دژافزارنت
DEZHAFZAR CORPORATION

ARIYADEZH

Ariadezh UTM

Unified Threat Management

Ariadezh, your network's reliable security

ARIYADEZH

http://www.dezhafzar.com

info@dezhafzar.com

Contents:

1- Authentication

To prevent unauthorized access and probable abuse of computer and network systems, Ariadezh UTM supports two levels of authentication. First, traffic authentication in the data plane, provides the ability to allow traffic only to/from network addresses belonging to authenticated users. Second, authentication in the control plane through the UTM's web interface which prevents unauthorized access to UTM's operational settings and control.

Traffic Authentication Features

- Supports RADIUS, and LDAP authentication sources.
- Customization of authentication portal through templates
- Support for various versions of Microsoft Windows Servers
- Displaying the list of users and management of their accounts' settings
- Detecting inactive users and closing their sessions

Web Interface Authentication

Support for two-step authentication through password and text messaging over cellular network.

Supports opening HTTP(S) ports only while an SSH session is authenticated and established. This adds another level of security to the control plane for remote management of the UTM.

Automatic Authentication in Windows Domains

Ariadezh UTM is capable of automatically authenticating supported clients through NTLM protocol and Active Directory servers. For more accurate tracking of users' activities, Ariadezh UTM provides mechanisms through which, user logoff events can be announced to the system.

2- Dashboard

The dashboard, provides a general overview of the system and services status. This environment consists of a set of drag & drop widgets that can be customized by the administrator. The available widgets include:

- High Availability
- Dynamic DNS
- Interface Statistics
- IPsec
- SSL VPN
- Load Balancer
- Firewall Logs
- Network Time
- Picture
- RSS
- System Log
- Thermal Sensors
- Traffic Graph
- Wake On LAN

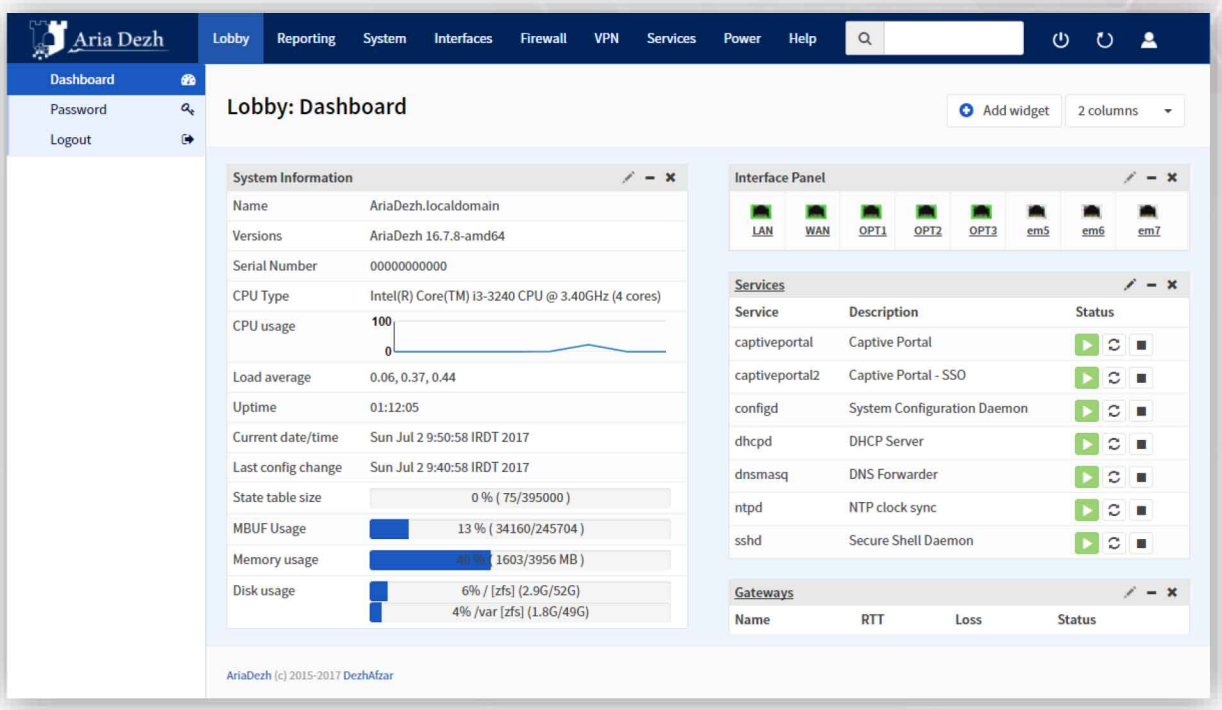

Figure 1- The dashboard: general status of the system and services can be viewed here

3- Reporting

In the reporting tab, the administrator can monitor various system and network events collected throughout the system's operation.

- Different protocols: TCP, UDP, ICMP, IGMP, …
- Traffic flow through different interfaces
- Traffic flow based on source/destination addresses
- Traffic flow based on TCP/UDP ports
- Brief and detailed reporting of network interfaces status and events

