# Preventing Known and Unknown Threats

# Agenda

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

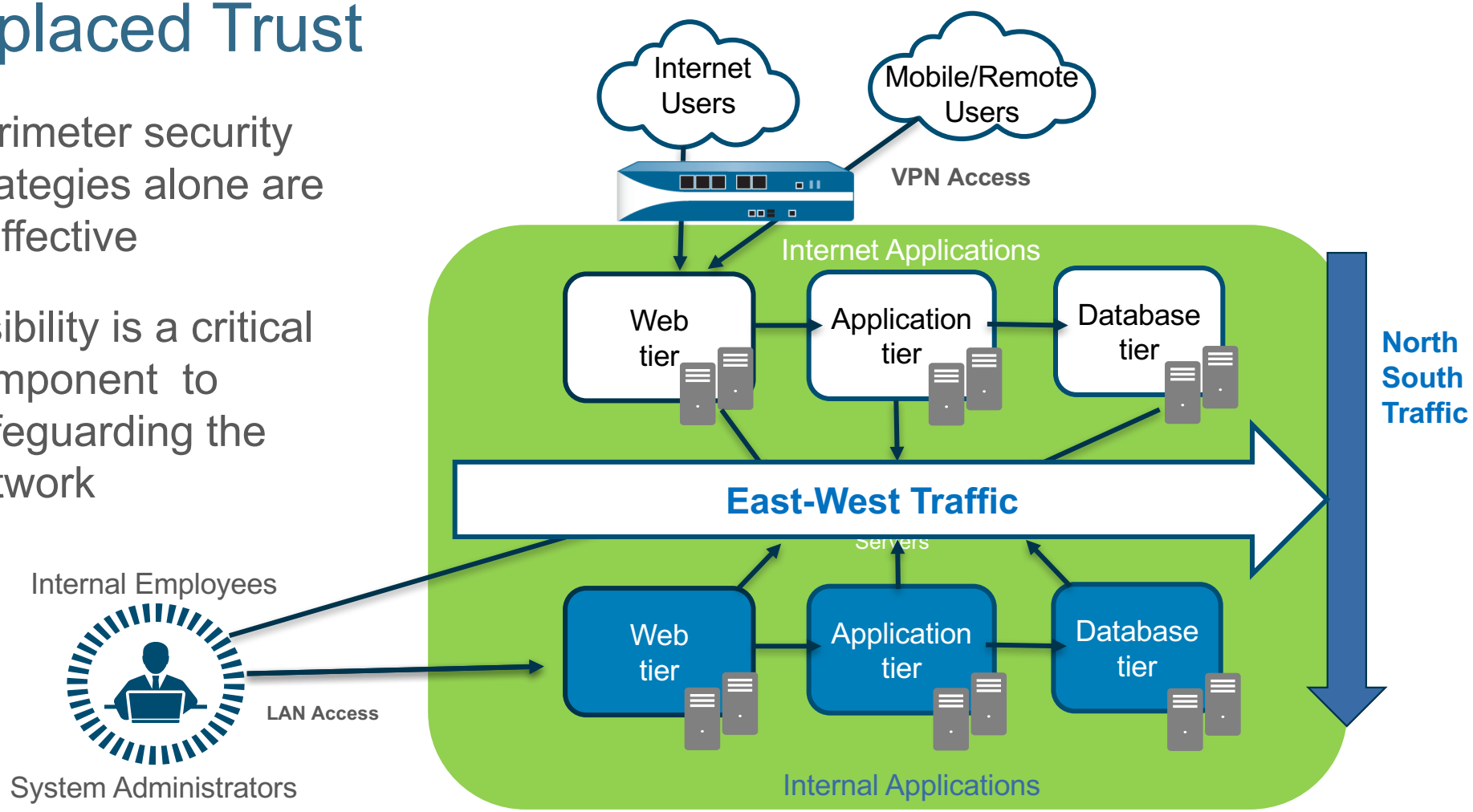
 

# Zero Trust

# Misplaced Trust

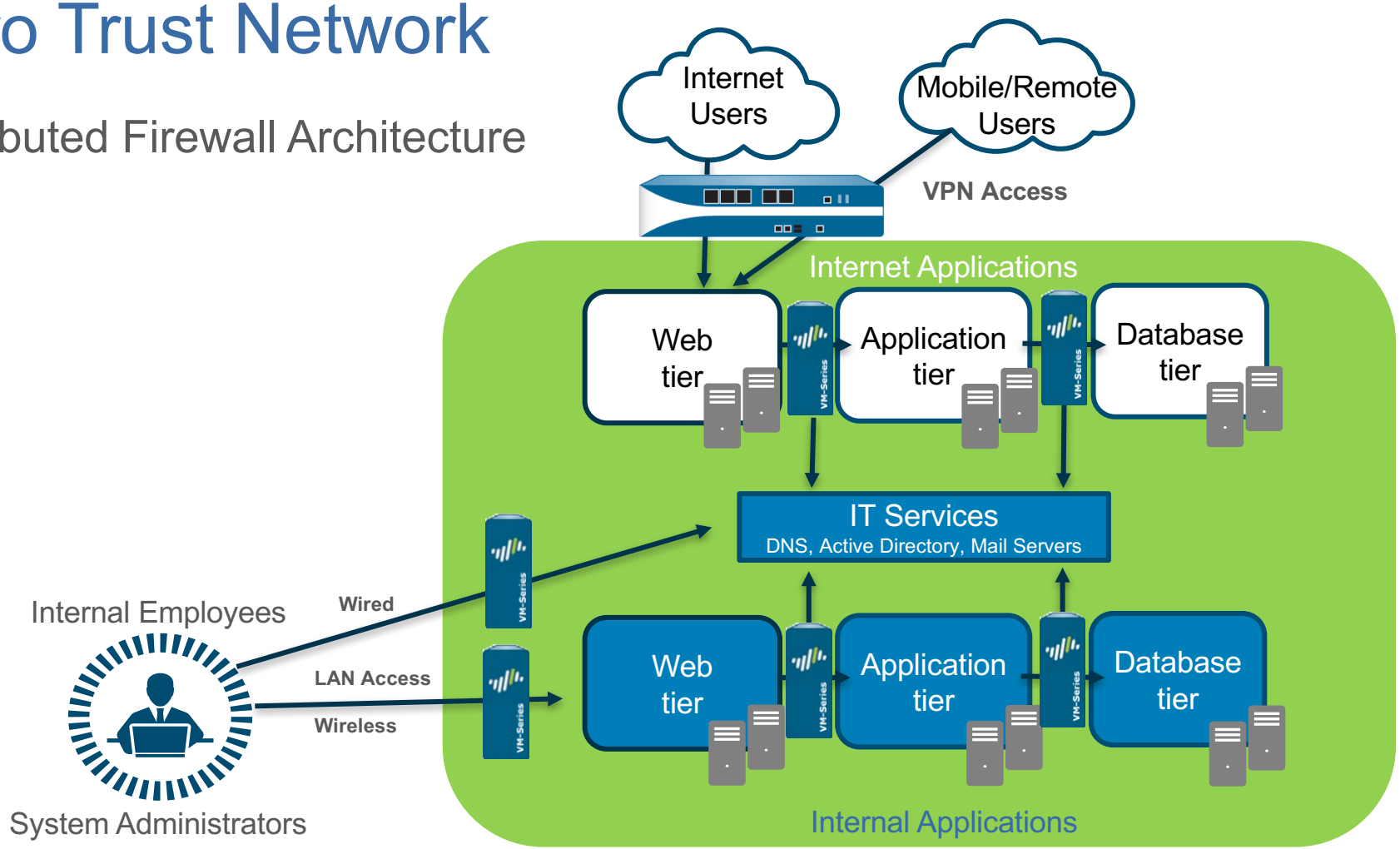
- Perimeter security strategies alone are ineffective
- Visibility is a critical component to safeguarding the network



