



Cybersecurity  
Partner of Choice

**Palo Alto Networks**

# SCM Config Management

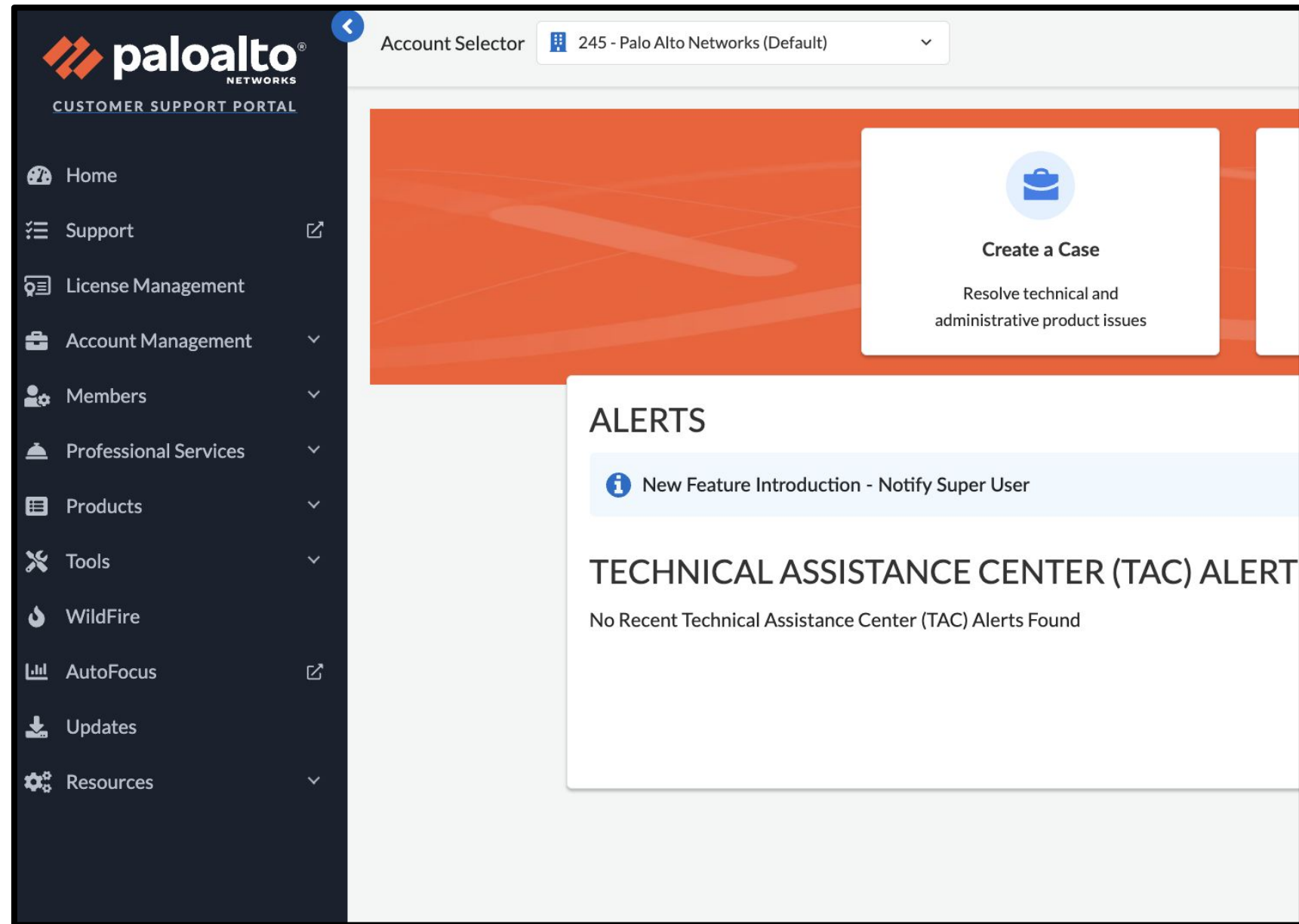
## Deep Dive

**Bingjun Wang**  
Technical Marketing Engineer

# CSP vs Tenant

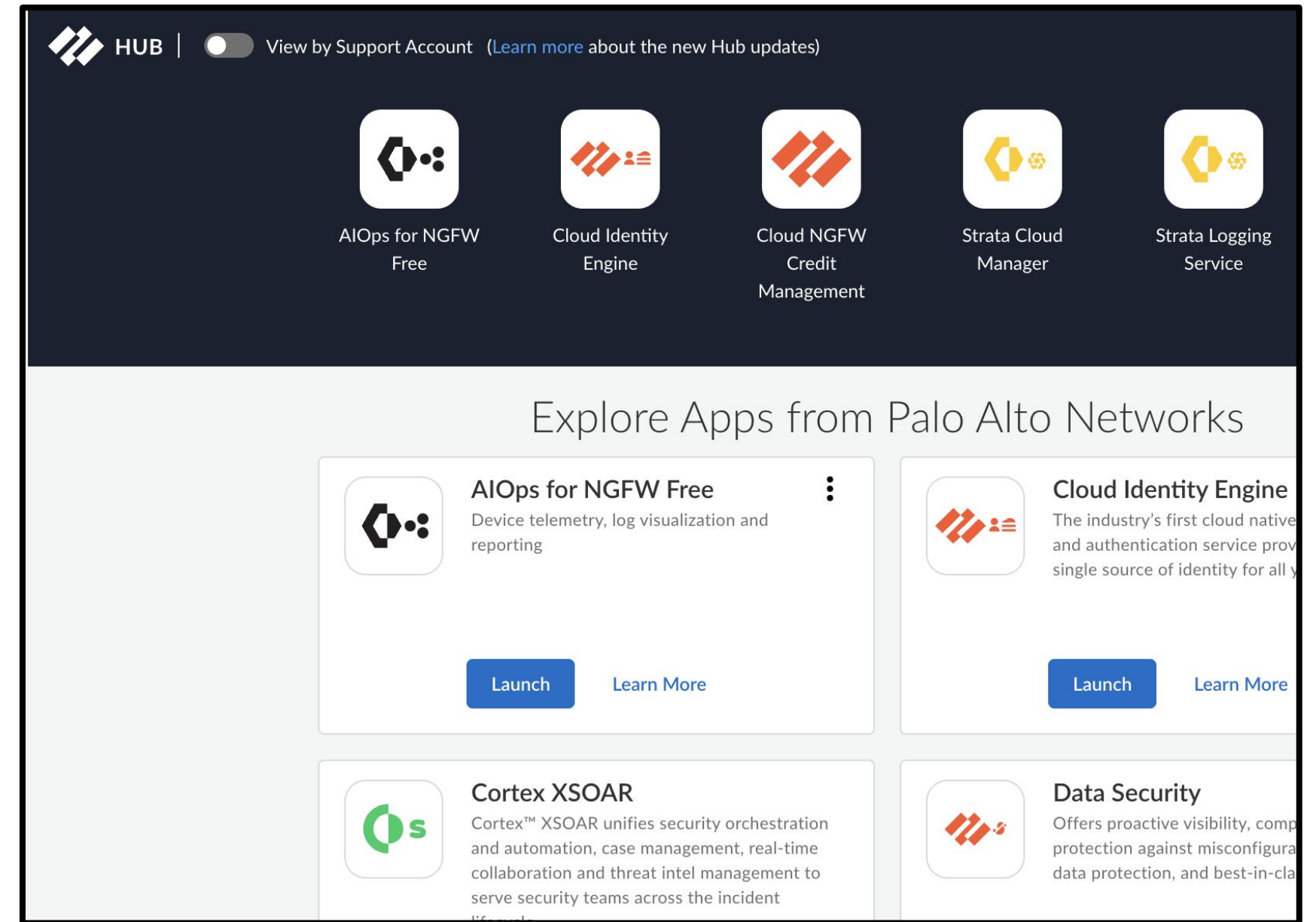
# Customer Support Portal and Tenant

Customer Support Portal



<https://support.paloaltonetworks.com/>

Tenant



<https://apps.paloaltonetworks.com/hub>

# SCM NGFW Onboarding

# Prerequisites for NGFW

- Minimum PAN-OS version supported:
  - 10.2.3 and above
- Firewall Models:
  - 4th Gen Hardware platforms (and Later)  
PA-220,220R, PA-400, PA-800, PA-1400, PA-3200, PA-3400, PA-5200, PA-5400, PA-5450
  - VM Series Firewalls
- FQDNs & Ports
  - <https://docs.paloaltonetworks.com/ngfw/administration/onboard-devices-and-deployments/prerequisites-for-cloud-management-onboarding>

# Hardware firewall Onboard to SCM Process

CSP/TSG

NGFW

- Register Device to CSP

# CSP Registration

The screenshot displays the Palo Alto Networks Customer Support Portal interface. On the left is a dark sidebar with navigation links: Home, Support, License Management, Account Management, Members, Professional Services, and Products. Under Products, 'Assets' is expanded to show 'Advanced Endpoint Protection', 'Asset History', 'Cloud Services', 'CN-Series Licensing', 'Device Certificates', 'Devices', and 'IONs'. The main content area is titled 'Device Registration' and features a progress bar with three steps: 'DEVICE TYPE' (active), 'DEVICE REGISTRATION', and 'DAY 1 CONFIGURATION (OPTIONAL)'. Below the progress bar is a white box titled 'Select Device Type' containing two radio button options: 'Register device using Serial Number' (selected) and 'Register usage-based VM-Series models (hourly/annual) purchased from public cloud Marketplace or Cloud Security