

Preventing Known and Unknown Threats



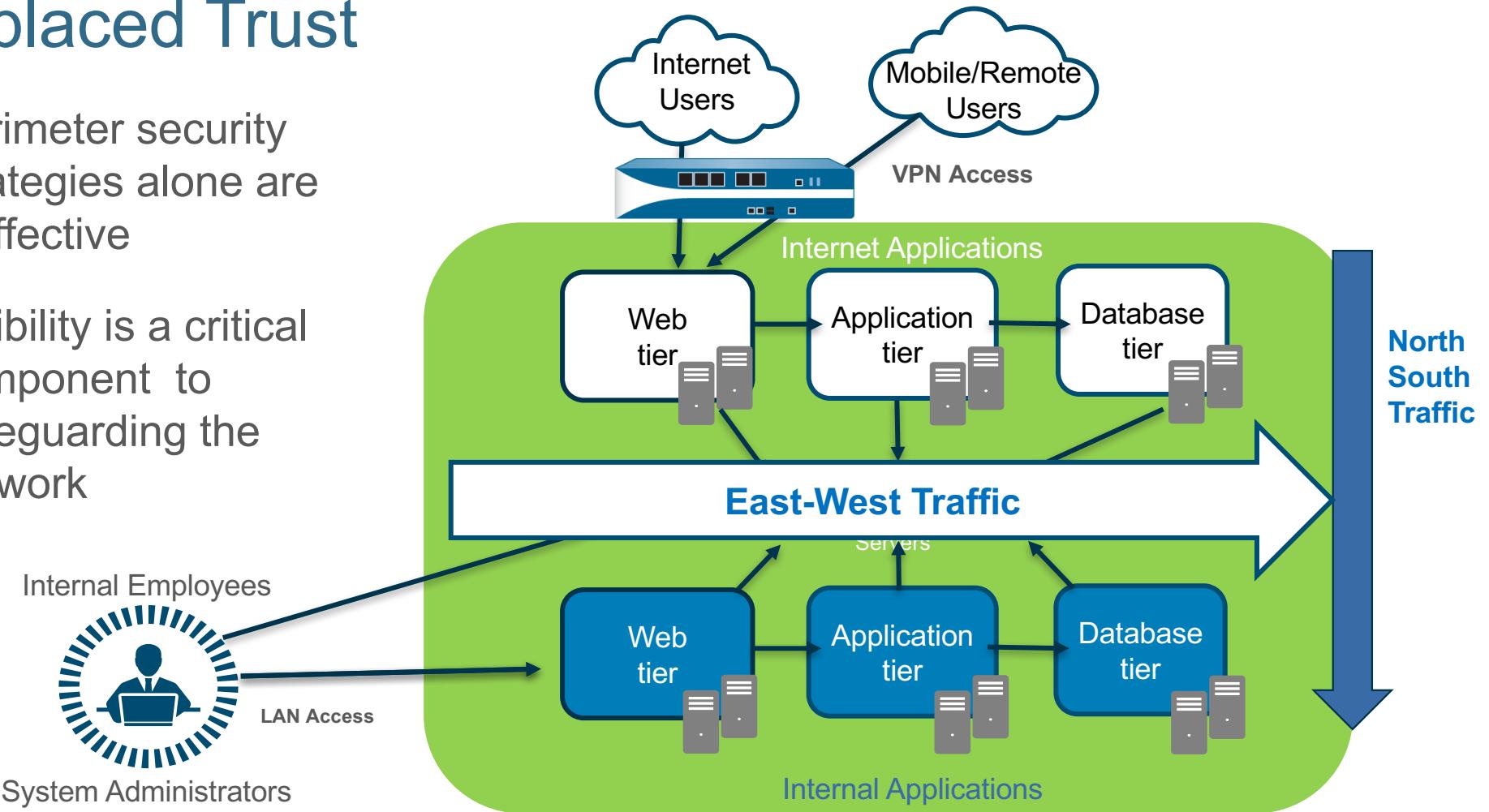
Agenda

- Zero Trust Overview
- Profiles
- URL Filtering
- Wildfire
- Reports
- Correlation Events

Zero Trust

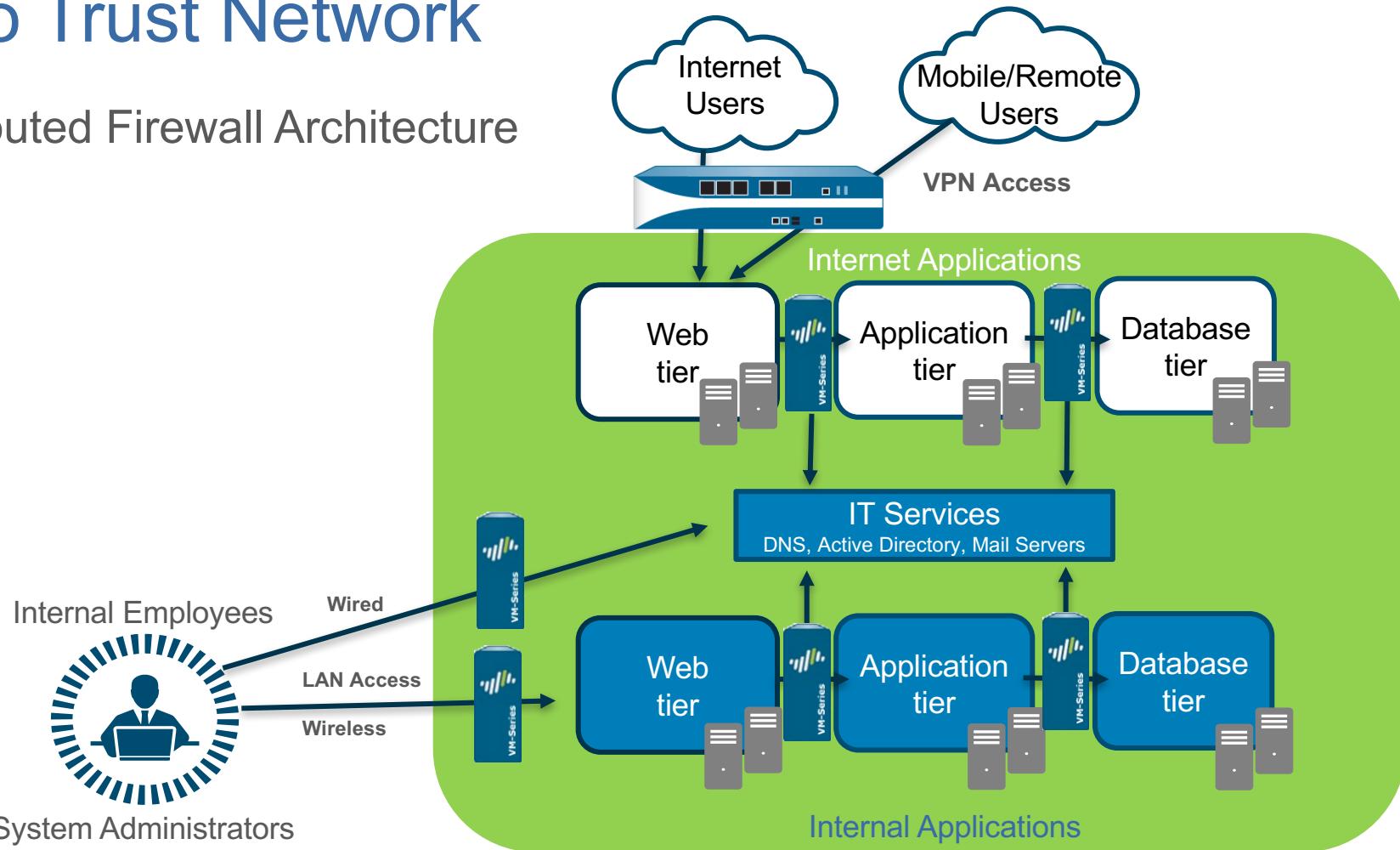
Misplaced Trust

- Perimeter security strategies alone are ineffective
- Visibility is a critical component to safeguarding the network



