

CONTENT-ID



EDU-210 Version A
PAN-OS® 9.0

REAL-TIME PREVENTION

- Content-ID overview
- Vulnerability Protection Security Profiles
- Antivirus Security Profiles
- Anti-Spyware Security Profiles
- File Blocking Profiles
- Data Filtering Profiles
- Attaching Security Profiles to Security policy rules
- Telemetry and threat intelligence
- Denial-of-service protection



Agenda

After you complete this module,
you should be able to:

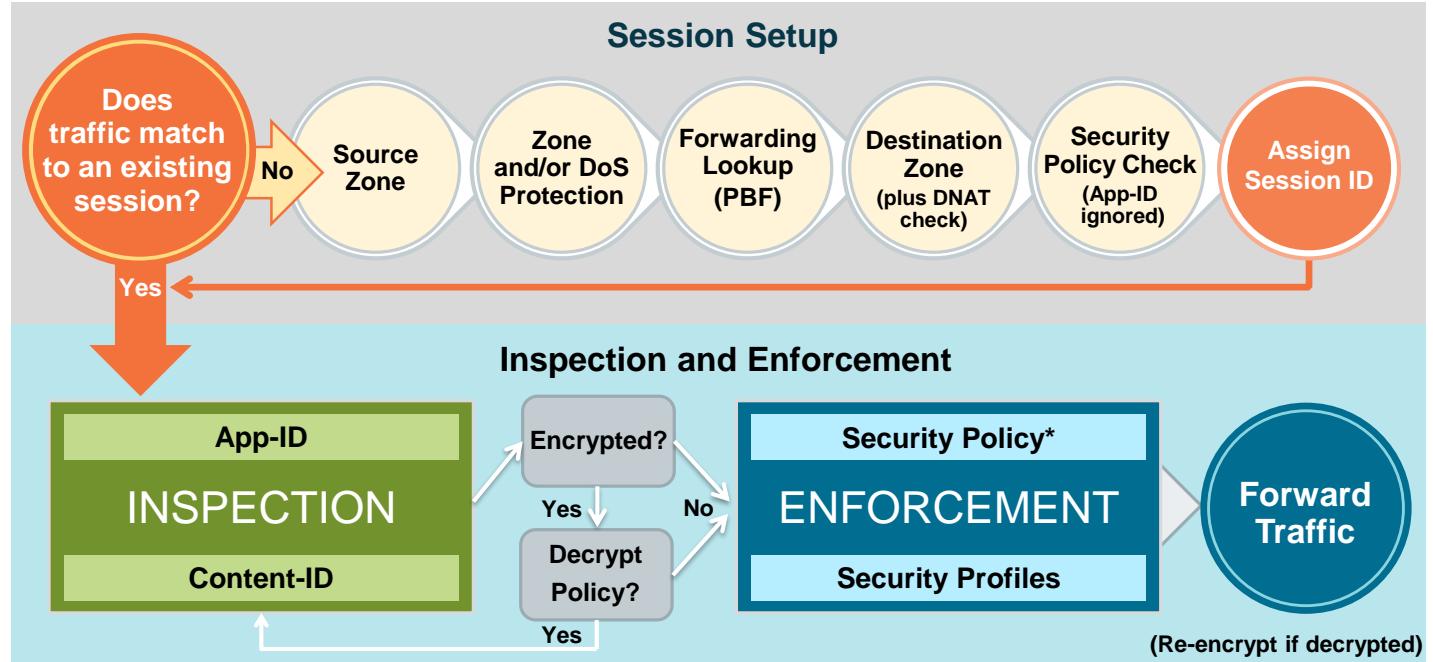


- Describe the seven different Security Profiles types
- Define the two predefined Vulnerability Protection Profiles
- Configure Security Profiles to prevent virus and spyware infiltration
- Configure File Blocking Profiles to identify and control the flow of file types through the firewall
- Configure a DoS Profile to help mitigate Layer 3 and 4 protocol-based attacks

After you complete this module, you should be able to:

- Describe the seven different Security Profiles types
- Define the two predefined Vulnerability Protection Profiles
- Configure Security Profiles to prevent virus and spyware infiltration
- Configure File Blocking Profiles to identify and control the flow of file types through the firewall
- Configure a DoS Profile to help mitigate Layer 3 and 4 protocol-based attacks

Flow Logic of the Next-Generation Firewall



* Policy check relies on pre-NAT IP addresses

3 | © 2019 Palo Alto Networks, Inc.



The Palo Alto Networks firewall enables granular control over network traffic to provide the most robust network security model possible.

The firewall allows or denies traffic based only on source, destination, application, user, and port information. It also can examine allowed traffic for specific threats, including viruses, spyware, and software designed to exploit application vulnerabilities. Traffic also can be scanned for prohibited action, such as the distribution of sensitive data.

For more information about the packet handling sequence inside of a PAN-OS® device, see the *Packet Flow Sequence in PAN-OS* document available on the Palo Alto Networks Support website at <https://live.paloaltonetworks.com/docs/DOC-1628>.



Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection

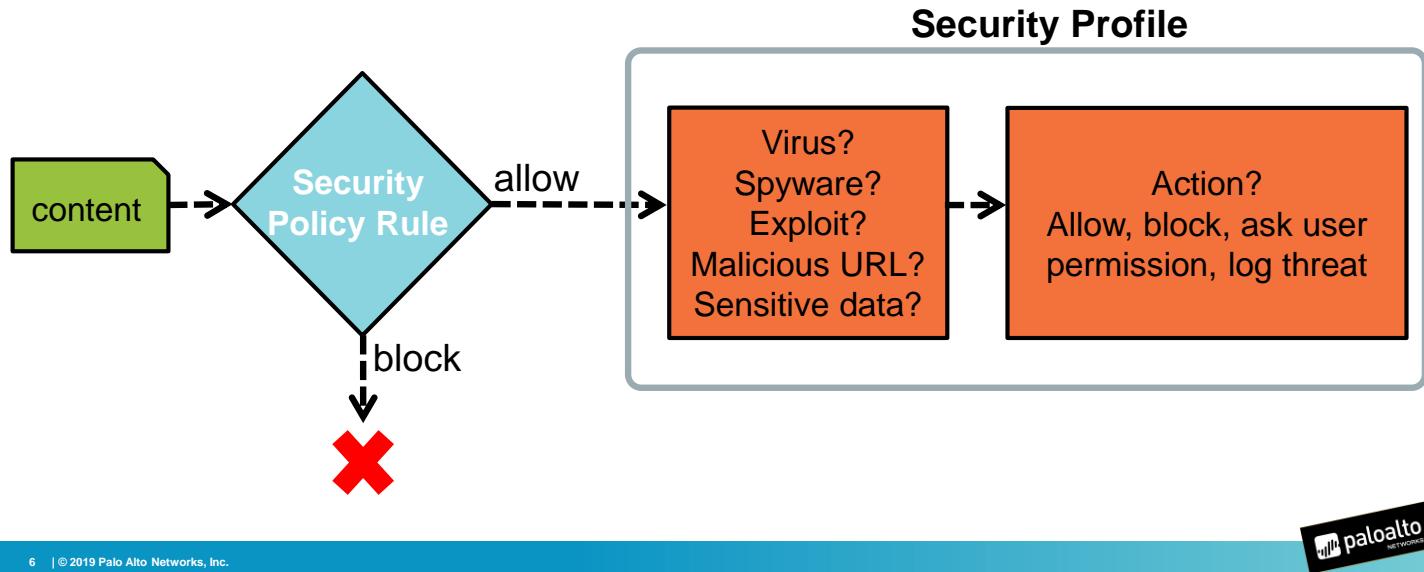
Content-ID

- Threat prevention engine and policies to inspect and control content traversing the firewall
- Scans network traffic for:
 - Software vulnerability exploits
 - Viruses
 - Spyware
 - Malicious URLs
 - Restricted files and data

Content-ID technology combines a real-time threat prevention engine with administrator-defined policies to inspect and control content traversing the firewall. Content-ID delivers a method of detection based on the complete analysis of all allowed traffic. Content-ID uses multiple threat prevention and data-loss prevention techniques in a single, unified engine. Palo Alto Networks controls the threat vectors themselves through the granular management of all types of applications, unlike the practice in traditional solutions. Applications are identified immediately by the firewall, thereby reducing the attack surface of the network, after which all allowed traffic is analyzed for exploits, viruses, spyware, malicious URLs, and dangerous or restricted files or content.

Security Policy with Security Profiles

- Security Profiles implement additional security checks on allowed traffic.



6 | © 2019 Palo Alto Networks, Inc.



Security Profiles are objects that are added to Security policy rules that are configured with an action of “allow.” Security Profiles are not necessary for Security policy rules configured with the “deny” action because no further processing is needed if the network traffic will be blocked. As with Security policy rules, Security Profiles are applied to all packets over the life of a session.

The Security Profiles represent additional security checks to be performed on allowed network traffic. Security Profiles enable you to have more granular control over allowed traffic. For example, web browsing may be allowed by a Security policy rule, but there still is the concern that users could download a virus from a website. An Antivirus Security Profile can be attached to the Security policy rule to detect, block, and log a virus. Security Profiles log detected threats to the logs found at **Monitor > Logs**.

Security Profile Types

Policies > Security

	Name	Tags	Type	Source			Destination			Service	Action	Profile
				Zone	Address	User	HIP Profile	Zone	Address			
1	internal-inside-dmz	internal	universal	inside	any	any	any	dmz	any	any	application-default	Allow
2	egress-outside	egress	universal	inside	any	any	any	outside	any	any	application-default	Allow
3	danger-simulated-tr...	danger	universal	dang	any	any	any	dang	any	any	application-default	Allow



Antivirus



File Blocking



Anti-Spyware



Data Filtering



Vulnerability Protection



WildFire Analysis



URL Filtering



Security Profile Group

7 | © 2019 Palo Alto Networks, Inc.



Types of Security Profiles are:

- Antivirus: Detects infected files being transferred with the application
- Anti-Spyware: Detects spyware downloads and traffic from already installed spyware
- Vulnerability Protection: Detects attempts to exploit known software vulnerabilities
- URL Filtering: Classifies and controls web browsing based on content
- File Blocking: Tracks and blocks file uploads and downloads based on file type and application
- Data Filtering: Identifies and blocks transfer of specific data patterns found in network traffic
- WildFire Analysis: Forwards unknown files to the WildFire® service for malware analysis

A Security Profile Group is a set of Security Profiles that are treated as a unit to simplify the task of adding multiple Security Profiles to a Security policy rule. For example, an administrator creating a Security policy rule can select a Security Profile Group containing all the recommended Security Profiles and attach them in a single step to a Security policy rule.

Threat Log

- Vulnerability Protection, Antivirus, and Anti-spyware Profiles log events to the Threat log.

Monitor > Logs > Threat

Click a column header to change number of displayed columns.

