

Next Generation Network Security

Labris **UTM** Series



The Solution You Need Exactly, For Your Privatized Business

Labris UTM does not obligate you to buy unnecessary modules/hardware while providing the flexibility that will adapt to your way of doing business. Whatever are your business's current needs, you buy that and use in the most appropriate way to your structure.

Labris continues its leading stance on issues that the sector needs such as new generation application recognition, centralized user directory, IP reputation network, guests authorization via SMS, appliance integrated logging and reporting, monitoring of distributed appliances, application of central policies on terminals.



CWL Cyber Warfare Lab

The advanced technologies and current critical defense measures used in Labris UTM product infrastructure are developed in **Cyber Warfare Lab** by a creative team that knows the risk well.



Close Security Support

CSS Close Security Support

Labris Networks, in addition to providing technologically advanced features, also promise you a solution partnership. It applies a product and process management close to users, sensitive to their wishes and needs. Within this scope, it offers the SLA packages appropriate to their needs.



EAL4+

Common Criteria is the ISO standard, the criteria of the world regulated for the products used in safety critical networks. Labris Networks is the only gateway company of Turkey and one of the world's leading firms that manufactures at **EAL4+** level.



Labris[®]
NETWORKS

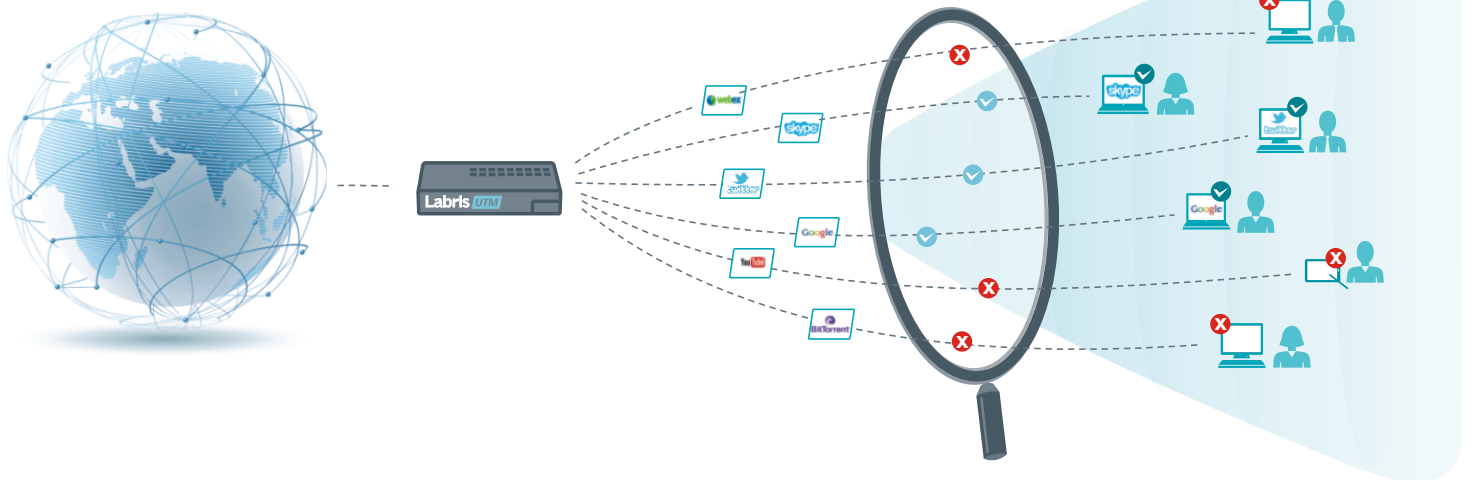
Next Generation Firewall: Labris UTM

- Labris UTM appliances, provides high level, user based control on your network with strong and continuously improved application control engine and a central user directory

■ Application Control (2000+ Application Signatures)

Internet and intranet traffic cannot be separated according to the ports that applications use. This situation has led to the development of port independent application recognition technologies in order to establish control over the applications.

Firewall technologies have evolved to be able to analyze the application layer (L7) activities more deeply.

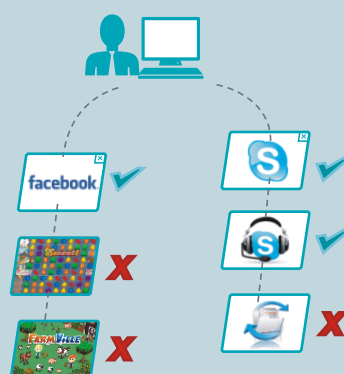


Application Signature Categories (15+)



It is possible to establish control over the applications, application functions and even application particles inside the application due to the deep packet inspection (DPI) technologies used and benefit from this information in firewall policies.

Control over Application Components



- Collaboration
- Database
- File Transfer
- Games
- Messaging
- Network
- Monitoring
- Networking
- Proxy
- Remote Access
- Social Networking
- Streaming Media
- VPN and Tunneling
- Web Services
- Mail
- Others



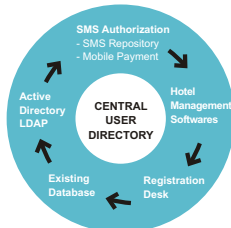
■ Central User Directory

One of the requirements of the new generation security appliances is to be able to query user information from external systems, use this information at a single point within the scope of a central authentication system inside the appliance and take application or application particles under control with this user information.