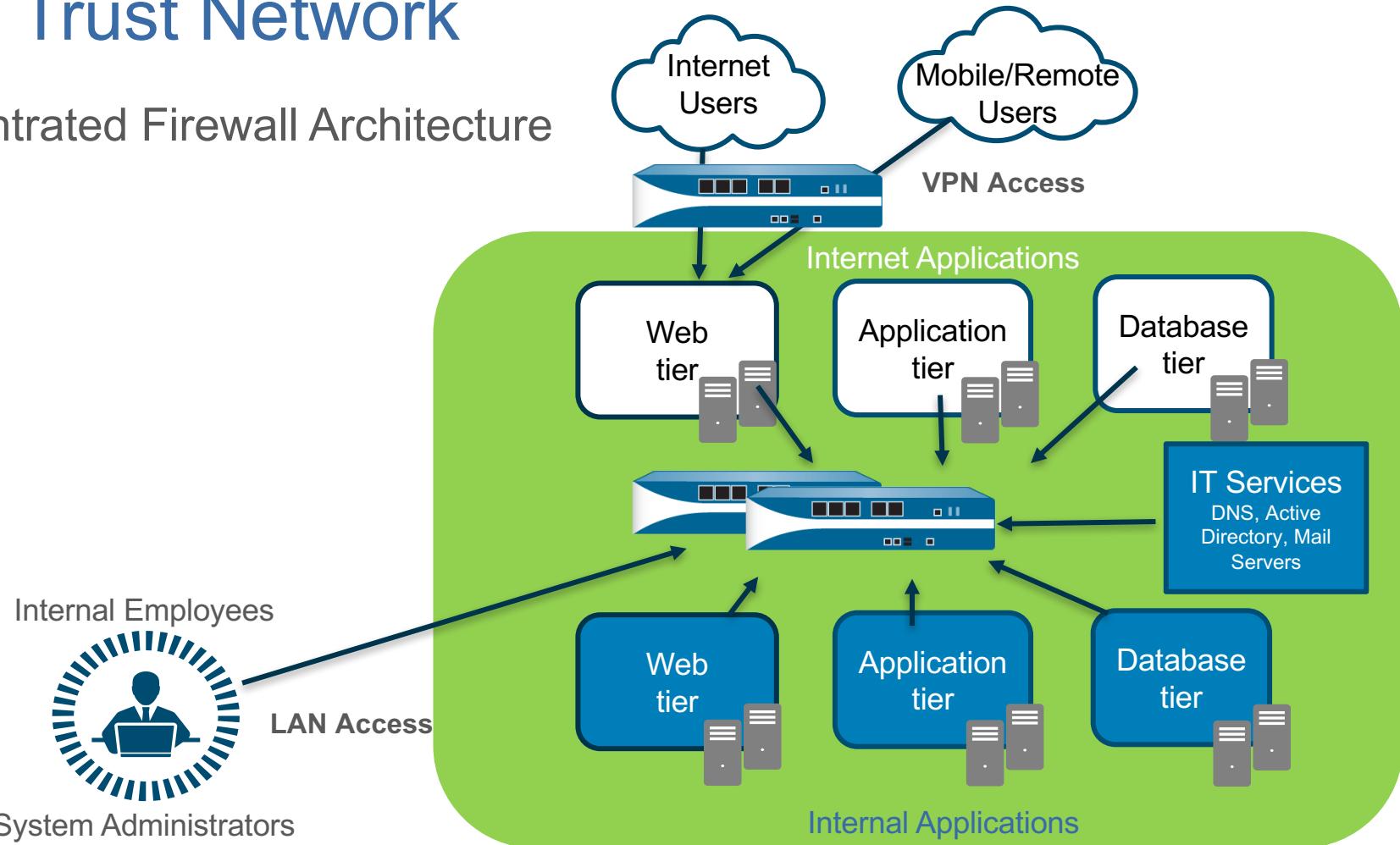
Zero Trust Network

Distributed Firewall Architecture



Zero Trust Network

Concentrated Firewall Architecture



Profiles

Security Profiles

Policies > Security

Name	Type	Source			Destination			Application	Service	Action	Profile	Options
		Zone	Addr...	User	Zone	Address						
1	Server-Access	universal	L3-untrust	any	any	L3-trust	any		application-default	Allow		
2	allow outbound	universal	L3-trust	any	any	L3-untrust	any	any	any	Allow		
3	allow NTP	universal	L3-untrust	any	any	L3-trust	any		application-default	Allow		
4	intrazone-default	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	none
5	interzone-default	interzone	any	any	any	any	any	any	any	Deny	none	none



Antivirus



URL Filtering



Anti-Spyware



File Blocking



Vulnerability



Data Filtering

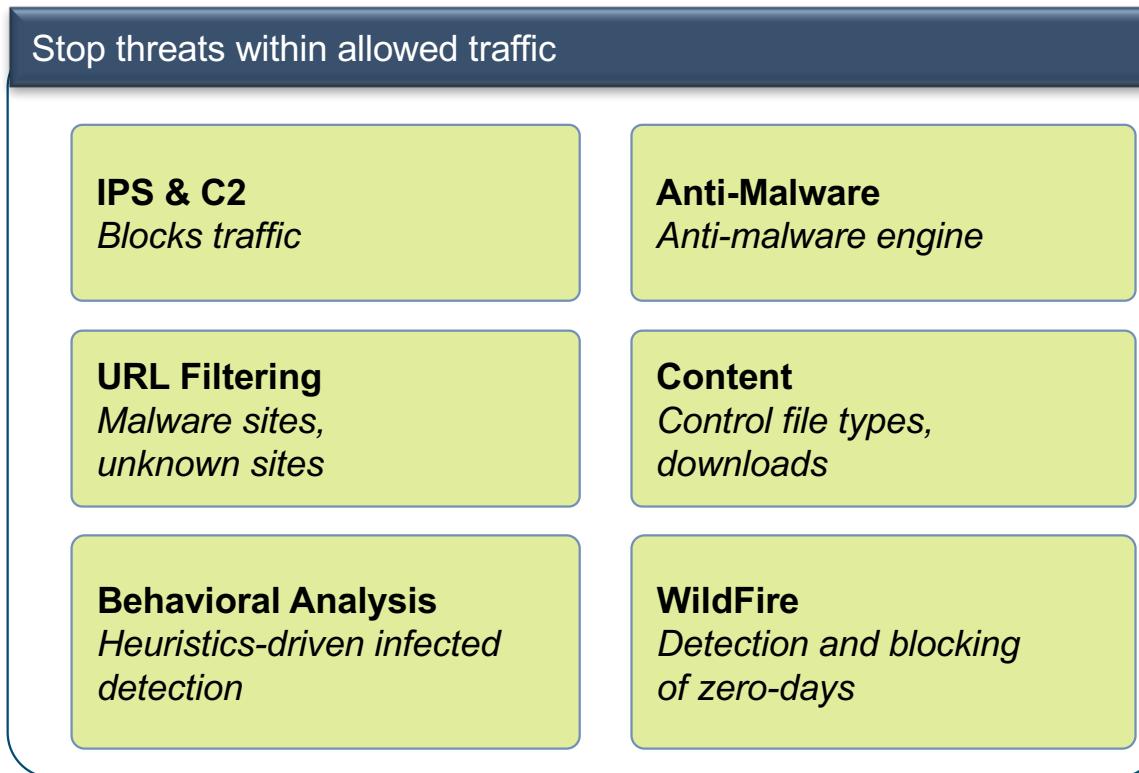


WildFire Analysis



Integrated Threat Prevention

- Multiple security disciplines in a single threat prevention engine



Antivirus Profile—Default Action

- Default Antivirus profile actions are set per protocol
 - allow
 - alert
 - drop
 - reset (client/server/both)
- Best practice is to apply the action based on the traffic direction

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

Anti-Spyware Profile—DNS Signature Tab

Anti-Spyware Profile

Name: New CnC profile

Description:

Rules Exceptions DNS Signatures

External Dynamic List Domains	Action on DNS Queries
Palo Alto Networks DNS Signatures	sinkhole