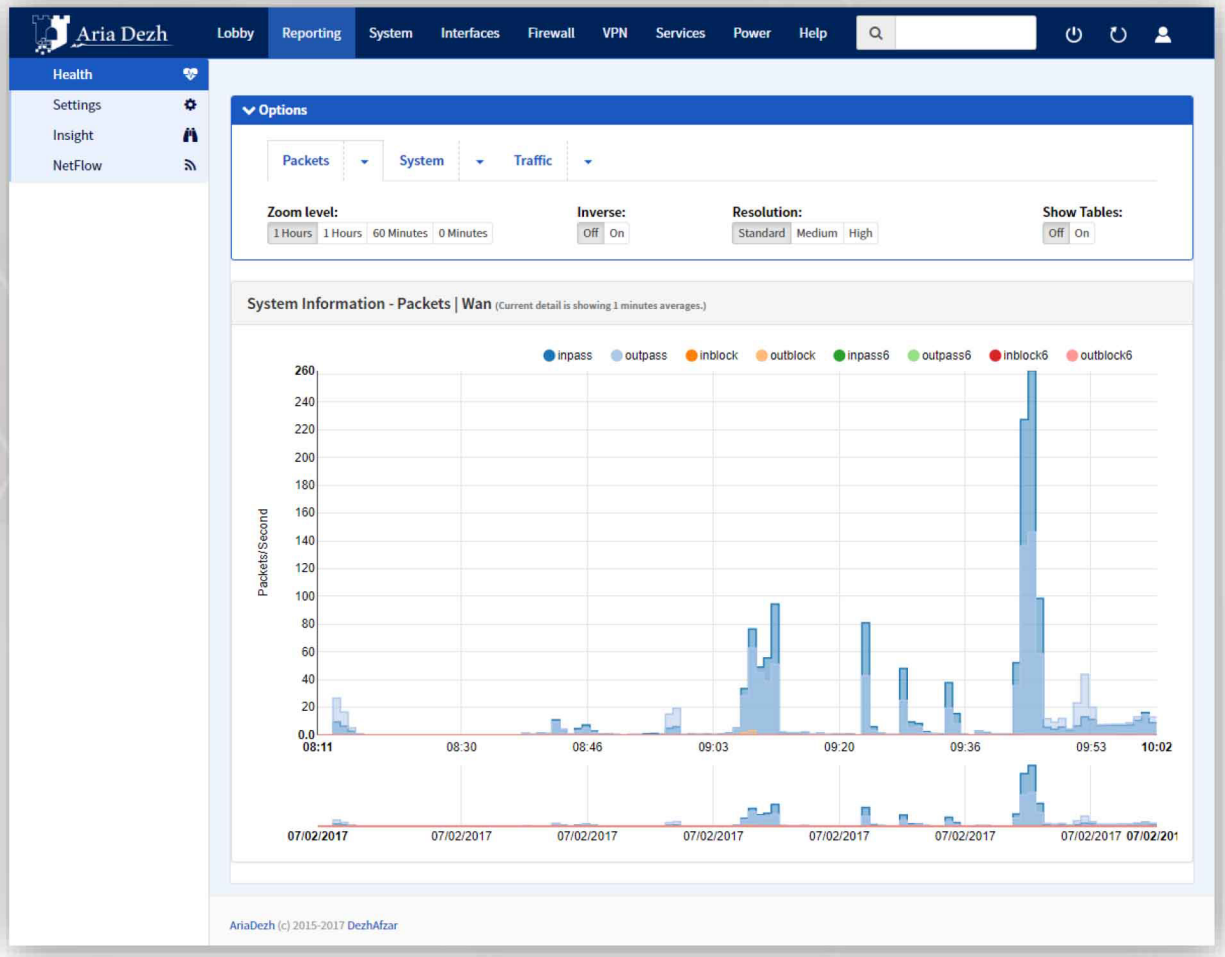

Figure 2- Diagram of network packets count on the firewall

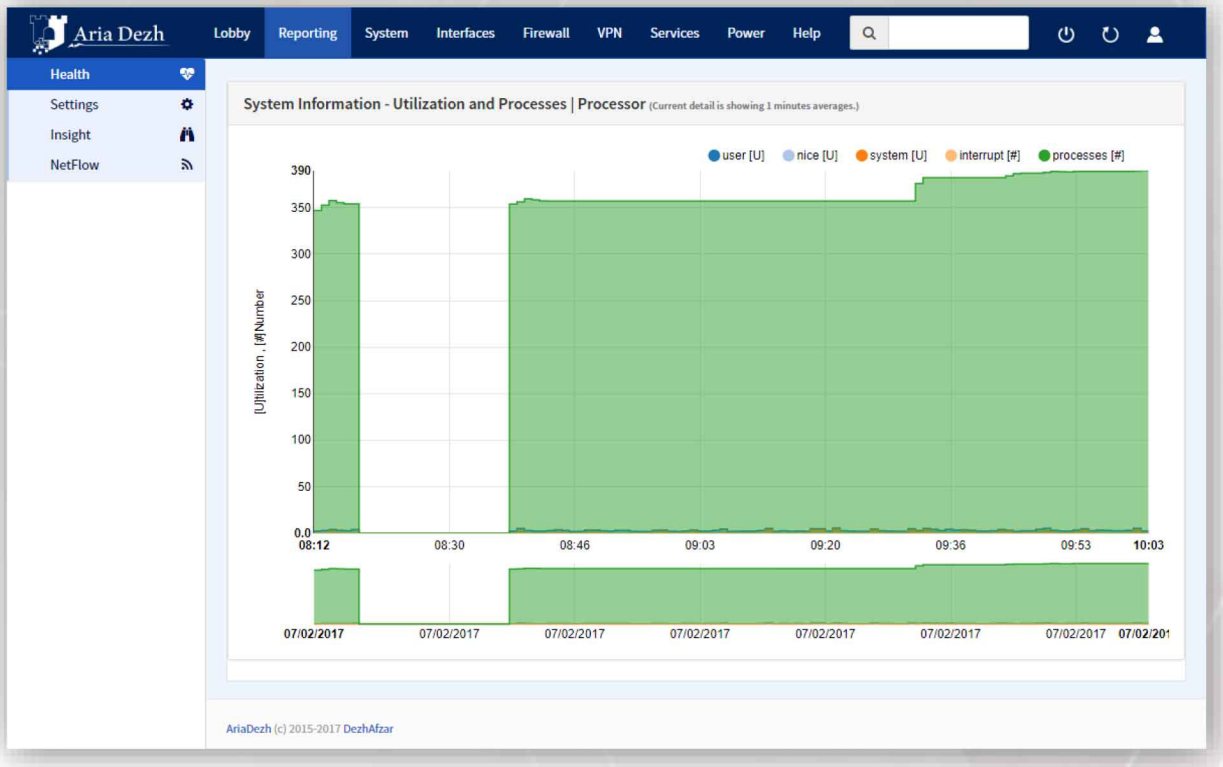

Figure 3- Diagram of system processes status over time

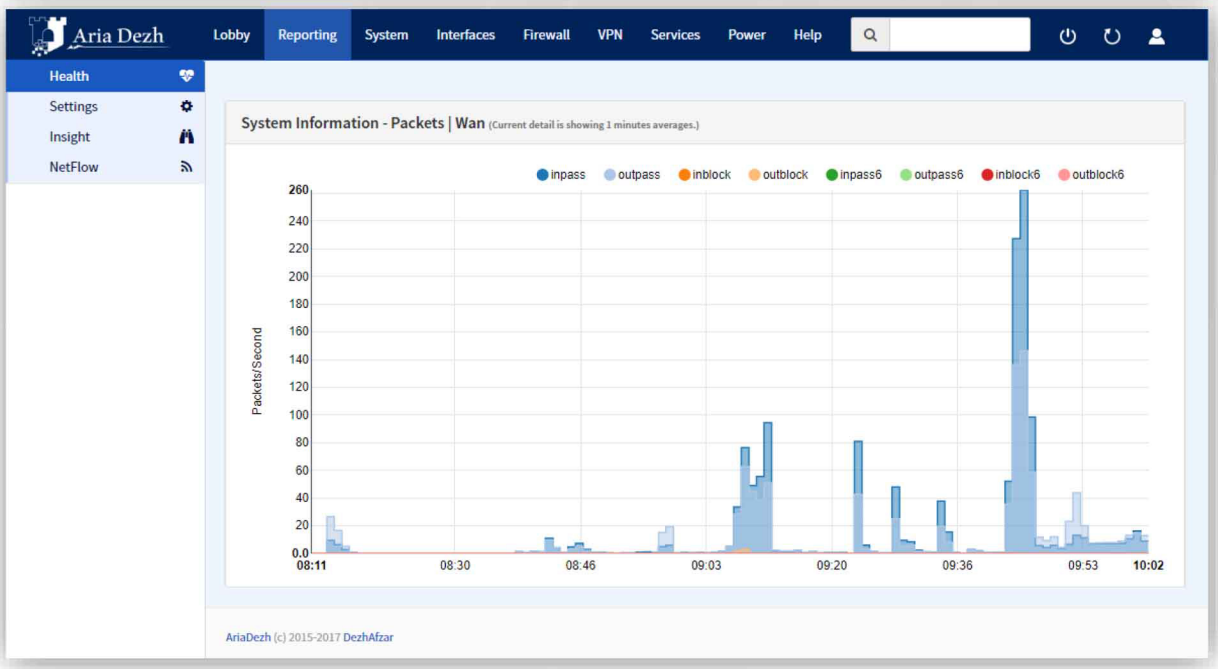

Figure 4- Diagram of network packets count on the WAN interface of the firewall

4- Diagnostics

Ariadezh UTM provides a full range of diagnostics and troubleshooting tools, including:

ARP Table	Displays the contents of the ARP table of the UTM.
NDP Table	Network discovery protocol, similar to ARP tables for IPv6 protocol.
Packet Capture	Can be used to capture network packets passing through firewall interfaces, using various filtering rules.
Test Port	Can be used to verify that a specific TCP port is open and is being services by a server.
Traffic Graph	Diagram of traffic flow rate on different interfaces.
Filter Reload	Used to reload the firewall ruleset and view the related error logs.
Afinfo, AfTop and AfTables	View online status of the firewall, (e.g. interfaces statistics, connections statistics, etc.)
States Dump	Ariadezh is a stateful firewall and keeps states for tracking of all ongoing network connections. This allows the administrator to view firewall connections states.
States Reset	This can be used to delete connections states and terminate ongoing connections.
States Summary	Displays a summary of the current connections states.
Ping Traceroute	Used for testing network connectivity.

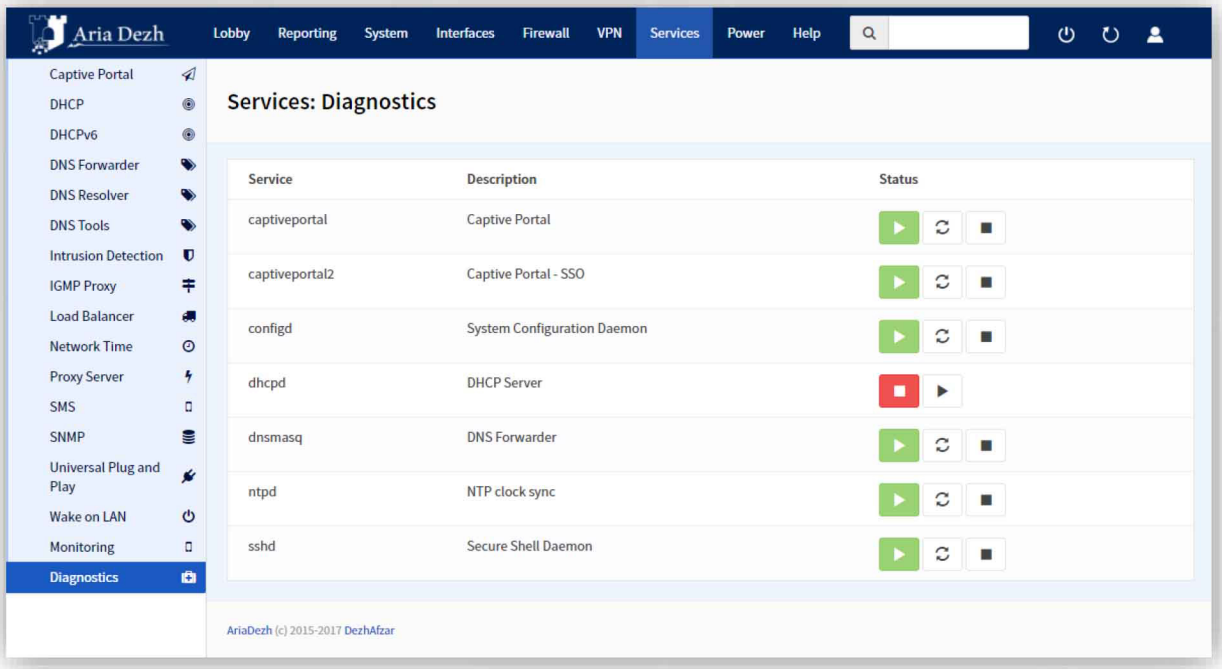

Figure 5- In this page, services can be enabled/disabled.

