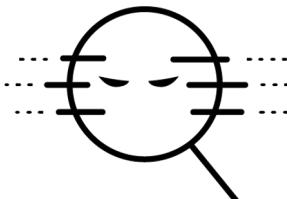


BLOCK THREATS USING SECURITY PROFILES



EDU-210 Version B
PAN-OS® 10.0

VERIFY THAT YOUR ALLOWED TRAFFIC IS SAFE

- Inspect allowed traffic
- Block threats detected by signatures
- Control URL access
- Block unauthorized file transfers
- Detect unknown threats
- Block sensitive data transfers
- Security policy modifications

Learning Objectives

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

- Identify methods to inspect allowed traffic for malicious content
- Block threats detected by known signatures
- Control access to URLs
- Block unauthorized file transfers
- Detect unknown threats
- Block the transfer of sensitive data
- Implement best-practice Security policy settings





Inspect allowed traffic

Block threats detected by signatures

Control URL access

Block unauthorized file transfers

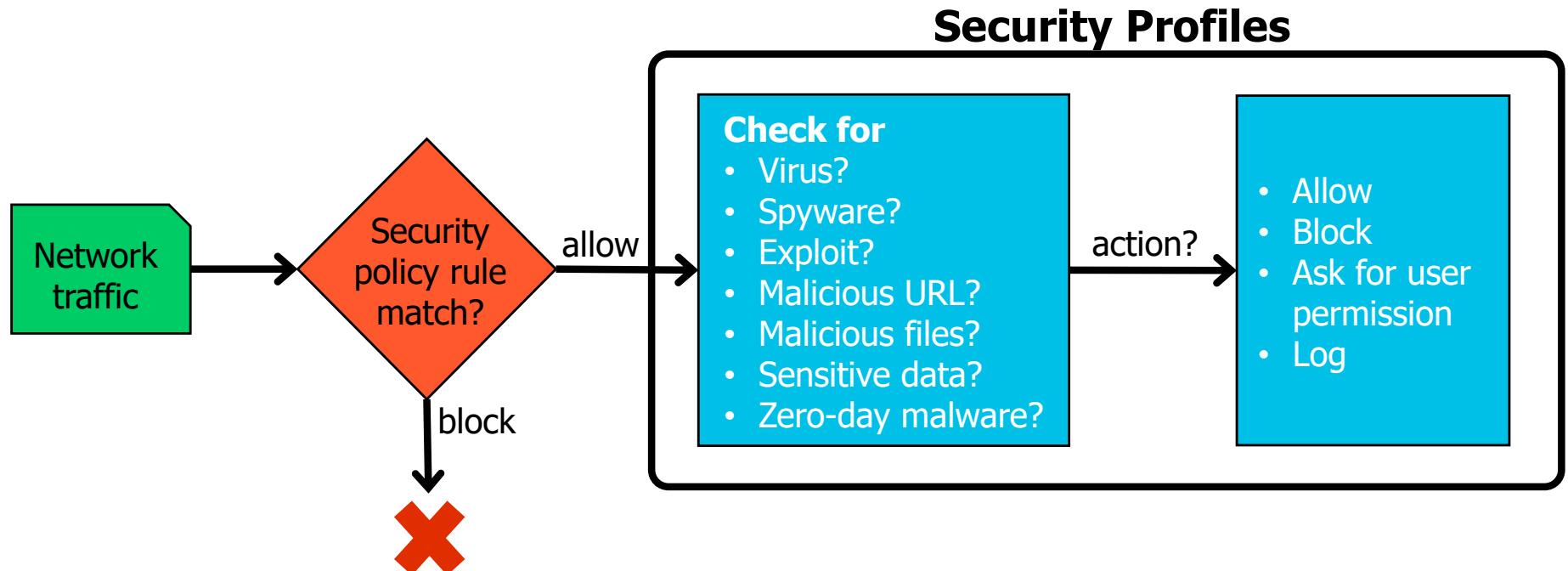
Detect unknown threats

Block sensitive data transfers

Security policy modifications

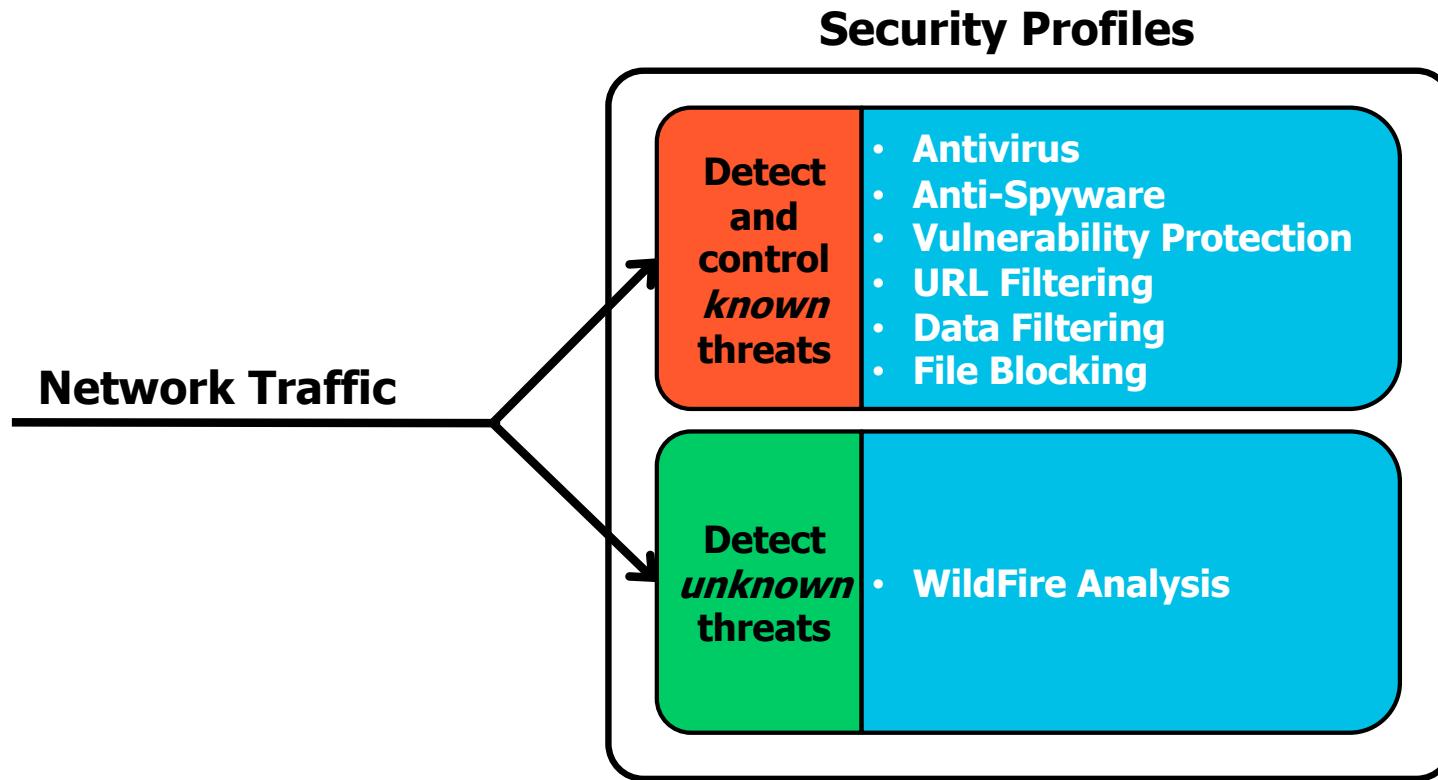
Inspect Allowed Traffic

- Security Profiles implement additional security checks on allowed traffic.
- Add Security Profiles to all allow rules in the Security policy.

