BLOCKING KNOWN THREATS USING SECURITY PROFILES

VERIFY THAT YOUR ALLOWED TRAFFIC IS SAFE

- Security Profile 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
- Denial-of-Service Protection

EDU-210 Version A
PAN-OS® 10.2

paloalto NETWORKS

© 2022 Palo Alto Networks, Inc.

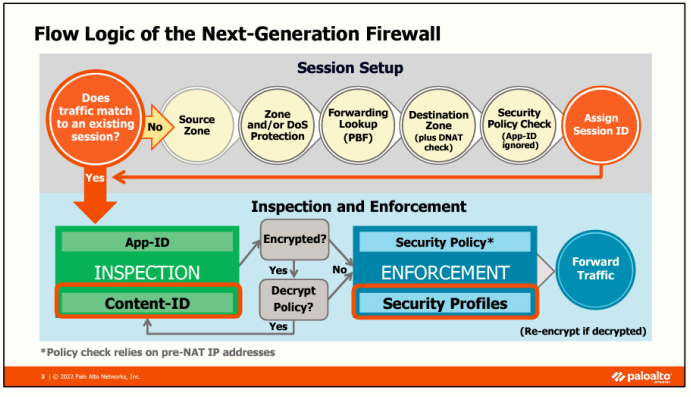
Learning Objectives

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

- Describe the seven different Security Profile 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 Protection Profile to help mitigate Layer 3 and 4 protocol-based attacks

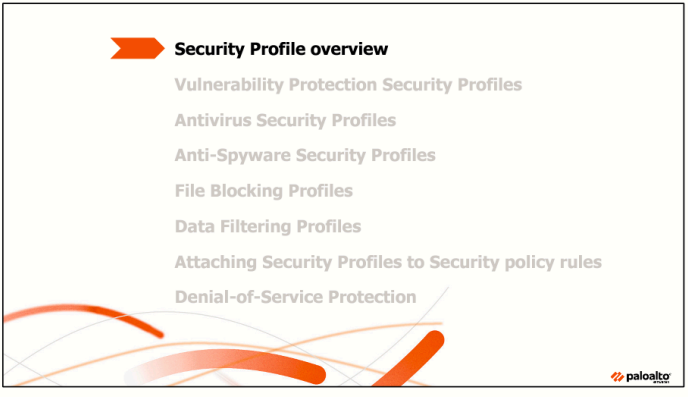
After you complete this module, you should be able to:

- Describe the seven different Security Profile 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 Protection Profile to help mitigate Layer 3 and 4 protocol-based attacks



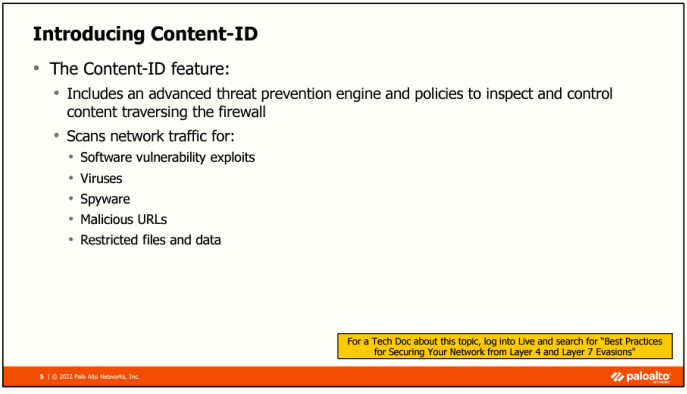
This diagram is a simplified version of the flow logic of a packet traveling through a Palo Alto Networks firewall. The course will reference this diagram to address where specific concepts fit into the packet processing sequence.

For more information about the packet handling sequence inside a PAN-OS® device, log into Live and search for "Packet Flow Sequence" or see the Packet Flow Sequence in the PAN-OS document available on the Palo Alto Networks Support website at https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0.

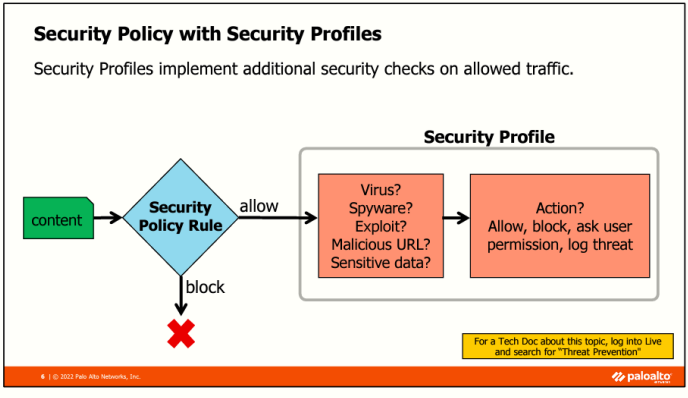


This section describes the operation of the Firewall Security Profiles.

© 2022 Palo Alto Networks, Inc.

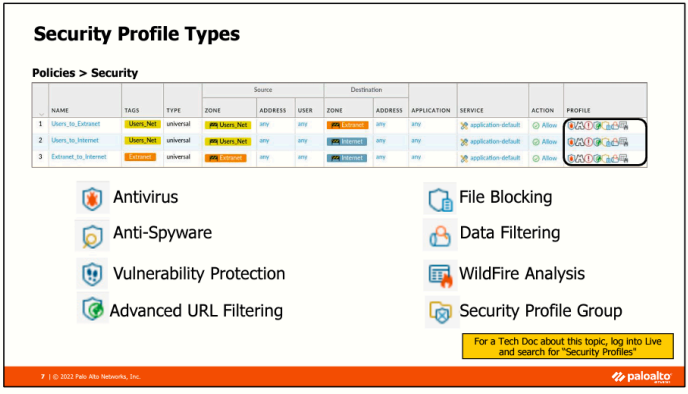


Content-ID technology combines a real-time advanced threat prevention engine with administrator-defined policies to inspect and control content traversing the firewall. Content-ID delivers a method of detection based on the complete analysis of all allowed traffic. Content-ID uses multiple advanced threat 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 applications are analyzed for exploits, viruses, spyware, malicious URLs, and dangerous or restricted files or content.



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.

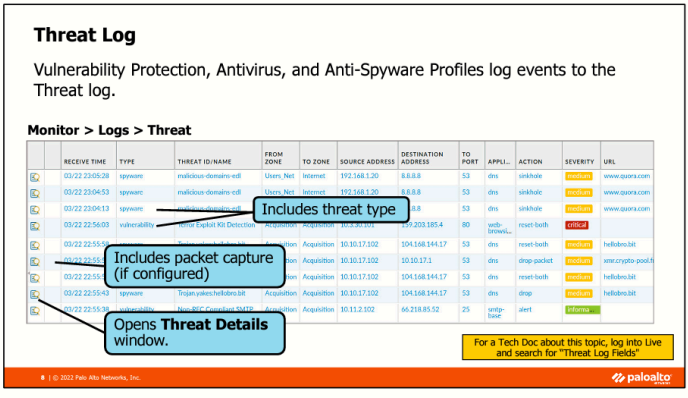
The Security Profiles represent additional security checks to be performed on allowed network traffic. Security Profiles enable you to have more granular control over allowed traffic. For example, web browsing might be allowed by a Security policy rule, but the concern remains that users could download 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**.



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
- Advanced 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.

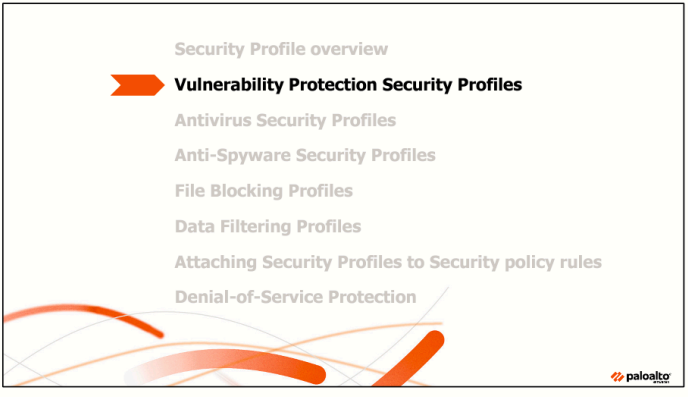


The firewall Threat log records antivirus, anti-spyware, and vulnerability threats discovered by the Security Profiles. Dozens of columns of information can be displayed. Examples of available columns are shown here. Click any column header to display the column header list. From the list you can select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

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

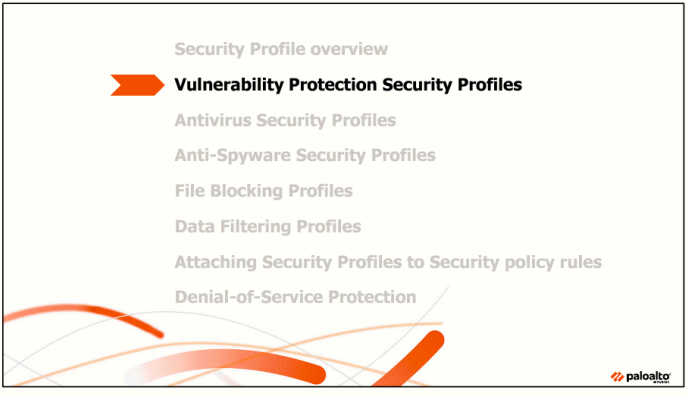
The firewall uses Threat log information as the source of information for the web interface reports and the information displayed on the **ACC** tab. "ACC" represents the Application Control Center.

