digitalscepter

PAN-OS Best Practices Workshop

ZACHRY SUM - DIRECTOR OF TECHNICAL SERVICES, DIGITAL SCEPTER
JON ROBINSON - PRESIDENT, DIGITAL SCEPTER
October 11th, 2023

About Digital Scepter

- Security focused network integrator
- Palo Alto Networks experts since 2007
- Specialized in K-12 deployments
- Working with over 100 districts, COEs, cities and counties

Agenda

- **Advanced Subscriptions** - difference compared to original subscriptions
- **Best Practices** - recommendations for different features across the platform
- **Zero Trust** - defined and how to configure
- **SSL Decryption** - breakdown of SSL outbound and inbound inspection
- **Network Segmentation** - brief overview of benefits to network segmentation and methods of implementation
- **GUI Walkthrough/Demos** - Review location of configuration items discussed and feature demonstrations

Advanced Subscriptions

Advanced Subscriptions and Machine Learning

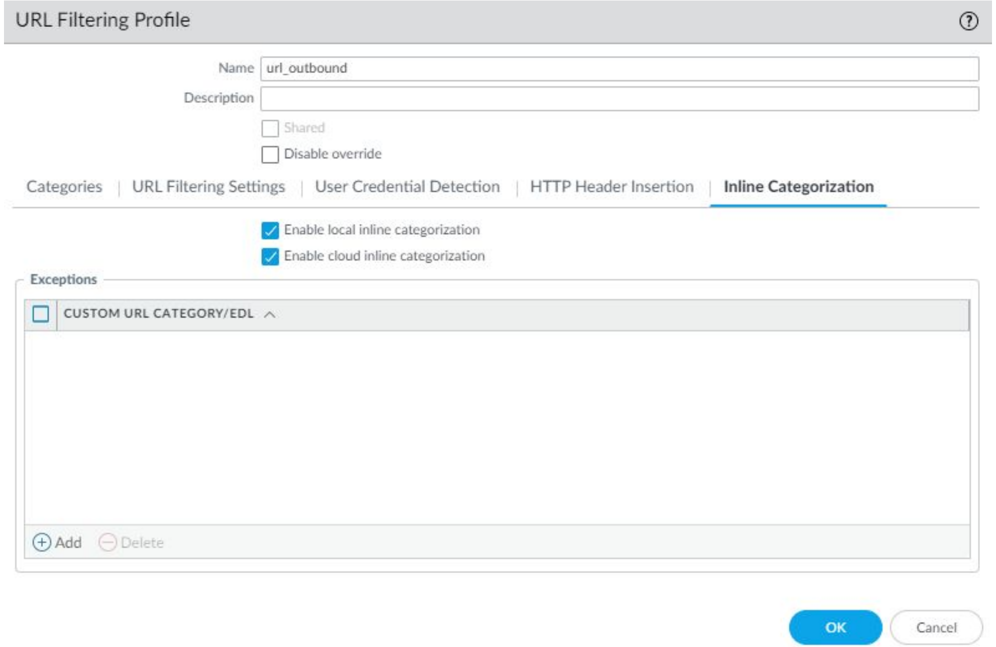
- Palo Alto has a cloud-native system of machine learning models that they can train and retrain using the massive amounts of data they collect from all of the 85,000+ customer around the globe and 42,000+ Wildfire users
- These models are focused on certain threats, e.g. command and control, SQLi, social engineering, etc.
- The architecture takes advantage of Intel 3rd gen Xeon CPUs and ML software development frameworks
- This ML powered analysis is incorporated in the cloud threat analysis and inline on the firewall in aspects of Advanced Wildfire, Advanced URL, Advanced Threat and DNS Security

Advanced URL Filtering

- Examples of analysis include javascript exploits and phishing attacks
- These will be expanded in the future
- Real-time protection delivered without impacting the user

Advanced URL Filtering will uncover attackers that were cloaking their attacks from web-crawlers and attacks that use new and unknown domains and URLs for phishing attacks.

Advanced URL Filtering



URL Filtering Profile

Name: url_outbound

Description:

□ Shared

□ Disable override

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | **Inline Categorization**

☑ Enable local inline categorization

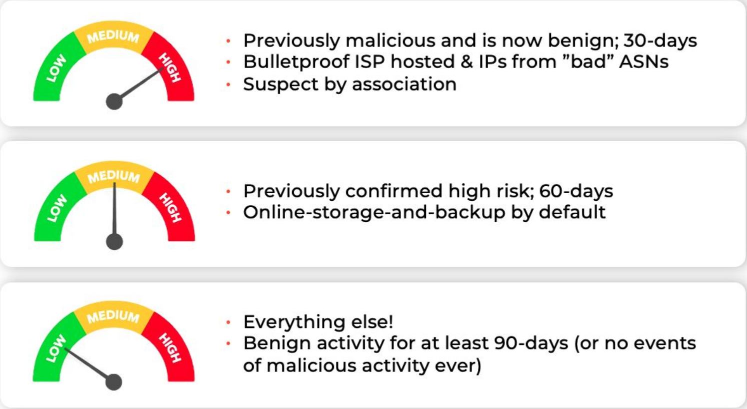
☑ Enable cloud inline categorization

Exceptions

□	CUSTOM URL CATEGORY/EDL

Advanced URL Filtering

- This will obviously be enhanced by SSL decryption.
- Palo Alto has risk-categories now that can be used to selectively apply SSL decryption short of a complete roll-out. For example, perform SSL Decryption on high and medium risk URL categories only.



- Previously malicious and is now benign; 30-days
- Bulletproof ISP hosted & IPs from ”bad” ASNs
- Suspect by association

- Previously confirmed high risk; 60-days
- Online-storage-and-backup by default

- Everything else!
- Benign activity for at least 90-days (or no events of malicious activity ever)

Advanced Threat Prevention

- Advanced Threat Prevention is integrated with Palo Alto’s cloud-based threat analysis infrastructure, like Advanced URL filtering
- The ML-Models now run deep-learning on live traffic
- First ML-models focus on command-and-control (C2) tactics like those used by Cobalt Strike. Stops 96% of these new tactics. 48% improvement over regular TP tactics
- PAN-OS Nova (11.0) adds ML models to focus on injection attacks. 90% of attacks stopped on unpatched systems and 60% improvement on 0-day injection attacks.
- ML models have to be trained. Palo Alto has the largest pile of threat analysis thanks to Wildfire and a huge customer base. The cloud security infrastructure will be improved with more threat models in the future.

Advanced Threat Prevention

- New models also analyse the SSL handshake to detect threats based on malicious flows and handshake info. This is an improvement that helps everyone not just SSL Decrypting networks
- Unknown C2 detection is focused on http, ssl, unknown-tcp, and unknown-udp apps

Advanced Threat Prevention

https://www.bleepingcomputer.com/news/security/alleged-source-code-of-cobalt-strike-toolkit-shared-online/

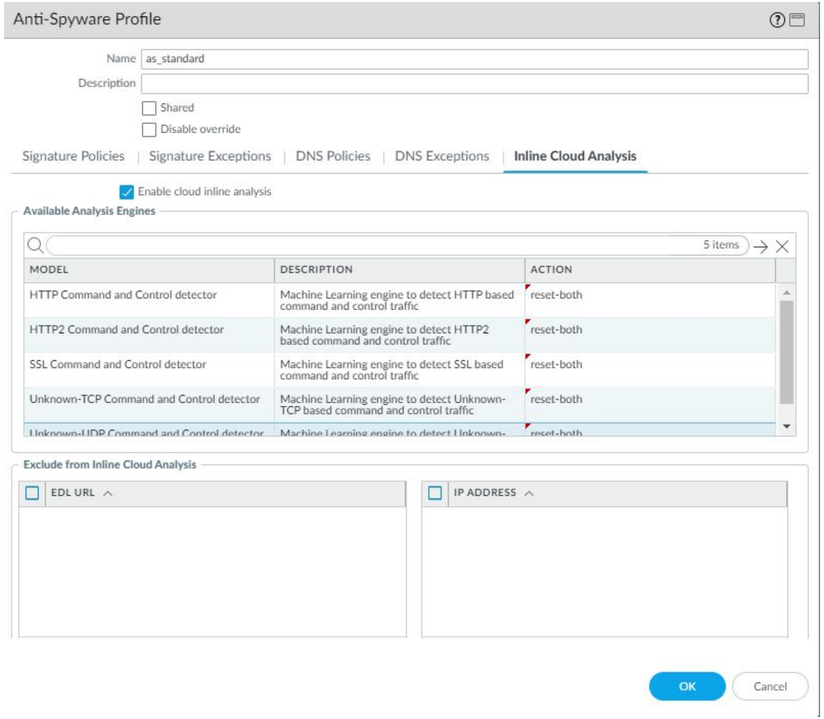
- Cobalt Strike source code leaked in 2020. This allowed anyone to more easily fire up attack networks, command-and-control servers, and distribute ransomware
- Cobalt Strike was used in multiple attacks including Solarwinds, Colonial Pipeline, Microsoft Exchange and Kaseya.
- Cobalt Strike is evasive and makes it easy to perform zero-day exploits
- Attackers use Cobalt Strike and other tools to automate attacks that look like normal traffic to old methods of Threat Prevention

Advanced Threat Prevention

Action plan:

- License Advanced Threat Prevention
- Enable inline ML models on anti-spyware and vulnerability protection security profiles
- Enable outbound/inbound SSL Decrypt to ensure threat prevention is applied to encrypted traffic

Advanced Threat Prevention



Anti-Spyware Profile

Name: as_standard

Description:

□ Shared

□ Disable override

Signature Policies | Signature Exceptions | DNS Policies | DNS Exceptions | **Inline Cloud Analysis**

☑ Enable cloud inline analysis

Available Analysis Engines

5 items

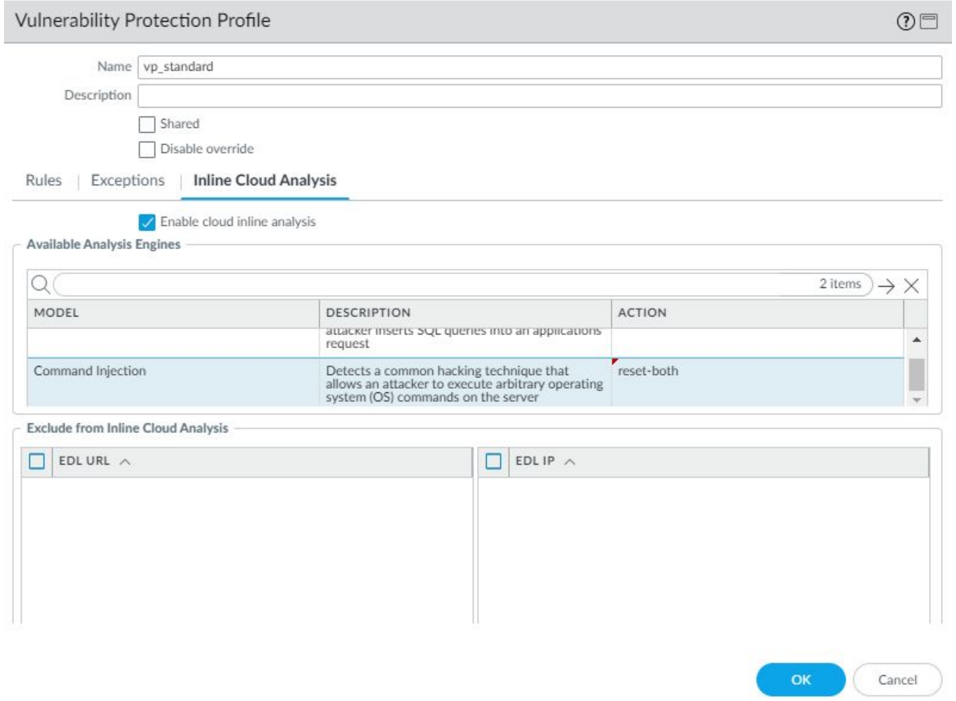
MODEL	DESCRIPTION	ACTION
HTTP Command and Control detector	Machine Learning engine to detect HTTP based command and control traffic	reset-both
HTTP2 Command and Control detector	Machine Learning engine to detect HTTP2 based command and control traffic	reset-both
SSL Command and Control detector	Machine Learning engine to detect SSL based command and control traffic	reset-both
Unknown-TCP Command and Control detector	Machine Learning engine to detect Unknown-TCP based command and control traffic	reset-both
Unknown-UDP Command and Control detector	Machine Learning engine to detect Unknown-	reset-both

