# PAN-0S - v8.0 and v8.1

The configuration snippet descriptions and the associated GitHub repository link for each xml snippet.

> **Instructions for Loading Templates**
> This document provides details about what's in each template element but does not provide application support or instruction for loading and using the templates. The Iron-Skillet GitHub repository wiki for this project does contain a short list of methods for loading templates in Panorama or a PAN-OS device.

> **For Non-Panorama Device Only**
> This document and associated config links, xpaths references, and load order are specific to non-Panorama device configuration. A companion document is used to cover the Panorama PANOS configuration

---



---

## GENERAL DEVICE CONFIGURATION

This section provides templated configurations for general device settings.

### Security-related Device Settings

device_setting.xml

General device settings that effect security posture. Found in Device > Setup in the GUI.

- X-Forwarded-For: To ensure that attackers can’t read and exploit the XFF values in web request packets that exit the firewall.Wildfire: set optimal file size limits for Wildfire uploads and show verdict responses for grayware, malware and phishing
  - Enable the firewall to use XFF values in policies and in the source user fields of logs
  - Remove XFF values from outgoing web requests.

- Session rematch: the firewall will go through all the existing sessions and apply the new security policy to any matching traffic
- Notify User: user should be notified when web-application is blocked; enables the application response page
- Log Suppression: disabled to ensure unique log entries even if similar session types

### System Configuration

device_system.xml

System configuration settings for dynamic updates and network services (eg. DNS, NTP).

- Update schedule settings: Turn on all telemetry settings; recommended dynamic updates schedule for threats, AV, and Wildfire
- Use SNMPv3
- Set default DNS and NTP values
- Set timezone to UTC

## LOGGING

Logging best practice configurations for logging output and forwarding profiles.

**Configure Logging profiles before Security Rules**
The template creates a log forwarding profile call default. This profile is referenced in the template security rules and should be configured before the security rules.

**Logging can be Deployment Dependent**
The destination in the logging profile is templated to a syslog server. This can vary based on actual deployment scenarios.

log_settings_profiles.xml

Log forward profile referenced in security rules to determine where to forward log related events.

- Forward all log activity to syslog (see the reference syslog configuration in shared_log_settings.xml)
- Email malicious and phishing Wildfire verdicts to the address in the email profile  (see shared_log_settings.xml)

shared_log_settings.xml

Device event logging including sample profiles for email and syslog forwarding.

- Reference syslog profile that can be edited for a specific IP address and UDP/TCP port
- Reference email profile that can be edited for specific email domain and user information
- System, configuration, user, HIP, and correlation log forwarding to syslog
- Email critical system events to the email profile

**Email Alerts - When to Use**
The purpose of select email alert forwarding is ensure not to under alert or over alert yet provide critical messages for key events. Under alerting reduces visibility to key events while over alerting creates too much noise in the system.

## REFERENCED OBJECTS

Address, External Dynamic List (EDL), and tag objects that are referenced in security rules by name.

### Address Object

address.xml

Address object used to reference named addresses.

- Sinkhole-IPv4: IP address used in security rule to block sinkhole traffic
- Sinkhole-IPv6: IP address used in security rule to block sinkhole traffic

### External Dynamic Lists

external_list.xml

Used for the firewall to pull in external elements such as IP, URL, or domain used in security rules

- Team Cymru Bogon Lists - IPv4 and IPv6 bogon IPs that should not be forwarded

**Remove Private Bogons**
Any private or other Bogon address that must be routed across the device must be added as exceptions in the external dynamic list object. These should be direction dependent and used in the respective outbound or inbound security rule.

### Tags

tag.xml

Tags used in security rules and related objects.

- Inbound - inbound (untrust to trust) elements
- Outbound - outbound (trust to untrust) elements
- Internal - internal (trust) segmentation elements

## SECURITY PROFILES AND GROUPS

The key elements for security posture are security profiles and the security rules. The templates ensure best practice profiles and profile groups are available and can be referenced in any security rules. The template security rules focus on 'top of the list' block rules to reduce the attack surface.

**Profiles and Subscriptions**
All of the template security profiles other than file blocking require Threat Prevention, URL Filtering, and Wildfire subscriptions. Ensure that the device is properly licensed before applying these configurations.

### Custom URL Category

profiles_custom_url_category.xml

Placeholder for custom url categories used in security rules and url profiles. Using these categories prevents the need to modify the default template.

- Black-List: placeholder to be used in block rules and objects to override default template behavior
- White-List: placeholder to be used in permit rules and objects to override default template behavior
- Custom-No-Decrypt: to be used in the decryption no-decrypt rule to specify URLs that should not be decrypted

### File Blocking

profiles_file_blocking.xml

Security profile for actions specific to file blocking (FB).

**File Blocking File Types**
The Block file type recommendation is based on common malicious file types with minimal impact in a Day 1 deployment. Although PE is considered the highest risk file type it is also used for legitimate purposes so blocking PE files will be deployment specific and not included in the template.