# Zero Trust Network

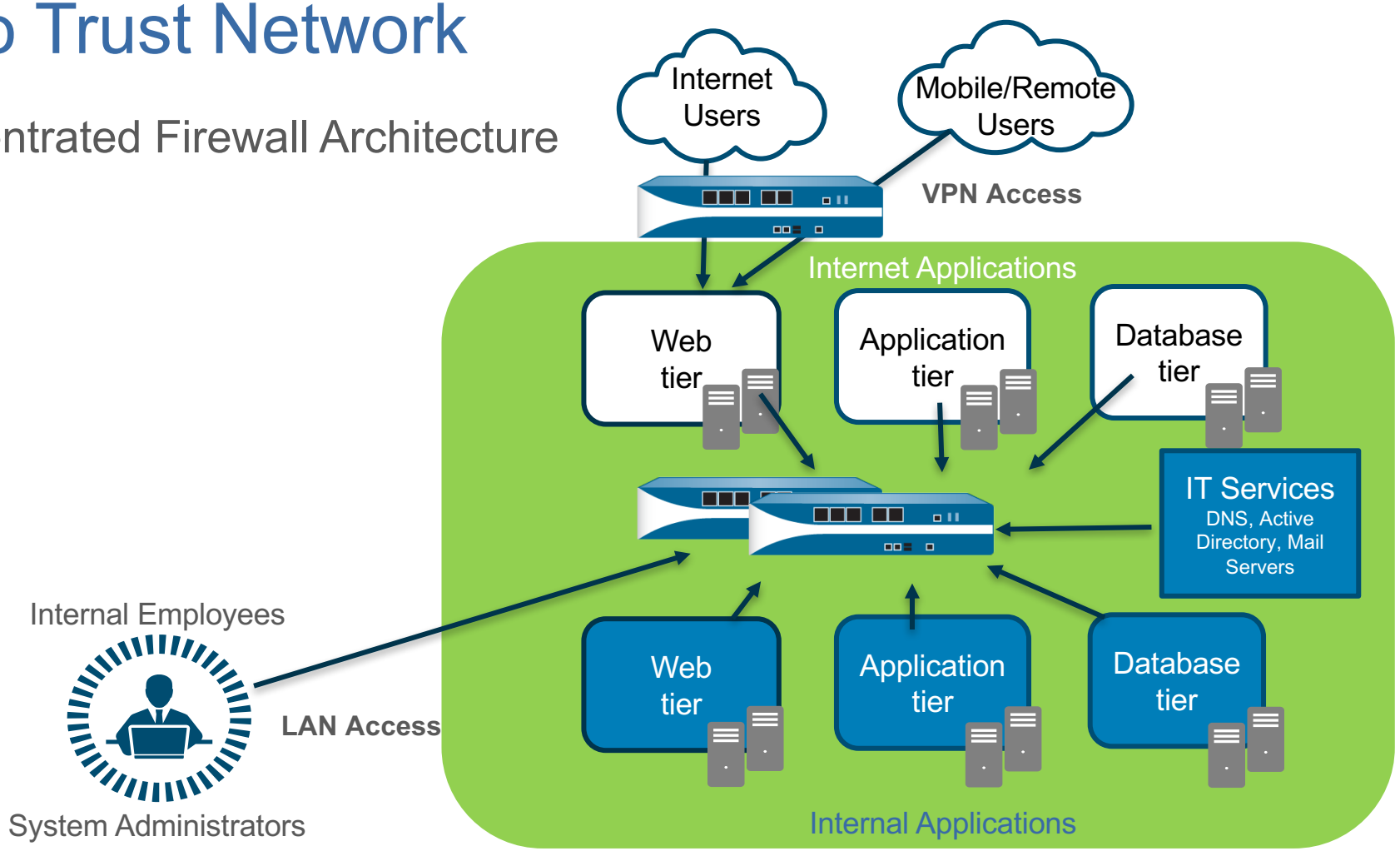
## Distributed Firewall Architecture



# Zero Trust Network

## Concentrated Firewall Architecture



# Profiles

# Security Profiles

**Policies > Security**

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

Antivirus

URL Filtering

Anti-Spyware

File Blocking

Vulnerability

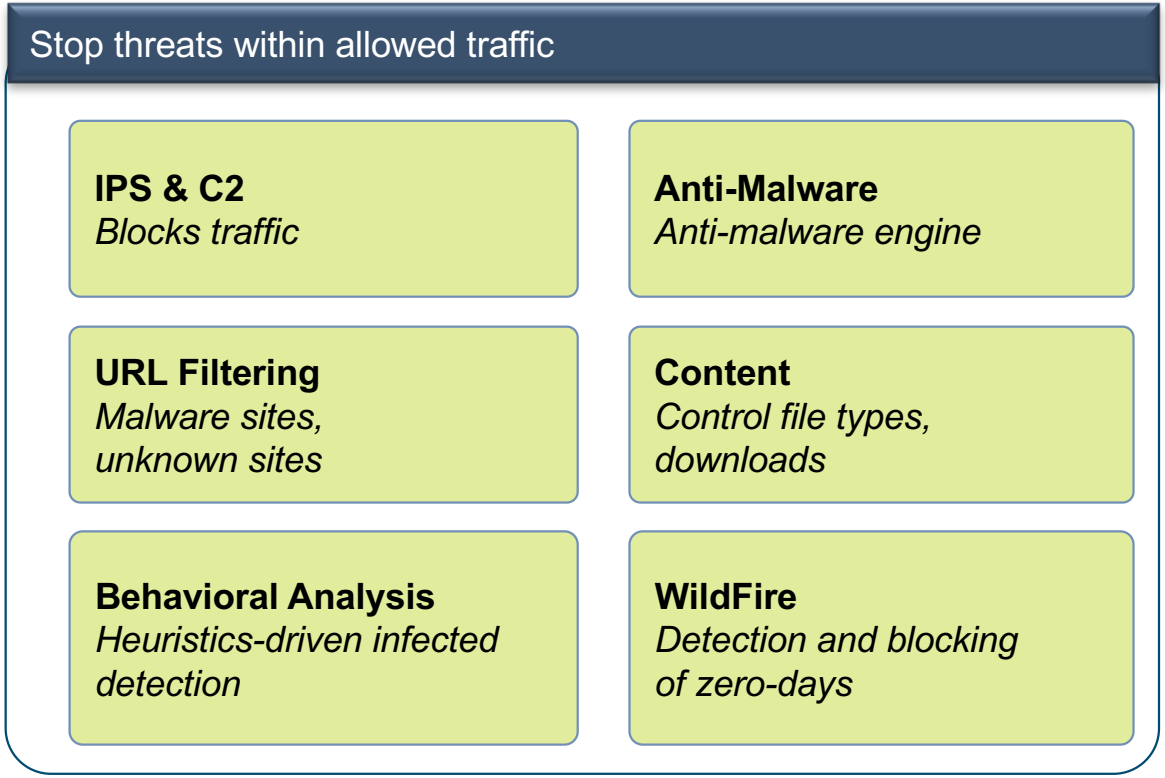
Data Filtering

WildFire Analysis

# Integrated Threat Prevention

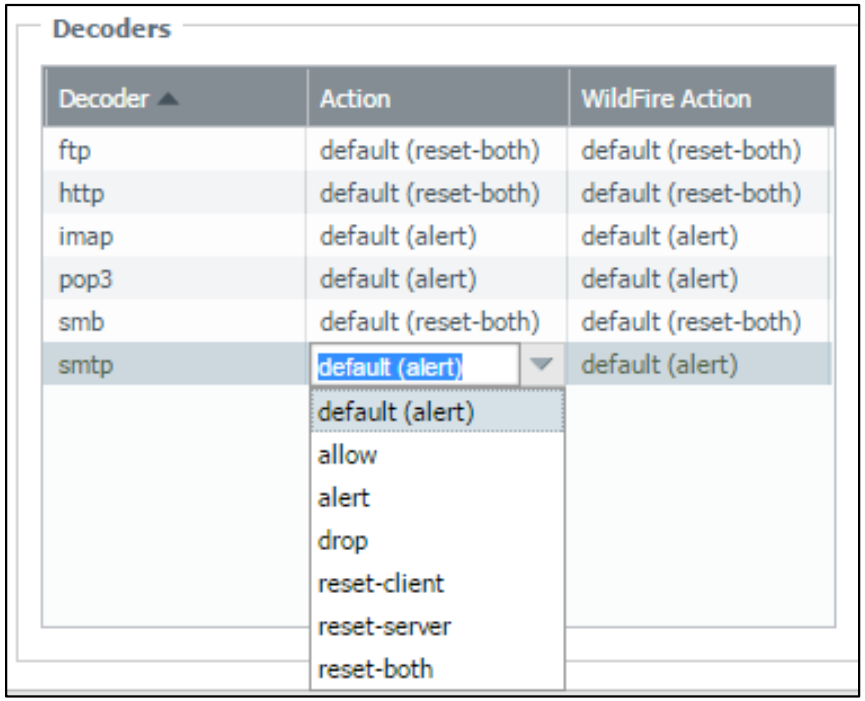
- Multiple security disciplines in a single threat prevention engine



