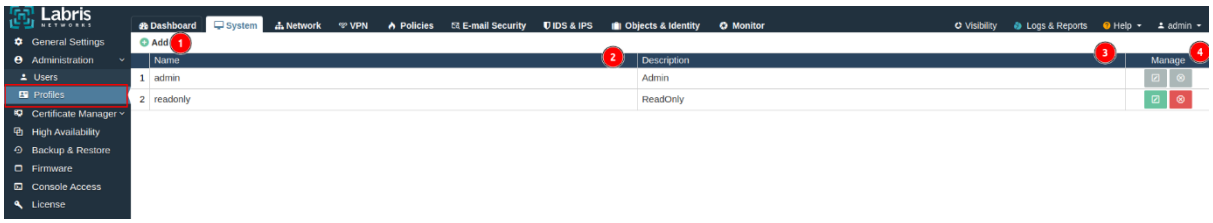


1	**Select User**	Users created in the Objects and Identities module are selected to be granted access authorization.
2	**Access Profile**	Users who are authorized to access the web interface are granted profile access authorizations. When a profile is created for the VPN module and a profile is assigned to the user, the user only shows the VPN module.
3	**Multiple Login**	This is where more than one login authorization is enabled for the user who has been granted access.
4	**API Key Service**	It is the key generated for authentication by the user who will be granted access. The API key is regenerated or deleted.
5	**IP Whitelist**	This is the section where the IP address that does not require an API Key is entered.
6	**Save**	It is the button where the settings of the user who will be authorized to access the web interface are saved.
7	**Close**	It is the button where the window opens after the Add

		button is pressed.

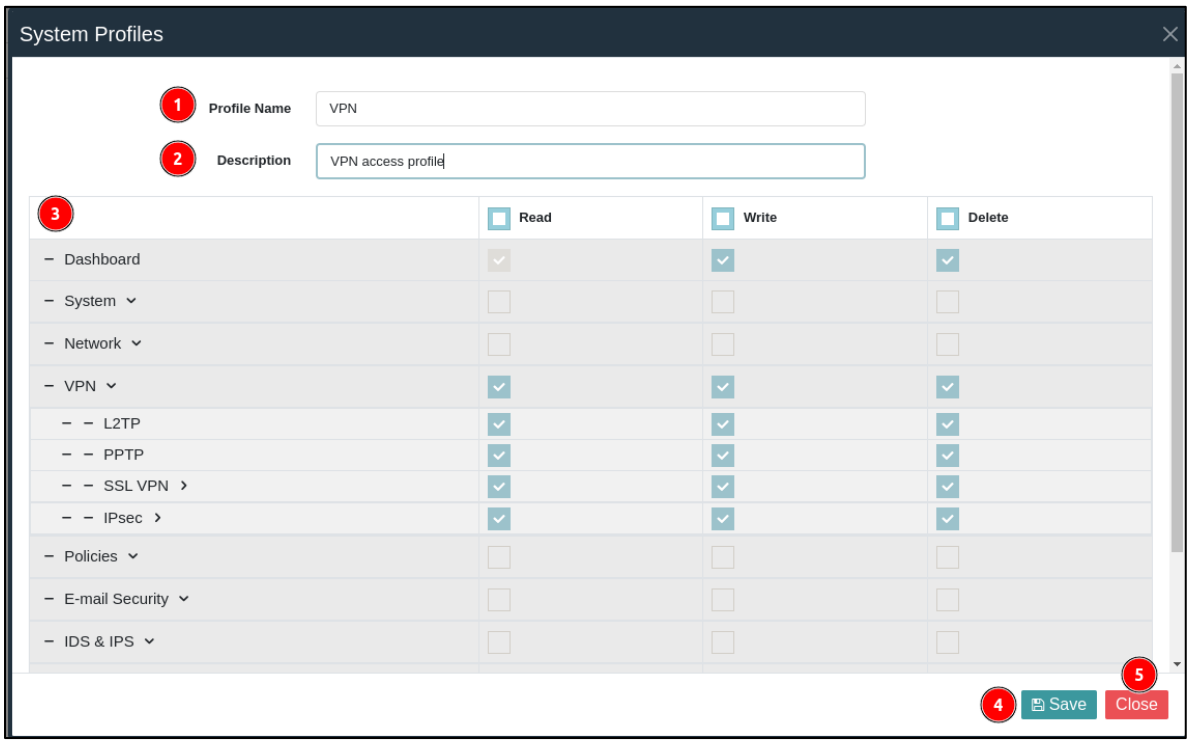
10.2.2 Profiles

It is the tab where the profile settings of the users who will be authorized to access the web interface are made. On the Profiles tab, the user is authorized to access the modules that they can access. By default, there are two profiles.



1	**Add**	It is the button where the profile of the user who will be connected to the Labris UTM device is added.
2	**Name**	This is the section where the name of the added profile is displayed.
3	**Description**	This is the section where the description of the added profile is displayed.
4	**Manage**	It is the section where the authorizations of the added profile are edited or deleted.

-Click the add button to add a profile. After clicking the Add button, the following screen appears.



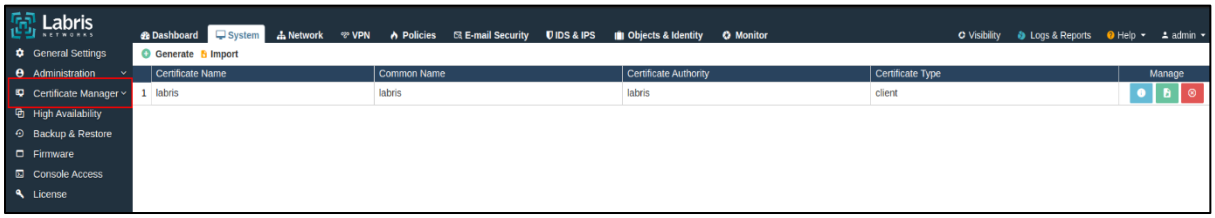
1	**Profile Name**	It is the place where the name is entered in the profile to be created. Ex. VPN
2	**Description**	It is the place where the description of the profile that will be created is written.
3	**Modules to be Authorized**	The module to be given management authority is selected by the user who will be given management authority. Read, write, and delete authorizations are granted for the module.
4	**Save**	It is the button where the settings are saved after the profile is set.
5	**Close**	It is the button where the window opened by clicking the Add button is closed.

Note

If the management authority module exists in other modules, the created profile is not saved. Ex. You need to grant VPN privileges to the user who is allowed to the objects and identities module.

10.3 Certificate Manage

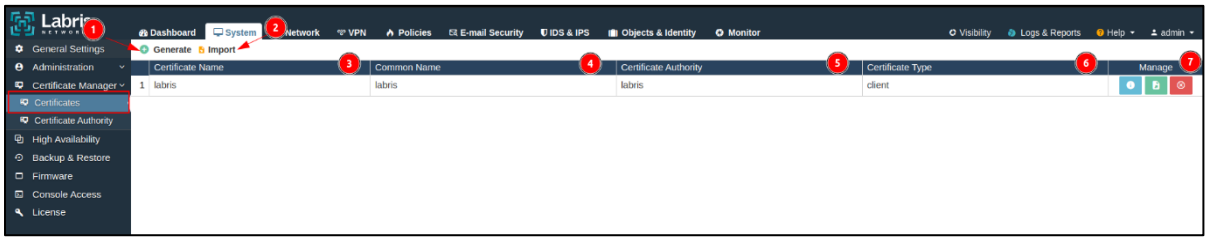
The Certificate Management tab allows the creation of certificates within the device. The generated certificate can also be user-based. The generated certificate uses SSL to access the web interface. In order to access the web interface with a certificate, it is necessary to activate the certificate in the General Settings module.



There are two sub-tabs on the Certificate Management tab. These are Certificates and Certificate Authority.

10.3.1 Certificates

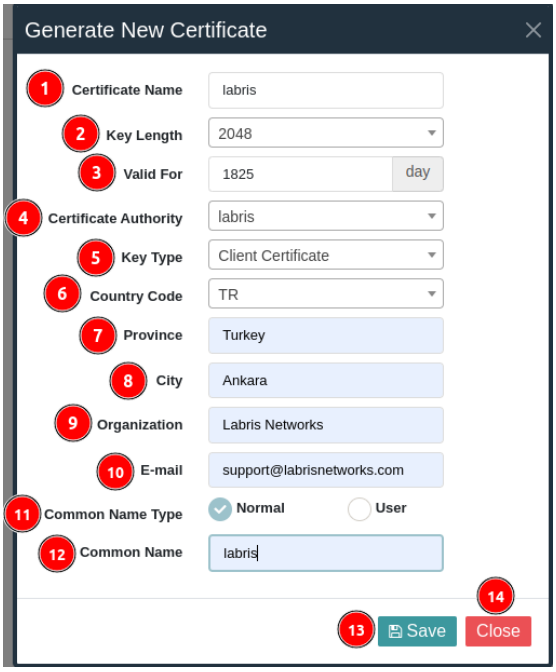
This is the tab on which the certificate is created on the device or where the generated certificate is added to the device. The certificate created on the Certificates tab is created in the client, and the client-based certificate is created. In addition, the generated certificate can be regular or user-based.



1	**Generate**	It is used to create certificates.
2	**Import**	It is used to add another certificate that has already been created to the device.
3	**Certificate Name**	The name of the generated certificate appears.

4	**Common Name**	The common name of the generated certificate appears.
5	**Certificate Authority**	Indicates the authority of the generated certificate.
6	**Certificate Type**	Indicates the type of certificate that was created. There are two types: Client and Server.
7	**Manage**	This is the section where the contents of the created certificate are displayed, and the certificate is downloaded and deleted.

-Click the Create button to create a certificate. After clicking the Create button, the screen that appears is as follows.

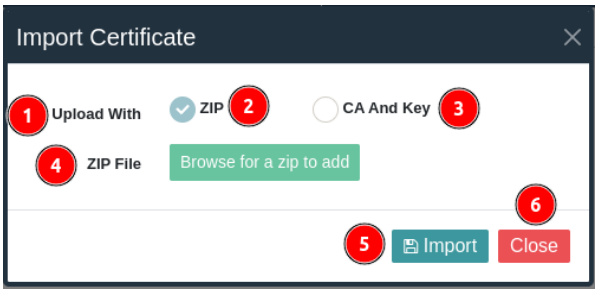


1	**Certificate Name**	This is the section where the name of the certificate to be created is entered.
2	**Key Length**	This is the section where the key length of the certificate to be created is selected. Select the length of the bits for which the encryption will be performed. The bit length is chosen from 1024, 2048, and 4096 lengths.

3	**Validity Period(Days)**	The validity period of the certificate to be created is entered. The entered validity period is determined by the day. Ex. After 1825 days, the validity period of the certificate expires.
4	**Certificate Authority**	This is where the authority created on the Certificate Authority tab is selected.
5	**Key Type**	This is where the key type of the certificate is selected. There are two key types: Client and Server.
6	**Country Code**	This is where the country code of the certificate is selected. Ex. TR.
7	**Province**	It is where the state of the certificate to be created is entered. Ex. Turkey.
8	**City**	It is the place where the city name of the certificate to be created is entered. Ex. Ankara.
9	**Organization**	It is where the name of the organization is entered. Ex. Labris Networks.
10	**E-mail**	This is where the email address is entered. Ex. support@labrisnetworks.com
11	**Common Name Type**	It is the place where it is selected whether the certificate to be created will be normal or user-based.
12	**Common Name**	When it is selected as normal, the public key must be entered. When a user is selected, the user created in the Objects and Identities module is selected. If a user is selected, the use case of the certificate in the SSLVPN and web interface is indicated.

13	**Save**	It is used in cases where the certificate to be created needs to be saved after it has been configured.
14	**Close**	It is used in cases where the screen needs to be closed after clicking the Add button.

-Click the download button to add the created Certificate Authority. After clicking the download button, the screen that appears is as follows.



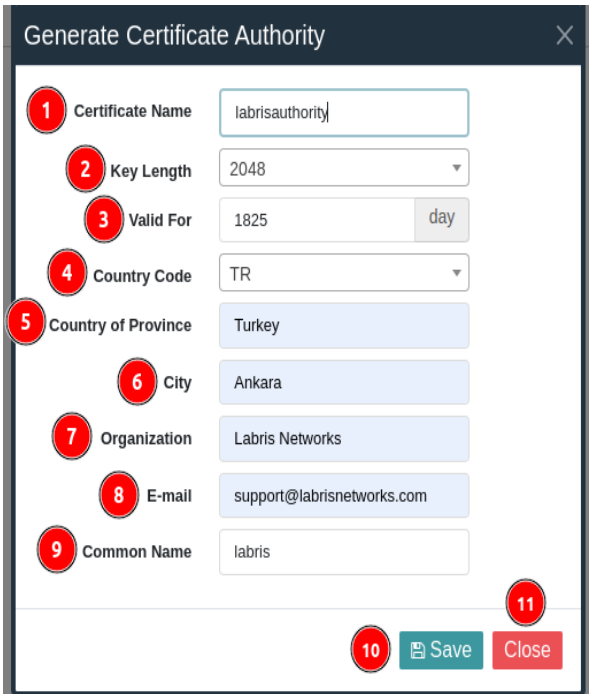
1	**Upload With**	Select the installation type of the Certificate Authority to be downloaded.
2	**ZIP**	It downloads the Certificate Authority via ZIP.
3	**CA and Key**	It downloads the Certificate Authority via CA and Key.
4	**ZIP File**	This is where the Certificate Authority that will be added from your computer is selected.
5	**Import**	This is the button where the selected Certificate Authority is downloaded.
6	**Close**	When the download button is clicked, it closes the window that opens.

10.3.2 Certificate Authority

An authority is created for the certificate created on the Certificates tab. Certificate authority that is not on the device can be added to devices.

1	**Generate**	It is used to establish the certificate authority.
2	**Import**	It is used to add another certificate authority outside of the device.
3	**Authority Name**	The name of the certificate authority is displayed.
4	**Common Name**	The common name of the certificate authority is displayed.
5	**Manage**	This is the section where the content of the created certificate authority is displayed, and the certificate authority is downloaded and deleted.

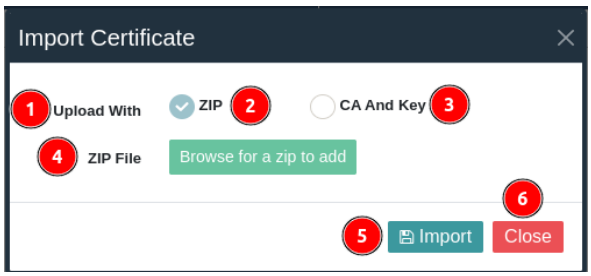
-Click the Create button to create a certificate authority. After clicking the Create button, the screen that appears is as follows.



1	**Certificate Name**	This is the section where the name of the certificate to be created is entered.
2	**Key Length**	This is the section where the key length of the certificate to be created is selected. Select the length of the bits for which the encryption will be performed. The bit length is chosen from 1024, 2048, and 4096 lengths.
3	**Valid For(Days)**	The validity period of the certificate to be created is entered. The entered validity period is determined by the day. Ex. After 1825 days, the validity period of the certificate expires.
4	**Country Code**	This is where the country code of the certificate is selected. Ex. TR.
5	**Country of Province**	It is where the state of the certificate to be created is entered.

		Ex. Turkey.
6	**City**	It is the place where the city name of the certificate to be created is entered. Ex. Ankara.
7	**Organization**	It is where the name of the organization is entered. Ex. Labris Networks.
8	**E-mail**	This is where the email address is entered. Ex. support@labrisnetworks.com
9	**Common Name**	It is the place where it is selected whether the certificate to be created will be normal or user-based.
10	**Save**	It is used in cases where the certificate to be created needs to be saved after it has been configured.
11	**Close**	It is used in cases where the screen needs to be closed after clicking the Create button.

-Click the Download button to add the created Certificate Authority. After clicking the download button, the screen that appears is as follows.

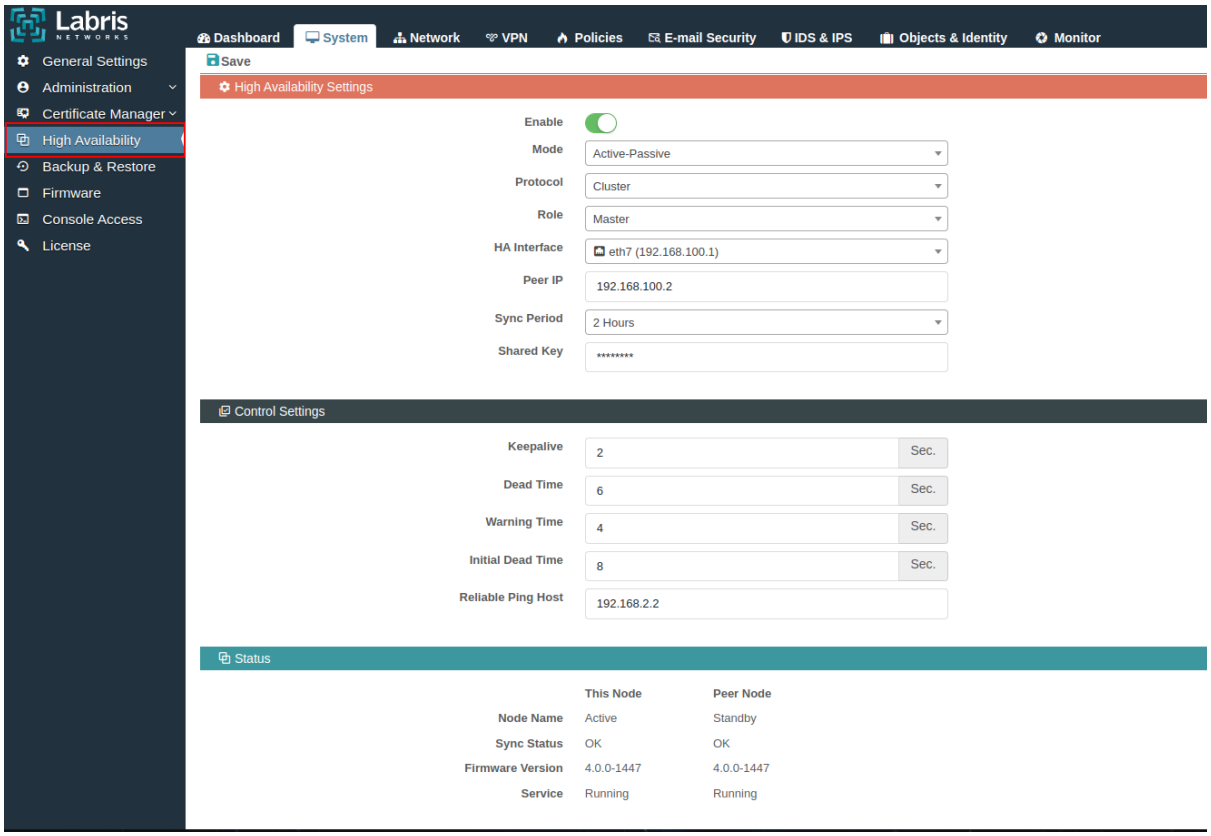


1	**Upload With**	Select the installation type of the Certificate Authority to be downloaded.
2	**ZIP**	It makes the download process of the Certificate Authority to be downloaded with ZIP.
3	**CA and Key**	It downloads the Certificate Authority to be downloaded with its CA and Key.

4	**ZIP File**	This is where the Certificate Authority that will be added from your computer is selected.
5	**Import**	This is the button where the selected Certificate Authority is downloaded.
6	**Close**	When the download button is clicked, it closes the window that opens.

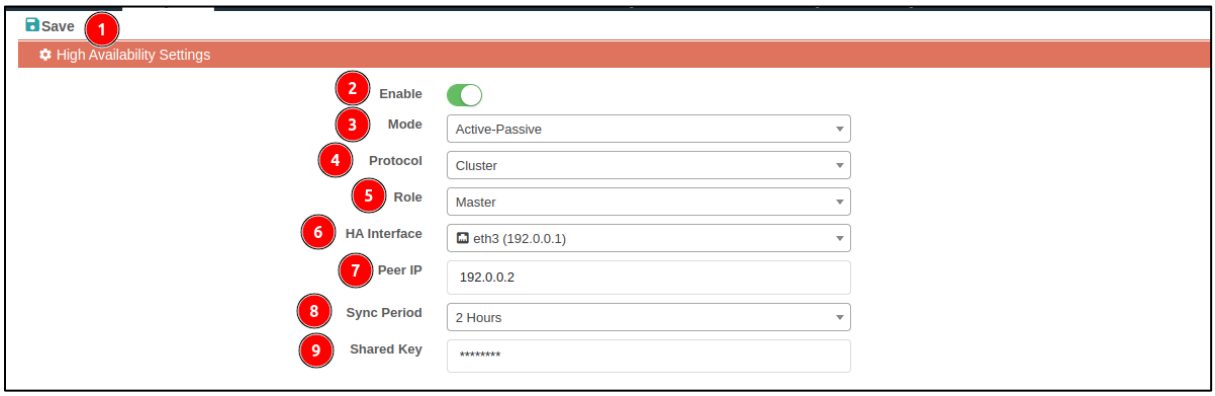
10.4 High Availability

It is the module where the high availability settings of Labris devices are made. It occurs when two devices back up each other, and in cases where one of the devices breaks down or malfunctions, a redundancy structure occurs when it switches to the passive device. Running devices will work as active-active or active-passive.



10.4.1 High Availability Settings

In the High Availability Settings section, the redundancy settings of the devices are made, and the protocol information, the interface to be redundant, and the pairing period of the device are selected.



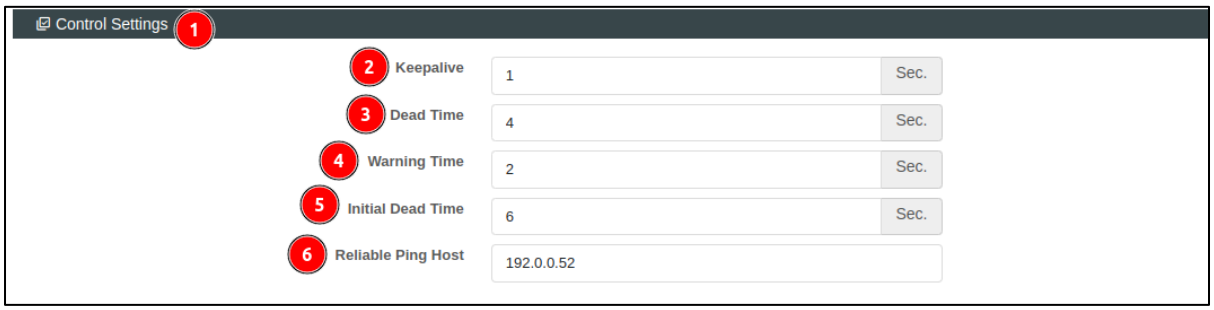
1	**Save**	It is the button where the redundancy configuration is saved.
2	**Enable**	It is the button where the redundancy settings are enabled.
3	**Mode**	It is the section where redundant devices are set as active-active or active-passive.
4	**Protocol**	The protocols of the devices that will work redundantly are selected. It is necessary to choose the protocol as a VRRP or a Cluster. When VRRP is selected, it looks at the state of the selected interface. When Cluster is selected, a reliable ping server must be entered, and it looks at the status on the ping server.
5	**Role**	The task of the device to be configured as redundant is selected. If Task Active is selected, the device you configured will continue its task until it is delegated to the passive device.
6	**HA Interface**	It is the section where the interface to be redundant is selected.
7	**Peer IP**	Redundant is the section where the IP address of the other device to be configured is entered.

8	**Sync Period**	The pairing period for the configuration of the device is selected. Pairing is done on active-passively installed devices by switching the configuration on the active device to the passive device.
9	**Shared Key**	This is the section where the shared key for the devices is entered.

10.4.2 Control Settings

Control Settings vary depending on the protocol selected in the High Availability Settings section.

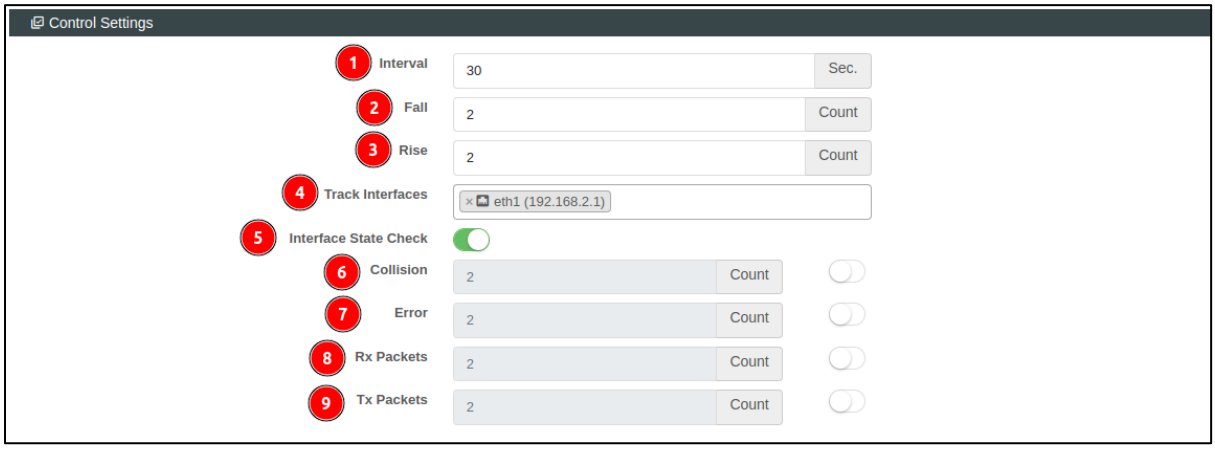
-If the protocol cluster is selected in the High Availability Settings, the following screen is edited.



1	**Control Settings**	It is the section where the control settings of redundant devices are made.
2	**Keepalive**	It is where the time to enter the time during which access to the trusted ping server will be tested.
3	**Dead Time**	This is the section where the time of discontinuation of access to the ping server is entered. Ex. If it cannot access it within 4 seconds, it transfers the task to the passive device at the end of 4 seconds.
4	**Warning Time**	If the ping receives a 2-second warning packet on accessing the server, it delegates the task to the passive device. The warning time is set in this section.
5	**Initial Dead Time**	It tests access to the ping presentation for 6 seconds from the time of death. When access to the ping server

		arrives, the active device takes over. When the ping server cannot be accessed, it remains on the passive device.
6	**Reliable Ping Host**	This is the section where the IP address of the server to which the device will ping is entered. The ping server written here can be a server running on an internal or external network.

-If the protocol VRRP is selected in High Availability Settings, the following screen is edited.

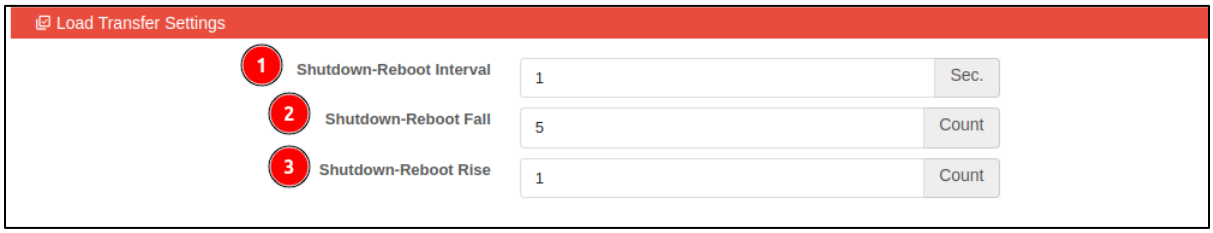


1	**Interval**	It is where the second is indicated, which controls the specified interface.
2	**Fail**	If it cannot reach 2 times in the second specified in the interval section, that is, 30 seconds, it transfers the task to the passive device.
3	**Rise**	If it reaches 2 times in the second specified in the increase section, that is, in 30 seconds, it continues the task.
4	**Track Interfaces**	It is the section where the interface to be controlled is selected.
5	**Interface State Check**	It is the section where checking the interface status is activated when desired.
6	**Collision**	This is the section where the collision values of the

		interface are entered.
7	**Error**	Error values in the packets coming to the interface are entered.
8	**Rx Packets**	Rx (Receiver) is specified in the number of packets.
9	**Tx Packets**	Tx (Transmitted) is specified as the number of packets.

10.4.3 Load Transfer Settings

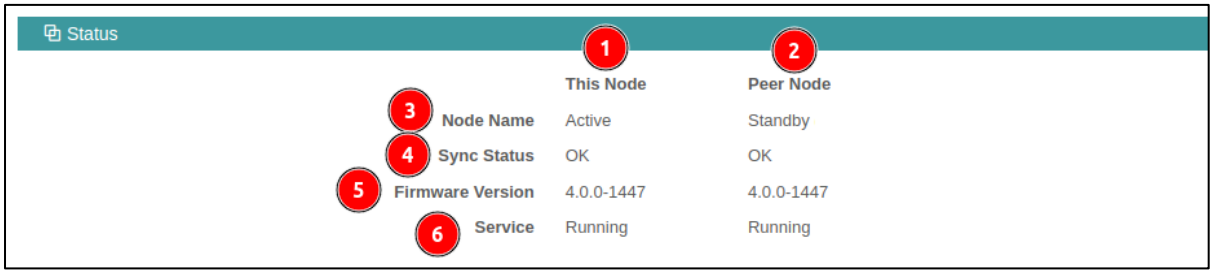
The protocol selected in High Availability Settings is turned on if it is VRRP. When VRRP is selected, the following section appears.



1	**Shutdown-Reboot Interval**	It is time to delegate the task to the **Passive** device in case of a problem with the interface followed by the actively running device.
2	**Shutdown-Reboot Fail**	It refers to the process of switching into operation as a result of the shutdown or restart of the actively operating device.
3	**Shutdown-Reboot Rise**	It refers to the time to compile the task in the case of power-on in the process of shutting down and restarting the actively running device.

10.4.4 Status

It is the section where the status of the devices set as backups is checked.



1	**This Node**	Shows the status information of the device connected to the web interface.
2	**Peer Node**	The status of the co-tasking device is displayed.
3	**Node Name**	The names of the redundant devices are displayed.
4	**Sync Status**	The pairing status of redundant devices is displayed.
5	**Firmware Version**	Shows the version information of the devices.
6	**Service**	Shows the operating status of the devices.

-The status information on the passively operating device should be as follows.

Note

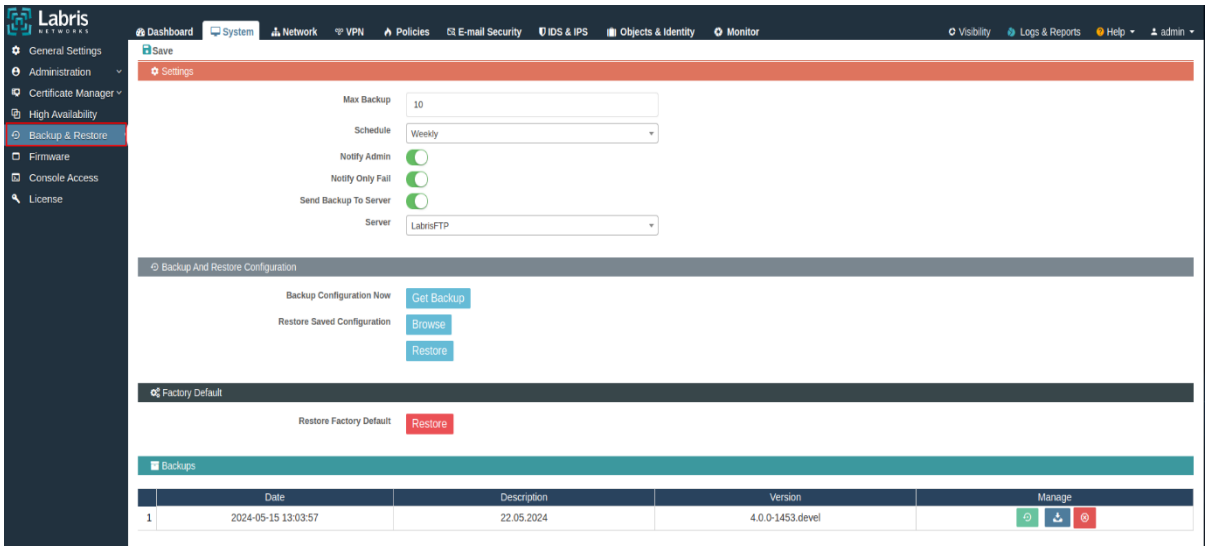
When Active is written in the node name, it indicates that the device is active. In the case of standby, it indicates that the device is waiting to receive the task from the Active device.

Note

When the settings are made in the redundancy module, it should not be forgotten to save the settings by clicking the Save button.

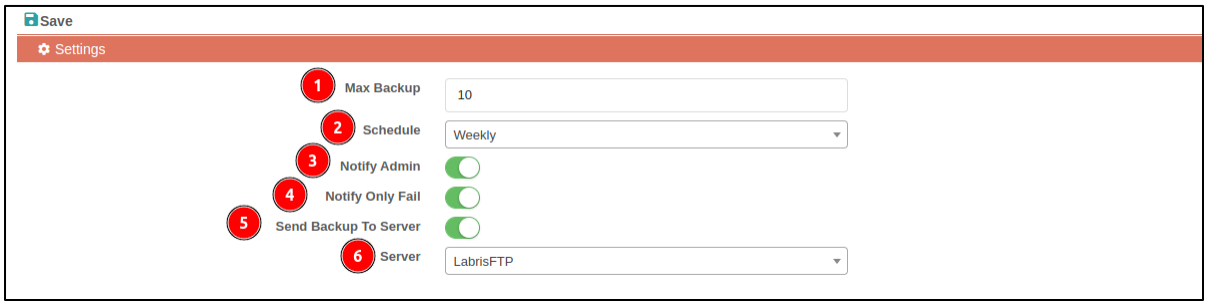
10.5 Backup & Restore

It is the module where the settings of the device are backed up, the backups taken are sent to the FTP server, and the backups are returned.



10.5.1 Settings

It is the section where the backups to be taken from the device are backed up to a server. Here, daily, weekly, and monthly backups are taken to the selected FTP server or device.

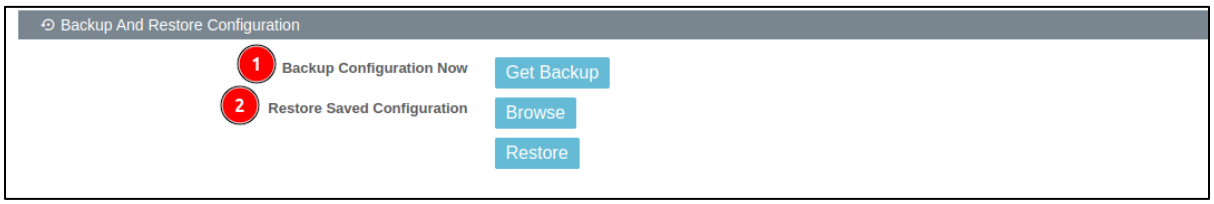


1	**Max Backup**	It is the section where the number to be saved is selected. Ex. If 10 is selected, it deletes the first backup it took.
2	**Schedule**	The time to take a backup is selected.

3	**Notify Admin**	When the backup is taken, it sends an e-mail to the administrator with the SMTP server in the General Settings module.
4	**Notify Only Fail**	Reports an error received during backup.
5	**Send Backup to Server**	**It** is used in cases where FTP needs to send backups to its server.
6	**Server**	The FTP server set in Objects and Identify is selected.

10.5.2 Backup and Restore Configuration

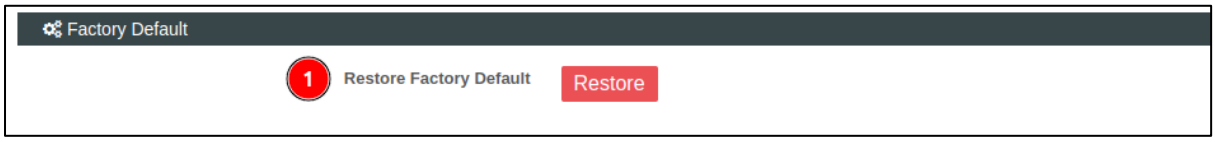
It is used in cases where it is necessary to manually take a backup from the device. The main purpose of this section is to take configuration backups from the device or to restore the configuration backups taken to the device.



1	**Backup Configuration Now**	This is the button where the configuration settings are backed up.
2	**Restore Saved Configuration**	These are the buttons where the previously taken configuration backup is selected, and the selected configuration backup is restored.

10.5.3 Factory Default

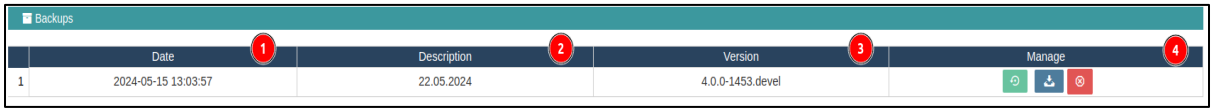
It is the section used when it needs to return to factory settings.



1	**Restore Factory Default**	It is the factory reset button.

10.5.4 Backups

This is the section where the backups taken from the device are displayed.



1	**Date**	Indicates the date when backups were taken.
2	**Description**	A description of the backup is displayed.
3	**Version**	Indicates the version from which the backup was taken.
4	**Manage**	It is the partition where the retrieved backup is restored, downloaded, and deleted.

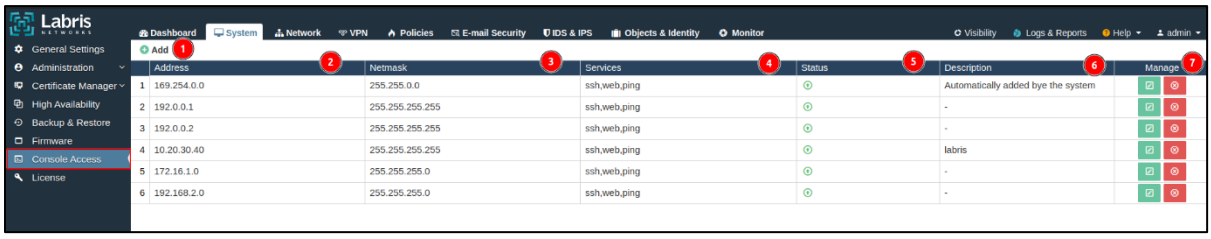
10.6 Firmware

It is the module where the software updates of the device are made and the version information of the device is displayed.

1	**Your Version**	The version of your device is displayed.
2	**Latest Firmware Version**	It is the button where the version update of the device is made.

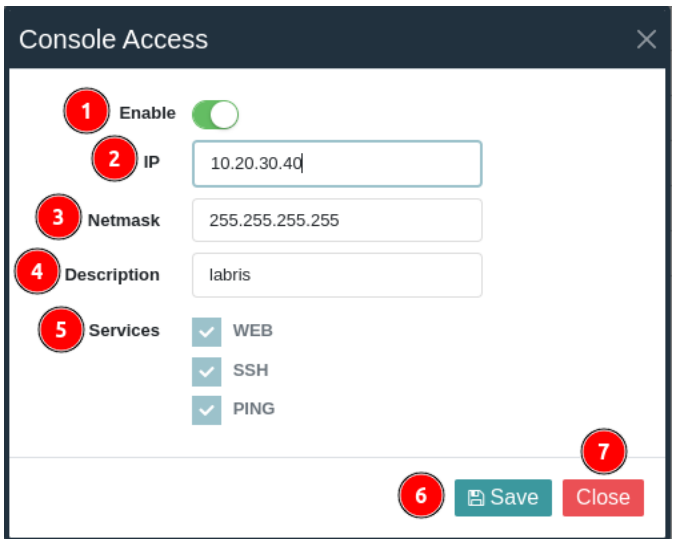
10.7 Console Access

It is the module where the public and private IP addresses that will be authorized to access the device are added, and access authorization is given to the added IP addresses. Access authorization can be set to ssh, web, and ping.



1	**Add**	This is where the IP address is entered for console access authority.
2	**Address**	The IP address that has been authorized to access the console appears.
3	**Netmask**	The netmask of the added IP address appears.
4	**Services**	The services that can be accessed by the IP address to be authorized to access the console are displayed.
5	**Status**	The status of the address to which access is authorized is displayed. If the status is green, it is active. If the status is red, it is passive.
6	**Description**	This is the section where the description of the IP address to be authorized is entered.
7	**Manage**	This is the section where the IP address that is authorized to access is changed or deleted.

-Click the add button to add the IP or network address to be authorized to access the console. After clicking the Add button, the following screen appears.

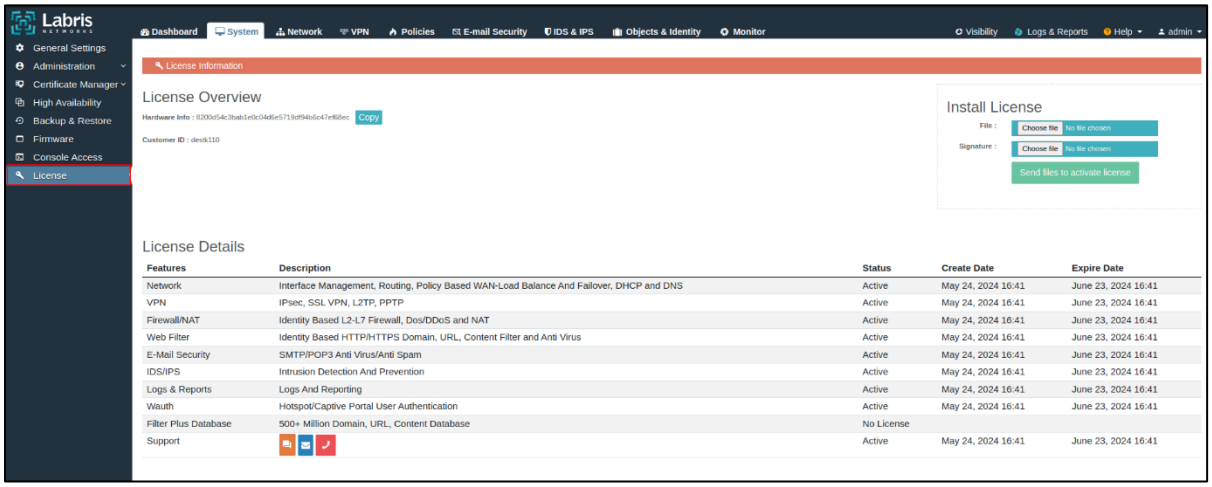


1	**Enable**	This is where console access authorized for IP or network addresses is enabled.

2	**IP**	Enter the IP address to which the console access will be authorized.
3	**Netmask**	The network mask of the IP address is entered.
4	**Description**	This is the section where the description associated with the IP address to be authorized to access the console is entered.
5	**Services**	It is the place where the services to be granted access authorization are selected.
6	**Save**	It is the button where the settings are saved.
7	**Close**	It is the button where the window that opens when the Add button is clicked is closed.

10.8 License

In the license module, the hardware code, license installation, and license details are displayed.



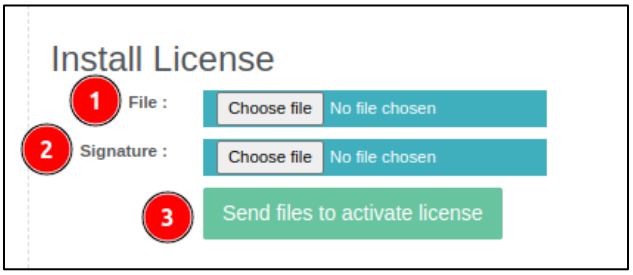
10.8.1 License Overview

In the license module, the hardware code, license installation, and license details are displayed.

1	**Hardware Info**	The hardware code of the device is displayed. The hardware code is used in the production of licenses.
2	**Customer ID**	The customer identification number is displayed.

10.8.2 Install License

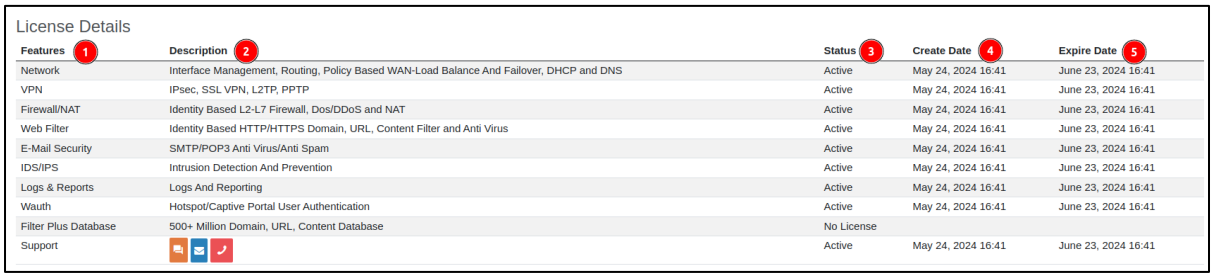
This is the section where the license created according to the Hardware Information in the Overview section is installed.



1	**File**	The file with the tar.gz extension produced according to the hardware information of the device is added.
2	**Signature**	A file with a sig extension produced according to the hardware information of the device is added.
3	**Submit files to activate the license**	It is the button used to activate the license after the added file and signature are selected.

10.8.3 License Details

In the Install License section, after the license is installed, the License Details are displayed.


License Details

Features 1	Description 2	Status 3	Create Date 4	Expire Date 5
Network	Interface Management, Routing, Policy Based WAN-Load Balance And Failover, DHCP and DNS	Active	May 24, 2024 16:41	June 23, 2024 16:41
VPN	IPsec, SSL VPN, L2TP, PPTP	Active	May 24, 2024 16:41	June 23, 2024 16:41
Firewall/NAT	Identity Based L2-L7 Firewall, Dos/DDoS and NAT	Active	May 24, 2024 16:41	June 23, 2024 16:41
Web Filter	Identity Based HTTP/HTTPS Domain, URL, Content Filter and Anti Virus	Active	May 24, 2024 16:41	June 23, 2024 16:41
E-Mail Security	SMTP/POP3 Anti Virus/Anti Spam	Active	May 24, 2024 16:41	June 23, 2024 16:41
IDS/IPS	Intrusion Detection And Prevention	Active	May 24, 2024 16:41	June 23, 2024 16:41
Logs & Reports	Logs And Reporting	Active	May 24, 2024 16:41	June 23, 2024 16:41
Wauth	Hotspot/Captive Portal User Authentication	Active	May 24, 2024 16:41	June 23, 2024 16:41
Filter Plus Database	500+ Million Domain, URL, Content Database	No License		
Support		Active	May 24, 2024 16:41	June 23, 2024 16:41

1	**Features**	The modules of the installed license are displayed.
2	**Description**	A description of the licensed modules is displayed.
3	**Status**	License status is displayed by features. If you have a license in the feature, it says active in the status line; if there is no license in the feature, it says no licence.
4	**Create Date**	The creation date of your license is displayed.
5	**Expire Date**	The expiration date of the license is displayed.

11.Network

In the Network menu, IP configuration, static routing, SD-WAN, DHCP, and DNS settings are made for the Labris UTM device. In this section, interfaces can be added, routing is written to the IP addresses we add, we can define your external links to SD-WAN, and a DHCP server can be defined for your local interfaces.

11.1 Interface

You can add IP under an interface where interfaces on the Labris UTM device are configured or as a alias. Apart from these, you can add bridge interfaces, VLANs, Connected interfaces, PPPoEs, and 3G/4G interfaces.

1	**Add**	It is the button where the alias, bridge interface, VLAN, bond interfaces, PPPoE, and 3G/4G interfaces are added.
2	**Interface**	It is the section where the name given to the system at the interface to be edited or added is displayed.
3	**Name**	The name of the edited or added interface is displayed.
4	**Interface Type**	The interface type of the modified or added interface is displayed.
5	**Status**	This is the section where the interface status is

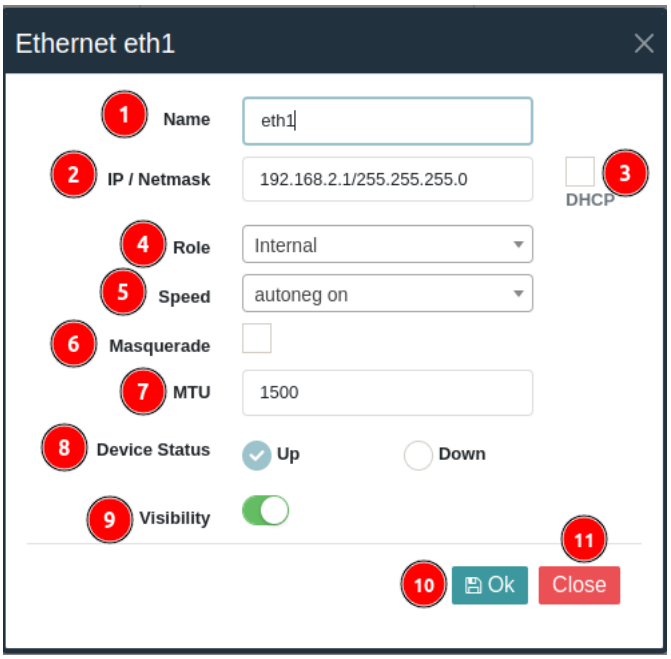
		displayed.
6	**IPv4 Address**	The IPv4 addresses of the interfaces are displayed.
7	**Role**	The role of the interface is displayed.
8	**MAC**	The MAC addresses of the interface are displayed.
9	**MTU**	The MTU value of the interface is displayed.
10	**Speed**	The speed of the interface is displayed.
11	**Manage**	It is the section where the statistics of the interface are displayed, the layout of the interface, or the deleted interface.

Note

The interfaces on the Labris UTM device cannot be deleted, they can be edited. Only added interfaces can be deleted.

11.1.1 Interface Editing

To edit the interface on the Labris device, click on the Edit button (green button) in the Manage section**.** You can edit according to your topology on the screen that appears. After clicking the Edit button, what comes up is as follows.

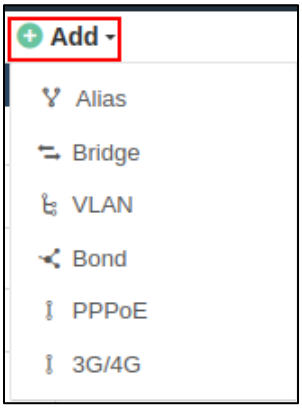


1	**Name**	Enter the name of the edited interface.
2	**IP/Netmask**	The edited interface IP and Netmask are entered.
3	**DHCP**	In cases where it needs to receive an IP from a device located in front of the interface, it must be marked.
4	**Role**	This is where the interface is set to internal (internal network) or external (external network).
5	**Speed**	It is the section where the speed of the interface is selected.
6	**Masquerade**	In cases where you have only one external network, it must be turned on. It is a dynamic address translation.
7	**MTU**	This is the section where the MTU value of the interface is entered.
8	**Device Status**	This is where the interface opens. It is the button used to activate the interface.
9	**Visibility**	Opens when the interface should be displayed in the traffic analytics menu.

10	**Save**	It is the button where the edited interface is saved.
11	**Close**	It is the button where the window that opens when the Edit button is clicked is closed.

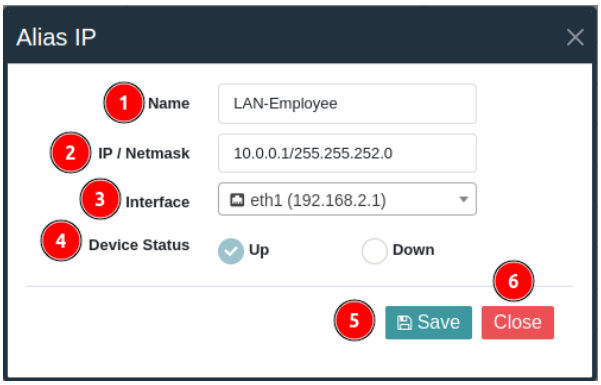
11.1.2 Adding an Interface

By default, on the Labris device, it is used to add interfaces outside of the interfaces. To add an interface, an interface is added by clicking the add button. After clicking the Add button, the screen that appears is as follows.



11.1.2.1 Alias

It is used in cases where it is necessary to add a virtual IP to the Labris device together with the Alias interface. The added Alias interfaces can be either internal or external networks.



1	**Name**	Enter the name to be given to the Alias interface to be added.

2	**IP / Netmask**	Alias Interface to be added is the part of the interface where the IP and subnet mask are entered.
3	**Interface**	Alias is the part of the interface under which the interface to be added is selected.
4	**Device Status**	This is the section where the Alias interface is enabled. If the Device State is up, the interface is active, and if Device Status is down, the interface is passive.
5	**Save**	It is the button where the settings are saved.
6	**Close**	It is the button that closes the window that opens when clicking on Nickname.

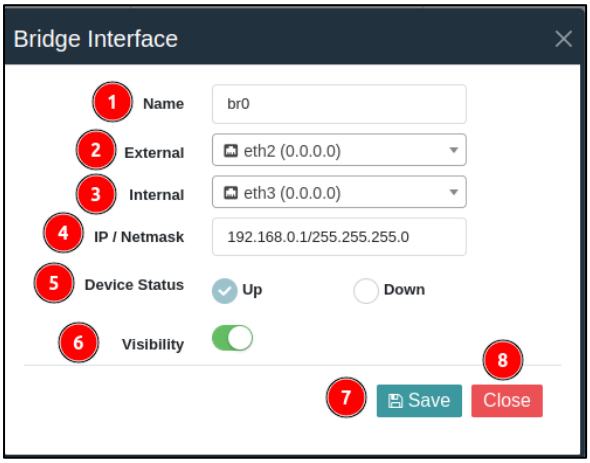
-The added Alias interface looks like this.

Note

The Added Alias takes on the role of the interface added to the interface below it. Ex. If the task of the added interface is Internal, the task of the added Alias is also Internal.

11.1.2.2 Bridge Interface

It is where the interfaces on the Labris device are bridged, along with the bridge interface. It is used in cases where it is not desired to change the configuration on the device in front of the Labris device.



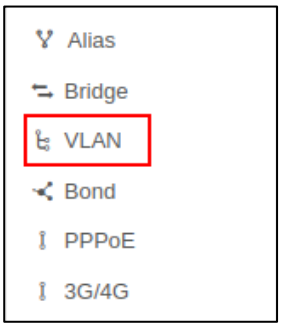
1	**Name**	Enter the name to be given to the bridge interface to be added.
2	**External**	It is where the interface that will be external (external network) is selected.
3	**Internal**	It is where the interface that will be internal (Internal network) is selected.
4	**IP / Netmask**	This is where information about the IP and network mask of the Bridge Interface is entered.
5	**Device Status**	This is the part where the device status of the bridge interface is specified. If the Device State is up, the interface is active, and if the Device Status is down, the interface is passive.
6	**Visibility**	In the Traffic Analysis module of the Bridge Interface, it is opened when it is desired to examine the traffic of the interface in detail.
7	**Save**	This is the button where the configuration made in the Bridge Interface is saved.

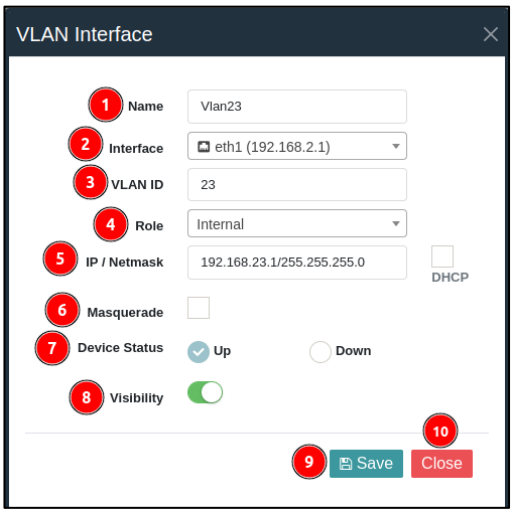
8	**Close**	This is the button that closes the window that opens after clicking on the Bridge Interface.

-The added Bridge Interface looks like the following.

11.1.2.3 VLAN Interface

It is used to define the VLAN interface to the Labris device. The VLAN configuration made on the switch can be defined on the Labris Device.





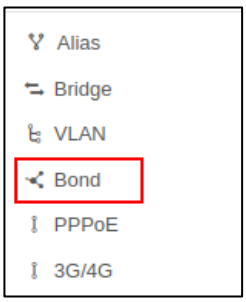
1	**Name**	Enter the name to be given to the VLAN interface to be added.
2	**Interface**	This is the section where the interface to be configured is selected.
3	**VLAN ID**	It is the place where the VLAN ID number designated on the switch is entered.
4	**Role**	VLAN is the section where the task of the interface is selected.
5	**IP / Netmask**	The VLAN is where the IP and Netmask information of the interface is entered.
6	**Masquerade**	It is the place where dynamic address conversion is turned on, on the VLAN interface.

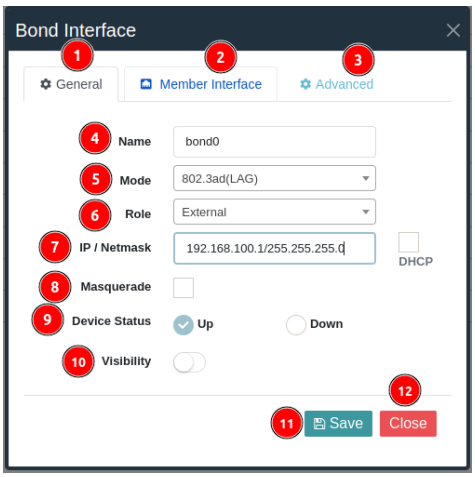
7	**Device Status**	This is the part where the device status of the VLAN Interface is specified. If the Device State is up, the interface is active, and if the Device Status is down, the interface is passive.
8	**Visibility**	In the Traffic Analysis module of the VLAN Interface, it is opened when it is desired to examine the traffic of the interface in detail.
9	**Save**	It is the button where the configuration made on the VLAN interface is saved.
10	**Close**	It is the button where the window that opens after clicking on the VLAN interface is closed.

-The added VLAN Interface looks like the following.

11.1.2.4 Bond Interface

It is used to define the Bond Interface to the Labris device. A redundancy structure is created by connecting the interfaces.

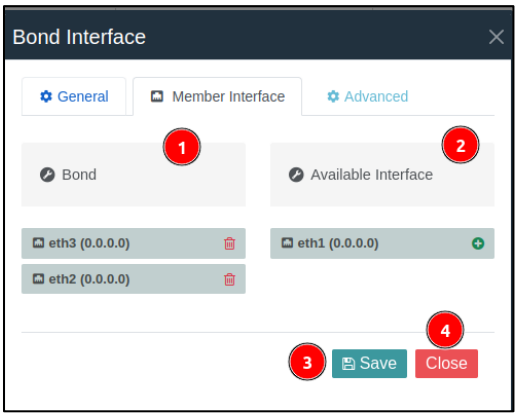




1	**General**	This is the tab where the general settings of the Bond Interface are made.
2	**Member Interface**	This is the tab where member interfaces are added to the bond interface.
3	**Advanced**	It is the tab where the advanced settings of the Bond

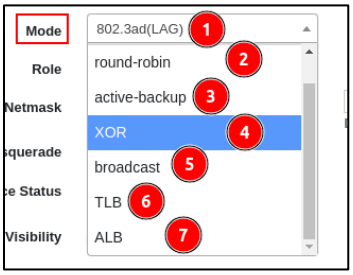
		Interface are made.
4	**Name**	This is the section where the name to be given to the bond interface is entered.
5	**Mode**	The operating mode of the Bond Interface is selected.
6	**Role**	This is where the bond interface is set to internal (internal network) or external (external network).
7	**IP / Netmask**	This is the section where the IP and netmask information of the bond interface is entered.
8	**Masquerade**	This is the button in the Bond Interface where dynamic address conversion is turned on.
9	**Device Status**	This is the part where the device status of the Bond Interface is specified. If the Device State is up, the interface is active, and if the Device Status is down, the interface is passive.
10	**Visibility**	In the Traffic Analysis module of the Bond Interface, it is opened when it is desired to examine the traffic of the interface in detail.
11	**Save**	It is the button where the configuration made on the Bond Interface is saved.
12	**Close**	It is the button where the window that opens after clicking on the Bond Interface is closed.

- The member interfaces of the Bond interface are added. To add a member interface, click on the Member Interface tab. After clicking, select the interface on the screen that appears.



1	**Bond**	This is the section where the interfaces added as members of the bond interface are displayed.
2	**Available Interface**	This is the section where the available interfaces that can be added as members of the bond interface are displayed.
3	**Save**	This is the button where the configurations made in the Bond Interface are saved.
4	**Close**	It is the button where the window that opens after clicking on the Bond Interface is closed.

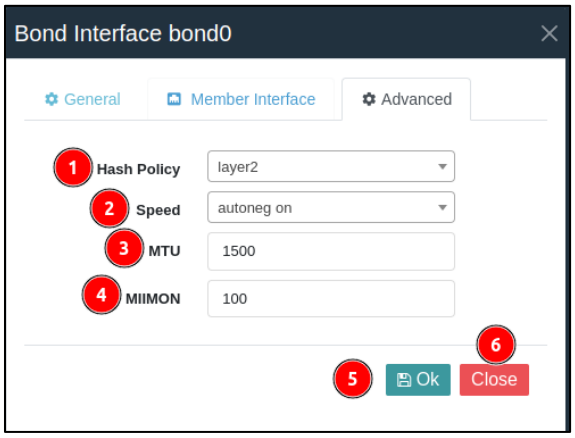
-The screen that comes up when the mode section is clicked is as follows.



1	**802.3ad (LAG)**	It is the protocol that allows you to combine multiple connections into a single connection.
2	**Round-robin**	It is an algorithm in which servers are selected sequentially and traffic is shared according to this

		order.
3	**Active-backup**	It works with active backup logic. Only one interface is active. If there is a problem with the actively running interface, it transfers the traffic to the passive interface.
4	**XOR**	The source MAC address sends packets according to the destination MAC address algorithm. Selects the same interface for each target.
5	**Broadcast**	Sends all packets to all interfaces.
6	**TLB**	The total load is shared by each interface according to its own load. The load of each interface is measured in proportion to its speed.
7	**ALB**	Both outbound and inbound traffic are load shared and do not require the support of a dedicated switching device.

- When the Advanced tab is clicked, the screen that appears is as follows.

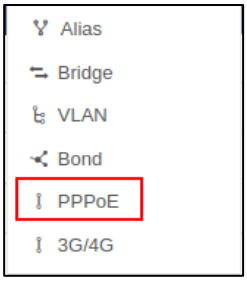


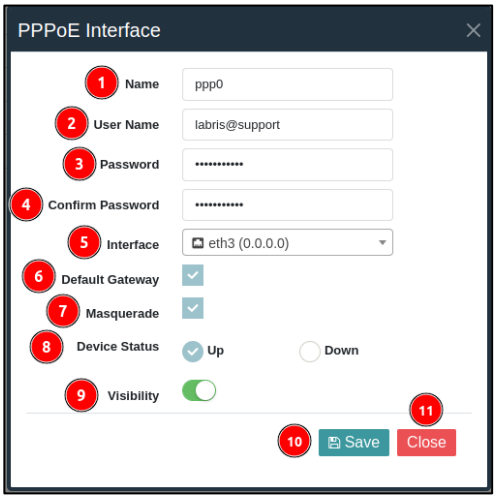
1	**Hash Policy**	Used in cases where XOR mode is selected.
2	**Speed**	It is where the speed of the interfaces that are connected is adjusted.
3	**MTU**	This is the part where the MTU value is entered.
4	**MIIMON**	The value at which the interface will be controlled is

		entered.
5	**Save**	It is the button where the interfaces set as Bond interfaces are saved.
6	**Close**	**It is the** button where the window that opens after clicking on the Bond Interface is closed.

11.1.2.5 PPPoE

In cases where the ADSL modem is put in bridge mode, the PPPoE interface is used on the Labris device. The username and password given by the Internet Service Provider (ISP) are defined by entering them correctly. If the information entered is correct, your external IP address appears in the IP section of the interface.

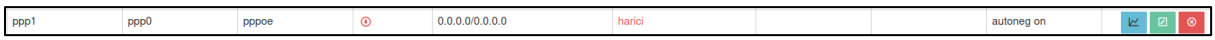




1	**Name**	Enter the name to be given to the PPPoE interface to be added.
2	**User Name**	It is the section where the username given by the Internet Service Provider is entered.
3	**Password**	This is the section where the password given by the Internet Service Provider is entered.
4	**Confirm Password**	It is the section where the password given by the Internet Service Provider is re-entered.

5	**Interface**	This is where the interface is selected to define the PPPoE interface.
6	**Default Gateway**	This is the button where the PPPoE interface is set as the default gateway.
7	**Masquerade**	It is the button where the dynamic address conversion of the PPPoE interface is turned on.
8	**Device Status**	This is the part where the device status of the PPPoE Interface is specified. If the Device State is up, the interface is active, and if the Device Status is down, the interface is passive.
9	**Visibility**	In the Traffic Analysis module of the PPPoE Interface, it is opened when it is desired to examine the traffic of the interface in detail.
10	**Save**	It is the button where the configuration made on the PPPoE Interface is saved.
11	**Close**	It is the button where the window that opens after clicking on the PPPoE Interface is closed.

-The added PPPoE Interface appears on the Labris UTM device as follows.

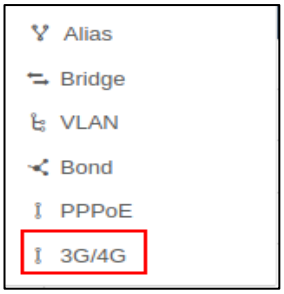


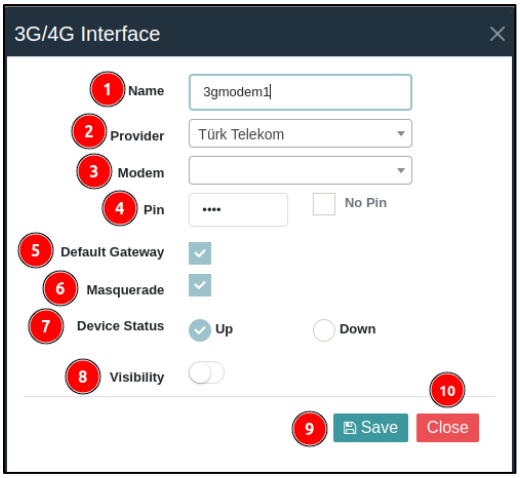
Note

In case of adding a PPPoE interface, the user name and password given by the Internet Service Provider must be entered correctly.

11.1.2.5 3G/4G

3G/4G modems (VINN etc.) It is used in cases where it needs to be defined on the Labris UTM device.





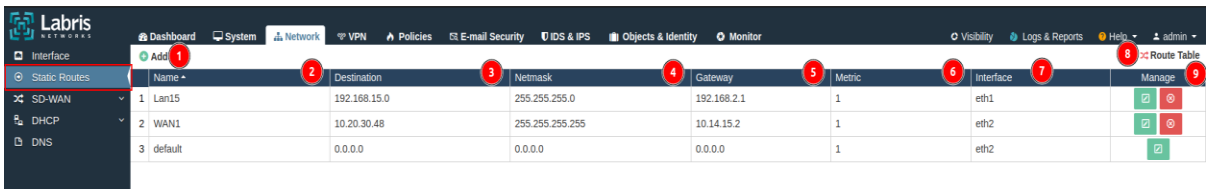
1	**Name**	It is where the name to be given to the 3G/4G Interface is entered.
2	**Provider**	This is where the provider of the 3G/4G Interface is selected.
3	**Modem**	This is where the modem information of the 3G/4G Interface is selected.
4	**Pin**	It is the section where the pin information of the 3G/4G Interface is written.
5	**Default Gateway**	It is used in cases where the 3G/4G Interface needs to be set as the default gateway.
6	**Masquerade**	It is the button where the dynamic address conversion of the 3G/4G Interface to be added is turned on.
7	**Device Status**	This is the part where the device status of the 3G/4G Interface is specified. If the Device State is up, the interface is active, and if the Device Status is down, the interface is passive.

8	**Visibility**	In the Traffic Analysis module of the 3G/4G Interface, it is opened when it is desired to examine the traffic of the interface in detail.
9	**Save**	This is the button where the configuration made on the 3G/4G Interface is saved.
10	**Close**	It is the button where the window that opens after clicking on the 3G/4G Interface is closed.

11.2 Static Routes

Static routing is the manually configured setting to define to route of an IP address to the next destination address. By specifying which interface or gateway the packet leaves and which device the packet is routed to, static routes control the traffic leaving Labris UTM.

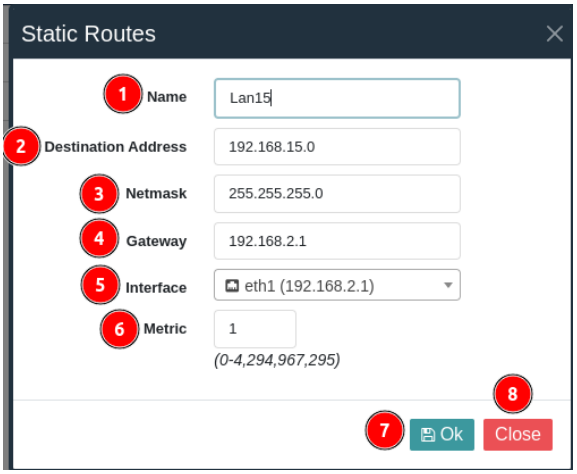
In the static routing section, the routes that are intended to direct the traffic allocated for a network or a computer through a different next stop are added instead of a default route.



1	**Add**	This is the button to which the Static Route is added.
2	**Name**	The name given to the Static Route is displayed.
3	**Destination**	The destination address is displayed.
4	**Netmask**	The network mask of the destination address is displayed.
5	**Gateway**	The gateway of the destination address is displayed.
6	**Metric**	The metric value of the routing is displayed.
7	**Interface**	The interface in which the routing is written is displayed.

8	**Route Table**	The Static Routing table in the monitoring module is displayed.
9	**Manage**	It is the section where the typed Static Routing is deleted or edited. The red button is selected to delete the route. The green button is selected to edit the typed route.

-To add Static Route, click the add button to add it. After clicking the Add button, Static Route is added by filling in the necessary information in the window that appears.



1	**Name**	It is the section where the name given to Static Route is entered.
2	**Destination**	It is the section where the destination address to be written forwarding is entered.
3	**Netmask**	This is the section where the network mask of the destination address is entered.
4	**Gateway**	This is the section where the gateway to which the destination address will be routed is entered.
5	**Interface**	This is the section where the Static Route interface to be written is selected.
6	**Metric**	It is the section where the metric unit of the Static Route to be written is written.

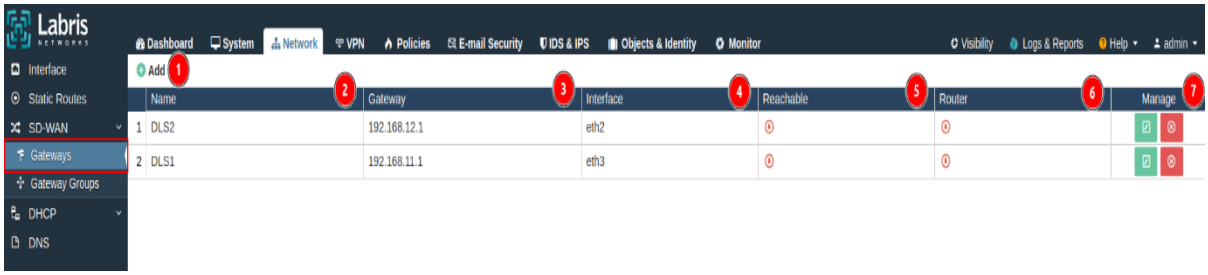
7	**Save**	It is the button where the configuration of the static route is saved.
8	**Close**	It is the button where the window opened by clicking the Add button is closed.

11.3 SD-WAN

It is a technology that handles traditional wide-area networks (WAN) with a modern approach. SD-WAN is used to provide network administrators with flexibility to increase the performance of their wide networks.

SD-WAN are software-based wide area networks. It offers a software-based backup structure in case of any interruption in the Internet links of the institutions.

In cases where there are two or more internet links, the internet links are configured as redundant by using the SD-WAN module on the Labris UTM device. The bandwidth of the Internet links is grouped.



1	**Add**	This is the button used to add the interfaces added as an external network to the SD-WAN.
2	**Name**	The name of the added gateway is displayed
3	**Gateway**	The interface address of the added gateway is displayed.
4	**Interface**	The interface of the added gateway is displayed.
5	**Reachable**	When the gateway is reached, it appears green, and if not, it appears red.
6	**Router**	When the gateway is routing traffic, it appears green, and if not, it appears red.

7	**Manage**	There are buttons where the added gateway can be edited or deleted. The gateway added with the green button is edited, and the gateway added with the red button is deleted.

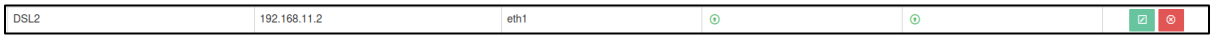
11.3.1 Gateway

It is the module where the gateways of the interfaces set as external networks are defined. To add a gateway, click the add button to add an SD-WAN gateway.

1	**Name**	This is the section where the name of the gateway to be added is entered.
2	**Interface**	This is the part where the interface of the gateway to be added is selected.
3	**Gateway**	This is where the gateway address is written.
4	**Ping Addresses**	This is the section where the ping server is entered, which the gateway can access.
5	**Add Ping Addresses**	This is the section where the ping server is added, which the gateway can access.
6	**List of Ping Addresses**	A list of ping addresses for the gateway is displayed.
7	**Save**	This is the button where the configuration of the gateway is saved.

8	**Close**	This is the button used to close the gateway configuration settings.

-The added gateways look like the following.

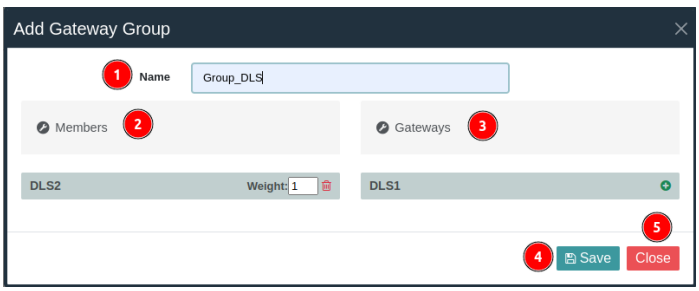


11.3.2 Gateway Groups

It is the module where the gateways are grouped in the SD-WAN module and the previously grouped gateways are displayed. Gateways are grouped by clicking the add button to create a gateway group.

1	**Add**	It is the button where the added Gateways are grouped.
2	**Group Name**	The name of the added gateway groups is displayed.
3	**Links / Weight**	The grouped gateways and the priority values of the gateways are displayed.
4	**Manage**	Can edit or delete grouped gateways.

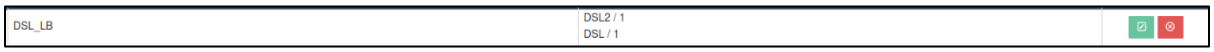
-To group the gateways added in the Gateway module**,** click the add button to group the gateways.



1	**Name**	Enter the name to be given to the gateway group.
2	**Members**	Indicates the gateways that are members of the gateway group. This is the section where the added gateways are deleted from the list of members.

3	**Gateways**	This is the section where the list of gateways is displayed and the displayed gateways are added as members.
4	**Save**	This is the button where the settings of the groups of gateways are saved.
5	**Close**	It is the button where the window opened by clicking the Add button is closed.

-The added Gateway Groups look like the following.



11.4 DHCP

DHCP stands for Dynamic Host Configuration Protocol.

The DHCP server provides the IP address and the relevant configuration information, such as the subnet mask and standard network relay point for the host systems within the LAN. Specifies a unique IP address for each computer to be assigned to the system.

DHCP is a useful protocol on large networks where it is desired to centralize IP management to reduce errors made by humans. A DHCP server is a server that automatically assigns IPs to clients within a specified IP range.

-Steps of operation of the DHCP service;

1.DHCP Discover: When a device first connects to the network or needs AP isolation, DHCP begins to discover. The device sends a broadcast message to find the DHCP server on the network. The content of the message contains information such as the network name and MAC address.

2.DHCP Offer: The DHCP server receives the DHCP discovery message and prepares a quote that includes one of the available IP addresses on the network and other network configuration information. This offer is sent to the device by the DHCP server.

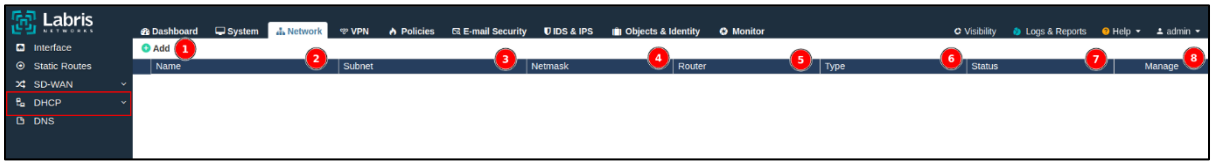
3.DHCP Request: The device accepts the DHCP offer and optionally sends a DHCP request indicating that it wants to use the IP address.

4.DHCP Acknowledge: The DHCP server sends an acknowledgment message (ACK) confirming that it has received the request. This message allows the device to use a specific IP address and contains other network configuration information.

Note

The above DHCP steps typically occur when a device connects to the network for the first time or when its current IP address expires during the lease period.

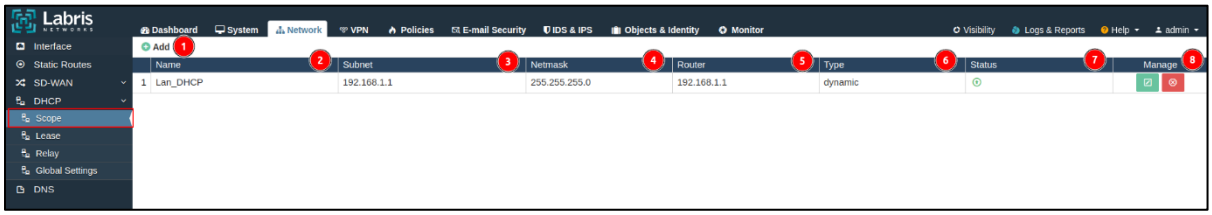
On the Labris UTM device, the DHCP server can distribute the DHCP's lease list from another DHCP server, and the DHCP global settings are made.



1	**Add**	It is the button where the DHCP server is added.
2	**Name**	The name given to the added DHCP server is displayed.
3	**Subnet**	The network address for which the DHCP server is identified is displayed.
4	**Netmask**	The network mask of the DHCP server is displayed.
5	**Router**	The router address of the DHCP server added is displayed.
6	**Type**	The type of the server is displayed. It can be dynamic or static.
7	**Status**	Indicates the status of the DHCP server. If there is a green expression in the status section, the DHCP server is active, and if there is a red expression, the DHCP server is inactive.
8	**Manage**	It is used to delete the added DHCP server and edit its configurations.

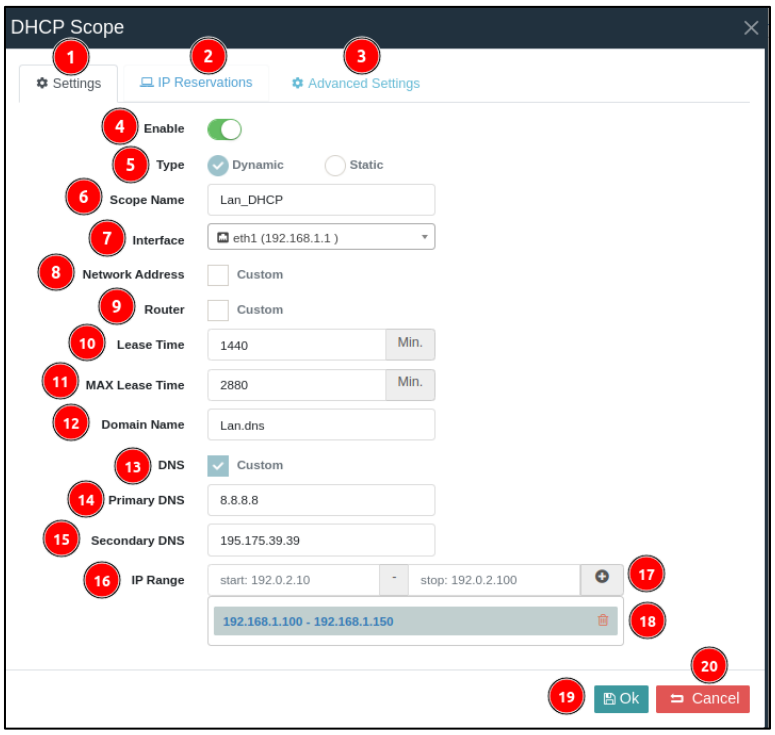
11.4.1 Scope

It is the module where the DHCP server is defined on the Labris UTM device. In this module, the Labris UTM device acts as a DHCP server.



Click the add button to add a DHCP server on the Labris UTM device. After clicking the Add button, the DHCP server can be defined on the Labris UTM device by filling in the information on the screen that appears.

After clicking the Add button, the screen that appears is as follows.



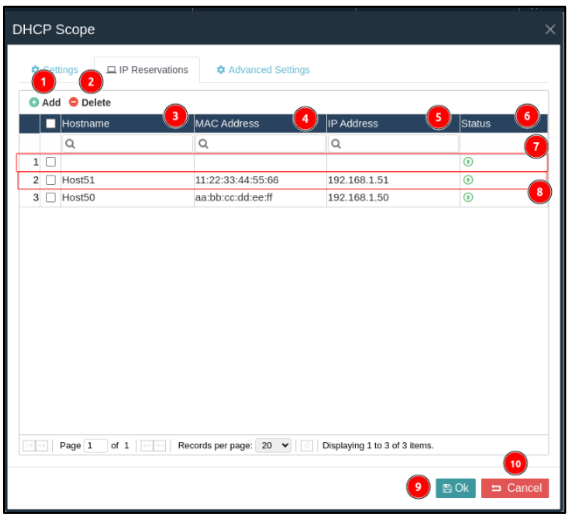
1	**Settings**	This is the screen where the DHCP Server settings are edited.
2	**IP Reservations**	This is the section where IP reservations are made on the DHCP server.
3	**Advanced Settings**	This is the section where advanced settings of the DHCP server to be added are made.

4	**Enable**	This is the button where the DHCP server is enabled.
5	**Type**	The type of DHCP to be added is set. Dynamic or Static is selected as the server type. If dynamic is selected, the DHCP server automatically distributes IP addresses. If static is selected, it must be added to the IP Reservation section on the DHCP server. The server does not automatically distribute IP addresses.
6	**Scope Name**	Enter the name of the DHCP server.
7	**Interface**	The interface on which to create the DHCP server is selected.
8	**Network Address**	This is the button used to enter the network address of the DHCP server specifically. If it is not checked, the network address of the interface is used.
9	**Router**	This is the button used to enter the router's address of the DHCP server exclusively. If it is not checked, the router address of the interface is used.
10	**Lease Time**	This is the section where the lease period of the IP address given by the DHCP server to the client will be set.
11	**MAX Lease Time**	This is the section where the maximum lease period of the IP address given by the DHCP server to the client will be set.
12	**Domain Name**	This is the section where the domain name of the DCHP server is entered.
13	**DNS**	Enables DNS addresses in cases where you want to set them to private.
14	**Primary DNS**	When the DNS section is checked, the primary DNS addresses are entered.
15	**Secondary DNS**	When the DNS section is checked, secondary DNS

		addresses are entered.
16	**IP Range**	This is the section where the IP Range of the DHCP server is selected. It is necessary to enter the starting and ending IP addresses.
17	**Add IP Range**	After entering the starting and ending IP addresses, it is necessary to click on the + button.
18	**IP Address List**	A list of added IP ranges is displayed.
19	**Save**	This is the button where the configuration settings made on the DHCP server are saved.
20	**Close**	It is the button where the window that opens when the Add button is clicked is closed.

-The following steps are performed to perform IP/MAC mapping on the DHCP server configured on the Labris device.

1- It is entered in the Network/Dhcp/Server module.
2- Click the edit button from the manage column of the server to be matched with the IP/MAC.
3- After clicking the Edit button, the IP Reservations section is selected from the screen that appears.
4- By clicking the add button in the IP Reservations section, IP/MAC matching is made by entering the hostname, MAC Address, and IP Address information.
5- Finally, to delete the clients with which you have an IP/MAC match, you can delete by selecting the match you want to delete and clicking the delete button.

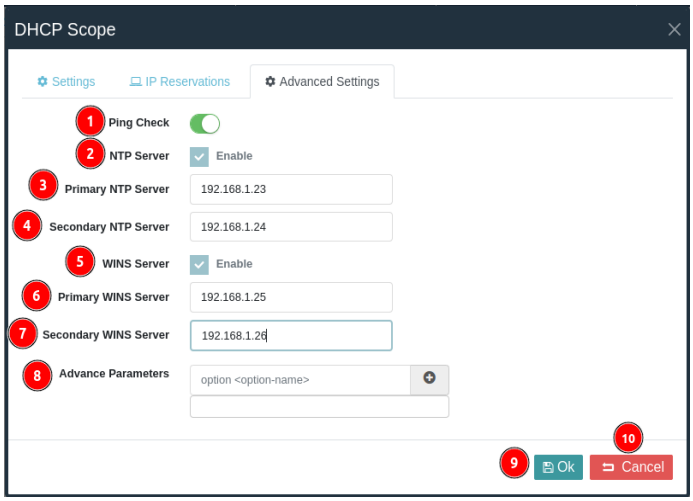


1	**Add**	It is used to perform IP/MAC matching.
2	**Delete**	It is used to delete clients with IP/MAC matching.
3	**Hostname**	This is the section where the name of the hostname with IP/MAC matching is displayed.
4	**MAC Address**	This is the section where the MAC address of the device with IP/MAC matching is displayed.
5	**IP Address**	This is the section where the IP address of the device with IP/MAC matching is displayed.
6	**Status**	The status of the IP/MAC matched device is displayed.

		If the status is green, IP/MAC matching has been made. If the status is red, there is no IP/MAC matching.
7	**Adding an Address**	After clicking the add button to add an IP/MAC match, the hostname, MAC address, IP address, and status information are set.
8	**Attached Address**	This is what clients with IP/MAC matching look like.
9	**Save**	It is the button where the IP/MAC matching is saved.
10	**Cancel**	DHCP is the button where the server's screen is canceled.

-The following steps apply advanced settings to the DHCP server configured on the Labris device. Advanced settings, DNS, default gateway, time server, WINS servers, etc., are performed on the DHCP server.

1- It is entered in the Network/Dhcp/Server module.
2- Click the edit button from the manage column of the server where the Advanced Settings will be made.
3- After clicking the Edit button, the Advanced Settings section is selected from the screen that appears.
4- From here, the NTP, WINS servers and DHCP advanced parameters to be added are added.

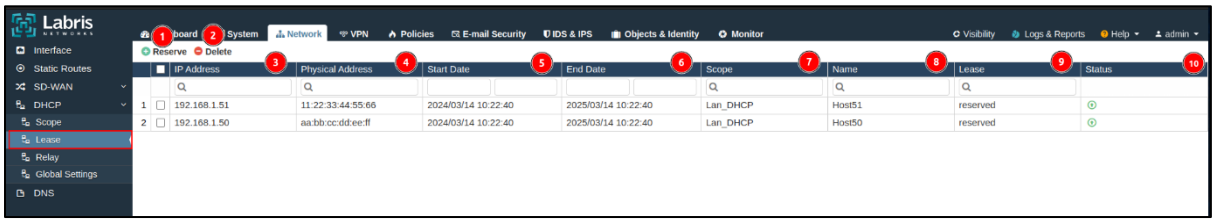


1	**Ping Check**	It is the button where ping control is turned on on DHCP.