ID	Receive Time	Type	Name	From Zone	To Zone	Source address	Destination address	To Port	Application	Action	Severity	File Name	URL
1	02/20 01:05:23	spyware	Suspicious HTTP Evasion Found	danger	danger	10.12.1.101	10.12.1.101	80	informational	block	informational	tischlerei-kreine...	
2	02/20 01:05:15	spyware	Suspicious HTTP Evasion Found	danger	danger	10.12.1.101	10.12.1.101	80	informational	block	informational	eastrutzmann....	
3	02/20 01:05:10	virus	TrojanSpy/Win32....	danger	danger	10.12.1.101	194.58.100.59	80	informational	block	informational	fix832922.ms	
4	02/20 01:05:08	spyware	Suspicious HTTP Evasion Found	danger	danger	10.5.3.101	74.208.248.199	80	informational	block	informational	abdellatifosman...	
5	02/20 01:05:06	spyware	Suspicious HTTP Evasion Found	danger	danger	10.5.3.101	85.13.133.73	80	informational	block	informational	brandsoutlet.ir/...	
6	02/20 01:05:05	spyware	Suspicious HTTP Evasion Found	danger	danger	10.5.3.101	72.52.179.2	80	web-browsing	reset-server	medium	89yg7g87byi	
7	02/20 01:05:04	spyware	Suspicious HTTP Evasion Found	danger	danger	10.5.3.101	185.23.21.18	80	web-browsing	alert	informational	elivo.pl/Y2hNDK...	
8	02/20 01:05:03	spyware	Suspicious HTTP Evasion Found	danger	danger	10.5.3.101	210.1.60.27	80	web-browsing	reset-server	medium	89yg7g87byi	
9	02/20 01:05:02	spyware	Suspicious HTTP Evasion Found	danger	danger	192.168.0.2	112.137.162.1...	80	web-browsing	drop	critical	controller.p...	

8 | © 2019 Palo Alto Networks, Inc.



Includes packet capture

Open Threat Details window.

The firewall Threat log records antivirus, anti-spyware, and vulnerability threats discovered by the Security Profiles. Dozens of columns of information can be displayed. Examples of available columns are shown here. Click any column header to display the column header list. From the list you can select additional columns to be displayed or you can deselect columns to be removed from the window pane.

The ID column displays threat ID numbers that are particularly useful for creating threat exceptions in the Antivirus, Anti-Spyware, and Vulnerability Protection Profile rules.

The firewall uses Threat log information as the source of information for the web interface reports and the information displayed on the ACC tab. “ACC” represents the Application Control Center.

Threat log entries at administrator-defined event severity levels can be forwarded by the firewall to remote locations. This functionality is named log forwarding. Log forwarding is useful for backup and log aggregation. Although log forwarding configuration is not described in this module, log entries can be forwarded to a Panorama device, a syslog server, a web server, or an email server, or can be sent as SNMP traps.



Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection

Default Vulnerability Protection Security Profiles

Objects > Security Profiles > Vulnerability Protection

Name	Location	Count	Rule Name	Threat Name	Host Type	Severity	Action	Packet Capture
strict	Predefined	Rules: 10	simple-client-critical simple-client-high simple-client-medium simple-client-informational simple-client-low simple-server-critical simple-server-high more...	any any any any any any any	client client client client client server server	critical high medium informational low critical high	reset-both reset-both reset-both default default reset-both reset-both	disable disable disable disable disable disable disable
default	Predefined	Rules: 6	simple-client-critical	any	client	critical	default	disable

To create customized profile actions:

- Clone the default read-only profile and edit the clone, or
- Add a brand new profile

Rules specify actions on detected events.

10 | © 2019 Palo Alto Networks, Inc.



Palo Alto Networks firewalls include two predefined, read-only Vulnerability Protection Security Profiles. These profiles contain rules that configure the actions taken by a firewall when it detects malware known to exploit system vulnerabilities of different severity levels and types. Exploits include buffer overflows and illegal code executions.

Every Palo Alto Networks-defined vulnerability protection signature includes a default action. To display the default actions, browse to **Objects > Security Profiles > Vulnerability Protection > Add > Exceptions**, and then select the **Show all Signatures** check box. Updated vulnerability protection signatures are made available every week by Palo Alto Networks as part of the content updates.

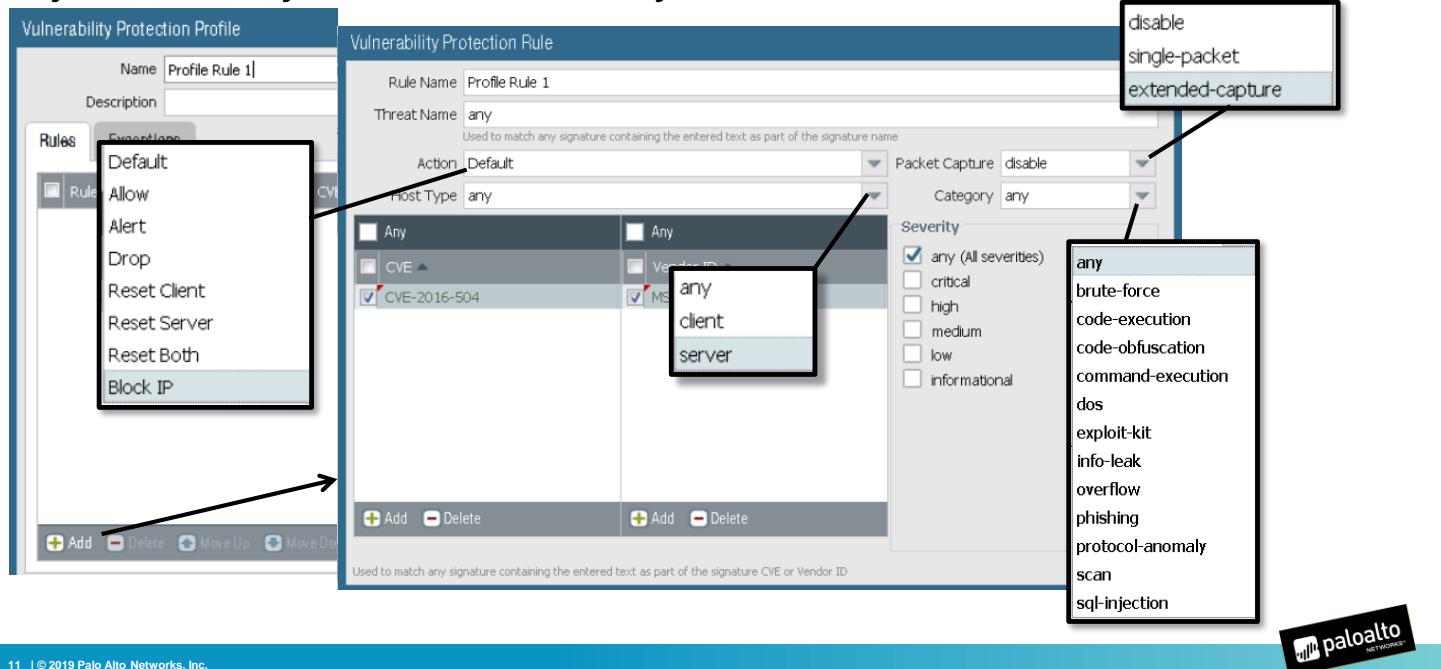
You can attach a Vulnerability Protection Profile to a Security policy rule. The firewall has two predefined Vulnerability Protection Profiles:

- default: This profile applies the “default” action to all client and server critical, high-severity, and medium-severity events. The *default* profile typically is used for proof-of-concept or first-phase deployments.
- strict: This profile applies the “reset-both” response to all client and server critical, high-severity, and medium-severity spyware events and uses the “default” action for all client and server informational and low events. The *strict* profile is used for out-of-the-box protection with a recommended block of critical, high-severity, and medium-severity threats.

The predefined profiles are read-only and cannot be modified or deleted. You can use these profiles without modification or clone them and edit the clone. You also can add new Vulnerability Protection Profiles. Use customized Vulnerability Protection Profiles to minimize inspection between more trusted zones or to maximize inspection between less trusted zones. In a Zero Trust configuration, no zone is completely trusted.

Vulnerability Protection Profile Rules

Objects > Security Profiles > Vulnerability Protection > Add



11 | © 2019 Palo Alto Networks, Inc.



Each Vulnerability Protection Profile can contain multiple rules to process different types of threats in different ways. Each rule can be configured to take a packet capture. A rule can inspect network traffic for all threat signatures or can be configured with one or more filters that scan only for specific threat signatures.

- For the **Threat Name**, use the keyword *any* to enable the rule to monitor any threat name. Alternatively, enter a string for the **Threat Name** and a rule will scan only for signatures whose names include the string.
- A rule can scan for signatures coming from any host in a connection, or just for the server or client host.
- A rule can scan for all signature types or just for those signatures that match a specific category of threat.
- A rule can scan for threats that match all, or for one or more specific severity levels.
- A rule also can scan only for threats that have been assigned a specific CVE or Vendor ID number.

Each rule also can specify an action to take with a threat is detected. Actions are:

- Allow: Permits the traffic without logging
- Alert: Generates a log entry and allows the traffic
- Drop: Discards the traffic and generates a log entry
- Reset Client: For TCP, resets the client-side connection. For UDP, drops the connection.
- Reset Server: For TCP, resets the server-side connection. For UDP, drops the connection.
- Reset Both: For TCP, resets the connection on both the client and server. For UDP, drops the connection.
- Block IP: Blocks traffic from either a source, or a source and destination, and for a configurable number of seconds.

Vulnerability Exceptions

Objects > Security Profiles > Vulnerability Protection > Add

The screenshot shows the 'Vulnerability Protection Profile' configuration screen. The 'Exceptions' tab is selected. A callout box with the text 'Override the action configured in the rules.' points to a link in the top right corner of the table header. Another callout box with the text 'Click to modify packet capture setting.' points to the 'Packet Capture' column. A third callout box with the text 'Click to view or add IP addresses.' points to the 'IP Address Exemptions' column. The table lists various threat signatures with columns for Enable, ID, Threat Name, IP Address Exemptions, Rule, CVE, Host, Category, Severity, Action, and Packet Capture.

Enable	ID	Threat Name	IP Address Exemptions	Rule	CVE	Host	Category	Severity	Action	Packet Capture
<input type="checkbox"/>	35931	HP Data Protector Omnilnet Opcode Buffer Overflow Vulnerability	3		CVE-2011-1865	server	overflow	high	default (alert)	disable
<input type="checkbox"/>	39371	HP Data Protector Client EXEC_CMD Command Execution Vulnerability			CVE-2011-0923	server	code-execution	high	default (alert)	disable
<input type="checkbox"/>	36958	HP Data Protector Opcode 11 and 28 Command Execution Vulnerability						high	default (alert)	disable
<input type="checkbox"/>	36771	HP Data Protector CRS Service Buffer Overflow Vulnerability						high	default (alert)	disable
<input type="checkbox"/>	34440	HP OpenView Storage Data Protector EXEC_CMD Buffer			CVE-2011-1866,CVE-2011-1865	server	overflow	high	default (alert)	disable

Show all signatures [PDF/CSV](#)

12 | © 2019 Palo Alto Networks, Inc. 

A profile's rules specify the actions to take when threats are found. The **Exceptions** tab enables you to override the rules' action responses for one or more threat signatures. Exceptions often are used as a way to handle false positives. For example, a profile rule could be configured to block all packets that match threat signatures with a critical severity level. However, you could create an "alert" action exception that overrides a "block" action for one or more specific threat signatures.

You can create even more granular exceptions by adding a list of one or more unicast IP addresses to the **IP Address Exemptions** column. Only a threat whose source or destination IP address matches an address on the list will have its action response changed by the exception. The **IP Address Exemptions** column does not display the IP addresses, but only the number of IP address exemptions. Click the number in the **IP Address Exemptions** column to display the list of IP addresses.

