PCNSE Bootcamp v10.1

Domain 3 - Deploy and Configure with Panorama

3.1 Configure templates and template stacks

3.1.1 Identify how to use templates and template stacks

- Use Templates to configure items in the Network and Device tabs in Panorama.
- Template stacks give you the ability to layer multiple templates to create a combined configuration.
- Variables can be used as a placeholder to be configured at a later time based on your configuration needs

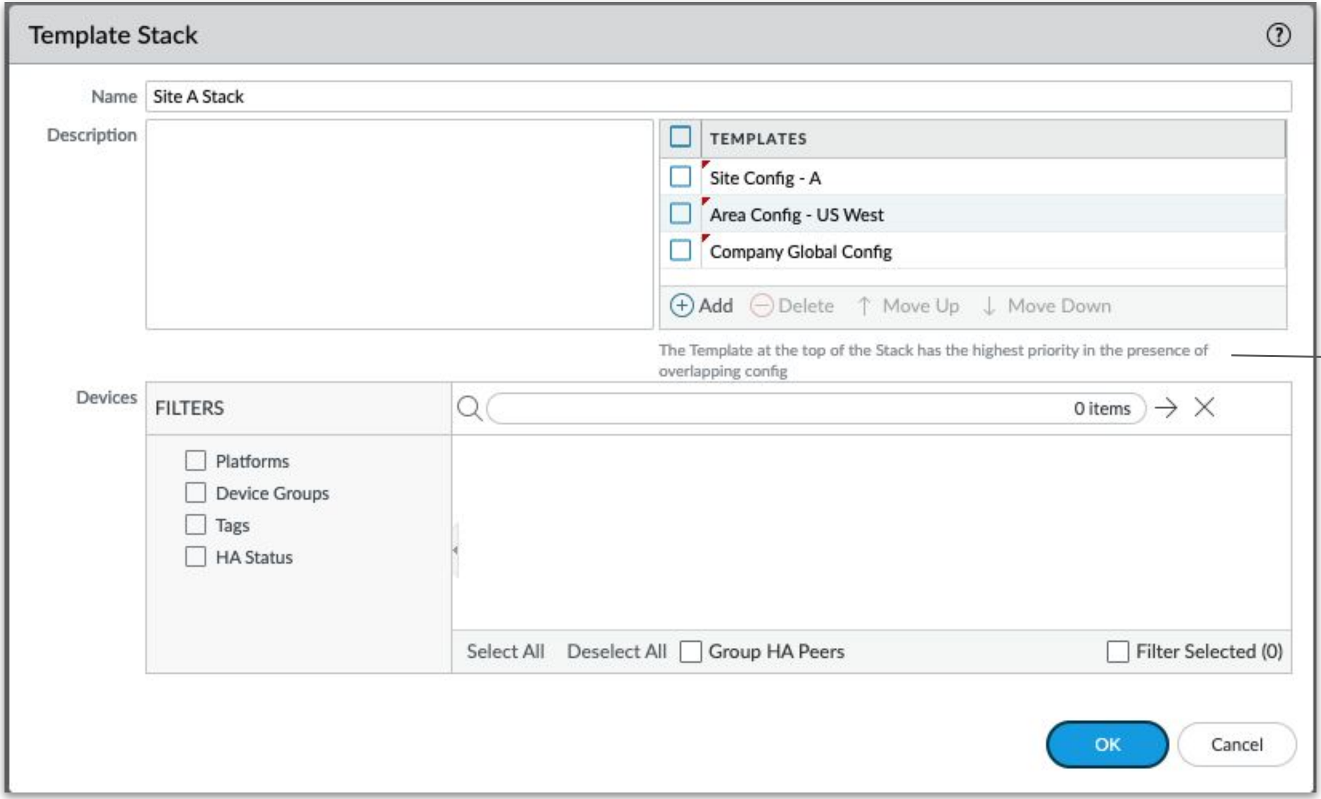
3.1.1 Identify how to use templates and template stacks

You can use Templates and Template Stacks to define a wide array of settings but you can perform the following tasks only locally on each managed firewall:

- Configure a device block list (Network > GlobalProtect > Device Block List) (legacy)
- Clear logs.
- Enable operational modes such as normal mode, multi-vsys mode, or FIPS-CC mode.
- Configure the IP addresses of firewalls in an HA pair (legacy)
- Configure a master key and diagnostics.
- Compare configuration files (Config Audit).
- Renaming a vsys on a multi-vsys firewall.

To Manage Licenses and Updates (software or content) for firewalls, use the **Panorama > Device Deployment** options; do not use templates. (Best Practice)

3.1.2 Identify how the order of templates in a stack affect the configuration push



Template Stack

Name: Site A Stack

Description:

□	TEMPLATES
□	Site Config - A
□	Area Config - US West
□	Company Global Config

The Template at the top of the Stack has the highest priority in the presence of overlapping config

Devices

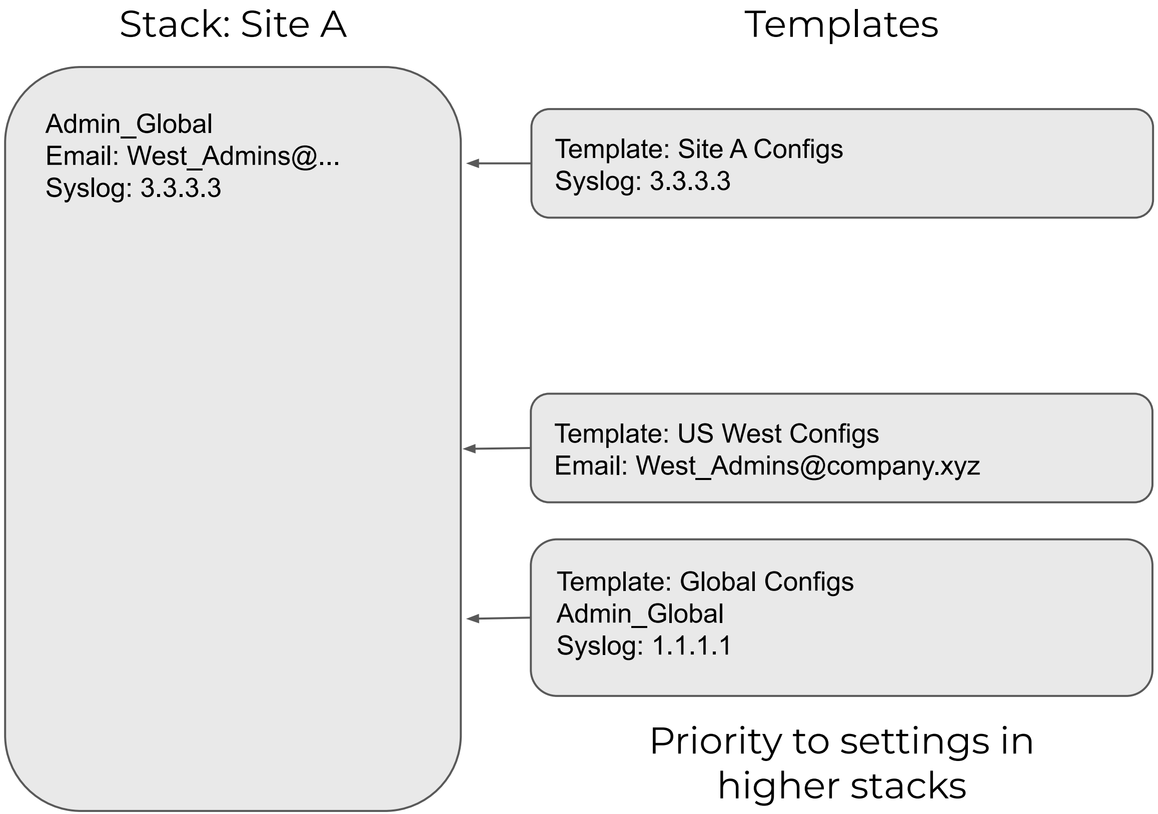
FILTERS

- □ Platforms
- □ Device Groups
- □ Tags
- □ HA Status

The Template at the **top of the Stack has the highest priority** in the presence of overlapping config