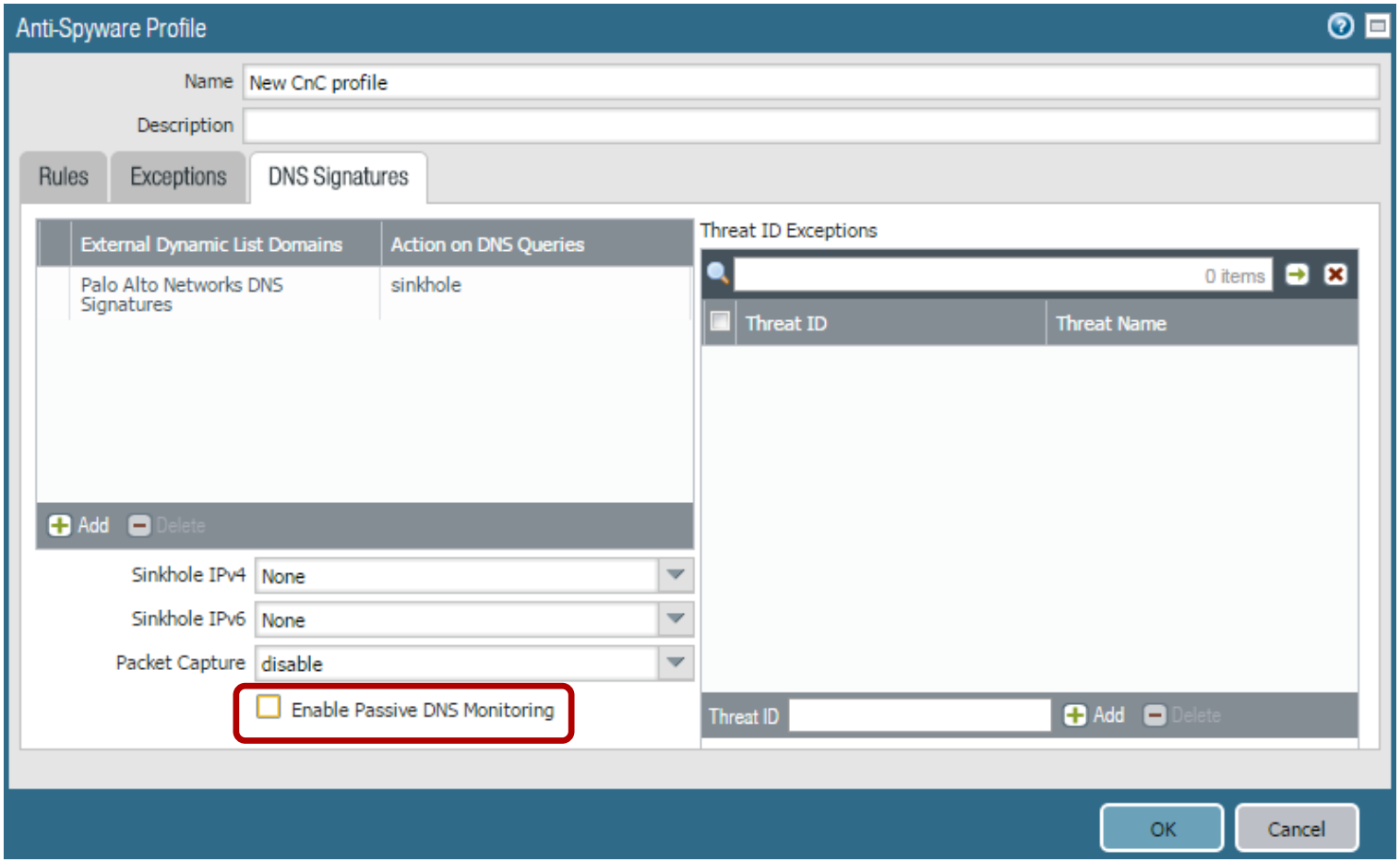
# Antivirus Profile—Default Action

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



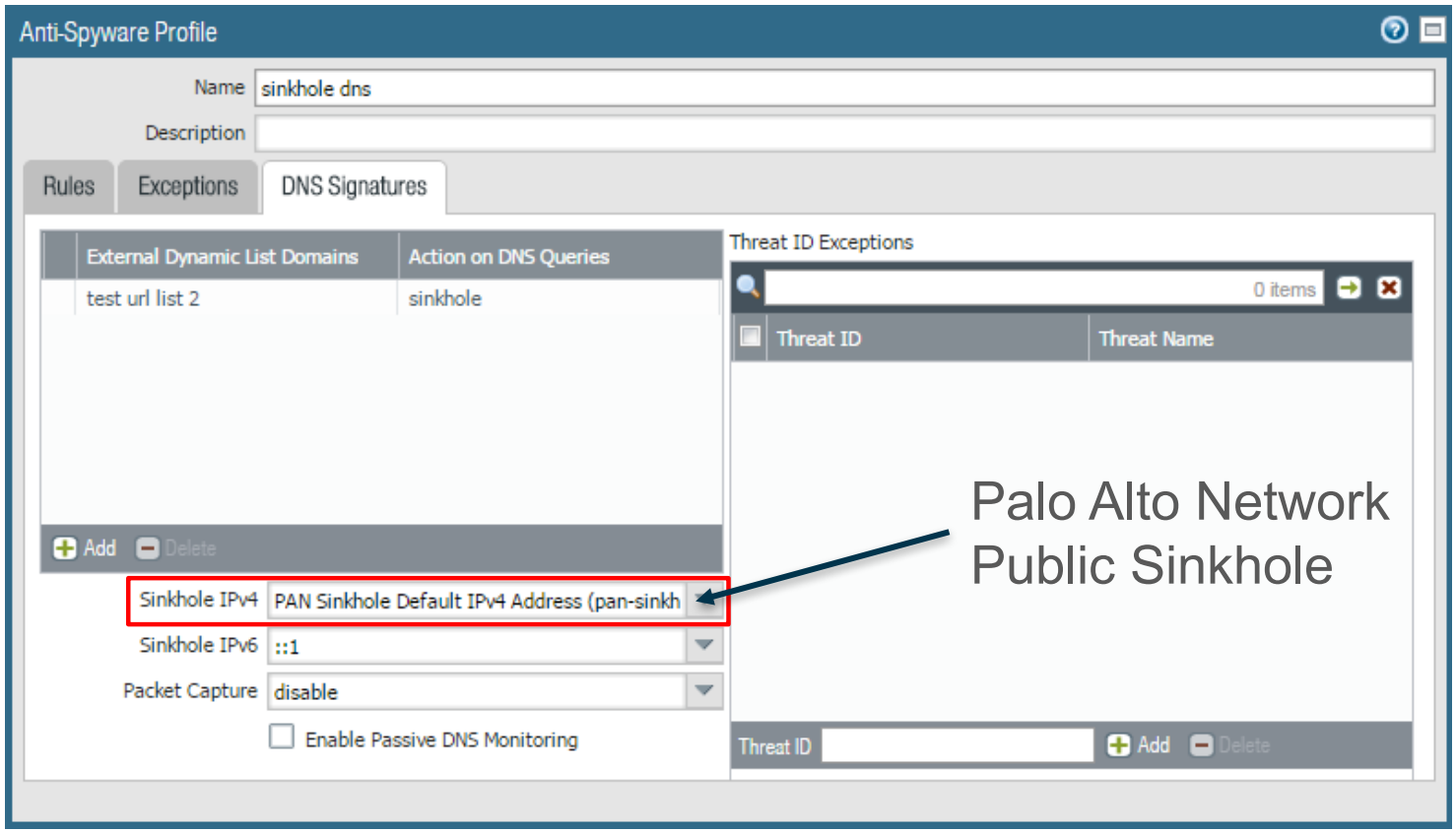
# Anti-Spyware Profile—DNS Signature Tab



# DNS Sinkhole Configuration

**Object > Anti-Spyware > DNS Signature**



# Vulnerability Protection Security Profile—Default Action

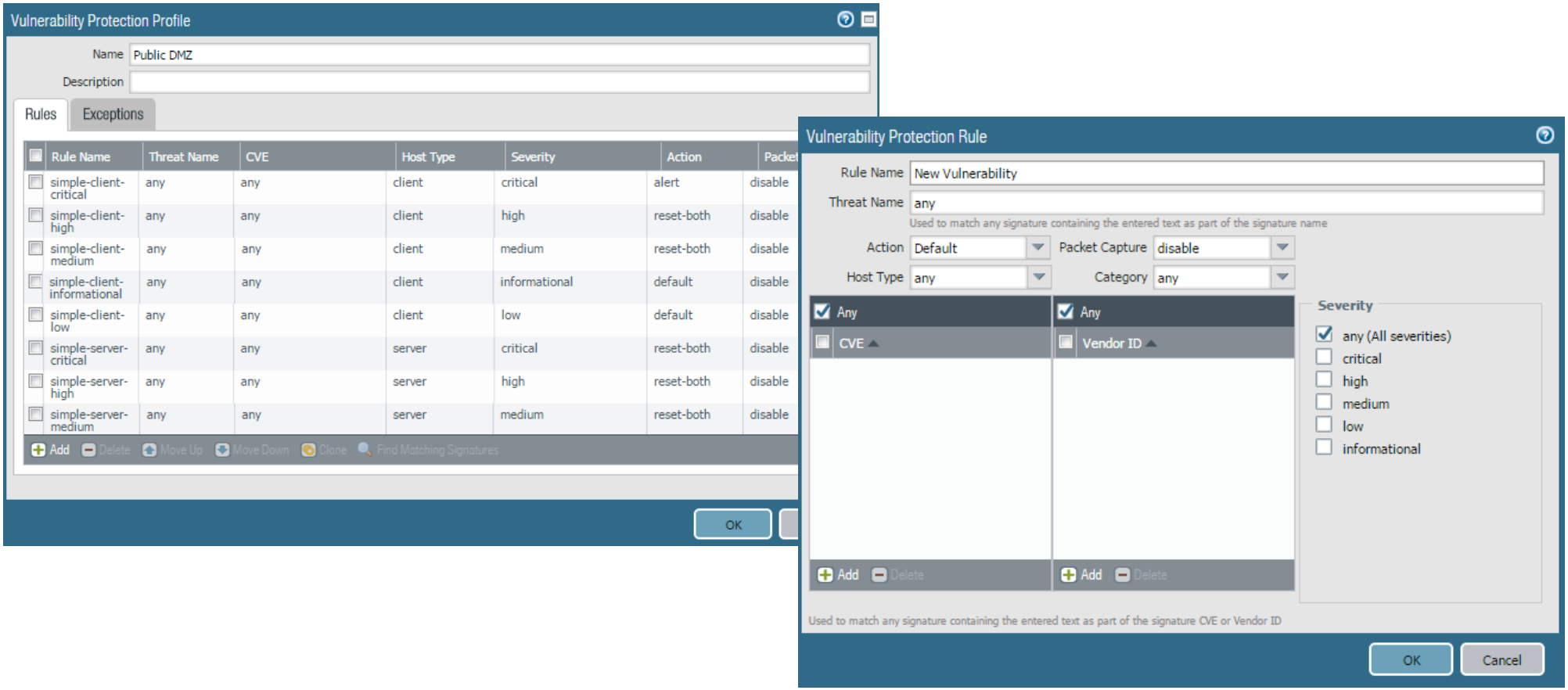
## Default action set by Palo Alto Networks within the signatures

**Objects > Security Profiles > Vulnerability Protection**

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

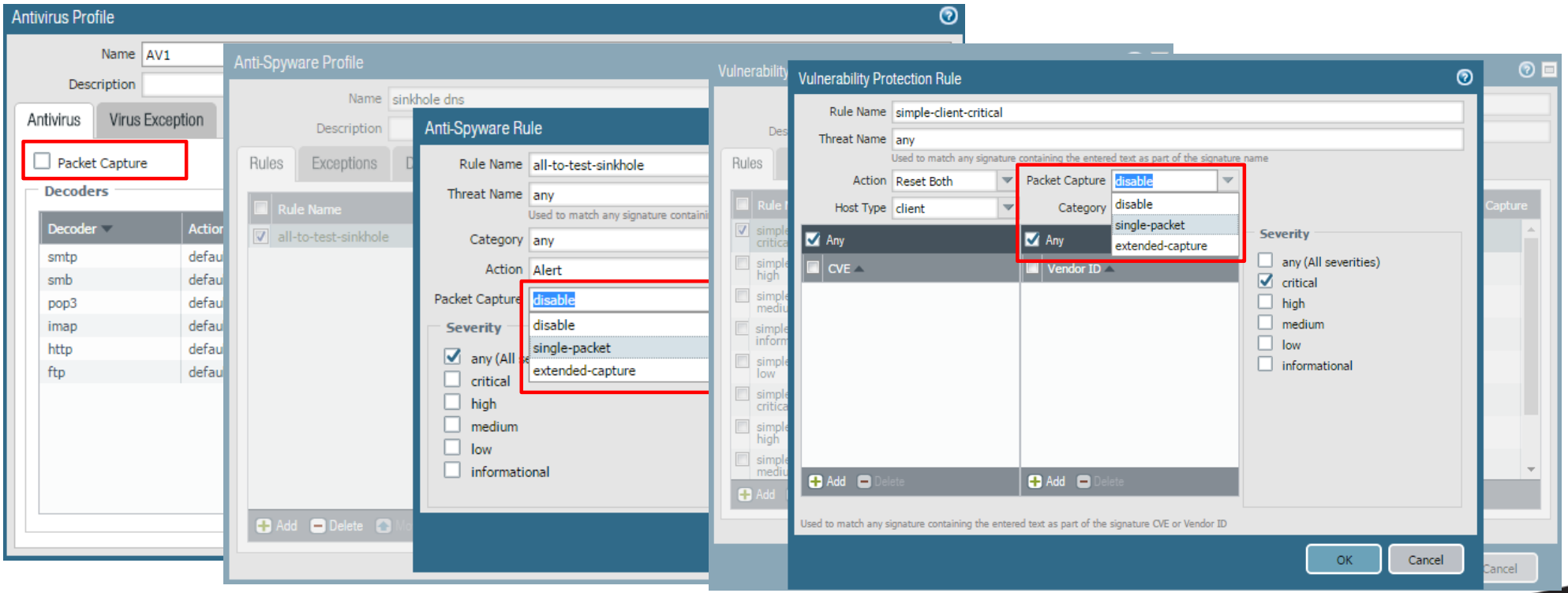
# Anti-Spyware and Vulnerability Protection