Use the **Exceptions** tab to override the profile rules' packet capture configurations. You can assign each threat signature a specific packet capture configuration.



Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection

Default Antivirus Security Profile

Objects > Security Profiles > Antivirus

Name	Location	Packet Capture	Decoders			Application Exceptions		Threat Exceptions
			Name	Action	WildFire Action	Name	Action	
default	Predefined		http	default (reset-both)	allow			0
			http2	default (reset-both)	allow			
			smtp	default (alert)	allow			
			imap	default (alert)	allow			
			pop3	default (alert)	allow			
			ftp	default (reset-both)	allow			
			smb	default (reset-both)	allow			

Add Delete Clone PDF/CSV

Out-of-the-box profile

- To create customized profile actions:
 - Clone the default read-only profile and edit the clone, or
 - Add a brand new profile

Action to take based on antivirus signatures delivered in content updates

WildFire Action to take based on signatures delivered by WildFire

14 | © 2019 Palo Alto Networks, Inc.



The Palo Alto Networks firewall includes a predefined, read-only default Antivirus Security Profile. The profile configures the actions taken by the firewall when a virus is detected. The default profile cannot be deleted or modified. To create a customized Antivirus Profile, clone the default profile and edit the clone. Or you can add a brand new, and empty, Antivirus Profile. Use customized Antivirus Profiles to minimize inspection between more trusted zones or to maximize inspection between less trusted zones. In a Zero Trust configuration, no zone is completely trusted.

The six listed protocols in the default profile can be used by applications to transfer files. These protocols can transfer files, so they also can transfer viruses. Consider a scenario where a security rule allows an application that uses SMTP to transfer email with file attachments. If the default Antivirus Profile were attached to the Security policy rule, the profile would enable virus detection on the application traffic.

A profile's actions specify how a firewall responds to a threat event. Updated virus signatures are made available every 24 hours by Palo Alto Networks. The **Action** field specifies the action taken when a virus is detected by antivirus signatures included in daily antivirus content updates. The **WildFire Action** field specifies the action taken when a virus is detected by antivirus signatures included in WildFire updates. You can modify **either** Action field in a custom Antivirus Profile.

An “alert” action allows the network traffic but creates an entry in the Threat log. The “reset-both” action resets the TCP server and client or drops UDP packets.

Creating a New Antivirus Profile

Objects > Security Profiles > Antivirus > Add

Available actions

default (alert)
allow
alert
drop
reset-client
reset-server
reset-both

Name: AV Profile

Description:

Antivirus Virus Exception

Packet Capture

Decoders

Decoder	Action	WildFire Action
ftp	default (reset-both)	default (reset-both)
http	default (reset-both)	default (reset-both)
imap	default (alert)	default (alert)
pop3	default (alert)	default (alert)
smb	default (reset-both)	default (reset-both)
smtp	default (alert)	default (alert)

Application Exception

Application	Action
0 items	

Add Delete

15 | © 2019 Palo Alto Networks, Inc.



In Antivirus Profiles other than the default profile, you can modify the **Action** and **WildFire Action** columns to something other than the default action defined by Palo Alto Networks. The default action is denoted in parentheses after the word “default.” For example, the default action for the FTP, HTTP, and SMB protocols is “reset-both,” which resets both the TCP server and client.

Available actions for traffic that matches an Antivirus Profile rule are as follows:

- allow: Permits the traffic without logging
- alert: Generates a log entry and allows the traffic
- drop: Discards the traffic and generates a log entry
- reset-client: For TCP, resets the client-side connection. For UDP, drops the connection.
- reset-server: For TCP, resets the server-side connection. For UDP, drops the connection.
- reset-both: For TCP, resets the connection on both the client and server. For UDP, drops the connection.

The default action for the IMAP, POP3, and SMTP protocols is “alert,” which does not block the traffic. However, the firewall will create entries in the Threat log. The IMAP and POP3 protocols are store-and-forward protocols, which means that if an intermediate device drops the packets, IMAP or POP3 will attempt to resend the data until it is delivered. For applications using these protocols, the infected file must be removed at the mail server. If you set these protocols to the “block” action, you will not get any email transferred until the virus has been removed from the server.

For the SMTP protocol, an SMTP 541 error message is sent by the firewall as part of the “alert” action when a virus is detected. This message tells the mail server not to retry sending the message. The virus still must be removed from the mail server. The 541 error message also is sent if the “reset-both” or “reset-server” action is selected in the profile.

Application exceptions typically are configured when false positives occur. Configuration of specific

application exemptions enables the firewall to pass the formerly blocked traffic. To create an application exception, search the Threat log for the application that is being blocked. Add the application to the list of **Application Exceptions** on the **Antivirus** tab.

If the **Packet Capture** check box is selected, any alert also is accompanied by a packet capture of the portion of the network traffic that triggered the antivirus signature. This capture can be used to verify the presence of the virus or to determine that it is a false positive.

Creating a New Antivirus Profile (Cont.)

Objects > Security Profiles > Antivirus > Add

The screenshot shows the 'Antivirus Profile' configuration screen. At the top, there are fields for 'Name' (set to 'AV Profile') and 'Description'. Below these are two tabs: 'Antivirus' (selected) and 'Virus Exception'. The main area displays a table with one item: Threat ID 281328 and Threat Name DOS/Virus.eicar_test_file.. At the bottom, there is a search bar labeled 'Threat ID', an 'Add' button, and a 'PDF/CSV' export button.

Type a threat ID and click **Add**.

- To reduce the number of false positives, use Threat ID to create an exemption.
- Threat IDs recorded in Threat log

Virus exceptions typically are created to handle false positives. To create a virus exception, first search the Threat log for the **Threat ID** that you want to exempt. Add the **Threat ID** to the **Virus Exception** tab. In this example, the profile will not alert or block when an Eicar test virus file is detected.



Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection

Default Anti-Spyware Security Profiles

Objects > Security Profiles > Anti-Spyware

Name	Location	Count	Rule Name	Threat Name	Severity	Action	Packet Capture	DNS Packet Capture
default	Predefined	Rules: 4	simple-critical	any	critical	default	disable	disable
strict	Predefined	Rules: 5	simple-high	any	high	default	disable	disable

Out-of-the-box profiles

Rules specify actions on detected spyware.

- To create customized profile actions:
 - Clone the default read-only profile and edit the clone, or
 - Add a brand new profile

18 | © 2019 Palo Alto Networks, Inc.



The Palo Alto Networks firewall includes two predefined, read-only Anti-Spyware Security Profiles. These profiles contain rules that configure the actions taken by the firewall when it detects spyware of different severity levels and types.

Every anti-spyware signature that is defined by Palo Alto Networks includes a default action. To display the default actions, browse to **Objects > Security Profiles > Anti-Spyware > Add > Exceptions**, and then select the **Show all Signatures** check box. Updated anti-spyware signatures are made available every 24 hours by Palo Alto Networks. Spyware often is detected when an infected host on your network attempts to make a *phone home* network connection to a C2 server.

You can attach an Anti-Spyware Profile to a Security policy rule. The firewall has two predefined Anti-Spyware Profiles:

- default: This profile applies the “default” action to all client and server critical, high-severity, medium-severity, and low-severity spyware events. The default profile typically is used for proof-of-concept or first-phase deployments.
- strict: This profile applies the “reset-both” response to all critical, high-severity, and medium-severity spyware events and uses the “default” action for all informational and low-severity spyware events. The *strict* profile is used for out-of-the-box protection with a recommended block of critical, high-severity, and medium-severity threats.

The predefined profiles are read-only and cannot be modified or deleted. You can use these profiles without modification or clone them and edit the clone. You also can create new Anti-Spyware Profiles. Use customized Anti-Spyware Profiles to minimize inspection between more trusted zones or to maximize inspection between less trusted zones. In a Zero Trust configuration, no zone is completely trusted.

Configuring Anti-Spyware Profile Rules

Objects > Security Profiles > Anti-Spyware > Add > Rules

The screenshot shows the 'Anti-Spyware Rule' configuration screen. The 'Rule Name' is 'New Rule', 'Threat Name' is 'any', 'Category' is 'backdoor', 'Action' is 'Default', and 'Packet Capture' is 'disable'. In the 'Severity' section, 'critical', 'high', 'medium', and 'extended-capture' are selected. A dropdown menu for 'Action' lists: Default, Allow, Alert, Drop, Reset Client, Reset Server, Reset Both, and Block IP. To the right, a list of threat names includes: adware, any, autogen, backdoor, botnet, browser-hijack, data-theft, dns, dns-wildfire, keylogger, net-worm, p2p-communication, phishing-kit, post-exploitation, spyware, and webshell.

19 | © 2019 Palo Alto Networks, Inc.



Each Anti-Spyware Profile can contain multiple rules to process different types of spyware threats in different ways. Each rule is configured with a unique name. A rule can inspect network traffic for all spyware threats or a rule can be configured with one or several filters so that it scans only for specific spyware threats.

Use the keyword “any” for the **Threat Name** to enable the rule to monitor any threat name. Alternatively, enter a string for the **Threat Name** and a rule will scan only for signatures whose names include the string. You also can configure each rule to monitor specific categories of spyware threats.

Use the keyword “any” for the **Category** to monitor all categories of viruses. You also can select a specific category of viruses to monitor.

You can specify an action to take in each rule when spyware is detected, configure each rule to monitor spyware for specific severity levels, and elect to have the firewall take a packet capture of the spyware.

Available actions for traffic that matches an Anti-Spyware Profile rule are as follows:

- Allow: Permits the traffic without logging
- Alert: Generates a log entry and allows the traffic
- Drop: Discards the traffic and generates a log entry
- Reset Client: For TCP, resets the client-side connection. For UDP, drops the connection.
- Reset Server: For TCP, resets the server-side connection. For UDP, drops the connection.
- Reset Both: For TCP, resets the connection on both the client and server. For UDP, drops the connection.
- Block IP: This action blocks traffic from either a source or a source and destination, and for a configurable number of seconds.

Anti-Spyware Exceptions

Objects > Security Profiles > Anti-Spyware > Add

Anti-Spyware Profile

Name: Strict-AntiSpyware

Description:

Rules Exceptions DNS Signatures

Enable	ID	Threat Name	IP Address Exemptions	Rule	Category	Severity	Action	Packet Capture
<input type="checkbox"/>	10585	CIA_1_22 Get password		simple-high	data-theft	high	default (alert)	disable
<input type="checkbox"/>	10313	Ezula_Toptext Popup		simple-low	adware	low	default (alert)	disable
<input type="checkbox"/>	10328	FeRAT_1		simple-high	adware	high	default (alert)	disable
<input type="checkbox"/>	10373	Wintective_Keylogger		simple-high	keylogger	high	default (alert)	disable
<input type="checkbox"/>	10046	Scar User-Agent Traffic		simple-medium	spyware	medium	default (alert)	disable
<input type="checkbox"/>	10522	SearchBossToolbar			low	low	default (alert)	disable
<input type="checkbox"/>	10223	FunBuddyIcons View Fub Buddy icons			low	low	default (alert)	disable
<input type="checkbox"/>	10286	Virtumonde info post			low	high	default (alert)	disable
<input type="checkbox"/>	10353	Opwin_Trojan_1_1 connection					default (alert)	disable

Show all signatures PDF/CSV

Page 1 of 138 Displaying 1-30/ 4118 threats

20 | © 2019 Palo Alto Networks, Inc.



