PAN-OS Threat Workshop

Created for Customers and Partners by
Narinder Singh (Staff Cybersecurity Specialist)

Topics

- Advanced Wildfire Public Cloud
- Antivirus
- Vulnerability
- Anti-Spyware
- DNS Security
- URL Filtering
- Others - Additional Features and Best Practices

Advanced Wildfire Public Cloud

What is Advanced Wildfire?

- Analyzes the samples (supported file type) using Static Analysis, Dynamic Analysis, Machine Learning, Dynamic Unpacking (global cloud only), and Intelligent Runtime Memory Analysis (Advanced WildFire + PAN-OS 10.0+, global cloud only). Signature is created and released globally.

- Malware/C2 domains identified based on wildfire analysis will eventually get coverage from DNS Signatures and URL filtering.

- Advanced WildFire License is required

  Without the license, the firewall can forward portable executable (PE) files for WildFire analysis, and can retrieve Antivirus signatures only with antivirus updates which are made available every 24-48 hours.

- Advanced Wildfire Inline Cloud Analysis was introduced in 11.1. The cloud-based engines enable the detection of never-before-seen malware (e.g., a Palo Alto Networks zero-day - malware previously unseen in the wild or by Palo Alto Networks) and block it from entering your environment.

Content Packages and Wildfire Updates

	AVAILABLE 24-48 HOURS	AVAILABLE IN REAL-TIME	AVAILABLE IN REAL-TIME	AVAILABLE IN REAL-TIME
Update Type	Antivirus Signatures		URL Category Updates	DNS Signature
Content Database	Antivirus (download daily)	WildFire (real-time updates)	URL Filtering (dynamically downloaded)	DNS Security (dynamically downloaded)
License Required	Advanced Threat Prevention License	Advanced WildFire License	Advanced URL Filtering License	Advanced DNS Security License

Firewall File Submission Workflow

- Session must hit a rule with Wildfire Analysis Profile attached.
- For encrypted traffic, the session must be decrypted and 'Allow forwarding of decrypted content' (Device>Setup>Content-ID>Content-ID Settings) must be checked. This is NOT enabled by default.

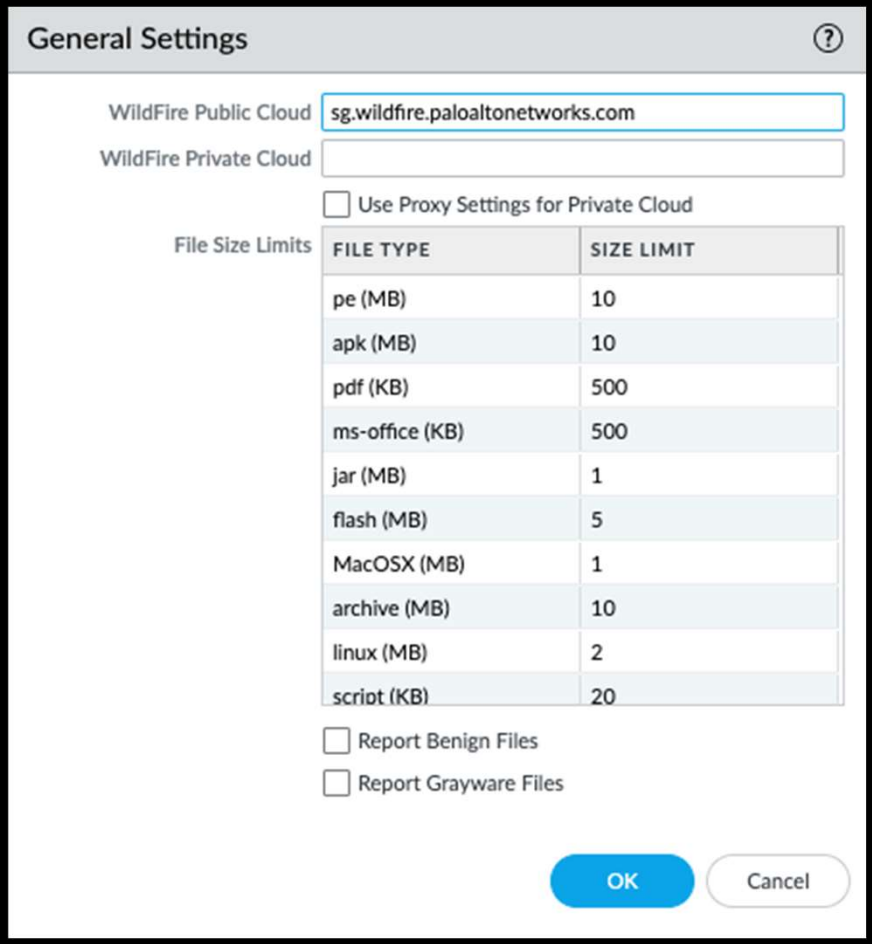
  This option is under Device> Virtual Systems>[Select VSYS]>Allow Forwarding of Decrypted Content if multiple vsys is enabled.
- During CTD inspection the dataplane forwards files and email links to the varrcvr process on MP.
- MP writes files received from DP to disk, calculates SHA256 hash, and uploads the files and session info if not known by cloud. If known, then only session info is uploaded.
- MP retrieves reports (with verdict) for files/sessions it has uploaded and a Wildfire Submissions log is written.
- Signature is generated for malware samples and released as a part of Wildfire package.
- New feature released in 11.0.2 - Hold Mode for WildFire Real Time Signature Lookup.
- Session Information Sharing is enabled by default — source/destination IPs, user identity, URL, filename, and email metadata are forwarded to the cloud alongside the file. Each data type is individually configurable (Device > Setup > WildFire > Session Information).

Advanced Wildfire Public Clouds

- We have Wildfire global cloud (US) and regional clouds:
  - Advanced WildFire Public Clouds
  - Review Advanced Wildfire Privacy Datasheet for more information.
- Each cloud analyzes samples and generates signature and verdicts independently and then shared globally.
- Configure Wildfire Public Cloud from Device>Setup>Wildfire>General Settings>Wildfire Public Cloud. Global Cloud is the default in firewalls.
- Unique samples sent to the WildFire cloud for analysis can now be deleted at the discretion of the user.

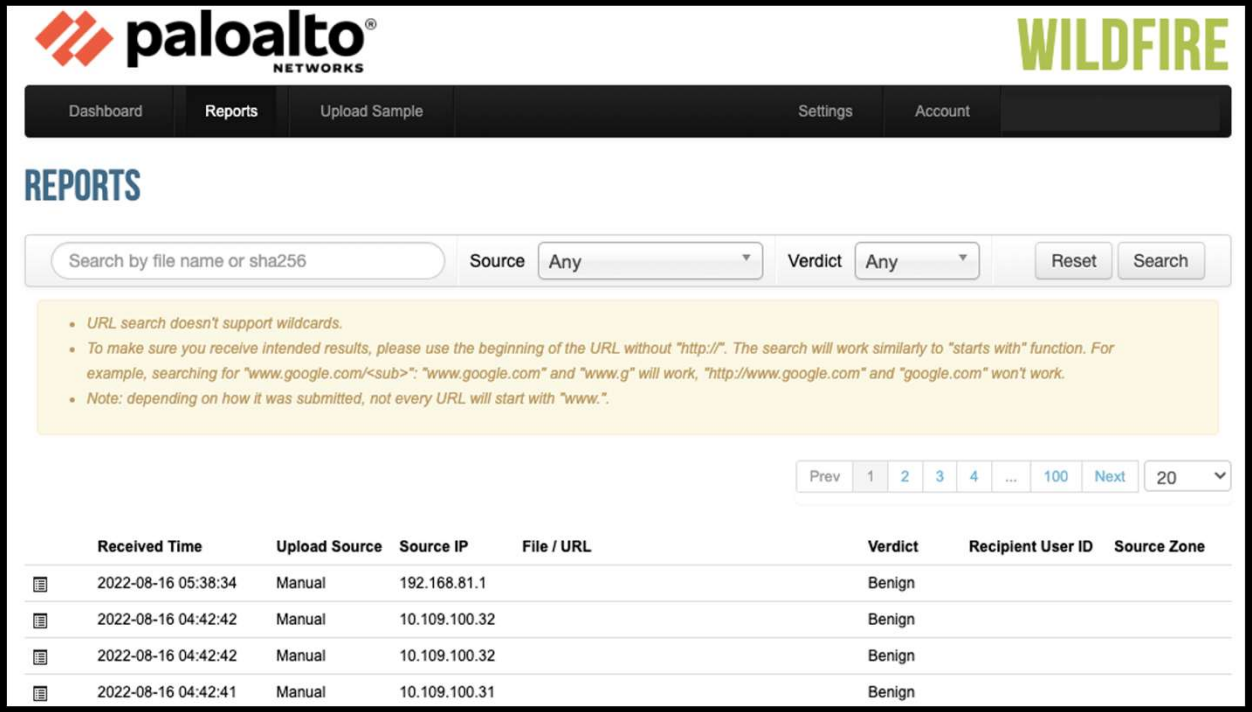
Wildfire File forwarding Size

- The default file size limit is designed to include majority of malware in the wild.
- Can be increased on forward uncommonly large malware samples.



Wildfire Portal

- Upload file (or URL to a File) manually for analysis.
- Get wildfire analysis report.
- Search previously uploaded samples.
- Filter samples based on upload source and verdict.
- Get the wildfire API.
- Configure email notification based on verdict.



- Deprecation Notice: The WildFire Portal is being deprecated on Aug 31, 2026 — verdict notifications are moving to Strata Cloud Manager.