- Day 1 Block file types: 7z, bat, chm, class, cpl, dll, hlp, hta, jar, ocx, pif, scr, torrent, vbe, wsf
- The profiles will alert on all other file types for logging purposes

Profiles:

- Outbound-FB: For outbound (trust to untrust) security rules
- Inbound-FB: For inbound (untrust to trust) security rules
- Internal-FB: For internal network segmentation rules
- Alert-Only-FB: No file blocking, only alerts for logging purposes
- Exception-FB: For exception requirements in security rules to avoid modifying the default template profiles

## Anti-Spyware

profiles_spyware.xml

Security profile for actions specific to anti-spyware (AS).

**Sinkhole Addresses**
The profiles use IPv4 and IPv6 addresses for DNS sinkholes. IPv4 is currently provided by Palo Alto Networks. IPv6 is a bogon address.

Profiles:

- **Outbound-AS**: For outbound (trust to untrust) security rules
  - Block severity = Critical, High, Medium
  - Default severity = Low, Informational
  - DNS Sinkhole for IPv4 and IPv6
  - Single packet capture for Critical, High, Medium severity
- **Inbound-AS**: For inbound (untrust to trust) security rules
  - Block severity = Critical, High, Medium
  - Default severity = Low, Informational
  - DNS Sinkhole for IPv4 and IPv6
  - Single packet capture for Critical, High, Medium severity
- **Internal-AS**: For internal network segmentation rules
  - Block severity = Critical, High
  - Default severity = Medium, Low, Informational
  - DNS Sinkhole for IPv4 and IPv6
  - Single packet capture for Critical, High, Medium severity
- **Alert-Only-AS**: No blocking, only alerts for logging purposes
  - Alert all severities and DNS sinkhole
  - No packet capture
- **Exception-AS**: For exception requirements in security rules to avoid modifying the default template profiles

## URL Filtering

profiles_url_filtering.xml

Security profile for actions specific to URL filtering (URL).

**Only Block Categories will be shown**
All URL categories will be set to Alert at a minimum for logging purposes. The profile descriptions will include the Block categories in the description.

Profiles:

- **Outbound-URL**: For outbound (trust to untrust) security rules
  - URL Categories
  - Site Access: Block command-and-control, malware, phishing, hacking, Black List (custom URL category)
  - User Credential Submission: Block all categories
  - Alert category = includes White List (custom URL category)
  - URL Filtering Settings: HTTP Header Logging (user agent, referer, X-Forwarded-For)

**Alert-Only-URL**: No  blocking, only alerts for logging purposes
- Alert all categories including custom categories Black List and White List

**Exception-URL**: For exception requirements in security rules to avoid modifying the default template profiles
- URL Categories
- Site Access: Block command-and-control, malware, phishing, hacking, Black List (custom URL category)
- User Credential Submission: Block all categories
- Alert category = includes White List (custom URL category)
- URL Filtering Settings: HTTP Header Logging (user agent, referer, X-Forwarded-For)

### Anti-Virus

profiles_virus.xml

Security profile for actions specific to AntiVirus (AV).

Profiles:

- Outbound-AV: For outbound (trust to untrust) security rules
- Inbound-AV: For inbound (untrust to trust) security rules
- Internal-AV: For internal network segmentation rules
- Alert-Only-AV: No blocking, only alerts for logging purposes
- Exception-AV: For exception requirements in security rules to avoid modifying the default template profiles

**Email Response Codes with SMTP not IMAP or POP3**
Reset-both is used for SMTP, IMAP, and POP3. SMTP '541' response messages are returned to notify that the session was blocked. IMAP and POP3 do not have the same response model. In live deployments, instead of DoS concerns with retries, the endpoints typically stop resending after a small number of sends with timeouts.

## Vulnerability Protection

profiles_vulnerability.xml

Profiles:

- **Outbound-VP**: For outbound (trust to untrust) security rules
  - Block severity = Critical, High, Medium
  - Alert severity = Low, Informational
  - Single packet capture for Critical, High, Medium severity
- **Inbound-VP**: For inbound (untrust to trust) security rules
  - Block severity = Critical, High, Medium
  - Alert severity = Low, Informational
  - Single packet capture for Critical, High, Medium severity
- **Internal-VP**: For internal network segmentation rules
  - Block severity = Critical, High
  - Alert severity = Medium, Low, Informational
  - Single packet capture for Critical, High, Medium severity
- **Alert-Only-VP**: No blocking, only alerts for logging purposes
  - Alert all severities
  - No packet capture
- **Exception-VP:** For exception requirements in security rules to avoid modifying the default template profiles

### Wildfire Analysis

profiles_wildfire_analysis.xml

Security profile for actions specific to Wildfire upload and analysis (WF).

**Public Cloud is the default**
All template profiles are configured to upload all file types in any direction to the public cloud for analysis.