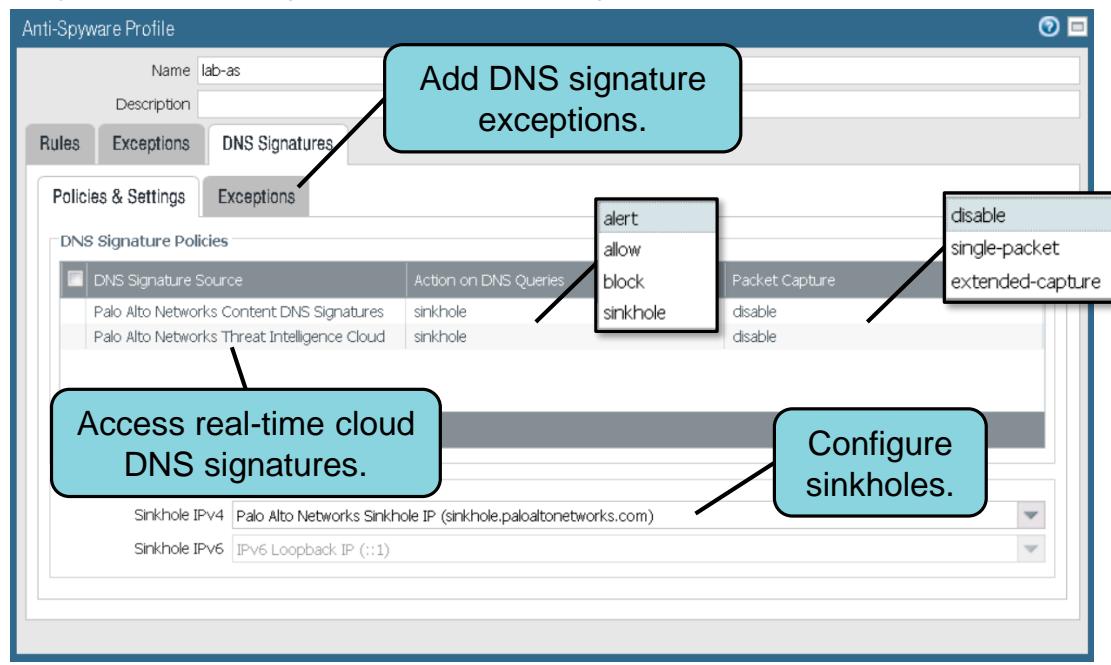
An Anti-Spyware Profile’s rules specify the actions to take when spyware is found. The **Exceptions** tab enables you to override the rules’ action responses for one or more spyware signatures. For example, you can configure a profile rule action to block all packets that match anti-spyware signatures with a critical severity level. However, you also can create an “alert” action exception that overrides a “block” action for one or more specific spyware threats.

Create even more granular exceptions by adding a list of one or more unicast IP addresses to the **IP Address Exemptions** column. Only a spyware packet whose source or destination IP address matches an address on the list will have its action response changed by the exception. The **IP Address Exemptions** column does not display the IP addresses, but only the number of IP address exemptions. Click the number in the **IP Address Exemptions** column to display the list of IP addresses.

Use the **Exceptions** tab to override the profile rules’ packet capture configurations. You can assign each spyware signature a specific packet capture configuration.

DNS Signatures

Objects > Security Profiles > Anti-Spyware > Add



21 | © 2019 Palo Alto Networks, Inc.

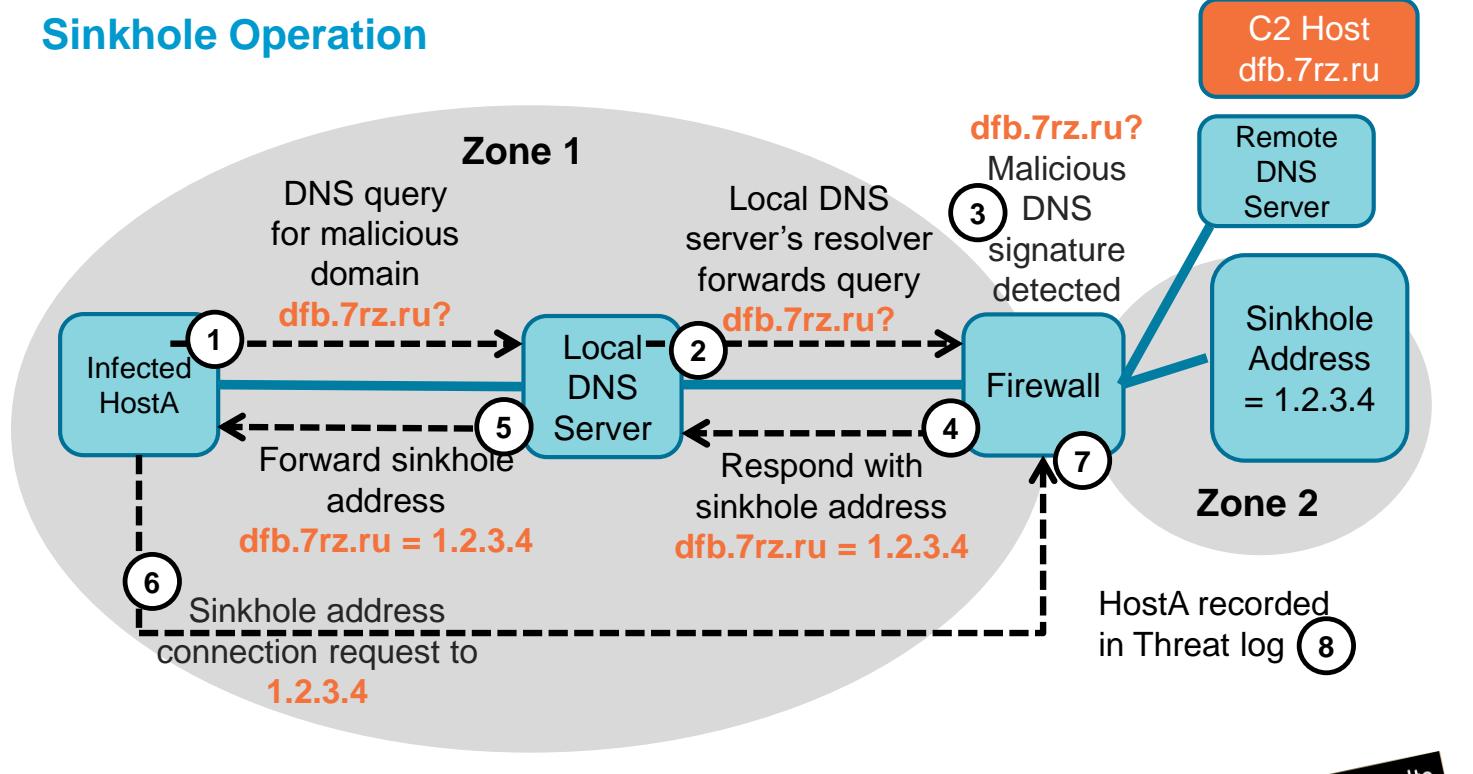


Starting with PAN-OS 9.0, DNS signatures are available through a real-time, on-demand cloud database providing you with access to the complete Palo Alto Networks DNS signature set. Previously, the downloadable DNS signature sets came with a hard-coded capacity limitation of 100K signatures, but with the on-demand cloud database, you have access to more than 36 million DNS signature sets. The cloud-based signature database provides you with instant access to newly added DNS signatures without the need to download updates. The cloud-based DNS signature database also includes built-in domain detection logic that can identify potentially malicious domains by analyzing lookups to suspiciously named domains and unusual DNS query patterns.

Each list you add to the profile can be configured with its own action. Available actions are “allow,” “alert,” “block,” and “sinkhole.” You also can enable single-packet or extended-capture packet captures when a malicious DNS signature is detected in network traffic.

You also can manually add DNS signature exceptions. Exceptions are meant to handle false positives. To add an exception, enter the DNS signature Threat ID number found in the Threat log, and then click **Add**.

Sinkhole Operation



22 | © 2019 Palo Alto Networks, Inc.



The DNS Sinkhole capability enables you to quickly identify infected hosts on the network. The default action for the Palo Alto Networks DNS signatures is “sinkhole,” and the sinkhole IP address is a Palo Alto Networks server. You can configure another IP address as the sinkhole address. The sinkhole IP address does not have to be assigned to a real host. The only recommendation is that the sinkhole address be in a different zone than the DNS client because by default only network traffic that travels between firewall zones is logged by the firewall.

DNS Sinkhole involves forging responses to select DNS queries so that clients on the network attempt to connect to the specified sinkhole IP address rather than to a known malicious domain name. You select the sinkhole IPv4 and IPv6 addresses. When the “sinkhole” action is taken, the firewall forges a response to the client and does not forward the query to the next DNS server.

The “sinkhole” action operates similarly to the “block” action. The original DNS query is never forwarded to the next DNS server, and sinkhole IP address records are not cached if DNS proxy caching is enabled.

Sinkhole Events in the Threat Log

Monitor > Logs > Threat

	Receive Time	Type	Name	From Zone	To Zone	Source address	Destination address	To Port	Applicati...	Action	Severity	URL
	02/20 00:13:15	spyware	Suspicious Domain	inside	outside	192.168.1.254	4.2.2.2	53	dns	sinkhole	medium	Suspicious DNS Qu...
	02/20 00:13:15	spyware	Suspicious Domain	inside	outside	192.168.1.20	8.8.8.8	53	dns	sinkhole	medium	Suspicious DNS Qu...
	02/20 00:12:59	spyware	Suspicious Domain	inside	outside	192.168.1.20	8.8.8.8	53	dns	sinkhole	medium	Suspicious DNS Qu...
	02/20 00:12:44	spyware	Suspicious Domain	inside	outside	192.168.1.20	8.8.8.8	53	dns	sinkhole	medium	Suspicious DNS Qu...

Potentially infected host

Infected hosts are easily identified in the Threat log or through use of reports. Any host that attempts to connect to the sinkhole IP address is potentially infected with malware. Hosts that attempt to connect to the sinkhole IP address also appear in the Botnet report.



Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

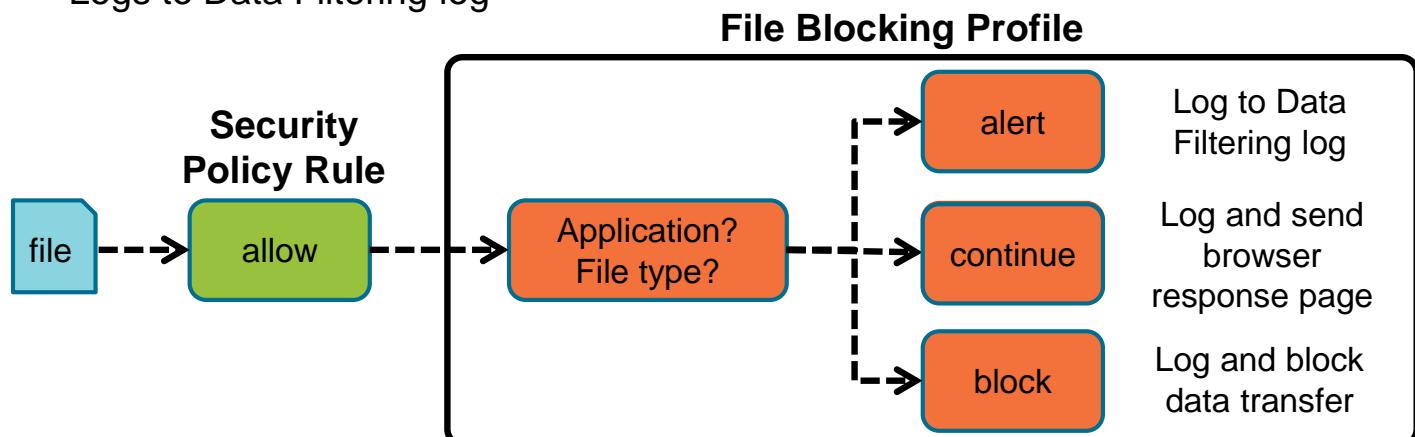
Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection

File Blocking Overview

- Prevent introduction of malicious data
- Prevent exfiltration of sensitive data
- Logs to Data Filtering log



25 | © 2019 Palo Alto Networks, Inc.



A File Blocking Profile enables you to block prohibited, malicious, and suspect files from being downloaded to or uploaded from your network. Its purpose is to prevent the introduction of malicious data and the exfiltration of sensitive data. File blocking activity is logged to the Data Filtering log.

File Blocking Profiles identify and control the flow of a wide range of file types. File type is identified by filename extension and by examination of the file content.

You can implement file blocking by type on a per-application basis. For example, you could configure a File Blocking Profile to block executable file attachments in Gmail while allowing executable file transfers in FTP.

You can configure a File Blocking Profile with three actions: “alert,” “continue,” and “block.” An “alert” action allows a file transfer but creates a log entry in the Data Filtering log. A “continue” action logs the activity but also allows a file transfer only with a user’s permission. The “block” action logs the activity and blocks a file transfer.

Data Filtering Log

- Data Filtering log records name and file type of blocked files
- Source is the system that sent the file.
- Destination is the system that received the file.

Monitor > Logs > Data Filtering

	Receive Time	Category	File Name	Name	From Zone	To Zone	Source address	Destination address	Action	To Port	Application
🔗	02/20 00:58:48	any	89yg7g87byi	Microsoft PE File	danger	danger	10.5.3.101	72.52.179.2	deny	80	web-browsing
🔗	02/20 00:58:46	any	89yg7g87byi	Microsoft PE File	danger	danger	10.5.3.101	210.1.60.27	deny	80	web-browsing
🔗	02/20 00:58:44	any	8_pdTQ.exe	Microsoft PE File	danger	danger	10.5.3.101	185.104.45.34	deny	80	web-browsing
🔗	02/20 00:58:41	any	Y2hNDK.exe	Microsoft PE File	danger	danger	10.5.3.101	185.23.21.18	deny	80	web-browsing
🔗	02/20 00:58:38	any	5t3VMv.exe	Microsoft PE File	danger	danger	10.5.3.101	185.68.16.210	deny	80	web-browsing
🔗	02/20 00:58:38	any	CV.Cindy.Nero.pdf	Adobe Portable Document Format (PDF)	danger	danger	10.10.10.10	192.168.1.121	deny	25	smtp
🔗	02/20 00:58:36	any	locky.exe	Windows Executable (EXE)	danger	danger	10.10.10.10	192.168.1.121	deny	25	smtp
🔗	02/20 00:58:36	any	locky.exe ...	Microsoft PE File	danger	danger	10.10.10.10	192.168.1.121	deny	25	smtp
🔗	02/20 00:58:30	any	onus.dll	Microsoft PE File	danger	danger	192.168.204....	64.202.116.124	deny	80	silverlight
🔗	02/20 00:55:36	any	multi-level-encoded-fil...	Multi-Level Encoding	inside	dmz	192.168.1.20	192.168.50.10	alert	80	web-browsing

26 | © 2019 Palo Alto Networks, Inc.



Use the Data Filtering log to display the list of files blocked by your File Blocking Profiles. The name and file type are recorded along with a wide range of other information. You can use the log information to adjust your firewall rules and File Blocking Profiles as necessary.

The **Source** and **Destination** in the Data Filtering log are different from the **Source** and **Destination** in the Traffic log. In the Data Filtering log, the **Source** is the system that sent the file and the **Destination** is the system that received the file. In the Traffic log, the **Source** refers to the system that initiates a session and the **Destination** refers to the system that responds in a session.

Creating a New File Blocking Profile

Objects > Security Profiles > File Blocking > Add

The screenshot shows the 'File Blocking Profile' configuration screen. At the top, there are fields for 'Name' (set to 'file-blocking') and 'Description' (set to 'Threat prevention through blocking file types'). Below these are two rules listed in a table:

Name	Applications	File Types	Direction	Action
A	web-browsing	any	both	alert
B	any	any	both	continue

A callout box points to the 'Add' button at the bottom left of the rule table, with the text: 'Add one or more rules to control file transfer.' Three separate callout boxes point to the 'File Types' column of each rule, the 'Direction' column of rule B, and the 'Action' column of rule B, respectively. Each callout box contains a list of file types, directions, and actions:

- File Types: bat, bmp, bmp-upload, cab, catpart
- Directions: upload, download, both
- Actions: alert, block, continue

27 | © 2019 Palo Alto Networks, Inc.



Unlike other Security Profiles, there is no predefined File Blocking Profile. You must create a File Blocking Profile to instruct the firewall how to treat a file that matches certain criteria when it is detected in a data stream.

A File Blocking Profile contains one or more rules that configure the actions taken by a firewall when it detects an application that is trying to transfer a file. Provide each rule with a unique name and then specify the applications, file types, and transfer directions to which the rule applies, and the action for the firewall to take. The direction of the transfer can be upload, download, or both. Files inside a ZIP file also are examined and the action applied. For example, if a rule is configured to block EXE files and a ZIP file containing an EXE file traverses the firewall, then the entire ZIP file is blocked.

Overlapping File Blocking Profile rules can exist with different actions. The File Blocking Profile rulebase does not follow a top-down approach when rule actions are applied. When traffic matches a single rule, the rule's action is taken. However, in the case where traffic matches multiple rules, the highest precedence action is taken.

The order of action precedence is “continue,” “block,” and “alert.” For example, browser traffic would match rule B in the illustration because the “continue” action has a higher precedence than the “alert” action.

Continue Response Page

- A “continue” action requires user permission to complete the file transfer.
- Operates only when paired with the application web-browsing

File Download Blocked

Access to the file you were trying to download has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

File name: Support_services_ds1.pdf

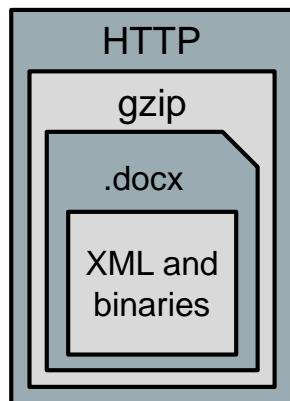
Please click **Continue** to download/upload the file.

An action of “continue” allows a file transfer only with a user’s permission. A web-based response page informs the user that an application is trying to transfer a file and prompts the user for permission to complete the transfer. The “continue” action operates only when paired with the application web-browsing. If you pair it with any other application, then file transfer is blocked.

Configuration of the “continue” action with the web-browsing application is useful to prevent drive-by downloads. A drive-by download occurs when a user connects to a webpage and a file is unknowingly downloaded to the user’s system. This attack vector is common.

Blocking Multi-level Encoded Files

Firewall decodes max of four levels



Objects > Security Profiles > File Blocking > Add

The screenshot shows the 'File Blocking Profile' configuration screen. The profile is named 'block-multi-level-encoding'. A table lists a single rule: 'block multiple levels' under 'Applications', 'any' under 'File Types', 'both' under 'Direction', and 'block' under 'Action'. A callout box points to the 'File Types' column, stating 'Blocks files encoded more than four levels'.

Name	Applications	File Types	Direction	Action
block multiple levels	any	Multi-Level-Encoding	both	block

Files can be encoded by multiple layers of protocols and applications. For example, a Word document with file extension .docx is an encoded file containing XML and binaries. If the file is zipped, then there are three levels of encoding. If the zipped file is sent using HTTP chunk encoding, then there are four levels of encoding. Encoding has legitimate uses but can be used to insert malicious data and exfiltrate sensitive data.

The firewall began decoding up to four layers of encoding in PAN-OS 7.0 to scan files for malicious or sensitive content. Earlier versions of PAN-OS software supported only two layers. Files encoded more than four layers cannot be completely decoded but can be blocked by a File Blocking Profile.

To block files that are encoded more than four times, create a File Blocking Profile with the File Types field set to Multi-Level-Encoding and the Action set to block. Assign the File Blocking Profile to the Security policy rule that will match your multi-level encoded traffic.

Encoding methods that can be decoded by the firewall are base64, gzip, HTTP 1.1 chunked encoding, pkzip, qpencode, and uuencode.

To test the configuration, you can zip a file five times and attempt to pass the file through the firewall with a File Blocking Profile applied to a Security policy rule. The attempt should be blocked with an error on the client side, and the firewall should log an entry in the Data Filtering log.

Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection



Creating a Data Pattern

Objects > Custom Objects > Data Patterns > Add

The screenshot shows the 'Data Patterns' configuration screen. At the top, there are fields for 'Name' (set to 'Confidential Data'), 'Description' (empty), and 'Pattern Type' (set to 'Predefined Pattern'). Below this is a table listing several predefined patterns:

Name	Description	File Type
Credit Card Numbers	US Credit Card Numbers pattern	Any
Social Security Numbers	US Social Security Numbers pattern	Any
Social Security Numbers (without dash separator)	US Social Security Numbers pattern without dash	Any

At the bottom of the table are 'Add' and 'Delete' buttons. A context menu is open over the last row of the table, with options: 'Predefined Pattern', 'Regular Expression', and 'File Properties'. The 'File Properties' option is highlighted with a black box.

31 | © 2019 Palo Alto Networks, Inc.



Data Filtering Profiles are used to prevent sensitive, confidential, and proprietary information from leaving your network. Data patterns are used to define the information types that you want the firewall to filter. Predefined patterns and built-in settings enable you to easily create custom data patterns for filtering on Social Security numbers, credit card numbers, or file properties such as a document title or author.

You can create three types of data patterns for the firewall to use when scanning for sensitive information:

- **Predefined:** Use the predefined data patterns to scan files for Social Security and credit card numbers.
- **Regular Expression:** Create custom data patterns using regular expressions.
- **File Properties:** Scan files for specific file properties and values.

To enable compliance for standards such as HIPAA, GDPR, Gramm-Leach-Bliley Act, PAN-OS 9.0 supports 19 predefined data-filtering patterns that help prevent the loss of sensitive information and records. These predefined patterns support checksum validation algorithms to ensure that data patterns are matched correctly and help to reduce the possibility of false positives.