Exclude from Inline Cloud Analysis

□ EDL URL

□ IP ADDRESS

Advanced Threat Prevention



Vulnerability Protection Profile

Name: vp_standard

Description:

☐ Shared

☐ Disable override

Rules | Exceptions | **Inline Cloud Analysis**

☑ Enable cloud inline analysis

Available Analysis Engines

2 items

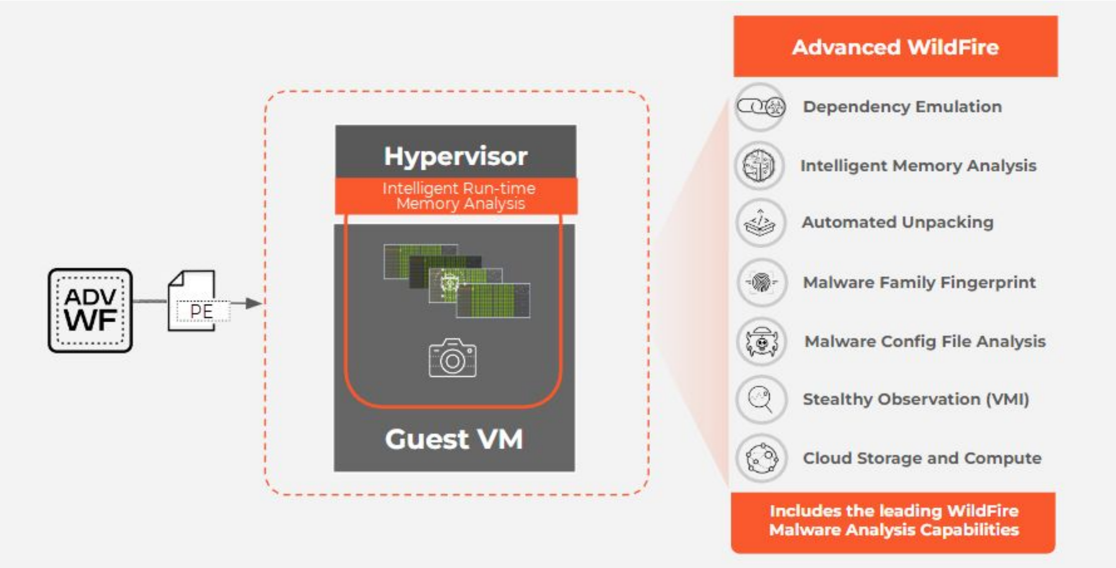
MODEL	DESCRIPTION	ACTION
	attacker inserts SQL queries into an applications request	
Command Injection	Detects a common hacking technique that allows an attacker to execute arbitrary operating system (OS) commands on the server	reset-both

Exclude from Inline Cloud Analysis

☐ EDL URL	☐ EDL IP

Advanced Wildfire

- Adds Intelligent Run-time Memory Analysis to Wildfire submissions


ADV WF
PE
Hypervisor
Intelligent Run-time Memory Analysis
Guest VM
Advanced WildFire
Dependency Emulation
Intelligent Memory Analysis
Automated Unpacking
Malware Family Fingerprint
Malware Config File Analysis
Stealthy Observation (VMI)
Cloud Storage and Compute
Includes the leading WildFire Malware Analysis Capabilities

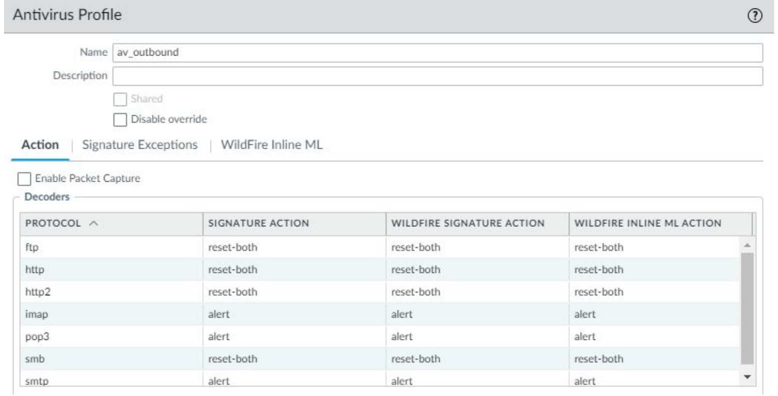
Best Practices

Security Profiles

- Create security profile groups based on direction of traffic flow, e.g. inbound, outbound, or internal traffic
- Likewise, create security profile groups based on direction and attach these to appropriate policies
- Exceptions on security profiles should be made as specific as possible to avoid broadly disabling protections

Antivirus

- Reset-both should be default for http, http2, ftp, and smb
- Reset-both can and should be set for imap, pop3, and smtp if it won't interfere with corporate mail flow–this should be handled by spam filter so you don't lose quarantine capability
- Signature Action column requires TP or advanced TP subscription, Wildfire Action columns require WF subscription



Antivirus Profile

Name: av_outbound

Description:

□ Shared

□ Disable override

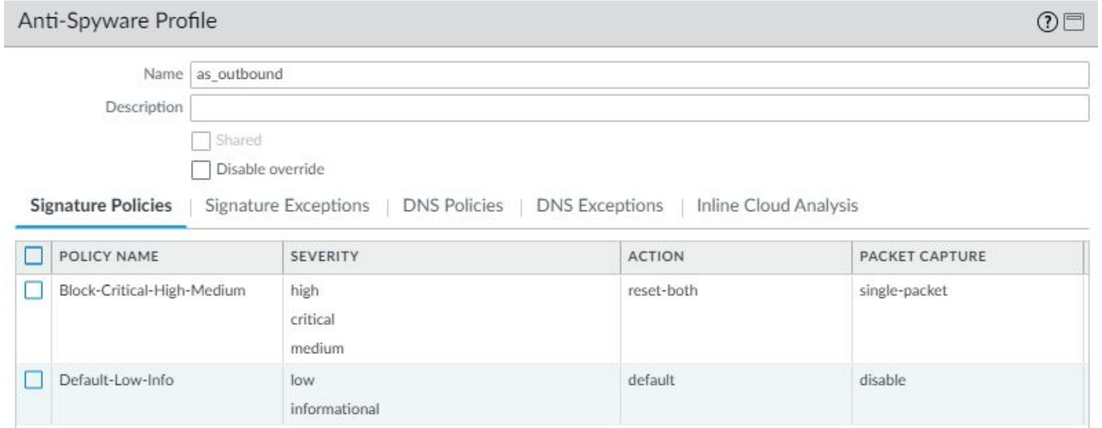
□ Enable Packet Capture

Decoders

PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
ftp	reset-both	reset-both	reset-both
http	reset-both	reset-both	reset-both
http2	reset-both	reset-both	reset-both
imap	alert	alert	alert
pop3	alert	alert	alert
smb	reset-both	reset-both	reset-both
smtp	alert	alert	alert

Anti-Spyware

- Reset-both should be used for critical, high, and medium
- Default (not alert) should be set for low and informational
- This requires Threat Prevention or Advanced Threat Prevention subscription



Anti-Spyware Profile

Name: as_outbound

Description:

□ Shared

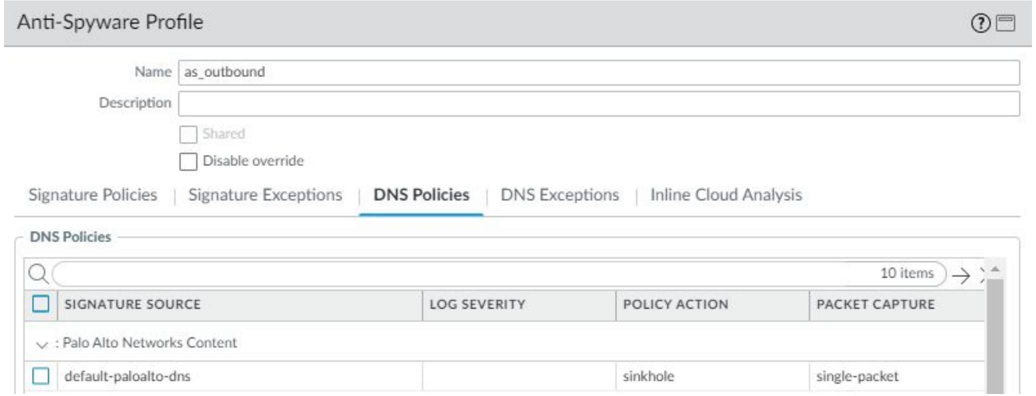
□ Disable override

Signature Policies | Signature Exceptions | DNS Policies | DNS Exceptions | Inline Cloud Analysis

□	POLICY NAME	SEVERITY	ACTION	PACKET CAPTURE
□	Block-Critical-High-Medium	high critical medium	reset-both	single-packet
□	Default-Low-Info	low informational	default	disable

Anti-Spyware

- Default-paloalto-dns signature source should be set to sinkhole. Block is also okay here, but sinkhole can offer additional visibility into infected endpoints on your network
- This requires Threat Prevention or Advanced Threat Prevention subscription



Anti-Spyware Profile

Name: as_outbound

Description:

□ Shared

□ Disable override

DNS Policies

10 items

□	SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
	: Palo Alto Networks Content			
□	default-paloalto-dns		sinkhole	single-packet

digitalscepter

URL Filtering

At a minimum, it is recommended to block the following URL categories:

- Adult
- Command-and-control
- Copyright-infringement
- Dynamic-dns
- Encrypted-dns
- Extremism
- Grayware
- Hacking
- Malware
- Parked
- Phishing
- Proxy-avoidance-and-anonymizers
- Ransomware
- Unknown (should review unknown URL logs prior to blocking this category)

URL Filtering

A note on blocking unknown URLs:

This is a great way to block new URLs that phishing attacks are using, but any of your apps using IP addresses instead of domain names may be categorized as unknown. Public sites that utilize source-based whitelisting will also show as unknown. Run a report ahead of time to see what this will block and make adjustments to security profiles to except them. Using separate profiles for internet traffic from datacenter traffic is recommended.

URL Filtering

It is recommended to consider blocking these URL categories:

- Newly-registered-domain
- Questionable

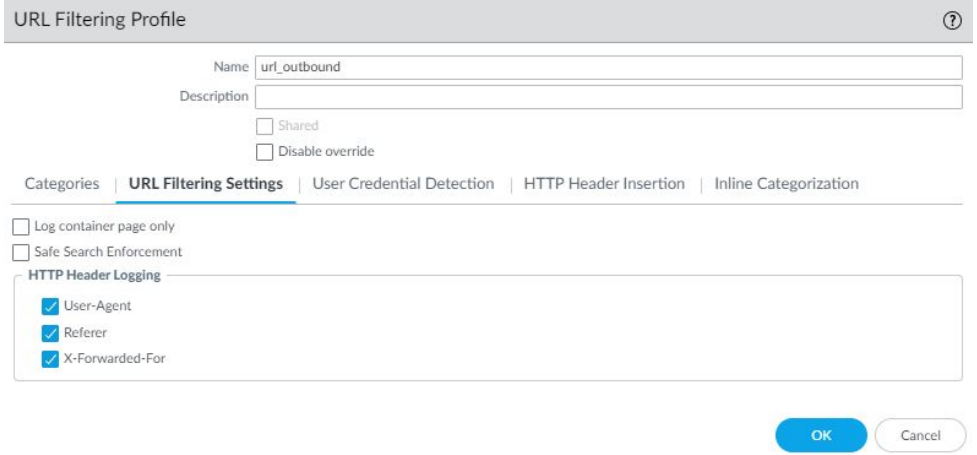
URL Filtering

It is recommended to alert on the remaining URL categories:

Important Note: Real-time-detection (requires Advanced URL sub) should be set to alert

URL Filtering

- Log container page only should be turned off if you want to maximize visibility
- HTTP Header Logging should be used if there are proxies on the network



URL Filtering Profile

Name: url_outbound

Description:

□ Shared

□ Disable override

□ Log container page only

□ Safe Search Enforcement

HTTP Header Logging

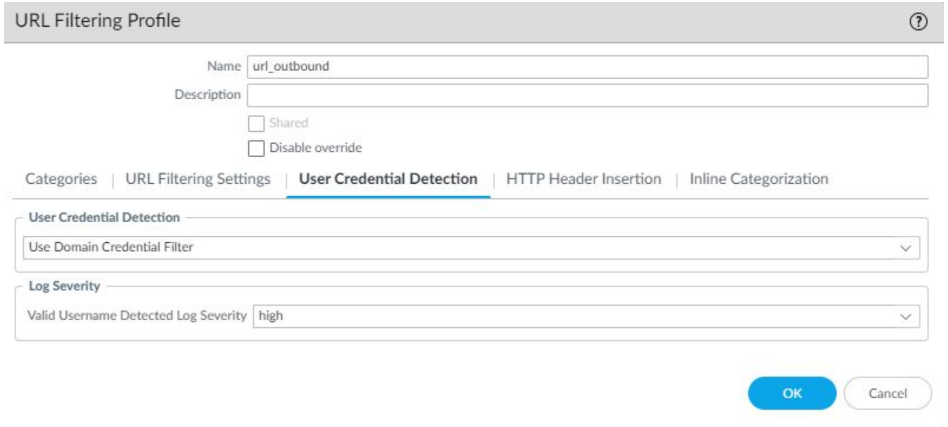
☑ User-Agent

☑ Referer

☑ X-Forwarded-For

URL Filtering

- Credential Theft Prevention should be enabled utilizing domain credential filter
- This requires a Server 2019 RODC on your network and works best in tandem with SSL Decryption



URL Filtering Profile

Name: url_outbound

Description:

□ Shared

□ Disable override

User Credential Detection: Use Domain Credential Filter

Log Severity

Valid Username Detected Log Severity: high

URL Filtering

Action plan:

- Make sure categories are not set to ‘allow’ (use ‘alert’ instead)
- Make sure any rules that permit traffic to leave your network have your outbound security profile group applied
- Leverage User-ID groups for permitting varying levels of internet access
- Enable Credential Theft Prevention to further reduce risk of phishing attacks and password reuse

File Blocking

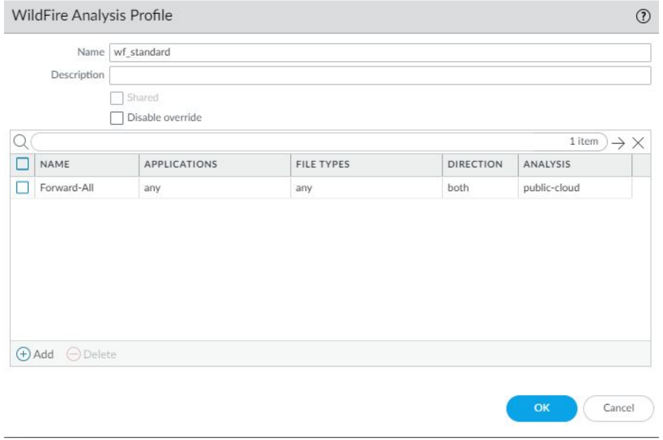
At a minimum, it is recommended to block the following file types:

- Chm
- Hlp
- multi-level -encoding
- Ocx
- Scr
- Torrent

Everything else should be set to alert

Wildfire

- It is recommended to forward all supported files to Wildfire for analysis
- Wildfire submission isn't necessarily required for internal traffic, although there are benefits



WildFire Analysis Profile

Name: wf_standard

Description:

□ Shared

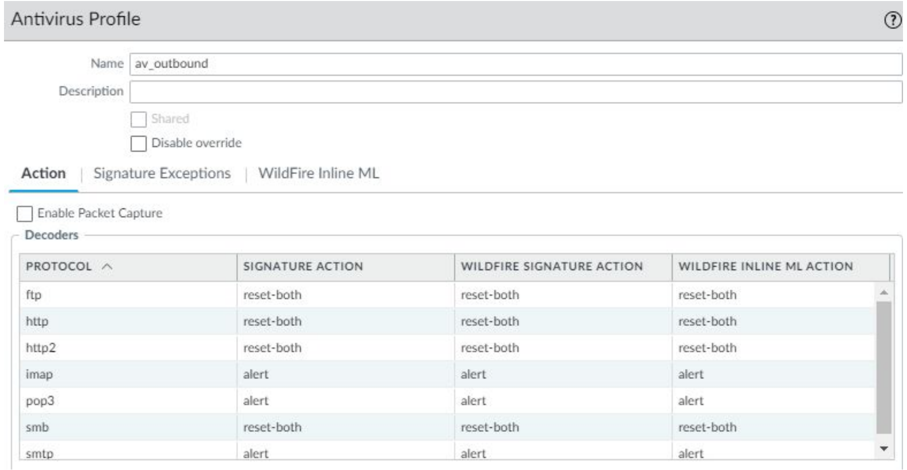
□ Disable override

1 item

□	NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
□	Forward-All	any	any	both	public-cloud

Wildfire

- Wildfire Signature action and inline ML action should be set identically to your antivirus signature action
- Wildfire Inline ML models should all be enabled



Antivirus Profile

Name av_outbound

Description

□ Shared

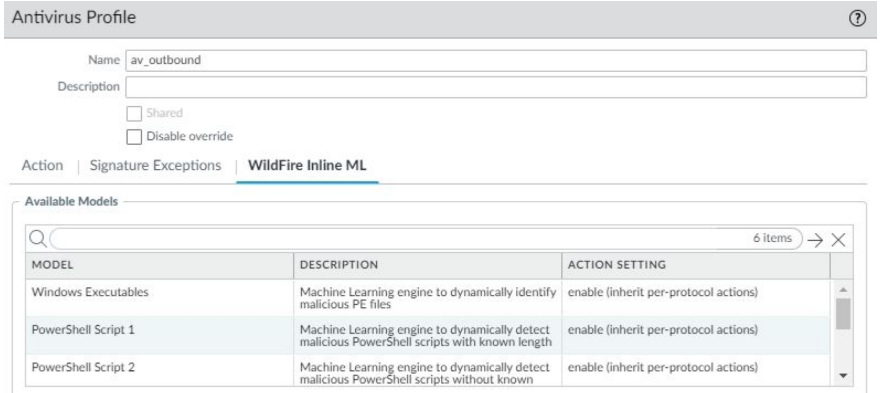
□ Disable override

Action | Signature Exceptions | WildFire Inline ML

□ Enable Packet Capture

Decoders

PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
ftp	reset-both	reset-both	reset-both
http	reset-both	reset-both	reset-both
http2	reset-both	reset-both	reset-both
imap	alert	alert	alert
pop3	alert	alert	alert
smb	reset-both	reset-both	reset-both
smtp	alert	alert	alert



Antivirus Profile

Name av_outbound

Description

□ Shared

□ Disable override

Action | Signature Exceptions | WildFire Inline ML

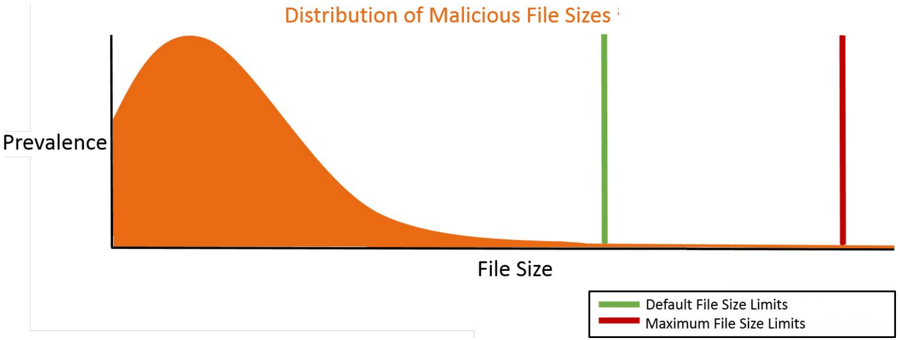
Available Models

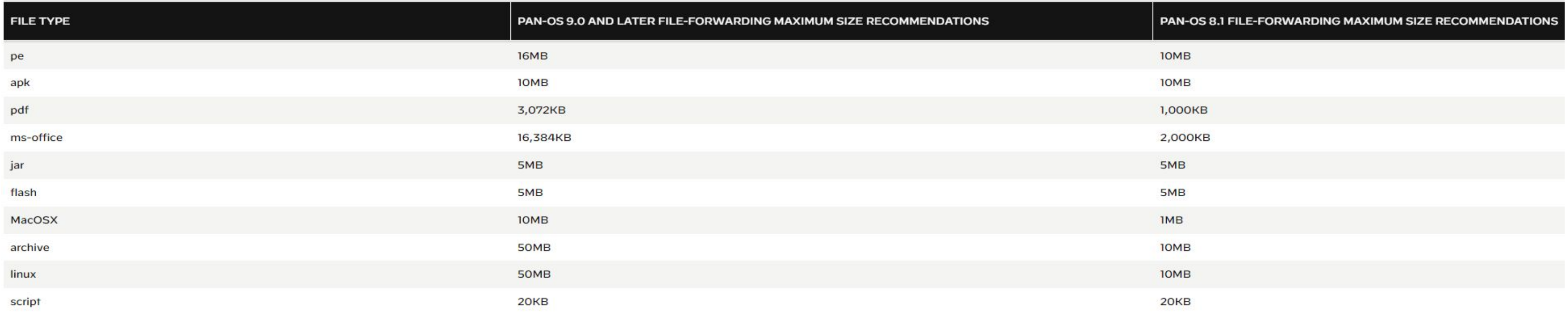
6 items

MODEL	DESCRIPTION	ACTION SETTING
Windows Executables	Machine Learning engine to dynamically identify malicious PE files	enable (inherit per-protocol actions)
PowerShell Script 1	Machine Learning engine to dynamically detect malicious PowerShell scripts with known length	enable (inherit per-protocol actions)
PowerShell Script 2	Machine Learning engine to dynamically detect malicious PowerShell scripts without known	enable (inherit per-protocol actions)

Wildfire

- PAN recommends setting file size limits to default values based on observed distribution of malware

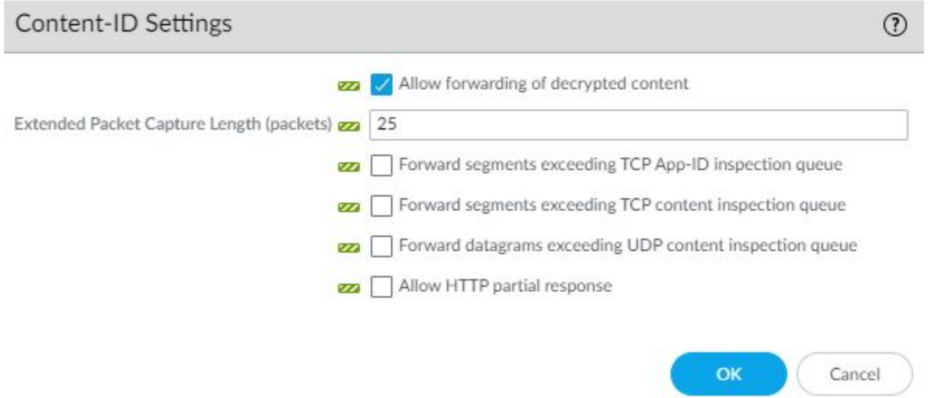




FILE TYPE	PAN-OS 9.0 AND LATER FILE-FORWARDING MAXIMUM SIZE RECOMMENDATIONS	PAN-OS 8.1 FILE-FORWARDING MAXIMUM SIZE RECOMMENDATIONS
pe	16MB	10MB
apk	10MB	10MB
pdf	3,072KB	1,000KB
ms-office	16,384KB	2,000KB
jar	5MB	5MB
flash	5MB	5MB
MacOSX	10MB	1MB
archive	50MB	10MB
linux	50MB	10MB
script	20KB	20KB