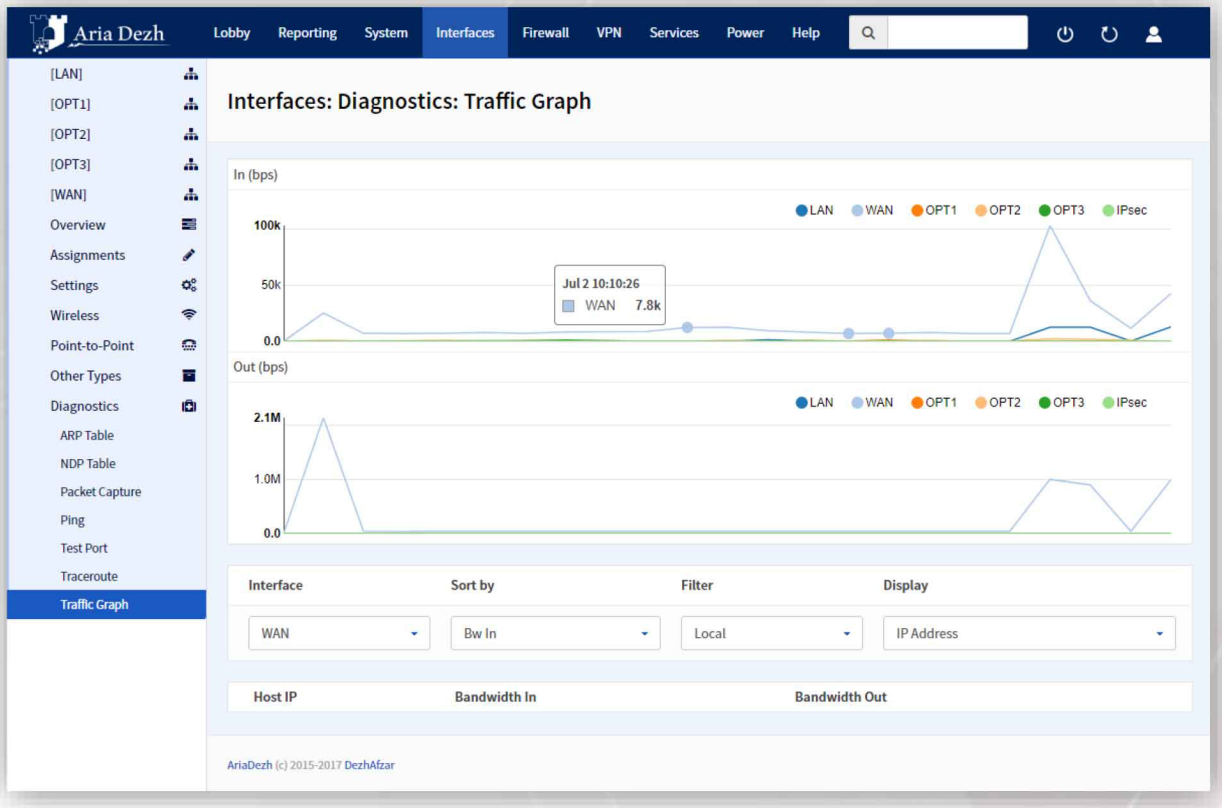

Figure 6- Network bandwidth usage on physical and virtual interfaces.

5- Application Layer Protocol Inspection

Ariadezh UTM provides a layer 7 protocol inspection capability which can be used to ensure that the specified traffic in a firewall, is used for a specified protocol only. This can ensure that open ports and addresses in the firewall are not misused for passing illegitimate traffic over other protocols.

Application layer protocols that Ariadezh UTM can detect:

- HTTP
- FTP
- IMAP
- SMTP
- SSL/TLS: supports HTTPS and may other protocols that implicitly use TLS, e.g. FTPS, SMTPS, IMAPS.
- SSH: supports all protocols that use SSH tunnels, e.g. SFTP, SCP, RSH, FISH.

It is also possible to add custom protocols to application layer inspection based on customer request.

6- SNMP

Ariadezh UTM supports the three versions of SNMP.

Capabilities

- Live monitoring of network connections
- Compatibility with many management and monitoring systems
- Monitoring servers: bandwidth usage, online status, …
- Real-time information about firewall status and possible faults and events in the firewall and network.

7- Web and FTP Proxy

Ariadezh UTM proxy service can be used to monitor and control HTTP, HTTPS, and FTP traffic. The proxy service supports web URL filtering and access control lists, and transparent proxying. By using this proxy service, as well as the firewall and the captive portal side-by-side, Ariadezh UTM can impose the desired control and monitoring over network users' activities. Captive portal can force users to authenticate before accessing the network. Firewall rules can be used to control network traffic based on source, destination, and protocol. Proxy can be used to monitor and control HTTP and HTTPS traffic. For example, you can block a user's access to a specific web site. There is also room for integration of ICAP-enabled antivirus software.

Other Features

- Enforcing ACLs on users
- Logging user-generated events
- Logging users' web access requests

8- H.323 and SIP Proxy

Ariadezh UTM can act as an H.323 gateway and proxy. This allows for greater control over VOIP traffic of the network. This feature will also resolve many issues that are usually associated with using H.323 and SIP behind corporate firewalls.

9- Firewall

Ariadezh firewall is stateful and keeps track of all open and recently closed TCP and UDP connections, as well as many other IP protocol transactions like various types of ICMP packets. It also allows easy management and categorization of firewall rules. The firewall can perform full normalization and reconstruction of IP packets to detect malformed packets that can harm network hosts. This normalization process removes any ambiguity in interpretation of TCP/IP headers of packets. It discards packets that have incorrect TCP flags which can potentially harm network hosts and the UTM itself.

Other Features

- Categorization and color coding of firewall rules
- Searching the ruleset
- User-based and group-based rule writing
- Scheduling of firewall rules

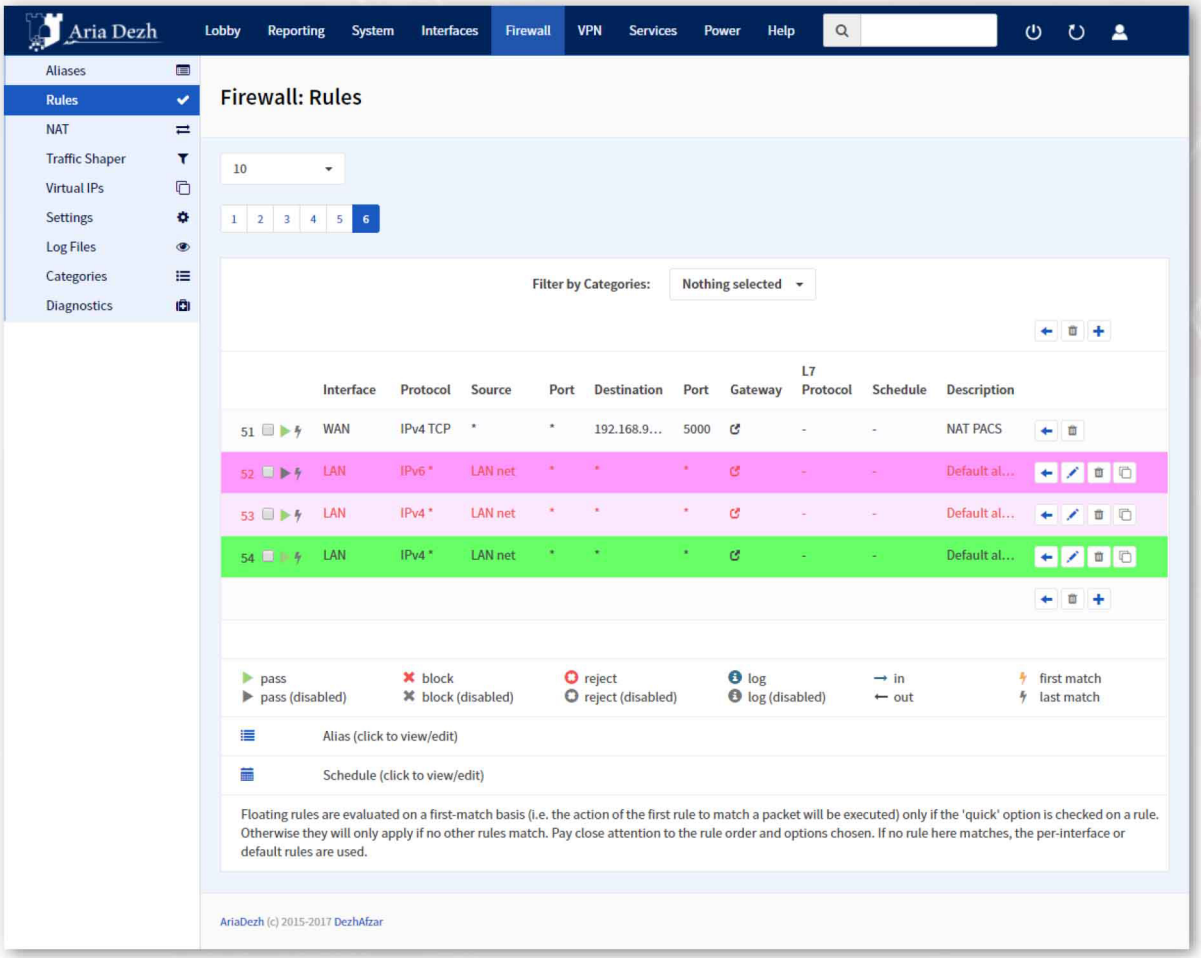

Figure 7- The main page for editing the firewall ruleset which also allows for color coding of rules.

10- Captive Portal

Through captive portal, the administrator can force the users to authenticate before they can access the network. For supported clients and systems, this authentication can take place automatically without user intervention. Captive portal is mostly used in hotspot networks, but in general it is usable in any network which needs another level of visibility and protection. It supports Active Directory and RADIUS as the authentication source.

Ariadezh captive portal also supports voucher-based authentication which can generate passwords that grant temporary (timed) network access to users. This can be used in public networks like hotels and restaurants to control internet access.

Features

- Automatic and transparent authentication of supported clients via NTLM protocol (Integrated Window Authentication or IWA)
- Support for multiple versions of Microsoft Windows Servers
- Support for LDAP as an authentication source
- Automatically closing sessions of logged off and inactive users

11- User Management

In the user management panel, the administrator can register and manage user accounts and groups settings.

Features

- Defining overlapping or separate groups of users
- Managing users' sessions timeout
- Defining various authentication sources, e.g. LDAP, Radius, Voucher, …
- Defining phone numbers for sending text message.
- Defining daily, weekly, and monthly traffic quotas.

