iron-skillet Documentation

Release 1.0

Palo Alto Networks

May 23, 2019

Contents:

CHAPTER 1

Iron Skillet Overview

Welcome to the Iron Skillet day one configuration templates library.

The next-generation firewall configuration templates are based on existing best practice recommendations from Palo Alto Networks.

Instead of extensive and detailed 'how to' documentation, the templates provide an easy to implement configuration model that is use case agnostic. The emphasis is on key security elements such as dynamic updates, security profiles, rules, and logging that should be consistent across deployments.

1.1 Why use day one templates?

Palo Alto Networks has expertise in both security prevention and its own product portfolio. Best practice documentation is designed to provide knowledge sharing of this expertise to customers and partners. This sharing helps improve security posture across various scenarios.

The templates play a complementary role by taking common best practices recommendations and compiling them into pre-built day one configurations that can be readily loaded into Panorama or a next-generation firewall. The benefits include:

- Faster time to implement
- Reduce configuration errors
- Improve security posture

1.2 Using the templates

The templates are available on GitHub at https://github.com/PaloAltoNetworks/iron-skillet/tree/panos_v8.0.

Select the branch specific to the software release for your deployment.

The library consists of a set of xml and set configuration templates grouped by:

- `panos` for stand-alone next-gen firewall deployments
- `panorama` for Panorama system and managed device configurations

The templates in each device-type folder include:

- `snippets` for more granular configuration elements
- `full config file` to use for bootstrap or full import + load into a device
- `set commands` for traditional CLI configuration

1.2.1 Quick start using loadable configurations

The repo contains a set of ready-to-go loadable configurations that use iron-skillet placeholder values. Formats include both xml and set commands.

The xml file can be imported and loaded easily to Panorama or a firewall. The set command model requires 'copy-and-paste' from the CLI.

More information for loading and editing these configurations can be found at: *Default Loadable Configurations*.

1.2.2 Excel set command spreadsheet

Also included for easy loading is an Excel formula-based spreadsheet with set commands. A variable value worksheet can be edited to update the spreadsheet using localized values for various configuratino attributes.

More information for using the spreadsheet can be found at: *Formula-based Excel Spreadsheet*.

1.2.3 Jinja-based xml snippet and set command templates

Scripting or automation-centric users may prefer to use the base template files. These are variable-based templates using a jinja `{{ variable }}` notation.

The xml snippets with metadata are designed to use API-based configuration loading into Panorama or the firewall and can be coupled with workflow tools for repeatable deployments.

Sample utilities are provided in the `tools` directory to create loadable configurations using these base templates.

See the sections *Creating Loadable Configurations* and *Loading the XML templates* for more information.

Note: Day one templates are not complete configuration templates. To insert the device into the network requires interface, zone, routing, and other settings outside the scope of the day one templates. Also not included are use-case specific items such as whitelist security rules, userID settings, and decryption policies that can be deployment and use case specific.

1.3 What is next after loading a template?

Based on the deployment scenario, the next steps may include:

- GUI configuration of additional configuration elements specific to the deployment use case
- API/scripted loading of additional configuration elements

In cases where the use case configuration has been merged with the templates, no further actions may be required. A key example would be interface, NAT, zone, and security rule additions for a simple Internet gateway deployments.

1.4 Where can I find complete reference use case configurations?

The initial release of the templates are use case agnostic. However, as the community creates and shared reference configurations, they will be shared across the community as an extension of the iron-skillet configurations.

CHAPTER 2

Requirements and Caveats

Please read before using the IronSkillet configuration templates.

2.1 Requirements

Using IronSkillet requires the following to properly load into Panorama and/or the NGFW

- **Running software version 8.0**
  - Upgrade the firewall to 8.0
  - Upgrade Panorama to 8.0
- **Active subscription for Threat Prevention**
  - Activate the subscription licenses
- **Updated application and antivirus content**
  - Install content and software updates

Note: Threat Prevention and the antivirus content update are both required to gain access to the Palo Alto Networks provided External Dynamic Lists (EDLs) used in the security policies.

Note: URL Filtering, DNS Cloud Service, and Wildfire subscriptions are not required to load the configuration but are highly recommended as part of the best practice to utilize IronSkillet elements such as the URL Filtering, Spyware, and Wildifre security profiles and associated profile groups

2.2 Caveats

Please review the following to understand any limitations or recommendations regarding the IronSkillet templates

- Be sure to edit or the default administrative superuser account if not part of initial configuration
  - If the default account information is used, the user is notified at login
  - To change or add superuser accounts see Configure a Firewall Administrator
- The current version only supports IPv4 management interface configuration
- **IronSkillet loaded into a VM-50 will utilize the full profile capacity**
  - See the section vm50_profile_reduction for more information
- **The Panorama full configuration template is based on a fully shared model**
  - All device-group configuration at the Shared top of tree
  - Additional Panorama template stacks should include the IronSkillet template

CHAPTER 3

PAN-OS templates

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

Note: The template version is found in the template xml file as a tag attribute

Note: The set commands utilize the same configuration settings

3.1 General Device Configuration

This section provides templated configurations for general device settings.

3.1.1 Security-related Device Settings

view xml template: device_setting

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

- Wildfire: set optimal file size limits for Wildfire uploads and show verdict responses for grayware, malware and phishing
- X-Forwarded-For: To ensure that attackers can't read and exploit the XFF values in web request packets that exit the firewall.
  - 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
- Prevent TCP and UDP buffer overflow and multi-part HTTP download evasions
  - Disable 'allow HTTP header range'
  - Disable 'tcp-bypass-exceed-queue'
  - Disable 'udp-bypass-exceed-queue'
- Enable high DP load logging
- Prevent App-ID buffer overflow evasion
  - set bypass-exceed-queue to 'no'
- Prevent TCP and MPTCP evasions
  - set urgent data to 'clear'
  - set drop zero flag to 'yes'
  - set bypass-exceed-oo-queue to 'no'
  - set check-timestamp-option to 'yes'
  - set strip-mptcp-option to yes
- set export of csv log file to maximum of 1,048,576

3.1.2 System Configuration

view xml template: device_system

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

- Update schedule settings
  - Turn on all telemetry settings
  - Check every 30 minutes for new threat signatures
  - Hourly checks for new AV signatures
  - Check every minute for new Wildfire signatures
  - Recommended time delays and thresholds for checks and installs
- Use SNMPv3
- Set default DNS and NTP values
- Set timezone to UTC
- Provide a standard login banner warning for unauthorized users

---

Note: The management config types include static, dhcp-client, or dhcp-cloud as a special case of dhcp-client. This is specific to each deployment and can be selected as part of the tools to build `my_config`. Since management interface is in the template config, this option must be included for deployment.

3.2 Logging

Logging best practice configurations for logging output and forwarding profiles.

Warning: 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.

Note: Logging can be deployment dependent The destination in the logging profile is templated to an unroutable syslog server address. This can vary based on actual deployment scenarios.

3.2.1 Log forwarding profile

view xml template: log_settings_profiles

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)

3.2.2 Device log settings

view xml template: shared_log_settings

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

Note: When to use email alerts 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. The templates are set with a median view to capture key events without too much 'log fatigue' noise

3.3 Referenced Objects

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

3.3.1 Address Object

view xml template: address

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

3.3.2 External Dynamic Lists

view xml template: external_list

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

Warning: 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.

3.3.3 Tags

view xml template: tag

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

3.4 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.

Warning: 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.

3.4.1 Custom URL Category

view xml template: profiles_custom_url_category

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

3.4.2 File Blocking

view xml template: profiles_file_blocking

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

Note: File blocking and 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

3.4.3 Anti-Spyware

view xml template: profiles_spyware

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

Note: 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

3.4.4 URL Filtering

view xml template: profiles_url_filtering

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

Note: Only `BLOCK` categories will be listed for each profile below. All other URL categories will be set to `ALERT` in the templates for logging purposes. The complete list of categories can be found in the url filtering template.

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)

3.4.5 Anti-Virus

view xml template: profiles_virus

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

---

Note: **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.

3.4.6 Vulnerability Protection

view xml template: profiles_vulnerability

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

3.4.7 Wildfire Analysis

view xml template: profiles_wildfire_analysis

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

Note: `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

3.4.8 Security Profile Groups

view xml template: profile_group

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

3.5 Security Rules

3.5.1 Recommended Block Rules

view xml template: rulebase_security

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

Warning: 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.

Note: 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.

3.5.2 Default Security Rules

view xml template: rulebase_default_security_rules

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
  - Explicit drop of traffic between zones
  - Enable logging at session-end using the default logging profile

3.6 Decryption

3.6.1 Profiles

view xml template: profiles_decryption

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

3.6.2 Decryption Rules

view xml template: rulebase_decryption

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`

3.7 Zone Protection

3.7.1 Profile

view xml template: zone_protection_profile

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

Note: **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

3.8 Reports

3.8.1 Reports

view xml template: reports_simple

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.

Note: **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.

3.8.2 Report Groups

view xml template: report_group_simple

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

3.8.3 Email Scheduler

view xml template: email_scheduler_simple

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

CHAPTER 4

Panorama templates

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

Panorama can be configured using shared elements and device-specific elements. For xml configurations the use of shared or device-specific configurations is based on the xpath location of the snippets. Set commmands also denote shared or device-specific configurations. The provided xml snippets have variations in the metadata.yaml files specifying shared or device-specific placement in the configuration while the set commands and default loadable configuration are shared only.

Grouping of XML snippets

The xml template directories are group according to the user environment:

- *snippets_panorama*: A full Panorama configuration using shared device-group and template configurations
- *snippets_panorama_dgstack_shared*: used to add additional device-groups and stacks based on the shared model
- *snippets_panorama_not_shared*: a full Panorama configuration with the device-group and stack containing all configuration elements. Nothing is shared.
- *snippets_panorama_dgstack_notshared*: used to add additional device-groups and stack, each with full configuration elements. Nothing is shared.

Note: The template version is found in the template xml file as a tag attribute

Note: The set commands utilize the same configuration settings

4.1 General Device Configuration

This section provides templated configurations for general device settings.

4.1.1 Panorama settings

view xml template: panorama_system

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

- Update schedule settings
  - Turn on all telemetry settings
  - Check every 30 minutes for new threat signatures
  - Hourly checks for new AV signatures
  - Check every minute for new Wildfire signatures
  - Recommended time delays and thresholds for checks and installs
- Use SNMPv3
- Set default DNS and NTP values
- Set timezone to UTC
- Provide a standard login banner warning for unauthorized users

---

Note: The Panorama deployment types include `standard` or `cloud` for AWS, Azure, or GCP environments. This is an option in the tools `build_my_config` utility to use the proper config option in the template.