Service Provider (CSSP)'. A 'Next >' button is located at the bottom right of the main content area. The top navigation bar includes an 'Account Selector' dropdown set to '245 - Palo Alto Networks (Default)', a 'Feedback' button, a search bar with the placeholder text 'ex. Where can I find my device serial num', and notification and help icons.

# Hardware firewall Onboard to SCM Process

CSP/TSG

NGFW

- Register Device to CSP
- Create Onboarding Rules (Optional) on Strata Cloud Manager



# Firewall Onboarding Rule (Optional)

Device Onboarding > Add Device Onboarding Rule

## Add Device Onboarding Rule

### General

Enabled

Name \*

Description

### Match Criteria

Models

Any  Match  Exclude (Negate)

Device S/N

Any  Match

Labels

### Action

Target Folder

All Firewalls

Snippet Association

Snippets (0)

Search

Snippet Name



Firewall can be matched with Model and/or Serial Number



Firewall location and snippet association after onboarding (config in sync after the onboarding)

# Hardware firewall Onboard to SCM Process

CSP/TSG

NGFW

- Register Device to CSP
- Create Onboarding Rules (Optional) on Strata Cloud Manager
- Associate Device to the TSG and Associate with the App (AIOPs Premium / SCM Pro)

# Add or remove devices to TSG

The screenshot shows the Strata Cloud Manager interface. On the left, a navigation menu is open, with 'Common Services' highlighted by a red arrow. Below it, 'Device Associations' is also highlighted. The main content area shows the 'Device Associations' page for a tenant group. A modal window titled 'Add devices associated with a Customer Support Account' is open, showing a list of devices with their serial numbers, names, models, and types. Two devices are selected. A red arrow points to the 'Save' button at the bottom right of the modal.