12- Modes of Deployment

Ariadezh UTM supports two modes of deployment.

Bridge Mode

In this mode, the UTM operates transparently in layer 2 of the TCP/IP network. However, the system is still capable of monitoring and inspecting packets at layer 3 and higher

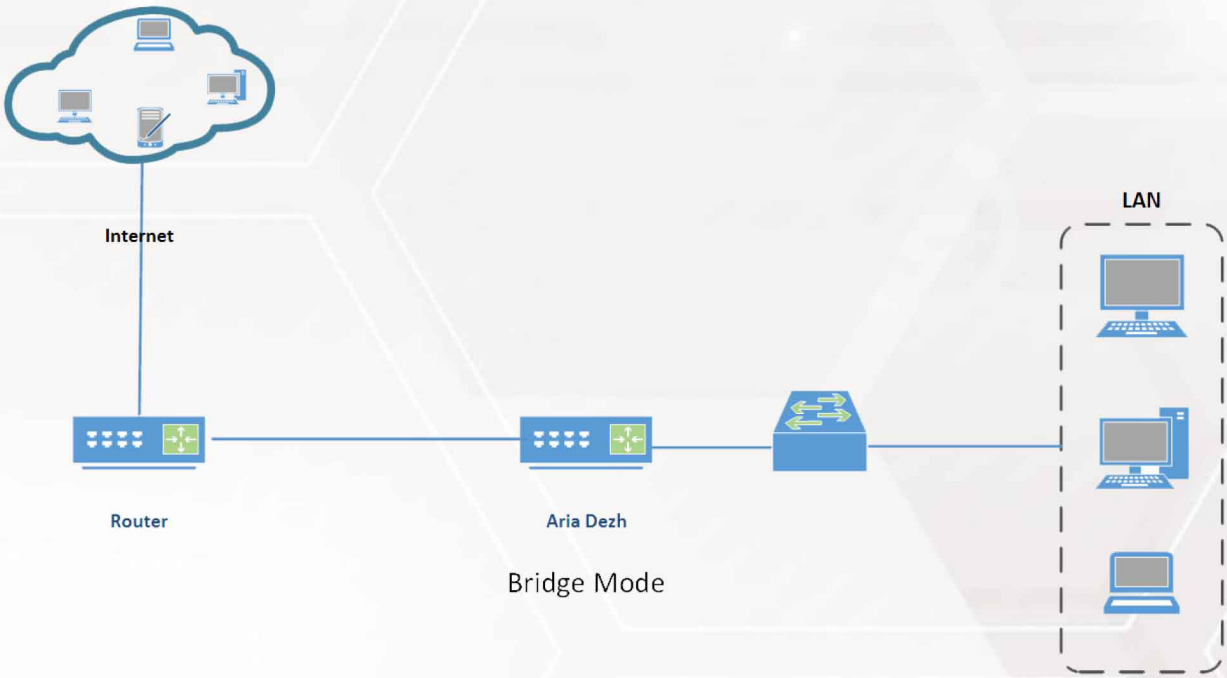

Figure 8- Transparent or Bridge mode of deployment of Ariadezh UTM

In this mode, the UTM is usually placed between the edge router and the internal network. In most cases this can be done transparently without making any changes to the network configuration.

Route/NAT Mode

In this mode, the router is operated as a gateway and router among two or more trusted or untrusted networks and/or the internet. The system will be in charge of performing network address translation and routing.

13- Accounting

Ariadezh UTM allows the administrator to monitor and control traffic usage of network users and clients.

Features

- Imposing daily, weekly, and monthly traffic quotas over users and groups.
- Viewing traffic usage and remaining quota of each user.
- Reporting remaining quota to the users.

14- Aliases

Through aliases you can group together many network addresses, host names, IP addresses, or port numbers under a single alias, and use them in one or more firewall rules. This makes the configuration of the UTM easier and less error-prone.

15- IP Geolocation

Ariadezh UTM enables the administrator to easily make a list of IP addresses based on the country in which the corresponding network resides. This allows for writing rules based on the geographical source/destination of a packet.

16- Network Address Translation

Full support for NAT modes:

Port Forwarding (Destination NAT)

Allows directly accessing an internal network server from an external network, without assigning it a public IP address.

Outbound NAT (Source NAT)

Translates outgoing traffic based on source address.

One-to-One

Translates one address to another specific address.

NPT (IPv6)

Translate one IPv6 address to another.

Figure 9- Network address translation (NAT)

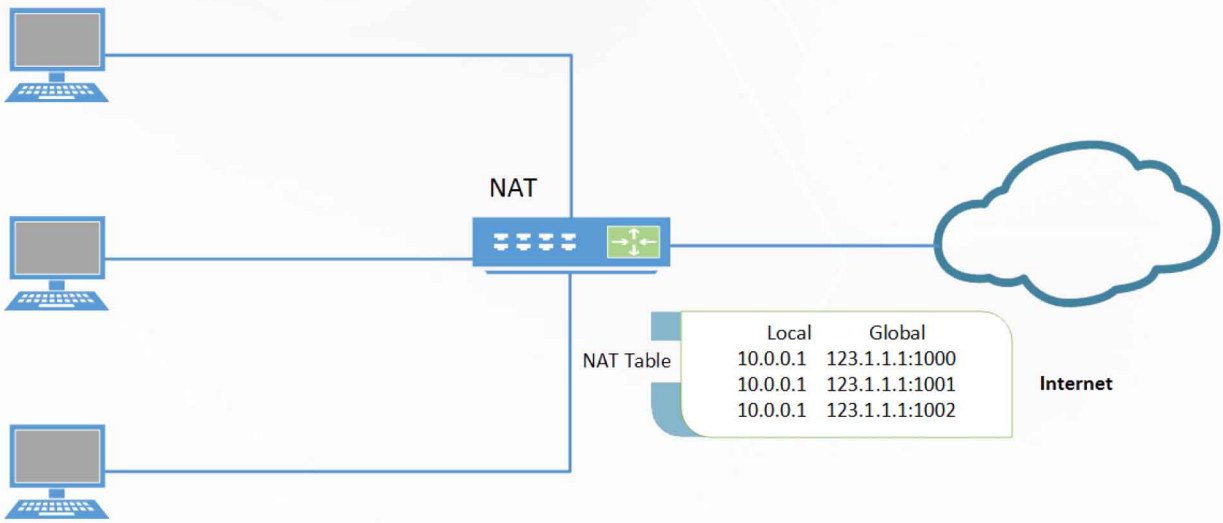

Figure 9- Network address translation (NAT)

17- Traffic Shaping

Ariadezh UTM traffic shaper allows the administrator to define a set of rules to manage how much of the total bandwidth of the network is utilized and how it is shared among existing clients. Ariadezh Traffic Shaper is very flexible and is designed based on pipes, queues, and rules defined for traffic selection.

Pipes limit the allowed bandwidth for the selected traffic, and queues define the relative priority of traffic flowing over a single pipe. Rules define which traffic goes over which pipe or queue. Traffic shaper rules work independently of firewall rules and other filtering stages of the UTM.

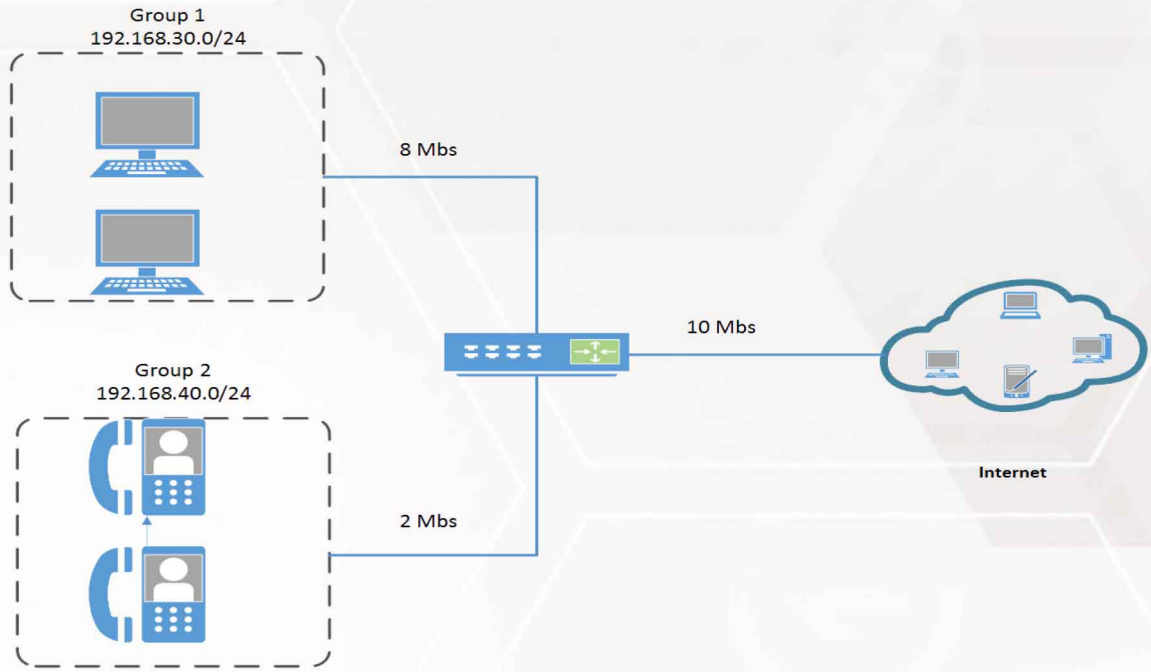

Figure 10- In above diagram, the bandwidth of users in group 1 is limited to 8 Mb/s, while the bandwidth of users in group 2 is limited to 2 Mb/s

18- DNS

DNS Forwarder

Allows forwarding of DNS queries to servers outside of internal network.