Panorama > Templates

3.1.2 Identify how the order of templates in a stack affect the configuration push



Stack: Site A

Admin_Global
Email: West_Admins@...
Syslog: 3.3.3.3

Templates

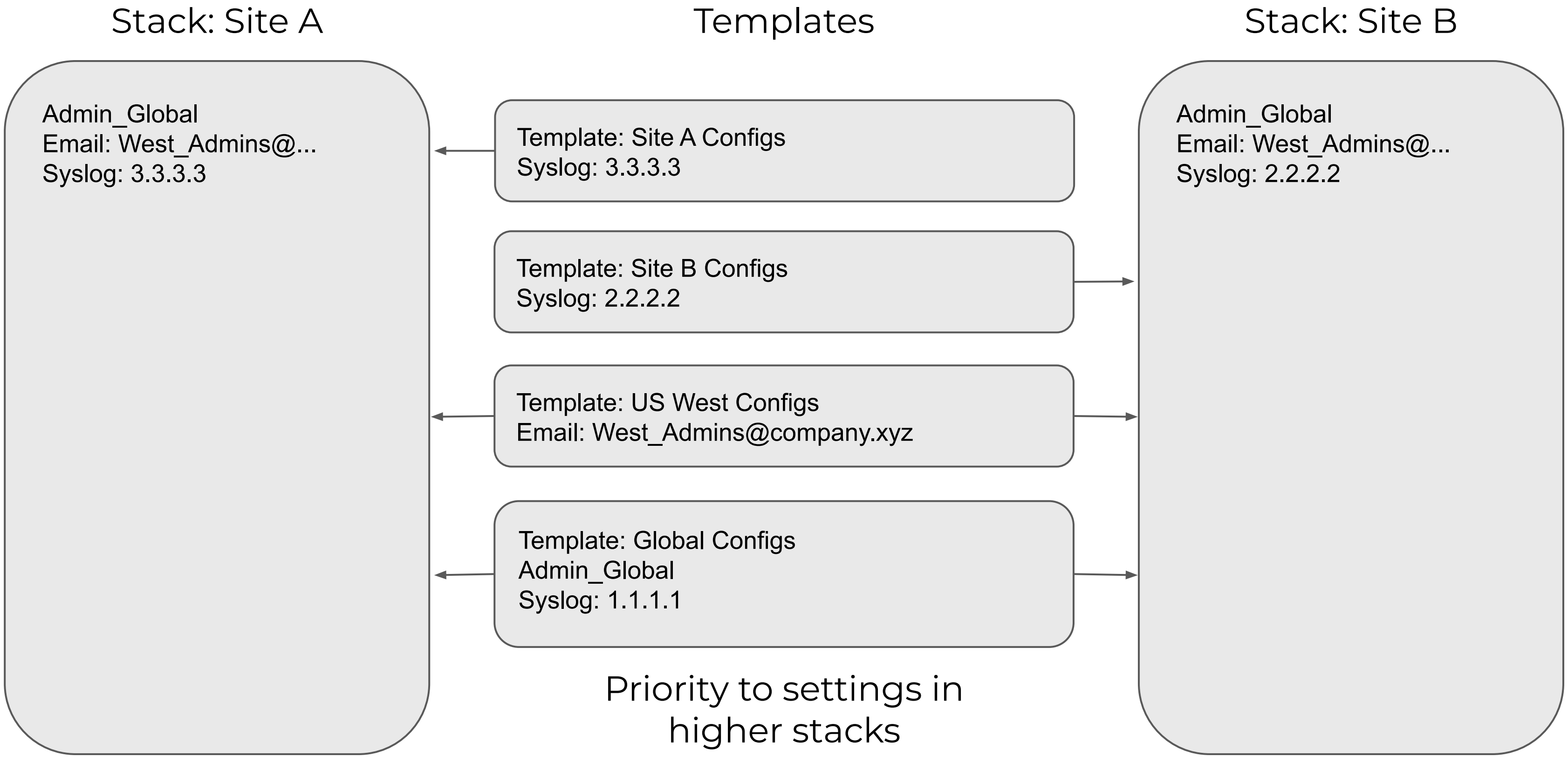
Template: Site A Configs
Syslog: 3.3.3.3

Template: US West Configs
Email: West_Admins@company.xyz

Template: Global Configs
Admin_Global
Syslog: 1.1.1.1

Priority to settings in higher stacks

3.1.2 Identify how the order of templates in a stack affect the configuration push



Stack: Site A

Admin_Global
Email: West_Admins@...
Syslog: 3.3.3.3

Templates

Template: Site A Configs
Syslog: 3.3.3.3

Template: Site B Configs
Syslog: 2.2.2.2

Template: US West Configs
Email: West_Admins@company.xyz

Template: Global Configs
Admin_Global
Syslog: 1.1.1.1

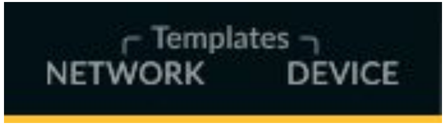
Stack: Site B

Admin_Global
Email: West_Admins@...
Syslog: 2.2.2.2

Priority to settings in higher stacks

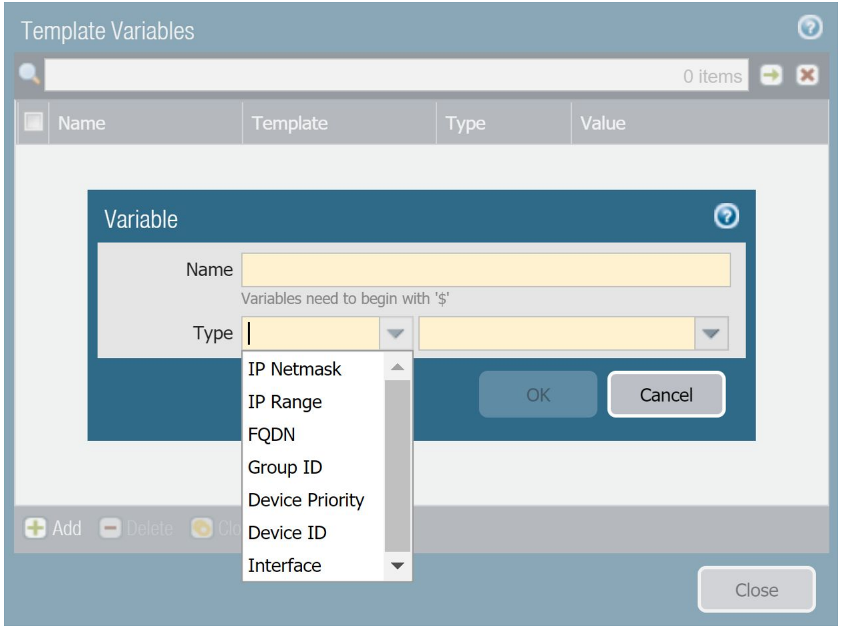
3.1.3 Identify the components configured in a template

- Use Templates and Template stacks to configure the settings that enable firewalls to operate on the network
- Settings in the **Network** and **Device** tabs
    - Examples
        - Zone configurations
        - Server profiles for logging, email, etc.
        - VPN Configurations
- Panorama supports up to 1,024 templates
- Every managed firewall must belong to a template
- Template Network and Device tabs in Panorama don't show up until you create your first Template



3.1.4 Configure variables in templates

- Use variables to make templates/stacks reusable
- Can be used for:
  - IP addresses
  - IP ranges
  - FQDN
  - Interfaces in IKE, VPN, and HA configs
  - Group IDs
- Variables start with $
- Variables in templates override those in template stacks
- Example
  - $DNS-primary
  - $DNS-secondary



Template Variables

0 items

Name	Template	Type	Value

Variable

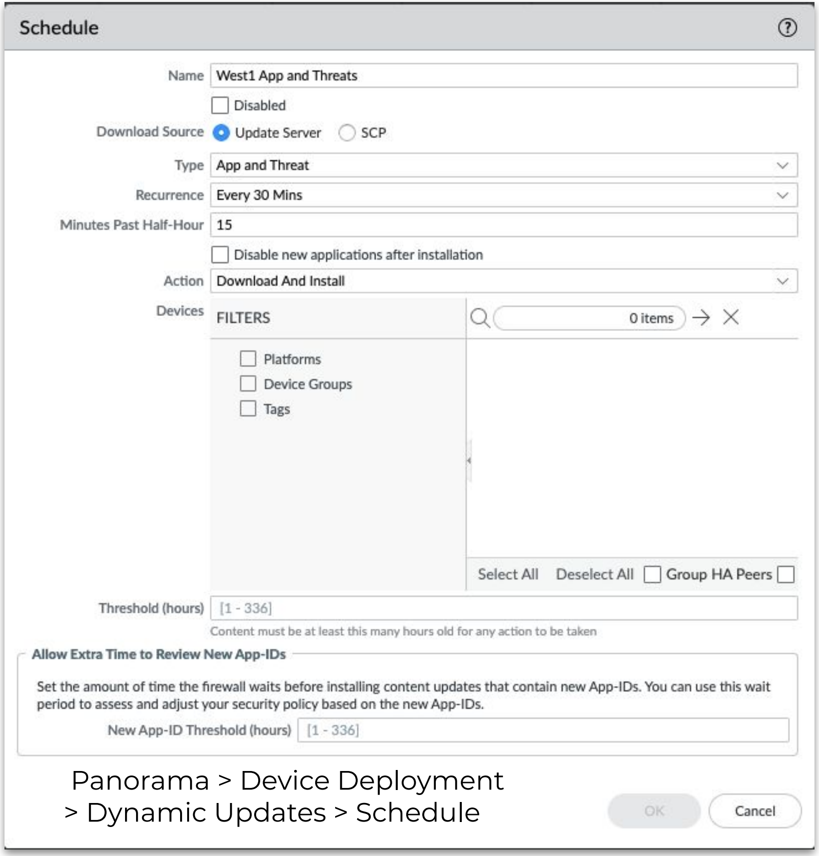
Name

Variables need to begin with '$'

Type

3.1.5 Identify the relationship between Panorama and devices within dynamic updates

- Two options for delivering updates to devices
  - Devices connect directly to update servers per schedule in Template > Device > Dynamic Updates
  - Panorama downloads updates from update server and pushes updates to devices per schedule set in Panorama > Device Deployment > Dynamic Updates



Schedule

Name: West1 App and Threats

□ Disabled

Download Source: ● Update Server ○ SCP

Type: App and Threat

Recurrence: Every 30 Mins

Minutes Past Half-Hour: 15

□ Disable new applications after installation

Action: Download And Install

Devices: FILTERS
□ Platforms
□ Device Groups
□ Tags

0 items

Select All Deselect All □ Group HA Peers □

Threshold (hours): [1 - 336]