Creating a Data Filtering Profile

Objects > Security Profiles > Data Filtering > Add

The screenshot shows the 'Data Filtering Profile' configuration screen. The profile is named 'Block Sensitive Data'. A 'Data Capture' checkbox is checked. The table below lists a single rule for 'Confidential Data' with 'any' applications and 'Any' file type, set to both upload and download directions. Annotations explain the 'Data Capture' checkbox, the alert threshold (0), and the number of instances (0).

Data Pattern	Applications	File Type	Direction	Alert Threshold	Block Threshold	Log Severity
Confidential Data	any	Any	both	0	0	informational

32 | © 2019 Palo Alto Networks, Inc.



Data filtering enables the firewall to detect sensitive information and prevent this data from leaving your network. Sensitive data can include Social Security numbers, credit card numbers, or internal corporate documents that may contain the word “confidential.” Before you enable data filtering, you must define the type of data you want to filter. A Data Filtering Profile can contain a single data pattern or multiple data patterns. After you attach a Data Filtering Profile to a Security policy rule, the firewall scans for each data pattern and blocks the matching traffic based on the profile settings.

A Data Filtering Profile contains one or more rules that configure the type of data that the firewall scans for and the actions to be taken when it detects an application that is trying to transfer a file. Provide each rule with a unique name and then specify the applications, file types, and transfer directions to which the rule applies, and the number of instances of the data pattern. The direction of the transfer can be upload, download, or both.

If the **Data Capture** check box is selected, the firewall automatically collects the data that is being blocked by the filter.



Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection

Assigning Security Profiles to Security Rules

Policies > Security > Add

The screenshot shows the 'Profile Setting' section of a 'Security Policy Rule' configuration. It includes fields for Action (Allow), Log Setting (Log at Session End checked), and Profile Type. The 'Profile Type' dropdown is highlighted with a black box, showing two options: 'Profiles' (selected) and 'Group'. A large black arrow points from the 'Profiles' box to the 'Group' box. Below the dropdown, there are additional settings like 'Group Profile' and 'Disable Server Response Inspection'.

- Assign individual Security Profiles to a Security policy rule, or
- Assign a Security Profile Group to a Security policy rule

You can assign either individual Security Profiles or a Security Profile Group to a Security policy rule. To assign individual Security Profiles to a Security policy rule, select **Profiles** as the **Profile Type**. To assign a Security Profile Group to a Security policy rule, select **Group** as the **Profile Type**.

Security Profile Groups

Objects > Security Profile Groups > Add

Name	Strict Profiles
Antivirus Profile	Strict Antivirus
Anti-Spyware Profile	Strict Anti-Spyware
Vulnerability Protection Profile	Strict Protection
URL Filtering Profile	Strict URL Filtering
File Blocking Profile	Strict File Transfer
Data Filtering Profile	None
WildFire Analysis Profile	None

OK Cancel

- Add Security Profiles that are commonly used together
- Security Profile Groups simplify Security policy rule administration

The firewall supports the ability to create Security Profile Groups, which specify sets of Security Profiles that you can add in one step to a Security policy rule. For example, you can create a Security Profile Group that includes Security Profiles for Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, and File Blocking, and then assign that Security Profile Group to a Security policy rule. Use of Security Profile Groups simplifies Security policy rule administration.

For example, you could create a Security Profile Group that could be applied to all Security policy rules that match traffic inbound from the internet. If a specific Security Profile within the group needs to be modified to create more stringent security checks, the modifications to the Security Profile can be made once but would be applied to all Security policy rules associated with the Security Profile Group.



Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

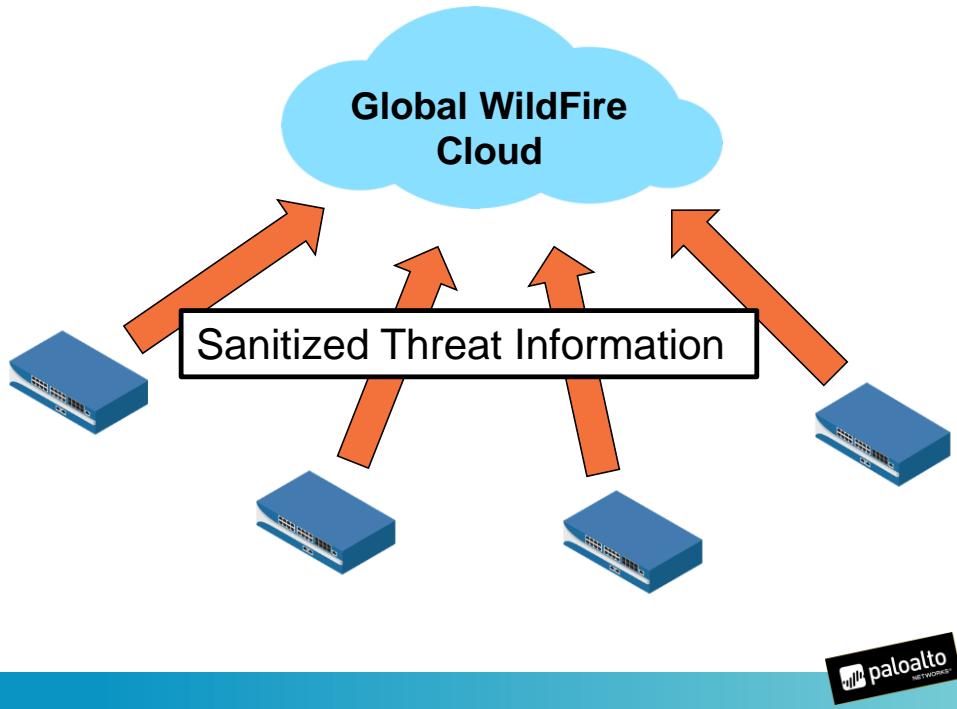
Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection

Telemetry and Threat Intelligence

- Opt-in feature; nothing selected by default
- Globally enhances threat protection
- Can preview data sent to Palo Alto Networks



37 | © 2019 Palo Alto Networks, Inc.



You can participate in telemetry, a community-driven approach to threat prevention. Telemetry enables your firewall to periodically collect and share information about applications, threats, and device health with Palo Alto Networks. The firewall now performs passive DNS monitoring, a type of telemetry that sends DNS information detected on your network to Palo Alto Networks, for all firewall traffic. Prior to PAN-OS® 8.0, the firewall collected only information from command and control, or C2, traffic that Anti-Spyware Profiles detected.

Palo Alto Networks uses the threat intelligence gathered from telemetry to deliver enhanced intrusion prevention system (IPS) and spyware signatures to you and other customers worldwide. For example, when a threat event triggers vulnerability or spyware signatures, the firewall shares the URLs that are associated with the threat with the Palo Alto Networks threat research team so that it can properly classify the URLs as malicious. Telemetry also allows Palo Alto Networks to rapidly test and evaluate experimental threat signatures with no impact to your network so that critical threat prevention signatures can be released to all customers more quickly.

Telemetry is an opt-in feature. You can choose which data the firewall shares through telemetry and view samples of this data through your **Telemetry** and **Threat Intelligence** settings. All telemetry information is saved to the WildFire global cloud. Palo Alto Networks preserves the anonymity of telemetry participants, and does not share your telemetry data with other customers or third-party organizations. For the Application, File Type Identification, Threat Prevention, and URL reports, you can preview the report information in XML format by clicking the report's **report** icon.

Configuring Telemetry

Device > Setup > Telemetry

Join other Palo Alto Networks customers in a global sharing community, helping to raise the bar against the latest attack techniques. Choose the type of data you share across applications, threat intelligence, and device health information to improve the fidelity of the protections we deliver. Palo Alto Networks will use the data you contribute to improve threat prevention, reduce noisy signatures, and enhance application and URL classifications.

Telemetry is an opt-in feature that is disabled by default and controlled with the settings below. You can enable or disable sharing at any time. The information you share may include personal information. To see what kind of information is collected for a report type, view the Threat Prevention Data. Click the Help icon to learn more about this feature.

Show reports sent to Palo Alto Networks

Download Threat Prevention Data

Settings

Application Reports
Threat Prevention Reports
URL Reports
File Type Identification Reports

Threat Prevention Data
Threat Prevention Packet Captures
Product Usage Statistics
Passive DNS Monitoring

Select All Deselect All

paloalto NETWORKS

38 | © 2019 Palo Alto Networks, Inc.

A single configuration window is available to enable a firewall to send threat intelligence data to Palo Alto Networks. Use the check boxes to configure the types of information to send. Click the **Download** icon to download a .tar.gz file containing the 100 most recent folders with **Threat Prevention Packet Captures** and **Threat Prevention Data** that has been sent to Palo Alto Networks.



Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

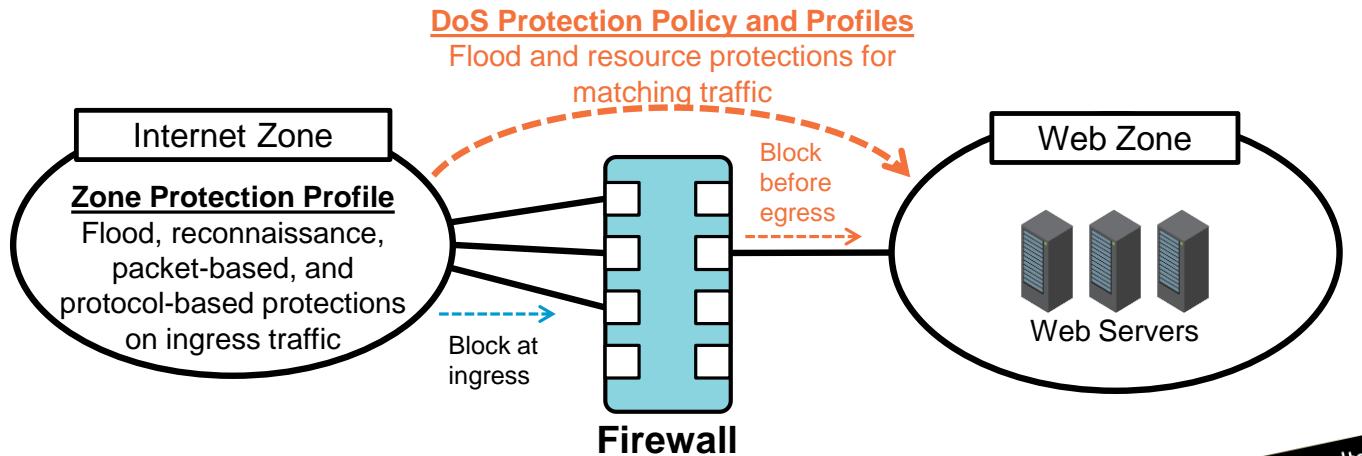
Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection

Denial-of-Service Protection

- Packet-based (not signature-based) and not linked to Security policy
- Two-pronged approach :
 - Zone Protection Profile protects ingress zone
 - DoS policy plus DoS Profile protects destination zone or specific hosts



40 | © 2019 Palo Alto Networks, Inc.



The firewall provides denial-of-service (DoS) protections that mitigate Layer 3 and 4 protocol-based attacks. DoS protections are packet-based rather than signature-based. DoS protections use packet header information to detect threats rather than a signature such as the antivirus, anti-spyware, and vulnerability protections. The DoS protections are not linked to Security policy.