DNS Resolver

Answers to name resolution queries, directly.

DNS Tools

A set of tools for better control and utilization of DNS, e.g. DNS lookup, dynamic DNS, DNS filter, …

19- Intrusion Detection and Prevention (IDS/IPS)

IDS/IPS service inspects the traffic more deeply than the firewall. Similar to anti-virus tools, they inspect the packets headers and payload, against a large set of known attack signatures, and then sends appropriate warnings to the administrator and/or blocks the offending packets. The IPS defends the network in two stages:

1. Detects abnormal activities in the network and prevents port scans and DDOS attacks,
2. Fights against backdoors and exploits using its built-in attack signatures database.

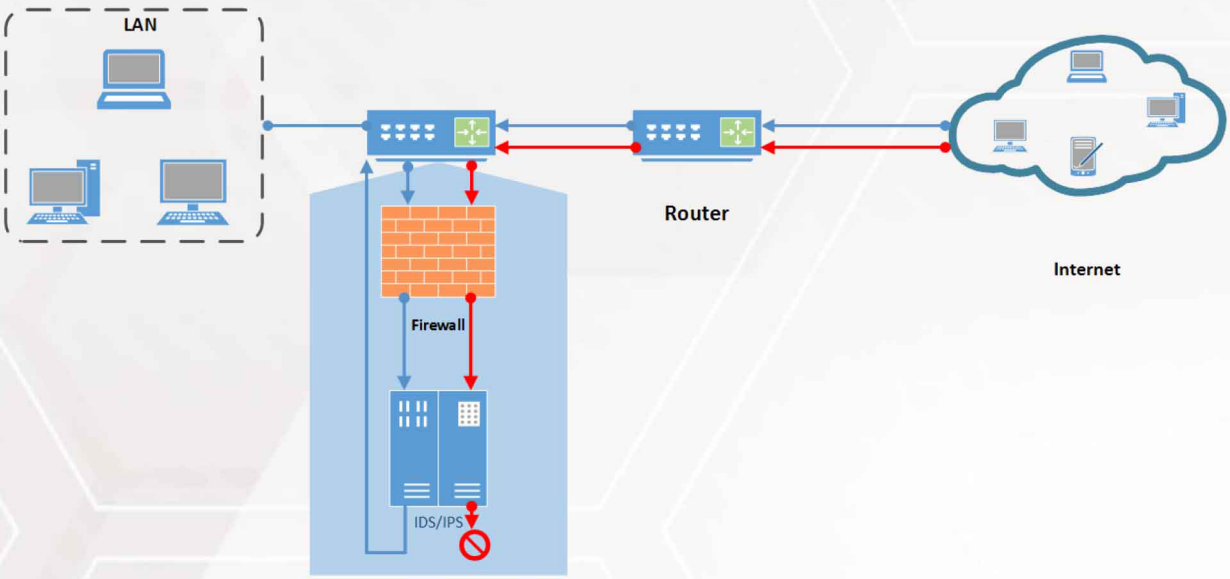

Figure 11- Intrusion detection and prevention system

20- Virtual Private Network (VPN)

VPNs are generally used to established a secure link among two or more networks.

Ariadezh UTM supports a wide range of VPN technologies including OpenVPN, IPsec, PPTP, and L2TP. Configuration of site-to-site and roadwarrior connections can be done in just a few minutes.

Other Features

Ariadezh UTM is able to support customized cipher algorithms for VPN connections based on customer's request.

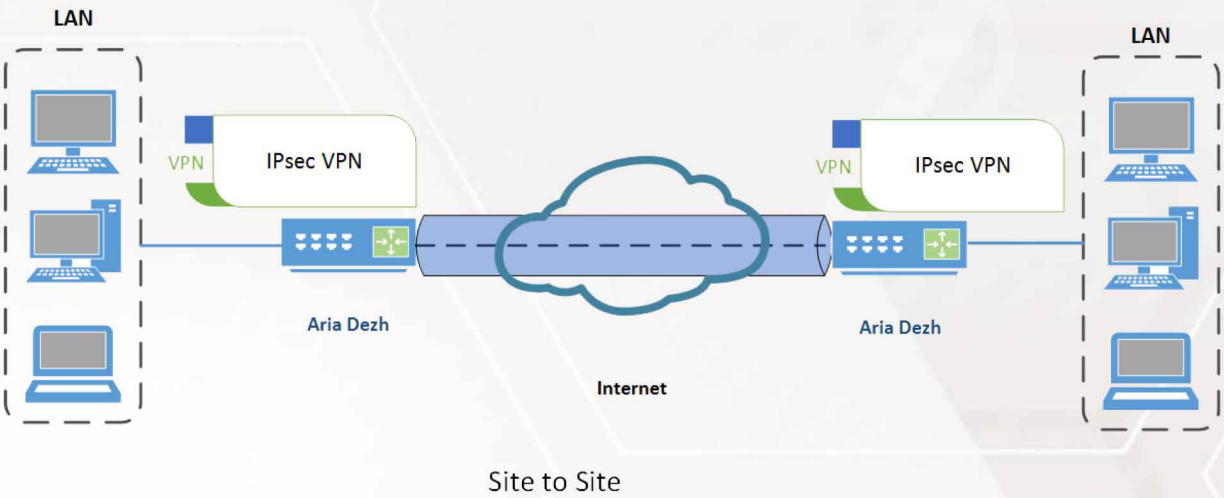

Figure 12- Host-to-net VPN configuration

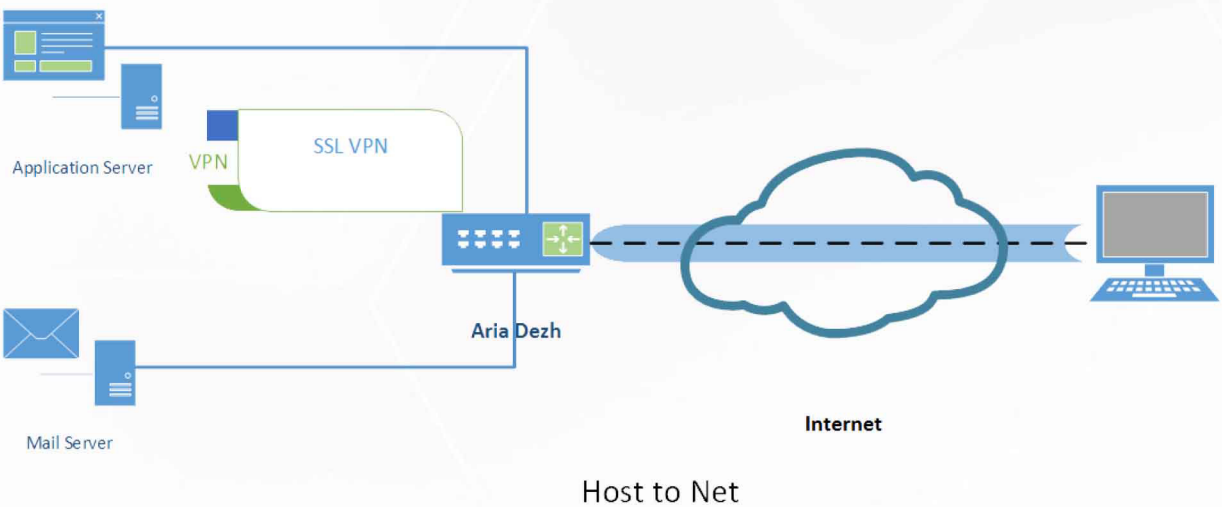

Figure 13- Net-to-net VPN configuration

21- High Availability (Hardware Failover)

Ariadezh UTM supports hardware failover, so that two or more UTMs can be configured as one failover group. If the primary system loses connection or fails, the secondary system takes over with no or minimal service disruption. This feature in effect turns Ariadezh UTM into a zero-downtime security appliance.

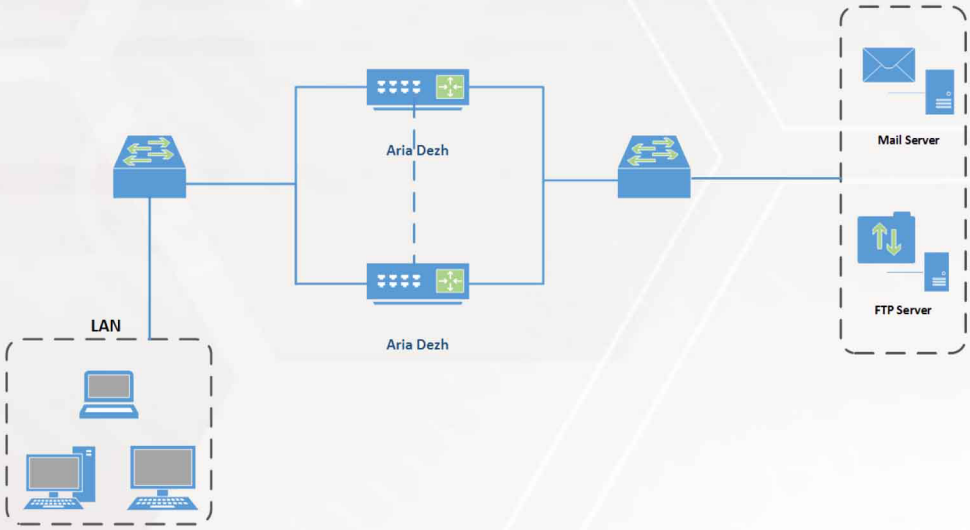

Figure 14- Network configuration in presence of High Availability(Hardware Failover)

22- Load Balancing

To prevent network servers from being overloaded, Ariadezh UTM features load balancing to distribute the load among multiple server. This also reduces service outage and downtime.