**Common Services**

- Subscriptions & Add-ons
- Tenant Management
- Identity & Access
- Device Associations**
- Cortex Data Lake
- Enable AI-based innovations for

**Device Associations**

Search serial numbers, models, device names

Serial Number	Device Name	Model	Type
<input checked="" type="checkbox"/>	01790006588	PA-SAAS-SW	Production
<input checked="" type="checkbox"/>	01790006978	PA-SAAS-SW	Production
<input type="checkbox"/>	01790006991	PA-SAAS-SW	Production
<input type="checkbox"/>	01790006995	PA-SAAS-SW	Production
<input type="checkbox"/>	01790007029	PA-SAAS-SW	Production
<input type="checkbox"/>	01790007054	PA-SAAS-SW	Production
<input type="checkbox"/>	01790007065	PA-SAAS-SW	Production
<input type="checkbox"/>	01790007112	PA-SAAS-SW	Production
<input type="checkbox"/>	01790007130	PA-SAAS-SW	Production
<input type="checkbox"/>	01790007148	PA-SAAS-SW	Production
<input type="checkbox"/>	01790007149	PA-SAAS-SW	Production
<input type="checkbox"/>	01790007216	PA-SAAS-SW	Production

2 Rows Selected

25 Rows Page 1 of 4

Cancel Save

# Associate SCM Product to Device

management Identity & Access / Access Management Device Associations Trusted IP List Name: Strata Cloud Manager NGFW Config 101- Lab Par... TSG ID: 1113860888

All Tenants > Strata Cloud Manager NGFW Config 101- Lab Parent Tenant (TSG ID: 1113860888)

[Add Device](#) [Associate Products](#) [Learn More](#)

### Device Associations for Strata Cloud Manager NGFW Config 101- Lab Parent Tenant

Search serial numbers, models, device names

<input type="checkbox"/>	Serial Number	Device Name	Model	Type
<input type="checkbox"/>	007958000548173	00795800054...	PA-VM	Production
<input type="checkbox"/>	007958000548168	00795800054...	PA-VM	Production


### Associate products with devices

Products

- Strata Cloud Manager

Search serial numbers, models, device names

<input type="checkbox"/>	Serial Number	Device Name	Model	Type
<input type="checkbox"/>	031901000503		PA-450R-...	Production



# Hardware firewall Onboard to SCM Process

CSP/TSG

NGFW

- Register Device to CSP
- Create Onboarding Rules (Optional) on Strata Cloud Manager
- Associate Device to the TSG and Associate with the App (AIOPs Premium / SCM Pro)
- Move Device from Available Device to Cloud Manage

# Move Firewall From Available Device to Cloud Manage Device

Cloud Managed Devices Available Devices

### Available Devices (1)

Search

<input checked="" type="checkbox"/>	Serial Number	Model	Onboarding Status
<input checked="" type="checkbox"/>	031101000025	PA-450R	

### Cloud Managed Devices (0)

Search

<input type="checkbox"/>	Serial Number	Model	Onboarding Labels	Onboarding Status
--------------------------	---------------	-------	-------------------	-------------------

[Move to Cloud Management >](#)

[< Back to Available Devices](#)

# Hardware firewall Onboard to SCM Process

## CSP/TSG

- Register Device to CSP
- Create Onboarding Rules (Optional) on Strata Cloud Manager
- Associate Device to the TSG and Associate with the App (AIOPs Premium / SCM Pro)
- Move Device from Available Device to Cloud Manage

## NGFW

- Initial Configurations needed:
  - Mgmt IP/Subnets/Gateway
  - DNS
  - NTP
- Device Certificates (Not Required for 4th Gen Firewalls)
- Retrieve Licenses From AuthCode
- Change Management Option

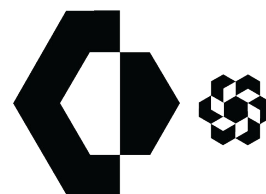
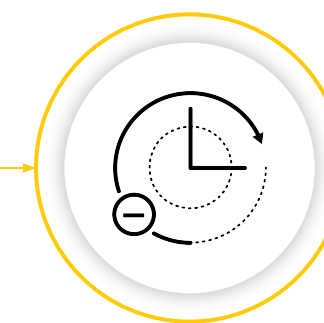
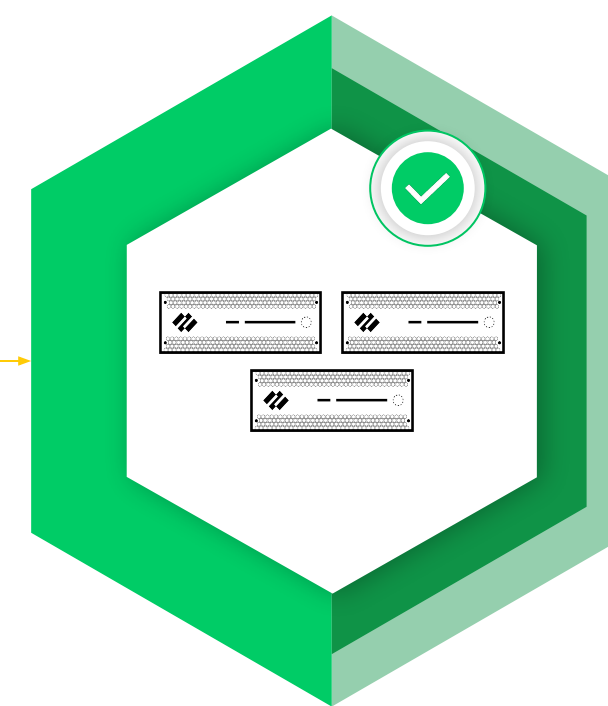
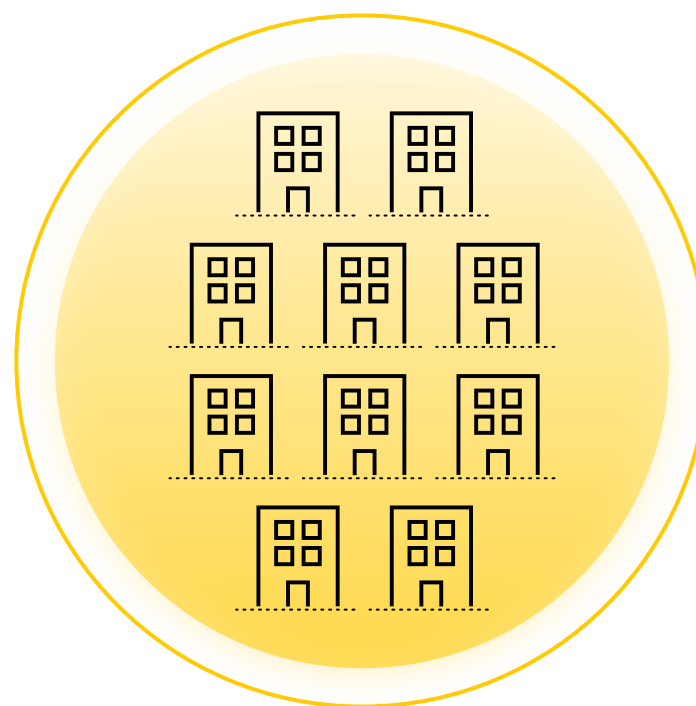
# Efficient Onboarding with Zero Touch Provisioning

Automate onboarding and day-0 workflows for increased productivity

I need to onboard 10 new sites, how can I simplify onboarding?