2	**NTP Server**	This is the button that needs to be checked to add an NTP server to your DHCP server. To add the IP address of the NTP server, the enable button must be checked.
3	**Primary NTP Server**	The address of the primary NTP server is entered.
4	**Secondary NTP Server**	The secondary NTP server address is entered.
5	**WINS Server**	This is the button used to add a WINS server on a DHCP server. To add a WINS server, the enable button must be checked.
6	**Primary WINS Server**	The WINS server is to be added as the primary.
7	**Secondary WINS Server**	The WINS server is to be added as a secondary.
8	**Advanced Parameters**	It is used for adding advanced parameters on the DHCP server.
9	**Save**	This is the button where DHCP settings are saved.
10	**Close**	This is the button where DHCP settings are canceled.

11.4.2 Lease

The Lease List module displays a list of IP addresses that the DHCP server has given to the client.



1	**Reserve**	It is the button where the IP and MAC addresses of the clients that receive IP from the DHCP server are

		mapped. The client to be matched must be marked.
2	**Delete**	It is the button where the clients that receive IP from the DHCP server are deleted from the lease list. The client to be deleted must be marked.
3	**IP Address**	This is the section where the IP address that the client receives from the DHCP server is displayed.
4	**Physical Address**	The MAC address of the client is displayed.
5	**Start Date**	The start date when the client obtained an IP from the DHCP server is displayed.
6	**End Date**	The date when the client will leave the IP address from the DHCP server is displayed.
7	**Scope**	The DHCP server from which it obtained its IP address is displayed.
8	**Name**	The name of the client is displayed.
9	**Lease**	The lease status of the client that receives an IP address from the DHCP server is displayed.
10	**Status**	The status of the client that receives an IP from the DHCP server is displayed.

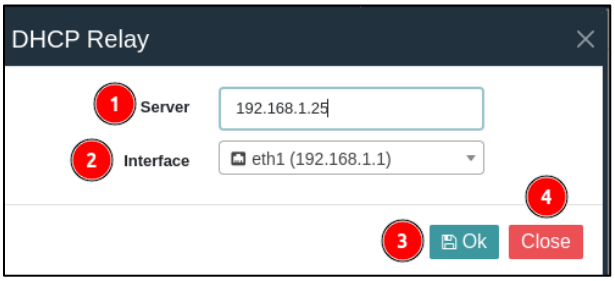
11.4.3 Relay

It is the module used to define the DHCP server that is not on the Labris UTM device.

1	**Add**	It is the button used to add a DHCP server that is not on the Labris UTM device.

2	**Interface**	The interface to which the DHCP server is connected is displayed.
3	**Server**	The IP address of the DHCP server is displayed.
4	**Manage**	This is the section where the DHCP server is deleted or the configuration is edited.

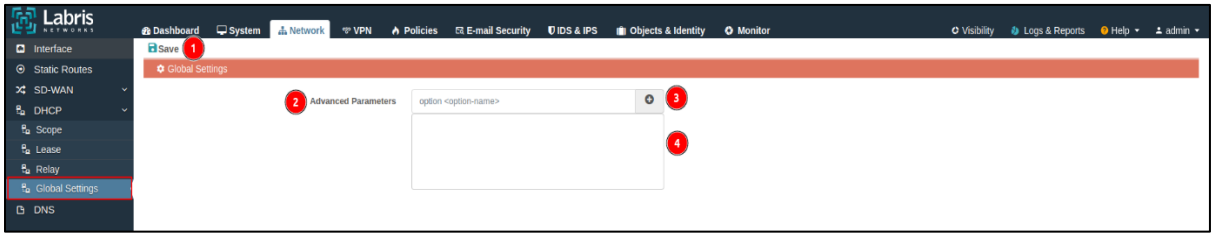
-Click the add button to add a DHCP server to the Labris UTM device. After clicking the Add button, the necessary information is entered on the screen that appears, and the DHCP server addition process is done.



1	Server	Enter the IP address of the DHCP server.
2	Interface	The interface where the DHCP server is located is selected.
3	Save	This is the button where the settings of the DHCP server are saved.
4	Close	This is the button where the settings of the DHCP server are turned off.

11.4.4 Global Settings

It is the section where the General Settings of the servers added in the DHCP module are made.



1	**Save**	It is the button where the typed advanced parameters

		are saved.
2	**Advanced Parameters**	This is where Advanced Parameters are entered with the DHCP server.
3	**Add Advanced Parameter**	It is the button where the entered parameter is added.
4	**Advanced Parameter List**	It is where the list of entered parameters is displayed.

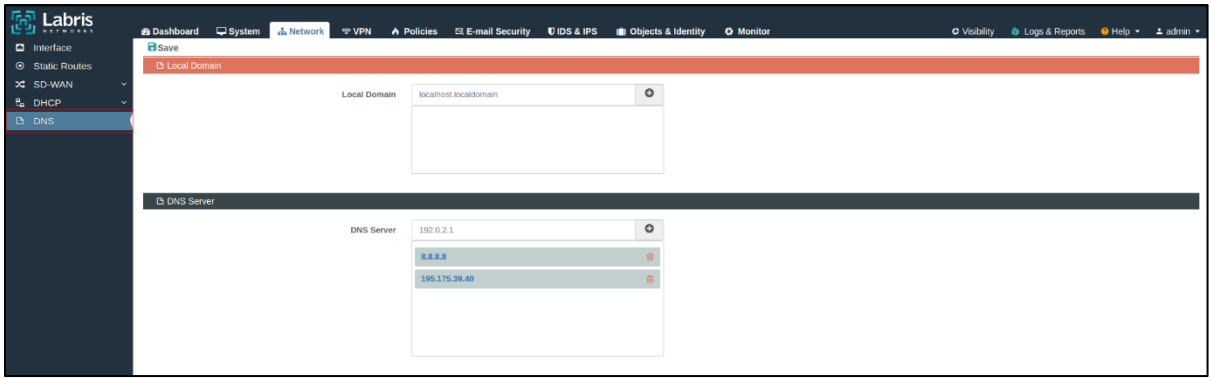
11.5 DNS

The Domain Name System is a system that matches the addresses of devices on the internet with meaningful and memorable domain names.

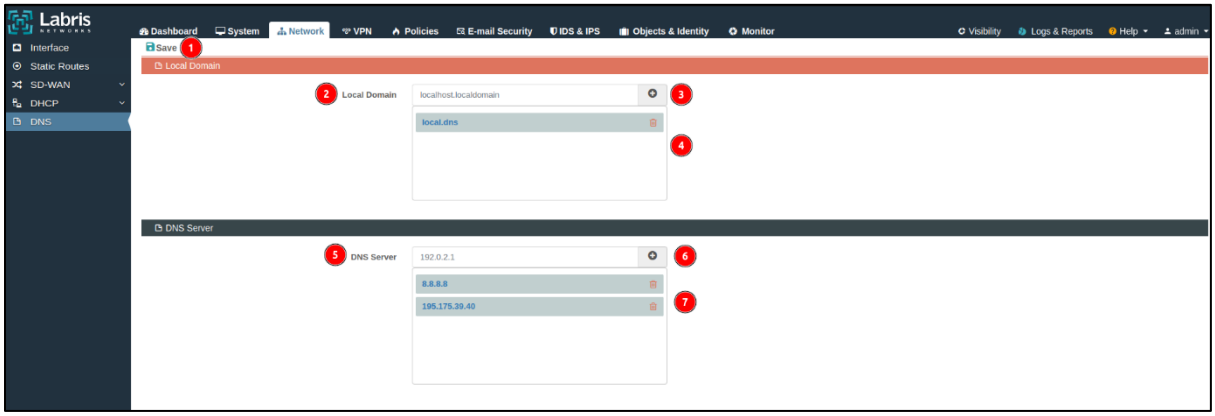
When you browse the Internet and want to access a website, the domain name you type in your browser is translated into the relevant IP address by DNS.

The main purpose of DNS is to convert domain names that people can easily understand into numerical IP addresses that the internet can understand. In this way, it makes the internet more user-friendly and accessible.

The purpose of use in the Labris UTM device is to resolve the DNS of the device.



It is done by entering the Local Domain Name or the IP address of the Domain Name Server on the Labris device.



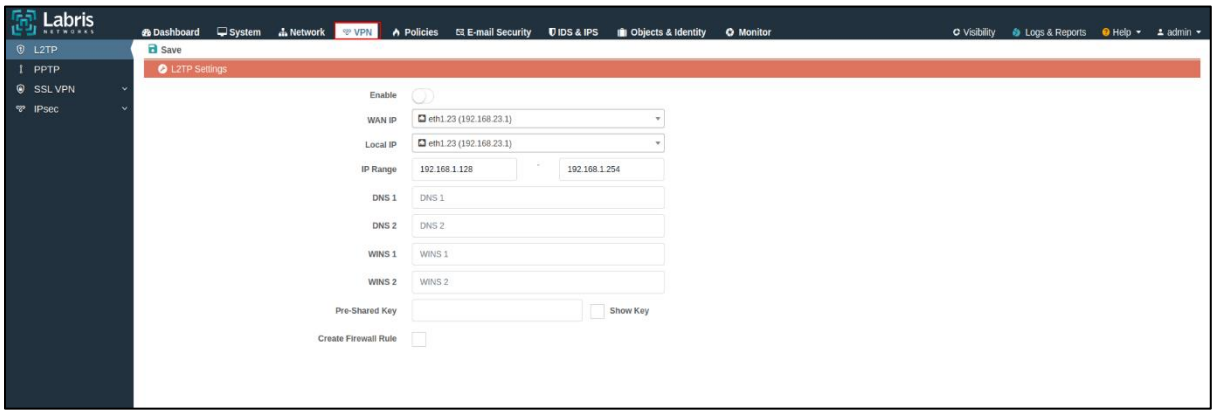
1	**Save**	This is the button where the changes made in the DNS module are saved.
2	**Local Domain**	Enter the domain address of the Local Name server. DNS is the domain address of your server.
3	**Add Local Domain**	It is the place where the typed domain address is added.
4	**List Added Local Domain Name**	This is where the list of domain addresses that have been added is displayed.
5	**DNS Server**	This is the section where the IP address of the domain name server is added. Enter the IP address of the DNS server to be added.
6	**Add a DNS Server**	This is where the IP address of the domain name server is added.
7	**Added DNS Server List**	This is where the list of the IP address of the DNS server that has been added is displayed.

12.VPN

VPN stands for Virtual Private Network. It is a private network that allows us to connect remotely to the public network through a secure path.

Personal VPNs are encrypted so that your data is not sent from your computer to a VPN server. This prevents hackers from stealing your information while you're connected to the internet via public Wi-Fi. VPNs can be used for several things other than just accessing blocked sites, but they can also be used to secure a public Wi-Fi hotspot, such as a torrent client, browser, upload manager, etc.

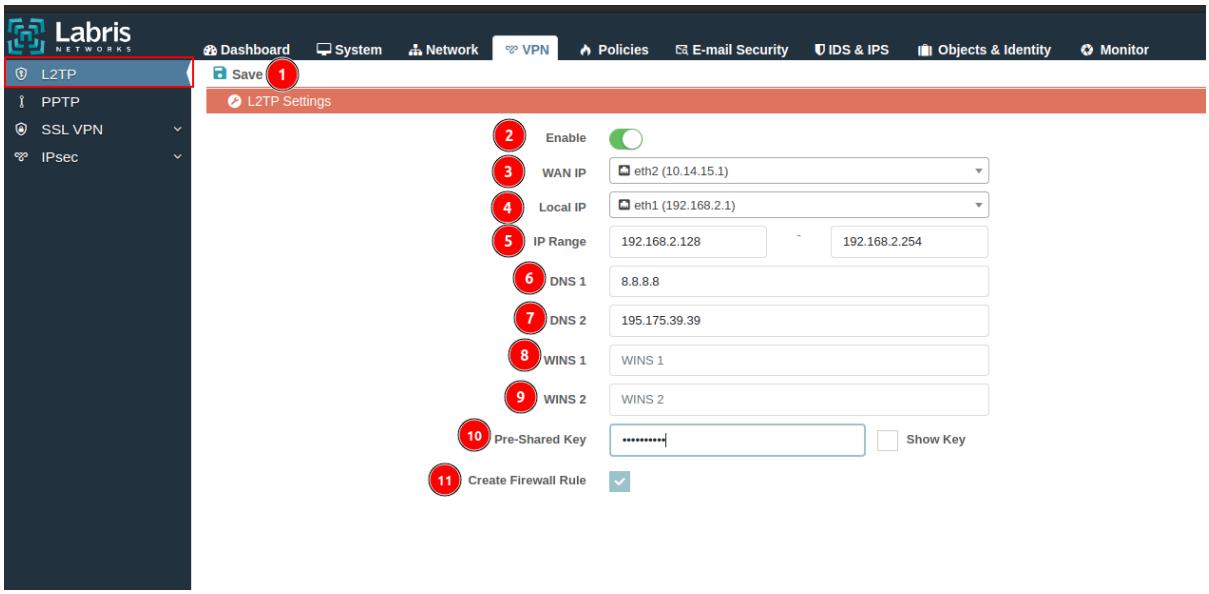
VPN on the Labris UTM device is used by organizations to access internal or inter-enterprise networks using a private network. L2TP, PPTP, SSLVPN, and IPSec are used to access on-device and inter-enterprise networks.



12.1 L2TP

L2TP (Layer 2 Tunneling Protocol) is a tunneling protocol used by virtual private networks (VPNs) or internet service providers (ISPs) to provide services. It runs at the data link layer (Layer 2) of the OSI model.

L2TP encapsulates PPP (Point to Point Protocol) frames into IP packets and enables them to transmit data over the internet or other IP-based networks.



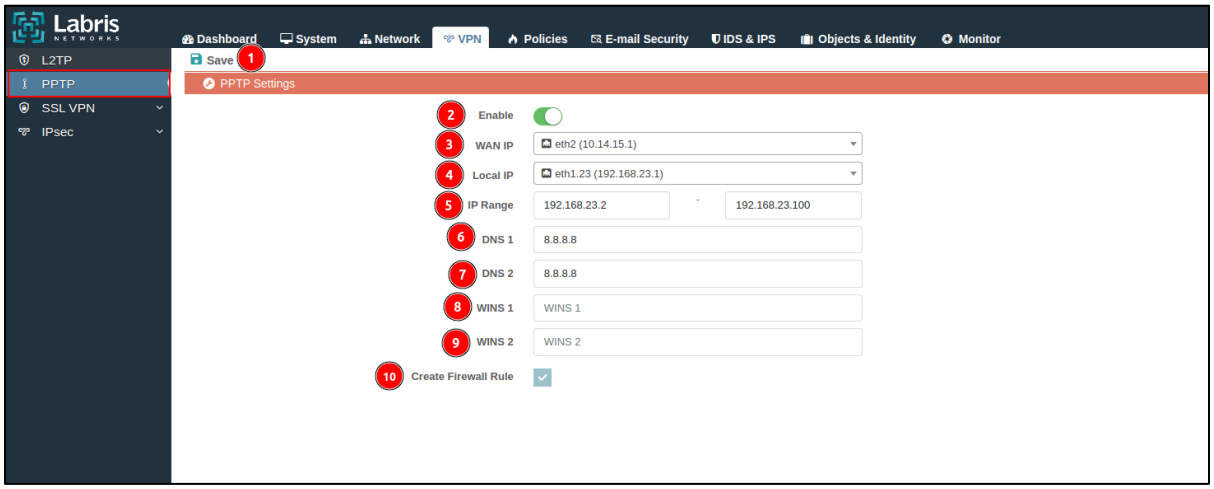
1	**Save**	This is the button where the L2TP configuration settings are saved.
2	**Enable**	This is the button where L2TP VPN is activated.
3	**WAN IP**	This is where the WAN IP address of the L2TP VPN is selected.
4	**Local IP**	This is where the Local IP address of the L2TP VPN is selected.
5	**IP Range**	This is where the IP address range that users who will connect to L2TP VPN will receive is entered.
6	**DNS 1**	For VPN users, the IP address of the first DNS server to be entered for DNS resolves is entered.
7	**DNS 2**	For VPN users, the IP address of the second DNS server to be entered for DNS resolves is entered.

8	**WINS 1**	It is the service used to resolve NetBIOS names on Windows networks. If you have WINS, your server's IP address is entered here.
9	**WINS 2**	It is the service used to resolve NetBIOS names on Windows networks. If a second WINS is available, the IP address of your server is entered here.
10	**Pre-Shared Key**	A shared key must be created in advance for an L2TP connection. From this section, the shared key is generated.
11	**Create Firewall Rule**	Creates a firewall rule for L2TP VPN.

12.2 PPTP

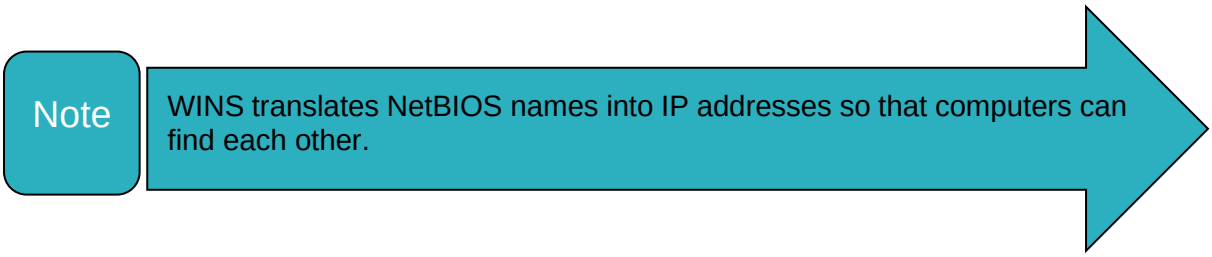
PPTP (Point-to-Point Tunneling Protocol) is a way to implement virtual private networks. PPTP is a communication protocol used for remote access VPNs.

PPTP allows a computer to securely connect to a remote network. This is often used to access an employee's company network from home or an outside office. By creating an encrypted tunnel over the Internet, it secures data transmission.



1	**Save**	This is the button where PPTP configuration settings are saved.
2	**Enable**	This is the button where PPTP VPN is enabled.
3	**WAN IP**	This is where the WAN IP address of the PPTP VPN is

		selected.
4	**Local IP**	This is where the local network that can be accessed via PPTP VPN is selected.
5	**IP Range**	This is where the IP range for users who will connect to PPTP VPN is entered.
6	**DNS 1**	For VPN users, enter the IP address of the first DNS server to be entered for DNS resolution.
7	**DNS 2**	For VPN users, enter the IP address of the second DNS server to be entered for DNS resolution.
8	**WINS (Windows Internet Naming Service) 1**	It is the service used to resolve NetBIOS names on Windows networks. If you have WINS, your server's IP address is entered here.
9	**WINS (Windows Internet Naming Service) 2**	It is the service used to resolve NetBIOS names on Windows networks. If a second WINS is available, the IP address of your server is entered here.
10	**Create Firewall Rule**	This is the button where the firewall rule is created for PPTP VPN.

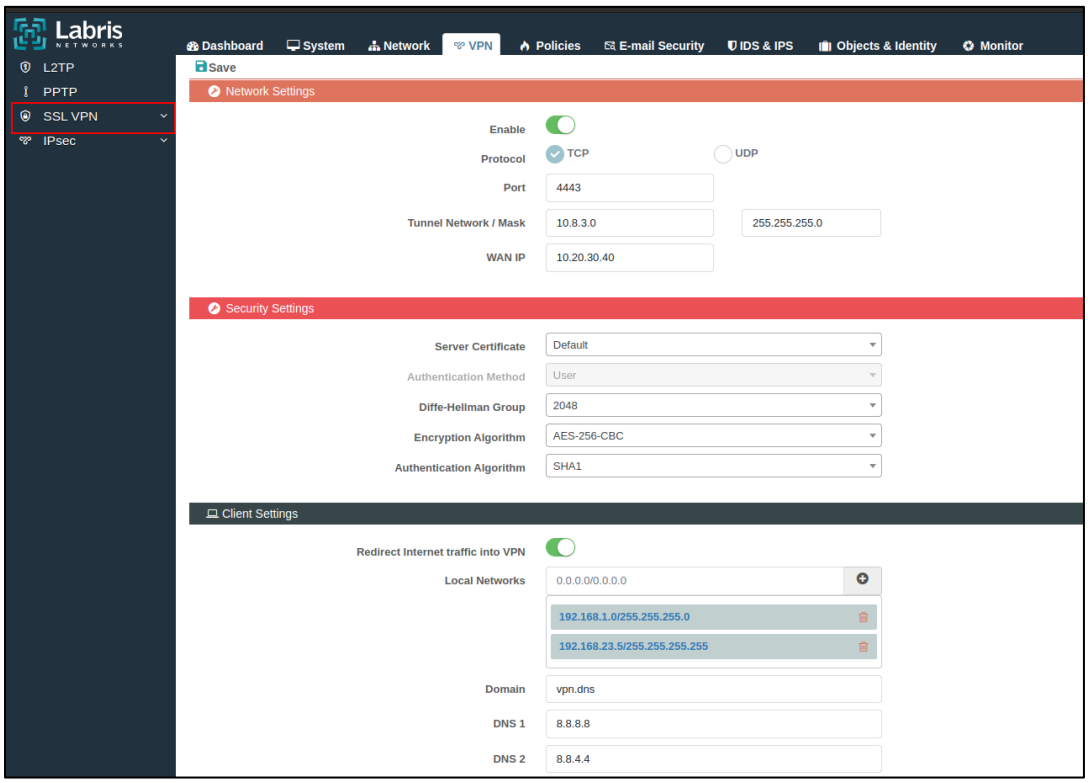


12.3 SSL VPN

SSL VPN (Secure Socket Layer Virtual Private Network) is a type of VPN that is used to provide remote access and can usually be accessed through web browsers. SSL is used in conjunction with a VPN to remotely access your local network.

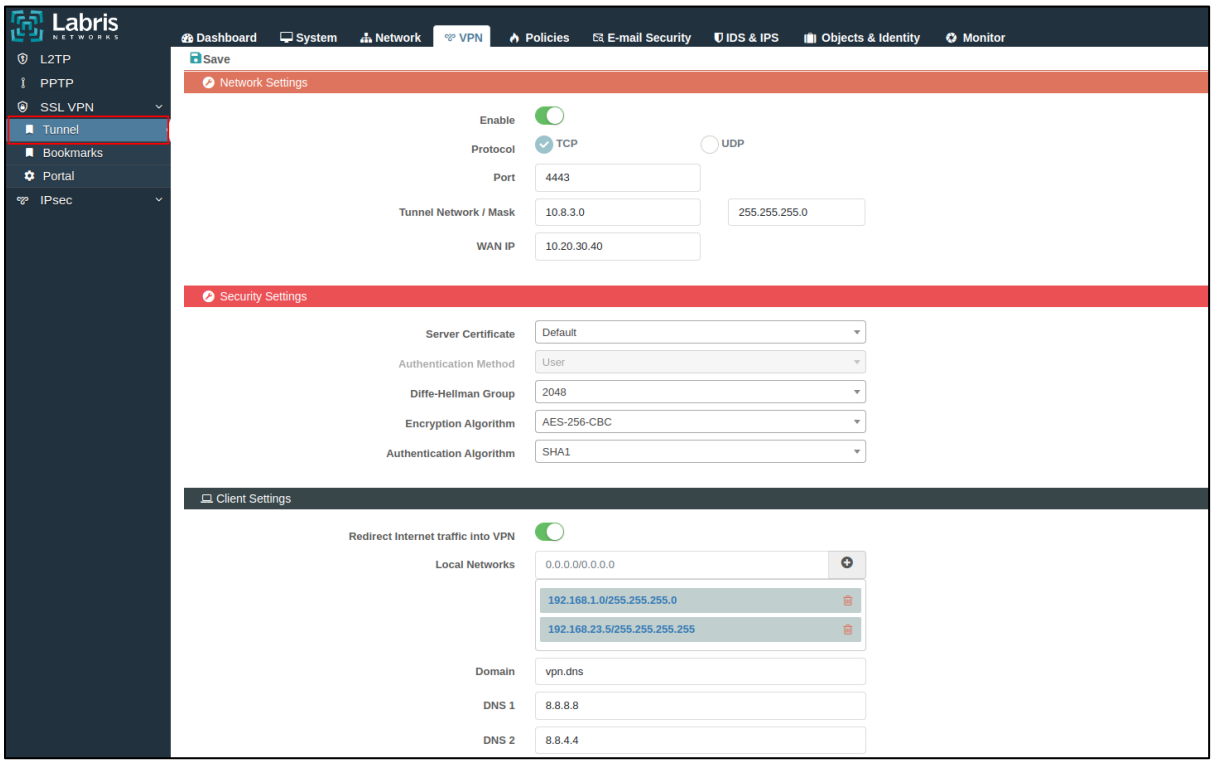
SSL VPN allows users to securely access remote network resources. VPN access is controlled through the Labris UTM device, and users can be authorized to access it if necessary.

SSL VPN is supported by the Labris UTM device and can be configured specifically according to the institutions' networks.



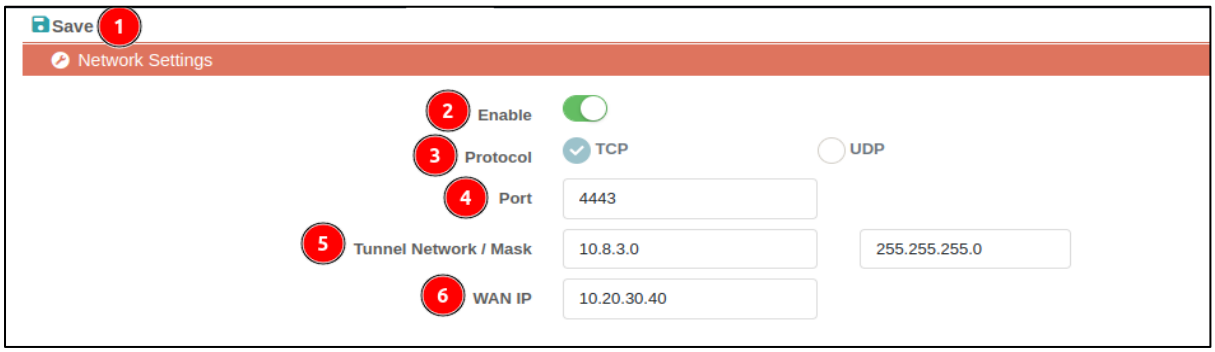
12.3.1 Tunnel

Tunnel settings are made for SSL VPN configuration on the Labris UTM device. The public IP address, the protocol information to be used, the port number, and the configurations of the networks that can be accessed using SSL VPN are made.



12.3.1.1 Network Settings

SSL is the section where VPN is enabled, and the protocol, port, tunnel network, and WAN IP address are entered.

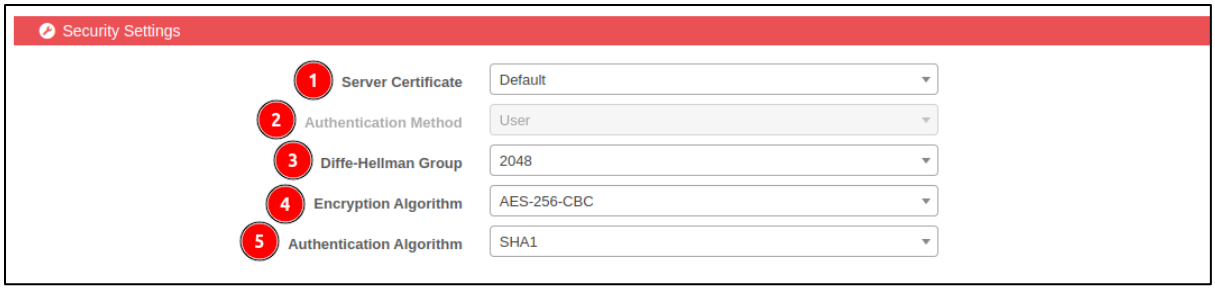


1	**Save**	This is the button where the SSL VPN configuration is saved.
2	**Enable**	This is the button where SSL VPN is enabled.
3	**Protocol**	The protocol to be used when connecting to SSL VPN

		is selected. If the TCP protocol is to be used, TCP should be selected, and if the UDP protocol is to be used, the UDP protocol should be selected.
4	**Port**	This is the section where the port number to be used when connecting to SSL VPN is entered.
5	**Tunnel Network / Mask**	It is where the network address that SSL VPN users will use after connecting to the VPN is specified.
6	**WAN IP**	This is the section where the WAN IP address to be used when connecting to SSL VPN is entered. If there is only one WAN IP, it should be left as any.

12.3.1.2 Security Settings

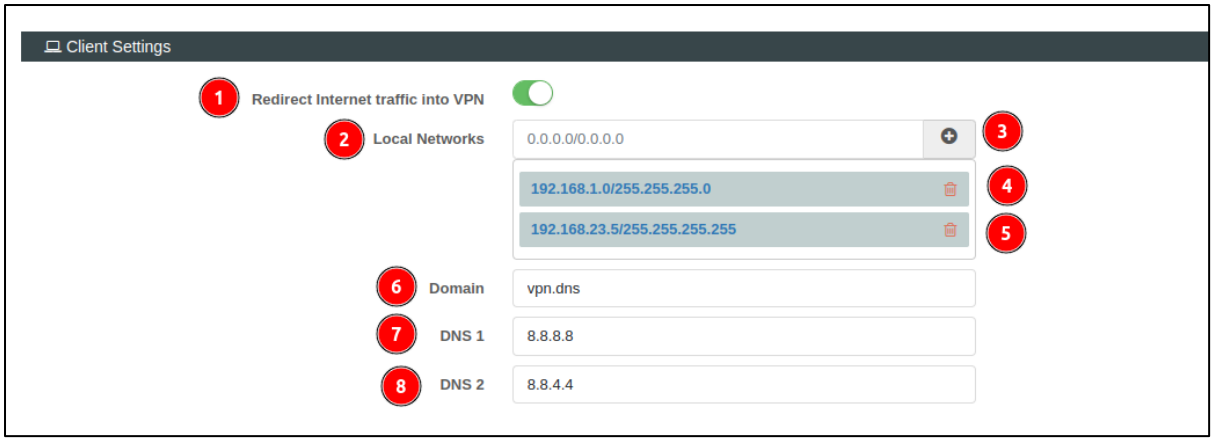
This is the section where the certificate and VPN encryption settings of the users connecting to SSL VPN are made.



1	**Server Certificate**	This is the section where the certificate of the user who will connect to SSL VPN is selected.
2	**Authentication Method**	The authentication method of the users who will connect to SSL VPN is selected.
3	**Diffe-Hellman Group**	This is the protocol that enables SSL VPN key sharing to be done securely.
4	**Encryption Algorithm**	This is the section where the encryption algorithm for users connecting to SSL VPN is selected.
5	**Authentication Algorithm**	This is the section where the authentication algorithm for users connecting to the SSL VPN is selected.

12.3.1.3 Client Settings

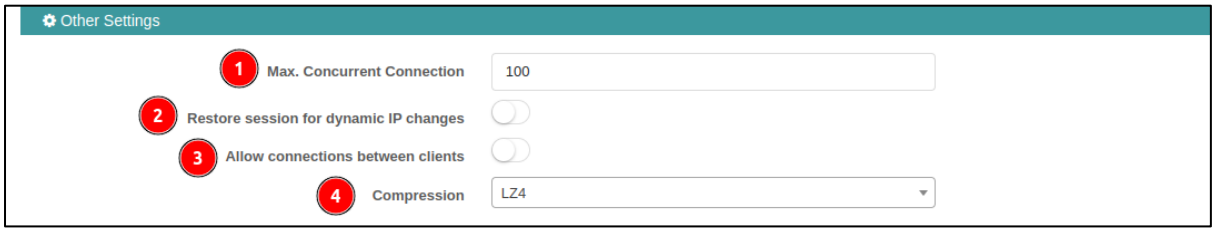
In the Client Settings, the local networks and DNS addresses that users who connect to SSL VPN can access in cases where they need to access the internet via VPN are specified.



1	**Redirect Internet Traffic into VPN**	It is used in cases where connecting users need to access the internet via VPN.
2	**Local Networks**	This is the section where local networks that can be accessed by users who connect to the SSL VPN are added.
3	**Add Local Network**	It is the button to which the typed local network is added. It is written as 192.168.23.22/255.255.255.255.
4	**Local Network List**	This is the section where the list of added local networks is displayed or the added local networks are removed from the list.
5	**Domain**	This is the section where the domain address of the domain name server is entered.
6	**DNS 1**	The IP address of the primary DNS server is entered, which is required for DNS resolution.
7	**DNS 2**	The IP address of the secondary DNS server is entered, which is required for DNS resolution.

12.3.1.4 Other Settings

This is the section where the number of users connecting to the SSL VPN is specified, and settings such as session status in dynamic IP change are made.

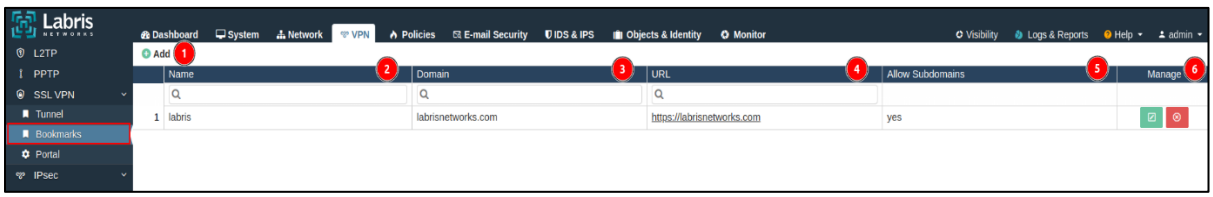


1	**Maximum Concurrent Connection**	The maximum number of connections to the SSL VPN.
2	**Restore session for dynamic IP changes**	It restores the session opened in case the dynamic IP address of users connecting to the SSL VPN changes.
3	**Allow connections between clients**	This is the button that allows communication between users connected to the SSL VPN.
4	**Compression**	This section is where protocols that perform compression are selected to optimize SSL VPN traffic and reduce bandwidth.

12.3.2 Bookmarks

SSL VPN Bookmarks is a port that users can use when accessing it on the SSL VPN client. Along with a bookmark, it is a shortcut or address that users can use to access a specific SSL VPN destination.

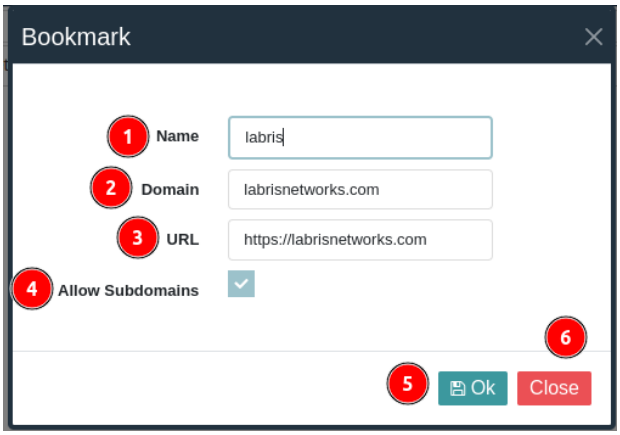
SSL VPN Bookmark allows users to get quick access to SSL VPN on any device. Users can save the bookmark in their browser.



1	**Add**	This is the button where the SSL VPN bookmark is added.

2	**Name**	This is the section where the name given to the SSLVPN bookmark is displayed.
3	**Domain**	The domain name of the bookmark added as a bookmark is displayed.
4	**URL**	This is the section where the bookmarked URL is displayed.
5	**Allow Subdomains**	This is the column that displays that the bookmarked domain is allowed to have subdomains.
6	**Manage**	This is the column in which the added bookmark is deleted or edited.

-To add an SSL VPN bookmark, click the add button.



1	**Name**	This is the section where the name given to the SSL VPN bookmark is entered.
2	**Domain**	This is the section where the Domain Name of the SSLVPN bookmark is entered.
3	**URL**	This is the section where the URL address given to the SSL VPN bookmark is entered.
4	**Allow Subdomains**	This is the section where the SSL VPN bookmark subdomains are allowed.
5	**Save**	This is the button where the SSL VPN bookmark

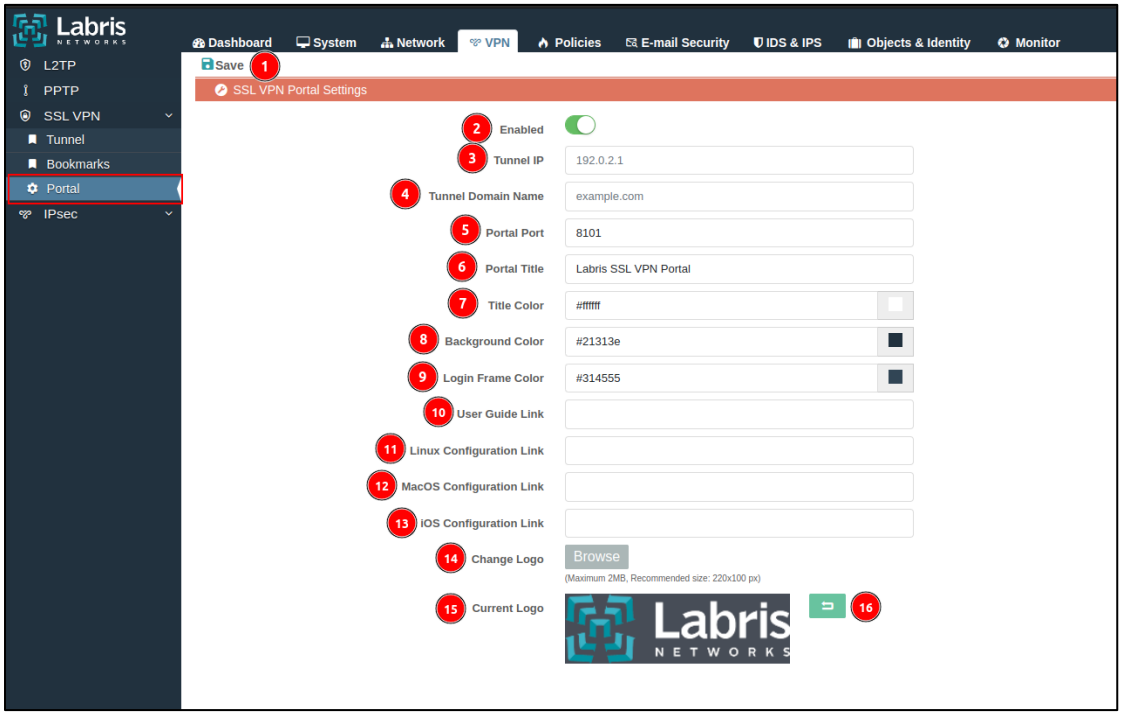
		configuration is saved.
6	**Close**	This is the button where the SSL VPN bookmark window is closed.

12.3.3 Portal

It is designed as a web-based portal where users gain access to the network resources they want to access remotely.

The SSL VPN portal allows users to securely connect to remote network resources using their browsers.

SSL VPN portal allows users to securely access network resources from different devices and different locations.



1	**Save**	This is the button where the settings of the SSL VPN portal are saved.
2	**Enable**	It is the button where the SSL VPN portal is enabled.
3	**Tunnel IP**	This is the section where the IP address of the SSL VPN portal is entered.
4	**Tunnel Domain**	This is the section where the domain name of the SSL

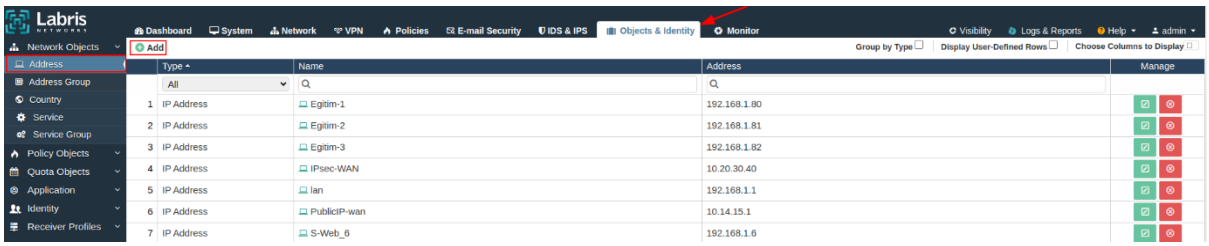
	Name	VPN portal is entered.
5	**Portal Port**	This is the section where the port of the SSL VPN portal is entered.
6	**Portal Title**	The header information of the SSL VPN portal is entered.
7	**Title Color**	This is the section where the header color of the SSL VPN portal is selected.
8	**Background Color**	This is the section where the background color of the SSL VPN portal is selected.
9	**Login Frame Color**	This is the section where the login frame color of the SSL VPN portal is selected.
10	**User Guide Link**	This is where the user contacts link is added for users who will connect to the SSL VPN.
11	**Linux Settings Link**	This is where the user Linux settings link is added for users who will connect to the SSL VPN.
12	**MacOS Settings Link**	This is where the user MacOS settings link is added for users who will connect to the SSL VPN.
13	**iOS Settings Link**	This is where the user iOS settings link is added for users who will connect to the SSL VPN
14	**Change the logo.**	This is the section where the logo of the SSL VPN portal is changed.
15	**Current Logo**	This is where the added logo is displayed.
16	**Reset Settings**	This is the section where the configuration settings made in the SSL VPN Portal are reset.

Note

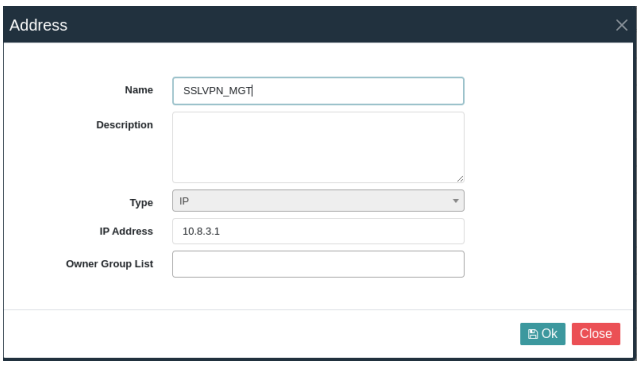
After configuring SSL VPN, the rules must be written in the Policies module.

-Steps to write the rule of SSL VPN in the Policies module;

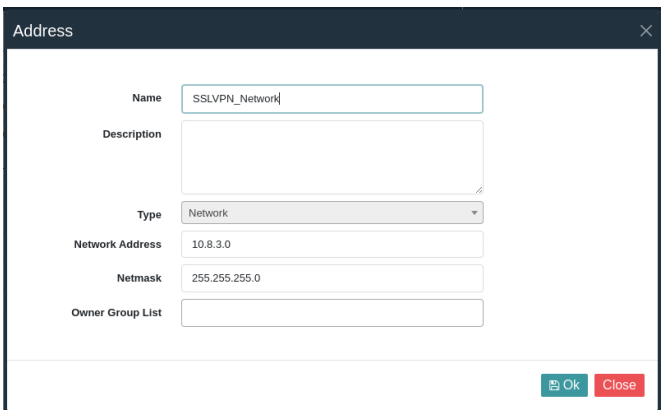
1. SSL VPN configuration is done.
2. The Objects and Identities module opens.



3. After the Objects and ID module is opened, objects are created for SSL VPN. Object addition is done by clicking the Add button.

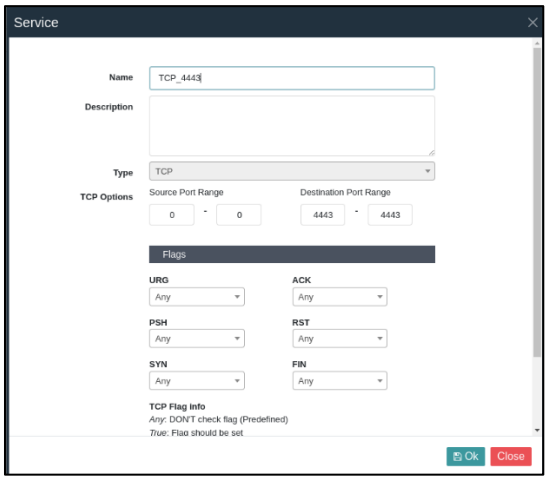


Add an SSL VPN Interface IP Address.



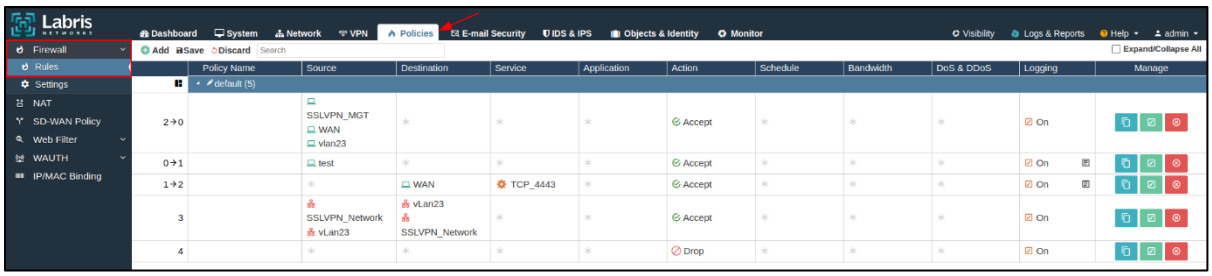
Adding the SSLVPN Network Address.

4. After the interface and network addresses are defined, they must be defined on the Labris UTM device at the port where the SSL VPN will be made.

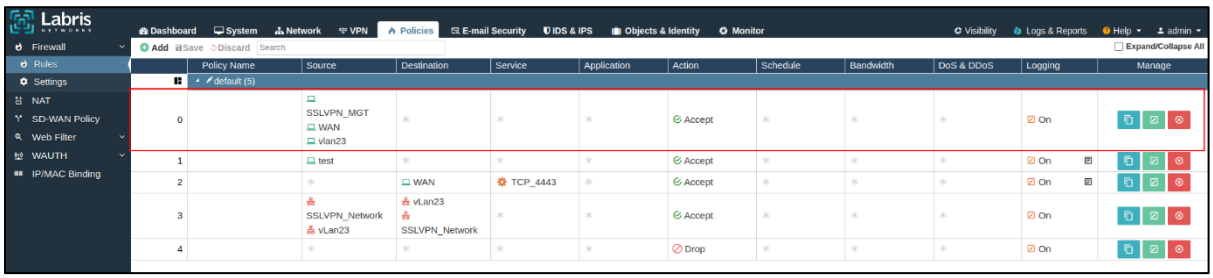


Add an SSL VPN port.

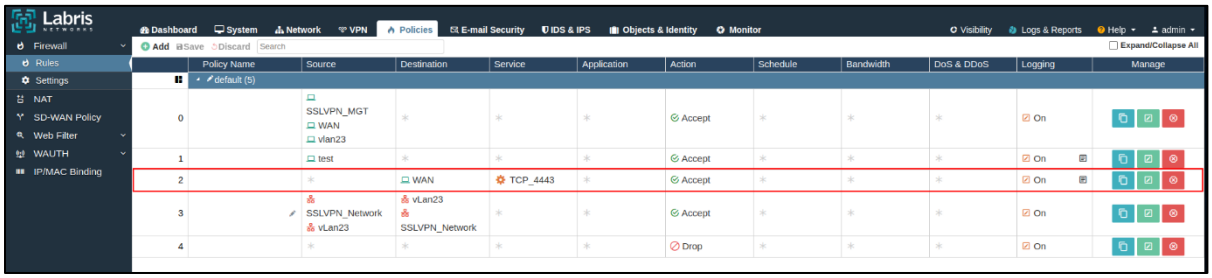
5. Objects for SSL VPN are added in the Objects and Identities module. After the objects are added, the Policies module opens.



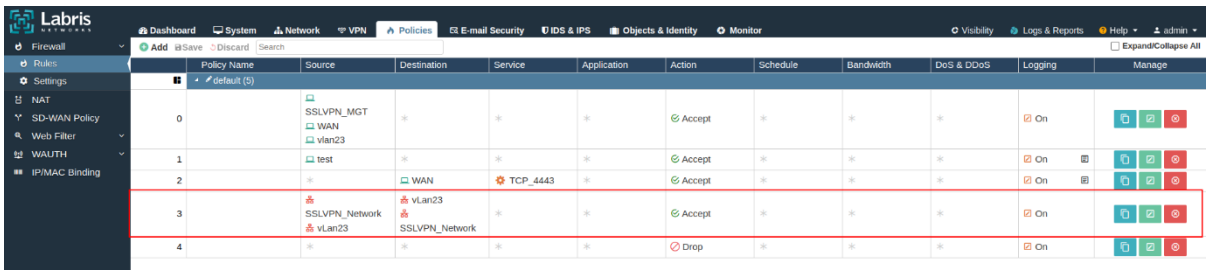
6. After the policy module is opened, the SSL VPN interface address is added to the first rule.



7. After adding the SSL VPN interface to the first rule, the following rule must be written under the first rule.



8. After writing the above access rule, SSL VPN and networks in the SSL VPN configuration settings must be allowed in the firewall rules.



9. After the definitions are made, you can test the SSL VPN connection.

12.4 IPSec

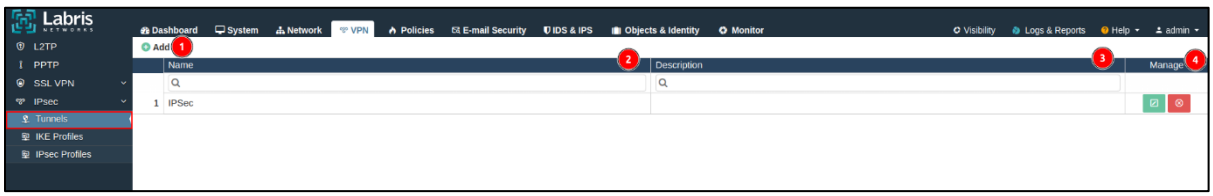
IPSec (Internet Protocol Security) is a security protocol used in data communication on the Internet.

IPSec is used to ensure the confidentiality, integrity, and reliability of data transmitted over the Internet.

IPSec is a set of protocols or protocols for establishing secure connections over a network.

12.4.1 Tunnel

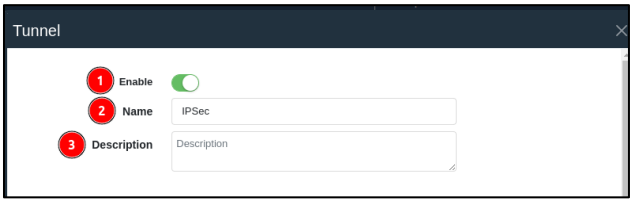
Phase 1 and phase 2 configuration for IPSec VPN is done.



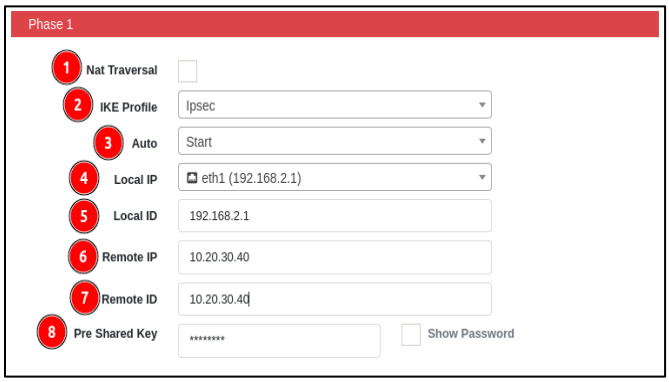
1	**Add**	This is the button where the IPSec tunnel is added.

2	**Name**	This is where the name given to the IPSec tunnel is displayed.
3	**Description**	This is the section where the description given to the IPSec tunnel is entered.
4	**Manage**	This is the section where the added IPSec tunnels are deleted or edited.

-To add an IPSec tunnel, stage-1 and stage-2 configurations must be set on the screen that opens when the 'add' button is pressed.

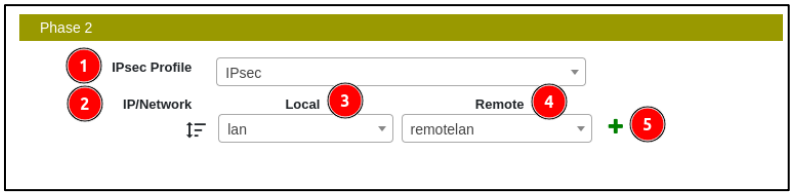


1	**Enable**	This is the button where IPSec tunnel configuration is enabled.
2	**Name**	This is the section where the IPSec tunnel is named.
3	**Description**	This is the section where the description of the IPSec tunnel is entered.



1	**NAT Traversal**	It is turned on or off to allow IPSec packets to pass through NAT devices.

2	**IKE Profile**	This is where the IKE profile prepared in the IKE profile module is selected.
3	**Auto**	It is used to automatically start the IKE protocol in Phase 1.
4	**Local IP**	This is the part where the local IP address to be IPSec is selected.
5	**Local ID**	This is the section where the local credential is written.
6	**Remote IP**	It is the section where the public IP address of the location to be IPSec is entered.
7	**Remote ID**	It is the section where the credential of the public IP address to be IPSec is entered.
8	**Pre Shared Key**	This is the section where the shared key created for the IPSec tunnel is entered.



1	**IPSec Profile**	This is the part where the IPSec Profile configured in the IPSec Profile module is selected.
2	**IP/Network**	Local and remote network addresses for IPSec must be selected. (First, local and remote network addresses need to be added to the Objects and IDs menu.)
3	**Local**	The local IP / Network address on the Labris UTM device is selected.
4	**Remote**	The local IP / Network address of the other device to be IPSec is selected.

5	**Add IP/Network**	It is the button where local and remote IP/Network addresses to be IPSec are added.

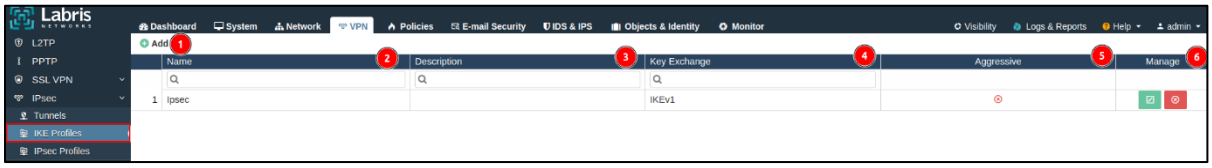
1	**Phase 1: Firewall Rule**	It is the button where the firewall rule is written for Phase 1.
2	**Phase 2: Firewall Rule**	It is the button where the firewall rule is written for Phase 2.
3	**Phase 2 No-NAT Rule**	It is the button where the No-NAT rule is written for Phase 2.
4	**Save**	This is the button where the IPSec tunnel configuration is saved.
5	**Close**	It is the button where the IPSec Tunnel window is closed, which is opened by clicking the Add button.

12.4.2 IKE Profiles

The IPSec IKE profile is used to configure IPSec VPN connections.

IKE is a protocol used to ensure that secure communication channels are established between two points.

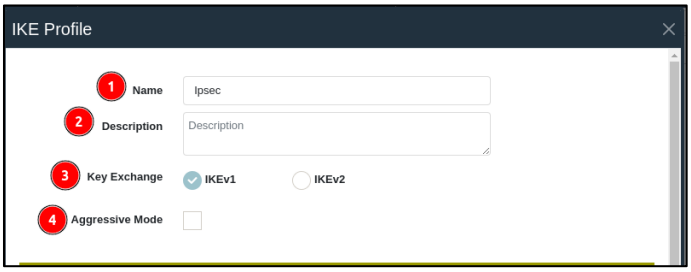
An IKE profile, on the other hand, contains several parameters that determine how IKE communications are performed.



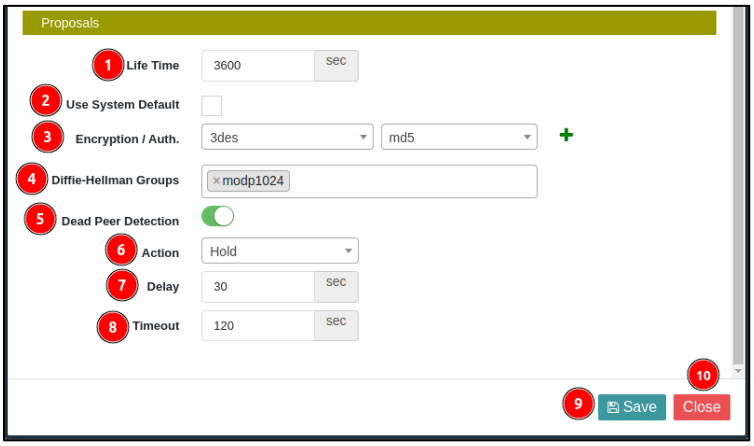
1	**Add**	This is the button where the process of adding IKE Profiles is done.

2	**Name**	This is the column where the name of the IKE Profiles is displayed.
3	**Description**	This is the column where the description of IKE Profiles is displayed.
4	**Key Exchange**	This is the column where the key exchange protocol is displayed. The key exchange protocols to choose from are IKEv1 and IKEv2. Both protocols are used to establish a secure connection over a VPN.
5	**Aggressive**	This is the column that shows the status of aggressive mode on IKE Profiles.
6	**Manage**	This is the column where the IKE Profiles that have been added are deleted or edited.

-To add an IKE Profile, click on the 'add' button to add an IKE Profile.



1	**Name**	This is the section where the name of the IKE Profile is entered.
2	**Description**	This is where the description of the IKE Profile to be added is entered.
3	**Key Exchange**	The key exchange protocol of the IKE Profile to be added is selected.
4	**Aggressive Mode**	In cases where the aggressive mode is turned on, they quickly authenticate the devices and exchange the keys. It is turned on when aggressive mode needs to be turned on.



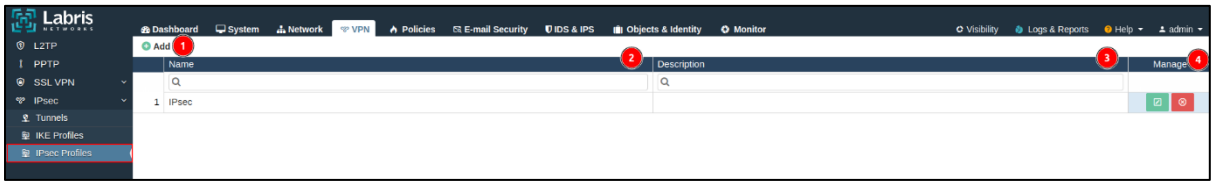
1	**Life Time**	Specifies the amount of time that the IKE Profile will be active.
2	**Use System Defaults**	It is the button where the settings that come by default via the Labris UTM device are used.
3	**Encryption/Authentication**	This is the section that specifies the encryption and authentication methods for the IKE profile.
4	**Diffie-Hellman Groups**	This is the section where the key exchange protocol for the IKE profile is selected.
5	**Dead Peer Detection (DPD)**	It is the protocol used to determine whether the device on the other side is working in the IKE profile connection.
6	**Action**	With the DPD protocol, the action to be taken in case the device on the other side cannot be accessed is selected.
7	**Delay**	The delay time in IKE communication is indicated.
8	**Timeout**	The timeout period for IKE communication is specified.
9	**Save**	This is the button where the IKE Profile settings are saved.

10	**Close**	This is the button where the IKE Profile window is closed.

12.4.3 IPsec Profiles

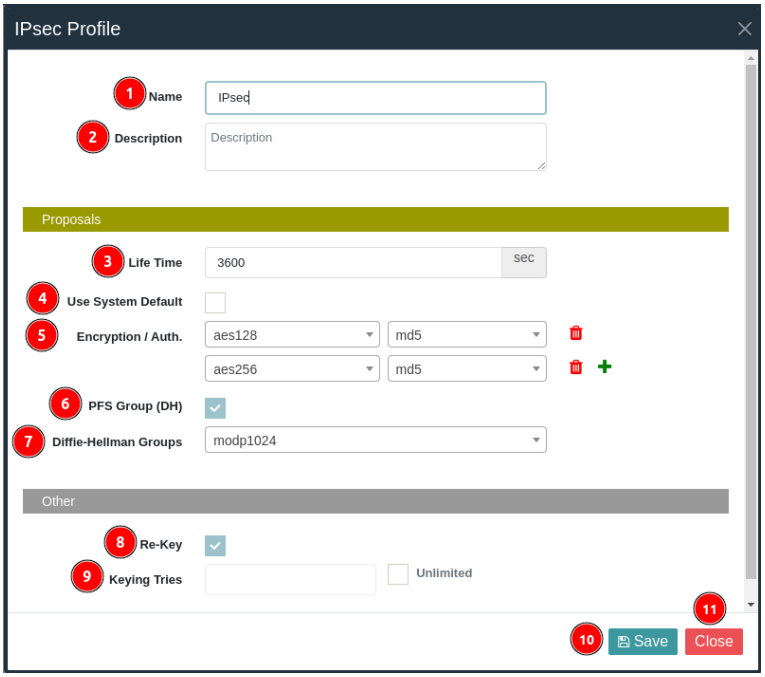
An IPSec profile contains key exchange algorithms and other parameters for specific security settings.

The IPSec profile determines which security algorithms will be used, key lengths, authentication methods, and other security parameters.



1	**Add**	This is the button used to add an IPSec Profile.
2	**Name**	This is the column where the name given to the IPSec Profile is displayed.
3	**Description**	This is the column in which the description given to the IPSec Profile is displayed.
4	**Manage**	This is the section where the IPSec Profile is deleted or edited.

-An IPSec Profile can be added by clicking the 'add' button.



1	**Name**	This is the section where the name to be given to the IPSec Profile is entered.
2	**Description**	This is the section where the description to be given to the IPSec Profile is entered.
3	**Life Time**	This is the section where the lifetime of the IPSec Profile proposal is specified.
4	**Use System Default**	The system defaults to Encryption / Authentications.
5	**Encryption / Authentication**	This is the section that specifies the encryption and authentication methods for the IPSec profile.
6	**PFS Group (DH)**	It is used to select the Diffie-Hellman groups.
7	**Diffie-Hellman Group**	This is the section where the key exchange protocol is selected for the IPSec profile.
8	**Re-Key**	This is the button where re-keying is turned on

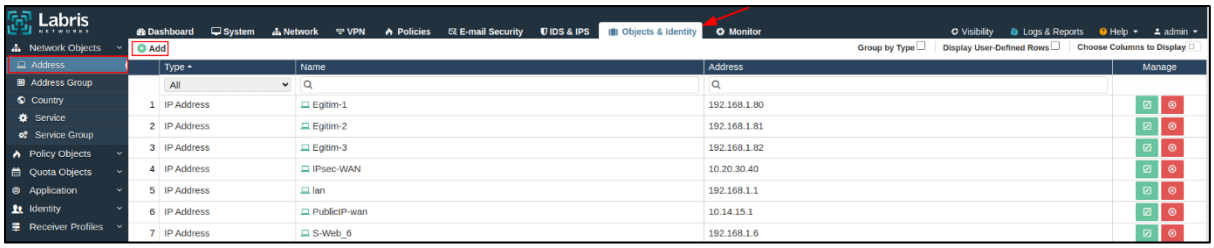
		for IPSec Profile.
9	**Keying Tries**	This is the section that specifies the number of entry attempts for the IPSec Profile offer.
10	**Save**	This is the button where the IPSec Profile configuration is saved.
11	**Close**	This is the button that closes the IPSec Profile window that opens.

Note

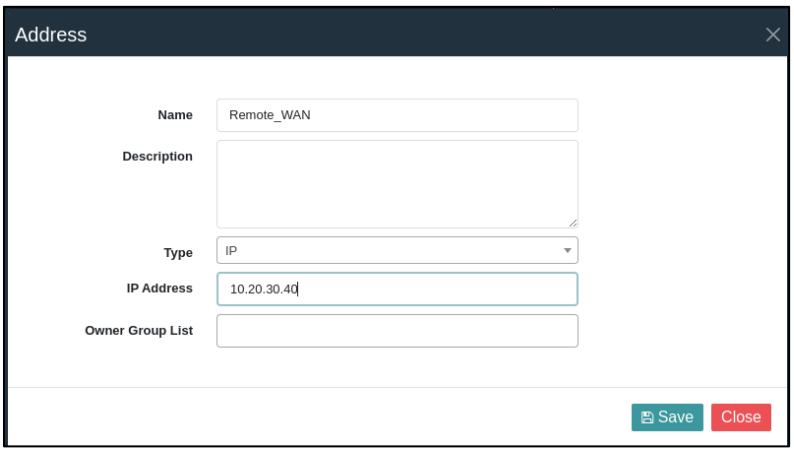
After configuring IPSec VPN, the rules must be written in the Policies module.

-Steps to write the rule in the Policies module of IPSec VPN

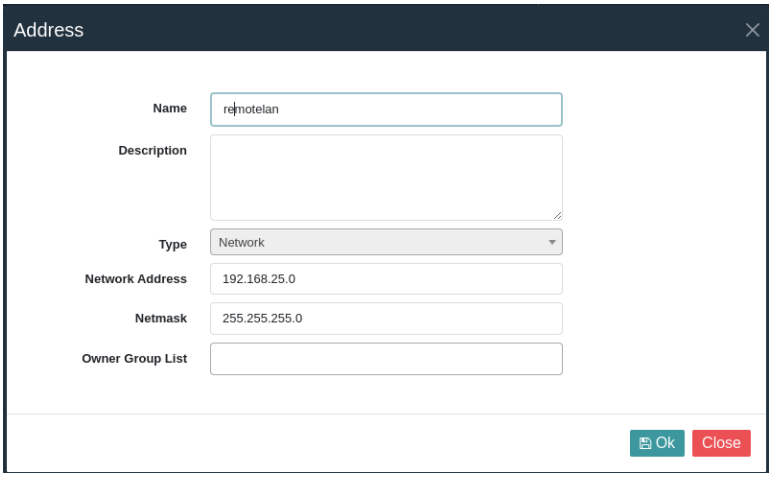
1. IPSec VPN is configured.
2. The Objects and Identities module opens.



3. After the Objects and IDs module is opened, objects are created for IPSec VPN. Object addition is done by clicking the Add button.

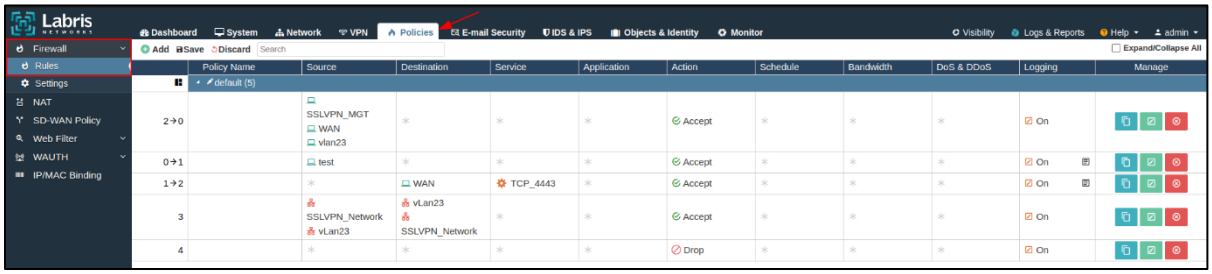


Add the Public IP of the remote device.

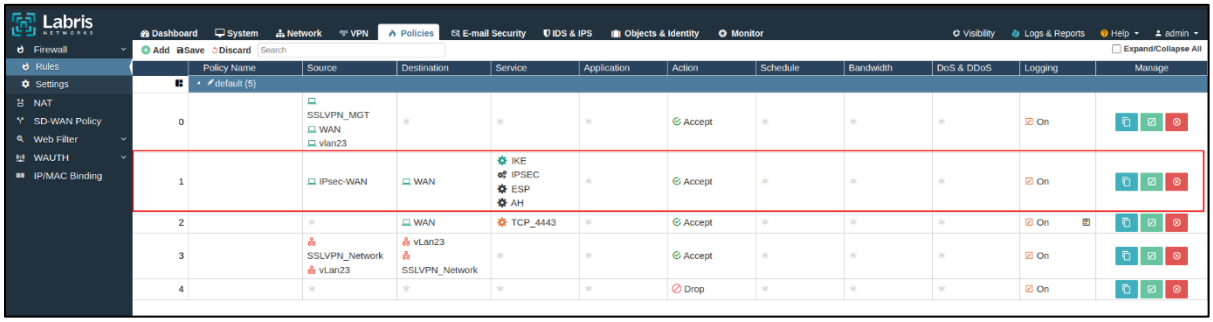


Add the local network of the remote device.

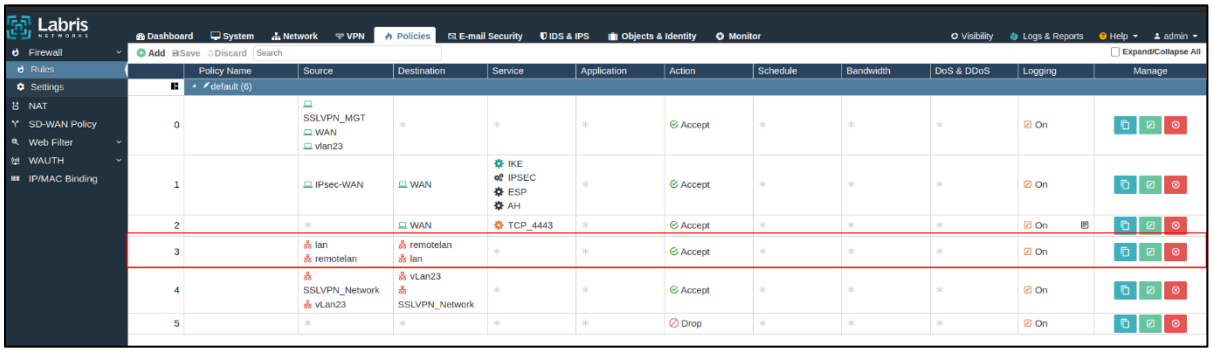
4. Objects for IPSec VPN are added in the Objects and Identities module. After the objects are added, the Policies module opens.



5. After the IPSec interface is added to rule 0, it is necessary to write the following rule between rule 0 and rule 1.



6. After the above access rule is written, it is necessary to write the communication rule of the local network on the other side where IPSec VPN will be made and the local network on the Labris UTM device.



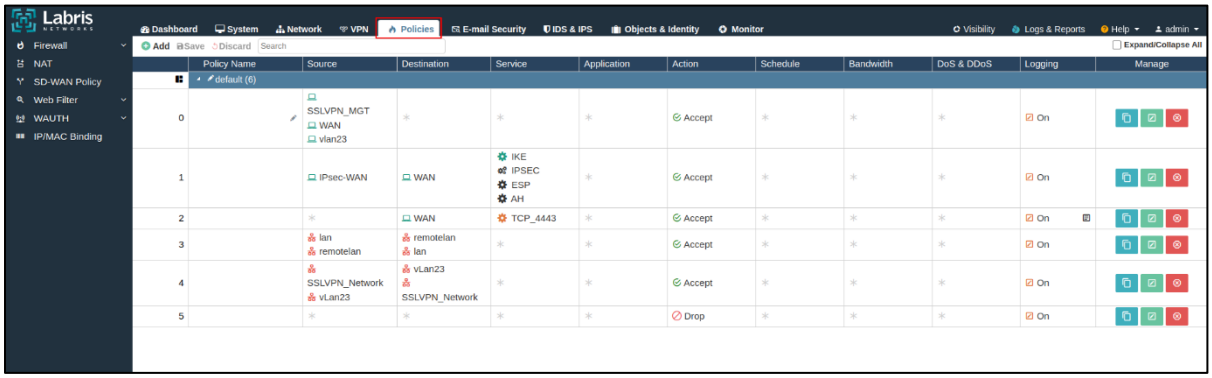
7. Once the definitions are made, you can test IPSec VPN access.

13. Policies

The Policies module is used to define security policies, such as what traffic the firewall will block or allow. This is the module where the firewall permissions or routing permissions on the Labris UTM device are written.

On the Labris UTM device, policies control inbound and outbound traffic by analyzing data packets that may be allowed or blocked on a network.

In the Policies menu, rules are written in the firewall, NAT, SD-WAN, Web Filter, WAUTH, and IP/MAC Matching modules.

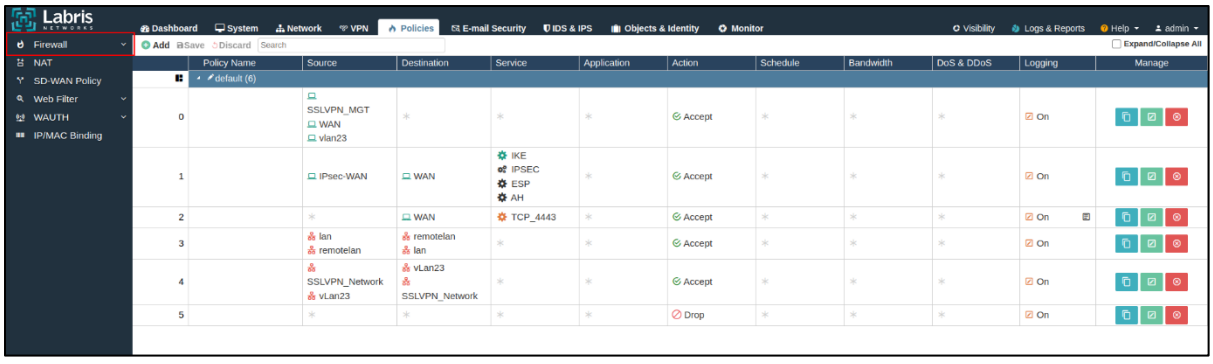


13.1 Firewall

The firewall module is used to protect a computer network or computer system from external threats.

The firewall can block incoming and outgoing traffic based on rules written in the firewall module.

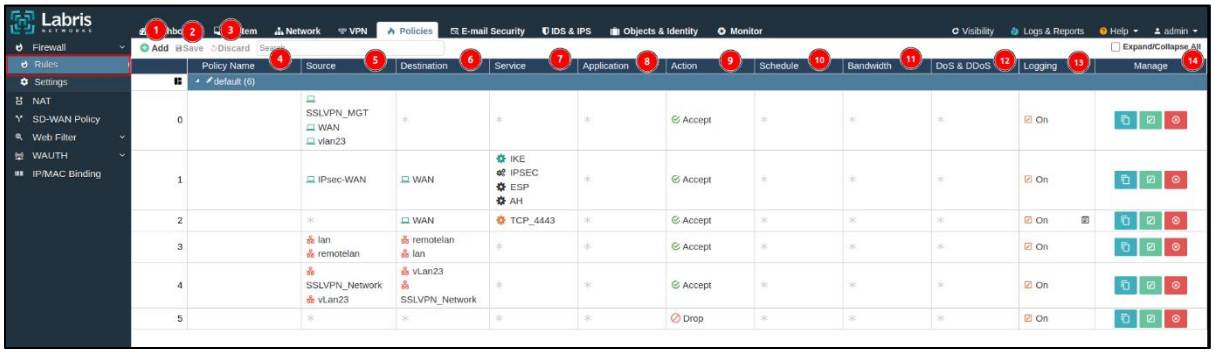
The firewall module is often based on policies such as blocking or allowing traffic coming through ports and restricting or blocking traffic from specific IP addresses. The firewall allows traffic from both sides of the network to flow as desired.



13.1.1Rules

It is the module on which the rules are written on the Labris UTM device. Traffic from the source to the destination is controlled.

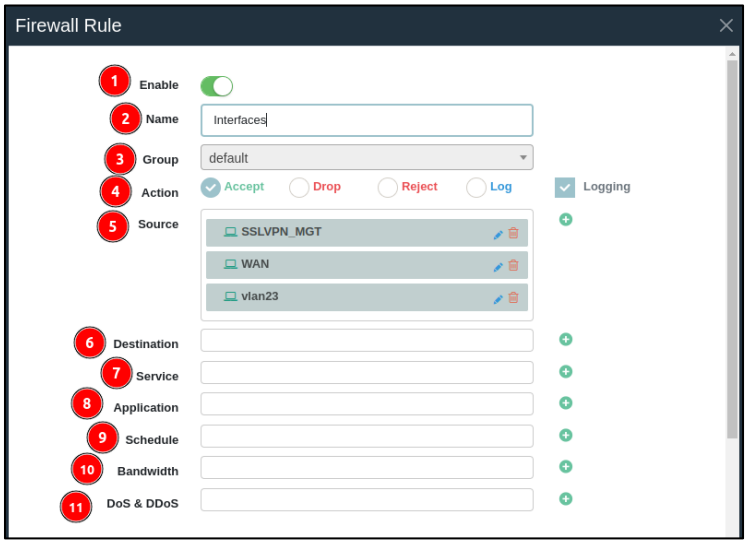
Source address, destination address, service, application, process, time, bandwidth, and DoS & DDoS objects are added to the rules to be written. The rules to be written can be arranged accordingly.



1	**Add**	It is the button where the rule addition process is done.
2	**Save**	It is the button where the added rules are saved.
3	**Discard**	It is the button used to cancel the rule to be added.
4	**Policy Name**	This is the column where the name of the added policy is displayed.
5	**Source**	This is the column where the source address(es) added to the rule are displayed.
6	**Destination**	This is the column where the destination address(es) added to the rule are displayed.
7	**Service**	This is the column where the service added to the rule is displayed.
8	**Application**	This is the column where the applications added to the rule are displayed.
9	**Action**	This is where the operation given to the rule is displayed. This column displays accept, drop, reject, or log.

10	**Schedule**	The rule is the column where the time is defined and displayed.
11	**Bandwidth**	The bandwidth objects that were added to the rule are displayed.
12	**DoS & DDoS**	This is the column where the DoS & DDoS object that is added to the rule is displayed.
13	**Logging**	This is the column where the added rule is recorded.
14	**Manage**	This is the column where the added rule is managed, deleted, or copied.

-To add a rule to the firewall, add a rule by clicking the 'add' button. After pressing the Add button, the rule is added by filling in the information on the screen that appears.



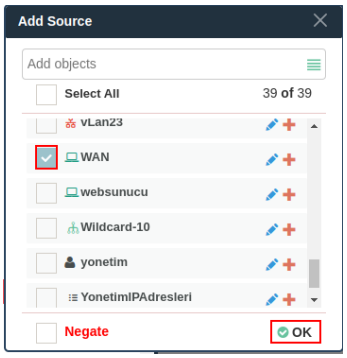
1	**Enable**	It is the button where the written rule is activated.
2	**Name**	It is where the name of the rule to be added is given.
3	**Group**	This is the section where the group to which the rule will be added is selected.

4	**Action**	This is the section where the operation of the rule is specified.
5	**Source**	This is the section where the source address(es) are selected. The Source addresses to be selected must be added to the Objects and Identities menu.
6	**Destination**	This is the section where the destination address(es) are selected. The destination addresses to be selected must be added in the Objects and Identities menu.
7	**Service**	This is the section where the services (TCP, UDP, IP, and ICMP) to be added to the rule are selected. The Services to be added must be added in the Objects and Identities menu.
8	**Application**	This is the section where applications that will be added to the rule are selected. To select an application, it must be listed in the Objects and Identities menu.
9	**Schedule**	This is the section where the running time interval of the rule is selected. To add a time object to a rule, it must be added to the Objects and Identities menu.
10	**Bandwidth**	This is the section where Bandwidth object to add to the rule is selected. To select the Bandwidth object, it must be added to the Objects and Identities menu.
11	**DoS&DDoS**	This is the section where DoS&DDoS object to be added to the rule is selected. To add the DoS&DDoS object to the rule, it must be added to the Objects and Identities menu.

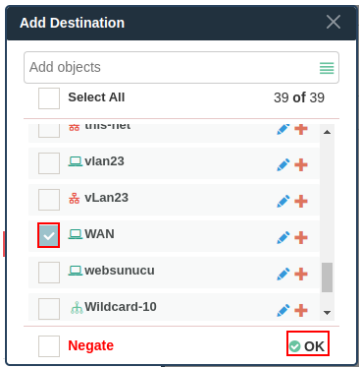
- There are 4 processes to be applied to the rules in the firewall. These are; Accept, Drop, Reject, and Log.

1. **Accept:** Allows the rule to be written. If there is a situation that complies with the rule, the rule is passed with permission.
2. **Drop:** It is the process by which the written rule is blocked. If there is a situation that complies with the rule, it makes a blocking operation.
3 **Reject:** It blocks the written rule but does not send a return packet.
4 **Log:** It is used in the bandwidth rule.

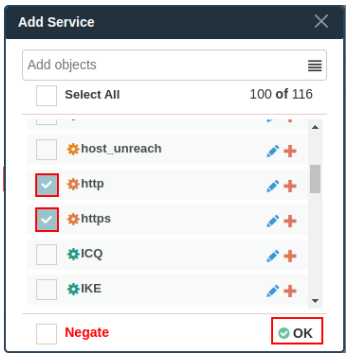
-To add the Source Address to the rule, click on the '+' expression where the source is written. On the screen that comes after clicking, the object or ID defined in the Objects and Identities module is added.



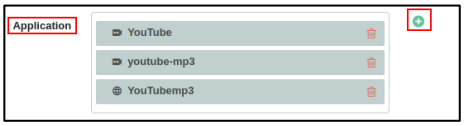
-To add the Destination Address to the rule, click on the '+' expression where the destination is written. On the screen that comes after clicking, the object or ID defined in the Objects and Identities module is added.

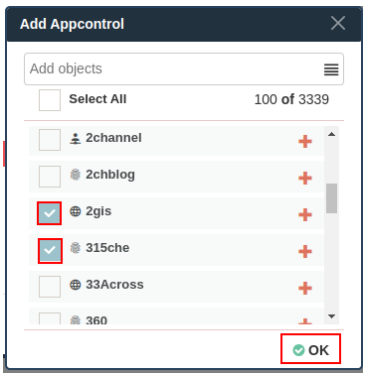


-To add a service to the rule to be written, click on the '+' expression in the place where the service is written. On the screen that comes after clicking, the service defined in the Objects and Identities module is added.

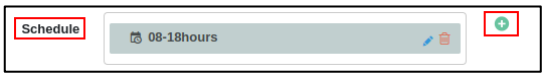


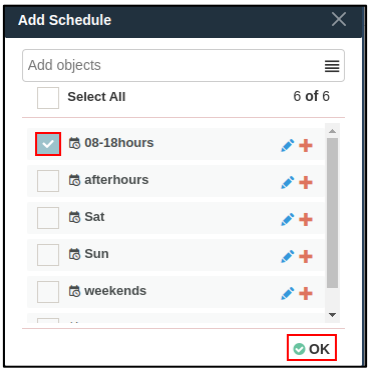
-To add an application to the rule to be written, click on the '+' expression where the application is written. On the screen that comes after clicking, application groups can be added to the rule, as well as selecting the applications in the database.



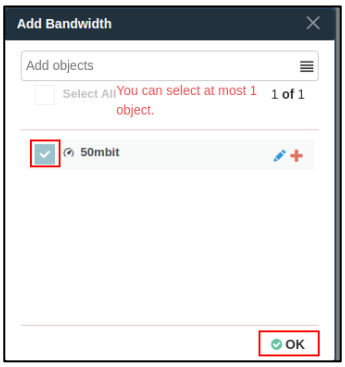


-To add time object to the rule to be written, click on the '+' expression where the time is written. On the screen that comes after clicking, time objects in the database or defined objects in the Objects and Identities module are selected and added to the rule.

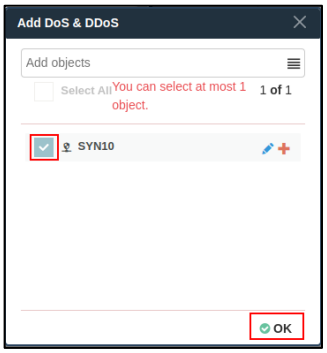




-To add a bandwidth object to the rule to be written, click on the '+' expression where bandwidth is written. On the screen that comes after clicking, time objects in the database or defined objects in the Objects and Identities module are selected and added to the rule.

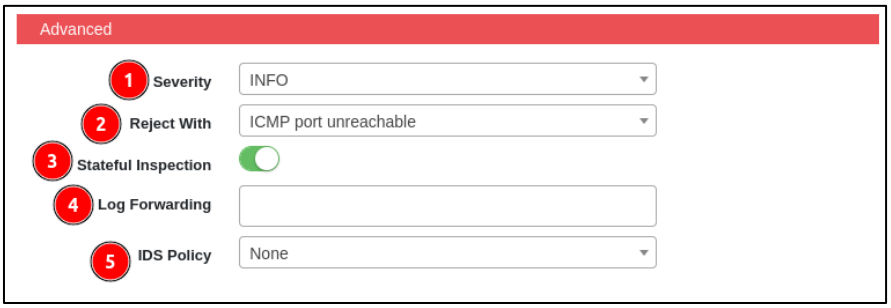


-To add a DDoS object to the rule to be written, click on the '+' expression where DDoS is written. On the screen that comes after clicking, DDoS objects in the database or added in the Objects and Identities module are selected and added to the rule.



Note

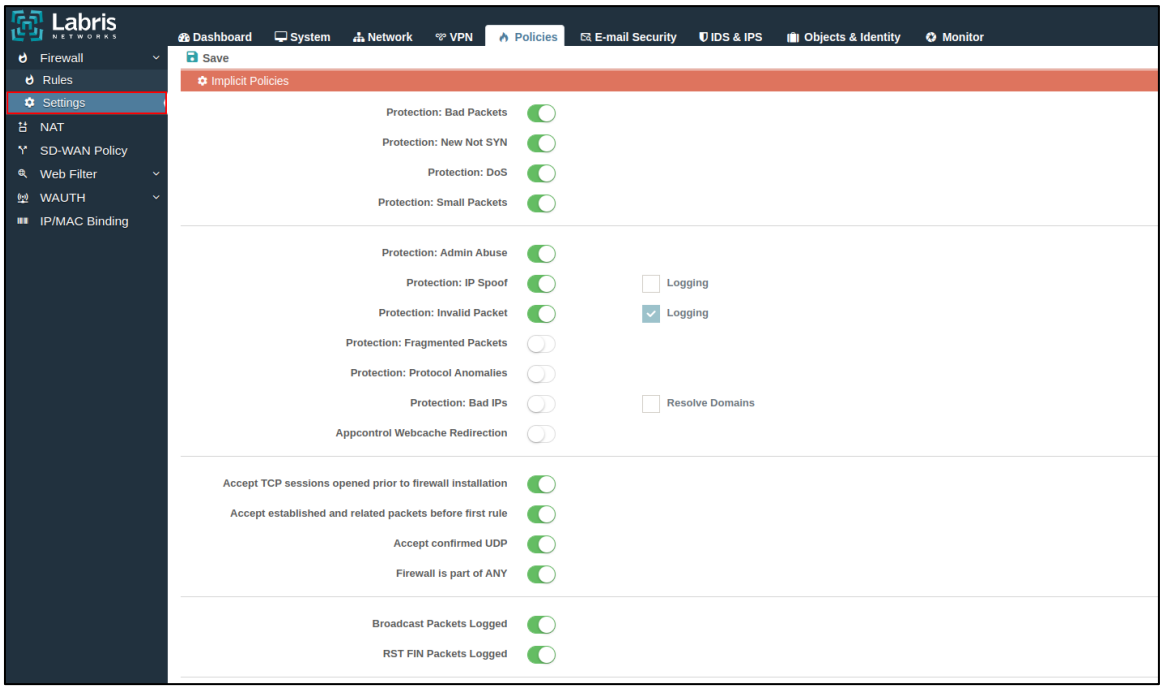
After the Firewall rule is added, the Save button must be pressed for the rule to take effect.