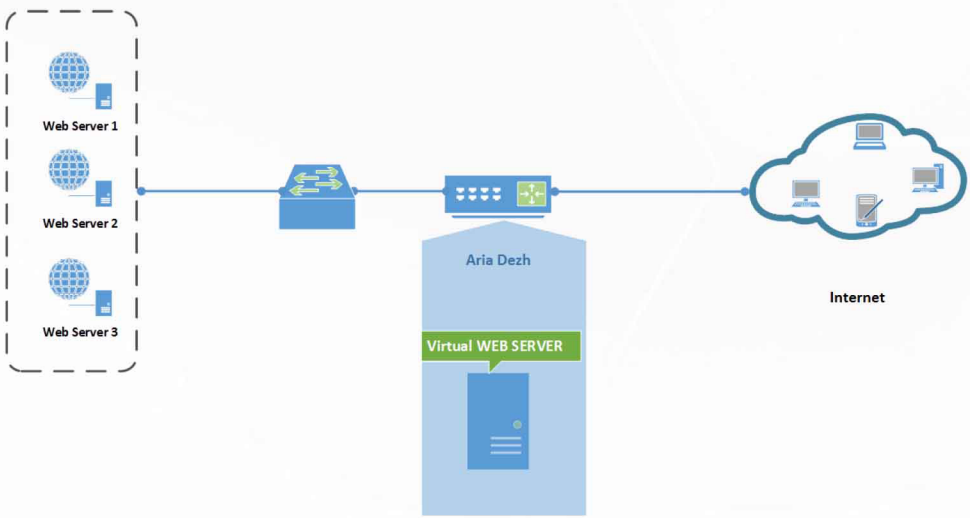

Figure 15- Deployment of Ariadezh UTM for load balancing

23- Simultaneous High Availability and Load Balancing

This will minimize the overall network and service outage.

24- DHCP

Full support for DHCP services:

DHCP Server

Automatic assignment of IP addresses to network hosts

DHCP Relay

Send/receive DHCP requests and responses among hosts that are not on the subnet.

DHCPv6 Server and Relay

Same capabilities as explained above, for IPv6 networks.

Other Features

- Display a list of leased IP addresses alongside more details about each host
- Reporting of DHCP service activities
- Support for static DHCP mapping, in order to statically assign IP addresses to specific hosts.

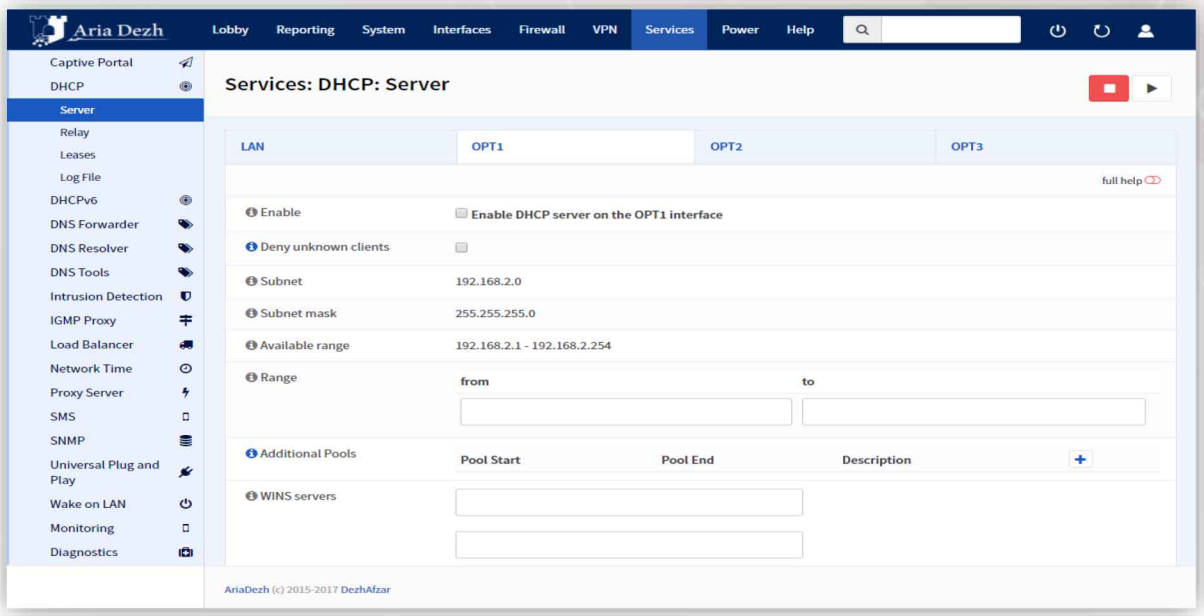

Figure 16- DHCP configuration page

25- SMS Module

Important system and network events can be texted to user-defined phone numbers.

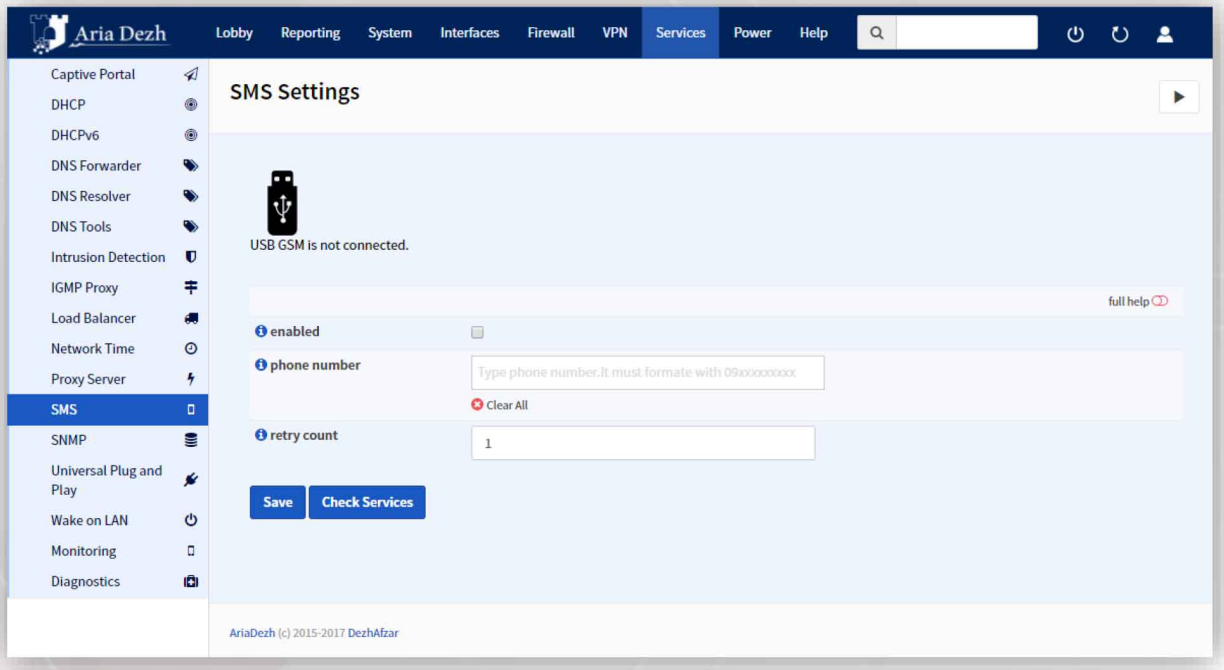

Figure 17- SMS module configuration page

26- Advanced User Manual

Ariadezh UTM user manual is fundamentally different from those of similar products. Our user manual is completely scenario-based. It presents step-by-step instructions for activation and configuration of each service for different use cases.

27- Management of Network Interfaces

The administrator is able to assign, configure, and control network interface properties. There are 6 types of network interfaces in Ariadezh UTM:

Bridge	Connecting two or more devices in bridge mode in the second layer of a TCP/IP network.
GIF	Creating a logical tunnel for IPv4 and IPv6 traffic.
GRE	Creating a point-to-point tunnel between hosts
Group	For grouping network interfaces, and writing firewall rules for groups instead of individual interfaces.
LAGG	For aggregating multiple interfaces into one virtual link with higher bandwidth and reliability.
VLAN	For virtual LANs