**Emily**  
NetSec Admin



1

10 new branch offices are opening and Emily needs to set up the new deployments

2

With Strata Cloud Manager, Emily uses zero touch provisioning to get the firewalls configured and automate onboarding and licensing

3

Emily remotely onboards the new sites without IT expertise in the branches while eliminating misconfigurations



# Pre-request for Zero Touch Provisioning

- Firewall Model:
  - PA-400 Series Firewalls
  - PA-820-ZTP and PA-850-ZTP
  - PA-1400 Series Firewalls
  - PA-3220-ZTP, PA-3250-ZTP, and PA-3260-ZTP
  - PA-3400 Series Firewalls
  - PA-5400 Series Firewalls
  - PA-5450
  
- Network Infra:
  - DHCP
  - Internet access
  - FQDN & Ports Open

# ZTP Hardware firewall Onboard to SCM Process

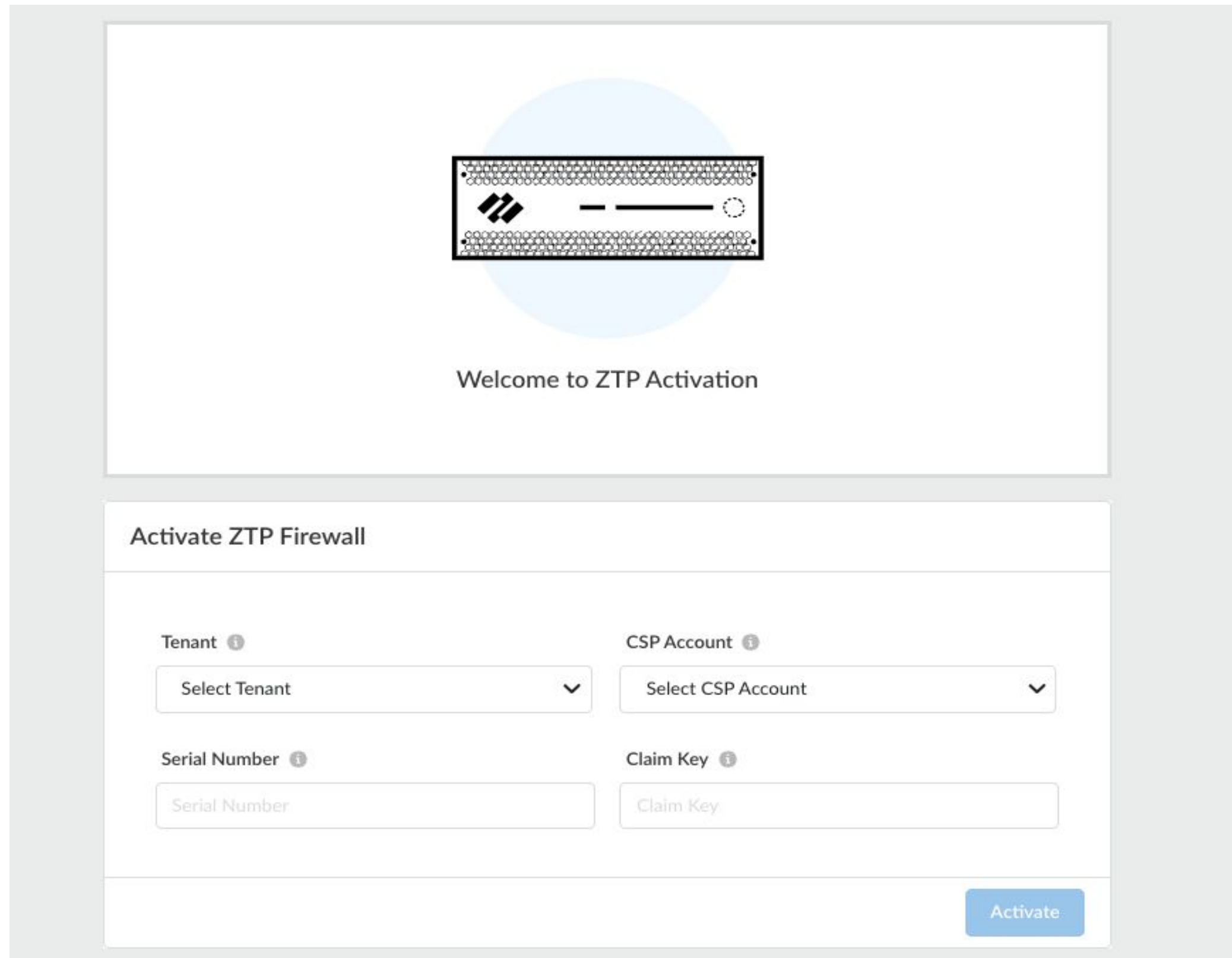
CSP/TSG

- ZTP Activation

NGFW

- Cabling the firewall and power up

# ZTP Hardware firewall



Welcome to ZTP Activation

### Activate ZTP Firewall

Tenant ⓘ CSP Account ⓘ

Select Tenant ▼ Select CSP Account ▼

Serial Number ⓘ Claim Key ⓘ

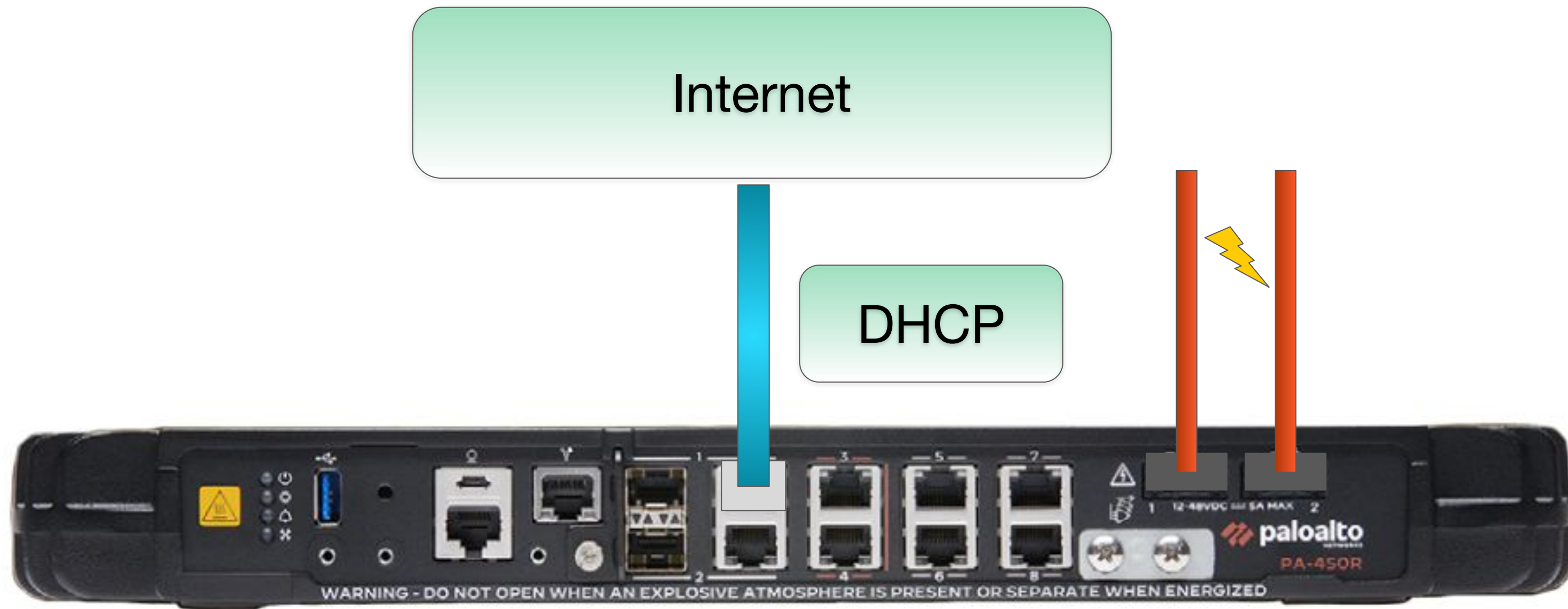
Serial Number Claim Key

Activate

- CSP Registration

- TSG Device/SCM Association

<https://stratacloudmanager.paloaltonetworks.com/ztpdeviceactivation>



## Factory Default State

# VM-Flex Credit Pool

The screenshot displays the 'VM-Series' configuration page. On the left, a sidebar shows 'So Ev Cre Exp Elig' and 'CREDIT USAGE' with a tree view containing 'Allocated', 'Consumed', 'Available', and 'Total Credits'. The main configuration area includes:

- Profile Name:
- \* Number of Firewalls:
- \* Number of vSYS:
- \* Planned vCPU per Firewall:
- \* Security Use Case:
- Customize Subscriptions:
  - Advanced URL Filtering
  - Global Protect
  - DLP
  - SD-WAN
  - Intelligent Traffic Offload
  - Advanced Threat Prevention
  - DNS
  - Network Packet Broker
  - Decryption Port Mirror
  - Panorama for Management
  - Strata Cloud Manager Pro
  - Strata Logging Service
- Additional Subscriptions:
  - Web Proxy (Promotional Offer)
  - Advanced Wildfire
  - SaaS Inline
  - Advanced DNS
  - IoT
  - Panorama as Dedicated Log Collector
- Use Credits to Enable:
  - Panorama for Management
  - Strata Cloud Manager Pro
  - Strata Logging Service

A tooltip for 'Strata Cloud Manager Pro' states: 'Includes AI Ops, ADEM, SLS, Cloud/Config Management. Strata Cloud Manager Pro'. At the bottom, there is a link 'Protect more, save more'.

- Credit pool is required for creating Deployment Profile
- Based on the number of VM firewalls & vCPUs reserved and Licenses selected, the credits are allocated from the Pool to deployment profile
- The credits allocated to the Deployment profile get consumed when the firewall has retrieve the licenses from the authcode (generated by deployment profile)

# VM-Series firewall Onboard to SCM Process

CSP/TSG

NGFW

- Create Deployment Profile
- Associate Deployment Profile to TSG

# Proceed to Finish Setup

The screenshot shows the Palo Alto Networks Customer Support Portal interface. The left sidebar contains navigation options like Professional Services, Products, Assets, and various management tools. The main content area is titled 'Current Deployment Profiles' and displays a table of profiles. A callout box points to the 'Finish Setup' button for the 'scmpro-flex-01' profile.

PROFILE NAME	ENFORCEMENT TYPE	PAN-OS VERSION	CREDITS CONSUMED/ALLOCATED	FIREWALLS DEPLOYED/PLANNED	VCPUS CONSUMED/ALLOCATED	AUTH CODE
AI-Runtime-Security-Deployment-Profile	AI	PAN-OS 11.2.2	0 / 212.52	0 / 4	0 / 16	D3803638 <a href="#">View Devices</a>
AI-RS-Demo	AI	PAN-OS 11.2.2	0 / 212.52	0 / 4	0 / 16	D9893476 <a href="#">View Devices</a> <a href="#">Finish Setup</a>
test_SCMpro	VM	Flexible vCPUs (PAN-OS 10.0.4 and above)	17.41 / 34.82	1 / 2	2 / 4	D3768758 <a href="#">View Devices</a>
testdemo92324	VM	Flexible vCPUs (PAN-OS 10.0.4 and above)	0 / 30.59	0 / 2	0 / 4	D1020201 <a href="#">View Devices</a> <a href="#">Finish Setup</a>
pano_test	VM	Flexible vCPUs (PAN-OS 10.0.4 and above)	0 / 38.64	0 / 2	0 / 4	D9641949 <a href="#">View Devices</a> <a href="#">Finish Setup</a>
scmpro-flex-01	VM	Flexible vCPUs (PAN-OS 10.0.4 and above)	0 / 18.17	0 / 1	0 / 2	<a href="#">View Devices</a> <a href="#">Finish Setup</a>

There are additional licenses that need to be activated on a tenant.

