



DoS / Flood Mitigation

Product: Antikor v2 - Next Generation Firewall
Guides

DoS / Flood Mitigation

The DDoS attack will send multiple requests to the attacked web resource with the aim of exceeding the website's capacity to handle multiple request and prevent the website from functioning correctly. Syn Flood, UDP Flood, ICMP Flood and ICMPv6 Flood attacks can be detected and prevented.

DoS / Flood Mitigation

ReloadAdd

FilterReset Filter

Order No	Status	Source Address	Services	Destination Address	Limit Criteria	Limit	Duration (sec)	Description	Actions
<div>« < > »</div>									

DoS / Flood Mitigation - New Record

General Rules

Order No

0

Status

Active

Log the Traffic

Passive

Description

Scope

The List is Excluded

Source Address

The List is Excluded

Destination Address

Services

ALL x

X | v

+

Connection Count Limits

Limit Criteria

Source Address

v

Limit

Duration (sec)

Cancel

Save

General Rules	DESCRIPTION
Order No	Determines the order of the rules.
Status	Allows the rule to be active or passive.
Process	Flood type to be blocked is selected (ICMP, ICMPv6, SYN, UDP)
Log the Traffic	If log is requested, the option is activated.
Description	Enter description.

Scope	DESCRIPTION
Source Address	Enter IPv4 or IPv6 adress.
Destination Address	Enter IPv4 or IPv6 address.
Services	Select the defined service or services to which the rule will apply.

Connection Count Limits	DESCRIPTION
Limit Criteria	The limit criterion to be blocked is selected. (Source Address, Destination Address, Matched Packet Count)
Limit	Maximum number of floods is written.
Time	Specifies the maximum number of seconds set as the limit. (Second)

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