Wildfire

- Allow forwarding of decrypted content
  - Device > Setup > Content-ID



Content-ID Settings

☑ Allow forwarding of decrypted content

Extended Packet Capture Length (packets) 25

□ Forward segments exceeding TCP App-ID inspection queue

□ Forward segments exceeding TCP content inspection queue

□ Forward datagrams exceeding UDP content inspection queue

□ Allow HTTP partial response

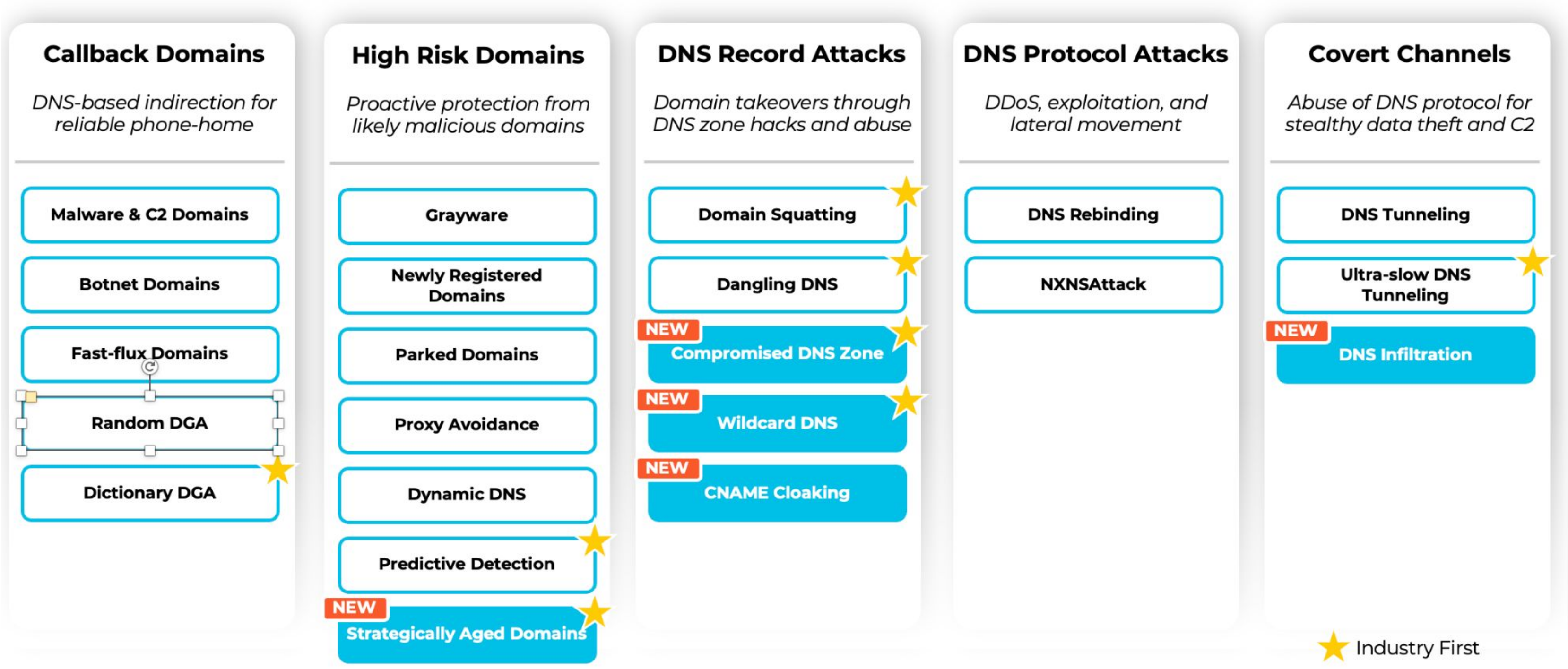
DNS Security

- DNS is fundamental to using any network
- Controlling DNS you can stop attacks at the beginning of the attack lifecycle but also in the middle and the end
- Palo Alto had a list of bad domains on the firewall based on intel from Wildfire, etc. but DNS Security now moves it to the cloud-based security architecture, which means the list size is basically infinite and takes advantage of the ML model architecture like the other subscriptions

DNS Security

- More than just blocking bad domains
- Looks at malicious usage of the protocol, e.g. tunneling
- Can see all DNS traffic through the box, not just from systems configured to use your approved DNS servers

DNS Security



Callback Domains

DNS-based indirection for reliable phone-home

- Malware & C2 Domains
- Botnet Domains
- Fast-flux Domains
- Random DGA
- Dictionary DGA ★

High Risk Domains

Proactive protection from likely malicious domains

- Grayware
- Newly Registered Domains
- Parked Domains
- Proxy Avoidance
- Dynamic DNS
- Predictive Detection ★
- NEW Strategically Aged Domains ★

DNS Record Attacks

Domain takeovers through DNS zone hacks and abuse

- Domain Squatting ★
- Dangling DNS ★
- NEW Compromised DNS Zone ★
- NEW Wildcard DNS ★
- NEW CNAME Cloaking

DNS Protocol Attacks

DDoS, exploitation, and lateral movement

- DNS Rebinding
- NXNSAttack

Covert Channels

Abuse of DNS protocol for stealthy data theft and C2

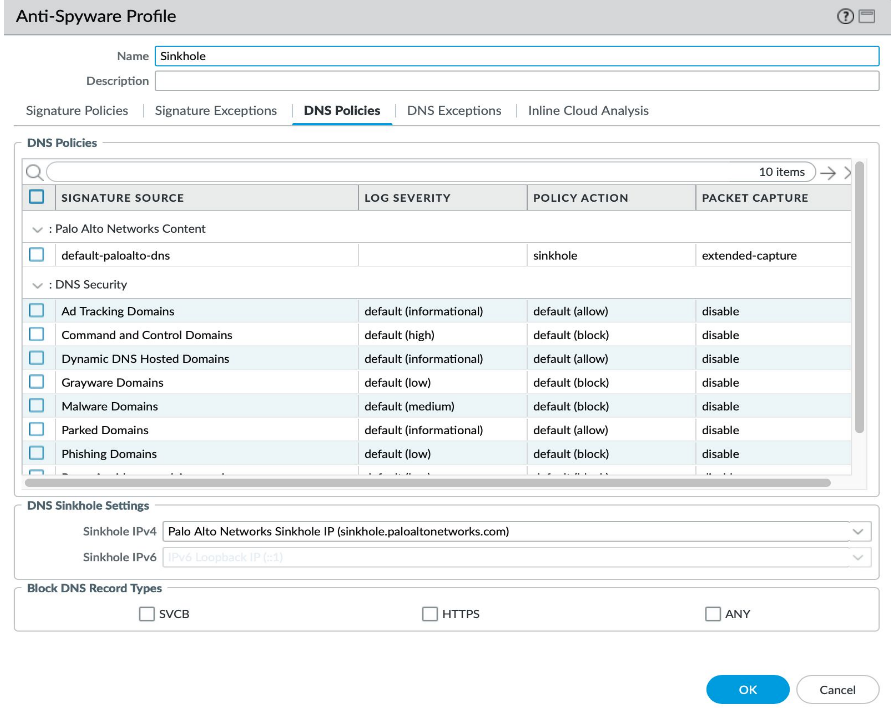
- DNS Tunneling
- Ultra-slow DNS Tunneling ★
- NEW DNS Infiltration

★ Industry First

DNS Security

- Since malicious DNS requests are indicators of compromise, it’s a good input for automating response, e.g. adding the IP address to a block list for limited network access, send to endpoint tools, etc.

DNS Security



Anti-Spyware Profile

Name: Sinkhole

Description:

Signature Policies | Signature Exceptions | **DNS Policies** | DNS Exceptions | Inline Cloud Analysis

DNS Policies

10 items

□	SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
	: Palo Alto Networks Content			
□	default-paloalto-dns		sinkhole	extended-capture
	: DNS Security			
□	Ad Tracking Domains	default (informational)	default (allow)	disable
□	Command and Control Domains	default (high)	default (block)	disable
□	Dynamic DNS Hosted Domains	default (informational)	default (allow)	disable
□	Grayware Domains	default (low)	default (block)	disable
□	Malware Domains	default (medium)	default (block)	disable
□	Parked Domains	default (informational)	default (allow)	disable
□	Phishing Domains	default (low)	default (block)	disable

DNS Sinkhole Settings

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

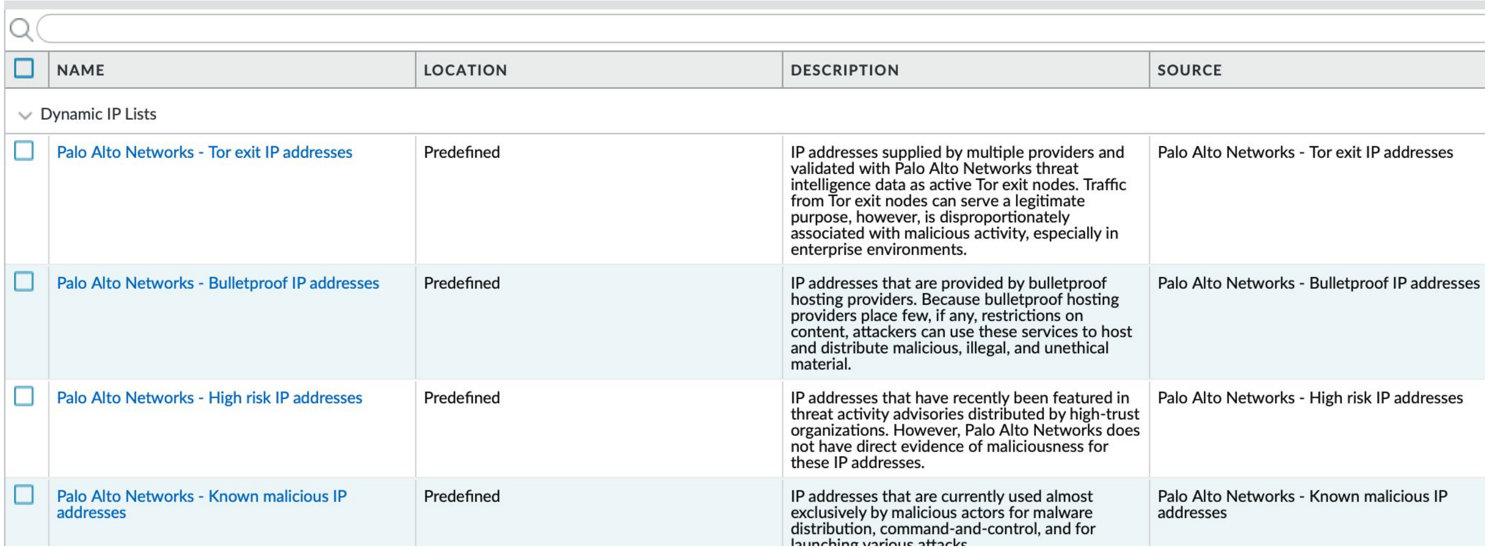
Sinkhole IPv6: IPv6 Loopback IP (::1)

Block DNS Record Types

□ SVCB □ HTTPS □ ANY

External Dynamic Lists

- Make sure you have rules blocking these inbound and outbound



□	NAME	LOCATION	DESCRIPTION	SOURCE
	Dynamic IP Lists			
□	Palo Alto Networks - Tor exit IP addresses	Predefined	IP addresses supplied by multiple providers and validated with Palo Alto Networks threat intelligence data as active Tor exit nodes. Traffic from Tor exit nodes can serve a legitimate purpose, however, is disproportionately associated with malicious activity, especially in enterprise environments.	Palo Alto Networks - Tor exit IP addresses
□	Palo Alto Networks - Bulletproof IP addresses	Predefined	IP addresses that are provided by bulletproof hosting providers. Because bulletproof hosting providers place few, if any, restrictions on content, attackers can use these services to host and distribute malicious, illegal, and unethical material.	Palo Alto Networks - Bulletproof IP addresses
□	Palo Alto Networks - High risk IP addresses	Predefined	IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations. However, Palo Alto Networks does not have direct evidence of maliciousness for these IP addresses.	Palo Alto Networks - High risk IP addresses
□	Palo Alto Networks - Known malicious IP addresses	Predefined	IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, and for launching various attacks	Palo Alto Networks - Known malicious IP addresses