A DoS attack is an attempt to disrupt network services by overloading the network with unwanted traffic. DoS protection in PAN-OS software features a two-pronged approach to mitigate DoS attacks:

- Zone-based protection: A Zone Protection Profile provides broad-based, comprehensive DoS protection at the edge of your network to prevent your enterprise from volumetric DoS attacks. The Zone Protection Profile acts as a first line of defense for your network.
- End host protection: The DoS Protection policy and profiles provide flexible rules and matching criteria that enable you to protect destination zones or even specific end hosts such as web servers, DNS servers, or any servers that are critical or have been prone to DoS attacks.

These approaches complement each other and are recommended to be deployed in tandem to achieve the best results against the various DoS attacks observed in the internet. Zone protection will be enforced before DoS Protection policy if an IP address happens to match both.

Zone Protection: Flood Protection

- Protects against most common flood attacks
- Alarm Rate: Threshold to trigger log events
- Activate: Threshold to activate mitigation response
- Maximum: Threshold after which all further packets dropped

Network > Network Profiles > Zone Protection > Add

The screenshot shows the 'Zone Protection Profile' configuration screen. The 'Name' field is set to 'Edge Zone Protection'. The 'Flood Protection' tab is active. Under the 'SYN' section, the 'Action' dropdown is set to 'Random Early Drop'. The 'Alarm Rate (connections/sec)' is 10000, 'Activate (connections/sec)' is 10000, and 'Maximum (connections/sec)' is 40000. Under the 'ICMP', 'UDP', and 'Other IP' sections, the 'Action' dropdown is set to 'SYN Cookies'. The 'Alarm Rate (connections/sec)', 'Activate (connections/sec)', and 'Maximum (connections/sec)' fields are all set to 10000. A callout box points to the 'Action' dropdown under SYN, stating: 'All categories use Random Early Drop except for SYN, which provides a choice.'

41 | © 2019 Palo Alto Networks, Inc.



A Zone Protection Profile protects against most common SYN flood, UDP flood, and ICMP flood attacks. The firewall determines packet rates by tracking the packets per second sent from one or many hosts to one or many ingress interfaces in the zone. The rates are effectively treated as packets per second because only initial packets that are *not* associated with an existing session are counted. Packets to all ingress interfaces in the zone are sampled at an interval of one second to determine if the collective rate matches an **Alarm Rate**, **Activate**, or **Maximum** threshold.

The **Alarm Rate** threshold determines when an alert should be triggered. Triggered alerts are recorded in the Threat log and on the **Dashboard**.

The **Activate** threshold determines when the mitigation response should be triggered. All flood protections use Random Early Drop, or RED, by default. RED operates by randomly dropping packets when the packet rate exceeds the **Activate** threshold. When the packet rate exceeds the **Maximum** threshold, all packets are dropped. When RED is in effect, it can drop valid connection request packets.

To mitigate SYN floods, you can configure the firewall to use SYN cookies instead of RED. If you configure SYN cookies, then you should set the **Activate** threshold to 0 to ensure that SYN cookies are used for all TCP connection attempts.

Zone protection is disabled on the firewall by default when the Threat Prevention license is installed. If you are using threat prevention, you might not need to enable zone protection. However, use of both threat protection and zone protection provides added security.

Zone Protection: Reconnaissance Protection

Network > Network Profiles > Zone Protection > Add

- Alerts or protects against port scans and host sweeps

Scan	Enable	Action	Interval (sec)	Threshold (events)
TCP Port Scan	<input type="checkbox"/>	alert	2	100
Host Sweep	<input type="checkbox"/>	alert	10	100
UDP Port Scan	<input type="checkbox"/>	alert	2	100

42 | © 2019 Palo Alto Networks, Inc.



Reconnaissance protection is used to alert or protect against reconnaissance attempts such as TCP or UDP port scans and ICMP/TCP/UDP host sweeps. The protection always is applied to the ingress interfaces in the protected zone, regardless of the zone where the destination hosts are located.

For port scans:

- The **Interval** is the time between successive probes for open ports on a destination host.
- The **Threshold** is the number of scanned ports on a destination host, within the specified time interval, that will trigger reconnaissance protection action.

For host sweeps:

- The **Interval** is the time between successive probes to a destination network.
- The **Threshold** is the number of scanned IP addresses on a destination network, within the specified time interval, that will trigger reconnaissance protection action.

You may configure the firewall to perform one of four possible actions:

- Allow: Permits port scan or host sweep attempts
- Alert: Generates an alert for each scan that matches the threshold within the specified time interval
- Block: Drops all traffic from the source
- Block IP: Drops all traffic for a specified duration of time. There are two options:
 - source: Blocks traffic from the source IP address
 - source-and-destination: Blocks traffic for the source and destination IP pair

Zone Protection: Packet-Based Attack Protection

Network > Network Profiles > Zone Protection > Add

- Blocks packets based on protocol options or packet malformation

The screenshot shows the 'Zone Protection Profile' configuration screen. At the top, there are fields for 'Name' (set to 'Edge Zone Protection') and 'Description'. Below these are four tabs: 'Flood Protection', 'Reconnaissance Protection', 'Packet Based Attack Protection' (which is selected), and 'Protocol Protection'. Under the 'Packet Based Attack Protection' tab, there are several sections: 'IP Drop' (selected), 'TCP Drop', 'ICMP Drop', 'IPv6 Drop', and 'ICMPv6 Drop'. Under 'IP Drop', there are three checkboxes: 'Spoofed IP address', 'Strict IP Address Check', and 'Fragmented traffic'. Under 'IP Option Drop', there are five checkboxes: 'Strict Source Routing', 'Loose Source Routing', 'Timestamp', 'Record Route', and two groups of two checkboxes each: 'Security', 'Stream ID', 'Unknown', and 'Malformed'. A help icon (a question mark) is located in the top right corner of the interface.

43 | © 2019 Palo Alto Networks, Inc.



Packet-based attacks use protocol options or malformed packets to adversely affect target systems. PAN-OS software provides the ability to block these packets when they are detected in a zone with a configured Zone Protection Profile.

Zone Protection: Protocol Protection

Network > Network Profiles > Zone Protection > Add

- Applies only to Layer 2 and Virtual Wire zones:
 - Firewall normally allows non-IP traffic in these zone types.
- Block non-IP traffic using EtherType codes

The screenshot shows the 'Zone Protection Profile' configuration screen. The 'Protocol Protection' tab is selected. The 'Rule Type' is set to 'Exclude List'. A table lists protocols with their EtherType values: 0x0000, 0x0800, 0x0806, 0x8100, and 0x86dd. An note states: 'Exclude list uses implicit allow for all non-listed protocols'. Buttons for 'Add' and 'Delete' are at the bottom.

44 | © 2019 Palo Alto Networks, Inc.



A firewall normally passes non-IP protocols between or within Layer 2 zones or between or within Virtual Wire zones. Configuration of **Protocol Protection** enables you to control which non-IP protocols are allowed to flow between or within these security zone types.

If you create an exclude list, then all other non-IP traffic is included. If you create an include list, then all other non-IP traffic is excluded. For example, if you want to enable the firewall to pass only EtherTalk packets, then create an include list that contains the EtherType 0x809B.

Enabling Zone Protection

Network > Zones > <select_zone>

- Profiles applied one per zone

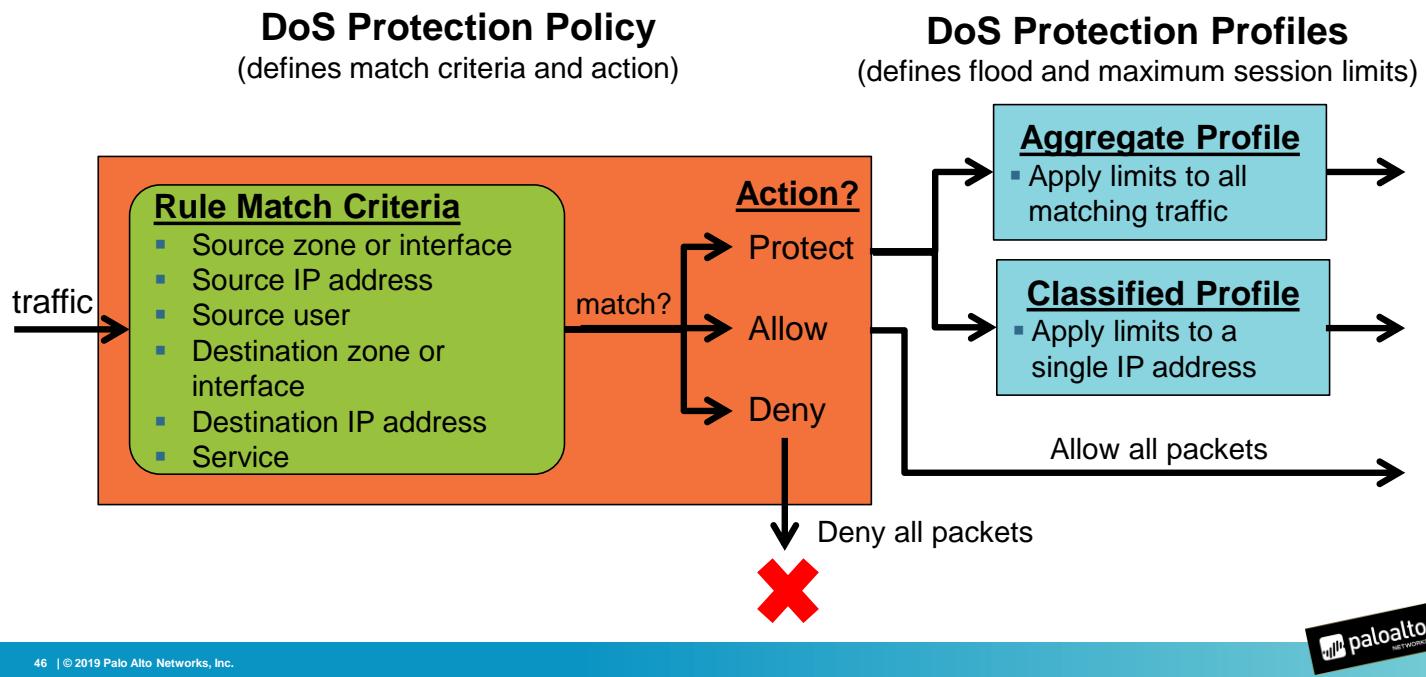
The screenshot shows the 'Zone' configuration page for the 'Internet' zone. The 'Name' field is set to 'Internet', 'Log Setting' is 'None', and 'Type' is 'Layer3'. Under the 'Interfaces' section, 'ethernet1/1' is listed. In the 'Zone Protection' section, the 'Zone Protection Profile' dropdown is set to 'Edge Zone Protection' (which is highlighted with a black box). There is also an unchecked checkbox for 'Enable Packet Buffer Protection'. On the right side, there are two sections: 'User Identification ACL' and 'Zone Protection ACL'. Both sections have 'Add' and 'Delete' buttons and include lists for selecting addresses or address groups.

45 | © 2019 Palo Alto Networks, Inc.



A Zone Protection Profile is enabled on a per-zone basis. Each zone can have only one Zone Protection Profile assigned to it.

DoS Protection Profiles and Policies



46 | © 2019 Palo Alto Networks, Inc.



A DoS Protection policy and DoS Protection Profiles are designed to work with Zone Protection Profiles. A Zone Protection Profile protects an ingress zone, but a DoS Protection policy and DoS Protection Profile provide protection for a destination zone or destination host.