Add **Delete**

Sinkhole IPv4: None

Sinkhole IPv6: None

Packet Capture: disable

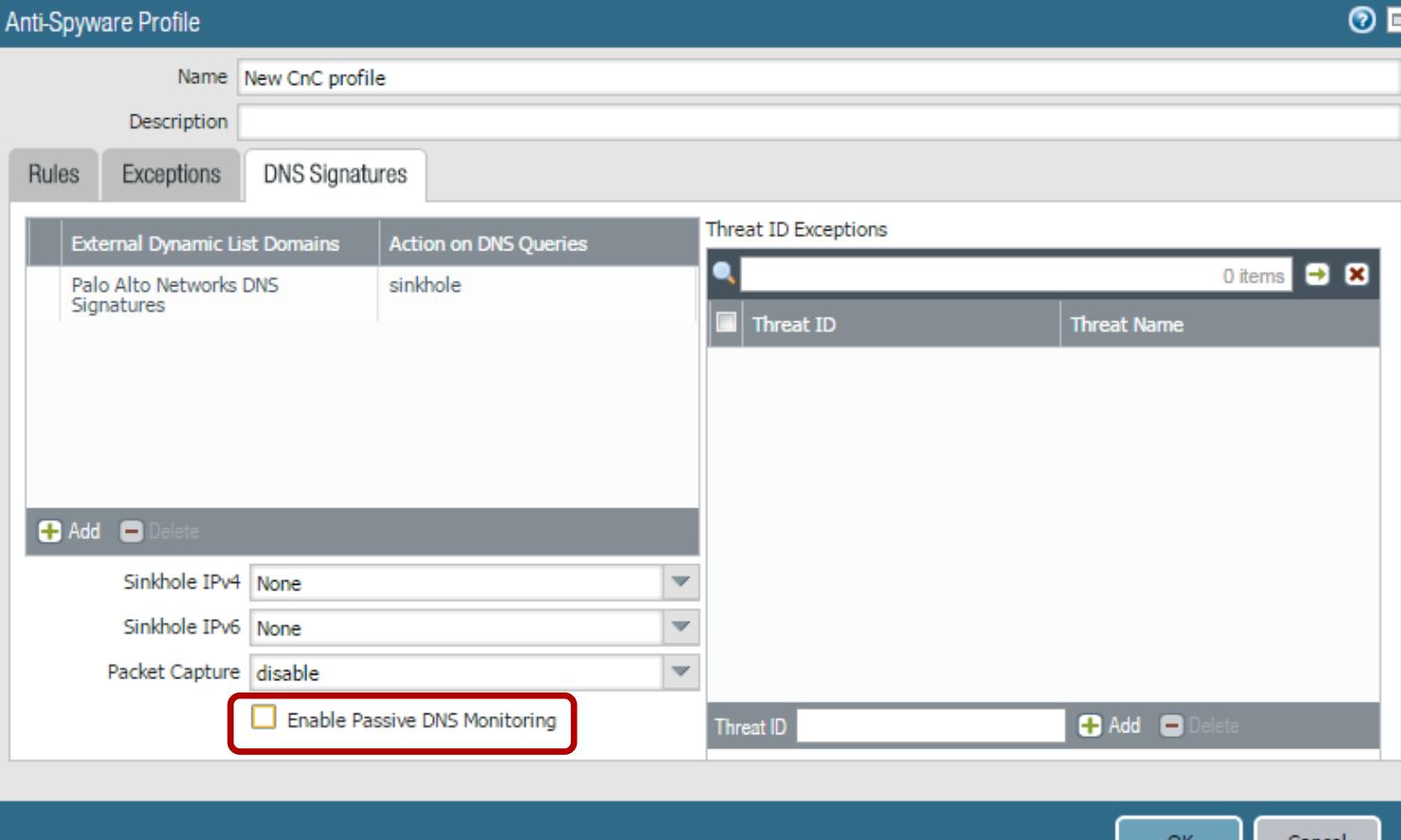
Enable Passive DNS Monitoring

Threat ID Exceptions

Threat ID	Threat Name
0 items	

Threat ID **Add** **Delete**

OK Cancel



DNS Sinkhole Configuration

Object > Anti-Spyware > DNS Signature

Anti-Spyware Profile

External Dynamic List Domains	Action on DNS Queries
test url list 2	sinkhole

Palo Alto Network Public Sinkhole

Sinkhole IPv4: PAN Sinkhole Default IPv4 Address (pan-sink)

Sinkhole IPv6: ::1

Packet Capture: disable

Enable Passive DNS Monitoring

Threat ID Exceptions

Threat ID	Threat Name
0 items	

Vulnerability Protection Security Profile—Default Action

Default action set by Palo Alto Networks within the signatures

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
			simple-client-high	any	client	high	default	disable
			simple-client-medium	any	client	medium	default	disable
			simple-server-critical	any	server	critical	default	disable
			simple-server-high	any	server	high	default	disable
			simple-server-medium	any	server	medium	default	disable

Anti-Spyware and Vulnerability Protection

Vulnerability Protection Profile

Name: Public DMZ
Description:

Rules Exceptions

Rule Name	Threat Name	CVE	Host Type	Severity	Action	Packets
simple-client-critical	any	any	client	critical	alert	disable
simple-client-high	any	any	client	high	reset-both	disable
simple-client-medium	any	any	client	medium	reset-both	disable
simple-client-informational	any	any	client	informational	default	disable
simple-client-low	any	any	client	low	default	disable
simple-server-critical	any	any	server	critical	reset-both	disable
simple-server-high	any	any	server	high	reset-both	disable
simple-server-medium	any	any	server	medium	reset-both	disable

+ Add - Delete ⌘ Move Up ⌘ Move Down ⌘ Clone 🔎 Find Matching Signatures

OK

Vulnerability Protection Rule

Rule Name: New Vulnerability
Threat Name: any
Used to match any signature containing the entered text as part of the signature name

Action: Default | Packet Capture: disable
Host Type: any | Category: any

Severity

Any Any

CVE Vendor ID

+ Add - Delete + Add - Delete

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

OK Cancel

The screenshot shows two windows from the Palo Alto Networks interface. The main window is titled 'Vulnerability Protection Profile' with a tab for 'Rules'. It lists several rules for different threat types (simple-client, simple-server) across various severity levels (critical, high, medium, informational, low). The second window is a detailed view of a specific rule named 'New Vulnerability', showing fields for Threat Name (any), Action (Default), Host Type (any), and Category (any). It also includes a 'Severity' section with checkboxes for different levels and a table for matching on CVE or Vendor ID.

Enable Packet Captures on other Security Profiles

Select the check box or appropriate pull down if you want to capture identified packets

The image displays three overlapping screenshots of the Palo Alto Networks interface, specifically focusing on enabling packet captures across different security profiles.

- Antivirus Profile (AV1):** Shows the "Antivirus" tab selected. Under the "Decoders" section, the "Decoder" dropdown is set to "smtp" and the "Action" dropdown is set to "default". A red box highlights the "Packet Capture" checkbox, which is currently unchecked.
- Anti-Spyware Profile (sinkhole dns):** Shows the "Anti-Spyware Rule" configuration. It includes fields for "Rule Name" (all-to-test-sinkhole), "Threat Name" (any), "Category" (any), and "Action" (Alert). The "Packet Capture" dropdown is set to "disable". A red box highlights the "Severity" dropdown, which lists "any (All)", "critical", "high", "medium", "low", and "informational".
- Vulnerability Protection Rule (simple-client-critical):** Shows the "Vulnerability Protection Rule" configuration. It includes fields for "Rule Name" (simple-client-critical), "Threat Name" (any), "Action" (Reset Both), "Host Type" (client), and "Category" (disabled). The "Packet Capture" dropdown is set to "enable". A red box highlights the "Category" dropdown, which lists "disabled", "single-packet", and "extended-capture".

Extended Packet Capture

Device > Setup > Content-ID

The screenshot shows the Palo Alto Networks Device Setup interface. The top navigation bar includes tabs for Management, Operations, Services, Content-ID (which is selected and highlighted in blue), WildFire, Session, and HSM. Below the navigation bar, there are two main sections: 'URL Filtering' on the left and 'Content-ID Settings' on the right. The 'Content-ID Settings' section contains options like 'Allow forwarding of decrypted content' (unchecked) and 'Extended Packet Capture Length (packets)' set to 5. A red arrow points from the 'Content-ID Settings' tab in the top navigation bar to the corresponding section in the main content area. A modal dialog box is overlaid on the page, also titled 'Content-ID Settings'. This dialog box has its own 'Content-ID Settings' section with the same options: 'Allow forwarding of decrypted content' (unchecked) and 'Extended Packet Capture Length (packets)' set to 5. It includes 'OK' and 'Cancel' buttons at the bottom.

View Packet Captures

Monitor > Logs > Threat

The screenshot shows the Palo Alto Networks Threat Log interface. On the left, a list of log entries is displayed with a red arrow pointing to the first entry, which has a green icon next to it. The main area is titled "Packet Capture" and displays two hex dump entries. The first entry is from 08:59:34.000000 and the second is from 08:59:34.000000. Both entries show network traffic details including source and destination MAC addresses, port numbers, and payload data. At the bottom of the "Packet Capture" window, there are "Export" and "Close" buttons, with the "Export" button also highlighted by a red box.

```
08:59:34.000000 00:1b:17:ea:de:12 > 00:1b:17:3f:a6:13, ethertype IPv4 (0x0800), length 89: (tos 0x0000: 001b 173f a613 001b 17ea de12 0800 4500 ...?.....E.  
0x0010: 004b 9d68 4000 3406 0000 ac10 4dd1 17cc .K.h@.4.....M...  
0x0020: e53b 0e9a 01bb 70fc c20f 93f8 7895 5010 .;....p....X.P.  
0x0030: 3908 0000 0000 df00 0016 0004 0005 000a 9.....  
0x0040: 0009 0064 0062 0003 0006 0013 0012 0063 ..d.b.....c  
0x0050: 0100 0005 ff01 0001 00 .....  
08:59:34.000000 00:1b:17:3f:a6:13 > 00:1b:17:ea:de:12, ethertype IPv4 (0x0800), length 981: (tos 0x0000: 001b 17ea de12 001b 173f a613 0800 4500 .....?....E.  
0x0010: 0514 9d68 4000 3406 ad92 17cc e53b ac10 ..h@.4.....;..  
0x0020: 4dd1 01bb 0e9a 93f8 7895 70fc c232 5010 M.....x.p..2P.  
0x0030: 3908 72ab 0000 1603 0100 4a02 0000 4603 9.r.....J..F.  
0x0040: 0155 8966 4694 f600 f612 04eb 7d33 9af7 .U.ff.....}3..  
0x0050: 53f9 8c09 247a 6e7a c874 88d7 c427 bdb0 $...$nz.t...'.  
0x0060: 8420 3c12 e74c 0178 5deb 98d7 c2f6 c1d5 ..<..L.X].....  
0x0070: 9f95 a40c ad6c cac3 0ecd d686 e81a 2048 ....l.....H  
0x0080: 49af 000a 0016 0381 1370 0b00 136c 0013 I.....p..1..  
0x0090: 6900 094d 3082 0949 3082 0831 a003 0201 i..M0..I0..1...  
0x00a0: 0202 187e 74da 8137 95fb f087 39e2 fc9b ...~t..7....9...  
0x00b0: 588e 6030 0d06 092a 8648 86f7 0d01 010b X.^0..*.H.....  
0x00c0: 0500 307e 310b 3009 0603 5504 0613 0255 ..0~1.0..U....U  
0x00d0: 5331 1d30 1b06 0355 040a 1314 5379 6d61 S1.0..U....Syma  
0x00e0: 6e74 6563 2043 6f72 706f 7261 7469 6f6e ntec.Corporation  
0x00f0: 311f 301d 0603 5504 0b13 1653 796d 616e 1.0..U....Syman  
0x0100: 7465 6320 5472 7573 7420 4e65 7477 6f72 tec.Trust.Networ  
0x0110: 6b31 2f30 2d06 0355 0403 1326 5379 6d61 k1/0..U..&Syma  
0x0120: 6e74 6563 2043 6c61 7373 2033 2053 6563 ntec.Class.3.Sec  
0x0130: 7572 6520 5365 7276 6572 2043 4120 2d20 ure.Server.CA..  
0x0140: 4734 301e 170d 3135 3034 3031 3030 3030 G40..1504010000  
0x0150: 3030 5a17 0d31 3630 3431 3032 3335 3935 00Z..16041023595  
0x0160: 395a 3081 8831 0b30 0906 0355 0406 1302 9Z0..1.0..U....
```