Content must be at least this many hours old for any action to be taken

Allow Extra Time to Review New App-IDs

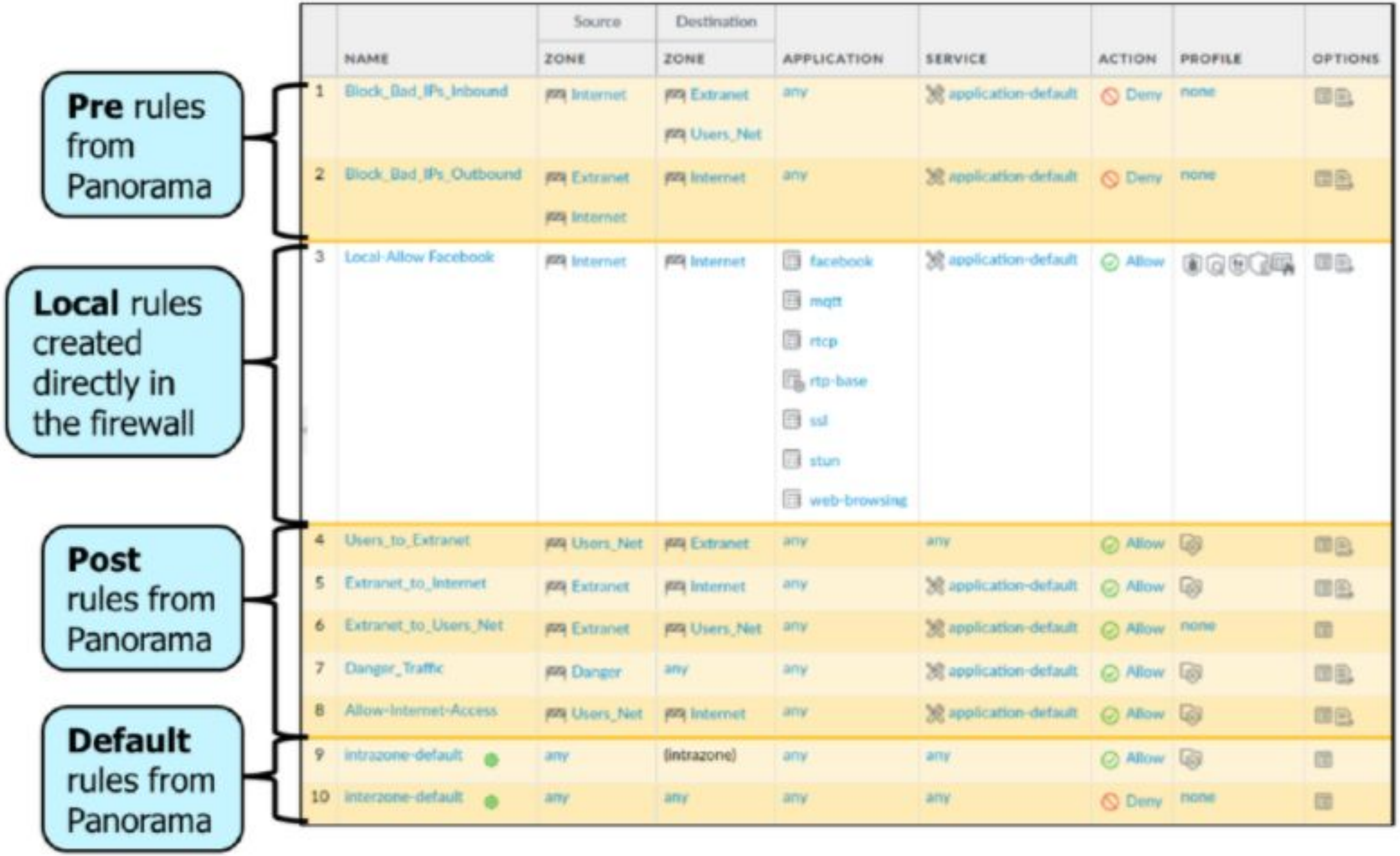
Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.

New App-ID Threshold (hours): [1 - 336]

Panorama > Device Deployment > Dynamic Updates > Schedule

3.2 Configure device groups

3.2.1 Understand device group hierarchies - Policies



Pre rules from Panorama

Local rules created directly in the firewall

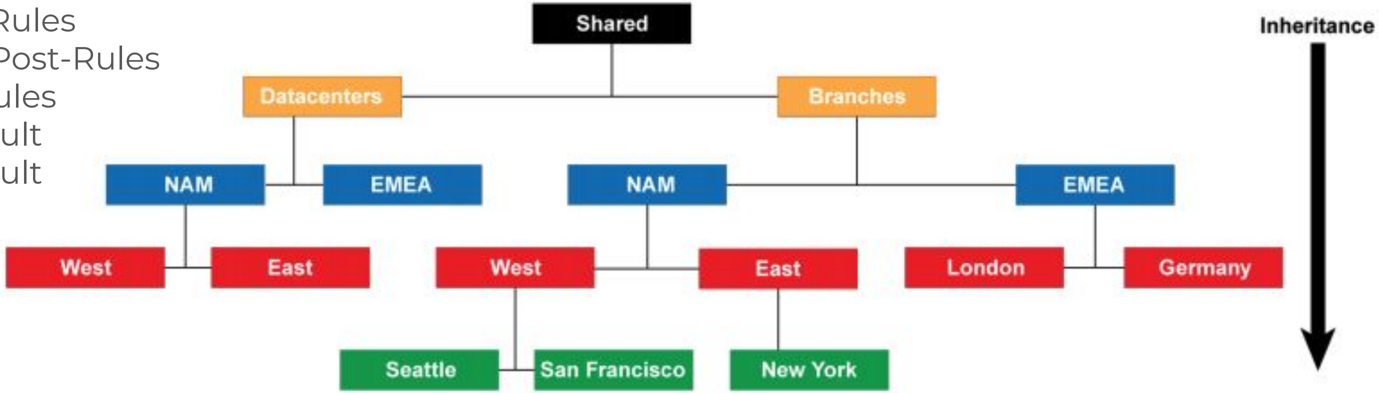
Post rules from Panorama

Default rules from Panorama

		Source	Destination					
	NAME	ZONE	ZONE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	Block_Bad_IPs_Inbound	Internet	Extranet Users_Net	any	application-default	Deny	none	
2	Block_Bad_IPs_Outbound	Extranet Internet	Internet	any	application-default	Deny	none	
3	Local-Allow Facebook	Internet	Internet	facebook mqtt rtcp rtp-base ssl stun web-browsing	application-default	Allow		
4	Users_to_Extranet	Users_Net	Extranet	any	any	Allow		
5	Extranet_to_Internet	Extranet	Internet	any	application-default	Allow		
6	Extranet_to_Users_Net	Extranet	Users_Net	any	application-default	Allow	none	
7	Danger_Traffic	Danger	any	any	application-default	Allow		
8	Allow-Internet-Access	Users_Net	Internet	any	application-default	Allow		
9	intrazone-default	any	(intrazone)	any	any	Allow		
10	interzone-default	any	any	any	any	Deny	none	

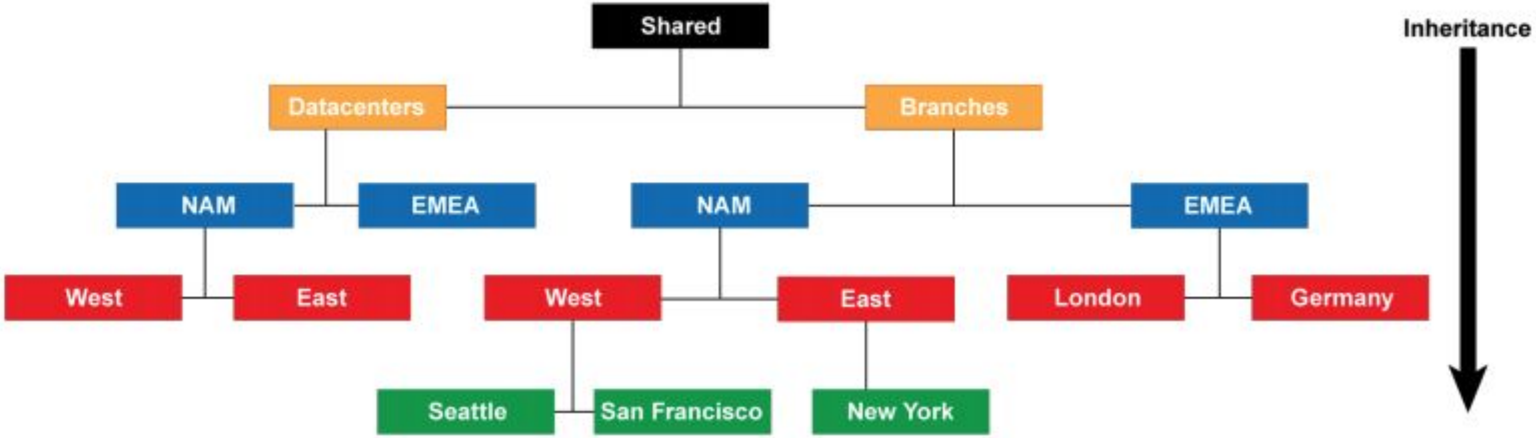
3.2.1 Understand device group hierarchies - Policies

- Remember, NGFWs evaluate rules from left to right, top to bottom
- When considering group hierarchy, highest first, lowest last
  - Lowest is group with no descendants
- Device Group Policies have Pre and Post rules
  - Security Policies include Default Rules too! (interzone and intrazone)
- Evaluation Order
  - Shared Pre-Rules
  - Device Group Pre-Rules
  - Local Firewall Rules
  - Device Group Post-Rules
  - Shared Post-Rules
  - Intrazone-default
  - Interzone-default



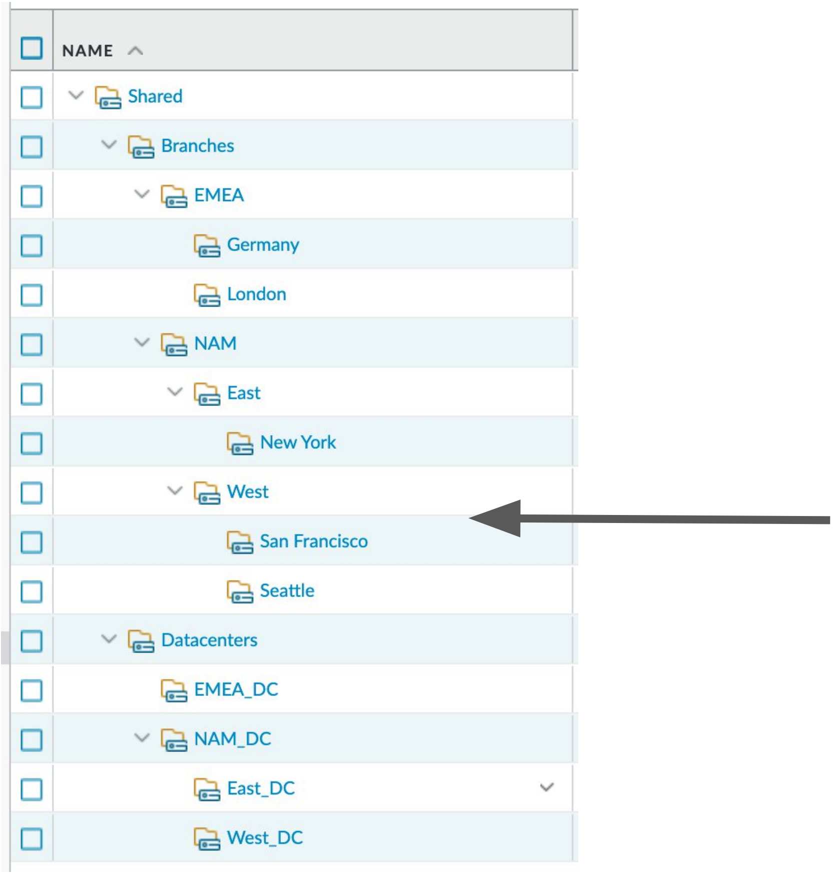
3.2.1 Understand device group hierarchies - Policies