WildFire Portal — Migrating to Strata Cloud Manager

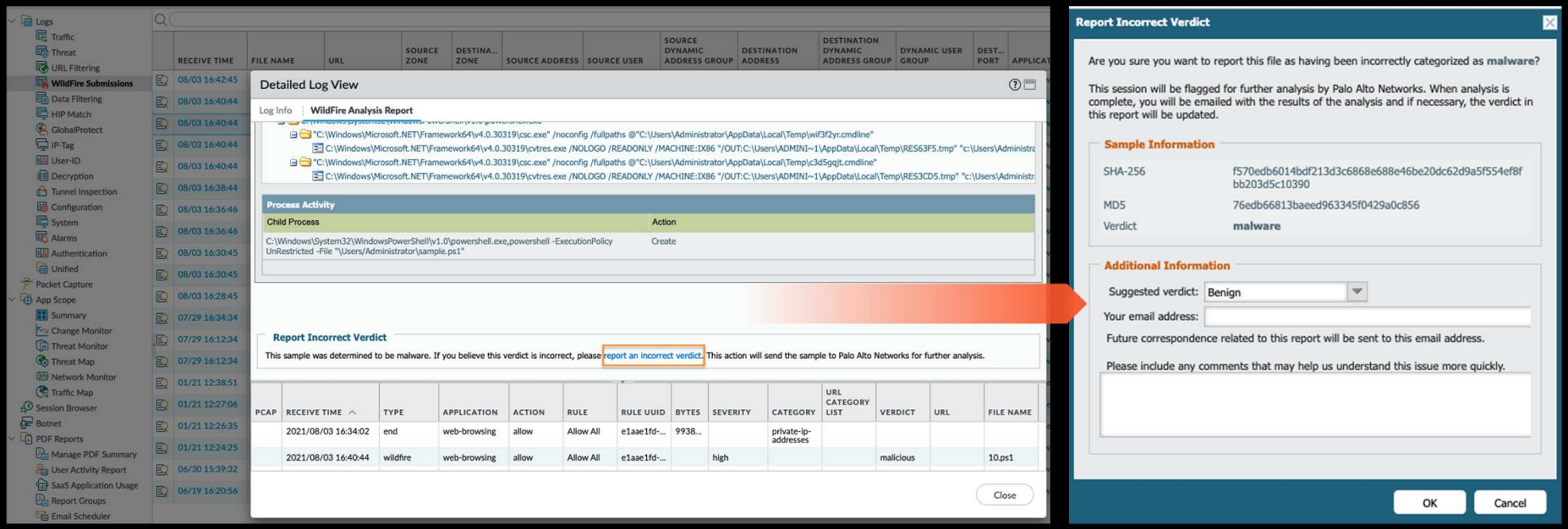
- Unified Experience: WildFire functionality across Customer Service Portal (CSP) and the WildFire Portal is now centralized in SCM, providing a single unified console for all WildFire services.
- Centralized Management in SCM: All core portal features—such as manual file submissions, analysis report downloads, and device associations—are moving to Strata Cloud Manager.
- Stronger API Security: Static API keys are transitioning to a token-based authentication mechanism for Wildfire RESTful API calls.
- SCM Essentials license is available at no additional cost for all Next-Generation Firewall (NGFW) and Prisma Access customers to facilitate this transition.

Wildfire Verdicts

- **Benign:** The sample is safe and does not exhibit malicious behavior.
- **Grayware**: The sample does not pose a direct security threat, but might display otherwise intrusive behavior.
- **Phishing (elink)**: The link directs users to a phishing site and poses a security threat. Phishing sites are sites that attackers disguise as legitimate websites with the aim to steal user information, especially corporate passwords that unlock access to your network.
- **Malicious**: The sample is malware and poses a security threat. Malware can include viruses, worms, Trojans, Remote Access Tools (RATs), rootkits, and botnets. For files identified as malware, signatures are generated and distributed to prevent against future exposure to the threat.

How to Submit Verdict Change Request?

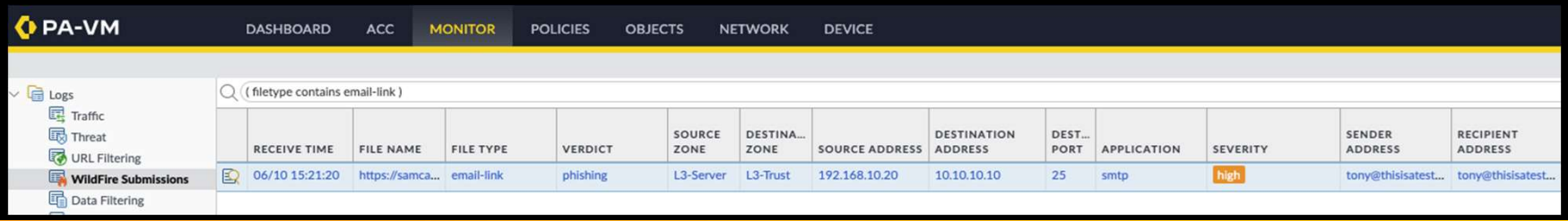
- From ‘Wildfire Analysis Report’ for a specific sample in the Panorama/Firewall GUI.



- This option is also available in the report from portal.
- Will receive an email update once the requested is reviewed by us.

Email-link Analysis

- WildFire visits submitted links to determine if the corresponding web page hosts any exploits or displays phishing activity. A link that WildFire finds to be malicious or phishing is:
  - Recorded on the firewall as a WildFire Submissions log entry.
  - Added to PAN-DB and the URL is categorized as malware/phishing.
- Elinks are uploaded in:
  - Batches of 100 email links ‘OR’
  - Every two minutes (depending on which limit is hit first).
- Disable email-link analysis (in profile attached to specific policy) while doing Phishing tests.
- **Email-links are only detected, the emails will not be blocked by the firewall**.



Wildfire Submissions Log

- ‘WildFire Submissions’ under the Monitor tab, are reports coming back from WildFire after analysis completes, It’s not ‘forwarding’.
- Log will be written for every instance the file has traversed, **irrespective of if it’s blocked or not.**
- ‘High’ and ‘Informational’ severity in Wildfire Submissions Log:
  - **High** > File was NOT blocked by signature.
  - **Informational** > File was blocked by an existing signature.
- Only ‘Malware’ files are logged by default, Benign and Grayware logging can be enabled from Device>Setup>Wildfire>General Settings.
- Use the sample malware file for testing.

Archive Files

- ZIP files (compressed upto 4 times) are decoded by the firewall and the supported file-type inside the ZIP file will be forwarded to Wildfire.
  - ZIP file never gets uploaded to wildfire from Firewall.
  - Signature will be created for decompressed samples uploaded to wildfire.
- RAR and 7-ZIP Files are not decoded by the firewall, they will be forwarded to Wildfire from the firewall.
- Signature will be created for RAR and 7-ZIP Files.

Wildfire Real-time Signature Update

- Feature introduced in 10.0, enable real-time for Wildfire schedule update and apply AV profile to security policy.
- Firewalls receive signatures in real-time as they become available.
- In real-time, until wildfire is installed, update schedule is every-min and after that it's changed to every-hour (at minute 0).
- Allow Access to https://realtimesignatures.service.paloaltonetworks.com/ on external Network devices.
- Use below command to check the connection status:

```
admin@PA-VM> show wildfire-realtime-cloud-status
RealTime WildFire Signature cloud
License:                valid
Current cloud server:           realtimesignatures.service.paloaltonetworks.com
Cloud connection:               connected
```

Troubleshooting - Wildfire Status

- Wildfire Profile has to be applied to at-least one security policy for wildfire registration to be successful.
- Global status of ‘Idle’ is good.

```
> show wildfire status

Connection info:
  Signature verification:        enable
  Server selection:              enable
  File cache:                    enable

WildFire Public Cloud:
  Server address:                wildfire.paloaltonetworks.com
  Best server:                   panos.wildfire.paloaltonetworks.com
  Device registered:             yes
  Through a proxy:               no
  Valid wildfire license:        yes
  Service route IP address:      10.194.106.31
  Global status:                 Idle
  Count of available workers:    10
```

Troubleshooting - Manual Registration

- Use the below command to initiate a registration:

```
admin@PA-VM> request wildfire registration channel public

WildFire registration for Public Cloud is triggered
```

- Check varrcvr.log to identify errors. Debug logs will give detailed info, **don't enable varrcvr debug without TAC confirmation.**

```
admin@PA-VM> tail follow yes mp-log varrcvr.log

2021-11-30 17:47:23.404 +0800 fwd thread for Public Cloud channel: cloud info is
updated

2021-11-30 17:47:23.510 +0800 curl params are modified

2021-11-30 17:47:23.511 +0800 Public Cloud channel cloud register successful.
the best server is selected as: sn1-panos.wildfire.paloaltonetworks.com
```

Troubleshooting - Wildfire Forwarding

- WildFire Forwarding (mp-log/wildfire-upload.log) logs

```
> less mp-log wildfire-upload.log
> tail follow yes mp-log wildfire-upload.log
> debug wildfire upload-log show

> debug wildfire upload-log log extended-log {yes/no} (yes: prints sha256)

> less mp-log wildfire-upload.log
Data and Time           filename     file type   action  channel   session_id   transaction_id  file_len   flag traffic_action
2026-07-27 21:52:27 +1000:  macos-file     MacOSX  upload success  PUB     41001   23      35248         0x801c      allow
2026-07-27 21:52:54 +1000:  apk-file.apk   apk     upload success  PUB     41006   24      1446955        0x801c     allow

Data and Time   filename        file type       action  channel session_id      transaction_id  file_len        flag
traffic_actionvsys_id  threat id       user_id app_id  unique_tid      source  destination     product src_zone        SHA256
2026-07-28 14:25:18 +1000:      wildfire-test-elf-file  linux   upload success  PUB     52156   33      8608    0x801c
allow   1     52175    0       0       0       172.16.16.10:57498      35.204.106.198:80       base    trust-zone
cdb9acce8b0717ab994518e858c7dbf7a86edf278fd39363fbf6d98c06dffb2a
```

- Find status of a recently forwarded file or URL

```
> grep pattern <Beginning of filename> mp-log wildfire-upload.log
> grep pattern <Beginning of URI> mp-log wildfire-upload.log
> grep pattern <sha256> mp-log wildfire-upload.log
```

Troubleshooting - DP-MP Connection

- Verify DP to MP connection using below commands:

```
admin@PA-VM> debug wildfire dp-status

DP status:

        DP:         127.131.2.1:31520


admin@PA-VM> show netstat numeric yes | match 3099

tcp         0      0 127.131.1.1:3099    127.131.2.1:31520       ESTABLISHED
```

Troubleshooting - Advanced WildFire - Inline Cloud Analysis

- Check ctd-agent cloud connection status:

```
> show ctd-agent status security-client
Security Client AceMlc2(1)
        Current cloud server:   ace.hawkeye.services-edge.paloaltonetworks.com:443
        Cloud connection:       connected
        Config:
                Number of gRPC connections: 2, Number of workers: 5
                Debug level: 2, Insecure connection: false, Cert valid: true, Key
valid: true, CA count: 383
                Maximum number of workers: 10
                Maximum number of sessions a worker should process before
reconnect: 1024
                Maximum number of messages per worker: 0
                Skip cert verify: false
        Grpc Connection Status:
                State Ready (3), last err <nil>
                …
```

Wildfire Best Practices

- Always enable Wildfire profile on all relevant security policies.
- Decryption plays an important role in visibility, also make sure that ‘Allow forwarding of decrypted content’ is checked.
- ‘High’ Priority Wildfire Submissions log should be reviewed on priority as those malwares were NOT blocked by AV signatures.
- Follow up on emails associated with malicious elink analysis verdicts.
- Wildfire content update should be scheduled ‘real-time’ (10.0).
- Leverage Hold Mode for WildFire Real Time Signature Lookup (11.0.2).
- Leverage the Advanced Wildfire Inline Cloud Analysis (11.1).
- Review Wildfire Best Practices.

DEMO

Antivirus

Antivirus Basics

- Pattern based signatures that provides protection against malware.
- Signatures are created based on samples uploaded to Wildfire.
- Signatures are released as a part of Antivirus and Wildfire bundles (Dynamic Updates).
- Protection is based on configuration in Antivirus Profile (Objects>Security Profile) attached to security policy.
- Wildfire Inline ML currently Supports PE (Windows Executable), ELF, MS Office, OOXML, Mach-O, PowerShell, and Shell scripts (introduced in 10.0).

Antivirus Signatures

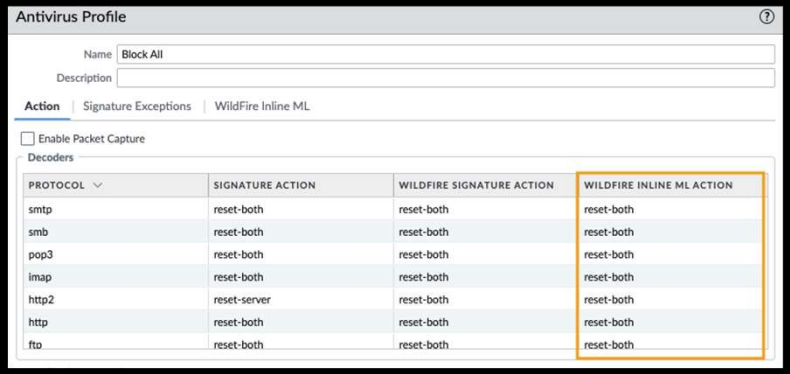
→ Hashes? → Too unique

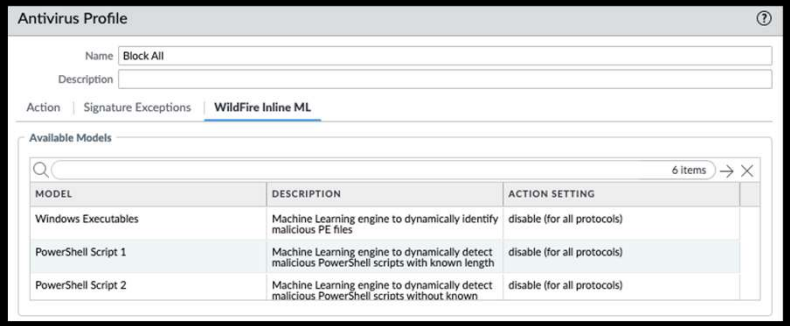
→ File names? → Not unique enough
They don't exist in the file

→ Signatures → Proprietary format of strategically placed concatenated chunks
Based on structure and content of file
Different for every file type
Able to identify variants of the same file

Wildfire Inline ML

- Advanced Wildfire subscription is required, Inline Ml was introduced in PAN-OS 10.0.
- Malicious files will be blocked in real-time without delay for content update or Wildfire's verdict.
- Supports **PE (Windows Executable), ELF, MS Office, OOXML, Mach-O, PowerShell, and Shell scripts**.
- Partial Hash can be used to create exception.





RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	PARTIAL_HASH	SOURCE ADDRESS	DESTINATION ADDRESS	TO PORT	APPLICATION	ACTION	SEVERITY	FILE NAME
03/17 18:01:18	ml-virus	Malicious Windows Executable	L3-Trust	L3-Untrust	156301209306...	172.16.26.59	11.11.11.65	80	web-browsing	alert	medium	11.11.11.65/files/petest1

Wildfire Inline ML

- Access to “ml.service.paloaltonetworks.com:443”(SSL) is required.

```
> show mlav cloud-status

MLAV cloud
Current cloud server:    ml.service.paloaltonetworks.com
Cloud connection:        connected
```

- Models is delivered by cloud, device server queries to cloud every 5 min. If there is update, download the latest model per file type from model cloud.
- After failures for 5 attempt, all MLAV models are disabled. Once disconnected, it’ll wait 15 min hold time.
- When connecting, FW will try to update to latest info and change the state to connected.

Troubleshooting False Positives - What Is Signature Collision?

- PanAV signatures are created based on content of a malicious file. The signatures are not hash based and do not use the full sample body. This approach provides the benefit that a signature created from one malicious sample can potentially match other similarly structured malicious samples (e.g. samples from the same malware family). **This approach does lead to a scenario wherein an unrelated (and potentially benign) sample may end up matching a signature created from a malicious sample. This is called a virus signature collision.**

- Upload the blocked sample to Wildfire and confirm that the verdict is Benign. Try creating an Antivirus exception if this is an internal sample.

- Open a TAC case with the sample (Password protected ZIP File) or sample hash (if sample is already uploaded to Wildfire) for further queries if this is a public sample and exception is not an option.

- TAC team will review the popularity of the sample being blocked and impact of disabling the signature.

Troubleshooting False Positives

- FP with Wildfire detection if wildfire classifies a benign sample as ‘Malware’:

  Check Threat ID in threatvault to get the sample based on which signature was created.

  Signature will be disabled (in a future AV release) if the verdict of that sample gets flipped to Benign, request verdict change through Wildfire.

- Open a TAC Case with below details for more information, create exception if required.

  https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm3aCAC

Troubleshooting False Negative

- Search for the hash in Threat Vault to check coverage.
- Is the traffic encrypted? Is SSL Decryption/Inbound Inspection enabled? Have the sample been uploaded to Wildfire?
- Manually upload the sample to Wildfire, signature will be released when sample get classified as malware.
- Request a verdict change if classified as Benign in Wildfire, signature will be released when the verdict get flipped to malware.
- Open a TAC case with the sample (Password protected ZIP File), URL for file download (if relevant), Threat log, Wildfire Submissions log and detailed information.

How to write a Custom Signature to block files?

- Spyware or Vulnerability Custom Objects can be used to create pattern based signature to block a file.

- Useful in blocking non malicious files that you want to block. Open the file in any Hex editor (Like HxD) and identify a unique pattern.

- Use the appropriate context and use the unique pattern.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HCHACA4

https://live.paloaltonetworks.com/t5/custom-signatures/detecting-a-specific-linux-binary-elf-file-using-a-custom/td-p/88888

Antivirus Best Practices

- Use a Strict AV Profile, where action for all the decoders are ‘reset-both’.
- Apply the AV Profile on all relevant security policies.
- Configure SSL Decryption and Inbound Inspection wherever relevant, make it mandatory for emails as well.
- Scheduled AV and Wildfire bundles (Device>Dynamic updates) to Download and Install:
  - AV Signatures can be set to ‘Download and Install’ hourly.
  - Wildfire Signatures can be configured to ‘Download and Install’ every minutes (for versions below 10.0) or real-time (10.0 and above).
- Review Best Practice Data Center Antivirus Profile and Best Practice Internet Gateway Antivirus Profile.

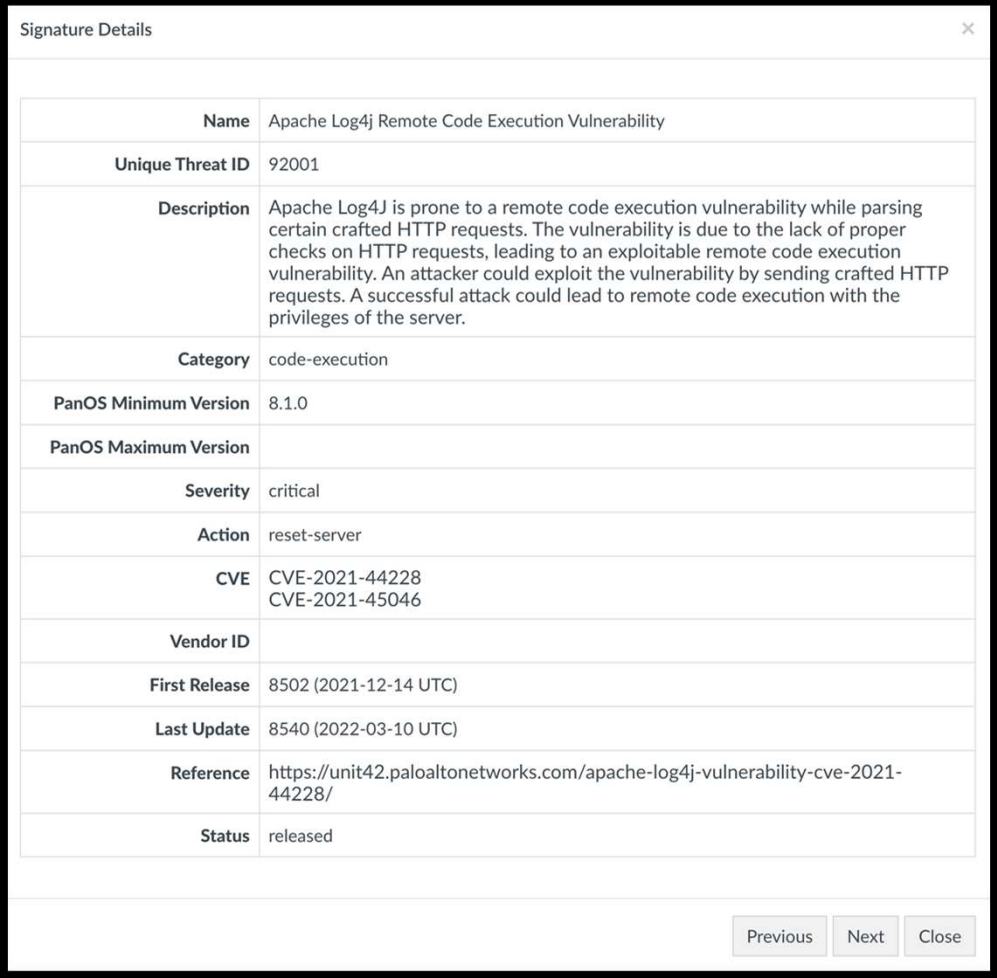
DEMO

Vulnerability Protection

Vulnerabilities & Exploits

- What is a software vulnerability?
  - A flaw or glitch in software that allows an attacker to perform unwanted actions.
  - Intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.
  - Exposed vulnerable elements of a system are referred to collectively as the ‘attack surface’.
- What is an Exploit?
  - A means of taking advantage of a vulnerability to achieve a desired goal.
- What is a zero day vulnerability?
  - A software bug that is unknown to the vendor and the general public.
  - Generally much harder to defend against 0-days because they are unknown.
- Our signatures are created based on patterns extracted from Exploits (or POCs).

Threat Vault - Example



Vulnerability Protection - Brute Force Signatures.

- The firewall includes two types of predefined brute force signatures—parent signatures and child signatures
- The relationship between Parent and Child Threat ID's is documented at https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CImpCAC
- Threat Log generation criteria for Brute Force parent/child Signature:

  https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000boRMCAY
- Customize the trigger condition for a Brute Force signatures if required.

  https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CImsCAC

IPS Signature Converter Plugin for Panorama

- Plugin Supported in Panorama starting from 10.0. Download and Install from Panorama>Plugins> IPS Signature Converter.

- Automated solution for converting rules from third-party IPS Snort and Suricata into custom Palo Alto Networks threat signatures.

- Review the attached Best Practice Guide:

  https://live.paloaltonetworks.com/t5/customer-resources/best-practices-for-working-with-snort-and-suricata-with-threat/ta-p/356849

- Additional resources for Custom Signature Creation:

  https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClOFCA0
  https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClUdCAK

Troubleshooting False Positives

- Read Description in threat vault for contextual information.
- Get more information regarding the CVE (from Mitre/NVD/Vendor).
- Assess if the server is Vulnerable to this CVE.
- Enable extended threat packet capture. Complete stream of PCAP if required.
- Open a TAC case with details:

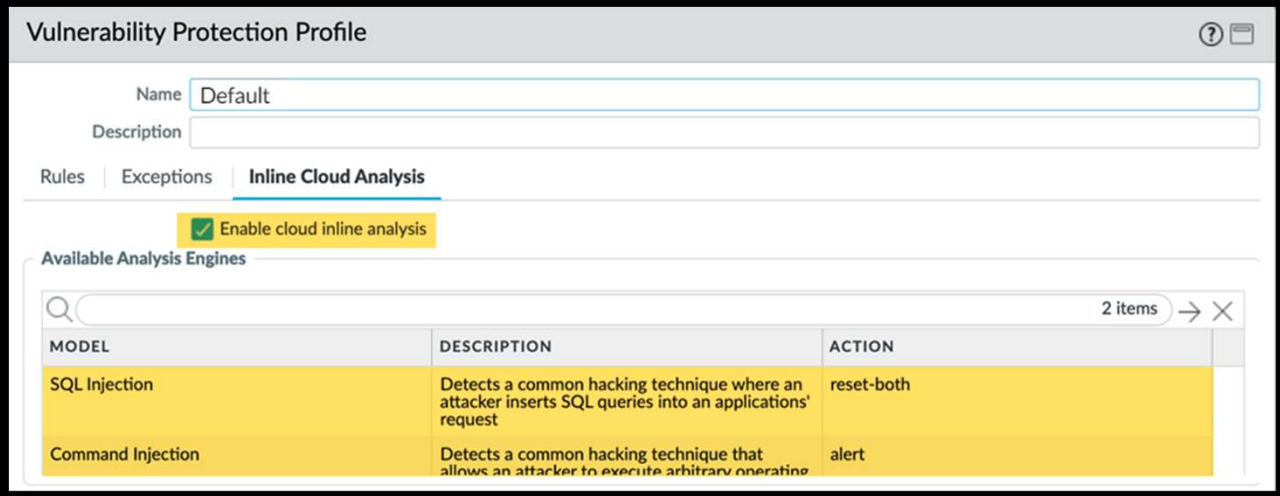
  https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClSBCA0

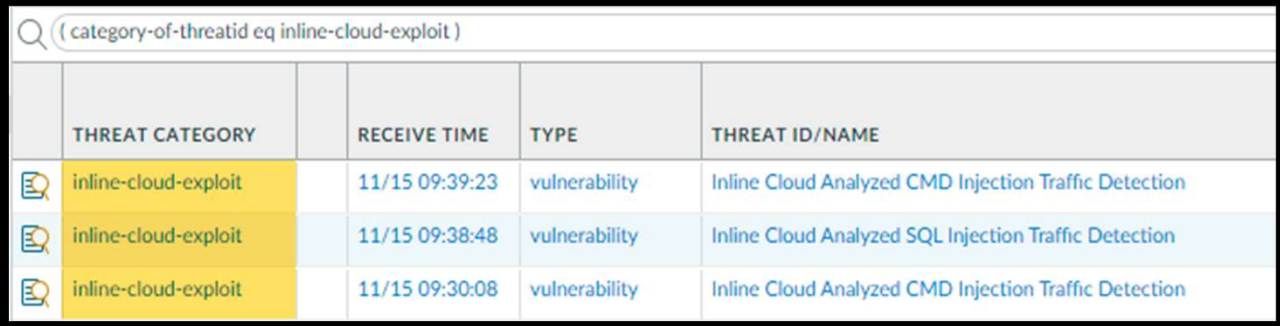
New Coverage and False Negatives

- Need an Exploit or POC for creating pattern based coverage.
- Types of vulnerabilities covered (local vs remote).
- If signature is already present, need complete stream of PCAPs to review FNs.
- Is the traffic encrypted?
- Is the Vulnerability profile applied to policy?

Advanced Threat Prevention - Inline Cloud Analysis

- Feature Introduced in 11.0. Advanced Threat Prevention License is required.
- Inline deep learning detection engines in the Advanced Threat Prevention cloud to analyze traffic for command injection (TID 99951) and SQL injection (TID 99950) vulnerabilities in real-time.
- Command to check connection status:






```
> show ctd-agent status security-client
```

Vulnerability Signature Best Practices

- Make SSL Inbound Inspection **mandatory** for all relevant servers that's accessible from internet.
- Work on hardening your vulnerability profiles, the goal should be to apply Strict profile.
- Apply the Vulnerability Profile on all relevant security policies.
- Leverage Inline Cloud Analysis for additional protection.
- Follow the Best Practices for content update to make sure that latest content updates gets installed.
- Review the best practice guide for Internet Gateway and Data Center.

DEMO

Anti-Spyware

Anti-Spyware Signatures

- Anti-Spyware signatures blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients.
- Limited number of Anti-Spyware DNS Signatures (Part of AV/WF Signature Bundle).
- The DNS capacity limitations have been overcome with the **DNS Security** Service.
- DNS Signature Support for DNS Over HTTPS was introduced in 11.0.

Threat Vault - Example

Signature Details

Name	TrickBot.Gen Command and Control Traffic Detection
Unique Threat ID	85959
Description	TrickBot is a banking malware, which appears to be the successor of the Dyre banking Trojan. Currently it is not making any effort to hide itself. It puts the word "malicious" on its user-agent.
Category	command-and-control
PanOS Minimum Version	7.1.0
PanOS Maximum Version	
Severity	critical
Action	reset-both
Vendor ID	
First Release	8292 (2020-07-14 UTC)
Latest Update	8292 (2020-07-14 UTC)
Reference	
Status	released

Previous Next Close

Anti-Spyware - DNS Signature

- DNS Signatures are delivered as a part of Antivirus Bundle, the goal is to block DNS resolution of malicious domains.

- 1) If Workstation >> Firewall >> DNS Server, then you will easily see the source IP.
  2) If Workstation >> DNS Server >> Firewall, then the firewall only sees queries sourced from the DNS Server.

  If you're with Scenario #2, then you don't have a way in the firewall to know who sent the DNS query. The place to check for that is the DNS Server logs.

  The DNS Sinkhole feature adds a 'workaround' to this issue.

- The idea is, Spyware runs the DNS query to subsequently connect to the Sinkhole IP (or CNAME).

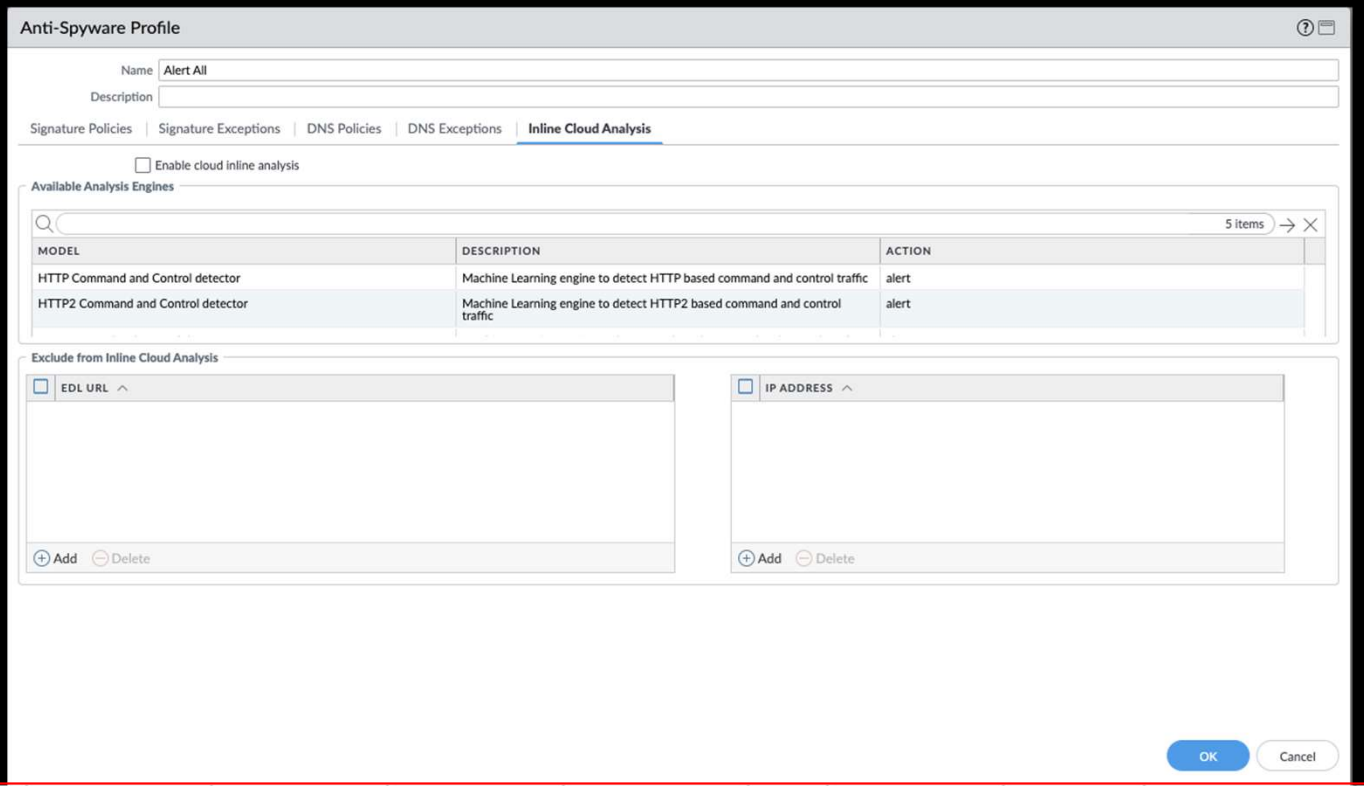
- We can filter using the Sinkhole IP in Traffic/URL Filtering logs to identify the IP address of infected hosts.

Data Needed for False Positive/Negatives

- Context/Reason (Why – What is the user trying to do?) is needed for False Positives.
- Threat/URL Filtering Log (CSV Output) and Tech Support File.
- Extended threat PCAP should be enough for majority of the False Positives. If not, complete stream of PCAP is needed.
- Complete stream of PCAP or relevant details required for False Negatives.

Advanced Threat Prevention - Inline Cloud Analysis

- New Feature Introduced in 10.2. Advanced Threat Prevention License is required.
- ML-based detection engines in the Advanced Threat Prevention cloud to analyze traffic for advanced C2 and spyware threats in real-time.
- Supports five analysis engines - HTTP, HTTP2, SSL, unknown-UDP, and unknown-TCP
- Local Deep Learning was introduced in 11.2.



		RECEIVE TIME	TYPE	THREAT ID/NAME	SOURCE ADDRESS	THREAT CATEGORY	CLOUD REPORT ID	DESTINATION ADDRESS	TO PORT	APPLICATION	ACTION	SEVERITY
		02/07 00:54:47	spyware	Inline Cloud Analyzed HTTP Command and Control Traffic Detection	192.168.180.151	inline-cloud-c2	3fab9c76b925fa...	153.92.0.100	80	web-browsing	reset-both	high

Anti-Spyware Signature Best Practices

- Set the action for DNS signatures to sinkhole wherever applicable.
- Work on hardening your Anti-Spyware profiles, the goal should be to apply Strict profile.
- Apply the Anti-Spyware Profile on all relevant security policies, this seems straight forward but I've seen this not followed in production environments.
- Leverage Inline Cloud Analysis for additional protection.
- Follow the Best Practices for content update to make sure that latest content updates gets installed.
- Review the best practice guide for Internet Gateway and Data Center.

DNS Security

Why We Introduced DNS Security?

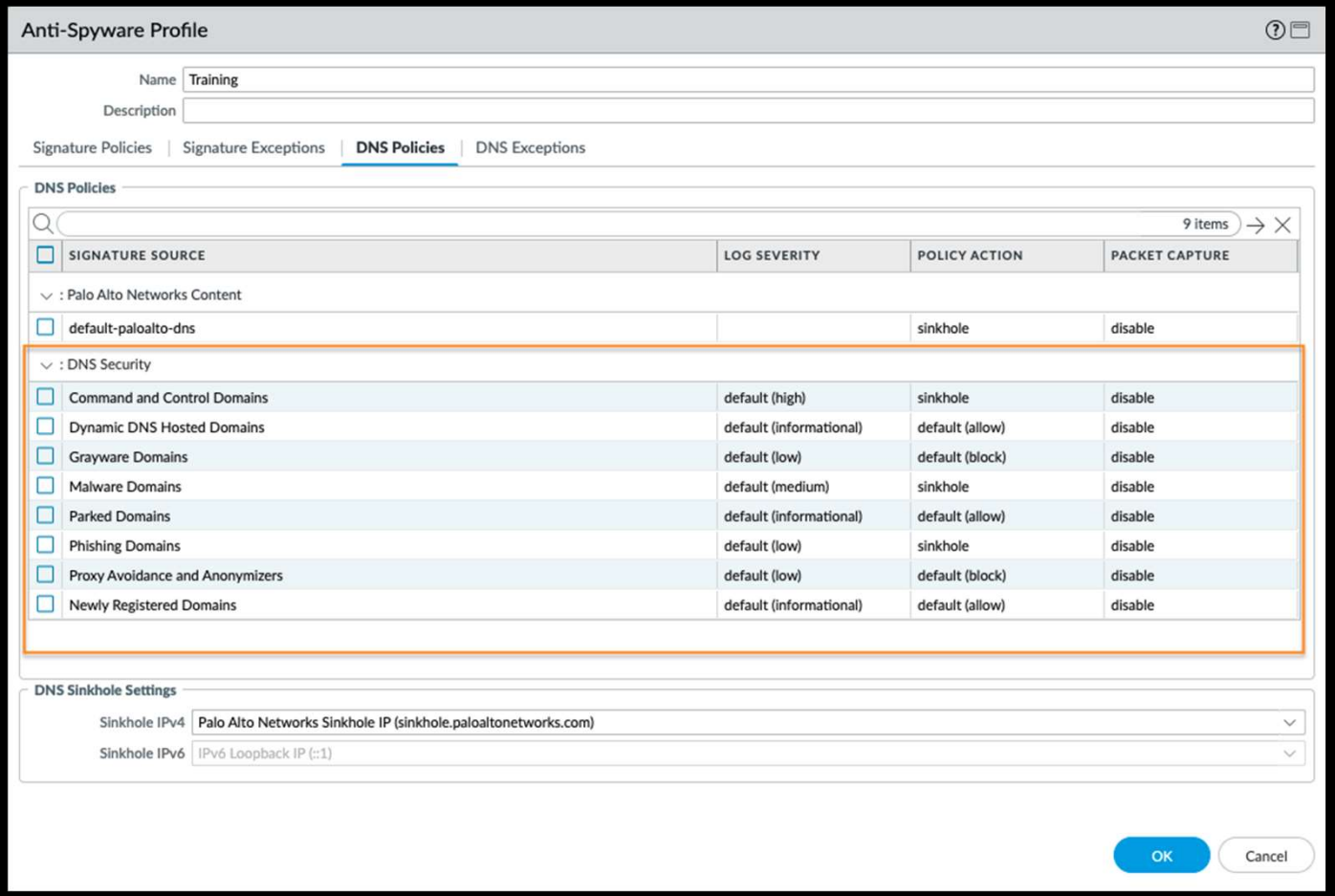
- Problem:
  - A WildFire and other IoC sources have created a proliferation of DNS signatures.
  - The number of available DNS signatures exceeds device capacity.
  - We have prioritized the “most important” sigs, and avoid shipping lower priority to work under the capacity limitations.
- Solution
  - Add capability to perform real-time signature lookups to block or sinkhole all known malware domains (also detects DNS Tunneling, DGA Domains etc).
  - Prevent initial client resolution of malicious domains by intercepting requests and performing necessary lookups via the Threat Intelligence Cloud.
  - Requires a valid **Threat Prevention** and **DNS Security License**.
- Advanced DNS Security Subscription (introduced PAN-OS 11.2) is a separate subscription offering.

Feature Details

- Policy Actions:
  - Sinkholing.
  - Blocking and Alerting.
- DNS signature checking will be completely transparent to DNS clients and servers for benign domains.
- DNS lookups will be cached (Lifetime determined by TTL of DNS record in server response) to reduce latency caused by this feature.
- Real-time DNS signature lookups will use the Palo Alto Networks Services service route.
- Connection to cloud will be held open and whitelist will be pre-populated when connection is initialized.
- DNS Security Support for DNS Over HTTPS (DoH) was introduced in PAN-OS 11.0.

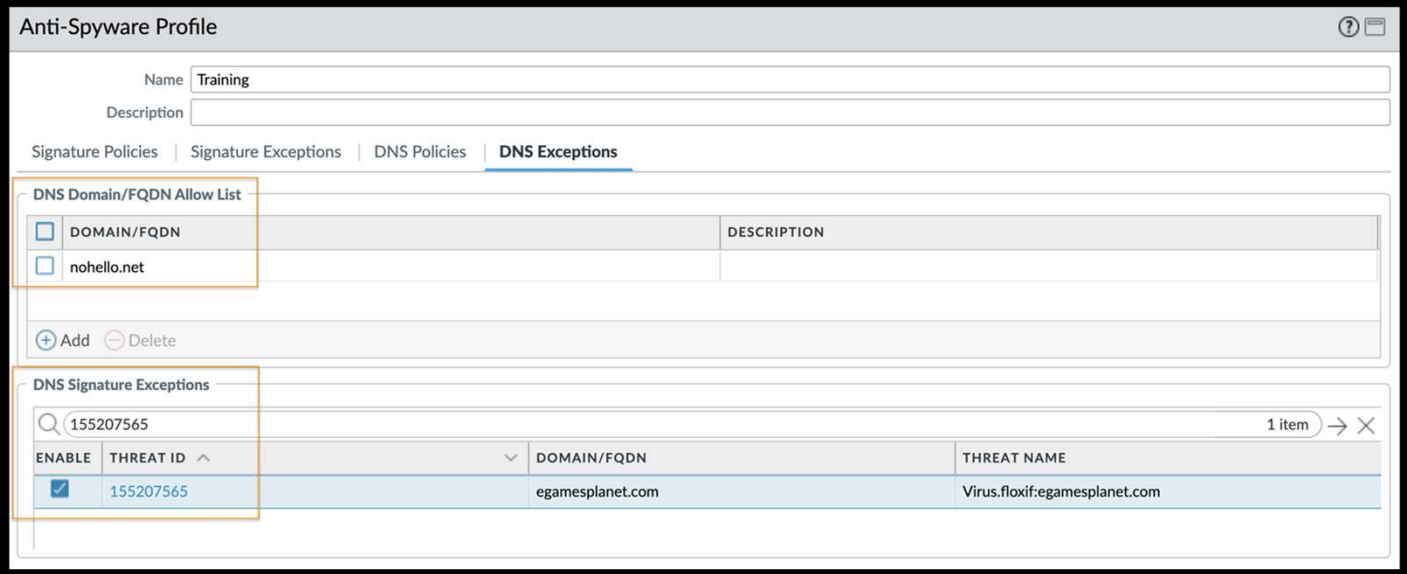
Configuration

- DNS Security is configured under Anti-Spyware Profile>DNS Policies>Signature Source.



DNS Exceptions

- Exceptions are added by searching for UTID (from Threat Vault) associated with the domain name.
- Click ‘Enable’ checkbox on desired exceptions
- ‘DNS Domain/FQDN Allow List’ can be used to add whitelist.
- Configure exception from CLI if there is connectivity issues with Threat Vault.




```
admin@PA-VM# set profiles spyware Training botnet-domains threat-exception 155207565
```

Cloud Lookup Timeout

- The cloud lookup timeout is configurable via a global setting called ‘DNS signature lookup timeout’.
  - Device > Setup > Content-ID > Realtime Signature Lookup (Default Value is 100 ms).

    Note: configuring too aggressive timeout value may result in effective persistent failure to resolve cloud lookups. How to Configure Lookup Timeout

- If connection fails or lookup times out:
  - Server response is passed to client unchanged
  - Signatures in local database are still applied
  - General approach is to fail-open

DNS Signature Cache

- From DP:

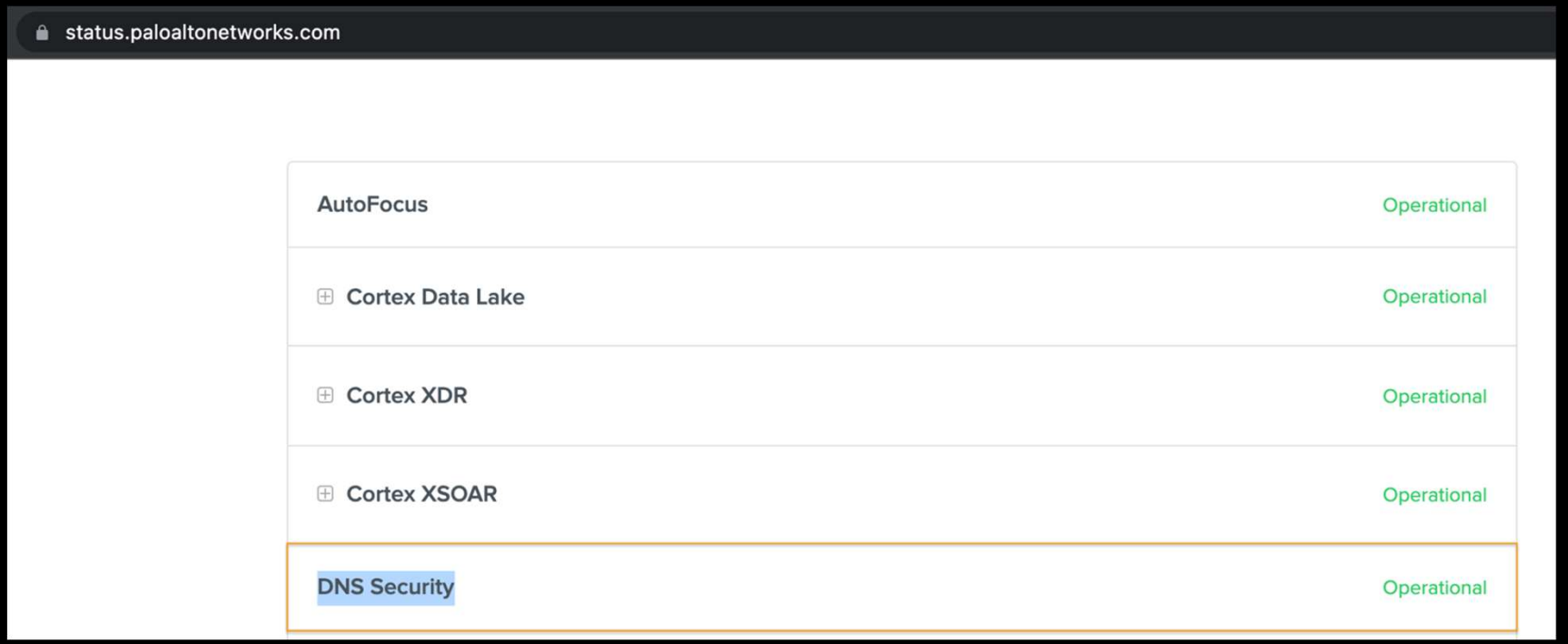
```
> debug dataplane show dns-cache print

microsoft.com, wildcard: yes, ttl: 23119/519023/0, temp: 0, verdict benign, utid: 0
msn.com, wildcard: yes, ttl: 86400/274823/0, temp: 0, verdict benign, utid: 0
oneclient.sfx.ms, wildcard: no, ttl: 3600/192028/0, temp: 0, verdict benign, utid: 0
```

- From MP:

```
> show dns-proxy dns-signature cache
Cache size: 10002
Domain                          Verdict     GTID        TTL          Hits
------------------------------------------------------------------------
*.dragonmart.ae                 White list              83472        0
*.gulftoday.ae                  White list              83453        0
```

Troubleshooting - Check Status Page

- Check that the DNS Security service is ‘Operational’ (from PA end) from https://status.paloaltonetworks.com



Troubleshooting - Check Connection Status

- Confirm the cloud connection status from CLI using the **`show dns-proxy dns-signature info`** command.
- Connection to *dns.service.paloaltonetworks.com* should be whitelist if there is another device doing decryption.

```
> show dns-proxy dns-signature info

Cloud URL: dns.service.paloaltonetworks.com:443
Telemetry URL: io.dns.service.paloaltonetworks.com:443
Last Result: Good ( 32 sec ago )
Last Server Address: 198.135.184.13
Parameter Exchange: Interval 1800 sec
Allow List Refresh: Interval 86400 sec ( Due 85733 sec )
Request Waiting Transmission: 0
Request Pending Response: 0
Cache Size: 41
```

Troubleshooting - Latency

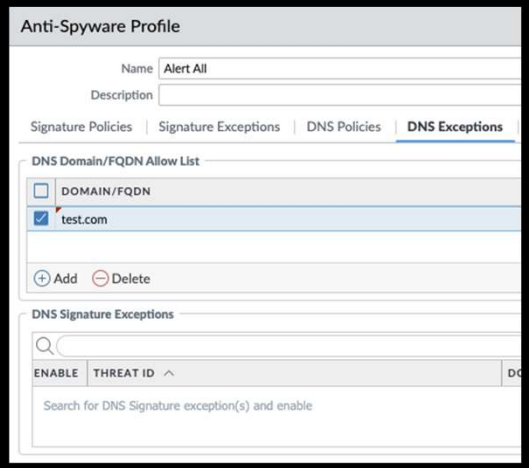
- Verify that the average latency falls within the defined timeout period.

```
> show dns-proxy dns-signature counters

Signature query API:
( ... )
  max         222 (ms)   min           4(ms)   avg       12(ms)
    50 or less : 41
   100 or less : 1
   200 or less : 0
   400 or less : 1
          else : 0
```

- Lookup timeout may need to be adjusted based on average latency to cloud.
- DNS signature counters can be reset on demand:

```
> clear dns-proxy dns-signature counters
```

Troubleshooting - FP and FN



- How to deal with False Positives?
  - Request a Verdict change for the domain from https://urlfiltering.paloaltonetworks.com/ , signature gets disabled when verdict is changed.
  - Create an Exception.
- How to deal with False Negatives?
  - Request a Verdict change for the domain from https://urlfiltering.paloaltonetworks.com/ , signature gets automatically generated when verdict gets changed to malware/C2/Phishing category.
  - Add the domain manually to an EDL that's called in DNS Policies.
  - Change the verdict of the domain to malware/c2 from CLI.

Troubleshooting - Clear Cache

- Clear DNS Proxy signature cache.
  - From DP:

```
> debug dataplane reset dns-cache
+ fqdn      fqdn
  <Enter>   Finish input
```

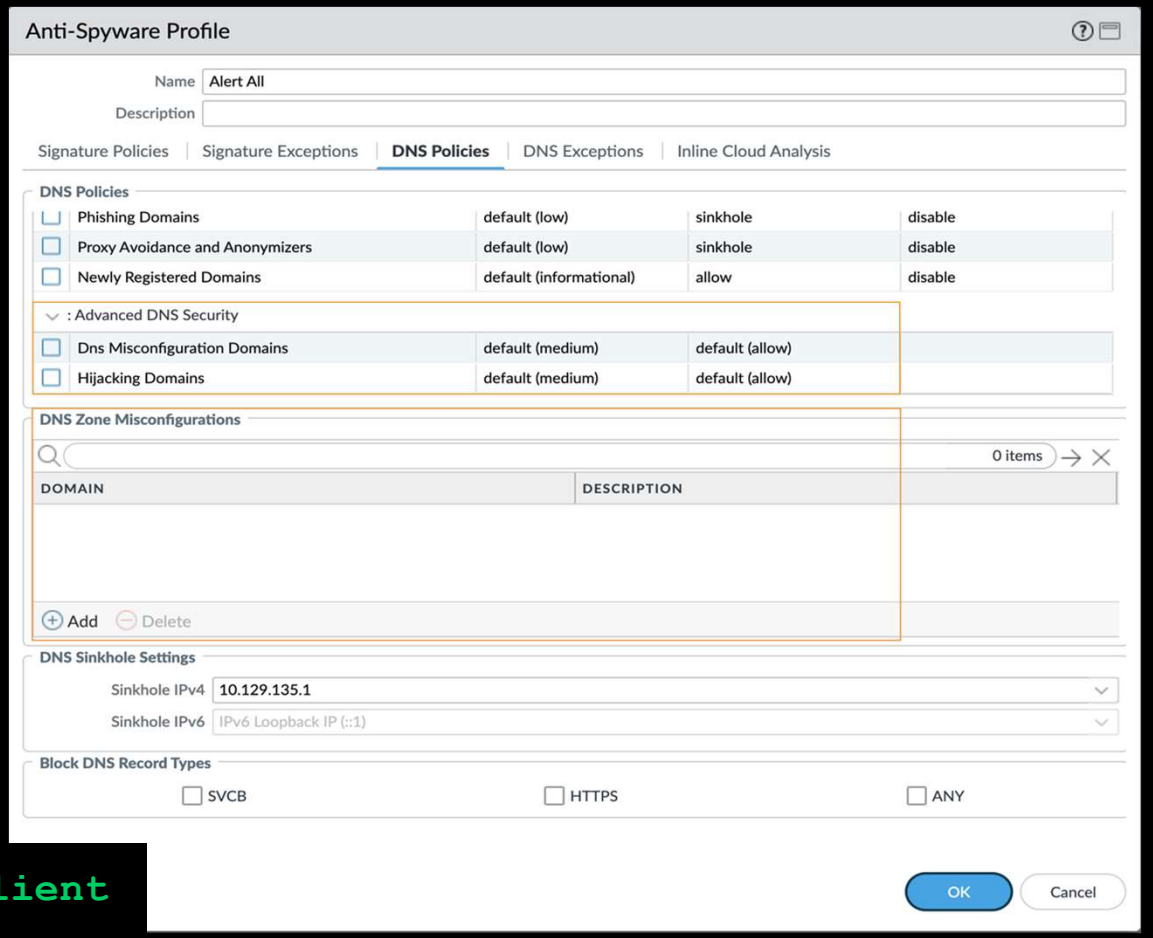
  - From MP:

```
> clear dns-proxy dns-signature cache
+ fqdn      fqdn
  <Enter>   Finish input
```

- **Caution**: if issued without an fqdn specified, command will clear the entire cache
  - Not recommended to clear full cache in production!

Advanced DNS Security Subscription

- Requires PAN-OS 11.2+ and Advanced DNS Security subscription that detects Hijacked Domains and Misconfigured DNS.
- Direct inline ML model running on a PAN-OS device to build a behavioral model of a company's normal DNS activity.
- Specify any public-facing parent domains within your organization that you want Advanced DNS Security to analyze and monitor for the presence of misconfigured domains.




```
> show ctd-agent status security-client
```

DEMO

URL Filtering

URL Filtering Basics

- URL Filtering requires Advanced URL Filtering license.
- URL Filtering can be applied as a security profile or a policy match condition, this is particularly useful for SSL Decryption policies.
- URL Filtering looks at HTTP requests from a client to identify the URL.
- Session end reason for URLs blocked will be ‘threat’.
- HTTP requests are encapsulated inside SSL when using HTTPS:
  - SSL decryption is required to see the HTTP Request.
  - Without decryption, URL Filtering decisions will be based on the SNI (Server Name Indication) value in ClientHello
    ‘or’ Domain names in the Common Name (CN) in the Subject field from the Server Certificate.
- Advance URL Filtering Security Subscription provides real-time URL analysis and malware prevention. This is available on firewalls operating PAN-OS 9.0 and later, with the installation of content release 8390-6607.
- Inline Categorization was first introduced in 10.0 and later modified with cloud Inline Categorization in 10.1

URL Filtering Details

- Management plane communicates with PAN-DB, the retrieves category information is cached in the management plane (MP) and it's then passed to the dataplane (DP).
- URL category lookup happens in below priority:
  - Firewall checks exception list first (Custom URL categories and EDL).
  - Firewall checks the DP cache.
  - Firewall checks the MP cache.
  - If none of the above has the category, firewall communicates with PAN-DB cloud to get the URL category.
  - Real-time-detection is done if Advanced URL Filtering License is present.
- Confirm that the 'cloud connection' is in 'connected' status using below command.

```
> show url-cloud status
```

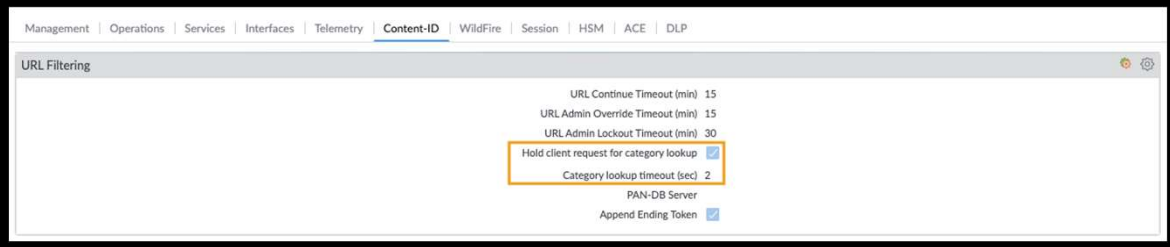
Security-Focused URL Categories

- Include High-Risk, Medium-Risk, Low-Risk and Newly-Registered Domains (NRD). This can be leveraged for targeted decryption and blocking.
- Unknown domains are classified as High-Risk until PAN-DB completes site analysis and categorization.
- Recommended to ‘Block’ NRDs as new domains are frequently used as tool in malicious campaigns.
- Recommended action is ‘Alert’ for high-risk and medium-risk.
- You cannot submit a change request for Security-Focused URL Categories, open a case with TAC of you have queries.

Hold Web Request During URL Category Lookup

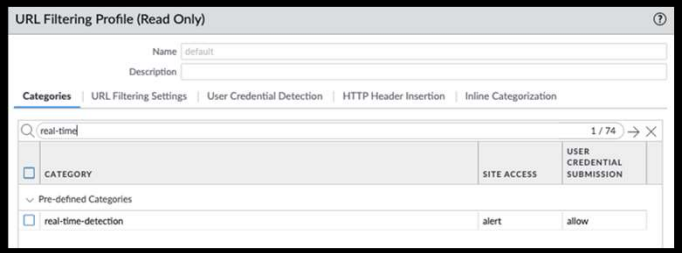
- Flexibility to hold or allow initial web requests while the firewall checks the URL category for the destination websites.

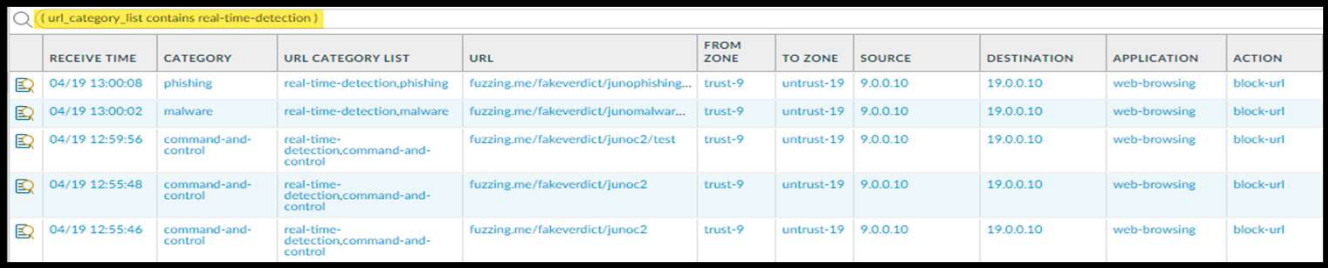
- Not enabled by default, the firewall allows the web requests to pass through during this cloud lookup and enforces policy as needed after the server responds.



Real-time-detection - Advanced URL Filtering

- Recommends setting the real-time-detection action setting to alert for your active URL filtering profiles. This provides visibility into URLs analyzed in real-time and will block (or allow, depending on your policy settings) based on the category settings configured for specific web threats.
- The firewall enforces the most severe action of the actions configured for detected URL categories of a given URL.
- URL Category list will have ***real-time-detection*** for URLs analyzed and categorized as malware/phishing in real-time.





RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	DESTINATION	APPLICATION	ACTION
04/19 13:00:08	phishing	real-time-detection,phishing	fuzzing.me/fakeverdict/junophishing...	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url
04/19 13:00:02	malware	real-time-detection,malware	fuzzing.me/fakeverdict/junomalwar...	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url
04/19 12:59:56	command-and-control	real-time-detection,command-and-control	fuzzing.me/fakeverdict/junoc2/test	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url
04/19 12:55:48	command-and-control	real-time-detection,command-and-control	fuzzing.me/fakeverdict/junoc2	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url
04/19 12:55:46	command-and-control	real-time-detection,command-and-control	fuzzing.me/fakeverdict/junoc2	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url

Inline ML

- License Requirement:

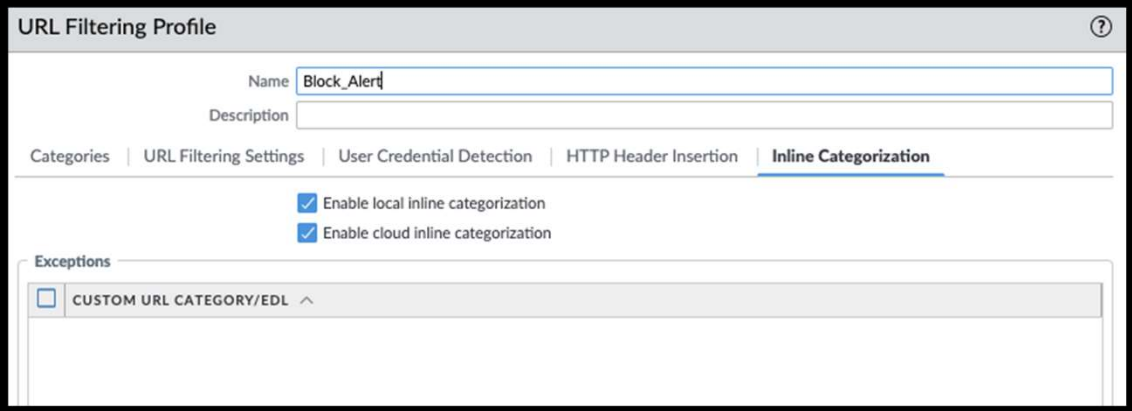
  Local inline categorization > Legacy or Advanced URL Filtering license.

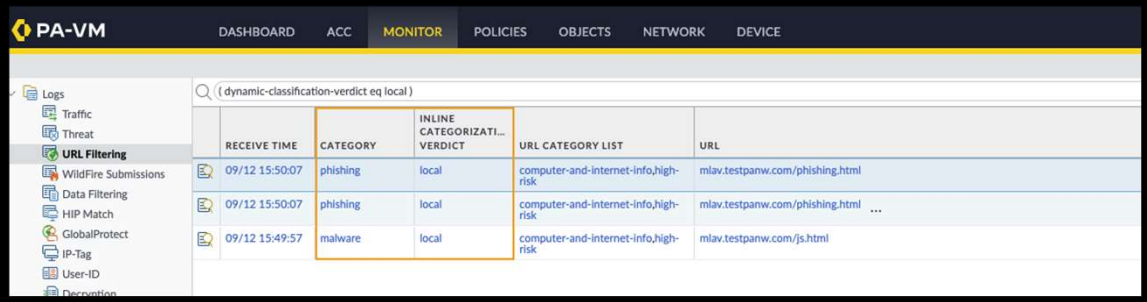
  Cloud inline categorization > Advanced URL Filtering license

- Firewall forwards HTTP payload to cloud to run more ML models to identify URL categories.

- Custom URL Categories/EDL can be added into Exceptions to exclude from Inline ML.

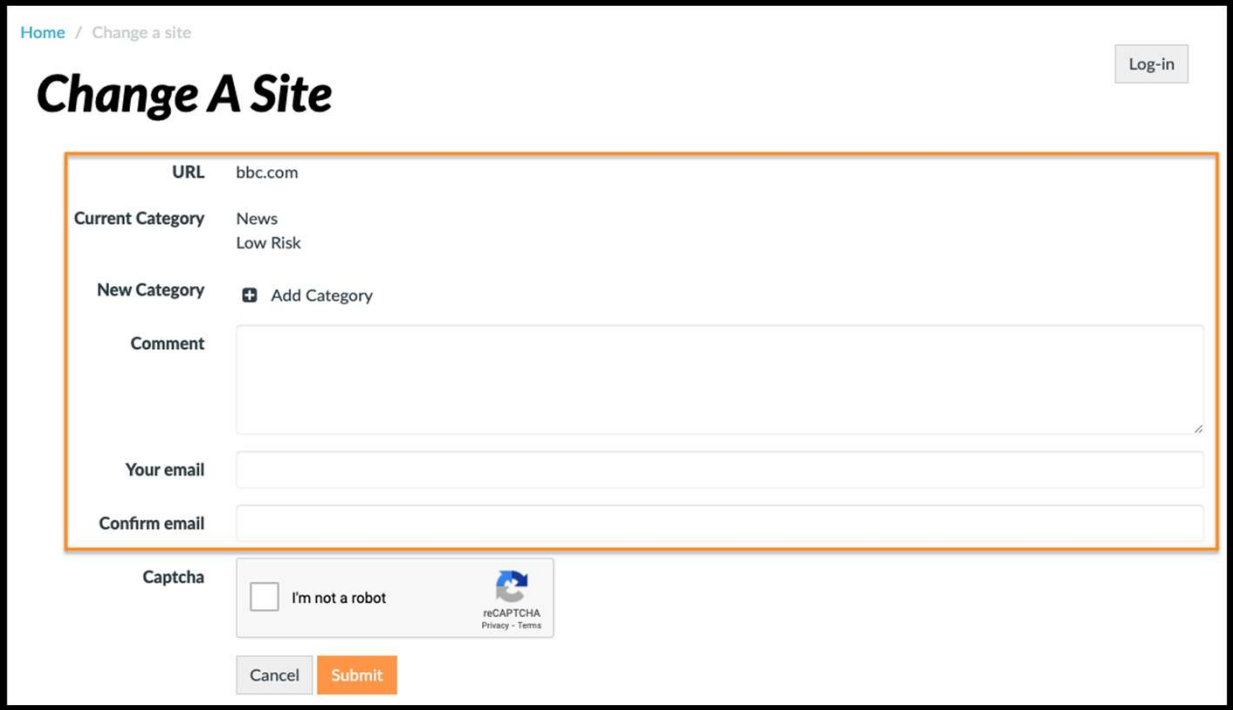
- Max-Latency and action on Max-Latency can be configured under ***Device>Setup>Content-ID>URL Inline Cloud Categorization.***





False Positive/Negative - Category Change

- Visit Test A Site to check the current category of a URL.
- Click ‘Request Change’ to submit a category change request.
- PAN-DB team will review the request and provide an update over email.
- Bulk change request is also possible after logging in.



False Positive/Negative - Exception and Category Change

- Create a Custom URL category for the Domain/URL while PAN-DB team is reviewing the change request as Custom URL category takes precedence.

- Check the URL cache and clear it if category is changed in PAN-DB and cache is showing a different category:

```
> test url <URL>                          (to view the URL category)
> clear url-cache url <URL>               (to delete cache from DP)
> delete url-database url <URL>           (to delete cache from MP)
```

URL Filtering Best Practices

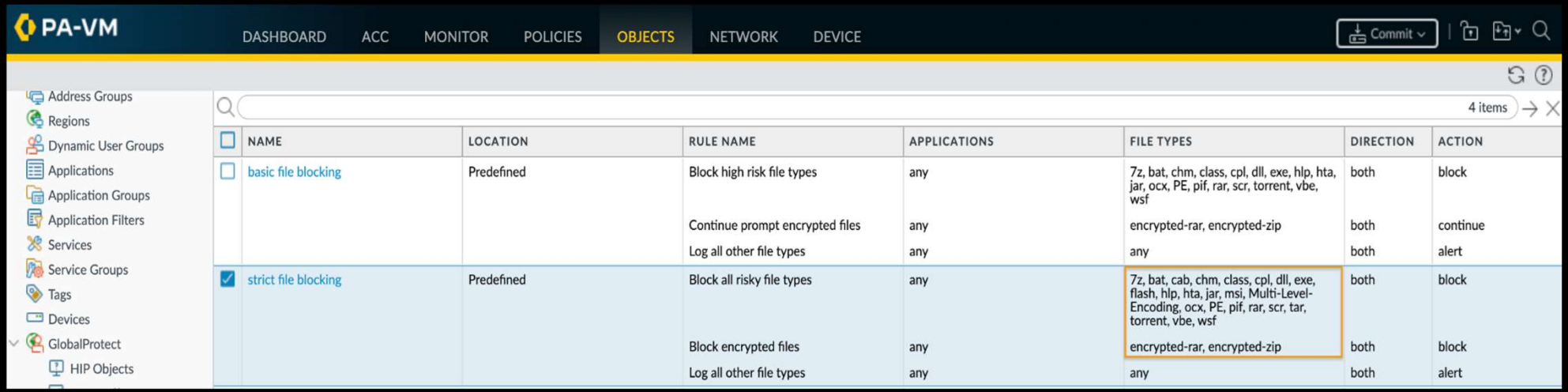
- Make sure to review and enable at-least ‘default’ URL Filtering on all relevant policies.
- Block Newly Registered Domains and closely monitor connection to Unknown URLs.
- Decrypt high-risk and medium-risk sites and enable Strict Profiles on security policy matching high-risk and medium-risk sites.
- Leverage real-time-detection and Inline Categorization for additional protection.
- Additionally, leverage the User Credential Detection feature in URL Filtering.
- Review URL Filtering Best Practices

DEMO

Others - Additional Features and Best Practices

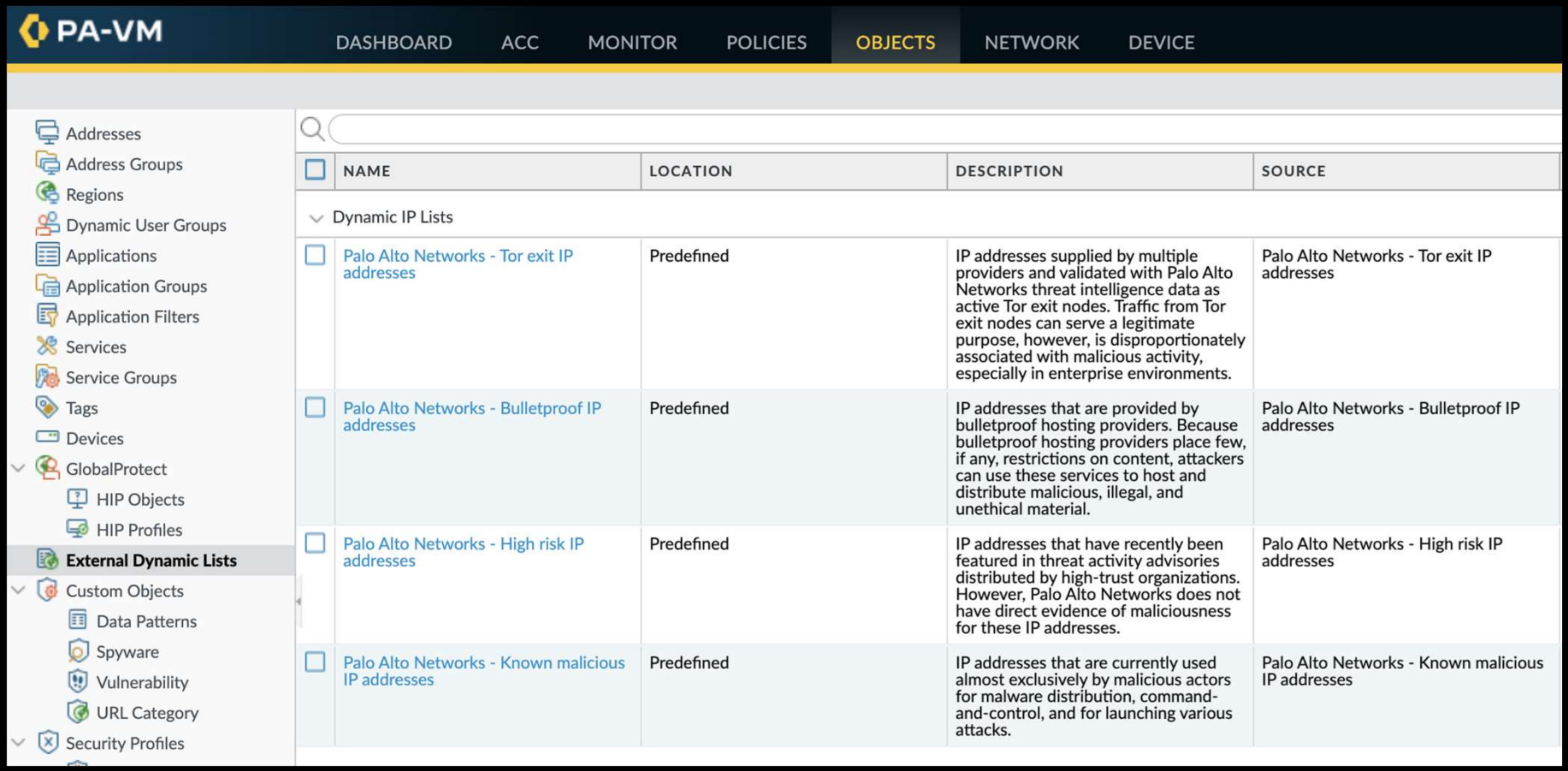
File Blocking

- Use Strict File Blocking profile whenever possible, specifically to High and Medium risk URL categories.
- Use APP-ID based security policy to add more granular and hardened File blocking profile, do you really need to allow PE or Powershell over SMTP??
- Encrypted-rar and encrypted-zip are actively used in malware campaigns.



NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
		Log all other file types	any	any	both	alert
strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
		Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
		Log all other file types	any	any	both	alert

PANW Predefined Dynamic List



Others

- Unknown-TCP, Unknown-UDP and Unknown-IP should not be allowed from/to Internet.
- Follow the best practices for securing admin access to the devices. Review https://docs.paloaltonetworks.com/best-practices.
- Leverage ‘Informational’ signatures whenever required. For example, below signature can be used to block remote execution of PsExec:

```
Name: PSEXEC SMB V2 Remote Execution Found
 Unique Threat ID: 36540
```

Questions?

Thank You

paloaltonetworks.com