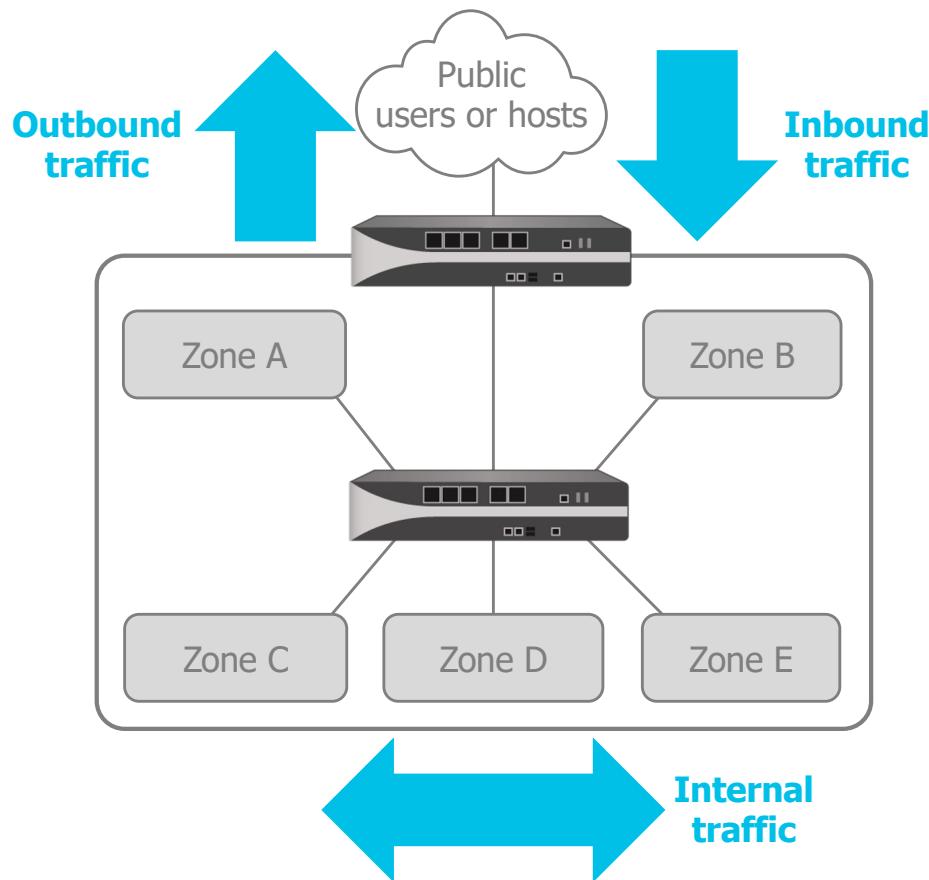


Detect Known and Unknown Threats

Security Profiles detect and control *known* and *unknown* threats.



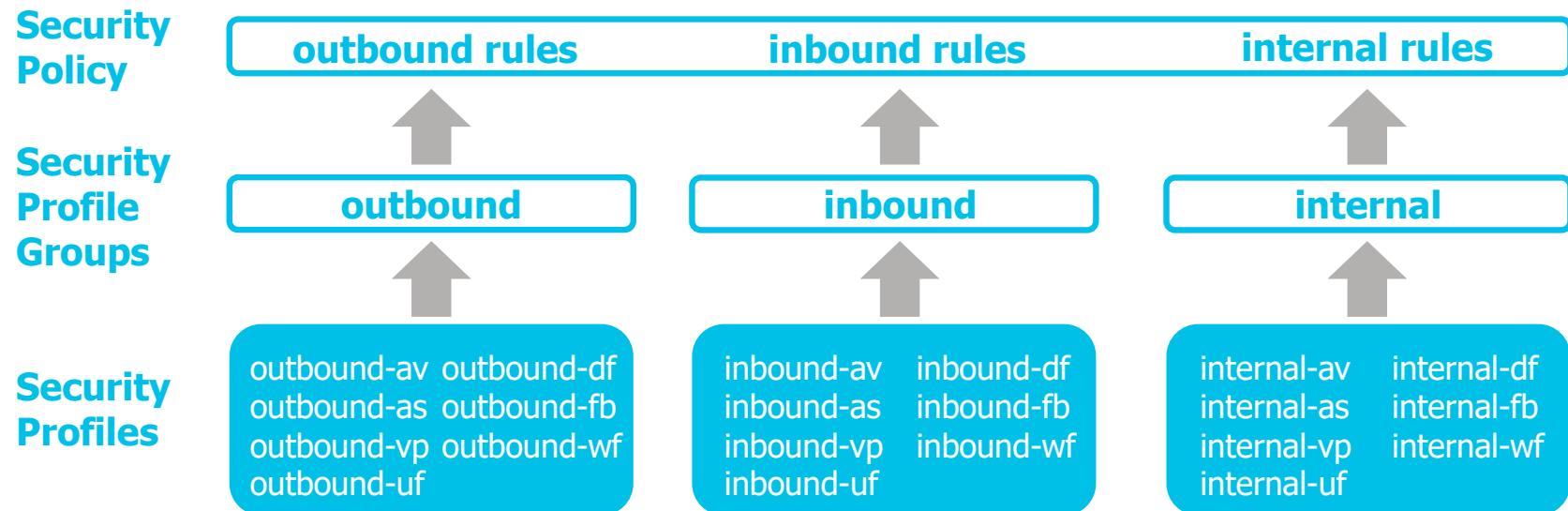
Simplified Traffic Flows



- Traffic flows can be conceptually simplified to:
 - *Outbound* to the internet
 - *Inbound* from the internet
 - *Internal* between internal nodes
- Enables simplified configuration of Security Profiles.

Day-One Security Profile Methodology

- The remainder of this module illustrates a *day-one* best practice configuration.
- This configuration is designed to:
 - Provide application and threat visibility
 - Block threats with minimal or no application downtime



Inspect allowed traffic



Block threats detected by signatures

Control URL access

Block unauthorized file transfers

Detect unknown threats

Block sensitive data transfers

Security policy modifications

Threats Detected by Signatures

- Firewall uses signatures to detect:
 - Known viruses
 - Known spyware
 - Known software exploits
- Updated signatures distributed in content updates:
 - Dynamic update virus signatures:
 - Schedule firewall to check hourly.
 - WildFire updated virus signatures:
 - Schedule firewall to check in real-time.
 - Spyware and exploit signatures:
 - Schedule firewall to check every 30 minutes.

Device > Dynamic Updates

Antivirus Update Schedule

Recurrence	Hourly
Minutes Past Hour	5
Action	download-and-install
Threshold (hours)	[1 - 336]

A content update must be at least this many hours old for the action to be taken.

WildFire Update Schedule

Recurrence	Real-time
------------	-----------

Applications and Threats Update Schedule

Recurrence	Every 30 Minutes
Minutes Past Half-Hour	1
Action	download-and-install
<input type="checkbox"/> Disable new apps in content update	
Threshold (hours)	[1 - 336]

A content update must be at least this many hours old for the action to be taken.

Block Known Viruses: Inbound and Outbound

Objects > Security Profiles > Antivirus

NAME	LOCATION	PACKET CAPTURE	Decoders			
			PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
Outbound-AV		<input type="checkbox"/>	http	default (reset-both)	default (reset-both)	default (reset-both)
			http2	default (reset-both)	default (reset-both)	default (reset-both)
			smtp	reset-both	reset-both	reset-both
			imap	reset-both	reset-both	reset-both
			pop3	reset-both	reset-both	reset-both
			ftp	default (reset-both)	default (reset-both)	default (reset-both)
			smb	default (reset-both)	default (reset-both)	default (reset-both)
Inbound-AV		<input type="checkbox"/>	http	default (reset-both)	default (reset-both)	default (reset-both)
			http2	default (reset-both)	default (reset-both)	default (reset-both)
			smtp	reset-both	reset-both	reset-both
			imap	reset-both	reset-both	reset-both
			pop3	reset-both	reset-both	reset-both
			ftp	default (reset-both)	default (reset-both)	default (reset-both)
			smb	default (reset-both)	default (reset-both)	default (reset-both)

Recommended settings
for outbound and
inbound profiles

Action to take based on
virus signatures
delivered in content
updates

WildFire action to take
based on signatures
delivered by WildFire
subscription

Block Known Viruses: Internal and Alert-Only

Objects > Security Profiles > Antivirus

NAME	LOCATION	PACKET CAPTURE	Decoders			
			PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
Internal-AV		<input type="checkbox"/>	http	default (reset-both)	default (reset-both)	default (reset-both)
			http2	default (reset-both)	default (reset-both)	default (reset-both)
			smtp	default (alert)	default (alert)	default (alert)
			imap	default (alert)	default (alert)	default (alert)
			pop3	default (alert)	default (alert)	default (alert)
			ftp	default (reset-both)	default (reset-both)	default (reset-both)
			smb	default (reset-both)	default (reset-both)	default (reset-both)
Alert-Only-AV		<input type="checkbox"/>	http	alert	alert	alert
			http2	alert	alert	alert
			smtp	default (alert)	default (alert)	default (alert)
			imap	default (alert)	default (alert)	default (alert)
			pop3	default (alert)	default (alert)	default (alert)
			ftp	alert	alert	alert
			smb	alert	alert	alert

Recommended settings for internal and alert-only profiles

Optional, for initial configuration only

Create Antivirus Exceptions

Objects > Security Profiles > Antivirus > Add

The screenshot shows the 'Antivirus Profile' configuration screen. At the top, there are fields for 'Profile Name' (Inbound-AV) and 'Description'. Below these are tabs for 'Action', 'Signature Exceptions' (which is selected), and 'WildFire Inline ML'. A search bar is present above a table. The table has columns for 'THREAT ID' and 'THREAT NAME'. One row is shown: Threat ID 281328 and Threat Name DOS/Virus.eicar_test_file. At the bottom, there is a 'Threat ID' input field containing '281328', an 'Add' button, and a 'PDF/CSV' link.

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

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

Block Known Spyware

Objects > Security Profiles > Anti-Spyware

	NAME	COUNT	POLICY NAME	THREAT NAME	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/> Outbound-AS	Policies: 2		Block-Critical-High-Medium	any	critical,high,medium	reset-both	single-packet
			Default-Low-Info	any	low,informational	default	disable
<input type="checkbox"/> Internal-AS	Policies: 2		Block-Critical-High	any	high,critical	reset-both	single-packet
			Default-Medium-Low-Info	any	medium,low,informational	default	disable
<input type="checkbox"/> Inbound-AS	Policies: 2		Block-Critical-High-Medium	any	critical,high,medium	reset-both	single-packet
			Default-Low-Info	any	low,informational	default	disable
<input type="checkbox"/> Alert-Only-AS	Policies: 1		Alert-All	any	any	alert	disable

- Recommended profiles and settings.
- Attach profiles to Security policy allow rules.

Rules specify actions on detected spyware.

Enable Sinkhole

- Use **sinkhole** action for traffic matching a DNS signature:
 - Default action starting with PAN-OS® 9.0
- Hosts attempting to resolve a malicious domain name are recorded in the Threat log.
- Helps discover hosts possibly infected with spyware.
- Leave **sinkhole** enabled for outbound-as, internal-as, and inbound-as profiles.

Objects > Security Profiles > Anti-Spyware

The screenshot shows the 'Anti-Spyware Profile' configuration screen. At the top, there are fields for 'Profile Name' (Outbound-AS) and 'Description' (Standard anti-spyware profile for all security policies). Below these are tabs for 'Signature Policies', 'Signature Exceptions', 'DNS Policies' (which is selected), and 'DNS Exceptions'. The 'DNS Policies' section contains a table with columns for 'SIGNATURE SOURCE', 'LOG SEVERITY', 'POLICY ACTION', and 'PACKET CAPTURE'. There are eight items listed in the table. One row is highlighted, showing 'default-paloalto-dns' as the source, 'sinkhole' as the policy action, and 'disable' as the packet capture status. A callout box with a black border and a light blue background points to the 'SIGNATURE SOURCE' column, containing the text 'Specific type of DNS signature'.

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
> : External Dynamic Lists			
▽ : Palo Alto Networks Content			
default-paloalto-dns		sinkhole	disable
▽ : DNS Security			
Benign Domains	default (none)	default (allow)	disable

DNS Sinkhole Settings

Sinkhole IPv4: Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)
Sinkhole IPv6: IPv6 Loopback IP (::1)

Anti-Spyware Exceptions

Objects > Security Profiles > Anti-Spyware > Add

Anti-Spyware Profile

Profile Name: Outbound-AS
Description: Standard anti-spyware profile for all security policy rules.

Signature Policies | **Signature Exceptions** | DNS Policies | DNS E...

9986 items → X

ENAB...	ID	THREAT NAME	IP ADDRESS EXEMPTIONS	POLICY	CATEGORY	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	18250	Microsoft Phishing Site Detection	3	Block-Critical-High-Medium	phishing-kit	critical	default (reset-both)	enable
<input type="checkbox"/>	18575	Bartblaze PHP Webshell Traffic Detection		Block-Critical-High-Medium	webshell	medium	default (alert)	enable
<input type="checkbox"/>	18864	FTSRAT Command and Control Traffic Detection				critical	default (reset-both)	enable
<input type="checkbox"/>	18412	CrimsonRAT.Gen Command And Control Traffic				critical	default (reset-both)	enable
<input type="checkbox"/>	18295	Florienzh4x bc0de PHP Webshell Upload Detection	▼	Block-Critical-High-Medium	webshell	critical	default (reset-both)	enable
<input type="checkbox"/>	18896	BabyShark Command and Control Traffic Detection		Block-Critical-High-Medium	spyware	critical	default (reset-both)	enable
<input checked="" type="checkbox"/>	18555	Microsoft Phishing Site		Block-Critical-	phishing-kit	critical	default (reset-both)	enable

Show all signatures [PDF/CSV](#)

Page 1 of 333 | [»](#) [»»](#) [🔍](#) Displaying 1 - 30 / 9986 threats

Can override the action configured in the rules

Click to view or add IP addresses.

Click to override rule's packet capture setting.

Block Known Exploits

Objects > Security Profiles > Vulnerability Protection

Recommended profile types and profile settings

	NAME	COUNT	RULE NAME	THREAT NAME	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	Outbound-VP	Rules: 2	Block-Critical-High-Medium	any	any	critical,high,medium	reset-both	single-packet
<input type="checkbox"/>			Default-Low-Info	any	any	low,informational	default	disable
<input type="checkbox"/>	Inbound-VP	Rules: 2	Block-Critical-High-Medium	any	any	critical,high,medium	reset-both	single-packet
<input type="checkbox"/>			Default-Low-Info	any	any	low,informational	default	disable
<input type="checkbox"/>	Internal-VP	Rules: 2	Block-Critical-High	any	any	critical,high	reset-both	single-packet
<input type="checkbox"/>			Default-Medium-Low-Info	any	any	medium,low,informational	default	disable
<input type="checkbox"/>	Alert-Only-VP	Rules: 1	Alert-All	any	any	any	alert	disable

Rules specify actions on detected threats.

Create Vulnerability Exceptions

Objects > Security Profiles > Vulnerability Protection > Add

Vulnerability Protection Profile

Profile Name: Outbound-VP
Description: Vulnerability Profile for Outbound Traffic

Rules | **Exceptions**

ENAB...	ID	THREAT NAME	IP ADDRESS EXEMPTI...	RULE	CVE	HOST	CATEGORY	SEVERI...	ACTION	PACKET CAPTURE
<input type="checkbox"/>	31673	SCADA ICCP Unauthorized MMS Write Request Attempt	3	Default-Low-Info		server	info-leak	low	default (alert)	enable
<input type="checkbox"/>	31676	SCADA ICCP COTP Disconnect Protocol Error		Default-Low-Info		client	info-leak	low	default (alert)	
<input type="checkbox"/>	31651	SCADA Modbus Server Information Fetch Attempt		Default-Low-Info		server	info-leak	low	default (alert)	
<input type="checkbox"/>	34678	GenBroker SCADA CSService Buffer Overflow Vulnerability		Default-Low-Info		server	overflow	high	default (alert)	

Override the action configured in the rules.

Click to view or add IP addresses.

Click to modify packet capture setting.

Show all signatures PDF/CSV

Page 1 of 486 | Displaying 1 - 30 / 14568 threats

View Threat Information

- Virus, spyware, and exploit threats are logged to the Threat log.
- Either the source or destination can send the malware.

Monitor > Logs > Threat

		RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	TO PORT	APPLICATION	ACTION	SEVERITY
		07/24 21:24:13	vulnerability					89.238.73.97	443	web-browsing	reset-both	medium
		07/24 21:24:09	vulnerability					89.238.73.97	443	web-browsing	reset-both	medium
		07/21 20:08:40	spyware					4.2.2.2	53	dns	drop	medium
		07/20 22:02:09	spyware	malicious-domains-edl	Users_Net	Internet	192.168.1.20	1.1.1.1	53	dns	sinkhole	medium
		07/20 22:01:59	spyware	malicious-domains-edl	Users_Net	Internet	192.168.1.20	4.2.2.2	53	dns	sinkhole	medium
		07/20 22:01:54	spyware		Internet	Internet	192.168.1.20	1.1.1.1	53	dns	sinkhole	medium
		07/20 22:01:44	spyware		Internet	Internet	192.168.1.20	4.2.2.2	53	dns	sinkhole	medium

Includes packet capture (only if an Antivirus, Anti-Spyware, or Vulnerability Protection Profile enables packet capture)

Open Threat Details window.

Inspect allowed traffic

Block threats detected by signatures



Control URL access

Block unauthorized file transfers

Detect unknown threats

Block sensitive data transfers

Security policy modifications

Control URL Access

Objects > Security Profiles > URL Filtering

NAME ^	SITE ACCESS	USER CREDENTIAL SUBMISSION
Alert-Only-UF	Allow Categories (0) Alert Categories (74) Continue Categories (0) Block Categories (0) Override Categories (0)	Allow Categories (0) Alert Categories (0)
default	Allow Categories (58) Alert Categories (4) Continue Categories (0) Block Categories (10) Override Categories (0)	Allow Categories (72)
Outbound-UF	Allow Categories (0) Alert Categories (57) Continue Categories (0) Block Categories (17) Override Categories (0)	Block known-risky categories and alert on all others.
Outbound-Unknown-Blocked-UF	Allow Categories (0) Alert Categories (56) Continue Categories (0) Block Categories (18) Override Categories (0)	Block known-risky categories and the <i>unknown</i> category, alert on all others.

Configure URL Filtering

Objects > Security Profiles > URL Filtering > Add

The screenshot shows the 'URL Filtering Profile' configuration page. At the top, there are fields for 'Profile Name' (Outbound-UF) and 'Description' (Company URL filtering profile for Outbound Traffic). Below these are tabs for 'Categories', 'URL Filtering Settings', 'User Credential Detection', 'HTTP Header Insertion', and 'Inline ML'. The 'Categories' tab is selected. It displays a table of pre-defined categories under 'Pre-defined Categories'. The columns are 'CATEGORY', 'SITE ACCESS', and 'USER CREDENTIAL SUBMISSION'. The rows include:

CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
abortion	allow	block
abused-drugs	allow	block
adult	block	block
alcohol-and-tobacco	allow	block
auctions	allow	block
business-and-economy	allow	block
command-and-control	block	block

* indicates a custom URL category, + indicates external dynamic list
[Check URL Category](#)

- For outbound-uf:
 - Block:
 - command-and-control
 - high-risk
 - malware
 - phishing
 - Consider blocking:
 - copyright-infringement
 - dynamic-dns
 - extremism
 - parked
 - medium-risk
 - new-registered-domain
 - proxy-avoidance-and-anonymizers
 - questionable
- For the outbound-unknown-blocked-uf, also block:
 - unknown

View the URL Filtering Information

URL filtering activity is recorded in the URL Filtering log.

Monitor > Logs > URL Filtering

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	DESTINATION	APPLICATION	ACTION
1	07/17 19:51:42	News-Sites	News-Sites,unknown,unknown	www.foxnews.com/	Users_Net	Internet	192.168.1.20	23.211.49.170	ssl	alert
2	07/17 19:49:40	News-Sites	News-Sites,unknown,unknown	www.foxnews.com/	Users_Net	Internet	192.168.1.20	23.211.49.170	ssl	alert
3	07/17 19:47:42	News-Sites	News-Sites,unknown,unknown	www.foxnews.com/	Users_Net	Internet	192.168.1.20	104.103.29.4	ssl	alert
4	07/17 19:45:38	News-Sites	News-Sites,unknown,unknown	smetrics.foxnews.com/	Users_Net	Internet	192.168.1.20	34.234.106.101	ssl	alert
5	07/17 19:45:38	News-Sites	News-Sites,unknown,unknown	smetrics.foxnews.com/	Users_Net	Internet	192.168.1.20	34.234.106.101	ssl	alert
6	07/17 19:45:27	News-Sites	News-Sites,unknown,unknown	a57.foxnews.com/	Users_Net	Internet	192.168.1.20	23.76.192.83	ssl	alert
7	07/17 19:45:27	News-Sites	News-Sites,unknown,unknown	static.foxnews.com/	Users_Net	Internet	192.168.1.20	23.207.13.234	ssl	alert
8	07/17 19:45:27	News-Sites	News-Sites,unknown,unknown	static.foxnews.com/	Users_Net	Internet	192.168.1.20	23.207.13.234	ssl	alert
9	07/17 19:45:27	News-Sites	News-Sites,unknown,unknown	static.foxnews.com/	Users_Net	Internet	192.168.1.20	23.207.13.234	ssl	alert
10	07/17 19:45:27	News-Sites	News-Sites,unknown,unknown	static.foxnews.com/	Users_Net	Internet	192.168.1.20	23.207.13.234	ssl	alert

Inspect allowed traffic

Block threats detected by signatures

Control URL access

► **Block unauthorized file transfers**

Detect unknown threats

Block sensitive data transfers

Security policy modifications

Block Unauthorized File Transfers

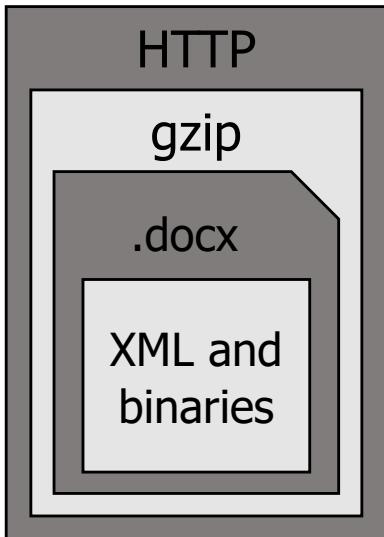
- Profiles detect and control file transfers.
- Can start with alert-only-fb, but other profiles provide protection rather than just logging.

Objects > Security Profiles > File Blocking

<input type="checkbox"/>	NAME	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
<input type="checkbox"/>	Outbound-FB	Block	any	7z, bat, chm, class, cpl, dll, hlp, hta, jar, ocx, pif, scr, torrent, vbe, wsf	both	block
		Alert-All	any	any	both	alert
<input type="checkbox"/>	Inbound-FB	Block	any	7z, bat, chm, class, cpl, hlp, hta, jar, ocx, pif, scr, torrent, vbe, wsf	both	block
		Alert-All	any	any	both	alert
<input type="checkbox"/>	Internal-FB	Block	any	7z, bat, chm, class, cpl, hlp, hta, jar, ocx, pif, scr, torrent, vbe, wsf	both	block
		Alert-All	any	any	both	alert
<input type="checkbox"/>	Alert-Only-FB	Alert-All	any	any	both	alert

