

epati

Dashboard

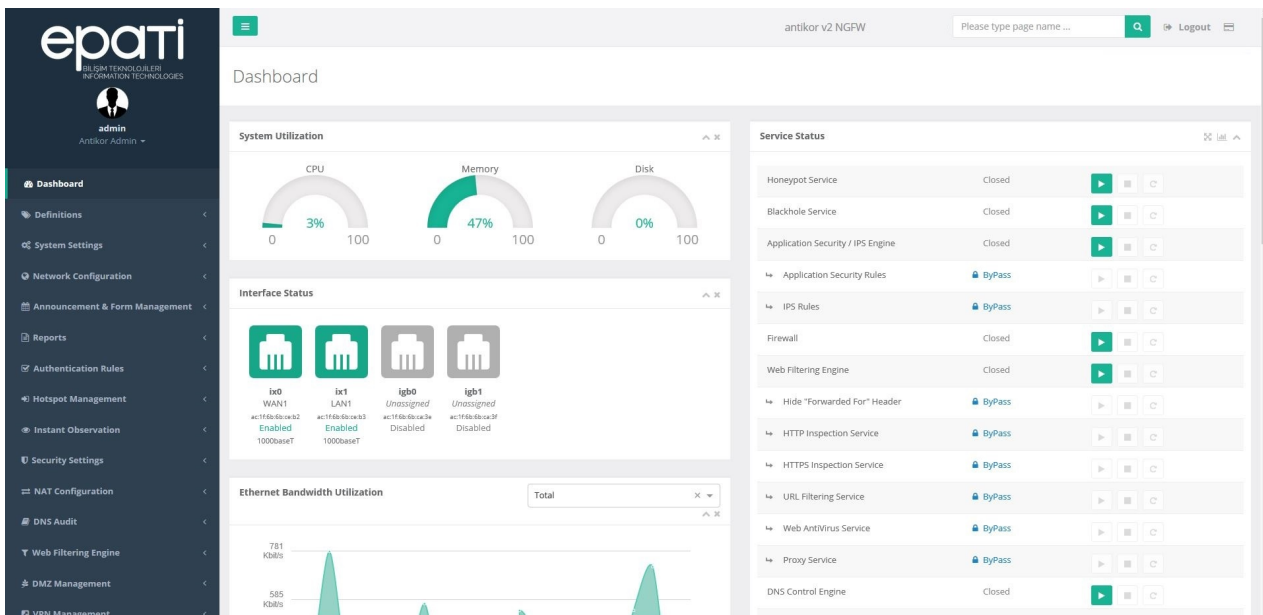
Product: Antikor v2 - Next Generation Firewall
Guides

Dashboard

The Dashboard instantly shows the following situations:

- System Utilization,
- Interface Status,
- Ethernet Bandwidth Utilization,
- Network Buffer Utilization,
- Network Counters,

Antikor System Updates are also performed on the Dashboard. The services that are automatically triggered when any setting is changed are again shown here. It also shows how many times each service is called out. As shown below, an image from the Service screen shall be showed in Service descriptions and Update screens, respectively.













Service Status

- **Honeypot Service**
Even though certain configurations (ports) are passive, honeypot can actively display these configurations. If any attacker tries to gain access by noticing this, it will be blocked and the log will be kept.
- **Blackhole Service**
This is the service that allows packets to be dropped for Dos/DDoS attacks transmitted by the router. To start the service, there must be more than one WAN IP address block in the IP pools.
- **Application Security/IPS Service**
Using the signature database, a service developed for filtering applications matching with signature.
- **Firewall**
Bypass without NAT, bypass with NAT, normal pass, block, deny is a service developed for filtering rules.