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, the Logging Service, a syslog server, a web server, or an email server, or log entries can be sent as SNMP traps to an SNMP manager.



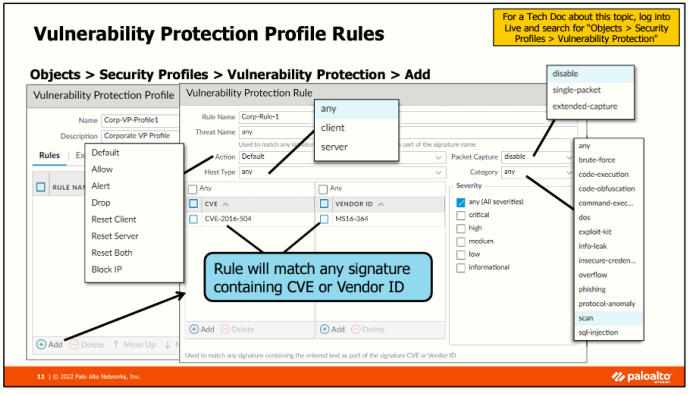
This section describes Vulnerability Protection Security Profiles.

© 2022 Palo Alto Networks, Inc.



This section describes Vulnerability Protection Security Profiles.

© 2022 Palo Alto Networks, Inc.

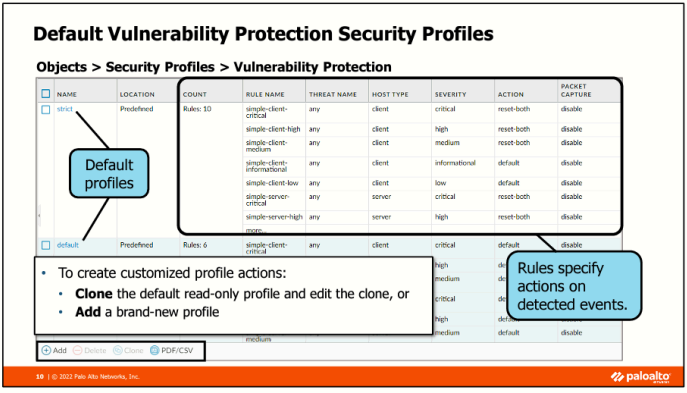


Each Vulnerability Protection Profile can contain multiple rules to process different types of threats in different ways. Each rule can be configured to take a packet capture. A rule can inspect network traffic for all threat signatures or can be configured with one or more filters that scan only for 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 any category of threats or just for those signatures that match a specific category of threat.
- A rule can scan for threats that match all or 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 when 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 Protection profiles stop attempts to exploit system flaws or gain unauthorized access to systems. While Anti-Spyware profiles help identify infected hosts as traffic leaves the network, Vulnerability Protection profiles protect against threats entering the network. For example, Vulnerability Protection profiles help protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities.

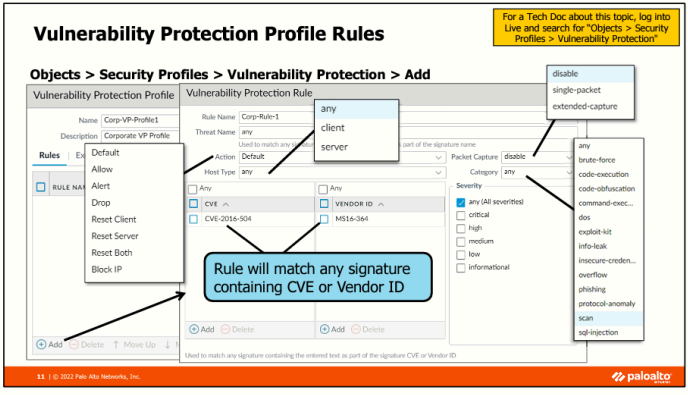
Palo Alto Networks firewalls include two predefined, read-only Vulnerability Protection Security Profiles. These profiles contain rules that configure the actions taken by a firewall when it detects malware known to exploit system vulnerabilities of different severity levels and types. Exploits include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

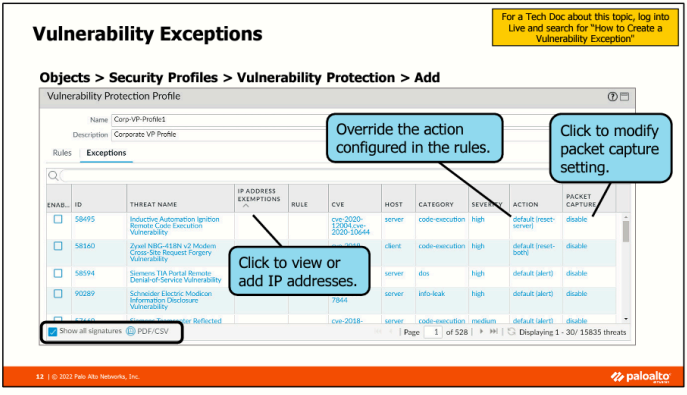


Each Vulnerability Protection Profile can contain multiple rules to process different types of threats in different ways. Each rule can be configured to take a packet capture. A rule can inspect network traffic for all threat signatures or can be configured with one or more filters that scan only for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



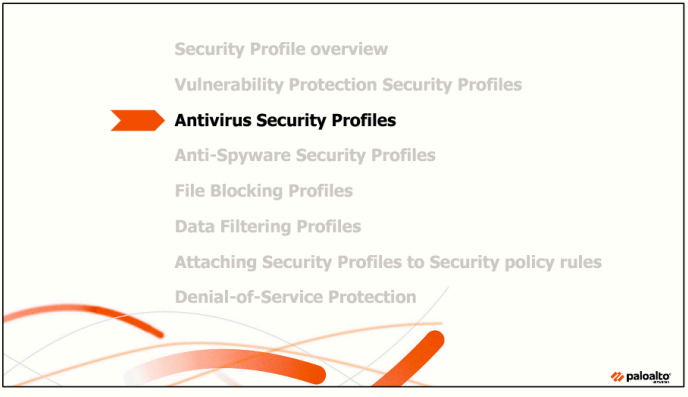
A profile's rules specify the actions to take when threats are found. The **Exceptions** tab enables you to override the rules' default action responses for one or more threat signatures. Exceptions often are used to handle false positives. For example, a profile rule could be configured to block all 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.

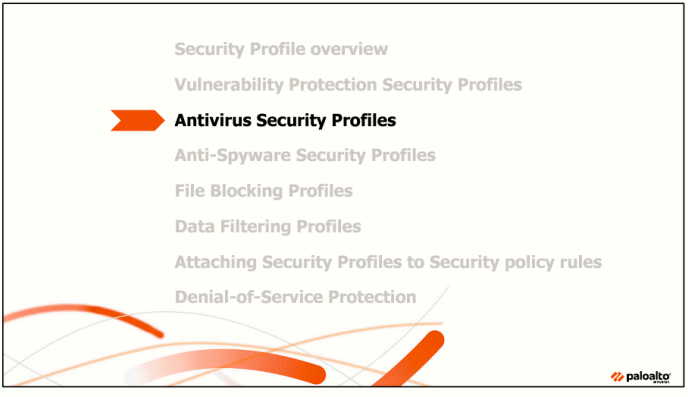
For more information about Vulnerability Exceptions, log into Live and search for "Vulnerability Exception Based Upon Source and Destination IP Address" and "What is the behavior when IP address/s are added under IP-address-exemptions" - or use the following links to view the articles:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhcCAC
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UscCAE



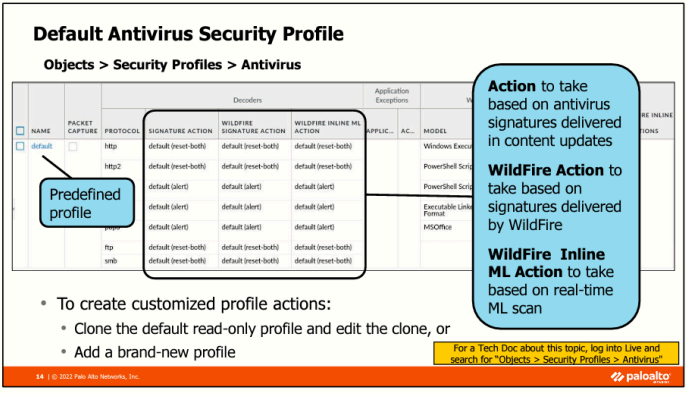
This section describes Antivirus Security Profiles.

© 2022 Palo Alto Networks, Inc.



This section describes Antivirus Security Profiles.

© 2022 Palo Alto Networks, Inc.



