epati
INFORMATION TECHNOLOGIES

Frequenty Asked Questions

Frequently Asked Questions

www.epati.com.tr

Frequenty Asked Questions

How do I install AntiKor ?

> You can easily set up by looking at the links to theAntiKor NGFW installation guide and the AntiKor Layer 2 Tunnel installation guide.

How many installations can I do with the current license ?

> With the current license **the same machine** can be installed a maximum of 10 times. If the right of installation is needed teknik@epati.com.tr e-mail address.

Where can I look at the scope of my license ?

> When the antikor web interface is opened, you can see your license content and version list by clicking on the card icon next to *log out* in the upper right corner.

I can’t access the interface, how do I turn it on ?

> After you access the console panel with user name: admin, password: antikor by connecting the keyboard and monitor to your device, you will be entered into the Administration panel Access Settings from the system settings and the IP address to be accessed with the add new registration wizard must be added.

I forgot my interface username or password. How do I reset a password ?

> After you access the console panel with user name: admin, password: antikor by connecting the keyboard and monitor to your device, you can enter Change User Password from System Settings, list users and change your password.

I can’t access the antikor NGFW from the network, how can I change the IP address ?

> After accessing the console panel with user name: admin, password: antikor by connecting the keyboard and monitor to your device, you can enter Network IP settings, WAN Settings, list users and change your IP address.

How do I provide SSH connectivity ?

> Users must first produce ssh-key and introduce it to the AntiKor. You can access your product’S IP address and port 22022 by using the ssh key that you produced and introduced to the antikor.

Can I change hardware after installation ?

> Antikor products detect hardware during installation and provide installation according to your hardware. No hardware changes should be made after installation.

How Can I do static NAT ?

> Static NAT configuration example will solve this problem.

How do I do Active Directory integration ?

> What to do on the Active Directory and Antikor side is described in the step - by-step example of configuring Active Directory-Kerberos SSO integration.

Can I give Network and menu-based authorization to other responsible friends in the organization while managing the AntiKor ?

> The AntiKor NGFW is also capable of authorization according to the network group when it makes authorization. You can authorize the management of each network to different users and share your workload. Administrators can only View and manage settings for the networks they are authorized to use. For detailed information, see the Administration Panel Users document.

Where should the AntiKor positioned, what type of internet connection does it support ?

> The AntiKor is positioned just in front of the incoming internet connection. It supports PPPoE mode for Xdsls as operating mode, and Routing mode for Metro ethernet and routers. It also supports Transparent (Bridge) mode for those who do not want to make any changes to their network.

Does the AntiKor Cluster support ?

> Yes, there are. Feature that supports redundant operation of the system. It is based on the basis of simultaneous and collaborative work of AntiKor's developed in order to ensure continuity. If a server in the cluster has a hardware or software problem, another server is automatically activated. Thus, continuity is ensured. For detailed information, see the Cluster Settings document and the Cluster Configuration example.

How to install updates or innovations from AntiKor ?

> The AntiKor has an Automatic Update System. New updates are checked online with AntiKor NGFW's automatic update system. Individual packages are listed as" ready to update". When the user says "start updating", the update is done. If the update is critical, "critical" is displayed in red. Databases are" automatically " updated. All packages can be rolled back to the previous version.

How do I verify the information of users on my local network ?

> Any client who wishes to join your local network in the AntiKor is met with the AntiKor NGFW Registration Service Form. Here is a check of TC identification number accuracy. In the background, the user'S MAC and IP information is also automatically retrieved. The credentials obtained from the form can be verified via KPS(MERNIS), as well as SMS, LDAP, RADIUS, POP3 verification. For more information, see the registration service configuration example.

How do I block infected computers on my local network ?

> The AntiKor NGFW Antibot module intercepts communication with botnet command servers so that infected computers on your Network do not serve botnets. For detailed information, see the Network Definitions document.

How does the AntiKor take precautions against those who scan IP addresses that are not on my local network ?

> The AntiKor NGFW sends IP addresses that are not in its own IP pool to the Black Hole Service. These packets are not routed and ignored.

Does the AntiKor pass traffic from non-defined IP addresses ?

- It should protect the network from IP spoofing attacks, known as IP Spoofing, by analyzing traffic from all users within the organization.
- The AntiSpoof service can automatically block IP traffic outside the network by mapping the network's communications.
- It can prevent dirty traffic from coming out of the network and prevent getting caught in the honeypot.

I have both IPv4 and IPv6 IP addresses on my network. Does it work at the same time ?