- **Web Filtering Engine**
 - It is a service developed for filtering rules for web pages.
- **DNS Control Engine**
 - It is a service developed for filtering web pages over DNS.
- **FTP Control Engine**
 - It is a service developed to connect to FTP server in Antikor.
- **DHCPv4 Service**
 - It is a protocol that enables the automatic configuration of address configurations such as IP, subnet, gateway of the devices which are on the local network and can be connected to the internet.
- **DHCPv6 Service**
 - It is a protocol that enables the automatic configuration of address configurations such as IP, subnet, gateway of the devices which are on the local network and can be connected to the internet. Unlike DHCPv4, it uses features such as NDP (Neighbor Detection Protocol).
- **DHCPv4 Relay Service**
 - DHCPv4 paketlerini belirlenen bir routera yönlendirilmesi için geliştirilmiş bir servistir.
- **DHCPv6 Relay Service**
 - DHCPv6 paketlerini belirlenen bir routera yönlendirilmesi için geliştirilmiş bir servistir.
- **Anti-Spoof Service**
 - Spoofing is a high-tech service designed to prevent attacks. For these types of attacks IP-Spoofing, DHCP-Spoofing MAC-Spoofing example can be shown.
- **QoS - Effective Bandwidth Management**
 - With this module, traffic flows can be prioritized, bandwidth can be booked and bandwidth limit can be set.
- **Hotspot Service**
 - Hotspot service ensures that internet access is safe in public spaces (universities, municipalities, etc.). Each user is provided with special records and logs are kept and necessary security measures are provided.
- **Bandwidth Monitor**
 - Monitor the current bandwidth of the total traffic on the line.
- **Registration Service**
 - Antikor may request registration from every client who wants to go online. After the service is activated, unregistered clients will not be able to access the internet.
- **Announcement Service**
 - Announcement can be made for Local Network or VLANs. When the client tries to access the Internet, the announcement is displayed and the connection cannot be continued unless the Read button is pressed.
- **MAC-IP Matching Service**
 - It is the service that enables the matching of MAC and IP information of the clients included in the network.
- **MAC Quarantine Service**
 - It is the service that prevents access to MAC addresses in quarantine.
- **Static ARP Service**
 - A service that ensures that the antibody does not connect with any MAC and IP address except for the clients registered on the LAN side.

- **Netflow Service**
It can collect traffic headers and send them to a designated collector. This makes it easier to analyze Internet traffic. It also facilitates the detection of IP blocks required for the implementation of the QoS service and the detection of IP blocks of DoS attacks.
- **RADIUS Service**
RADIUS (Remote Authentication Dial-In User Service) is a service developed for users to access AAA (authentication, authorization and registration).
- **SSL VPN Services**
SSL VPN (Secure Sockets Layer Virtual Private Network) is used to securely access any network remotely. SSL encrypted communication is provided through SSL VPN.
- **VPN-IPSec Service**
It is a protocol that connects the central and central endpoints to each other using validation and encryption. It has the authority of mutual verification and key exchange with the protocols it contains.
- **Site to Site VPN Service**
Site to site VPN is a common network used to provide secure communication between organizations for remote location offices or with any organization.
- **Dynamic Routing Engine**
Dynamic routing is that routers used on the network share routing tables with each other.
- **LLDP Service**
LLDP operates independently of the brand of network devices used and is used as a protocol for network topologies and network devices discovery. If this service is to be used, this service must be started after the required LLDP settings have been made.
- **Routing - Policy Based Routing (PBR)**
The PBR service directs packets to the desired routers according to the requested protocol, source/destination address and port information.
- **HTTP(s) Server Forwarding Service**
It is a service developed for HTTP / HTTPS servers on the LAN to connect to the internet.
- **SNMP Service**
Works in Layer 7 (Application Layer) layer. It is the service that enables the network devices to be managed and monitored more easily.
- **Campus Information Service**
By drawing the RRD graphs of the external campuses via the output ethernet in the system, it allows to obtain these RRD graphics from the links created. It also gives the number of Active Devices instantaneously. It is sufficient to copy the generated links to the relevant fields in ULAKBİM end statistics.

Area	Explanation
	Click the button to start the service.
	Click the button to stop the service.
	Click the button to restart the service.

Area	Explanation
	Indicates that the service is down.
	Indicates that the service is running.
	Indicates that the child service is in ByPass. This symbol indicates that the sub service will not start even if the main service is started.
	Indicates that the child service is in ByPass. This symbol indicates that if the main service is opened, the sub service will also start.
	Indicates that no configuration related to the service has been made. In order to start the service, settings related to the relevant service must be made in the interface.
	If service-related configurations have been made but then started without entering any settings, the user will encounter this symbol. (For example, if the security rules are empty, the Firewall will not be started.)
	It shows that the service is still running in the background and cannot be stopped. (If there are any settings entered, you should set them to Passive.)

Dashboard Page Search and License Version List

The above illustration shows where to search the page and how to navigate to the [License Version List](#).

ePati Cyber Security Technologies Inc.
Mersin Universitesi Ciftlikkoy Kampusu
Teknopark Idari Binasi Kat: 4 No: 411
Zip Code: 33343 Yenisehir / MERSIN / TURKIYE

 www.epati.com.tr
 info@epati.com.tr
 +90 324 361 02 33
 +90 324 361 02 39