# Enable Packet Captures on other Security Profiles

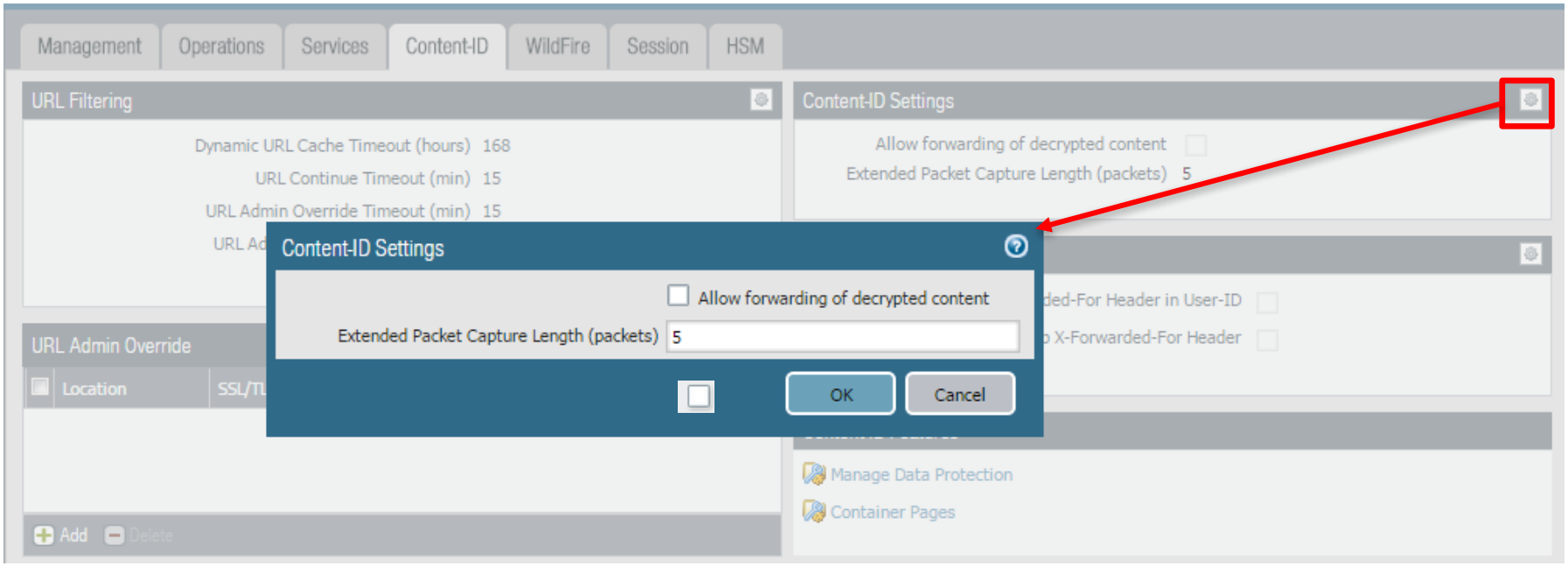
Select the check box or appropriate pull down if you want to capture identified packets



# Extended Packet Capture

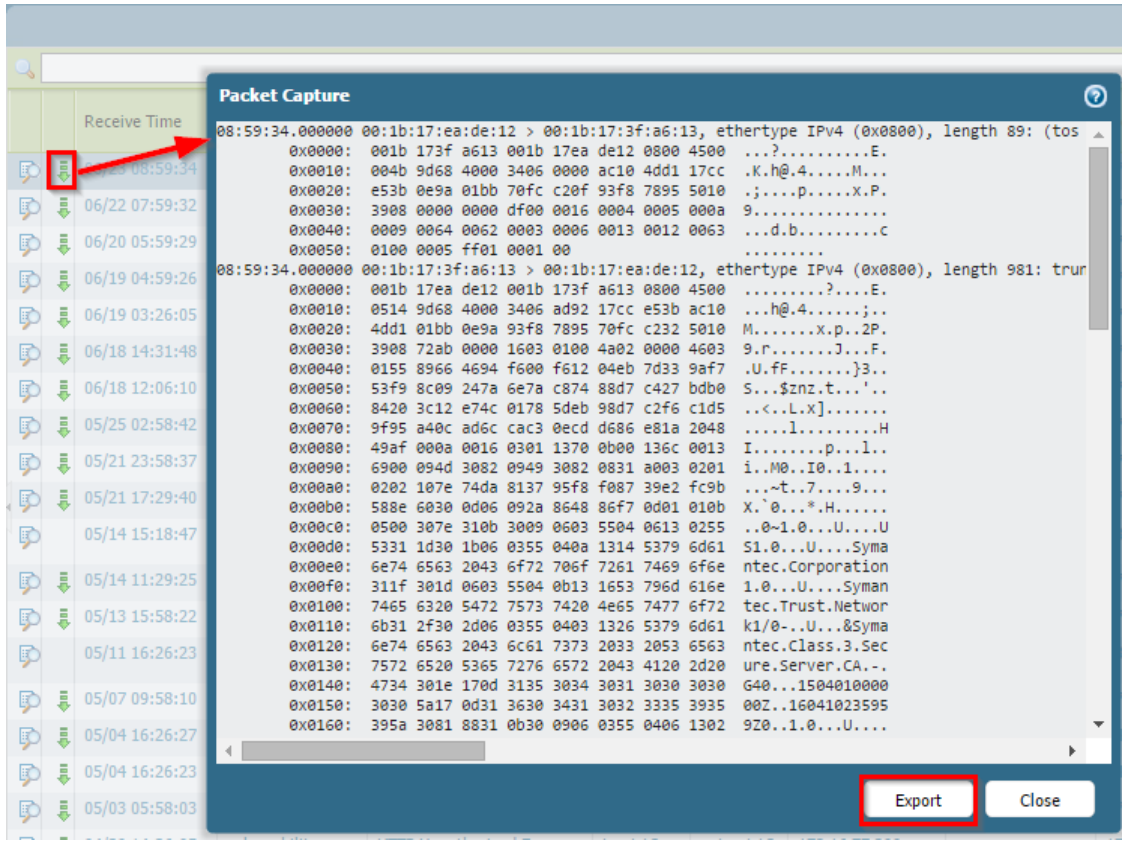
**Device > Setup > Content-ID**



# View Packet Captures

**Monitor > Logs > Threat**



# Unified Log

## Monitor > Logs > Unified

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

# AutoFocus Integrates with Log Files

**Monitor > Logs**

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

AutoFocus

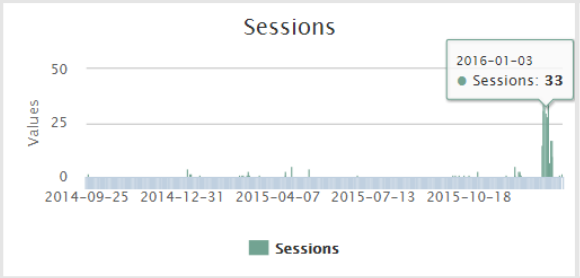
AutoFocus Intelligence Summary - 74.1.2.110 (Read Only)

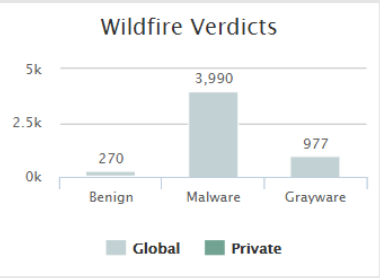
Search Autofocus for 74.1.2.110

Passive DNS

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

Matching Tags



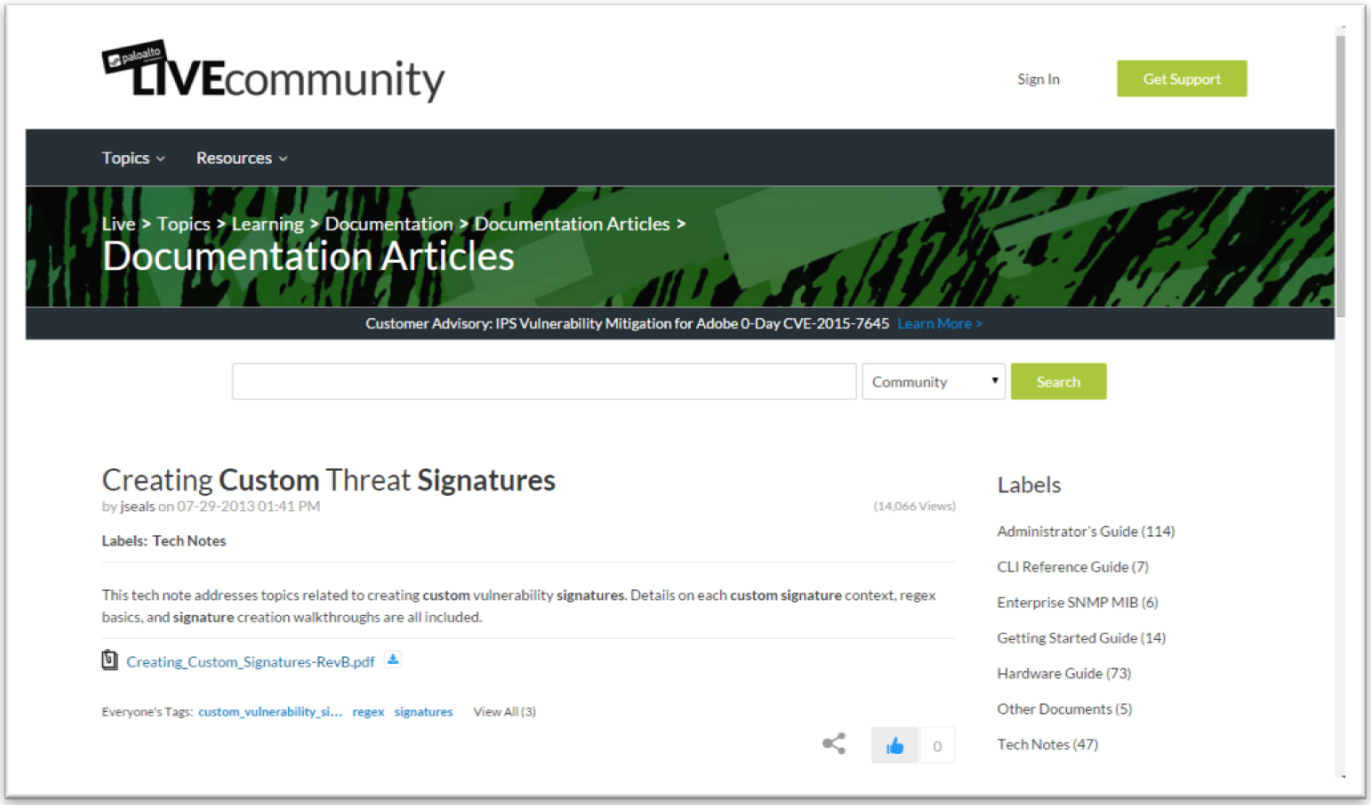

Recent WildFire Results

| SHA256 | File Type | Create Date | Update Date | Verdict |
|---|---|---|---|---|
| fd4efa91eb7d2b3b170973b3403808034bb28e5dca721d7bf308b7173e9fa... | PE | 2015-12-09T11:39:21 | | Grayware |
| cb36f3c8d0eed0e076fbcfab98fd2f0756e67be08fd1cefe8cca1b8c8acb70f8 | PE | 2015-12-07T21:31:23 | | Benign |
| 039859085627f8e59ee728a1d801c3edd4a20c40044de14c175fbf25a5e689... | PE | 2015-12-04T09:34:21 | | Benign |
| 3f74e2e41db7a84577b7ad2b5553684d6295a312891dfb77afab878636477... | PE | 2015-12-04T09:30:45 | | Benign |
| 7ac4d6758648f84837068a785741ccf9f2a282446242add76da73af5d9a8b1... | PE | 2015-12-04T07:24:48 | | Benign |