- Assume San Francisco FW 1 (SF-FW1)
- Assume each Device Group has a Security Policy “pre-rule1” and “post-rule1”
- Let’s step through the security policy layout



3.2.1 Understand device group hierarchies

Example in Panorama



□ NAME

- □ Shared
  - □ Branches
    - □ EMEA
      - □ Germany
      - □ London
    - □ NAM
      - □ East
        - □ New York
      - □ West
        - □ San Francisco
        - □ Seattle
  - □ Datacenters
    - □ EMEA_DC
    - □ NAM_DC
      - □ East_DC
      - □ West_DC

3.2.1 Understand device group hierarchies - Policies

Shared pre-rule1

Branches pre-rule1

NAM pre-rule1

West pre-rule1

San Francisco pre-rule1

LOCAL Rules

San Francisco post-rule1

West post-rule1

NAM post-rule1

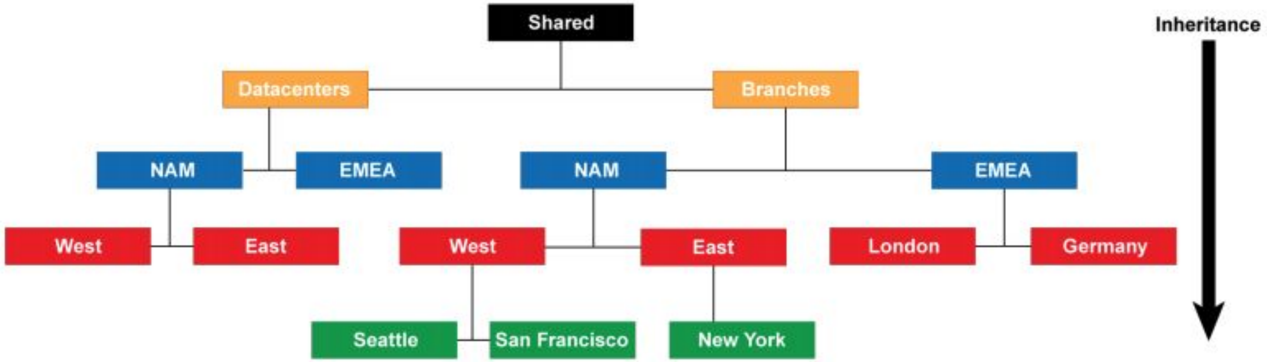
Branches post-rule1

Shared post-rule1

Intrazone-default

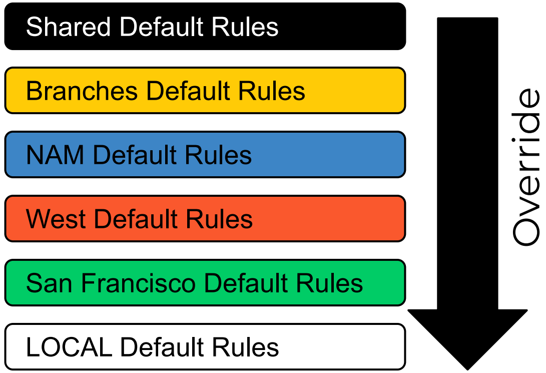
Interzone-default

Let’s talk more about these two



3.2.1 Understand device group hierarchies - Policies

- The default rules apply only to the Security rulebase, and are predefined on Panorama (at the Shared level) and the firewall (in each vsys).
- These rules specify how PAN-OS handles traffic that doesn’t match any other rule.
- The intrazone-default rule allows all traffic within a zone.
- The interzone-default rule denies all traffic between zones.
- If you override default rules, their order of **precedence runs from the lowest context to the highest**:
  - Overridden settings at the firewall level take precedence over settings at the device group level, which take precedence over settings at the Shared level.



Shared Default Rules

Branches Default Rules

NAM Default Rules

West Default Rules

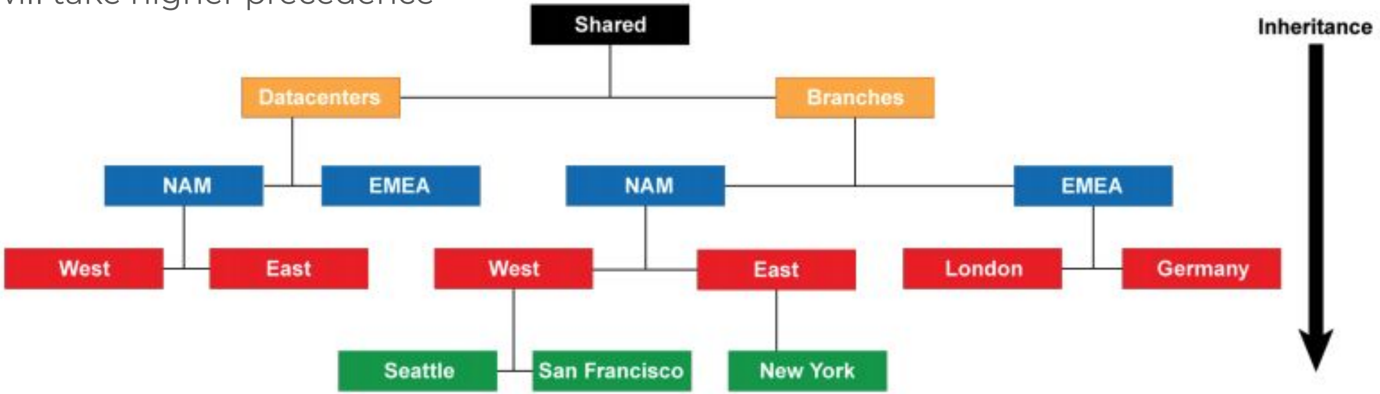
San Francisco Default Rules

LOCAL Default Rules

Override

3.2.1 Understand device group hierarchies - Objects

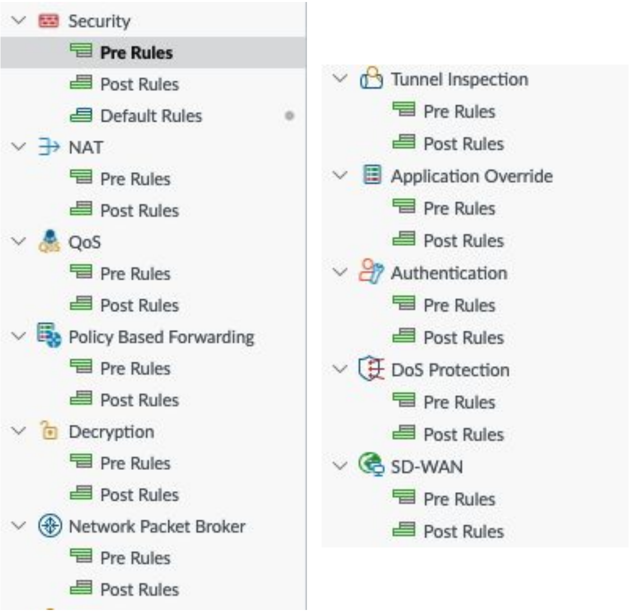
- Objects are configuration elements that policy rules reference, for example: IP addresses, URL categories, security profiles, users, services, and applications.
- By default, when device groups at multiple levels in the hierarchy have an object with the same name but different values (because of overrides, as an example), policy rules in a descendant device group use the object values in that descendant instead of object values inherited from ancestor device groups or Shared.
- Optionally, you can reverse this order of precedence to push values from Shared or the highest ancestor containing the object to all descendant device groups.
  - Panorama > Setup > Management > Edit Panorama Settings: Select Objects defined in ancestors will take higher precedence



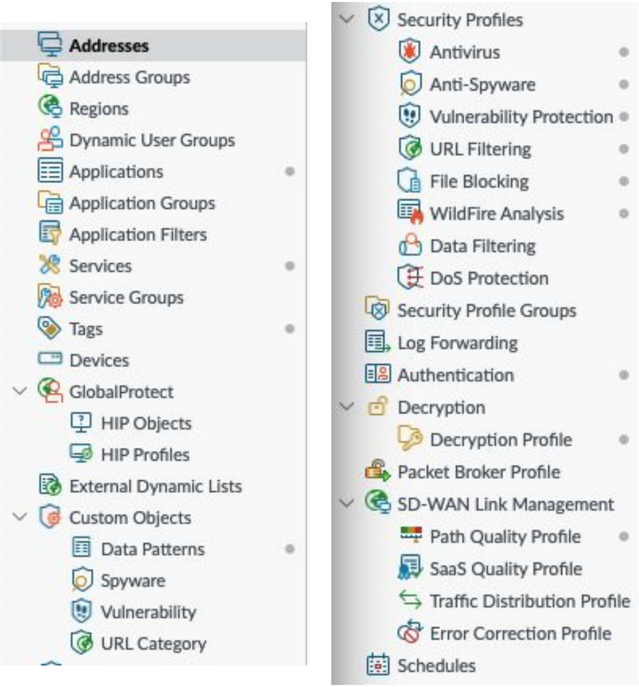
3.2.2 Identify what device groups contain

- Configure policy rules and the objects they reference

Policies



Objects



3.2.3 Differentiate between different use cases for pre-rules and post-rules

- Pre Rules
  - You can use pre-rules to enforce the acceptable use policy of an organization. For example, a pre-rule might block access to specific URL categories or allow Domain Name System (DNS) traffic for all users.
- Post Rules
  - Post-rules typically include rules to deny access to traffic based on the App-ID™ signatures, User-ID™ information (users or user groups), or service.