---

view xml template: panorama_setting

Panorama management settings

- Set 'enable reporting on groups' to 'yes'
- Disable sharing unused objects with devices
- set export of csv log file to maximum of 1,048,576

4.1.2 Security-related Device Settings

view xml template: device_setting

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

- Wildfire: set optimal file size limits for Wildfire uploads and show verdict responses for grayware, malware and phishing
- X-Forwarded-For: To ensure that attackers can't read and exploit the XFF values in web request packets that exit the firewall.
  - 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
- Prevent TCP and UDP buffer overflow and multi-part HTTP download evasions

  - Disable 'allow HTTP header range'
  - Disable 'tcp-bypass-exceed-queue'
  - Disable 'udp-bypass-exceed-queue'
- Enable high DP load logging
- Prevent App-ID buffer overflow evasion
  - set bypass-exceed-queue to 'no'
- Prevent TCP and MPTCP evasions
  - set urgent data to 'clear'
  - set drop zero flag to 'yes'
  - set bypass-exceed-oo-queue to 'no'
  - set check-timestamp-option to 'yes'
  - set strip-mptcp-option to yes
- set export of csv log file to maximum of 1,048,576

4.1.3 System Configuration

view xml template: device_system_shared

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

- Update schedule settings
  - Turn on all telemetry settings
  - Check every 30 minutes for new threat signatures
  - Hourly checks for new AV signatures
  - Check every minute for new Wildfire signatures
  - Recommended time delays and thresholds for checks and installs
- Use SNMPv3
- Set default DNS and NTP values
- Set timezone to UTC
- Provide a standard login banner warning for unauthorized users

Note: The management config types include static, dhcp-client, or dhcp-cloud as a special case of dhcp-client. This is specific to each deployment and can be selected as part of the tools to build `loadable_configs`. Since management interface is in the template config, this option must be included for deployment.

4.2 Logging

Logging best practice configurations for logging output and forwarding profiles. Also Panorama-specific settings for Panorama as a log collector

Warning: 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.

Note: Logging can be deployment dependent The destination in the logging profile is templated to an unroutable syslog server address. This can vary based on actual deployment scenarios.

4.2.1 Log forwarding profile

view xml template: log_settings_profiles

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

- Forward all log activity to Panorama (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)

4.2.2 Device log settings

view xml template: shared_log_settings

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

Note: When to use email alerts 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. The templates are set with a median view to capture key events without too much 'log fatigue' noise

4.2.3 Panorama log settings

view xml template: panorama_log_settings

Panorama 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 Panorama
- Traffic and threat related log configuration forwarding to Panorama

4.2.4 Panorama log collector group

view xml template: log_collector_group

After you configure Log Collectors and firewalls, you must assign them to a Collector Group so that the firewalls can send logs to the Log Collectors.

This is a placeholder default log collector group providing proper log forwarding and real-time email alerting configuration. In many cases deployments under-alert or over-alert real time losing visibility to something drastic because it is never sent to lost in then noise of too many emails.

- Syslog all logs using the sample syslog profile
- Email alerts for critical system logs and Wildfire malware/phishing verdicts that require immediate attention

4.3 Referenced Objects

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

4.3.1 Address Object

view xml template: address

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

4.3.2 External Dynamic Lists

view xml template: external_list

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

> **Warning:** **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.

4.3.3 Tags

view xml template: tag

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

4.4 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.

Warning: 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.

4.4.1 Custom URL Category

view xml template: profiles_custom_url_category

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

4.4.2 File Blocking

view xml template: profiles_file_blocking

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

Note: File blocking and 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

4.4.3 Anti-Spyware

view xml template: profiles_spyware

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

Note: **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

4.4.4 URL Filtering

view xml template: profiles_url_filtering

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

Note: Only `BLOCK` categories will be listed for each profile below. All other URL categories will be set to `ALERT` in the templates for logging purposes. The complete list of categories can be found in the url filtering template.

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)

4.4.5 Anti-Virus

view xml template: profiles_virus

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

---

Note: **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.

4.4.6 Vulnerability Protection

view xml template: profiles_vulnerability

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

4.4.7 Wildfire Analysis

view xml template: profiles_wildfire_analysis

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

Note: `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

4.4.8 Security Profile Groups

view xml template: profile_group

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

4.5 Security Rules

4.5.1 Recommended Block Rules

view xml template: pre_rulebase_security

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

Warning: 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.

Note: 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.

4.5.2 Default Security Rules

view xml template: post_rulebase_default_security_rules

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
  - Explicit drop of traffic between zones
  - Enable logging at session-end using the default logging profile

4.6 Decryption

4.6.1 Profiles

view xml template: profiles_decryption

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

4.6.2 Decryption Rules

view xml template: pre_rulebase_decryption

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

view xml template: post_rulebase_decryption

Recommended SSL decryption post-rules for no-decryption.

- NO decrypt rule used to validate SSL communications based on the `Recommended Decrypt profile`

4.7 Zone Protection

4.7.1 Profile

view xml template: zone_protection_profile

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

Note: **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

4.8 Reports

4.8.1 Reports

view xml template: reports_simple

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.

Note: 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.

Note: To generate reports that include PA-7000 Series log data not forwarding to Panorama, use Remote Device Data as the Data Source. This is only viewable from the `All device group option and not a specific device group.

4.8.2 Report Groups

view xml template: report_group_simple

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

4.8.3 Email Scheduler

view xml template: email_scheduler_simple

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

CHAPTER 5

Default Loadable Configurations

The default loadable configurations have been created using the iron-skillet default and sample values. These configurations can be loaded into Panorama or a firewall for day one purposes.

Warning: Before committing the default configuration, be sure to edit the superuser name and password to avoid unauthorized access

Note: The values for syslog IP address, the email profile, and the config export IP address are sample information and should be updated specific to the user's environment.

Each directory corresponds to variations in the configuration specific to the Panorama and firewall management IP addresses:

- sample-cloud options: management interfaces for Panorama and PAN-OS use DHCP
- sample-mgmt-dhcp: PAN-OS default to DHCP while Panorama uses a static IP interface
- sample-mgmt-static: both PAN-OS and Panorama use static IP Interfaces for management

Included for each type are a set command .conf file and xml full configuration file. Both include the same configurations. Also in each directory is the config_variables.yaml file to see what values were used to create the full configuration.

Note: Panorama can be configured using shared elements and device-specific elements. The default loadable configuration are specific to the shared model only.

5.1 SET commands

This model uses traditional CLI 'copy-and-paste' to load in the configuration line by line. Users can elect to edit default values for their specific deployment as each line is added or load the configuration as-is and then edit using the instructions below for *GUI variable edits* or *CLI variable edits* to the default configuration.

Note: The set command conf file includes options for standard/static or dhcp management interfaces. Only load the commands specific to the interface type to be used.

Adding the configuration with set commands

- get the conf file specific to the deployment type
- log into the CLI and enter *configure* for configuration mode
- copy set commands from the .conf file and paste into the terminal

---

Note: It is recommended that the user only grab 30-40 set commands per paste to avoid any buffer issues resulting in errors.

5.2 XML configuration file

The full configuration file can be imported and loaded using the management GUI.

Instead of using scripting tools, the instructions below allow a user to `Import` and `Load` a candidate configuration that can be manually edited by *GUI variable edits* or *CLI variable edits*.

Warning: Loading a full configuration file will replace the existing candidate configuration. Save a copy of the existing configuration prior to loading the iron-skillet xml configuration file. Edit any local values before committing as a running configuration.

5.2.1 Import the configuration file using the GUI

1. Click on the `Device` tab
2. Select `Setup` in the left nav bar
3. Click on the `Operations` tab
4. Then `Import named configuration snapshot` choosing the day one config xml file

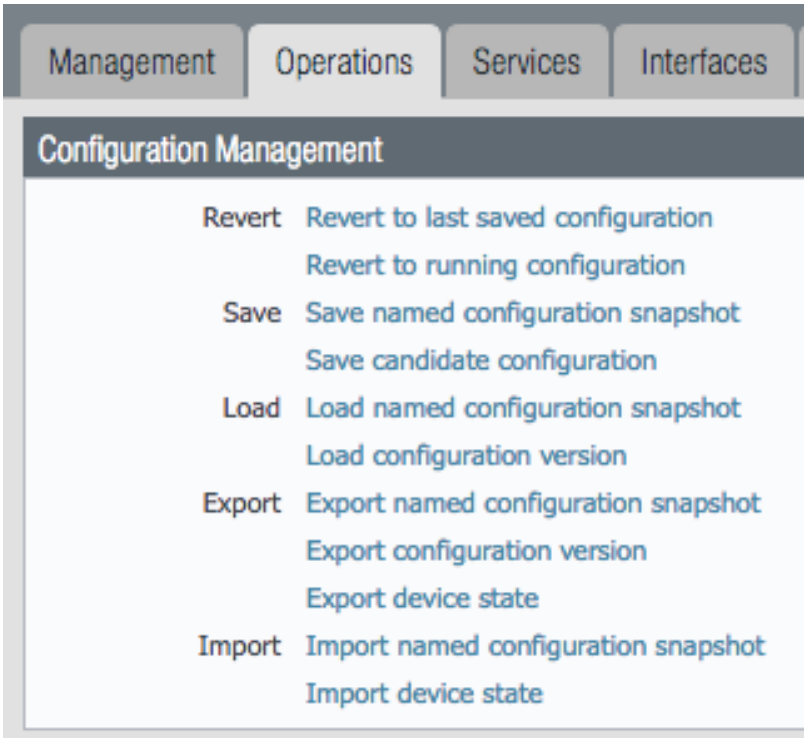
Note: You should perform a `Save named configuration snapshot` as backup prior to loading the new configuration

---

5.2.2 Load the configuration

1. Still under the `Operations` tab, use `Load named configuration snapshot` choosing the day one config xml file

2. Ensure no errors loading the configuration.



Note: If you see {{ text }} related import or load errors ensure you have the template file imported from the loadable_configs directory and not the templates directory.

5.3 GUI variable edits

After loading the configurations using set or xml commands, users can edit specific values instead of using the iron-skillet defaults.

The complete list of variables used by iron-skillet can be found at *Creating Loadable Configurations*.

5.3.1 GUI variable edits: Firewall

The steps below are for a stand-alone NGFW platform without Panorama.