# Creating Custom Threat Signatures

- Custom Signatures can be added to the Security Profiles



# URL Filtering

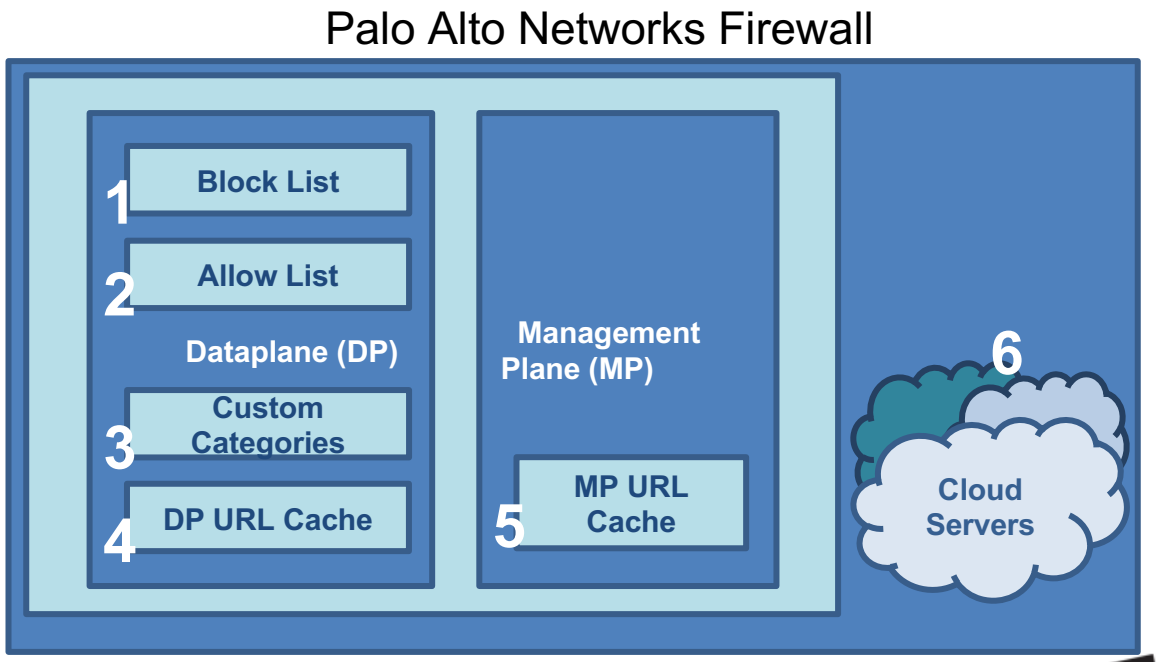
# Threat Intelligence Cloud

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

# Why PAN-DB?

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



# PAN-DB Private Offline Database Server

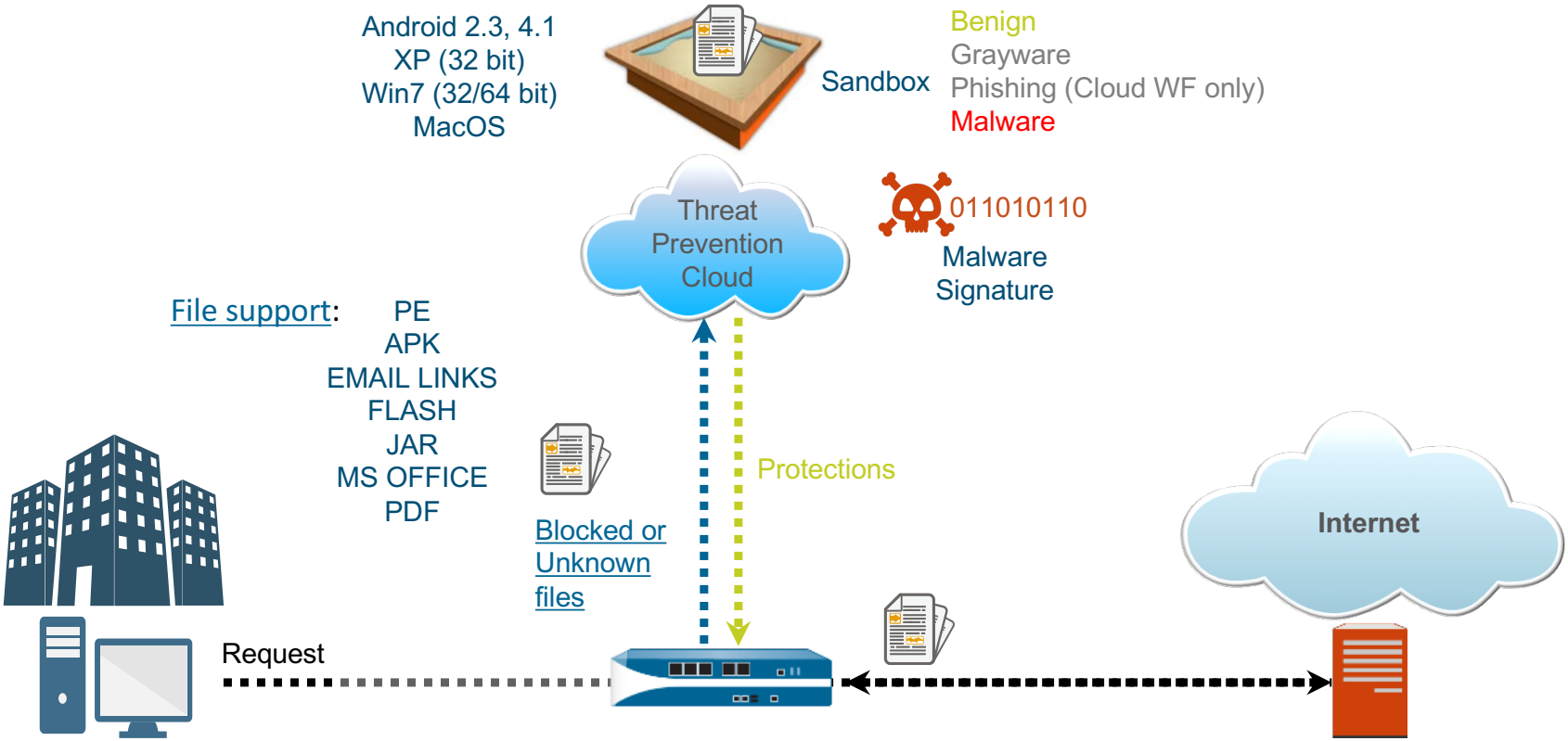
- Conforms to the strictest of security requirements
  - When no outside connectivity is allowed
- Complete privacy
  - Your URL usage is private
  - Not shared or collected as part of a public online metric
- Same functions and capabilities as the online version of PAN-DB
- Supported on the M-500 only.

# Wildfire

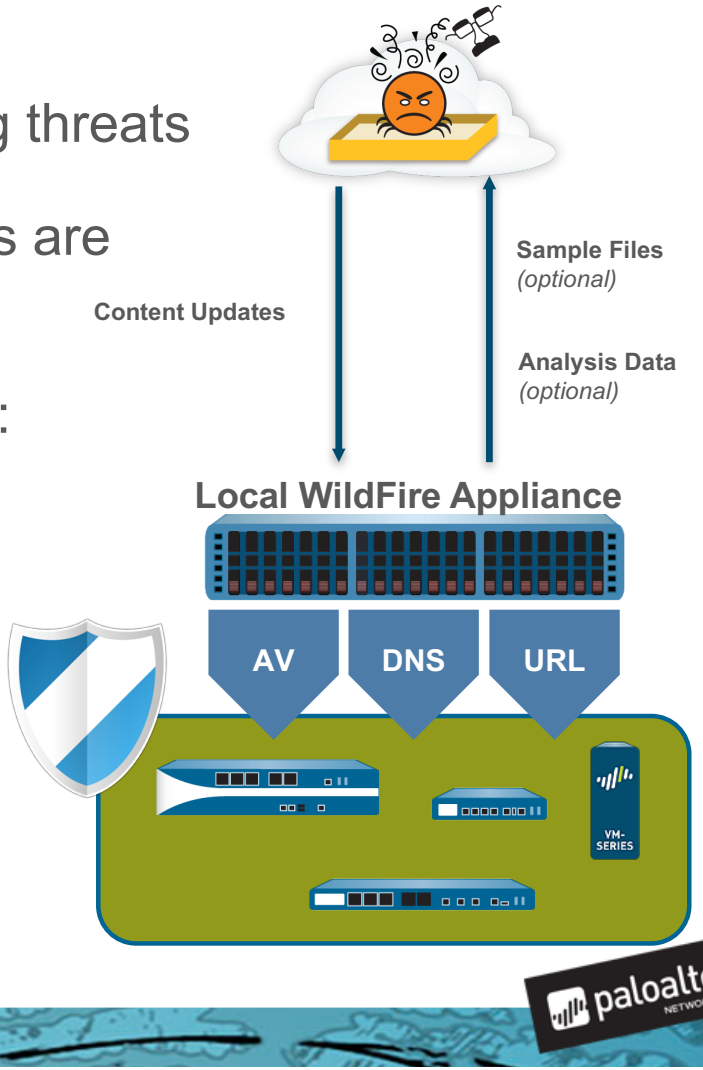
# Wildfire



# Wildfire Retention

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



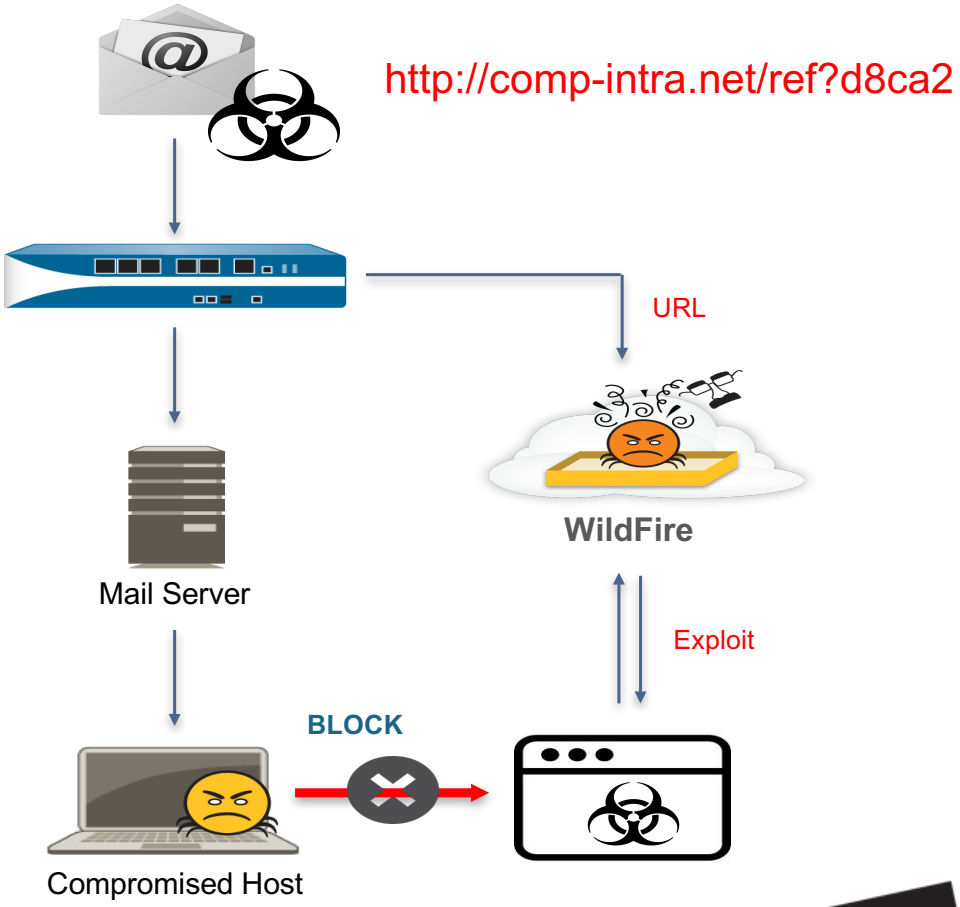
# Wildfire Techniques

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

# Identify and Protect Against Malicious Email Links

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



# WF-500

***Cloud innovation will always be faster***

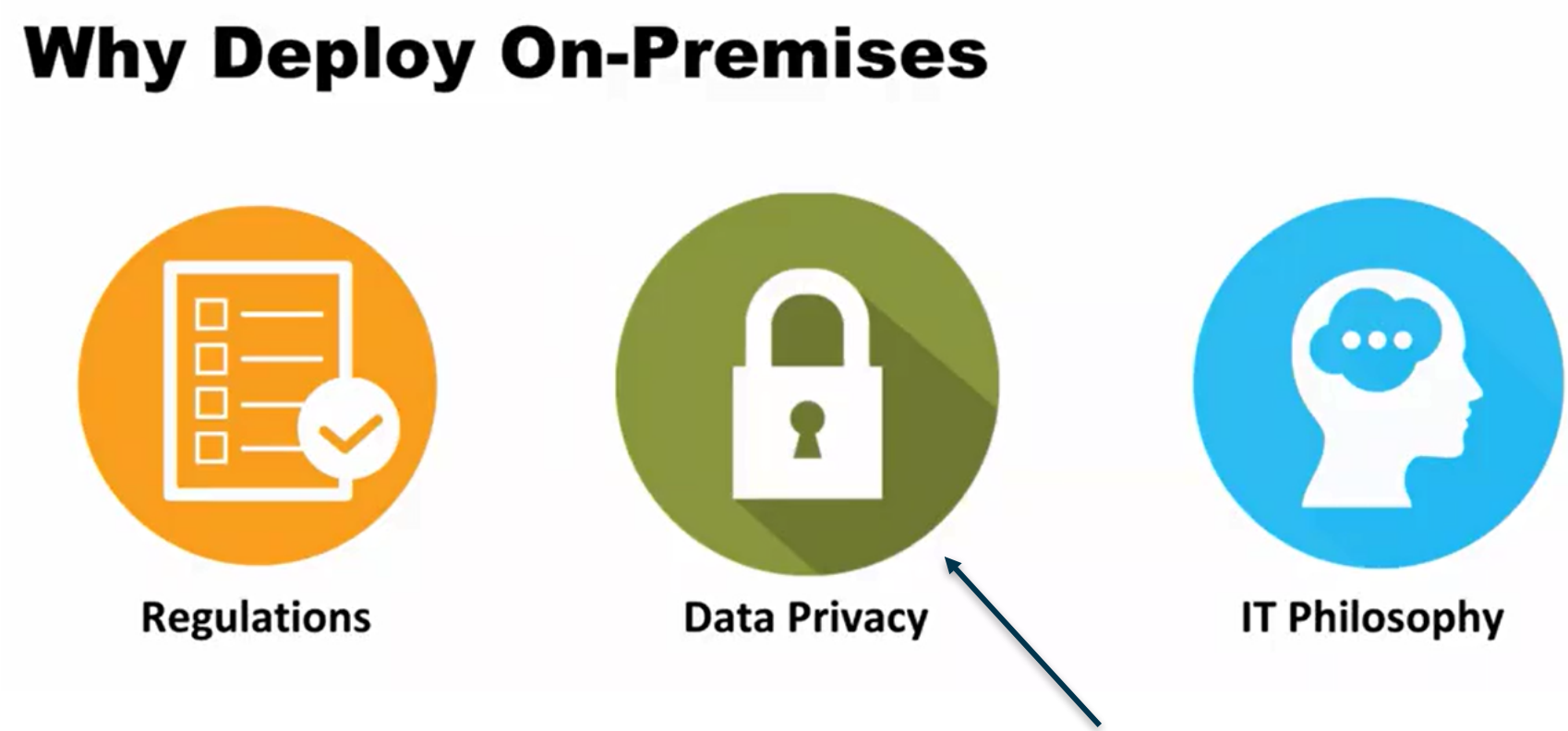

- Custom hypervisor
- Bare Metal analysis
- Support for Mac and APK file analysis

WF-500 appliance

- Local sample analysis

# WF-500



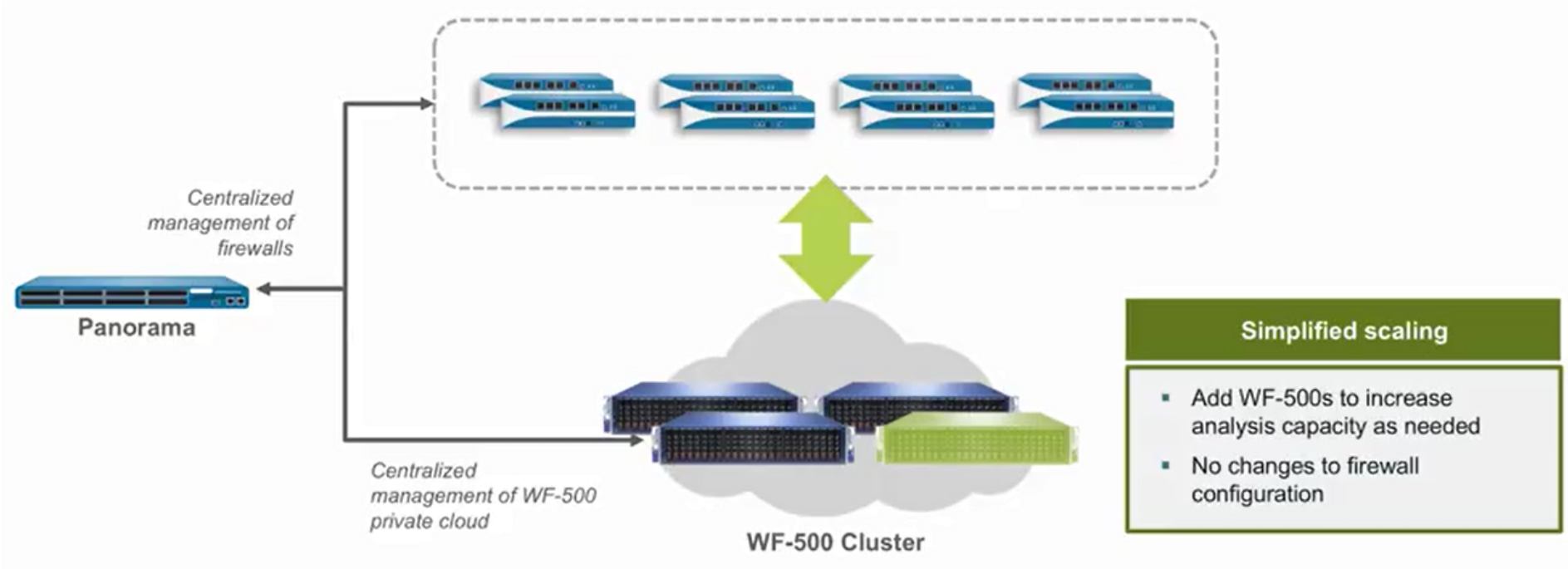

 

# WF-500

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

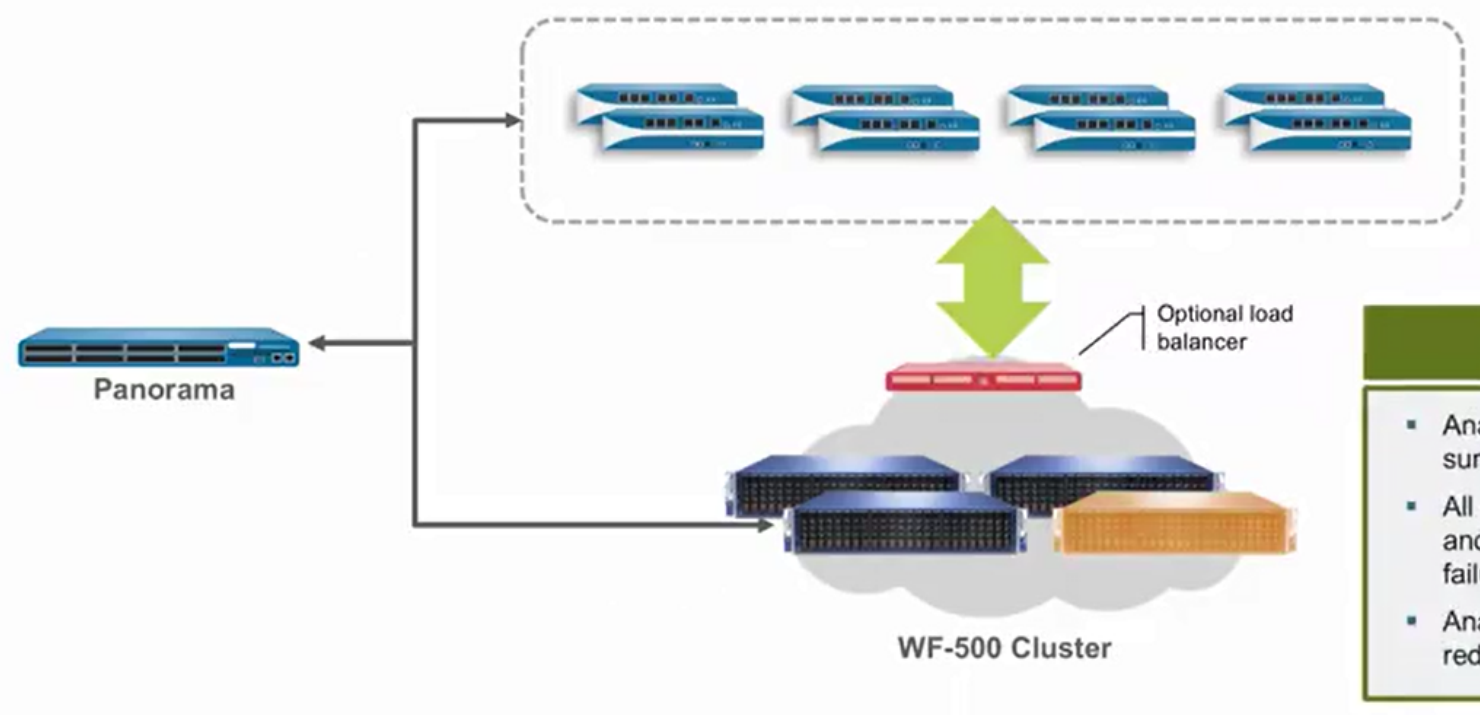
 

# WF-500 > 8.0.1 > Cluster



# WF-500 > 8.0.1 > Cluster




**High availability**

- Analysis capability and data survive appliance failures
- All data is stored redundantly and redistributed in case of failure
- Analysis is load balanced and redistributed in case of failure