3.3 Manage firewall configurations within Panorama

3.3.1 Identify how the Panorama commit recovery feature operates

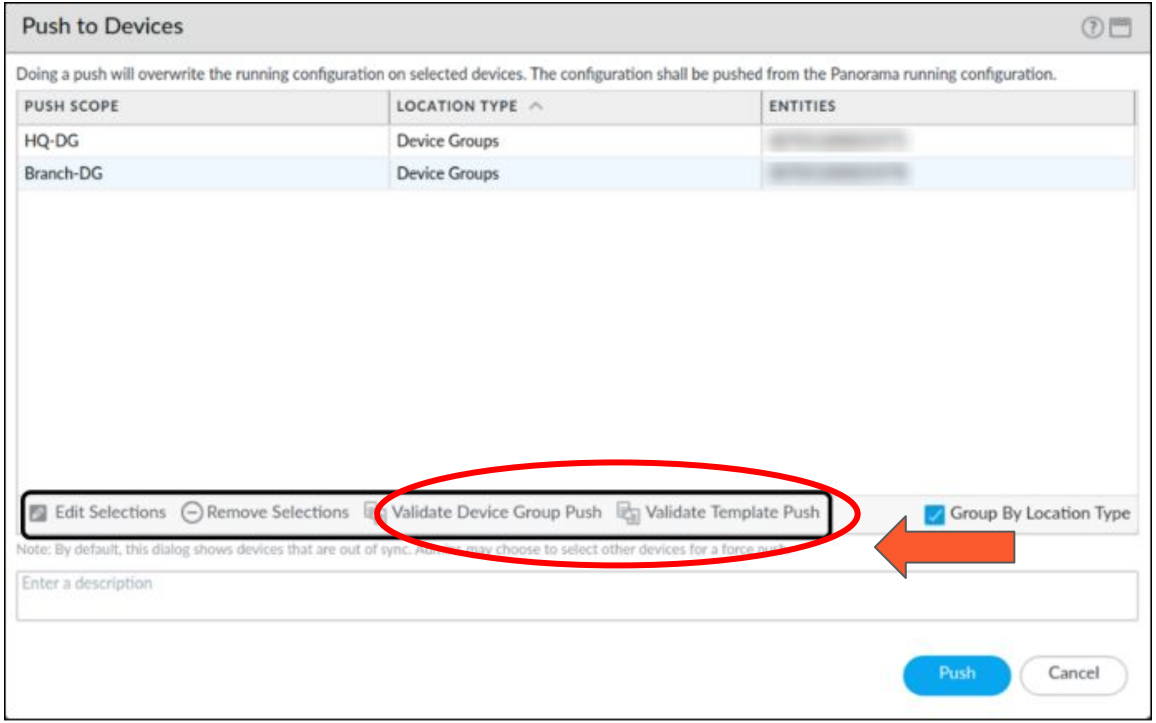
- When you initiate a commit, Panorama **checks the validity of the changes** before activating them.

- The validation output displays conditions that block the commit (errors) or that are important to know (warnings). For example, validation could indicate an invalid route destination that you need to fix for the commit to succeed.

- The **validation process enables you to find and fix errors before you commit** because no changes to the running configuration are made. This is useful if you have a fixed commit window and want to be sure the commit will succeed without errors.

3.3.1 Understand Validity checks

Select Edit Selections at the bottom of the window to get a granular selection of the data to be pushed



Doing a push will overwrite the running configuration on selected devices. The configuration shall be pushed from the Panorama running configuration.

PUSH SCOPE	LOCATION TYPE	ENTITIES
HQ-DG	Device Groups	[redacted]
Branch-DG	Device Groups	[redacted]

☑ Group By Location Type

Note: By default, this dialog shows devices that are out of sync. Admins may choose to select other devices for a force push.

3.3.2 Identify the configuration settings for Panorama automatic commit recovery

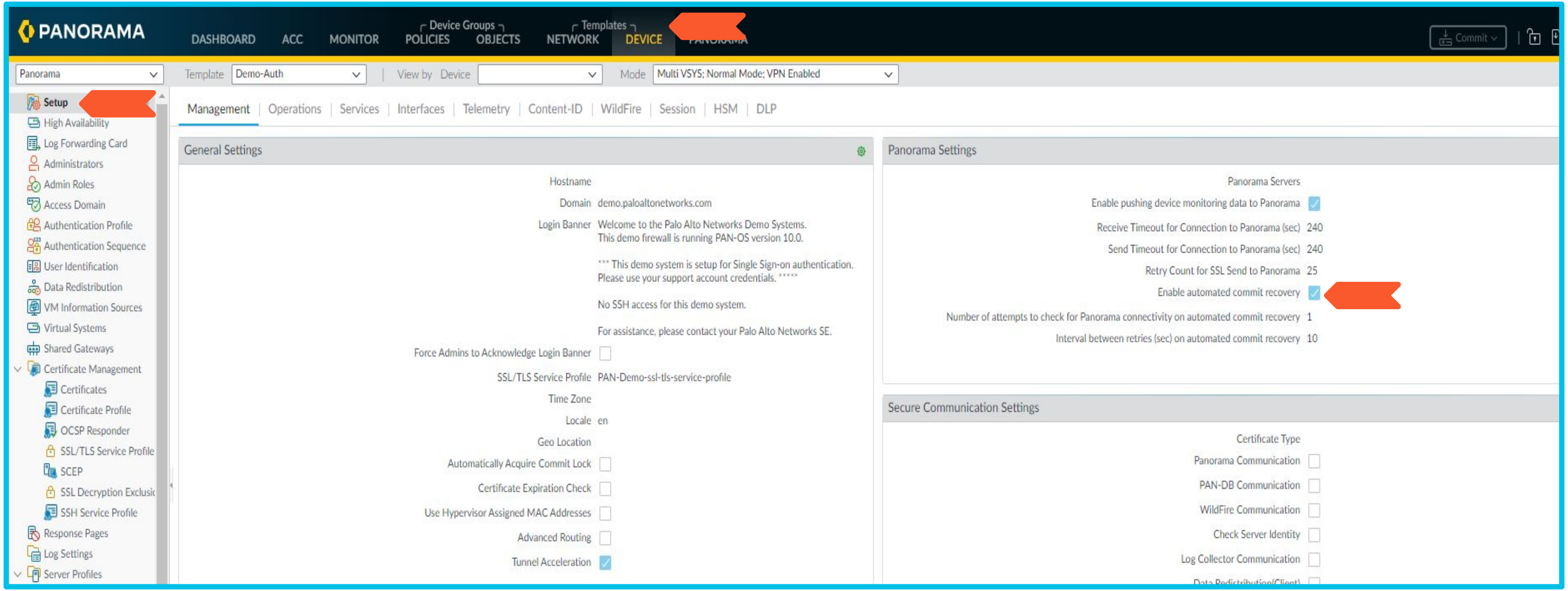
- PAN-OS has the ability for managed firewalls to check for connectivity to the Panorama management server and to automatically revert to the last running configuration when the firewall is unable to communicate with Panorama.

- **Automatic commit recovery** enables you to configure the firewall to attempt a specified number of connectivity tests and the interval at which each test occurs before the managed firewall automatically reverts its configuration to the previous running configuration after you push a configuration from Panorama or commit a configuration change locally on the firewall.

- The firewall also checks connectivity to Panorama every hour to ensure consistent communication if unrelated network configuration changes have disrupted connectivity between the firewall and Panorama or if implications to a pushed committed configuration have affected connectivity.

- If an hourly connectivity check fails, the firewall generates a system log to alert an administrator of a potential configuration or network connectivity issues.

3.3.2 Identify the configuration settings for Panorama automatic commit recovery



Panorama | Template: Demo-Auth | View by Device | Mode: Multi VSYS; Normal Mode; VPN Enabled

General Settings

Hostname

Domain: demo.paloaltonetworks.com

Login Banner: Welcome to the Palo Alto Networks Demo Systems.
This demo firewall is running PAN-OS version 10.0.

*** This demo system is setup for Single Sign-on authentication.
Please use your support account credentials. *****

No SSH access for this demo system.

For assistance, please contact your Palo Alto Networks SE.

Force Admins to Acknowledge Login Banner ☐

SSL/TLS Service Profile: PAN-Demo-ssl-tls-service-profile

Time Zone

Locale: en

Geo Location

Automatically Acquire Commit Lock ☐

Certificate Expiration Check ☐

Use Hypervisor Assigned MAC Addresses ☐

Advanced Routing ☐

Tunnel Acceleration ☑

Panorama Settings

Panorama Servers

Enable pushing device monitoring data to Panorama ☑

Receive Timeout for Connection to Panorama (sec): 240

Send Timeout for Connection to Panorama (sec): 240

Retry Count for SSL Send to Panorama: 25

Enable automated commit recovery ☑

Number of attempts to check for Panorama connectivity on automated commit recovery: 1