Device Settings

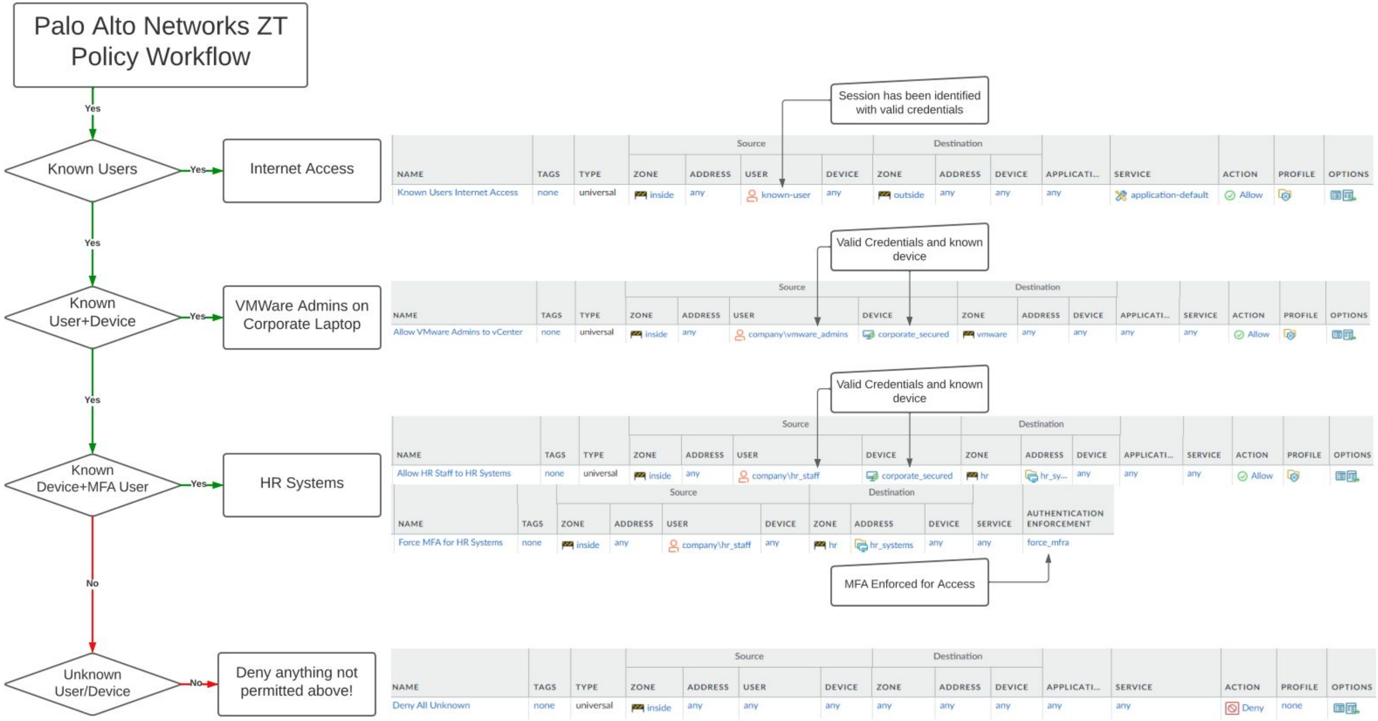
- Management TLS Mode set to TLS 1.3 only
- Enable log on high DP load
- Log Admin Activity (sends to a syslog server)
- Forward segments exceeding inspection queues
- Strip-X-Forwarded-For header
- Log traffic not scanned
- Rematch Sessions
- Forward segments exceeding TCP out of order queue

Zero Trust

What is Zero Trust?

- Zero trust is a concept that no user or device should be inherently trusted, whether inside or outside of a corporate network. Instead **all** traffic should be, by default, dropped. Required traffic flows should then be explicitly permitted based on principles of least privilege. Traffic should be validated against the following:
    - **Known User** - authenticated frequently with multiple factors
    - **Known Device** - corporate managed and secured with next-gen antivirus
    - **Source/Destination** - specific source and destination address
    - **Service** - nailed down for static ports, or application-default for dynamic ports
    - **Application** - static list of applications as required for inbound/internal traffic, application filters for outbound access
    - **URL Category** - an optional match condition that can be used in place of or in conjunction with a destination address

Zero Trust Policy Flow



Palo Alto Networks ZT Policy Workflow

Yes

Known Users — Yes → Internet Access

Yes

Known User+Device — Yes → VMWare Admins on Corporate Laptop

Yes

Known Device+MFA User — Yes → HR Systems

No

Unknown User/Device — No → Deny anything not permitted above!

Session has been identified with valid credentials

NAME	TAGS	TYPE	Source				Destination			APPLICATI...	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Known Users Internet Access	none	universal	inside	any	known-user	any	outside	any	any	any	application-default	Allow		

Valid Credentials and known device

NAME	TAGS	TYPE	Source				Destination			APPLICATI...	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Allow VMware Admins to vCenter	none	universal	inside	any	company\vmware_admins	corporate_secured	vmware	any	any	any	any	Allow		

Valid Credentials and known device

NAME	TAGS	TYPE	Source				Destination			APPLICATI...	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Allow HR Staff to HR Systems	none	universal	inside	any	company\hr_staff	corporate_secured	hr	hr_sy...	any	any	any	Allow		

NAME	TAGS	Source				Destination			SERVICE	AUTHENTICATION ENFORCEMENT
		ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
Force MFA for HR Systems	none	inside	any	company\hr_staff	any	hr	hr_systems	any	any	force_mfra

MFA Enforced for Access

NAME	TAGS	TYPE	Source				Destination			APPLICATI...	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Deny All Unknown	none	universal	inside	any	any	any	any	any	any	any	any	Deny	none	

Zero Trust Journey

The idea of getting to a zero trust model can be overwhelming. Try to break it into manageable chunks of work. For example:

- Enable inbound inspection and convert inbound rules to use App-id
- Create internet access rules based on application filters
- Add User-ID to policies that enable access to critical systems
- Add MFA to GlobalProtect
- Analyze the rulebase and try to find 3 things that you can change to improve security

Zero Trust Prioritization

1. MFA for remote access
2. Security Profiles
3. SSL Decryption
4. App-ID
5. User-ID
6. Device-ID

SSL Decryption

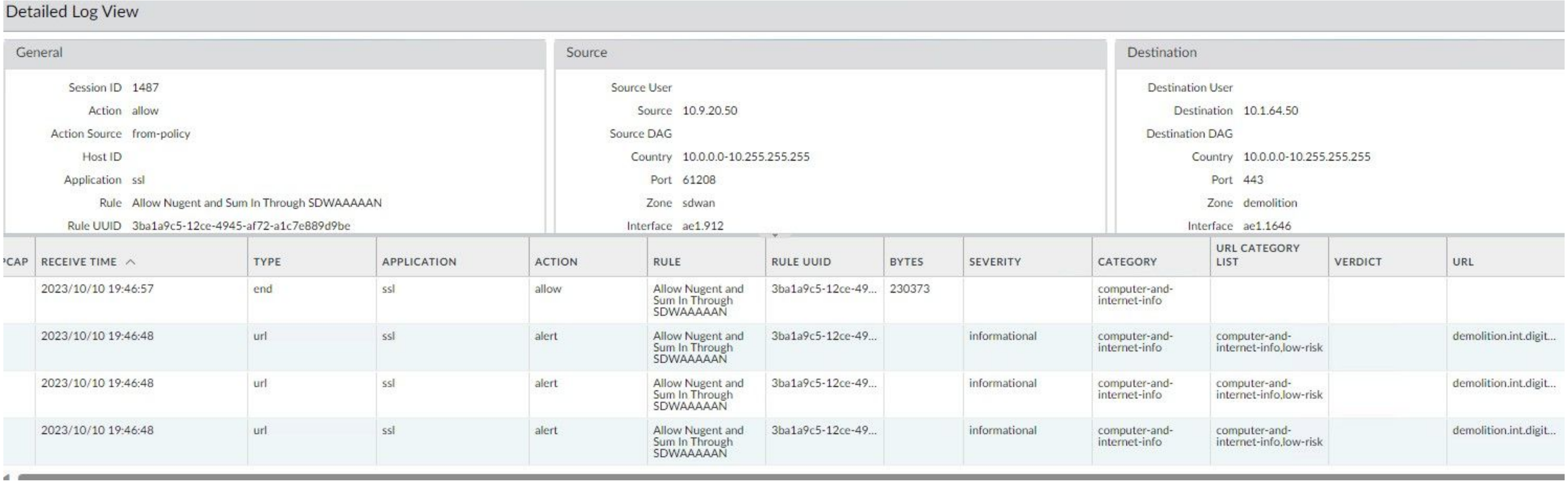
Types of Decryption

- SSL Forward Proxy (Outbound Decryption)
  - Provides the firewall with visibility into encrypted traffic originating from users within your network
- SSL Inbound Inspection (Inbound Decryption)
  - Provides the firewall with visibility into encrypted traffic originating from the internet destined to servers on your network

What the firewall sees *without* decryption

```
...........uJ...l.>k.;..;....g......1...... ...k.}..>l.h.>..o0...|......~
..."........+./.....,.0.
.            ........./.5.............example.com..........
.......................#.........h2.http/1.1.........".
...........3.k.i...
X.-DS..!c..>...d......fG.9..}.....A...Q...       }.[G.......Nr}r....6S!.y.....5.!,..'....o..E.S.Zte\../....+........
...........................-........@...................................................................................................................................................................x..{.t....'.{.....*..bs
j.S ...k.}..>l.h.>..o0...|......~
......O.+.....3.E...A..r....0{.(.....!.@..L.........0:...........-.......~....Loep.\.".......... .<k.T.7v...u....Mm.H|.
tal.lXB...........a_.M[.K...!...*...9.................5..U........^/.W.b :.r....s..].n.@.....d...5.w....
......5...dx..0..O.Lm......w.yo......Ep......c1EL...2.q.f.3.O..t.=C.Y..k.n...fw..r.?9.=T..>......O~...d,QB.m.kl.a.Q.
...YUM.y.n....4=..[.g...h....}......<..6.&7...".B.T.;.L.i.E.<r.""../.Snx..K..
.rj..zBX.sE.u.....{~.A.Z@L.Y.
..{....`Ynh..*;;!......&.2.T̀.V2e.,B....J...^.!"v.teC..W.'..k....   .
..X.L..~NUw.....S..Hc"|....7....9._...7A.@.+....F....u..d...6.Q...z..R.5.C..........z_..*.D...F.....*Ct9J.....by...,...jh.|.&./E.GfOY]...;-...(.kE.a........
..s...?....&.d.)......C.....e.#3f.a...:D..........U...1...Ut..).?....P..V\"......
....<....`r3[...._,R.
```

What the firewall sees *without* decryption



Detailed Log View

General

Session ID 1487
Action allow
Action Source from-policy
Host ID
Application ssl
Rule Allow Nugent and Sum In Through SDWAAAAAN
Rule UUID 3ba1a9c5-12ce-4945-af72-a1c7e889d9be

Source

Source User
Source 10.9.20.50
Source DAG
Country 10.0.0.0-10.255.255.255
Port 61208
Zone sdwan
Interface ae1.912

Destination

Destination User
Destination 10.1.64.50
Destination DAG
Country 10.0.0.0-10.255.255.255
Port 443
Zone demolition
Interface ae1.1646

CAP	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT	URL
	2023/10/10 19:46:57	end	ssl	allow	Allow Nugent and Sum In Through SDWAAAAAN	3ba1a9c5-12ce-49...	230373		computer-and-internet-info			
	2023/10/10 19:46:48	url	ssl	alert	Allow Nugent and Sum In Through SDWAAAAAN	3ba1a9c5-12ce-49...		informational	computer-and-internet-info	computer-and-internet-info,low-risk		demolition.int.digit...
	2023/10/10 19:46:48	url	ssl	alert	Allow Nugent and Sum In Through SDWAAAAAN	3ba1a9c5-12ce-49...		informational	computer-and-internet-info	computer-and-internet-info,low-risk		demolition.int.digit...
	2023/10/10 19:46:48	url	ssl	alert	Allow Nugent and Sum In Through SDWAAAAAN	3ba1a9c5-12ce-49...		informational	computer-and-internet-info	computer-and-internet-info,low-risk		demolition.int.digit...

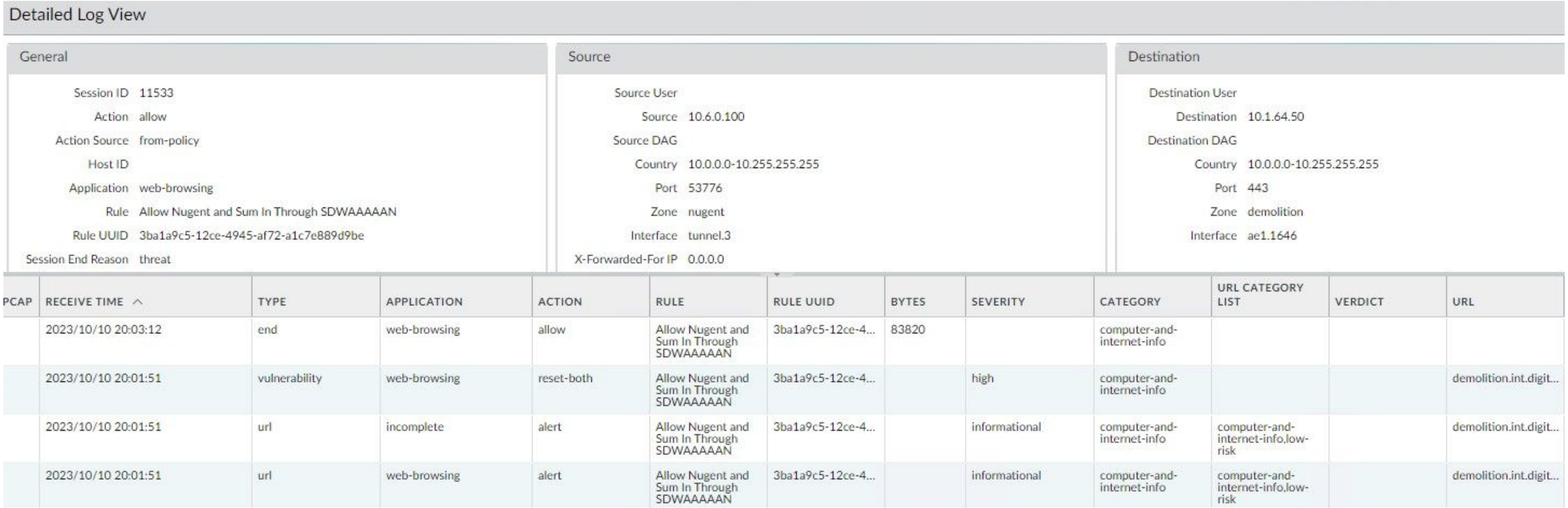
What the firewall sees *with* decryption

```
GET /classes/details?id=CS101 DROP TABLE STUDENTS; HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Encoding: gzip
Accept-Ranges: bytes

Age: 460608
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Mon, 21 Mar 2022 23:54:11 GMT
```

What the firewall sees *with* decryption



Detailed Log View

General

Session ID	11533
Action	allow
Action Source	from-policy
Host ID	
Application	web-browsing
Rule	Allow Nugent and Sum In Through SDWAAAAAN
Rule UUID	3ba1a9c5-12ce-4945-af72-a1c7e889d9be
Session End Reason	threat

Source

Source User	
Source	10.6.0.100
Source DAG	
Country	10.0.0.0-10.255.255.255
Port	53776
Zone	nugent
Interface	tunnel.3
X-Forwarded-For IP	0.0.0.0

Destination

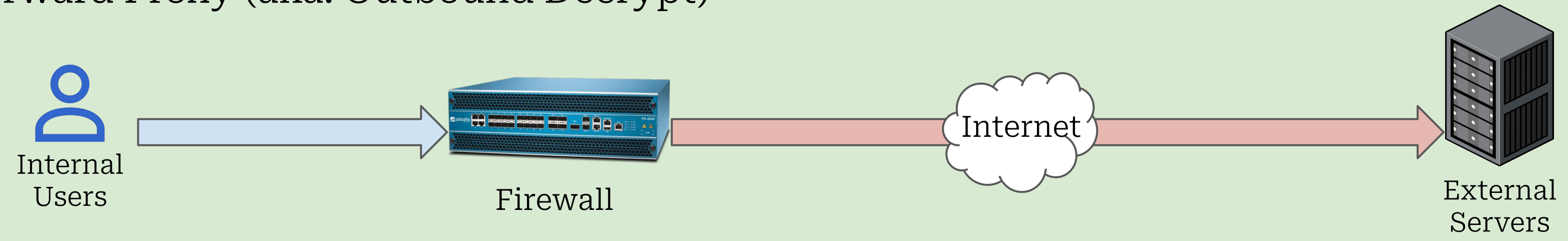
Destination User	
Destination	10.1.64.50
Destination DAG	
Country	10.0.0.0-10.255.255.255
Port	443
Zone	demolition
Interface	ae1.1646

PCAP	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT	URL
	2023/10/10 20:03:12	end	web-browsing	allow	Allow Nugent and Sum In Through SDWAAAAAN	3ba1a9c5-12ce-4...	83820		computer-and-internet-info			
	2023/10/10 20:01:51	vulnerability	web-browsing	reset-both	Allow Nugent and Sum In Through SDWAAAAAN	3ba1a9c5-12ce-4...		high	computer-and-internet-info			demolition.int.digit...
	2023/10/10 20:01:51	url	incomplete	alert	Allow Nugent and Sum In Through SDWAAAAAN	3ba1a9c5-12ce-4...		informational	computer-and-internet-info	computer-and-internet-info,low-risk		demolition.int.digit...
	2023/10/10 20:01:51	url	web-browsing	alert	Allow Nugent and Sum In Through SDWAAAAAN	3ba1a9c5-12ce-4...		informational	computer-and-internet-info	computer-and-internet-info,low-risk		demolition.int.digit...

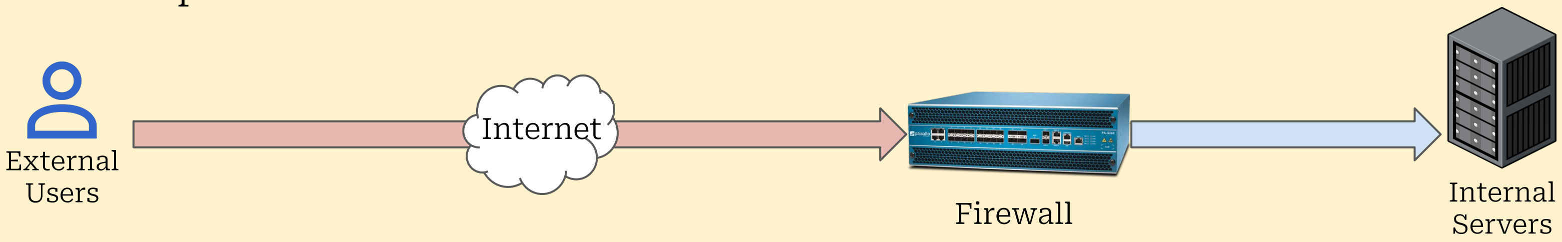
digitalscepter

Inbound vs Outbound

Forward Proxy (aka. Outbound Decrypt)



Inbound Inspection



SSL Decryption Benefits

- App-ID visibility
- Granular app control
- Threat Prevention
- Full URL visibility
- File download/upload visibility

SSL Forward Proxy - What's Required

- Private CA Certificate trusted by all endpoints/browsers
- Periodic exclusions for sites that don't support decryption
  - Certificate pinning
  - Client-cert authentication

SSL Forward Proxy - Certificate Authority Options

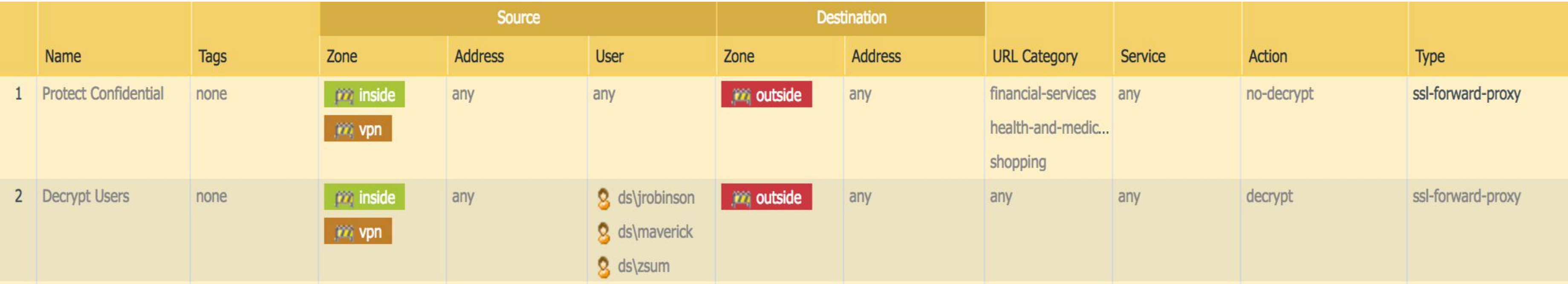
- PAN firewall Self-Signed Certificate
  - Less secure, but doesn’t require in-house certificate infrastructure
  - Requires distribution of PAN certificate to machines
- Subordinate CA template to PAN firewall from enterprise CA
  - Simple revocation if PAN private key is compromised
  - Does not need to be distributed to domain-joined machines since enterprise CA should already be trusted

SSL Forward Proxy - Certificate Authority Options

- PAN firewall Self-Signed Certificate
  - Less secure, but doesn’t require in-house certificate infrastructure
  - Requires distribution of PAN certificate to machines
- Subordinate CA template to PAN firewall from enterprise CA
  - Simple revocation if PAN private key is compromised
  - Does not need to be distributed to domain-joined machines since enterprise CA should already be trusted

SSL Forward Proxy - What to Decrypt

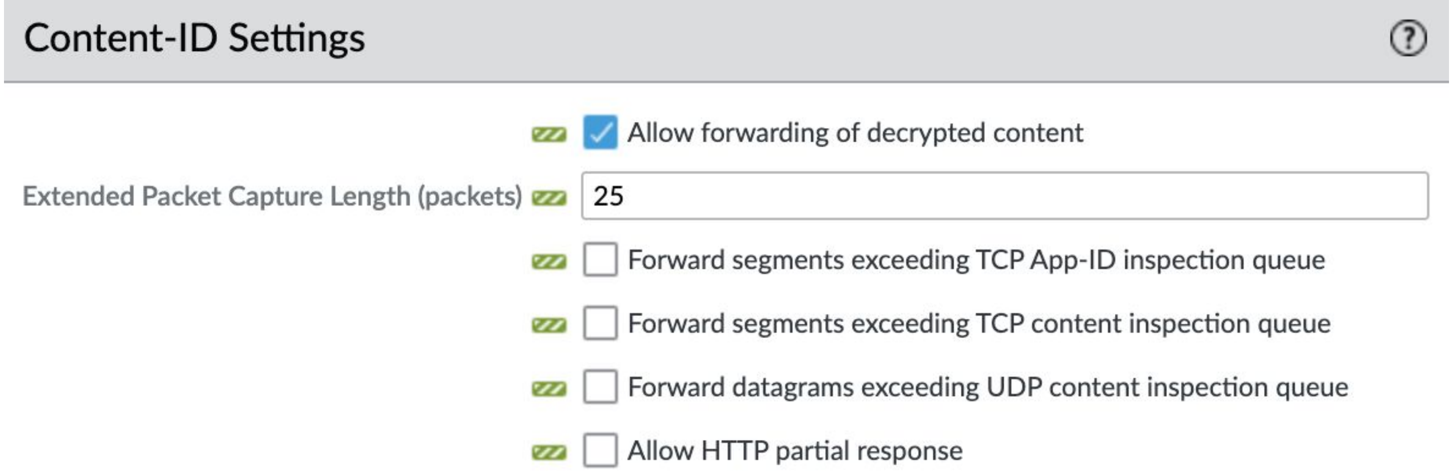
- Decrypt all URL categories except those that contain sensitive, private data, such as:
  - Financial-services
  - Health-and-medicine
  - Shopping
- Start with a test group as shown below. Only three users are being decrypted. As testing progresses, expand test group



			Source			Destination					
	Name	Tags	Zone	Address	User	Zone	Address	URL Category	Service	Action	Type
1	Protect Confidential	none	inside vpn	any	any	outside	any	financial-services health-and-medic... shopping	any	no-decrypt	ssl-forward-proxy
2	Decrypt Users	none	inside vpn	any	ds\jrobinson ds\maverick ds\zsum	outside	any	any	any	decrypt	ssl-forward-proxy

SSL Forward Proxy - Important Settings

- Decrypted files should be sent to WildFire
  - Device > Setup > Content-ID > Content-ID Settings



Content-ID Settings

☑ Allow forwarding of decrypted content

Extended Packet Capture Length (packets): 25

□ Forward segments exceeding TCP App-ID inspection queue

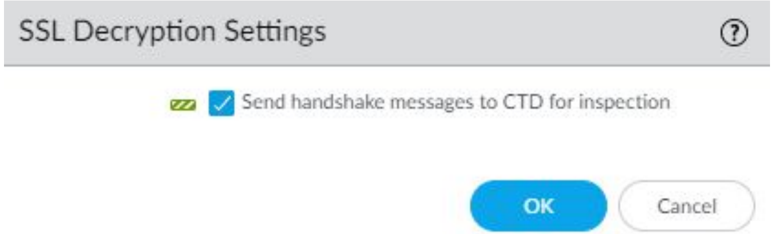
□ Forward segments exceeding TCP content inspection queue

□ Forward datagrams exceeding UDP content inspection queue

□ Allow HTTP partial response

SSL Forward Proxy - Important Settings

- (PAN-OS 11 only) Enable inspection of SSL handshake messages
    - Device > Setup > Session > SSL Decryption Settings

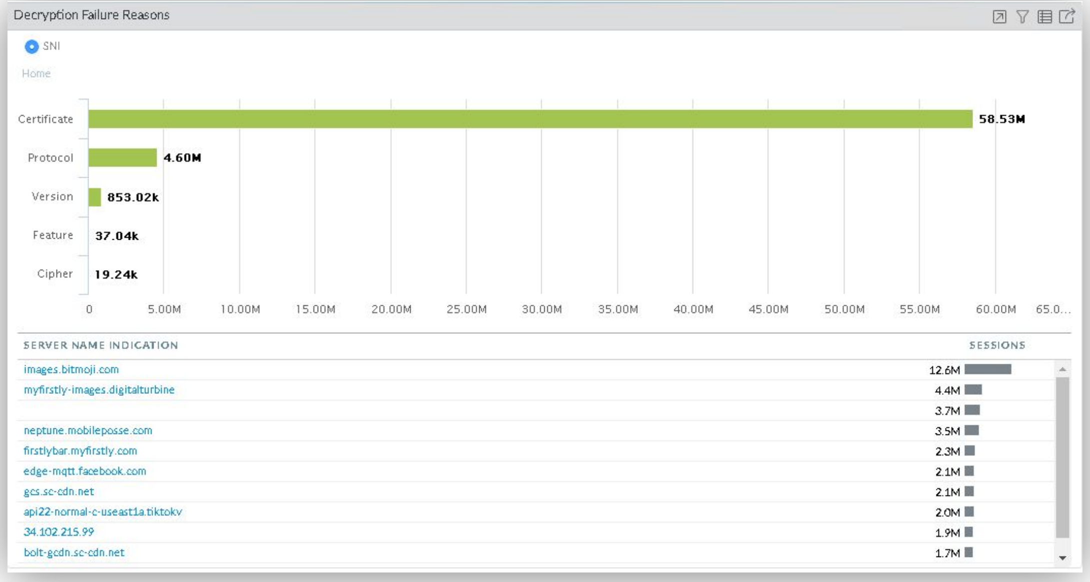


SSL Decryption Settings

☑ Send handshake messages to CTD for inspection

SSL Forward Proxy - Decrypt Failures

- Find unsupported sites
- Decide if exclusions should be made
- Create exclusion globally or on a per-user/per-IP basis



SERVER NAME INDICATION	SESSIONS
images.bitmoji.com	12.6M
myfirstly-images.digitalturbine	4.4M
	3.7M
neptune.mobileposse.com	3.5M
firstlybar.myfirstly.com	2.3M
edge-mqtt.facebook.com	2.1M
gcs.sc-cdn.net	2.1M
api22-normal-c-useast1a.tiktokv	2.0M
34.102.215.99	1.9M
bolt-gcdn.sc-cdn.net	1.7M

SSL Inbound Inspection - What’s Required

- Certificates for servers you want to inspect, e.g. company wildcard, www, etc.
- Endpoint, PAN firewall, and server all need to support common cipher suite

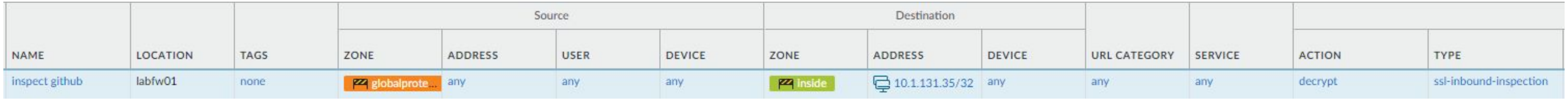
SSL Decryption - Time to Configure

- It is recommended to be running PAN-OS ≥ 10.1.0 for better cipher support with inbound inspection
- Get a list of all the services you want to decrypt
- Identify any need for specific TLS versions or ciphers
- Gather certificates for all services
- Import all certificates into the firewall
- Create a decryption profile
- Create decryption rules to decrypt inbound/outbound connections
- Validate that applications work as expected

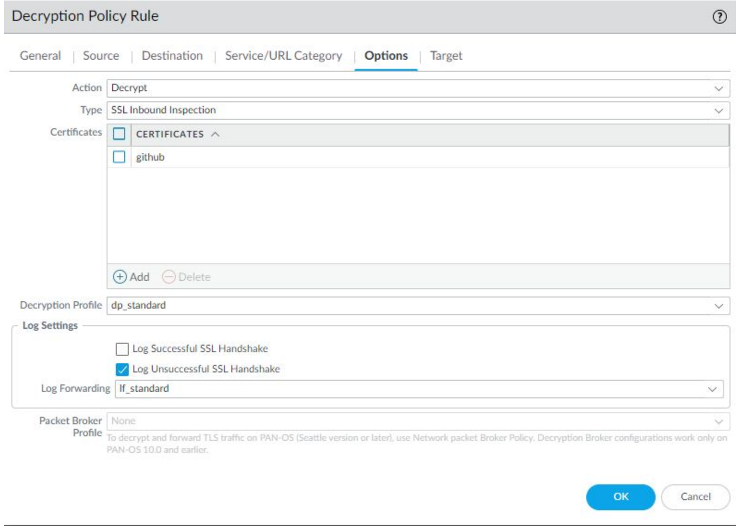
SSL Decryption - Time to Configure

- It is recommended to be running PAN-OS ≥ 10.1.0 for better cipher support with inbound inspection
- Get a list of all the services you want to decrypt
- Identify any need for specific TLS versions or ciphers
- Gather certificates for all services
- Import all certificates into the firewall
- Create a decryption profile
- Create decryption rules to decrypt inbound/outbound connections
- Validate that applications work as expected

SSL Decryption - Time to Configure



			Source				Destination						
NAME	LOCATION	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	URL CATEGORY	SERVICE	ACTION	TYPE
inspect github	labfw01	none	globalprote...	any	any	any	inside	10.1.131.35/32	any	any	any	decrypt	ssl-inbound-inspection



Decryption Policy Rule

?
General | Source | Destination | Service/URL Category | Options | Target

Action: Decrypt

Type: SSL Inbound Inspection

Certificates:
□ CERTIFICATES
□ github

Decryption Profile: dp_standard

Log Settings

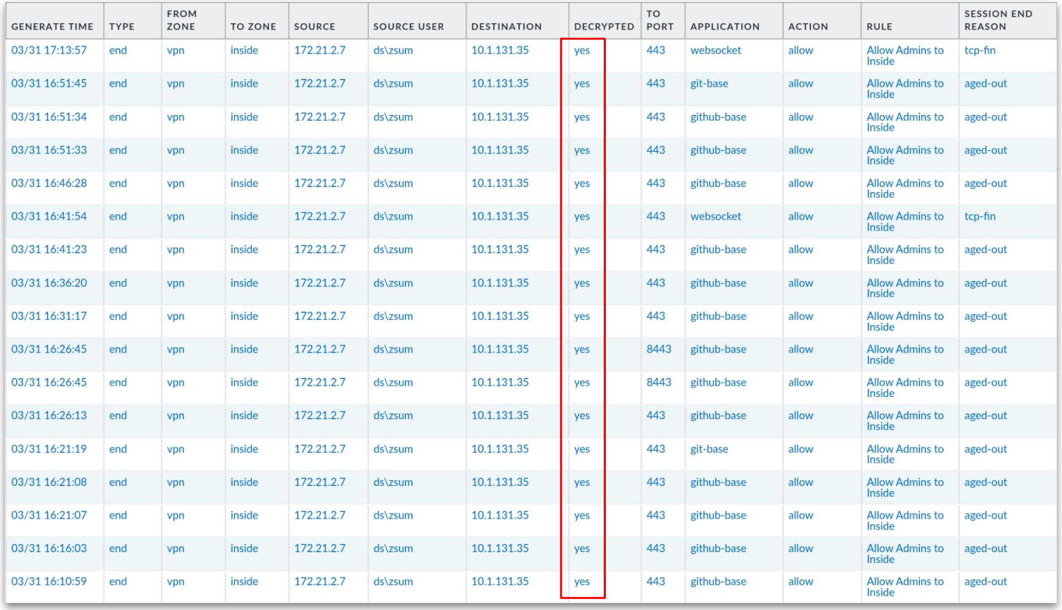
□ Log Successful SSL Handshake

☑ Log Unsuccessful SSL Handshake

Log Forwarding: lf_standard

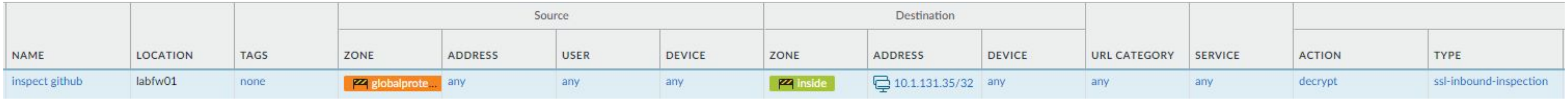
Packet Broker Profile: None

To decrypt and forward TLS traffic on PAN-OS (Seattle version or later), use Network packet Broker Policy. Decryption Broker configurations work only on PAN-OS 10.0 and earlier.

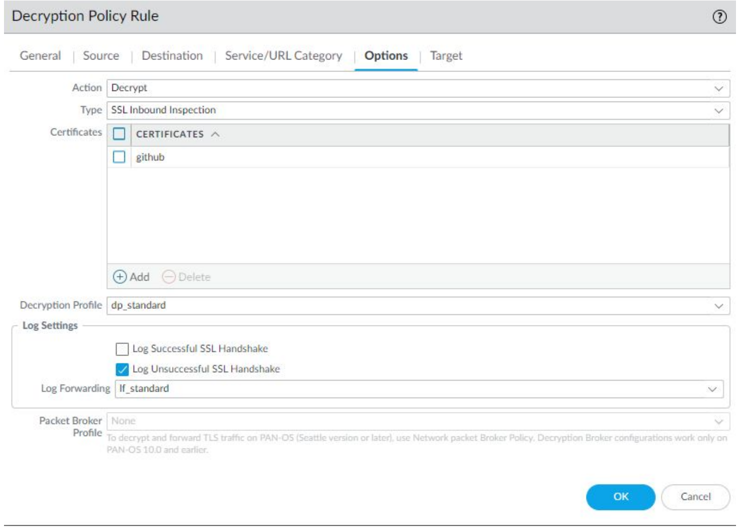


GENERATE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	DECRYPTED	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON
03/31 17:13:57	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	websocket	allow	Allow Admins to Inside	tcp-fin
03/31 16:51:45	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	git-base	allow	Allow Admins to Inside	aged-out
03/31 16:51:34	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:51:33	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:46:28	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:41:54	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	websocket	allow	Allow Admins to Inside	tcp-fin
03/31 16:41:23	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:36:20	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:31:17	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:26:45	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	8443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:26:45	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	8443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:26:13	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:21:19	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	git-base	allow	Allow Admins to Inside	aged-out
03/31 16:21:08	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:21:07	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:16:03	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:10:59	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out

SSL Decryption - Time to Configure



			Source				Destination					
NAME	LOCATION	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	URL CATEGORY	SERVICE	ACTION	TYPE
inspect github	labfw01	none	globalprote...	any	any	any	inside	10.1.131.35/32	any	any	any	decrypt	ssl-inbound-inspection