# WF-500 > 8.0.1 > Cluster

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

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

# WF-500 > 8.0.1 > Cloud Query

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

# WildFire Licensing

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

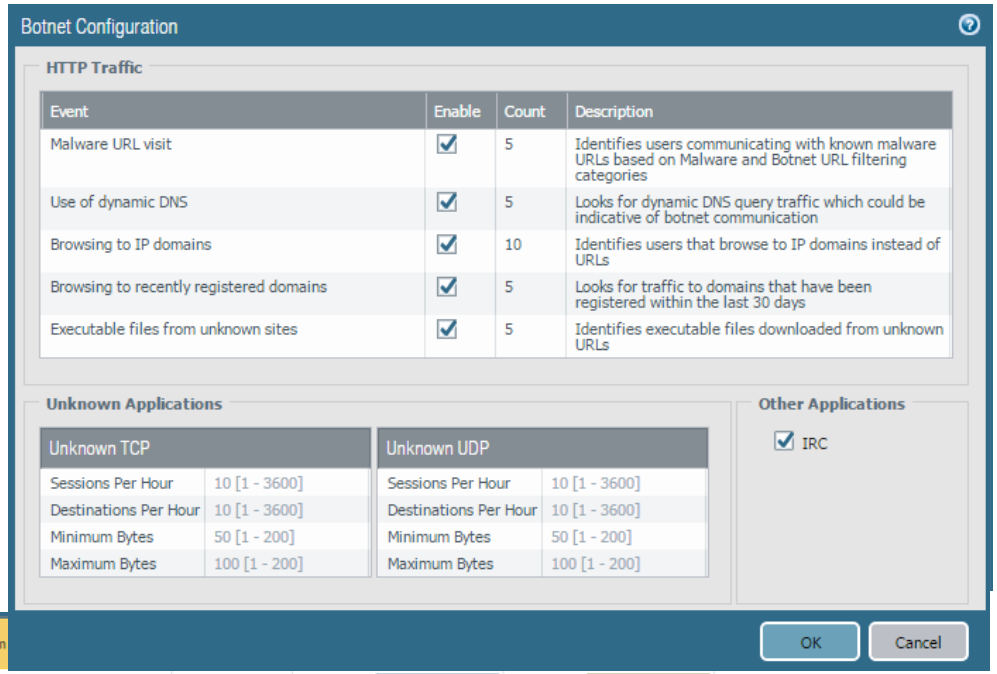
 

# Reports

# Botnet Report

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

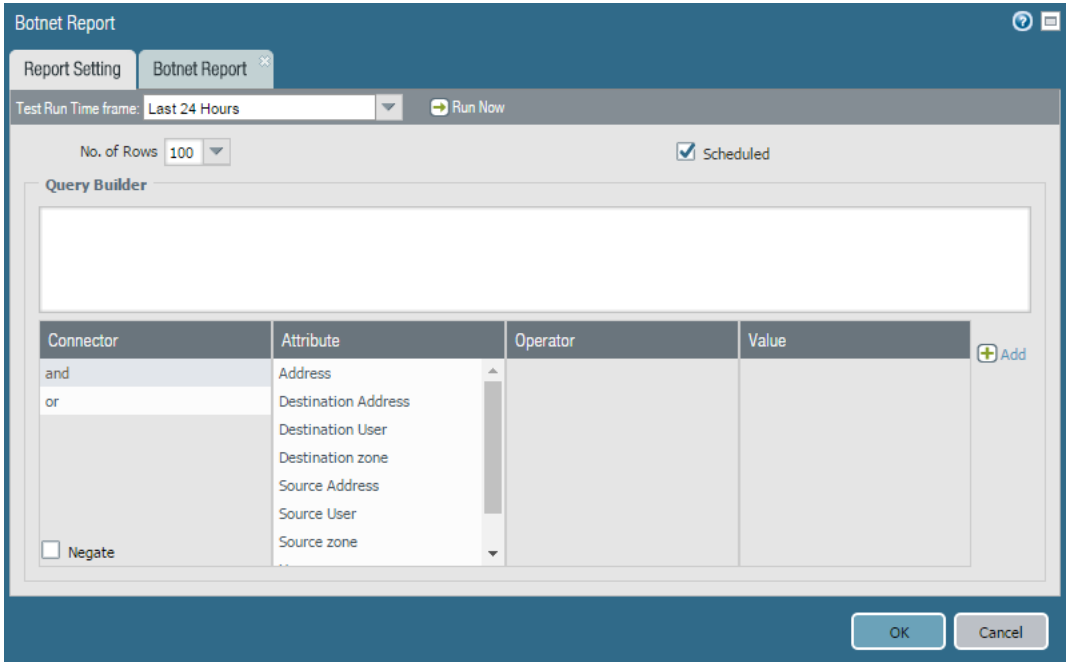



| | Source Address | Source Host Name | Source User | Destination Address | Destination | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | 10.31.33.131 | 10.31.33.131 | | 10.31.33.26 | 10.31.33.26 | | 95.4M | 17.5k |
| 2 | 10.31.33.26 | 10.31.33.26 | | 8.8.8.8 | google-public-dns-a.google.com | | 1.7M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

