mssp-templates Documentation

Release 1.0

Palo Alto Networks

Mar 22, 2019

Contents:

CHAPTER 1

MSSP Templates Overview

The Palo Alto Networks MSSP templates are provided to simplify the deployment of security services. Instead of extensive and detailed 'how to' documentation, the MSSP templates provide an easy to implement configuration model.

The benefits of this template model include:

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

For the MSSP, the focus of templating is on the repeatable aspects of deployment. This can include day one starter configs for bespoke deployments, branch deployments, or SMB Internet Gateway offerings bundle with network services.

With the emphasis on repeatability, the templates provided cover:

- Panorama-based internet gateway services
- Direct firewall internet gateway configs (xml and set snippets)
- GPCS core and remote_branch using Panorama
- Sample CPE IPSEC tunnel snippets for GCPS remote networks

1.1 Relationship to the IronSkillet Project

Instead of a complete set of configuration snippets, the MSSP templates are incremental to the IronSkillet day one best practice configurations.

More information about IronSkillet can be found at:

https://iron-skillet.readthedocs.io/en/90dev/

The day one configuration provides reference configurations primarily including security profiles, logging, reporting, device hardening, and dynamic update scheduling. It is use-case agnostic and relies on additional configuration elements such as the MSSP internet gateway templates to be deployment ready.

1.2 Gold-Silver-Bronze Variants

IronSkillet assume that users have all subscriptions (Threat Protection, URL Filtering, Wildfire) enabled to meet the criteria of best practice. However, the MSSP can elect to tier services with incremental price points based on subscriptions.

The template tiers using the generic Gold/Silver/Bronze naming convention provide alignment to subscription tiers:

- Gold: includes all subscriptions (Threat, URL, Wildfire)
- Silver: includes Threat (no URL or Wildfire)
- Bronze: No subscriptions providing for limited or port-based protections

1.3 Using the templates

The templates are available on GitHub at https://github.com/scotchoaf/mssp-templates/tree/90dev.

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
- `set commands` for traditional CLI configuration

1.3.1 PAN-OS 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*.

Note: The spreadsheet set commands are specific to the firewall for sandboxing and non-Panorama deployments. The current Panorama model is focused on API-based xml configuration elements.

1.3.2 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.

CHAPTER 2

What's New

Currently there are no updates to the MSSP template based on the 9.0 software release.

There are however key features used in the IronSkillet 9.0 release:

- New URL filtering multi-tagging categories for risk and newly registered domains
- Addition of the cloud-based DNS signature service
- Support for http/2 in the AntiVirus decode engine
- New Wildfire file type 'script'
- API key lifetime

CHAPTER 3

Internet Gateway 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. The MSSP templates are based on a non-shared model to isolate each customer configuration. Deployments requiring shared or mixed models will need to edit the templates specific to their environment.

The templates are incremental to and reference the IronSkillet day one configurations. The details of the IronSkillet templates can be found at:

https://iron-skillet.readthedocs.io/en/90dev/panorama_template_guide.html.

The .meta-cnc.yaml file in each configuration directory contains:

- list of variables and default values
- load order including the xpaths and snippet file names

Note: SET commands are also included with the panos templates for users requiring quick configuration to sandbox or test. These can also be used for network deployments where Panorama is not leveraged.

3.1 Internet Gateway Baseline

This section provides templated configurations for network elements used by Gold, Silver, and Bronze services.

The Internet gateway deployment is a 2-zone, 2-interface model with IP routing.

3.1.1 Interface settings

Panorama template: internet_gateway_base/interface_template.xml Panorama template: internet_gateway_base/interface_stack.xml

PAN-OS template: internet_gateway_base/interface.xml

Sample interface configurations with one for external/untrust and one internal/trust.

- untrust interface uses DHCP and provides default route inheritance to the internet
- trust interface is uses a static IP configuration
- the interface names and the trust IP address are variables to adjust as needed

---

Note: The Panorama template is an extension of IronSkillet and includes network elements including interfaces and zones. Thus this model uses 2 templates (skillet and internet gateway) with zones and address override in the stack. The internet gateway (ig) template is required to add the interface while the stack is required to associate to a device.

3.1.2 Zones

Panorama template: internet_gateway_base/zone.xml

PAN-OS template: internet_gateway_base/zone.xml

Two zones are provided in the template. The names are variables with default values set to trust and internet.

3.1.3 Vsys Import

Panorama template: internet_gateway_base/vsys_imports.xml

PAN-OS template: internet_gateway_base/vsys_imports.xml

Although not seen in the GUI or CLI configuration, the xml loading requires this mapping to associate interfaces to zones.