Decryption Policy Rule

General | Source | Destination | Service/URL Category | Options | Target

Action: Decrypt

Type: SSL Inbound Inspection

Certificates:

□ CERTIFICATES

□ github

Decryption Profile: dp_standard

Log Settings

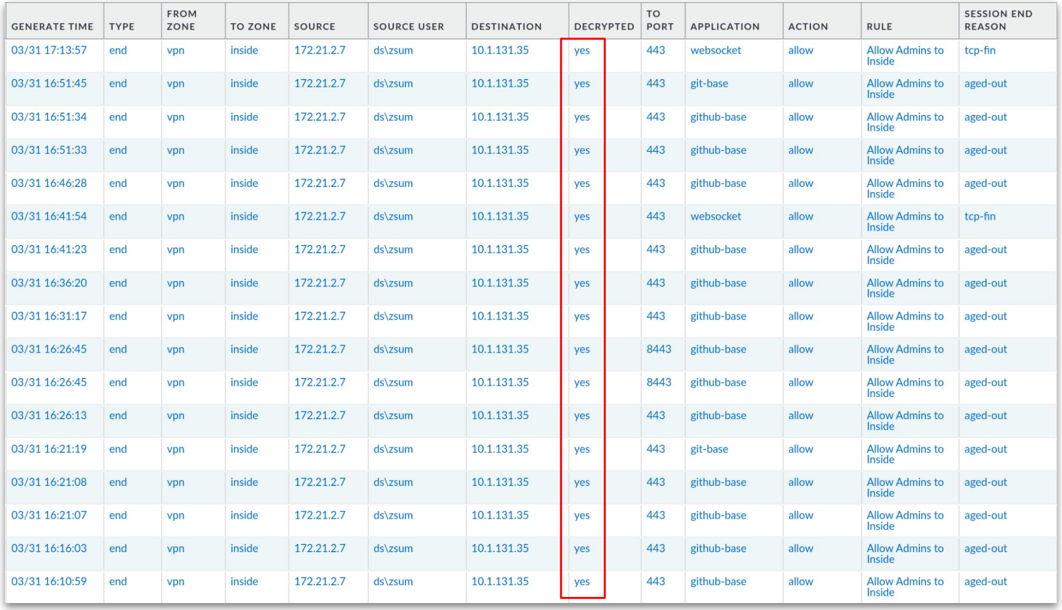
□ Log Successful SSL Handshake

☑ Log Unsuccessful SSL Handshake

Log Forwarding: lf_standard

Packet Broker Profile: None

To decrypt and forward TLS traffic on PAN-OS (Seattle version or later), use Network packet Broker Policy. Decryption Broker configurations work only on PAN-OS 10.0 and earlier.



GENERATE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	DECRYPTED	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON
03/31 17:13:57	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	websocket	allow	Allow Admins to Inside	tcp-fin
03/31 16:51:45	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	git-base	allow	Allow Admins to Inside	aged-out
03/31 16:51:34	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:51:33	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:46:28	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:41:54	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	websocket	allow	Allow Admins to Inside	tcp-fin
03/31 16:41:23	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:36:20	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:31:17	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:26:45	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	8443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:26:45	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	8443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:26:13	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:21:19	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	git-base	allow	Allow Admins to Inside	aged-out
03/31 16:21:08	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:21:07	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:16:03	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:10:59	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out

Network Segmentation

Overview

- Network segmentation is the process of classifying assets into unique subnets on your network with the intent of firewalling between these subnets
- Firewalling these subnets is generally achieved by making the firewall the default gateway for the subnets assets are on, but another common option is using VRFs to force inter-subnet traffic through a firewall

Benefits

- Content inspection between subnets
- Visibility into traffic flows between subnets
- Ability to easily isolate assets that may be compromised

Methods of Implementation

- Option 1 - Migrate server vlan interfaces from existing core switch and place them on firewall
    - Quicker to implement
    - May need to migrate ACLs from switch
    - Existing subnets may not sufficiently segment assets
- Option 2 - Create new server subnets on firewall and migrate applications to new subnets
    - Migrating applications to new subnets is a large effort that carries risk (services using IP address versus hostname will break)
    - Will require rulebase updates for IP changes, but will lead to cleaner rulebase
    - Applications can be moved one at a time allowing slow, methodical approach

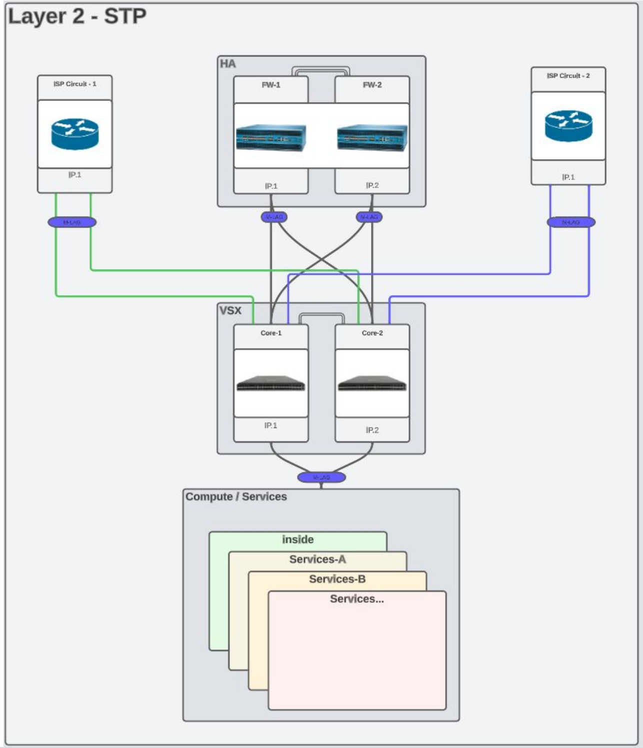
Recommendations

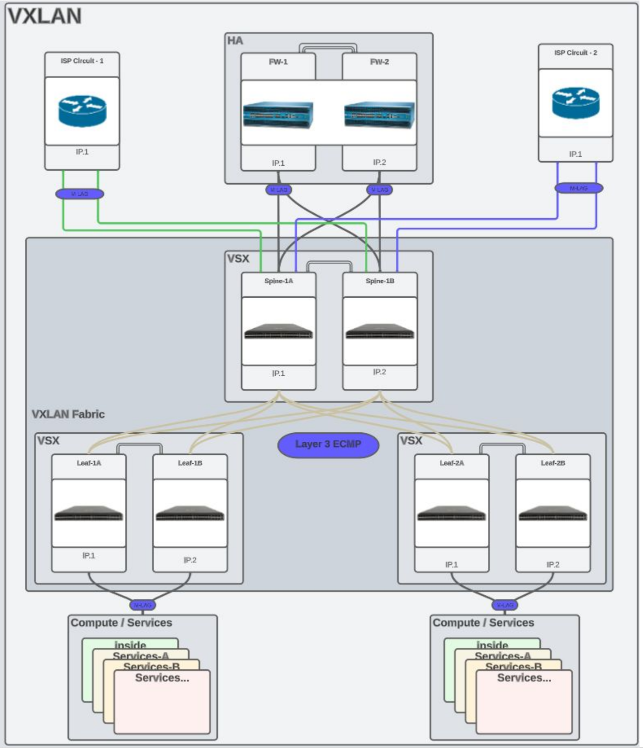
- If there are just a few server subnets
  - Option 1, followed by option 2
  - This will allow instant improvement of security posture by getting subnets on the firewall
  - Option 2 can then be implemented over time to continue improving posture
- If there are significant server subnets
  - Option 1
  - If assets are already properly categorized into subnets, migrating the subnets straight to the firewall should be all that is needed
  - Make sure ACLs are properly migrated prior to migrating

Considerations

- Security and NAT policies will need to be updated to reflect changes to zones
- Load balancers can lead to asymmetric routes and will need to be considered before migrating subnets

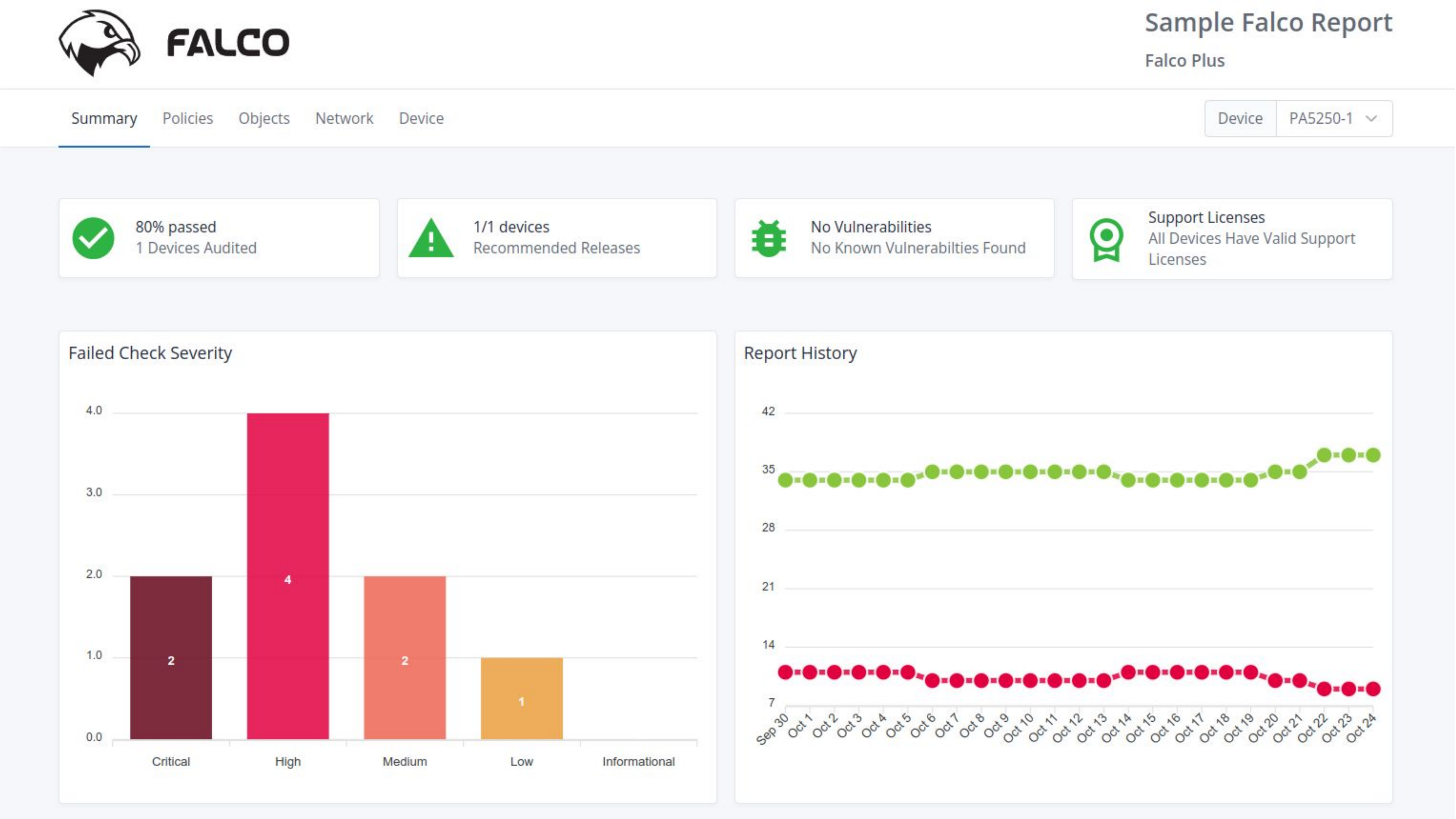
Example Diagrams





What is Falco?

- A tool to detect configuration issues
- A managed service to assist with fixing them



FALCO

Sample Falco Report

Falco Plus

Summary | Policies | Objects | Network | Device

Device | PA5250-1

80% passed
1 Devices Audited

1/1 devices
Recommended Releases

No Vulnerabilities
No Known Vulnerabilties Found

Support Licenses
All Devices Have Valid Support Licenses

Failed Check Severity

Report History

digitalscepter

sales@digitalscepter.com
(888) 299-3718

digitalscepter.com