epati

Firewall Setttings

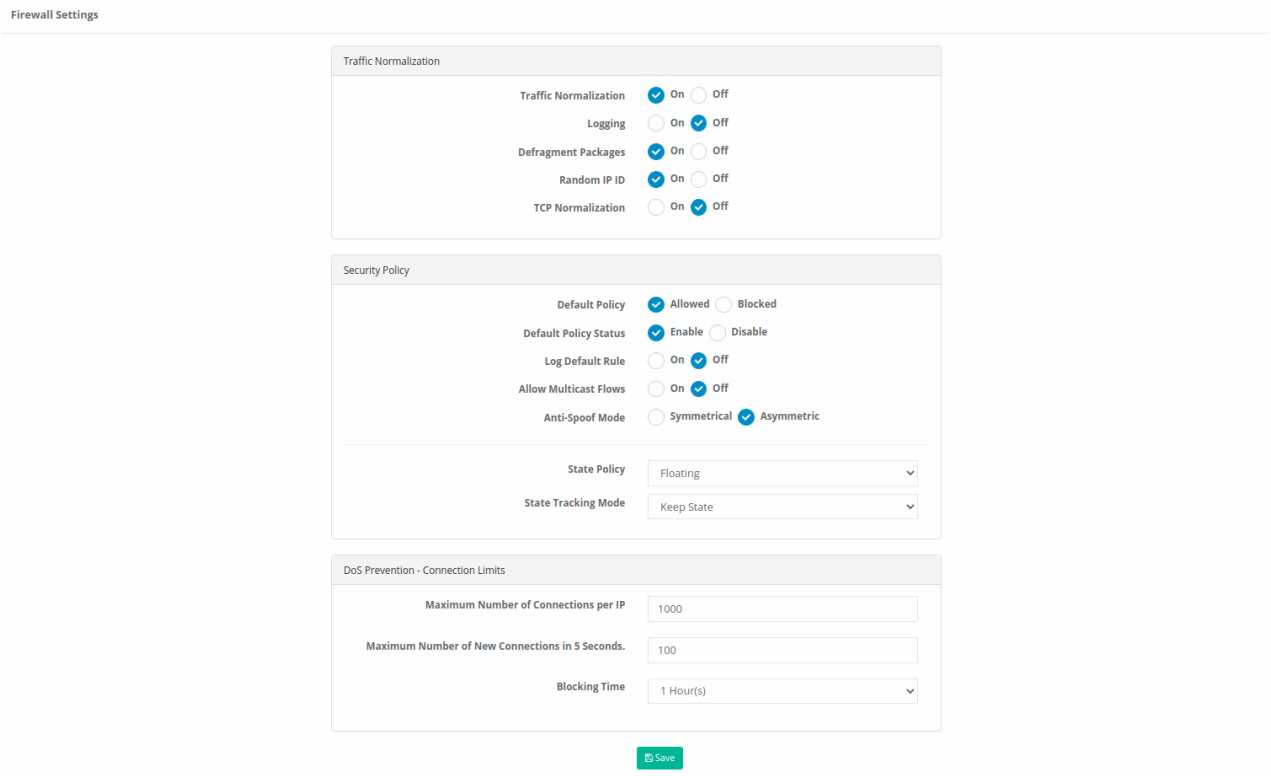
Product: Antikor v2 - Next Generation Firewall

Guides

www.epati.com.tr

Firewall Setttings

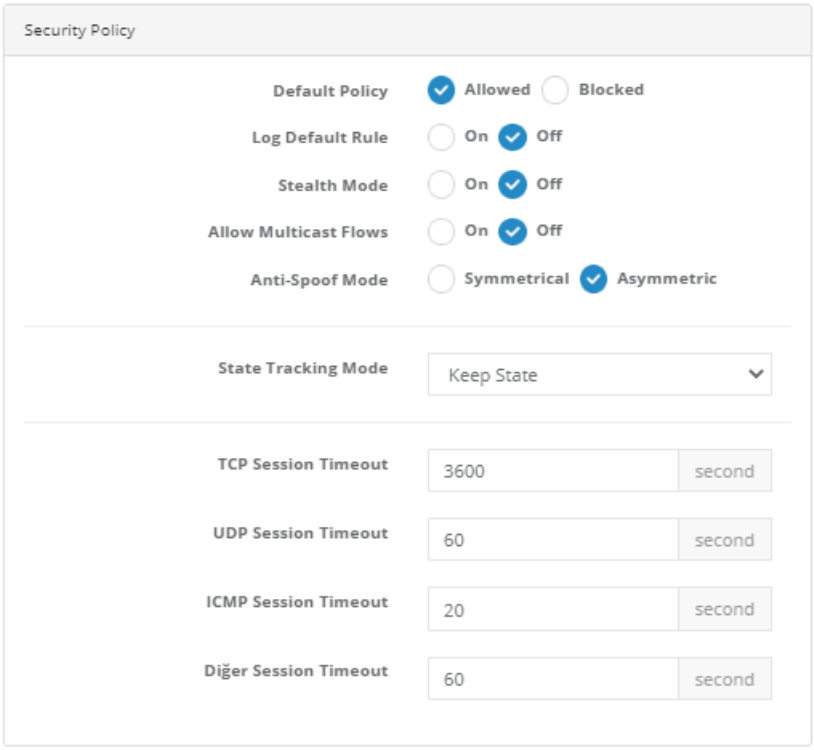
The traffic normalization, Security Policy and DoS blocking - connection limits settings for the firewall are made in this section.