> In the AntiKor, Dual Stack, i.e. both IPv4 and IPv6, both protocols work at the same time. It provides traffic control and analysis over both IPv4 and IPv6 simultaneously.

What layers of protection does the AntiKor provide ?

> AntiKor Dual Layer-double layer works simultaneously. You can take advantage of both Layer 2 and Layer 3 Communication at the same time. The AntiKor NGFW can communicate with your VLANs with Layer2 and collect MAC addresses, detect abnormalities, and even direct routing of Layer3+ and above in your connected networks.

Is there any protection against SYN attacks ?

> The AntiKor has SynFlood protection. Protects against Syn attacks from both the local network and the internet. The desired IP and ports can be excluded from this system.

How is the AntiKor prevented from interfering with internet traffic ?

> The AntiKor has a SPI-Statefull Packet Inspection module. Keeps track of what stage your packages are at from the start. Each link that is followed is stored in the state table. It takes your security to the next level by preventing intrusions and unsolicited answers.

Can I apply separate bandwidth to users on my local network ?

> AntiKor has QoS-enabled Bandwidth Management. Person-based maximum bandwidth can be defined. Speed Guarantee, priority assignment, rule-based QoS implementation, different configuration possibilities for each Ethernet interface. For detailed information, see the Ethernet QoS and Ethernet QoS Rules document.

Can I identify and block networks from the internet in the AntiKor ?

> The AntiKor can create network groups, and these groups can be defined as IP addresses or networks. These definitions can also be used in security rules, in access permissions, and in the private users section. Network group members can also automatically pull from the internet.(for example, ready IP lists or URL lists) For detailed information, see the network definitions document .

Can I identify port groups in the AntiKor ?

> In the AntiKor, Port definitions (Group) are made and port can be defined in 140 different protocols. These definitions are used in the firewall. For detailed information, see the Port Definitions document.

Can I Group clients on my local network in the AntiKor and define rules for these groups ?

> For clients, scope can be specified and groups can be created. It is also set here whether or not the group of users subject to the created groups will be shown in the registration form. The necessary operations can be done in filtering these groups. For detailed information, see the Client groups document.

Can I perform different filters on the AntiKor to my own users ?

> In the AntiKor, which users and computers will have what kind of powers are assigned. Filters also work as assigned to these clients. For detailed information, see the Private Users document.

Can I authenticate the AntiKor ?

> Authentication can be performed in the AntiKor through RADIUS service. AntiKor users are allowed to perform AAA (Authentication, Authorization, Accounting), authorization and registration. The required adjustments for RADIUS profiles, NAS definitions, RADIUS Proxy pools, and Proxy domains are made here. For detailed information, see the RADIUS Settings document.

How do I connect from home to the online databases of which the institution is a member ?

> Through the Proxy service, sites and memberships with membership of the institution can be entered as if they were at work from home. It can also be selected whether users will be included in the policies defined in the Web Filtering Management section. Logs of users entering the House are also kept. For detailed information, see the Proxy configuration example on the client side.

What logs does the AntiKor hold? What format does it hold ?

> The AntiKor supports 24 different log types and 7 different log formats. The settings of the syslog server/servers on which the server system logs will be recorded are made and forwarded to your log collector or SIEM in the preferred raw or structural log format. For detailed information, see the Syslog Settings document.

Can I identify the institution’s certificate to the AntiKor ?

> In AntiKor, the SSL Certificate Management menu is the section where the institution’s SSL certificate is defined. You can create your own certificate or install your existing certificate using the same module. For more information, see the SSL Certificate Management document.

The organization has only one IP address but I have more than one server, can I distribute it to those servers by domain name ?

> HTTP(s) server forwarding is the module in which forwarding is made necessary to eliminate the problem of access to network components that use the same WAN (real) IP address in an enterprise and serve people inside or outside the enterprise with the IP addresses they use. For detailed information, see the HTTP(s) Server Forwarding document.

Can I do an IP-MAC matching ?

> The AntiKor performs a special IP assignment to the devices thanks to DHCP. During the registration service, it automatically connects to the IP-MAC binary and matches it to the user.When the IP-MAC match is turned on from the services, those who change the IP cannot go online. For more information, see the DHCP Settings document.

Can I log traffic to all ports on the AntiKor ?

> The NetFlow service in the AntiKor can hold header(IP and TCP/UDP header) information and send it to a collector, not the content of traffic information. When sending this information, it can send all the information, only an IP, or a network group to the Collector. For detailed information, see the NetFlow Settings document.

How many different languages does the AntiKor support ?