Unified Log

Monitor > Logs > Unified

	Log Type	Receive Time	Log Subtype	Source Zone	Destinat... Zone	Source address	Destination address	Desti... Port	Application	Action	Rule	Bytes	Severity	Url
	traffic	12/21 13:13:03	end	L3-Untrust	L3-Untrust	10.31.33.131	10.31.33.26	443	ssl	allow	Unknown User SSL and Web-1	5.4k		
	url	12/21 13:13:03	url	L3-Untrust	L3-Untrust	10.31.33.131	10.31.33.26	443	ssl	alert	Unknown User SSL and Web-1		informational	*.paloaltonetwo...
	traffic	12/21 13:13:02	end	L3-Untrust	L3-Untrust	10.31.33.26	8.8.8.8	53	dns	allow	Watch Public DNS and SMTP-1	184		
	traffic	12/21 13:13:02	end	L3-Untrust	L3-Untrust	10.31.33.26	8.8.8.8	53	dns	allow	Watch Public DNS and SMTP-1	198		
	traffic	12/21 13:13:02	end	L3-Untrust	L3-Untrust	10.31.33.26	8.8.8.8	53	dns	allow	Watch Public DNS and SMTP-1	192		
	traffic	12/21 13:13:00	end	L3-Untrust	L3-Untrust	10.31.33.131	10.31.33.26	443	ssl	allow	Unknown User SSL and Web-1	5.5k		
	url	12/21 13:13:00	url	L3-Untrust	L3-Untrust	10.31.33.131	10.31.33.26	443	ssl	alert	Unknown User SSL and Web-1		informational	*.paloaltonetwo...
	url	12/21 13:12:57	url	L3-Untrust	L3-Untrust	10.31.33.131	10.31.33.26	443	ssl	alert	Unknown User SSL and Web-1		informational	*.paloaltonetwo...
	traffic	12/21 13:12:56	end	L3-Untrust	L3-Untrust	10.31.33.131	10.31.33.26	443	ssl	allow	Unknown User SSL and Web-1	5.3k		
	traffic	12/21 13:12:54	end	L3-Untrust	L3-Untrust	10.31.33.26	10.31.33.130	3978	panorama	allow	Required Infrastructure-1	30.5k		
	url	12/21 13:12:54	url	L3-Untrust	L3-Untrust	10.31.33.131	10.31.33.26	443	ssl	alert	Unknown User SSL and Web-1		informational	*.paloaltonetwo...
	traffic	12/21 13:12:52	end	L3-Untrust	L3-Untrust	10.31.33.131	10.31.33.26	443	ssl	allow	Unknown User SSL and Web-1	5.4k		
	traffic	12/21 13:12:52	end	L3-Untrust	L3-Untrust	15.0.0.205	15.0.0.255	138	netbios-dg	allow	Unexpected Traffic-1	243		
	traffic	12/21 13:12:52	end	L3-Untrust	L3-Untrust	10.31.32.229	10.31.32.255	138	netbios-dg	allow	Unexpected Traffic-1	243		
	traffic	12/21 13:12:50	end	L3-Trust1	L3-Untrust	172.16.33.226	4.2.2.1	53	dns	allow	SaaS-IWS	180		
	traffic	12/21 13:12:50	end	L3-Trust1	L3-Untrust	172.16.33.226	4.2.2.1	53	dns	allow	SaaS-IWS	168		
	url	12/21 13:12:50	url	L3-Untrust	L3-Untrust	10.31.33.131	10.31.33.26	443	ssl	alert	Unknown User SSL and Web-1		informational	*.paloaltonetwo...
	traffic	12/21 13:12:49	end	L3-Untrust	L3-Untrust	10.31.33.131	10.31.33.26	443	ssl	allow	Unknown User SSL and Web-1	5.4k		
	url	12/21 13:12:47	url	L3-Untrust	L3-Untrust	10.31.33.131	10.31.33.26	443	ssl	alert	Unknown User SSL and Web-1		informational	*.paloaltonetwo...
	traffic	12/21 13:12:46	end	L3-Untrust	L3-Untrust	10.31.33.131	10.31.33.26	443	ssl	allow	Unknown User SSL and Web-1	5.4k		

AutoFocus Integrates with Log Files

Monitor > Logs

Source	Destination	To Port	Application	Action	Rule	Session End Reason
10.154.6.23	72.1.2.11		AutoFocus			
10.154.14.14	20.81.23.54	80	web-browser			
10.154.3.78	28.2.236.208	80	web-browser			
10.154.14.27	7.8.135.170	80	web-browser			
10.154.6.132	6.5.129.250	80	web-browser			
10.154.6.16	10.50.102.50	80	web-browser			
10.154.14.13	27.42.93.166	443	ssl			

AutoFocus Intelligence Summary - 74.1.2.110 (Read Only)

Search Autofocus for 74.1.2.110

Passive DNS

Request	Type	Response	Count	First Seen	Last Seen
88428406.google.com	A	74.1.2.110	1326	2015-05-01T00:21:31	2015-08-01T13:25:46
99dollarusicvideo.com	A	74.1.2.110	2	2015-10-31T23:56:06	2015-10-31T23:56:06
99dollarusicvideos.com	A	74.1.2.110	40	2014-01-03T15:31:36	2015-12-09T03:45:17
abc.xyz	A	74.1.2.110	17161	2015-08-10T20:43:01	2016-01-23T19:08:22
accountchooser.com	A	74.1.2.110	1292	2014-01-04T22:40:02	2016-01-23T03:37:13

Matching Tags

Sessions

Wildfire Verdicts

Recent WildFire Results

SHA256	File Type	Create Date	Update Date	Verdict
fd4efa91eb7d2b3b170973b3403808034bb28e5dca721d7bf308b7173e9fa...	PE	2015-12-09T11:39:21		Grayware
cb36f3c8d0eed0e076fbcfab98fd2f0756e67be08fd1cef08cca1b8c8acb70f8	PE	2015-12-07T21:31:23		Benign
039859085627f8e59ee728a1d801c3edd4a20c40044de14c175fb25a5e689...	PE	2015-12-04T09:34:21		Benign
3f74e2e1db7a84577b7ad2b5553684d6295a312891fb77afab878636477...	PE	2015-12-04T09:30:45		Benign
7ac4d6758648f84837068a785741ccf9f2a282446242add76da73af5d9a8b1...	PE	2015-12-04T07:24:48		Benign

Creating Custom Threat Signatures

- Custom Signatures can be added to the Security Profiles

The screenshot shows a web browser displaying the Palo Alto Networks LIVEcommunity website. The page title is "Documentation Articles". The main content area features an article titled "Creating Custom Threat Signatures" by jseals, posted on 07-29-2013 01:41 PM. The article has 14,066 views. It includes a PDF download link for "Creating_Custom_Signatures-RevB.pdf". The "Labels" section lists "Tech Notes". The "Comments" section shows 0 comments. The "Share" button is present. To the right, a sidebar titled "Labels" lists various categories: Administrator's Guide (114), CLI Reference Guide (7), Enterprise SNMP MIB (6), Getting Started Guide (14), Hardware Guide (73), Other Documents (5), and Tech Notes (47). The footer of the page includes the Palo Alto Networks logo and copyright information: "20 | © 2016, Palo Alto Networks, Inc."