Interval between retries (sec) on automated commit recovery: 10

Secure Communication Settings

Certificate Type

Panorama Communication ☐

PAN-DB Communication ☐

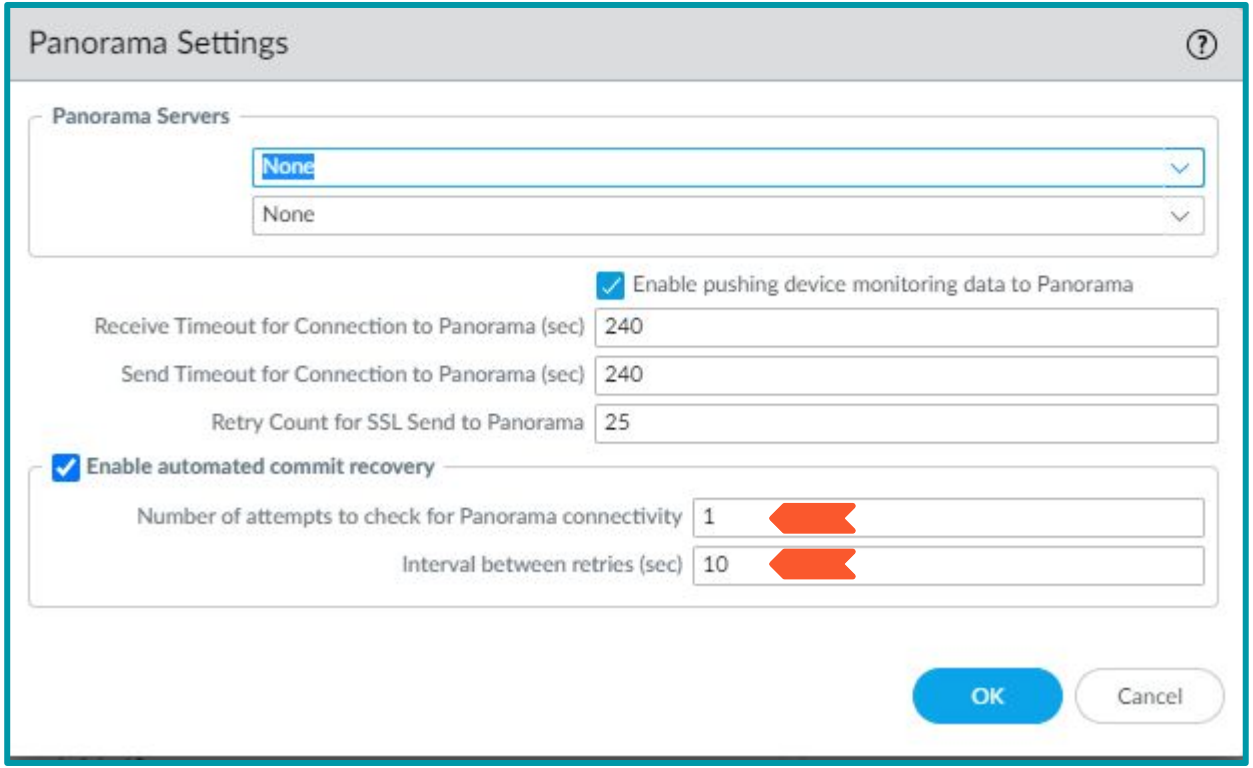
WildFire Communication ☐

Check Server Identity ☐

Log Collector Communication ☐

Data Redistribution(Client) ☐

3.3.2 Identify the configuration settings for Panorama automatic commit recovery



Panorama Settings

Panorama Servers

None

None

☑ Enable pushing device monitoring data to Panorama

Receive Timeout for Connection to Panorama (sec) 240

Send Timeout for Connection to Panorama (sec) 240

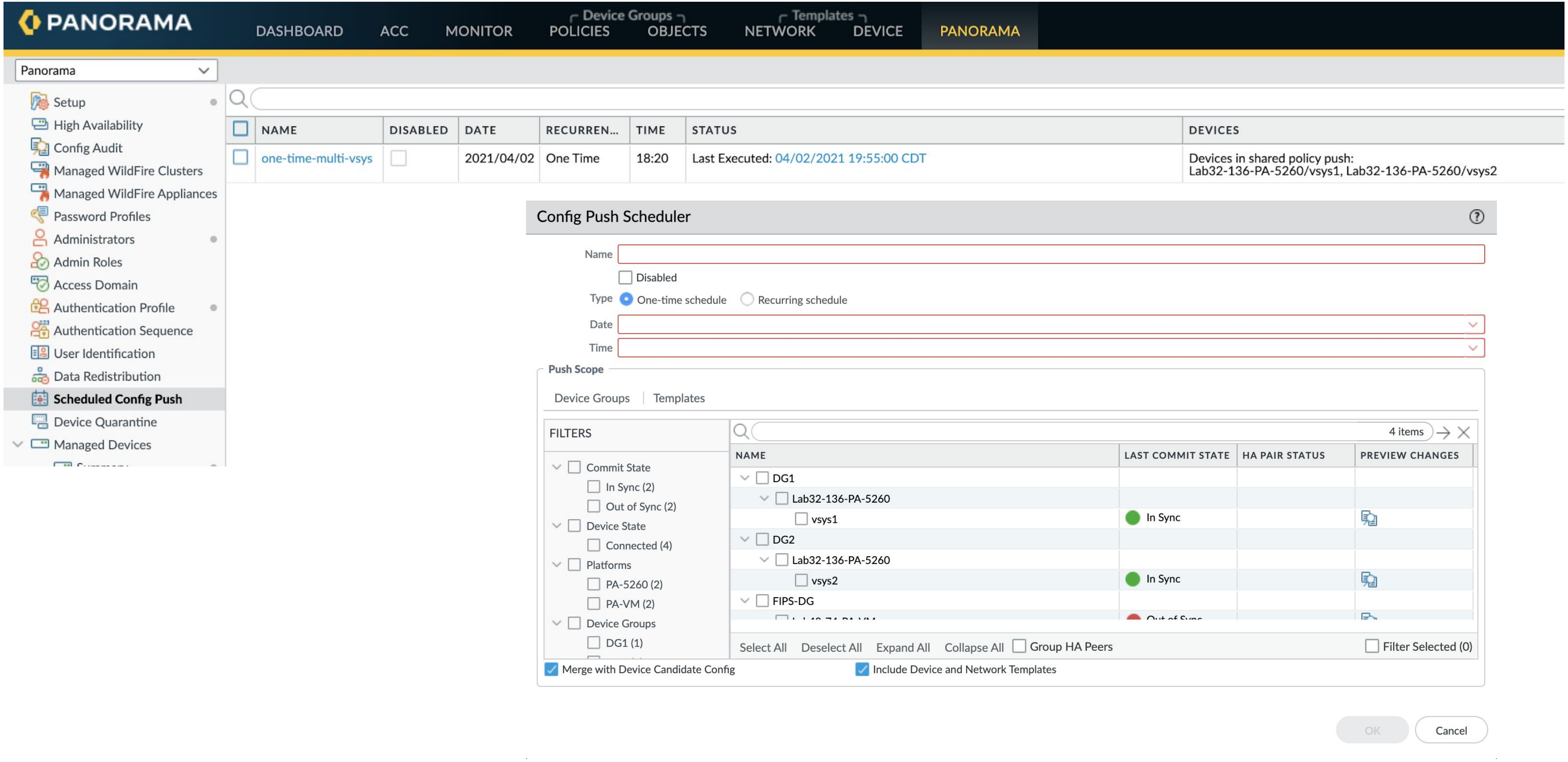
Retry Count for SSL Send to Panorama 25

☑ Enable automated commit recovery

Number of attempts to check for Panorama connectivity 1

Interval between retries (sec) 10

3.3.3 Configure Scheduled push to Devices



□	NAME	DISABLED	DATE	RECURREN...	TIME	STATUS	DEVICES
□	one-time-multi-vsys	□	2021/04/02	One Time	18:20	Last Executed: 04/02/2021 19:55:00 CDT	Devices in shared policy push: Lab32-136-PA-5260/vsys1, Lab32-136-PA-5260/vsys2

Config Push Scheduler

Name

□ Disabled

Type ● One-time schedule ○ Recurring schedule

Date

Time

Push Scope

- □ Commit State
  - □ In Sync (2)
  - □ Out of Sync (2)
- □ Device State
  - □ Connected (4)
- □ Platforms
  - □ PA-5260 (2)
  - □ PA-VM (2)
- □ Device Groups
  - □ DG1 (1)

NAME	LAST COMMIT STATE	HA PAIR STATUS	PREVIEW CHANGES
□ DG1			
□ Lab32-136-PA-5260			
□ vsys1	● In Sync		
□ DG2			
□ Lab32-136-PA-5260			
□ vsys2	● In Sync		
□ FIPS-DG			

□ Group HA Peers

□ Filter Selected (0)

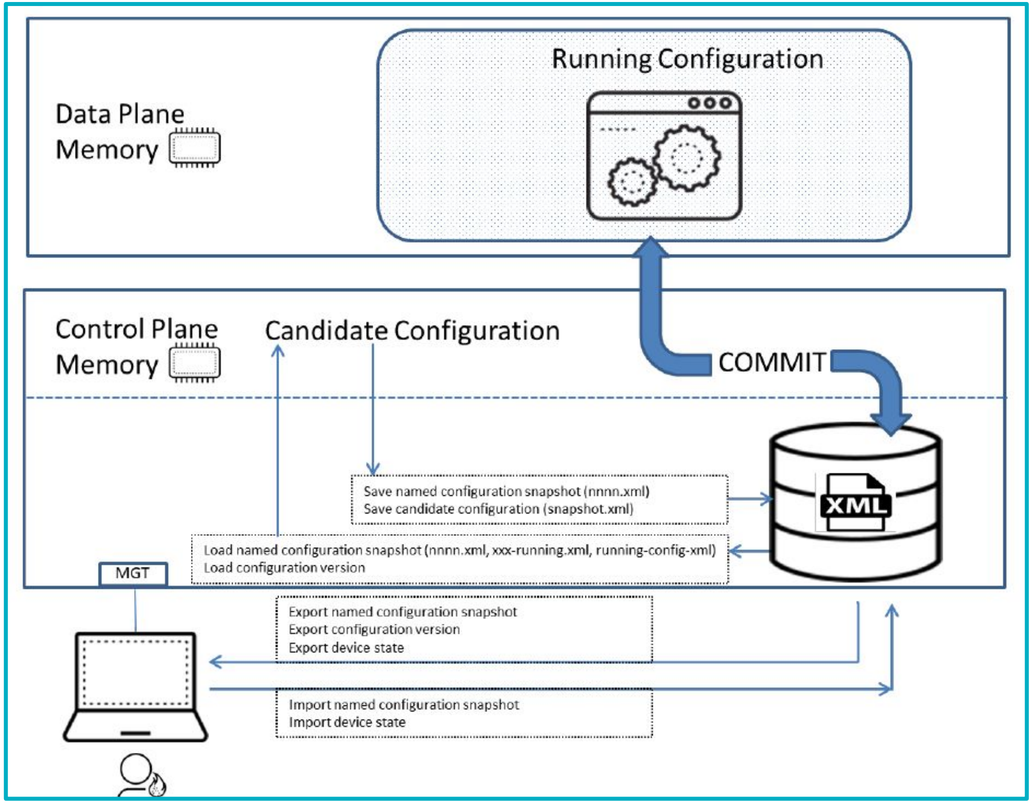
☑ Merge with Device Candidate Config

☑ Include Device and Network Templates

3.3.3 Configure Scheduled push to Devices

- Schedules can be created irrespective of the device status
- Schedule push will only happen to out-of-sync devices.
- Last DG/TPL config available will be picked incase of a conflict job
- Scheduled push happens at local time to Panorama
- Schedule changes requires a commit
- DG/TPL push for devices can overlap across schedules
- Optimized push if DG/TPL push is scheduled at the same time to the same device
- A multi-vsys device can belong to different schedules