1	**Severity**	This is the section where the record level of the rule is specified.
2	**Reject With**	It is the section where the type of rejection of the rule is specified.
3	**Stateful Inspection**	This is the section where the status check of the rule is opened.
4	**Log Forwarding**	Select the Syslog server to which the record of the rule will be sent.
5	**IDS Policy**	Select the IDS policy.

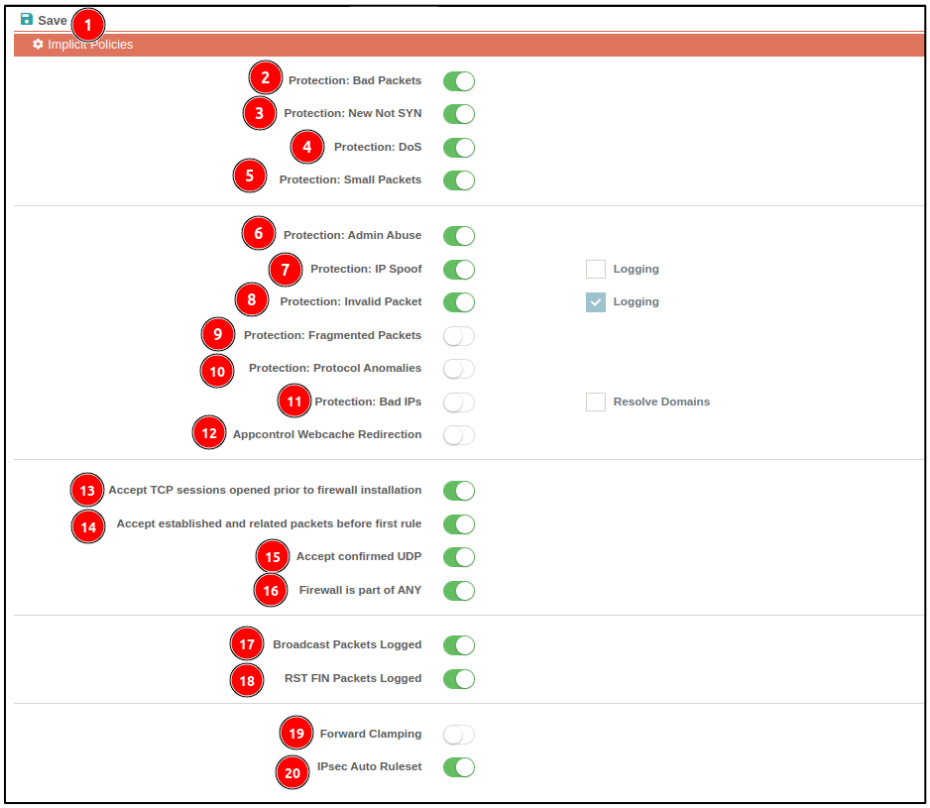
13.1.2 Settings

It is the module where firewall settings are made. In this module, indirect policies, protection port scanners, intrusion control, and SSH examination are performed.



13.1.2.1 Implicit Policies

Implicit policies are usually the part where longer-term and comprehensive policies are determined, rather than directly intervening like the rules set in the firewall.



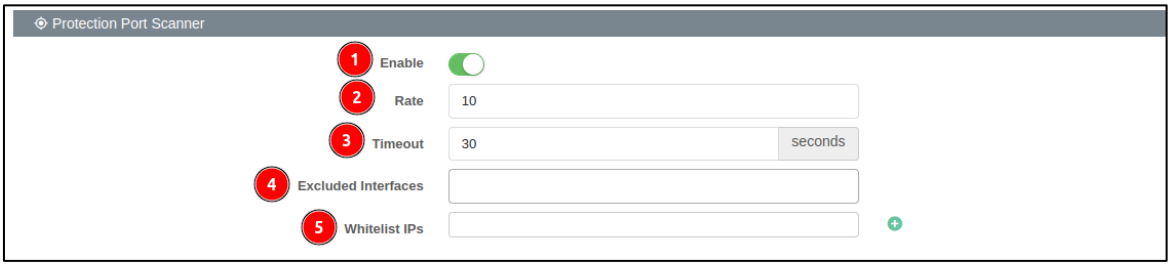
1	**Save**	It is the button where the changes made in the settings module are saved.
2	**Protection: Bad Packets**	It is a feature used to detect and block bad packets.
3	**Protection: New Not Syn**	It is a feature that prevents cases where the three-way handshake is not made.
4	**Protection: DoS**	It is the feature that prohibits requests that it defines as DoS.
5	**Protection: Small Packets**	It is the feature where the process of prohibiting small-sized packets.
6	**Protection: Admin Abuse**	It is a feature that prevents abuse of access authority by controlling the traffic of the user on the network to

		whom administrative access is granted.
7	**Protection: IP Spoof**	It is a feature that protects against spoofed IP addresses.
8	**Protection: Invalid Packet**	It is a feature that protects packets that are detected as invalid.
9	**Protection: Fragmented Packet**	It is a feature that protects fragmented IP packets.
10	**Protection: Protocol Anomalies**	It is the feature that protects in case the protocols in the network traffic are non-standard traffic.
11	**Protection: Bad IPs**	It is the property that controls IP addresses in network traffic.
12	**AppControl Webcache Redirection**	It is a feature that allows it to redirect to the cache for clients that are stuck in the application control rule.
13	**Accept TCP sessions opened prior to firewall installation**	It is a feature that allows the firewall to accept previously opened TCP sessions at the time changes are saved.
14	**Accept established and related packets before first rule**	It is the feature that allows it to accept established connections and related packets before the first rule.
15	**Accept Confirmed UDP**	It is the property that accepts validated UDP connections.
16	**Firewall is part of ANY**	It is the feature that the firewall is considered part of ANY.
17	**Broadcast Packets Logged**	It is a feature that records broadcast packets.

18	**RST FIN Packets Logged**	It is the feature that keeps track of RST and FIN packets.
19	**Forward Clamping**	It is the feature where forward clamping is turned on.
20	**IPsec Auto Ruleset**	It is a feature that sets an automatic rule for IPsec.

13.1.2.2 Protection Port Scanner

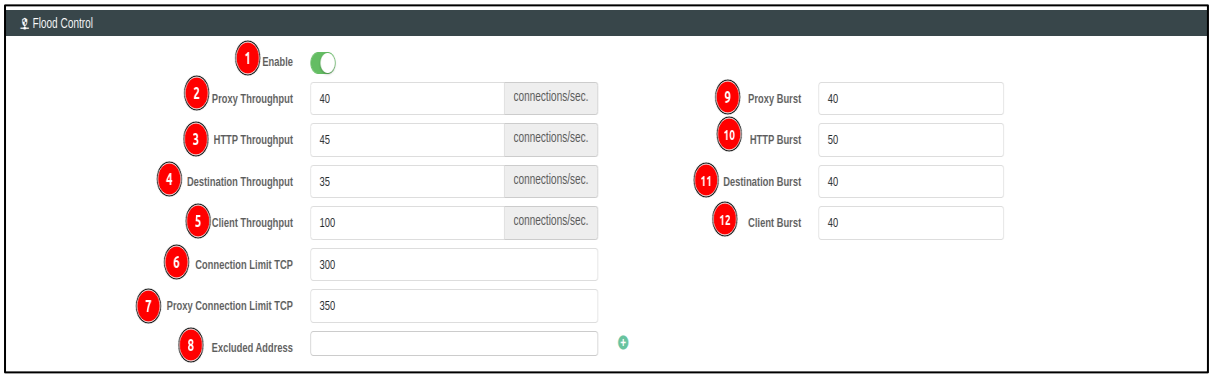
This section is the part of the Labris UTM device that monitors network traffic and blocks requests from an IP address to different ports.



1	**Enable**	This is the button where the protection port scanner is activated.
2	**Rate**	The total number of requests from the IP address is indicated.
3	**Timeout**	The period (sec) during which the IP address exceeding the rate will be banned is specified.
4	**Excluded Interface**	Select the interface that will not be included in the protection.
5	**Whitelist IPs**	IP addresses that will not be included in the protection are selected.

13.1.2.3 Flood Control

This is the section where attack control is performed by monitoring your network traffic.

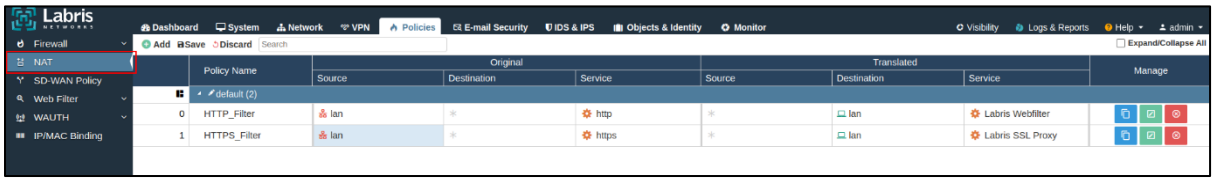


1	**Enable**	It is the button where attack control is activated.
2	**Proxy Throughput**	The total number of requests from the IP address is indicated.
3	**HTTP Throughput**	This is the section where the connection value per second of HTTP traffic is entered.
4	**Destination Throughput**	The throughput value of the target traffic is entered.
5	**Client Throughput**	The throughput value of the traffic created by the client is entered.
6	**Connection Limit TCP**	The value of the TCP connection limit is entered.
7	**Proxy Connection Limit TCP**	The value of the proxy's TCP connection limit is entered.
8	**Excluded Address**	The address or addresses that will not be included in the attack protection are entered.
9	**Proxy Burst**	The Proxy burst value is entered.
10	**HTTP Burst**	The HTTP burst value is entered.
11	**Destination Burst**	The target burst value is entered.

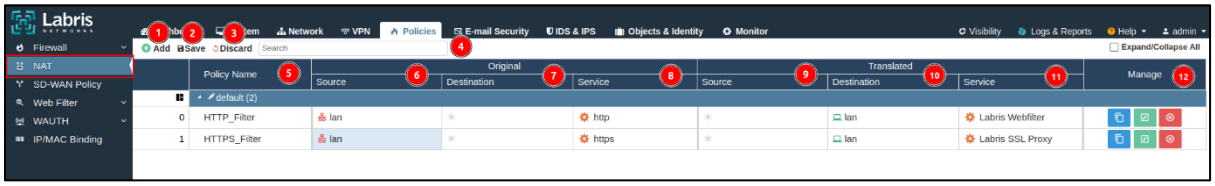
12	**Client Burst**	The client burst value is entered.

13.2 NAT(Network Address Translation)

Network Address Translation (NAT) means that the private IP addresses of devices on a network (192.168.x.x or 10.x.x.x) are replaced with public. NAT allows multiple devices on the same network to access the internet using the same public IP.



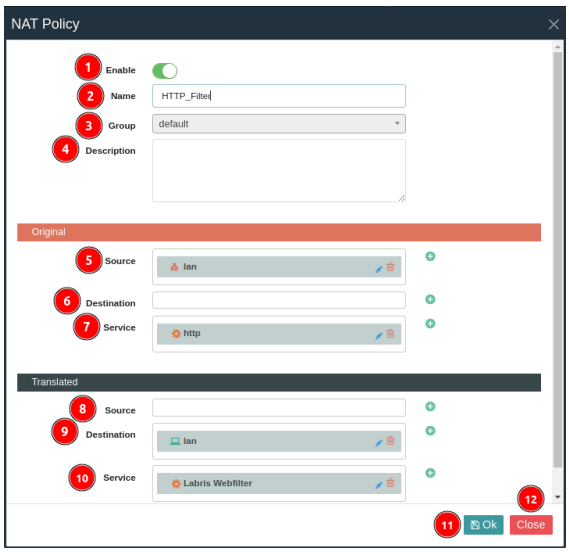
-Explanation of the table and software of the NAT rule in the NAT module;



1	**Add**	It is the button where the NAT rule is added.
2	**Save**	It is the button where the added NAT rules are saved.
3	**Discard**	It is the button where the added NAT rule is canceled.
4	**Search**	It is the section that is searched in the added rule.
5	**Policy Name**	This is the column where the name of the added NAT rule is displayed.
6	**Original Source**	This is the column that displays the original source address(es) that are added to the rule.
7	**Original Destination**	This is the column that displays the original destination address(es) that are added to the rule.
8	**Original Service**	It is the column where the original service added to the rule is displayed.
9	**Translated Source**	This is the column that displays the Changed source address(es) that are added to the rule.

10	**Translated Destination**	This is the column that displays the Changed destination address(es) that are added to the rule.
11	**Translated Service**	This is the column that displays the Changed service address(es) that are added to the rule.
12	**Manage**	It is the section where the written rule is edited, copied or deleted.

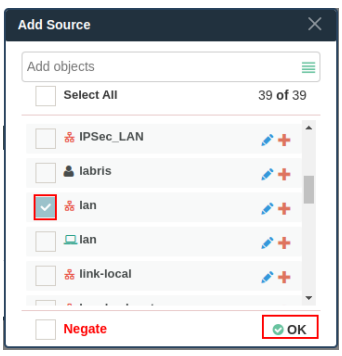
-For NAT rule addition, click the 'add' button and fill in the information on the screen that appears.



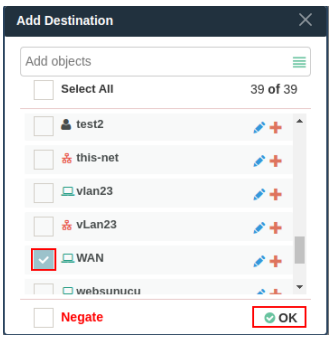
1	**Enable**	It is the button where the NAT rule to be written is enabled.
2	**Name**	Enter the name to be given to the NAT rule to be added.
3	**Group**	The group of the NAT rule to be added is selected.
4	**Description**	A description of the NAT rule to be added is entered.
5	**Original Source**	This is the section where the original source address(es) are selected. The Source addresses to be selected must be added to the Objects and Identities menu.

6	**Original Destination**	This is the section where the original destination address(es) are selected. The destination addresses to be selected must be added in the Objects and Identities menu.
7	**Original Service**	This is the section where the original service address(es) are selected. The service addresses to be selected must be added to the Objects and Identities menu.
8	**Translated Source**	This is the section where the changed source address(es) are selected. The Source addresses to be selected must be added to the Objects and Identities menu.
9	**Translated Destination**	This is the section where the changed destination address(es) are selected. The destination addresses to be selected must be added to the Objects and Identities menu.
10	**Translated Service**	This is the section where the original service address(es) are selected. The service addresses to be selected must be added to the Objects and Identities menu.
11	**Add**	It is the button where the typed NAT rule is saved.
12	**Close**	It is the button where the window that opens after clicking the Add button is closed.

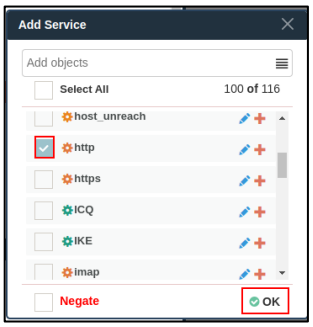
-To add the Original Source Address to the NAT rule, click on the '+' expression where the source is written. On the screen that comes after clicking, the object or ID added in the Objects and Identities menu is added.



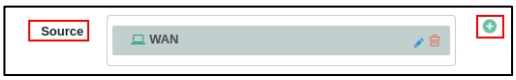
-To add the Original Destination Address to the NAT rule, click on the '+' expression where the destination is written. On the screen that comes after clicking, the object or ID added in the Objects and Identities menu is added.

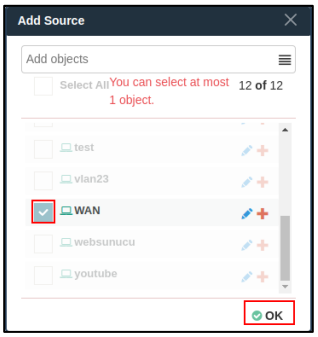


- To add the Original Service to the NAT rule, click on the '+' expression where the service is written. On the screen that comes after clicking, the object or ID added in the Objects and Identities menu is added.

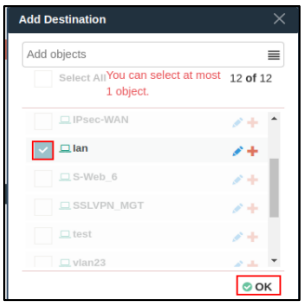


-To add a Changed Source Address to the NAT rule, click on the '+' expression where the Source is written. On the screen that comes after clicking, the object or ID added in the Objects and Identities menu is added.

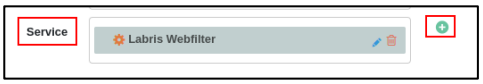


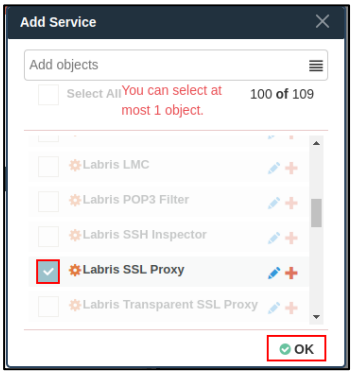


-To add a Changed Destination Address to the NAT rule, click on the '+' expression where the destination is written. On the screen that comes after clicking, the object or ID added in the Objects and Identities menu is added.



-To add a Changed service to the NAT rule, click on the '+' expression where the service is written. On the screen that comes after clicking, the object or ID added in the Objects and Identities menu is added.

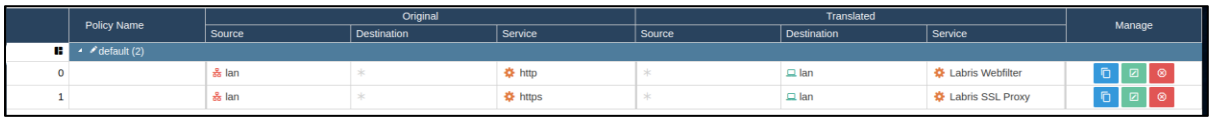




Note

After the NAT rule is added, the Save button must be pressed for the rule to take effect.

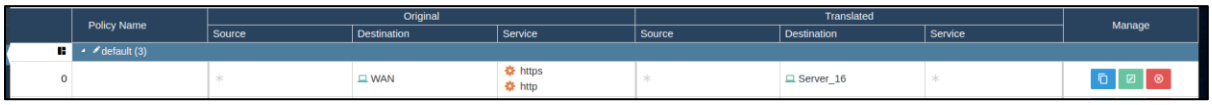
-HTTP and HTTPS filtering rules are written on the Labris UTM device as follows. The purpose of writing these rules is to block the sites that will be blocked in the Web Filter module. If there is a HTTP filtering rule, HTTP sites can be checked. If there is a HTTPS filtering, the certificate found on the Labris UTM device must be installed on the clients. In this way, the rule is written in the Web Filter module on HTTPS sites.



	Policy Name	Original			Translated			Manage
		Source	Destination	Service	Source	Destination	Service	
	default (2)							
0		lan	*	http	*	lan	Labris Webfilter	
1		lan	*	https	*	lan	Labris SSL Proxy	

-Example: Writing NAT and Firewall rules for access to the Web Server inside;

NAT Policy;



Global Policy;

Note

The places that appear as * in the rules written in Nat and General Policy mean any.When we examine Example-1, we see that the source part is *. We can read this NAT rule as redirecting http(80) and https(443) requests coming from any source to the external line to the web server.

Note

The order in the NAT and General Policy rules to be written is important. The written rules are read in order from top to bottom.

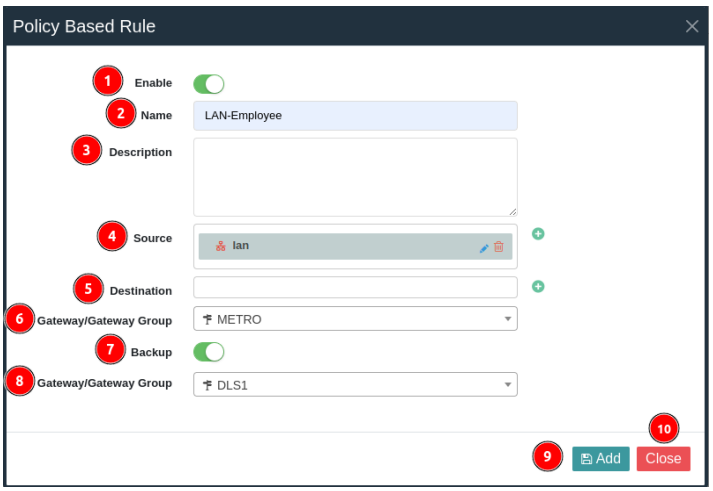
13.3 SD-WAN Policy

It is the module where rules are written for the Gateways added in the Network menu.

It is used in cases where there are two or more external links. In this module, the rule of which link to use to go from the source address to the destination address is written. A backup link is also added to the written rule.

1	**Add**	This is the button where the SD-WAN policy is added.
2	**Save**	This is the button where the changes made in the SD-WAN Policy are saved.
3	**Discard**	It is the button where the changes made in the SD-WAN Policy are canceled.
4	**Search**	This is the section where SD-WAN Policies are searched.
5	**Policy Name**	The name given to the SD-WAN Policy is displayed.
6	**Source**	This is the section where the source addresses are displayed.
7	**Destination**	This is the section where the destination addresses are displayed.
8	**Gateway**	This is the section where the selected gateway is displayed.
9	**Backup Gateway**	This is the section where the gateway selected as a backup is displayed.
10	**Manage**	This is the section where added SD-WAN Policies are edited, deleted, or copied.

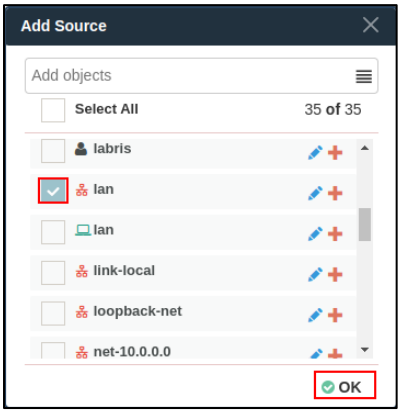
-The SD-WAN policy is added by clicking the 'add' button. After pressing the 'add' button, the SD-WAN Policy is written by filling in the information on the screen that appears.



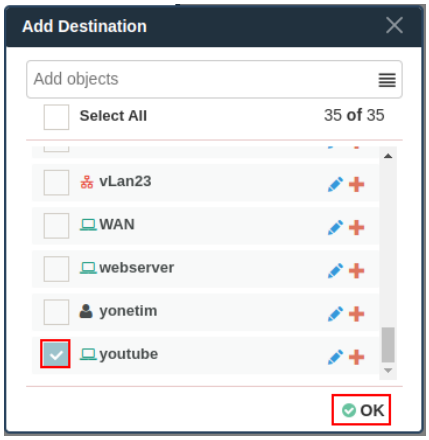
1	**Enable**	This is the button where SD-WAN is enabled.
2	**Name**	This is the section where the name of the SD-WAN policy is entered.
3	**Description**	This is the section where the description of the SD-WAN policy is entered.
4	**Source**	This is the section where the source address is selected.
5	**Destination**	This is the section where the destination address is selected.
6	**Gateway/Gateway Group**	This is the section where the grouped gateway is selected. A single gateway can also be selected.
7	**Backup**	This is the partition where the gateways are backed up.
8	**Gateway/Gateway Group**	A backup gateway is selected.
9	**Save**	This is the button where the SD-WAN policy is saved.

10	**Close**	It is the button where the SD-WAN policy is closed.

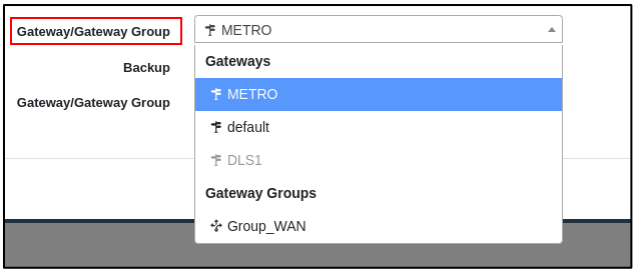
-To add a source address to the SD-WAN policy to the rule to be written, click on the '+' expression where the source is written. On the screen that comes after clicking, the address or addresses in the database or added in the Objects and Identities module are selected and added to the rule.



-To add a destination address to the SD-WAN policy to the rule to be written, click on the '+' expression in the place where the target is written. On the screen that comes after clicking, the address or addresses in the database or added in the Objects and Identities module are selected and added to the rule.

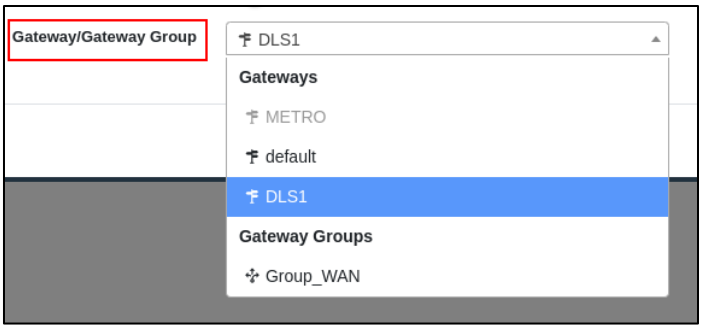


-Click '+' to add a gateway or gateway group to the SD-WAN policy in the rule to be written. After clicking, the gateways or gateway groups added in Network>SDWAN>Gateways are selected.



-The Backup button must be activated to add another link as a backup next to the gateway added for the rule to be written.

- After the backup link button is activated, it is necessary to select the link that will be the backup.

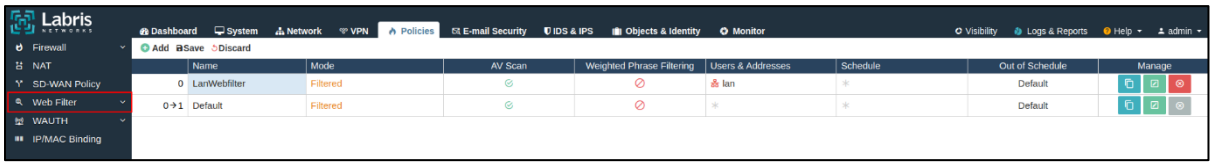


13.4 Web Filter

Web Filter is used to monitor and filter web traffic on the network.

It allows users to control access to certain websites and block certain categories of content. In this way, harmful content is prevented from entering the network, and provides security by restricting access to certain websites.

After adding HTTP and HTTPS rules to the NAT module on the Labris UTM device, the Web Filter module is edited.

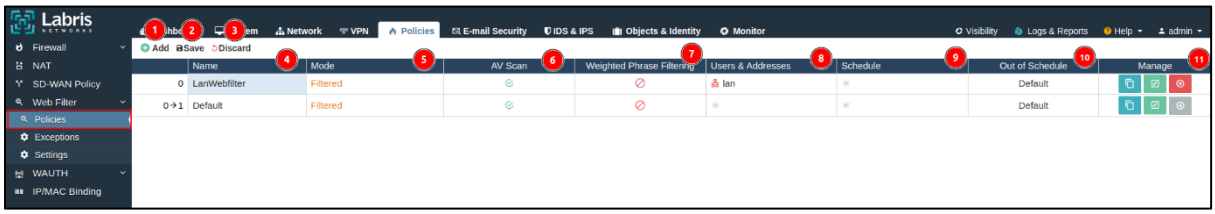


Note

If an HTTP rule is written, only rules are written on HTTP sites in the Web Filter module. If the HTTPS rule is written, rules can also be written on HTTPs sites after SSL

13.4.1Policies

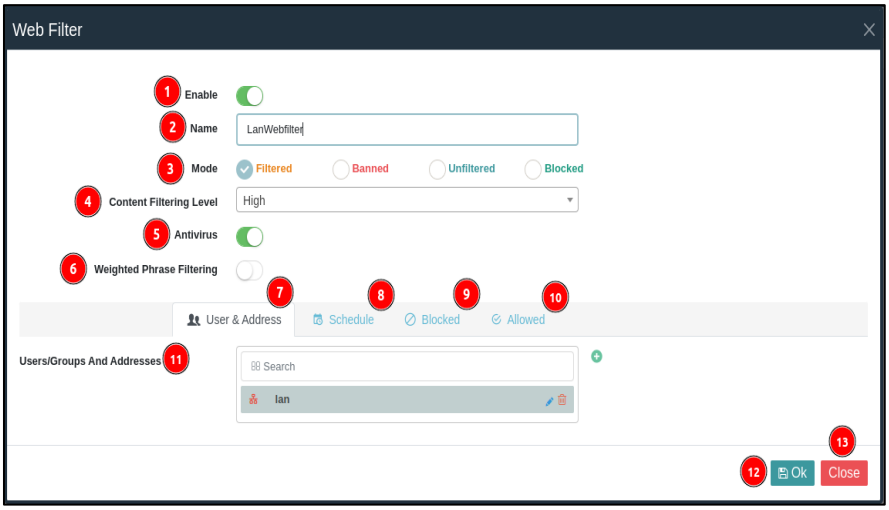
After the HTTP and HTTPS filtering rules are written, the Web Filter rules are edited. User, device, and network address-based rules can be written and edited according to your topology.



1	**Add**	This is the button where the Web Filter policy is added.
2	**Save**	This is the button where the changes made in the Web Filter policy are saved.
3	**Discard**	This is the button where the changes made in the Web Filter policy are abandoned.
4	**Name**	The name of the added Web Filter policies is displayed.
5	**Mode**	The Mode of the added Web Filter policies is displayed.
6	**AV Scan**	The status of whether the Antivirus Scan is on or off for the added Web Filter policies is displayed.
7	**Weighted Phrase Filtering**	The status of the Web Filter policies that have been added, whether Weighted Phrase Filtering is turned on or off, is displayed.
8	**Users & Address**	The users and addresses that have been added to the Web Filter policies are displayed.
9	**Schedule**	The runtime of the typed rule in the Web Filter is displayed.
10	**Out of Schedule**	Displays which rule applies out of schedule.

11	**Manage**	This is the section where the Web Filter rule is copied, edited, or deleted.

-To add a policy, the Web Filter policy can be added by clicking the 'add' button. After the Add button is pressed, the Web Filter rule can be added by filling in the information on the screen that appears.



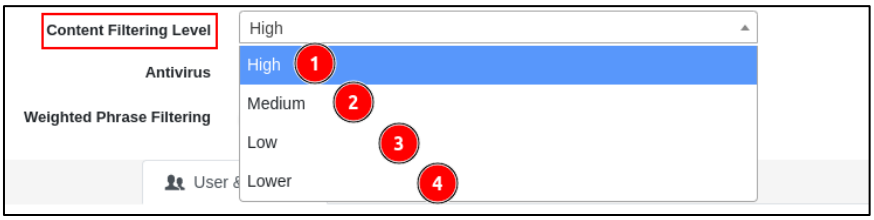
1	**Enable**	This is the button where the Web Filter policy is enabled.
2	**Name**	Enter the name of the Web Filter policy.
3	**Mode**	The mode of the Web Filter policy is selected.
4	**Content Filtering Level**	The content filtering level of the Web Filter policy is specified.
5	**Antivirus**	It is the button where the antivirus mode is turned on in the Web Filter policy.
6	**Weighted Phrase Filtering**	It is the button where the weighted expression filtering mode is turned on in the Web Filter policy.
7	**User & Address**	Select the users and addresses to which the Web Filter policy will be applied.
8	**Schedule**	Specifies when the Web Filter policy will take effect.

9	**Blocked**	This is the section that contains domain names, URLs, extensions, application types, regular expressions, and contents to be blocked in the Web Filter policy.
10	**Allowed**	This section is where domains, URLs, and content are allowed in the web filter policy.
11	**Users/Groups Addresses**	In this section, user and address information is added to the Web Filter policy.
12	**Save**	This is the button where the Web Filter policy is saved.
13	**Close**	It is the button where the Web Filter policy screen that opens after clicking the 'add' button is closed.

- Filter Mode must be selected to write a Web Filter Policy. The task of each selected mode is different.

1	**Filtered**	The disabled and permitted sections of the Web Filter policy are used. If this mode is active, the blocked and allowed sections are active.
2	**Banned**	Disabled and permitted sections cannot be used. All sites are banned. If this mode is active, the blocked and allowed sections are inactive.
3	**Unfiltered**	Block and allow sections are not available. Users use the internet unfiltered without being stuck with the web filtering policy. If this mode is active, the blocked and allowed sections are inactive.
4	**Blocked**	All of the categories in the disabled section are selected. All sites or categories are blocked, except for sites that have been added to the Allowed section.

-The content filtering level is used to determine the types of content that users are allowed or blocked to access. The Labris UTM device has four content filtering levels: 'lower, low, medium, and high'.

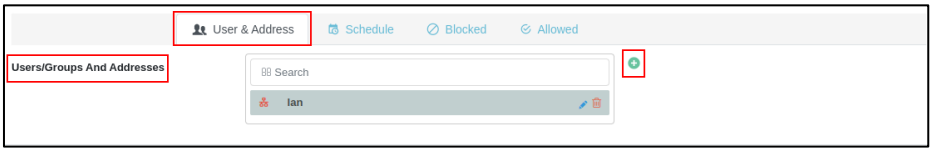


1	**High**	It is the most restrictive level of filtering. If the content filtering level is set high, malicious content such as adult content, violent content, gambling sites, etc. will be blocked.
2	**Medium**	If the content filtering level is set to medium, it blocks adult and violent content while providing a wider reach to content in some categories.
3	**Low**	When a low level is selected, it is usually intended for children or sensitive users. It blocks adult and violent content and certain categories, such as gambling.
4	**Lowest**	It is the least restrictive level of filtering. The level of filtering is less restrictive and allows users to access a wider variety of content.

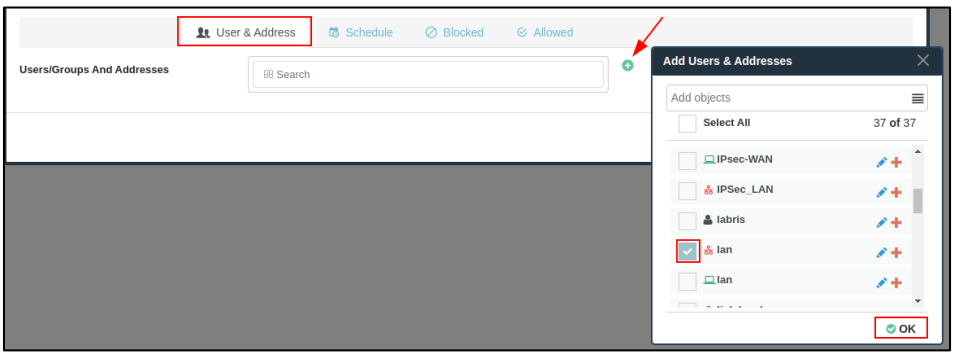
- When the Anti-Virus option is enabled, it checks and blocks access to infected sites.

- Weighted Phrase Filtering blocks a particular keyword or phrase by deciding whether it poses a threat or is content that should be allowed.

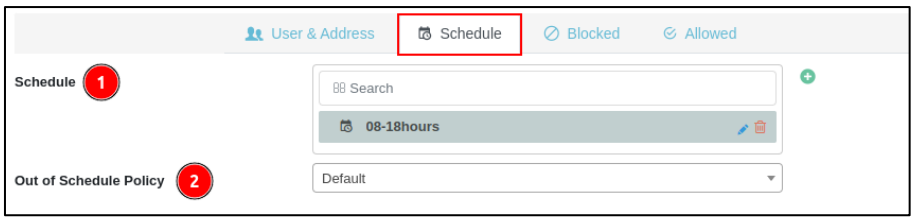
- To add Users & Addresses to the Web Filter policy, users or addresses must be added in the Objects and Identities module. After this process, the user and address can be added to the web filter rule.



-User or address can be added to the Web Filter rule by clicking the 'add' button.

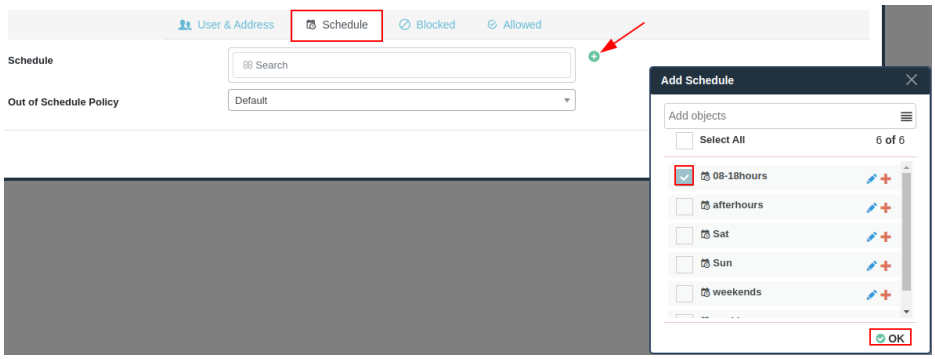


-A schedule object must be added to the Objects and Identities menu to add a schedule to a Web Filter policy. After you add the schedule object, this object can be added to the Web Filter policy.

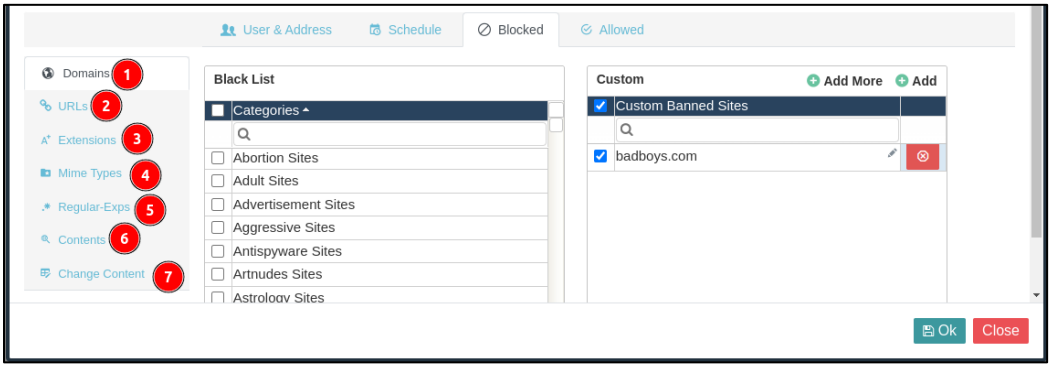


1	**Schedule**	Specify the time at which the web filter rule will run.
2	**Out of Schedule Policy**	In this section, it is determined which Web Filter policy should be applied at a different time interval than the specified time.

-To add time to the policy, click the 'add' button and select the schedule of the Web Filter policy.



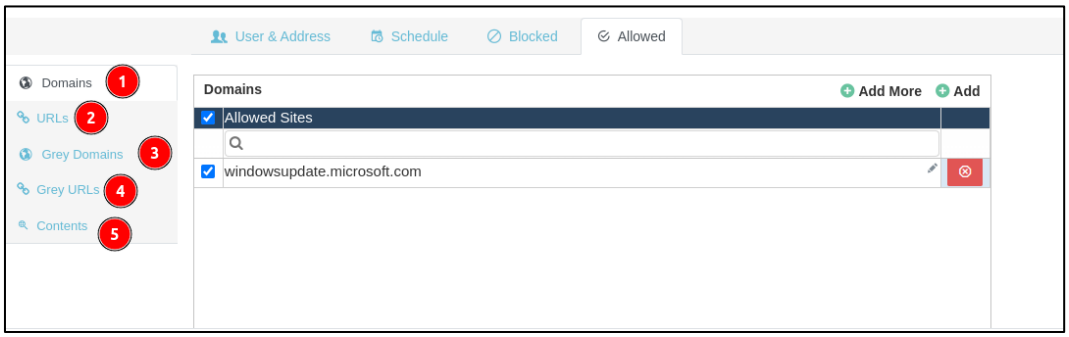
-In the Web Filter policy, the Blocked tab is used to block Domains, URLs, Extensions, Mime Types, Regular Expressions, Contents, and Content Replacement.



1	**Domain**	In this section, the categories selected to block Domain Names in certain categories, or the Domain Names that are specifically wanted to be added can be blocked. For example, a specific Domain Name such as "youtube.com" can be blocked specifically or blocked by categories.
2	**URLs**	In this section, the categories selected to block URLs in certain categories, or the URLs that are specifically wanted to be added can be blocked. For example, a specific URL such as "profile.youtube.com" can be blocked specifically or blocked by categories.
3	**Extensions**	This is the section where the extensions to be blocked are selected. Extensions can be added specifically. (**ex.** .pdf)
4	**Mime Type**	It blocks a file by identifying its content type. Application types can be selected as default on the Labris UTM device or custom application types can be added to Web Filter rules. (**ex.** application/mp4, image/jpeg)
5	**Regular-Exps**	Regular Expressions, which are on the device by default, can be selected or Regular Expressions can be added. (**ex.** (yimg.com\/image\/))
6	**Contents**	This is the section where the contents of the site are prohibited. Default content can be selected on the

		device or added customarily. (**ex**. gambling)
7	**Change Content**	It is the section where the content of the text on the site is changed. Here the text is to be replaced and the new text is entered. (Ex. changes a text that contains gambling to forbidden.)

-In the Web Filter policy, the Allowed tab is used to allow Domain Name, URLs, Extensions, Gray Sites, Gray URLs, and Content.



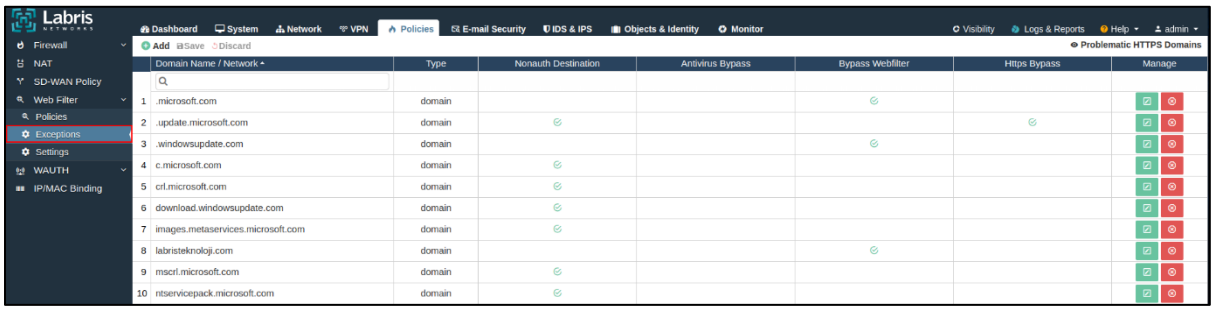
1	**Domains**	This is the section where Added Domains are allowed. (**ex.** youtube.com)
2	**URLs**	This is the section where the inserted URL address is allowed. (**ex.** youtube.com/spor)
3	**Grey Domains**	It is used to filter an entire site. (**ex.** labristeknoloji.com)
4	**Grey URLs**	It is used in cases where it is desired to filter a certain part of a site and not the rest. (**ex.** labristeknoloji.com/support)
5	**Contents**	This is the section where content within the site is allowed. Default Content on the device can be selected or content can be added specifically. (**ex.** gambling)

Note

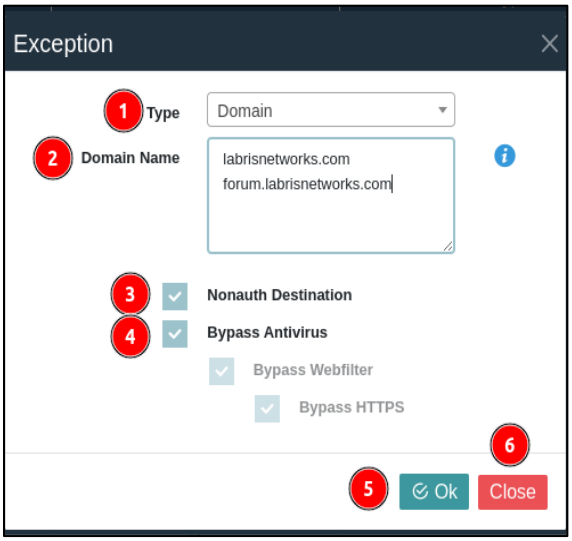
Sites added with exceptions work on a priority basis.

13.4.2 Exception

This is the module where sites that will not be included in the web filter policy are entered. Sites added as exceptions that come by default in the Labris UTM device can be used, or a new site can be added as an exception.



-To add a website as an exception, click the 'add' button to add the exception site.



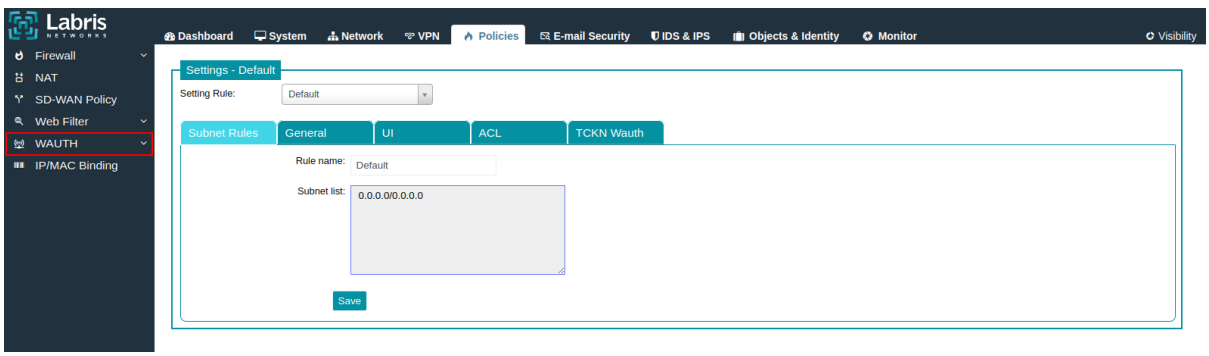
1	**Type**	The type to be added is selected as an exception. Adding is done by selecting the Domain Name or Network Address type.
2	**Domain Name**	This is the section where the Domain Names to be added as an exception are entered.

3	**Nonauth Destination (Type: Domain)**	It is the button where access to unauthorized targets within the site is allowed.
4	**Bypass Antivirus (Type: Domain)**	It skips antivirus scanning on the site to be added as an exception.
5	**Bypass Webfilter (Type: Domain)**	It bypasses the Web filtering policy on the site to be added as an exception.
6	**Bypass HTTPS (Type: Domain)**	The site to be added as an exception bypasses HTTPS filtering.
7	**Bypass HTTPS (Type: Network Address)**	It opens when the network address is selected as the type. HTTPS is the section where Network Addresses that will not be included in the filter are added.
7	**Save**	It is the button where the changes made are saved.
8	**Close**	It is the button where the window that opens is closed.

13.5 Wauth

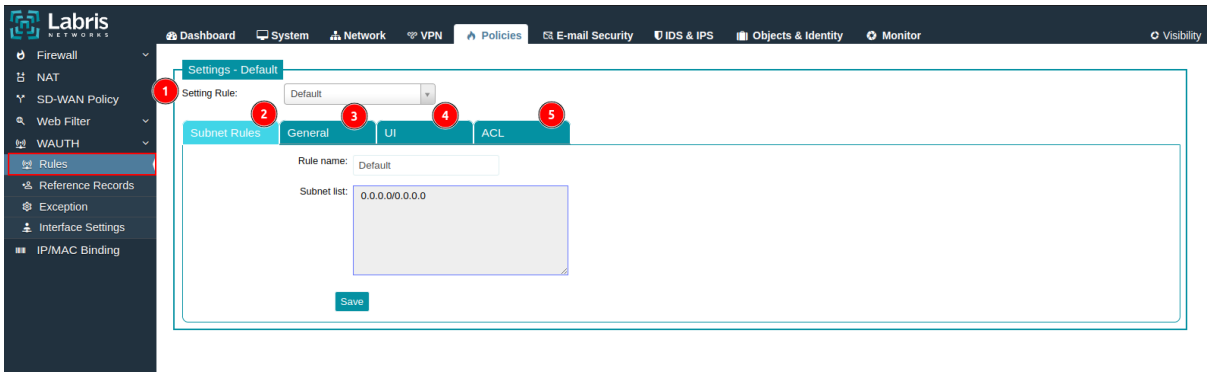
Wauth is the module used for authentication for users and guests. In corporate networks or networks used for guests, login processes are performed with user authorization. It allows users to record their browsing on the Internet with their login information.

Labris UTM devices have Local Authorization, SMS, Active Directory, Hotel Integration, TC NO NVI Verification, and Passport authorizations.



13.5.1Policy

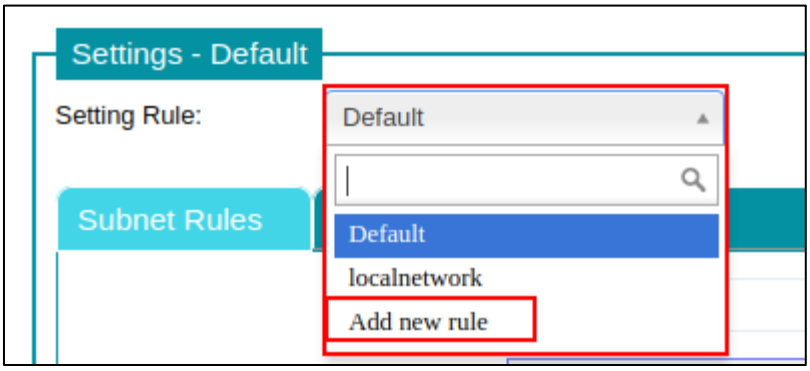
It is the module where the authorization forms of users and guests are adjusted, and the settings are made as the information on the login screen is edited. It is the module where the Wauth rule for local IP addresses is regulated.



1	**Setting Rule**	In this section, which wauth policy will be written is selected.
2	**Subnet Rules**	This is the section where the network address of the selected rule is entered.
3	**General**	This is the section where the authorization of the users who will log in to Wauth is set.
4	**UI**	It is the section where the user interface arrangement is made for the users who will log in to Wauth.
5	**ACL**	It is the section where the rules for controlling the access of users who will log in to Wauth are written.

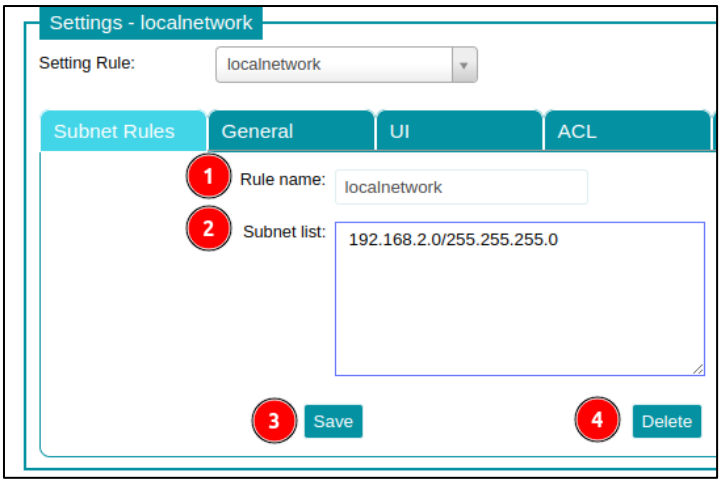
13.5.1.1 Add New Rule

It is used to add a new rule to the Labris UTM device other than the default Wauth rule. The purpose of adding a new rule may be to use different authorizations on both of your local networks or to manage two local networks with different rules.



13.5.1.2 Subnet Rules

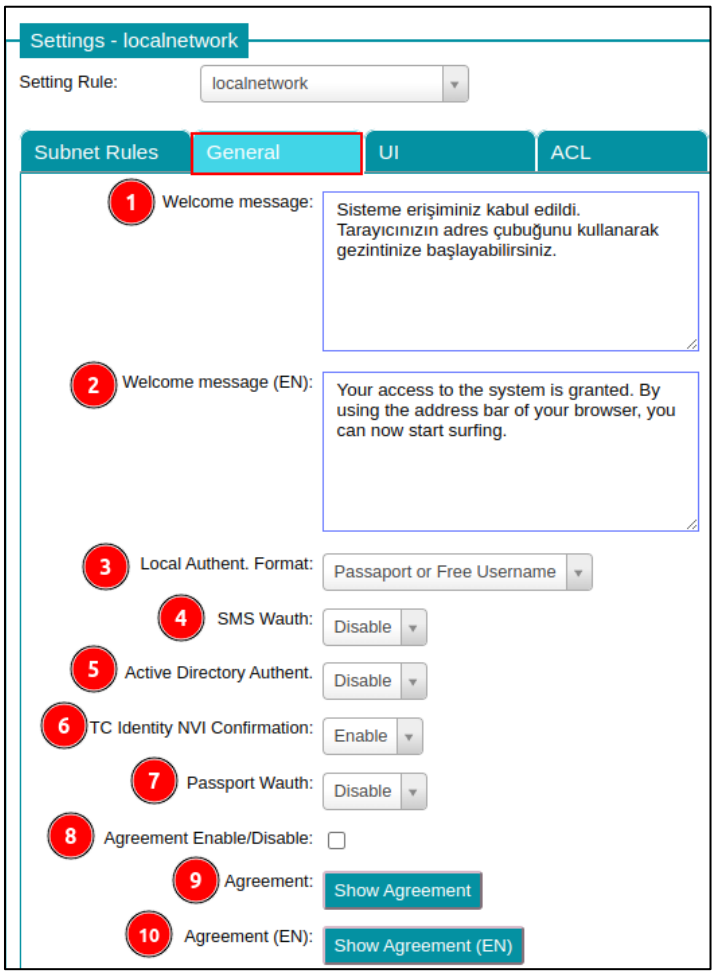
This is the section where the network address to which the Wauth rule will be applied is entered. By default on the Labris UTM device, it comes as '0.0.0.0/0.0.0.0'. A new rule needs to be added to add a new IP address.



1	**Rule Name**	This is where the name of the Subnet Rule is entered.
2	**Subnet List**	This is where the local network address to which the policy will be applied is entered. More than one local network address is entered. (**Ex.**192.168.2.0/255.255.255.0, 10.10.1.0/255.255.0.0)
3	**Save**	This is the button where the Subnet Rules are saved.
4	**Delete**	This is the button where the Subnet Rule is deleted.

13.5.1.3 General

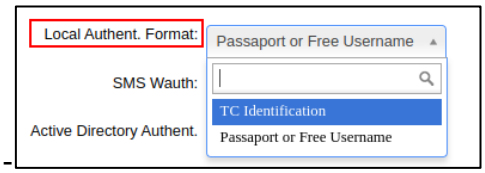
In the General Settings section, the welcome screen for users and the authorization formats of users are set.



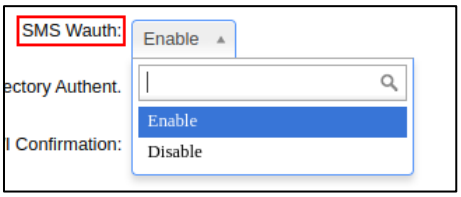
1	**Welcome Message**	It is the welcome message that users receive after logging into Wauth.
2	**Welcome Message (EN)**	It is the English welcome message that users receive after logging in to Wauth.
3	**Local Authent. Format**	This is the button where the subnet rules are saved. Users who are added to the Objects and Identities module on the Labris UTM device log in to Wauth.
4	**SMS Wauth**	It authenticates users via SMS to join the network.
5	**Active Directory Authent.**	It is used in cases where users in the Active Directory need to log in to Wauth with their usernames and

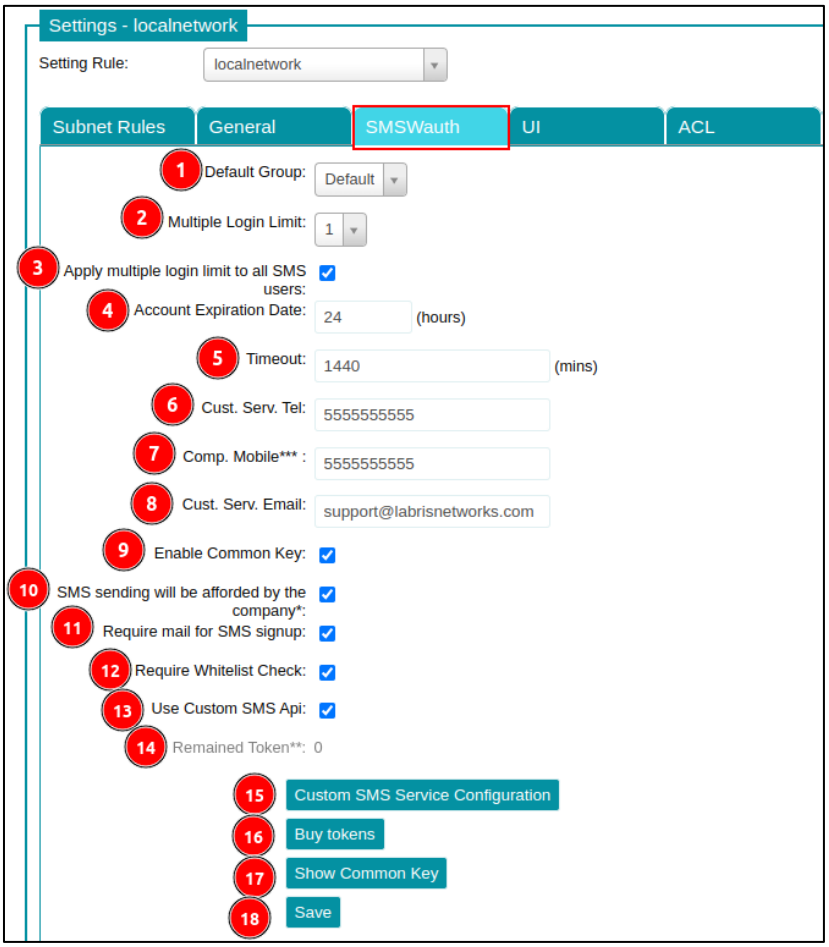
		passwords after Active Directory integration is made on the Labris UTM device.
6	**TC Identity NVI Confirmation**	It is used for users to log in to Wauth using their TR ID numbers.
7	**Passport Wauth**	It is used for users to log in to Wauth using their Passport details.
8	**Agreement Enable/Disable**	This is the button where the contract is activated or deactivated when logging into Wauth.
9	**Agreement**	It is the button where the Turkish version of the contract is displayed.
10	**Agreement (EN)**	It is the button where the English version of the contract is displayed.

- In case the Local Authorization Form is enabled, authorization is made with the TR ID number or passport of the users.



-When SMS Wauth is enabled, it allows users to log in to Wauth via SMS. After SMS Wauth is enabled, the SMS Wauth section opens.



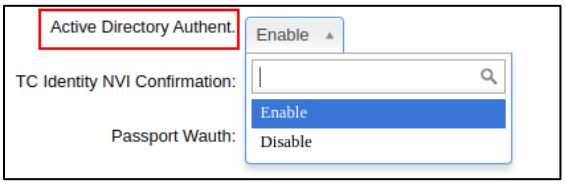


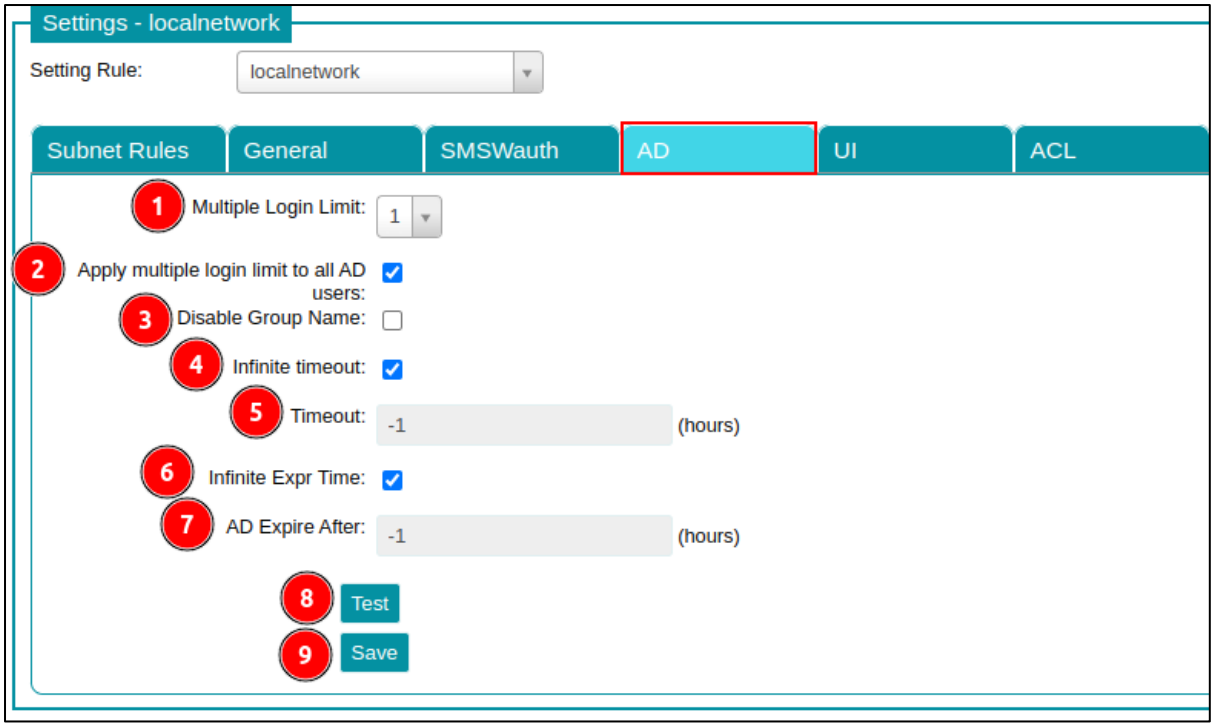
1	**Default Group**	The group in which SmsWauth will be enabled is selected.
2	**Multiple Login Limit**	The number of different devices that the user logged in with the SMS auth method can connect to with the same user is selected.
3	**Apply Multiple login limit to all SMS users**	In the section where the multiple login limit is enabled for users who interact with SMS.
4	**Account Expiration Date**	This is the section where the deletion time of the account opened with SMS Wauth is specified.
5	**Timeout**	This is the section where the timeout period of the logged-in user is specified.

6	**Cust. Serv. Tel**	This is the section where the Technical Support phone number is entered.
7	**Comp. Mobile**	This is the section where the Institution's Mobile phone number is entered.
8	**Cust. Serv. Email**	It is the section where the technical support e-mail is entered.
9	**Enable Common Key**	This is the section where the public key is activated.
10	**SMS Sending will be afforded by the company**	If the SMS sending is to be met by the company and the institution, it is opened. If it is opened, it is necessary to buy tokens from the company.
11	**Require Mail For SMS Signup**	It is enabled in cases where the mail address is required to log in SMS Wauth.
12	**Request Whitelist Check**	Allowed GSM numbers are allowed to login via SMSWauth.
13	**Use Custom SMS Api**	It is used in the case where the SMS provider is to be used.
14	**Remained Token**	In the case of receiving a token, the remaining token is seen. Each token means one SMS.
15	**Custom SMS Service Configuration**	It is the button where the provider settings to be used as the SMS provider are made.
16	**Buy Token**	In cases where the Labris UTM device is used as an SMS provider. It is the place where the remaining SMS right is displayed.
17	**Show Common Key**	This is the button where the public key specified for SMS Wauth is displayed.

18	**Save**	This is the button where SMSWauth settings are saved.

-It is used when users who will log in to Wauth need to be withdrawn from Active Directory. When enabled, users in Active Directory will be able to log in to Wauth.

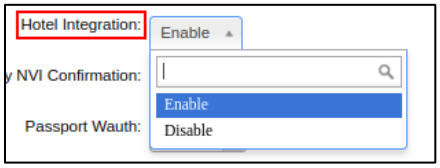


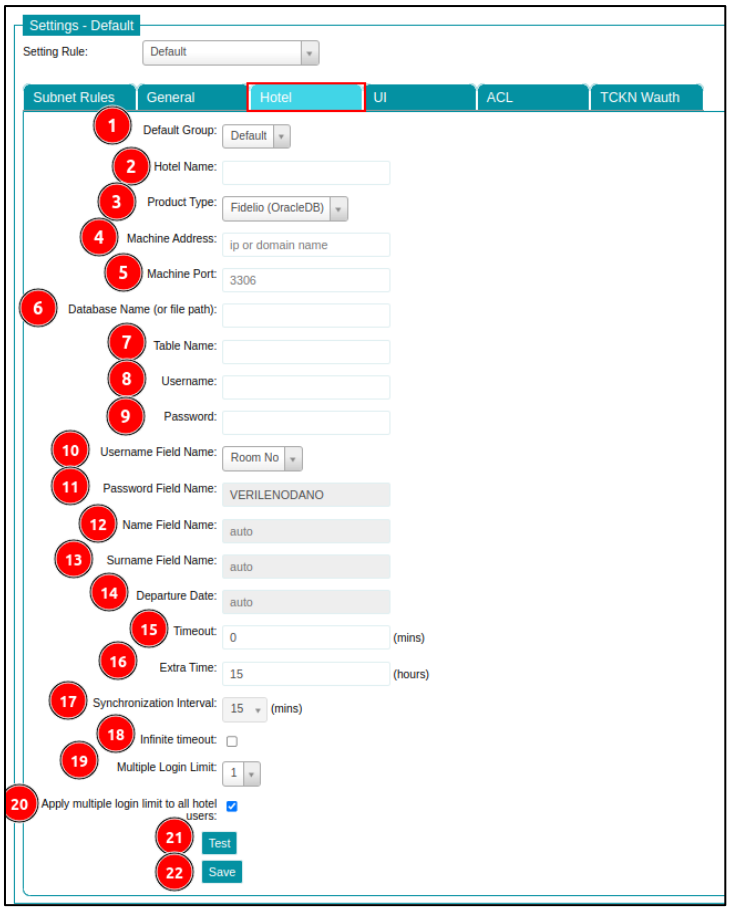


1	**Multiple Login Limit**	This is the section where the number of multiple logins of users in Active Directory to WAUTH is regulated.
2	**Apply multiple login limit to all AD Users**	This is the section where multiple limit entries are enabled for users in the Active Directory.
3	**Disable Group Name**	This is the section where the group names in the Active Directory are disabled.
4	**Infinite Timeout**	This is the section where the timeout period for users in the Active Directory is disabled.

5	**Timeout**	The AD timeout period is specified.
6	**Infinite Expr. Time**	This is the section where the infinite expiration time of user accounts is activated.
7	**AD Expire After**	It is the section on AD where the expiration time is indicated.
8	**Test**	This is the button where users in the Active Directory are tested.
9	**Save**	This is the button where the Active Directory Authorize settings are saved.

-If enabled, Hotel Integration provides the ability to log in to Wauth using data held in the database.



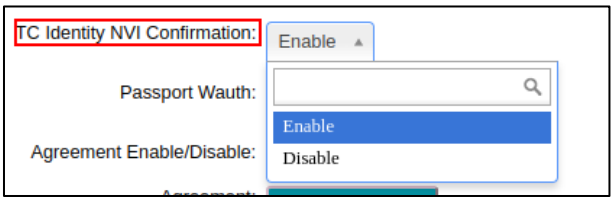


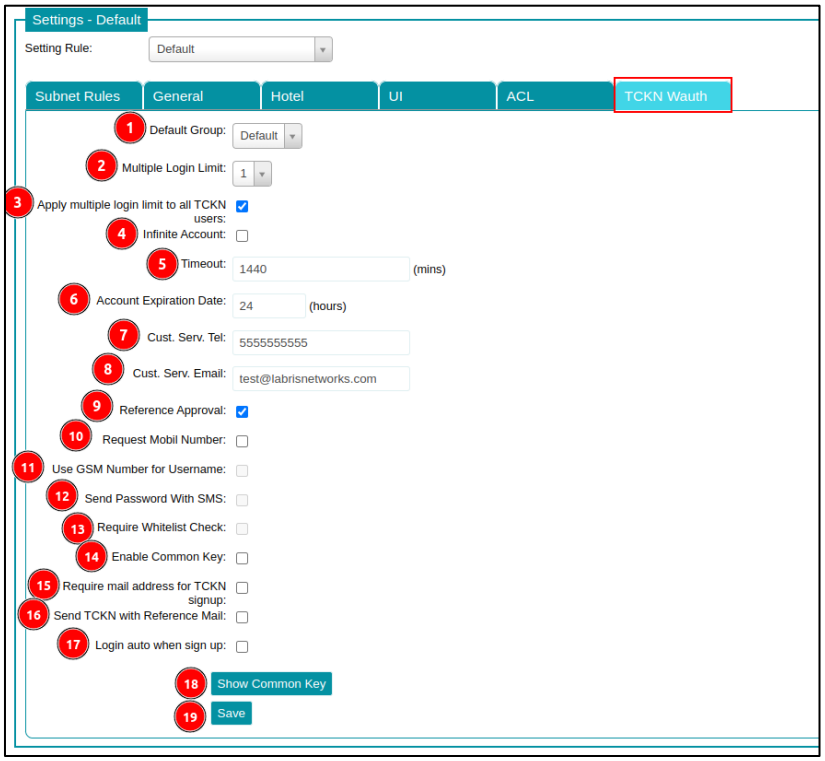
1	**Default Group**	The group for which the hotel integration is enabled is selected.
2	**Hotel Name**	This is the section where the hotel name is entered.
3	**Product Type**	The type of database is selected. Database types supported in the Labris UTM device are Fidelio (OracleDB), Synthesis (MsSQL), Amonra (XML), Rmos (XML), Akinsoft_Wolvox (Firebird), and Asyasoft. Apart from the supported database types, data is taken from the database as custom.

4	**Machine Address**	This is the section where the address of the database server is entered.
5	**Machine Port**	This is the section where the port of the database server is entered.
6	**Database Name (or file path)**	This is the section where the name of the database server is entered.
7	**Table Name**	This is the section where the table name of the database is entered.
8	**Username**	This is the section where the user name used to log in to the database is entered.
9	**Password**	This is the section where the password used to log in to the database is entered.
10	**Username Field**	This is the section where the domain name of the user who logs in to Wauth is selected.
11	**Password Field**	It is automatically pulled from the database.
12	**Name Field Name**	It is automatically pulled from the database.
13	**Surname Field Name**	It is automatically pulled from the database.
14	**Departure Date**	It is automatically pulled from the database.
15	**Timeout**	This is the section where the user's timeout after logging in is indicated.
16	**Extra Time**	This is the section where the extra permission period given to users after logging in is specified.
17	**Synchronization Interval**	This is the section where the time when the new data added to the database is transferred to the Labris

		UTM device is specified.
18	**Multiple Timeout**	It is used in cases where the timeout should be unlimited.
19	**Multiple Login Limit**	This is the section where the number of times users will be connected from the same account is specified.
20	**Apply multiple login limit to all hotel users**	A multi-connection limit is turned on for all users.
21	**Test**	It is the button where database integration is tested.
22	**Save**	This is the button where hotel integration settings are saved.

-It opens in cases where it is necessary to log in with the TC Identity Number. When users register with their TC ID, NVI matches the user's TC ID number with their date of birth. In cases of matching, the user logs in to WAUTH with his TC Identity Number and year of birth.



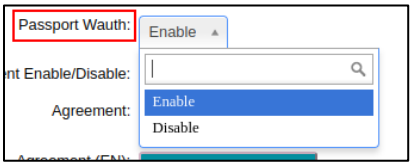


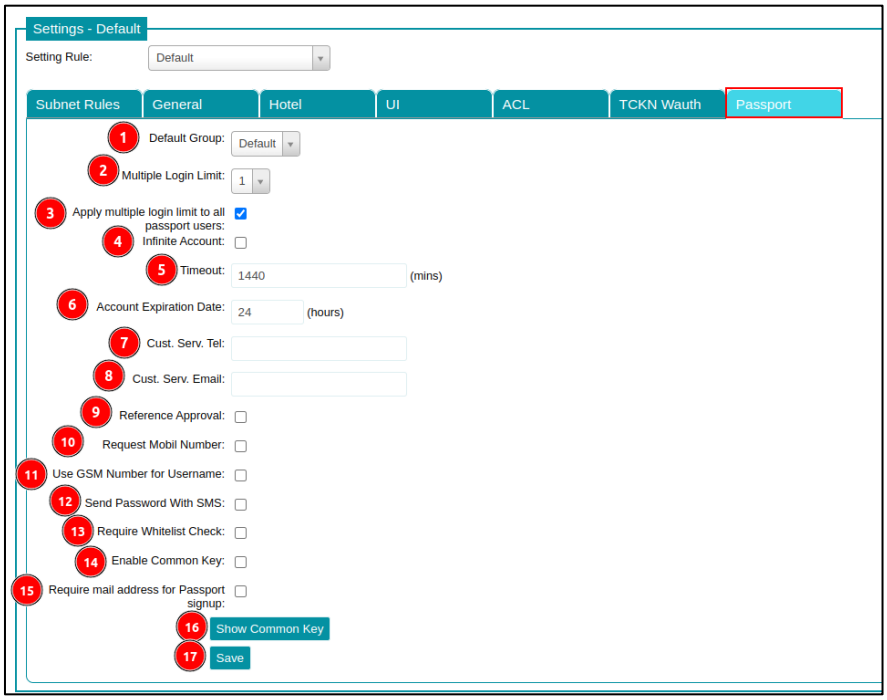
1	**Default Group**	The default group of TCKN Wauth is selected.
2	**Multiple Login Limit**	The multiple connection limit of the users who will log in to Wauth is specified.
3	**Apply multiple login limit to all TCKN users**	It is the section used to apply the multi-connection limit to all TCKN users.
4	**Infinite Account**	It is marked in cases where the expiration period should be unlimited.

5	**Timeout**	This is the part where the timeout period is specified in minutes.
6	**Account expiration date**	It is the section where the expiration time of the accounts opened by the users is specified in hours.
7	**Cust. Serv. Phone**	This is the section where the Technical Support Phone is entered.
8	**Cust. Serv. Email**	This is the section where the Technical Support e-mail address is entered.
9	**Reference Approval**	It is opened in cases where users who register with TCKN need to be logged in after reference approval.
10	**Request Mobile Number**	It is activated in cases where users need to request a GSM number when registering.
11	**Use GSM Number for Username**	It is activated in cases where users want to set their usernames as phone numbers after logging in.
12	**Send Password with SMS**	When enabled, users' login information will be sent via SMS.
13	**Require Whitelist Check**	Users who are on the allowed list of their GSM number are allowed to enter WAUTH.
14	**Enable Common Key**	This is the section where the public key specified by the administration for entry to WAUTH is specified.
15	**Require Mail Address for TCKN signup**	It is activated in cases where the postal address must be entered by logging in with the TCKN.
16	**Send TCKN with reference mail**	Sends the TCKN by reference mail.
17	**Login auto when sign up**	After registration, they are automatically logged in to WAUTH.

18	**Show common key**	Indicates the specified public key.
19	**Save**	TCKN is the button where the settings made in WAUTH are saved.

-In cases where users need to use a passport when registering with Wauth, Passport Wauth is activated. Once activated, users use their passport number when registering on Wauth.





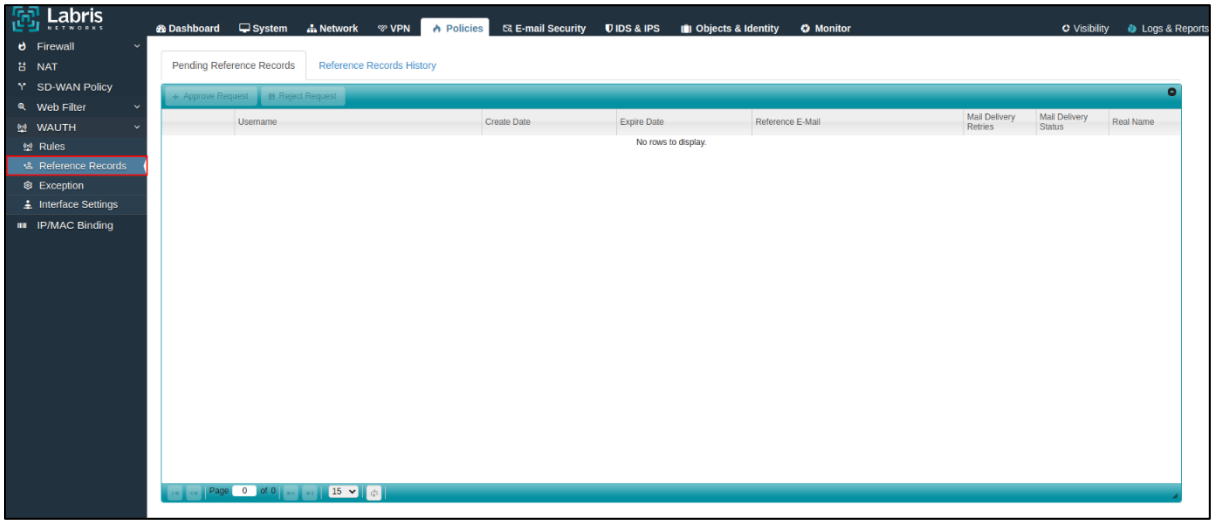
1	**Default Group**	The default group of Passport Wauth is selected.
2	**Multiple Login Limit**	The multiple connection limit of the users who will log in to Wauth is specified.
3	**Apply multiple login limit to all Passport users**	It is the place used to apply the multi-connection limit to all Passport users.

4	**Infinite Account**	It is marked in cases where the expiration period should be unlimited.
5	**Timeout**	This is the part where the timeout period is specified in minutes.
6	**Account expiration date**	It is the section where the expiration time of the accounts opened by the users is specified in hours.
7	**Cust. Serv. Phone**	This is the section where the Technical Support Phone is entered.
8	**Cust. Serv. Email**	This is the section where the Technical Support e-mail address is entered.
9	**Reference Approval**	It is opened in cases where users who register with TCKN need to be logged in after reference approval.
10	**Request Mobile Number**	It is activated in cases where users need to request a GSM number when registering.
11	**Use GSM Number for Username**	It is activated in cases where users want to set their usernames as phone numbers after logging in.
12	**Send Password with SMS**	When enabled, users' login information will be sent via SMS.
13	**Require Whitelist Check**	Users who are on the allowed list of their GSM number are allowed to enter WAUTH.
14	**Enable Common Key**	This is the section where the public key specified by the administration for entry to WAUTH is specified.
15	**Require Mail Address for Passport signup**	It is activated in cases where users login with their e-mail address.
16	**Show common key**	Indicates the specified public key.

17	**Save**	Passport is the button where the settings made in WAUTH are saved.

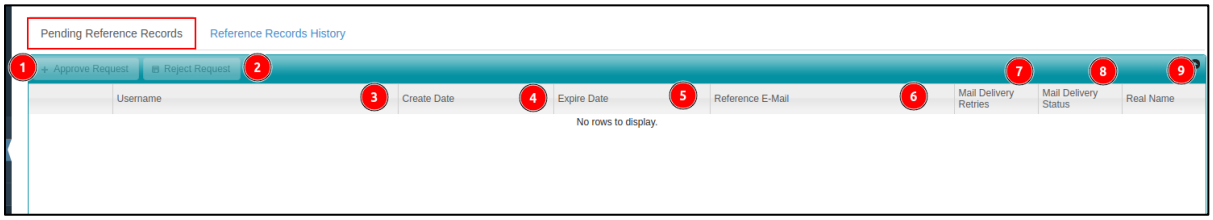
13.5.2 Reference Records

It is used when Reference Approval is enabled in Wauth rules. The account of the users who have been given reference approval is approved and the users log in to WAUTH with the account they registered.



13.5.2.1 Pending Reference Records

Shows a list of reference records that are awaiting reference approval when users log in to WAUTH.

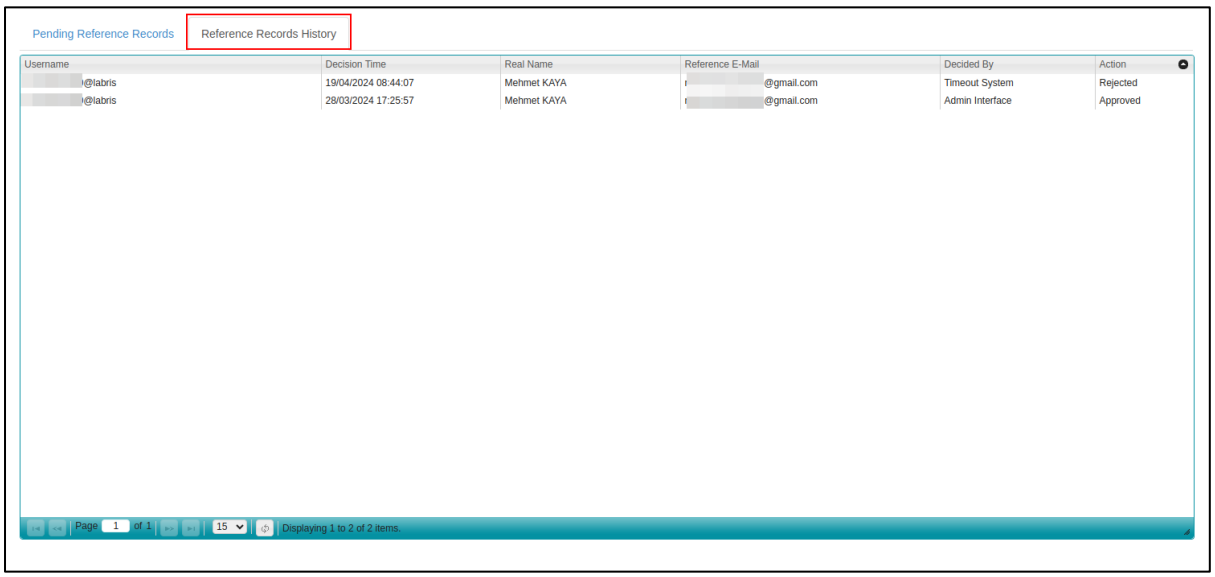


1	**Approve Request**	It is the button where the WAUTH request of the users who have registered with WAUTH is approved.
2	**Reject Request**	It is the button where the WAUTH request of users who have registered with WAUTH is rejected.
3	**Username**	This is the section where the User Name of the user logged in to WAUTH is displayed.
4	**Create Date**	This is the section where the creation date of the WAUTH account is displayed.

5	**Expire Date**	The experation period of the reference request is displayed.
6	**Reference E-mail**	This is the section where the reference e-mail address is displayed.
7	**Mail Delivery Retries**	This is the section that shows the number of attempts to send an e-mail
8	**Mail Delivery Status**	This is the section where the mail delivery status is displayed.
9	**Real Name**	It is opened in cases where users who register with a passport need to be logged in after reference approval.

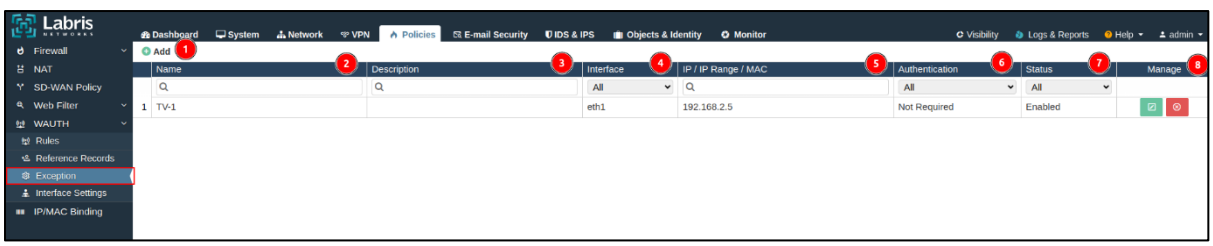
13.5.2.2 Reference Records History

A list of reference records made in the past is displayed.



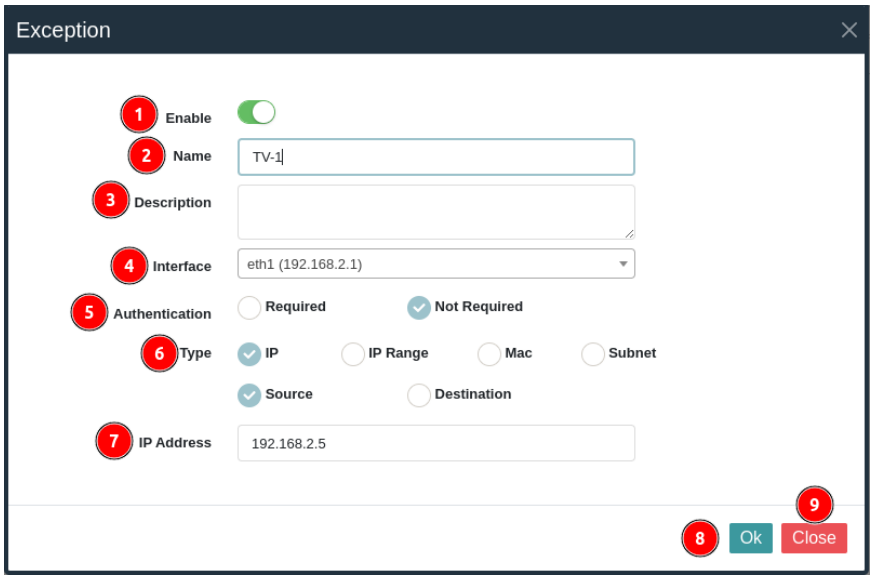
13.5.3 Exception

It allows IP addresses added as an exception to access the internet without asking WAUTH. Exceptions are typically used for devices that can't log in to WAUTH.



1	**Add**	It is the button where the IP, IP Range, and MAC Addresses to be added as an exception are added.
2	**Name**	It is the section where the name of the device added as an exception is displayed.
3	**Description**	This is the section where the description about the device added as an exception is displayed.
4	**Interface**	It is the section where the interface of the device added as an exception is displayed.
5	**IP/IP Range/ MAC**	It is the section where the IP, IP Range, or MAC address of the added device is displayed.
6	**Authentication**	The authentication method with WAUTH is displayed for the onboarded device.
7	**Status**	It is displayed whether the typed exception works or not. If the status is enabled, the added exception will work. If the status is disabled, the added exception will not work.
8	**Manage**	This is the section where the added exception is edited or deleted.

-To add an exception, click the 'add' button, and the exception IP, IP Range, and MAC Address are added to the exception rule.

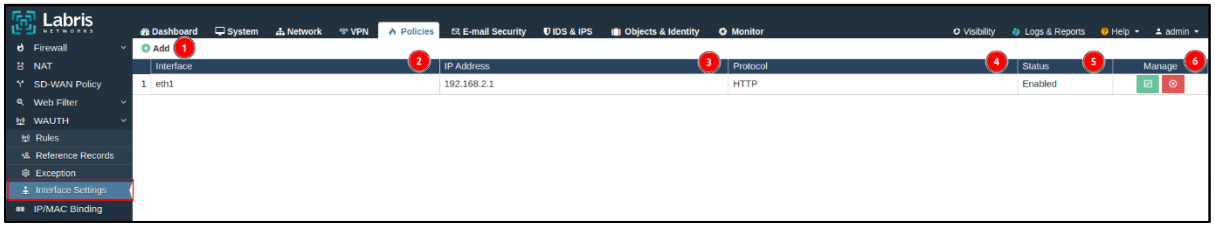


1	**Enable**	It is the button where the exception rule to be added is activated.
2	**Name**	It is the section where the name of the device to be added as an exception is entered.
3	**Description**	It is the section where the description about the device to be added as an exception is entered.
4	**Interface**	This is the section where the interface to which the device to be added will be connected is selected. (WAUTH must be turned on on the selected interface.)
5	**Authentication**	This is the section where the authentication method of the device to be added is selected. If the required option is selected, it is necessary to log in to WAUTH. If Not Required is selected, the added device does not need to log in to WAUTH.
6	**Type**	This section specifies the type of exception rule. If IP is selected, only 1 IP address is allowed (ex. 192.168.1.25). If IP Range is selected, a specific IP range is entered (ex. 192.168.30.1-192.168.30.20). If MAC is selected, the exception rule is written according to the MAC address of the device (ex.