URL Filtering

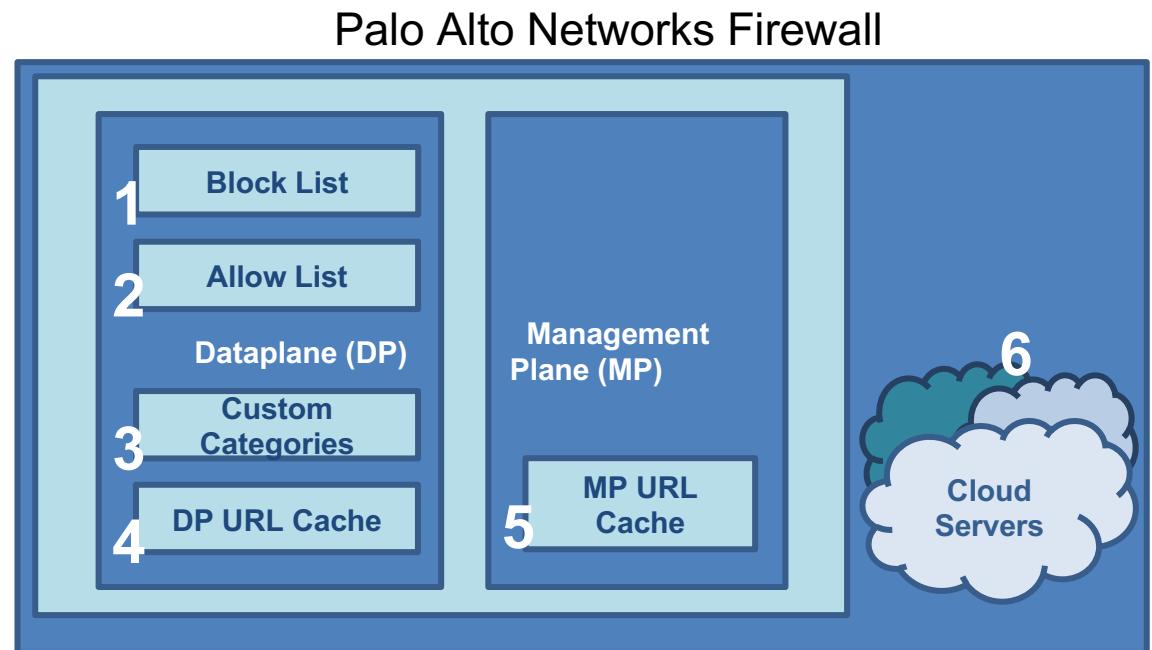
Threat Intelligence Cloud

- WildFire/Threat Prevention
 - Advanced persistent threat detection and prevention
 - Unknown threats are processed within 15 minutes
 - Updates are shared with all Palo Alto Networks customers
- URL Filtering - PANDB
 - Categorization of web URLs
 - Impact command-and-control URL communications
- GlobalProtect
 - Extends the protections of the firewall to the mobile device



Why PAN-DB?

- Threat Integration
 - PAN-DB receives updates from WildFire
- Better Performance
 - Faster URL category returns
 - Higher capacity caches



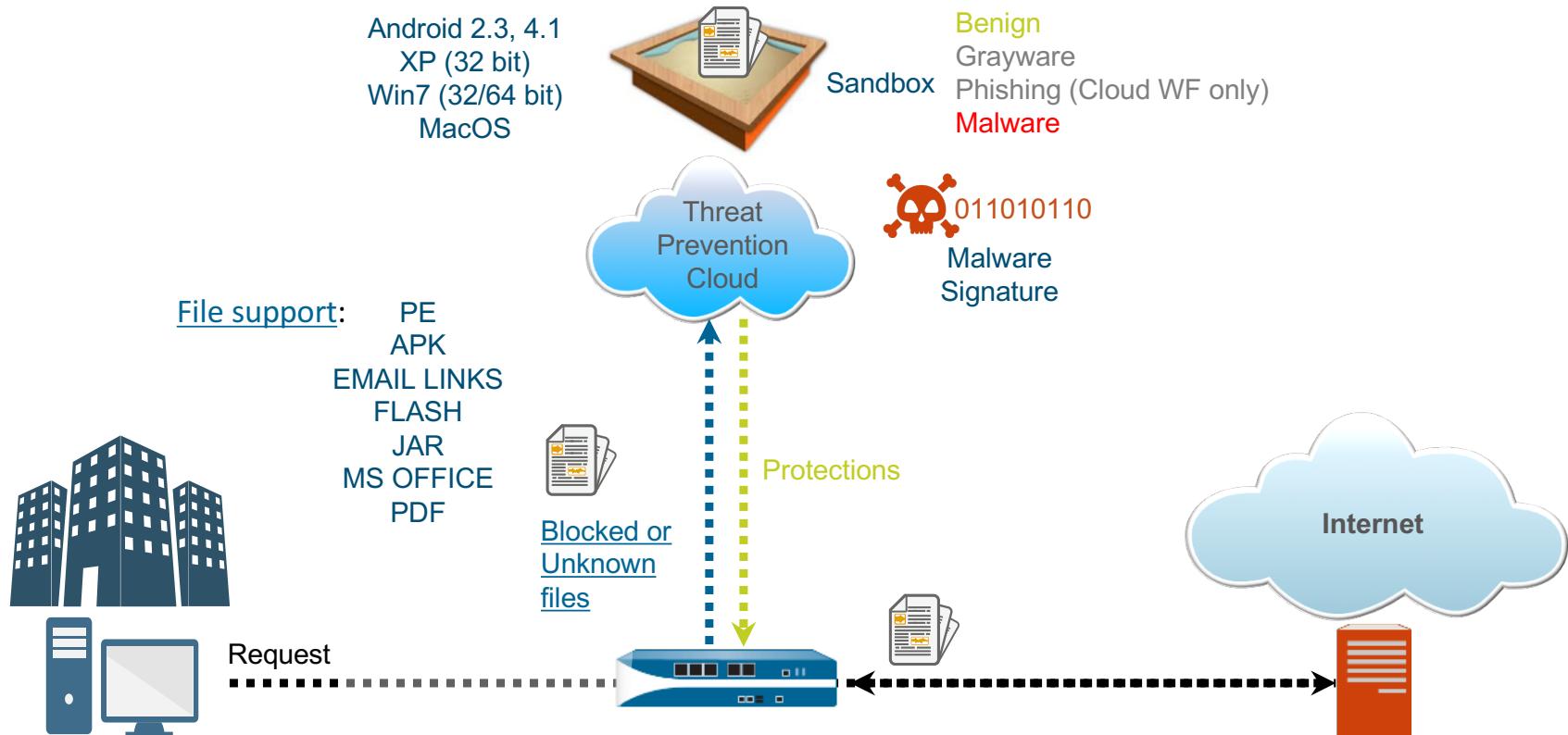
PAN-DB Private Offline Database Server

- Conforms to the strictest of security requirements
 - When no outside connectivity is allowed
- Complete privacy
 - Your URL usage is private
 - Not shared or collected as part of a public online metric
- Same functions and capabilities as the online version of PAN-DB
- Supported on the M-500 only.



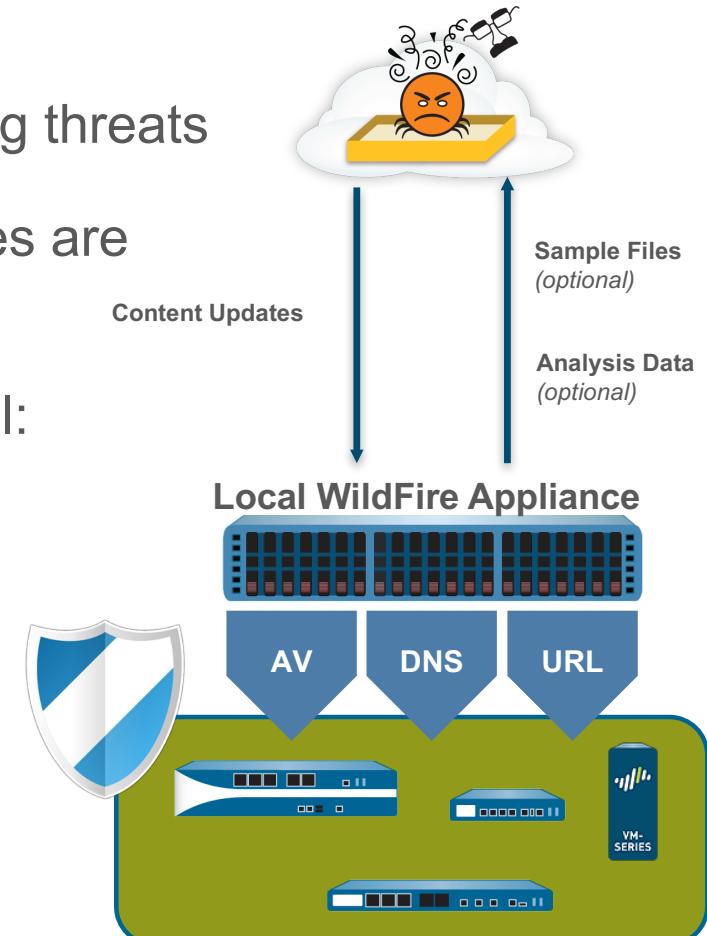
Wildfire

Wildfire



Wildfire Retention

- We receive feeds from over 55 sources regarding threats
- 250,000 files per day from external threat sources are uploaded into WildFire
- We are refreshing signatures daily on the firewall:
 - Signature retention on the firewall
 - AV signatures – 1M
 - WF signatures – 100K
 - DNS signatures – 100K