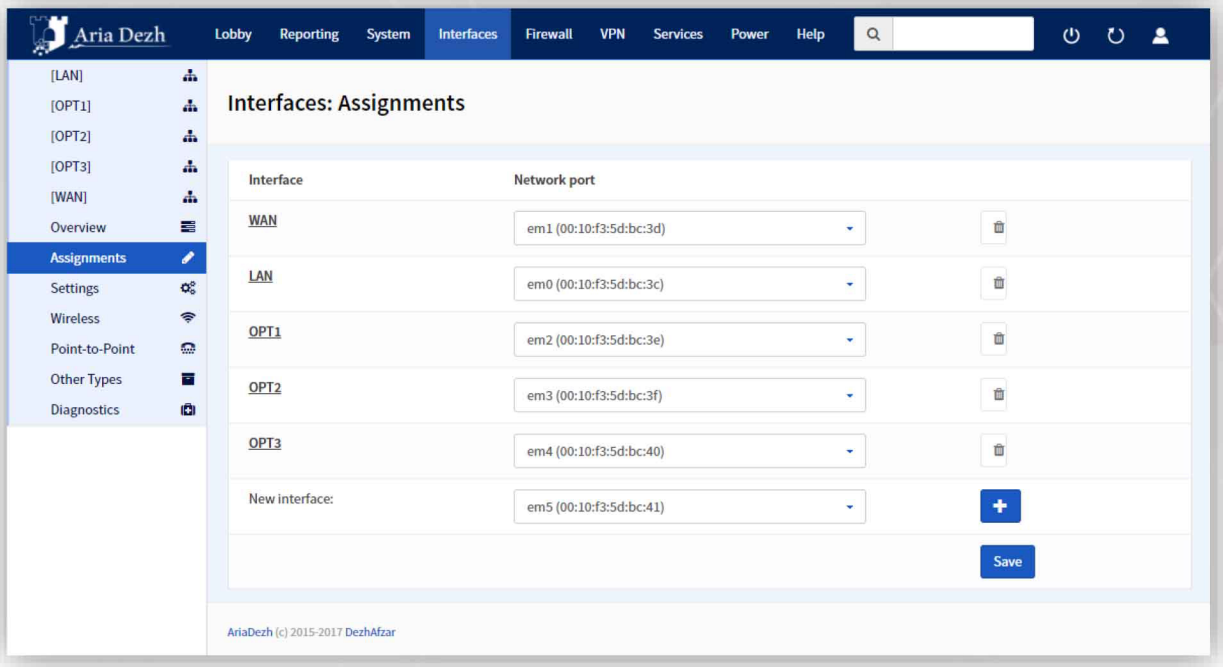

Figure 18- Web interface for definition of network interfaces.

28- Application Layer Network Monitoring

One of advanced features of Ariadezh UTM is its ability to inspect application layer traffic in detail, and present it to network administrators in neat diagrams and tables. This service can present network traffic in the following forms:

- Sort traffic log based on various criteria e.g. IP address, TCP/UDP port numbers, Layer 7 protocol, …
- Visualizing network traffic (IPv4 and IPv6).
- Generating extensive reports about various aspects of the network e.g. operation capabilities and protocols.
- Generating report for each network flow including RTT delay, TCP statistics, bytes/packets.
- Continuous storage of traffic statistics on disk in RRD format
- Generating reports based on geographical location of hosts.
- Detection of application layer protocols through deep packet inspection.
- Inspection of certificates of SSL/TLS connections.
- Reports on how TCP/IP traffic is spread among different protocols.
- Analyzing IP traffic and sorting based on source/destination addresses.
- Displaying subnet matrix IP traffic (specifying connection endpoints)
- Reporting IP traffic and sorting based on protocol type.
- Generating HTML5/Ajax traffic statistics

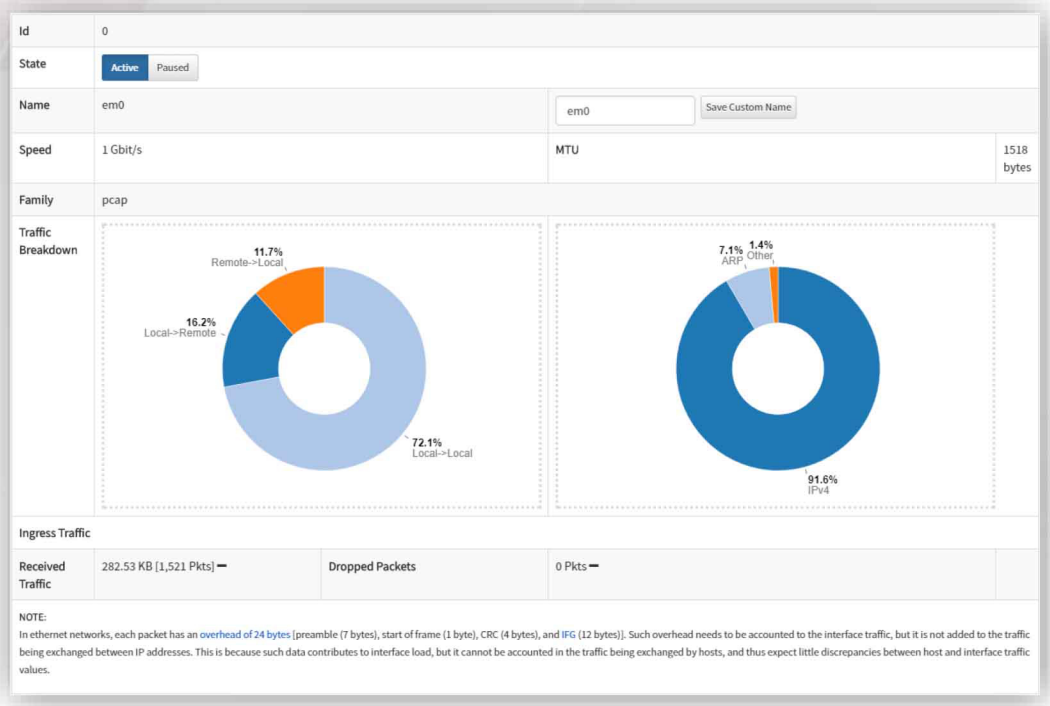

Figure 19- In this page you can view inbound-outbound transmission statistics.

