

epati

Application Security / IPS Settings

Product: Antikor v2 - Next Generation Firewall
Guides

Application Security / IPS Settings

General policies for Application Security and IPS Settings can be determined.

Application Security / IPS Settings

Reload Save

General

Networks

Application Detection Service On Off

Rate Filter On Off

Inspection Services

<p>Stream <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>IP Stream <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>ICMP Stream <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>TCP Stream <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>UDP Stream <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <hr/> <p>FTP Server <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>FTP Client <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>FTP Data <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <hr/> <p>ARP Spoofing <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>Back Orifice <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>Distributed Network Protocol v3 <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p>	<p>Normalizer <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>DNS <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>HTTP <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>HTTP 2.0 <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>IMAP <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>Modbus Protocol <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>POP <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>RPC Decode <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>SIP <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>SSH <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>SSL <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>Telnet <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p>	<p>DCE over SMB <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>DCE over TCP <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>DCE over UDP <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>DCE over HTTP Proxy <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>DCE over HTTP Server <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <hr/> <p>Port Scan <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>Profile <input type="text" value="Middle"/></p> <hr/> <p>GPRS Tunneling Protocol (GTP) <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p> <p>SMTP <input type="radio"/> Block <input checked="" type="radio"/> Log <input type="radio"/> Off</p>
---	---	---

General

Field	Description
Networks	Network to which policies apply to should be selected.
Application Detection Service	The active/passive status of policies should be selected for applications.
Rate Limit	Depending on the settings specified on the connection limits page, the active/passive status of the connection number settings must be selected.

Inspection Services

Field	Description
Stream	The active/passive status of the traffic stream can be selected.
IP Stream	The active/passive status of the IP stream can be selected.
ICMP Stream	The active/passive status of the ICMP stream can be selected.
TCP Stream	The active/passive status of the IP stream can be selected.
UDP Stream	The active/passive status of the UDP stream can be selected.
FTP Server	The active/passive status of the FTP server traffic stream can be selected.

Field	Description
FTP Server	The active/passive status of the FTP server traffic stream can be selected.
FTP Client	The active/passive status of the FTP client traffic stream can be selected.
FTP Data	The active/passive status of the FTP data streams can be selected.
ARP Spoofing	The active/passive status can be selected for the analysis of ARP Spoofing attacks.
Back Orifice	The active/passive status can be selected for the analysis of Back Orifice (developed program for remote system management).
Distributed Network Protocol v3	The active/passive status can be selected for the analysis of Distributed Network Protocol v3.
Normalizer	
DNS	The active/passive status of the DNS analysis can be selected.
HTTP	The active/passive status of the HTTP analysis can be selected.
HTTP 2.0	The active/passive status of the HTTP 2.0 analysis can be selected.
IMAP	The active/passive status of the IMAP analysis can be selected.
Modbus Protocol	The active/passive status of the Modbus Protocol can be selected.
POP	The active/passive status of the POP analysis can be selected.
RPC Decode	The active/passive status of the RPC Decode analysis can be selected.
SIP	The active/passive status of the SIP analysis can be selected.
SSH	The active/passive status of the SSH analysis can be selected.
SSL	The active/passive status of the SSL analysis can be selected.
Telnet	The active/passive status of the Telnet analysis can be selected.
DCE over SMB	The active/passive status of the DCE over SMB analysis can be selected.
DCE over TCP	The active/passive status of the DCE over TCP analysis can be selected.
DCE over UDP	The active/passive status of the DCE over UDP analysis can be selected.
DCE over HTTP Proxy	The active/passive status of the DCE over HTTP Proxy analysis can be selected.
Port Scan	The active/passive status can be selected to prevent port scans.
Profile	Port Scan must be enabled for this option to be active. Low, medium and high options are available. Analysis is performed according to the selected level.
GPRS Tunneling Protocol (GTP)	The active/passive status of the GPRS Tunnel analysis can be selected.
SMTP	The active/passive status of the SMTP analysis can be selected.