By this way, it becomes possible to view the logs of firewall, web filter and similar integrated applications as user based.

■ Directory Modules Collecting User Information

- Registration Desk Module
- Active Directory Integration Module
- SMS Authorization *
 - SMS Repository **
 - Mobile Payment
 - External SMS Repository Integration
- Hotel Management Software Integration *
- Enterprise Applications Integration Requirements *



* Option ** An additional contract or procedure is not required to use SMS authorization functions.

Central User Directory Application Examples

■ Firewall, Routing, Bandwidth Management, SSL VPN Client

You may use the central user directory created by combining many sources as you wish, in the firewall and routing rules or during bandwidth management or for authorization of SSL VPN clients.

By this way, capabilities that cannot be thought before such as writing a firewall rule using mobile phone number for a user that got password from its mobile phone via SMS, are provided.

■ Wauth+ Module (Hot Spot and Network Authorization)

Hot Spot authorization for users can be made with **Labris Wauth+** module used in **Labris UTM** and **Labris LOG** appliances.

Owing to the central user directory, user information that the appliance acquired as a result of integrations like active directory, LDAP as well as SMS, hotel software integrations can be used. By this way, this module gained the feature of **Network Authorization** application that meets the authorization needs of internal networks besides being a hotspot.

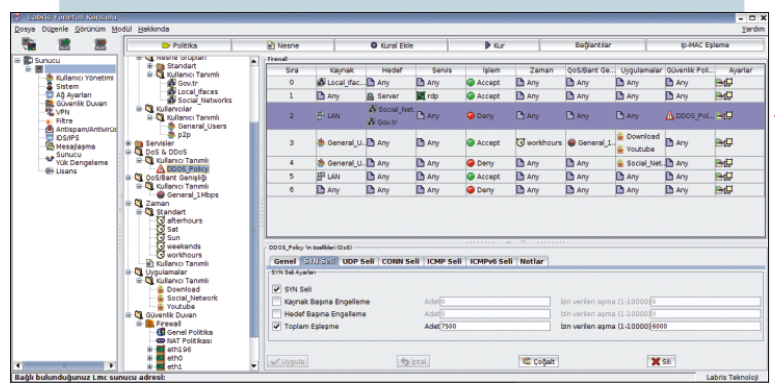
■ Labris Web Filter



The usage of users and user groups that exist in this directory inside the user groups created in **Labris Web Filter** is possible. Thus users obtained in many ways can be taken as a base while creating web filter policies.

■ Firewall "Security Policy Objects"

Firewall rules-based Security Policy objects can be used. These objects stand by as prepared and usable in firewall rules like application signatures. New objects may also be created if desired.



The most important area of usage is **providing a tailor-made, very important infrastructure for the detection of DDOS and similar abnormalities in determined traffics by Firewall.**

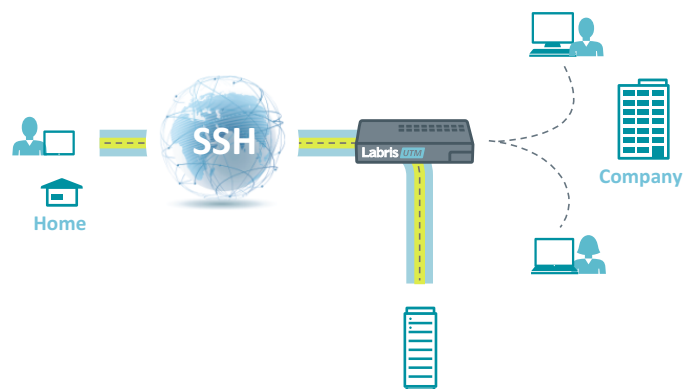
For example, **Security Policy Objects** that will be created in the form of "the traffic outgoing from A to B shall not more than X packages per second or more than Y SYN packages per second" can be defined in firewall rules.

■ SSH Control Engine

It creates a recognition and blocking infrastructure in order to prevent attempts that may threaten your network over SSH traffic.

SSH traffic usage areas

- Appliance management traffic
- File transfers with SFTP/SCP
- Backward and forward tunnels with tunneling
- Tunneling HTTP traffic

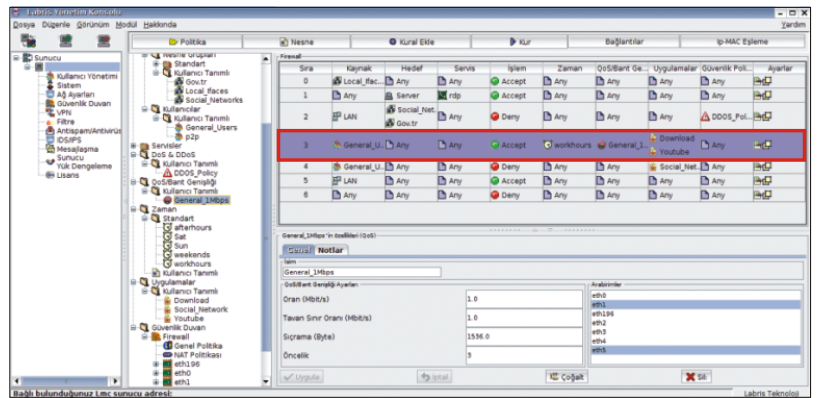


- Labris UTM appliances allows you to apply safe and redundant access configurations in distributed topologies and multi-lines.