Traffic Normalization

On the Internet, incoming and outgoing packets may not always be ideal as desired. There could be more than one reason. One of these may be due to a misconfigured router setting. Moreover, malicious people often use defragmented packets to exploit the TCP/IP structure. Traffic normalization is used to resolve these abuses.

Security Policy



It is the instruction used to keep status information of packets that comply with the rule. It considers Stateful Inspection. The access information that clients make through the firewall is kept in a table. The answers returned to this partner are checked from the State table in the firewall. If the request exists in the status table, that is, if it is a continuation of an internal request, the packet is allowed to enter. Otherwise, the package is dropped.

Default Rule

FIELD	DESCRIPTION
Default Policy	If disabled, all ports other than the allowed ports (TCP, UDP) will be blocked.
Default Policy Status	For new rules to be added to the security rules, the default active or passive arrival is set.
Log Default Rule	If activated, traffic matching the default rule is logged.
Allow Multicast Flows	The option parameter for Multicast traffic is allowed when the property is turned on. If firewall settings are used as the" default block", a security rule must be written to allow Multicast ip addresses. If the firewall settings are being used as "default permission", turning this feature on for Multicast traffic will suffice.
Anti-Spoof Mode	In symmetric mode, packets follow the routing points they skip when rotating, while in asymmetric mode they use a different route.

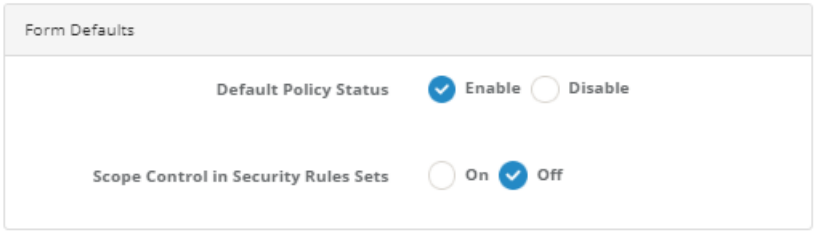
Note: If the default rule is disabled and the web filtering service is turned on, TCP 80 (HTTP port) and 443 (HTTPS port) must be allowed in the security rules. Otherwise, these ports will also be blocked.

Inspection Method for TCP Packets

FIELD	DESCRIPTION
Keep State	It's just a status check. This status check applies to TCP, UDP, and ICMP protocols.
Modulate State	It is used to strengthen the ISN(Initial Sequence Number) section of data that is starting to flow within the TCP protocol. It is usually a measure against the abuse of gaps in the TCP/IP layer. This applies only to the TCP protocol.
Syn Proxy	It is a condition used especially in SYN attacks. (Spoofed TCP SYN Flooding Attacks) a buffer is created by the firewall to protect against attacks by malicious people using the TCP SYN dominant attack from pseudo-networks. As TCP connections pass through this buffer area, all SYN packets are checked to ensure that they comply fully with the 3-step handshake procedure, without being delivered directly to their recipient. Syn packet raids (all SYN packets sent repeatedly) that arrive without complying with this procedure are not delivered to the recipient by the firewall and are dropped. This way, Syn raid attacks are prevented. The Syn Proxy state directive also contains both the Keep State directive and the Modulate State directive.

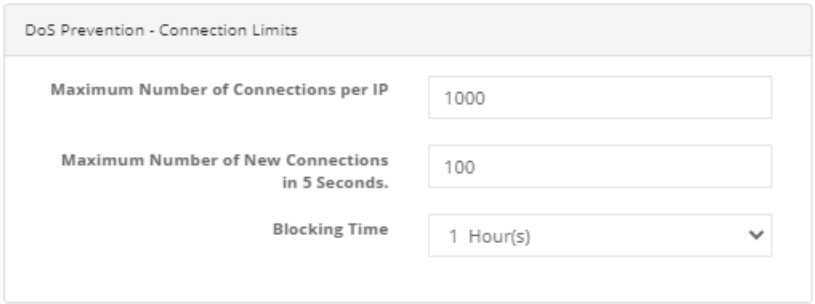
There is a protocol-based default timeout configuration. The default TCP timeout is 3600 ms.

Form Defaults



By default, Active or Passive arrival is set for new rules to be added to security rules.

DoS Prevention - Connection Limits



A Dos (Denial of service) attack is a type of attack against a target that prevents the system from serving and users from accessing the system. The maximum number of connections per person and the maximum number of connections in 5 seconds can be limited so that access to the system is not blocked. If these limits are exceeded, the blocking time of the attacker can be determined by the user.