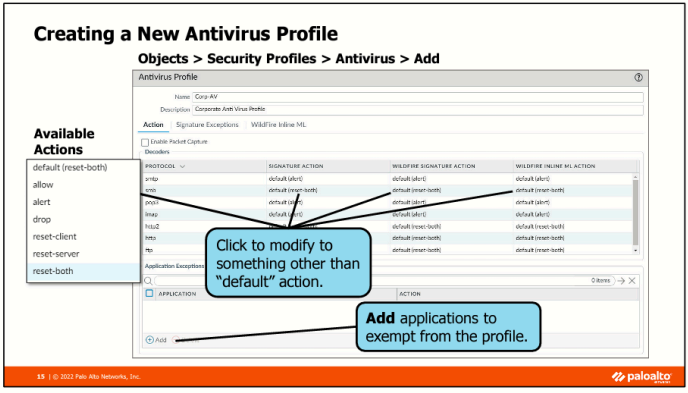
Antivirus profiles protect against viruses, worms, and trojans as well as spyware downloads. Using a stream-based malware prevention engine, which inspects traffic the moment the first packet is received, the Palo Alto Networks antivirus solution can provide protection for clients without significantly impacting the performance of the firewall.

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 and data, 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 day 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. The **WildFire Inline ML Action** field specifies action taken when a virus is detected by Machine Learning on PowerShell scripts, PE (portable executable), and ELF (executable and linked format) files in real-time.

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.



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: Permits and logs 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.

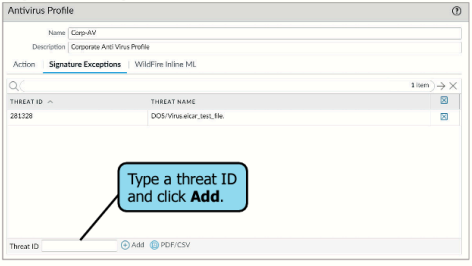
If the **Packet Capture** check box is selected, any alert also is accompanied by a packet capture of the portion of the network traffic that triggered the antivirus signature. This capture can be used to verify the presence of the virus or to determine that it is a false positive.

© 2017-2021 Palo Alto Networks, Inc.

Antivirus Profile Signature Exceptions

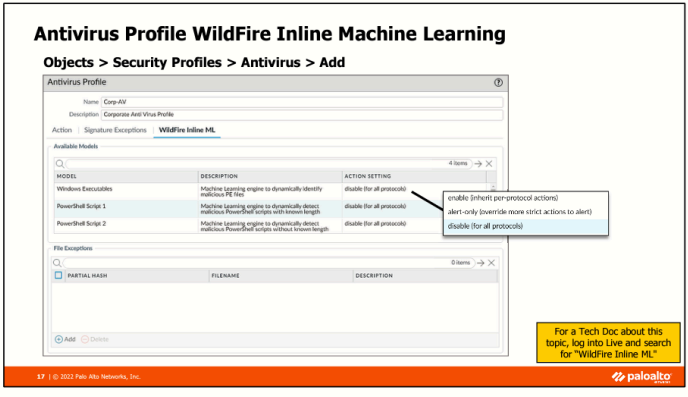
For a Tech Doc about this topic, log into Live and search for "How to Use Anti-Spyware, Vulnerability and Antivirus Exceptions to Block or Allow Threats"

Objects > Security Profiles > Antivirus > 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.



The WildFire Inline ML tab is used to enable and configure real-time WildFire analysis of files using a firewall-based machine learning model.

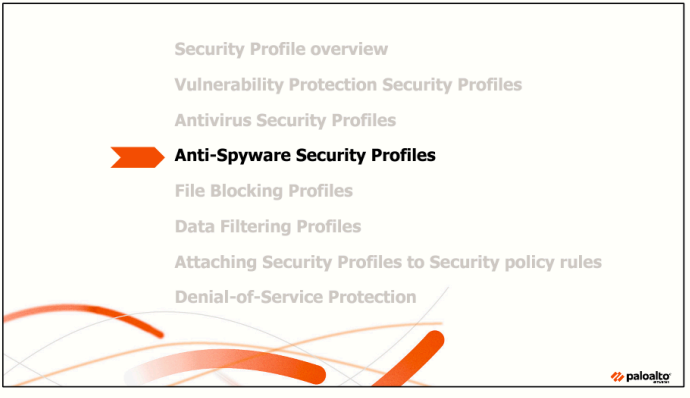
For each available WildFire inline ML Model, you can select one of the following action settings:

•**enable (inherit per-protocol actions)**—Traffic is inspected according to your selections in the **WildFire Inline ML Action** column in the decoders section of the **Action** tab.

•**alert-only (override more strict actions to alert)**—Traffic is inspected according to your selections in the **WildFire Inline ML Action** column in the decoders section of the **Action** tab. Any action with a severity level higher than alert (drop, reset-client, reset-server, reset-both) will be overridden to alert, allowing traffic to pass while generating and saving an alert in the threat logs.

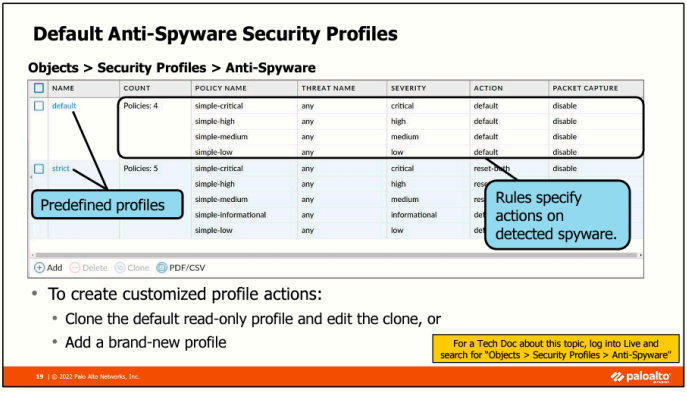
•**disable (for all protocols)**—Traffic is allowed to pass without any policy action.

The File Exceptions table allows you to define specific files that you do not want analyzed, such as false-positives. To create a new file exception entry, Select Add to create a new file exception entry and provide the partial hash, filename, and description of the file that you want to exclude from enforcement. You can add the file exception details directly to the exception list or by specifying a file from the threat logs.



This section describes Anti-Spyware Security Profiles.

© 2022 Palo Alto Networks, Inc.



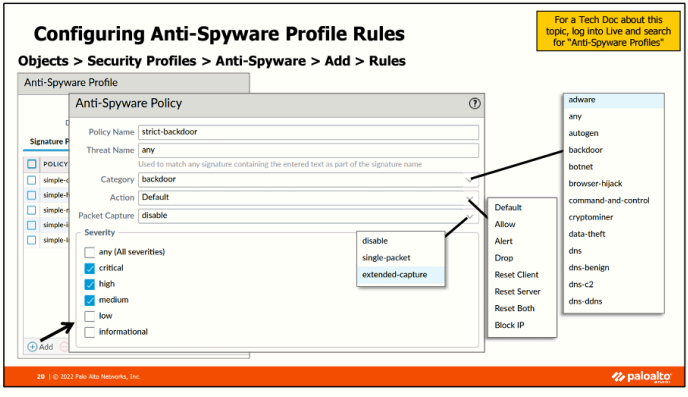
Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients. You can apply various levels of protection between zones. For example, you may want to have custom Anti-Spyware profiles that minimize inspection between trusted zones, while maximizing inspection on traffic received from an untrusted zone, such as internet-facing zones. 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 day 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.



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.

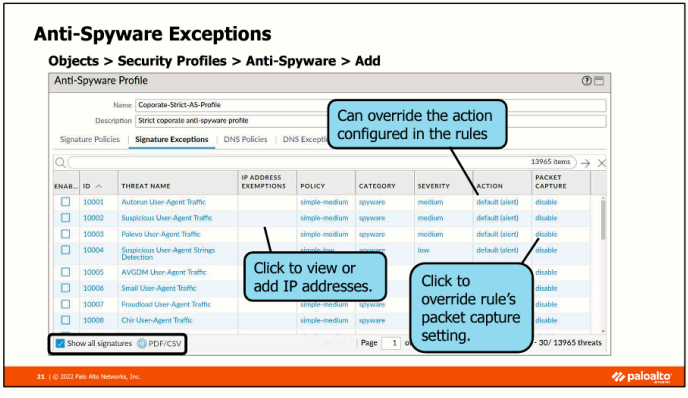
Use the keyword “any” for the **Threat Name** to enable the rule to monitor any threat name. Alternatively, enter a string for the **Threat Name** and a rule will scan only for signatures whose names include the string. You also can configure each rule to monitor specific categories of spyware threats.

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: Permits and logs 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.



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.

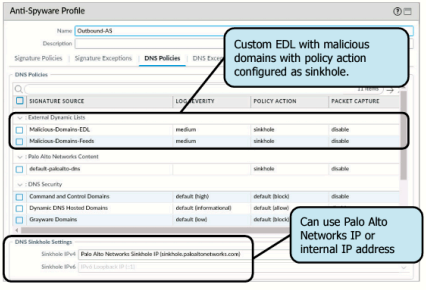
Use the **Exceptions** tab to override the profile rules' packet capture configurations. You can assign each spyware signature a specific packet capture configuration.

Configure DNS Signature Match Protection

Objects > Security Profiles > Anti-Spyware > Add

- Third-party malicious domain lists are made available as EDLs.
- Best practice is to enable sinkhole.
- Can use the Palo Alto Networks IP address or, optionally, your own internal address.