3.3.4 Manage Configuration Backups


Running Configuration
Data Plane Memory
Control Plane Memory
Candidate Configuration
COMMIT
XML
MGT
Save named configuration snapshot (nnnn.xml)
Save candidate configuration (snapshot.xml)
Load named configuration snapshot (nnnn.xml, xxx-running.xml, running-config-xml)
Load configuration version
Export named configuration snapshot
Export configuration version
Export device state
Import named configuration snapshot
Import device state

Running Configuration and Candidate Configuration

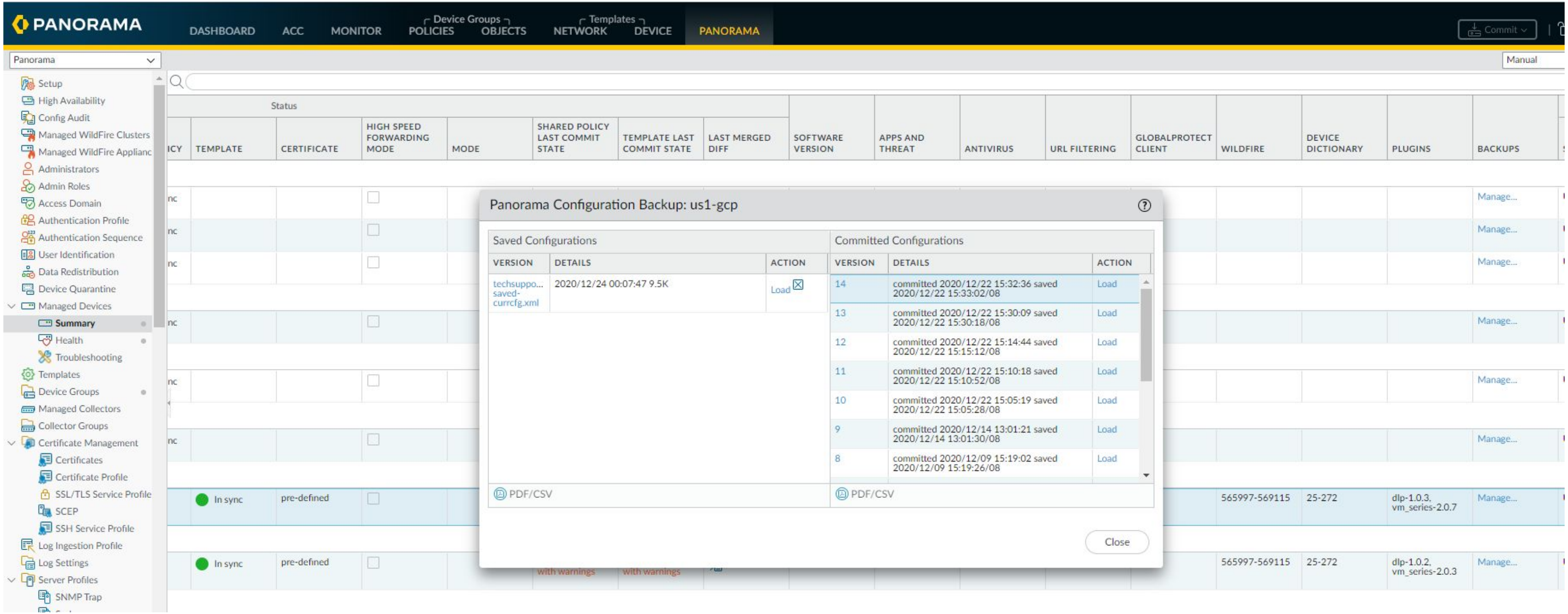
- Firewall settings are stored in XML configuration files that can be archived, restored, and otherwise managed.
- A firewall contains both a running configuration that contains all settings currently active, and a candidate configuration. The candidate configuration is a copy of the running configuration that also includes settings changes that are not yet committed.
- Changes you make using the management web interface, the CLI, or the XML API are staged in the candidate configuration until you perform a commit operation.
- During a commit operation, the candidate configuration replaces the running configuration

3.3.4 Manage Configuration Backups

Panorama and Firewall Configuration Backups and Restorations

- When a Panorama has a management relationship with a firewall, the Panorama can obtain copies of both that firewall’s Panorama managed and locally managed configurations.
- After a commit on a local firewall that runs PAN-OS 5.0 or later, a backup is sent of the running configuration to Panorama.
- Any commits performed on the local firewall will trigger the backup, including any commits that an administrator performs locally on the firewall or that PAN-OS initiates and automatically commits (such as an FQDN refresh).
- By default, Panorama stores up to 100 backups for each firewall, though this is configurable.
- To store Panorama and firewall configuration backups on an external host, you can schedule exports from Panorama or complete an export on demand.
- These saved configuration files can be restored to the firewall at any time by a Panorama administrator using the Panorama > Managed Devices > Summary tools

3.3.4 Manage Configuration Backups



Panorama Configuration Backup: us1-gcp

Saved Configurations

VERSION	DETAILS	ACTION
techsuppo... saved-currcfg.xml	2020/12/24 00:07:47 9.5K	Load ☒

PDF/CSV

Committed Configurations

VERSION	DETAILS	ACTION
14	committed 2020/12/22 15:32:36 saved 2020/12/22 15:33:02/08	Load
13	committed 2020/12/22 15:30:09 saved 2020/12/22 15:30:18/08	Load
12	committed 2020/12/22 15:14:44 saved 2020/12/22 15:15:12/08	Load
11	committed 2020/12/22 15:10:18 saved 2020/12/22 15:10:52/08	Load
10	committed 2020/12/22 15:05:19 saved 2020/12/22 15:05:28/08	Load
9	committed 2020/12/14 13:01:21 saved 2020/12/14 13:01:30/08	Load
8	committed 2020/12/09 15:19:02 saved 2020/12/09 15:19:26/08	Load

PDF/CSV

Close

3.3.4 Manage Configuration Backups

RMA Replacement of a Panorama-Managed Firewall

To minimize the effort required to restore the configuration on a managed firewall, you can use a Return Merchandise Authorization (RMA) to replace the serial number of the old firewall with that of the new firewall on Panorama.

To then restore the configuration on the replacement firewall, either import a firewall state that you previously generated and exported from the firewall or use Panorama
to generate a partial device state for managed firewalls running PAN-OS 5.0 and later versions.

By replacing the serial number and importing the firewall state, you can resume using Panorama to
manage the firewall.