Secure and Redundant Access Method

■ Bandwidth Management Criteria

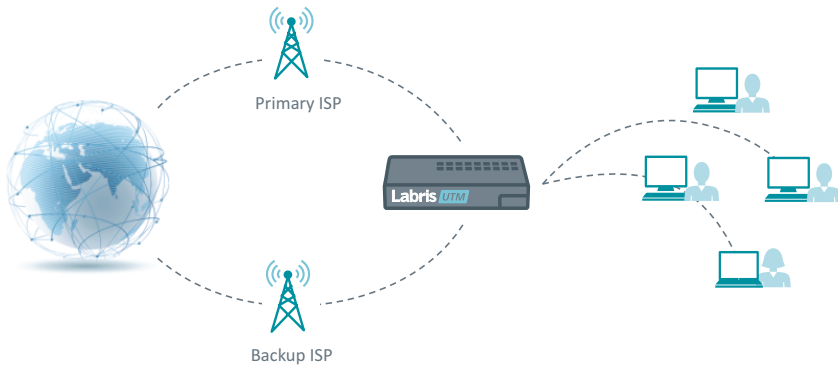
Bandwidth Management is made on the Firewall policy creation screen. All components that can be considered in a firewall rule can also be used as a rule condition.



Who	What	From Where	To Where	When
User* User Group*	Applications	Source IP Source Network	Destination IP Destination Network Port	Duration Recurrence Frequency Time Independent

* * Can be selected in Central User Directory

■ WAN / VPN Backup



Gateway VPN Redundancy



Redundant VPN connections can be defined on more than one internet line managed by Labris UTM appliances.

Organization policies can be applied on these connections. Arrangements like "connection and VPN shall continue on the other line" when a line is broken can be possible.



- All ports of Labris UTM series appliances have independent ethernet chip that can be used for LAN / WAN; they are not multiplexed with switch.
- USB ports of Labris UTM appliances are automatically defined as an internet path when 3G Modems are plugged. These outputs can be used as redundant emergency line or support remote access line within the scope of the needs of organizations.
- Labris UTM appliances can enable the usage of internet connections of multiple numbers and types as a single line by combining them at different ports or with switch.



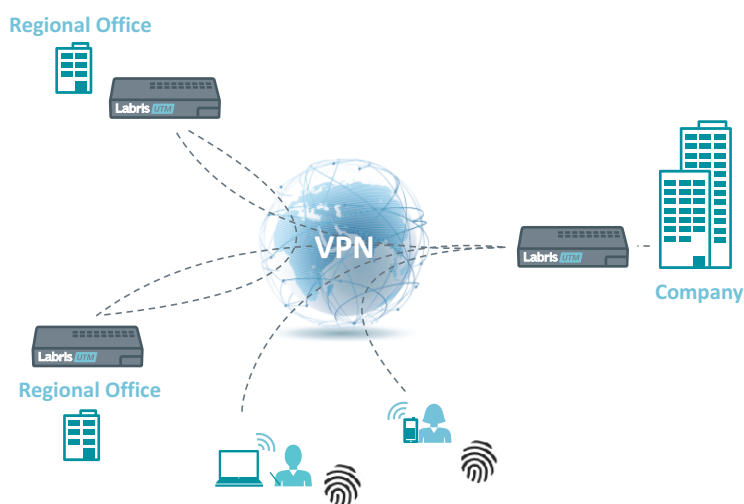
■ Multiple Output 3G Router Mode

Using multiple 3G USB modems in a redundant and coordinated manner

- Managing 3G modems separately
- Grouping modems
- Running with redundancy


■ Secure Remote Communication (VPN / SSL VPN)

VPN technologies are used to let remote users and regions access center and each other via secure, encrypted ways. Labris UTM VPN features are fully compliant with international standards and can be positioned as compatible with appliances of different brands in high traffic.



■ Labris WAUTH+ (Hotspot and Network Authorization)

- Determining the network zones that authorization will be made independently from network components
 - Authorizing users at remote locations from center by working over WAN
 - Determining user and network-based policies
-
- Common Key feature to prevent unauthorized usage of internet via SMS from corporate wireless networks
 - Determining duration quota
 - Determining timeout period
 - Turkish and English interface support changing according to the language of Internet browser
 - Customizable "Welcome" page
 - "Log Out" option for the user
-
- Adding credit for SMS usage without the need for an additional procedure
 - User search engine
 - Monitoring of active connections, disconnecting the desired user connections

SSL VPN Client Software	
SSL VPN Client softwares are used to let users access central network securely from outside the organization.	
Supported Operating Systems	Windows, Linux, iPhone, Android, MacOS 
Authorization Methods	All methods supported by Central User Directory

■ E-Signature / Mobile Signature

E-Signature / Mobile Signature Integration

E-signature and mobile signature services can run as integrated with the Central User Directory. By this way, it became possible to use and manage the users coming by this authorization methods in the directory, consequently in all of the applications on the appliance.