For a Tech Doc about this topic, log into Live and search for "Configure DNS Sinkholing for a List of Custom Domains"



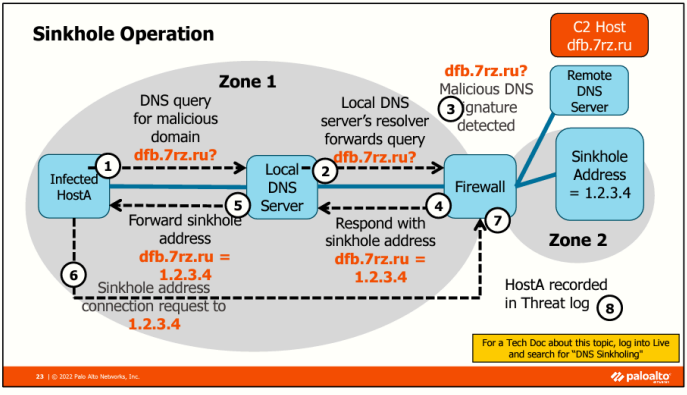
Palo Alto Networks recommends that you configure a custom Anti-Spyware Profile to use the "sinkhole" action.

Many third-party organizations also maintain and distribute malicious domain lists. Some lists are free. If the third-party website formats the list as one domain per line, then the list can be accessed by the firewall as an EDL. In the screenshot, the **Malicious-Domains-Feed** is an example of a custom domain list.

You can apply different actions to traffic matching a malicious domain signature or domain name. The actions are "alert," "allow," "block," and "sinkhole." The default and recommended action is "sinkhole" because it protects your environment and also provides increased visibility into hosts that might be infected.

You can either use the sinkhole FQDN supplied by Palo Alto Networks, or you can configure a real host and IP address as the sinkhole address. A real host should reside in a different security zone than the DNS client because only network traffic that traverses security zones is logged by the firewall. One reason to use a real "sinkhole" host is to enable you to analyze the behavior of an infected host on the network.

For more information about configuring DNS Sinkhole, log into Live and search for "how to configure DNS sinkhole" or see the knowledgebase documentation https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGECA0



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. After 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.

View Malicious Domains in the Threat Log

Monitor > Logs > Threat

	RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	TO PORT	APPLI...	ACTION	SEVERITY	URL
	03/22 23:05:28	spyware	malicious-domains-edl	Users_Net	Internet	192.168.1.20	8.8.8.8	53	dns	sinkhole	medium	www.quora.com
	03/22 23:04:53	spyware	malicious-domains-edl	Users_Net	Internet	192.168.1.20	8.8.8.8	53	dns	sinkhole	medium	www.quora.com
	03/22 23:04:13	spyware	malicious-domains-edl	Users_Net	Internet	192.168.1.20	8.8.8.8	53	dns	sinkhole	medium	www.quora.com
	03/22 22:54:38	spyware	malicious-domains-edl	Users_Net	Internet	192.168.1.20	8.8.8.8	53	dns	sinkhole	medium	www.quora.com

Internal DNS server or infected host

Typically, an external DNS server

- If you see a sinkhole in the Threat log:
  - Filter the Traffic log to see who is attempting to connect to the sinkhole IP address.
  - Hosts attempting to connect to the sinkhole address could be infected.
- Check logs daily or run a daily report.

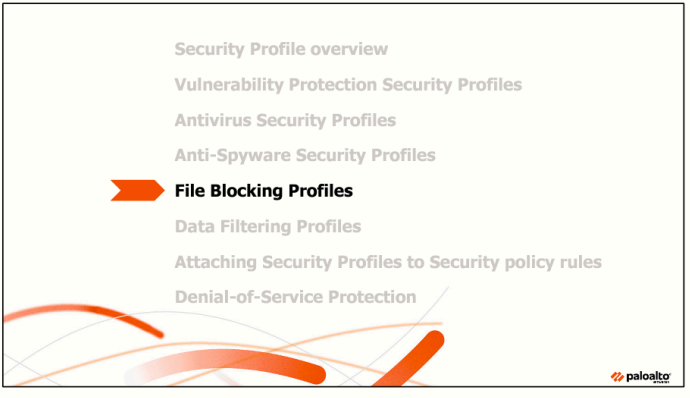
For a Tech Doc about this topic, log into Live and search for "Threat Log Fields"

24 | © 2022 Palo Alto Networks, Inc.

If you find a "sinkhole" action in the Threat log, then filter the Traffic log for the sinkhole IP address. Any host in the Traffic log that has attempted to connect to the sinkhole address could be an infected host with malware that is attempting to phone home.

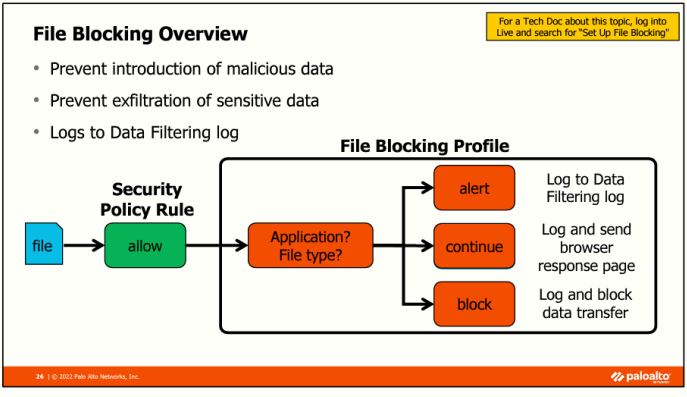
In a typical deployment where the firewall is north of the local DNS server, the Threat log would identify the local DNS resolver as the **Source Address** rather than the actual infected host. The actual infected host would not be logged. If the firewall is south of the local DNS server, then the **Source Address** would identify the infected host.

In the example shown, the local DNS server is listed in the **Source Address** column because it is the host that sent the DNS malicious domain name query to the external DNS server. The host shown in the **Destination Address** column is the external DNS server.



This section describes File Blocking Profiles.

© 2022 Palo Alto Networks, Inc.

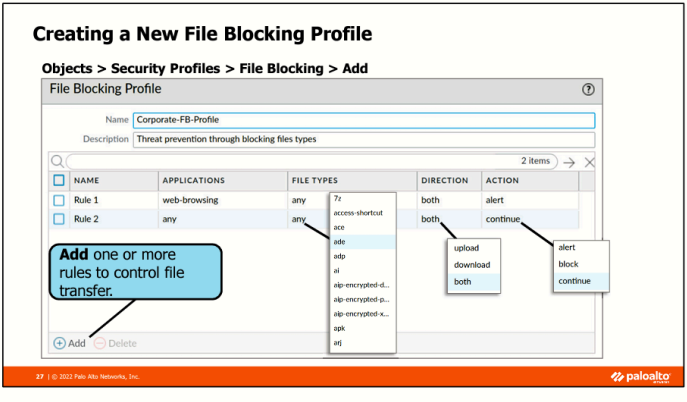


A File Blocking Profile enables you to block prohibited, malicious, and suspect files from being downloaded to or uploaded from your network. Its purpose is to prevent the introduction of malicious data and the exfiltration of sensitive data. File blocking activity is logged to the Data Filtering log.

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.



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.

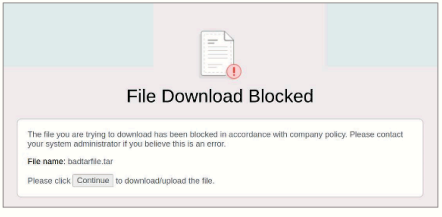
A File Blocking Profile contains one or more rules that configure the actions taken by a firewall when it detects an application that is trying to transfer a file. Provide each rule with a unique name and then specify the applications, file types, and transfer directions to which the rule applies, and 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

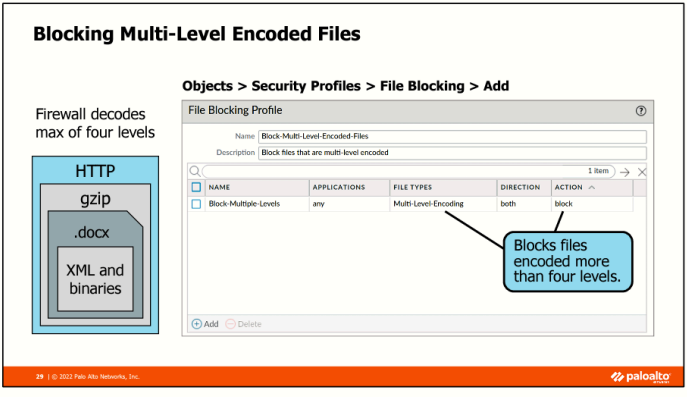
- A "continue" action requires user permission to complete the file transfer.
- Operates only when paired with the application web-browsing



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.

© 2022 Palo Alto Networks, Inc.



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 and hide malicious data or hide 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.