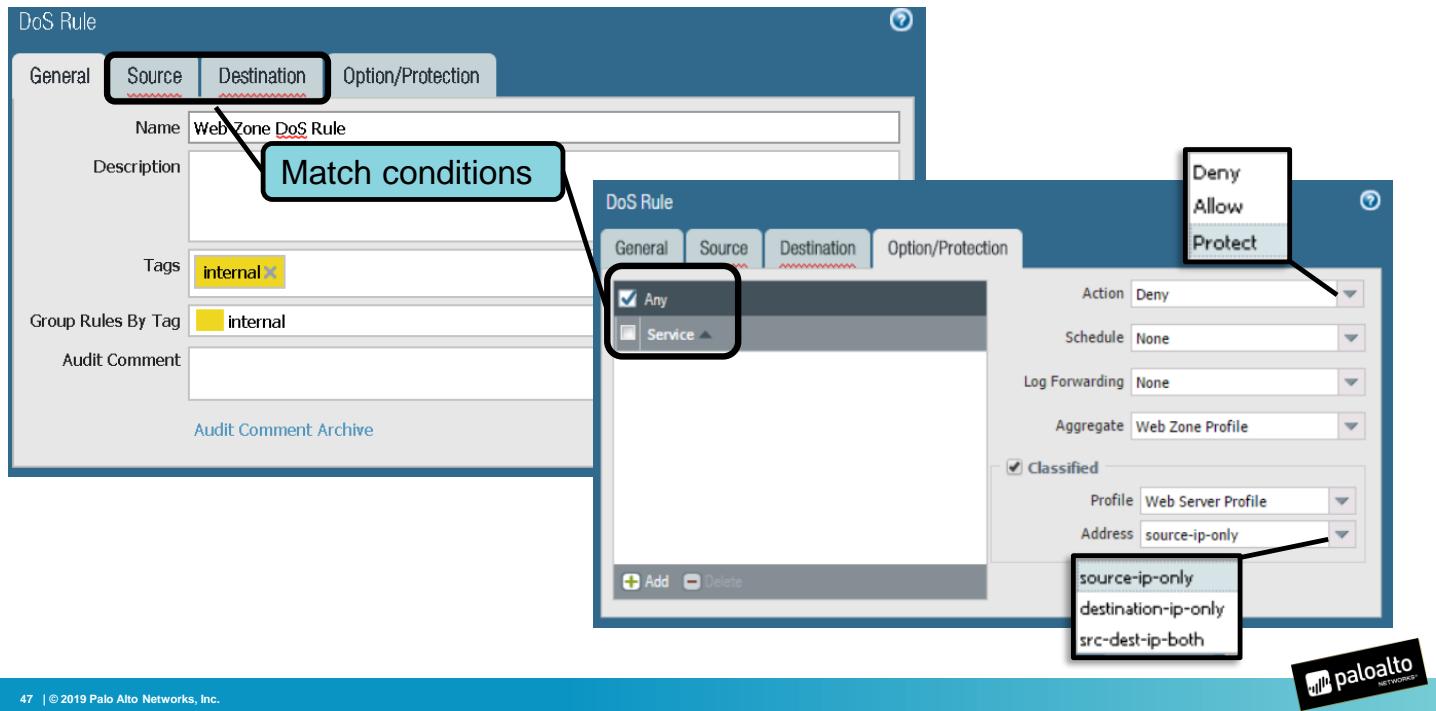
DoS Protection policy rules can be configured to use zones, interface names, IP addresses, usernames, or service names as match conditions for blocking DoS attacks. If traffic matches a policy rule, you can configure the firewall to allow all traffic, deny all traffic, or protect traffic. If you configure the rule action to be “Protect,” then any matching traffic is controlled by the limits set in a DoS Protection Profile. For example, a DoS Protection Profile can specify a maximum session limit.

A DoS Protection Profile can be an Aggregate or Classified type. For example, an Aggregate Profile enables the creation of a maximum session limit for *all* connections matching a DoS Protection policy rule. The threshold applies the maximum session limit to *all* IP addresses that match the policy rule. If new sessions created for a single IP address result in the maximum sessions limit being exceeded, then no new sessions can be created for any other IP addresses matched to the DoS Protection policy rule. However, a Classified Profile enables the creation of a session limit that applies to just a single IP address. You configure whether that IP address is matched to the source address, the destination address, or either the source or destination address. For example, you can configure a maximum session limit per IP address that will prohibit new sessions for just that IP address after that IP address has exceeded the limit.

Both Aggregate Profiles and Classified Profiles can be applied to a DoS Protection policy rule. Aggregate Profile limits generally are greater than Classified Profile limits.

Configuring a DoS Protection Policy

Policies > DoS Protection > Add



47 | © 2019 Palo Alto Networks, Inc.

Browse to **Policies > DoS Protection** and click **Add** to add a new DoS Protection policy rule. Specify the match criteria on the **Source**, **Destination**, and **Option/Protection** tabs.

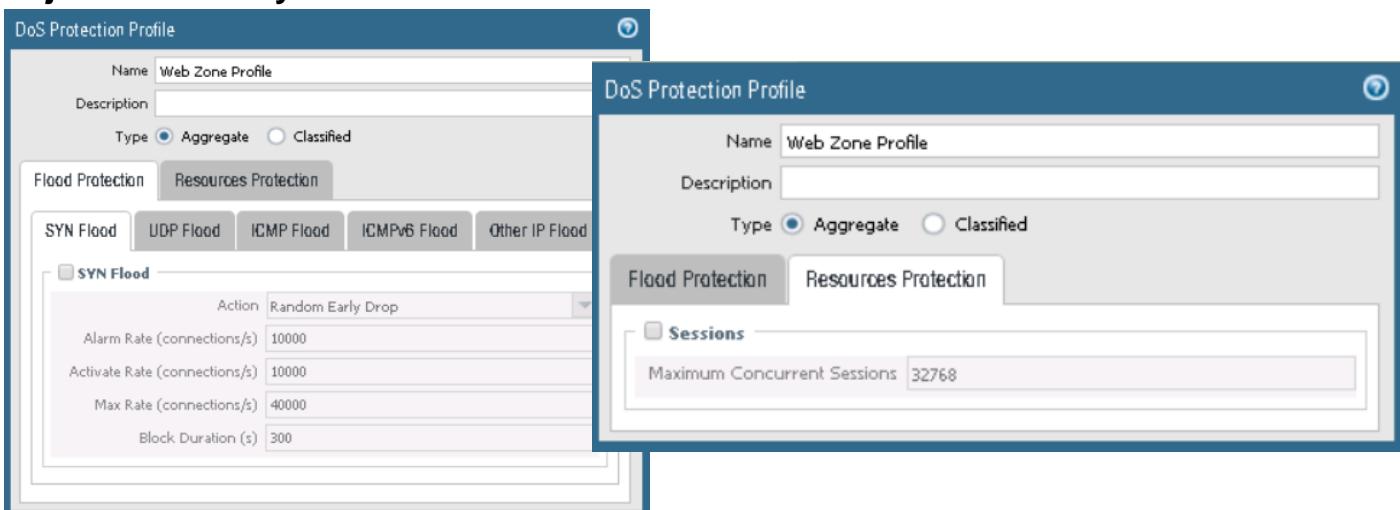
The **Option/Protection** tab is where you specify an action. You can deny all packets, allow all packets, or choose **Protect**. If you choose **Protect**, then you can choose to limit traffic using a specified DoS Protection Profile. You can specify either an Aggregate Profile, a Classified Profile, or both. If you specify both profile types, then the Aggregate Profile's rate limits generally should be greater than the Classified Profile's rate limits.

If you specify a Classified Profile, then you must specify one of the following options:

- **source-ip-only**: Each source IP is tracked individually for rate limiting. A typical use case is when you do not want any host on your network to start a DoS attack.
- **destination-ip-only**: Each destination IP is monitored individually for incoming traffic to prevent it from going above the configured rate limits for any number of source IPs. A typical use case is to protect web or DNS servers on your network.
- **src-dest-ip-both**: This setting has the firewall track the traffic flow between a given source and destination IP pair for the configured rate limits.

Configuring a DoS Protection Profile

Objects > Security Profiles > DoS Protection > Add



48 | © 2019 Palo Alto Networks, Inc.



Browse to **Objects > Security Profiles > DoS Protection** and click **Add** to add a new DoS Protection Profile.

You must select either the **Aggregate** or **Classified** type:

- Aggregate Profiles control the total traffic between all devices matched by the rule to which the profile is attached. This type of profile is similar to a Zone Protection Profile in that it manages the total traffic flow visible to the rule.
- A Classified Profile is designed to protect individual IP connections.

Two DoS protection mechanisms are configured using either the **Flood Protection** or **Resources Protection** tab:

- **Flood Protection:** Detects and prevents attacks where the network is flooded with packets, which results in too many half-open sessions or services being unable to respond to each request. You specify the flood threshold rates at which new connections per second trigger an alarm. The action taken when an alarm is triggered is specified by the DoS Protection policy rule that matched the traffic.
- **Resources Protection:** Detects and prevents session exhaustion attacks. You specify the maximum number of concurrent sessions. This setting helps to prevent an attack where a large number of hosts are used to establish as many fully established sessions as possible to consume all of a system's resources.

You can enable both types of protection mechanisms in a single DoS Protection Profile.

Module Summary

Now that you have completed this module, you should be able to:



- Describe the seven different Security Profiles types
- Define the two predefined Vulnerability Protection Profiles
- Configure Security Profiles to prevent virus and spyware infiltration
- Configure File Blocking Profiles to identify and control the flow of file types through the firewall
- Configure a DoS Profile to help mitigate Layer 3 and 4 protocol-based attacks

Now that you have completed the module, you should be able to:

- Describe the seven different Security Profiles types
- Define the two predefined Vulnerability Protection Profiles
- Configure Security Profiles to prevent virus and spyware infiltration
- Configure File Blocking Profiles to identify and control the flow of file types through the firewall
- Configure a DoS Profile to help mitigate Layer 3 and 4 protocol-based attacks

Questions



50 | © 2019 Palo Alto Networks, Inc.



Review Questions

1. Which anti-spyware feature enables an administrator to quickly identify a potentially infected host on the network?
 - a. Data Filtering log entry
 - b. continue response page
 - c. DNS sinkhole
 - d. CVE number
2. True or false? A Security Profile attached to a Security policy rule is evaluated only if the Security policy rule matches traffic and the rule action is set to “Allow.”
 - a. true
 - b. false
3. Zone Protection Profiles are applied to which item?
 - a. ingress ports
 - b. Security policy rules
 - c. egress ports
 - d. Address Groups
4. True or false? The Antivirus Security Profile defines actions to be taken if an infected file is detected as part of an application.
 - a. true
 - b. false
5. True or false? Each Anti-Spyware Security Profile contains one master rule to handle all types of threats.
 - a. true
 - b. false

Content-ID Lab (Pages 90-128 in the Lab Guide)

- Load a firewall lab configuration
- Create and test an Antivirus Security Profile
- Create and test an Anti-Spyware Security Profile
- Create and test a Vulnerability Protection Security Profile
- Create and test a File Blocking Profile

PROTECTION. DELIVERED.



Answers to Review Questions

1. c
2. a (true)
3. a
4. a (true)
5. b (false)