■ Guest Authentication (Hot Spot)

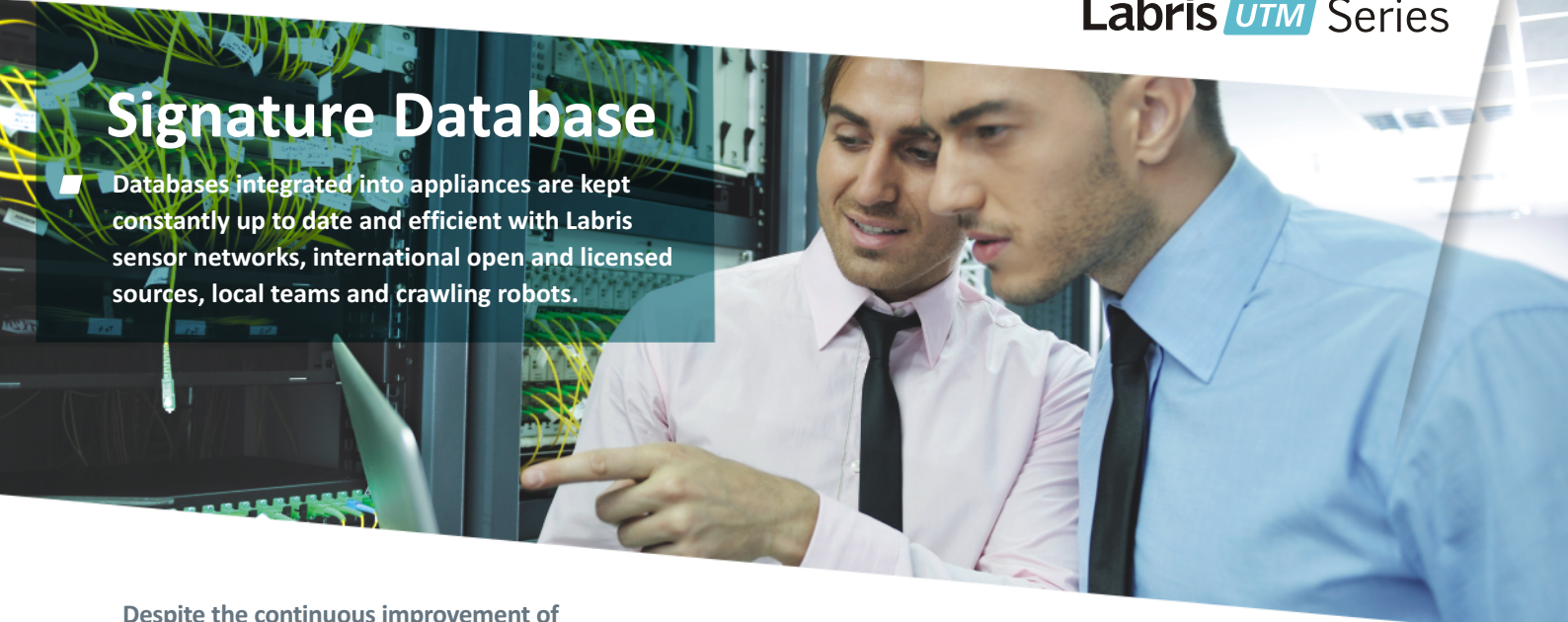
Labris WAUTH+, is different from the hotspot solutions in the market. It considers this work as an important part of the security and offers comprehensive solutions that can be integrated into any kind of internet network.



- Labris WAUTH+, offers solutions compatible with guest user type and guest authorization scenarios of each organization.

Signature Database

■ Databases integrated into appliances are kept constantly up to date and efficient with Labris sensor networks, international open and licensed sources, local teams and crawling robots.



Despite the continuous improvement of abnormality detection methods, the need for continuously updated databases in security applications is more than ever.

Owing to these databases, while abnormality engines' working with less load is provided, with a local perspective product's efficiency and performance, compatibility to organization/community behavior can be increased to very high levels.

■ Spam Sensor Network

The detection of multiple targeted malicious propagations originating from a single point before arriving to appliances is important. During the singular decision-making of each device with abnormality methods, the most important information not in its hand is what other targets and how frequent this traffic is sent.

With widely positioned sensors network, the signature information regarding the traffic of malicious propagations is also obtained along the IP information of the source and distributed to the appliances immediately.

■ IP Reputation Network (2000+Points)

Labris Networks is performing intense researches on widespread and critical importance networks with owned and installed appliances and sensor networks. These studies are transformed to technological infrastructure or signature by **Cyber Warfare Lab** which is the security incidents research center of **Labris Networks** and distributed to appliances.