View Blocked Files in the Data Filtering Log

For a Tech Doc about this topic, log into Live and search for "Review Data Filtering Logs"

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

Monitor > Logs > Data Filtering

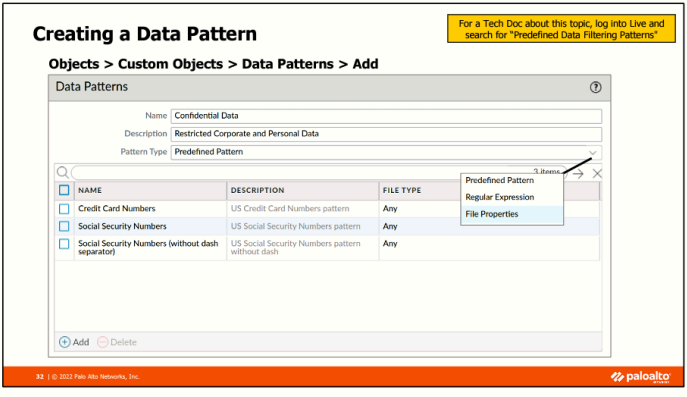
	RECEIVE TIME	CAT...	FILE NAME	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	TO PORT	APPLICATION	ACTION
	03/22 22:56:03	any	gwccax.exe-rc4.exe	Unknown Binary File	Acquisition	Acquisition	10.3.30.101	159.203.185.4	80	web-browsing	alert
	03/22 22:56:03	any	SilverApp1.dll	Microsoft PE File	Acquisition	Acquisition	10.3.30.101	159.203.185.4	80	silverlight	deny
	03/22 22:56:03	any	SilverApp1.xap	ZIP	Acquisition	Acquisition	10.3.30.101	159.203.185.4	80	silverlight	alert
	03/22 22:55:53	any	gate.php	Hypertext Preprocessor PHP File	Acquisition	Acquisition	10.10.17.102	188.209.52.233	80	web-browsing	alert
	03/22 22:55:43	any		US-SSNs	Acquisition	Acquisition	10.10.17.102	204.79.197.200	80	web-browsing	reset-both
	03/22 22:55:38	any		Email Link	Acquisition	Acquisition	10.11.2.102	66.218.85.52	25	smtp-base	alert
	03/22 22:55:38	any	logout.php	Hypertext Preprocessor PHP File	Acquisition	Acquisition	10.11.2.102	118.193.174.133	80	web-browsing	alert
	03/22 22:55:33	any		Email Link	Acquisition	Acquisition	10.11.2.102	74.125.24.27	25	smtp-base	alert
	03/22 22:55:23	any	logout.php	Hypertext Preprocessor PHP File	Acquisition	Acquisition	10.11.2.102	118.193.174.133	80	web-browsing	alert
	03/22 22:55:18	any		Email Link	Acquisition	Acquisition	10.11.2.102	66.218.85.139	25	smtp-base	alert
	03/22 22:55:08	any	logout.php	Hypertext Preprocessor PHP File	Acquisition	Acquisition	10.11.2.102	118.193.174.133	80	web-browsing	alert

30 | © 2022 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 Data Filtering log also displays information for Data Filtering Profiles.

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.

This section describes Data Filtering Profiles.

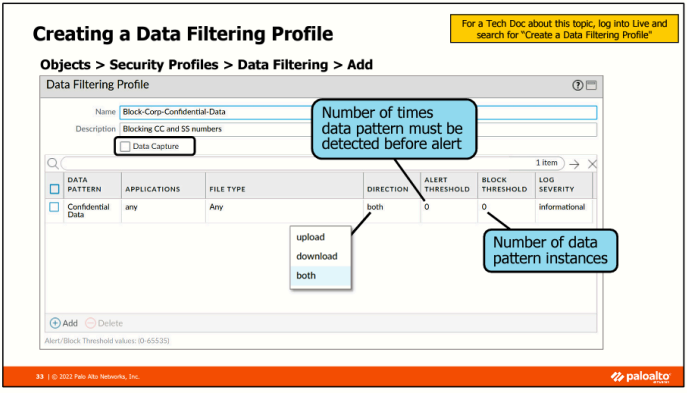


Data Filtering Profiles are used to prevent sensitive, confidential, and proprietary information from leaving your network. Data patterns are used to define the information types that you want the firewall to filter. The data filtering profile enables you to filter on key words, such as a sensitive project name or the word confidential. 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 Pattern: 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: Scans files for specific file properties and values

To enable compliance for standards such as HIPAA, GDPR, Gramm-Leach-Bliley Act, PAN-OS 9.1 supports more than 20 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 to help to reduce the possibility of false positives.



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 might 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 and logs the data that is being blocked by the filter.

View the Data Filtering Log

For a Tech Doc about this topic, log into Live and search for "Review Data Filtering Logs"

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

Monitor > Logs > Data Filtering

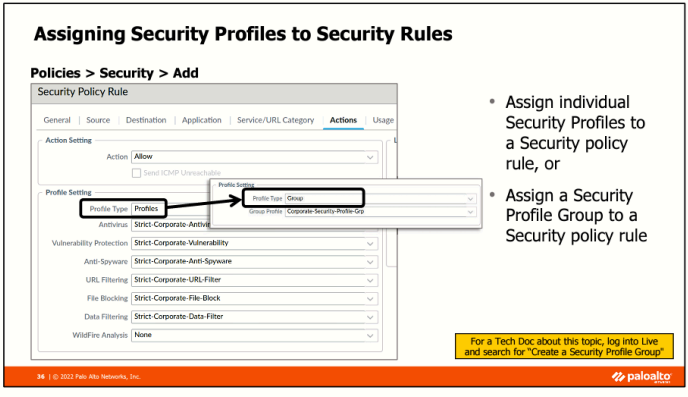
	RECEIVE TIME	CAT	FILE NAME	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	TO PORT	APPLICATION	ACTION
	03/12 21:31:01	any	AMJjTK02zjzkwpOkoN-EWD0	Google Chrome Extension CRX File	Users_Net	Internet	192.168.1.20	142.250.34.2	80	web-browsing	alert
	03/12 18:03:51	any	apachewithsigned.pfx	DER Encoded X509 Certificate	Extranet	Users_Net	192.168.50.80	192.168.1.20	47145	ftp	alert
	03/12 18:03:51	any	apache-selfsigned.crt	PEM Encoded X509 Certificate	Extranet	Users_Net	192.168.50.80	192.168.1.20	56967	ftp	alert
	03/12 18:01:44	any	AOAb1VvObIkRVGlP54MKrl	Google Chrome Extension CRX File	Users_Net	Internet	192.168.1.20	142.250.34.2	80	web-browsing	alert
	03/12 18:01:43	any	XZyR5qQ7gb8FpWW3-n-P3Q	Google Chrome Extension CRX File	Users_Net	Internet	192.168.1.20	173.194.55.108	80	web-browsing	alert

The Data Filtering log display entries for the security policy rules that help prevent sensitive information such as credit card numbers and social security numbers from leaving the area that the firewall protects. 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 Data Filtering Profiles, as necessary. The Data Filtering log also displays information for File Blocking Profiles.

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.

This section describes attaching Security Profiles to Security policy rules.

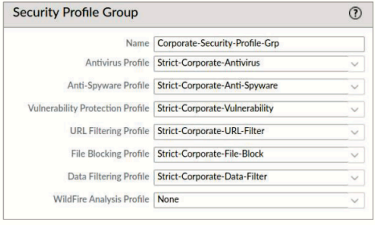
© 2022 Palo Alto Networks, Inc.



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

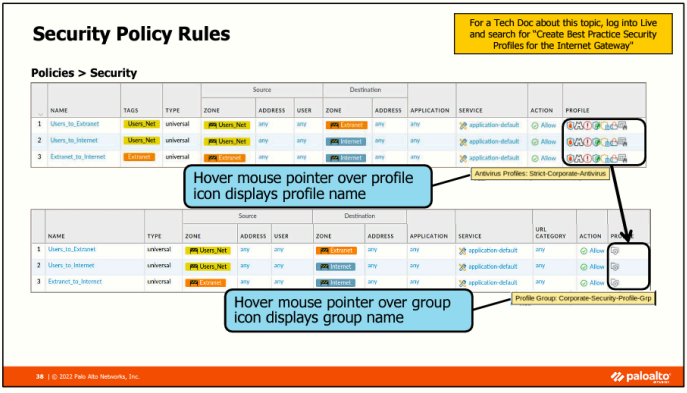


- Add Security Profiles that are commonly used together
- Security Profile Groups simplify Security policy rule administration.

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, Advanced 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.

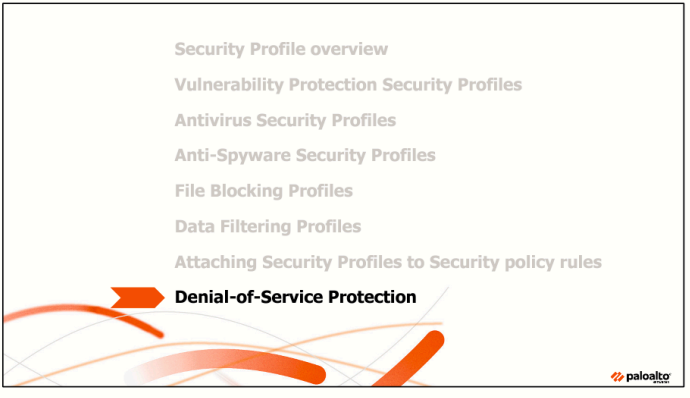
For example, you could create a Security Profile Group that could be applied to all Security policy rules that match traffic inbound from the internet. If a specific Security Profile within the group needs to be modified to create more stringent security checks, the modifications to the Security Profile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

© 2022 Palo Alto Networks, Inc.