It is the area where language settings are made in AntiKor. Total of 3 language options (Turkish, English, Arabic). For different web interface operations (e.g. user registration, announcement screen, access block Page, etc.) can work with different language options. For detailed information, see the Language Settings document.

Can I get the port names from the switches that the AntiKor is attached to ?

Settings for the LLDP connection are made in this menu. The settings are complemented by entering the system name and description of the LLDP network. After the necessary settings are made, observation can be made from the LLDP status under the Instant observation menu. For detailed information, see the LLDP Settings document.

Is it possible to use unclaimed WAN IP addresses ?

We need to define the IP ranges (internal and external) of the network you are managing in the IP Pools section of the AntiKor. These ranges will be used in AntiKor control mechanisms. Automatically fetches the added VLAN IP addresses. Some operations (client definitions, static NAT, etc. Can not be done without adding IP addresses to the IP pool. See the IP Pools document for detailed information.

Can ethernets be assigned more than one VLAN or IP address ?

In AntiKor, Ethernet settings, Ethernet (LAN), internet output (WAN), server zone (DMZ) and PPPoE settings are made from this section. Multiple LAN, WAN and DMZ interfaces can be added according to license content. If more than one IP address is required to be given to different or same ethernet interfaces in AntiKor, it can be given from this section. For detailed information, see the IP Alias, Ethernet Assignment and VLAN Configuration documentation.

Which types of AntiKor Link Aggregation support ?

It is used to increase the rate at which the AntiKor passes over it or to run the AntiKor as a Cluster. There are 6 different options as a merge type.

- Bridging
- Bridging - Rapid STP
- Link Aggregation - Failover
- Link Aggregation - Load Balance
- Link Aggregation - LACP
- Link Aggregation - Round Robin

For detailed information, see the Virtual Ethernet Aggregation document.

Can QoS be performed on Ethernet in AntiKor ?

Ethernet packets (audio, video, etc.) is used to determine the order of precedence. The main purpose of QoS applications is to enable the most efficient use of bandwidth. 3 different types of QOS (Quality of Service) can be defined: qfq (Quick Fair queuing), CBQ (Class Based queuing), HFSC (Hierarchical Fair-Service Curve). See the Ethernet QoS document for detailed information.

How do I deliver my announcements to local users on the AntiKor ?

You can make announcements to all users, groups, IP or IP blocks on your Network. No matter which Page the people you are making an announcement on appear in front of the announcement. He can’t keep going on the internet unless you press the I’ve Read button. For detailed information, see the Announcement Entry document.

Can I keep the reports somewhere else? How long do I have to keep it?

It has Samba or NFS support. You can discard these reports to your remote server. 6 of law 5651.these reports should be kept for 2 years as required by Paragraph B. For detailed information, see the Report Archive document.

What sources can I authenticate from ?

Services such as Hotspot, Proxy, VPN can be assigned an authentication policy with different identity providers. Supported Sources;

- Local Sources
- HTTP (Authentication)
- LDAP
- SSO : Negotiate/Kerberos - Active Directory
- RADIUS
- SMS
- Local Groups
- POP3 / IMAP
- HTTP (Api)
- TACACS+

For detailed information, see the Local Users document and Hotspot HTTP API Integration, Hotspot HTTP Authentication Integration, Hotspot LDAP Integration, Hotspot POP3 - IMAP Integration, Hotspot RADIUS Integration, Hotspot SMS Integration, Hotspot Local User configuration examples.

What supports are there in the Hotspot ?

Time-based quota support, traffic-based quota support, tracking of quota limits in relation to the account, per person login limit, support to continue traffic despite closing session information window, Hotspot module integrated into the software, staff in the organization, student mail addresses or student information systems can work together with the structure, the client/networks to be included in the Hotspot service and The software can verify credentials from mernis servers. If requested, it is possible to verify credentials by SMS. The service has LDAP, Active Directory, RADIUS, POP3, IMAP, POP3 SSL, IMAP SSL, JSON Web Service, XML Web service integrations. For detailed information, see the Hotspot Settings document.

How much is Application Security performance and the application it recognizes ?

It provides high performance thanks to the RSS-sensitive Multithreaded application recognition engine. It detects over 4500 applications with its extensive AppID database. The system can automatically update application signatures over the internet. System Layer 7 can perform deep packet inspection, detect and block application signatures. For detailed information, see the Application Security and IPS Settings document.

Intrusion detection and Prevention (IPS) also prevents what types of attacks ?