Reputation Network Going Down to Local	IP reputation network not only in ISPs, but reaching to networks of 50 users
Malicious traffic inspection to identify IP	Inspection of malicious traffic like spam, viruses, malware propagation, open proxy
IP Archive Data	IP reputation database based upon years

Standard Signature Counts



Firewall Application: **2000 +**
 Application Category: **15 +**
 URL: **3 Million +**
 URL Category: **85 + (18 in TR)**
 IPS: **9000**

Additional Subscription Options

Web Filter+ Database Membership
 URL: **500 Million +**
 Web Page: **6 Billion +**
 Category: **150 +**
IPS+ Database Membership
 Built-Signature: **20,000 +**
 Category: **74 +**

Logging

■ Labris UTM products are equipped with internal and remote logging capabilities. Appliances have internal log spaces from 8 GB up to 3TB according to their sizes. All log storage and regulatory compliance operations are carried out at the gateway without the need for an additional measure, investment, equipment and software.

Redundant Logging

In Labris UTM 62 and above appliances, which have more than one logging disk, RAID 1 redundancy of internal logs can be supported.

Log Storage in accordance with the Laws

The originality of a log can be proved by storing the log after stamping it with a time stamp.

In Labris products, qualified time stamps produced by Türkrust which is authorized in T.C. e-signature law are used.

Time Stamp Usage Frequency

In Labris products, pre-defined time stamp usage frequency can be increased optionally, in case of need e-signature certificate server in the corporate network can be used.

Remote Logging

Labris UTM products can send appliance logs to a remote location in different ways during the creation of them.

Remote Logging to Labris LOG Products

Labris UTM appliances can perform remote logging to Labris LOG products that are either attached to appliance or positioned away, with all the features mentioned in Remote Logging section.

Remote Logging to SIEM Products

The logs created in the product family are produced in international standards, readable and correlatable by SIEM products. Logs can be transferred to SIEM products with Syslog, FTP and similar methods.

Secure Logging

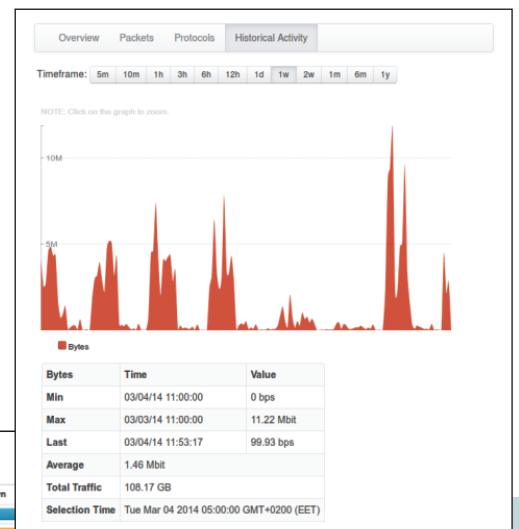
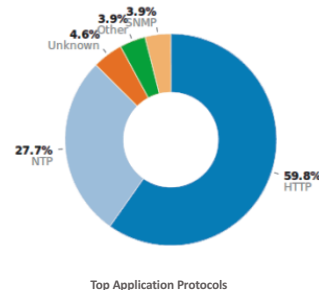
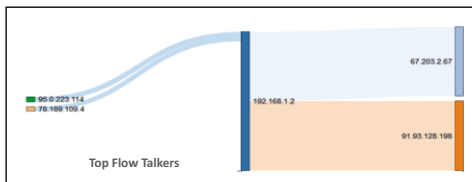
Storing the log where it is written firstly is the first step in preserving the evidential value of log. By this way, proving the originality of the log during rewriting it and examining the issues such as the security of the connection between the location that the log will be written and the appliance, being under physical risk of the hardware that the log is transferred are not needed.

Log Lifecycle

Logs that are kept internally are stored in accordance with the size of internal log area within the scope of lifecycle operations, archived in appropriate disc types.

Instant Monitoring

■ Instant Monitoring Module makes visual analysis of your current traffic in real time.



Active Flows

Info	Application	L4 Proto	VLAN	Client	Server	Duration	Breakdown
Info	HTTP	TCP		10.100.1.225:84571	www.dmi.gov.ir:3128	1 h, 20 min, 6 sec	Client Server
Info	NTP	UDP		10.100.0.42:32774	192.168.1.201:123	18 h, 21 sec	Client
Info	Unknown	TCP		10.100.1.233:52962	85.111.24.198.static...1935	5 h, 52 min, 27 sec	Server
Info	ICMP	ICMP		www.dmi.gov.ir	10.100.0.42	6 days, 5 h, 24 min, 55 sec	Client
Info	SMB	TCP		www.dmi.gov.ir:42969	elmadag.com	36 min, 57 sec	Client Server
Info	SNMP	UDP		elmadag.com	172.16.0.25:161	6 days, 5 h, 25 min, 50 sec	Client
Info	SNMP	UDP		elmadag.com	172.16.0.33:161	6 days, 5 h, 25 min, 50 sec	Client
Info	SNMP	UDP		elmadag.com	172.16.0.29:161	6 days, 5 h, 25 min, 50 sec	Client
Info	SNMP	UDP		elmadag.com	172.16.0.22:161	6 days, 5 h, 25 min, 50 sec	Client
Info	SNMP	UDP		elmadag.com	172.16.0.13:161	6 days, 5 h, 25 min, 50 sec	Client