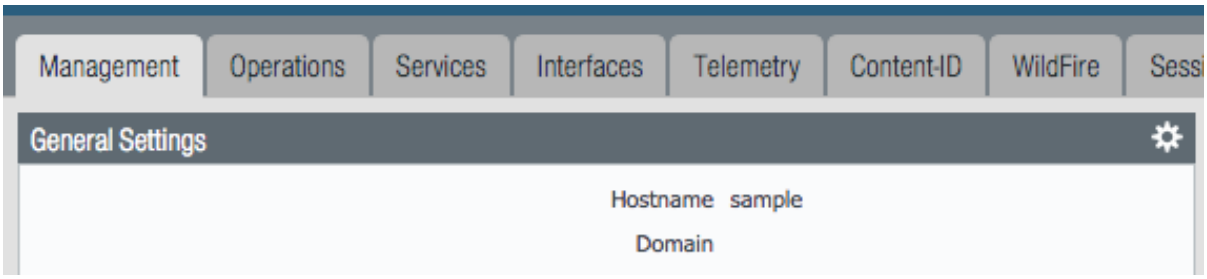
Device tab edits

The following edits are found under the `Device` tab

From here the following edits can be made:

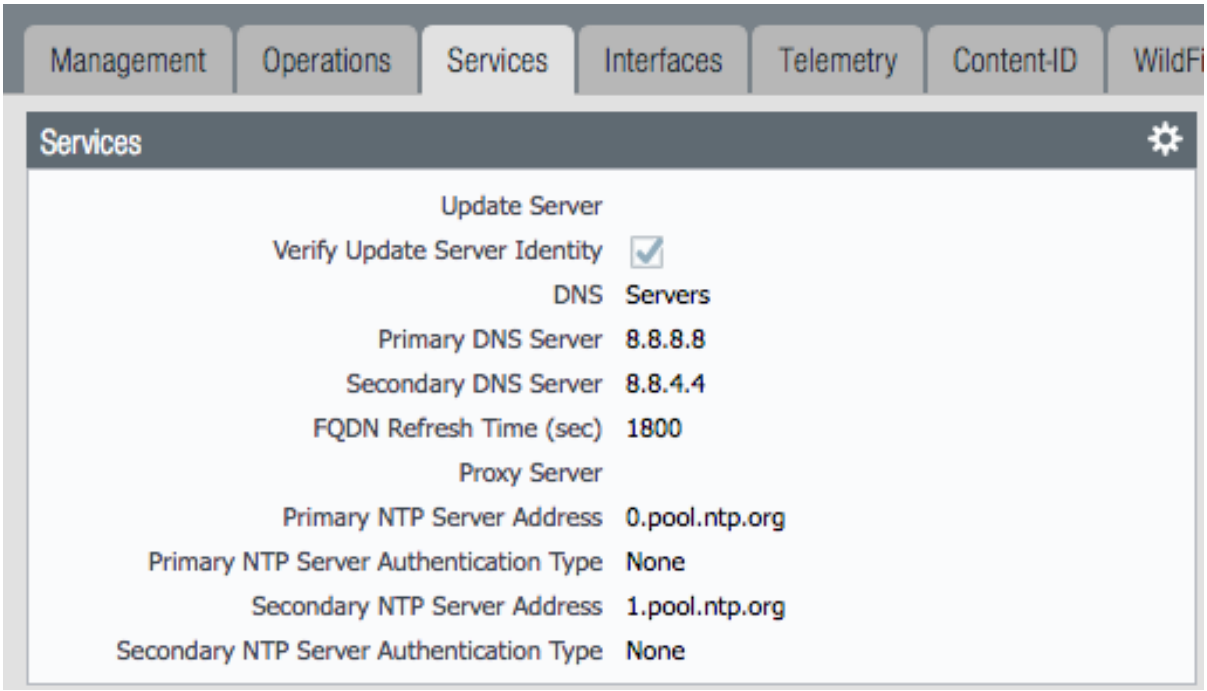
Hostname

1. Go to Device –> Setup –> Management
2. Click the `gear` icon to edit the hostname



DNS and NTP servers

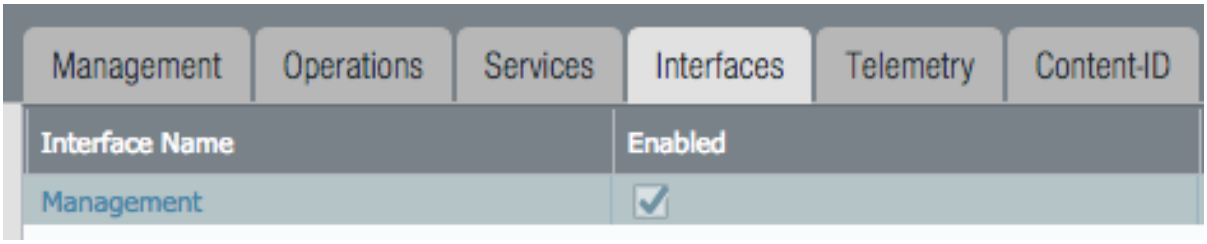
1. Go to Device –> Setup –> Services
2. Click the `gear` icon to edit the server values
3. Choose the Services (DNS) and NTP tabs accordingly



Static Management Interface

For a static management interface configuration, edit the IP address, subnet mask, default gateway.

1. Go to Device –> Setup –> Interfaces
2. Click on the `Management` link
3. Edit the management interface attributes



Superuser Administrator

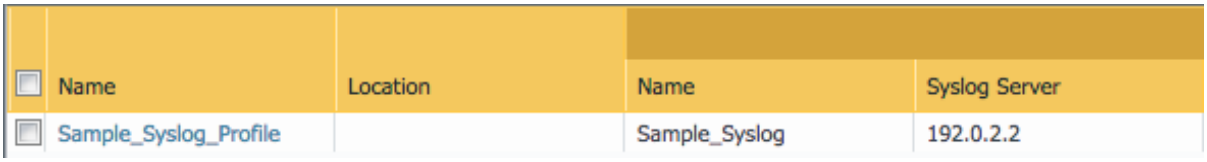
The sample configuration uses the default admin/admin username and password setting. It is recommended to remove this user and add a new superuser or at a minimum change the admin user password.

1. Go to Device –> Administrators
2. Select and delete the `admin` user account
3. Choose to `Add` a new user entering the username and password in the pop-up window

Syslog IP Address

Syslog is used to send traffic, threat and other log updates to an external system.

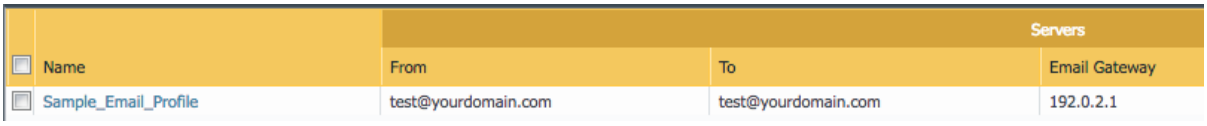
1. Go to Device –> Server Profiles –> Syslog
2. Click on the Sample_Syslog_Profile link and edit the IP address



Email Server Profile

The email profile is used to send key alerts to select recipients.

1. Go to Device –> Server Profiles –> Email
2. Click on the Sample_Email_Profile link and edit the from, to, and gateway values in the pop-up window.



Object tab edits

The following edits are found under the `Objects` tab

From here the following edits can be made:

Addresses

The template uses two address objects for sinkhole values, one each for IPv4 and IPv6. These are referenced in security rules.

1. Go to Objects –> Address
2. Click on the Sinkhole IPv4 and IPv6 links and edit the IP address

Name	Type	Address
Sinkhole-IPv4	IP Netmask	72.5.65.111
Sinkhole-IPv6	IP Netmask	2600:5200::1

Anti-Spyware Security Profiles

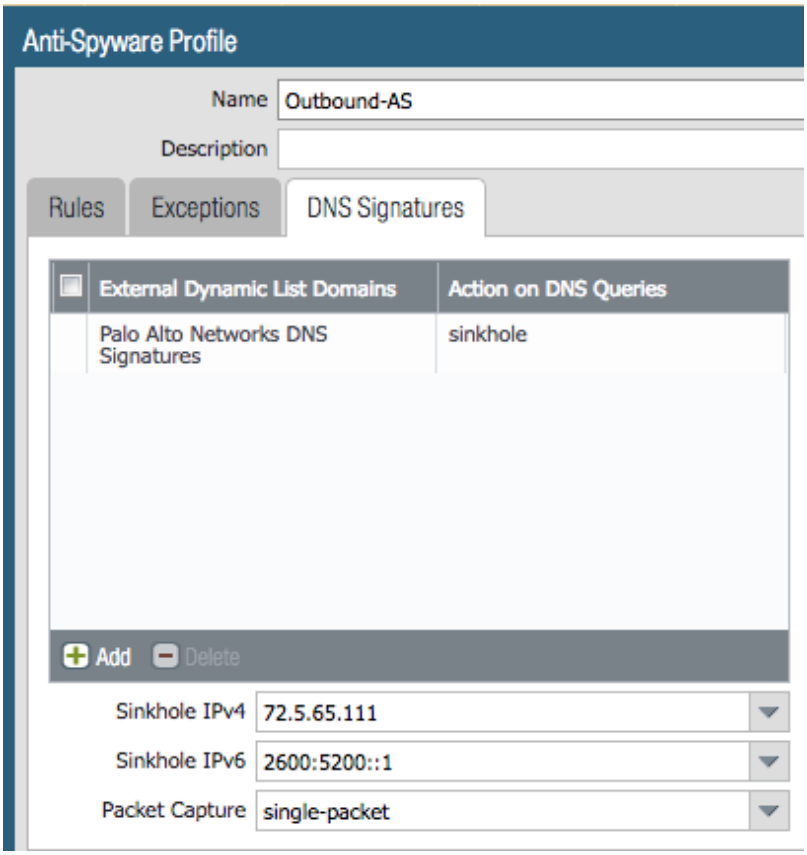
The templates define multiple named Anti-Spyware profiles all appended with `-AS`. Each of these profiles must be updated with new sinkhole address if non-default values are required.

These values should match the sinkhole IP addresses configured under `Addresses`.

1. Go to Objects –> Security Profiles –> Anti-Spyware

Name	Location	Count	Rule Name	Threat Name	Severity	Action	Packet Capture
default	Predefined	Rules: 4	simple-critical	any	critical	default	disable
			simple-high	any	high	default	disable
			simple-medium	any	medium	default	disable
			simple-low	any	low	default	disable
strict	Predefined	Rules: 5	simple-critical	any	critical	reset-both	disable
			simple-high	any	high	reset-both	disable
			simple-medium	any	medium	reset-both	disable
			simple-informational	any	informational	default	disable
			simple-low	any	low	default	disable
Outbound-AS		Rules: 2	Block-Critical-High-Medium	any	high,critical,med...	reset-both	single-packet
			Default-Low-Info	any	low,informational	default	disable
Inbound-AS		Rules: 2	Block-Critical-High-Medium	any	high,critical,med...	reset-both	single-packet
			Default-Low-Info	any	low,informational	default	disable
Internal-AS		Rules: 2	Block-Critical-High	any	high,critical	reset-both	single-packet
			Default-Medium-Low-Info	any	low,informationa...	default	disable
Alert-Only-AS		Rules: 1	Alert-All	any	any	alert	disable
Exception-AS							

2. Click on one of the template specific profiles ending in `-AS`
3. Click on the DNS Signatures tab and update the IPv4 and IPv6 sinkhole addresses



5.3.2 GUI variable edits: Panorama

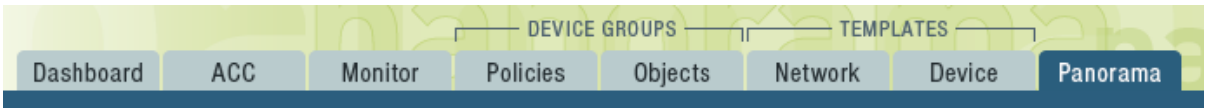
The steps below are for edits to the Panorama configuration. Variable edits in the GUI will include both the Panorama system edits and managed firewall device-group and template configurations.