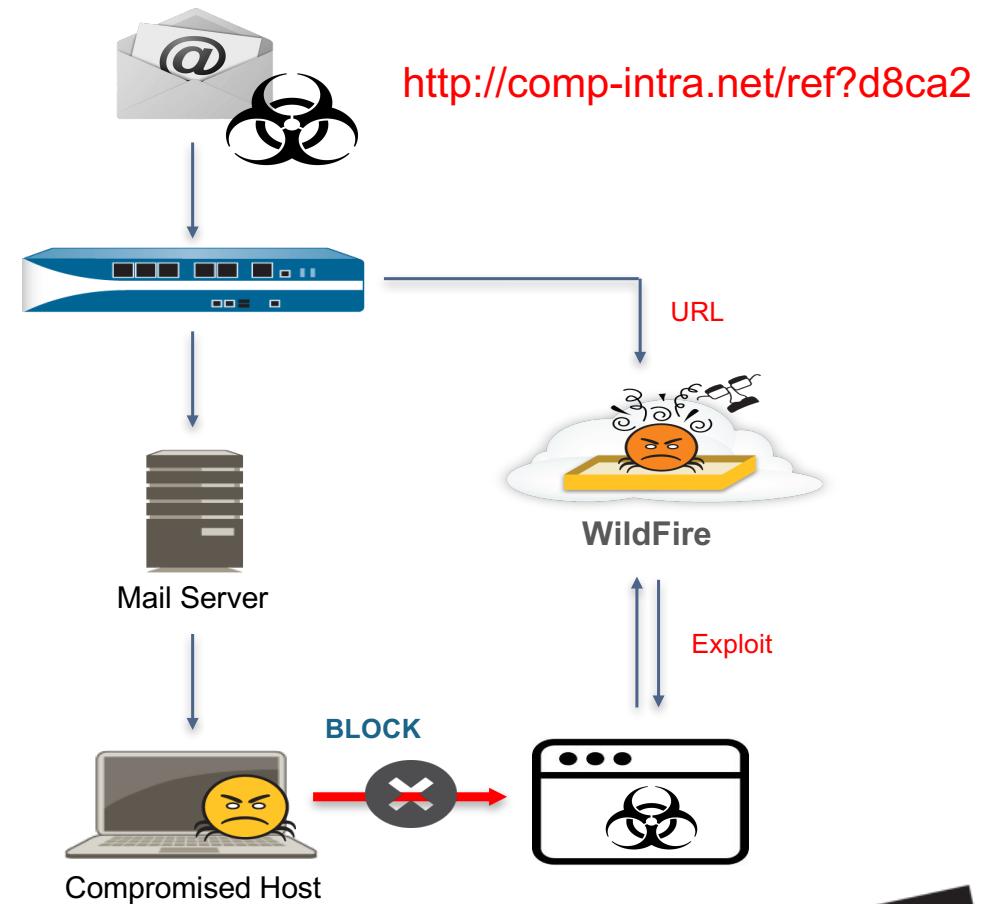


Wildfire Techniques

- WildFire performs static analysis
 - Static analysis occurs on files such as Office, PDF and Flash
 - Checks are for macros, embedded files, embedded code, anomalies in file structure
- WildFire signatures are resistant to polymorphism
 - WildFire loads / executes each sample
 - Don't rely on hashes, file names or content that can be changed
 - Based on the payload of the sample
- Recursion is supported in versions 6.x (up to 2) and 7.x (up to 4)

Identify and Protect Against Malicious Email Links

- PAN-OS firewalls detect and send Web links in suspicious emails to WildFire
- WildFire visits the Web page and analyzes the traffic to detect exploits and malware
- Available service with all solutions
 - WildFire public cloud
 - WildFire WF-500
 - Hybrid cloud solution



WF-500

Cloud innovation will always be faster



- Custom hypervisor
- Bare Metal analysis
- Support for Mac and APK file analysis



WF-500 appliance

- Local sample analysis

WF-500

Why Deploy On-Premises



Regulations



Data Privacy



IT Philosophy

privacyteam@paloaltonetworks.com

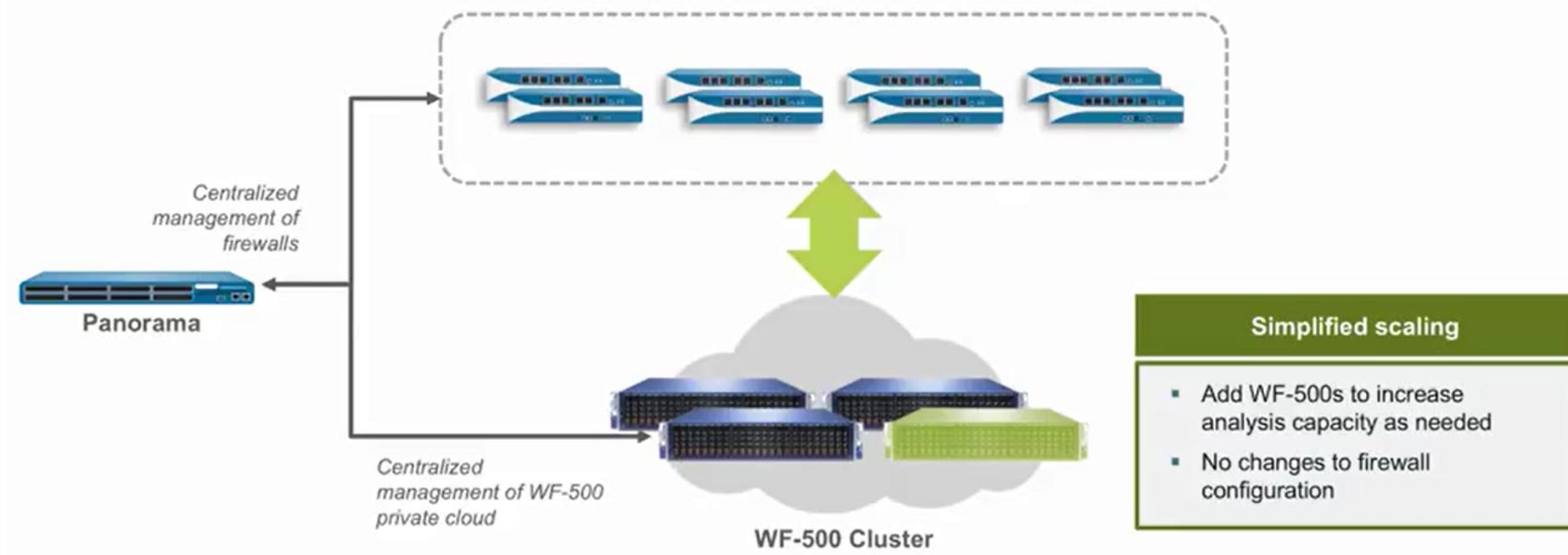


WF-500

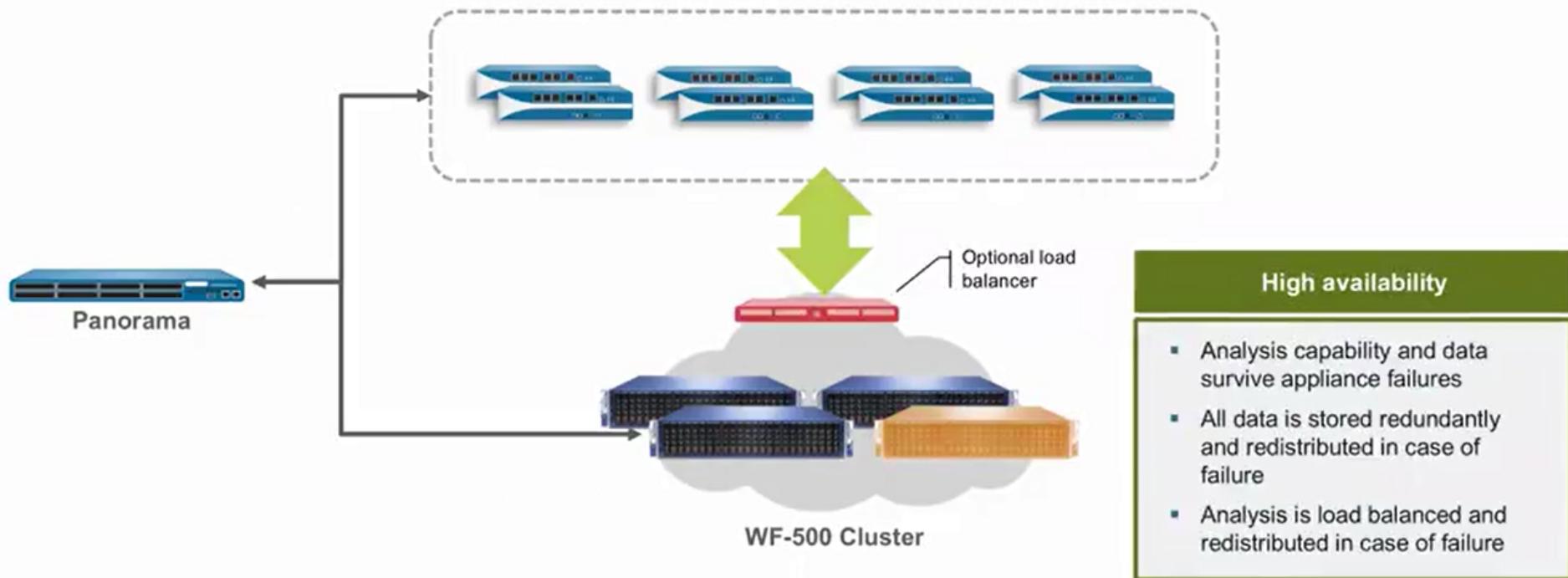


- Receive / Analyze files from up to 100 firewalls
- Handle ~10k dynamic analysis sessions / day
- Can buffer files if temporarily overwhelmed (~1000 files)
- Option to manually load files (WF portal) or use WF API