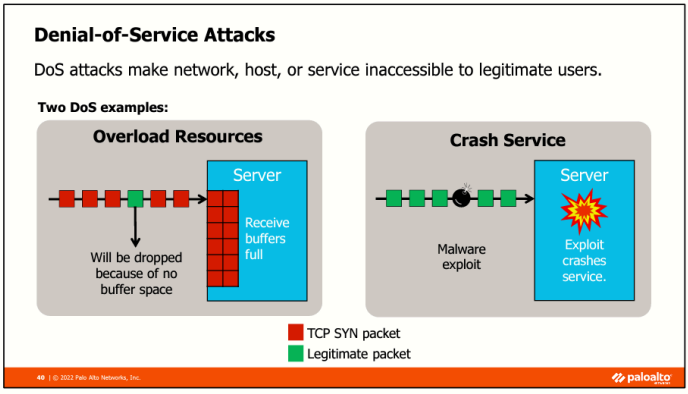
While security policy rules enable you to allow or block traffic on your network, security profiles help you define an allow but scan rule, which scans allowed applications for threats, such as viruses, malware, spyware, and DDOS attacks. When traffic matches the allow rule defined in the security policy, the security profile(s) that are attached to the rule are applied for further content inspection rules such as antivirus checks and data filtering.

You can add security profiles that are commonly applied together to create a Security Profile Group. A Security Profile Group is set of profiles can be treated as a unit and added to security policies in one step or included in security policies by default, if you choose to set up a default security profile group.



This section describes the purpose, operation, and configuration of Zone and DoS Protection Profiles.

© 2022 Palo Alto Networks, Inc.



A denial-of-service (or DoS) attack is meant to overload or shut down a network, host, or service, thus making it inaccessible to users or applications. DoS attacks make services inaccessible by flooding the target with traffic or sending it malware that triggers a crash. In either example, the DoS attack deprives legitimate users access to the service or resource they expected. Though DoS attacks typically do not result in the theft or loss of significant information or other assets, they can cost the victim substantial time and money.

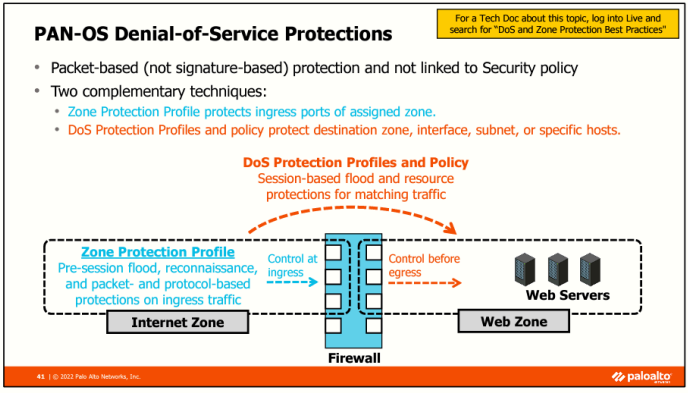
For example, an ICMP flood leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The attack is designed to flood network bandwidth with illegitimate traffic. This attack has been called the *smurf* attack or the *ping of death*.

A TCP SYN flood is depicted in the Overload Resources illustration. A TCP SYN flood continually initiates but never completes the TCP three-way handshake. This behavior continues until all available network buffers are consumed and no buffers remain available for legitimate TCP connections.

The Crash Service illustration depicts another type of DoS attack that exploits vulnerabilities that cause the target system or service to crash. In these attacks, malware is sent that takes advantage of bugs in the target's software that subsequently crash or severely destabilize the target. The "ping of death" attack is an example.

Supplemental Notes

A distributed DoS (or DDoS) attack occurs when multiple systems are used to mount a synchronized DoS attack on a single target. The primary difference between a DDoS attack and a DoS attack is that the target is attacked from many sources at once instead of from a single source.



The firewall provides DoS protections that mitigate Layer 3 and 4 protocol-based attacks. DoS protections use packet header information to detect threats rather than the signatures used by antivirus, anti-spyware, and vulnerability protections. DoS protections are packet-based rather than signature-based. The DoS protections are not linked to Security policy rules and are employed before a Security policy rule.

DoS protection in PAN-OS® software includes two capabilities to mitigate DoS attacks:

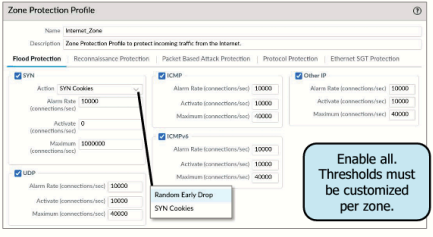
- Zone-based protection: A Zone Protection Profile provides pre-session, broad-based, comprehensive DoS protection at the edge of your network to protect your enterprise from DoS attacks. The Zone Protection Profile acts as a first line of defense for your network. Zone protection is described in this module.
- End host protection: The DoS Protection policy and DoS Protection Profiles provide session-based 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 historically have been prone to DoS attacks.

These two capabilities complement each other. You should deploy them in tandem to achieve the best results against the various DoS attacks observed on the internet today. Zone protection will be enforced before DoS Protection policy if an IP address happens to match both.

Flood Protection Thresholds

- **Alarm**: Threshold to trigger log events to the Threat log
- **Activate**: Threshold to activate protection response
- **Maximum**: Threshold after which all further packets are dropped

Network > Network Profiles > Zone Protection > Add



For a Tech Doc about this topic, log into Live and search for "Flood Protection"

Packets to all ingress interfaces in a zone are sampled at one-second intervals to determine if the collective rate matches an **Alarm Rate**, **Activate**, or **Maximum** threshold.

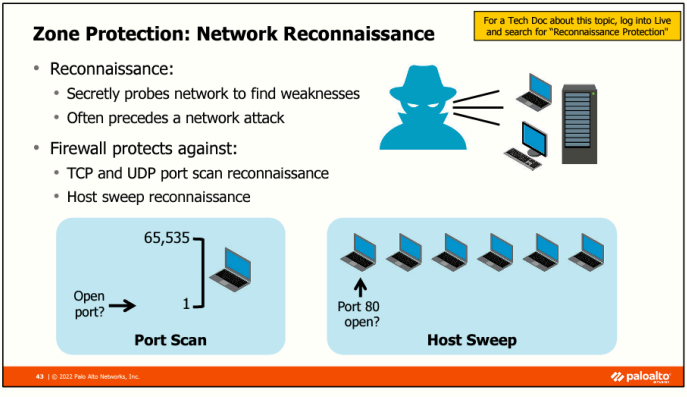
The **Alarm Rate** threshold determines when an alert should be triggered. Triggered alerts are recorded in the Threat log and on the web interface **Dashboard**.

The **Activate** threshold determines when the RED or SYN cookie protection response should be triggered.

After the packet rate exceeds the **Maximum** threshold, all packets that exceed the maximum rate are dropped.

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. However, you also should initially configure an extremely high **Maximum** setting to prevent inadvertent blocking of legitimate traffic. Use a lower **Alarm Rate** setting to help determine what your normal number of cps is, and then set the **Maximum** to a value about 30% higher.

You also can view the data plane monitor log to see your current number of cps and use that value to set your **Alarm Rate** and **Maximum** settings. The CLI operational command is **`less mp-log dp-monitor.log`**. Look for the *New connection establish rate*.



An attacker uses network reconnaissance to gain information about your network vulnerabilities. Reconnaissance activities often precede a network attack.

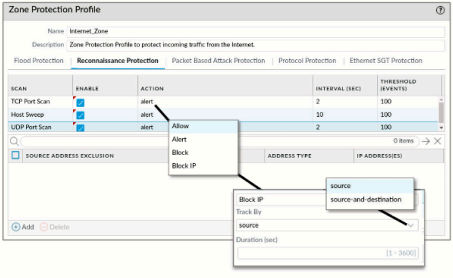
A Zone Protection Profile defends against TCP and UDP port scan and host sweep reconnaissance:

- Port scans discover open ports on a network. A port scanning tool sends requests to a range of port numbers on a host, with the goal of locating an open port to exploit.
- Host sweeps attempt to contact multiple hosts to determine which hosts are running and if specific ports are open and vulnerable.

Enabling Reconnaissance Protection

- Enable port scan and host sweep protection.
- Start with the default **Interval** and **Threshold** values.
- **source-and-destination** in the **Track By** field can block traffic more quickly than can **source**.

Network > Network Profiles > Zone Protection > Add



You should enable reconnaissance protection on any zone that could be the source of a port scan or host sweep. In a Zero Trust deployment, you might enable reconnaissance protection on all zones. Enable reconnaissance protection by selecting the three **Enable** check boxes on the **Reconnaissance Protection** tab.

An action of **Alert**, **Block**, or **Block IP** will ensure that detected events are logged to the Threat log.

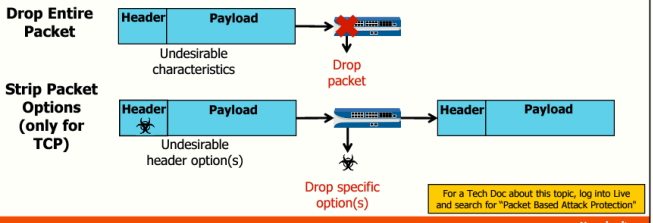
The default values will identify a scan by an uneducated or opportunistic attacker. The default values yield very few false positives, but they will not detect a scan set to occur using a longer interval. An educated or cautious attacker can use a utility such as Nmap with special options to slowly scan to avoid detection. Monitor your Traffic logs and Threat logs to identify your optimal settings.

If you select **Block IP** as the action, then you also must configure the **Track By** and **Duration** settings. **Track By** determines whether the firewall blocks reconnaissance packets based on their source IP address or on their source and destination IP address pair. Selection of **source** means that the firewall drops all packets from a single source to any destination when the number of packets exceeds the threshold for the specified **Duration**. Selection of **source-and-destination** blocks traffic more quickly than does selection of **source**.