The AntiKor NGFW makes Attack Detection fast and powerful with its Multi-threaded analysis engine. By making rule-based identification, you can run different application filters on each client or network:

- Signature-based Intrusion Detection and Prevention
- ARP poisoning Attack Detection and Prevention
- Syn Flood Attack Detection and Prevention
- UDP Flood Attack Detection and Prevention
- DoS Attack Detection and Prevention

> See the Intrusion Detection and Prevention(IPS) document for detailed information.

What are the types of NAT used in AntiKor ?

> Dynamic NAT, static NAT, Nat by Destination, Port routing. For detailed information, see the Dynamic NAT, Static NAT, NAT by Destination and Port Forwarding documentation.

What are the DNS filtering options, how do I do it ?

> DNS blocking process is done and domain names, address-based, Active Time Zone, category-based configuration can be written. Different policies can be created according to client groups. For detailed information, see the DNS Filtering document and examples of DNS Filtering Address-Based Configuration, DNS Filtering Active Time Period Configuration, DNS Filtering SafeSearch Configuration, DNS Filtering Category-Based Configuration.

Can I cache my website-based sites for the AntiKor ?

> In the sites to be cached section, the names of the sites that users visit frequently and the programs that perform updates are written here. For example, update addresses of Windows and antivirus addresses can be written. In this way, after the first person who downloads, others receive automatic updates from this service. For detailed information, see the Cached Sites document.

How do I limit the speed of some sites ?

> Limits the speed of the sites entered in the sites to limit section to per client, the total of users in that VLAN(network) to per Network, and the total of all VLANs to the total category. Especially sites like rapidshare, megaupload, Hotmail are entered. For detailed information, see the document of Speed Limit Sites.

Can I Manage category for Web filtering and DNS filtering ?

> Category management can be added On Demand. There are also more than a hundred predefined categories on the AntiKor. The desired categories are allowed and the desired ones can be blocked in web and DNS filtering. For detailed information, see the Category Management document.

How do I separate my servers from the local network on the AntiKor, what are my options ?

> There are 3 different types of servers separation on the AntiKor;
>
> 1. Access Without NAT → DMZ zone the actual IP is used. Again, certain ports can be opened and closed to these IPs.
> 2. Real IP Access from Anywhere → DMZ zone. Both from the local network and from the outside world, this server is entered by NAT.
> 3. Real IP Access Only from the WAN → the server can be accessed via virtual IP from our local network, while it can be accessed via NAT from the outside world.

> For detailed information, see the Access without NAT Configuration, Real IP Access from Anywhere Configuration, and the Real IP Access Only from the WAN Configuration.

What types of VPN can I use on the AntiKor ?

> IPSEC VPN, L2TP/PPTP VPN, SSL VPN, Site to site VPN types are available. For detailed information, see IPSEC VPN Settings, L2TP/PPTP VPN Settings, SSL VPN Settings, and Site to site VPN Settings.

Can I conduct Policy-based Routing on the AntiKor ?

PBR is performed according to Protocol (IP, TCP, UDP, ICMP …), source address (IPv4 / IPv6), source Port, destination address (IPv4 / IPv6), Destination Port criteria. For detailed information, see the Policy-based Routing document.

How do I quarantine computers that distribute MAC addresses ?

In the case of AntiKor quarantine, it quarantines computers that perform arp poisoning at the Layer 2 level and present themselves as gateways and distribute the MAC address. After that, it prevents poisoning of the network by giving IP addresses from an unused IP block. Unless the system administrator removes that MAC address from quarantine from the web Administration panel, that computer will be denied internet access. In addition, manually add the MAC address we want to prevent the internet. For detailed information, see the Quarantine Status document.

Can I open trap ports for attackers on the AntiKor ?

On the honeypot service, they are traps that can detect port scans and connections to popular services. Trap and multi-attacked ports are entered into the system. The system fakes these ports. It prohibits those who attack these ports until the selected “blocking time”. We may enter and exclude “ignored” on our own network within our own IP. For detailed information, see the Honeypot Settings document.

How do I change my AntiKor server, transfer users and settings on it ?

All the settings in the AntiKor can be taken to our own computer and restored from backup at any time with Restore or these settings can be uploaded to another AntiKor. It is saved to our backup computer by pressing the Download button. AntiKor setting backups can be automatically assigned to an external server using FTP, SAMBA, SCP, NFS, SFTP, yearly, monthly, weekly and daily. For detailed information, see the Backup / Restore document.

How can I be aware of important events on the AntiKor ?

Important states on the AntiKor are identified to the notification system. The group and users to which these notifications go are also defined. It is also defined by which method it will be delivered. For example, CPU, Ram, Disk usage exceeds the specified value, or ethernets are turned off and on. For detailed information, see the Notification History document.