		FF:FF:FF:FF:FF:AB). If SUBNET is selected, an exception is added according to the specified subnet (ex. 192.168.1.0/24). If the source is selected, IP, IP Range, and Subnet values are entered according to the source. If Target is selected, IP, IP Range, and Subnet values are entered according to the target address.
7	**Network Address**	The network addresses to be entered vary according to the selected type.
8	**Save**	It is the button where the written exception rule is saved.
9	**Close**	It is the button where the screen that opens after clicking the Add button is closed. Closes the transactions made without being saved.

13.5.4 Interface Settings

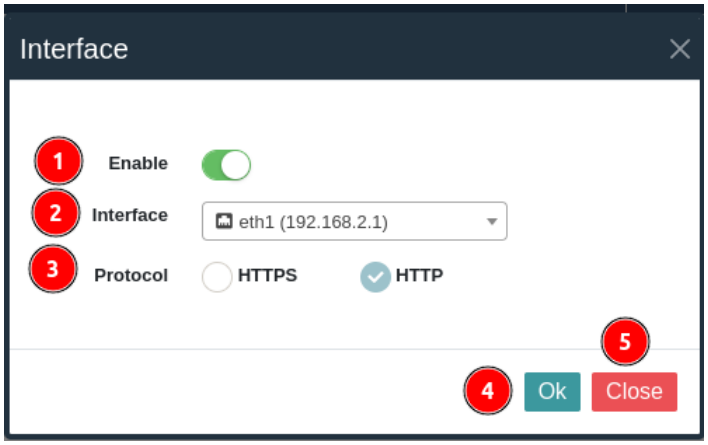
Wauth validation is the module in which the interface to be opened is selected or the interfaces selected for WAUTH are displayed.



1	**Add**	This is the button where the interface to enable Wauth verification is added.
2	**Interface**	This is the section where the interface in which Wauth validation is turned on is displayed.
3	**IP Address**	This is the section where the IP address from which the WAUTH interface will be accessed is displayed.
4	**Protocol**	The protocol in which WAUTH runs is displayed. (HTTP or HTTPS)

5	**Status**	The status of the interface selected as WAUTH is displayed. If it is enabled, WAUTH is turned on on the selected interface. If it is disabled, WAUTH is closed on the selected interface.
6	**Manage**	These are the buttons where the interfaces added to perform WAUTH verification are edited or deleted.

-To select the interface that Wauth will work with, click the 'add' button and select the interface on the screen that appears. The interface to be selected must be the internal network.



1	**Enable**	This is the button where WAUTH is activated.
2	**Interface**	The interface on which WAUTH runs is selected.
3	**Protocol**	The protocol on which WAUTH runs is selected. (HTTP or HTTPS).
4	**Save**	This is the button where the written configurations are saved.
5	**Close**	The screen that opens is closed.

13.6 IP/MAC Binding

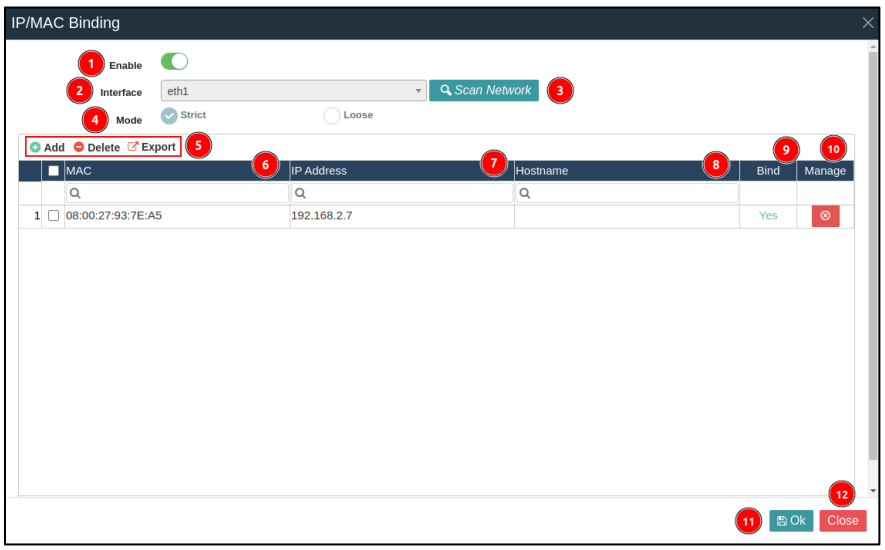
IP MAC Mapping is the process of matching the MAC address with the IP address of the device on a network. Devices on the network are assigned a MAC address that is unique to the device's hardware.

Strict Mode requires IP-MAC bindings of network devices. An IP address is associated with a specific MAC address, and packets with a different MAC address are rejected. It rejects incoming packets when a new network device joins the network, other than the network devices for which IP-MAC binding is made. For the packets to be accepted, the IP-MAC binding must be done on the new device. Strict Mode provides tighter control over network security.

Loose Mode, the IP-MAC binding of network devices is more flexible. Allows packets from a different MAC address that has just joined the network, except for IP-MAC binded devices.

1	**Add**	This is the button where the IP-MAC Binding policy is added.
2	**Interface**	This is the section where the interface where IP-MAC Binding is opened is displayed.
3	**Mode**	This is the section where the mode of IP-MAC Binding is displayed. (Strict or Loose)
4	**Manage**	This is the section where the added IP-MAC Binding is edited or deleted.

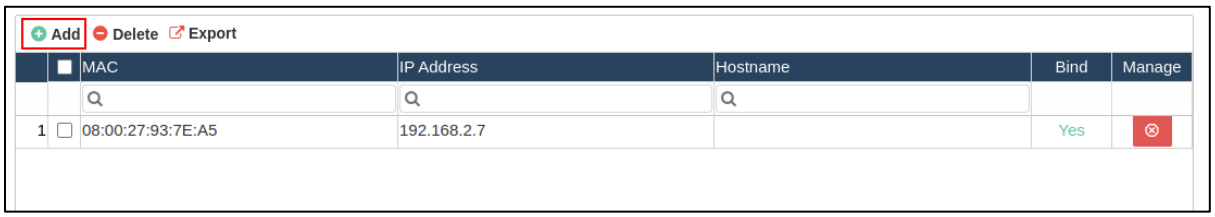
-IP-MAC Binding is done by clicking the 'add' button.



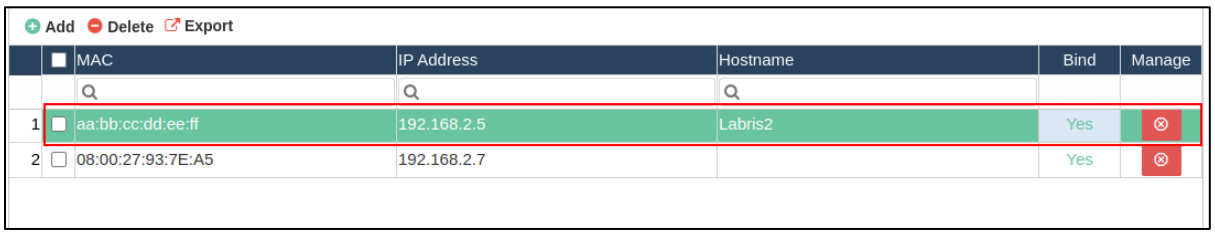
1	**Enable**	This is the button where the IP-MAC binding policy is enabled.
2	**Interface**	It is the button that displays the interface where IP-MAC binding will be opened.
3	**Network Scan**	It is the button that displays the MAC and IP addresses of the network devices connected to the selected interface.
4	**Mode**	The mode of the IP-MAC binding is selected.
5	**Add-Delete-Export**	When the Add button is pressed, the MAC and IP addresses of the device belonging to the selected interface are added. The Delete button deletes the selected IP-MAC bind. The Export button exports the added IP-MAC binding table.
6	**MAC**	After pressing the Scan Network button, the MAC addresses of the devices that have been IP-MAC matched are displayed.
7	**IP Address**	After pressing the Scan Network button, the IP addresses of the devices that have been matched with IP-MAC are displayed.

8	**Server Name**	The server names of the devices on the network are displayed.
9	**Bind**	The pairing status of the IP-MAC bindings of the devices is displayed. To make a binding, the bind status must be yes.
10	**Manage**	This is the section where the IP-MAC bind is deleted.
11	**Save**	This is the button where the IP-MAC bind policy is saved.
12	**Close**	It is the button where the IP-MAC binding screen is turned off.

-Click the 'add' button to make IP-MAC binding of the devices.



-After pressing the Add button, a new line is added. By filling in the boxes corresponding to the added line, the IP address of the newly added device is added together with its MAC address.



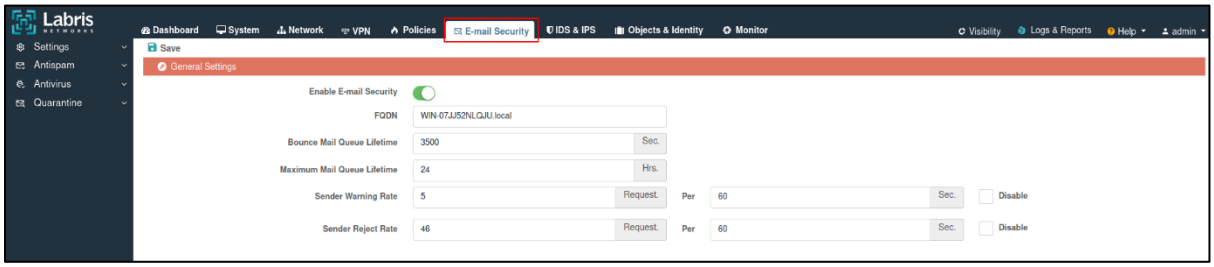
Note

If strict mode is selected, the packets of devices that do not have IP-MAC matching will be dropped.

14. E-mail Security

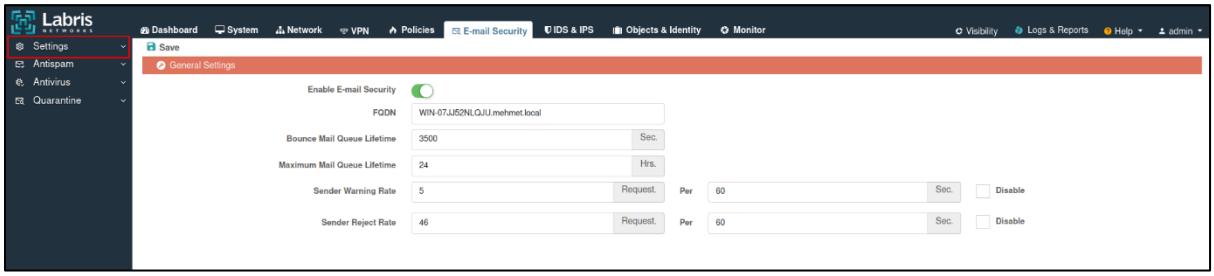
It is used by the Labris UTM device to protect email traffic. It monitors, filters, and controls email traffic, thus preventing malware, spam, and other threats from reaching the network.

It filters incoming and outgoing email messages, helping to prevent various threats such as spam, phishing, malware, and data leakage.



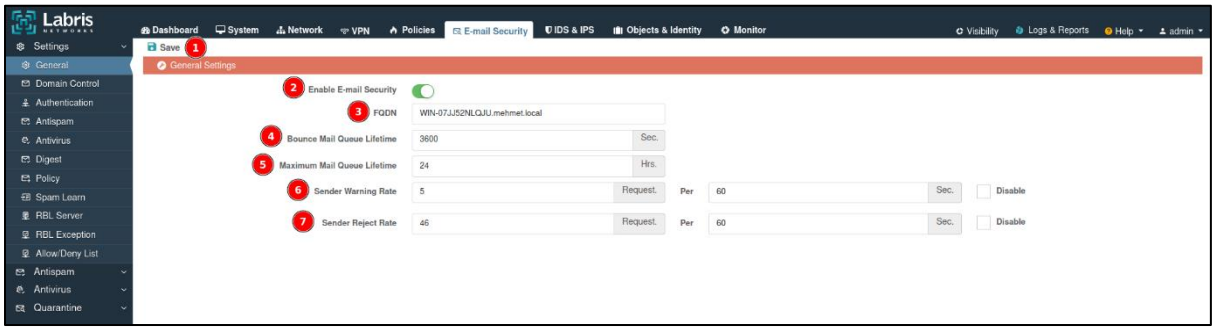
14.1 Settings

It is the section where the information of the e-mail server running in the internal network is edited, spam, domain control, authentication, antispam, antivirus, e-mail blocking, RBL server settings are made.



14.1.1 General

It is the module where the general settings of e-mail security in the Labris UTM device are made.



1	**Save**	It is the button where the settings of e-mail security are saved.

2	**Enable E-mail Security**	It is the button where e-mail security is enabled.
3	**Fully Qualified Domain Name(FQDN)**	This is the section where the full domain name of the mail server is entered. EG; 'mail.google.com'
4	**Bounce Mail Queue Lifetime**	Determines how long bounce messages are kept in the queue. In the event that a bounced message cannot be delivered within the specified time, the message is considered undeliverable and is deleted from the queue. It allows bounced messages to be kept in the queue for the specified amount of time.
5	**Maximum Mail Queue Lifetime**	Determines how long a message can be held after it is queued. Messages that are not delivered at the end of the specified time are sent back.
6	**Sender Warning Rate**	It allows senders to send 5 e-mails within the specified time and sends a warning message to the sender when the limit is exceeded.
7	**Sender Reject Rate**	It allows senders to send 5 e-mails within the specified time, and e-mails exceeding the limit are rejected.

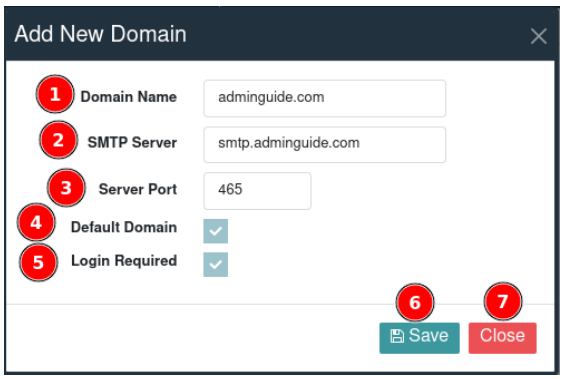
14.1.2 Domain Control

It is the module where the domain names of the mails coming to the mail server are checked.

1	**Add**	It is the button where the domain name control is added.
2	**Save**	This is the partition where the added domain control server is registered.

3	**Discard**	It is the button where the transactions are abandoned.
4	**Domain Name**	This is the section where the domain name of the added domain control server is displayed.
5	**SMTP Server**	This is the section where the SMTP server information is displayed.
6	**Port**	This is the section where the port information of the SMTP server is displayed.
7	**Login Required**	It is used to prevent unauthorized logins from accessing email accounts.
8	**Manage**	There are buttons where the added server is edited and deleted.

-Click the 'add' button to add a domain name control server. After clicking the 'Add' button, the information in the window that appears is filled in and the process of adding a domain name control server is done.

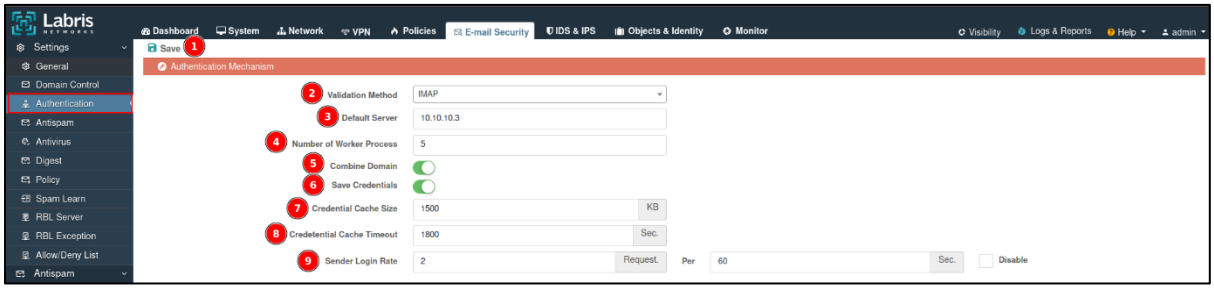


1	**Domain Name**	This is the section where the domain name of the server is entered.
2	**SMTP Server**	This is the section where the domain name of the STMP server is entered.
3	**Server Port**	This is the section where the port information of the server is entered.

4	**Default Domain**	Opens when the added server should be the default domain.
5	**Login Required**	Opens when a login is required for the Domain Name check.
6	**Save**	This is the button where the domain name check is saved.
7	**Close**	It is the button where the window opened by clicking the 'Add' button is closed.

14.1.3 Authentication

This is the section where the mail coming to the Mail server is authenticated. The authentication process verifies the credentials of the users who send the mail.

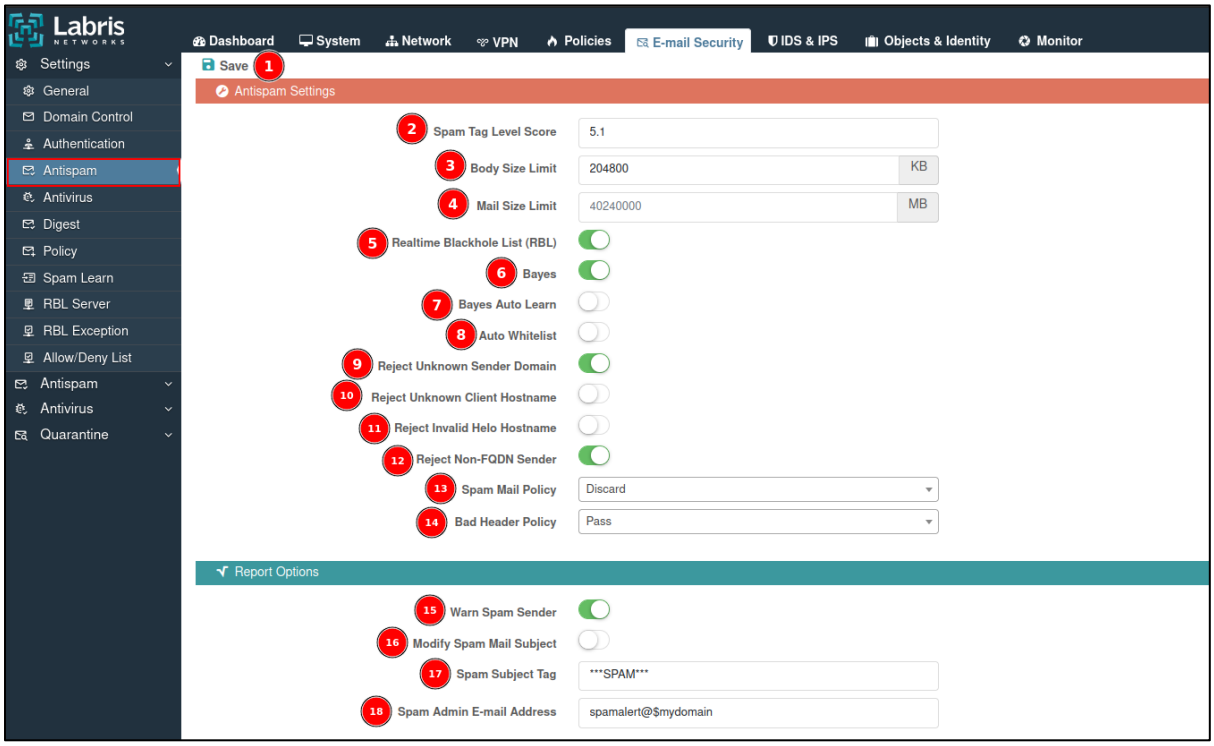


1	**Save**	This is the button where the authentication settings are saved.
2	**Validation Method**	This is the section where the protocol information to which the verification method will be made is selected. POP3 and IMAP protocols are used as authentication methods.
3	**Default Server**	This is the section where the IP address of the server where clients will make authentication requests is specified.
4	**Number of Worker Process**	It is the section where it is specified how many operations can be performed at the same time during the authentication process.
5	**Combine Domain**	It merges the field with the login before entering the

		authentication mechanism.
6	**Save Credentials**	This is the section where the credentials of the clients that are authenticated are saved.
7	**Credential Cache Size**	This is the section where the maximum amount of memory for each process is specified.
8	**Credetential Cache Timeout**	This is the section where it is specified how long the temporary files will be valid for each authentication process.
9	**Sender Login Rate**	It allows senders to send 2 requests within the specified time (60 seconds) and sends a warning message to the sender when the limit is exceeded.

14.1.4 Antispam

It is the section where the necessary settings are made for the e-mails coming to the mail server to be detected as antispam.



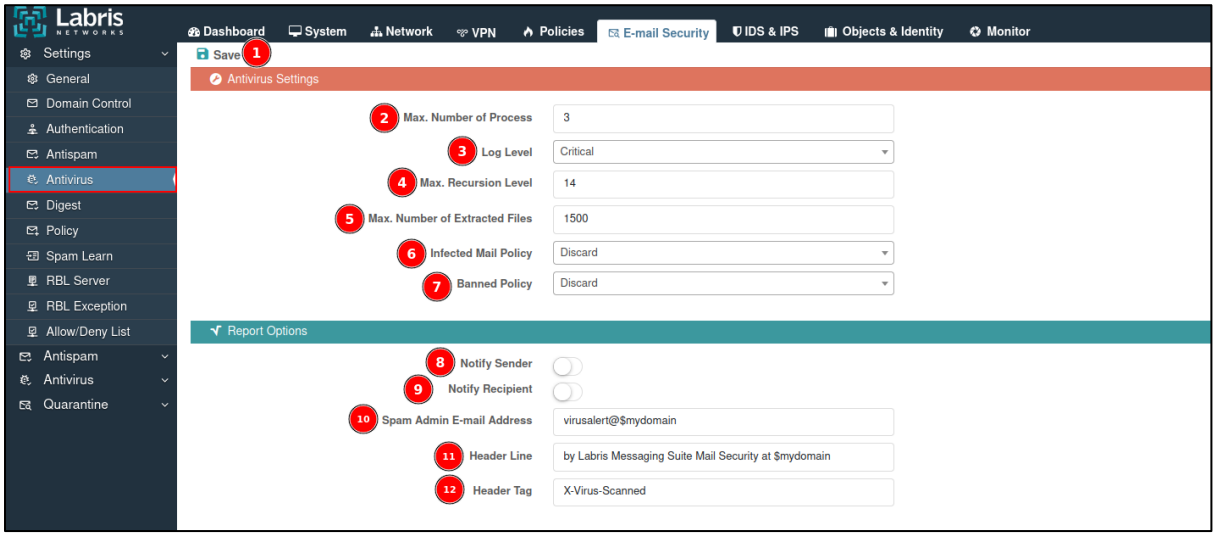
1	**Save**	This is the button where the antispam settings are saved.

2	**Spam Tag Level Score**	Specifies the default score threshold required for an Email to be classified as spam. If an email's spam score crosses this threshold, the email is considered spam. When '5.1' is set, emails are considered spam because they have a score of 5.1 or higher.
3	**Body Size Limit**	Specifies the maximum size of the email body to be processed for spam analysis. If the body of an email exceeds this size limit, it doesn't analyze the entire content and skips portions.
4	**Mail Size Limit**	If the size of the incoming e-mail exceeds the limit, it detects the incoming e-mail as spam and blocks it.
5	**Realtime Blackhole List (RBL)**	It is the section where it is activated in cases where blocking is desired by looking at the black hole list for spam e-mail control.
6	**Bayes**	It must be enabled to detect and filter unsolicited e-mails (spam). If enabled, it analyzes the e-mail message content and distinguishes between spam and requested e-mails.
7	**Bayes Auto Learn**	In the case of Bayesian automatic learning turned on, it continuously improves spam filtering by learning based on the emails that the user has flagged.
8	**Auto Whitelist**	It prevents messages from trusted email addresses from being accidentally blocked by the spam filter, allowing users to perceive important messages as spam.
9	**Reject Unknown Sender Domain**	Blocks the sender's mail in case the domain name of the incoming mail is not resolved or unknown.
10	**Reject Unknown Client Hostname**	Blocks incoming mail from the sender if the server name of the incoming mail is not resolved or unknown.
11	**Reject Invalid Helo Hostname**	While the e-mail server identifies itself with the Helo command, it blocks incoming e-mail if an invalid server

		name is not used.
12	**Reject Non-FQDN Sender**	Blocks incoming email when the sender domain of the email server is not a fully qualified domain name.
13	**Spam Mail Policy**	The action taken during the blocking of e-mails perceived as antispam is indicated. The specified actions are Block (Warn Sender), R, Block (Report to Sender) or Block.
14	**Bad Header Policy**	By checking the header of the incoming email, it blocks, rejects or does not block the email it perceives as spam.
15	**Warn Spam Sender**	Alerting the sender of the mail detected as spam is done.
16	**Spam Admin E-mail Address**	The subject of the mail that is detected as spam is changed.
17	**Spam Admin E-mail Address**	It is the section where the label of the subject of the mail that is detected as spam is changed.
18	**Spam Admin E-mail Address**	It is the section where the address to which the e-mails detected as spam will be sent is entered.

14.1.5 Antivirus

It is the section where the necessary settings are made for the e-mails coming to the mail server to be detected as viruses. It warns the sender and receiver in cases where incoming e-mails are detected as viruses.

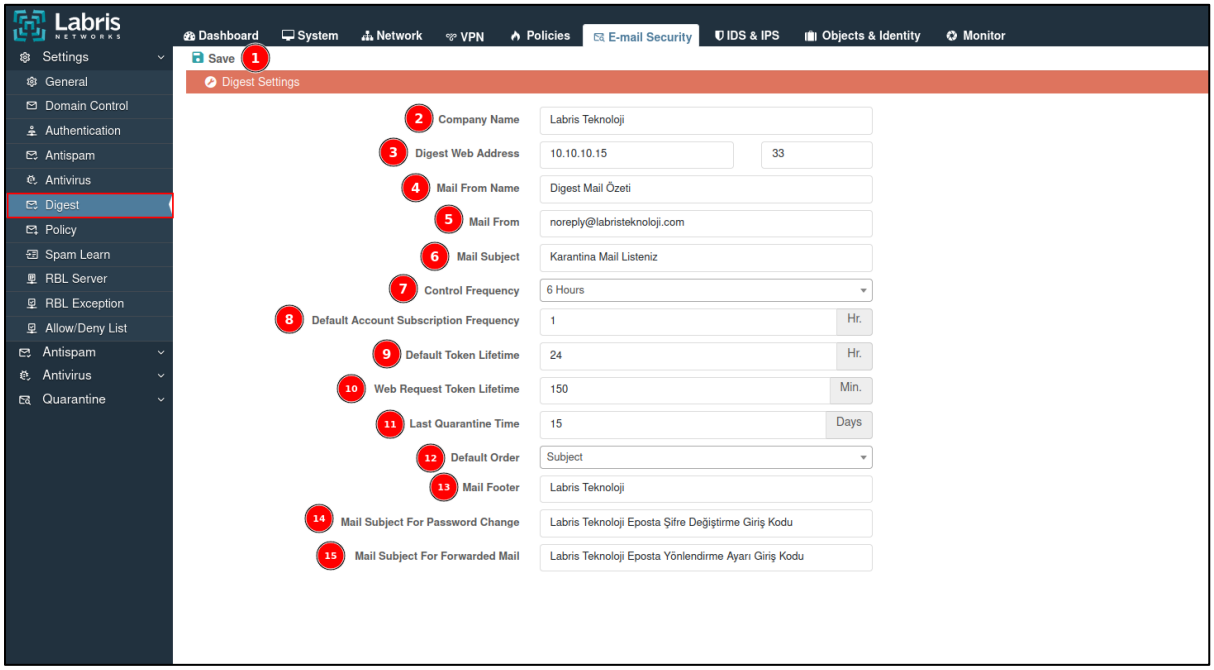


1	**Save**	This is the section where the antivirus settings are saved.
2	**Max. Number of Process**	This is the section where the number of operations of the antivirus scan is indicated.
3	**Log Level**	The registration level of the e-mails detected as viruses is selected.
4	**Max. Recursion Level**	This is the section where it is specified how deep to go in case of scanning files or archives. A depth level of 1-20 is entered.
5	**Max. Number of Extracted Files**	This is the section where it is specified how many files will be scanned when scanning or decompressing compressed files or archives in the incoming e-mail.
6	**Infected Mail Policy**	The policy to be applied in case it is detected as a virus is selected.
7	**Banned Policy**	This is the section where the policy to be applied for

		emails caught in the prohibited policy is selected.
8	**Notify Sender**	It is the section where e-mails are sent to the sender for e-mails detected as viruses.
9	**Notify Recipient**	It is the section where e-mails are sent to the recipient for e-mails detected as viruses.
10	**Spam Admin E-mail Address**	This is the section where the address to which the spam will be sent is entered.
11	**Header Line**	This is the section where the title information of the mail to be sent is entered.
12	**Header Tag**	This is the section where the title tag information of the mail to be sent is entered.

14.1.6 Digest

. It is the section where the summary of quarantined e-mails is sent in the Labris UTM device.



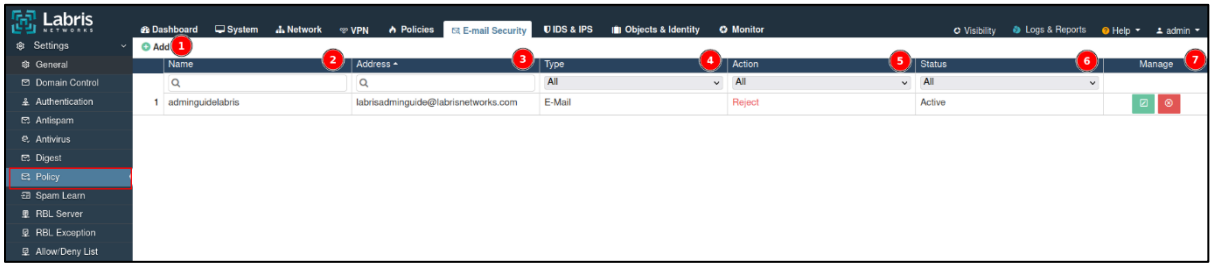
1	**Save**	This is the section where the quarantine summary

		settings are saved.
2	**Company Name**	This is the section where the name of the company to which the quarantine summary e-mail will be sent is entered.
3	**Digest Web Address**	This is the section where the network address of the quarantine private server is entered.
4	**Mail From Name**	Quarantine is the section where the sender address of the mail sent as a summary is entered.
5	**Mail From**	Quarantine is the section where the mailing address sent as a summary is entered.
6	**Mail Subject**	Quarantine is the section where the subject of the mail to be sent is entered.
7	**Control Frequency**	This is the section where it is specified how often a summary report will be sent to the user about quarantined emails.
8	**Default Account Subscription Frequency**	An initial setting that determines how often a user receives email notifications or reports when they sign up for a particular service or system.
9	**Default Token Lifetime**	This is the section where it is specified how long the session used during viewing, retrieving or managing the Quarantine Summary report will remain active.
10	**Web Request Token Lifetime**	This is the section where the duration of the session used during the creation or receipt of the Quarantine Summary report will remain active.
11	**Last Quarantine Time**	Quarantine refers to the time of the last email or message quarantined in the Summary report.
12	**Default Order**	Quarantine is the section where the standard format of the summary report is specified when it is created or

		sent to the user.
13	**Mail Footer**	Quarantine is the section where the postal signature of the report to be sent as a summary is entered.
14	**Mail Subject For Password Change**	This is the section where the information required for password change is entered.
15	**Mail Subject For Forwarded Mail**	This is the section where the mail subject is entered for the forwarded E-mail.

14.1.7 Policy

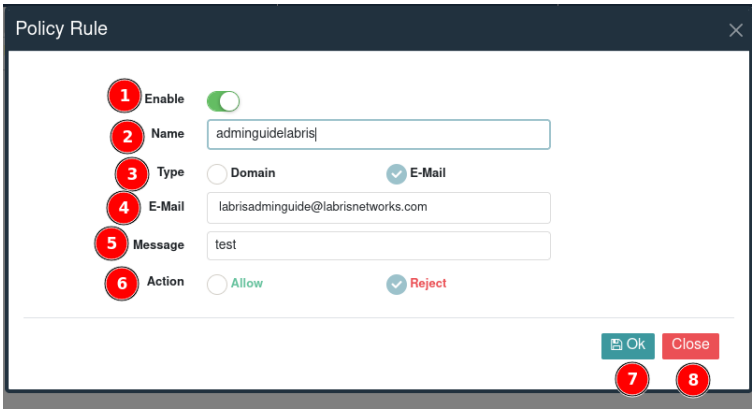
The rules defined in the Labris UTM device are displayed, this is the section where the block or permission is made by typing the rule in the domain name or e-mail address.



1	**Add**	This is the button where the policy is added.
2	**Name**	This is the section where the written policy names are displayed.
3	**Address**	This is the section where the typed policy addresses are displayed.
4	**Type**	This is the section where the type of policies written is displayed. The type includes Domain Name and Email.
5	**Action**	This is the section where the action information of the written policy is displayed. Allows or blocks as an action.
6	**Status**	The status information of the written policy is displayed.

7	**Manage**	This is the section where the written rule is deleted or edited.

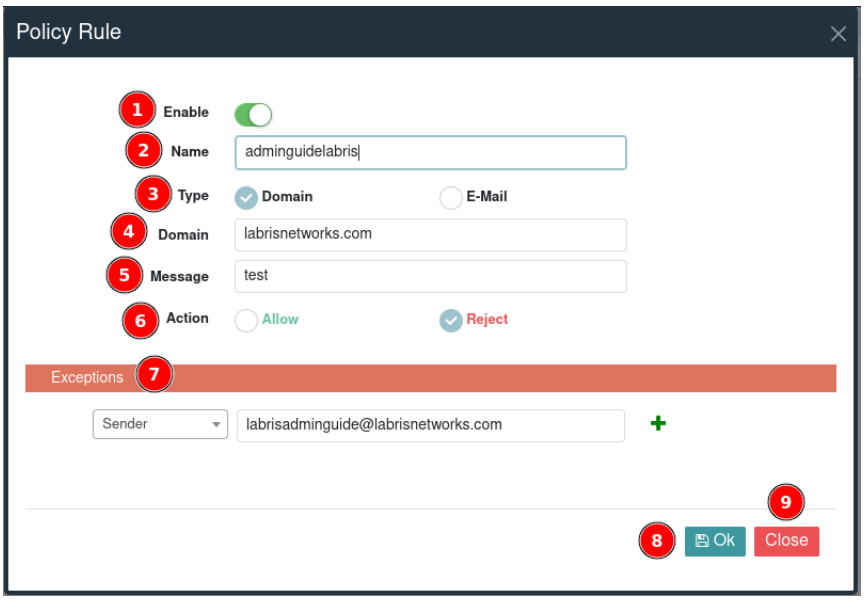
-Click on the 'add' button to add a policy. After clicking the Add button, if the type of policy to be written cannot be selected as 'e-mail', the rule to be blocked or allowed according to the e-mail address is written.



1	**Enable**	It is the button where the policy to be written is activated.
2	**Name**	This is the section where the name of the policy to be written is entered.
3	**Type**	The type of policy is selected and the policy is written according to the selected type.
4	**E-Mail**	If the type is selected as 'e-mail', the e-mail address to be blocked or allowed is written.
5	**Massage**	It is the section where the message information about the written rule is entered.
6	**Action**	The action of the policy to be written is selected. Allow mail to be received from the entered e-mail address is selected. If the mail will not be sent from the entered e-mail address, block is selected.
7	**Save**	This is the section where the written rule is saved.
8	**Close**	It is the button where the screen opened by clicking the

		Add button is closed.

-Click on the 'add' button to add a policy. After clicking the Add button, if the type of policy to be written cannot be selected as 'domain name', the rule to be blocked or allowed according to the e-mail address is written.

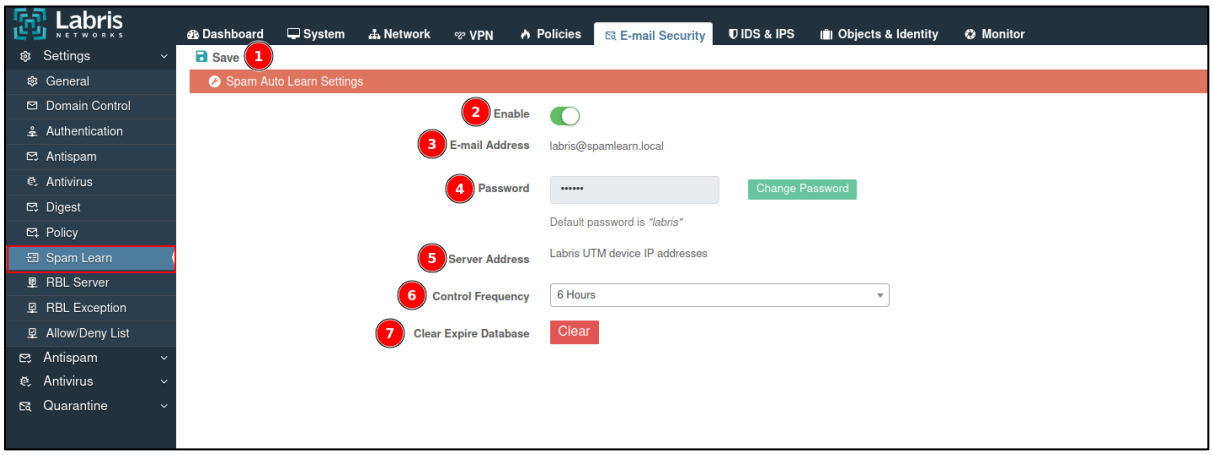


1	**Enable**	It is the button where the policy to be written is activated.
2	**Name**	This is the section where the name of the policy to be written is entered.
3	**Type**	The type of policy is selected and the policy is written according to the selected type.
4	**Domain Name**	If the type is selected 'Domain Name', the domain name address to be blocked or allowed is written.
5	**Massage**	It is the section where the message information about the written rule is entered.
6	**Action**	The action of the policy to be written is selected. Allow mail to arrive from the entered domain address is selected. If mail will not be received from the domain name address entered, block is selected.

7	**Exception**	In case of receiving mail from e-mail addresses belonging to the domain name, it is necessary to define it as an exception.
7	**Save**	It is the section where the written policy is recorded.
8	**Close**	It is the button where the screen opened by clicking the Add button is closed.

14.1.8 Spam Learn

This is the section where the necessary settings are made for spam learning in e-mail security.



1	**Save**	It is the button where spam learning is recorded.
2	**Enable**	It is the button where spam learning is enabled.
3	**E-mail Address**	This is the section where the e-mail address entered for spam learning is displayed.
4	**Password**	It is the section where the password defined for spam learning is changed.
5	**Server Address**	This is the section where the server address is displayed for spam learning.
6	**Control Frequency**	It is the section where the control frequency of the server is selected for spam learning.

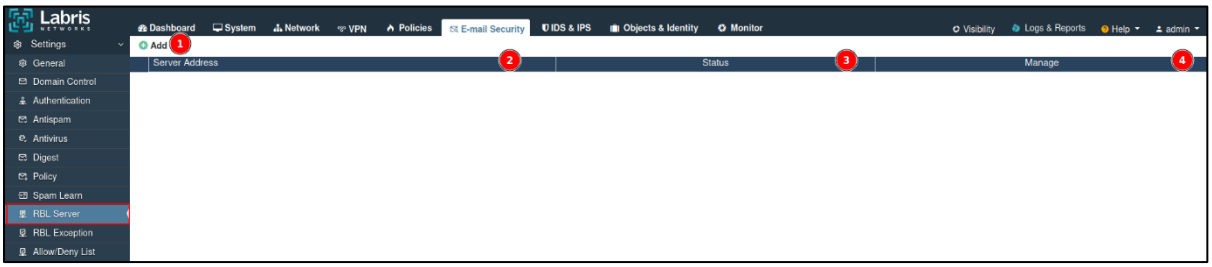
7	**Clear Expire Database**	It is the button where expired and spam e-mail addresses are cleared from the database.

14.1.9 RBL Server

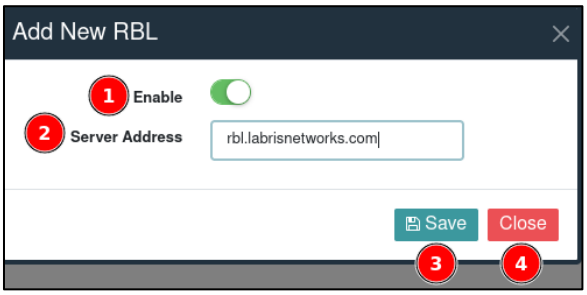
RBL Server is a blacklist server that email servers use to block spam and other unsolicited e-mail. It often hosts spammer IP addresses and domain names, and email servers use this list to verify the origin of incoming emails.

It is the database that e-mail servers instantly apply to detect and block spammers.

It is the section where RBL server definition is made in the Labris UTM device.



1	**Add**	RBL is the button where the server is added.
2	**Enable**	RBL is the section of the server where the server addresses are displayed.
3	**Status**	This is the section where the status of the added RBL server is displayed.
4	**Manage**	The added RBL is the partition where the edit or deletion of the server is performed.

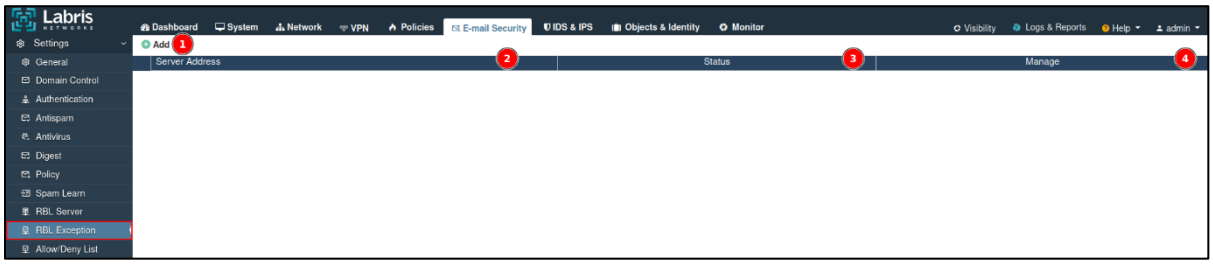


1	**Enable**	RBL is the button where the server is activated.

2	**Server Address**	RBL is the part of the server where the server address is entered.
3	**Save**	This is the section where the RBL server addresses to be added are saved.
4	**Close**	It is the button where the window that opens by clicking the Add button is closed without saving.

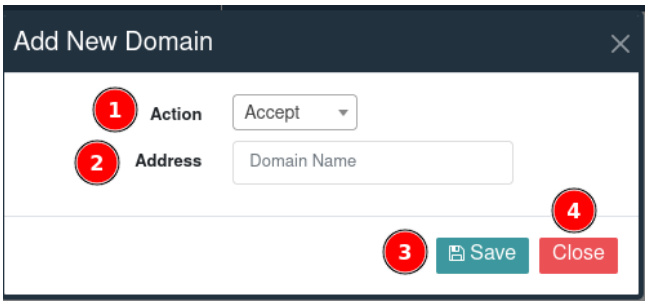
14.1.10 RBL Exception

RBL is used to receive mail from domain name addresses that are in the server's list.



1	**Add**	RBL Privileges is the button where the process is added.
2	**Server Address**	RBL is the section where the domain names of the servers added as privileges are displayed.
3	**Save**	This is the button where RBL Privileges are saved.
4	**Close**	It is the button where the window that opens by clicking the Add button is closed without saving.

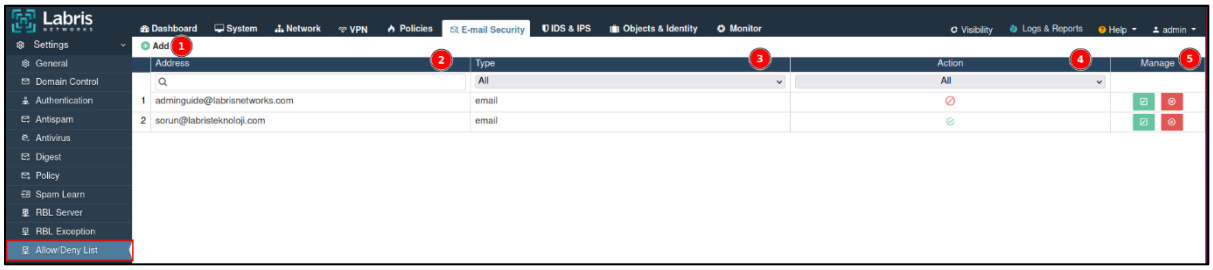
-To add a domain name as an RBL privilege, the addition process is done by clicking the 'add' button.



1	**Action**	This is the section in the RBL server list where the action to be taken for mail from the server address added as a privilege is specified.
2	**Address**	RBL is the section where the domain name added as a privilege is entered.
3	**Save**	This is the button where RBL Privileges are saved.
4	**Close**	It is the button where the window that opens by clicking the Add button is closed without saving.

14.1.11 Allow/Deny List

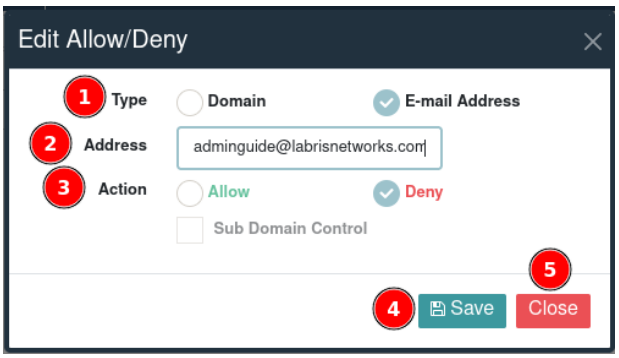
It is the module where mails from domain name and e-mail addresses are allowed or denied.



1	**Add**	It is the button where the allowed/denied domain name or e-mail addresses are added.
2	**Address**	This is the section where the added domain names or e-mail addresses are displayed.
3	**Type**	This is the section where the type of allowed/denied e-

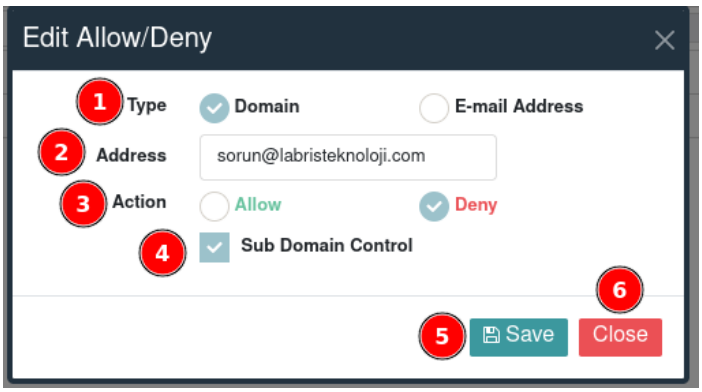
		mail addresses is displayed.
4	**Action**	This is the section where the actions of the added mail addresses are displayed.
5	**Manage**	This is the section where added mail addresses are edited or deleted.

-Click the 'add' button to add e-mail addresses to be allowed/blocked. After clicking the Add button, if the type of policy to be written is not selected as 'e-mail address', the rule to block or allow according to the e-mail address is written.



1	**Type**	The type of rule to be written is selected.
2	**Address**	If the type is selected as 'email address', the email address to be blocked or allowed is written.
3	**Action**	The action of the policy to be written is selected. Allow mail to be received from the entered e-mail address is selected. If the mail will not be sent from the entered e-mail address, block is selected.
4	**Save**	This is the button where the added rule is saved.
5	**Close**	It is the button where the window opened by clicking the Add button is closed.

-Click the 'add' button to add e-mail addresses to be allowed/blocked. After clicking the Add button, if the type of policy to be written is 'domain name', the rule to be blocked or allowed according to the domain name address is written.



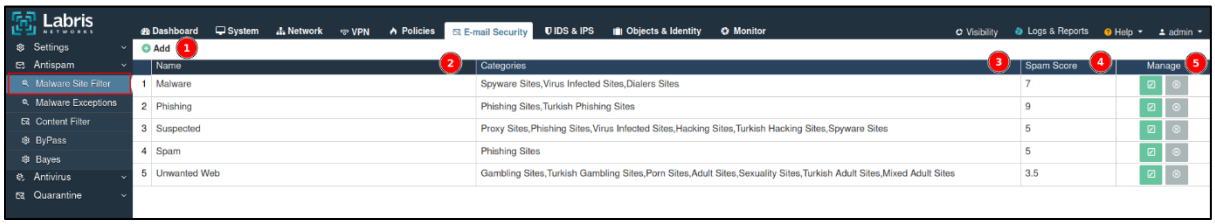
1	**Type**	The type of rule to be written is selected.
2	**Address**	If the type is selected 'Domain Name', the domain name address to be blocked or allowed is written.
3	**Action**	The action of the policy to be written is selected. Allow mail to arrive from a mailing address belonging to the domain entered is selected. If mail will not be received from the domain name address entered, block is selected.
4	**Save**	This is the button where the added rule is saved.
5	**Close**	It is the button where the window opened by clicking the Add button is closed.

14.2 Antispam

It is the module used to identify, filter and block unwanted e-mails coming to your mail server.

14.2.1 Malware Site Filter

Website filtering scans the content and domain names of websites that users visit, detects sites that contain spam, phishing, malware, or other threats, and blocks mail from these domains.



1	**Add**	It is the button used to add a website filter.
2	**Name**	This is the section where the name of the added website filter is displayed.
3	**Categories**	This is the section where the categories with the added website filter are displayed.
4	**Spam Score**	This is the section where the score of the mail that will be counted as spam is displayed.
5	**Manage**	This is the section where the website filter is deleted or edited.

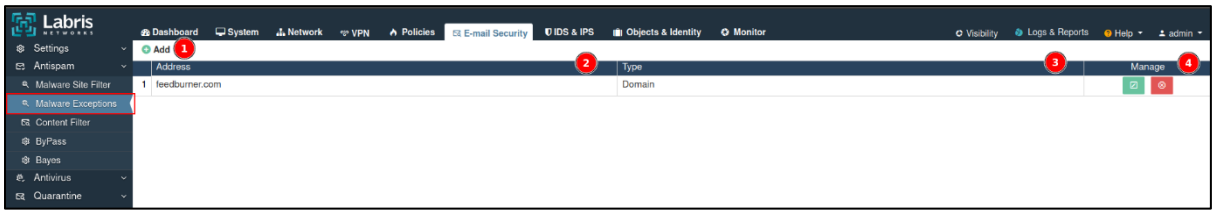
-To add a website filter, click the 'add' button to add a website filter.

1	**Name**	This is the section where the name of the website filter is entered.
2	**Categories**	This is the section where the categories to be added for the website filter rule are selected. Multiple

		categories can be added.
3	**Spam Score**	Spam is the section where the score is entered.
4	**Save**	This is the button where the added Web site filter is saved.
5	**Close**	It is the section where the window opened by clicking the Add button is closed.

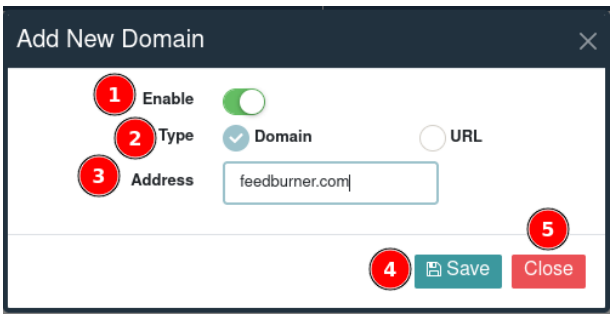
14.2.2 Malware Exceptions

It is the module where it is added as an exception in cases where mail needs to come from a domain name in the categories in the added website filter.



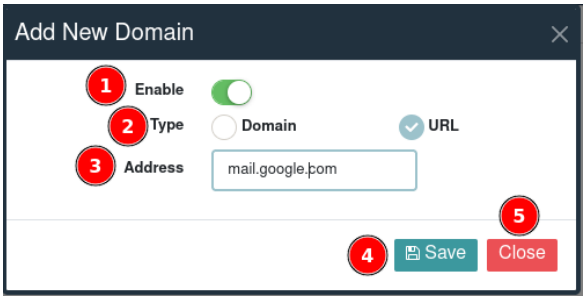
1	**Add**	An exception is the button used to add a domain name or url.
2	**Address**	This is the section where the added exception addresses are displayed.
3	**Type**	This is the section where the type of added exception addresses is displayed.
4	**Manage**	This is the section where the added exception addresses are edited or deleted.

-To add a domain name or url as a exception, click the 'add' button to add the domain name or url as an exception. If the type is selected as a field, an exception is defined by entering the field name.



1	**Enable**	It is the button where the address to be added as an exception is activated.
2	**Type**	It is the section where the type of address to be added as an exception is selected.
3	**Address**	If the type is 'domain name', it is the section where the domain name is entered.
4	**Save**	It is the button where the addresses added as an exception are saved.
5	**Close**	It is the button where the window opened by clicking the Add button is closed. The transaction made by clicking the close button is not saved.

-If the exception type is selected as 'URL', the exception is defined by entering the URL address.

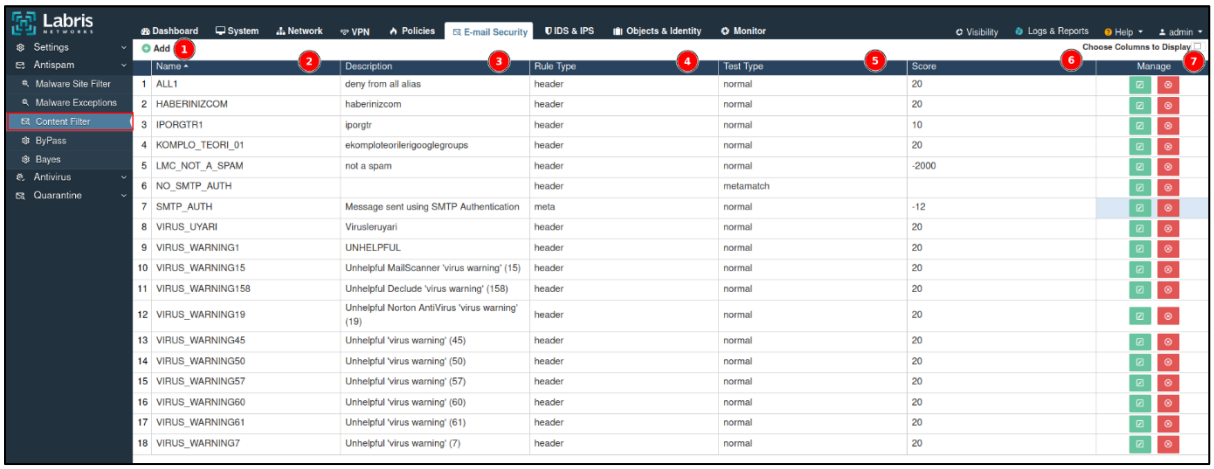


1	**Enable**	It is the button where the address to be added as an exception is activated.

2	**Type**	It is the section where the type of address to be added as an exception is selected.
3	**Address**	If the type 'URL' is selected, it is the section where the domain name is entered.
4	**Save**	It is the button where the addresses added as an exception are saved.
5	**Close**	It is the button where the window opened by clicking the Add button is closed. The transaction made by clicking the close button is not saved.

14.2.3 Content Filter

It is the module that analyzes the content in e-mail communication and detects or blocks spam, malware, phishing and other unwanted or harmful content.

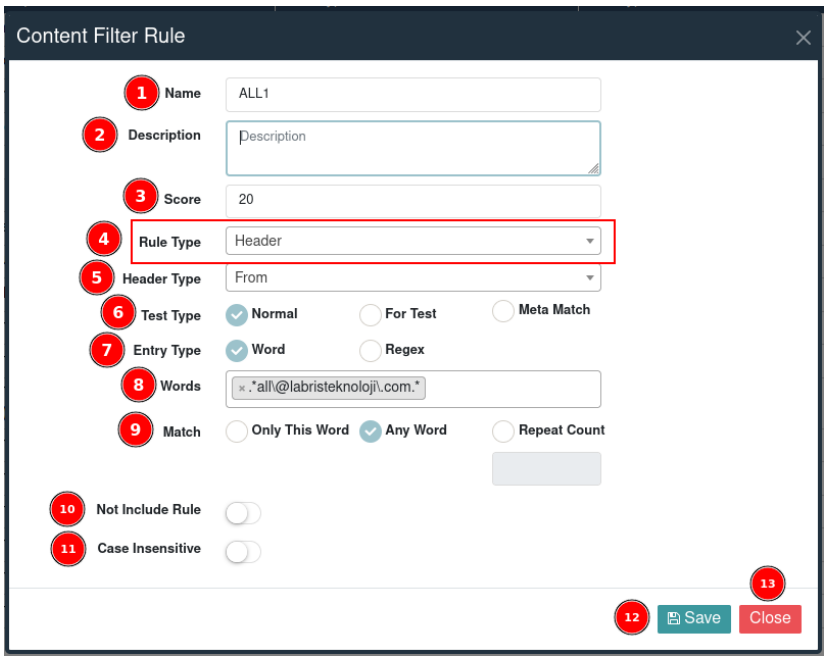


1	**Add**	This is the button where the Content Filtering rule is added.
2	**Name**	This is the section where the name given to the content filtering rule is displayed.
3	**Description**	This is the section where the description of the added content filtering rule is displayed.
4	**Rule Type**	This is the section where the rule type of the added content filtering rule is displayed.

5	**Test Type**	This is the section where the test type of the added content filtering rule is displayed.
6	**Score**	This is the section of the added content filtering rule where the score is displayed.
7	**Manage**	This is the section where the added content filtering rule is edited or deleted.

-Click the 'add' button to add a Content Filtering rule. By selecting the rule type, the content filtering rule is written according to the rule type.

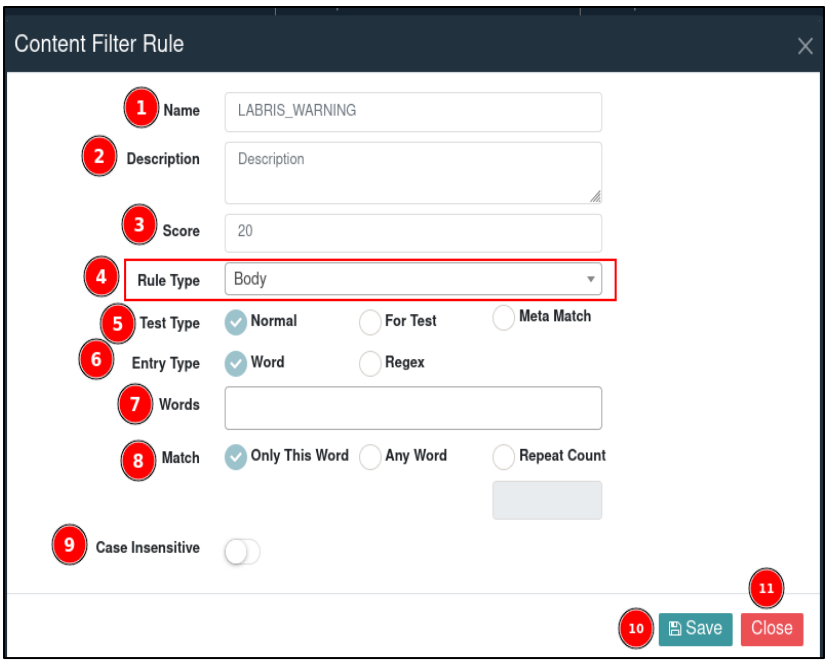
- Rule type: If the Header is selected, the content filtering rule is written by selecting the title type.



1	**Name**	This is the section where the name of the content filtering rule is entered.
2	**Description**	This is the section where the description of the content filtering rule is entered.
3	**Score**	This is the section of the content filtering rule where the spam score is entered.
4	**Rule Type**	This is the section where the rule type of the content

		filtering rule is selected.
5	**Header Type**	This is the section where the title type of the content filtering rule is selected.
6	**Test Type**	This is the section where the type of test used to detect spam e-mails or unwanted content is selected.
7	**Entry Type**	This is the section where the added content filtering rule is edited or deleted.
8	**Words**	This is the section where the content information is entered. Here, the word or regex url to be filtered as content is entered.
9	**Match**	If it matches the word of the written content, it filters. Matches all words to content or counts matches based on the word typed.
10	**Not Include Rule**	This is the section where cases that are not included in the rule are marked.
11	**Case Insensitive**	It is used in cases where it is desired to be case-insensitive.
12	**Save**	This is the button where the content filtering rule is saved.
13	**Close**	It is the button where the window opened by pressing the Add button is closed. Changes made when the window is closed are not saved.

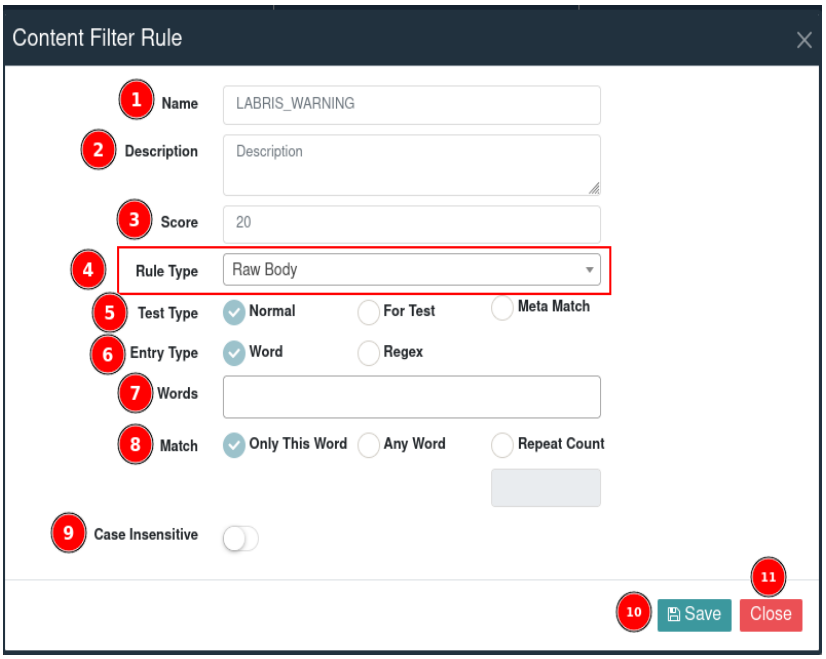
- If the rule type is selected Body, the content filtering rule that controls the body of the e-mail is written.



1	**Name**	This is the section where the name of the content filtering rule is entered.
2	**Description**	This is the section where the description of the content filtering rule is entered.
3	**Score**	This is the section of the content filtering rule where the spam score is entered.
4	**Rule Type**	This is the section where the rule type of the content filtering rule is selected.
5	**Test Type**	This is the section where the type of test used to detect spam e-mails or unwanted content is selected.
6	**Entry Type**	This is the section where the added content filtering rule is edited or deleted.
7	**Words**	This is the section where the content information is entered. Here, the word or regex url to be filtered as content is entered.

8	**Match**	If it matches the word of the written content, it filters. Matches all words to content or counts matches based on the word typed.
9	**Case Insensitive**	It is used in cases where it is desired to be case-insensitive.
10	**Save**	This is the button where the content filtering rule is saved.
11	**Close**	It is the button where the window opened by pressing the Add button is closed. Changes made when the window is closed are not saved.

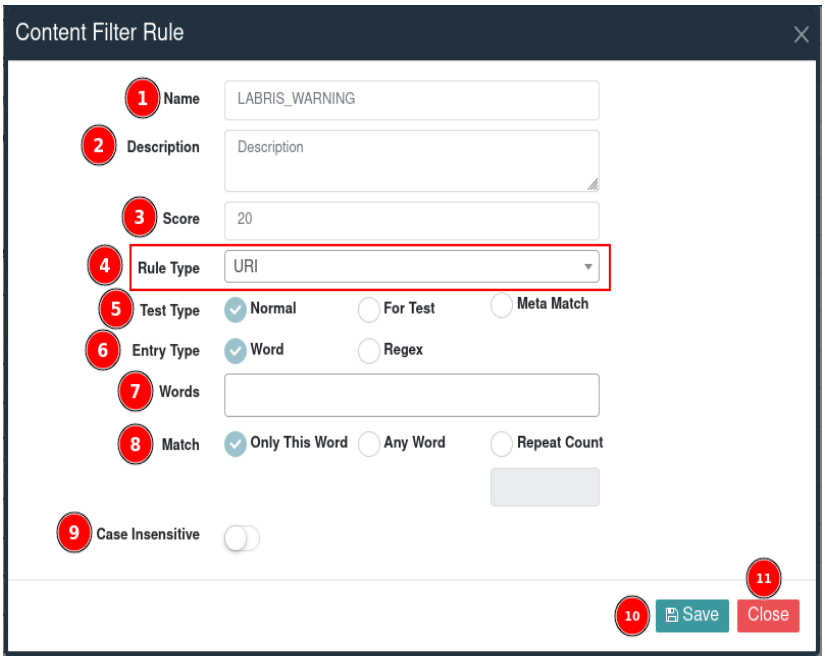
- If the rule type Raw Body is selected, the content filtering rule that controls the body of the e-mail is written.



1	**Name**	This is the section where the name of the content filtering rule is entered.
2	**Description**	This is the section where the description of the content filtering rule is entered.
3	**Score**	This is the section of the content filtering rule where the spam score is entered.

4	**Rule Type**	This is the section where the rule type of the content filtering rule is selected.
5	**Test Type**	This is the section where the type of test used to detect spam e-mails or unwanted content is selected.
6	**Entry Type**	This is the section where the added content filtering rule is edited or deleted.
7	**Words**	This is the section where the content information is entered. Here, the word or regex url to be filtered as content is entered.
8	**Match**	If it matches the word of the written content, it filters. Matches all words to content or counts matches based on the word typed.
9	**Case Insensitive**	It is used in cases where it is desired to be case-insensitive.
10	**Save**	This is the button where the content filtering rule is saved.
11	**Close**	It is the button where the window opened by pressing the Add button is closed. Changes made when the window is closed are not saved.

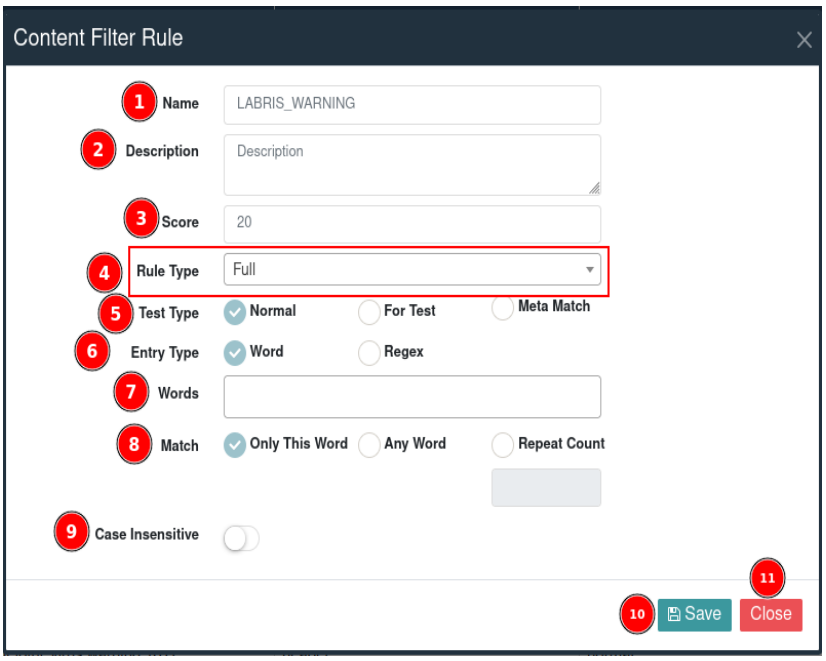
- If the rule type URI is selected, a content filtering rule is written that checks the URI information.



1	**Name**	This is the section where the name of the content filtering rule is entered.
2	**Description**	This is the section where the description of the content filtering rule is entered.
3	**Score**	This is the section of the content filtering rule where the spam score is entered.
4	**Rule Type**	This is the section where the rule type of the content filtering rule is selected.
5	**Test Type**	This is the section where the type of test used to detect spam e-mails or unwanted content is selected.
6	**Entry Type**	This is the section where the added content filtering rule is edited or deleted.
7	**Words**	This is the section where the content information is entered. Here, the word or regex url to be filtered as content is entered.

8	**Match**	If it matches the word of the written content, it filters. Matches all words to content or counts matches based on the word typed.
9	**Case Insensitive**	It is used in cases where it is desired to be case-insensitive.
10	**Save**	This is the button where the content filtering rule is saved.
11	**Close**	It is the button where the window opened by pressing the Add button is closed. Changes made when the window is closed are not saved.

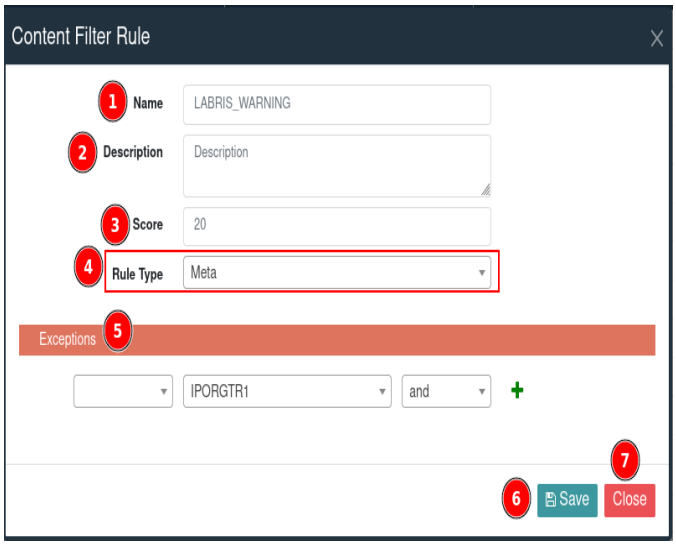
- If the rule type is selected as All, the content filtering rule that controls the entire e-mail is written.



1	**Name**	This is the section where the name of the content filtering rule is entered.
2	**Description**	This is the section where the description of the content filtering rule is entered.
3	**Score**	This is the section of the content filtering rule where

		the spam score is entered.
4	**Rule Type**	This is the section where the rule type of the content filtering rule is selected.
5	**Test Type**	This is the section where the type of test used to detect spam e-mails or unwanted content is selected.
6	**Entry Type**	This is the section where the added content filtering rule is edited or deleted.
7	**Words**	This is the section where the content information is entered. Here, the word or regex url to be filtered as content is entered.
8	**Match**	If it matches the word of the written content, it filters. Matches all words to content or counts matches based on the word typed.
9	**Case Insensitive**	It is used in cases where it is desired to be case-insensitive.
10	**Save**	This is the button where the content filtering rule is saved.
11	**Close**	It is the button where the window opened by pressing the Add button is closed. Changes made when the window is closed are not saved.

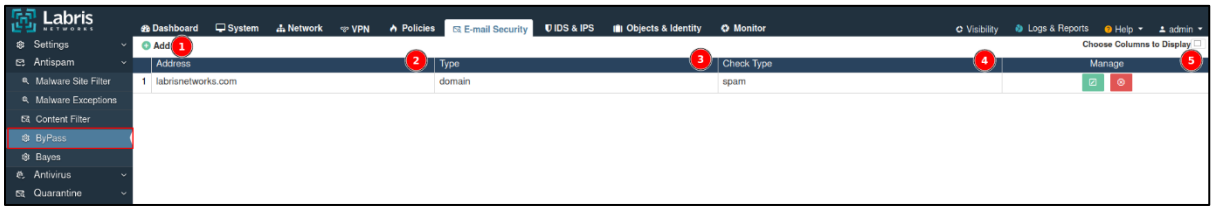
- If the rule type is Meta, a content filtering rule is written that controls the Meta information.



1	**Name**	This is the section where the name of the content filtering rule is entered.
2	**Description**	This is the section where the description of the content filtering rule is entered.
3	**Score**	This is the section of the content filtering rule where the spam score is entered.
4	**Rule Type**	This is the section where the rule type of the added content filtering rule is displayed.
5	**Exception**	It is the section where exceptions to the written rules are defined.
6	**Save**	This is the button where the content filtering rule is saved.
7	**Close**	It is the button where the window opened by pressing the Add button is closed. Changes made when the window is closed are not saved.

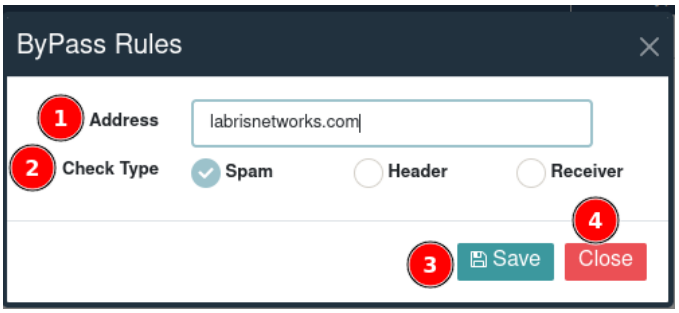
14.2.4 ByPass

It is the module where e-mail addresses that should not be detected as spam are displayed or IP addresses that should not be perceived as spam are added.



1	**Add**	It is the section where e-mail addresses that should not be perceived as spam are added.
2	**Address**	It is the section where the address information of the added e-mail addresses is displayed.
3	**Type**	The address type of the added e-mail addresses is displayed.
4	**Check Type**	It is the section where the control type of the added e-mail addresses is displayed.
5	**Manage**	It is the section where the attachment e-mail addresses are edited or deleted.

-To add a domain address that should not be detected as spam, the addition process is done by clicking the 'add' button.

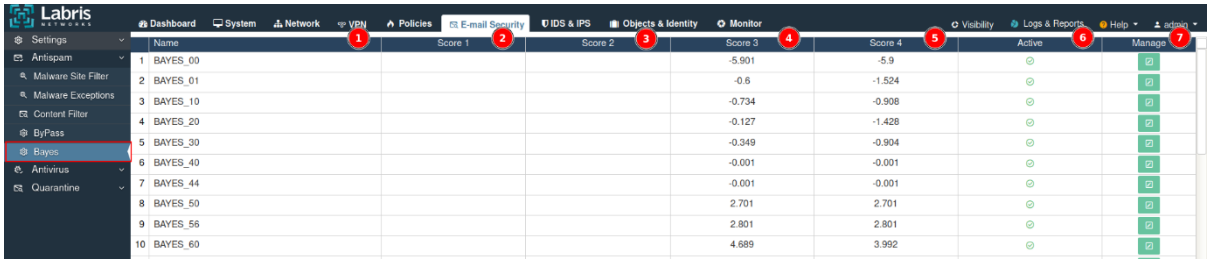


1	**Address**	It is the section where addresses that will not be detected as spam are entered.
2	**Check Type**	This is the section where the type of control of e-mail addresses is selected.
3	**Save**	It is the button where the changes made are saved.
4	**Close**	It is the button where the window opened by clicking the Add button is closed. When the Close button is

		pressed, the transactions made are not saved.

14.2.5 Bayes

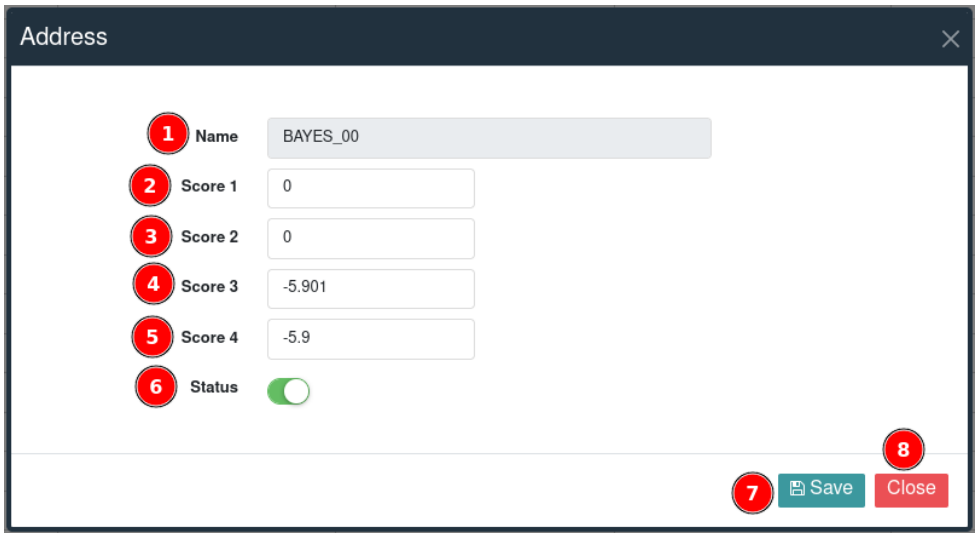
Labris is the section where the Bayesian scores kept in the database of the UTM device are displayed or their scores are changed.



	Name	Score 1	Score 2	Score 3	Score 4	Active	Manage
1	BAYES_00			-5.901	-5.9		
2	BAYES_01			-0.6	-1.524		
3	BAYES_10			-0.734	-0.908		
4	BAYES_20			-0.127	-1.428		
5	BAYES_30			-0.349	-0.904		
6	BAYES_40			-0.001	-0.001		
7	BAYES_44			-0.001	-0.001		
8	BAYES_50			2.701	2.701		
9	BAYES_56			2.801	2.801		
10	BAYES_60			4.689	3.992		

1	**Name**	This is the section where the name Bayes is displayed.
2	**Score 1**	It is the section where Bayes score 1 in the database is displayed.
3	**Score 2**	It is the section where Bayes score 2 in the database is displayed.
4	**Score 3**	It is the section where Bayes score 3 is displayed in the database.
5	**Score 4**	It is the section in the database where Bayes score 4 is displayed.
6	**Active**	This is the section where Bayes' activity status is displayed.
7	**Manage**	It is the section where the Bayesians' scores kept in the database are updated.

-To edit the added Bayesian scores, the edit is made by clicking the edit button.



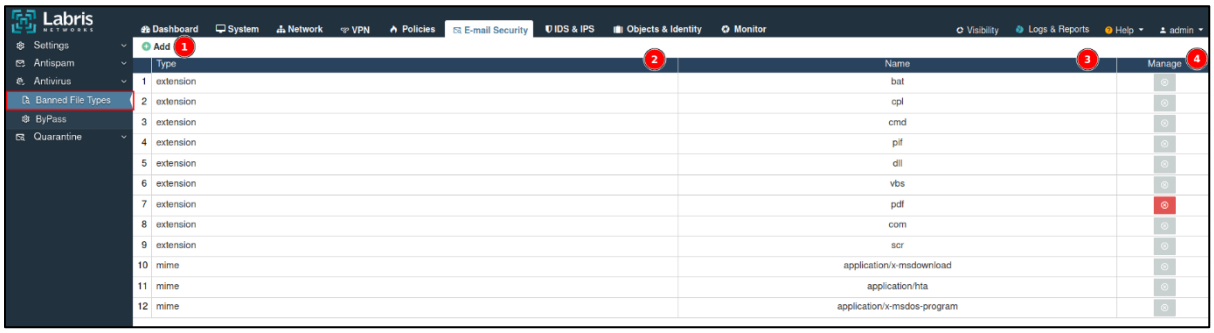
1	**Name**	This is the section where the name Bayes is displayed.
2	**Score 1**	Bayesian score 1 is the section where it is arranged.
3	**Score 2**	Bayesian is the section where score 2 is arranged.
4	**Score 3**	Bayesian is the section where score 3 is arranged.
5	**Score 4**	Bayes is the section where score 4 is arranged.
6	**Active**	This is the section where Bayes is activated.
7	**Save**	It is the section where the change made in the Bayesians' scores kept in the database is recorded.
8	**Close**	It is the button where the window opened by pressing the Edit button is closed.

14.3 Antivirus

It is the section where the content of the e-mails sent to your mail server is examined and the virus control is performed in the mail content.

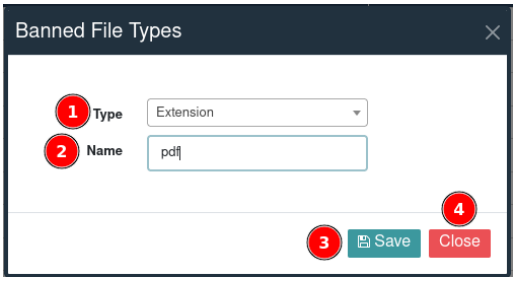
14.3.1 Banned File Type

It is the module where the extensions to be detected as a virus are added or the added extensions are displayed.



1	**Add**	It is the button where the extensions to be detected as viruses are added.
2	**Type**	This is the section where the added extension type is displayed.
3	**Name**	This is the section where the extension name is displayed.
4	**Manage**	It is the section where the added extensions are deleted.

-A prohibited extension can be added by clicking the 'add' button to add an extension that will be detected as a virus.



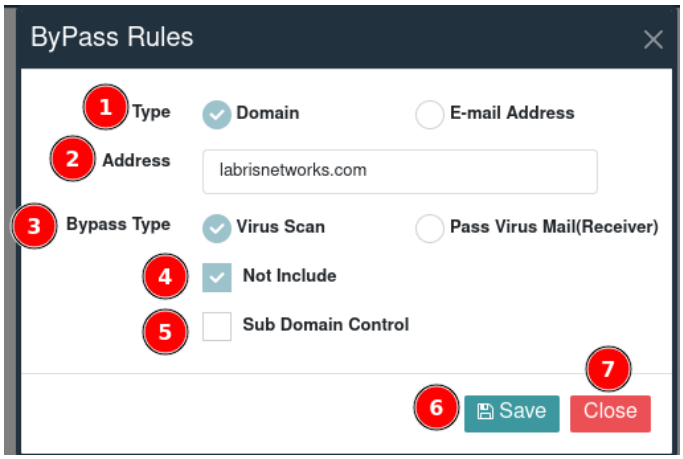
1	**Type**	This is the section where the type of extension to be blocked is selected.
2	**Name**	This is the section where the name of the extension to be blocked is entered.
3	**Save**	It is the button where the extension to be blocked is saved.
4	**Close**	It is the button where the window opened by pressing the Add button is closed.

14.3.2 Bypass

It is the module where the e-mails coming to the mail server are excluded from virus scanning.

1	**Add**	It is the button where the addresses that will not pass the virus scan are added.
2	**Address**	This is the section where the mail addresses to be excluded from virus scanning are displayed.
3	**Type**	This is the section where the type of mail addresses to be excluded from virus scanning is displayed.
4	**Bypass Type**	This is the section where the type of bypassing is displayed.
5	**Manage**	This is the section where domain names or email addresses that are excluded from virus scanning are removed or edited.

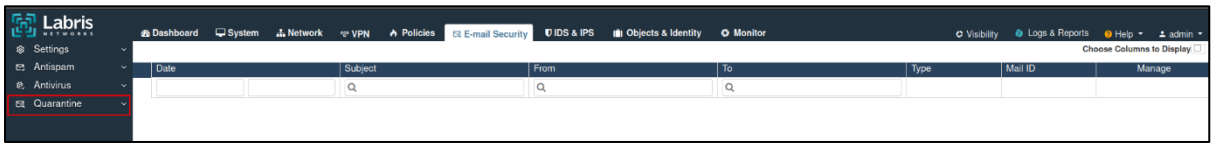
-To add domain names or e-mail addresses that will not be scanned for viruses, the addition process is done by clicking the 'add' button.



1	**Type**	This is the section where the type of addresses that will not be scanned for viruses is selected. The domain name or email address is added as a type.
2	**Address**	Depending on the type, it is the section where the domain name, address or email address is added.
3	**Bypass Type**	This is the section where the type of bypassing of the typed domain name address or e-mail address is selected.
4	**Not Include**	It is opened in cases where it is desired not to be included in the virus scan.
5	**Sub Domain Control**	It opens in cases where the subdomain name of the added address needs to be checked.
6	**Save**	It is the button where the addresses that will not pass the virus scan are saved.
7	**Close**	It is the button where the window opened by clicking the Add button is closed.

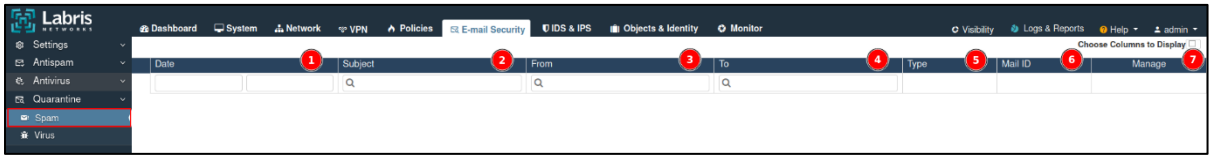
14.4 Quarantine

It is the section where the e-mails quarantined by the Labris UTM device are displayed.



14.4.1 Spam

This is the section where the mails detected as spam by the UTM device are displayed.



1	**Date**	This is the section where the date the spam was quarantined is displayed.
2	**Subject**	This is the section where the subject of the quarantined mail is displayed.
3	**From**	This is the section where the sender address of the quarantined mail is displayed.
4	**To**	This is the section where the recipient address of the quarantined mail is displayed.
5	**Type**	This is the section where the type information of the quarantined mail is displayed.
6	**Mail ID**	This is the section where the Email ID of the quarantined mail is displayed
7	**Manage**	It is the section where quarantined mail is issued.

14.4.2 Virus

It is the section where the e-mails detected as infected by the Labris UTM device are displayed.

1	**Date**	This is the section where the date of quarantine of the e-mail detected with the virus is displayed.	
2	**Virus Name**	This is the section where the virus name of the quarantined infected mail is displayed.	

3	**From**	This is the section where the sender address of the quarantined infected mail is displayed.	
4	**To**	This is the section where the recipient address of the quarantined infected mail is displayed.	
5	**Mail ID**	This is the section where the Email ID of the quarantined infected mail is displayed	
6	**Manage**	It is the section where quarantined infected mail is issued.	

15. IDS&IPS

IDS (Intrusion Detection System) is a system that monitors and detects potential malicious activities in network or computer systems. It detects anomalous activities by analyzing network traffic.

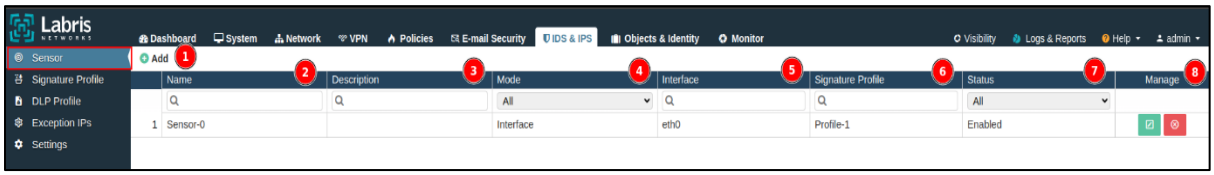
IPS (Intrusion Prevention System) can automatically intervene and stop the attack attempt after a specific threat is detected. IPS detects and responds to attacks by inspecting network traffic or performing system-level behavioral analysis.