The are four areas to be edited:

- Panorama platform settings
- iron-skillet template for shared device and network items
- sample template stack for device-specific items
- Shared device-group for shared objects and policies

Panorama tab edits

The following edits are found under the `Panorama` tab

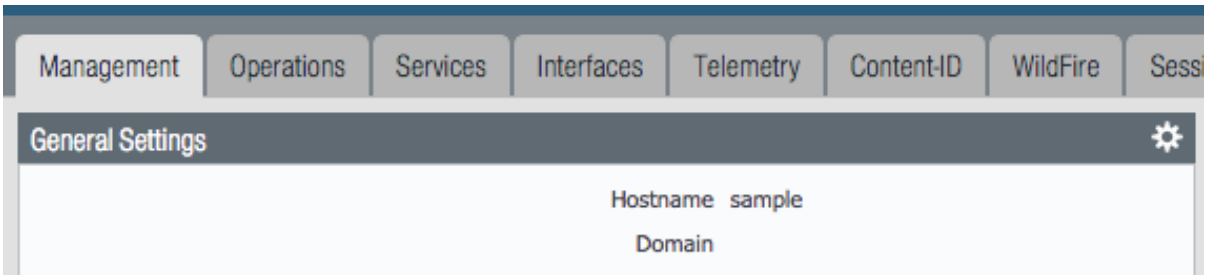


From here the following edits can be made:

Panorama > Hostname

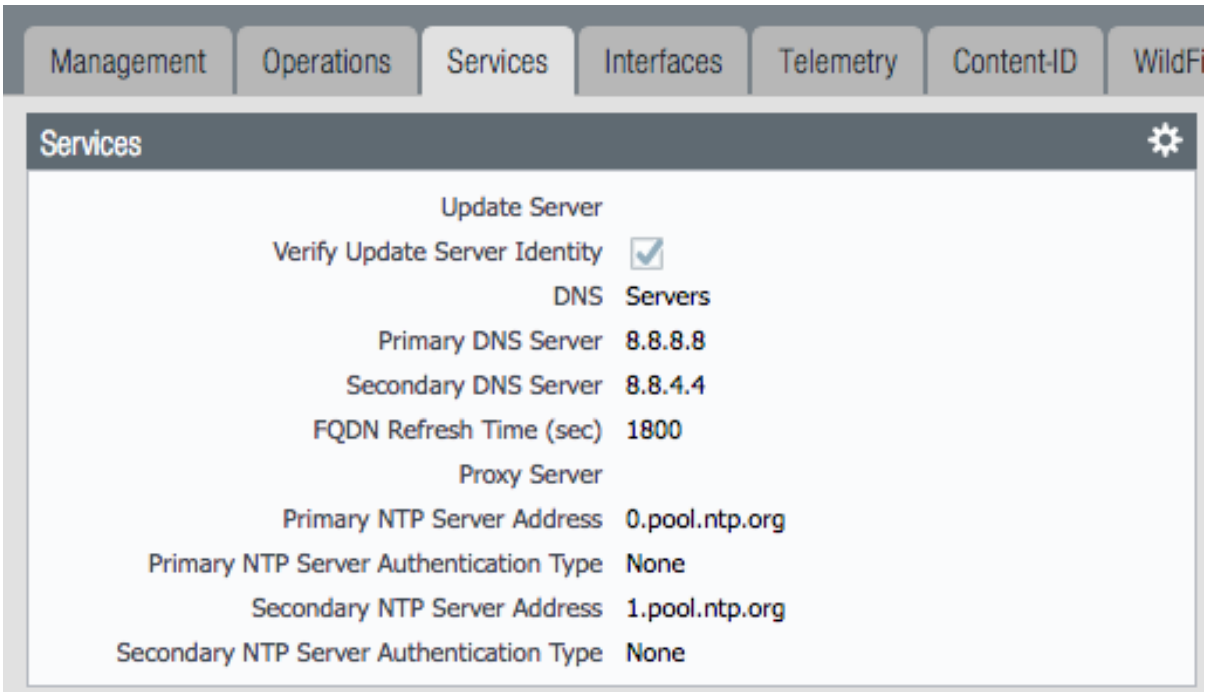
1. Go to Panorama –> Setup –> Management

2. Click the `gear` icon to edit the Panorama hostname



Panorama > DNS and NTP servers

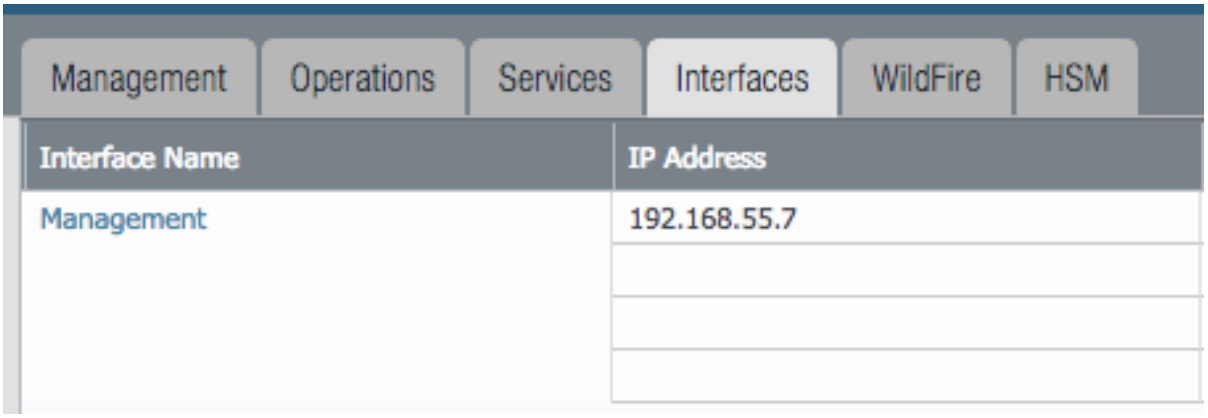
1. Go to Panorama –> Setup –> Services
2. Click the `gear` icon to edit the server values
3. Choose the Services (DNS) and NTP tabs accordingly



Panorama > Management Interface

This configuration is specific to the Panorama management interface when statically defined.

1. Go to Panorama –> Setup –> Interfaces
2. Click on the `Management` link
3. Edit the management interface attributes



Panorama > Superuser Administrator

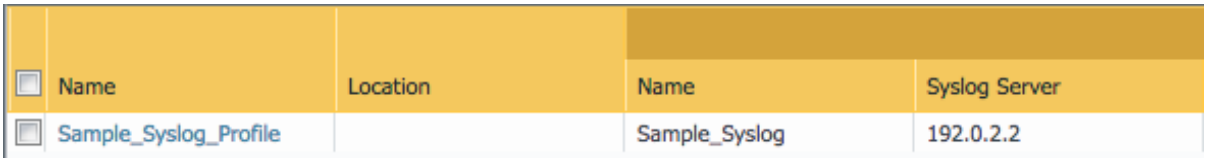
The sample configuration uses the default admin/admin username and password setting. It is recommended to remove this user and add a new superuser or at a minimum change the admin user password.

1. Go to Panorama –> Administrators
2. Select and delete the `admin` user account
3. Choose to `Add` a new user entering the username and password in the pop-up window

Panorama > Syslog IP Address

Syslog is used to send traffic, threat and other log updates to an external system.

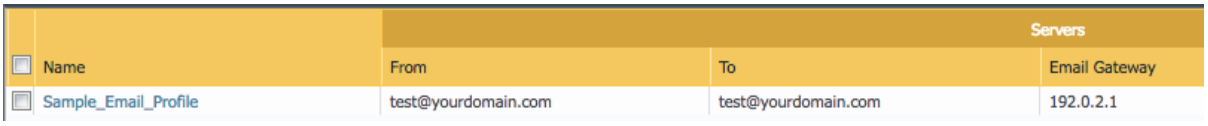
1. Go to Panorama –> Server Profiles –> Syslog
2. Click on the Sample_Syslog_Profile link and edit the IP address



Panorama > Email Server Profile

The email profile is used to send key alerts to select recipients.

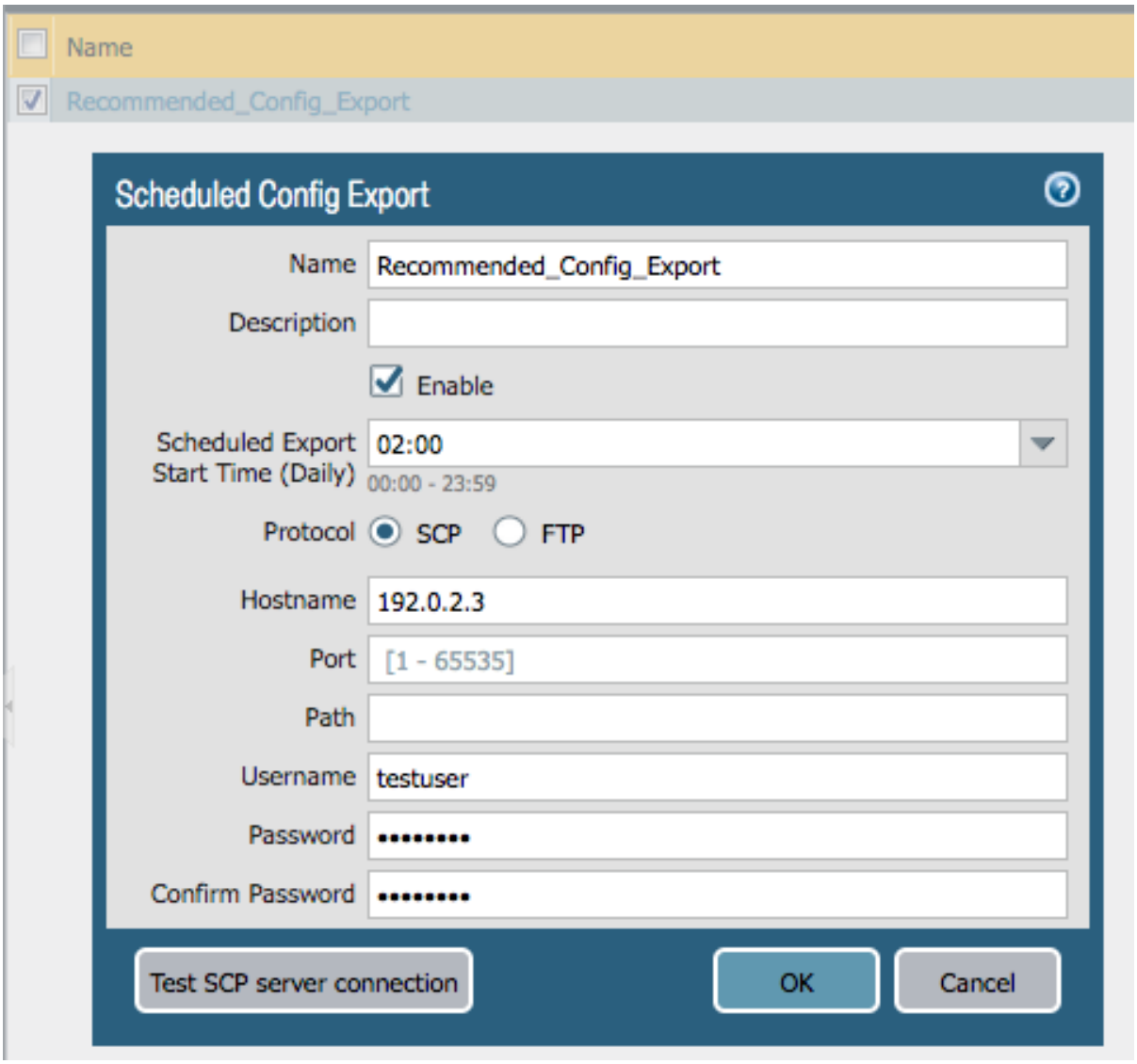
1. Go to Panorama –> Server Profiles –> Email
2. Click on the Sample_Email_Profile link and edit the from, to, and gateway values in the pop-up window.