# VM-Series firewall Onboard to SCM Process

## CSP/TSG

- Create Deployment Profile
- Associate Deployment Profile to TSG

## NGFW

- Initial Configurations needed:
  - Mgmt IP/Subnets/Gateway
  - DNS
  - NTP
- Retrieve Licenses
  - Apply Deployment Profile Auth-codes
- Device Certificates
- Change Management Option



# Bootstrap VM-Series firewall Onboard to SCM Process (VMware)

## CSP/TSG

- Create Deployment Profile
- Associate Deployment Profile to TSG

## NGFW

- Prepare bootstrap package and convert to ISO image
- Insert bootstrap package as ISO image before the VM first boot up

# Bootstrap Package for VM Series Firewall onboard to SCM



Insert authcode from Deployment profile (make sure the authcode file does not have any file extension)

Add Initial configs

# init-cfg.txt

```
type=static
ip-address=xxx.xxx.xxx.xxx
netmask=xxx.xxx.xxx.xxx
default-gateway=xxx.xxx.xxx.xxx
hostname=<Hostname>
panorama-server=cloud
plugin-op-commands=advance-routing:enable
dns-primary=xxx.xxx.xxx.xxx
vm-series-auto-registration-pin-id=<String>
vm-series-auto-registration-pin-value=<String>
```

## Activity 2 Step 1:

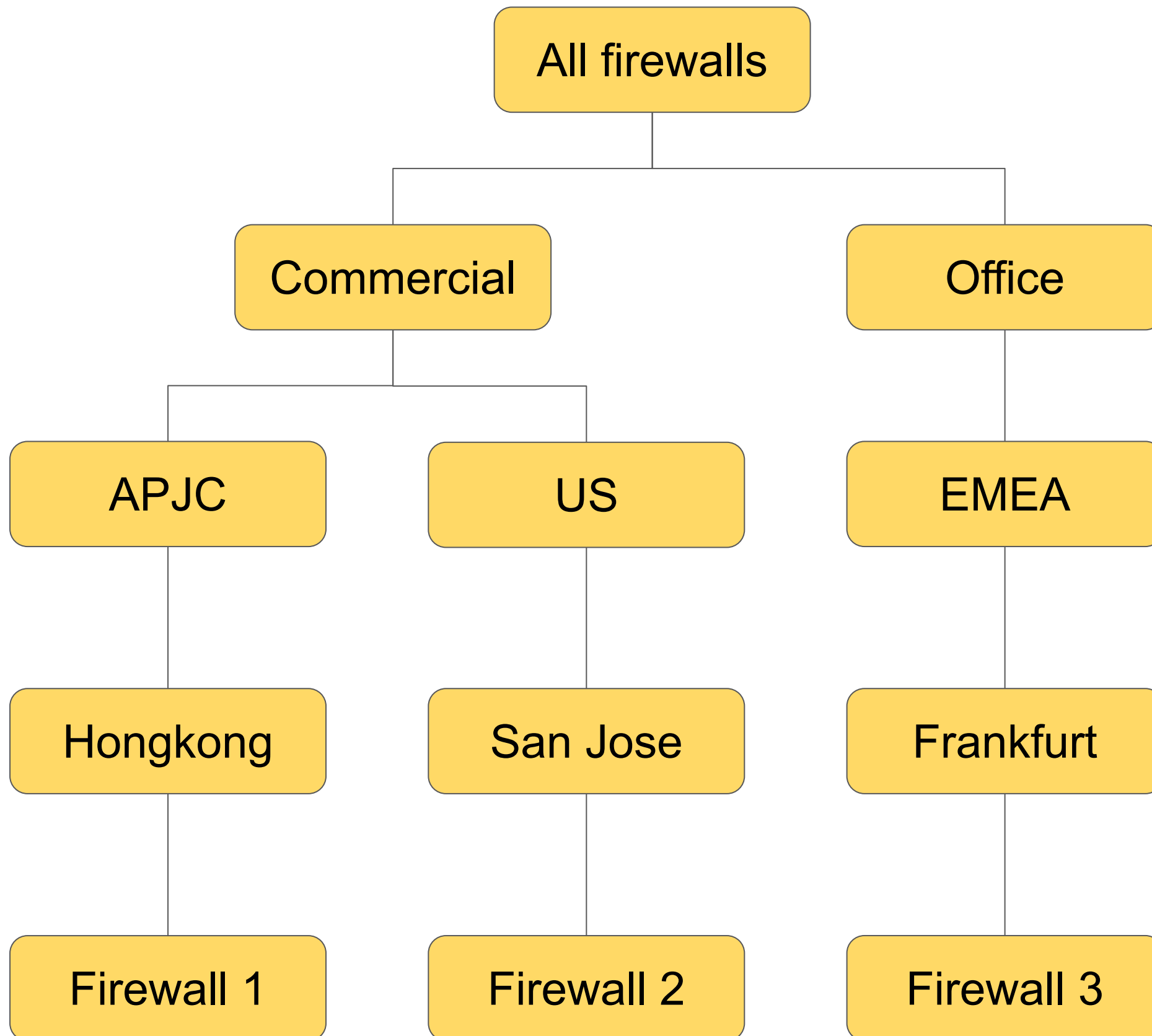
1. Join Webex meeting with your email address
2. Follow the lab instructions to use the authcode to generate the firewall serial number
3. Post the NGFW 1 and NGFW 2 Serial number into the chat with your Pod number and email address
4. Instructor will reply back with the OTP that you need for the next step