WF-500 > 8.0.1 > Cluster



WF-500 > 8.0.1 > Cluster



WF-500 > 8.0.1 > Cluster

Setup	Capacity
Stand-alone mode	6,500 files/day
Stand-alone device (cluster mode)	6,000 files/day
2-device cluster	12,000 files/day
3-device cluster	15,000 files/day
4-device cluster	21,000 files/day
4+N device cluster	N(6,000) files/day

- A single node can register up to 100 firewalls.
- Up to 20 nodes can be clustered

WF-500 > 8.0.1 > Cloud Query

- Send hash of file to WildFire Cloud to determine if it has been seen before.
 - If found:
 - Download previous verdict
 - Download report and associated files
 - Generate local signature
 - If not found:
 - Continue with local analysis
- WildFire can override verdicts
 - WF Cloud can override local verdicts
 - Manually override WF cloud verdict with WF appliance verdict

WildFire Licensing

	WildFire	WildFire Subscription
Use of WildFire cloud for PE analysis	✓	✓
Daily signature feed	✓	✓
WildFire logs integrated within PAN-OS	✓	✓
Use of WildFire cloud for all other file types (PDF, Office, APK*, Java)		✓
5-min signature feed (previously 15)		✓
WildFire API* key		✓
Use of WF-500		✓

Reports

Botnet Report

- Activity on Known Malware Sites
- Presence of Dynamic DNS
- Browsing to IP domains Instead of URL
- Visiting Recently Registered Domains
- Executable files from unknown sites
- Unknown TCP/UDP
- IRC traffic

Botnet Configuration

HTTP Traffic

Event	Enable	Count	Description
Malware URL visit	<input checked="" type="checkbox"/>	5	Identifies users communicating with known malware URLs based on Malware and Botnet URL filtering categories
Use of dynamic DNS	<input checked="" type="checkbox"/>	5	Looks for dynamic DNS query traffic which could be indicative of botnet communication
Browsing to IP domains	<input checked="" type="checkbox"/>	10	Identifies users that browse to IP domains instead of URLs
Browsing to recently registered domains	<input checked="" type="checkbox"/>	5	Looks for traffic to domains that have been registered within the last 30 days
Executable files from unknown sites	<input checked="" type="checkbox"/>	5	Identifies executable files downloaded from unknown URLs

Unknown Applications

Unknown TCP		Unknown UDP	
Sessions Per Hour	10 [1 - 3600]	Sessions Per Hour	10 [1 - 3600]
Destinations Per Hour	10 [1 - 3600]	Destinations Per Hour	10 [1 - 3600]
Minimum Bytes	50 [1 - 200]	Minimum Bytes	50 [1 - 200]
Maximum Bytes	100 [1 - 200]	Maximum Bytes	100 [1 - 200]

Other Applications

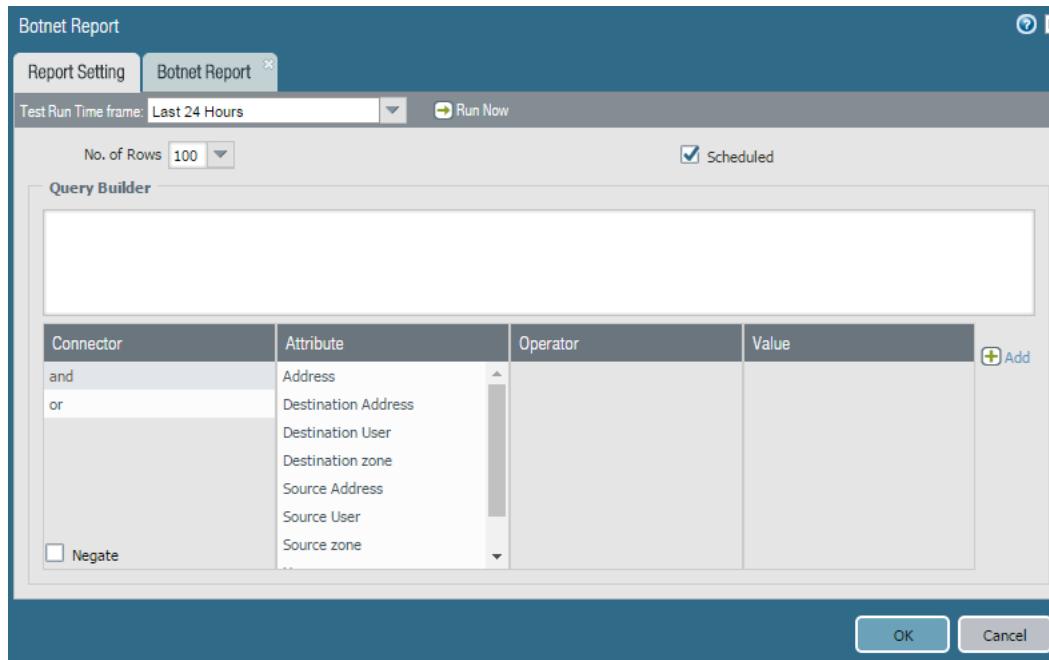
IRC

OK Cancel

	Source Address	Source Host Name	Source User	Destination Address	Destination			
1	10.31.33.131	10.31.33.131		10.31.33.26	10.31.33.26	95.4M	17.5k	
2	10.31.33.26	10.31.33.26		8.8.8.8	google-public-dns-a.google.com	1.7M	6.8k	
3	172.16.33.226	172.16.33.226		4.2.2.1	a.resolvers.level3.net	482.5k	2.3k	
4	10.31.33.26	10.31.33.26		10.31.33.130	ca1rama	40.5M	1.3k	
5	15.0.0.203	15.0.0.203		15.0.0.255	15.0.0.255	286.3k	414	
6	10.31.33.26	10.31.33.26		184.72.53.186	ec2-184-72-53-186.us-west-1.compute.amazonaws.com	3.2M	375	
7	10.31.33.26	10.31.33.26		50.18.183.118	ec2-50-18-183-118.us-west-1.compute.amazonaws.com	3.1M	347	
8	15.0.0.201	15.0.0.201		15.0.0.255	15.0.0.255	73.3k	297	
9	172.16.33.226	172.16.33.226		172.16.33.255	172.16.33.255	58.9k	235	
10	10.31.33.12	10.31.33.12		10.31.33.255	10.31.33.255	58.8k	235	
11	15.0.0.204	15.0.0.204		15.0.0.255	15.0.0.255	62.4k	225	

Schedule Botnet Report

- Schedule a report to run nightly against log data
- Investigate all hosts with a high confidence score



WildFire Dashboard



WILDFIRE

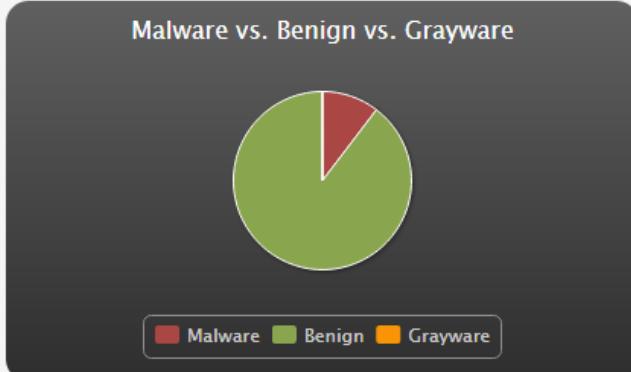
[Dashboard](#)[Reports](#)[Upload Sample](#)[Settings](#)[Account](#)

Ha, Nguyen-Hung ▾

DASHBOARD

Update your timezone preference in [Settings](#) to show report timestamps in your timezone.