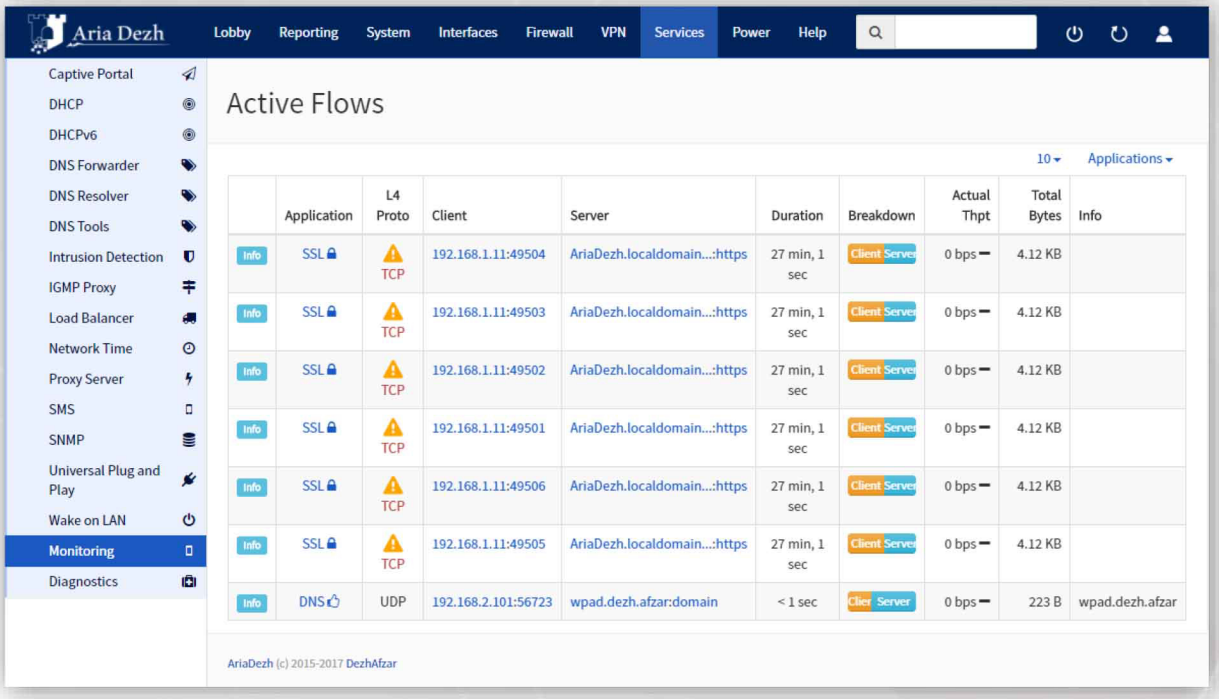

Figure 20- Viewing active network connections

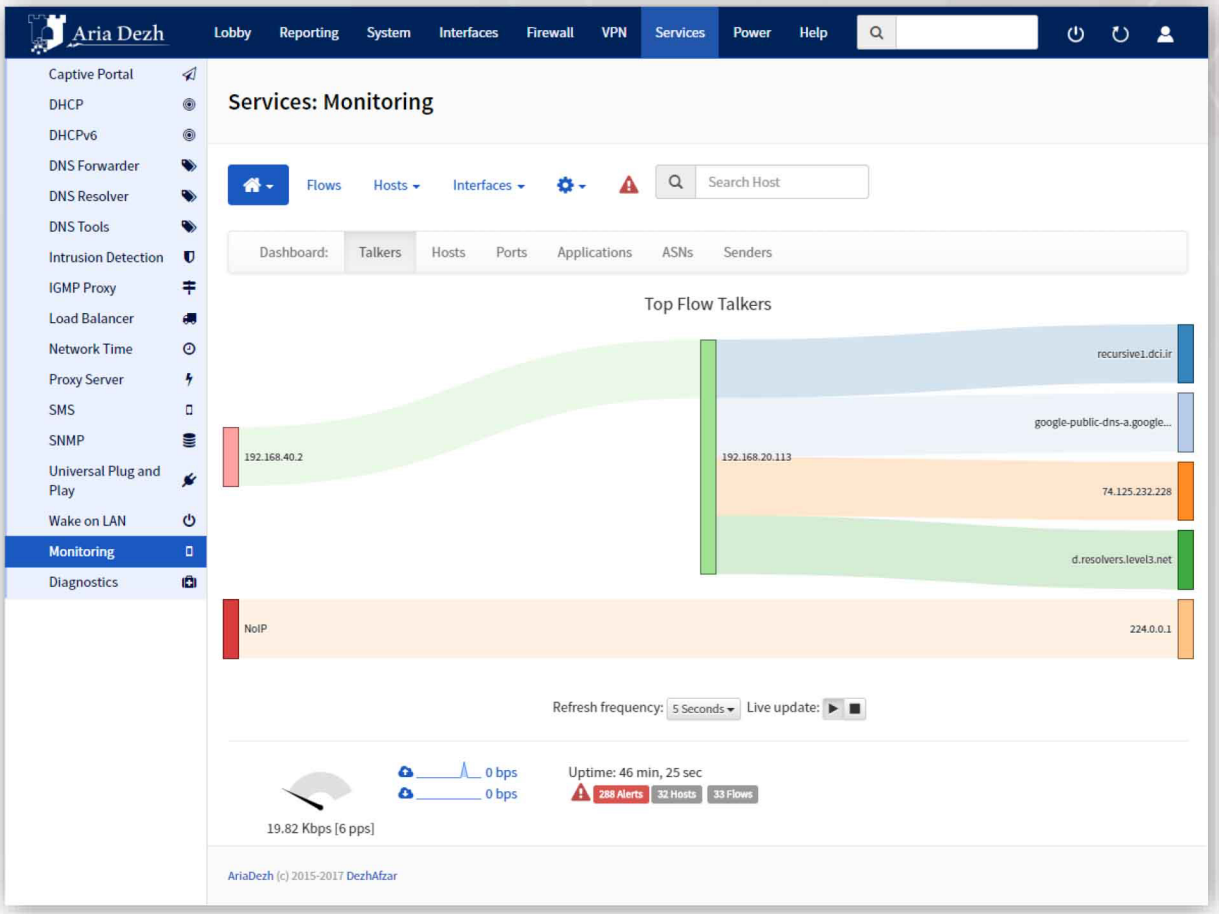

Figure 21- Viewing per-IP address network connections

29- Routing

Static routing: in this mode, the administrator can define routing tables statically based on destination addresses of packets.

Policy-based routing: In this method, the administrator can use many more parameters of the traffic in the routing decision, such as source IP address, source/destination port numbers, etc. In this mode, the routing decision is made through firewall rules and a gateway that can be defined for each rule. Leaving the gateway empty will prompt the UTM to use the default routing mechanism for the packet.

30- Web GUI

Simple and well-classified web interface of Ariadezh UTM, allows the administrator to use the system and monitor its subsystems, with minimal complications.

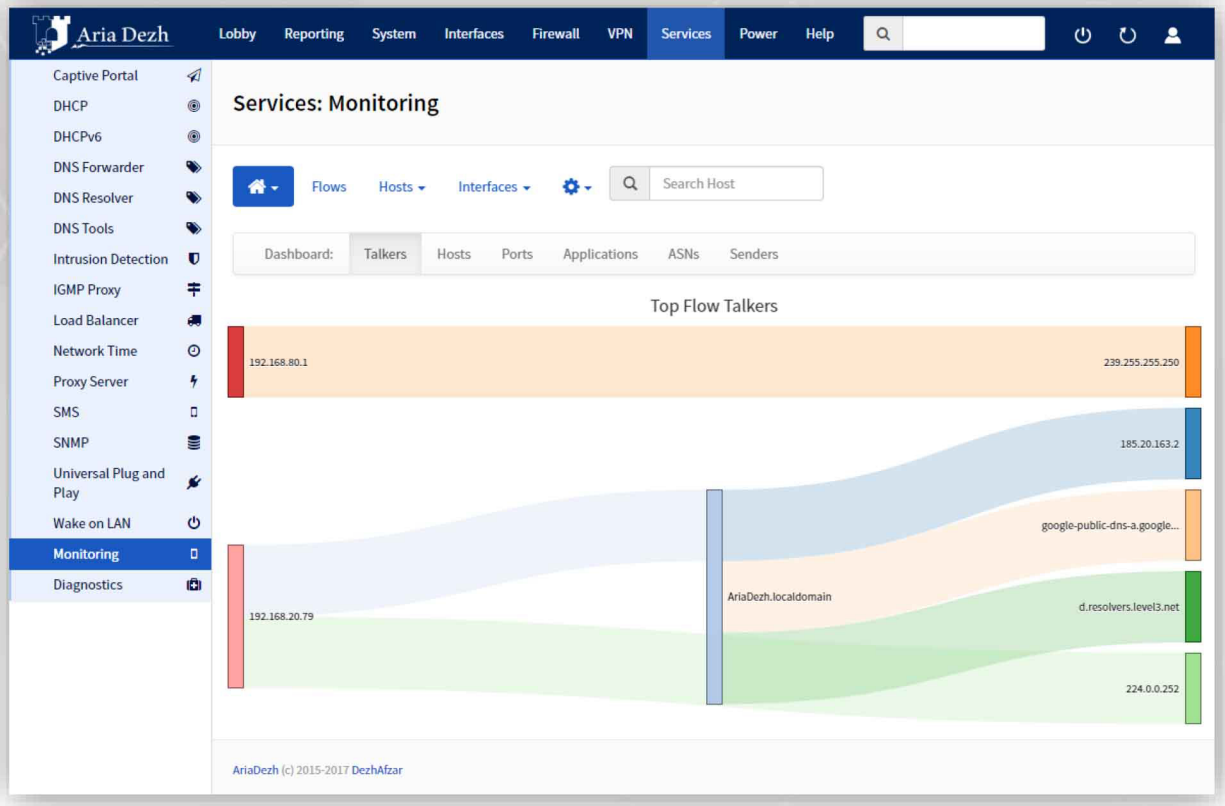

Figure-22 Viewing current network connections

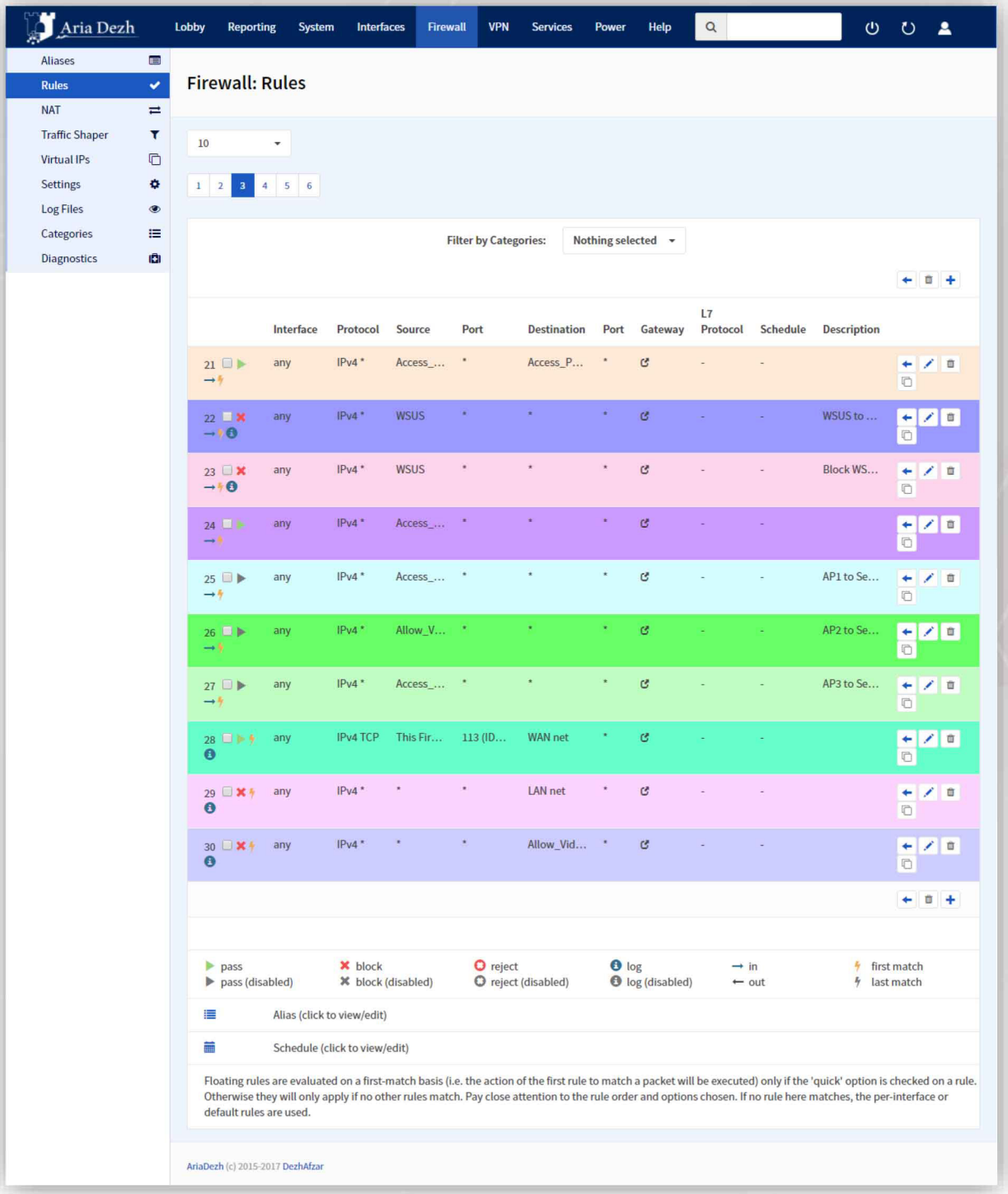

Figure-23 Firewall rules table

Memo:

Memo:

http://www.dezhafzar.com info@dezhafzar.com