# SCM NGFW Configuration

# SCM NGFW Configurations

- Configuration Schema (Folders and Snippets)
- Variables

# Folders



- Unified Configuration Container  
*Folders Contains all Configuration form factors (Security, Object, Network, Device ).*
- Configuration Inheritance Behavior  
*All the configurations from the higher level folder, will be inherited to the sub-folders in the same stream.*
- Configuration Modifications  
*The inherited configurations can be modified/overridden in the sub-folder level. The a inherited configuration **cannot be deleted.** (can only be reverted back to inherited)*
- Folder Hierarchy Limits  
*Four nested folder level under **All Firewall Folders***

# Predefined Folders

Global



The parent folder for all folders. Security rules added in this level will be applied to the entire Security Platform (Unified Security Configuration)

Prisma Access  
(Hierarchy)



Prisma Access Folder Hierarchy will appear only if you enabled Prisma Access. Prisma Access Folder Hierarchy will be predefined, users are not able to add subfolders in the PA hierarchy

All Firewalls



All Firewall folder will be the parent folder of all Hardware/VM NGFWs. A new device onboarding to SCM without onboarding rules will be located in the All Firewall Folders.

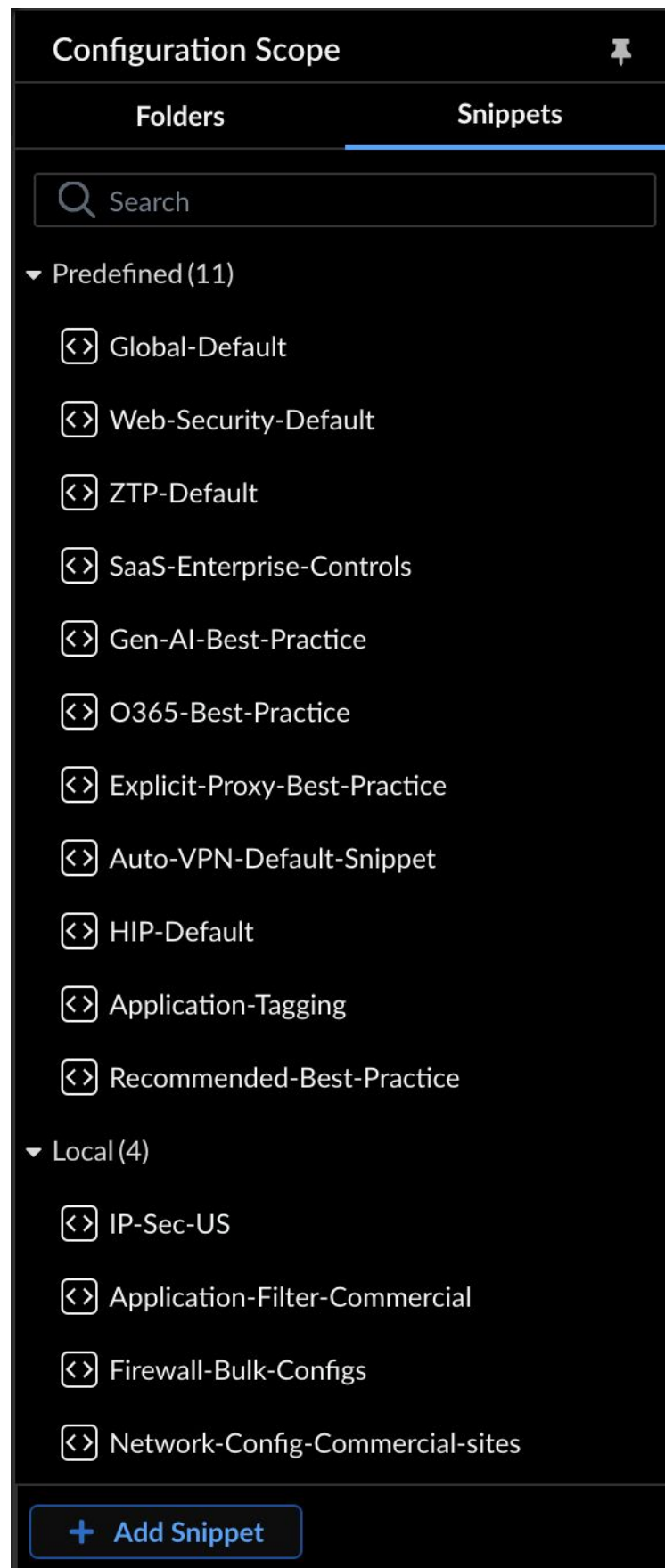
FW Device



Firewall Device will be presented as Folder. Configuration can be applied. (Device Level Configuration is supported in Strata Cloud Manager)