IPS is used to prevent harmful movements or harmful connections within your network traffic.

In the Labris UTM device, sensor settings, signature profiles in the database, DLP profile, exception IP addresses and general settings of IDS and IPS are made regarding IDS and IPS.

15.1 Sensor

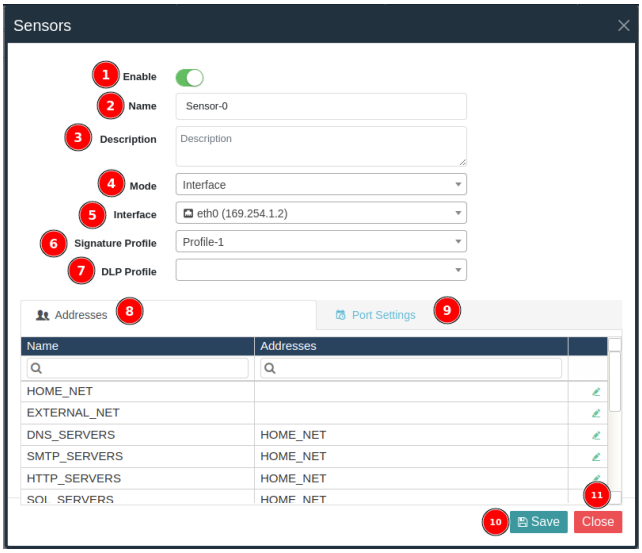
It is the module where the port where the traffic will be listened to in the Labris UTM device is selected. Here, the IDS&IPS sensor is switched on at the selected interface. By examining the traffic passing through the specified interface, attacks on network traffic are detected and prevented.



1	**Add**	This is the button to which the IDS&IPS sensor is added.	
2	**Name**	This is the section where the name of the added IDS&IPS sensor is displayed.	
3	**Description**	This is the section where the description of the added IDS&IPS sensor is displayed.	
4	**Mode**	The mode for IDS&IPS operation is displayed. If the mode interface is selected, IDS&IPS listens to the traffic on the interface and detects and blocks it. In the	

		case where the mode of the policy is selected, it detects and blocks according to the specified Rule set.	
5	**Interface**	This is the section where the interface where IDS&IPS is opened is displayed.	
6	**Signature Profile**	This is the section where the signature profile of IDS&IPS is displayed.	
7	**Status**	The status of IDS&IPS is displayed. If the status is active, IDS&IPS runs on the selected interface. If the status is inactive, IDS&IPS is turned off.	
8	**Manage**	This is the section where the added IDS&IPS sensors are edited or deleted.	

-To add a sensor, click the 'add' button to add an IDS&IPS sensor. After clicking the Add button, the information on the screen is filled in and the IDS&IPS sensor is added.

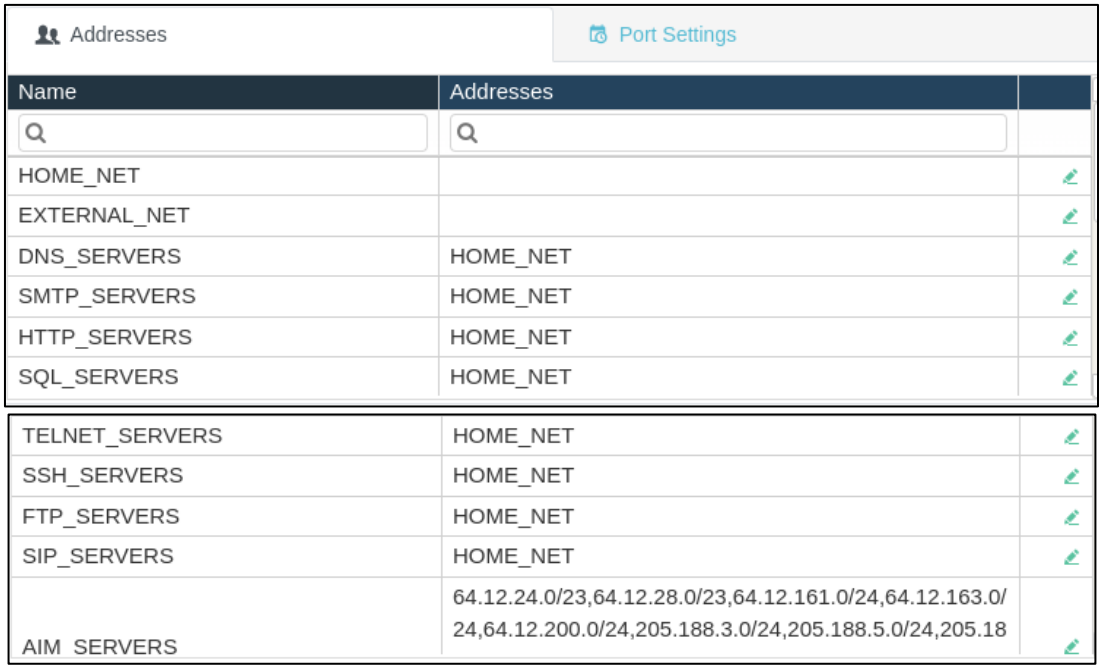


1	**Enable**	This is the button where the IDS&IPS sensor is activated.
2	**Name**	This is the section where the name of the IDS&IPS sensor is entered.
3	**Description**	This is the section where the description of the IDS&IPS sensor is entered.

4	**Mode**	The mode for IDS&IPS to operate is selected. If the mode interface is selected, IDS&IPS listens to the traffic on the interface and detects and blocks it. In the case where the mode of the policy is selected, it detects and blocks according to the specified Rule set.
5	**Interface**	This is the section where the interface to open IDS&IPS is selected.
6	**Signature Profile**	This is the section where the added signature profile is selected.
7	**DLP Profile**	This is the section in the DLP Profile where the added DLP is selected.
8	**Addresses**	This is the section where the address information to be controlled by the IDS&IPS sensor is located and the address information is edited.
9	**Port Settings**	This is the section where the port information to be inspected by the IDS&IPS sensor is located and the port information is arranged.
10	**Save**	This is the button where the IDS&IPS sensor is saved.
11	**Close**	The IDS&IPS sensor is the button on which the display is turned off.

15.1.1 Address Settings

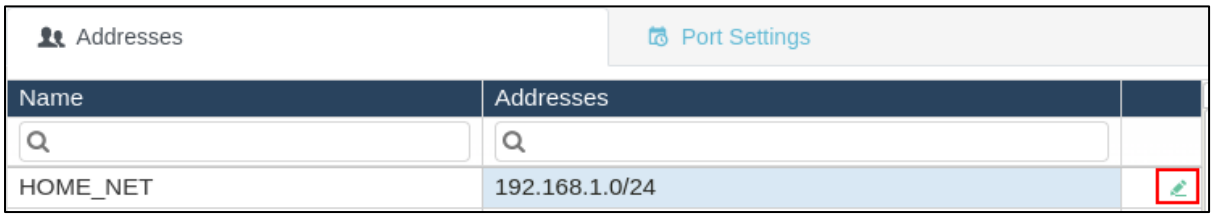
IDS&IPS is the section where the address settings of the sensor are made.

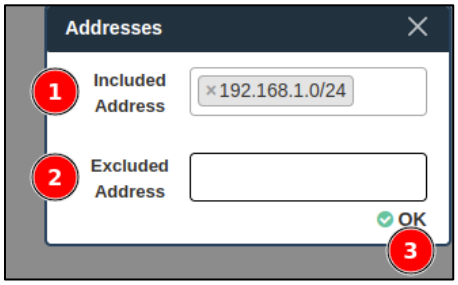


1	**HOME_NET**	This is the section where the IDS&IPS internal network address is written.
2	**EXTERNAL_NET**	This is the section where IDS&IPS external network addresses are written. It is usually left as 'any'. This means that the IDS&IPS sensor will monitor traffic from the external IP address.
3	**DNS_SERVER**	The DNS server information on the internal network is entered. If there is no DNS server, it is left at $Home_NET.
4	**SMTP_SERVER**	The SMTP server information on the internal network is entered. If there is no SMTP server, it is left as $HOME _NET.
5	**HTTP_SERVER**	The HTTP server information on the internal network is entered. If there is no HTTP server, it is left at $HOME_NET.
6	**SQL_SERVER**	SQL server information on the internal network is entered. If the SQL server does not exist, it is left as

		$HOME _NET.
7	**TELNET_SERVER**	Telnet server information on the internal network is entered. If there is no Telnet server, it is left as $HOME _NET.
8	**SSH_SERVER**	SSH server information on the internal network is entered. If there is no SSH server, it is left as $HOME_NET.
9	**FTP_SERVER**	FTP server information on the internal network is entered. If there is no FTP server, it is left as $HOME _NET.
10	**SIP_SERVER**	The SIP server information on the internal network is entered. If there is no SIP server, it is left as $HOME_NET.
11	**AIM_SERVER**	The AIM server information on the internal network is entered. If there is no AIM server, it is left as $HOME _NET. IP addresses detected as AIM servers come by default.

-Click on the 'edit' button to edit the addresses.



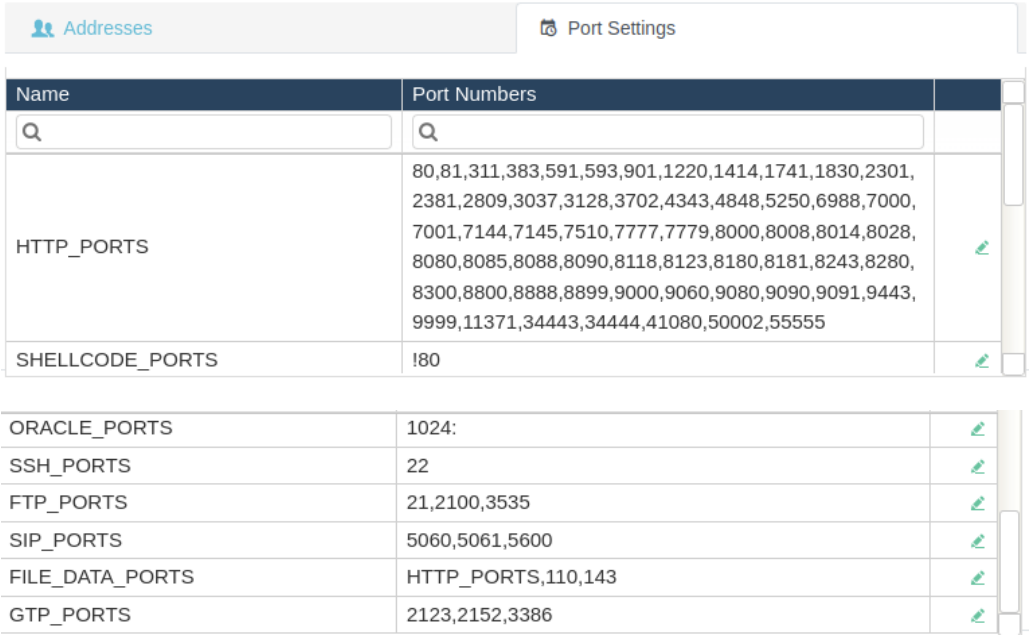


1	**Included Address**	This is the section where the internal IP addresses for

		the IDS&IPS sensor are selected.
2	**Excluded Address**	This is the section where the excludes addresses for the IDS&IPS sensor are selected.
3	**Save**	The added IDS&IPS sensor is the button where IP addresses are stored.

15.1.2 Port Settings

IDS&IPS is the section where the port settings of the sensor are made.

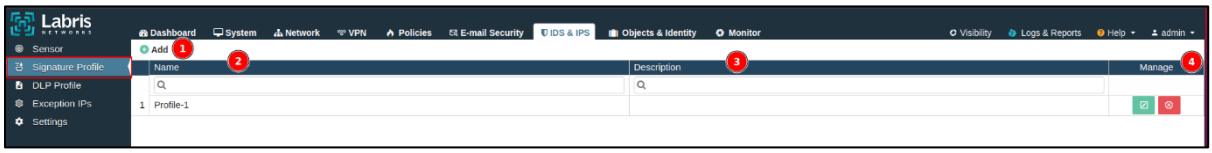


1	**HTTP_PORTS**	The ports where HTTP traffic is controlled are displayed and port addition is made.	
2	**SHELLCODE_PORTS**	It is the section where the ports to be used for shellcode detection are displayed or the port information to be detected is entered. The phrase '!80' is written to exclude port 80 from detection.	
3	**ORACLE_PORTS**	The ports used to monitor Oracle database traffic are displayed, and the desired port numbers are entered to examine Oracle database traffic. The phrase '1024:' is written to monitor all ports above 1024.	

4	**SSH_PORTS**	The port information where SSH traffic is controlled is displayed and the port number used for SSH is entered, if any.	
5	**FTP_PORTS**	The port information where FTP traffic is controlled is displayed and the port number used for FTP is entered, if any.	
6	**SIP_PORTS**	The port information through which the SIP traffic is controlled is displayed. If a port number other than the SIP ports is used, this section is added.	
7	**FILE_DATA_PORTS**	The ports used to monitor file data streams in network traffic belonging to the selected interface are displayed. By default, adding another port number other than the specified ports is done in this section.	
8	**GTP_PORTS**	The ports used to monitor GTP flows in network traffic that belong to the selected interface are displayed. By default, adding another port number other than the specified ports is done in this section.	

15.2 Signature Profile

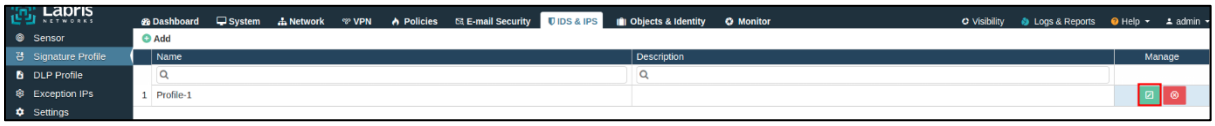
By listening to network traffic, abnormal traffic or blocking operations are done according to the IDS&IPS signature profile. By analyzing network traffic, it detects behaviors that comply with certain signature rules and takes action accordingly. In this module, the added signature profiles are displayed.

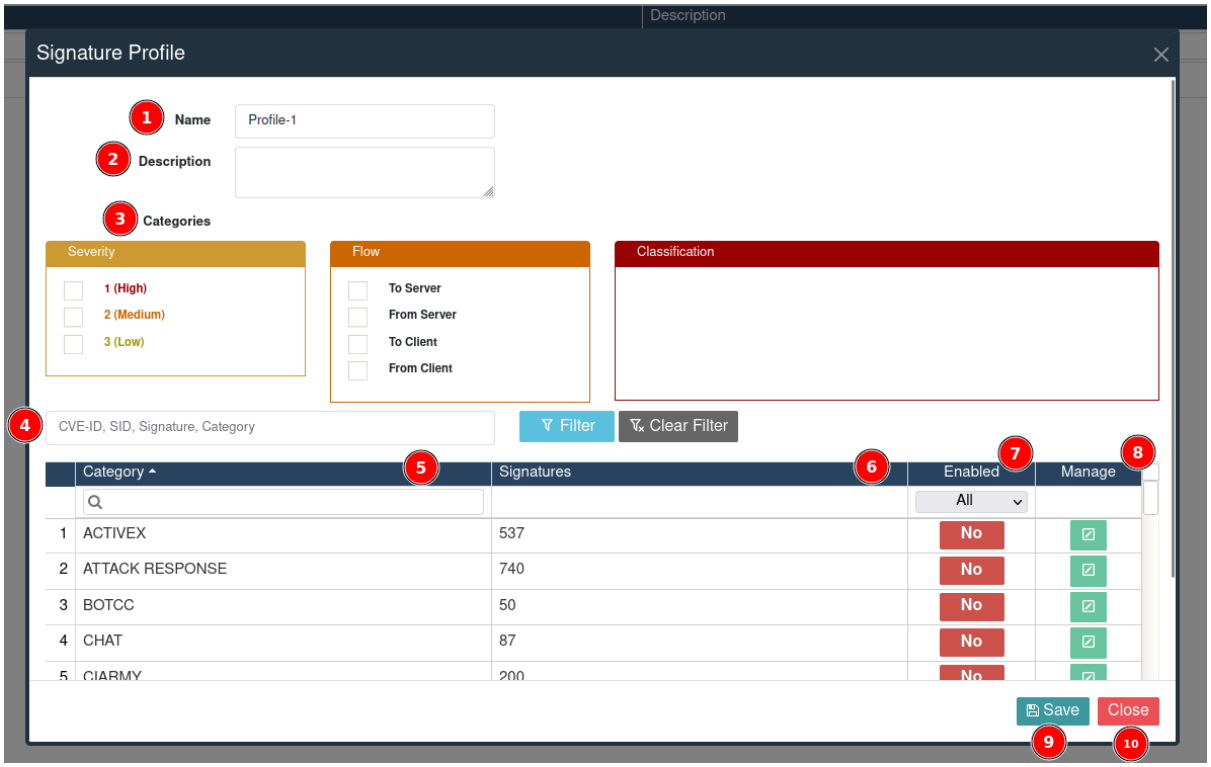


1	**Add**	It is the button where the process of adding a signature profile is done.
2	**Name**	The name of the added signature profile is displayed.
3	**Description**	A description of the added signature profile is displayed.

4	**Manage**	This is the section where signature profiles are edited or deleted.

-The edit button is pressed to edit the signature profile. After pressing the Edit button, the signature profiles are edited.

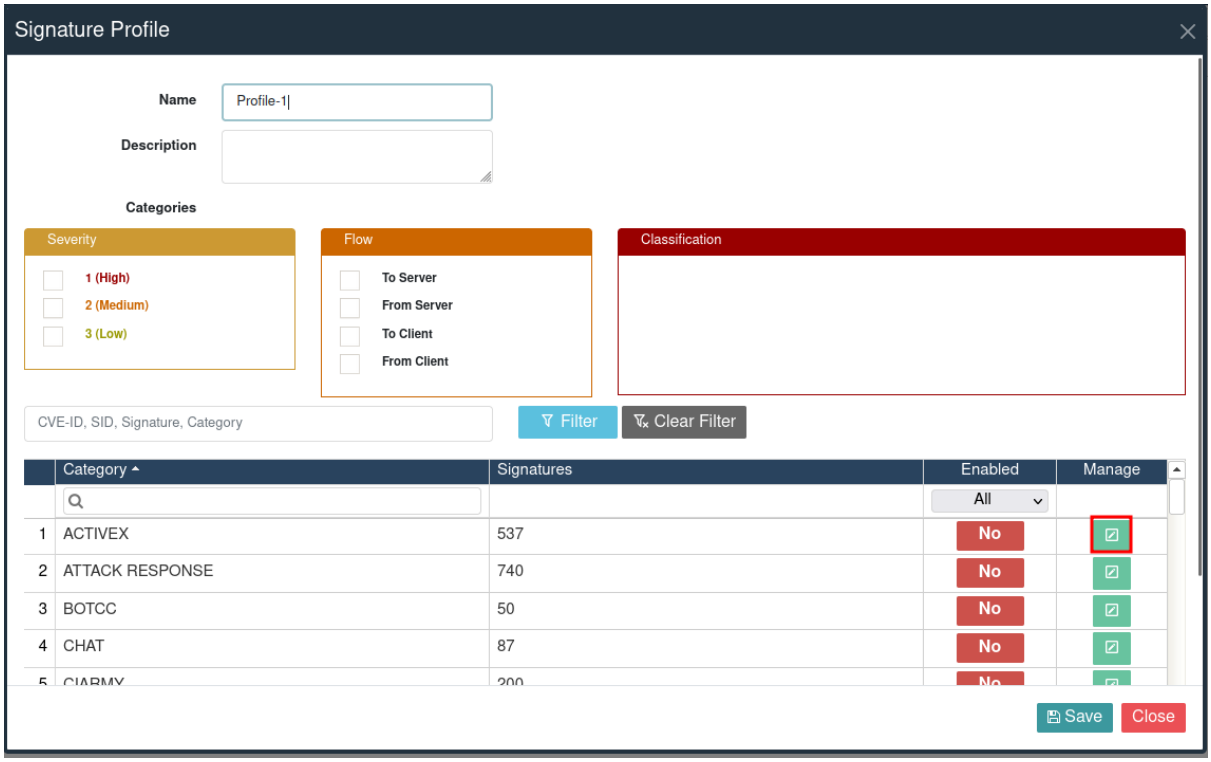




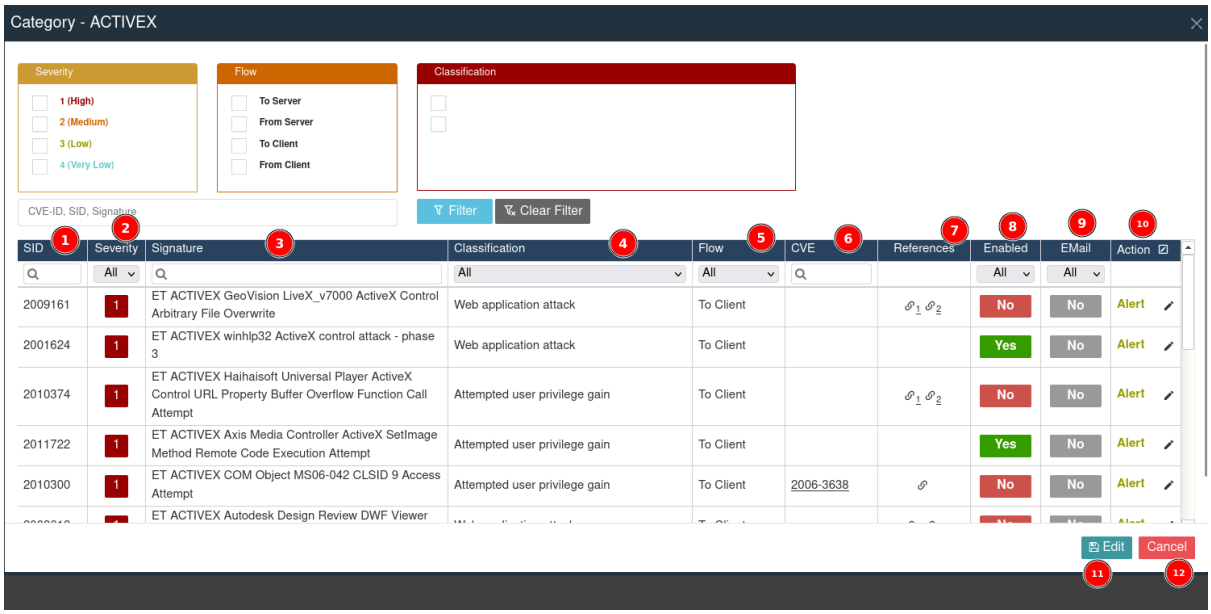
1	**Name**	This is the section where the name of the signature profile is entered.
2	**Description**	This is the section where the description about the signature profile is entered.
3	**Classfication**	This is the section where filtering signature profiles by categories is done. Severity is classified according to the severity of the incident detected by a rule. The criticality level, on the other hand, usually represents very serious security threats or attack attempts. If the criticality level is in the middle, it is a potentially significant security incident that does not pose a major direct threat. If it is selected low, it is usually a less

		critical or informational event. The flow specifies which traffic direction and connection status the rule will monitor. Specifies that traffic is coming from the server, traffic is coming from the server, traffic is coming from the client, and traffic is coming from the client. Classification, on the other hand, is determined by the level of flow and criticality.
4	**Signature Search**	It is the section where the signatures in the signature database are filtered according to CVE-ID, SID, Signature and Category.
5	**Category**	This is the section where the category name of the signature is displayed.
6	**Signatures**	This is the section where the number of signatures in the signature category is displayed.
7	**Enabled**	The activity status of the signature is displayed.
8	**Manage**	This is the section where signatures are arranged.
9	**Save**	This is the button where the edited Signature profile is saved.
10	**Close**	This is the button where the signature profile screen is turned off.

-Click the 'edit' button to edit the signature profile.



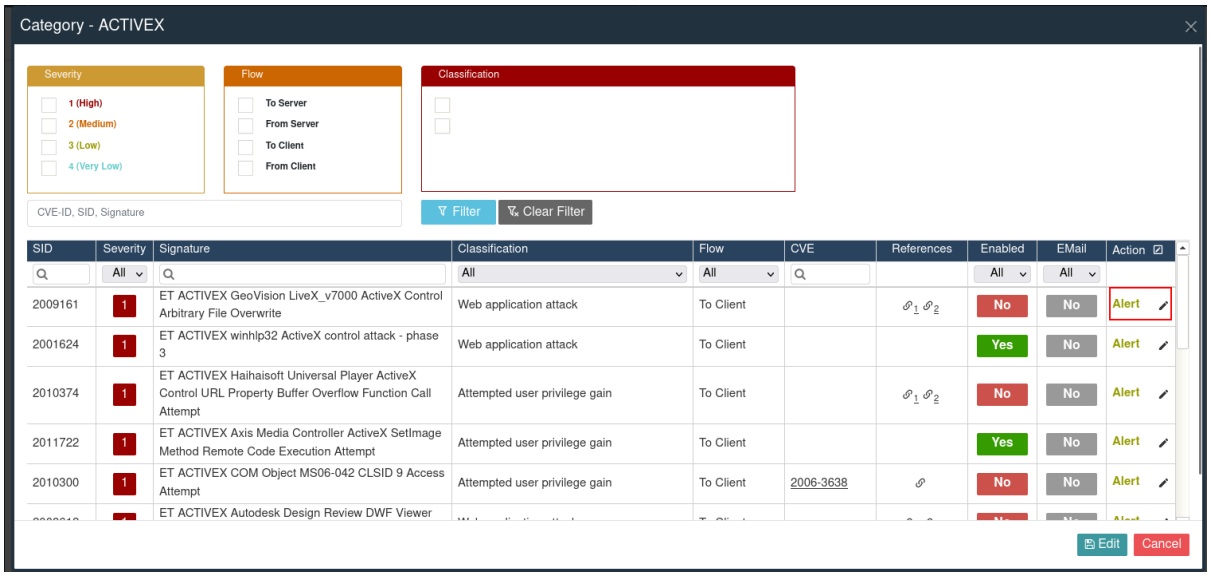
-After clicking the Edit button, the edited signature profile is edited.

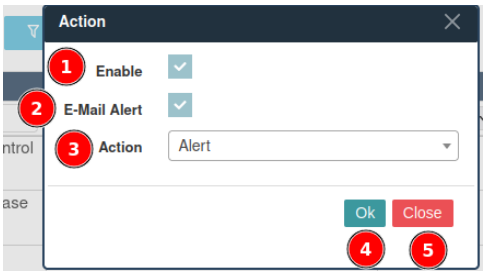


1	**SID**	This is the section where the signature ID number is displayed.
2	**Severity**	The criticality level for IDS&IPS signatures is displayed. 1- High, 2- Medium, 3- Low and 4- Very Low

3	**Classification**	The classification name of the signatures is displayed.
4	**Flow**	The flow information of the IDS&IPS signature is displayed.
5	**CVE**	The CVE uses it for the identification and classification of software and hardware vulnerabilities. In this section, the CVE numbers of the signatures are displayed.
6	**References**	The reference information for the signatures is displayed. It is found in the details about the reference.
7	**Enabled**	The activity status of the signature is displayed. If it is active, it writes 'yes', if it is inactive, it writes 'no'.
8	**Email**	The status of sending e-mails of alerts attached to the signature is displayed. If the e-mail will be sent, it will write 'yes', if the e-mail will not be sent, it will write 'no'.
9	**Action**	Anomalies in network traffic are detected and a warning or block is made for those who are caught in the signature.
10	**Edit**	It is the button where the edit related to signatures is saved.
11	**Close**	This is the button where the signature profile screen is turned off.

-The edit button in the action section is pressed to edit the action to be taken regarding the rules in the signature profile.

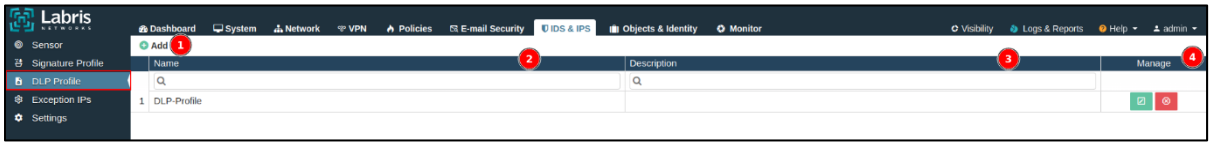




1	**Enable**	This is the button where the IDS&IPS rule is activated.
2	**E-Mail Alert**	It is enabled to send e-mail alerts for abnormal traffic detected by the IDS&IPS rule.
3	**Action**	This is the section where the action is selected for the IDS&IPS rule. A warning is generated about the rule edited in this section, or traffic passing through the rule is blocked.
4	**Save**	It is the button where the changes made to the action are saved.
5	**Close**	It is the button where the window that opens to fix the action is closed.

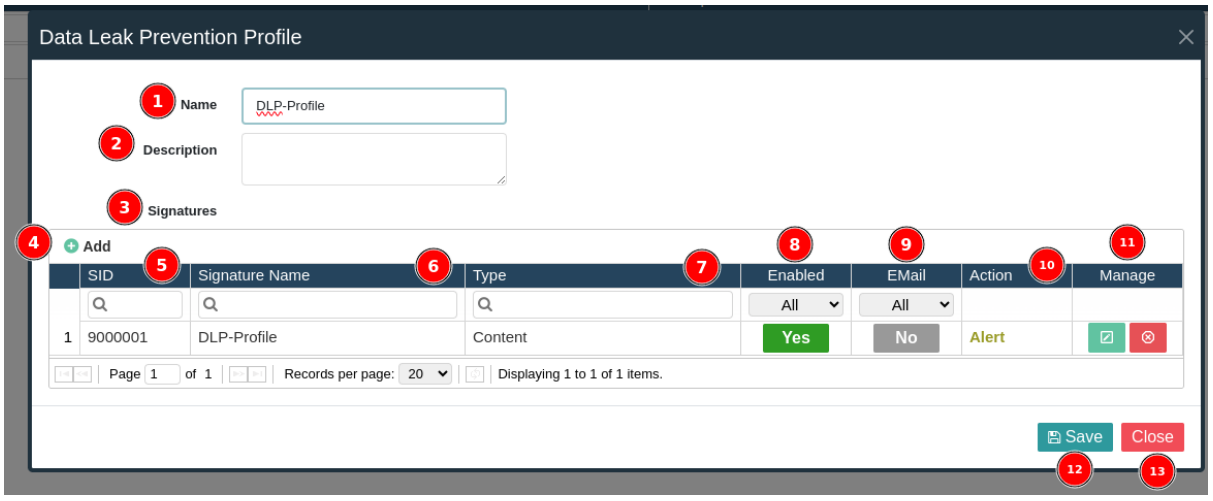
15.3 DLP Profile

A DLP Profile is a set of rules created to protect an organization's sensitive information from unauthorized access, use, transfer, and exfiltration. It is created to ensure that sensitive data is protected. The created profiler is intended to prevent data leaks and breaches. DLP Profiles increase data security over network traffic.



1	**Add**	This is the button used to add a DLP Profile.
2	**Name**	The name of the added DLP Profile is displayed.
3	**Description**	This is the section where the description about the added DLP Profile is displayed.
4	**Manage**	DLP Profilinin silindiği veya düzenlendiği bölümdür.

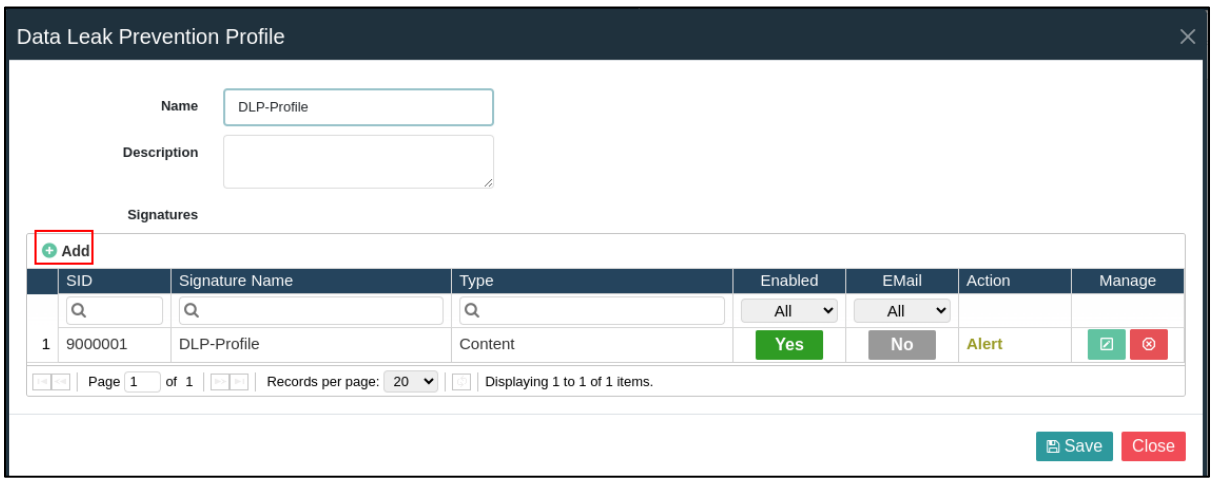
-Click the 'add' button to add a DLP Profile. After clicking the Add button, the DLP rule is added.



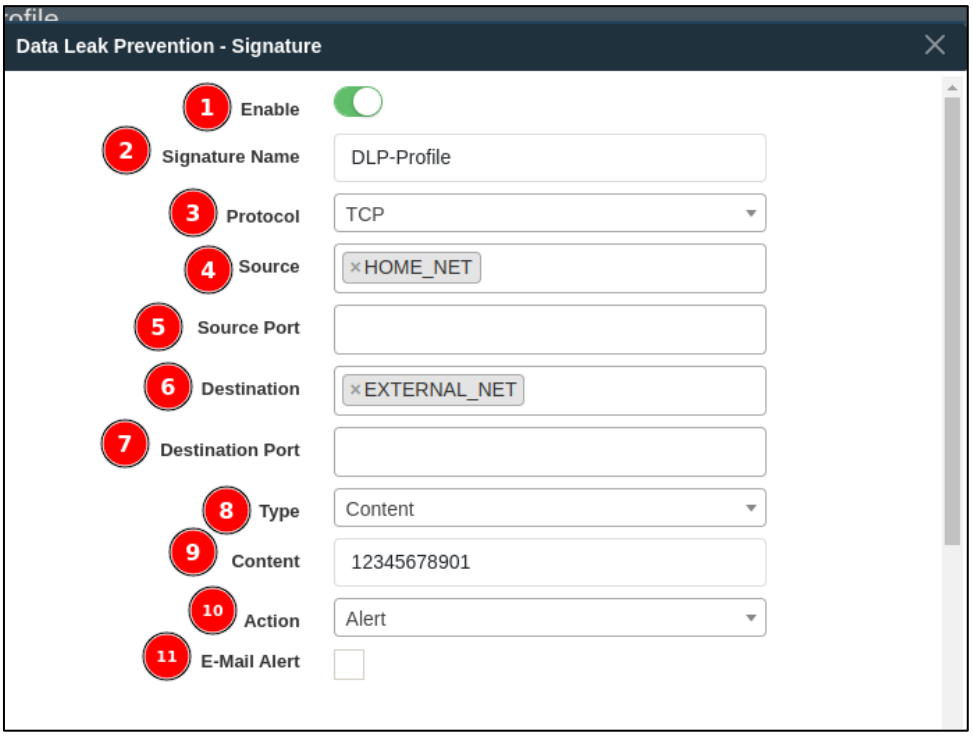
1	**Name**	This is the section where the name of the DLP Profile is entered.
2	**Description**	This is the section where the description of the DLP Profile is entered.

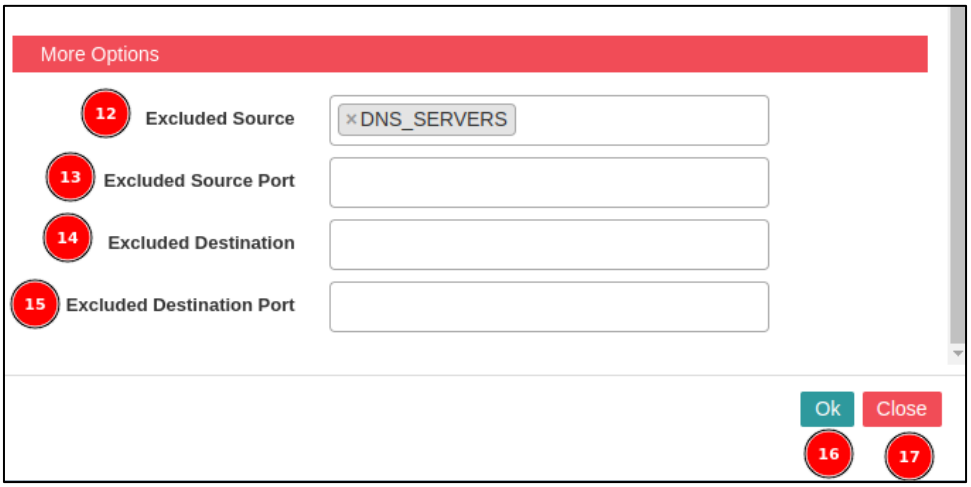
3	**Signatures**	This is the section where the added DLP rules are displayed or the DLP rule is added.
4	**Add DLP Rule**	This is the button used to add a DLP rule.
5	**SID**	This is the section where the SID number of the added DLP rule is displayed.
6	**Signature Name**	This is the section where the name of the added DLP signature is displayed.
7	**Type**	The type of DLP signature is displayed.
8	**Enabled**	The activity of the DLP signature is displayed. If it says 'yes', DLP signature is enabled. If 'No', the DLP signature is off.
9	**Email**	The email status related to the traffic caught in the DLP Signature is displayed. If it is 'yes', it sends an email. If it is 'no', it does not send an email.
10	**Action**	This is the section where the action is selected for the DLP rule. A warning is generated about the rule edited in this section, or traffic passing through the rule is blocked.
11	**Manage**	This is the section where DLP rules are regulated.
12	**Save**	This is the button where the DLP profile is saved.
13	**Close**	It is the button where the window opened by clicking the 'Add' button is closed.

-Click the 'add' button to add a DLP rule.



- After clicking the Add button, the DLP rule is edited.





1	**Enable**	This is the partition where DLP signature is enabled.
2	**Signature Name**	This is the section where the name of the DLP signature is entered.
3	**Protocol**	This is the section where the protocol is selected for the DLP signature
4	**Source**	This is the section where the source address is selected for the DLP signature. It examines the traffic at the selected source address and makes a decision based on the traffic.
5	**Source Port**	This is the section where the source port is selected for the DLP signature. If the source port is specified, it decides the anomalies by looking at the source port.
6	**Destination**	This is the section where the destination address is selected for the DLP signature. It examines the traffic towards the selected destination address and makes a decision based on the traffic.
7	**Destination Port**	This is the section where the target port is selected for the DLP signature. If the destination port is specified, it decides the anomalies by looking at the destination port.
8	**Type**	The type of DLP signature is selected. A DLP rule is

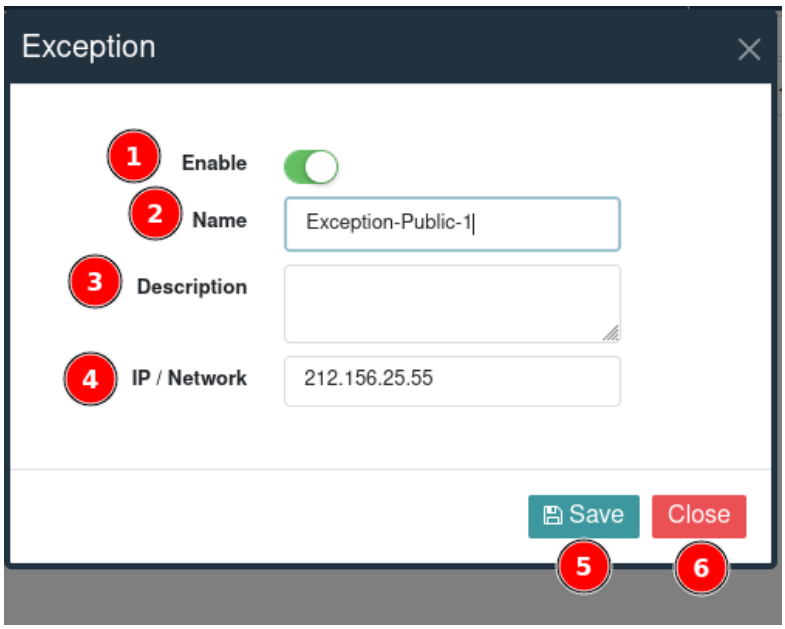
		created according to the selected type. There are 3 DLP types. These; content, regex, file extension.
9	**Content/Regex/File Extension**	If content is selected as the type, it blocks according to the specified content. If type regex is selected, it analyzes the traffic according to the specified regexe and blocks it or warns the user. If Type file extension is selected, it blocks or generates a warning based on the selected file extension.
10	**Action**	The action of the traffic caught in the DLP signature is specified.
11	**E-mail Alert**	Traffic caught in the DLP signature is used to generate an Email alert.
12	**Excluded Source**	This is the section where source addresses that are not included in DLP protection are selected.
13	**Excluded Source Port**	This is the section where the source ports that are not included in DLP protection are selected.
14	**Excluded Destination**	This is the section where the destination address information that is not included in DLP protection is selected.
15	**Excluded Destionation Port**	This is the section where destination ports that are not included in DLP protection are selected.
16	**Save**	This is the button where the DLP signature is saved.
17	**Close**	It is the button where the window opened by clicking the 'Add' button is closed.

15.4 Exception IPs

This is the section where IP addresses that do not comply with IDS&IPS rules are added.

1	**Add**	It is the button where the IP addresses that do not comply with the IDS&IPS rules are added.
2	**Name**	This is the section where the name given to the IP addresses added as an exception is displayed.
3	**Description**	This is the section where the explanation information given to the IP addresses added as an exception is displayed.
4	**IP/Network**	This is the section where the IP Address or Network address added as an exception is displayed.
5	**Status**	The status of IP or Network addresses that have been added as a reference is displayed. If the status is enabled, the IP address that appears is not included in the IDS&IPS protection. The IP or Network address that appears as inactive is included in IDS&IPS protection.
6	**Manage**	It is the section where the added exception IP/Network addresses are deleted or edited.

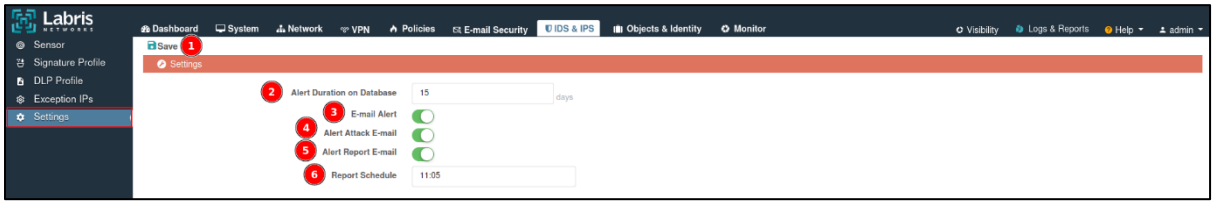
-Click the 'add' button to add IP or Network addresses that will not be included in IDS&IPS protection. IP or Network addresses entered after clicking the 'add' button are not included in the IDS&IPS protection.



1	**Enable**	It is the section where the IP address that is added as an exception is enabled.
2	**Name**	This is the section where the name given to the IP addresses added as an exception is displayed.
3	**Description**	This is the section where the explanation information given to the IP addresses added as an exception is displayed.
4	**IP/Network**	This is the section where the IP Address or Network address added as an exception is displayed.
5	**Save**	The status of IP or Network addresses that have been added as a reference is displayed. If the status is enabled, the IP address that appears is not included in the IDS&IPS protection. The IP or Network address that appears as inactive is included in IDS&IPS protection.
6	**Close**	It is the section where the added exception IP/Network addresses are deleted or edited.

15.5 Settings

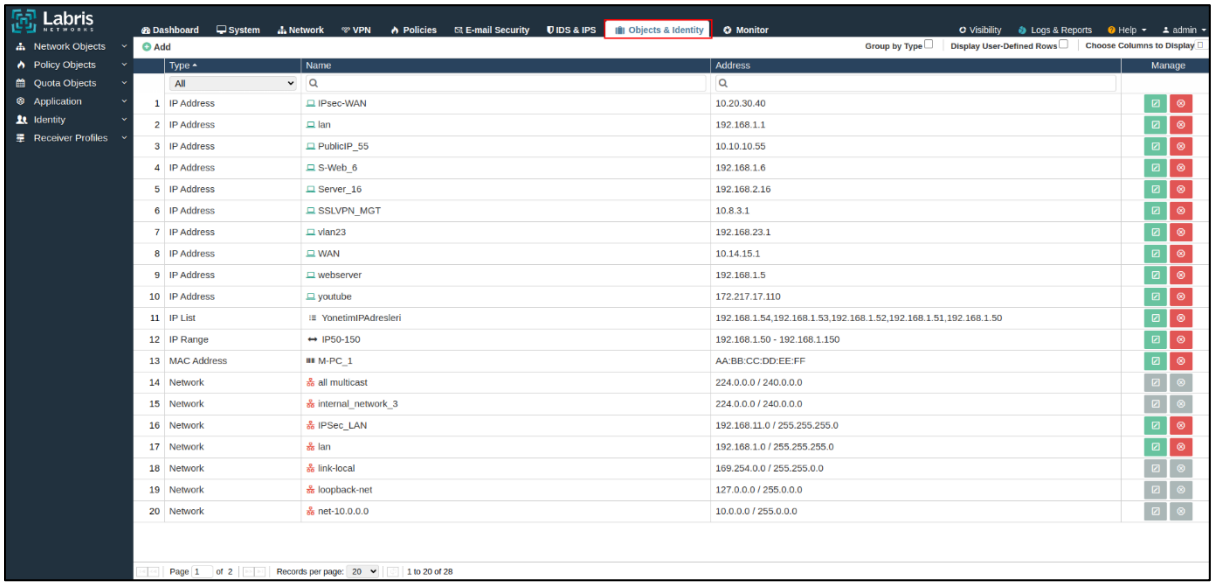
This is the section where the settings to which IDS&IPS's alerts will be sent are made. In this module, IDS&IPS attacks and alerts are sent to the e-mail address defined in the system module.



1	**Save**	This is the section where IDS&IPS mail settings are saved.
2	**Alert Duration on Database**	It is the section in the database where the time of keeping the warnings is regulated. It is organized in days.
3	**E-mail Alert**	It is the button that opens to send the warnings of the attacks by e-mail.
4	**Alert Attack E-mail**	It is activated in case of IDS&IPS attacks, in case of sending a warning e-mail.
5	**Alert Report E-mail**	Alert reports are enabled in case they need to be sent by email.
6	**Report Schedule**	Sends the generated report in a scheduled manner.

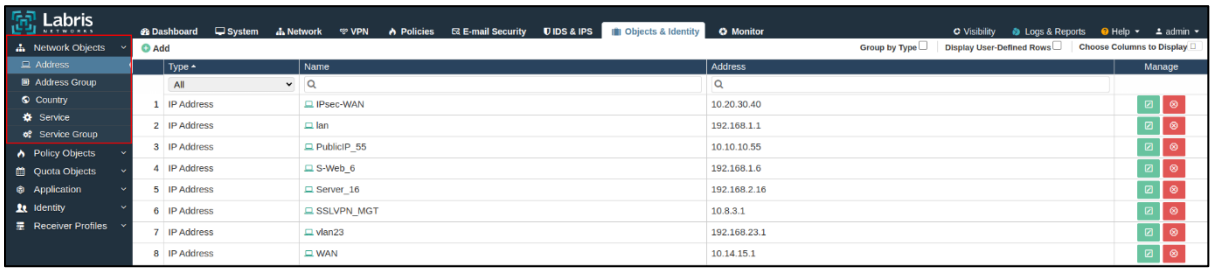
16.Objects & Identity

It is the module where the objects and identities to be used in firewall rules are added. Added objects are used in firewall and NAT policies. In addition to these, identity objects are also used in the Policies module. Adding users to the Labris UTM device is done with Active Directory integration. In this way, users added to the Active Directory are transferred to the Labris UTM device. A rule is written in the Policy module for users who are withdrawn from the Active Directory. In the Object and Identities module, Network Objects, Policy Objects, Quota Objects, Application, Identity, and Receiver Profiles are added.



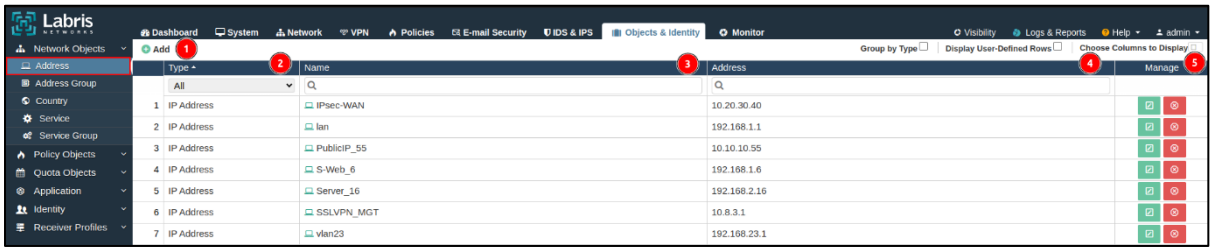
16.1 Network Objects

It is the module where the network objects to be used in the Policies module are created. The rules are written in the firewall and NAT policy for the Network Objects that are created. On the Network Objects menu, Addresses, Address Group, Country, Service, and Service Group are added.



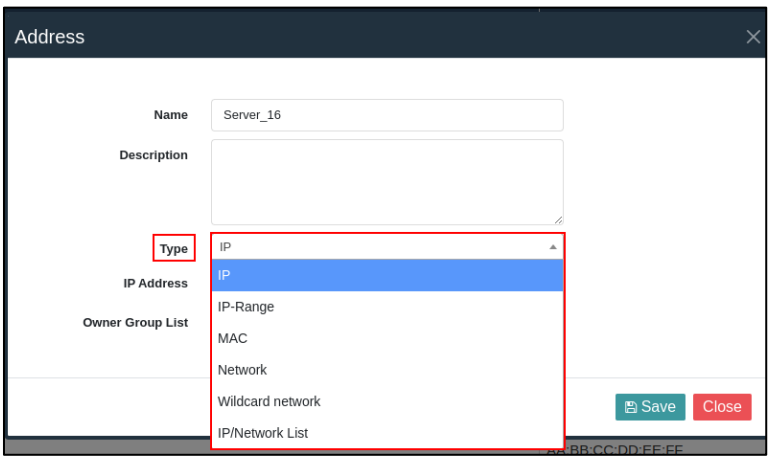
16.1.1 Address

The IP Address, IP-Range, MAC Address, Network Address, Wildcard Network, and IP/Network List objects to be used in the Policies module are added.

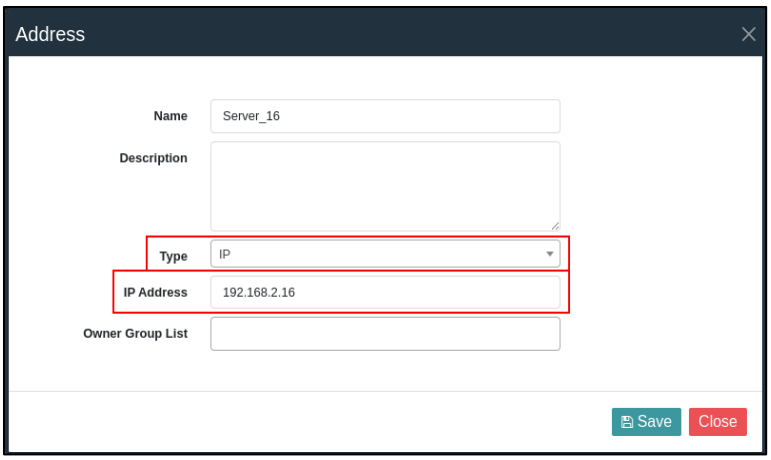


1	**Add**	IP Address, IP-Range, MAC Address, Network Address, Wildcard Network, and IP/Network List are added.
2	**Type**	This is the section where the type of the added address is displayed.
3	**Name**	This is the section where the name given to the added address is displayed.
4	**Address**	This is the section where the information about the added address is displayed.
5	**Manage**	This is the section where the information about the added address is changed or deleted. Addresses added by the system cannot be deleted or changed.

-Click on the 'add' button to add an address. After clicking the 'Add' button, the type of address you want to add is selected on the screen that appears. As the address type, it is selected from one of the options: IP, IP-Range, MAC, Network, Wildcard Network, and IP/Network List.

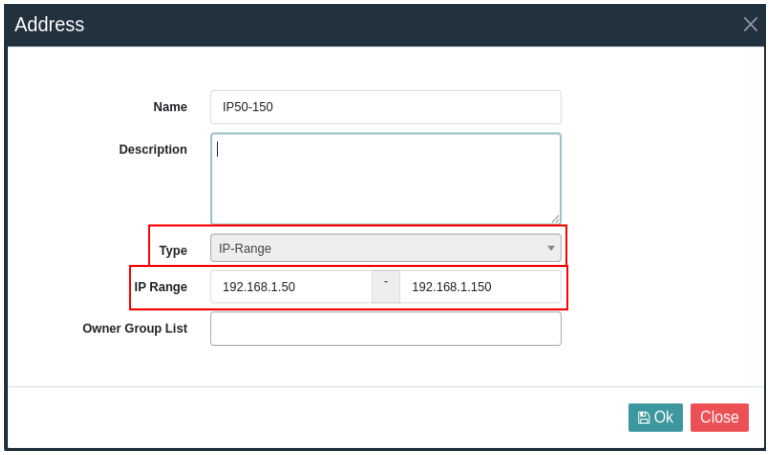


- If the address type is selected as IP, the address to be added is a single IP address. For example: 192.168.1.6.



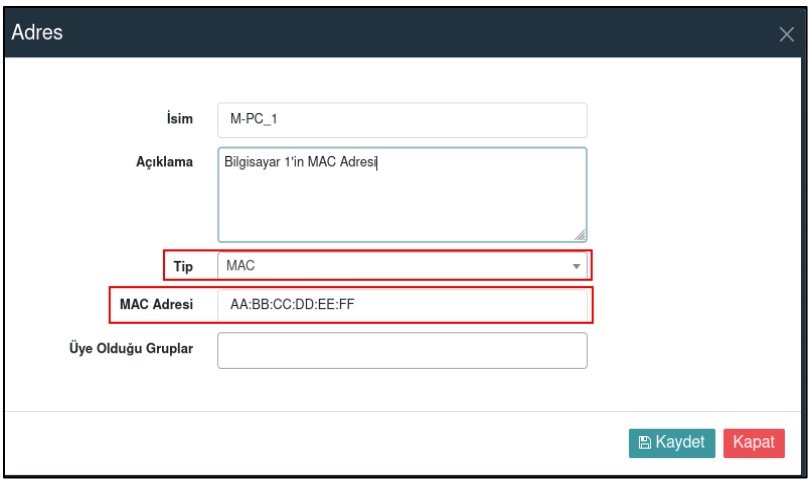
IP Address	S-Web_6	192.168.1.6

- If the address type is selected as IP-Range, the address for the specific IP range is added. For example: 192.168.1.50 - 192.168.1.150,

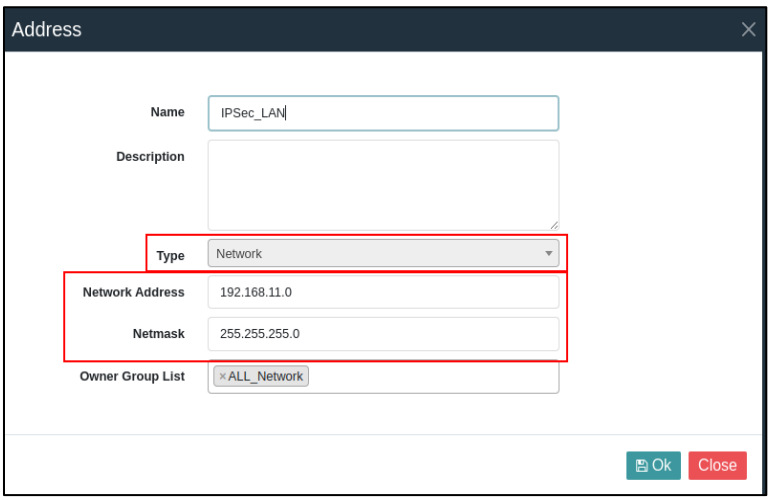


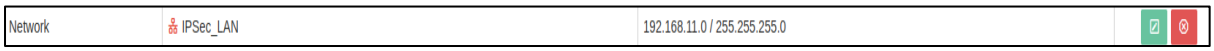
IP Range	IP50-150	192.168.1.50 - 192.168.1.150

- If the address type is selected as MAC Address, the MAC Addresses of the devices are added. For example: AA:BB:CC:DD:EE:FF.

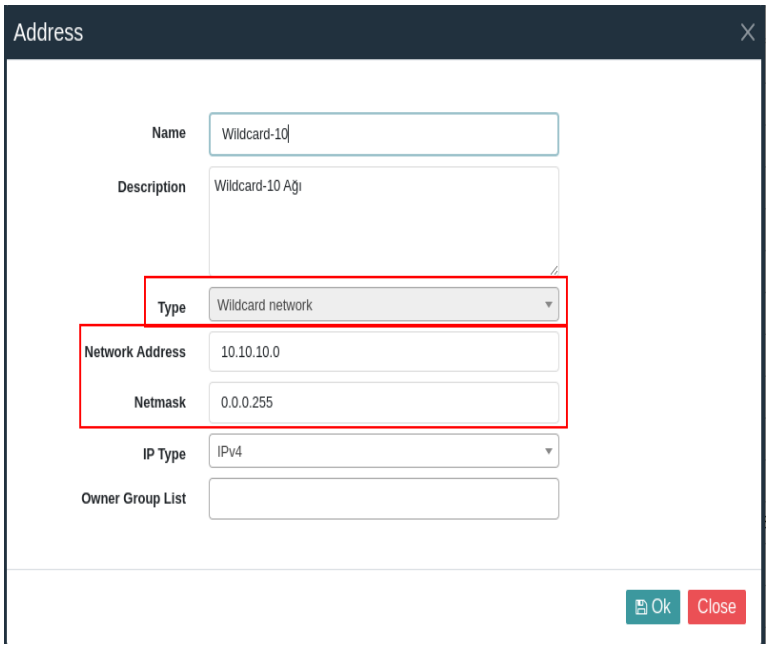


- If the address type is selected as Network, the Network Addresses of the devices are added. For Example: 192.168.11.0 / 255.255.255.0



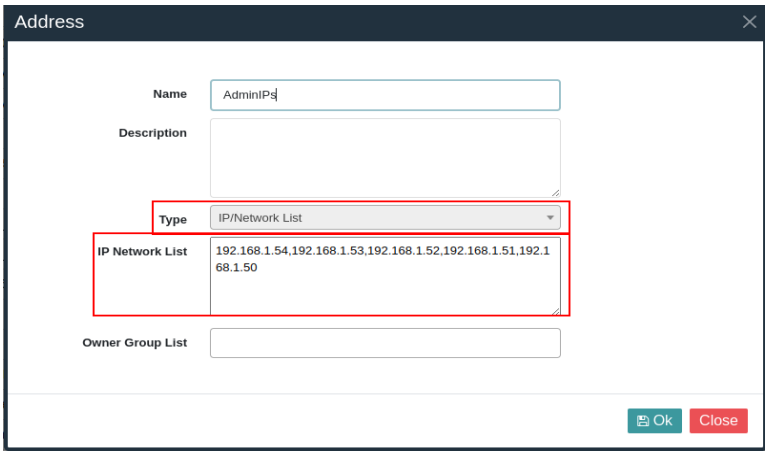


- If the address type is selected as Wildcard network, the Wildcard network Addresses of the devices are added. For example: 10.10.10.0 / 0.0.0.255



Wildcard Network	Wildcard-10	10.10.10.0 / 0.0.0.255

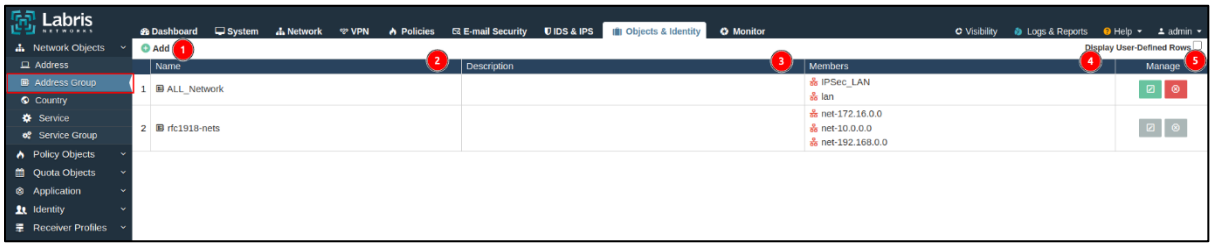
- If the address type is selected as IP List, more than one IP address is added. For example: 192.168.1.50, 192.168.1.51, 192.168.1.52, 192.168.1.53.



IP List	AdminIPs	192.168.1.54,192.168.1.53,192.168.1.52,192.168.1.51,192.168.1.50	

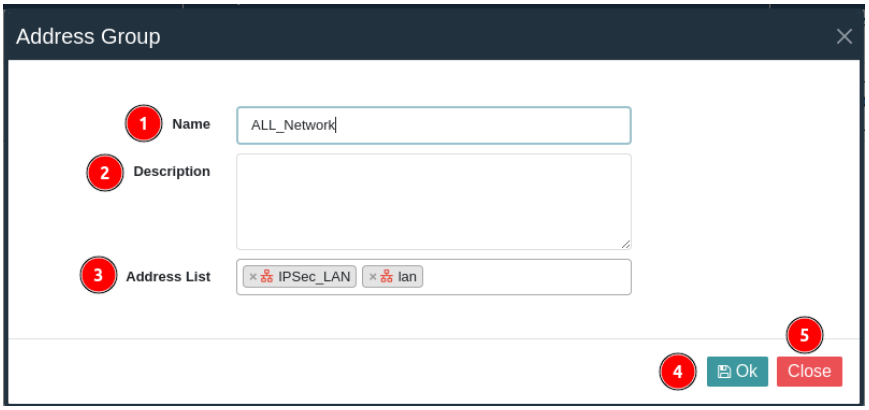
16.1.2 Address Group

It is the module where the objects added as addresses are grouped. IP addresses that are related to each other are grouped into the rules written in the Policies module.



1	**Add**	This is the button used to group the addresses added in the address module.
2	**Name**	This is the section where the name of the added address group is displayed.
3	**Description**	This is the section where the description of the added address group is displayed.
4	**Members**	This is the section where the members added to the address group are displayed.
5	**Manage**	This is the section where the information about the added address groups is changed or deleted. Address groups added by the system cannot be deleted or modified.

-Click the 'add' button to add an address group. After clicking the Add button, the addresses added in the Address module are grouped on the screen that opens.

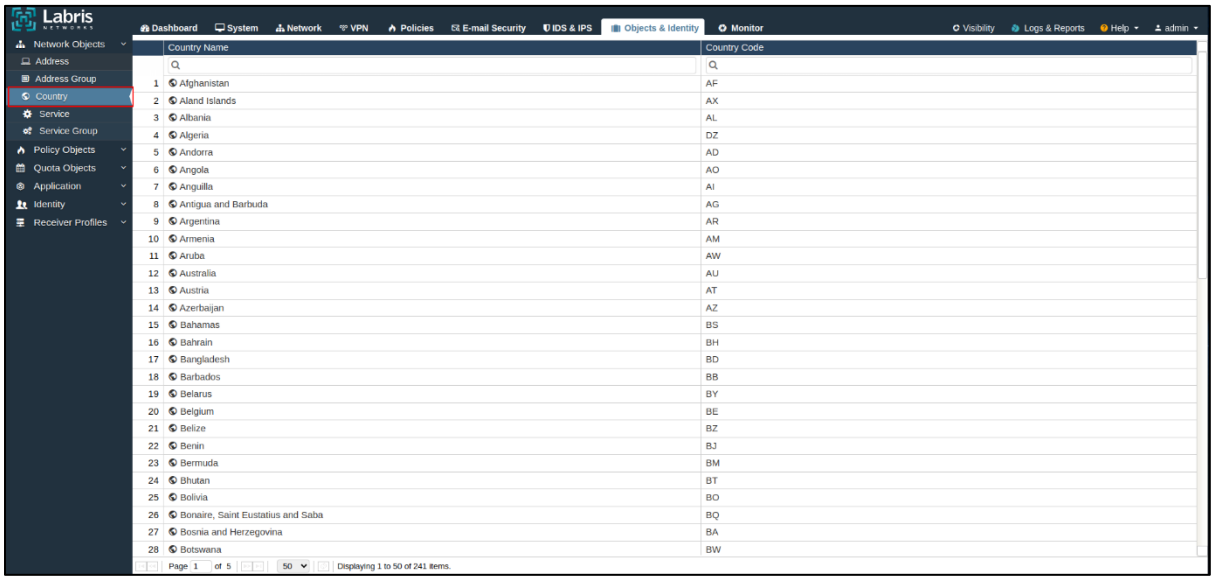


1	**Name**	It is the section where the name given to the added

		address group is entered.
2	**Description**	This is the section where the description given to the added address group is entered.
3	**Address List**	This is the section where the address is added to the added address group.
4	**Save**	This is the button where the address group is saved.
5	**Close**	This is the button where the screen that opens after pressing the 'Add' button is closed.

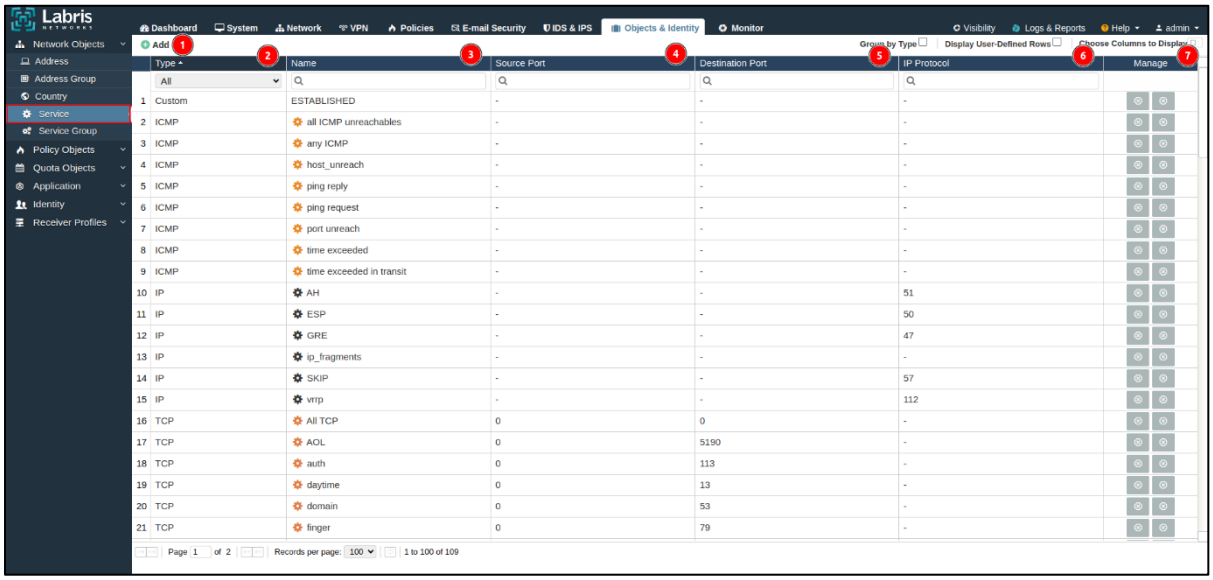
16.1.3 Country

This is the section where the countries in the database are displayed.



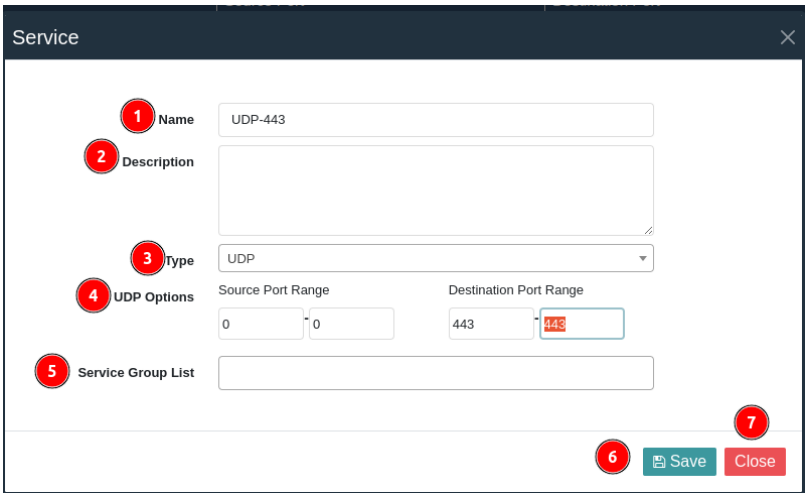
16.1.4 Service

This is the section where the attached services on the device are displayed and new services are added.



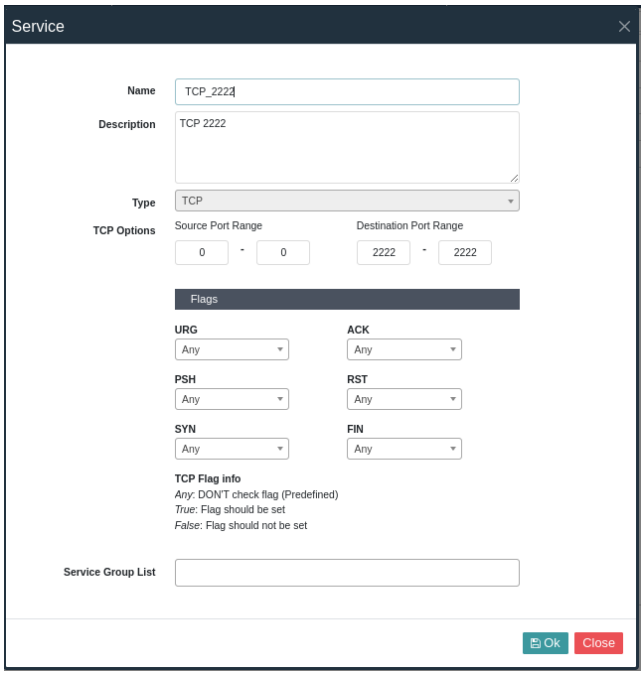
1	**Add**	This is the button where TCP, UDP, IP, and ICMP services are added.
2	**Type**	This is the section where the type of service added is displayed.
3	**Name**	This is the section where the name given to the added service is displayed.
4	**Source Port**	This is the section where the source port number of the added Service is displayed.
5	**Destination Port**	This is the section where the destination port number of the added service is displayed.
5	**IP Protocol**	This is the section where the port number of the added ICPM service is displayed.
6	**Manage**	It is the section where the information of the Added Services is changed or deleted. Services added by the system cannot be deleted or changed.

-To add a service, click the 'add' button. The service is added by filling in the information on the screen.



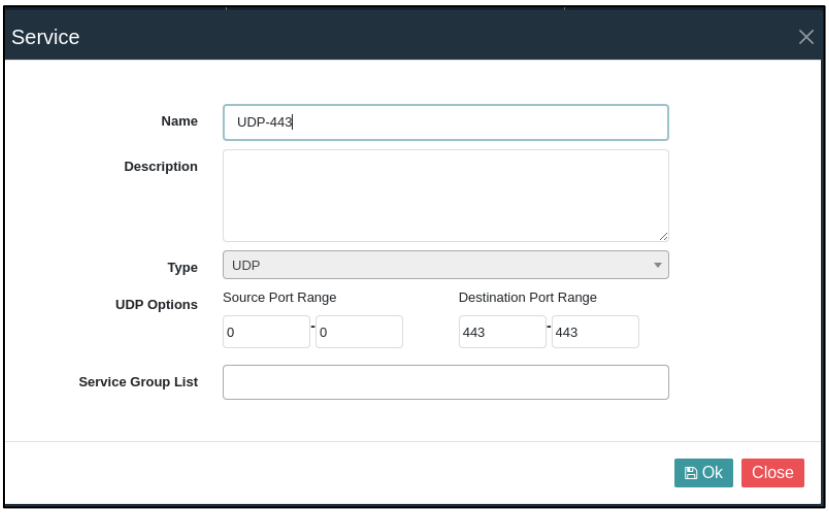
1	**Name**	This is the section where the name of the service to be added is entered.
2	**Description**	This is the section where the type of service added is displayed.
3	**Type**	Select the type of service to be added. TCP, UDP, ICMP, and IP types are available.
4	**Options for Type**	It varies according to the type selected.
5	**Service Group List**	This is the section where the group to which the service to be added will be included is selected.
6	**Save**	This is the button where the service information is saved.
7	**Close**	It is the button that is removed from the screen that opens.

-If the service type TCP is selected, the TCP Service is added. Source Port, Destination Port, and TCP flags are arranged according to their information.



TCP	TCP_2222	0	2222	-

-If the service type UDP is selected, the UDP Service is added. It is arranged according to the Source Port and Destination Port information.



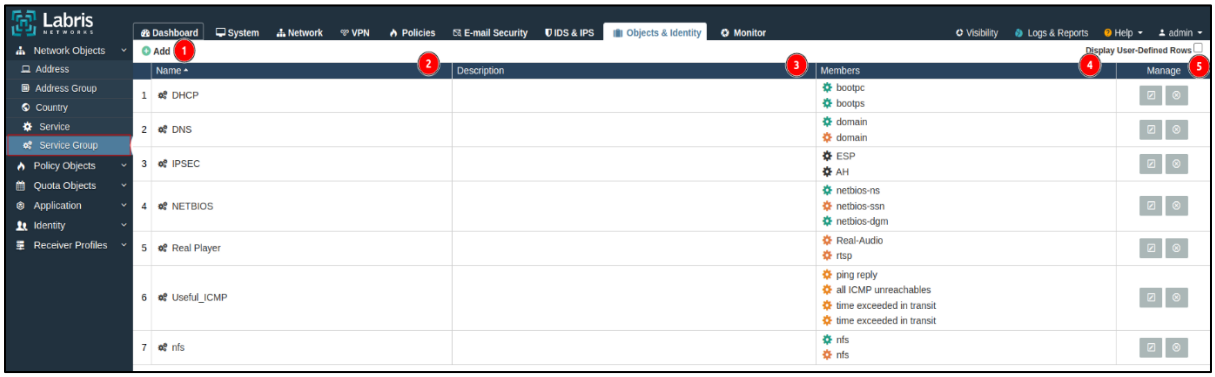
UDP	UDP-443	0	443	-

-If the service type IP is selected, the IP Service is added according to the number of IP Protocols.

-If the service type is ICMP, ICMP options (Echo Reply, Destination Unreachable, etc.) The addition process is done accordingly.

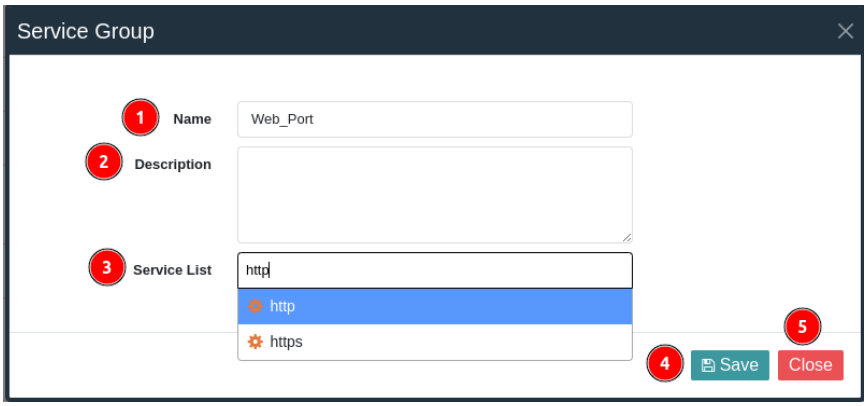
16.1.5 Service Group

It is the module where the grouping of the added services is made.



1	**Add**	It is the button where the added services are grouped.
2	**Name**	This is the section where the name of the added service group is displayed.
3	**Description**	This is the section where the description of the service group is displayed.
4	**Members**	This is the section where the list of services added to the service group is displayed.
5	**Manage**	This is the section where the added service group is deleted or edited. By default, no edits are made to the service groups that come on the device.

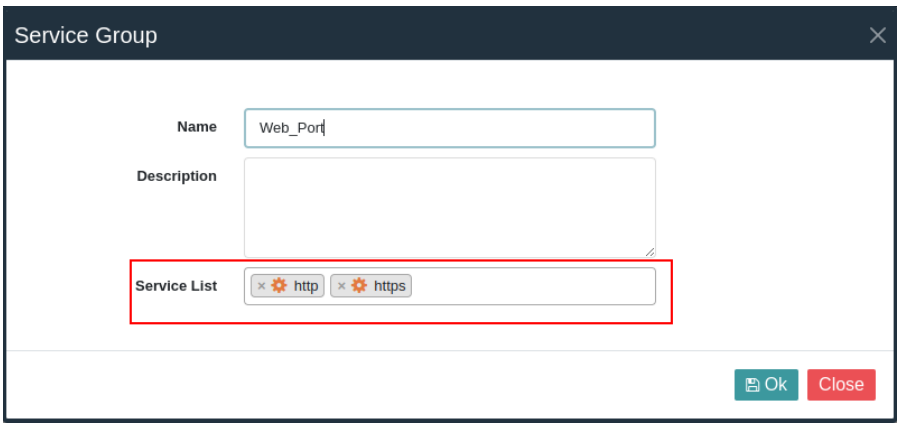
-After clicking the 'add' button to add a Service Group, the Services on the Labris UTM device are grouped.



1	**Name**	This is the section where the name to be given to the services to be grouped is specified.
2	**Description**	This is the section where a description is entered into the service group to be added.
3	**Service List**	It is the section where the services on the device or the added services are selected.
4	**Save**	It is the button where the grouped services are saved.
5	**Close**	It is the button where the screen that opens after pressing the 'Add' button is closed.

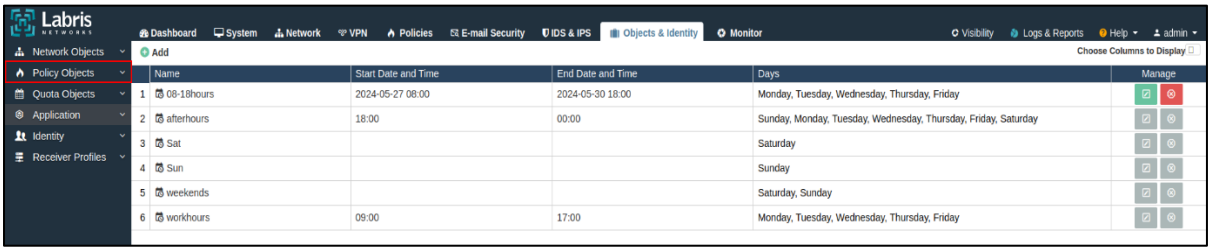
Note

The services added to the Service Group are in the screen below.



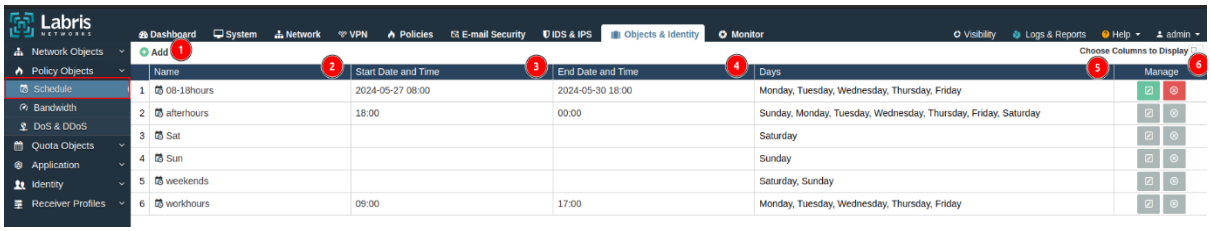
16.2 Policy Objects

It is the module where the Policy Objects to be used in the Policies module are created. In the Policy Objects menu, add Schedule, Bandwidth, and DoS&DDoS objects.



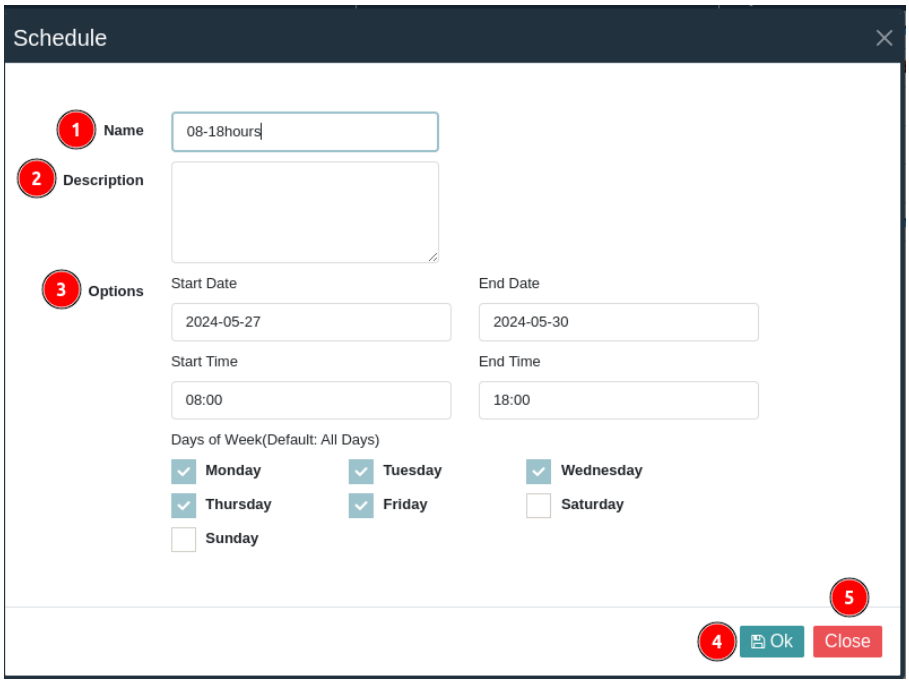
16.2.1 Schedule

It is the module where a schedule object is added to be used in the General Policy module in the Policies module or the time objects that come by default on the Labris UTM device are displayed. The schedule objects that are added to the rule in the inbound policy module specify the runtime of the rule.



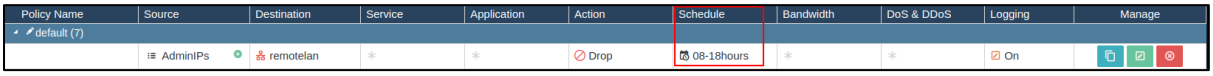
1	**Add**	It is the button where the time object is added.
2	**Name**	The name of the added time objects is displayed.
3	**Start Date and Time**	This is the section where the start date and time of the added time objects are displayed.
4	**End Date and Time**	This is the section where the end date and time of the added time objects are displayed.
5	**Days**	This is the section where the selected days are displayed in the added time objects.
6	**Manage**	Inserted is the section where the time object is edited or deleted. By default, time objects on the device can't be deleted or edited.

-Click the 'add' button to add a Time object. After clicking the button, select the start and end time, or days.



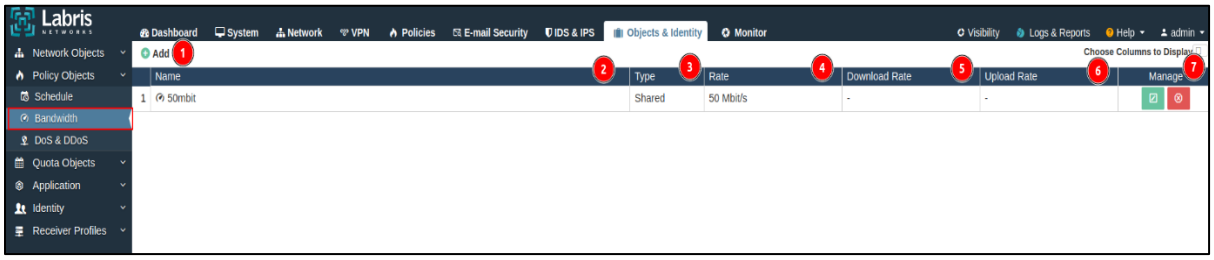
1	**Name**	This is the section where the name of the schedule object to be added is entered.
2	**Description**	This is the section where the description of the Time to Insert object is entered.
3	**Options**	Start and end dates, times, and days of the week are selected for the rule to run.
4	**Save**	This is the button where the time object is saved.
5	**Close**	It is the button where the screen opens by clicking the 'Add' button is closed.

-The use of the object added as a time object in the general policy is as follows.



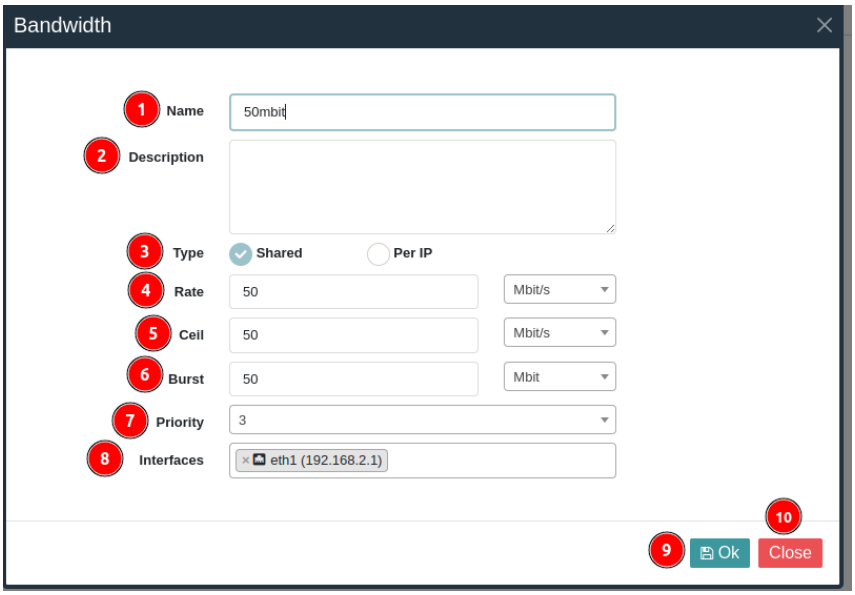
16.2.2 Bandwidth

The bandwidth object is defined for use in the General Policy module. Adding a Bandwidth object is used to control the bandwidth of internal network.



1	**Add**	This is the button where the bandwidth object is added.
2	**Name**	This is the section where the name of the added bandwidth object is displayed.
3	**Type**	This is the section where the type of the bandwidth object is displayed. There are two types: shared and common.
4	**Rate**	This is the section where the rate of the bandwidth object is displayed.
5	**Download Rate**	This is the section where the download rate of the bandwidth object is displayed.
6	**Upload Rate**	This is the section where the upload rate of the bandwidth object is displayed.
7	**Manage**	This is the section where the added bandwidth object is deleted or edited.

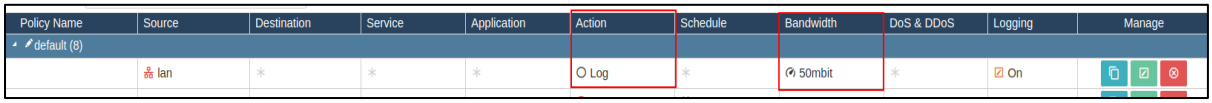
-To add a Bandwidth object, click the 'add' button. After clicking the button, adjustments are made by specifying the type of bandwidth.



1	**Name**	This is the section where the name of the bandwidth object is entered.
2	**Description**	This is the section where the description of the bandwidth object is entered.
3	**Type**	This is the section where the type of the bandwidth object is selected. If shared is selected, it divides the specified value for everyone involved in the network. For example, if 50Mbps is selected and there are 50 users on the network, the devices connected to the network bandwidth is 1 Mbps (50/50 = 1Mbps). If Per IP is selected, it is user-based and the bandwidth of the connecting user is fixed.
4	**Rate**	This is the value entered if the type is selected as shared. Internet speed is indicated.
5	**Cell**	This is the value entered if the type is selected as shared. The ceiling value of the bandwidth is entered.
6	**Burst**	This is the value entered if the type is selected as shared. The breakthrough value of the bandwidth is entered.

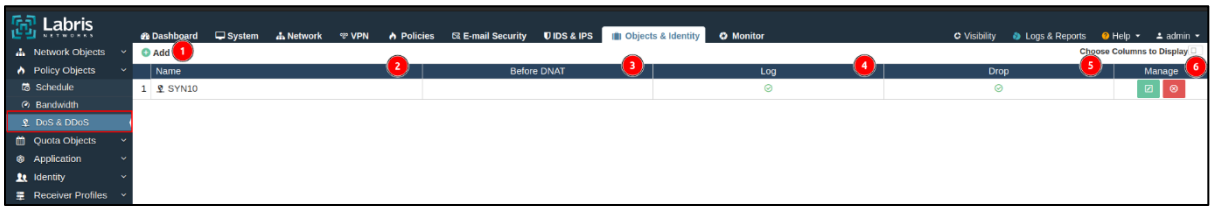
7	**Priority**	This is the value entered if the type is selected as shared. The priority value of the bandwidth is entered.
8	**Interface**	This is the value entered if the type is selected as shared. The interface to which the bandwidth will be applied is selected.
9	**Save**	This is the button where the bandwidth settings are saved.
10	**Close**	This is the button where the window opened by clicking the 'Add' button is closed.

-**The use** of the bandwidth object in the **general policy** is as follows.



16.2.3 DoS&DDoS

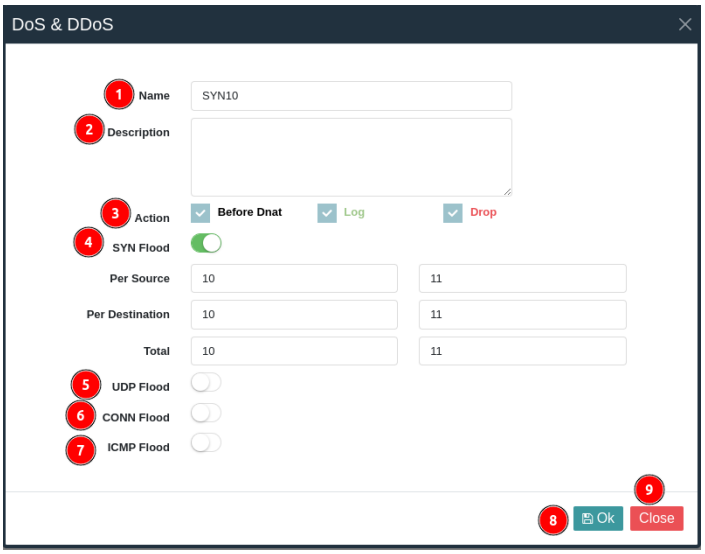
A DoS&DDoS object is defined for use in the General policy module. It protects the services running on the internal network according to the exact values of the DoS&DDoS object.



1	**Add**	This is the section where the name of the DoS&DDOS object is entered.
2	**Name**	This is the section where the description of the DoS&DDOS object is entered.
3	**Before DNAT**	This is the section where information is given about whether the object was running before the DNAT operation.
4	**Log**	This is the section where the DoS&DDoS object is shown to be logged in case of blocking.

5	**Drop**	This is the section where the blocking process of the DoS&DDoS object is shown.
6	**Manage**	This is the partition where the DoS&DDoS object is deleted or managed.

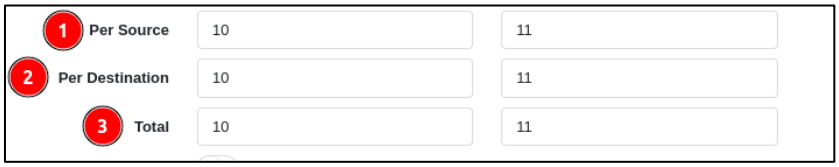
-To add a DoS&DDoS object, click the 'add' button. After clicking the button, the attacks to be prevented by the DoS&DDoS object to be added are selected. These are SYN, UDP, Link, and ICMP attacks.



1	**Name**	This is the section where the name of the DoS&DDoS object is entered.
2	**Description**	This is the section where the description of the DoS&DDoS object is entered.
3	**Action**	The process of the DoS&DDoS object is selected.
4	**Syn Flood**	Enter the values that the DoS&DDoS object will detect as a Syn Flood attack.
5	**UDP Flood**	Enter the values that the DoS&DDoS object will detect as a UDP Flood attack.
6	**CONN Flood**	Enter the values that the DoS&DDoS object will detect as a Connection (CONN) Flood attack.

7	**ICMP Flood**	Enter the values that the DoS&DDoS object will detect as an ICMP Flood attack.
8	**Save**	This is the button where the DoS&DDoS object is saved.
9	**Close**	This is the button where the screen that opens after clicking the 'Add' button is closed.

- In cases of SYN, UDP, Connection, and ICMP Attack, the DoS&DDoS object is set per source, per target, and total incoming requests.

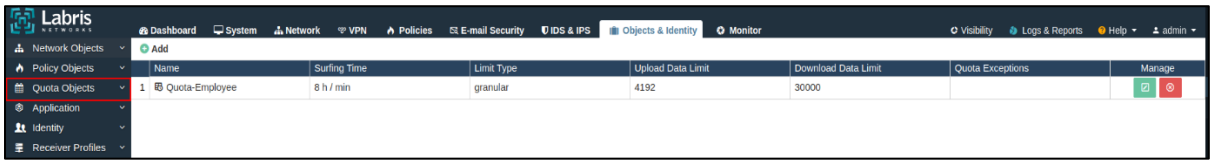


1	**Per Source**	This is the section where the number of requests per source is specified.
2	**Per Destination**	This is the section where the number of requests per destination is specified.
3	**Total**	This is the section where the total number of requests is specified.

-The use of the DoS&DDoS object in the general policy is as follows.

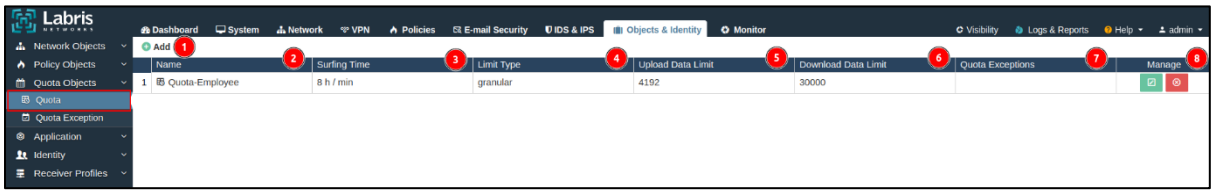
16.3 Quota Objects

This is the section where Quota Objects to be used in the Policies module are created. Quota and Quota Exception objects are added in the Quota Objects menu.



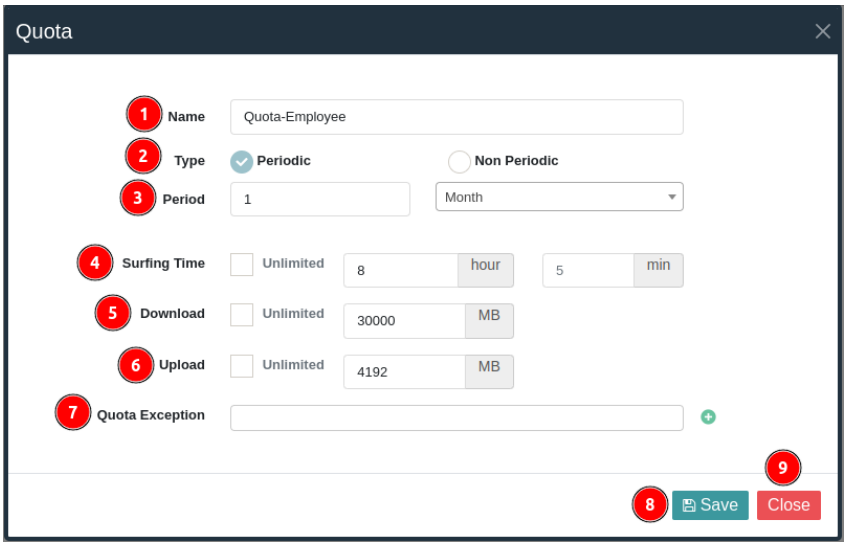
16.3.1 Quota

If you want to add a quota object to the users added in the Objects and Identities module, it is necessary to create a Quota object. The user added in the Objects and Identities module can surf the internet according to the quota policy set when logged in to Wauth.



1	**Add**	This is the button where the quota object is added.
2	**Name**	This is the section where the name of the quota object is displayed.
3	**Surfing Time**	This is the section where the browsing time of the user to who the quota policy is applied is displayed.
4	**Limit Type**	This is the section where the limit type of the quota object is displayed.
5	**Upload Data Limit**	This is the section where the upload limit of the quota object is displayed.
6	**Download Data Limit**	This is the section where the download limit of the quota object is displayed.
7	**Quota Exceptions**	This is the section where the quota exception is selected. To use this section, it is necessary to add a quota exception.
8	**Manage**	This is the section where the added quota exception is deleted or edited.

-To add a quota object, click the 'add' button. After clicking the button, the web browsing, upload, and download values of the Quota object to be added are specified.

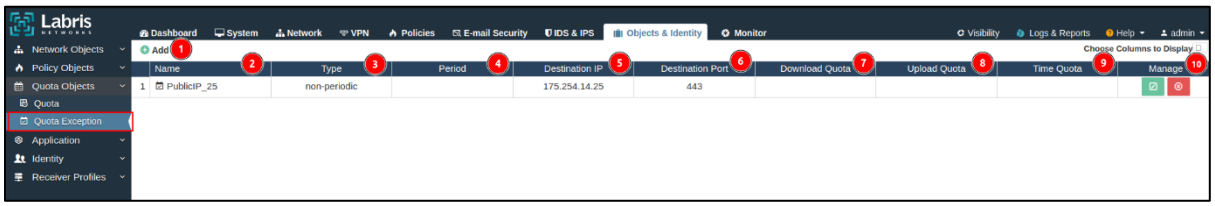


1	**Name**	This is the section where the name of the quota object is entered.
2	**Type**	This is the section where the type of the quota object is selected. If periodic is selected, the quota object is reset for the specified period. If non periodic is selected, the quota object runs only at the specified time.
3	**Period**	It is set if the periodic option is selected, configurations are as day, week, month, and year.
4	**Surfing Time**	The duration of the Internet browsing is indicated. In case of marking unlimited, the time of surfing the Internet is unlimited.
5	**Download**	The download limit for the quota object is specified. The download limit is unlimited if it is marked unlimited.
6	**Upload**	The upload limit of the quota object is specified. If it is marked unlimited, the upload limit is unlimited.
7	**Quota Exceptions**	This is the section where the quota exception is selected. To use this section, it is necessary to add a quota exception.

8	**Save**	This is the button where the quota object is saved.
9	**Close**	It is the button where the screen that opens after pressing the 'Add' button is closed.

16.3.2 Quota Exception

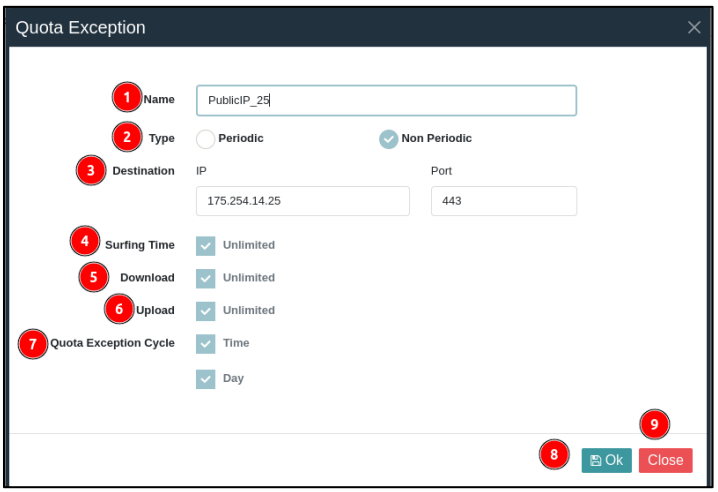
In the quota exception module, an exception is defined that will not be stuck in the quota policy during Internet browsing. When defining an exception, the destination IP address and Port information must be known.



1	**Add**	It is the button used to add a quota exception.
2	**Name**	This is the section where the name of the quota exception is displayed.
3	**Type**	This is the section where the type of quota exception is displayed.
4	**Period**	This is the section where the time to be spent on the destination IP address is displayed. If it appears as empty, it is unlimited.
5	**Destination IP**	This is the section where the Destination IP address for which the quota exception is written is displayed.
6	**Destination Port**	It is the section where the Destination Port for which the quota exception is written is displayed.
7	**Download Quota**	It is the section where the download quota is specified specific to the destination IP address.
8	**Upload Quota**	This is the section where the upload quota specific to the destination IP address is displayed.

9	**Time Quota**	This is the section where the time quota specific to the destination IP address is displayed.
10	**Manage**	This is the section where the quota exception is edited or deleted.

-To add a quota exception, click the 'add' button.

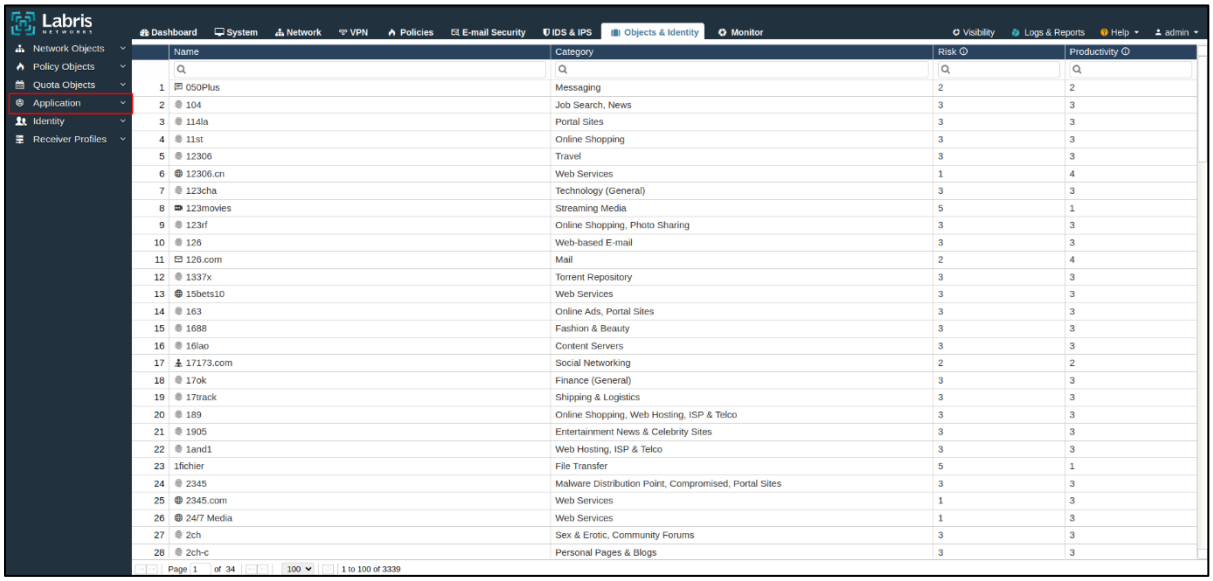


1	**Name**	This is the section where the name of the quota exception is displayed.
2	**Type**	This is the section where the type of quota exception is selected.
3	**Destination IP/Port**	It is the section where the IP address or port information to be written quota exception is entered.
4	**Surfing Time**	This is the section where the surfing time at the specified destination IP address is specified.
5	**Download**	This is the section where the download limit at the specified Destination IP address is specified.
6	**Upload**	This is the section where the upload limit at the specified Destination IP address is specified.
7	**Quota Exception Cycle**	This is the section where the frequency of repetition of the quota exception is specified.

8	**Save**	It is the button where the quota exception is saved.
9	**Close**	‘It is the button where the screen that opens after pressing the 'Add' button is closed.

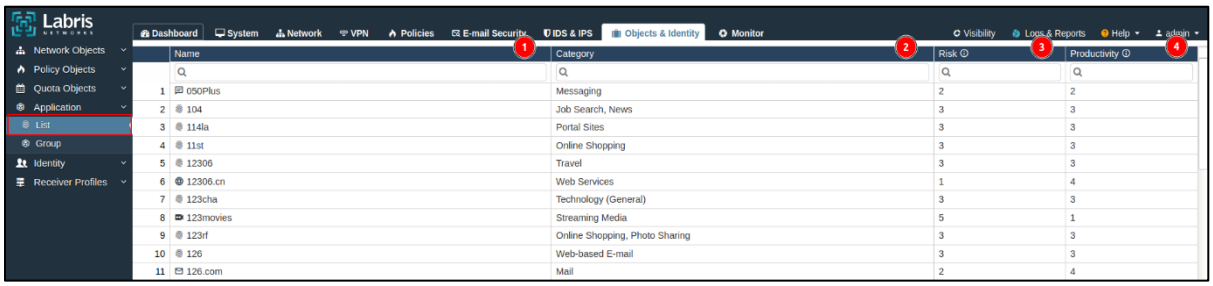
16.4 Application

It is the module where the applications kept on the Labris UTM device are displayed. Applications in this module are used in the Policies module.



16.4.1 List

It is the module where the list of applications stored on the Labris UTM device is displayed.

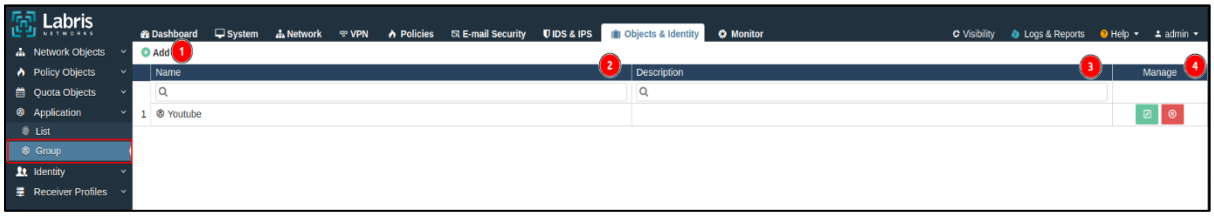


1	**Name**	This is the section where the names of the applications are displayed.
2	**Category**	This is the section where the categories of applications are displayed.

3	**Risk**	This is the section where the risk values of the applications are displayed. The risk level indicates that undesirable situations may occur while using the application.
4	**Productivity**	This is the section where the efficiency values of the applications are displayed. Productivity is the ratio of whether the app is used for entertainment or work.

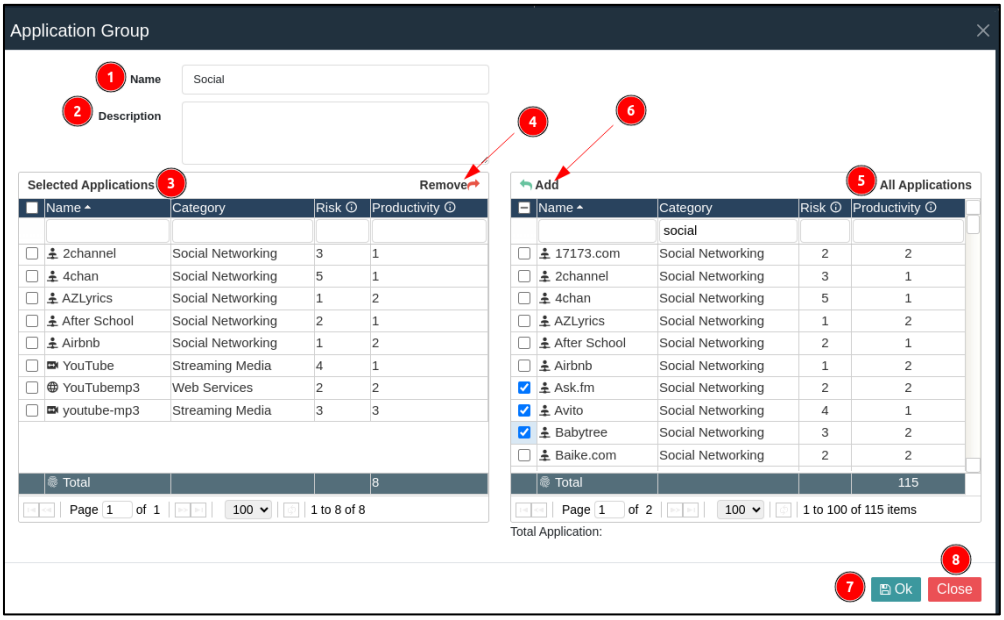
16.4.2 Group

It is the module in which the applications in the application list are grouped.



1	**Add**	It is the button where the application group is added.
2	**Name**	This is the section where the name of the application group is displayed.
3	**Description**	This is the section where the description of the application group is displayed.
4	**Manage**	This is the section where the application group is edited or deleted.

-It is necessary to click on the 'add' button. After clicking the button, the applications on the Labris UTM device are grouped.

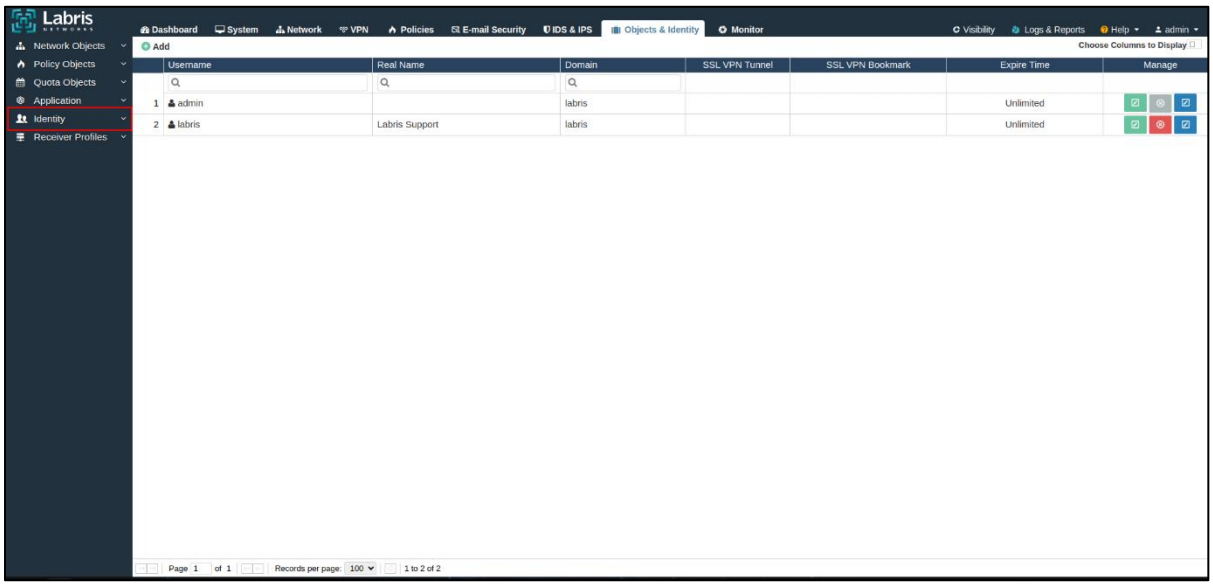


1	**Name**	This is the section where the name of the application group is entered.
2	**Description**	This is the section where the description of the application group is entered.
3	**Selected Applications**	This is the section where the applications added from the All Applications list are displayed.
4	**Remove**	It is the button where the selected application is removed from the list of selected applications.
5	**All Applications**	It is the button that displays the list of applications on the Labris UTM device.
6	**Add**	This is the button where the applications selected from the list of all applications are added to the list of Selected Applications.
7	**Save**	It is the button where application groups are saved.
8	**Close**	It is the button where the screen that opens after

		clicking the 'Add' button is closed.

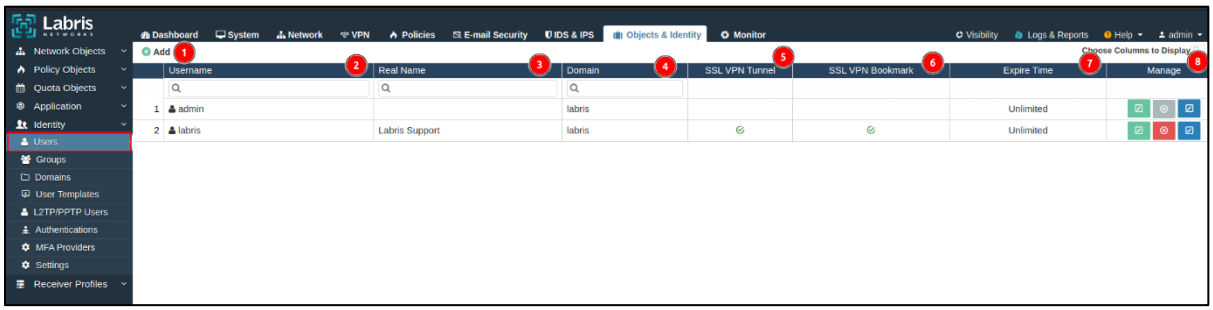
16.5 Identity

On the Labris UTM device, users can be grouped, users' field names can be changed, and user templates can be created. Also, users can be created for L2TP/PPTP VPN, users on the Active Directory server can be withdrawn, and the MFA provider to be used in SSLVPN is added and it is the module where the Identity Settings are made.



16.5.1 Users

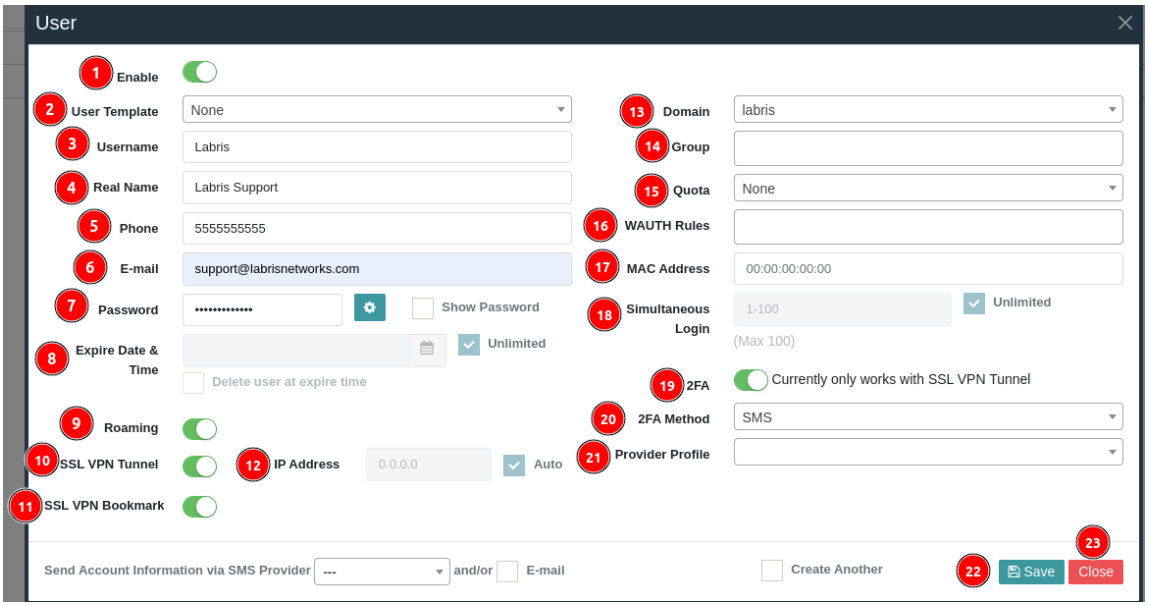
This is the section where the process of adding users to the Labris UTM device is done. Users added to this module are given admin authority to log in to the Labris UTM device. The necessary authorization is made to connect to the SSL VPN. In addition, created users can log in to WAUTH.



1	**Add**	This is the button where users are added to the Labris UTM device.
2	**User Name**	The section where the username of the added user is displayed. Users can log in to SSL VPN and Labris

		Web Interface using their username.
3	**Real Name**	This is the section where the real name of the added user is displayed.
4	**Domain Name**	The domain name of the added user is displayed.
5	**SSL VPN Tunnel**	This is the section where it is displayed whether the added user has SSL VPN authorization or not.
6	**SSL VPN Bookmark**	This is the section where it is displayed whether the added user has SSL VPN Bookmark authorizationor not.
7	**Expire Time**	This is the section where the expiration date of the added user's account is displayed.
8	**Manage**	It is the section where the added user edits, deletes, and resets their quotas.

-Click the 'add' button to add a user. After clicking the button, the user adding process is completed by filling in the information about the user in the window that opens.

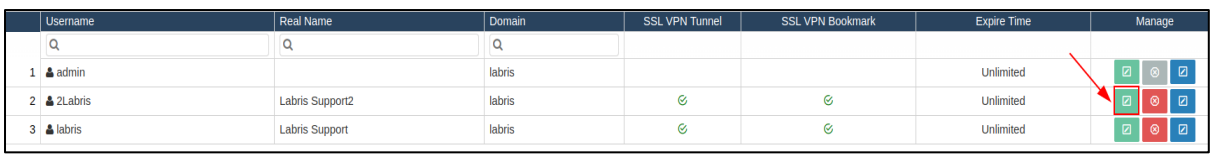


1	**Enable**	It is the button where the user to be added is activated.

2	**User Template**	This is the section where the added user template is selected.
3	**Username**	This is the section where the username of the user to be added is entered.
4	**Real Name**	This is the section where the real name of the user to be added is entered.
5	**Phone**	This is the section where the user's phone number is entered.
6	**E-mail**	This is the section where the user's e-mail address is entered.
7	**Password**	This is the section where the user's password is entered. It is necessary to click on the 'wheel' button to give the password randomly.
8	**Expire Date & Time**	This is the section where the date on which the user's account will be expire is selected.
9	**Roaming**	It is the button where the user is authorized to roam.
10	**SSL VPN Tunnel**	It is the button where the user is authorized to log in to SSL VPN.
11	**SSL VPN Bookmark**	It is the button where the user is authorized to log in to SSL VPN Bookmark.
12	**IP Address**	This is the section where the IP address that the user receives when connected to SSL VPN is specified. If you want to write an IP address, the check in the automatic must be removed.
13	**Domain**	It is the button where the domain name of the user is selected.
14	**Group**	This is the section where the group to which the user

		is to be added is selected.
15	**Quota**	In cases where a quota policy will be applied to the user, the added quota object is selected.
16	**Wauth Rules**	If there is a WAUTH rule written for the user, the WAUTH rule is selected.
17	**MAC Address**	This is the section where the user's MAC address information is entered.
18	**Simultaneous Login**	This is the section where the number of simultaneous sessions for the user is set.
19	**2FA**	It is the button that allows the user to enter two-factor authentication to verify the identity information when logging into SSL VPN.
20	**2FA Methods**	This is the section where the 2FA method is selected.
21	**Providers Profiles**	This is the section where the 2FA provider information is selected.
22	**Save**	It is the button where the information of the user to be added is saved.
23	**Close**	It is the button where the window opened by clicking the 'Add' button is closed. When the Close button is pressed, it closes the changes made for the user without saving them.

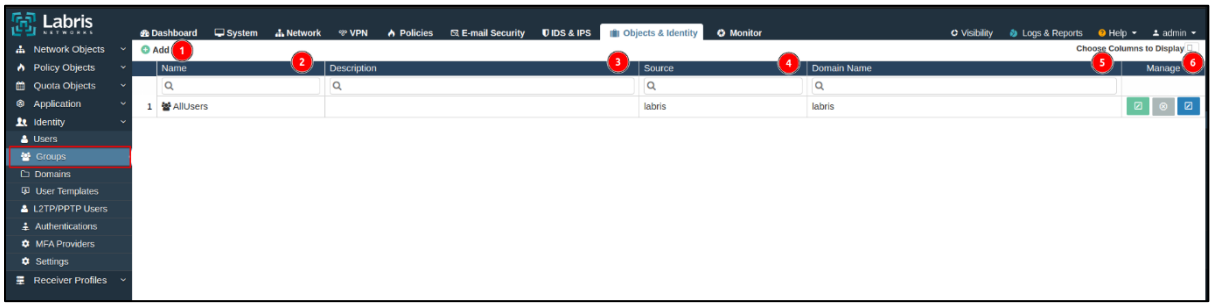
-Click the edit button in the Manage section to change the information of the added user.



-After pressing the button, users' information can be edited.

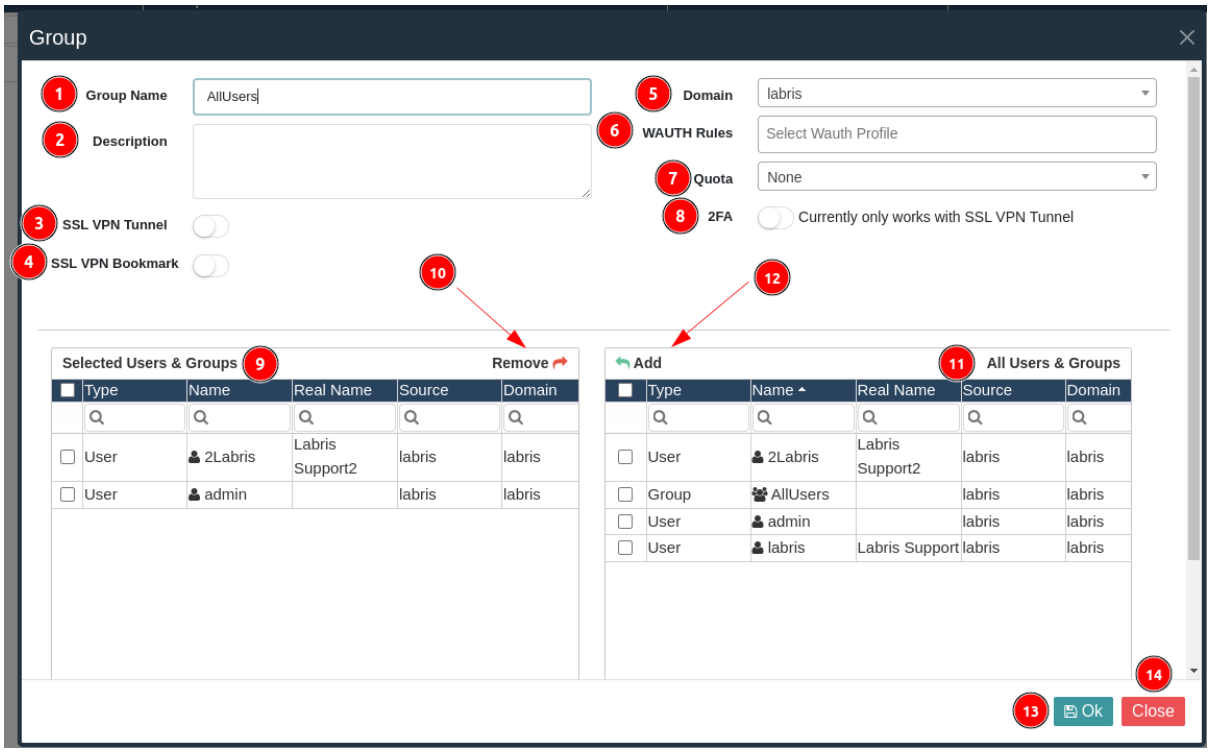
16.5.2 Groups

This is the section where the added users are grouped. All users included in the group are granted SSL VPN, Quota, or Wauth privileges.



1	**Add**	It is the button where the process of adding a user group is made.
2	**Name**	This is the section where the name of the user group is displayed.
3	**Description**	This is the section where the description of the user group is displayed.
4	**Source**	This is the section where the source information of the user group is displayed.
5	**Domain Name**	This is the section where the domain name of the user group is displayed.
6	**Manage**	This is the section where the user group is edited, deleted, or their quota is reset.

-Click on the 'add' button to add a user group. After clicking on the button, the group information to be added or the added users will be grouped.

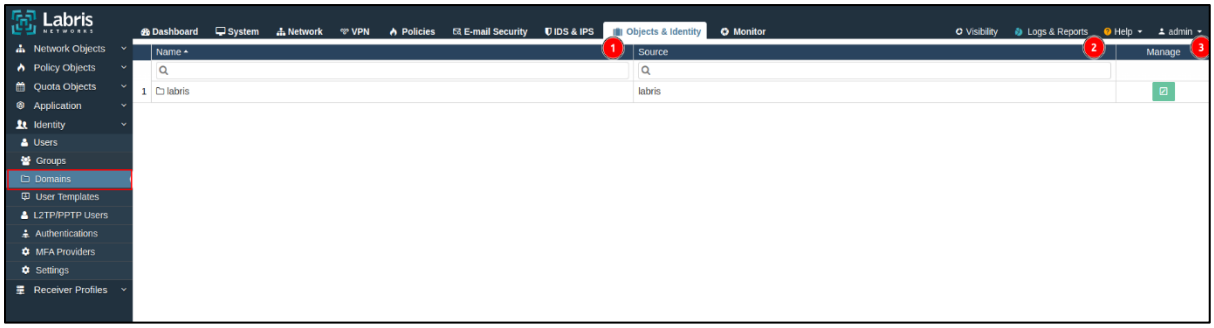


1	**Group Name**	This is the section where the group name of the group to be added is entered.
2	**Description**	This is the section where the description of the group to be added is entered.
3	**SSL VPN Tunnel**	It is the button where the users added to the group are given SSL VPN authorization.
4	**SSL VPN Bookmark**	It is the button where the users added to the group are given SSL VPN Bookmark authorization.
5	**Domain**	This is the section where the field name of the group to be added is selected.
6	**Wauth Rules**	This is the section where the WAUTH Rule of the Group to be added is selected.
7	**Quota**	This is the section where the Quota object is selected for the users included in the group.

8	**2FA**	This is the section where two-factor authentication is turned on for users who are included in the group.
9	**Selected Users & Groups**	This is the section where the users included in the group are displayed.
10	**Remove**	It is the button where the users and groups included in the group are removed.
11	**All Users & Groups**	This is the section where all added users and groups are displayed.
12	**Add**	It is the button where selections from all Users and Groups are used to include them in the group.
13	**Save**	This is the button where the user group is saved.
14	**Close**	It is the button where the window that opens after clicking the 'Add' button is closed.

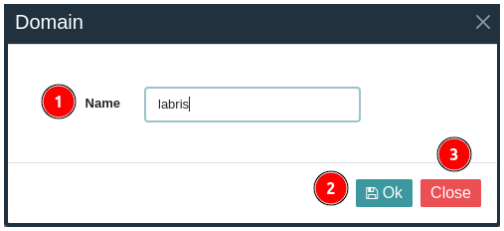
16.5.3 Domains

It is the section where the domain name that comes by default in the Labris UTM device is displayed or edited.



1	**Name**	This is the section where the name of the domain name is displayed.
2	**Source**	This is the section where the domain name is displayed.
3	**Manage**	This is the section where the domain name is changed.

-To edit the Domain Name, click the 'edit' button.



1	**Name**	This is the section where the name of the domain name is changed.
2	**Save**	It is the button where the changed domain name is saved.
3	**Close**	It is the button that closes the window that opens without changing the domain name.

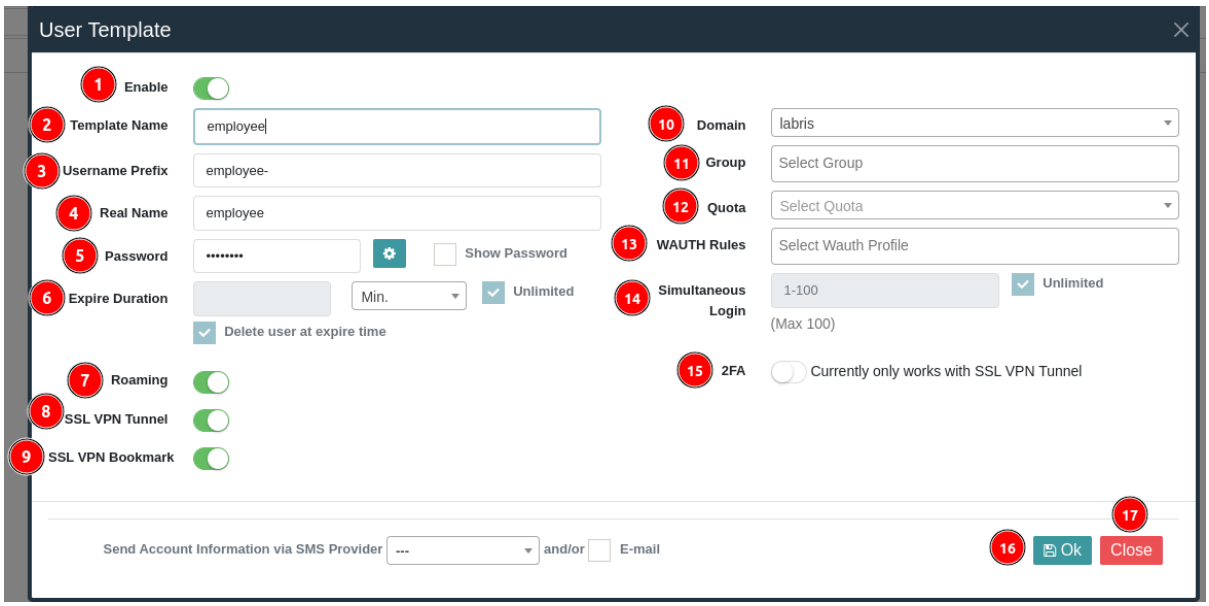
16.5.4 User Templates

It is the module used for the creation of users according to the user template.

1	**Add**	It is the button where the user template is added.
2	**Template Name**	This is the section where the template name is displayed.
3	**Username Prefix**	This is the section where the username prefix of the added user template is displayed.
4	**Domain**	This is the section where the domain name of the user template is displayed.
5	**SSL VPN Tunnel**	This is the section where the SSL VPN Tunnel authority of the user template is displayed.

6	**SSL VPN Bookmark**	This is the section where the SSL VPN Bookmark authority of the user template is displayed.
7	**Expire Duration**	This is the section where the expiration date of the user's account added according to the user template is displayed.
8	**Manage**	This is the section where the template is edited or deleted.

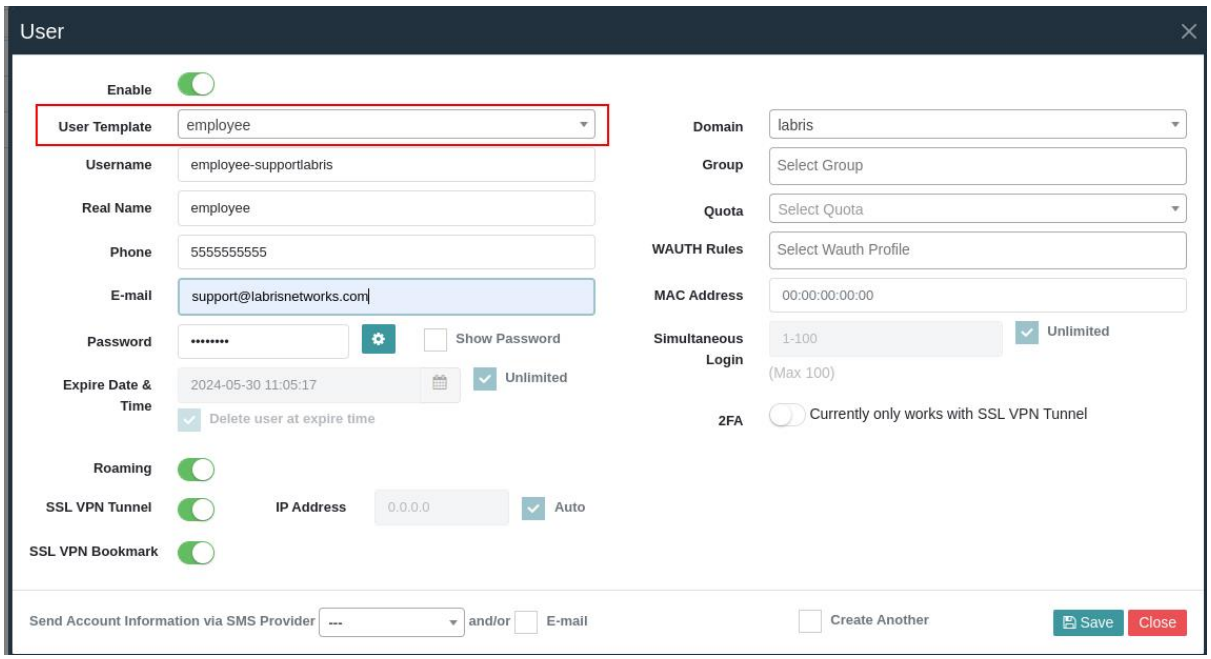
-Click on the 'add' button to add a user template.



1	**Enable**	It is the button where the user template to be added is activated.
2	**Template Name**	This is the section where the template name is entered.
3	**Username Prefix**	This is the section where the username prefix is entered.
4	**Real Name**	This is the section where the real name of the template is entered.
5	**Password**	It is the section where the password of the user to be created according to the user template is entered.

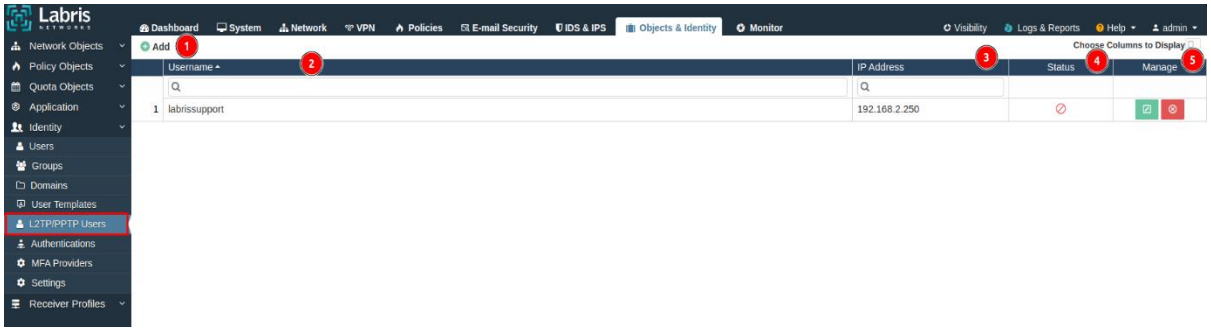
6	**Expire Duration**	This is the section where the expiration date of the template is selected.
7	**Roaming**	This is the section where the navigation of the user template is opened.
8	**SSL VPN Tunnel**	This is the section where the template is authorized to log in to SSL VPN.
9	**SSL VPN Bookmark**	This is the section where the template is authorized to log in to SSL VPN Bookmark.
10	**Domain**	This is the section where the domain name of the template is selected.
11	**Group**	This is the section where the group in which the template will be included is selected.
12	**Quota**	This is the section where the quota object to which the template will be included is selected.
13	**Wauth Rules**	This is the section where the WAUTH Rule is selected to include the template.
14	**Simultaneous Login**	This is the section where the number of simultaneous sessions of the template is regulated.
15	**2FA**	It is a button that allows users to enter two-factor authentication to verify their credentials when logging into SSL VPN.
16	**Save**	It is the button where the template information to be added is saved.
17	**Close**	It is the button where the window opened by clicking the 'Add' button is closed. When the Close button is pressed, it closes the changes made to the template without saving them.

-To create a user according to the user template, it is necessary to click the 'add' button in the User module open the user adding window, and select the User Template.



16.5.5 L2TP/PPTP Users

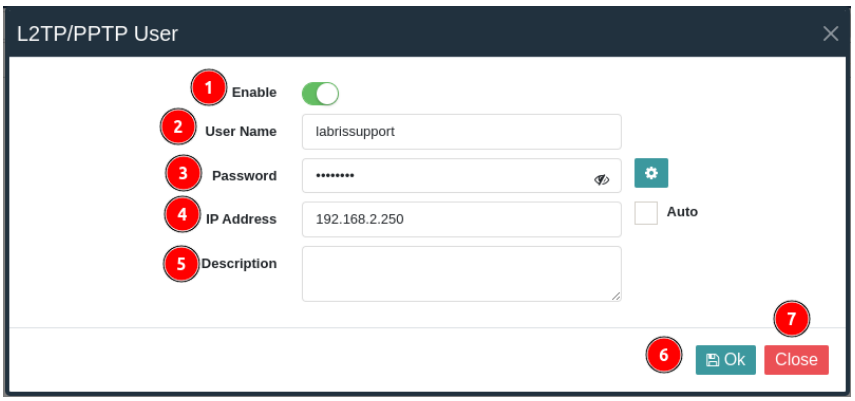
L2TP/PPTP is the module where users who will connect to the VPN are added. It is added by entering the usernames, password, and IP information of the users who will make the connection.



1	**Add**	This is the button where L2TP/PPTP users are added.
2	**Username**	This is the section where the usernames of the added L2TP and PPTP users are displayed.
3	**IP Address**	This is the section where the IP addresses of the added L2TP and PPTP users are displayed.

4	**State**	This is the section where the VPN status is displayed.
5	**Manage**	These are the sections where the added L2TP and PPTP VPN user information is edited or deleted.

-To add L2TP/PPTP user, you need to click on the 'add' button. After clicking the button, the L2TP / PPTP VPN in the window that opens is saved by entering the username, password, and IP address information of the user to be connected.

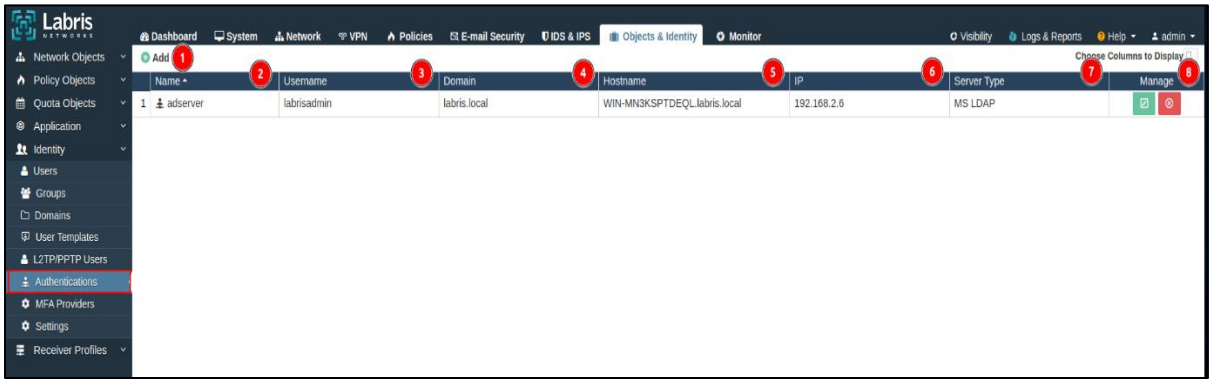


1	**Enable**	This is the button where L2TP/PPTP users are enabled.
2	**Username**	This is the section where the username of the L2TP/PPTP user to be added is entered.
3	**Password**	This is the section where the password of the L2TP/PPTP user to be added is entered.
4	**IP Address**	This is the section where the IP Address of the L2TP/PPTP user to be added is entered.
5	**Description**	This is the section where the description of the L2TP/PPTP user is entered.
6	**Save**	This is the button where the information of the L2TP/PPTP user is saved.
7	**Close**	**It** is the button where the window opened by clicking the 'Add' button is closed. **When the Close** button is pressed, it closes the changes made for the

		L2TP/PPTP User without saving them.

16.5.6 Authentication

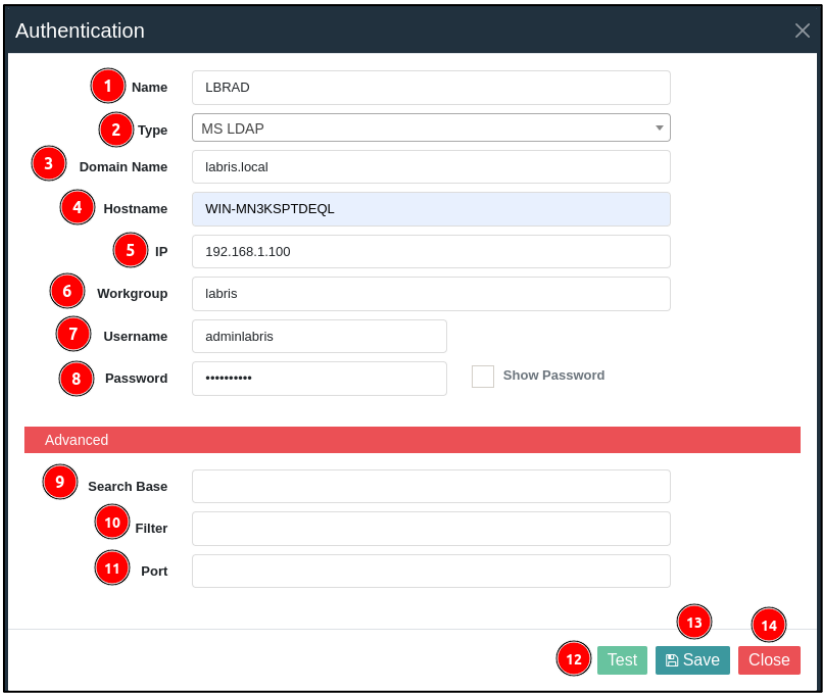
It is the module used to pull users from the Active Directory in the Labris UTM device. By obtaining the information of users in the Active Directory, users are authorized to access WAUTH, SSL VPN, and Labris Web Interface.



1	**Add**	It is the button where the process of adding an authentication server is done.
2	**Name**	This is the section where the name given to the authentication server is displayed.
3	**Username**	This is the section where the username of the admin authorized user opened on the authentication server is displayed.
4	**Domain**	This is the section where the domain name of the authentication server is displayed.
5	**Hostname**	This is the section where the name of the authentication server is displayed.
6	**IP Address**	The IP address of the authentication server is displayed.
7	**Server Type**	The server type of the authentication server is displayed. The server types are: MS LDAP, MS LDAP + NTML, and Open LDAP.

8	**Manage**	This is the section where the added authentication server is edited or deleted.

-Click the "add" button to add an authentication server. After clicking the button, the server type, domain name, server name, IP address of the server, workgroup, admin authorized username, and password information must be entered.

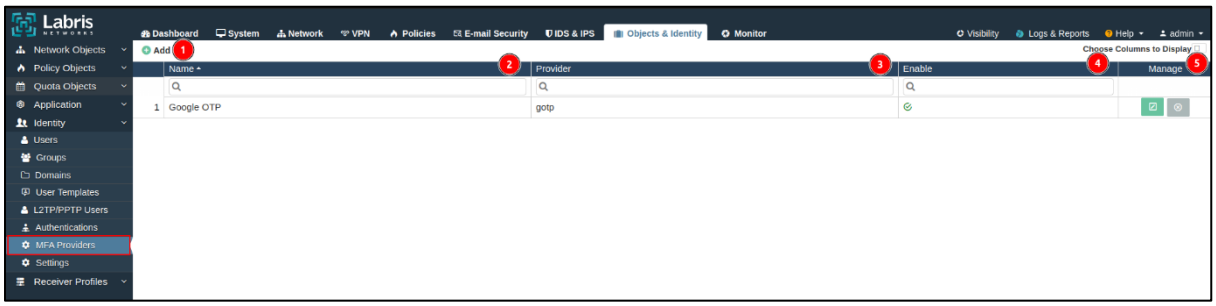


1	**Name**	This is the section where the name of the authentication server is entered.
2	**Type**	This is the section where the authentication type of the authentication server is selected.
3	**Domain Name**	Enter the domain name of the authentication server.
4	**Hostname**	This is the section where the hostname of the authentication server is entered.
5	**IP**	This is the section where the IP address of the authentication server is entered.
6	**Workgroup**	This is the section where the workgroup of the authentication server is entered.

7	**Username**	The username of the admin authorized user opened on the authentication server is entered.
8	**Password**	The password of the admin authorized user opened on the authentication server is entered.
9	**Search Base**	The search base information of the authentication server is entered.
10	**Filter**	The filter from the authentication server is used to pull the user internally.
11	**Port**	This is the section where the port to be used to pull users from the authentication server is entered.
12	**Test**	It is the button where the accuracy of the data received from the authentication server is tested.
13	**Save**	This is the button where the entered values on the authentication server are saved.
14	**Close**	It is the button where the window opened by clicking the 'Add' button is closed. When the close button is pressed, it closes the changes made to the authentication server without saving them.

16.5.7 MFA Provider

It is the module where the MFA providers to be used in SSL VPN are displayed or the MFA Provider is added. SecurityID and Google AUTH. can be used as MFA Provider, you can add it. By default, Google OTP comes in the Labris UTM device.

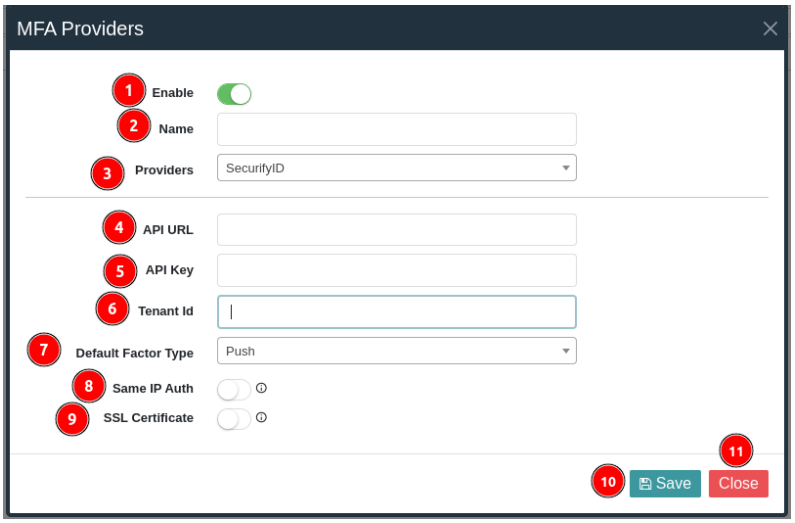


1	**Add**	This is the button where the MFA Provider is added.

2	**Name**	This is the section where the added MFA Provider name is displayed.
3	**Provider**	The provider information is displayed.
4	**Enable**	This is the section where the MFA Provider's activity is displayed.
5	**Manage**	MFA is the section where the provider is edited or deleted.

-Click the 'add' button to add MFA Provider. After clicking the 'add' button, select the type of MFA Provider, SecurifyID or Google Authenticator. Based on the MFA Provider type selected, the data in the window is entered.

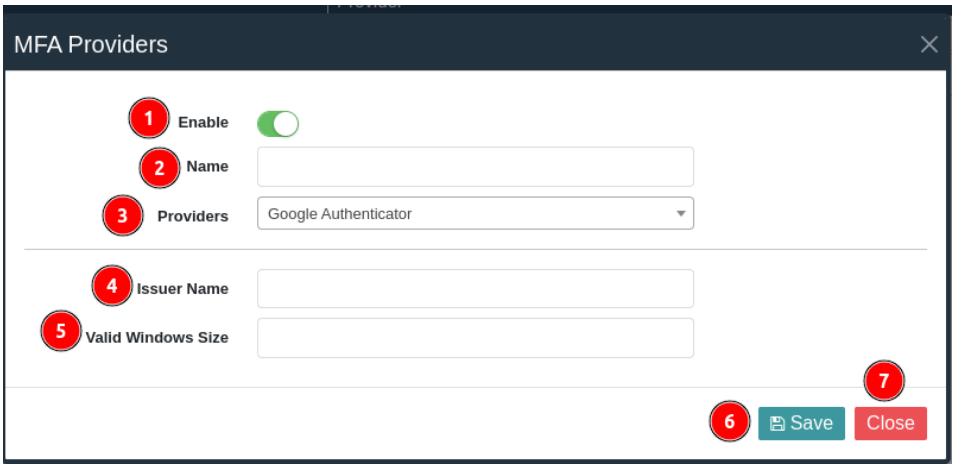
-If SecurifyID is selected for the MFA Provider, API URL, API Key, Identity Number, and Factor Type (PUSH, Email, SMS and Totp) information is entered.



1	**Enable**	This is the button where the MFA Provider to be added is enabled.
2	**Name**	This is the section where the name of the MFA Provider is entered.
3	**Providers**	This is the section where the MFA Provider is selected.
4	**API URL**	If SecurifyID is selected, the provider's API URL is to be entered.

5	**API Key**	If SecurifyID is selected, the provider's API Key is to be entered.
6	**Tenant ID**	If SecurifyID is selected, the identification number of the provider is entered.
7	**Default Factor Type**	The default factor type is selected.
8	**Same IP Auth**	It is activated if OTP-free requests from the same IP address are allowed.
9	**SSL Certificate**	It is enabled in cases where requests need to use the SSL Certificate.
10	**Save**	This is the button where MFA Provider settings are saved.
11	**Close**	It is the button where the window opened by clicking the 'Add' button is closed. When the close button is pressed, it closes the changes made to the MFA Provider without saving them.

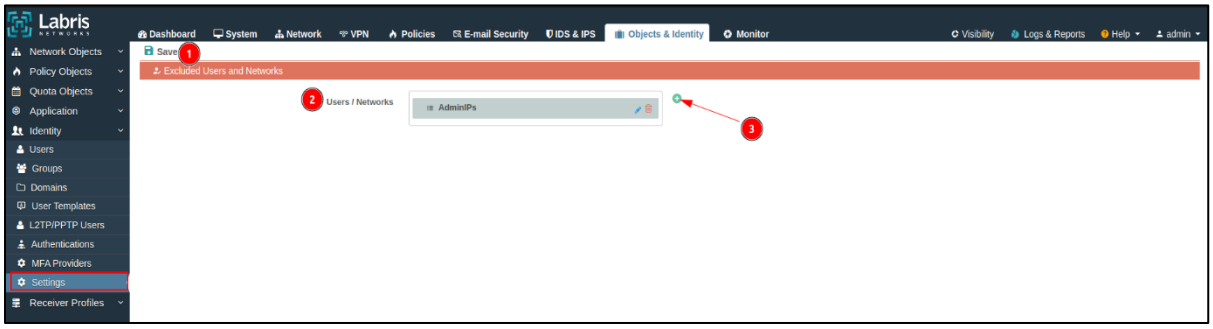
-If the MFA Provider is selected as Google Authenticator, the Provider name and Current Window Size are entered.



1	**Enable**	This is the button where the MFA Provider to be added is enabled.
2	**Name**	This is the section where the name of the MFA provider is entered.
3	**Providers**	This is the section where the MFA Provider is selected.
4	**Issuer Name**	If Google Auth. is selected, the issuer name of the provider is entered.
5	**Valid Windows Size**	If Google Auth. is selected, the valid window size of the provider is entered.
6	**Save**	This is the button where MFA Provider settings are saved.
7	**Close**	It is the button where the window opened by clicking the 'Add' button is closed. When the Close button is pressed, it closes the changes made to the MFA Provider without saving them.

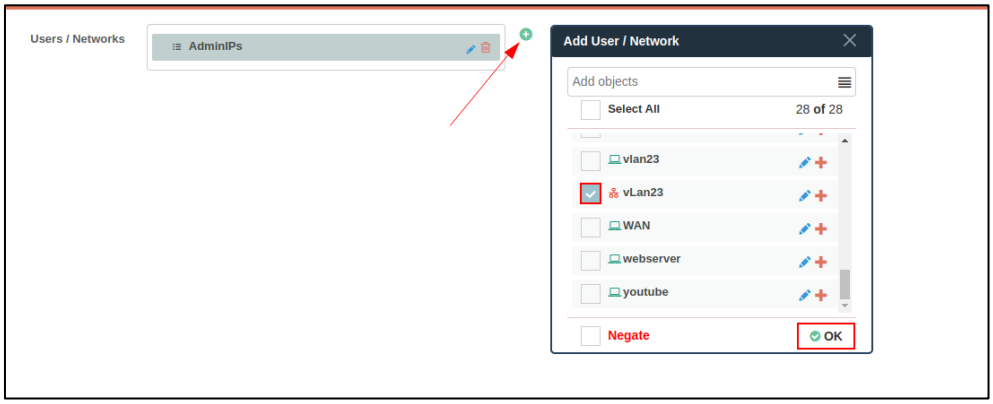
16.5.8 Settings

It allows specific users or networks to be exempt from firewall restrictions.



1	**Save**	This is the button where unincluded users and networks are registered.
2	**Users/Networks**	This is the section where the added users and networks are displayed.
3	**Add**	This is the button where unincluded users and networks are added.

-Users and networks are added by clicking the '+' button to add them to the list of unincluded users and networks.



16.6 Receiver Profiles

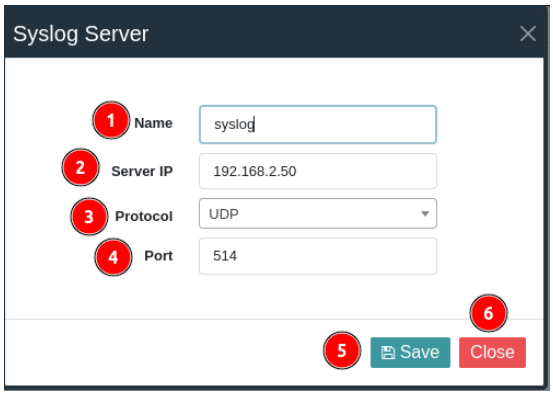
Syslog, SNMP, HTTP, E-mail, and FTP profiles are added to the Labris UTM device.

16.6.1 Syslog

It is used to add a Syslog server to a Labris UTM device. The added Syslog server is used in the Firewall module.

1	**Add**	This is the button where the Syslog server is added.
2	**Name**	This is the section where the name of the Syslog server is displayed.
3	**Server IP**	This is the section where the IP address of the Syslog server is displayed.
4	**Port**	The port information of the Syslog server is displayed.
5	**Protocol**	The protocol of the added Syslog server is displayed. The protocol can be UDP or TCP.
6	**Manage**	This is the section where the added Syslog server is edited or deleted.

-Click the 'add' button to add a Syslog Server. After clicking the button, the IP, port, and protocol information of the Syslog server are entered.

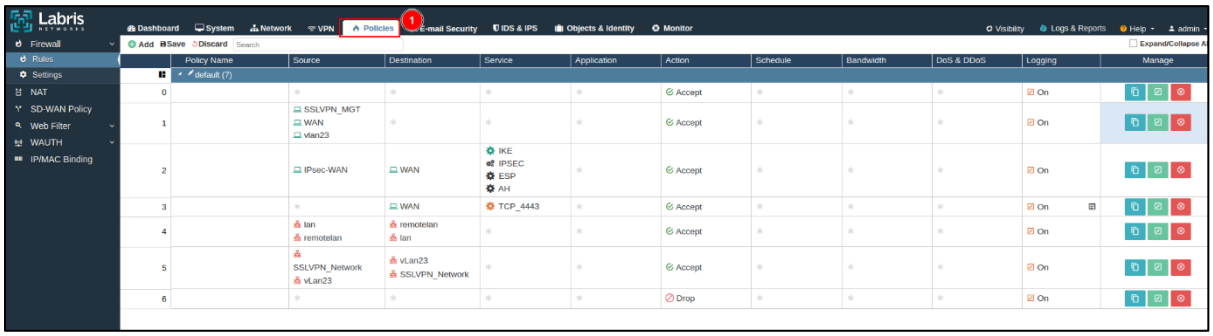


1	**Name**	This is the section where the name of the Syslog server is entered.

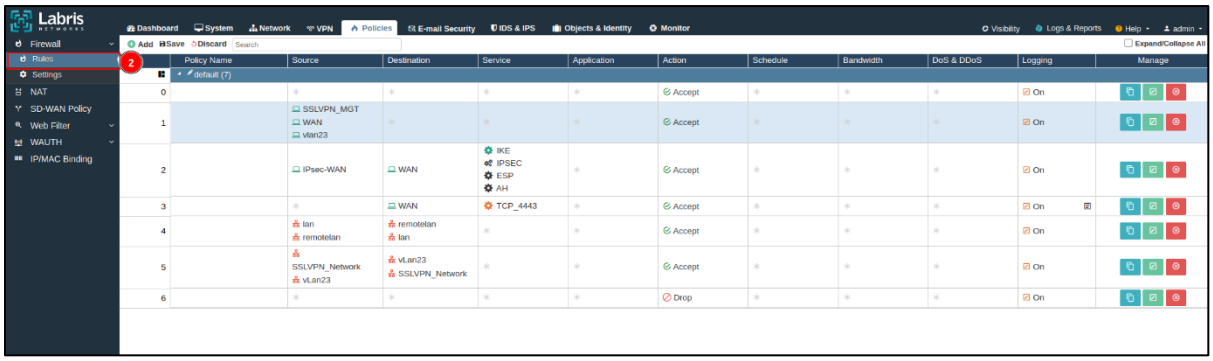
2	**Server IP**	This is the section where the IP address of the Syslog server is entered.
3	**Protocol**	This is the section where the protocol of the Syslog server is selected. TCP and UDP can be selected.
4	**Port**	This is the section where the port number of the Syslog server is entered.
5	**Save**	This is the button where the syslog server settings are saved.
6	**Close**	This is the button where the window opened by clicking the 'add' button is closed. When the Close button is pressed, it closes the Syslog Server without saving the changes made.

- To use the added Syslog server;

1. The Policies menu opens.

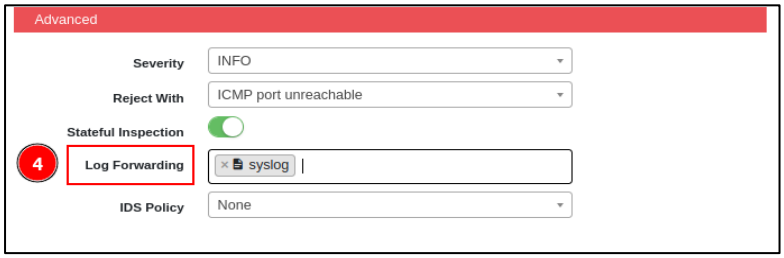


2. The Firewall module opens.

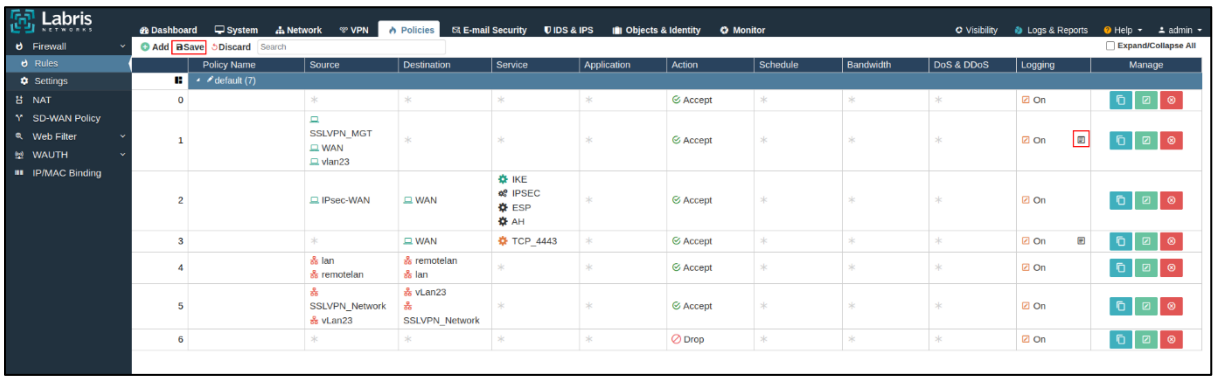


3. Click the 'edit' button for the rule that needs to be added to the syslog server.

4. The added Syslog server is selected in the Log Forwording section.



5. The Syslog server object is added to the rule and the rule is saved.



6. Requests that pass through the rule are also sent to the Syslog Server.

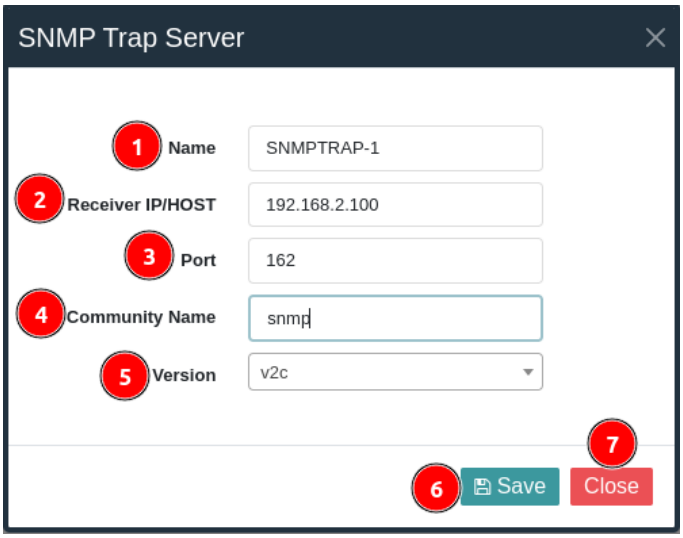
16.6.2 SNMP Trap

They are automatically alerted when a specific event occurs on the device connected to the network. SNMP Trap servers are also added to the Labris UTM device.

1	**Add**	It is the button where the SNMP Trap is added.
2	**Name**	This is the section where the name of the added SNMP Trap is displayed.
3	**Version**	The version of the SNMP Trap server is displayed.

4	**Receiver**	The IP address of the SNMP Trap server is displayed.
5	**Port**	The port information of the SNMP Trap server is displayed.
6	**Security Level**	The security level of the SNMP Trap server is displayed.
7	**Manage**	This is the section where the SNMP Trap server that is added is edited and deleted.

- Click the 'add' button to add an SNMP Trap. After clicking the button, the IP, port information is entered.

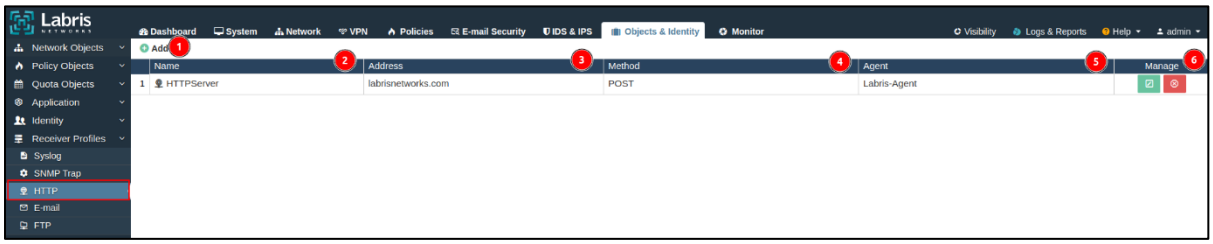


1	**Name**	This is the section where the name of the SNMP Trap server is entered.
2	**Receiver IP/Host**	This is the section where the IP address of the SNMP Trap server is entered.
3	**Port**	The port information on which the SNMP Trap server is running is displayed.
4	**Community Name**	This is the section where the community name of the SNMP Trap server is entered.
5	**Version**	This is the section where the SNMP version

		information is selected.
6	**Save**	This is the section where the information of the SNMP Trap server is saved.
7	**Close**	It is the button where the window opened by clicking the 'Add' button is closed. When the Close button is pressed, it closes the changes made to the SNMP Trap Server without saving it.

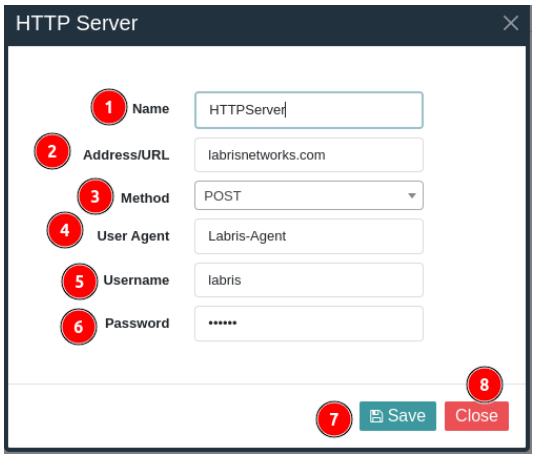
16.6.3 HTTP

The HTTP Recipient profile typically sends POST and Get requests to a specific URL of a web service. Sends monitoring, logging, and alerts on the HTTP website.



1	**Add**	It is the button where the HTTP server addition process is performed.
2	**Name**	The name of the HTTP server is displayed.
3	**Address**	The address of the HTTP server is displayed.
4	**Method**	This is the section where the method of the HTTP server is displayed.
5	**Agent**	This is the section where the HTTP server's Agent is displayed.
6	**Manage**	This is the section where the added HTTP server is edited or deleted.

-Click the 'add' button to add an HTTP Server. After clicking the button, the IP and port information is entered to add an HTTP server.



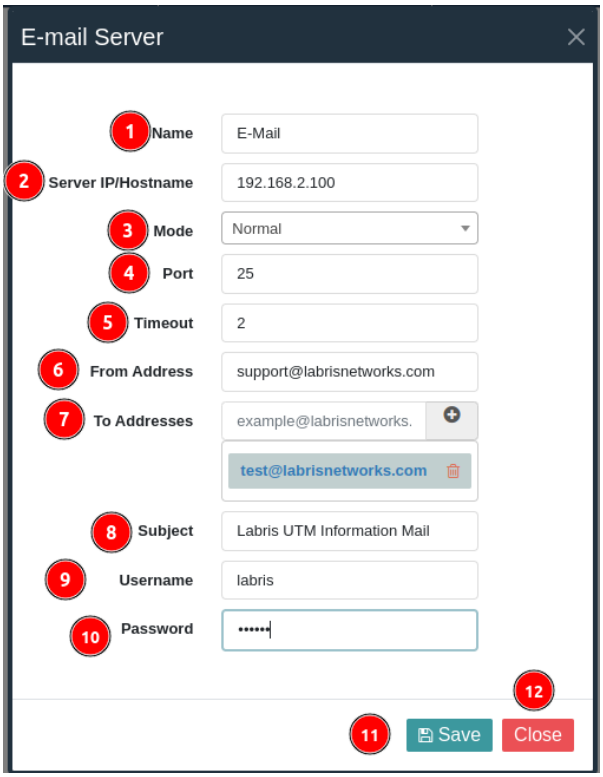
1	**Name**	This is the section where the name of the HTTP server is entered.
2	**Address/URL**	This is the section where the URL of the HTTP server is entered.
3	**Method**	This is the section where the method of the HTTP server is selected.
4	**User Agent**	This is the section where the user agent to be added to the HTTP server is selected.
5	**Username**	This is the section where the username on the user application is entered.
6	**Password**	This is the section where the password on the user application is entered.
7	**Save**	It is the button where HTTP Server information is saved.
8	**Close**	It is the button where the window opened by clicking the 'Add' button is closed. When the Close button is pressed, it closes the changes made for the HTTP Server without saving them.

16.6.4 E-Mail

It is the module where the e-mail server is added to the Labris UTM device.

1	**Add**	This is the section where the e-mail server is added.
2	**Name**	This is the section where the name of the e-mail server is displayed.
3	**Server**	This is the section where the address of the mail server is displayed.
4	**Mode**	This is the section where the mode of the mail server is displayed.
5	**Port**	The port of the mail server is displayed.
6	**From**	This is the section where the sender's mail address is displayed.
7	**To**	This is the section where the recipient's mail address is displayed.
8	**Subject**	It is the section where the subject to send e-mail is displayed.
9	**Manage**	This is the section where the added mail server is edited or deleted.

-Click on the 'add' button to add a mail server. After clicking the button, enter the server IP, mode, port, sender, and recipient information to add an E-Mail Server.



1	**Name**	This is the section where the name of the mail server is entered.
2	**Server IP/Hostname**	This is the section where the server IP address of the mail server is entered.
3	**Mode**	This is the section where the mode in which the mail server is running is selected.
4	**Port**	The main port where the server is running is the interface.
5	**Timeout**	This is the section where the timeout value of the mail server is entered.
6	**From Address**	This is the section where the sender's e-mail address is entered.
7	**To Addresses**	This is the section where the recipient e-mail address

		is entered.
8	**Subject**	This is the section where the subject of the e-mail is entered.
9	**Username**	This is the section of the mail server where the username of the authorized user is entered.
10	**Password**	This is the section on the mail server where the password of the authorized user is entered.
11	**Save**	It is the button where mail server information is saved.
12	**Close**	It is the button where the window opened by clicking the 'Add' button is closed. When the close button is pressed, it closes the changes made to the e-mail server without saving them.

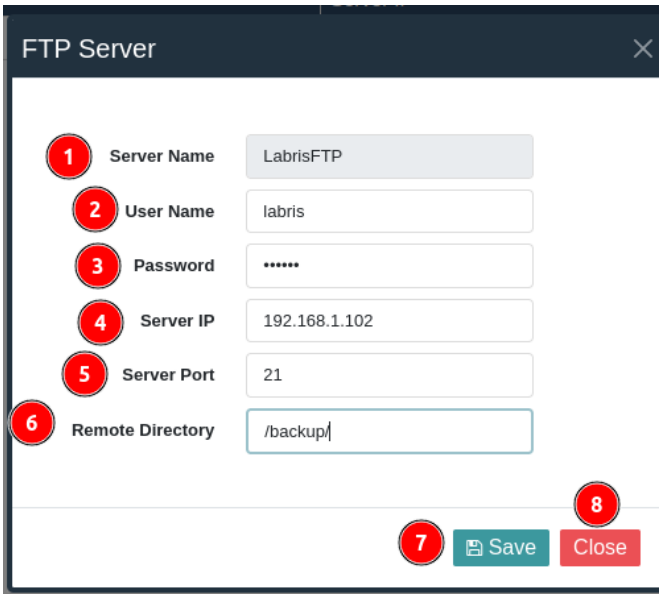
16.6.5 FTP

It is the module where the FTP server is added to the Labris UTM device. The added FTP server is used in the Backup menu located in the System module.

1	**Add**	This is the section where the FTP server is added.
2	**Server Name**	This is the section where the name of the FTP server is displayed.
3	**User**	This is the section on the FTP server where the user name of the authorized user is entered.
4	**Server IP**	This is the section where the IP address of the FTP server is displayed.

5	**Server Port**	This is the section where the port of the added FTP server is displayed.
6	**Manage**	This is the section where the added FTP server is edited or deleted.

-Click the 'add' button to add an FTP Server**.** After clicking the button, the server IP, port, username, and password information authorized on the FTP server are entered.

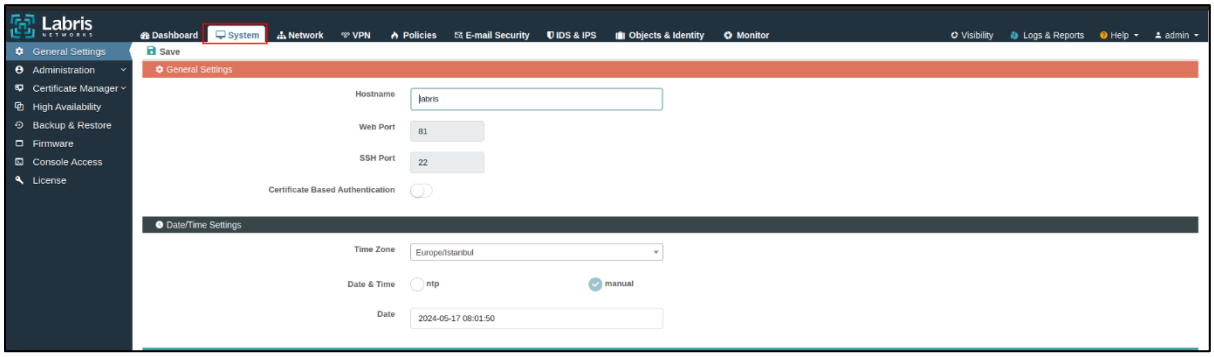


1	**Server Name**	This is the section where the name of the FTP server is entered.
2	**User Name**	This is the section where the user name of the authorized user is entered on the FTP server.
3	**Password**	This is the section where the password of the authorized user is entered on the FTP server.
4	**Server IP**	This is the section where the IP address of the FTP server is entered.
5	**Server Port**	This is the section where the port of the FTP server is entered.
6	**Remote Directory**	This is the section where the directory of the FTP server is entered.

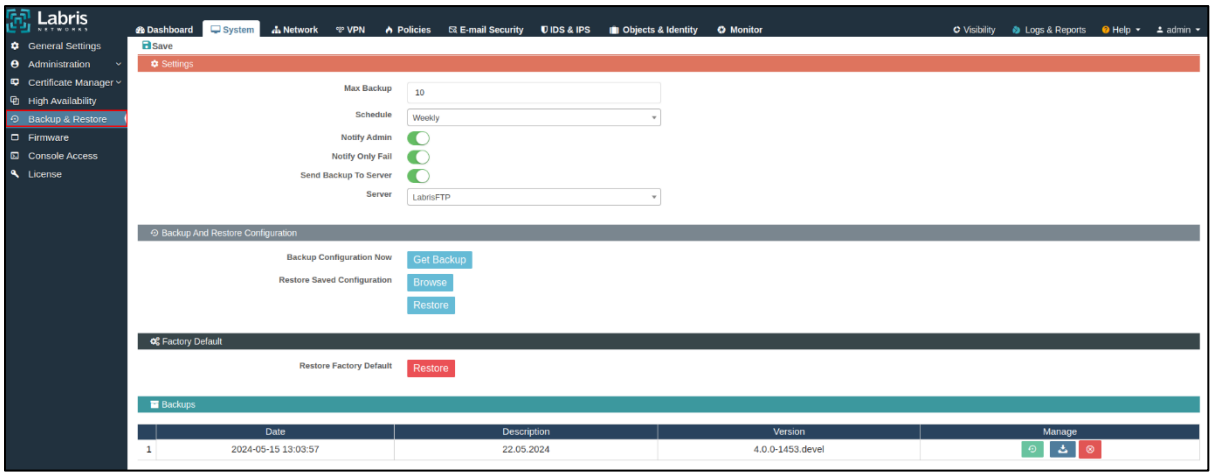
7	**Save**	It is the button where HTTP Server information is saved.
8	**Close**	It is the button where the window opened by clicking the 'Add' button is closed. When the Close button is pressed, it closes the changes made to the E-Mail Server without saving them.

-Added to use FTP server;

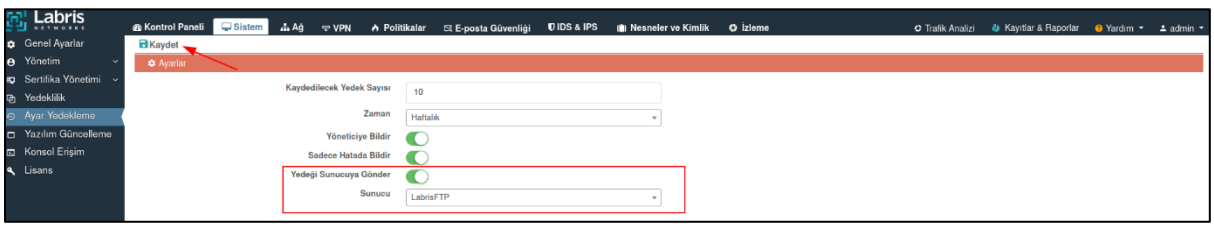
1. It is entered into the system module.



2. Backup & Restore module opens.



3.Send backup to server is activated and FTP server is selected. Then press the save button.

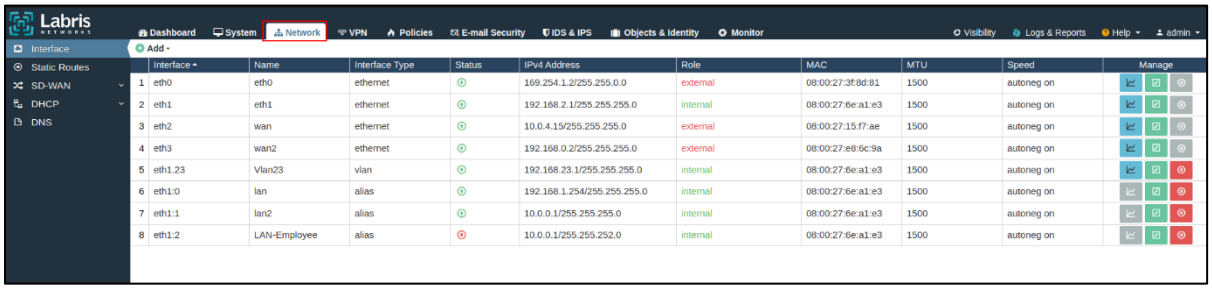


17. Visibility

It is the module where traffic analysis is performed on the Labris UTM device, and the details of the traffic passing through the interfaces are displayed. Traffic analysis can be performed by selecting the interface for which visibility is desired. In the interface where visibility is desired, the visibility option of the interface must be opened in the Network module.

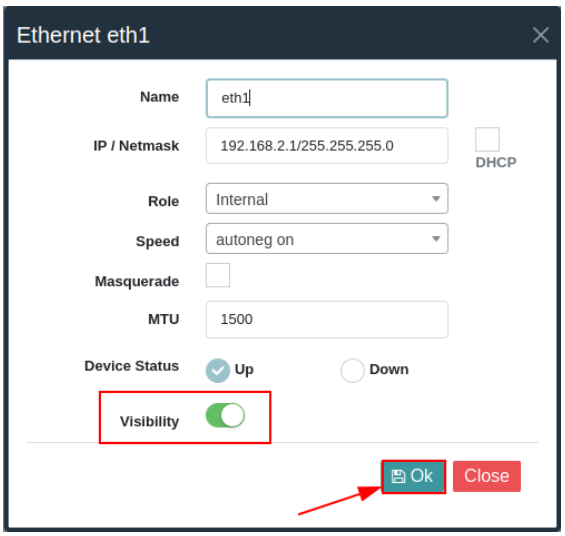
-Steps to turn on visibility in the interface;

1. Click on the network module.



2. Click on the 'edit' button of the interface where the visibility option will be opened.

3. After clicking the edit button on the selected interface, the visibility option in the window is selected, and the interface settings are saved.

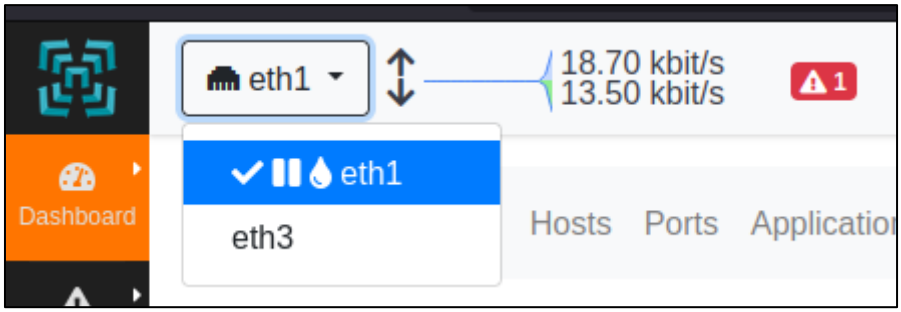


4. After the visibility option is turned on in the selected interface, the visibility module opens.

5. After clicking on the visibility, a new window opens, and the traffic details are examined.

17.1 Interface Selection

The interface to be analyzed for traffic is selected. It is displayed with the speed information of the selected interface.

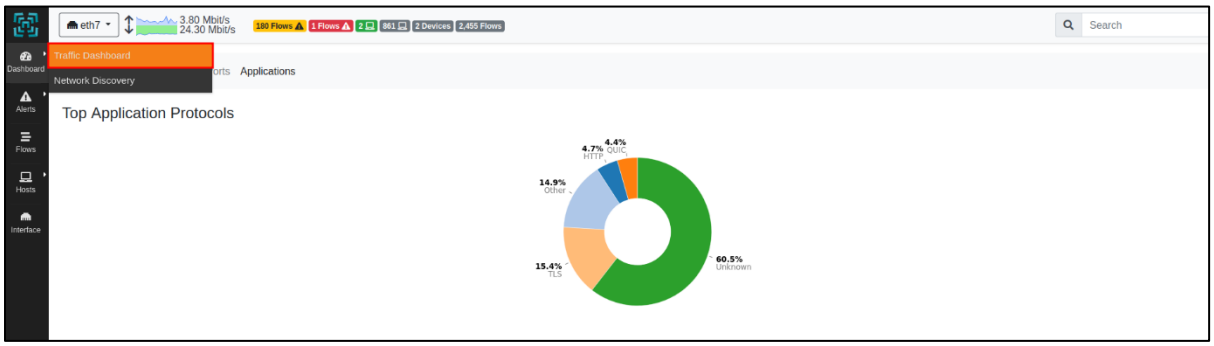


17.2 Dashboard

It is the module where the traffic belonging to the selected interface is examined in detail. In this module, the source and destination IP addresses that generate the most traffic, the IP address of the clients that generate the most traffic, port information and application information are displayed in the control panel.

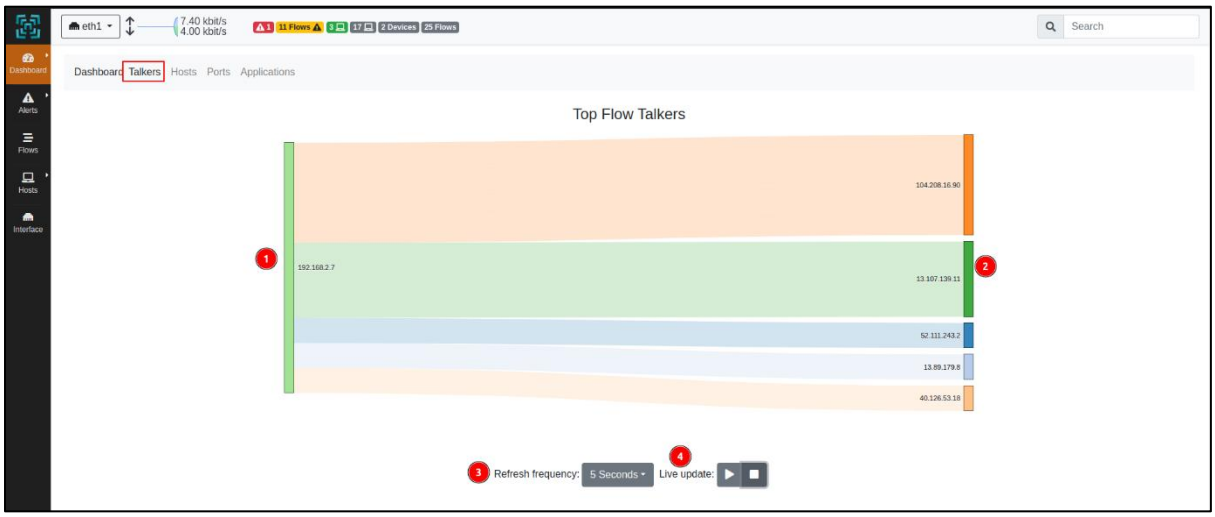
17.2.1 Traffic Dashboard

It is the section where the IP addresses that communicate the most, the hosts that create traffic, the ports with the most requests and the applications are displayed.



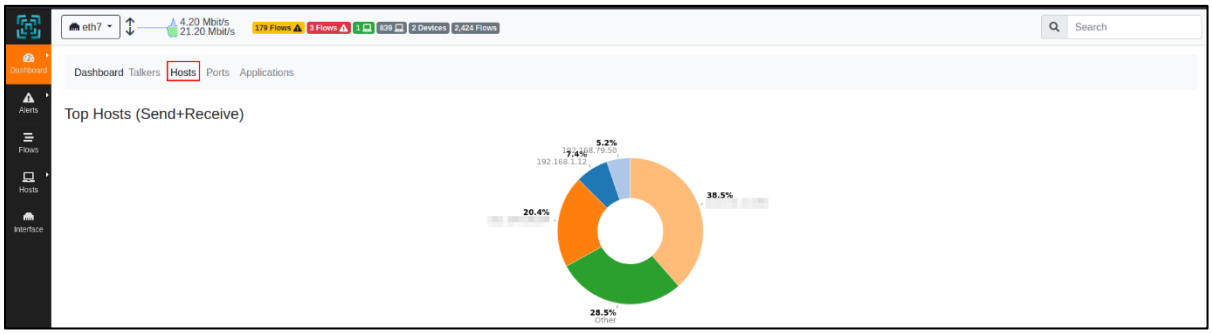
17.2.1.1 Talkers

This section displays the IP addresses that generate the most traffic. The requests made are from the source to the destination.



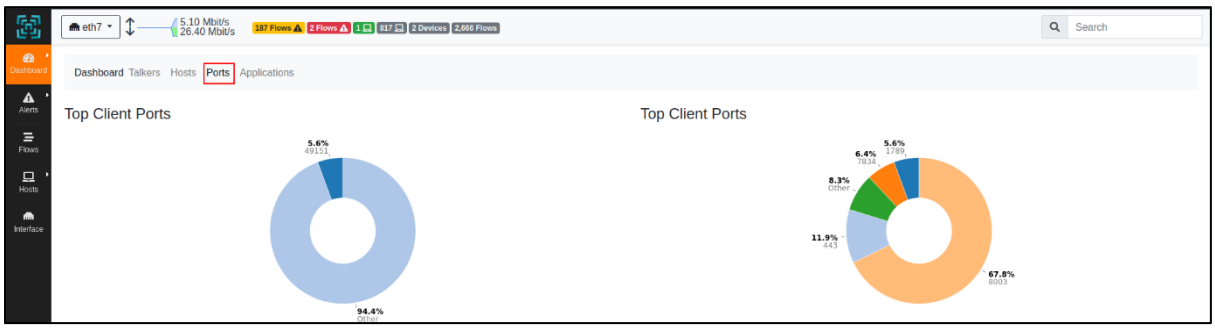
17.2.1.2 Hosts

The traffic generated by the users is displayed in a graph. The IP addresses of the hosts to which the request is sent or received are displayed.



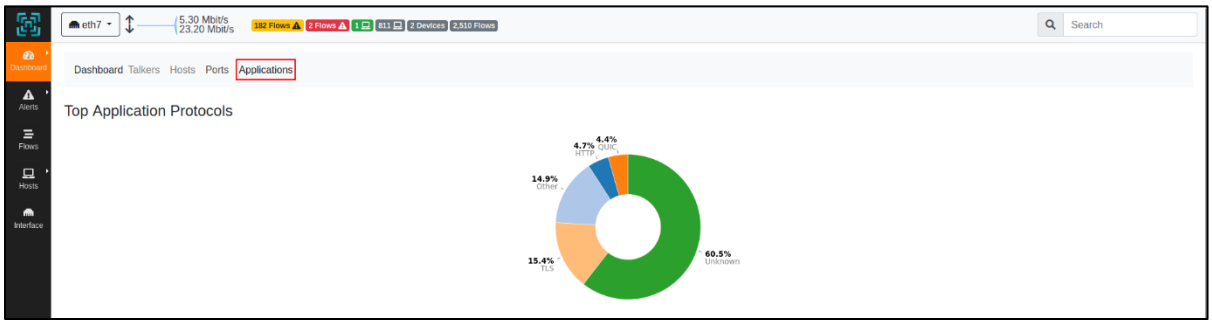
17.2.1.3 Ports

The most requested port information is displayed.



17.2.1.4 Applications

The most used application information in the user-generated traffic is displayed.



17.2.2 Network Discovery

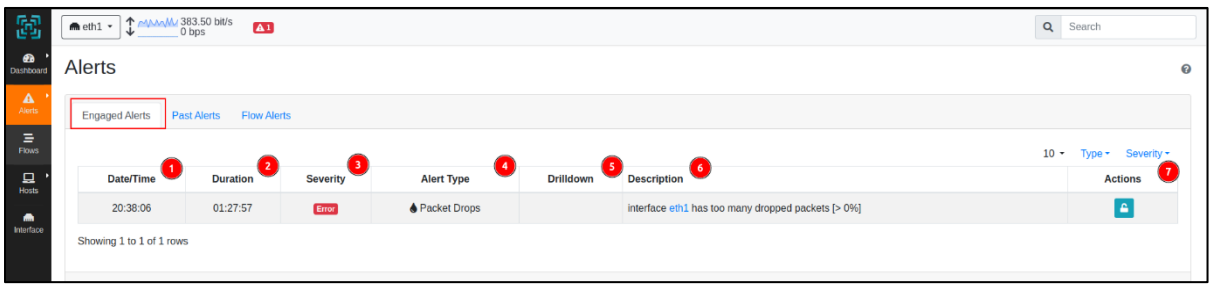
It is the section where devices and resources on computer networks are detected. This is the section where the devices in the network traffic are displayed.

17.3 Alerts

This is the section where abnormal and potential warnings in network traffic are displayed.

17.3.1 Engaged Alerts

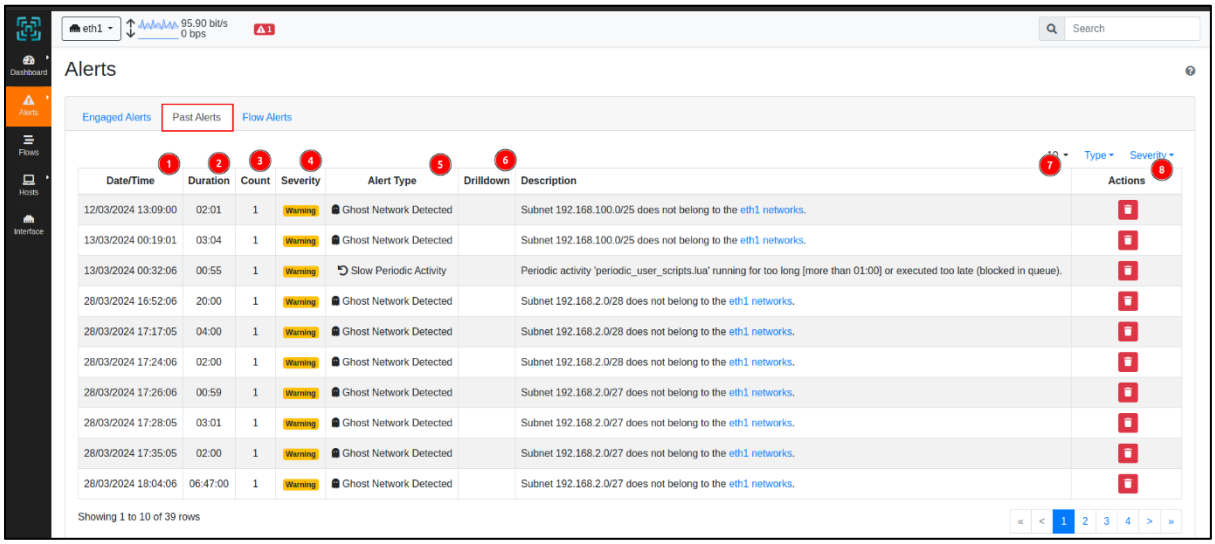
This is the section where abnormal traffic in network traffic is displayed.



1	**Date/Time**	This is the section where the date and time of the alert are displayed.
2	**Duration**	This is the section where the duration of the alerts is displayed.
3	**Severity**	This is the section where the severity level of the alert is displayed.
4	**Alert Type**	This is the section where the alert type is displayed.
5	**Drilldown**	This is the section where detailed information about the alert is displayed.
6	**Description**	This is the section where explanations about the alert are displayed.
7	**Action**	This is the section where the action to be taken regarding the alert is selected.

17.3.2 Past Alerts

This is the section where past alerts are displayed.

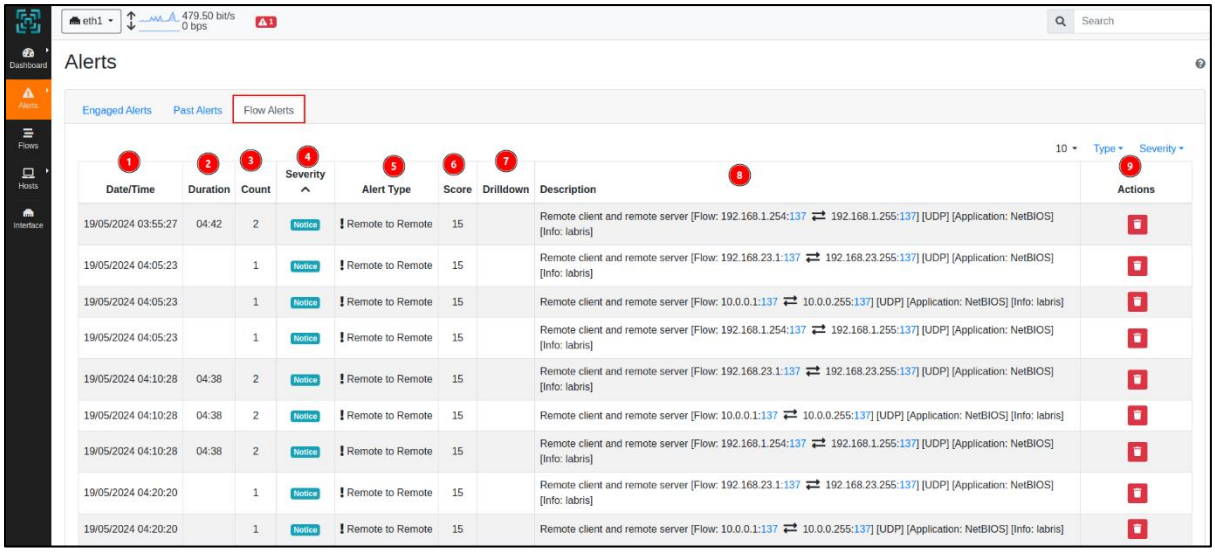


1	**Date/Time**	This is the section where the date and time of past alerts are displayed.
2	**Duration**	This is the section where the duration of incoming

		alerts is displayed.
3	**Count**	This is the section where the total number of the incoming alerts is displayed.
4	**Severity**	It is the section where the severity level of the incoming alerts is displayed.
5	**Alert Type**	This is the section where the types of incoming alerts are displayed.
6	**Drilldown**	This is the section where detailed information about the incoming alerts is displayed.
7	**Description**	This is the section where explanations about incoming alerts are displayed.
8	**Action**	This is the section where the action to be taken regarding the incoming alerts is selected. This is the button where the alerts are deleted.

17.3.3 Flow Alerts

This is the section where the details of incoming alerts are displayed in flow form.

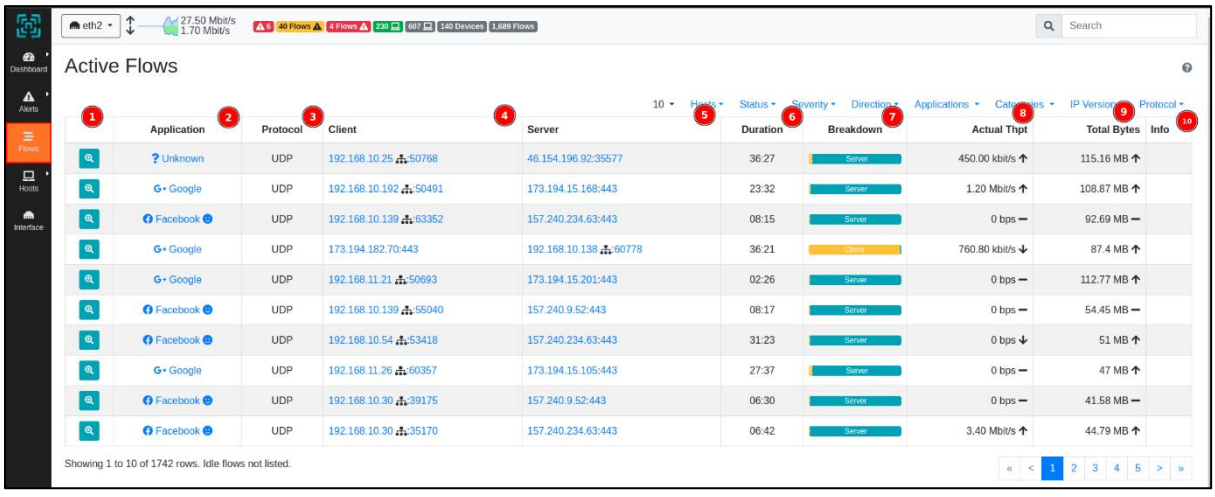


1	**Date/Time**	This is the section where the date and time of alerts are displayed.

2	**Duration**	This is the section where the duration of the alerts is displayed.
3	**Count**	This is the section where the total number of incoming alerts is displayed.
4	**Severity**	It is the section where the severity level of the incoming alerts is displayed.
5	**Alert Type**	This is the section where the types of incoming alerts are displayed.
6	**Score**	This is the section where the score of the incoming alerts is displayed.
7	**Drilldown**	This is the section where detailed information about the incoming alerts is displayed.
8	**Description**	This is the section where explanations about incoming alerts are displayed.
9	**Action**	This is the section where the action to be taken regarding the incoming alerts is selected. This is the button where the alerts are deleted.

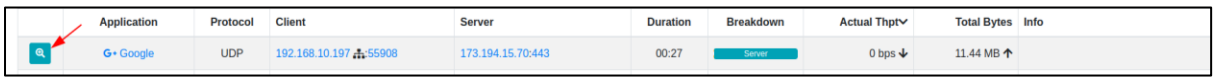
17.4 Flow

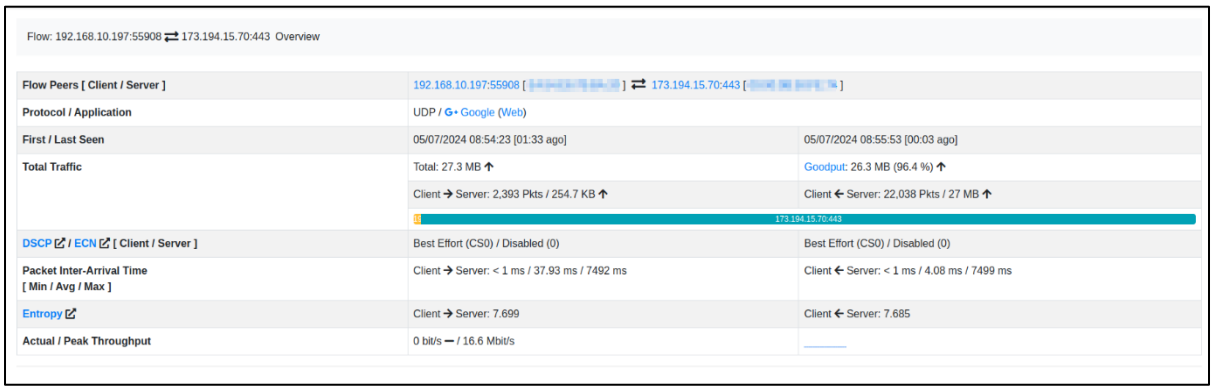
This is the section where the traffic flow of the interface where the visibility feature is turned on is displayed.



1	**Details**	Details of the traffic flow are displayed.
2	**Application**	The application information in the traffic is displayed.
3	**Protocol**	The protocol information in the traffic created by the client is displayed.
4	**Client**	The client's IP address and source port are displayed.
5	**Server**	The server IP address and destination port information are displayed.
6	**Duration**	The duration of traffic generated by the client towards a specific destination is displayed.
7	**Breakdown**	Indicates client-to-server or server-to-client traffic. If there is a traffic flow from the client to the server, it is displayed in orange, and if there is a traffic flow from the server to the client, it is displayed in blue.
8	**Actual Thpt**	The client's bandwidth usage is displayed.
9	**Total Bytes**	This is the section where the total byte size of the traffic between client and server or server and client is displayed.
10	**Description**	A description of the traffic flow is displayed.

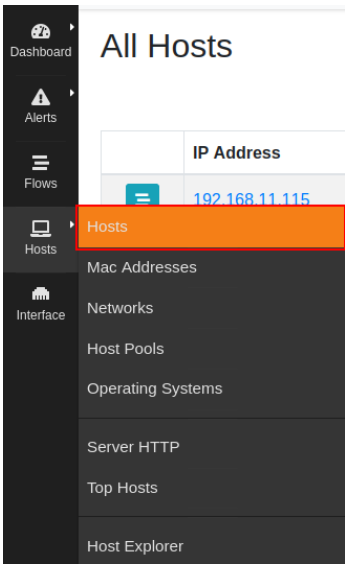
-The magnifying glass button is pressed to see the traffic flow details.





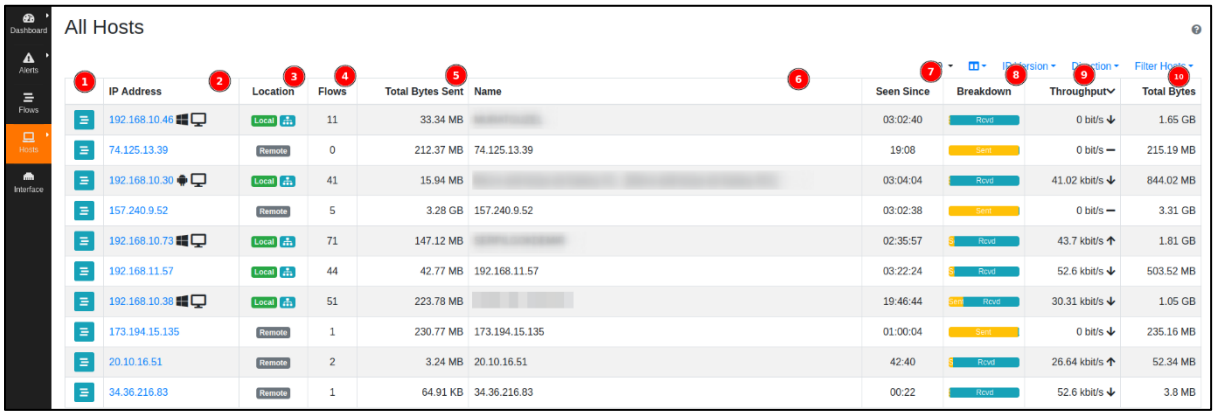
17.5 Hosts

It is the module where the network traffic of the devices is analyzed.



17.5.1 Hosts

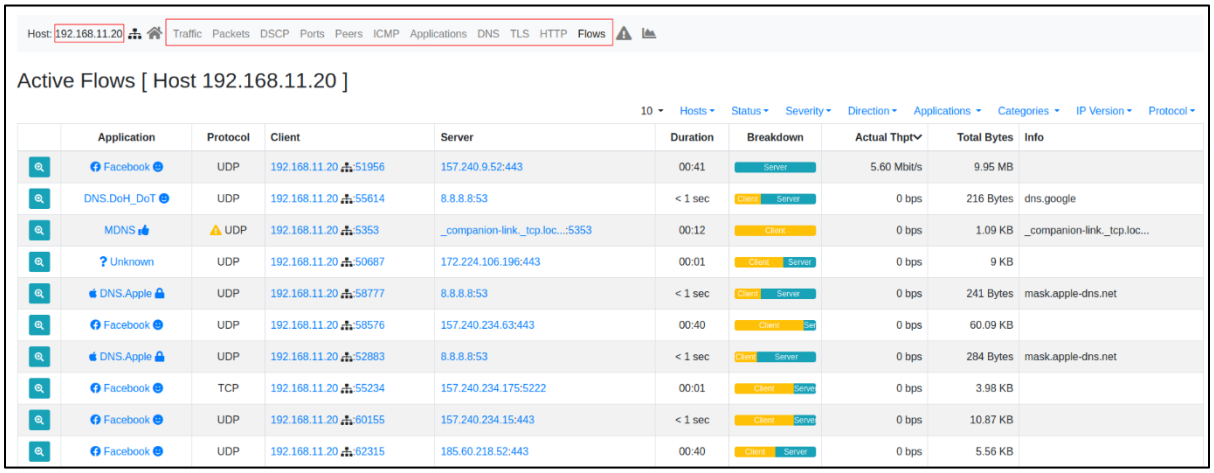
This is the section where all the devices in the interface where traffic analysis is turned on are displayed.



1	**Details**	Details of the traffic flow generated by the devices are displayed.
2	**IP Address**	The IP addresses of the devices are displayed.
3	**Location**	The location information of the devices on the network is displayed.
4	**Flows**	The total number of flows from the device is displayed.
5	**Total Bytes Sent**	The total byte size of the devices sent is displayed.
6	**Name**	The time that the client has created towards a specific destination is displayed.
7	**Seen Since**	The last seen time in the traffic generated by the devices is displayed.
8	**Breakdown**	Shows graphs of incoming and outgoing packets from devices.
9	**Throughput**	The bandwidth usage of the devices is displayed.

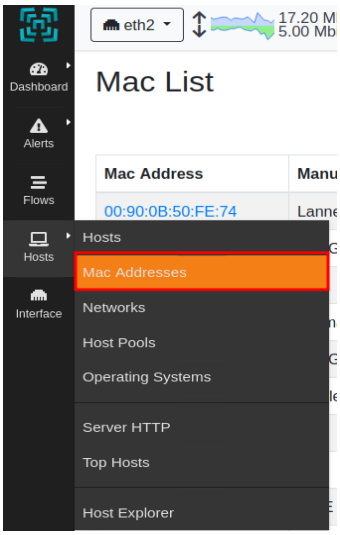
10	**Total Bytes**	The total byte size of the devices is displayed.

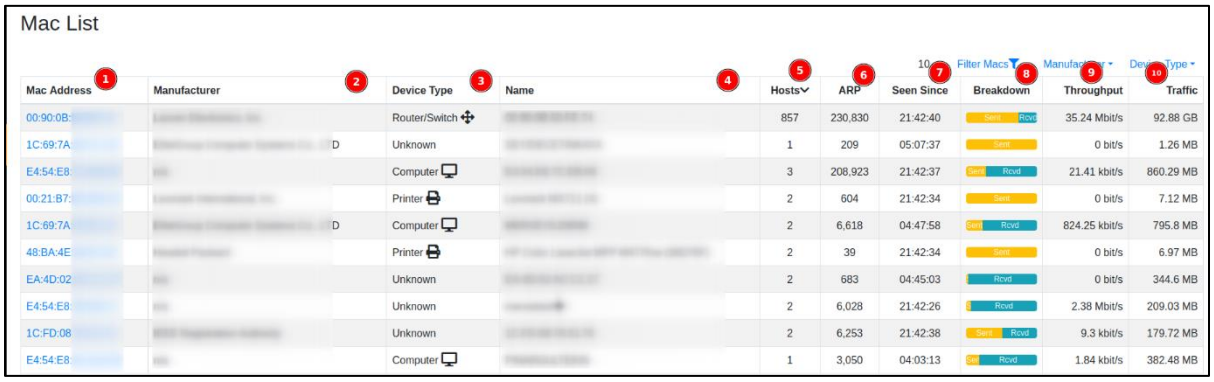
-The detail button is pressed to examine the device's traffic in detail. On the screen after the detail button is pressed, traffic, packet, DSCP, port, mapped IP addresses, ICMP requests, application, DNS, TLS, HTTP and flow details are displayed according to the selected device.



17.5.2 Mac Address

It is the section where the traffic flow is analyzed according to MAC addresses.

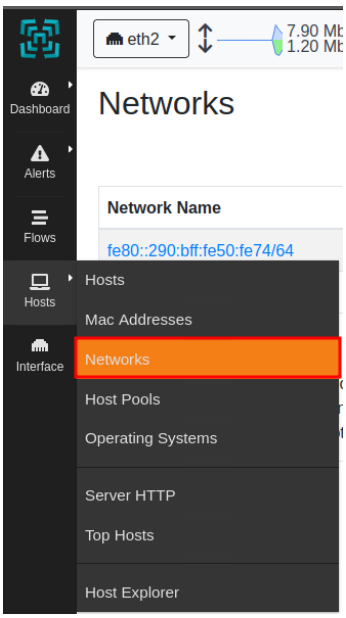


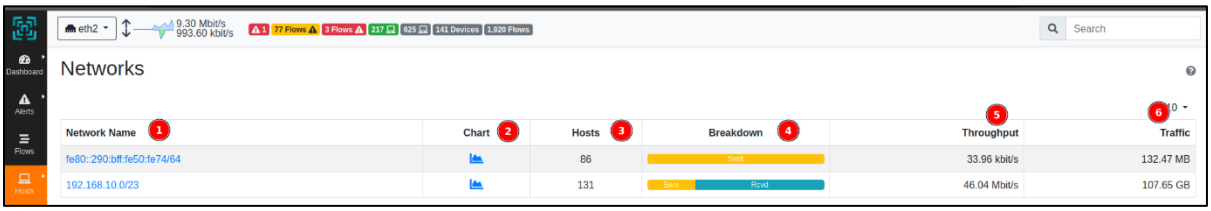


1	**Mac Address**	The MAC address information is displayed.
2	**Manufacturer**	The manufacturer's information is displayed. (Detection is made by looking at the MAC address.)
3	**Device Type**	By looking at the MAC address, the type of device is displayed.
4	**Name**	The name of the device is displayed.
5	**Hosts**	The total number of devices is displayed.
6	**ARP**	The total number of the device's ARP requests is displayed.
7	**Seen Since**	It is the section where the time elapsed since the first packet sent/received by MAC addresses was observed is displayed.
8	**Breakdown**	Shows graphs of incoming and outgoing packets. Shows graphs of incoming and outgoing packets.
9	**Throughput**	The bandwidth usage of the devices is displayed.
10	**Traffic**	The total byte size of the devices is displayed.

17.5.3 Networks

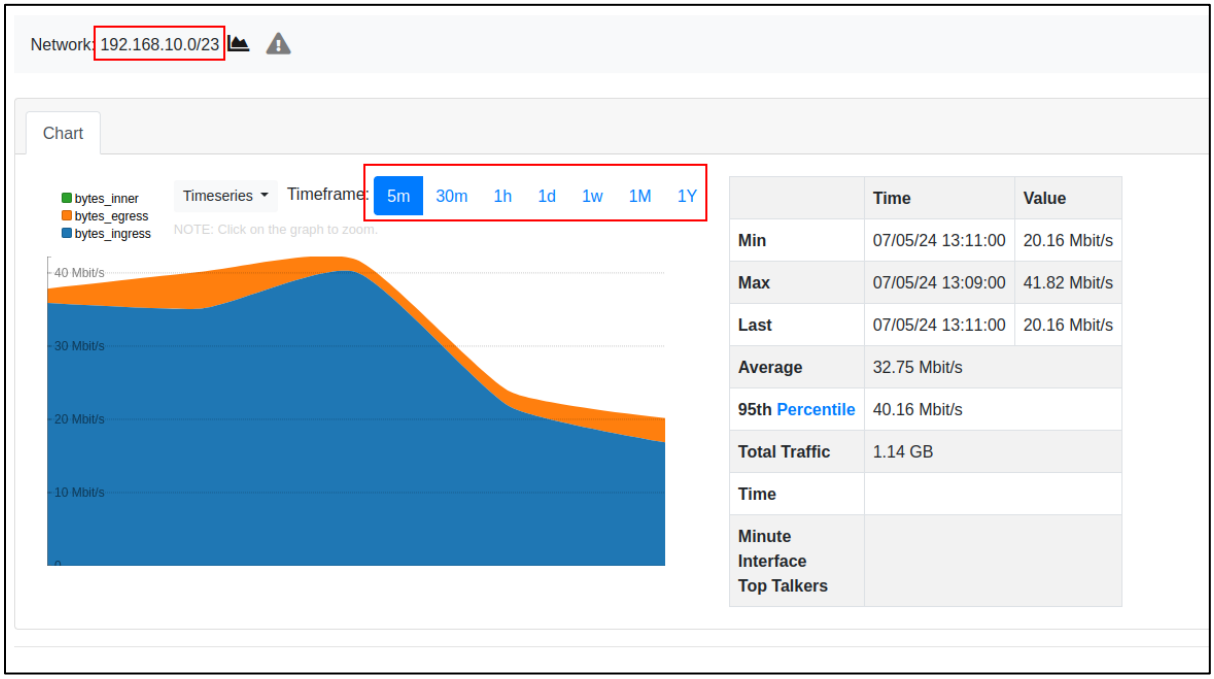
It is the section where the analysis of traffic flow according to network addresses is made.





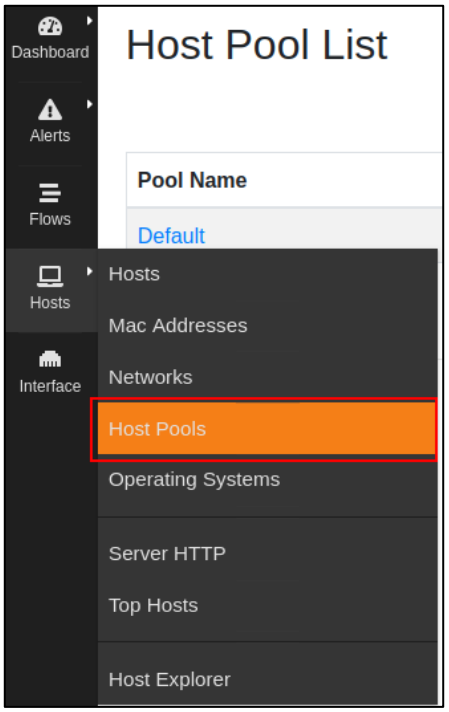
1	**Network Name**	The part where the network name is displayed.
2	**Chart**	This is the section where traffic related to network addresses is displayed as a chart.
3	**Hosts**	The number of devices for the network address is displayed.
3	**Breakdown**	Shows graphs of incoming and outgoing packets associated with the network address.
4	**Throughput**	The bandwidth for the network address is displayed.
5	**Traffic**	The packet size of traffic for network addresses is displayed.

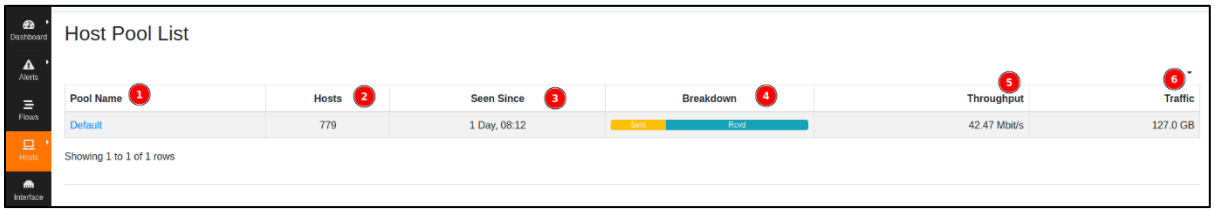
-The details of the traffic related to the network address are displayed in 5 minutes, 30 minutes, 1 hour, 1 day, 1 week, 1 month, and 1 year of data.



17.5.4 Host Pools

Shows a list of device pools that have been defined and are active.

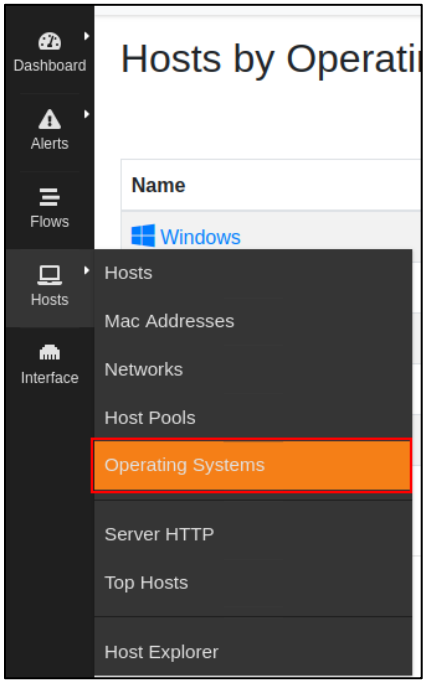


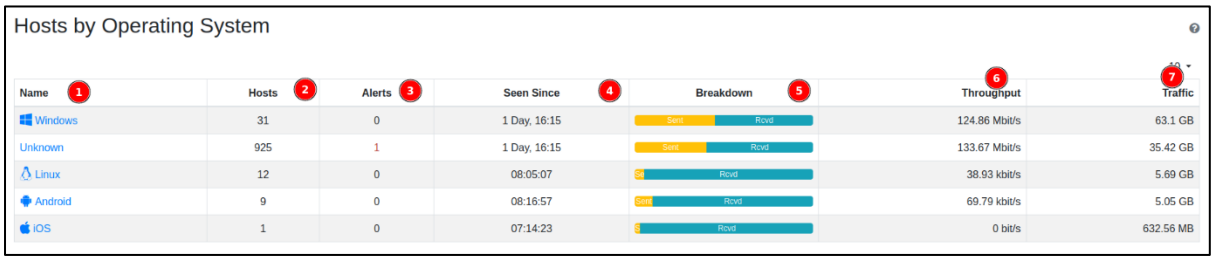


1	**Pool Name**	This is the section where the name of the device pool is displayed.
2	**Hosts**	This is the section where the number of devices included in the pool is displayed.
3	**Seen Since**	It is the section where the time elapsed since the first packet sent/received by hosts was observed is displayed.
3	**Breakdown**	Shows graphs of the inbound and outbound packets associated with the device pool.
4	**Throughput**	The bandwidth for the device pools is displayed.
5	**Traffic**	The packet size of the traffic belonging to the device pools is displayed.

17.5.5 Operating System

This is the section where the operating systems detected by the Labris UTM device are displayed in the traffic flow.



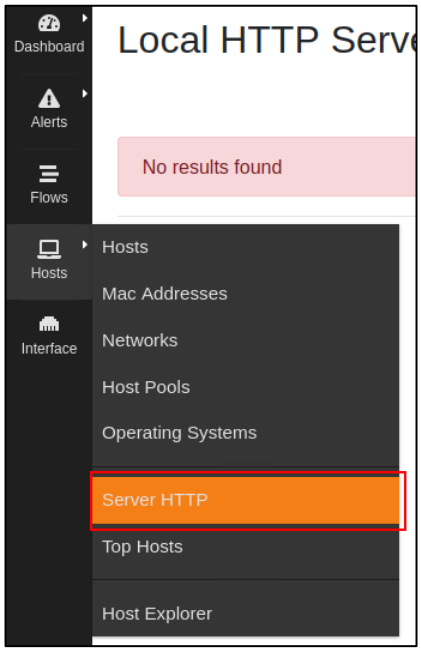


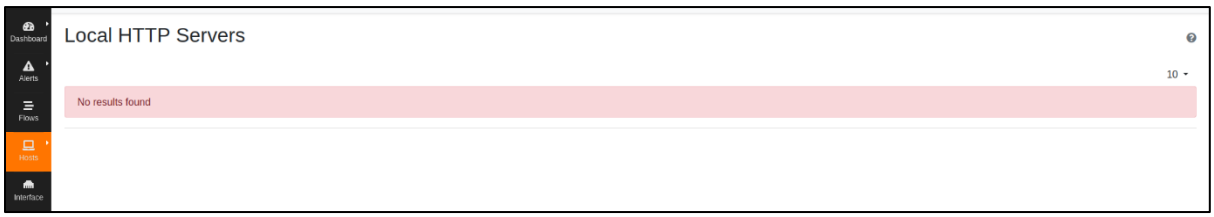
1	**Name**	It is the section where the operating system detected by the Labris UTM device is displayed.
2	**Hosts**	The number of devices using the operating system is displayed.
3	**Alerts**	The number of alerts for devices in the operating system is displayed.
4	**Seen Since**	This is the section where the time elapsed since the first packet sent/received by the operating system was observed is displayed.

5	**Breakdown**	Shows graphs of incoming and outgoing packets associated with the operating system.
6	**Throughput**	It shows the total bandwidth used by devices with the operating system detected by the Labris UTM device.
7	**Traffic**	It shows the total traffic generated by the devices with the operating system detected by the Labris UTM device.

17.5.6 HTTP Server

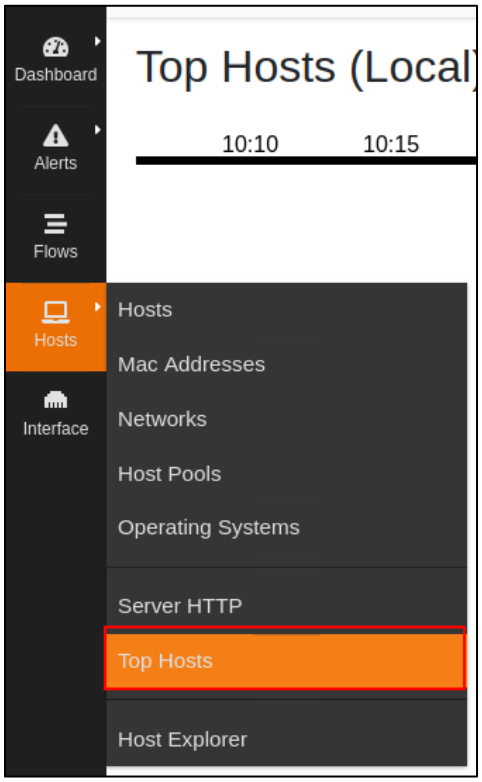
A list of HTTP servers located on the local network is displayed. If there is no http server in the interface where Traffic Analysis is opened, the page gives an error as 'no results found'.

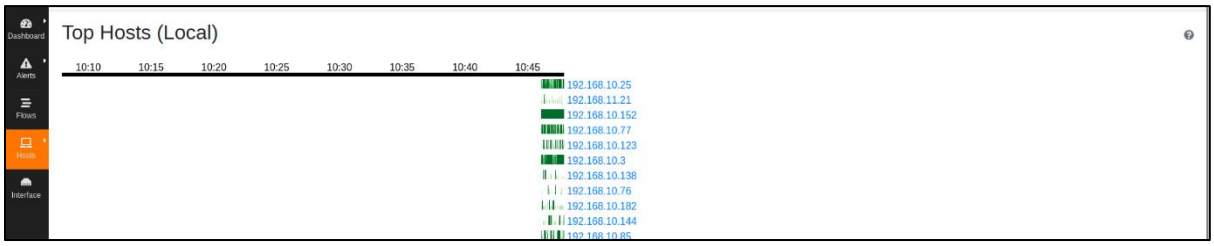




17.5.7 Top Hosts

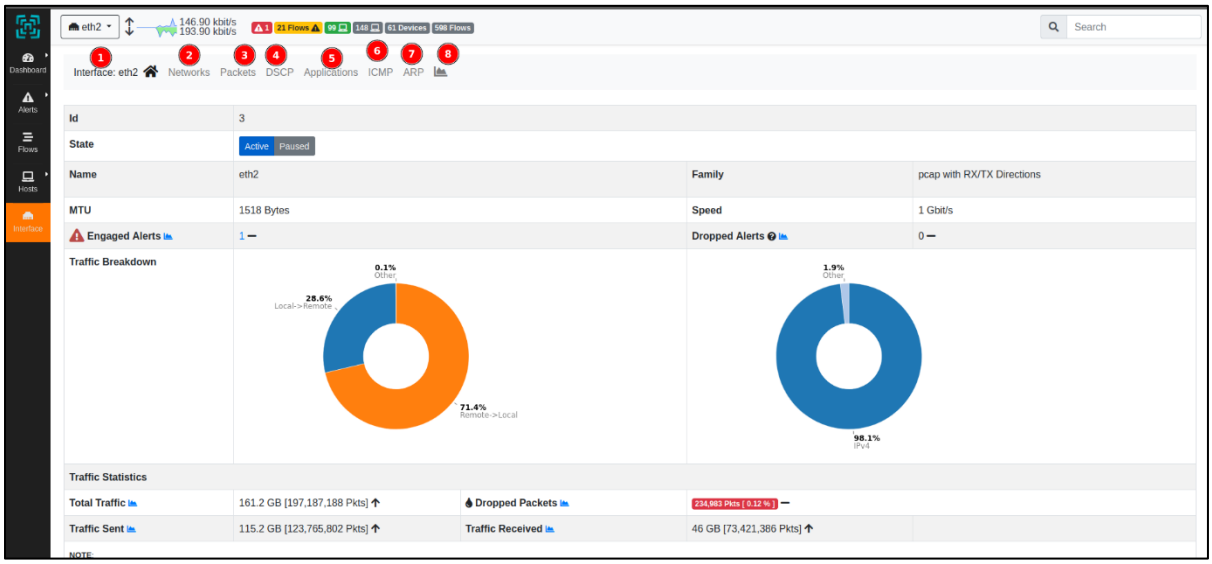
In this module, a list of devices on the local network that generate the most traffic is displayed.





17.6 Interface

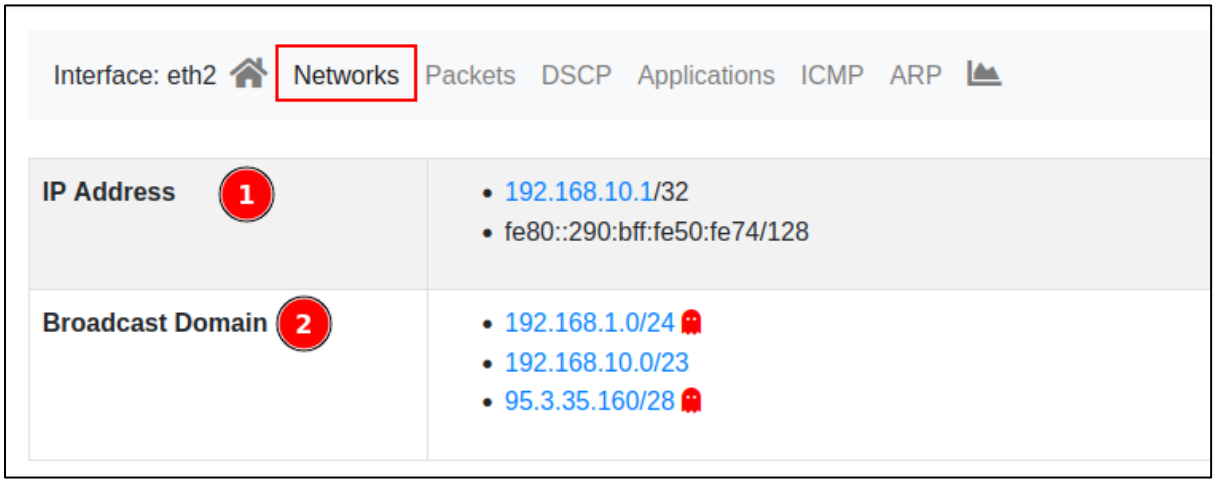
It is the section where the details of the information of the interface where traffic analysis is opened are displayed.



1	**Interface**	This is the section where the examined interface is displayed.
2	**Network**	The network addresses for the selected interface are displayed.
3	**Packets**	Shows a pie chart of the packet size distribution for the selected interface.
4	**DSCP**	The DSCP packet information for the interface is displayed.
5	**Application**	The information that passes through the interface is displayed to the application.
6	**ICMP**	The ICMP traffic for the interface is displayed.
7	**Arp**	The ARP traffic for the interface is displayed.
8	**Graphic**	The traffic for the interface is displayed graphically.

17.6.1 Networks

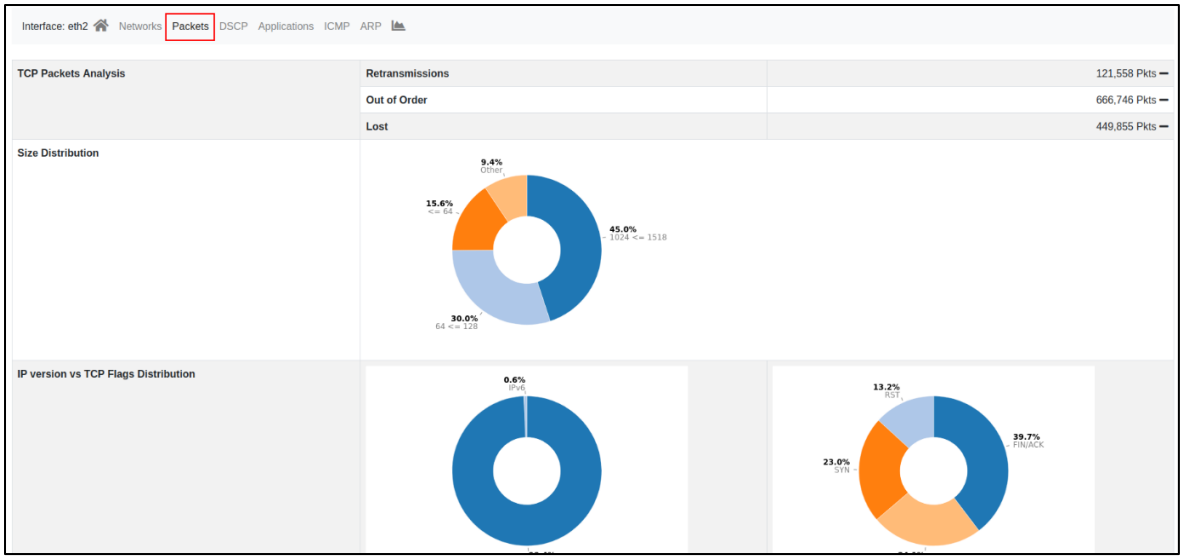
Details of the network traffic on the interface are displayed.



1	**IP Address**	The IP address information of the interface under investigation is included.
2	**Broadcast Domain**	ARP traffic is examined and broadcast domains of the interface are detected.

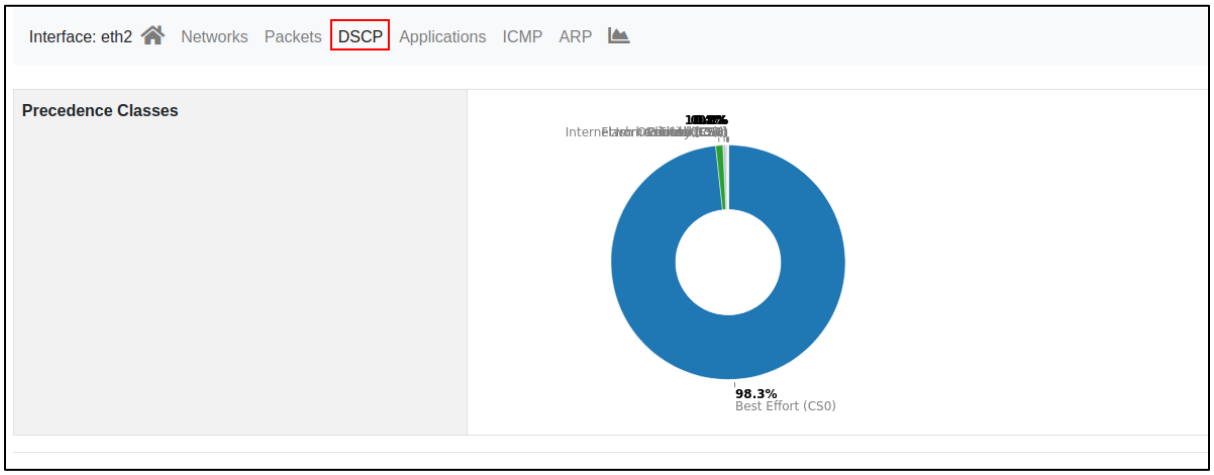
17.6.2 Packets

The distribution of packet size in traffic is displayed in the form of a pie chart.



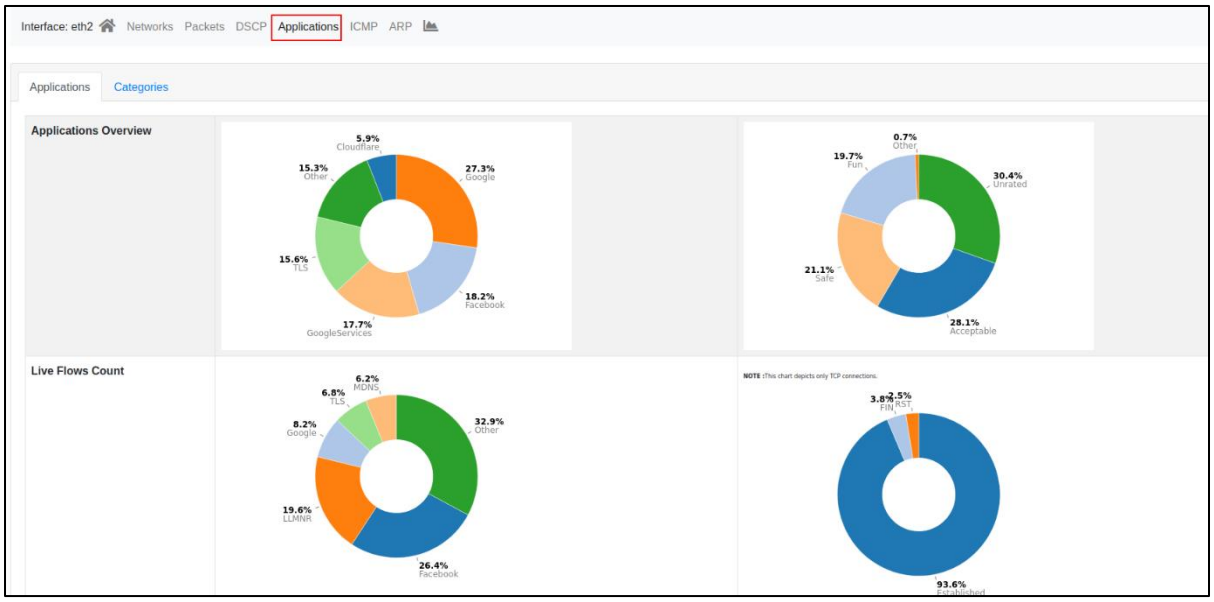
17.6.3 DSCP

DSCP is a quality service mechanism used in data transmission over the internet. In this section, you can see the DSCP distribution in the form of a pie chart.



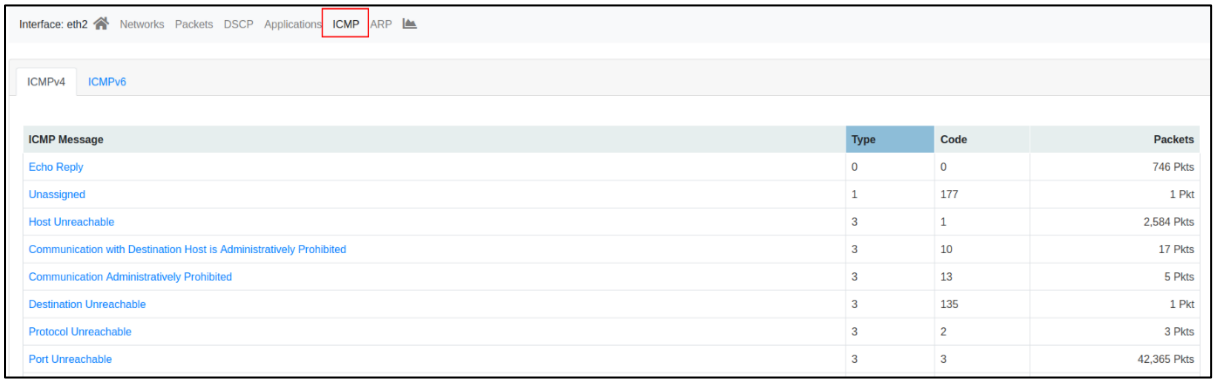
17.6.4 Applications

It is the section where we can see the application usage details in the network traffic of the interface in the form of a pie chart.



17.6.5 ICMP

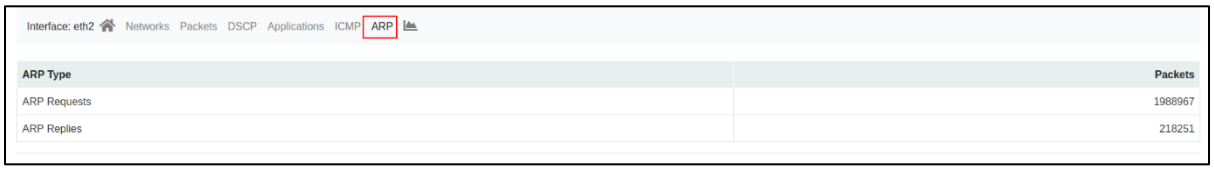
This is the section where the ICMP statistics of the interface are displayed.



ICMP Message	Type	Code	Packets
Echo Reply	0	0	746 Pkts
Unassigned	1	177	1 Pkt
Host Unreachable	3	1	2,584 Pkts
Communication with Destination Host is Administratively Prohibited	3	10	17 Pkts
Communication Administratively Prohibited	3	13	5 Pkts
Destination Unreachable	3	135	1 Pkt
Protocol Unreachable	3	2	3 Pkts
Port Unreachable	3	3	42,365 Pkts

17.6.6 ARP

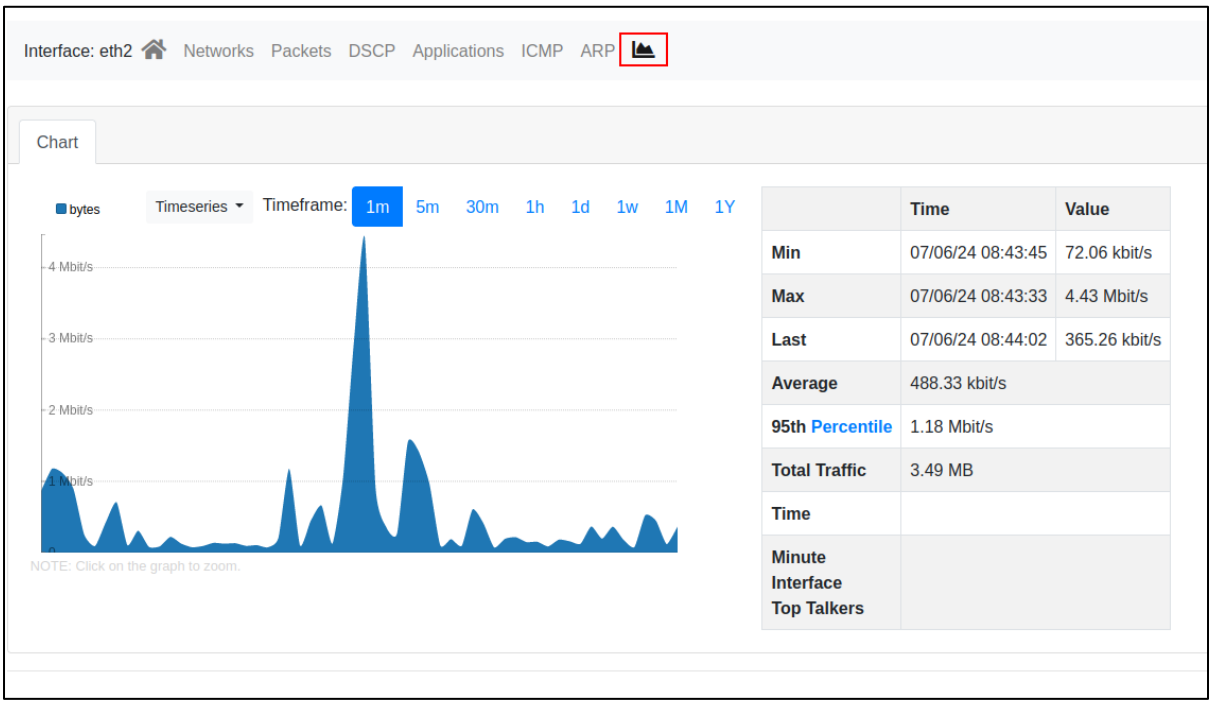
This is the section where the ARP statistics of the interface are displayed.



ARP Type	Packets
ARP Requests	1988967
ARP Replies	218251

17.6.7 Graphic

This is the section where the details of the selected interface are displayed. Traffic reports for 1 minute, 5 minutes, 30 minutes, 1 hour, 1 day, 1 week, 1 month and 1 year are displayed.

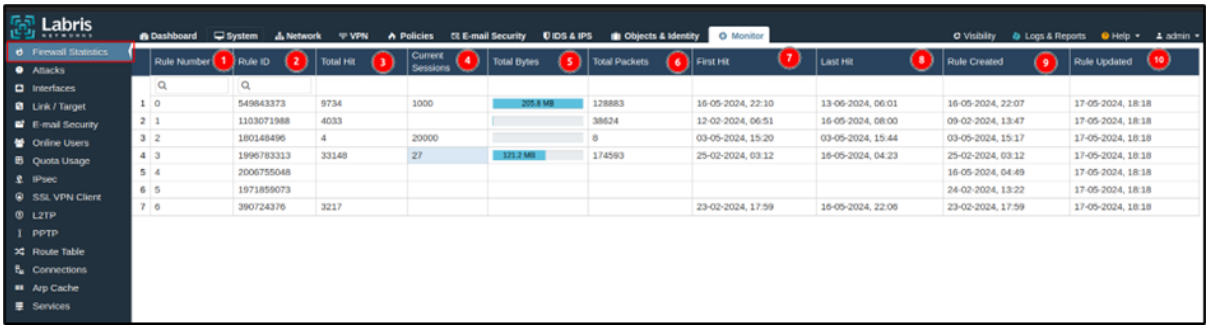


18. Monitor

It is the module where the activities on the Labris UTM device are displayed. This module displays firewall statistics, attacks, interface statistics, connection/destination statistics, active users, quota usage, IPSec connection status, users connected to SSLVPN, L2TP users, PPTP users, routing table, ARP table, and services running on the device.

18.1 Firewall Statistics

Statistics on the use of rules written in the firewall in the Policies module are displayed. The rule number, the rule ID, the match time of the rule, and the times when the rule was added and modified are displayed.

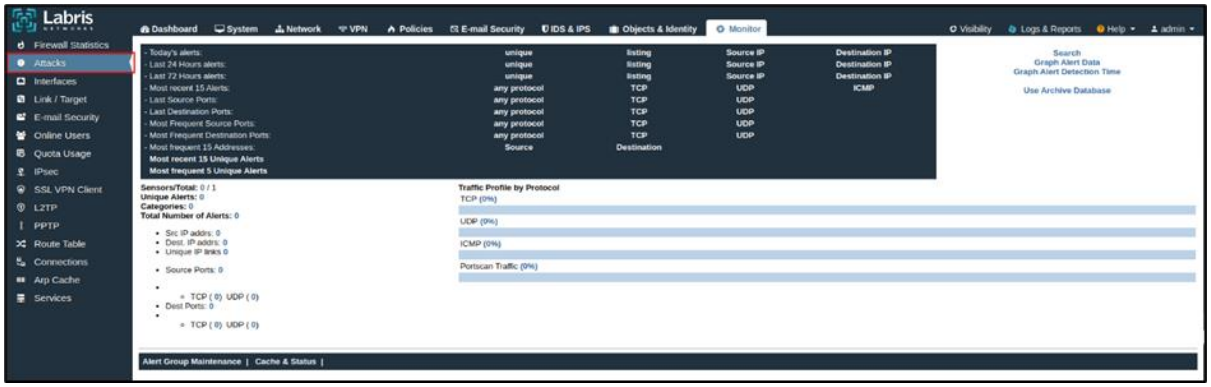


1	**Rule Number**	This is the section where the rule number is displayed.
2	**Rule ID**	This is the section where the rule ID is displayed.
3	**Total Hit**	The total mapping time in the firewall rule is displayed.
4	**Current Session**	The number of active sessions for the rule is displayed.
5	**Total Bytes**	The total byte size of the traffic that passes through the rule is displayed.
6	**Total Packets**	The total packet size of the traffic that passes through the rule is displayed.
7	**First Hit**	The time information for the first traffic that passes through the rule is displayed.
8	**Last Hit**	The time information for the last traffic that passed through the rule is displayed.

9	**Rule Created**	The time when the rule was added is displayed.
10	**Rule Updated**	The time of changes made to the rule after the time it was added is displayed.

18.2 Attacks

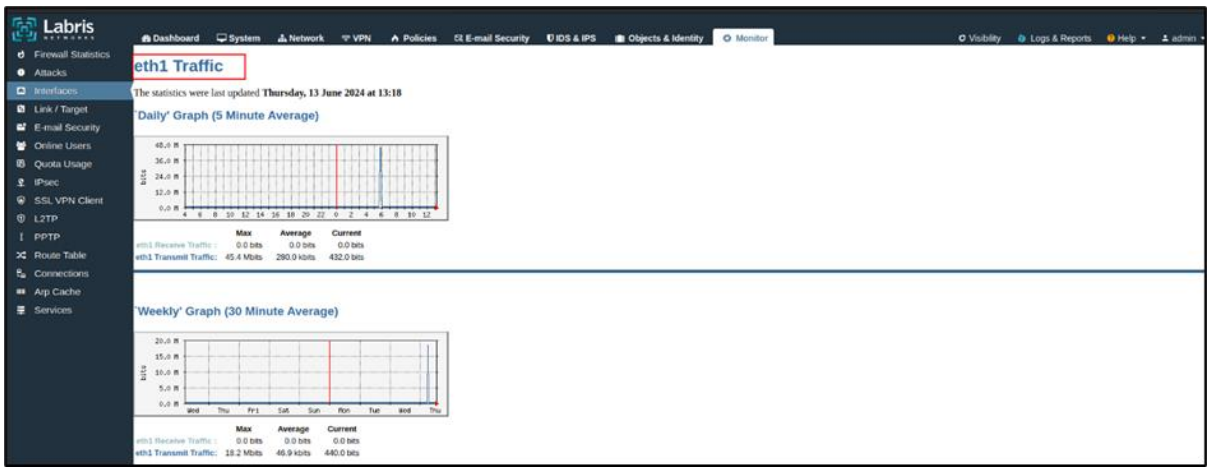
The details of the attacks coming to the Labris UTM device are displayed. IDS&IPS must be turned on to view the attack details.



18.3 Interfaces

The incoming and outgoing packets of the interfaces on the Labris UTM device are displayed graphically.

-In order to look at the details of the traffic coming and going to the interfaces, click on the interface to be displayed as a detail. The data for the selected interface is 5 min, 30 min, 2 hours and 1 day.



18.4 Link/Target

This is the section where the network access of the Labris UTM device and the access to the default gateway are displayed graphically.

1	**UTM Networking Availability**	The network availability of the Labris UTM device is displayed.
2	**Gateway Availability**	The availability of the Labris UTM device to the gateway is displayed.

-In order to view the network or gateway availability in detail, click on the UTM network availability or gateway availability to be displayed. It is displayed graphically for 3 hours, 30 hours, and 10 days.

18.5 E-Mail Security

Records of e-mail security on the Labris UTM device are displayed. Email security must be turned on.

18.6 Online Users

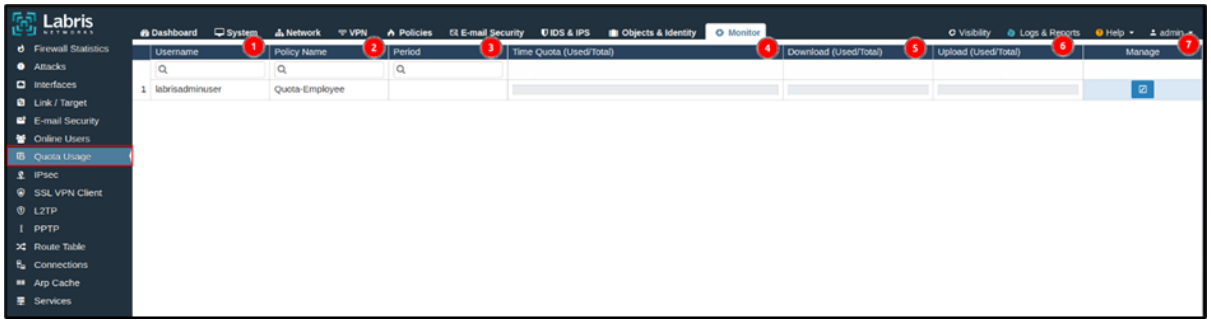
This is the section where users who are connected to wauth are displayed.

1	**Disconnect**	It is the button where users who are connected to wauth are disconnected.
2	**Flush All Users**	It is the button where all users connected to wauth are cleared.
3	**Username**	This is the section where the usernames of the users who are connected to wauth are displayed.

4	**Real Name**	This is the section where the real names of the users connected to wauth are displayed.
5	**IP**	This is the section where the IP addresses of users connected to Wauth are displayed.
6	**MAC**	This is the section where the MAC addresses of users connected to Wauth are displayed.
7	**Time Quota (Used/Total)**	The time quota of wauth users is displayed.
8	**Downloads(Used/Total)**	The download quota of wauth users is displayed.
9	**Upload (Used/Total)**	The upload quota of wauth users is displayed.
10	**Login Time**	The login time of the wauth user is displayed.
11	**Login Rule**	The wauth rule of the user who is connected to wauth is displayed.

18.7 Quota Usage

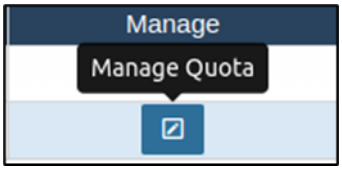
The quota usage of users who are connected to Wauth is displayed.

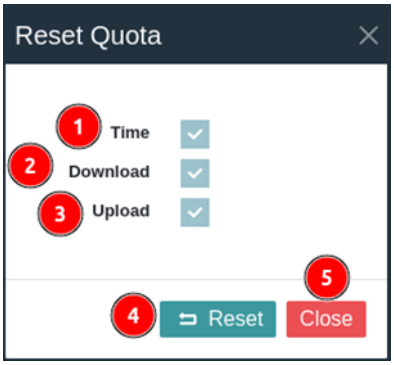


1	**Username**	The user name of the user to whom the quota policy is applied is displayed.
2	**Policy Name**	This is the section where the name of the quota policy is displayed.

3	**Period**	This is the section where the quota duration is displayed.
4	**Time Quota (Used/Total)**	The time quota of the user to whom the quota policy is applied is displayed.
5	**Downloads(Used/Total)**	The time quota of the user to whom the quota policy is applied is displayed.
6	**Upload (Used/Total)**	The upload quota of the user to whom the quota policy is applied is displayed.
7	**Manage**	This is the section where the quota policy of the users is managed. The quota policy is reset in the manage section.

-The edit button is pressed to reset the quotas of the user to whom the quota policy is applied. After pressing the edit button, the user's quotas are reset.





1	**Time**	The time quota of the user to whom the quota policy is applied is reset.
2	**Download**	The download quota of the user to whom the quota policy is applied is reset.
3	**Upload**	The upload quota of the user to whom the quota policy is applied is reset.
4	**Reset**	It is the button where the quotas are reset.

5	**Close**	It is the button where the window opened by clicking the Manage button is closed.

18.8 IPSec

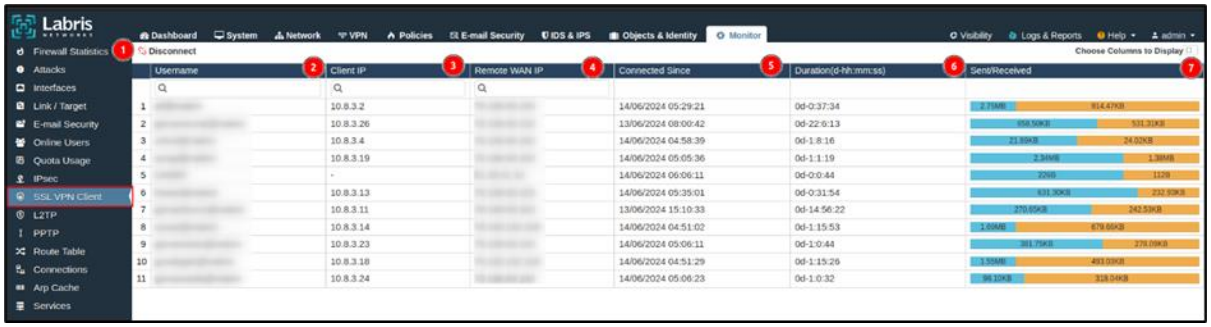
This is the section where the information of the IPSec connections on the Labris UTM device is displayed.

1	**Disconnect**	This is the button where the IPSec connection is disconnected.
2	**Reconnect**	This is the button where the IPSec connection is reconnected.
3	**Connection**	This is the section where the name of the IPSec connection is displayed.
4	**Phase 1**	It is the section where the Stage-1 connection is displayed. If a step-1 connection is provided, it is displayed as 'connected'.
5	**Local IP**	This is the section where the public IP address of the Labris UTM device with IPSec is displayed.
6	**Remote IP**	This is the section where the public IP address of the other IPSec device is displayed.
7	**Phase 2**	It is the section where the Stage-2 connection is displayed. If a Stage-2 connection is provided, it is displayed as 'connected'.
8	**Local Network**	This is the section where the local network address of the Labris UTM device with IPSec is displayed.

9	**Remote Network**	It is the section where the local network address of the other IPsec device is displayed.
10	**Byte Received/Sent**	The amount of data received and sent on the IPSec connection is displayed.
11	**Packet Received/Sent**	The amount of packets received and sent on the IPSec connection is displayed.

18.9 SSL VPN Client

It is the module where users who are connected to SSLVPN are displayed.

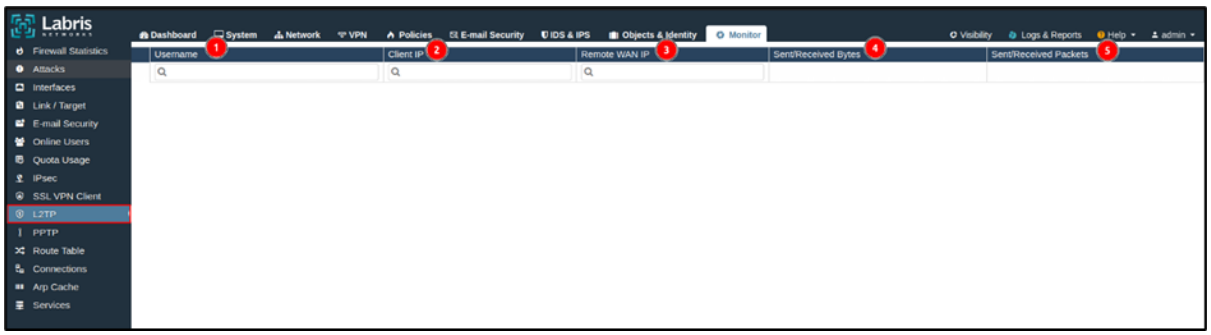


1	**Disconnect**	This is the button that disconnects the user who is connected to the SSL VPN.
2	**Username**	This is the section where the usernames of the users connected to the SSL VPN are displayed.
3	**Client IP**	Private IP addresses of users connecting to SSL VPN are displayed.
4	**Remote WAN IP**	This is the section where the public IP addresses of users connected to the SSL VPN are displayed.
5	**Connected Since**	This is the section where the time when users connected to SSL VPN is displayed.
6	**Duration(day-hour-minute-second)**	The amount of time connected to the SSL VPN is displayed in days, hours, minutes, and seconds.

7	**Sent / Received**	Display the amount of data sent and received after users connect to SSL VPN.

18.10 L2TP

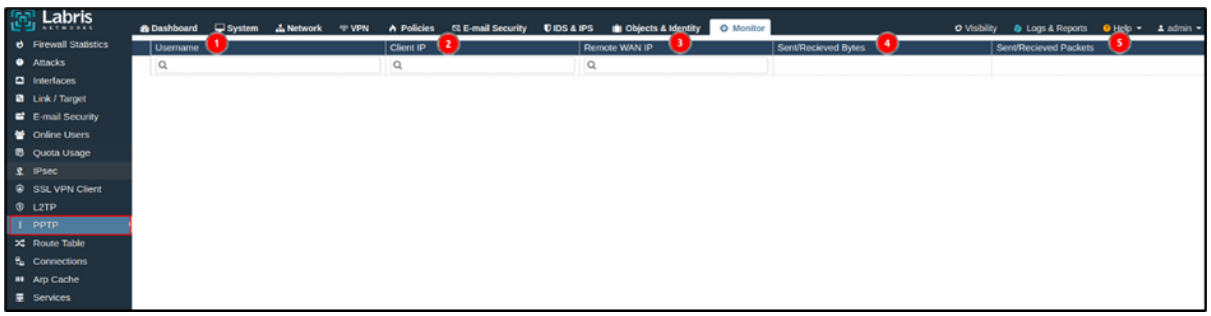
This is the module where users connected to the L2TP VPN are displayed.



1	**Username**	This is the section where the usernames of users who are connected to the L2TP VPN are displayed.
2	**Client IP**	Private IP addresses of users connecting to L2TP VPN are displayed.
3	**Remote WAN IP**	The public IP addresses of users who connect to the L2TP VPN are displayed.
4	**Sent and Received Bytes**	This is the section where the amount of data sent and received after users connect to the L2TP VPN is displayed.
5	**Sent and Received Packet**	This is the section where the amount of packets sent and received after users connect to the L2TP VPN is displayed.

18.11 PPTP

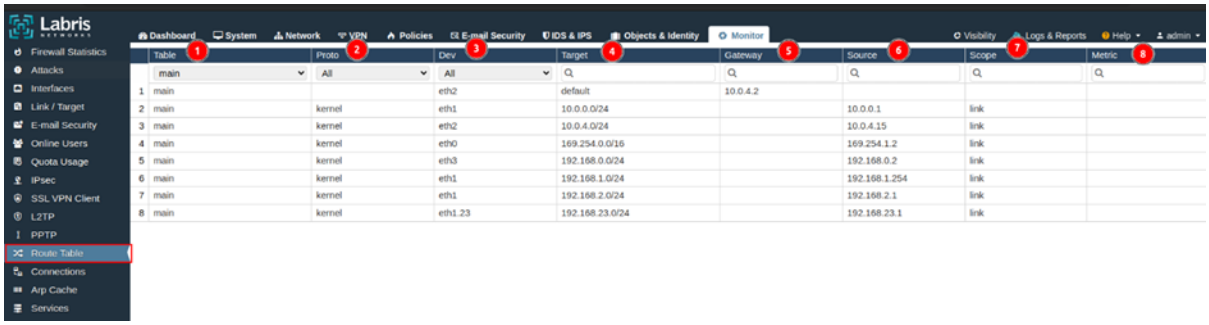
This is the module where users connected to the PPTP VPN are displayed.



1	**Username**	This is the section where the usernames of users who are connected to the PPTP VPN are displayed.
2	**Client IP**	After connecting to the PPTP VPN, the IP addresses they receive are displayed.
3	**Remote WAN IP**	Private IP addresses of users connecting to PPTP VPN are displayed.
4	**Sent and Received Bytes**	This is the section where the amount of data sent and received after users connect to the PPTP VPN is displayed.
5	**Sent and Received Packet**	This is the section where the amount of packets sent and received after users connect to the PPTP VPN is displayed.

18.12 Route Table

This is the section where the routing table on the Labris UTM device is displayed.

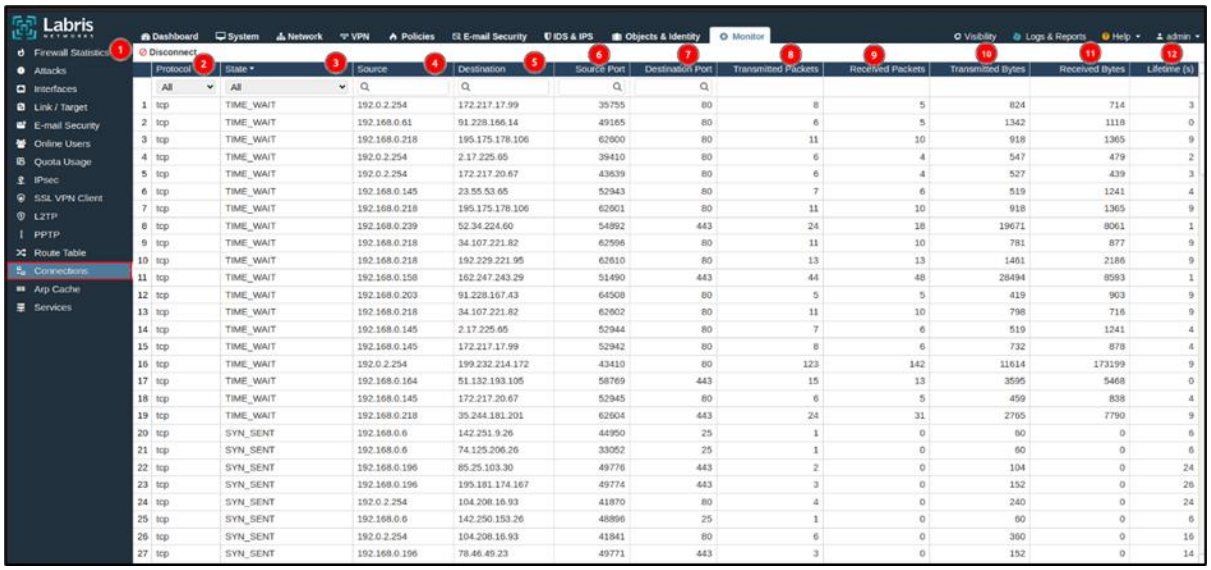


1	**Table**	This is the section where the table name of the typed route is displayed.
2	**Proto**	This is the section where the proto information of the route table is displayed.
3	**Dev**	This is the section where the interface where the route is written is displayed.
4	**Target**	This is the section where the destination IP address where the routing is written is displayed.

5	**Gateway**	This is the section where the gateway to which the routing is written is displayed.
6	**Source**	This is the section where the source IP address where the routing is written is displayed.
7	**Scope**	The scope information of the typed routing is displayed.
8	**Metric**	The metric value of the typed routing is displayed.

18.13 Connections

The connection information on the Labris UTM device is displayed.

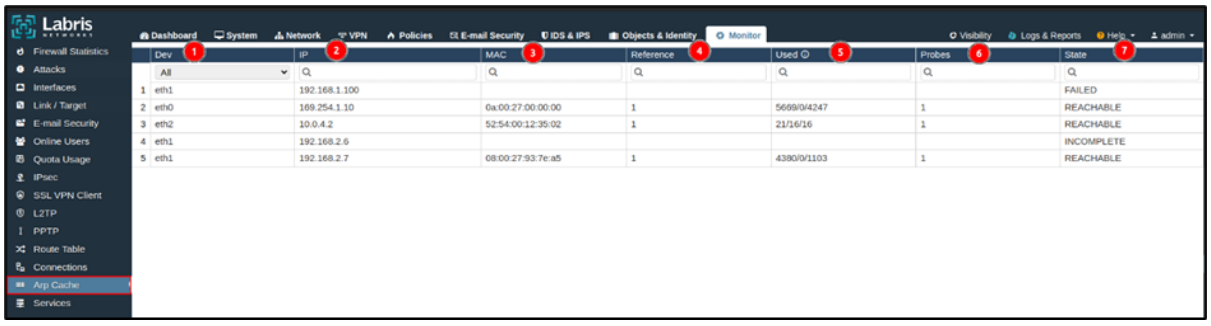


1	**Disconnect**	It is the button where the selected connection is disconnected.
2	**Protocol**	This is the section where the protocol information in the connection is displayed.
3	**State**	This is the section where the connection status is displayed.
4	**Source**	This is the section where the source IP address in the connection is displayed.

5	**Destination**	This is the section where the destination IP address in the connection is displayed.
6	**Source Port**	This is the section where the source port in the connection is displayed.
7	**Destination Port**	This is the section where the destination port in the connection is displayed.
8	**Transmitted Packets**	This is the section where the amount of packets sent on the link is displayed.
9	**Received Packets**	This is the section where the amount of packets received on the connection is displayed.
10	**Transmitted Bytes**	This is the section where the amount of data sent on the connection is displayed.
11	**Received Bytes**	This is the section where the amount of data received on the connection is displayed.
12	**Lifetime (s)**	This is the section where the waiting time of the connection is displayed.

18.14 Arp Cache

It is the section where the Arp table in the Labris UTM device is displayed.

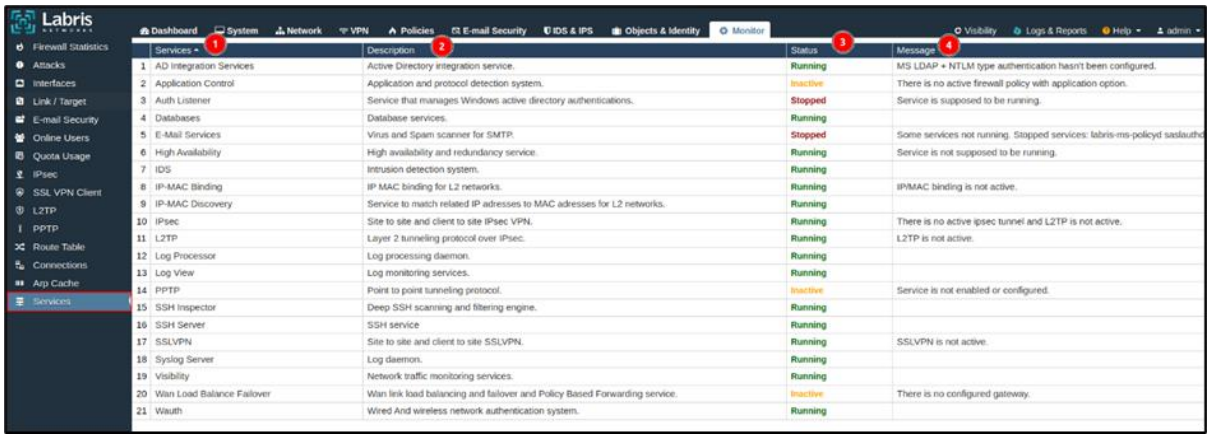


1	**Dev**	This is the section where the interface from which the Arp input is received is displayed.
2	**IP**	This is the section in the Arp table where the IP address is displayed.

3	**MAC**	This is the section in the Arp table where the MAC address is displayed.
4	**Reference**	It is the section where the reference value in the Arp table is displayed.
5	**Used**	This is the section where the number of times the Arp input is used is displayed.
6	**Probes**	Indicates the number of times an ARP query was sent for the ARP entry.
7	**State**	This is the section where the status information of the Arp entry is displayed.

18.15 Services

It is the section where the status of the running services on the Labris UTM device is displayed.

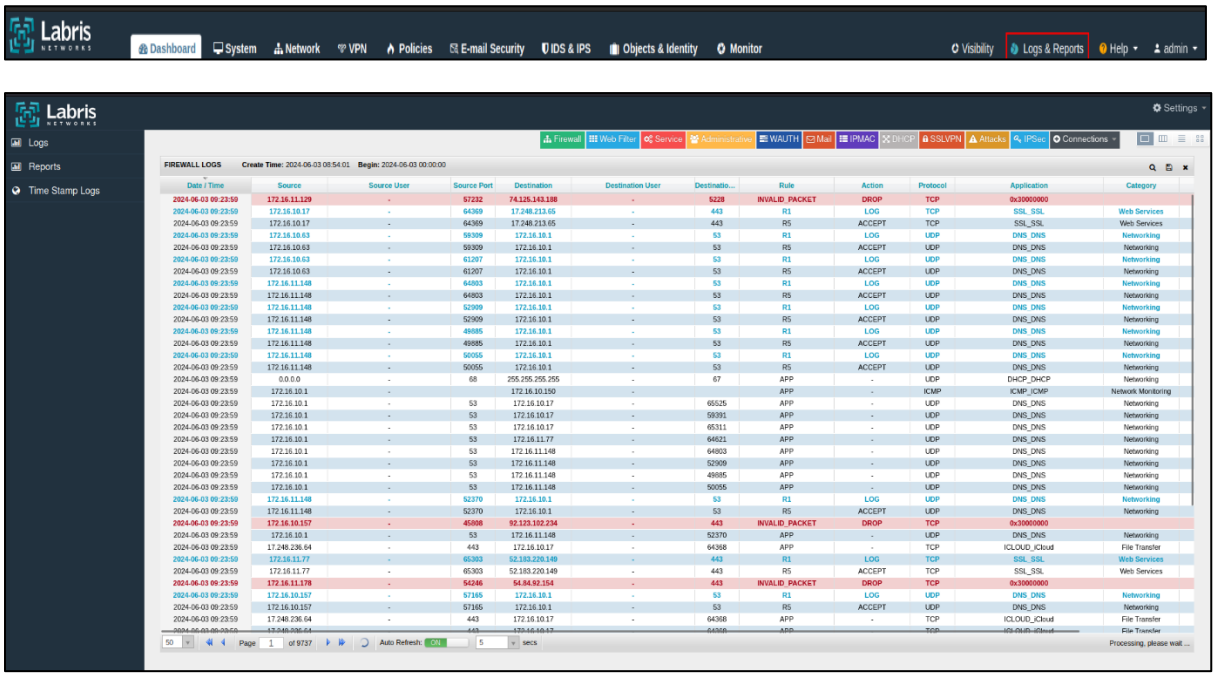


1	**Services**	It is the section where the names of the running services in the Labris UTM device are displayed.
2	**Description**	It is the section where the explanations about the running services in the Labris UTM device are displayed.
3	**State**	It is the section where the operating status of the running services in the Labris UTM device is displayed.

4	**Message**	This is the section where the names of the running services in the Labris UTM device are displayed.

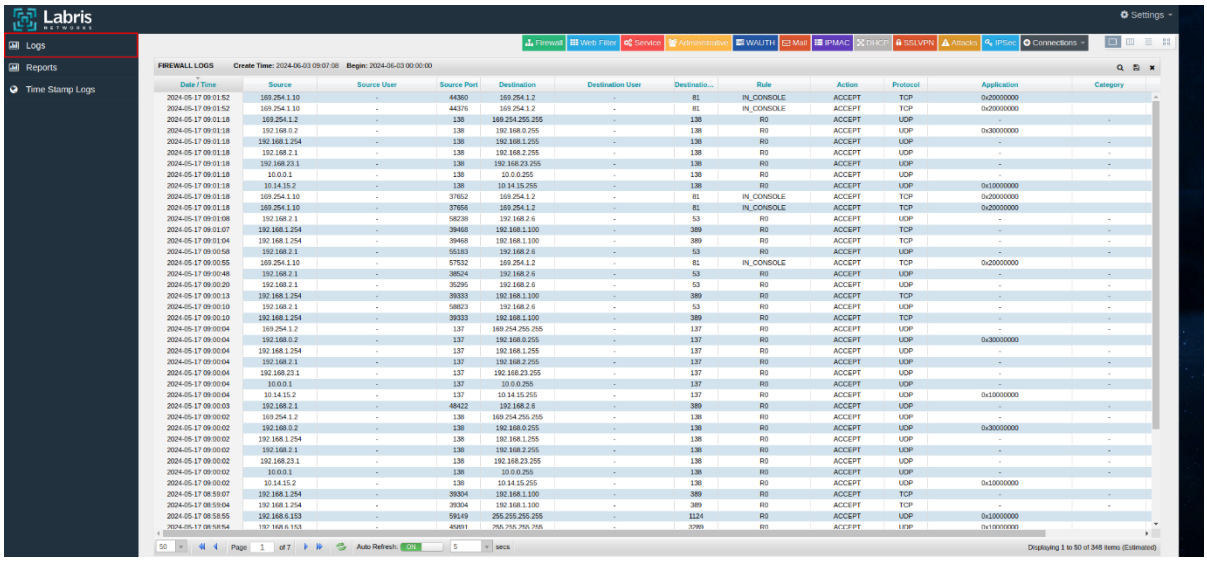
19. Logs&Reports

This is the module where the records kept on the Labris UTM device are displayed, and the records kept are reported. The Records and Reports module contains records, reports, and timestamp logs. The logs kept can be monitored instantly, or the logs kept in the archive are displayed. Click on Records and Reports to open the Records and Reports page.



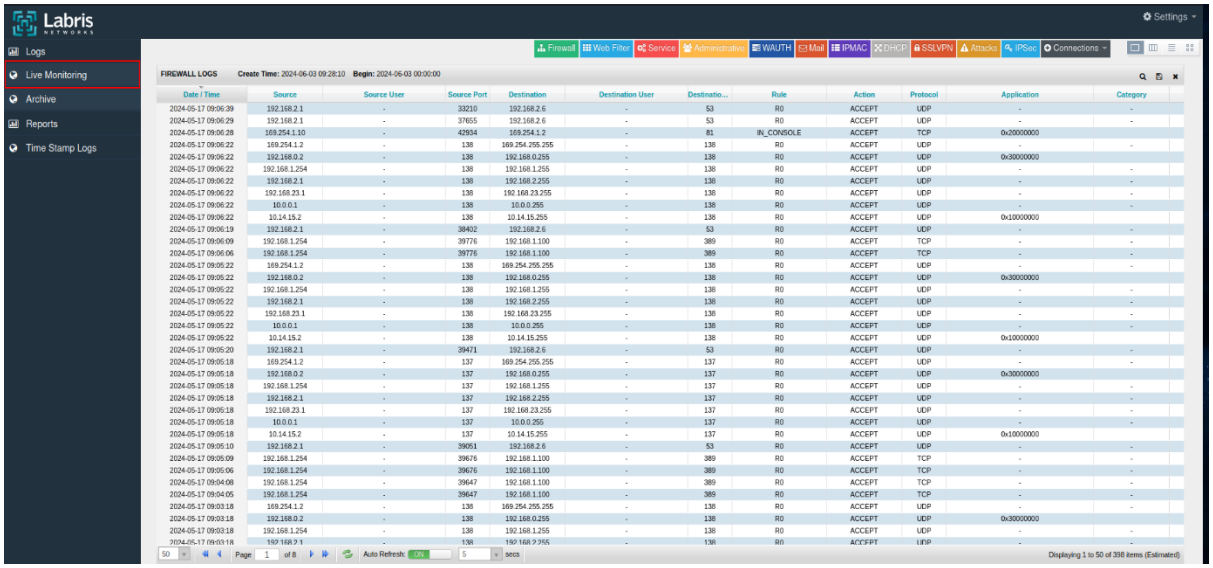
19.1 Logs

It is the module where the records kept on the Labris UTM device are displayed. In this module, the records are kept instantly, and the logs in the archive are displayed. Records kept; Firewall, Web Filter, Service, Administrative, WAUTH, Mail, IPMAC, DHCP, SSLVPN, Attacks, IPSec, and Connection logs are displayed.



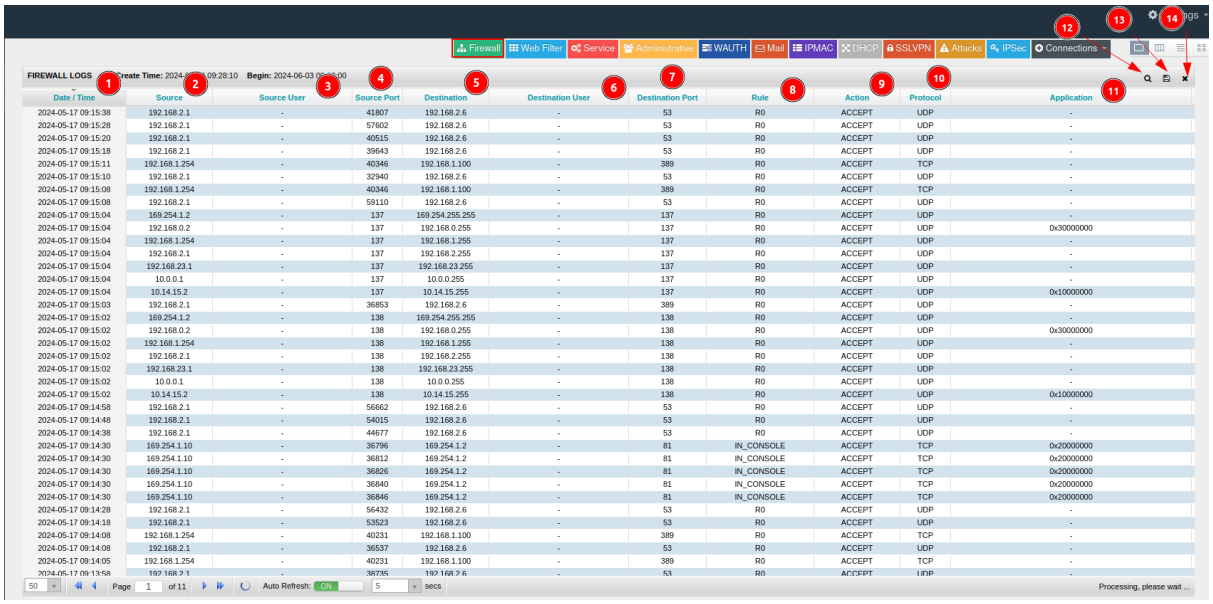
19.1.1Live Monitoring

It is the module where the logs kept on the Labris UTM device are displayed instantly. Firewall, Web Filter, Service, Administrative, WAUTH, Mail, IPMAC, DHCP, SSLVPN, Attacks, IPSec and Connection logs are displayed instantly.



19.1.1.1 Firewall

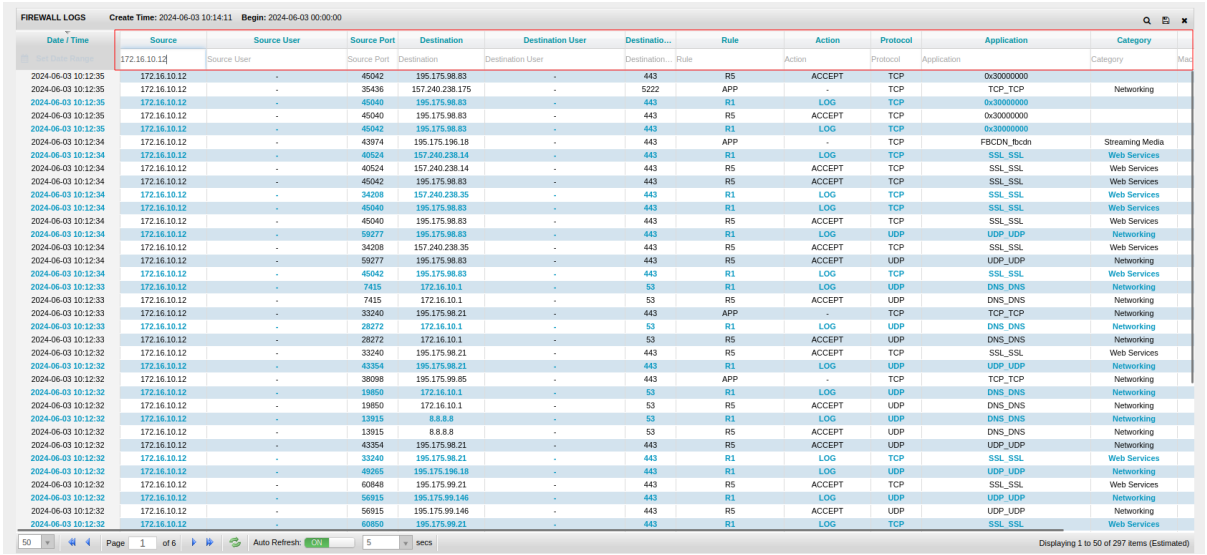
This is the section where the firewall logs kept on the Labris UTM device are displayed. Records of rules written in the Firewall module are displayed.



1	**Date / Time**	The date and time the record was kept are displayed.
2	**Source**	The source IP address information in the record is displayed.

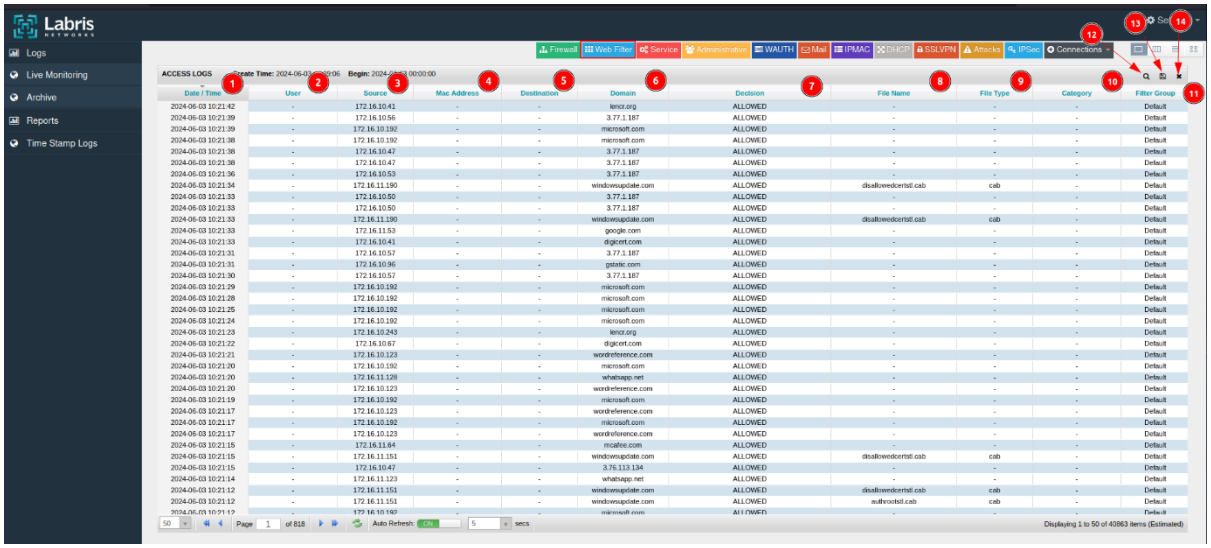
3	**Source User**	The source user information in the record is displayed. If there is no source user, it is indicated by a '-' sign.
4	**Source Port**	The source port information in the record is displayed.
5	**Destination**	The destination IP address information in the record is displayed.
6	**Destination User**	The destination user information in the record is displayed. If there is no user information in the target, it is indicated by a '-' sign.
7	**Destination Port**	The destination port information in the record is displayed.
8	**Rule**	Indicates the firewall rule through which the traffic passes. If it reads R3, it indicates that the traffic is passing through Firewall rule 3.
9	**Action**	The transaction information of the traffic is displayed. Usually, 'ACCEPT, DROP, and APP LOG' are displayed in this section.
10	**Protocol**	The protocol information in the recording is displayed. The protocols are TCP, UDP, and ICMP.
11	**Application**	The registered application information is displayed. Applications are those that are kept on the Labris UTM device.
12	**Filter**	This is the section where the records are filtered. It is filtered by typing the desired value in the section to be filtered.
13	**Export**	It is the section where the logs are exported. Logs are exported in TXT and CVS formats.
14	**Delete**	It is the section where the logs are deleted.

-Click the filtering button to filter the firewall records. Filtering is done by typing the information, such as the IP address, user, port, etc., to be filtered.



19.1.1.2 Web Filter

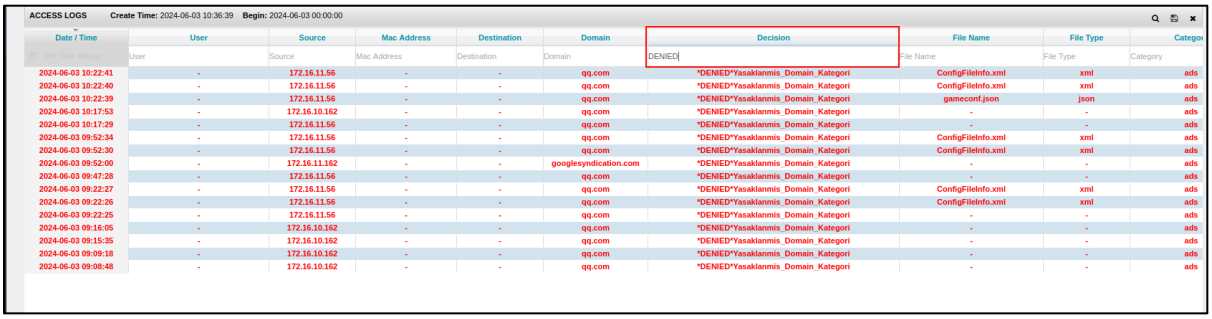
Web filter records kept in the Labris UTM device are displayed instantly. To view Web Filter records, HTTP or HTTPS filtering rules must be written in the NAT module. In the case of writing an HTTPS filtering rule, certificates must be installed on users' network devices.



1	**Date / Time**	The date and time the log was kept are displayed.
2	**User**	The user information in the Web Filter records is displayed.

3	**Source**	The source IP information in the Web Filter records is displayed.
4	**Mac Address**	The MAC address information is displayed. If there is no Mac address information, the '-' sign is displayed.
5	**Destination**	The destination IP information in the record is displayed.
6	**Domain**	The domain address in the record is displayed.
7	**Decision**	The decision information in the record is displayed. Decisions are 'ALLOWED and DENIED'.
8	**File Name**	The file name in the Web Filter record is displayed. If there is no file name in the record, it is shown as '-'.
9	**File Type**	The file type in the Web Filter record is displayed. If there is no file type in the record, it is displayed as '-'.
10	**Category**	The category type in the Web Filter records is displayed. If there is no category type in the record, it is displayed as '-'.
11	**Filter Group**	This is the section where the Filter group created in the Web Filter module is displayed.
12	**Filter**	This is the section where the records are filtered. It is filtered by typing the desired value in the section to be filtered.
13	**Export**	It is the section where the logs are exported. Logs are exported in TXT and CVS formats.
14	**Delete**	It is the section where the logs are deleted.

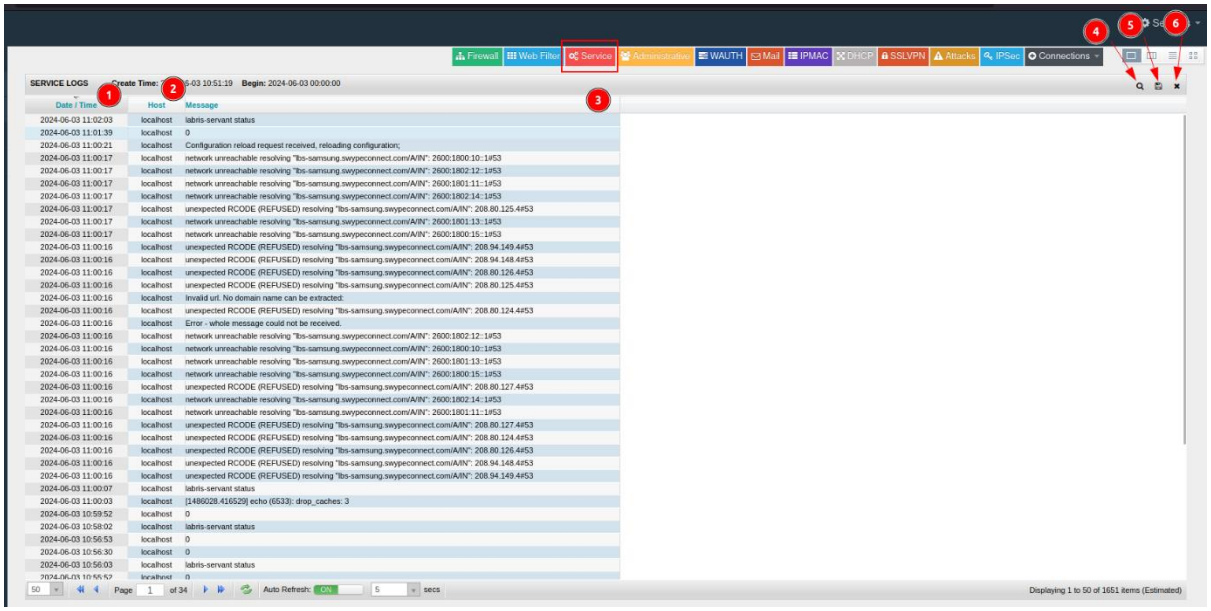
-Click on the filtering button to filter the Web Filter records. Filtering is done by typing the source IP address, user, domain, decision, etc. information to be filtered.



-Click the download button to download the web filter records. The download is done by entering the file type and file name to be downloaded.

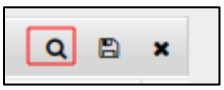
19.1.1.3 Service

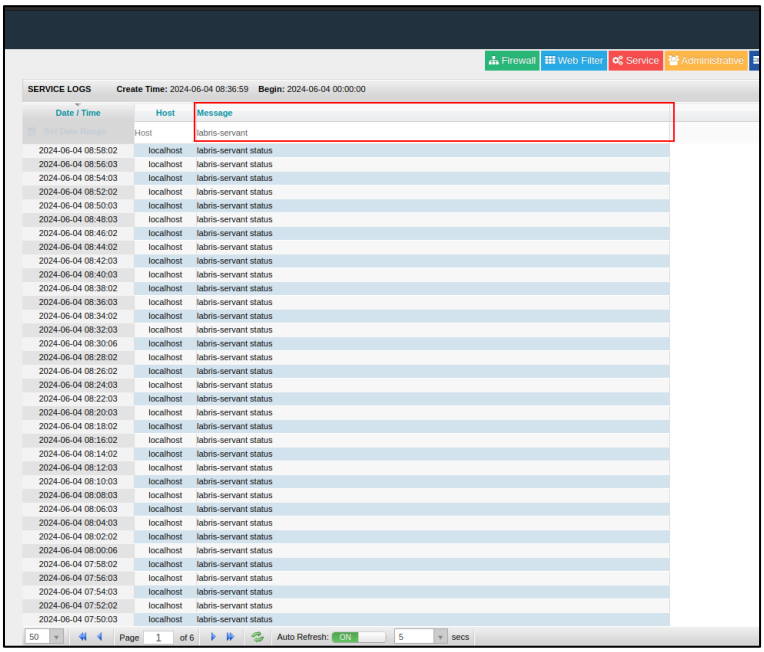
Service records are displayed instantly on the Labris UTM device.



1	**Date / Time**	The date and time the record was kept are displayed.
2	**Host**	The name of the Labris UTM device is displayed.
3	**Message**	The message of the service records is displayed.
4	**Filter**	This is the section where the records are filtered. It is filtered by typing the desired value in the section to be filtered.
5	**Export**	It is the button where the kept logs are exported. Logs are exported in TXT and CVS formats.
6	**Delete**	It is the button where the kept logs are deleted.

-Click the filtering button to filter the service records. Filtering is done by typing the date, hostname, and message information to be filtered.

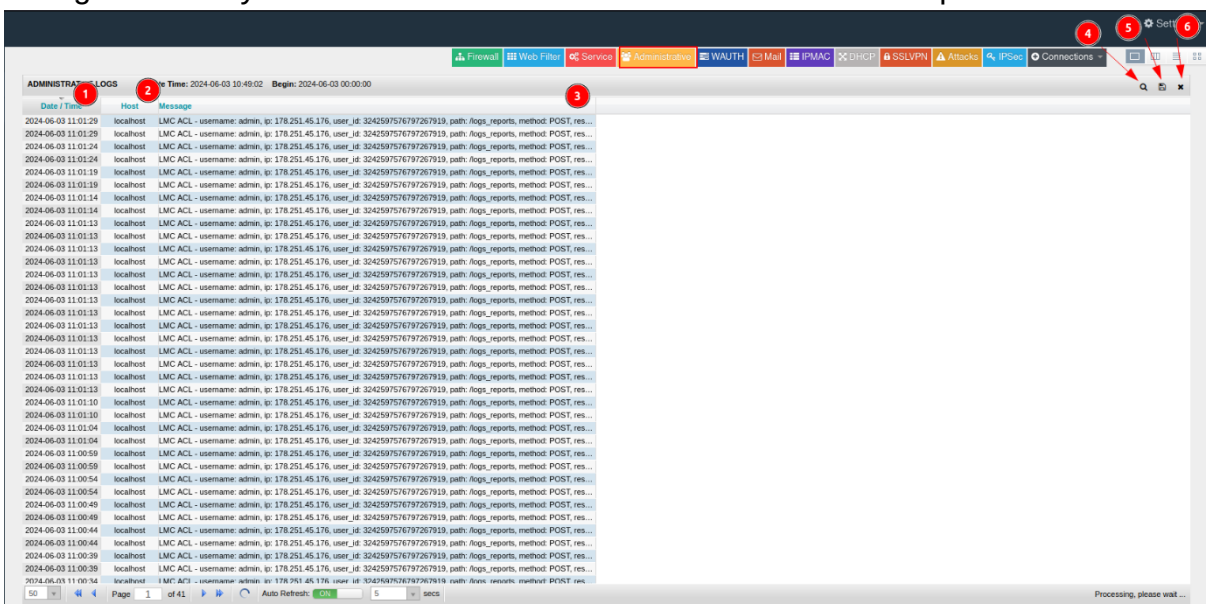




-Click the download button to download the web filter records. The download is done by entering the file type and file name to be downloaded.

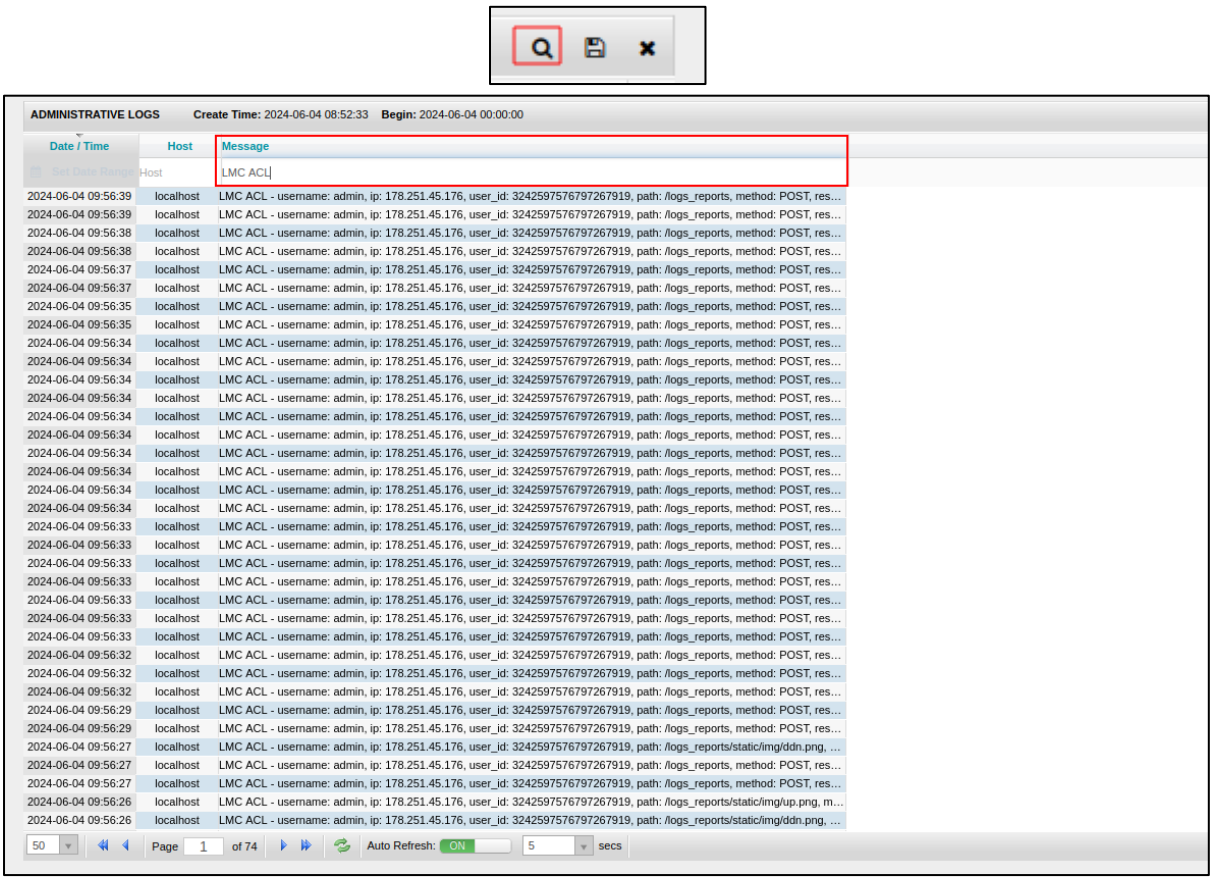
19.1.1.4 Administrative

Administrative records on the Labris UTM device are displayed. Records of the changes made by the users connected to the web interface are kept.

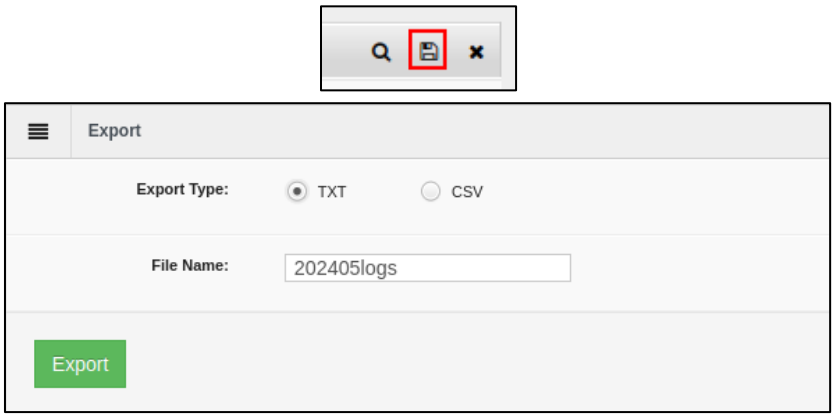


1	**Date / Time**	The date and time the record was kept are displayed.
2	**Host**	The name of the Labris UTM device is displayed.
3	**Message**	A description of the administrative logs is displayed.
4	**Filter**	This is the section where the records are filtered. It is filtered by typing the desired value in the section to be filtered.
5	**Export**	It is the section where the logs are exported. Logs are exported in TXT and CVS formats.
6	**Delete**	It is the button where the kept logs are deleted.

-Click the filtering button to filter the administrative records. Filtering is done by typing the date, hostname, and message information to be filtered.

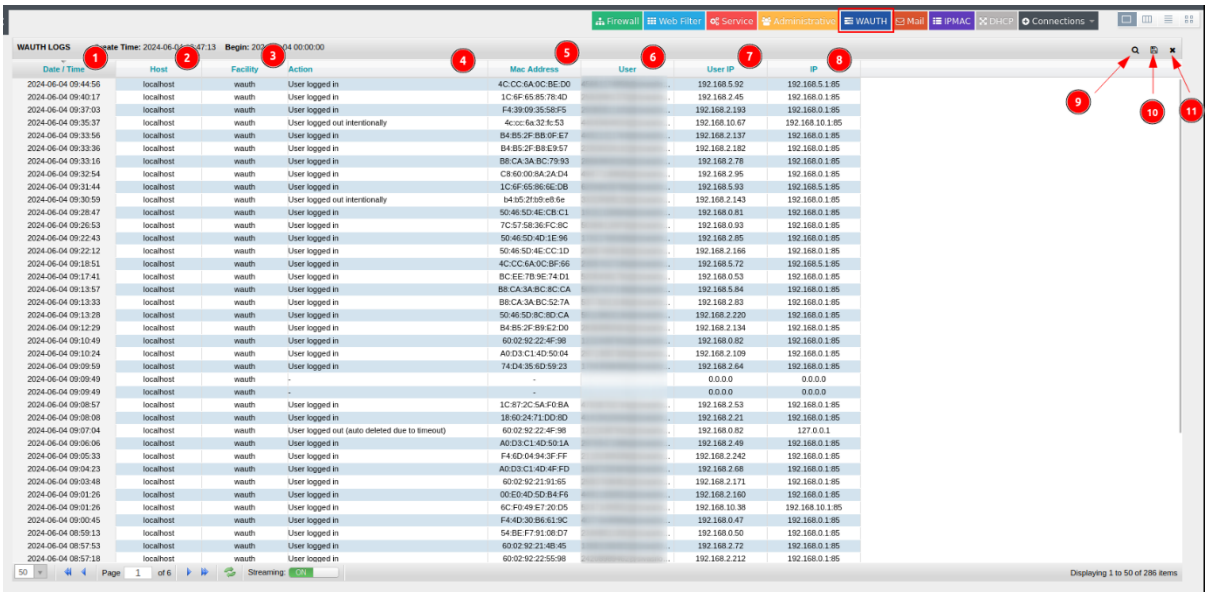


-Click the download button to download the administrative records. The download is done by entering the file type and file name to be downloaded.



19.1.1.5 WAUTH

Records related to the user connected to WAUTH are displayed.

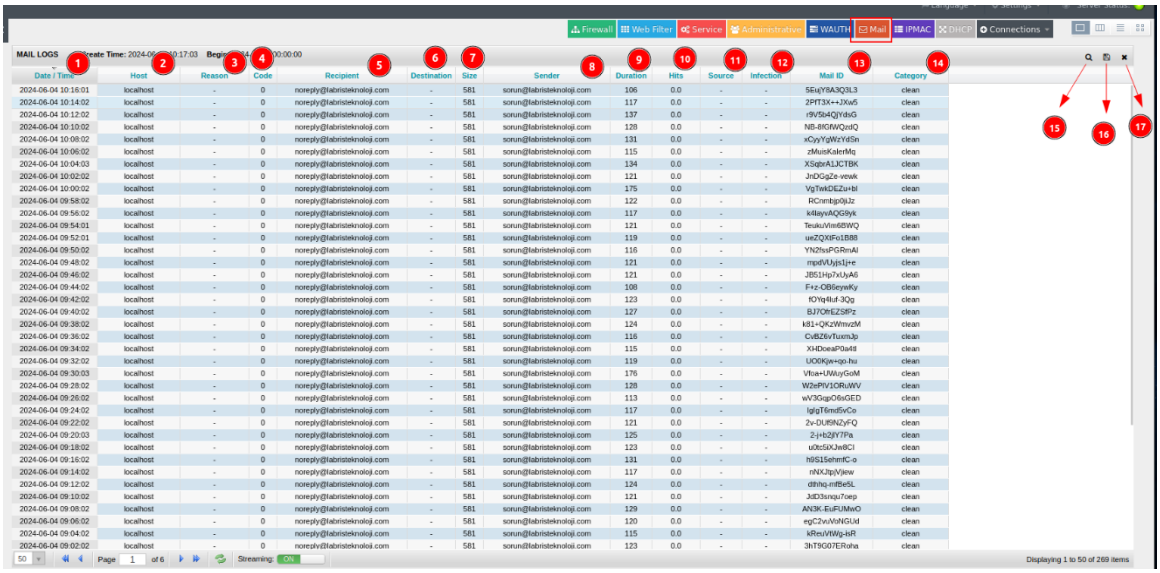


1	**Date / Time**	The date and time the record was kept are displayed.
2	**Host**	The name of the Labris UTM device is displayed.
3	**Facility**	Indicates the module in which the record is kept.
4	**Action**	The transaction information of the user connecting to Wauth is displayed.
5	**MAC Address**	The MAC address information of the user connecting to Wauth is displayed.
6	**User**	This is the section where the name of the user connecting to Wauth is displayed.
7	**User IP**	This is the section where the IP address of the user connecting to Wauth is displayed.
8	**IP**	The IP address of the interface through which Wauth is opened is displayed.
9	**Filter**	This is the section where the records are filtered. It is filtered by typing the desired value in the section to be

		filtered.
10	**Export**	It is the section where the logs are exported. Logs are exported in TXT and CVS formats.
11	**Delete**	It is the button where the kept logs are deleted.

19.1.1.6 Mail

This is the section where mail records are kept and records are displayed in the Labris UTM device.



1	**Date / Time**	The date and time the record was kept are displayed.
2	**Host**	The name of the Labris UTM device is displayed.
3	**Reason**	This is the section where the reason for sending the mail is displayed.
4	**Code**	This is the section where the code of mail is displayed.
5	**Recipient**	This is the section where the recipient address of the mail is displayed.

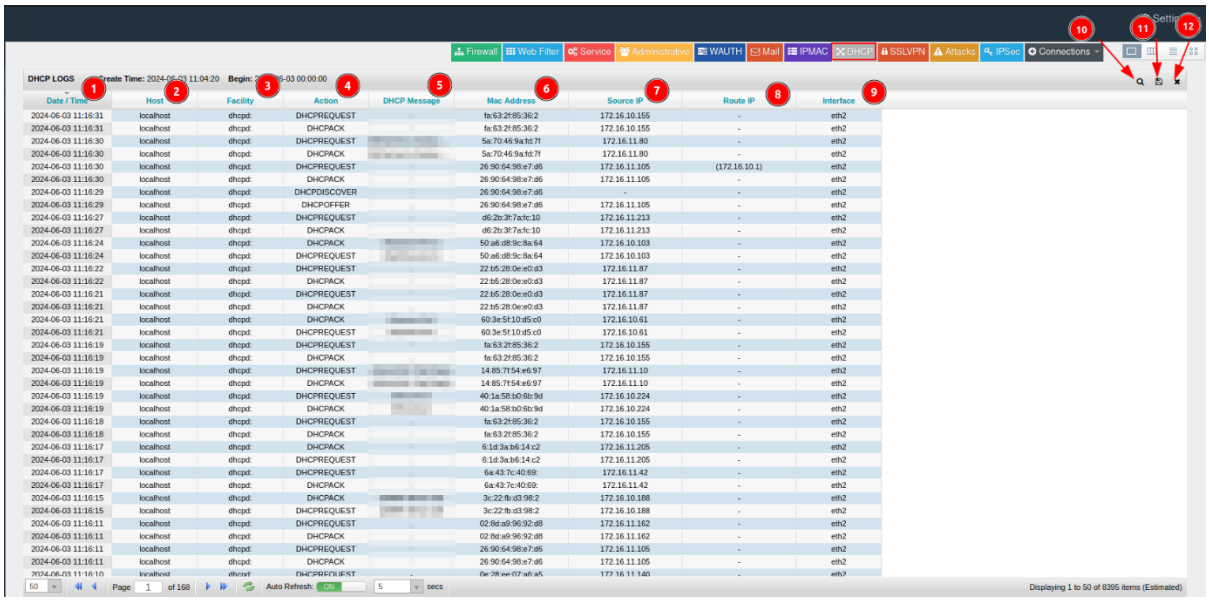
6	**Destination**	This is the section where the mail destination address is displayed.
7	**Size**	The mail size is displayed.
8	**Sender**	The address that sent the mail is displayed.
9	**Duration**	The time it takes to send mail is displayed.
10	**Hits**	The delivery value of the mail is displayed.
11	**Source**	The source of the mail is displayed.
12	**Infection**	The infection value of the mail is displayed.
13	**Mail ID**	The mail code is displayed.
14	**Category**	The Mail category is displayed.
15	**Filter**	This is the section where the records are filtered. It is filtered by typing the desired value in the section to be filtered.
16	**Export**	It is the section where the logs are exported. Logs are exported in TXT and CVS format.
17	**Delete**	It is the button where the kept logs are deleted.

19.1.1.7 IP/MAC

IPMAC records are displayed on the Labris UTM device.

19.1.1.8 DHCP

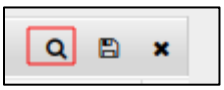
If the Labris UTM device is used in the DHCP server role, the DHCP records are displayed.

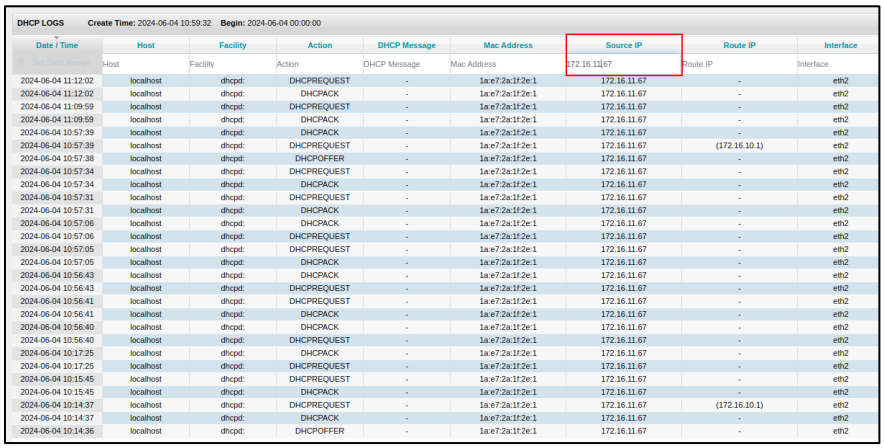


1	**Date / Time**	The date and time the record was kept is displayed.
2	**Host**	The name of the Labris UTM device is displayed.
3	**Facility**	The module in which the recording is kept is displayed.
4	**Action**	This is the section where the process step of the DHCP record is displayed.
5	**DHCP Message**	The DHCP message in the record is displayed.
6	**MAC Address**	The Mac address made the DHCP request is displayed.
7	**Source IP**	The IP address that receives the IP from DHCP is displayed.
8	**Route IP**	The IP address of the router is displayed.
9	**Interface**	The interface on which DHCP is running is displayed.

10	**Filter**	This is the section where the records are filtered. It is filtered by typing the desired value in the section to be filtered.
11	**Export**	It is the section where the logs are exported. Logs are exported in TXT and CVS formats.
12	**Delete**	It is the button where the kept logs are deleted.

-Click the filtering button to filter DHCP records. Filtering is done by typing the date, hostname, and message information to be filtered.

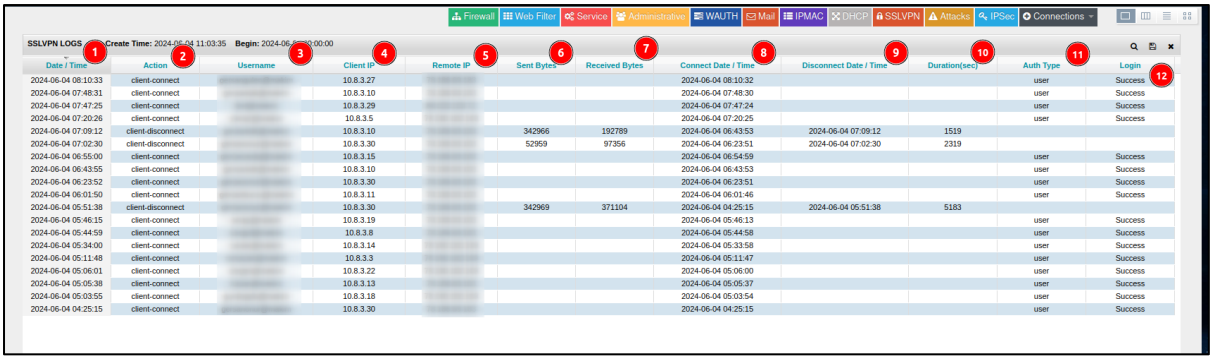




-The download button is pressed to download the DHCP records. The download is done by entering the file type and file name to be downloaded.

19.1.1.9 SSLVPN

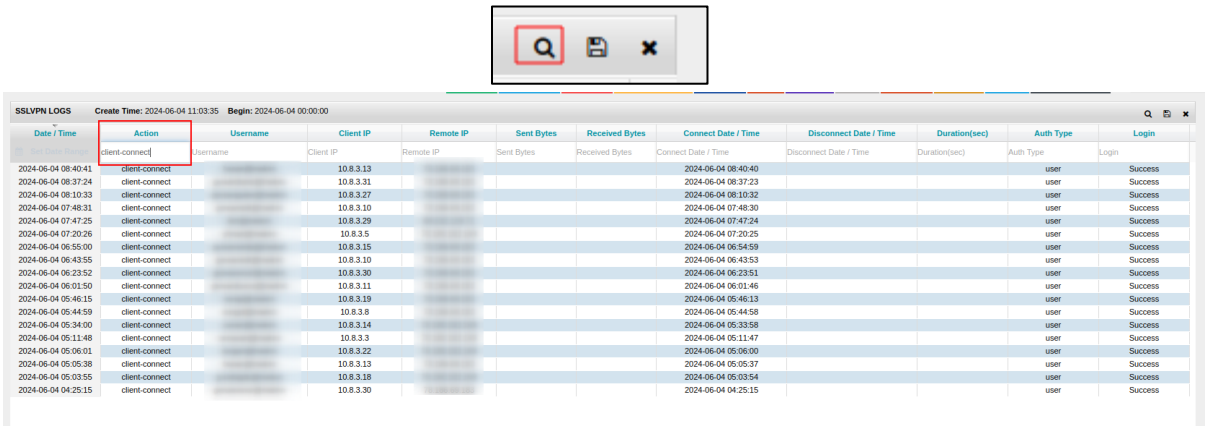
Records of users who are connected to SSLVPN are displayed.



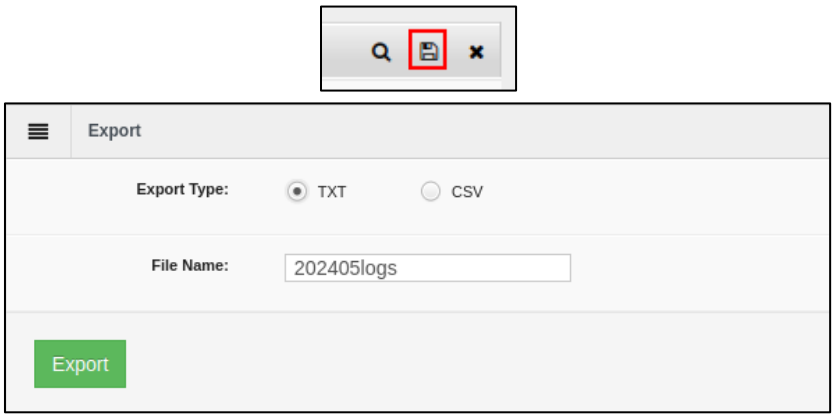
1	**Date / Time**	The date and time the record was kept are displayed.
2	**Action**	It is the section where the operation of the kept record is displayed. Depending on the user's connection status, it says ‘client connected’ or ‘client disconnected’
3	**Username**	The usernames of users who connect to SSLVPN are displayed.
4	**Client IP**	This is the section where the IP address of the user connected to SSLVPN is displayed. These are the IP addresses given by Labris UTM when connected to SSLVPN.
5	**Remote IP**	The Public IP addresses connected to SSLVPN are displayed.
6	**Sent Byte**	The byte size sent on the SSLVPN connection is displayed.
7	**Received Byte**	The received byte size on the SSLVPN connection is displayed.
8	**Connect Date / Time**	The date and time of connecting to SSLVPN are displayed.
9	**Disconnect Date/Time**	The date and time of disconnection from SSLVPN are displayed

10	**Duration (Sec)**	The amount of time you have been connected to SSLVPN is displayed.
11	**Auth Type**	The login type of users logged in to SSLVPN is displayed.
12	**Login**	This is the section where the login record is kept in the connection to SSLVPN.

-Click on the filtering button to filter SSLVPN records. Filtering is done by typing the date, hostname, and message information to be filtered.

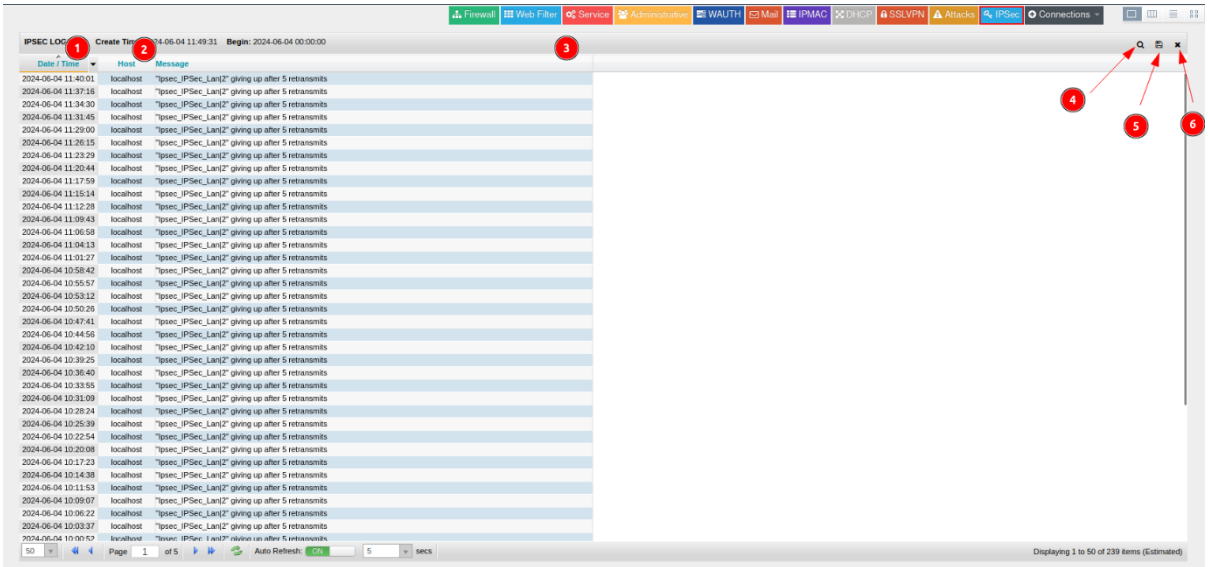


-Click the download button to download the SSLVPN recordings. The download is done by entering the file type and file name to be downloaded.



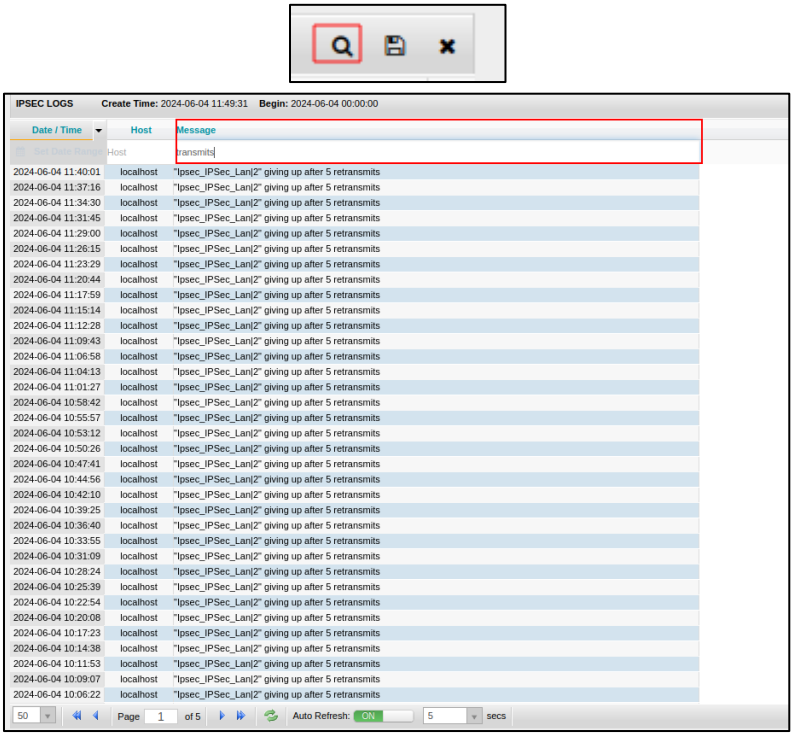
19.1.1.10 IPSec

The IPSec records held on the Labris UTM device are displayed.

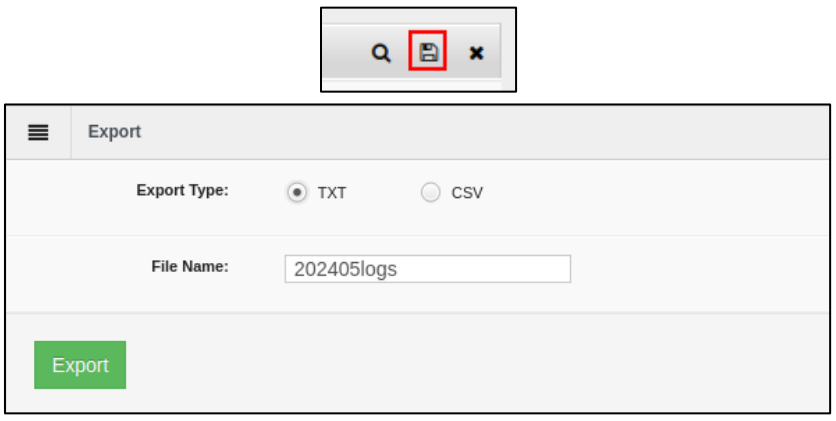


1	**Date / Time**	The date and time the record was kept is displayed.
2	**Host**	The name of the Labris UTM device is displayed.
3	**Message**	A description of the IPSec logs is displayed.
4	**Filter**	This is the section where the records are filtered. It is filtered by typing the desired value in the section to be filtered.
5	**Export**	It is the section where the logs are exported. Logs are exported in TXT and CVS formats.
6	**Delete**	It is the button where the kept logs are deleted.

-Click the filter button to filter the IPSec records. Filtering is done by typing the date, hostname, and message information to be filtered.

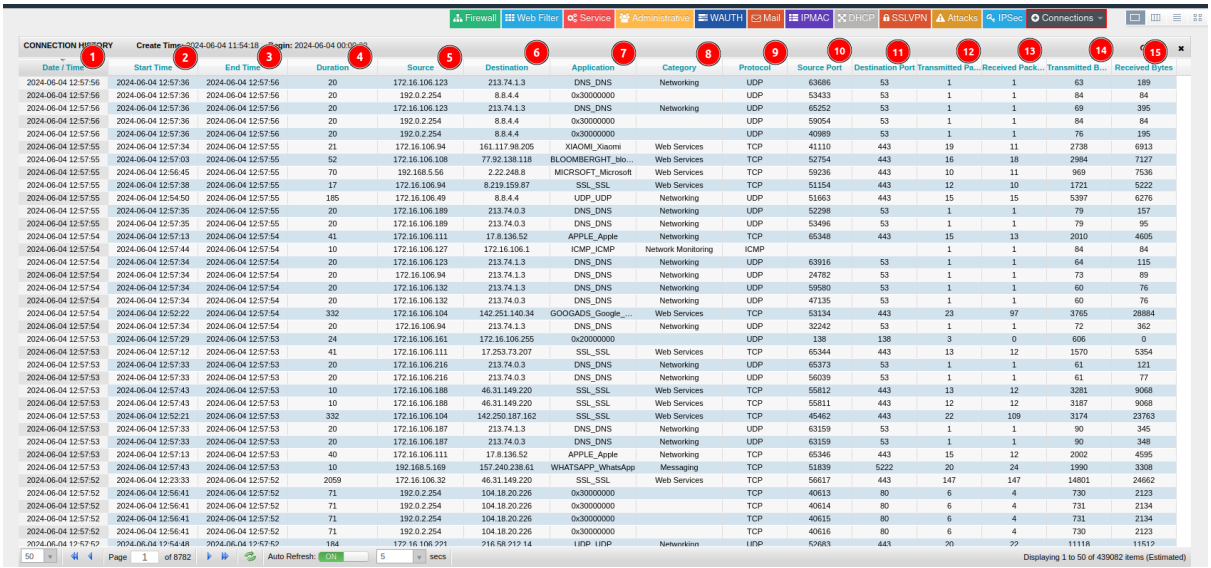


-Click the download button to download the IPSec records. The download is done by entering the file type and file name to be downloaded.



19.1.1.11 Connections

Connection logs kept in the Labris UTM device are displayed. There are details of incoming and outgoing packets in the traffic to the device.

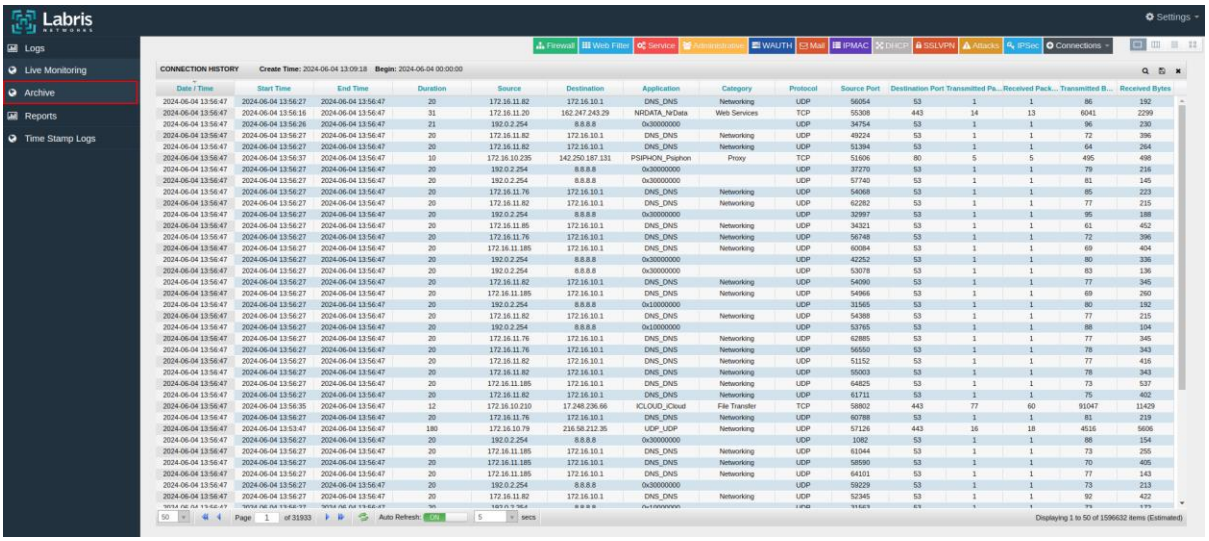


1	**Date / Time**	The date and time the record was kept are displayed.
2	**Start Time**	The start time of establishing the connection is displayed.
3	**End Time**	The end time of the connection is displayed.
4	**Duration**	This is the section where the connection time is displayed.
5	**Source**	This is the section where the source IP information is displayed.
6	**Destination**	This is the section where the destination IP information is displayed.
7	**Application**	The types of applications in the connection record are displayed.
8	**Category**	The category types in the connection record are displayed.

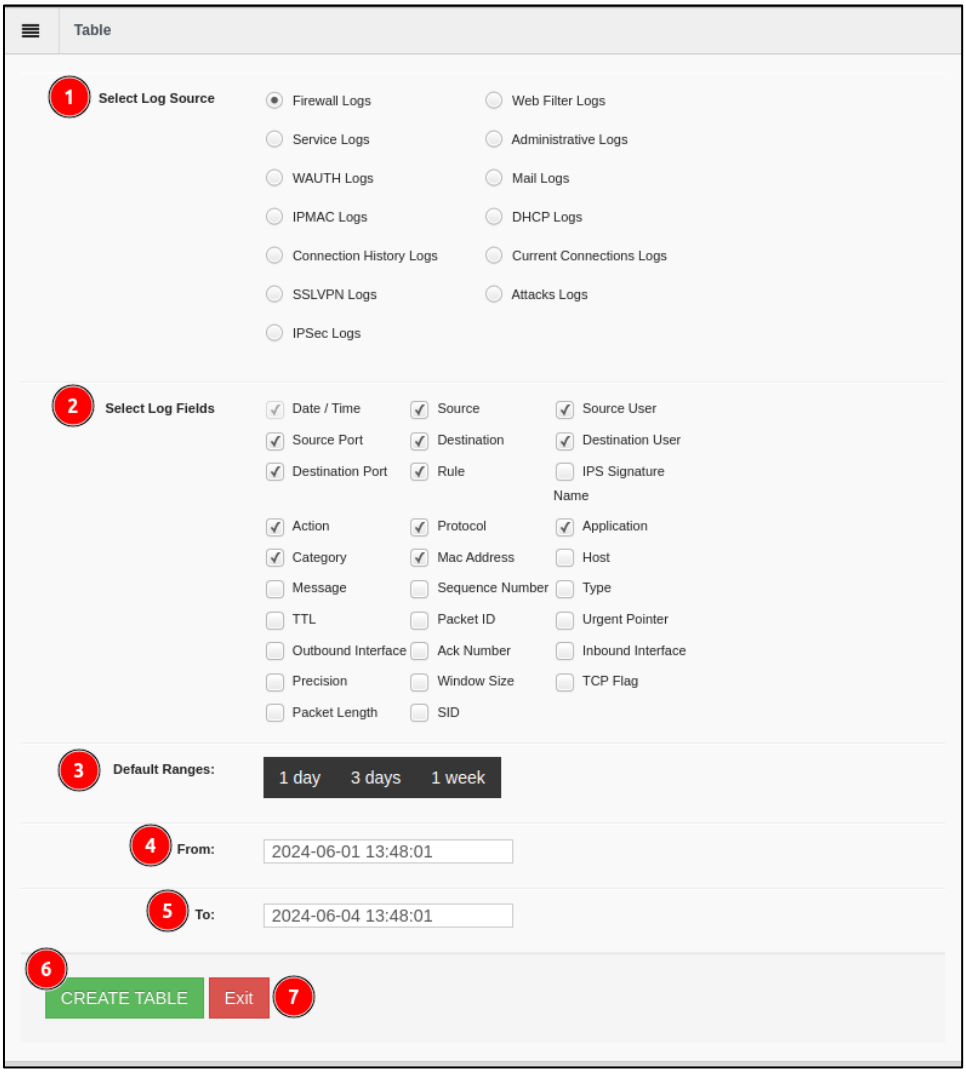
9	**Protocol**	The protocol type in the connection record is displayed.
10	**Source Port**	The source port information is displayed.
11	**Destination Port**	The destination port information is displayed.
12	**Transmitted Packet**	The received packet size in the connection is displayed.
13	**Received Packet**	The sent packet size in the link is displayed.
14	**Transmitted Byte**	The received byte size in the connection is displayed.
15	**Received Byte**	The byte size sent in the connection is displayed.

19.1.2Archive

Record queries are made in the record files archived in the Labris UTM device. Recordings from the archive are shown according to the selected record type.



-When the archive is clicked, the desired records are selected from the archive by selecting the record to be retrieved on the screen that appears.



1	**Select Log Source**	This is the section where the log source is selected.
2	**Select Log Fields**	It varies according to the selected log source.
3	**Default Range**	Time intervals are standard in Labris UTM devices. You can choose one of these time intervals.
4	**From**	The start date of the recording from the archive is selected.

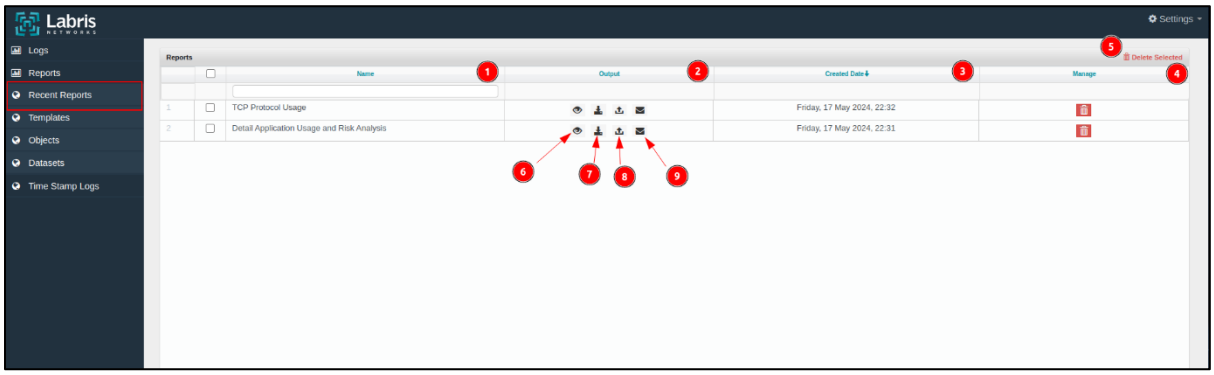
5	**To**	The end date of the archived recording is selected.
6	**Create Table**	It is the button where the table is created according to the selected values.
7	**Exit**	It is the button where the screen is closed.

19.2 Reports

It is the section where reports are created on the records kept in the Labris UTM device.

19.2.1 Recent Reports

It is the section where the received reports are viewed and downloaded in the Reports module, and the received reports are sent to the FTP server or via e-mail.

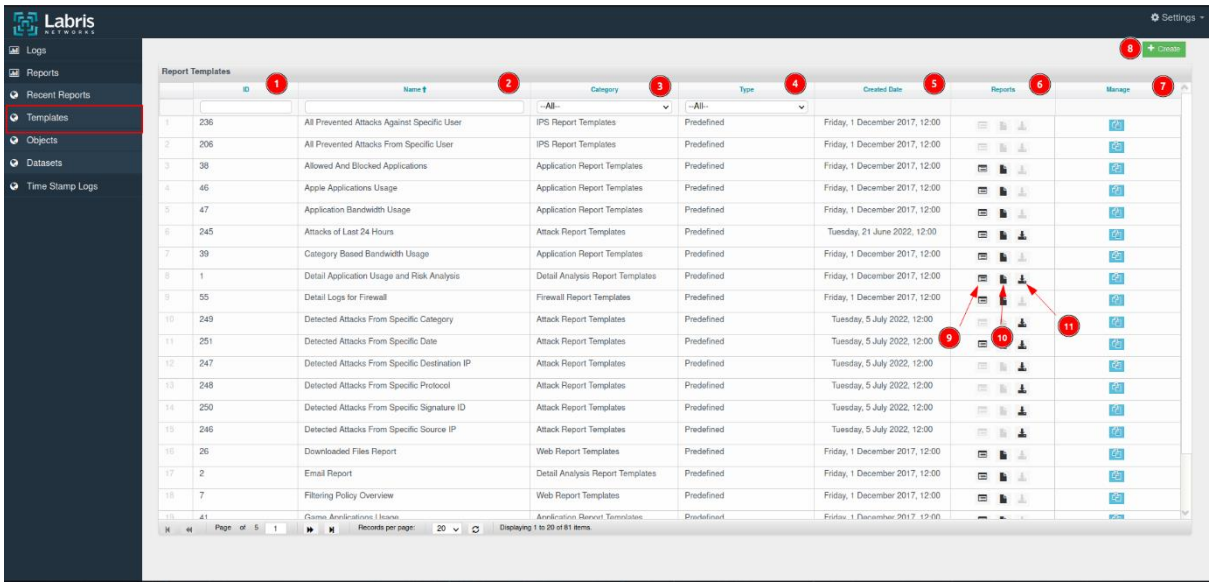


1	**Name**	The names of the received reports are displayed.
2	**Output**	It is the section where the received reports are downloaded, viewed, sent to the FTP server, and sent by e-mail.
3	**Created Date**	The date the report was created is displayed.
4	**Manage**	This is the section where the received report is deleted.

5	**Delete Selected**	This is the section where the selected reports are deleted.
6	**View Reports**	This is the section where the received report is displayed.
7	**Download Reports**	This is the section where the generated report is downloaded.
8	**Upload Reports**	The generated report is sent to the FTP server.
9	**Sent With Mail**	The generated report is sent to the Mail server.

19.2.1 Templates

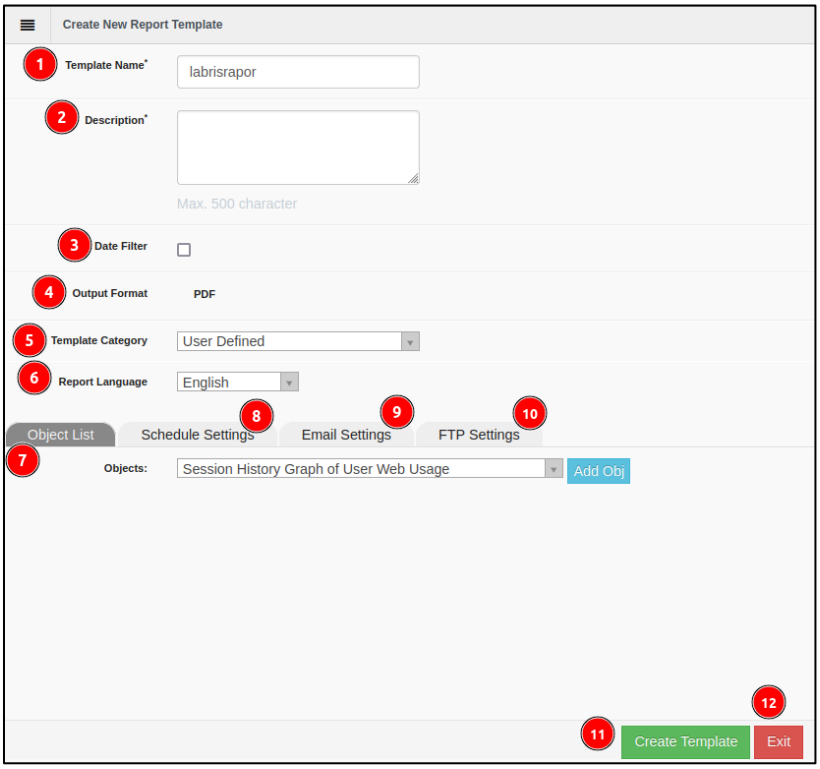
Registration reports are generated from the templates that come by default in the Labris UTM device.



1	**ID**	This is the section where the ID number of the templates is displayed.
2	**Name**	This is the section where the name of the templates is displayed.
3	**Category**	This is the section where the category types of the templates are displayed.

4	**Type**	This is the section where the type of templates is displayed.
5	**Create Date**	This is the section where the creation date of the template is displayed.
6	**Reports**	Depending on the template, it is the section where the report is generated, the report table from which the template was created, and the section where the last report created is displayed.
7	**Manage**	This is the section where the created templates are copied or deleted.
8	**Create**	It is the button where the template creation process is done.
9	**Show Report Tables**	The template is displayed in the report table.
10	**Create Report**	Depending on the template, the report is generated.
11	**Download the last Report**	This is the section in the template where the last generated report is displayed.

-Click on the 'create' button to add a template.

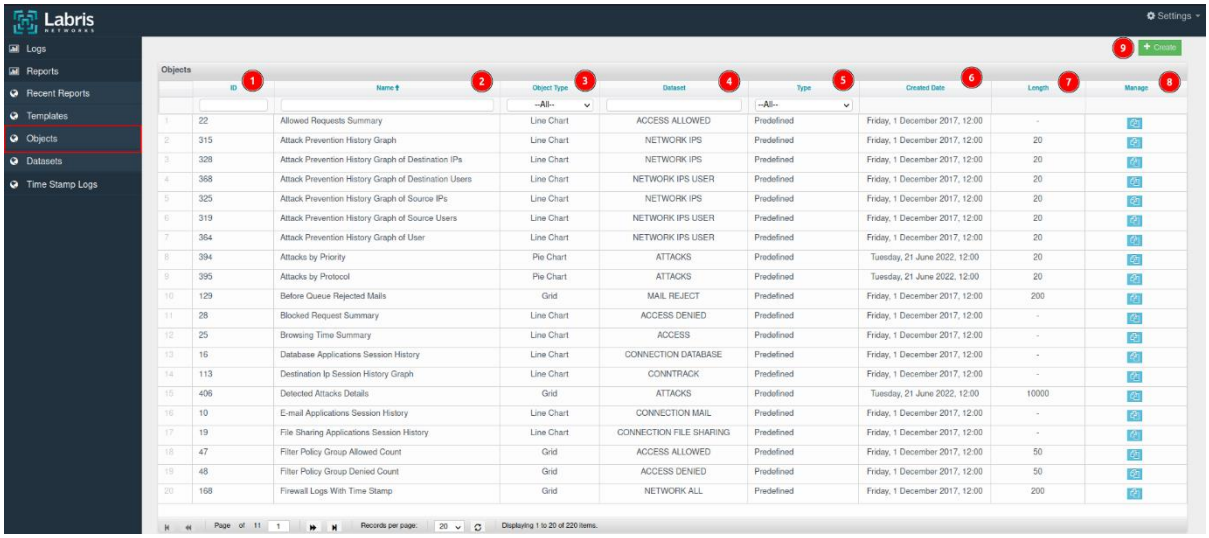


1	**Template Name**	This is the section where the name to be given to the template is entered.
2	**Description**	This is the section where the description of the template is entered.
3	**Data Filter**	It is the button where the date filter is entered into the template.
4	**Output Format**	This is the section where the output format of the template is displayed.
5	**Template Category**	This is the section where the category of the template is selected.
6	**Report Language**	This is the section where the report language of the template is selected.
7	**Object List**	It is the section where the objects added or found by default in the Object module are selected.

8	**Schedule Settings**	This is the section where the date filter is applied to the template.
9	**Email Settings**	This is the section where the template to be added is sent to the mail server. In this section, the subject of the mail, the address to be sent to the mail and the message are entered.
10	**FTP Settings**	This is the section where the added Template is sent to the FTP server. In this section, the IP address where the FTP server is located, the username and password information on the FTP Server, and the directory information on the FTP server are entered.
11	**Create Template**	Depending on the template, the report is generated.
12	**Exit**	It is the button where the screen that comes after clicking the 'Add' button is closed.

19.2.2 Objects

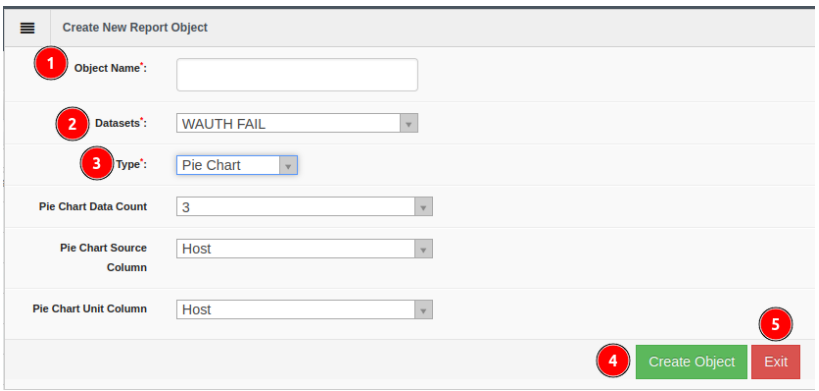
By default, registration reports are generated from incoming objects in the Labris UTM device. Added objects are used in templates.



1	**ID**	The ID of the existing object is displayed.
2	**Name**	This is the section where the name of the object is displayed.

3	**Object Type**	It is the section where the type of object is displayed.
4	**Dataset**	The data set of the object is displayed.
5	**Type**	The object type is displayed.
6	**Create Date**	This is the section where the creation date of the object is displayed.
7	**Length**	The length of the object's contents is displayed.
8	**Manage**	This is the section where the object is copied or deleted.
9	**Create**	It is the button where the object is created.

-Click on the 'create' **button** to add an object.

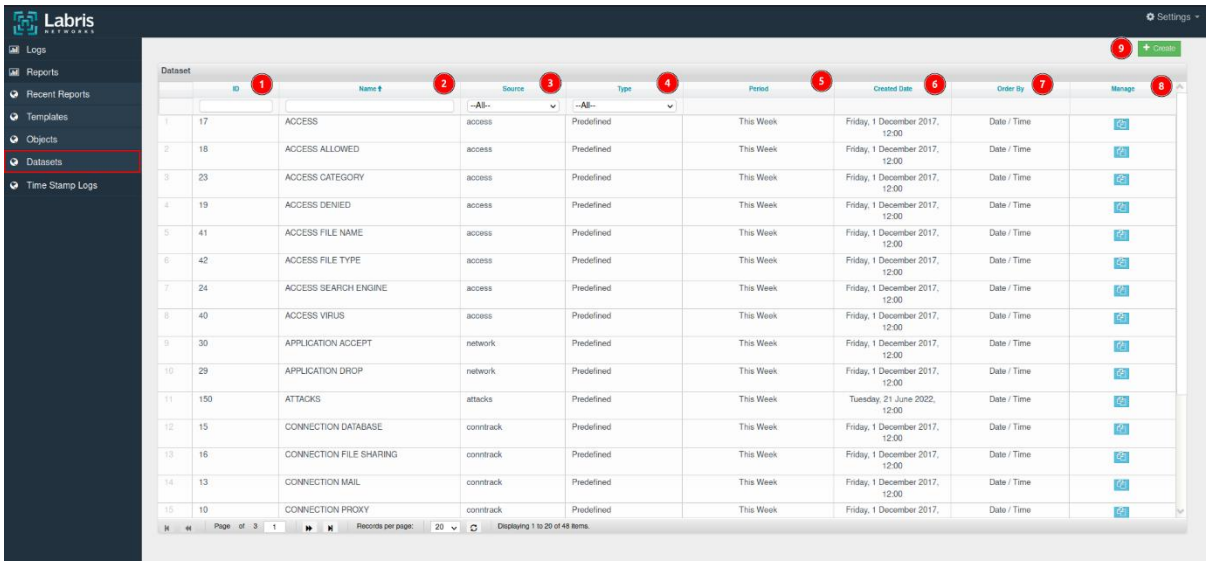


1	**Object Name**	It is the section where the name of the object to be added is entered.
2	**Datasets**	The data set of the object is selected.
3	**Type**	The type of creation of the object is specified. The object to be created will vary according to the type selection.
4	**Create Object**	It is the button where the object is created according to the entered values.

5	**Exit**	**It** is the button where the screen that opens after clicking the 'Create' button is closed.

19.2.3 Datasets

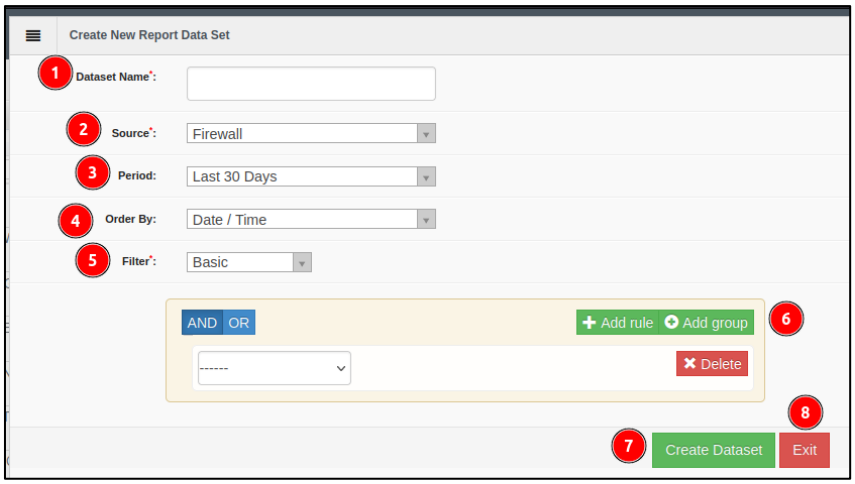
It is the module where the data sets to be used when creating objects are created. By default, the Labris UTM device has data sets.



1	**ID**	This is the section where the data set ID is displayed.
2	**Name**	This is the section where the name of the datasets is displayed.
3	**Source**	This is the section where the source information of the dataset is displayed.
4	**Type**	This is the section where the type of dataset is displayed.
5	**Period**	The period information of the dataset is displayed.
6	**Created Date**	The creation date of the dataset is displayed.
7	**Order BY**	This is the section where the sorting type of the dataset is displayed.
8	**Manage**	It is the section where the dataset is copied and the

		created dataset is deleted.
9	**Create**	It is the button where the dataset is created.

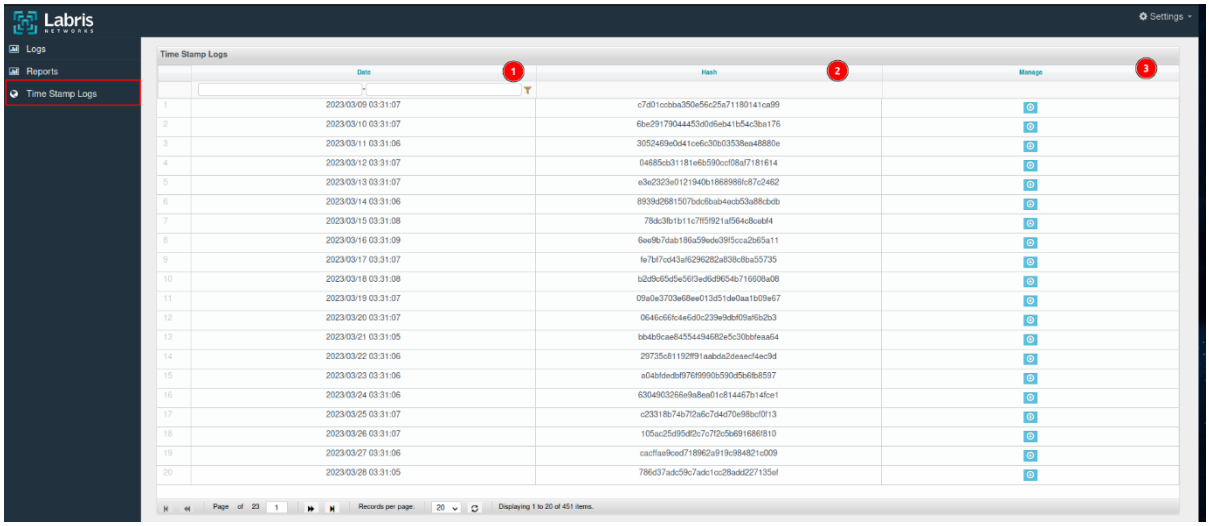
-Click the 'create' button to create a dataset.



1	**Dataset Name**	This is the section where the name of the dataset is entered.
2	**Source**	This is the section where the source of the dataset is selected. The desired data set is selected from the records kept in the Labris UTM device.
3	**Period**	The period of the dataset to be created is selected.
4	**Order By**	The sorting type of the dataset to be created is selected.
5	**Filter**	This is the section where the dataset is filtered.
6	**Rule**	It is the section where the rule of the dataset is written.
7	**Create Dataset**	It is the button where the dataset is created.
8	**Close**	**It** is the button where the screen that opens after clicking the 'Create' button is closed.

19.3 Time Stamp Logs

It is the section where the records kept in the Labris UTM device are kept with time stamps.



1	**Date**	It is the section where the date of the records kept as Time Stamped is displayed.
2	**Hash**	This is the section where the hash of Time-Stamped records is displayed.
3	**Manage**	It is the section where Time Stamped recordings are downloaded.