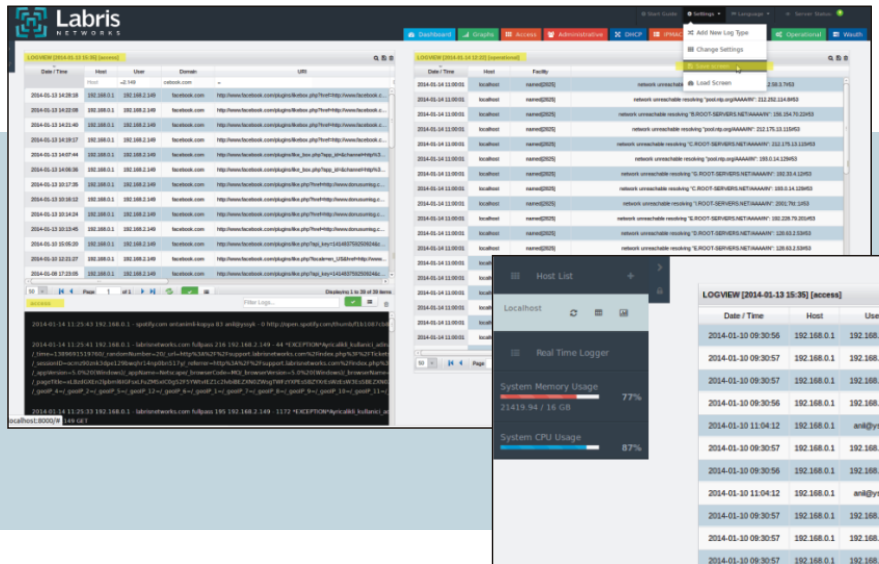
Showing 1 to 10 of 896 rows

All Hosts

IP Address	VLAN	Location	Name	Seen Since	ASN	Breakdown	Throughput	Traffic
10.100.0.254		Remote	im.bloomberght.com	7 days, 40 min, 5 sec		Client	3.92 Mbit	90.99 GB
10.100.0.42		Local	10.100.0.42	6 days, 5 h, 25 min, 30 sec		Client	350.86 Kbit	3.91 GB
192.168.1.201		Local	192.168.1.201	6 days, 5 h, 25 min, 30 sec		Client	350.86 Kbit	3.88 GB
10.100.0.1		Remote	int-dc-1.elmadag.com	7 days, 40 min, 5 sec		Client	171.53 Kbit	2.37 GB
10.100.1.100		Remote	10.100.1.100	4 h, 48 min, 40 sec		Client	0 bps	1.13 GB
10.100.1.225		Remote	10.100.1.225	1 h, 26 min, 23 sec		Client	619.73 Kbit	1.08 GB
10.100.0.7		Remote	10.100.0.7	2 days, 8 h, 19 sec		Client	0 bps	463.73 MB
10.100.0.250		Remote	10.100.0.250	7 h, 14 min, 12 sec		Client	0 bps	296.99 MB
193.255.217.57		Remote	193.255.217.57	7 h, 59 min, 52 sec		Client	34.99 Kbit	279.13 MB
10.100.0.50		Remote	10.100.0.50	6 days, 5 h, 25 min, 28 sec		Client	264 bps	179.51 MB

Showing 1 to 10 of 212 rows

Log View



Viewable Log Types	<ul style="list-style-type: none"> - Operational Logs - Firewall Logs - UTM Function Logs
Management	<ul style="list-style-type: none"> - Instant Monitoring - Hierarchical Filtering - Defining multiple appliances - Web-based rapid management
Reporting Formats	PDF, XML, HTML, XLS, CSV

Integrated Reporting

The logs collected on the appliances are offering a graphical, easily understandable by administrative managers, rapid analysis tool with integrated reporting module integrated to appliances.

Web General View

- Web Filter General View
- WWW Traffic Characteristics
- Filtering Policy Statistics
- Risk Map

Instant Reports

- Last Half Hour
- Instant Users
- Instant Sites
- Instant Addresses
- Instant Blocked Categories

Web User Tracking

- User Web Access Summary
- User Access Cost
- User Favorite Sites
- User Site Accesses

Web Summary Reports

- Top Sites according to Connections
- Top Sites according to Bandwidth
- Top Sites according to Usage Time
- Top Users according to Connections
- Top Users according to Usage Time
- Top Blocked Sites
- Top Blocked Users
- Top Viruses
- Content Type Distribution
- Blocking Category Distribution
- Top File Downloads according to Number
- Top File Downloads according to Size
- Top File Types
- Top Search Engines
- Top Search Patterns
- Frequenters of Blocked Categories
- Bandwidth Consumed to Blocked Categories
- Site Based Cost Analysis
- Category Based Cost Analysis
- Green Computing and Savings

Detailed Lists (Web)

- Sites
- Users
- Web Flow
- Sites per User
- Addresses (URL) per User
- Users per Site
- User and Addresses (URL) per Site

E-mail Traffic General View

- Message Filtering Summary Report
- General Character of Message Traffic
- Messages Filtering Results Distribution
- Green Computing and Savings