KB article : How to configure RMA replacement firewall

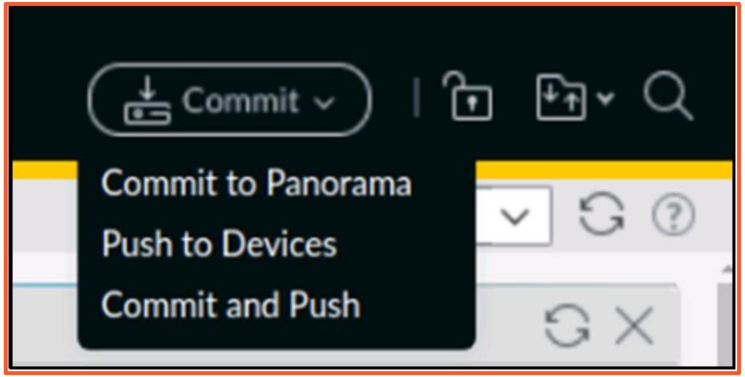
3.3.5 Understand various Commit options

Committing Changes with Panorama

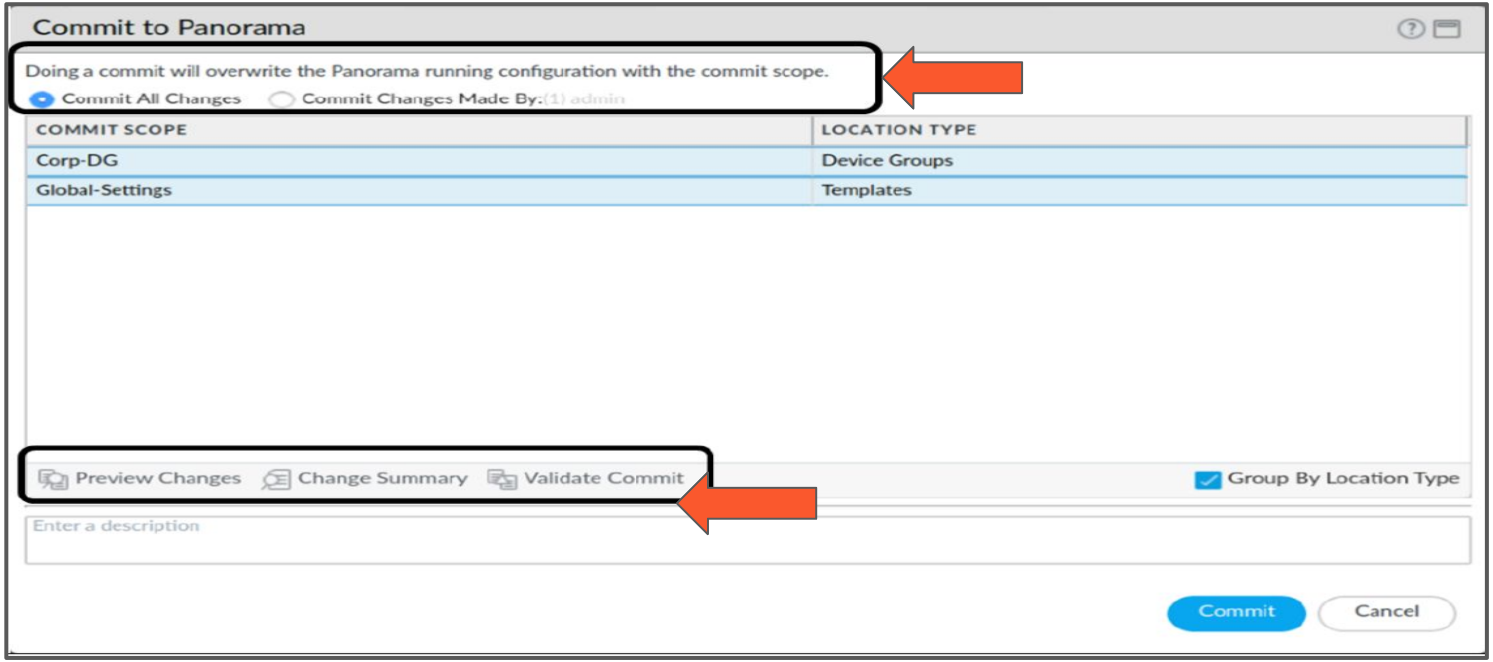
Panorama uses a similar commit concept to firewalls but uses a process with multiple phases. After changes have been made in Panorama, data must first be committed to Panorama and then pushed to devices.

Both processes provide methods to push partial data.

A commit to Panorama commits either the changes made by a chosen admin or all staged changes, as shown in the following figure



3.3.5 Understand various Commit options



Commit to Panorama

Doing a commit will overwrite the Panorama running configuration with the commit scope.

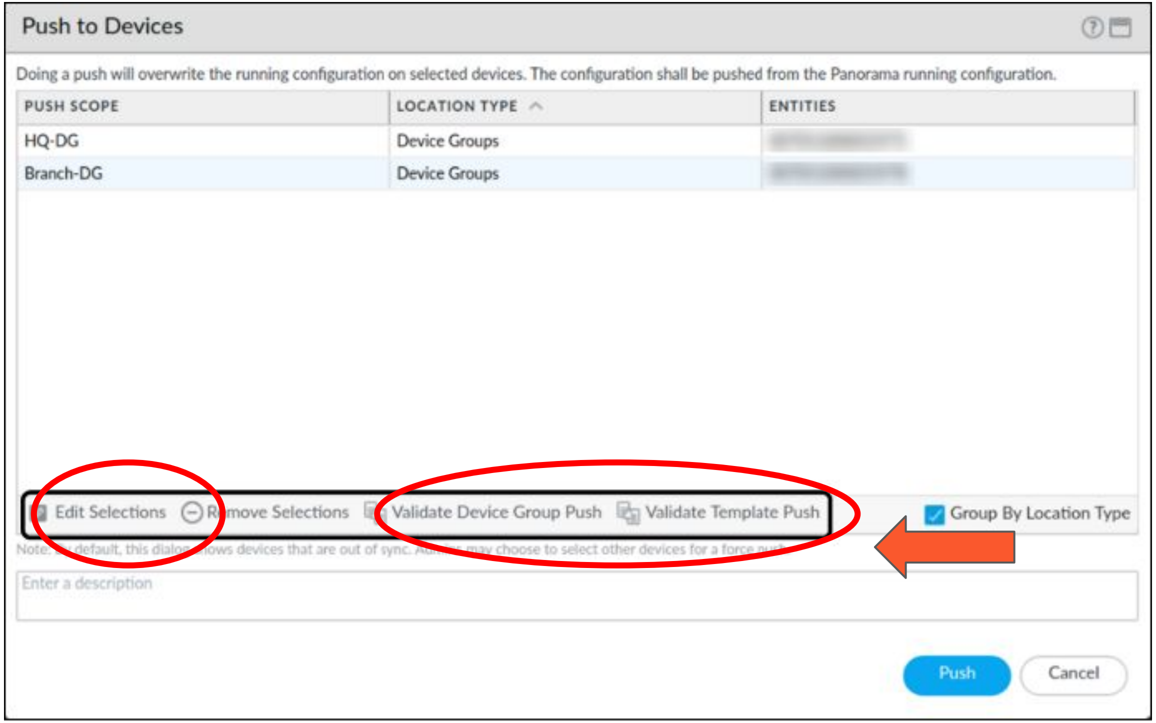
● Commit All Changes ○ Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE
Corp-DG	Device Groups
Global-Settings	Templates

After changes are committed to Panorama, they are pushed to firewalls according to their assigned device groups and template stacks. This push process either can push all queued changes or be done selectively for specific device groups or template stacks. And specific firewalls can be chosen for the update.

3.3.5 Understand various Commit options

Select Edit Selections at the bottom of the window to get a granular selection of the data to be pushed



Push to Devices

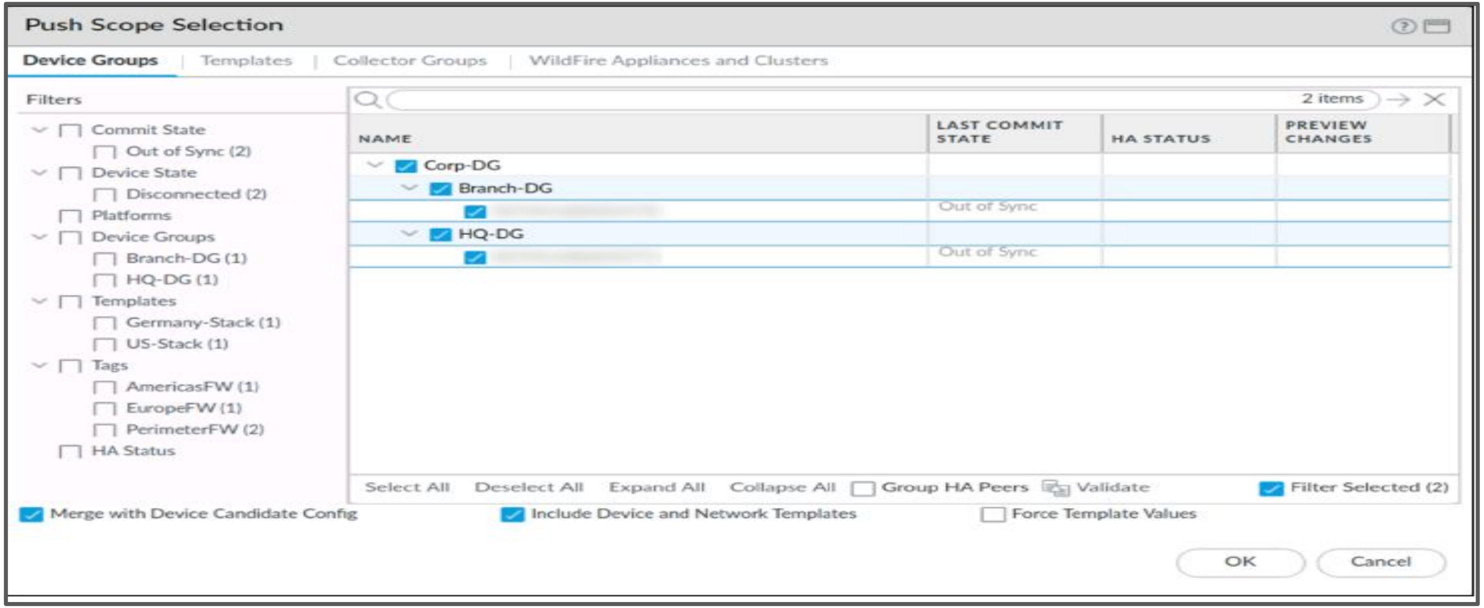
Doing a push will overwrite the running configuration on selected devices. The configuration shall be pushed from the Panorama running configuration.

PUSH SCOPE	LOCATION TYPE	ENTITIES
HQ-DG	Device Groups	[redacted]
Branch-DG	Device Groups	[redacted]

Note: By default, this dialog shows devices that are out of sync. Admins may choose to select other devices for a force push.

Enter a description

3.3.5 Understand various Commit options



Filters

- ☐ Commit State
  - ☐ Out of Sync (2)
- ☐ Device State
  - ☐ Disconnected (2)
- ☐ Platforms
- ☐ Device Groups
  - ☐ Branch-DG (1)
  - ☐ HQ-DG (1)
- ☐ Templates
  - ☐ Germany-Stack (1)
  - ☐ US-Stack (1)
- ☐ Tags
  - ☐ AmericasFW (1)
  - ☐ EuropeFW (1)
  - ☐ PerimeterFW (2)
- ☐ HA Status

NAME	LAST COMMIT STATE	HA STATUS	PREVIEW CHANGES
☑ Corp-DG			
☑ Branch-DG			
☑ [redacted]	Out of Sync		
☑ HQ-DG			
☑ [redacted]	Out of Sync		

☐ Group HA Peers

☑ Filter Selected (2)

☑ Merge with Device Candidate Config

☑ Include Device and Network Templates

☐ Force Template Values

3.3.6 References

Panorama Commit, Validation, and Preview Operations
https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/panorama-overview/panoramacommit-validation-and-preview-operations.html
Enable Automatic Commit Recovery
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administer-panorama/enableautomated-commit-recovery
Manage Configuration Backups
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/firewall-administration/manageconfiguration-backups.html
Manage Panorama and Firewall Configuration Backups
https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/administer-panorama/managepanorama-and-firewall-configuration-backups.html
Replace an RMA Firewall
https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/troubleshooting/replace-an-rmafirewall.html
Backing Up and Restoring Configurations
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRcCAK