

CONTENT-ID



EDU-210 Version A
PAN-OS® 9.0

REAL-TIME PREVENTION

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

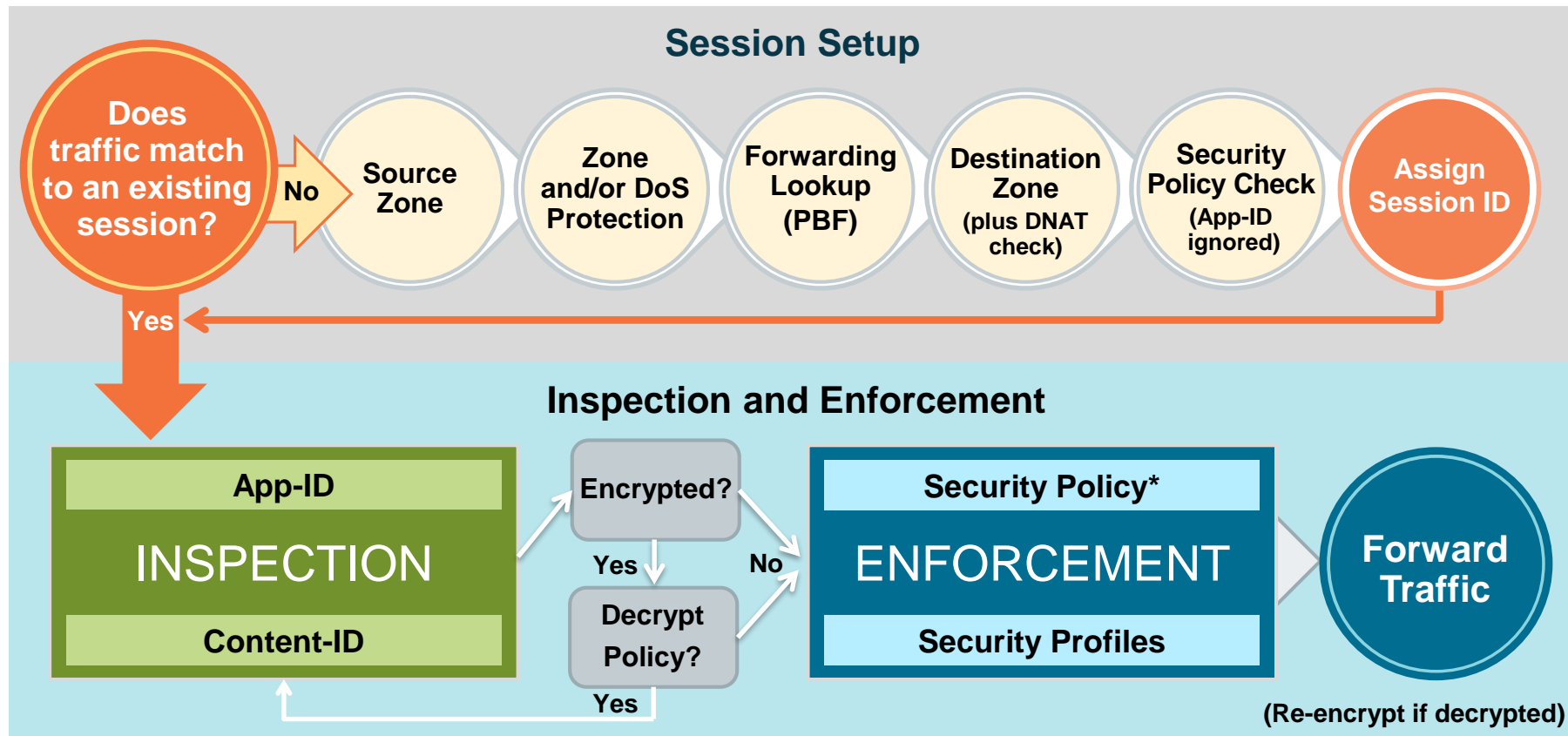
Agenda

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



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

Flow Logic of the Next-Generation Firewall



* Policy check relies on pre-NAT IP addresses



Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

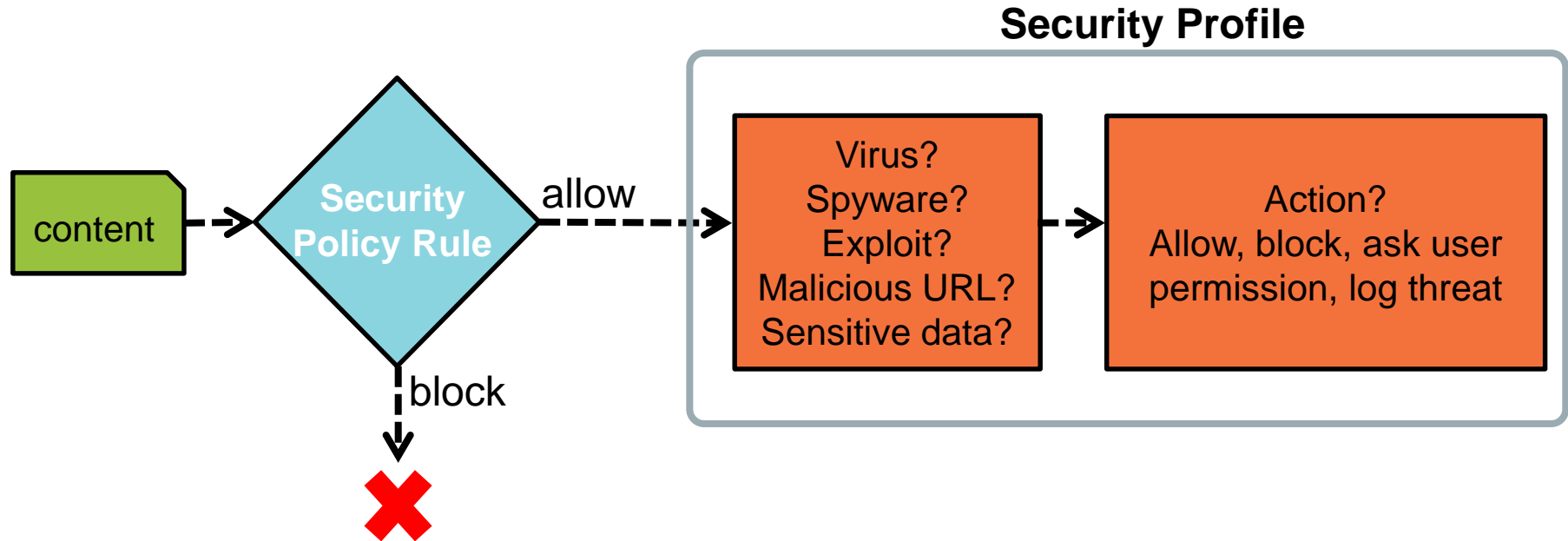
Denial-of-service protection

Content-ID

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

Security Policy with Security Profiles

- Security Profiles implement additional security checks on allowed traffic.



Security Profile Types

Policies > Security

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



Antivirus



Anti-Spyware



Vulnerability Protection



URL Filtering



File Blocking



Data Filtering



WildFire Analysis



Security Profile Group

Threat Log

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

Monitor > Logs > Threat

Click a column header to change number of displayed columns.

	Receive Time	Type	Name	From Zone	To Zone	Source address	Destination address	To Port	Applicati...	Action	Severity	File Name	URL
	02/20 01:05:23	spyware	Suspicious HTTP Evasion Found	danger	danger	10.12.1.101	79.133.57.13				informational		tischlerei-creine...
	02/20 01:05:15	spyware	Suspicious HTTP Evasion Found	danger	danger	10.12.1.101	194.58.100.59				informational		evastrutzmann...
	02/20 01:05:10	virus	TrojanSpy/Win32....	danger	danger	10.12.1.101	74.208.248.199				medium	fix832922.ms	
	02/20 01:05:08	spyware	Suspicious HTTP	danger	danger	10.5.3.101	85.13.133.73				informational		abdellatifosman...
	02/20 01:05:06			danger	danger	10.5.3.101	72.52.179.2	80	web-browsing	reset-server	informational		brandsoutlet.ir/...
	02/20 01:05:05			danger	danger	10.5.3.101	185.23.21.18	80	web-browsing	alert	medium	89yg7g87byi	
	02/20 01:05:04			danger	danger	10.5.3.101	210.1.60.27	80	web-browsing	reset-server	informational		elivo.pl/Y2hNDK...
	02/20 01:05:03			danger	danger	192.168.0.2	112.137.162.1...	80	web-browsing	drop	medium	89yg7g87byi	
	02/20 01:05:02			danger	danger						critical	controller.p...	

Includes packet capture

Open Threat Details window.



Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection

Default Vulnerability Protection Security Profiles

Objects > Security Profiles > Vulnerability Protection

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

Default (read-only) profiles

Rules specify actions on detected events.

To create customized profile actions:

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

+ Add - Delete Clone PDF/CSV

Vulnerability Protection Profile Rules

Objects > Security Profiles > Vulnerability Protection > Add

The screenshot displays the 'Vulnerability Protection Rule' configuration window. The 'Rule Name' is 'Profile Rule 1'. The 'Threat Name' is 'any'. The 'Action' is 'Default'. The 'Host Type' is 'any'. The 'Packet Capture' is 'disable'. The 'Category' is 'any'. The 'Severity' is 'any (All severities)'. The 'Rules' list on the left shows 'Default', 'Allow', 'Alert', 'Drop', 'Reset Client', 'Reset Server', 'Reset Both', and 'Block IP'. The 'Host Type' dropdown shows 'any', 'client', and 'server'. The 'Packet Capture' dropdown shows 'disable', 'single-packet', and 'extended-capture'. The 'Severity' dropdown shows 'any', 'brute-force', 'code-execution', 'code-obfuscation', 'command-execution', 'dos', 'exploit-kit', 'info-leak', 'overflow', 'phishing', 'protocol-anomaly', 'scan', and 'sql-injection'. The 'Rules' list on the left also includes 'Add', 'Delete', 'Move Up', and 'Move Down' buttons.

Vulnerability Protection Profile

Name: Profile Rule 1

Description:

Rules

- Default
- Allow
- Alert
- Drop
- Reset Client
- Reset Server
- Reset Both
- Block IP

Vulnerability Protection Rule

Rule Name: Profile Rule 1

Threat Name: any

Used to match any signature containing the entered text as part of the signature name

Action: Default

Host Type: any

☐ Any

☐ CVE

☒ CVE-2016-504

☐ Any

☐ Vendor ID

☒ MS

☒ any

☐ client

☐ server

Packet Capture

disable

Category

any

Severity

- ☒ any (All severities)
- ☐ critical
- ☐ high
- ☐ medium
- ☐ low
- ☐ informational

any

- brute-force
- code-execution
- code-obfuscation
- command-execution
- dos
- exploit-kit
- info-leak
- overflow
- phishing
- protocol-anomaly
- scan
- sql-injection

Rules

+ Add - Delete Move Up Move Down

Used to match any signature containing the entered text as part of the signature CVE or Vendor ID

Vulnerability Exceptions

Objects > Security Profiles > Vulnerability Protection > Add

Vulnerability Protection Profile

Name: PAN-Vulnerability-Profile

Description:

Rules Exceptions

10410 items

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

☒ Show all signatures PDF/CSV

Page 1 of 347 | Displaying 1 - 30 / 10410 threats

Override the action configured in the rules.

Click to modify packet capture setting.

Click to view or add IP addresses.



Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection

Default Antivirus Security Profile

Objects > Security Profiles > Antivirus

	Name	Location	Packet Capture	Decoders		Application Exceptions		Threat Exceptions
				Name	Action	WildFire Action	Name	Action
<input checked="" type="checkbox"/>	default	Predefined	<input type="checkbox"/>	http	default (reset-both)	allow		
				http2	default (reset-both)	allow		
				smtp	default (alert)	allow		
				imap	default (alert)	allow		
				pop3	default (alert)	allow		
				ftp	default (reset-both)	allow		
				smb	default (reset-both)	allow		

Buttons: Add, Delete, Clone, PDF/CSV

Out-of-the-box profile

Action to take based on antivirus signatures delivered in content updates

WildFire Action to take based on signatures delivered by WildFire

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

Creating a New Antivirus Profile

Objects > Security Profiles > Antivirus > Add

Available actions

default (alert)

allow

alert

drop

reset-client

reset-server

reset-both

Click to modify to something other than “default” action.

Add applications to exempt from the profile.

Antivirus Profile

Name: AV Profile

Description:

Antivirus Virus Exception

☐ Packet Capture

Decoders

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

Application Exception

0 items

Application	Action
-------------	--------

+ Add - Delete

Creating a New Antivirus Profile (Cont.)

Objects > Security Profiles > Antivirus > Add

Antivirus Profile

Name: AV Profile

Description:

Antivirus Virus Exception

Threat ID	Threat Name
281328	DOS/Virus.eicar_test_file.

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

Threat ID: Add PDF/CSV

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



Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection

Default Anti-Spyware Security Profiles

Objects > Security Profiles > Anti-Spyware

<input type="checkbox"/>	Name	Location	Count	Rule Name	Threat Name	Severity	Action	Packet Capture	DNS Packet Capture
<input type="checkbox"/>	default	Predefined	Rules: 4	simple-critical	any	critical	default	disable	disable
				simple-high	any	high	default	disable	
				simple-medium	any	medium	default	disable	
				simple-low	any	low	default	disable	
<input type="checkbox"/>	strict	Predefined	Rules: 5	simple-critical	any	critical	reset-both	disable	disable
				simple-high	any	high	reset-both		
				simple-medium	any	medium	reset-both		
				simple-informational	any	informational	default		
				simple-low	any	low	default		

Out-of-the-box profiles

Rules specify actions on detected spyware.

+ Add - Delete Clone PDF/CSV

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

Configuring Anti-Spyware Profile Rules

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

Anti-Spyware Profile

Name: Strict-AntiS

Description:

Rules Exceptions DNS

Rule Name

- ☐ simple-critical
- ☐ simple-high
- ☐ simple-medium
- ☐ simple-informational
- ☐ simple-low

Rule Name: New Rule

Threat Name: any

Used to match any signature containing the entered text as part of the signature name

Category: backdoor

Action: Default

Packet Capture: disable

Severity

- ☐ any (All severities)
- ☒ critical
- ☒ high
- ☒ medium
- ☐ low
- ☐ informational

disable

single-packet

extended-capture

Default

Allow

Alert

Drop

Reset Client

Reset Server

Reset Both

Block IP

adware

any

autogen

backdoor

botnet

browser-hijack

data-theft

dns

dns-wildfire

keylogger

net-worm

p2p-communication

phishing-kit

post-exploitation

spyware

webshell

Anti-Spyware Exceptions

Objects > Security Profiles > Anti-Spyware > Add

Anti-Spyware Profile

Name: Strict-AntiSpyware

Description:

Rules Exceptions DNS Signatures

Can override the action configured in the rules

Click to view or add IP addresses.

Click to override rule's packet capture setting.

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

Show all signatures PDF/CSV

Page 1 of 138 | Displaying 1-30/ 4118 threats

DNS Signatures

Objects > Security Profiles > Anti-Spyware > Add

Anti-Spyware Profile

Name: lab-as

Description:

Rules Exceptions **DNS Signatures**

Policies & Settings Exceptions

DNS Signature Policies

DNS Signature Source	Action on DNS Queries	Packet Capture
Palo Alto Networks Content DNS Signatures	sinkhole	disable
Palo Alto Networks Threat Intelligence Cloud	sinkhole	disable

Alert: alert, allow, block, sinkhole

Packet Capture: disable, single-packet, extended-capture

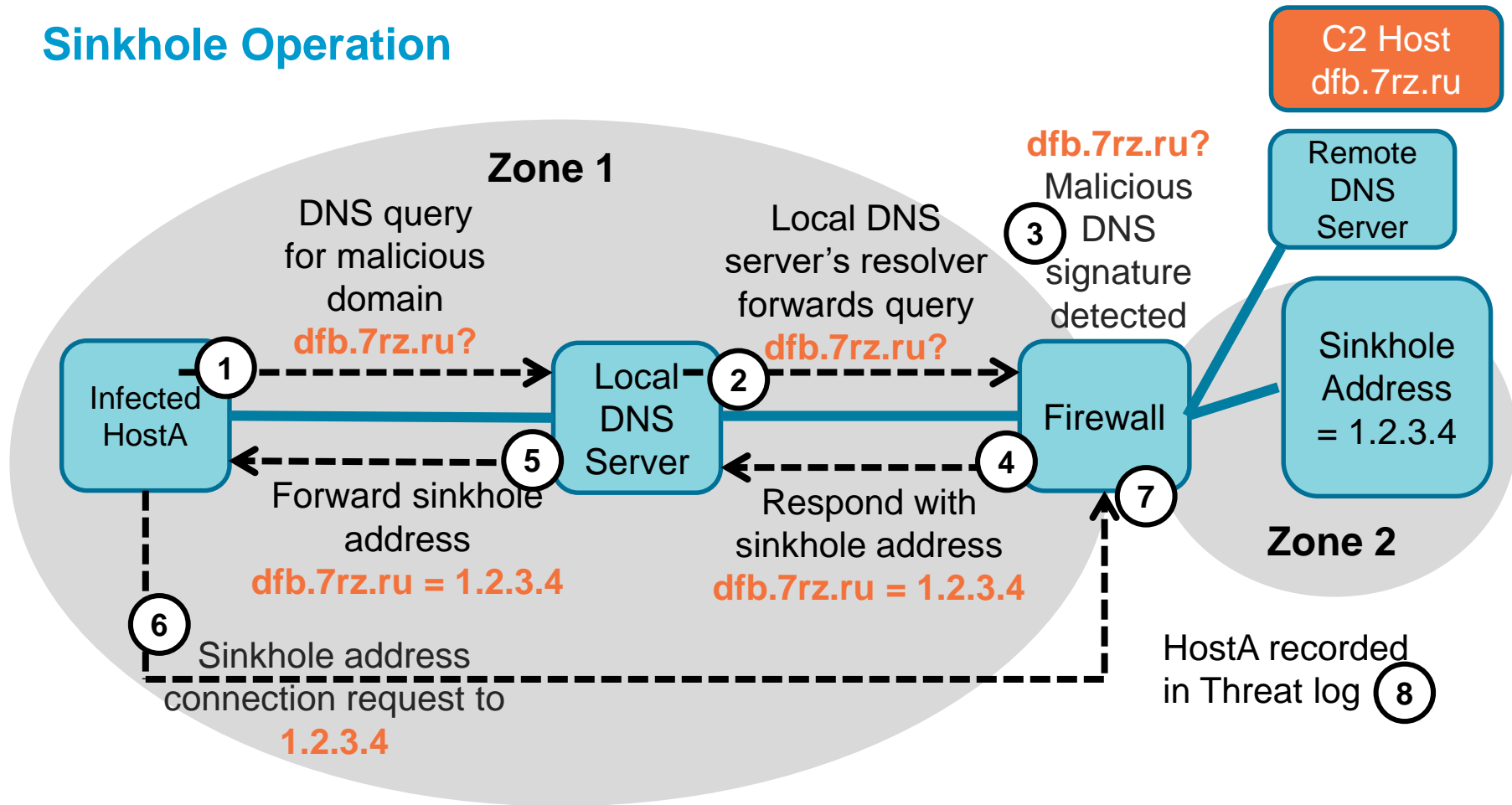
Access real-time cloud DNS signatures.

Configure sinkholes.

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





Sinkhole IPv6: IPv6 Loopback IP (::1)

Sinkhole Operation



Sinkhole Events in the Threat Log

Monitor > Logs > Threat

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

Potentially
infected host



Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

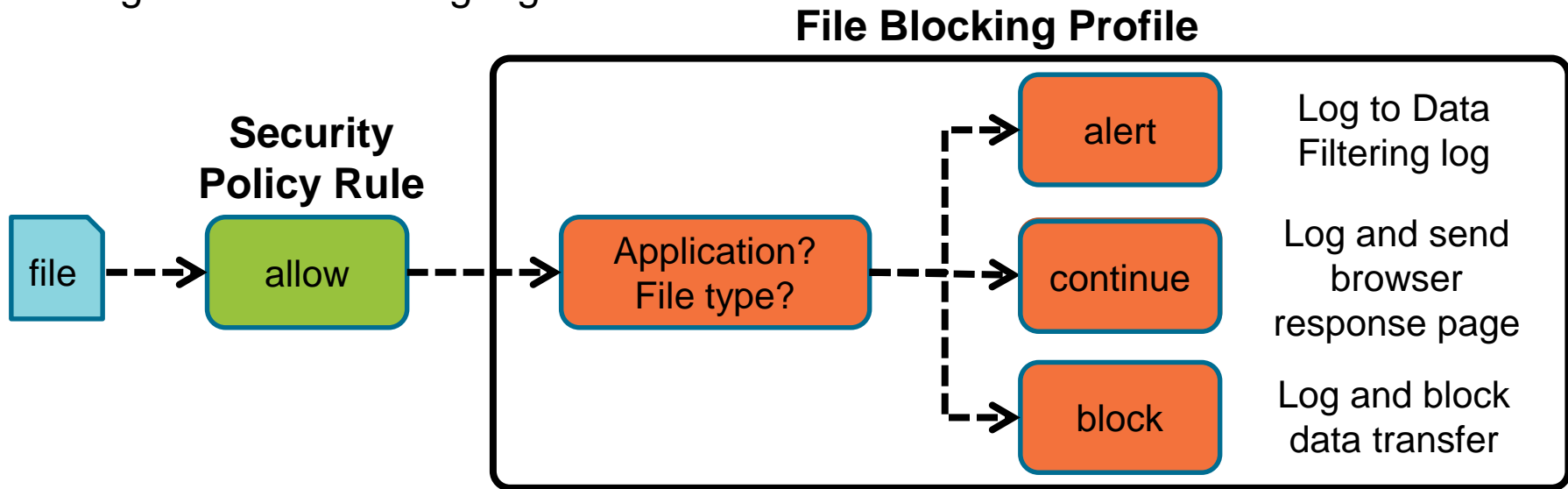
Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection

File Blocking Overview











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



Data Filtering Log

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

Monitor > Logs > Data Filtering

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

Creating a New File Blocking Profile

Objects > Security Profiles > File Blocking > Add

File Blocking Profile

Name: file-blocking

Description: Threat prevention through blocking file types

2 items

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

Add one or more rules to control file transfer.

bat
bmp
bmp-upload
cab
catpart

upload
download
both

alert
block
continue

+ Add - Delete

Continue Response Page

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

File Download Blocked

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

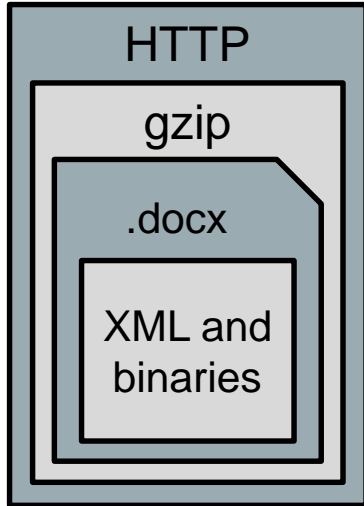
File name: Support_services_ds1.pdf

Please click to download/upload the file.

Blocking Multi-level Encoded Files

Objects > Security Profiles > File Blocking > Add

Firewall decodes
max of four levels



File Blocking Profile

Name: block-multi-level-encoding

Description:

Name	Applications	File Types	Direction	Action
<input checked="" type="checkbox"/> block multiple levels	any	Multi-Level-Encoding	both	block

Blocks files encoded more than four levels

+ Add - Delete

Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles



Data Filtering Profiles

Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection

Creating a Data Pattern

Objects > Custom Objects > Data Patterns > Add

Data Patterns

Name: Confidential Data

Description:

Pattern Type: Predefined Pattern

Name	Description	File Type
<input type="checkbox"/> Credit Card Numbers	US Credit Card Numbers pattern	Any
<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

Predefined Pattern
Regular Expression
File Properties

+ Add - Delete

Creating a Data Filtering Profile

Objects > Security Profiles > Data Filtering > Add

Data Filtering Profile

Name: Block Sensitive Data

Description:

☐ Data Capture

Number of times data pattern must be detected before alert

	Data Pattern	Applications	File Type	Direction	Alert Threshold	Block Threshold	Log Severity
<input checked="" type="checkbox"/>	Confidential Data	any	Any	both	0	0	informational

upload
download
both

Number of data pattern instances

+ Add - Delete

Alert/Block Threshold values: (0-65535)

Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles



Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection

Assigning Security Profiles to Security Rules

Policies > Security > Add

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Action Setting

Action: Allow
☐ Send ICMP Unreachable

Log Setting

☐ Log at Session Start
☒ Log at Session End

Profile Setting

Profile Type: Profiles

Antivirus: Strict-AntiVirus

Vulnerability Protection: Strict-Protection

Anti-Spyware: Strict-Anti-Spyware

URL Filtering: Strict-URL-Filtering

File Blocking: Strict-File-Transfer

Data Filtering: None

WildFire Analysis: None

Profile Setting

Profile Type: Group
Group Profile: Strict Profiles

☐ Disable Server Response Inspection

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

Security Profile Groups

Objects > Security Profile Groups > Add

Security Profile Group

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

OK Cancel

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

Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

Attaching Security Profiles to Security policy rules

Telemetry and threat intelligence

Denial-of-service protection



Telemetry and Threat Intelligence

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



Configuring Telemetry

Device > Setup > Telemetry

Telemetry

Telemetry Sharing

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

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

Settings

<input checked="" type="checkbox"/> Application Reports		<input checked="" type="checkbox"/> Threat Prevention Data	
<input checked="" type="checkbox"/> Threat Prevention Reports		<input checked="" type="checkbox"/> Threat Prevention Packet Captures	
<input checked="" type="checkbox"/> URL Reports		<input checked="" type="checkbox"/> Product Usage Statistics	
<input checked="" type="checkbox"/> File Type Identification Reports		<input checked="" type="checkbox"/> Passive DNS Monitoring	

Select All Deselect All

Show reports sent to Palo Alto Networks

Download Threat Prevention Data

Content-ID overview

Vulnerability Protection Security Profiles

Antivirus Security Profiles

Anti-Spyware Security Profiles

File Blocking Profiles

Data Filtering Profiles

Attaching Security Profiles to Security policy rules

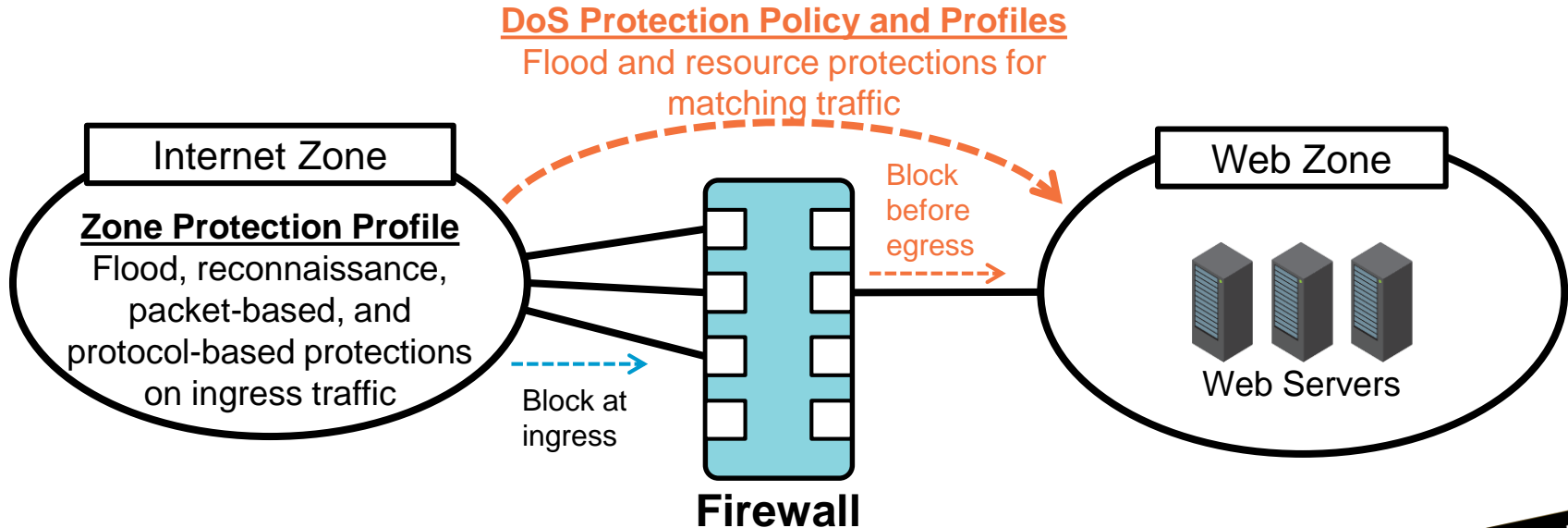
Telemetry and threat intelligence

Denial-of-service protection



Denial-of-Service Protection

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



Zone Protection: Flood Protection

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

Network > Network Profiles > Zone Protection > Add

Zone Protection Profile

Name: Edge Zone Protection

Description:

Flood Protection | Reconnaissance Protection | Packet Based Attack Protection | Protocol Protection

☐ SYN

Action: Random Early Drop

Alarm Rate (connections/sec): 10000

Activate (connections/sec): 10000

Maximum (connections/sec): 40000

☐ UDP

Alarm Rate (connections/sec): 10000

Activate (connections/sec): 10000

Maximum (connections/sec): 40000

☐ ICMP

Alarm Rate (connections/sec): 10000

Activate (connections/sec): 10000

Maximum (connections/sec): 40000

☐ ICMPv6

Alarm Rate (connections/sec): 10000

Activate (connections/sec): 10000

Maximum (connections/sec): 40000

☐ Other IP

Alarm Rate (connections/sec): 10000

Activate (connections/sec): 10000

Maximum (connections/sec): 40000

All categories use Random Early Drop except for SYN, which provides a choice.

Zone Protection: Reconnaissance Protection

Network > Network Profiles > Zone Protection > Add

- Alerts or protects against port scans and host sweeps

Zone Protection Profile

Name: Edge Zone Protection

Description:

Flood Protection Reconnaissance Protection Packet Based Attack Protection Protocol Protection

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

Allow
Alert
Block
Block IP

Block IP

Track By
source

Duration (sec)
[1 - 3600]

Source Address Exclusion

Zone Protection: Packet-Based Attack Protection

Network > Network Profiles > Zone Protection > Add

- Blocks packets based on protocol options or packet malformation

Zone Protection Profile

Name: Edge Zone Protection

Description:

Flood Protection Reconnaissance Protection **Packet Based Attack Protection** Protocol Protection

IP Drop **TCP Drop** ICMP Drop IPv6 Drop ICMPv6 Drop

☐ Spoofed IP address

☐ Strict IP Address Check

☐ Fragmented traffic

IP Option Drop

☐ Strict Source Routing ☐ Security

☐ Loose Source Routing ☐ Stream ID

☐ Timestamp ☐ Unknown

☐ Record Route ☐ Malformed

Zone Protection: Protocol Protection

Network > Network Profiles > Zone Protection > Add

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

The screenshot shows the 'Zone Protection Profile' configuration window. The 'Name' field is 'Edge Zone Protection' and the 'Description' field is empty. The 'Protocol Protection' tab is selected. The 'Rule Type' is set to 'Exclude List'. Below this is a table with columns 'Protocol Name', 'Enable', and 'Ethertype (hex)'. The table is currently empty. Below the table, there is a note: 'Ethertype value in hex between 0x0000 and 0xFFFF. Ethertypes 0x0800, 0x0806, 0x8100, and 0x86dd are reserved and cannot be excluded.' At the bottom of the table area are 'Add' and 'Delete' buttons. A footer note states: 'Exclude List uses implicit allow for all non-listed protocols'.

Protocol Name	Enable	Ethertype (hex)
---------------	--------	-----------------

Ethertype value in hex between 0x0000 and 0xFFFF.
Ethertypes 0x0800, 0x0806, 0x8100, and 0x86dd are reserved and cannot be excluded.

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

Exclude List uses implicit allow for all non-listed protocols

Enabling Zone Protection

Network > Zones > <select_zone>

- Profiles applied one per zone

The screenshot shows the 'Zone' configuration page for a zone named 'Internet'. The 'Log Setting' is 'None' and the 'Type' is 'Layer3'. Under the 'Interfaces' section, 'ethernet1/1' is listed. The 'Zone Protection' section at the bottom is highlighted with a red box, showing the 'Zone Protection Profile' set to 'Edge Zone Protection'. The 'User Identification ACL' section on the right is also visible, with 'Enable User Identification' unchecked. The 'Include List' and 'Exclude List' sections are empty, with instructions to select an address or address group.

Zone

Name: Internet

Log Setting: None

Type: Layer3

Interfaces

- ethernet1/1

+ Add - Delete

Zone Protection

Zone Protection Profile: Edge Zone Protection

Enable Packet Buffer Protection

User Identification ACL

Enable User Identification

Include List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add - Delete

Users from these addresses/subnets will be identified.

Exclude List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

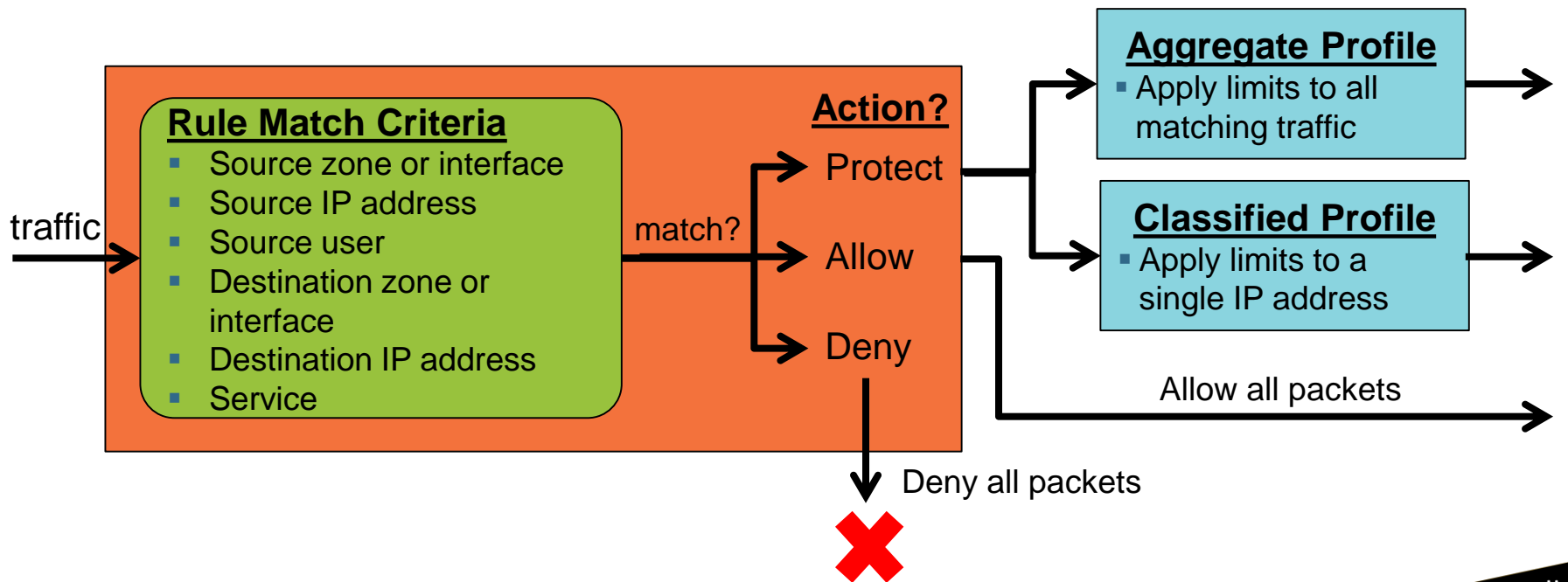
+ Add - Delete

Users from these addresses/subnets will not be identified.

DoS Protection Profiles and Policies

DoS Protection Policy

(defines match criteria and action)



Configuring a DoS Protection Policy

Policies > DoS Protection > Add

The screenshot displays the 'DoS Rule' configuration page in the Palo Alto Networks management console. The interface is divided into several sections and tabs.

General Tab:

- Name:** Web Zone DoS Rule
- Description:** (Empty field)
- Tags:** internal
- Group Rules By Tag:** internal
- Audit Comment:** (Empty field)
- Audit Comment Archive:** (Link)

Match conditions (Source Tab):

- The **Source** tab is selected, showing a dropdown menu with options: **Any** (checked) and **Service**.
- An annotation box labeled "Match conditions" points to this dropdown.

Action and Classification (Option/Protection Tab):

- The **Option/Protection** tab is selected.
- Action:** Deny
- Schedule:** None
- Log Forwarding:** None
- Aggregate:** Web Zone Profile
- Classified:** (Checked)
 - Profile:** Web Server Profile
 - Address:** source-ip-only

Annotations:

- A box labeled "Deny Allow Protect" points to the **Action** dropdown.
- A box labeled "source-ip-only destination-ip-only src-dest-ip-both" points to the **Address** dropdown.

Configuring a DoS Protection Profile

Objects > Security Profiles > DoS Protection > Add

DoS Protection Profile

Name: Web Zone Profile

Description:

Type: ☒ Aggregate ☐ Classified

Flood Protection | **Resources Protection**

SYN Flood | UDP Flood | ICMP Flood | ICMPv6 Flood | Other IP Flood

☐ **SYN Flood**

Parameter	Value
Action	Random Early Drop
Alarm Rate (connections/s)	10000
Activate Rate (connections/s)	10000
Max Rate (connections/s)	40000
Block Duration (s)	300

DoS Protection Profile

Name: Web Zone Profile

Description:

Type: ☒ Aggregate ☐ Classified

Flood Protection | **Resources Protection**

☐ **Sessions**

Maximum Concurrent Sessions	32768
-----------------------------	-------

Module Summary



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

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

Questions



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

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

PROTECTION. DELIVERED.