Panorama > Config Bundle Export Server

1. Go to Panorama –> Scheduled Config Export

2. Click on the Recommended_Config_Export link
3. In the pop-up window, edit the Hostname value

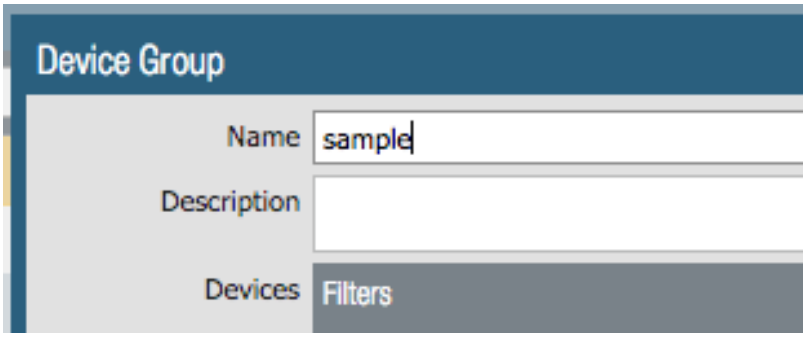


Panorama > Template Stack

1. Go to Panorama –> Template
2. Click on the `sample_stack` link and edit the name

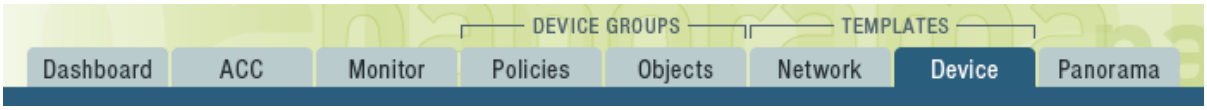
Panorama > Device-Group

1. Go to Panorama –> Device-Groups
2. Click on the `sample_devicegroup` link and edit the name



Templates > Device tab edits

The following edits are found under the `Device` tab



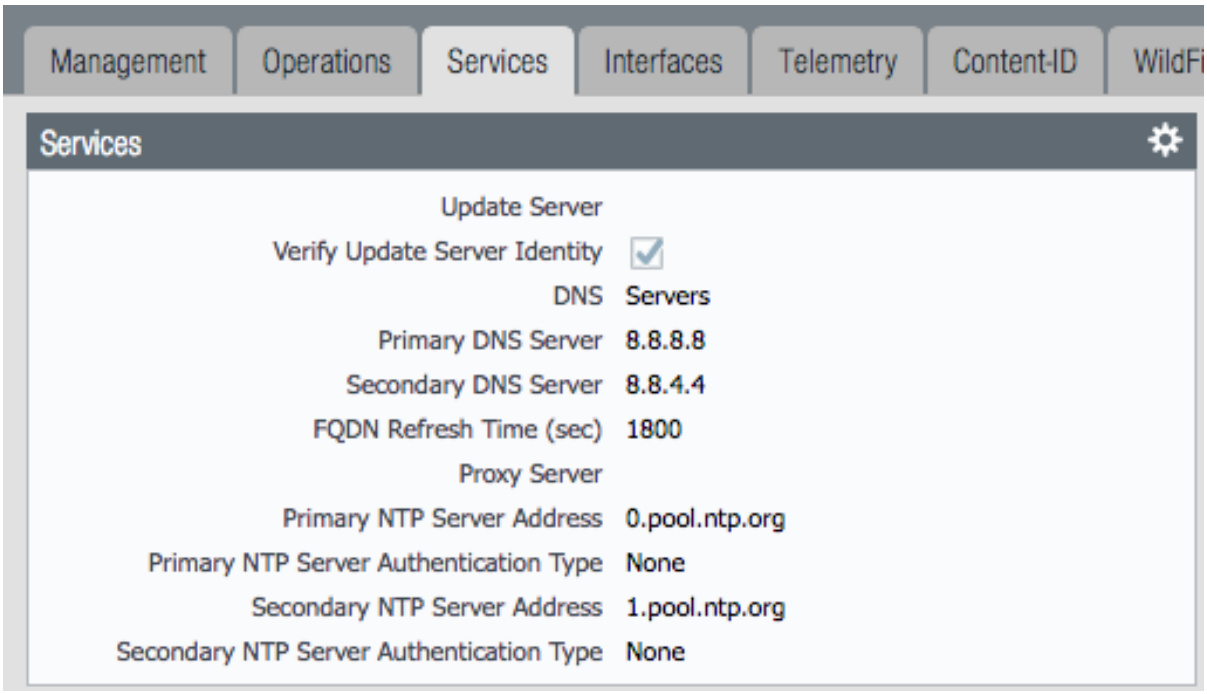
Note: The edits are grouped by the *iron-skillet* template edits and *sample_stack* template stack edits

** iron-skillet template edits**

Note: Make sure the template selected in the GUI is *iron-skillet* before completing the steps below

DNS and NTP servers

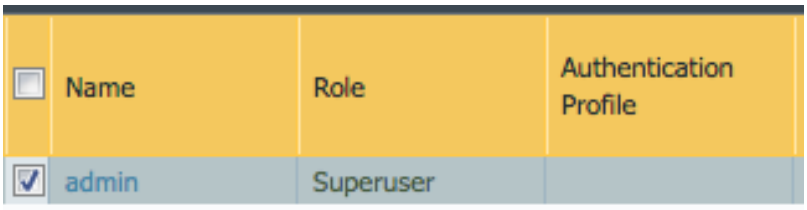
1. Go to Device –> Setup –> Services
2. Click the `gear` icon to edit the server values
3. Choose the Services (DNS) and NTP tabs accordingly



Superuser Administrator

The sample configuration uses the default admin/admin username and password setting. It is recommended to remove this user and add a new superuser or at a minimum change the admin user password.

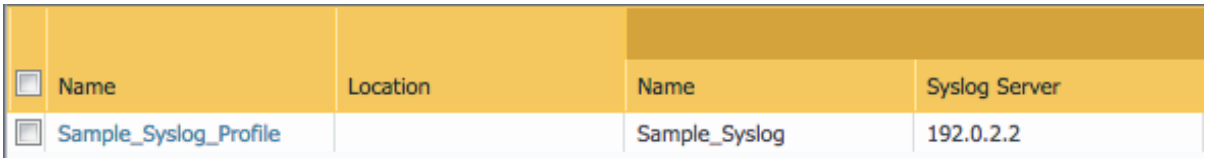
1. Go to Device –> Administrators
2. Select and delete the `admin` user account
3. Choose to `Add` a new user entering the username and password in the pop-up window



Syslog IP Address

Syslog is used to send traffic, threat and other log updates to an external system.

1. Go to Device –> Server Profiles –> Syslog
2. Click on the Sample_Syslog_Profile link and edit the IP address

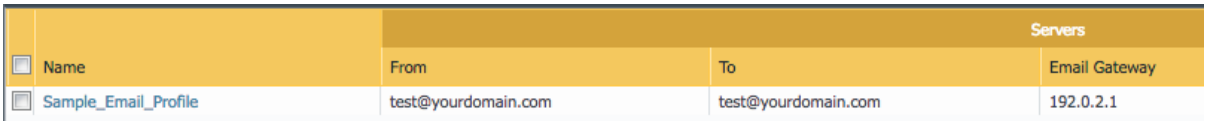


Email Server Profile

The email profile is used to send key alerts to select recipients.

1. Go to Device –> Server Profiles –> Email

2. Click on the Sample_Email_Profile link and edit the from, to, and gateway values in the pop-up window.

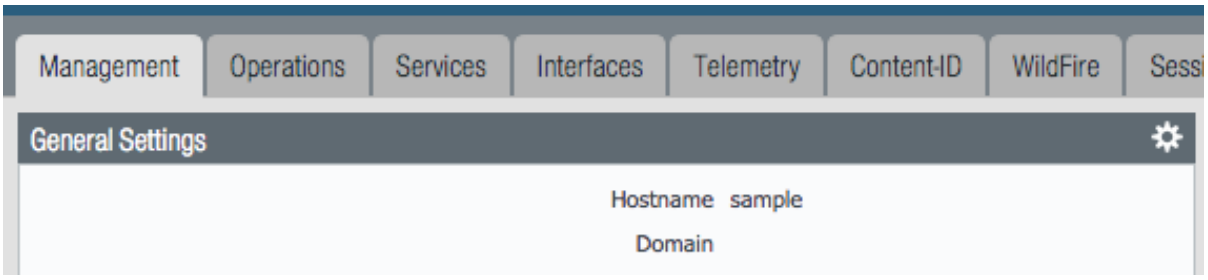


** iron-skillet template edits**

Note: Make sure the template selected in the GUI is *sample_stack* (or the updated name) before completing the steps below

Hostname

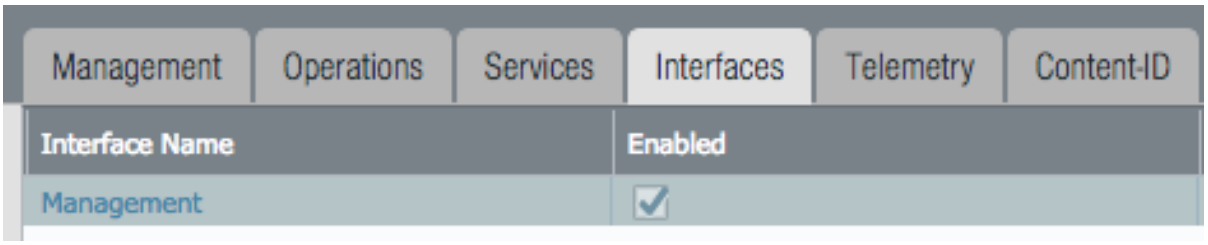
1. Go to Device –> Setup –> Management
2. Click the `gear` icon to edit the hostname



Static Management Interface

For a static management interface configuration, edit the IP address, subnet mask, default gateway.

1. Go to Device –> Setup –> Interfaces
2. Click on the `Management` link
3. Edit the management interface attributes



** Shared device-group edits**

Note: Make sure the device-group selected in the GUI is *Shared* before completing the steps below

Device-Group > Objects tab edits

The following edits are found under the `Objects` tab

From here the following edits can be made:

Addresses

The template uses two address objects for sinkhole values, one each for IPv4 and IPv6. These are referenced in security rules.