Block Multi-Level Encoded Files

Firewall decodes
max of four levels



Objects > Security Profiles > File Blocking > Add

File Blocking Profile

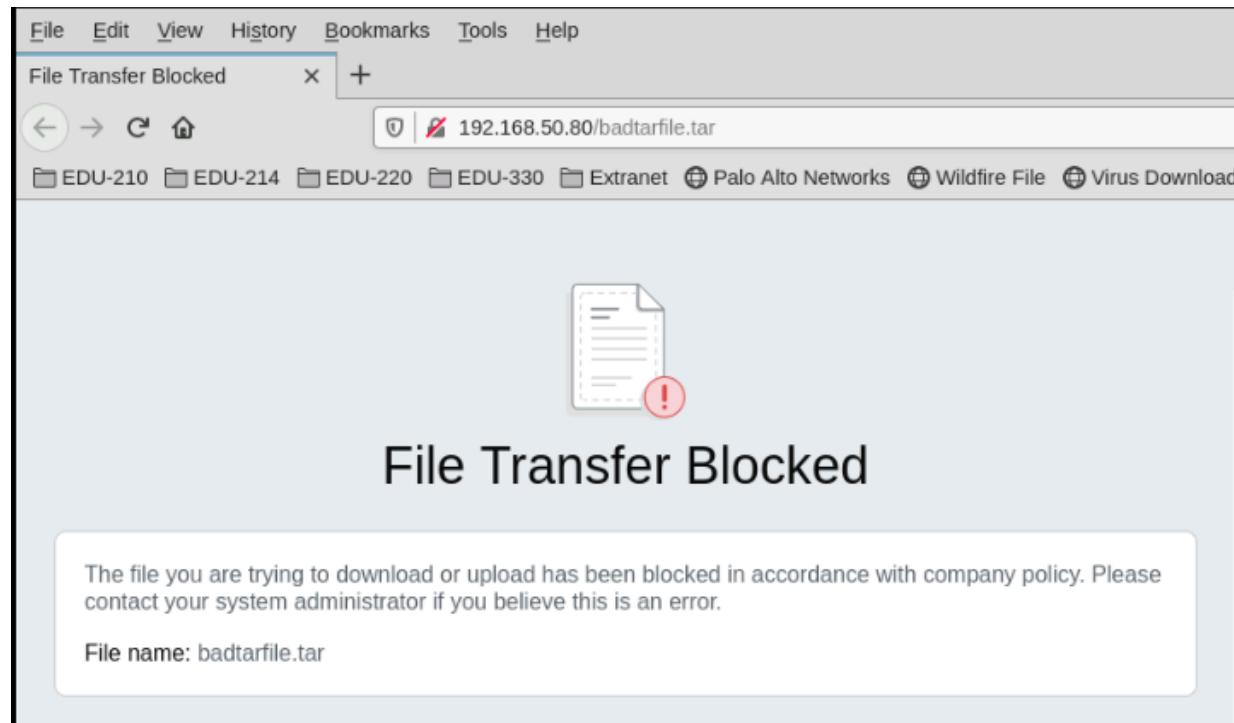
NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
Block-Multiple-Levels	any	Multi-Level-Encoding	both	block

+ Add - Delete

Blocks files encoded more than four levels

Continue Response Page

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



View File Blocking Information

- Data Filtering log records the 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	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	TO PORT	APPLICATION	ACTION
	07/17 17:55:24	private-ip-addresses	webmail.php	Hypertext Preprocessor PHP File	Users_Net	Extranet	192.168.1.20	192.168.50.150	80	squirrelmail	alert
	07/17 17:55:16	private-ip-addresses	login.php	Hypertext Preprocessor PHP File	Users_Net	Extranet	192.168.1.20	192.168.50.150	80	web-browsing	alert
	07/17 17:51:58	computer-and-internet-info	04457f5911080bb0...	Unknown Binary File	Extranet	Internet	192.168.50.150	91.189.91.38	80	apt-get	alert
	07/17 17:51:44	computer-and-internet-info	Packages.gz	GZIP	Extranet	Internet	192.168.50.150	104.207.151.13	80	apt-get	alert
	07/17 17:51:34	computer-and-internet-info	ec430cd4d2899367...	Unknown Binary File	Extranet	Internet	192.168.50.150	91.189.91.39	80	apt-get	alert

Inspect allowed traffic

Block threats detected by signatures

Control URL access

Block unauthorized file transfers

► **Detect unknown threats**

Block sensitive data transfers

Security policy modifications

Detect Unknown Threats

Objects > Security Profiles > WildFire Analysis > Add

<input type="checkbox"/>	NAME	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
<input type="checkbox"/>	default	default	any	any	both	public-cloud
<input type="checkbox"/>	Outbound-WF	Forward-All	any	any	both	public-cloud
<input type="checkbox"/>	Inbound-WF	Forward-All	any	any	both	public-cloud
<input type="checkbox"/>	Internal-WF	Forward-All	any	any	both	public-cloud
<input type="checkbox"/>	Alert-Only-WF	Forward-All	any	any	both	public-cloud

- Determines which files to forward to analyze for unknown threats
- Recommended profile settings illustrated here
- Can start with alert-only-wf to gather log information:
 - Later update to use outbound-wf, inbound-wf, and internal-wf profiles
- Recommend to set **File Types** to **any**:
 - Automatically includes any new file types added to WildFire

Verify Submissions and View Reports

> debug wildfire upload-log show

```
admin@firewall-a> debug wildfire upload-log show

Upload Log disk log rotation size: 2.000 MB.
Public Cloud upload logs:

log: 0, filename: wildfire-test-pe-file.exe
processed 6393 seconds ago, action: upload success
vsys_id: 1, session_id: 196, transaction_id: 3
file_len: 55296, flag: 0x801c, file type: pe
threat_id: 52020, user_id: 0, app_id: 109
from 192.168.1.20/50731 to 52.20.176.145/80
SHA256: d6fbef577a5336641f184ef4a3136889fed8Fd0a37741165f01cd202549b637
```

CLI command to verify successful file upload



View returned report information.

Monitor > Logs > WildFire Submissions

	RECEIVE TIME	FILE NAME	SOURCE ZONE	SOURCE ADDRESS	APPLICATION	RULE	VERDICT	SEVERITY
	07/10 17:04:24	wildfire-test-pe-file.exe	Users_Net	192.168.1.20	web-browsing	Users_to_Internet	malicious	high