E-mail Report Summaries

- Active Users
- External Senders of Incoming Messages
- Internal Recipients of Incoming Messages
- Internal Senders of Incoming Messages
- Foreign Recipients of Incoming Messages
- Internal Senders of Internal Messages
- Internal Recipients of Internal Messages
- Recipient Domain Names
- Sender Domain Names
- Incoming Virus Types
- Outgoing Virus Types

Time Distribution of E-mails

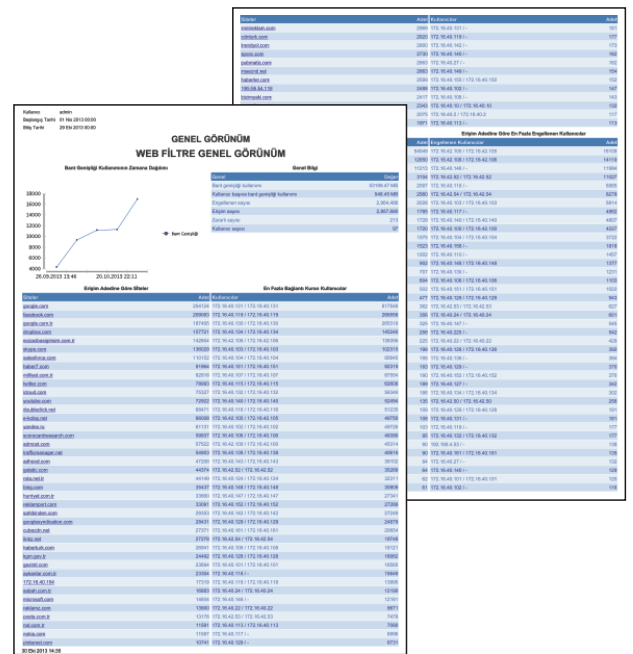
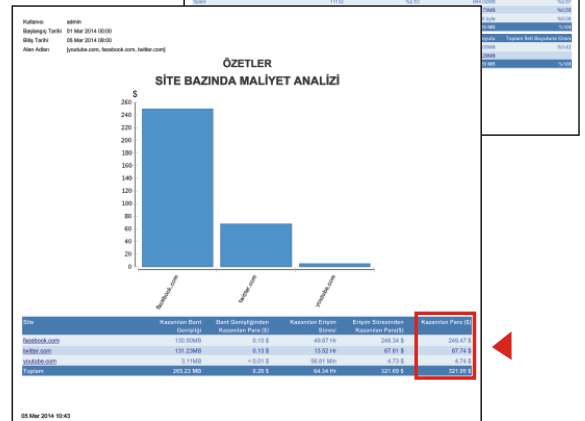
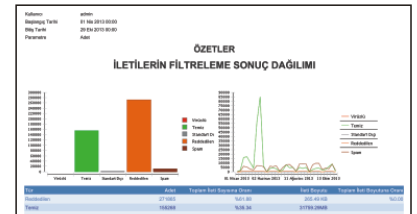
- Non-standard Messages
- Rejected Messages Before Entering Queue
- Blocked Messages in Spam and Policy Filter
- Infected Messages
- Clean Messages

Detailed Lists (E-mail)

- Non-standard Messages
- Messages Before Queue
- Spam Messages
- Infected Messages

Web Time Distribution

- Time Distribution of Web Access
- Time Distribution of Bandwidth Usage
- Time Distribution of Access Time
- Time Distribution of Filtering/Collection Access Rate
- Time Distribution of Filtering
- Time Distribution of Virus Events



Next Generation UTM General Specifications

Network Access and Services

- TCP/IP
- IPv4 and IPv6 support
- Hybrid IP (ipv4/ipv6) topology support
- PPPoE Support
- Dynamic Routing (OSPF , RIP , BGP, Multicast)
- Policy based routing
- Real Multizone Support
- Link aggregation (802.3ad)
- Transparent Bridge Mode
- VLANs (802.1Q)
- DHCP Server
- DHCP Proxy
- Caching DNS Server

Operating/Lifecycle

- Stiffened and secure LabrisOS Firmware
- Partial firmware infrastructure
- Firmware upgrading process without the need to install all firmware and without the need of manual intervention
- Operating with redundancy in high performance with more than one appliance
- Automatically updated signature and databases

User Authorization

- Authorizing and managing all applications and users from a single point with central user directory
- Active Directory integration with/without agent (NTLM, LDAP)
- Wauth Hotspot authorization
- Guest users acceptance with SMS and registration desk
- Structure compatible with the mobile payment infrastructures of GSM operators
- Radius / TACACS authorization

WAN/LAN/ETHERNET

- Flexibility of using all ports of the products as WAN/LAN
- Connection redundancy support
- Applying connection based traffic policy
- Load balancing in WAN connections
- Defining connection status based actions
- Defining 3G USB modems automatically as WAN outputs
- Plenty metro ethernet, fiber, 10G termination options
- Using ethernet ports by aggregating (Port Aggregation)