1. Go to Objects –> Address
2. Click on the Sinkhole IPv4 and IPv6 links and edit the IP address

Name	Type	Address
Sinkhole-IPv4	IP Netmask	72.5.65.111
Sinkhole-IPv6	IP Netmask	2600:5200::1

Anti-Spyware Security Profiles

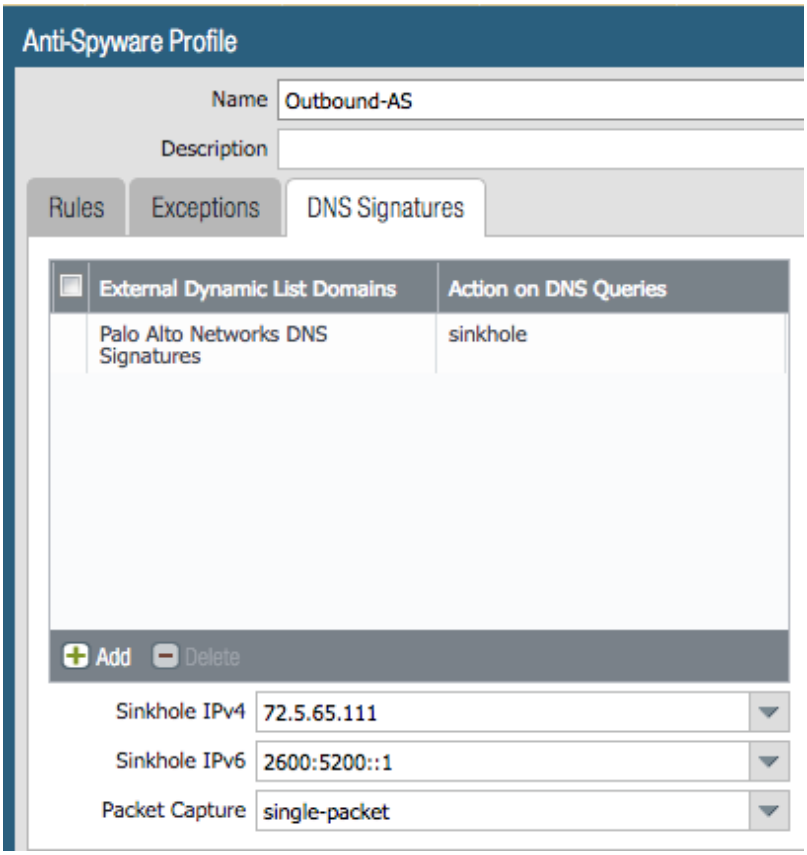
The templates define multiple named Anti-Spyware profiles all appended with `-AS`. Each of these profiles must be updated with new sinkhole address if non-default values are required.

These values should match the sinkhole IP addresses configured under `Addresses`.

1. Go to Objects –> Security Profiles –> Anti-Spyware

Name	Location	Count	Rule Name	Threat Name	Severity	Action	Packet Capture
default	Predefined	Rules: 4	simple-critical	any	critical	default	disable
			simple-high	any	high	default	disable
			simple-medium	any	medium	default	disable
			simple-low	any	low	default	disable
strict	Predefined	Rules: 5	simple-critical	any	critical	reset-both	disable
			simple-high	any	high	reset-both	disable
			simple-medium	any	medium	reset-both	disable
			simple-informational	any	informational	default	disable
			simple-low	any	low	default	disable
Outbound-AS		Rules: 2	Block-Critical-High-Medium	any	high,critical,med...	reset-both	single-packet
			Default-Low-Info	any	low,informational	default	disable
Inbound-AS		Rules: 2	Block-Critical-High-Medium	any	high,critical,med...	reset-both	single-packet
			Default-Low-Info	any	low,informational	default	disable
Internal-AS		Rules: 2	Block-Critical-High	any	high,critical	reset-both	single-packet
			Default-Medium-Low-Info	any	low,informationa...	default	disable
Alert-Only-AS		Rules: 1	Alert-All	any	any	alert	disable
Exception-AS							

2. Click on one of the template specific profiles ending in `-AS`
3. Click on the DNS Signatures tab and update the IPv4 and IPv6 sinkhole addresses



5.4 CLI variable edits

After loading the configurations using set or xml commands, users can edit specific values instead of using the iron-skillet defaults.

The complete list of variables used by iron-skillet can be found at *Creating Loadable Configurations*.

5.4.1 CLI variable edits: Firewall

This section is specific to a non-Panorama managed NGFW.

Instead of using the GUI to make template edits for each variable value, below are steps using SET commands to make the same candidate configuration changes.

The {{ text }} values denotes where a variable is used in the template.

Hostname

```
set deviceconfig system hostname {{ hostname }}
```

DNS and NTP Servers

```
set deviceconfig system dns-setting servers primary {{ DNS 1 }} secondary {{ DNS 2 }}
set deviceconfig system ntp-servers primary-ntp-server ntp-server-address {{ NTP 1 }}
set deviceconfig system ntp-servers secondary-ntp-server ntp-server-address {{ NTP 2 }
↪}
```

(continues on next page)

(continued from previous page)

Static management interface

```
set deviceconfig system ip-address {{ ip address }} netmask {{ mask }} default-
↪gateway {{ gateway }}
```

Superuser admin account

```
set mgt-config users {{ username }} permissions role-based superuser yes
set mgt-config users {{ username }} password
```

When the password command is entered, the user will be prompted for a password.

Syslog and Email Server Profiles

```
set shared log-settings syslog Sample_Syslog_Profile server Sample_Syslog server {{␣
↪ip address }}
set shared log-settings email Sample_Email_Profile server Sample_Email_Profile from {
↪{ from }}
set shared log-settings email Sample_Email_Profile server Sample_Email_Profile to {{␣
↪to }}
set shared log-settings email Sample_Email_Profile server Sample_Email_Profile␣
↪gateway {{ address }}
```

Address Objects

```
set address Sinkhole-IPv4 ip-netmask {{ IPv4 address }}
set address Sinkhole-IPv6 ip-netmask {{ IPv6 address }}
```

Anti-Spyware Security Profiles

The same commands are used across all of the template security profiles ending in `-AS`.

```
set profiles spyware {{ profile name }} botnet-domains sinkhole ipv4-address {{ IPv4␣
↪address }}
set profiles spyware {{ profile name }} botnet-domains sinkhole ipv6-address {{ IPv6␣
↪address }}
```

5.4.2 CLI variable edits: Panorama

This section is specific to configuration of a Panorama management system.

Instead of using the GUI to make template edits for each variable value, below are steps using SET commands to make the same candidate configuration changes.

The {{ text }} values denotes where a variable is used in the template.

Note: The initial configurations are specific to the Panorama platform itself. The managed firewall configurations are added under the template and device-group configurations.

Panorama > Hostname

```
set deviceconfig system hostname {{ hostname }}
```

Panorama > DNS and NTP Servers

```
set deviceconfig system dns-setting servers primary {{ DNS 1 }} secondary {{ DNS 2 }}
set deviceconfig system ntp-servers primary-ntp-server ntp-server-address {{ NTP 1 }}
set deviceconfig system ntp-servers secondary-ntp-server ntp-server-address {{ NTP 2 }
↪}
```

Panorama > Static management interface

```
set deviceconfig system ip-address {{ ip address }} netmask {{ mask }} default-
↪gateway {{ gateway }}
```

Panorama > Superuser admin account

```
set mgt-config users {{ username }} permissions role-based superuser yes
set mgt-config users {{ username }} password
```

When the password command is entered, the user will be prompted for a password.

Panorama > Syslog and Email Server Profiles

```
set panorama log-settings syslog Sample_Syslog_Profile server Sample_Syslog server {{␣
↪ip address }}
set panorama log-settings email Sample_Email_Profile server Sample_Email_Profile from
↪{{ from }}
set panorama log-settings email Sample_Email_Profile server Sample_Email_Profile to {
↪{ to }}
set panorama log-settings email Sample_Email_Profile server Sample_Email_Profile␣
↪gateway {{ address }}
```

Panorama > Config Bundle Export Schedule

```
set deviceconfig system config-bundle-export-schedule Recommended_Config_Export␣
↪protocol scp hostname {{ ip address }}
```

Note: The configuration for Panorama has some element in the iron-skillet shared template and others specific to the device captured as a template-stack called sample_stack. The same is true for device-group items that are either shared or contained in a device-specific group, namely reports.

Template > Hostname

```
set template sample_template config deviceconfig system hostname {{ hostname }}
```

Template > DNS and NTP Servers

```
set template iron-skillet config deviceconfig system dns-setting servers primary {{␣
↪DNS 1 }} secondary {{ DNS 2 }}
set template iron-skillet config deviceconfig system ntp-servers primary-ntp-server␣
↪ntp-server-address {{ NTP 1 }}
set template iron-skillet config deviceconfig system ntp-servers secondary-ntp-server␣
↪ntp-server-address {{ NTP 2 }}
```

Template > Static management interface

This is to be configured for a firewall with a static management interface.

```
set template sample_template config deviceconfig system ip-address {{ ip address }}
set template sample_template config deviceconfig system netmask {{ mask }}
set template sample_template config deviceconfig system default-gateway {{ gateway }}
```

Template > Superuser admin account

```
set template iron-skillet config mgt-config users {{ username }} permissions role-
↪based superuser yes
set template iron-skillet config mgt-config users {{ username }} password
```

When the password command is entered, the user will be prompted for a password.

Template > Syslog and Email Server Profiles

```
set template iron-skillet config shared log-settings syslog Sample_Syslog_Profile␣
↪server Sample_Syslog server {{ ip address }}
set template iron-skillet config shared log-settings email Sample_Email_Profile␣
↪server Sample_Email_Profile from {{ from }}
set template iron-skillet config shared log-settings email Sample_Email_Profile␣
↪server Sample_Email_Profile to {{ to }}
set template iron-skillet config shared log-settings email Sample_Email_Profile␣
↪server Sample_Email_Profile gateway {{ address }}
```

Device-Group > Address Objects

```
set shared address Sinkhole-IPv4 ip-netmask {{ IPv4 address }}
set shared address Sinkhole-IPv6 ip-netmask {{ IPv6 address }}
```

Device-Group Anti-Spyware Security Profiles

The same commands are used across all of the templated security profiles ending in `-AS`.

```
set shared profiles spyware {{ profile name }} botnet-domains sinkhole ipv4-address {
↪{ IPv4 address }}
set shared sample profiles spyware {{ profile name }} botnet-domains sinkhole ipv6-
↪address {{ IPv6 address }}
```

CHAPTER 6

Formula-based Excel Spreadsheet

For users who want to customize their configuration before loading without the use of python utilities, this is a preferred model for configuration.

The spreadsheets can be found at set commands panos and set commands panorama

The `values` worksheet can be updated with user-specific values. Formulas embedded in the `set commands` worksheet will use the user added values.

Once the spreadsheet is updated, the traditional copy-and-paste model can be used to load the configuration using the CLI.

Warning: The set commands use formulas referencing cells in the values worksheet. Use caution if making changes to the base spreadsheet to avoid incorrect references to cell values.

CHAPTER 7

Creating Loadable Configurations

The base templates are designed for variable substitution. The variables provide flexibility for templates configurations to be modified specific to each deployment.

