

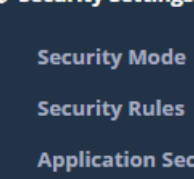
epati

Intrusion Detection and Prevention(IPS)

Product: Antikor v2 - Next Generation Firewall
Configuration Examples

Summary

Configuration



The screenshot shows the 'Security Settings' menu in a dark-themed interface. The menu items are listed vertically: 'Security Mode', 'Security Rules', 'Application Security / IPS Settings', 'Application Security Rules', 'Intrusion Detection and Prevention (IPS)', 'IPS Category Management', and 'Connection Limits'. The 'Intrusion Detection and Prevention (IPS)' item is highlighted with a red rectangular box.

- Security Mode
- Security Rules
- Application Security / IPS Settings
- Application Security Rules
- Intrusion Detection and Prevention (IPS)**
- IPS Category Management
- Connection Limits

Intrusion Detection and Prevention (IPS)										<div> <div>Reload</div> <div>Add</div> </div>
<div> <div>XLS</div> <div>CSV</div> <div>PDF</div> </div> <div> <div>Filter</div> <div>Clear</div> </div>										
#	Status	Category	Network Group	Client Group	Action Type	QoS Queue	Transactions			
1	Active	policy-social	0.0.0.0/0	0/0	Block		<div> <div>Edit</div> <div>Delete</div> <div>Rules</div> <div>↑</div> <div>↓</div> </div>			
2	Active	browser-other	0.0.0.0/0	0/0	Block		<div> <div>Edit</div> <div>Delete</div> <div>Rules</div> <div>↑</div> <div>↓</div> </div>			
3	Active	os-linux	0.0.0.0/0	0/0	Warn		<div> <div>Edit</div> <div>Delete</div> <div>Rules</div> <div>↑</div> <div>↓</div> </div>			

Status

Active ☒

Category

Select...

Source Field

☒ Network Group ☐ Client Group

Network Group

Action Type

Allow ▾

Description

Cancel

Save

Field	Description
Status	Active and passive status can be specified.
Category	Signature is the field where databases are selected.
Source Field	Network Group and Client Group can be specified.
Action Type	Action type can be specified.
Description	Enter description.

Signatures in the Application Database are described below.

Field	Description
botcc (Bot Comma nd and Contr ol)	These are autogenerated from several sources of known and confirmed active Botnet and other Command and Control hosts. Updated daily, primary data source is Shadowserver.org. Bot command and control block rules generated from shadowserver.org, as well as spyeyetracker, palevotracker and zeustracker. Port grouped rules offer higher fidelity with destination port modified in rule.
botcc .port group ed	Same as above, but grouped by destination port.
ciarm y	Collective Intelligence generated IP rules for blocking based upon
compr omise d	This is a list of known compromised hosts, confirmed and updated daily as well. This set varied from a hundred to several hunderd rules depending on the data sources. This is a compilation of several private but highly reliable data sources. Warming: Snort does not handle IP matches well load-wise. If your sensor is already pushed to the limits this set will add significant load. We recommend staying with just thebotccrules in a high load case.
drop	Rules to block spamhaus “drop” listed networks. IP based. This is a daily updated list of the Spamhaus DROP (Don’t Route or Peer) list. Primarily known professional spammers.

Field	Description
dshield	IP based rules for Dshield Identified attackers. Daily updated list of the DShield top attackers list.
id	Also very reliable.
activex	Attacks and vulnerabilities(CVE, etc.) regarding ActiveX.
attack_response	Responses indicative of intrusion—LMHost file download, certain banners, Metasploit Meterpreter kill command detected, etc. These are designed to catch the results of a successful attack. Things like “id=root”, or error messages that indicate a compromise may have happened.
chat	identification of traffic related to numerous chat clients, irc and possible check-in activity.
current_events	Category for active and short lived campaigns. This category covers exploit kits and malware that will be aged and removed quickly due to the short lived nature of the threat. High profile items that we don't expect to be there long—fraud campaigns related to disasters for instance. These are rules that we don't intend to keep in the ruleset for long, or that need to be tested before they are considered for inclusion. Most often these will be simple sigs for the Storm binary URL of the day, sigs to catch CLSID's of newly found vulnerable apps where we don't have any detail on the exploit, etc.
deleted	Rules removed from the rule set.
dns	Rules for attacks and vulnerabilities regarding DNS. Also category for abuse of the service for things such as tunneling.
dos	Denial of Service attempt detection. Intended to catch inbound DOS activity and outbound indications.
exploit	Exploits that are not covered in specific service category. Rules to detect direct exploits. Generally if you're looking for a windows exploit, Veritas, etc, they'll be here. Things like SQL injection and the like, while they are exploits, have their own category.
ftp	Rules for attacks, exploits and vulnerabilities regarding FTP. Also includes basic none malicious FTP activity for logging purposes, such as login, etc.
games	Rules for the Identification of gaming traffic and attacks against those games. World of Warcraft, Starcraft and other popular online games have sigs here. We don't intend to label these things evil, just that they're not appropriate for all environments.
icmp	Rules for attacks and vulnerabilities regarding ICMP. Also included are rules detecting basic activity of the protocol for logging purposes.
icmp_info	Rules to log ICMP protocol specific events, typically normal operation.
imap	Rules for the identification, as well as attacks and vulnerabilities regarding the IMAP protocol. Also included are rules detecting basic activity of the protocol for logging purposes.
inappropriate	Rules for the identification of pornography related activity. Includes Porn, Kiddy porn, sites you shouldn't visit at work, etc. Warning: These are generally quite Regex heavy and thus high load and frequent false positives. Only run these if you're really interested.
info	It contains rules regarding RFC standards.
malware	Malware and Spyware related, no clear criminal intent. The threshold for inclusion in this set is typically some form of tracking that stops short of obvious criminal activity. This set was originally intended to be just spyware. That's enough to several rule categories really. The line between spyware and outright malicious bad stuff has blurred to much since we originally started this set. There is more than just spyware in here, but rest assured nothing in here is something you want running on your net or PC. There are URL hooks for known update schemes, User-Agent strings