3.1.4 Virtual Router

Panorama template: internet_gateway_base/virtual_router.xml

PAN-OS template: internet_gateway_base/virtual_router.xml

The internet gateway deployment uses L3 zones and interfaces so routing configuration is required.

- adds each of the firewall interfaces
- uses inheritance from the DHCP internet interface to create a default gateway route to the internet

3.1.5 Source NAT

Panorama template: internet_gateway_base/source_nat_to_untrust.xml

PAN-OS template: internet_gateway_base/source_nat_to_untrust.xml

Provides dynamic ip and port mapping using the public internet interface address.

3.1.6 Network Profiles

Panorama template: internet_gateway_base/network_profiles.xml

PAN-OS template: internet_gateway_base/network_profiles.xml

Interface management profiles

- sets the interface interface for ping only
- allows for configuration access from the trust interface

Note: Device management will vary by MSSP. It is expected that these profiles will be updated specific to the MSSP management model.

3.2 Gold Template

The gold configuration provides outbound security rules referencing the IronSkillet security profiles and logging. It requires all subscription tiers for full functionality.

3.2.1 Unknown URL Category Profile Group

Panorama template: gold/profile_group_unknown_url.xml

PAN-OS template: gold/profile_group_unknown_url.xml

This adds additional protections with a more aggressive file blocking posture when the URL category is unknown. It is referenced in the gold security rules.

3.2.2 Gold Security Rules

Panorama template: gold/security_rules_gold.xml

PAN-OS template: gold/security_rules_gold.xml

These are outbound-specific rules levering the IronSkillet security profile groups.

- Aggressive file blocking including PE file types when URL category = *unknown*
- Outbound access for all applications using 'application default' port requirements
- Non-defaul SSL ports: allows bypass of app defaults for SSL traffic; tracking for non-standard ports
- Non-default web ports: allows bypass of app defaults for web traffic; tracking for non-standard ports
- Non-default application ports: allows bypass of app defaults for all traffic; tracking for non-standard ports

Warning: The non-default ports effectively allow all outbound traffic on any port. These are provided due to the variance of ports used and for SMB deployments to avoid rampant support calls. The explicit rules provide for hit counts to track and monitor out-of-bounds and suspicious applications.

3.2.3 Gold Tag

Panorama template: gold/tag.xml

PAN-OS template: gold/tag.xml

The gold tag is provided and use by the security rules to view rules associated to the gold service.

3.3 Silver Template

The silver configuration provides outbound security rules referencing the IronSkillet security profiles and logging.

Warning: This tier does not provide support for best-practice security configurations due to the lack of URL Filtering and Wildfire subscriptions. Although the configuraiton from IronSkillet does embed these elements, they are ignored with a commit warning that the license is invalid.

3.3.1 Silver Security Rules

Panorama template: silver/security_rules_silver.xml

PAN-OS template: silver/security_rules_silver.xml

These are outbound-specific rules levering the IronSkillet security profile groups.

- Outbound access for all applications using 'application default' port requirements
- Non-defaul SSL ports: allows bypass of app defaults for SSL traffic; tracking for non-standard ports
- Non-default web ports: allows bypass of app defaults for web traffic; tracking for non-standard ports
- Non-default application ports: allows bypass of app defaults for all traffic; tracking for non-standard ports

Warning: The non-default ports effectively allow all outbound traffic on any port. These are provided due to the variance of ports used and for SMB deployments to avoid rampant support calls. The explicit rules provide for hit counts to track and monitor out-of-bounds and suspicious applications.

3.3.2 Silver Tag

Panorama template: silver/tag.xml

PAN-OS template: silver/tag.xml

The silver tag is provided and use by the security rules to view rules associated to the silver service.

3.4 Bronze Template

The bronze configuration provides outbound security rules referencing the IronSkillet security profiles and logging.

Warning: This tier does not provide support for best-practice security configurations due to the lack of Threat Protection, URL Filtering and Wildfire subscriptions. Although the configuraiton from IronSkillet does embed these elements, they are ignored with a commit warning that the license is invalid.

3.4.1 Bronze Security Rules

Panorama template: bronze/security_rules_bronze.xml

PAN-OS template: bronze/security_rules_bronze.xml

These are outbound-specific rules levering the IronSkillet security profile groups.

- Outbound access for all applications using 'application default' port requirements
- Non-defaul SSL ports: allows bypass of app defaults for SSL traffic; tracking for non-standard ports
- Non-default web ports: allows bypass of app defaults for web traffic; tracking for non-standard ports
- Non-default application ports: allows bypass of app defaults for all traffic; tracking for non-standard ports

Warning: The non-default ports effectively allow all outbound traffic on any port. These are provided due to the variance of ports used and for SMB deployments to avoid rampant support calls. The explicit rules provide for hit counts to track and monitor out-of-bounds and suspicious applications.