A jinja model for variables is used with the form `{{ variable }}`

Warning: The configuration templates for device and Panorama system include jinja 'if' conditionals. These are used by the create_loadable_configs.py tool to determine what IP information should be added regarding the management interface.

If the tool or jinja formats will not be used, remove the {% text %} statements. The user will also have to manually replace the variables in order for the config to load and commit

7.1 Variables list and descriptions

The table below lists the template variables along with placeholder or recommended settings.

Variable name	Default value	Description
ADMINISTRATOR_USERNAME	admin	superuser id; prompted when using build_my_config tool
ADMINISTRATOR_PASSWORD	admin [change first]	superuser password; prompted and hashed in build_my_config
FW_NAME	sample	used for hostname and device-group/template in Panorama
TEMPLATE	sample_template	template for device specific configurations
STACK	sample_stack	Panorama sample template stack
DEVICE_GROUP	sample_devicegroup	Panorama sample device-group name
DNS_1	8.8.8.8 (Google)	primary DNS server
DNS_2	8.8.4.4 (Google)	secondary DNS server
NTP_1	0.pool.ntp.org	primary NTP server
NTP_2	1.pool.ntp.org	secondary NTP server
SINKHOLE_IPV4	72.5.65.111	IPv4 sinkhole address (Palo Alto Networks)
SINKHOLE_IPV6	2600:5200::1	IPv6 sinkhole address (IPv6 bogon)
INTERNET_ZONE	internet	baseline exception for reports
EMAIL_PROFILE_GATEWAY	192.0.2.1	email profile gateway address; NET-1 default
EMAIL_PROFILE_FROM	sent-from@yourdomain.com	from address for email alerts
EMAIL_PROFILE_TO	sendto@yourdomain.com	to address for email alerts
SYSLOG_SERVER	192.0.2.2	syslog IP address; NET-1 unroutable default
CONFIG_EXPORT_IP	192.0.2.3	config bundle export target from Panorama; NET-1 default
MGMT_TYPE	dhcp-client	Firewall mgmt IP type (dhcp-client or static)
MGMT_IP	192.168.55.10	Firewall mgmt IP if type=static
MGMT_MASK	255.255.255.0	Firewall netmask if type=static
MGMT_DG	192.168.55.2	Firewall default gateway if type=static
CONFIG_PANORAMA_IP	yes	For build_my_config, determine if Panorama IP to be added
PANORAMA_TYPE	standard	Used in order to set mgmt interface for standard or cloud
PANORAMA_IP	192.168.55.7	Panorama IP if to be added to my_config
PANORAMA_MASK	255.255.255.0	Panorama netmask if to be added to my_config
PANORAMA_DG	192.168.55.2	Panorama default gateway if to be added to my_config
INCLUDE_PAN_EDL	yes	Include the panw edl object security rules

7.2 Create Loadable Configuration python utility

The tools folder in the iron-skillet repo contains a simple python utility for variable substitution.

This tools folder can be found at https://github.com/PaloAltoNetworks/iron-skillet/tree/panos_v8.0/tools

The directions below detail how to use the utility in a python virtual environment on Mac or Linux. Similar instructions can work for Windows with python and pip installed.

Note: This tool is designed for Python 3.6 or layer.

7.2.1 Install the repo and tools

The initial step is to clone the repo to a local machine with release panos_v8.0.

Clone using ssh:

$ git clone -b panos_v8.0 git@github.com:PaloAltoNetworks/iron-skillet.git

Clone using https:

$ git clone -b panos_v8.0 https://github.com/PaloAltoNetworks/iron-skillet.git

After the repo is cloned locally, the following steps are used to setup and activate the python virtual environment.

Note: The example below shows python version 3.6 in the second step. If using python 3.5 or 3.7, replace with the respective version

---

```
$ cd iron-skillet/tools
$ python3.6 -m venv env
$ source env/bin/activate
(env)$ pip install -r requirements.txt
```

The virtual environment name is `env` and if active will likely be shown to the left of the command prompt. If successful, the iron-skillet templates and tools are now ready to use.

7.2.2 Update the variable values

Inside the tools directory, update the config_variables.yaml file then run create_loadable_configs.py. The example shows the vi text editor but any text editor may be used.

```
(env)$ cd iron-skillet/tools  [if not in the tools directory]
(env)$ vi config_variables.yaml
```

Edit the config_variables.yaml file for your local deployment and save.

Key variables to edit include:

- management interface type: static, dhcp-client, dhcp-cloud based on firewall deployment
- Panorama deployment type: standard or cloud based on Panorama deployment

7.2.3 Run the application

Ensure the variable values are correct and run the application.

```
(env)$ python3 create_loadable_configs.py
>>> Enter the name of the output directory:
>>> Enter the superuser administrator account username:
>>> Enter the superuser administrator account password:
```

This will run the python utility and output set commands and full xml config files. Loadable configs are stored in the loadable_configs directory. The config folder prefix is based on the output directory name used when running the script.

Warning: You will be prompted for a username/password that will be used in the configuruation file. A hash is created for the password so it is unreadable and the default admin/admin is removed. Remember the user/password information before committing to a running firewall or Panorama.

CHAPTER 8

Loading the XML templates

The template are xml file format that have to be loaded into the device as a full config or with modular partial loading.

Multiple options including GUI, CLI, and API can be utilized. The sections below give details for template loading using various models specific to the users expertise and current operational environment.

Note: Sample configuration files are in the loadable_configs directory. Samples include a static management interface, basic dhcp-client management interface, and additional dhcp-client options for cloud deployments. These configurations are loadable and can be manually edited although user-specific configurations can be created using the `create_loadable_configs` utility in the tools folder.

8.1 Preparing the configuration files

The template files in the panos and panorama directories are xml format. These templates are using a jinja variable model in the xml as `{{ variable name }}`. In order to have a loadable configuration, the recommended practice is to use create_loadable_configs.py in the tools folder.

The *Creating Loadable Configurations* documentation section details how to use this tool.

The output of the tool will be a set of xml snippet and full configuration files stored in the *loadable_configs* folder.

8.2 Load full configuration file

Either at the time of VM instantiation or post deploy, a full xml can be loaded into the system as a candidate configuration. This provides the simplicity of loading a new configuration but will replace any configuration currently in the device.

In comparison, a load config partial requires additional steps but merges into the existing configuration instead of replacing.

The steps below are for for a full configuration load and replace.

8.2.1 Edit the full xml configuration file

Since this will replace the existing configuration, the user is required to modify the xml file with admin accounts, management IP, and other initial configuration values. The template uses `{{ text }}` markers in the config file to denote values that MUST be changed.

Warning: During a commit, the device will show an error with the variable `{{ text }}` values in the error message. These values must be modified offline and the file imported for a successful load and commit.

Note: The user is recommended to use the create_loadable_configs.py tool to have a loadable configuration file

8.2.2 Import the configuration file using the GUI

1. Log into the firewall and click on the `Device` tab
2. Select `Setup` in the left nav bar
3. Click on the `Operations` tab
4. Then `Import named configuration snapshot` choosing the day one config xml file

Note: You should perform a `Save named configuration snapshot` as backup prior to loading the new configuration

8.2.3 Load and commit the configuration

1. Still under the `Operations` tab, use `Load named configuration snapshot` choosing the day one config xml file
2. Ensure no errors loading the configuration.
3. Once loaded use the GUI to verify the configuration elements have been loaded then `commit`

Note: As referenced above, you may see `{{ text }}` related errors during the commit. If this happens, you will need to edit the pre-imported xml file and then repeat the steps above to import, load, and commit the configuration.

8.3 Using Load Config Partial

The configuration file uses the xml format. Therefore each configuration element sits in the xml tree and is referenced by its `xpath`.

Using this concept, a template configuration file can be imported into Panorama or the firewall with only the referenced elements merged into the existing configuration. This is more modular than loading a full configuration file that replaces the existing configuration.

The syntax used for loading the templates is:

> load config partial from `{{filename}}` from-xpath `{{xpath}}` to-xpath `{{xpath}}` mode merge

where:

> `{{filename}}` is the xml file loaded into the device
>
> `{{xpath}}` denotes what part of the configuration is being merged from the day one file to the candidate configuration.

8.3.1 Edit the configuration xml file

Since this will replace the existing configuration, the user is required to modify the xml file with admin accounts, management IP, and other initial configuration values. The template uses `{{ text }}` markers in the config file to denote values that MUST be changed.

Warning: During a commit, the device will show an error with the variable `{{ text }}` values in the error message. These values must be modified offline and the file imported for a successful load and commit.

Note: The user is recommended to use the create_loadable_configs.py tool to have a loadable configuration file

8.3.2 Import the Day One configuration: GUI

1. Log into the firewall and click on the `Device` tab
2. Select `Setup` in the left nav bar
3. Click on the `Operations` tab
4. Then `Import named configuration snapshot` choosing the day one config xml file

Note: You can perform a `Save named configuration snapshot` as backup prior to loading the new configuration

8.3.3 Load the configuration elements: CLI

1. Log into the PAN-OS command line interface
2. Enter `configure` to go into configuration mode
3. Paste in each of the `load config partial` commands, in order
4. Once complete use the GUI to verify the configuration elements have been loaded then `commit`

8.3.4 PAN-OS load config partial commands

Cut-and-paste from the table below into the PAN-OS command line while in configuration mode.

You can paste multiple items. The system will pause during each load config partial, return a status message, then move to the next load. When complete, ensure the final load is entered and a status message received.

```
load config partial from iron_skillet_panos_full.xml from-xpath /config/
 ↪shared/log-settings to-xpath /config/shared/log-settings mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
 ↪tag to-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/
 ↪entry[@name='vsys1']/tag mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/deviceconfig/system to-xpath␣
 ↪/config/devices/entry[@name='localhost.localdomain']/deviceconfig/system␣
 ↪mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/deviceconfig/setting to-xpath␣
 ↪/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting␣
 ↪mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
 ↪address to-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/
 ↪entry[@name='vsys1']/address mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
 ↪external-list to-xpath /config/devices/entry[@name='localhost.localdomain']/
 ↪vsys/entry[@name='vsys1']/external-list mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
 ↪profiles to-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/
 ↪entry[@name='vsys1']/profiles mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
 ↪profile-group to-xpath /config/devices/entry[@name='localhost.localdomain']/
 ↪vsys/entry[@name='vsys1']/profile-group mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
 ↪rulebase to-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/
 ↪entry[@name='vsys1']/rulebase mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/network/profiles/zone-
 ↪protection-profile to-xpath /config/devices/entry[@name='localhost.
 ↪localdomain']/network/profiles/zone-protection-profile mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
 ↪shared/reports to-xpath /config/shared/reports mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
 ↪shared/report-group to-xpath /config/shared/report-group mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
 ↪shared/email-scheduler to-xpath /config/shared/email-scheduler mode merge
```

Note: The filename is specific to the iron-skillet templates but can be renamed if the base file is renamed. Simply use

a text editor to replace the template filename with the update name.

Note: For subsequent updates, specific `load config partial` commands can be used.