PREVIOUS 1 HOUR



Source	Malware	Benign	Grayware	Registered
Manual	12	348	0	
007200002792	680	522	0	2016-03-30 20:37:08
007200002525	611	7	0	2016-03-25 19:20:41
001701003221	16	0	0	2016-03-29 23:43:14
001901001137	1	32	2	2016-03-30 10:01:32
0008C101950	1	16	0	2016-03-30 16:54:51
0011C101628	1	6	0	2016-03-30 12:18:58
001701000852	1	192	0	2016-03-30 19:09:25
001801025951	0	56	0	2016-03-25 16:00:00
0009C101912	0	202	0	2016-03-25 15:59:32
001606035396	0	19	0	2016-03-25 15:59:42



WildFire Reports



WILDFIRE



REPORTS

Source Any

Verdict Any

Reset Search

Prev 1 2 3 4 ... 100 Next 20 ▼

Received Time	Source	File / URL	Verdict
2016-03-30 20:38:38	001901001577	service.morphotak.com/content/software/Configuration%20Tool/Co	Benign
2016-03-30 20:38:37	0003C104846	imasdk.googleapis.com/flash/sdkloader/adsapi_3.swf	Benign
2016-03-30 20:38:37	0009C101289	200.242.37.2/os2pdf/usuarios/G166041/emitido/IMPRTEL_A_4837.pdf	Pending
2016-03-30 20:38:36	0008C100647	mail.uol.com.br/attachment?msg_id=MTA2NTU&ctype=PROJETO+GREMIO+	Benign



WildFire Submissions Log

Monitor > Logs > WildFire Submissions

The screenshot shows the 'Logs' section of the Palo Alto Networks interface. The 'WildFire Submissions' option is selected in the left sidebar. A table lists the following data:

Receive Time	File Name	Source Zone	Destinati... Zone	Attacker	Attacker Name	Victim	Desti... Port	Application	Rule	Verdict
12/18 10:42:12	vbaProject.bin	L3-Trust1	L3-Untrust	172.16.33.226		173.194.126.150	443	gmail-base	SaaS-IWS	benign
12/18 10:42:12	vbaProject.bin	L3-Trust1	L3-Untrust	172.16.33.226		173.194.126.150	443	gmail-base	SaaS-IWS	benign
12/18 10:42:12	vbaProject.bin	L3-Trust1	L3-Untrust	172.16.33.226		173.194.126.150	443	gmail-base	SaaS-IWS	benign
12/18 10:40:12	5860174520a3a46974c750b52d7a56...	L3-Trust1	L3-Untrust	172.16.33.226		206.190.61.106	443	yahoo-mail	SaaS-IWS	malicious
12/18 10:34:15	deadd7daf4d56ffff65a05c4155a41e4...	L3-Trust1	L3-Untrust	172.16.33.226		173.194.126.150	443	gmail-base	SaaS-IWS	malicious

Use the CLI to verify the successful uploading of a file. From the CLI, enter the **debug wildfire upload-log** command

The PuTTY terminal window shows the following command and its output:

```
student72@Student-72>
student72@Student-72>
student72@Student-72> debug wildfire upload-log

Public Cloud upload logs:
[Red box highlights the following line]
log: 0, filename: wildfire-test-pe-file.exe
processed 834 seconds ago, action: upload success
[Red box highlights the following line]
vsys_id: 1, session_id: 1005, transaction_id: 1
file_len: 55296, flag: 0x801c, file type: pe
threat id: 52020, user_id: 0, app_id: 109
from 192.168.72.51/50696 to 54.241.8.199/80
SHA256: a84ad2330a4fba46e1c507b0e69f71148018c6334ed673b64ad4d56fd43c274b

Private Cloud upload logs:

student72@Student-72>
```

Correlation Report

Correlation Objects

Title	Category	State	Description
Compromise Activity Sequence	compromised-host	active	This correlation object detects a host involved in a sequence of activity indicating remote compromise, starting with scanning or probing activity, progressing to exploitation, and concluding with network contact to a known malicious domain.
WildFire C2	compromised-host	active	This correlation object detects hosts that have exhibited command-and-control (C2) network behavior corresponding to malware detected by WildFire elsewhere on your network.
Beacon Detection	compromised-host	active	This correlation object detects likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to recently registered domains or dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc.
Exploit Kit Activity	compromised-host	active	This object detects probable exploit kit activity targeted at a host on the network. Exploit kits are identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature.
Exploit Kit Delivering XOR obfuscated malware	compromised-host	active	This correlation object detects exclusive-or (XOR) obfuscated malware downloaded to a host. XOR obfuscation is a technique to evade detection by encrypting portions of a file in order to hide malicious code. This correlation object specifically identifies XOR obfuscated malware that is delivered to the host by an exploit kit. While the Exploit Kit Activity object detects exploit kits combined with either a malware download signature or a known command-and-control signature, this object is provided to specifically detect an event where XOR obfuscation malware inserted on a host by an exploit kit and to distinguish such an event from other exploit kit activities.
WildFire Correlated C2	compromised-host	active	This correlation object detects hosts that have received malware detected by WildFire, and have also exhibited command-and-control (C2) network behavior corresponding to the detected malware.

- Correlation Events are logged when traffic matches a correlation object

Match Time	Update Time	Object Name	Source address	Source User	Severity	Summary
2015/02/04 11:20:35	2015/02/04 11:41:10	C2 Detected	192.168.61.51	panqa\aa...	high	Host visited 101 URLs including: hawet.zapto.org/,hawet.zapto.org/,hawet.zapt...
2015/02/03 21:35:47	2015/02/04 09:17:39	Compromise Lifecycle	192.168.61.51	panqa\aa...	critical	Host appears to be compromised based on a sequence of recent threat log activity.
2015/02/03 21:43:44	2015/02/04 09:17:29	Beacon Detection	192.168.61.51	panqa\aa...	high	Host repeatedly visited malware domains (100).
2015/01/28 17:17:02	2015/01/28 17:25:06	Compromise Lifecycle	192.168.61.51	panqa\yos...	critical	Host appears to be compromised based on a sequence of recent threat log activity.
2015/01/28 17:16:35	2015/01/28 17:16:35	Compromise Lifecycle	192.168.61.51	panqa\yos...	critical	Host appears to be compromised based on a sequence of recent threat log activity.
2015/01/28 16:31:25	2015/01/28 17:14:11	Beacon Detection	192.168.61.51	panqa\jui...	high	Host repeatedly visited malware domains (100).
2015/01/28 16:21:49	2015/01/28 16:21:49	Compromise Lifecycle	192.168.61.51	panqa\jui...	critical	Host appears to be compromised based on a sequence of recent threat log activity.
2015/01/28 14:54:44	2015/01/28 15:24:11	Beacon Detection	192.168.61.51	panqa\jui...	high	Host repeatedly visited malware domains (100).
2015/01/28 13:55:25	2015/01/28 14:53:00	Beacon Detection	192.168.61.51	panqa\do...	high	Host repeatedly visited malware domains (100).
2015/01/28 11:15:54	2015/01/28 11:20:10	C2 Detected	192.168.61.51	panqa\do...	high	Host visited 103 URLs including: hawet.zapto.org/,hawet.zapto.org/,hawet.zapt...
2015/01/22 15:41:25	2015/01/28 10:51:15	C2 Detected	192.168.61.51	panqa\pla...	high	Host visited 101 URLs including: hawet.zapto.org/,hawet.zapto.org/,hawet.zapt...
2015/01/26 17:40:56	2015/01/26 23:10:00	Beacon Detection	134.154.10.201		low	Host is generating unknown TCP or UDP network traffic.
2015/01/26 23:09:57	2015/01/26 23:09:57	Beacon Detection	134.154.254.64		low	Host is generating unknown TCP or UDP network traffic.

ACC Correlation Events

The screenshot shows the Palo Alto Networks Advanced Correlation Center (ACC) interface. The top navigation bar includes tabs for Dashboard, ACC (which is selected), Monitor, Policies, Objects, Network, and Device. Below the tabs are buttons for Commit, Save, and Search, along with an Auto Refresh checkbox and a Help link. A color-coded scale from 1 (green) to 5 (red) is displayed with a value of 3.1. The main content area is titled "Compromised Hosts" and lists several entries:

Severity	Host	User	Matching Objects	Match Count
CRITICAL	192.168.61.51	kingsbeach	Beacon Detection, Compromise Lifecycle	2
CRITICAL	192.168.61.51	yosemite	Compromise Lifecycle	1
CRITICAL	192.168.61.51	yosemitiae	Compromise Lifecycle	1
HIGH	192.168.61.51	donnerlake	Beacon Detection	1
HIGH	192.168.61.51	placerville	C2 Detected	1
LOW	134.154.10.201		Beacon De	1

A tooltip for the "C2 Detected" entry for host 192.168.61.51 provides the following description:

This correlation object detects hosts that have exhibited command-and-control (C2) network behavior corresponding to malware detected by WildFire elsewhere on your network.

What the Correlation Engine is NOT

- It is not a statistical based correlation engine
 - The goal is **not** to establish baselines and look for anomalies
 - Therefore there is **no** threshold alerting
- It is not user definable
 - All of the correlations are defined internally and should be relevant to all customers
 - This means we will **not** create a correlation object that would only be meaningful to a small subset of customers
- It is not a true AI system
 - The correlation engine is **not** a cognitive learning engine looking at the network and finding malware behavior
 - The engine does **not** improve automatically through experience

Configuration Best Practices

- A poorly configured firewall is vulnerable.
- A firewall left with Default Configs is vulnerable.
- Refer to the following document for Configurational Best Practices designed to address L4 and L7 Evasions:

<https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/threat-prevention/best-practices-for-securing-your-network-from-layer-4-and-layer-7-evasions.html>