Field	Description
misc	Miscellaneous rules for those rules not covered in other categories.
mobile_malware	Specific to mobile platforms: Malware and Spyware related, no clear criminal intent.
netbios	Rules for the identification, as well as attacks, exploits and vulnerabilities regarding Netbios. Also included are rules detecting basic activity of the protocol for logging purposes.
p2p	Rules for the identification of Peer-to-Peer traffic and attacks against. Including torrents, edonkey, Bittorrent, Gnutella, Limewire, etc. We're not labeling these things malicious, just not appropriate for all networks and environments.
policy	Application Identification category. Includes signatures for applications like DropBox and Google Apps, etc. Also covers off port protocols, basic DLP such as credit card numbers and social security numbers. Included in this set are rules for things that are often disallowed by company or organizational policy. Myspace, Ebay, etc.
pop3	Rules for the identification, as well as attacks and vulnerabilities regarding the POP3 protocol. Also included are rules detecting basic activity of the protocol for logging purposes.
rpc	RPC related attacks, vulnerabilities and protocol detection. Also included are rules detecting basic activity of the protocol for logging purposes.
scada	Signatures for SCADA attacks, exploits and vulnerabilities, as well as protocol detection.
scan	Things to detect reconnaissance and probing. Nessus, Nikto, portscanning, etc. Early warning stuff.
shellcode	Remote Shellcode detection. Remoteshellcode is used when an attacker wants to target a vulnerable process running on another machine on a local network or intranet. If successfully executed, the shellcode can provide the attacker access to the target machine across the network. Remote shellcodes normally use standard TCP/IP socket connections to allow the attacker access to the shell on the target machine. Such shellcode can be categorised based on how this connection is set up: if the shellcode can establish this connection, it is called a "reverse shell" or a connect-backshellcode because the shellcode connects back to the attacker's machine.
smtp	Rules for attacks, exploits and vulnerabilities regarding SMTP. Also included are rules detecting basic activity of the protocol for logging purposes.
snmp	Rules for attacks, exploits and vulnerabilities regarding SNMP. Also included are rules detecting basic activity of the protocol for logging purposes.
sql	Rules for attacks, exploits and vulnerabilities regarding SQL. Also included are rules detecting basic activity of the protocol for logging purposes.
telnet	Rules for attacks and vulnerabilities regarding the TELNET service. Also included are rules detecting basic activity of the protocol for logging purposes.
tftp	Rules for attacks and vulnerabilities regarding the TFTP service. Also included are rules detecting basic activity of the protocol for logging purposes.
trojan	Malicious software that has clear criminal intent. Rules here detect malicious software that is in transit, active, infecting, attacking, updating and whatever else we can detect on the wire. This is also a highly important ruleset to run if you have to choose..
user_agents	User agent identification and detection.
voip	Rules for attacks and vulnerabilities regarding the VOIP environment. SIP, h.323, RTP, etc.

Field	Description
web_client	Web client side attacks and vulnerabilities.
web_server	Rules for attacks and vulnerabilities against web servers.
web_specific_apps	Rules for very specific web applications.
worm	Traffic indicative of network based worm activity.
rbn & rbn-malvertising (Russian Business Network)	IP based rules for the identification of the Russian Business Network. [THIS RULESET HAS BEEN OBSOLETE AND REMOVED. IT IS NO LONGER USED. IT IS INCLUDED AS A RULE FILE TO INFORM USERS OF ITS REMOVAL]
tor	IP Based rules for the identification of traffic to and from TOR exit nodes.

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

