

# epati

## Application Security Rules

Product: Antikor v2 - Next Generation Firewall  
Guides

# Application Security Rules

The page for set the rules for application security.

Application Security Rules

Sequence No	ID	Status	Action Type	Protocol	Source	Target	Application Detector	QoS Queue	Transactions
0	abvN_baR77Vr	Active	Block	IP	0.0.0.0/0	0.0.0.0/0	Facebook		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
1	ab_ZLeq1M5o	Active	Block	IP	0.0.0.0/0	0.0.0.0/0	Youtube		<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Click the Add button to enter the new rule.

Application Security Rules - New Record

Sequence No:

Status:  Active

Action Type:

Protocol:

Source:

Target:

Application Detector:

Content Filter:

Description:

Field	Description
Status	The active / passive state of the rule can be specified.
Action Type	The action to be implemented should be indicated if the application matches the specified rules. This is action Allow, Block, Warn and Bandwidths Limits.
Protocol	Protocol should be selected. This field is active if allow, block, or warn is selected.
Source IP	The source IP address to which the rule will be applied must be specified.
Target IP	Enter the target IP address.
Application Detector	Includes application categories. (WhatsApp, Facebook etc.)
Content Filter	Deep packet inspection can be done for the selected categories in the Application Detector. The content that corresponds to the selected category should be written.
Description	Enter description.

**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](http://www.epati.com.tr)  
[info@epati.com.tr](mailto:info@epati.com.tr)  
+90 324 361 02 33  
+90 324 361 02 39