Some applications, such as Skype, perform port scans. You will need to monitor the Threat logs and Traffic logs to ensure that your settings are not blocking legitimate traffic.

Packet-Based Attacks

- Zone Protection Profile protects against IP, IPv6, ICMP, ICMPv6, TCP, and UDP packet-based attacks.
- Two protection methods:

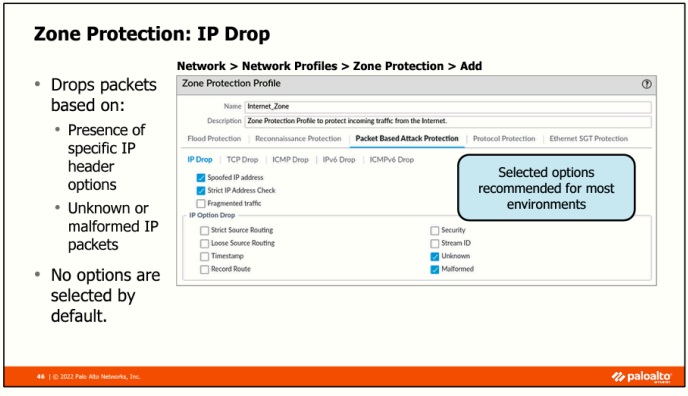


Packet-based attacks take many forms. A Zone Protection Profile checks IP, IPv6, ICMP, ICMPv6, TCP, and UDP packet header parameters. The firewall has two methods to protect against packet-based attacks:

- Drop an entire packet that has undesirable characteristics.
- Strip undesirable options from TCP packet headers.

You select the drop characteristics for each packet type when you configure packet-based attack protection in the Zone Protection Profile. For example, you can drop malformed IP packets, TCP SYN and SYN-ACK packets that contain data, and fragmented ICMP packets. Each packet type has a set of characteristics and options that you select to control whether the firewall drops a packet.

An example of a dangerous TCP option is the **Record Route** option. If this option is set, then the TCP packet header records the IP addresses of the devices a packet traversed to get to its destination. This information can be used to gather network reconnaissance for use in a later attack.



The firewall can drop IP packets that contain specific header options or that are malformed.

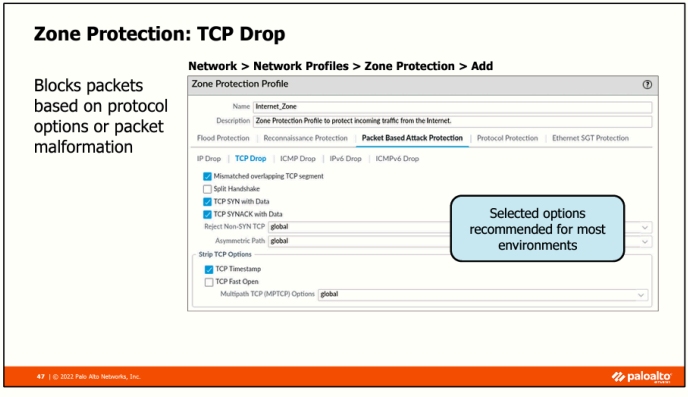
Some packet-based attack protection recommendations apply somewhat equally to all organizations. For example, prevent IP address spoofing in security zones by selecting **Spoofed IP address**. PAN-OS software uses the routing table on the firewall to verify whether the source IP address of the arriving packet is on an interface appropriate for that source IP address.

You also can drop malformed IP addresses by selecting **Strict IP Address Check**, which is a common practice. For example, the firewall will drop packets where the source or destination IP address is the same as the network interface address, is a broadcast address, is a loopback address, is a link-local address, is an unspecified address, or is reserved for future use.

Select the **Unknown** and **Malformed IP** options to have the firewall drop packets that contain specific header options, or unknown or malformed options. For example, the packet includes an unknown option if its protocol field contains an invalid protocol number. Packets are considered malformed if they have incorrect combinations of class, number, and length based on RFCs 791, 1108, 1393, and 2113.

Select the remaining options on an as-needed basis, depending on your security requirements and your types of network traffic.

For assistance with Zone Protection Profiles, use the web interface online help. You can also log into Live and search for “zone protection profiles” or see the Zone Protection Profile information a https://knowledgebase.paloaltonetworks.com/servlet/fileField?entityId=ka10g000000CySkAAK&field=Attachment_1__Body__s for descriptions of each option.



The firewall can drop TCP packets that contain specific header values. The firewall also can strip specific options from TCP packets.

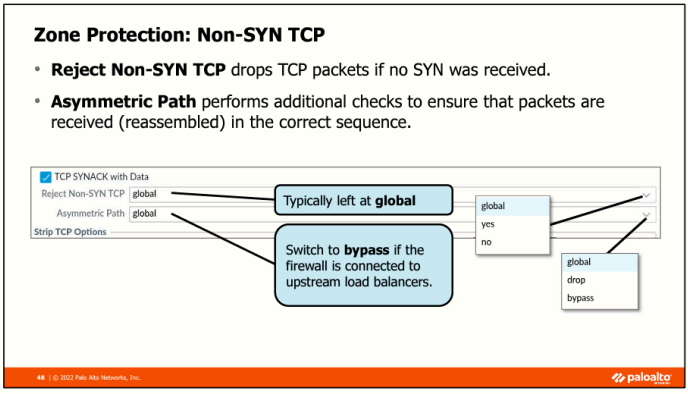
Select the **Mismatched overlapping TCP segment** option to prevent certain evasive techniques from being successful through the firewall. This option generally is recommended for all firewalls.

The **TCP SYN with Data** and **TCP SYNACK with Data** options are selected by default. Dropping of SYN and SYN/ACK packets that contain payload data improves security by blocking malware that could be contained in the payload. This configuration prevents an attacker from extracting unauthorized data before the TCP handshake is completed.

Also select the **TCP Timestamp** option to prevent attacks that use different timestamps on multiple packets for the same sequence number.

Select the remaining options on an as-needed basis, depending on your security requirements and your types of network traffic.

For assistance with Zone Protection Profiles, use the web interface online help. You can also log into Live and search for “zone protection profiles” or see the Zone Protection Profile information a https://knowledgebase.paloaltonetworks.com/servlet/fileField?entityId=ka10g000000CySkAAK&field=Attachment_1__Body__s for descriptions of each option except TCP Fast Open. Use a browser-based search engine to find more information about TCP Fast Open.



The default global behavior of **Reject Non-SYN TCP** is to drop the first TCP packet in a new connection if the packet contains payload data but does not include the SYN flag. If non-SYN TCP packets with data are allowed, File Blocking Profiles can be prevented from working as expected because data can be exfiltrated before a session is established and Content-ID inspection can be performed.

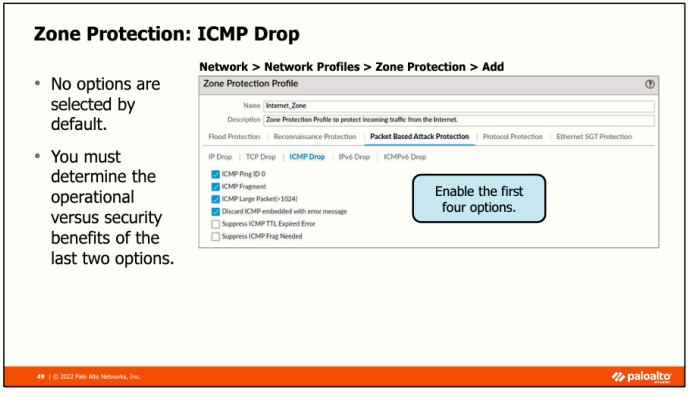
One reason to override the global behavior on a per-zone basis is to accommodate an asymmetric routing path that prevents the firewall from seeing the client-to-server and server-to-client flows. In these rare situations, the same firewall interface might not see the first SYN packet but might see and drop the remaining TCP packets with data. You can select **no** for **Reject Non-SYN TCP** and the firewall will allow these data packets to traverse the zone.

The default behavior of **Asymmetric Path** is to drop TCP packets that fail additional checks that confirm packets are being received in the correct sequence order despite an asymmetric route. If you have asymmetric routes for specific zones and traffic is being incorrectly dropped, then you can set the **Asymmetric Path** option to **bypass** these additional checks.

Supplemental Notes

Use the CLI to see and change the global settings for **Reject Non-SYN TCP** and **Asymmetric Path**:

- **`> show session info`** displays the current global non-SYN TCP setting.
- **`# set deviceconfig setting session tcp-reject-non-syn no`** globally allows non-SYN TCP traffic.
- **`# set deviceconfig setting session tcp-reject-non-syn yes`** globally disables non-SYN TCP traffic.
- **`> show running tcp state | match asymmetric`** displays the current global asymmetric path setting.
- **`# set deviceconfig setting tcp asymmetric-path bypass`** globally disables the additional checks.
- **`# delete deviceconfig setting tcp asymmetric-path`** globally re-enables the additional checks.