Inspect allowed traffic

Block threats detected by signatures

Control URL access

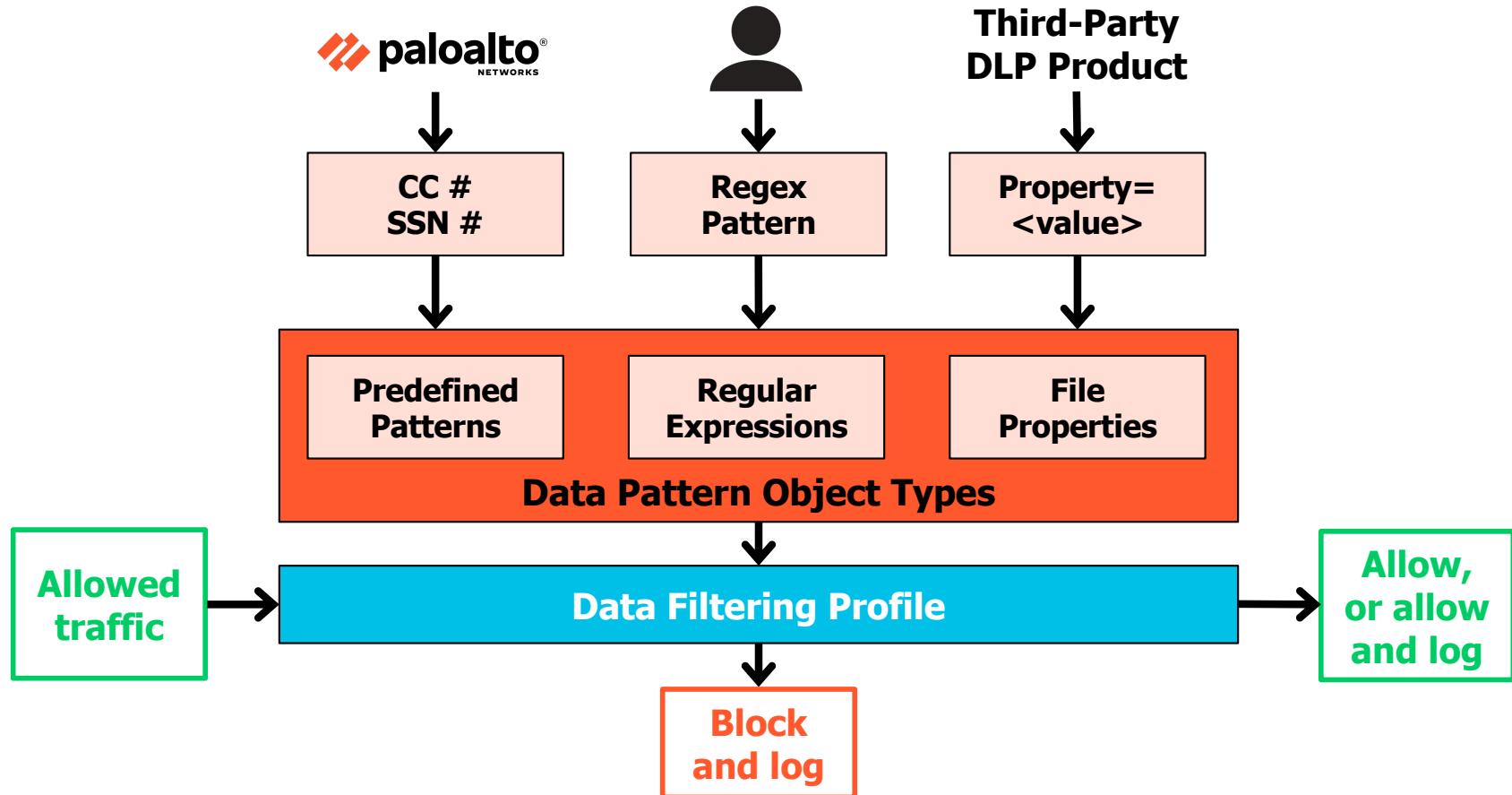
Block unauthorized file transfers

Detect unknown threats

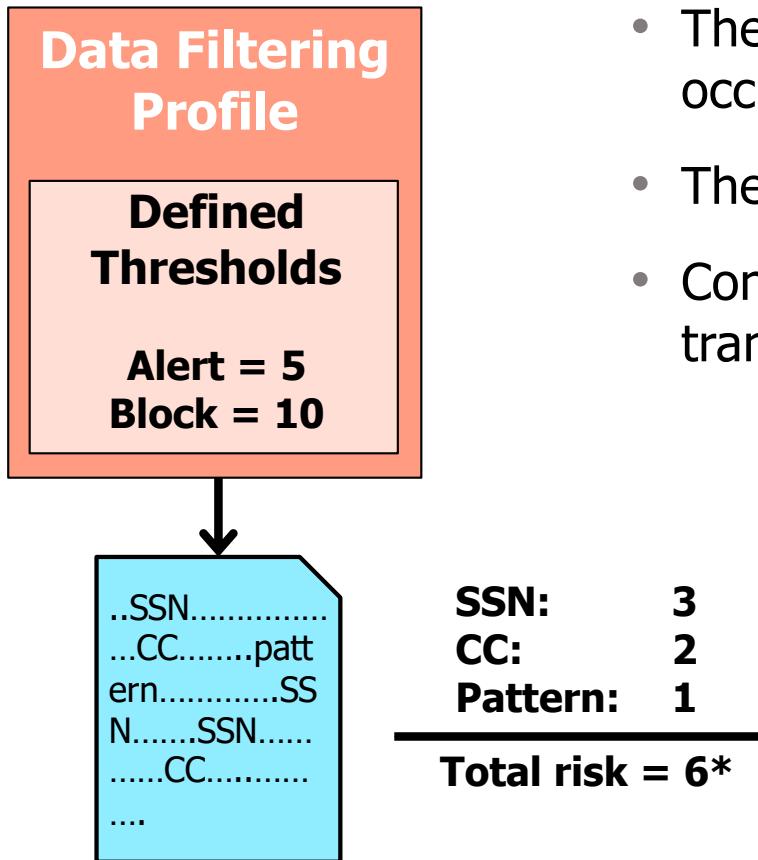
► **Block sensitive data transfers**

Security policy modifications

Block Sensitive Data Transfers



Threshold Values



- The firewall maintains a count of each matching occurrence.
- The firewall compares the count to thresholds.
- Configured thresholds determine when data transfers are logged or blocked.

*Triggers an alert

Configure Custom Data Patterns: Predefined Patterns

Objects > Custom Objects > Data Patterns > Add

Data Patterns

Profile Name: SSN-and-CCN-DP

Description: Data Pattern for US Social Security Numbers and Credit Card Numbers

Pattern Type: Predefined Pattern

<input type="checkbox"/>	NAME	DESCRIPTION	FILE TYPE
<input type="checkbox"/>	Social Security Numbers	US Social Security Numbers pattern	Any
<input type="checkbox"/>	Social Security Numbers (without dash separator)	US Social Security Numbers pattern without dash	Any
<input type="checkbox"/>	Credit Card Numbers	US Credit Card Numbers pattern	Any

NAME
<input checked="" type="checkbox"/> Any
<input type="checkbox"/> HTML
<input type="checkbox"/> Microsoft Office Documents
<input type="checkbox"/> Microsoft Excel
<input type="checkbox"/> Microsoft Excel 97-2004
<input type="checkbox"/> Microsoft PowerPoint
<input type="checkbox"/> Microsoft PowerPoint 97-2004
<input type="checkbox"/> Microsoft Word
<input type="checkbox"/> Microsoft Word 97-2004

Configure Custom Data Patterns: Regular Expressions

Objects > Custom Objects > Data Patterns > Add

Data Patterns

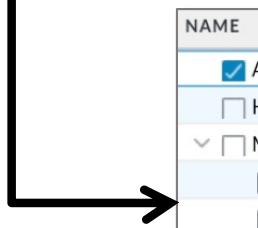
NAME	FILE TYPE	DATA PATTERN
<input type="checkbox"/> Engineering Specs	Any	Engineering (S) (s)pecs:[0-9]+

Pattern Type: Regular Expression

Available File Types:

- Any
- HTML
- Microsoft Office Documents
 - Microsoft Excel
 - Microsoft Excel 97-2004
 - Microsoft PowerPoint
 - Microsoft PowerPoint 97-2004
 - Microsoft Word
 - Microsoft Word 97-2004

Action Buttons: Add Delete Clone



Configure Custom Data Patterns: File Properties

Objects > Custom Objects > Data Patterns > Add

Data Patterns

Profile Name Internal-Filters

Description Data Pattern Profile for Internal Filtering

Pattern Type File Properties

NAME	FILE TYPE	FILE PROPERTY	PROPERTY VALUE
Word Confidential	Microsoft Word	Keywords/Tags	Confidential
Excel Proprietary	Microsoft Excel	Keywords/Tags	Proprietary
PDF Confidential	Adobe PDF	Sensitivity	Confidential

