epati

SSH Inspection

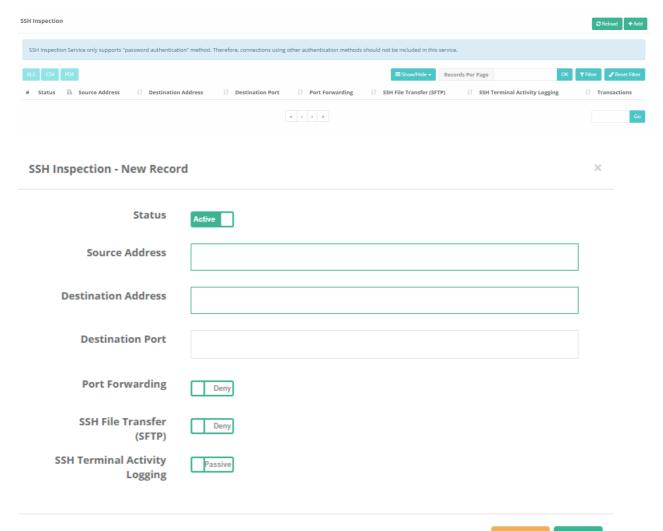Product: Antikor v2 - Next Generation Firewall

Guides

SSH Inspection

This is the section where SSH traffic passing through the Firewall is set to access options with different protocols.

Note: IP addresses are given as examples.

- Only SSH servers connected with password auth can be set. (Public Key should not be.) `

- A Shell connection must always be made for the server/client to be connected regardless of the options selected in the rules.`

- After pressing the Add button, the operations are performed in the pop-up window.

SSH Inspection - New Record

Status	Active
Source Address	
Destination Address	
Destination Port	
Port Forwarding	Deny
SSH File Transfer (SFTP)	Deny
SSH Terminal Activity Logging	Passive

Cancel   Save

FIELD	DESCRIPTION
Status	Active or passive status is selected.
Source Address	Enter the source address to which the rule will be applied.
Destination Address	Enter the destination address to which the rule will be applied.
Destination Port	The destination port(s) to which the rule will be applied are written.
Port Forwarding	**Allow** or **Block** options are selected for Port Forwarding.
SSH File Transfer (SFTP)	**Allow** or **Block** is selected for SSH File Transfer (SFTP).
SSH Terminal Activity Logging	**Active** is selected if SSH Terminal activity is to be logged.