ICMP provides network error reporting and probe capabilities as a companion to IP. An ICMP session is identified by the firewall using the *type* and *code* values of the ICMP packet:

- **ICMP Ping ID 0**: Configures the firewall to drop initial ICMP packets with a *type* value of 0. Zero is the *type* value for an echo reply, and no ICMP session should start with an echo reply. This option should be enabled.
- **ICMP Fragment**: Drops ICMP packets requesting fragmentation. There are few legitimate reasons for an ICMP packet to be fragmented. This option should be enabled.
- **ICMP Large Packet (>1024)**: Drops ICMP packets larger than 1,024 bytes. ICMP carries small data payloads that typically are fewer than 1,024 bytes. This option can be enabled to prevent successful "ping of death" attacks.
- **Discard ICMP embedded with error message**: Drops ICMP packets with embedded error messages. These ICMP packets can be safely dropped, so this option should be enabled.
- **Suppress ICMP TTL Expired Error**: Drops ICMP packets that inform an IP packet sender that their IP packet was dropped because its *TTL* value reached 0. Traceroute commonly uses this method to trace the network path to a host. However, the TTL expired message also can be used by malicious users to determine the path to a host. You will need to determine, per zone, if these TTL expired messages create a security problem in your environment. Tracing of the network path to an internal host can be a form of network reconnaissance and thus can be a security risk.
- **Suppress ICMP Frag Needed**: Drops "need to fragment" messages. An IP packet sender can set a *Don't Fragment* flag on an IP packet. The receiver is not allowed to fragment the IP packet even if it must forward the packet on an interface with a small MTU size. In such a case the receiver sends an ICMP "need to fragment" message to the sender. These messages can be used to determine the path to a host. You will need to determine, per zone, if these messages create a security risk in your environment.

Supplemental Notes

A legitimate reason for an ICMP packet to be fragmented is with a custom ping where a large packet size is specified to determine the MTU of an intermediate link that the customer might not control. This type of ping

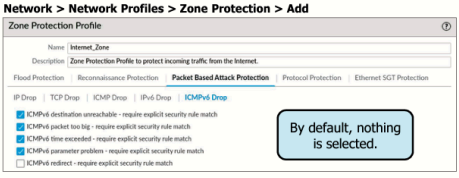
could be useful for testing certain links, such as VPN links.

A network administrator who is not aware that the firewall drops these packets will see packet loss instead of fragmented packets, which might lead them to wrong conclusions.

© 2017-2021 Palo Alto Networks, Inc.

Zone Protection: ICMPv6 Drop

- You typically can safely enable the first four options.
- You must determine the operational versus security benefits of the last option.



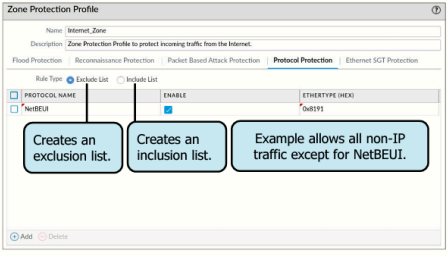
Determine whether to enable any of these settings on a case-by-case basis. The first four options typically are safe and will not result in dropped legitimate traffic. Note that if you select a specific type of ICMPv6 packet, all packets of that type will be dropped by the firewall. However, you can configure Security policy rules to allow all ICMPv6 packets between specific sources and destinations. Use the application name *ipv6-icmp* in the Security policy rule. A Security policy rule will override any Zone Protection Profile settings.

You should understand each **ICMPv6 Drop** option and how to determine whether you should select it. For assistance with Zone Protections, use the web interface online help. You can also log into Live and search for "zone protection profiles" or see the Zone Protection Profile information a https://knowledgebase.paloaltonetworks.com/servlet/fileField?entityId=ka10g000000CySkAAK&field=Attachment_1__Body__s for descriptions of each option.

Zone Protection: Protocol Protection

- Applies only to Layer 2 and virtual wire zones:
  - Firewall normally allows non-IP traffic between these zone types.
- Blocks or allows specific non-IP traffic using Ethertype codes.

Network > Network Profiles > Zone Protection > Add



For a Tech Doc about this topic, log into Live and search for "Protocol Protection"

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

To block specific non-IP protocol traffic, select **Exclude List** and then create a protocol exclusion list. In the example, the firewall allows all non-IP traffic except for NetBEUI traffic.

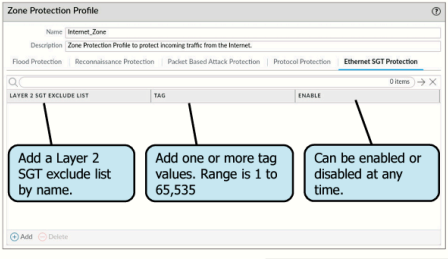
To allow only specific non-IP protocol traffic, select **Include List** and then create a protocol inclusion list. For example, if you want to enable the firewall to pass only EtherTalk packets, then create an include list that contains only Ethertype 0x809B.

© 2022 Palo Alto Networks, Inc.

Zone Protection: Ethernet SGT Protection

- Used if firewall is part of a Cisco TrustSec Network
- Inspects headers with 802.1Q
- Applies only to Layer 2 or virtual wire security group tag (SGT) values
- Drops packet if SGT matches listed configuration

Network > Network Profiles > Zone Protection > Add

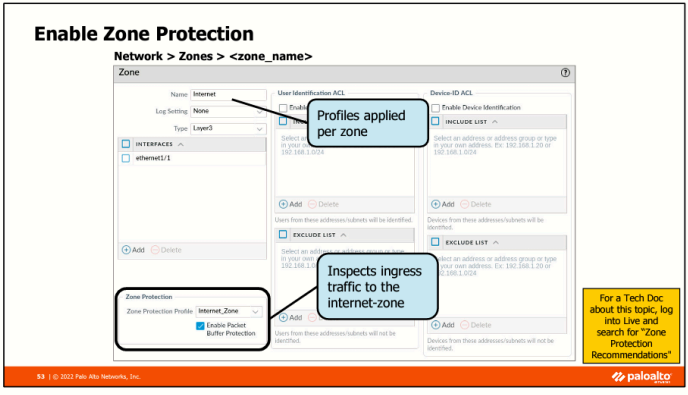


For a Tech Doc about this topic, log into Live and search for "Ethernet SGT Protection"

When your firewall is part of a Cisco TrustSec network, the firewall can now inspect headers with 802.1Q (Ethertype 0x8909) for specific Layer 2 security group tag (SGT) values and drop the packet if the SGT matches the list configured in the Zone Protection Profile attached to the interface.

When configuring Ethernet SGT protection, you enter one or more **Tag** values for the list; range is 1 to 65,535. You can enter individual entries that are a contiguous range of tag values, for example, 100 to 500. You can add up to 100 individual or range tag entries in an exclude list.

You apply the Zone Protection Profile to a security zone configured with a Layer 2 or virtual wire interface. You can view the global counter of packets that the firewall has dropped as a result of all Zone Protection Profiles that employ Ethernet SGT protection by using the CLI command **`show counter global name pan_flow_dos_l2_sec_tag_drop`**.



A Zone Protection Profile is enabled on a per-zone basis. You assign only a single Zone Protection Profile to a zone.

Module Summary

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

- Describe the seven different Security Profile 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 Protection Profile to help mitigate Layer 3 and 4 protocol-based attacks

54 | © 2022 Palo Alto Networks, Inc.

Now that you have completed the module, you should be able to perform the tasks listed.

Additional Resources

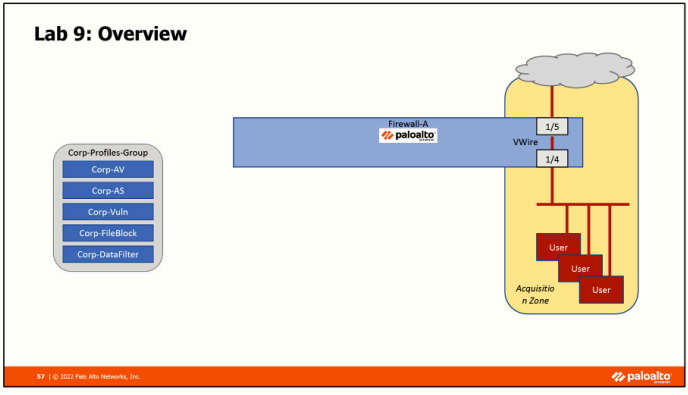
For a digital review of this module, log into Beacon and search for:

"Security Profiles and Security Policies"

© 2022 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. A Zone Protection Profile is applied to which item?
    a. ingress ports
    b. Security policy rules
    c. egress ports
    d. Address Groups
4. Network traffic matches an “allow” rule in the Security policy, but the attached File Blocking Profile is configured with a “block” action. To which two locations will the traffic be logged? (Choose two.)
    a. Threat log
    b. Traffic log
    c. Data Filtering log
    d. Alarms log
5. Which profile type is designed to protect against reconnaissance attacks such as host sweeps and port scans?
    a. Ant-Spyware
    b. Data Filtering
    c. Zone Protection
    d. DoS Protection



Your instructor can provide an overview of the lab environment and the details needed for this lab. See the following page for a list of tasks that you will carry out in this lab.

Lab 9: Blocking Known Threats Using Security Profiles

- Load a baseline configuration
- Generate traffic without profiles and examine logs
- Create Security Profiles
- Create a Security Group
- Apply the Security Group to existing Security policy rules
- Generate traffic with profiles and examine logs

© 2022 Palo Alto Networks, Inc.

Answers to Review Questions

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