Profiles:

- Outbound-WF: For outbound (trust to untrust) security rules

- Inbound-WF: For inbound (untrust to trust) security rules
- Internal-WF: For internal network segmentation rules
- Alert-Only-WF: No blocking, only alerts for logging purposes
- Exception-WF: For exception requirements in security rules to avoid modifying the default template profiles

### Security Profile Groups

profile_group.xml

Security profile groups based on use case

- Inbound: For rules associated to inbound (untrust to trust) sessions
- Outbound: For rules associated to outbound (trust to untrust) sessions
- Internal: For rules associated to trust-domain network segmentation
- Alert Only: Provides visibility and logging without a blocking posture

## SECURITY RULES

### Recommended Block Rules

rulebase_security.xml

Recommended block rules for optimal security posture with associated default log-forwarding profile

- Outbound Block Rule: Block destination IP address match based on the Palo Alto Networks predefined externals dynamic lists
- Inbound Block Rule: Block source IP address match based on the Palo Alto Networks predefined externals dynamic lists
- DNS Sinkhole Block: Block sessions redirected to defined sinkhole addresses using the address objects (address.xml)
- Inbound/Outbound Bogon Block Rules: Prevent bogon addresses from being forwarded; uses Team Cymru Bogon EDL

**Check Bogons before enabling the Bogon block rule**
The bogon rules are disabled in the template and should only be activated once determined that all bogons should be blocked. Exceptions may be private address space that may be allowed to cross device boundaries.

**Security Rules in the template are block only**
The template only uses block rules. Allow rules are zone, direction and use case dependent. Additional templating work will provide recommended use case case security rules.

### Default Security Rules

rulebase_default_security_rules.xml

Configuration for the default interzone and intrazone default rules

- Intrazone: Enable logging at session-end using the default logging profile; Use the Internal security profile-group
- Interzone: Enable logging at session-end using the default logging profile

## DECRYPTION

### Profiles

profiles_decryption.xml

Recommended_Decryption_Profile. Referenced by the default decryption rule.

- SSL Forward Proxy
  - **Server Cert Verification**: Block sessions with expired certs, Block sessions with untrusted issuers, Block sessions with unknown cert status
  - **Unsupported Mode Checks**: Block sessions with unsupported versions, Blocks sessions with

unsupported cipher suites

- SSL No Proxy
  - **Server Cert Verification**: Block sessions with expired certs, Block sessions with untrusted issuers

- SSH Proxy
  - **Unsupported Mode Checks**: Block sessions with unsupported versions, Block sessions with unsupported algorithms

- SSL Protocol Settings:
  - Minimum Version: TLSv1.2; Any TLSv1.1 errors can help find outdated TLS endpoints
  - Key Exchange Algorithms: RSA not recommended and unchecked
  - Encryption Algorithms: 3DES and RC4 not recommended and unavailable when TLSv1.2 is the min version
  - Authentication Algorithms:MD5 not recommended and unavailable when TLSv1.2 is the min version

### Decryption Rules

rulebase_decryption.xml

Recommended SSL decryption pre-rules for no-decryption.

- NO decrypt rule for select URL categories; Initially disabled in the Day 1 template until SSL decryption to be enabled
- NO decrypt rule used to validate SSL communications based on the Recommended Decrypt profile

## ZONE PROTECTION

### Profile

zone_protection_profile.xml

Recommended_Zone_Protection profile for standard, non-volumetric best practices. This profile should be attached to all interfaces within the network.

Recon Protection: Default values enabled in alert-only mode; active blocking posture requires network tuning

Packet Based Attack Protection

- IP Drop: Spoofed IP Address, Malformed
- TCP Drop: Remove TCP timestamp, No TCP Fast Open, Multipath TCP (MPTCP) Options = Global

## REPORTS

### Reports

reports_simple.xml

Series of reports to look for traffic anomalies, where to apply or remove rules, etc. Reports are grouped by topic per the report group section below.

**Zones and Subnets in Report Queries**
The repo contains a separate folder for custom reports that use a placeholder zone called 'internet' for match conditions in reports. This value MUST be changed to match the actual public zone used in a live network. Additional zones and/or subnets to be used or excluded in the reports would be added in the query values.

### Report Groups

report_group_simple.xml

Report groups allow you to create sets of reports that the system can compile and send as a single aggregate PDF report with an optional title page and all the constituent reports included.

Template report groups include:

**Simple (included in Day One template)**

- Possible Compromise: malicious sites and verdicts, sinkhole sessions

**Custom**

- User Group Activity (eg. Employee, Student, Teacher): user-id centric reports grouped by user type
- Inbound/Outbound/Internal Rule Tuning: Used rules, app ports, unknown apps, geo information
- Inbound/Outbound/Internal Threat Tuning: Allowed threats traversing the device
- File Blocking Tuning: View of upload/download files and types with associated rule
- URL Tuning: Views by categories, especially questionable and unknown categories
- Inbound/Outbound/Internal Threats Blocked: Threat reports specific to blocking posture; complement to threat tuning
- Non-Working Traffic: View of dropped, incomplete, or insufficient data sessions

## Email Scheduler

email_scheduler_simple.xml

Schedule and email recipients for each report group. The template uses a sample email profile configured in shared_log_settings.