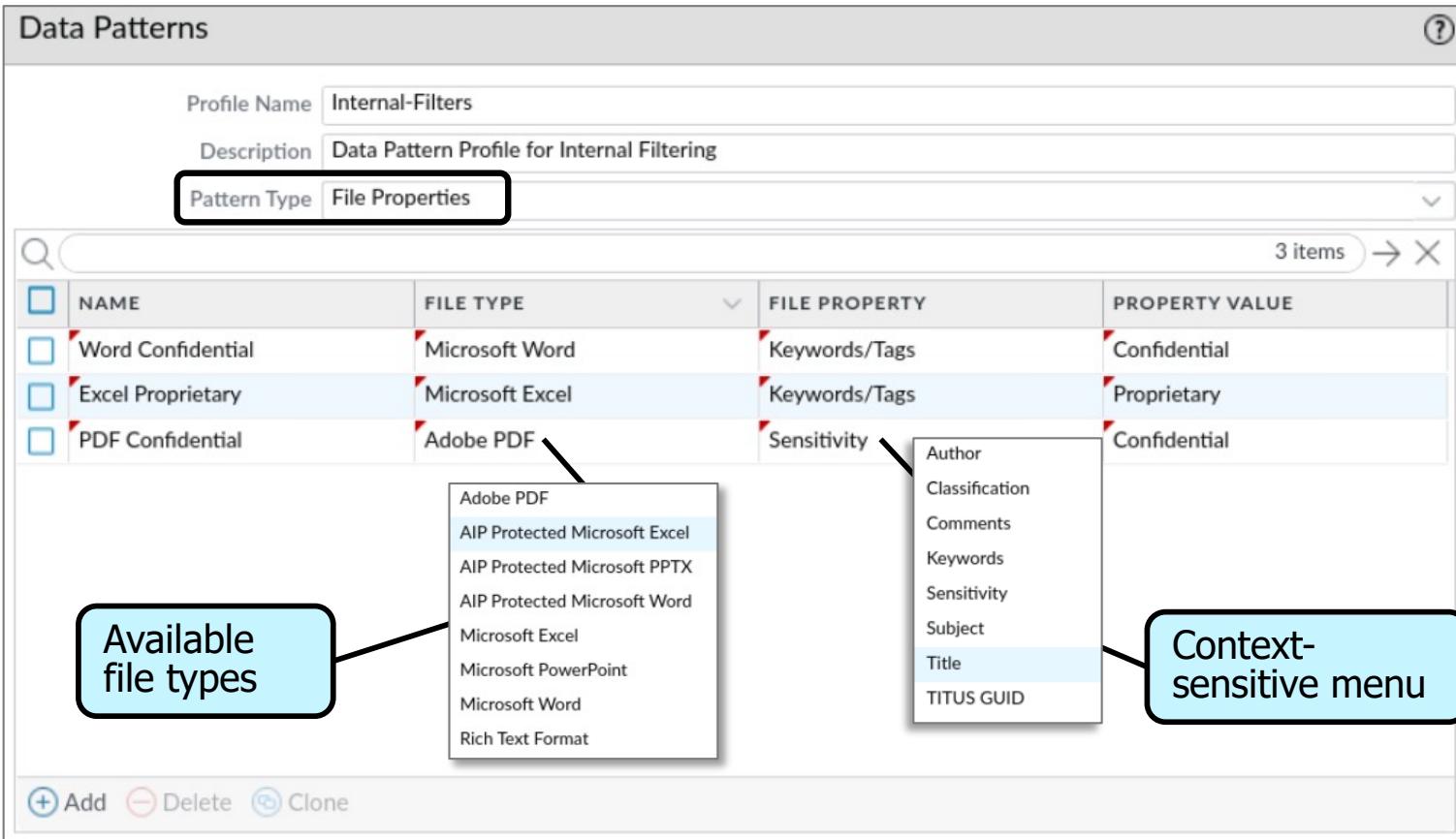
Available file types

Context-sensitive menu

Adobe PDF
AIP Protected Microsoft Excel
AIP Protected Microsoft PPTX
AIP Protected Microsoft Word
Microsoft Excel
Microsoft PowerPoint
Microsoft Word
Rich Text Format

Author
Classification
Comments
Keywords
Sensitivity
Subject
Title
TITUS GUID

+ Add - Delete ⚡ Clone



Configure a Data Filtering Profile

Objects > Security Profiles > Data Filtering > Add

Data Filtering Profile

Profile Name: Outbound-DF
Description: Outbound data filtering profile
 Data Capture

DATA PATTERN	APPLICATIONS	FILE TYPE	DIRECTION	ALERT THRESHOLD	BLOCK THRESHOLD	LOG SEVERITY
Internal-Filters	any	Any	both	1	1	high
Proprietary-Data-Pattern	any	Any	both	1	1	medium
SSN-and-CCN-DP	any	Any	both	2	4	critical

[+ Add](#) [Delete](#)

Alert/Block Threshold values: (0-65535)

Enable for increased visibility.

upload
download
both

critical
high
informational
low
medium

3 items →

<input type="checkbox"/> Adobe PDF
<input type="checkbox"/> AIP Protected Microsoft Excel
<input type="checkbox"/> AIP Protected Microsoft PPTX
<input type="checkbox"/> AIP Protected Microsoft Word
<input checked="" type="checkbox"/> Any
<input type="checkbox"/> HTML
<input type="checkbox"/> Microsoft Office Documents
<input type="checkbox"/> Microsoft Excel
<input type="checkbox"/> Microsoft Excel 97-2004
<input type="checkbox"/> Microsoft PowerPoint
<input type="checkbox"/> Microsoft PowerPoint 97-2004
<input type="checkbox"/> Microsoft Word
<input type="checkbox"/> Microsoft Word 97-2004
<input type="checkbox"/> Rich Text Format

Protect Access to Data Filtering Log Data

Device > Setup > Content-ID > Manage Data Protection

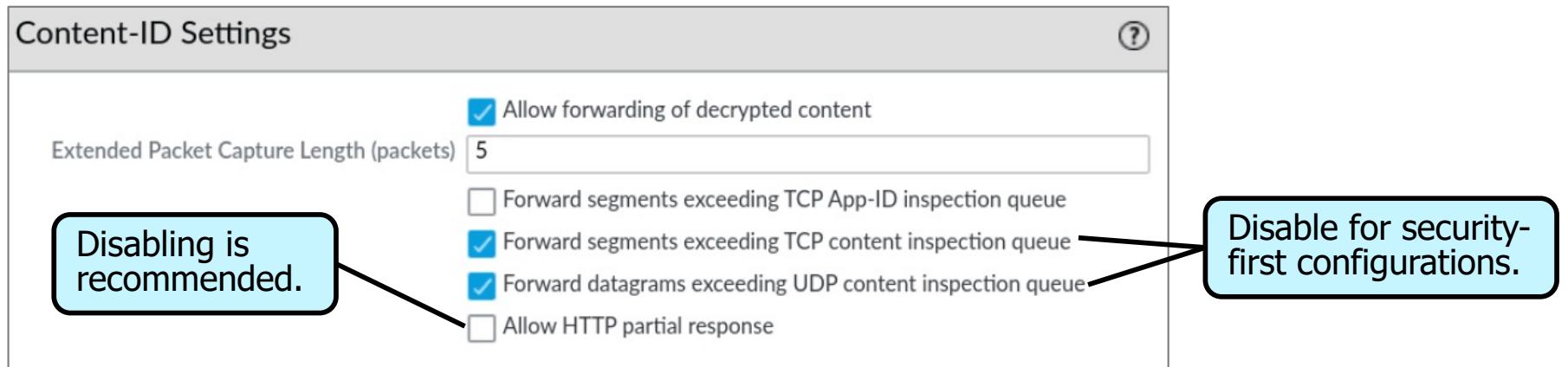
The screenshot shows a 'Manage Data Protection' dialog box. At the top, it says 'Manage Data Protection' and has a question mark icon. Below that, there's a dropdown menu labeled 'Action' set to 'Set Password'. Underneath are two password input fields: 'New Password' and 'Confirm New Password', both showing a series of six dots. At the bottom are two buttons: a blue 'OK' button and a white 'Cancel' button.

- Sensitive data (matched to a pattern) is contained in Data Filtering packet captures.
- You must password-protect packet capture data:
 - Minimum length of six characters
 - If no password is configured, then no packet capture occurs.

Disable the HTTP “Accept-Ranges” Option

- HTTP Accept-Ranges option enables browsers to request partial data transfers.
- If data filtering is configured, disable **Allow HTTP partial response**.
- Prevents browsers from attempting to restart a terminated data transfer.

Device > Setup > Content-ID > Content-ID Settings



View the Data Filtering Log

Monitor > Logs > Data Filtering

		RECEIVE TIME	CATEGORY	FILE NAME	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	TO PORT	APPLICATION	ACTION
		07/17 17:55:24	private-ip-addresses	webmail.php	Hypertext Preprocessor PHP File	Users_Net	Extranet	192.168.1.20	192.168.50.150	80	squirrelmail	alert
		07/17 17:55:16	private-ip-addresses	login.php	Hypertext Preprocessor PHP File	Users_Net	Extranet	192.168.1.20	192.168.50.150	80	web-browsing	alert
		07/17 17:51:58	computer-and-internet-info	04457f5911080bb0...	Unknown Binary File	Extranet	Internet	192.168.50.150	91.189.91.38	80	apt-get	alert

- Use log information to look for unauthorized data transfers.
- Which hosts are involved?
- Use the packet capture to see the sensitive data.
- Packet captures are password-protected:
 - Manage the password here.

Device > Setup > Content-ID



Inspect allowed traffic

Block threats detected by signatures

Control URL access

Block unauthorized file transfers

Detect unknown threats

Block sensitive data transfers

Security policy modifications

Configure Security Policy Rule Tags and Descriptions

- Create tags based on traffic direction.
- Tag your Security policy rules.
- Add a description to your rules.