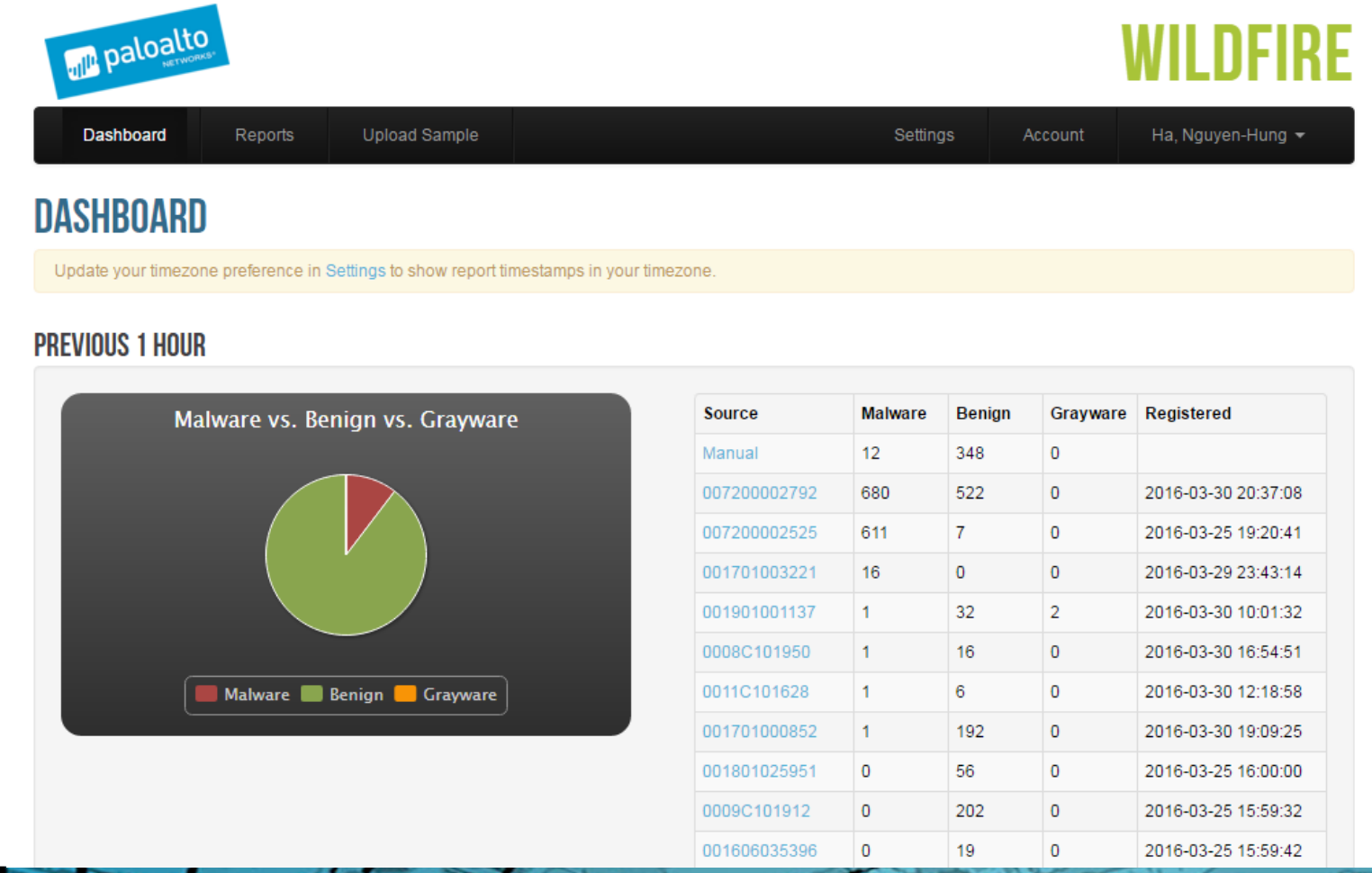
# Schedule Botnet Report

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



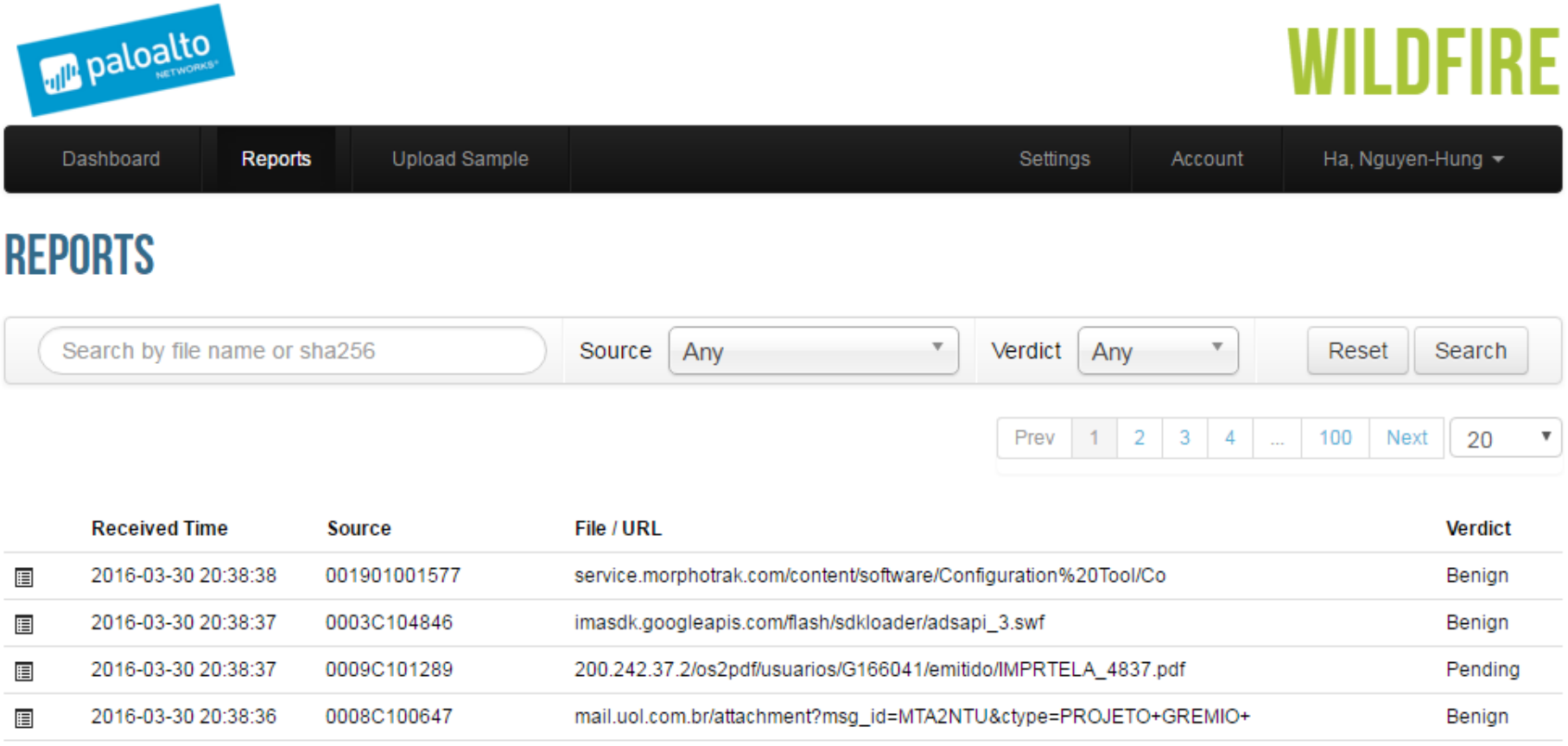

 

# WildFire Dashboard




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

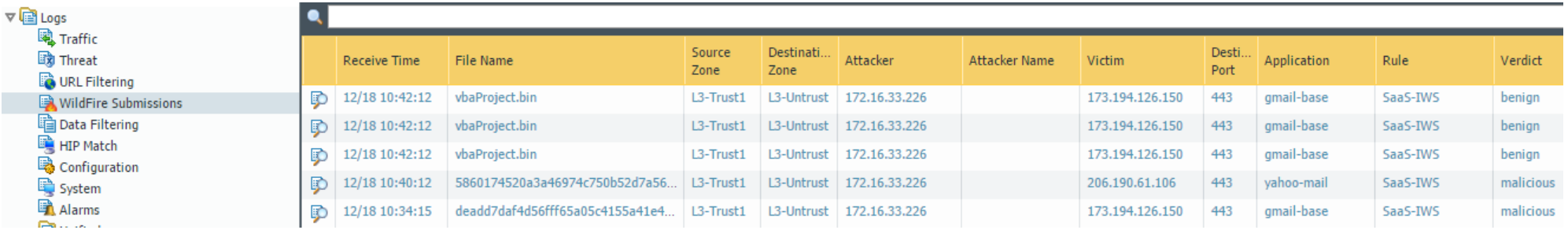
# WildFire Reports



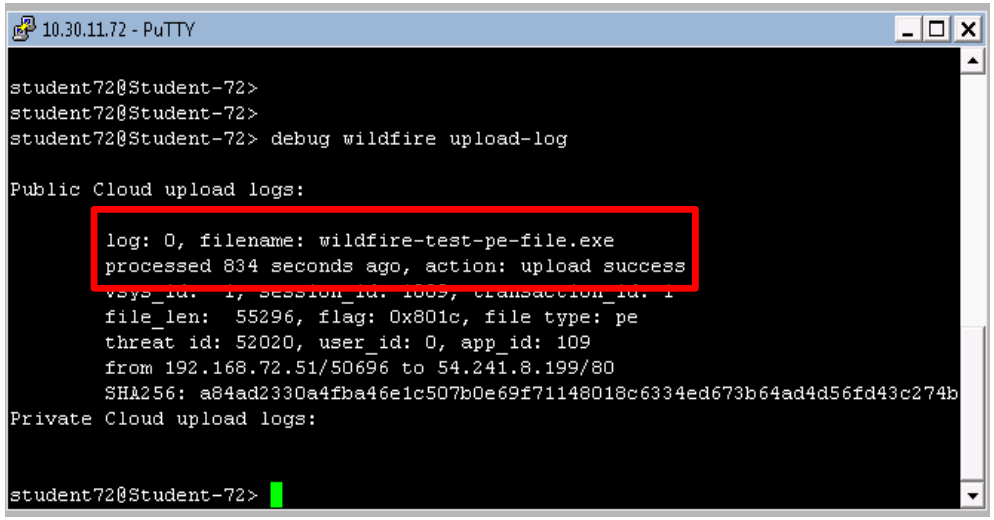
# WildFire Submissions Log

**Monitor > Logs > WildFire Submissions**




| Receive Time | File Name | Source Zone | Destinati... Zone | Attacker | Attacker Name | Victim | Desti... Port | Application | Rule | Verdict |
|---|---|---|---|---|---|---|---|---|---|---|
| 12/18 10:42:12 | vbaProject.bin | L3-Trust1 | L3-Untrust | 172.16.33.226 | | 173.194.126.150 | 443 | gmail-base | SaaS-IWS | benign |
| 12/18 10:42:12 | vbaProject.bin | L3-Trust1 | L3-Untrust | 172.16.33.226 | | 173.194.126.150 | 443 | gmail-base | SaaS-IWS | benign |
| 12/18 10:42:12 | vbaProject.bin | L3-Trust1 | L3-Untrust | 172.16.33.226 | | 173.194.126.150 | 443 | gmail-base | SaaS-IWS | benign |
| 12/18 10:40:12 | 5860174520a3a46974c750b52d7a56... | L3-Trust1 | L3-Untrust | 172.16.33.226 | | 206.190.61.106 | 443 | yahoo-mail | SaaS-IWS | malicious |
| 12/18 10:34:15 | deadd7daf4d56fff65a05c4155a41e4... | L3-Trust1 | L3-Untrust | 172.16.33.226 | | 173.194.126.150 | 443 | gmail-base | SaaS-IWS | malicious |

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



# Correlation Report

# Correlation Objects

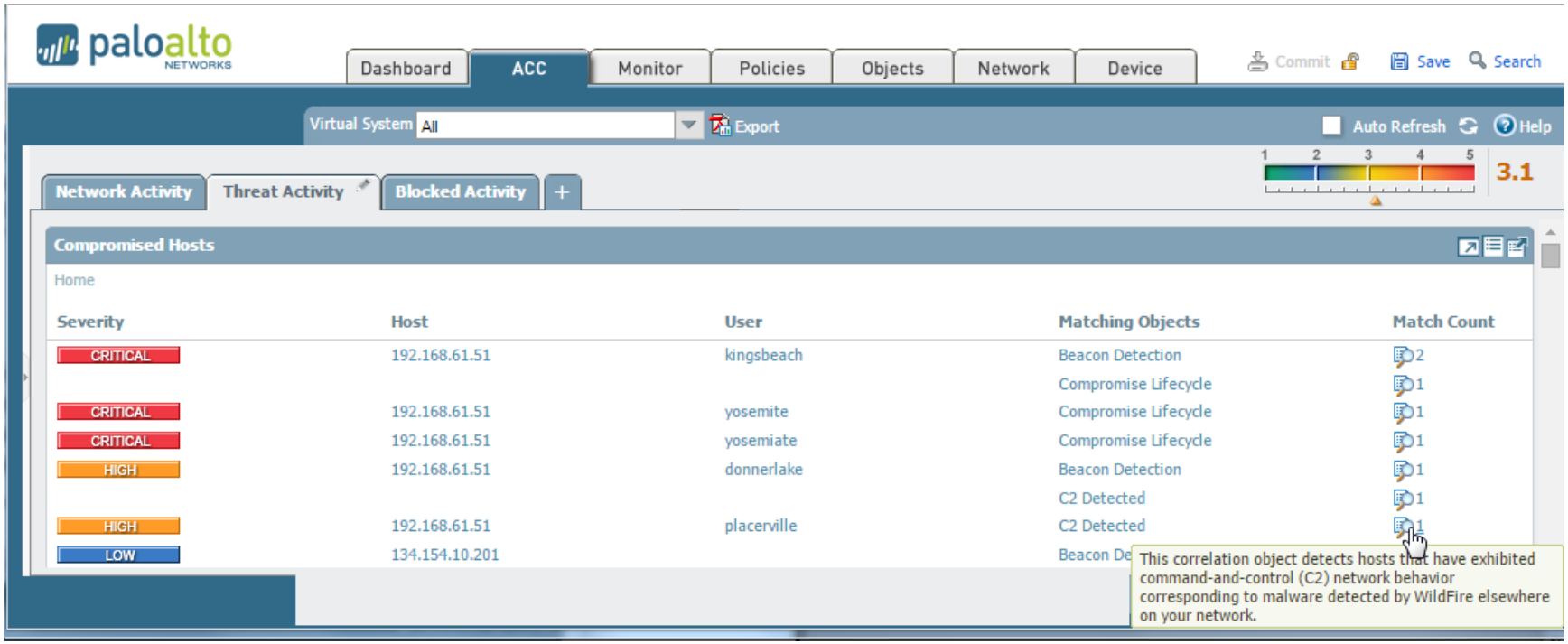
| Title | Category | State | Description |
|---|---|---|---|
| Compromise Activity Sequence | compromised-host | active | This correlation object detects a host involved in a sequence of activity indicating remote compromise, starting with scanning or probing activity, progressing to exploitation, and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

- Correlation Events are logged when traffic matches a correlation object

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

# ACC Correlation Events



# What the Correlation Engine is NOT

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

# Configuration Best Practices

- A poorly configured firewall is vulnerable.
- A firewall left with Default Configs is vulnerable.

- Refer to the following document for Configurational Best Practices designed to address L4 and L7 Evasions:

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