Warning: Due to the lack of subscription services, the only active security profile is file-blocking. Customers should consider a service upgrade to increase their security posture.

3.4.2 Bronze Tag

Panorama template: bronze/tag.xml

PAN-OS template: bronze/tag.xml

The bronze tag is provided and use by the security rules to view rules associated to the silver service.

CHAPTER 4

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 spreadsheet can be found at set commands panos

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 5

Global Protect Cloud Service (GPCS) Templates

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

The GPCS templates are provided for 3 deployment needs:

- Initial infrastructure setup configuration
- Addition of remote branch sites
- sample IPSEC tunnel configurations for select CPE vendors

The templates are incremental to and reference the IronSkillet day one configurations. The details of the IronSkillet templates can be found at:

https://iron-skillet.readthedocs.io/en/90dev/panorama_template_guide.html.

The .meta-cnc.yaml files in each configuration directory contain:

- list of variables and default values
- load order including the xpaths and snippet file names

Note: GPCS can only be configured using Panorama. Therefore no PAN-OS only templates are provided.

5.1 Core Service Setup

This section shows the configuration elements to automate the addition of a new GPCS cloud service instance.

(coming soon)

5.1.1 Core Setup

Panorama template: gpcs/something.xml

5.2 Remote Network using IPSEC

This configuration uses the Panorama API interface to configure the 3 elements requires for a new remote site:

- IKE gateway
- IPSEC tunnel
- GPCS plug-in elements

5.2.1 IKE Gateway

Panorama template: gpcs_remote/ike_gateway.xml

A simple reference IKE gateway configuration reference by the IPSEC tunnel.

- include NAT traversal
- simple passphrase connectivity

(have team help with a starter config)

5.2.2 IPSEC Tunnel

Panorama template: gpcs_remote/ipsec_tunnel.xml

A simple reference IPSEC tunnel configuration using the IKE gateway and reference in the GPCS plug-in.

(have team help with a starter config)

5.2.3 GPCS Plug-In Onboarding Configuration

Panorama template: gpcs_remote/onboarding.xml

Onboarding elements for a new remote site including:

- IPSEC tunnel
- remote subnet
- tunnel connect site selection
- bandwidth for remote site connectivity

(have team help with a starter config)

5.3 GPCS CPE Tunnel Configuration

Panorama template: gpcs/cpe_configs

Provides reference configurations for CPE vendor products that will connect back to GPCS

Note: These are sample reference configurations only and not supported by Palo Alto Networks

(work in progress to include)

CHAPTER 6

Template Format

The snippet directories are based on a common modeling including:

- a .meta-cnc.yaml file
- xml config snippets

6.1 The .meta-cnc.yaml file

This file contains descriptive elements for loading the xml snippets using the Panorama or PAN-OS API.

Key elements of the metadata file include:

- name: unique name descriptor specific to the directory contents
- label: can be used by automation tools to create selection menus
- description: what configuration content is contained in the directory
- type: intended use by automation tools to determine API and commit models
- extends: used to reference configurations to be loaded prior to this snippet
- service_type: grouping label for automated selection menus
- variables: variables used in the snippets include defaults and type if used by web utilities
- snippets: ordered list of elements include the xml xpath and file pairing for API configuration

6.2 XML file snippets

A complete set of xml elements to be loaded as part of the temmplate configuration.

- any variables required must be added to the .meta-cnc.yaml file if used by configuration tools
- the filenames are referenced in the snippets section of the .meta-cnc.yaml file

Note: For common xml snippets, relational references can be used to pull xml elements from other directories

CHAPTER 7

Release and Update History

Includes:

- template releases
- tools updates
- documentation revisions

7.1 Template Release History

Template content updates are high level. Details can be found in the template guides.

7.1.1 0.2.0

Released March 15th, 2019

Template Content

- updated yaml files with 9.0 versions
- no local content changes - new features come from IronSkillet 9.0 baseline

0.1.0

Released January 4, 2019

Template Content

- first update with iron-skillet baseline
- Gold/Silver/Bronze with shared internet gateway baseline
- GPCS strawman configuration

7.2 Tools Release Updates

First release based on 8.1 tools and content

7.3 Documentation Revisions

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

Initial content based on 8.1 baseline

7.3.1 Mar 15, 2019

- create 9.0 branch and associated documentation
- update links to 9.0 template branches