Objects > Tags

	NAME	LOCATION	COLOR
	Sanctioned	Predefined	Olive
	empty	Predefined	
	Users_Net		Yellow
	Extranet		Orange
	Internet		Blue
	Danger		Red

Policies > Security

NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION
			ZONE	ADDRESS	USER	ZONE	ADDRESS				
1	Users_to_Extranet	universal	Users_Net	any	any	Extranet	any	any	any	any	Allow
2	Users_to_Internet	universal	Users_Net	any	any	Internet	any	dns ping ssl web-browsing	application-default	any	Allow
3	Extranet_to_Internet	universal	Extranet	any	any	Internet	any	any	application-default	any	Allow

Force Use of Per-Rule Tag, Description, and Audit Comments

Device > Setup > Management > Policy Rulebase Settings

The screenshot shows two windows side-by-side. On the left is the 'Policy Rulebase Settings' window, which contains a list of configuration options. A callout bubble labeled 'Not selected by default' points to the first option: 'Require Tag on policies'. The other three options are checked: 'Require description on policies', 'Fail commit if policies have no tags or description', and 'Require audit comment on policies'. Below this list are sections for 'Audit Comment Regular Expression' and 'Policy Rule Hit Count' and 'Policy Application Usage'. On the right is the 'Security Policy Rule' configuration window, showing a 'General' tab with a policy named 'Users_to_Internet' (Rule Type: universal (default), Description: Allows hosts in Users_Net zone to access Internet). The 'Tags' section shows 'Users_Net' and 'Internet' assigned. A callout bubble labeled 'View audit comment history.' points to the 'Audit Comment Archive' link at the bottom of the window.

Policy Rulebase Settings

- Require Tag on policies
- Require description on policies
- Fail commit if policies have no tags or description
- Require audit comment on policies

Audit Comment Regular Expression

Policy Rule Hit Count

Policy Application Usage

Not selected by default

Security Policy Rule

General | Source | Destination | Application

Name: Users_to_Internet

Rule Type: universal (default)

Description: Allows hosts in Users_Net zone to access Internet

Tags: Users_Net, Internet

Audit Comment Archive

Configure Security Profile Groups

Objects > Security Profile Groups

	NAME	LOCATION	ANTIVIRUS PROFILE	ANTI-SPYWARE PROFILE	VULNERABILITY PROTECTION PROFILE	URL FILTERING PROFILE	FILE BLOCKING PROFILE	DATA FILTERING PROFILE	WILDFIRE ANALYSIS PROFILE
<input type="checkbox"/>	Outbound-SG		Outbound-AV	Outbound-AS	Outbound-VP	Outbound-UF	Outbound-FB	Outbound-DF	Outbound-WF
<input type="checkbox"/>	Inbound-SG		Inbound-AV	Inbound-AS	Inbound-VP		Inbound-FB	Inbound-DF	Inbound-WF
<input type="checkbox"/>	Internal-SG		Internal-AV	Internal-AS	Internal-VP		Internal-FB	Internal-DF	Internal-WF

- Create three Security Profile groups:
 - outbound, inbound, internal
- This configuration *blocks* malware.
- **Note:** Only **outbound** includes a URL Filtering Profile.

Attach Security Policy Groups to Policy Rules

Attach *inbound*, *outbound*, and *internal* Security policy groups to rules.

Policies > Security

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE
				ZONE	ADDRESS	USER	ZONE	ADDRESS					
1	Users_to_Extranet	Users_Net Extranet	universal	Users_Net	any	any	Extranet	any	any	any	any	Allow	
2	Users_to_Internet	Users_Net Internet	universal	Users_Net	any	any	Internet	any	dns ping ssl web-brow...	application-default	any	Allow	

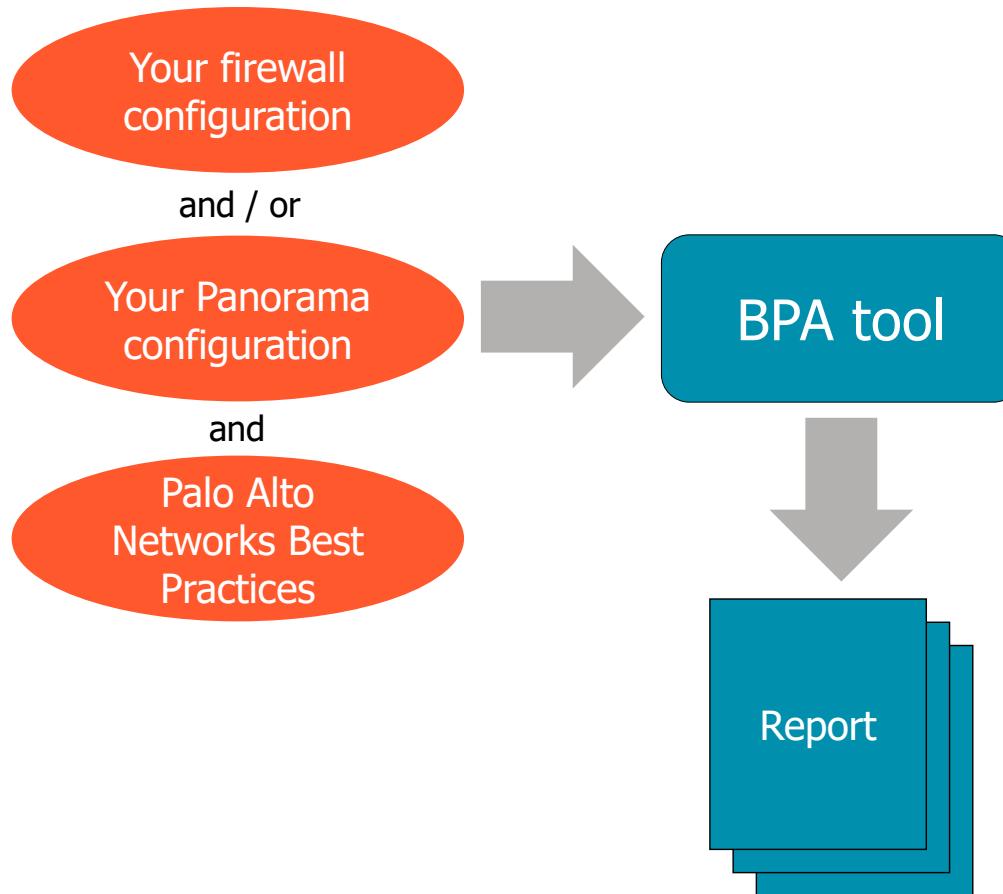
Optional Initial Configuration

Objects > Security Profile Groups

<input type="checkbox"/>	NAME	LOCATION	ANTIVIRUS PROFILE	ANTI-SPYWARE PROFILE	VULNERABILITY PROTECTION PROFILE	URL FILTERING PROFILE	FILE BLOCKING PROFILE	DATA FILTERING PROFILE	WILDFIRE ANALYSIS PROFILE
<input type="checkbox"/>	Outbound-SG		Alert-Only-AV	Alert-Only-AS	Alert-Only-VP	Alert-Only-UF	Alert-Only-FB	Alert-Only-DF	Alert-Only-WF
<input type="checkbox"/>	Inbound-SG		Alert-Only-AV	Alert-Only-AS	Alert-Only-VP		Alert-Only-FB	Alert-Only-DF	Alert-Only-WF
<input type="checkbox"/>	Internal-SG		Alert-Only-AV	Alert-Only-AS	Alert-Only-VP		Alert-Only-FB	Alert-Only-DF	Alert-Only-WF

- Alternate configuration if you are concerned about false positives:
 - Only sends malware *alerts*. It does *not* block malware.
 - Use logs and reports to determine legitimate traffic.
 - Later switch to Security Profile groups that block illegitimate traffic.

How Good Is Your Configuration?



- Palo Alto Networks provides the Best Practice Assessment tool.
- Compares your configuration to best practices
- Generates a report, makes recommendations
- Compares reports over time to track prevention feature adoption
- Available only for firewalls associated with your Support account

Module Summary

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

- Identify methods to inspect allowed traffic for malicious content
- Block threats detected by known signatures
- Control access to URLs
- Block unauthorized file transfers
- Detect unknown threats
- Block the transfer of sensitive data
- Implement best-practice Security policy settings



Questions



Lab 18: Blocking Threats with Security Profiles

- Generate Traffic Without Security Profiles
- Modify Existing Security Profiles
- Create a Vulnerability Security Profile
- Create a File Blocking Profile
- Create Data Filtering Profiles
- Create a Security Profile Group
- Apply a Security Profile Group to Security Policy Rules
- Generate Attack Traffic with Security Profiles
- Create and Apply Tags
- Enforce Rule Tags and Description Requirements
- Test the Rule Requirements



**Protecting our
digital way
of life.**