Firewall

- Application Recognition (2000+ application signatures)
- Control of application components (e.g. facebook chat, facebook video, farmville, skype ...)
- Deeper configuration capabilities with integrated HTTP/HTTPS proxy engine (using rules based on file type, mime type and content)

- P2P blocking
- Stateful packet inspection
- Time-based dynamic rules
- Unlimited rules and sessions
- DoS and DDoS prevention functions
- Blocking abnormal packets
- Policy-based flexible NAT/PAT
- Automatic IP/MAC mapping
- Bandwidth, QoS management
- Control of encrypted SSH- traffic with SSH inspection engine

Web Filtre

- URL filtering
- HTTPS filtering
- White lists/Black lists
- Content based signatures
- Ready category database
- Querying for zero hour information from a broader database with Webfilter+subscription
- Feature of monitoring and reporting without blocking
- Creating different policy groups according to different users
- Policy groups based on IPs, IP range, local users and groups, active directory users and groups
- Applet, Cookie, ActiveX blocking
- Applying time-based policies
- Content changing support
- Antispyware, Antimalware, antitrojan, antiphishing support
- Inspecting archive files

Antivirüs

- Web (http/https) virus protection
- E-mail (server, client) virus protection
- Signature-based blocking
- Heuristics-based analysis
- Limited DLP integrated into antivirus engine
- Determining policy based on file type/size
- Multiple types archive files support

Antispam

- Constantly updated signature database
- Heuristics-based analysis
- Intelligent learning spam engine
- Spam sensor network feedbacks
- Integrated image OCR analysis
- Integrated PDF OCR analysis
- User adjustable filtering support
- RBL support
- Content filtering
- Read content signatures
- White Lists/Black Lists
- End-user spam quarantine
- End-user spam report screen
- End-user quarantine notification e-mail

Server Load Balancing

- L4 (Layer 4) load balancing
- SSL termination and L7 load balancing with integrated reverse proxy

Monitoring and Analysis

- Instant playback
- Graphical network usage monitoring
- Viewing session details

Central Monitoring

- Full compliance with Labris MNG Central Management System product family
- Taking policy centrally from single point accompanied by Labris MNG
- Monitoring centrally accompanied by Labris MNG
- Configuration and backing up record centrally accompanied by Labris MNG

Management

- Configuration interface at ease of drag & drop
- Web-based monitoring, reporting interface
- HTTPS/SSH/LMCCP management support
- Virus/spam quarantine manageable by end-user
- Secure remote access with SSL
- Local language support (Turkish, ...) and ease of adaptability
- Object-based management
- Platform independent management infrastructure
- Role-based management authorization
- Saving retrospective configuration backups
- Returning to the old policies
- Replacing of a new appliance with the old one just with the installation of configuration backup and without requiring an additional process

Registering

- Keeping log internally
- Sending log to remote locations (SYSLOG, ftp, remote disk spaces, ...)

Reporting

- Graphics-based reporting engine
- Integrated, safe and fast database
- Producing reports internally without the need for an additional system
- Giving regular reporting orders
- Sending produced reports to an e-mail address
- Ready report categories and templates
- Reporting infrastructure compliant with scheduled or instant needs

FLEX FIRMWARE OPTIONS

Firmware FLEX	A	B	C	D
Firewall	✓	✓	✓	✓
VPN/SSL VPN	✓	✓	✓	✓
IPS (Attack Prevention)	✓			✓
Web Filter		✓	✓	✓
Antivirus/Antispam Gateway			✓	✓
Wauth+ (Hotspot and Network Authorization)				

ETHERNET CART OPTIONS



PRODUCT	Cart Slot	GIGABIT (4 or 8 ports)	FIBER SFP (4 or 8 ports)	10G SFP+ (2 ports)	10G SFP+ (4 ports)
Labris UTM 52/56	1	✓	✓	✓	✓
Labris UTM 62/64	2	✓	✓	✓	✓
Labris UTM 150/155	3	✓	✓	✓	✓
Labris UTM 170/175	4	✓	✓	✓	✓

SUPPLEMENTARY PRODUCT FAMILIES

Labris **LOG**



Labris LOG product family can collect the logs of Labris UTM appliances at a single point besides collecting logs by listening to the network and obtain reports from these logs.

Labris **MNG**



Labris MNG product family can be used for monitoring Labris UTM appliances from a singular center, setting policies in one place and applying them to all appliances simultaneously.

RELATED PRODUCT FAMILIES

Labris **CLOUD**



It is possible to obtain the functionality that you can get with Labris UTM appliances, for your server infrastructures in the cloud. Labris CLOUD solutions can provide both the security of your structures in the cloud and that you get the security services while your traffic is on the ISP yet.

Labris Software, VM Compatibility



Labris UTM firmware can also be obtained as the software that can run on VMs. If required in the project, the applications in Labris UTM can be obtained as individual software.

PRODUCT LIFECYCLE

Please refer to **Labris Support Services Datasheet** for appropriate SLA packages that you can obtain with your product.

For the most appropriate lifecycle for your product and operating way, you can reach us using the **+90 850 455 45 55 (pbx)**; **support@labrisnetworks.com** contact details.

<http://labrisnetworks.com/tr/support-training/>