8.3.5 PAN-OS config elements used in load config partial

Each xpath in the load config partial gives an indication of each element loaded. Below is a simple explanation of the configuration elements with key items in the xml load.

xpath	suffix description
log settings	settings syslog/email profiles and system, configuration logging
tag	referenced tags used in security rules
system	dynamic updates, dns and ntp server settings
setting	Wildfire max file sizes, disable log suppression
address	named references for sinkholes values used in security rules
external list	EDLs referenced in security rules, eg. IPv4/v6 bogons
profiles	Threat, URL Filtering, Wildfire, and decryption profile configurations
profile-group	Group settings for the security profiles, eg. Inbound, Outbound, Alert-All
rulebase	template security and decryption rules
zone protection	recommended zone protection profile
reports	traffic and threat reports
report groups	grouping of reports for viewing and scheduling
email scheduler	email schedule for report groups

8.3.6 Panorama load config partial commands

Cut-and-paste from the table below into the PAN-OS command line while in configuration mode.

You can paste multiple items. The system will pause during each load config partial, return a status message, then move to the next load. When complete, ensure the final load is entered and a status message received.

```
load config partial from iron_skillet_panorama_full.xml from-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/deviceconfig/system to-xpath␣
 ↪/config/devices/entry[@name='localhost.localdomain']/deviceconfig/system␣
 ↪mode merge
load config partial from iron_skillet_panorama_full.xml from-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/deviceconfig/setting to-xpath␣
 ↪/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting␣
 ↪mode merge
load config partial from iron_skillet_panorama_full.xml from-xpath /config/
 ↪panorama/log-settings to-xpath /config/panorama/log-settings mode merge
load config partial from iron_skillet_panorama_full.xml from-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/template to-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/template mode merge
load config partial from iron_skillet_panorama_full.xml from-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/device-group to-xpath /config/
 ↪devices/entry[@name='localhost.localdomain']/device-group mode merge
load config partial from iron_skillet_panorama_full.xml from-xpath /config/
 ↪shared to-xpath /config/shared mode merge
```

```
load config partial from iron_skillet_panorama_full.xml from-xpath /config/
↪devices/entry[@name='localhost.localdomain']/log-collector-group to-xpath␣
↪/config/devices/entry[@name='localhost.localdomain']/log-collector-group␣
↪mode merge
```

Note: The filename is specific to the iron-skillet templates but can be renamed if the base file is renamed. Simply use a text editor to replace the template filename with the update name.

Note: For subsequent updates, specific `load config partial` commands can be used.

8.3.7 Panorama config elements used in load config partial

Each xpath in the load config partial gives an indication of each element loaded. Below is a simple explanation of the configuration elements with key items in the xml load.

This uses an aggregate template loading module with multiple configuration elements contained under the template, device-group, and shared parts of the xml tree. The hierarchical nature of Panorama simplifies the configuration loading.

xpath	suffix description
panorama system	panorama specific dynamic updates, dns and ntp server settings
panorama settings	enable reporting on groups and sharing of unused objects
panorama log settings	syslog/email profiles and system, configuration logging
template	test template configuration with device settings and zone profile
device-group	reports, report groups, and email scheduler
shared	profile object, rules, and other device-group 'top of tree' items
log collector	settings for Panorama when used as a log collector

8.4 Loading Configuration Snippets with Pan-Python

8.4.1 pan-python overview

Pan-python provides a simple command-line model to use the Panorama/PAN-OS API. It leverages the standard xml xpath+element model to push configuration changes to the device. The GitHub repo is found here:

pan-python repo

Training for pan-python including the initial install and getting the device api-key are found here:

pan-python api lab

Before using pan-python, it helps to be familiar with the xpaths used in the template along with the configuration load order. These provide the foundation for the xpath and element references in the examples below.

xpath and snippet load order

8.4.2 pan-python full syntax for loading a config element

The standard entry model is

```
panxapi.py -h {{ ip address }} -K {{ api-key }} -S {{ filename.xml }} "{{ xpath }}"
```

where the elements are:

```
{{ ip address }} is the device ip address
{{ api-key }} is the user/device specific api-key
{{ filename }} is the xml snippet to be loaded
{{ xpath }} is the xpath specific to the config element
```

For example, to load the tag.xml file to ip address 192.168.55.10 and api-key: 12345 would be

```
panxapi.py -h 192.168.55.10 -K 12345 -S tag.xml "/config/devices/entry[@name=
↪'localhost.localdomain']/vsys/entry[@name='vsys1']/tag"
```

or an external list object (aka EDL)

```
panxapi.py -h 192.168.55.10 -K 12345 -S external_list.xml "/config/devices/
↪entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/external-list"
```

Simple scripts can be used to iterate through multiple load requests.

Note: Based on the local pan-python install and use of .panrc you may not require the -h and -K elements and only have to reference the xpath and filename.

Warning: Before loading configurations, use the create_loadable_configs.py tool to create loadable configuration snippets. The templates have `{{ variable }}` elements that must be replaced.

8.5 The Panorama/PAN-OS API and XML

8.5.1 API Overview

For extended reading about the API, you can access the documentation for 8.1 here:

PAN-OS API Reference

Additional information can be found as part of the pan-python documentation:

pan-python api lab

The configuration file and api calls are XML specific. XML is based on XML nodes with the xpath specifying the node in the tree to be referenced. Thus in order to use the API, two configuration items are needed:

1. The xpath pointing to the node to be configured
2. The xml snippet to be used as the element in the configuration

Along with these two items, the IP address of the device and a user-based API are required to modify the configuration.

Note: Each *snippets* directory in templates contains a metadata.yaml file that includes xpath and related file names

CHAPTER 9

VM-50 Security Profile Limits

IronSkillet includes a broad set of security profiles to simplify the usage in security policies. However, the VM-50 limits the number of security profiles that can be configured to 38 resulting in possible commit errors if this limit is exceeded.

Note: If > 49 profiles, the user may see an error message that the number of profiles (39) exceeds capacity (38). This is an error in the message output and the user will have to remove enough profiles for the 38 count limit.

Note: Make sure the firewall is licensed. An unlicensed firewall will allow only 20 profiles, far below what is configured with IronSkillet.

The *delete* commands below can be used to delete security profiles and profile groups from an IronSkillet template load that may not be required for a basic VM-50 configuration yet allow for a reduced number of profiles.

Copy/paste all or part of these commands into the console before any of the profiles or profiles groups are referenced by other items in the configuration. This will leave the Outbound, Inbound, and Alert-Only profiles in the configuration.

This frees up space for nine other security profiles not part of IronSkillet.

```
delete profile-group Internal
delete profiles virus Internal-AV
delete profiles spyware Internal-AS
delete profiles vulnerability Internal-VP
delete profiles file-blocking Internal-FB
delete profiles wildfire-analysis Internal-WF
delete profiles virus Exception-AV
delete profiles spyware Exception-AS
delete profiles vulnerability Exception-VP
delete profiles url-filtering Exception-URL
```

CHAPTER 10

Common or per-device elements

Many of the configuration elements are common between Panorama and panos. The variance is the xpath branch naming where the elements sits in the config tree.

Note: The '*' at the end of a template name denotes multiple files with the same leading text

10.1 Common snippets

These xml files are common across both platforms

- address
- device_setting
- device_system
- email_scheduler_simple
- external_list
- profile_group
- profiles_*
- report_group_simple
- tag
- zone_protection*

The rest are device specific based on xpath reference or configuration settings. Examples are deltas between rule configuration with pre/post in Panorama and log forwarding targets as Panorama or syslog.

10.2 Firewall specific

- log_settings_profiles
- reports_simple
- rulebase_*
- shared_log_settings

10.3 Panorama specific

- device group
- log_collector_group
- log_settings_profiles
- panorama*
- post_rulebase*
- pre_rulebase*
- reports_simple
- shared_log_settings
- templates

CHAPTER 11

Release and Update History

Includes:

- template releases
- tools updates
- documentation revisions

11.1 Template Release History

Template

11.1.1 1.0.5

Released March 18, 2019

Template Content

- added max lines for log csv output

11.1.2 1.0.4

Released January 8, 2019

Template Content

- updated virus profiles from ‘default’ to ‘reset-both’ so explicit blocking
- added set commands template as text file and Excel spreadsheet
- loadable default configurations include full xml and set commands
- update to the template stack snippet including <config> tree elements

11.1.3 1.0.3

Released Oct 3, 2018

Template Content

- added a default security profile group based on the Outbound group
- fixed http-range syntax error in device-setting snippet

Documentation

- fixed errors in the tools installation instructions

11.1.4 1.0.2

Released August 30, 2018

Template Content

- modified device_system type=dhcp configuration elements to fix dhcp-client commit error

11.1.5 1.0.1

Released: August 7, 2018

Template Content

- Device settings updates to increase security hardening
  - Prevent TCP and UDP buffer overflow and multi-part HTTP download evasions
  - Enable high DP load logging
  - Prevent App-ID buffer overflow evasion
  - set bypass-exceed-queue to 'no'
  - Prevent TCP and MPTCP evasions
- Include default login banner
- Correct url-filtering Alert-All profile to include command-and-control
- Set default interzone action to a drop instead of deny
- include firewall management interface options for dhcp-client, standard or cloud models
- include Panorama options for standard or cloud deployments
- using a tag attribute for the template version numbering

Documentation

- moved docs to readthedocs.io
- move to release-specific documentation

Template Archive

- moved to release branch per software release in github

11.1.6 1.0.0

Released: May 10, 2018

- first release on github
- xml snippets and full config
- static pdf documentation

11.2 Tools Release Updates

11.2.1 March 18, 2019

- added instructions to remove security profiles for reduced capacity VM-50
- updated with inclusion of max csv lines for log output

11.2.2 Jan 8, 2019

- moved config variables from a python dictionary to a yaml format
- updated existing tools to support the yaml variables file
- added a utility to create the Excel spreadsheet from the set conf file
- removed the creation of default snippets output to loadable configs
- renamed the output from 'my configs' to 'loadable configs' for clarity

11.2.3 Oct 3, 2018

- modified variable model to support python 3.5 instead of 3.6 and later

11.2.4 August 7, 2018

- added the build_full_config utility to create a full template from the config snippets
- added the build_my_config utility
  - provide simple variable substituions using the my_variable inputs
  - store output into the my_config folder with unique naming

11.2.5 May 3rd, 2019

- fix issues allowing load of panw edl based security rules

11.3 Documentation Revisions

Documentation revisions outside of template-tooling updates. These are documented by date, not verison.

11.3.1 Jan 8, 2019

- simplified repo main README for non-python users
- added documentation for the SET command spreadsheet
- added next-level directory README files for added context
- general edits for using tools based on tools changes
- added description for Panorama template variations in Panorama template docs

11.3.2 Nov 2, 2018

- added instructions for editing the full configuration template variables in the GUI
- added instructions for editing the full configuration template variables using the console

11.3.3 Oct 3, 2018

- fixed errors in the tools installation instructions

11.3.4 August 7, 2018

- moved docs to readthedocs.io
- move to release-specific documentation

11.3.5 May 10, 2018

- first release on github
- static pdf documentation