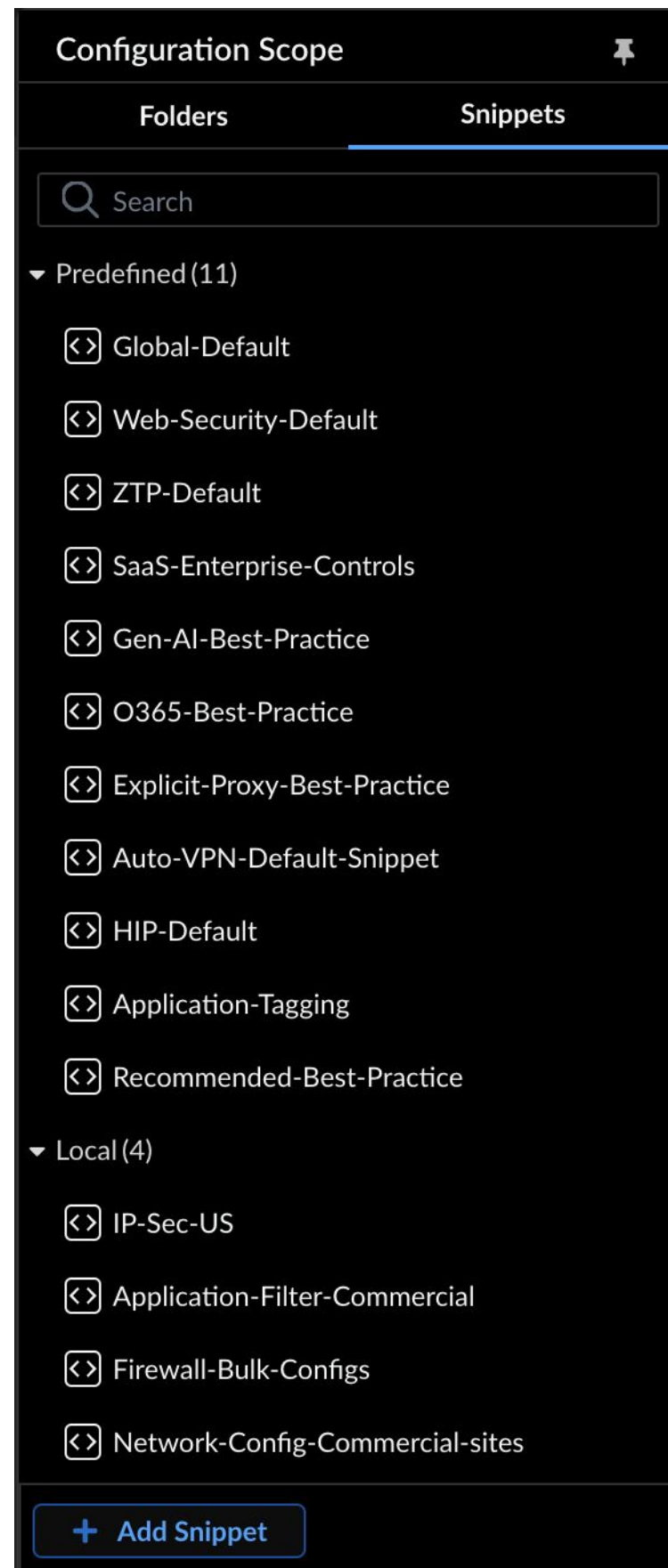


# Snippets



- Snippet has the same configuration Schema as Folders (including all form factors)
- The creation of Snippet will not apply to any folders and Devices. The Snippet can be created and stored.
- Snippet can be associated with any folders for devices. The snippet configuration will also be inherited to subfolders of the folder that it associates with.
- Changes that been made in the snippets will be apply to all the folders that the snippet has been associated with.

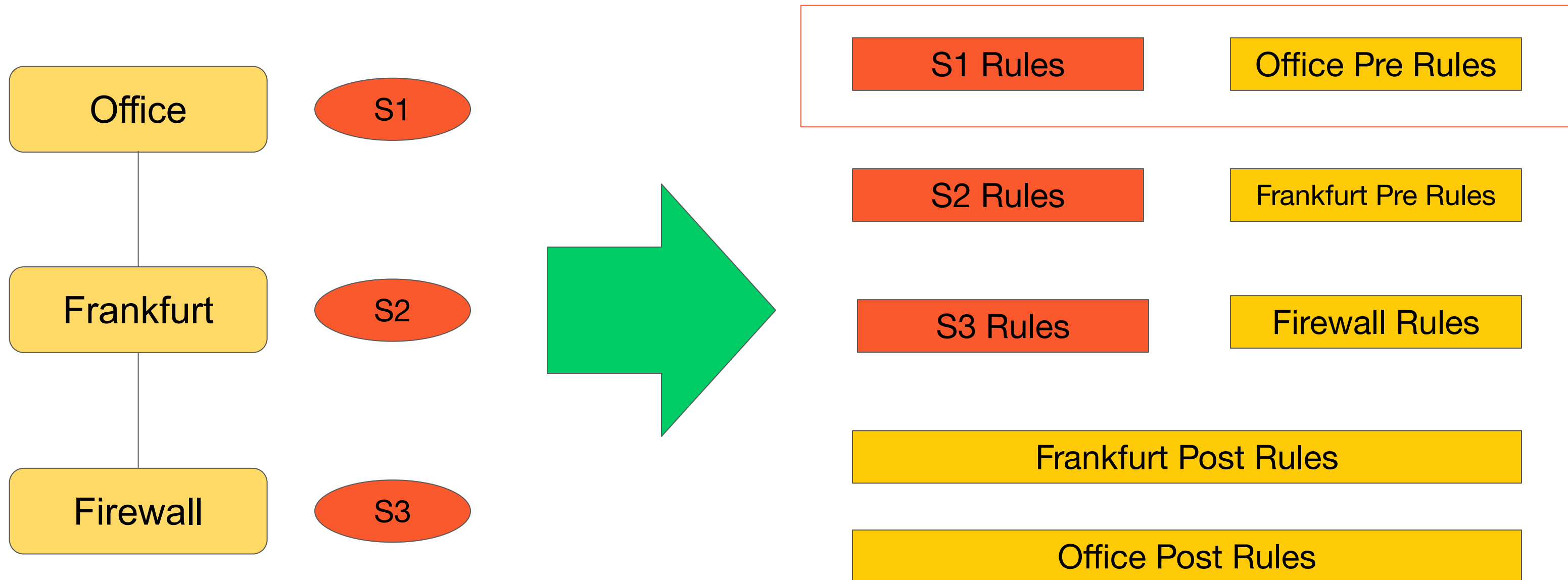
# Snippets Use Case



- Modularize Configuration
- Configuration Template for the set of configurations that hard to fit in the hierarchy.
- Configuration Sharing across tenants
- Predefined Snippets

# Security Rules Merge Logic (Folders + Snippets)

Based on the order of rule creation and Snippet association



Re-Ordering: Folder/Device Rules cannot be reordered in the middle of the Snippet Rules

# Keep/Remove Default Configurations - SCM

SCM by default come with configurations in All Firewall Folder. These Configuration can be removed.

- Remove Zones (local, Internet)
- Remove Router (Default)
- Remove Interface (eth-internet / eth-local)

The image displays three screenshots of the Palo Alto Networks configuration interface, stacked vertically. Each screenshot shows the 'Configuration Scope: All Firewalls' and the 'Device Settings' menu.

**Interfaces Screenshot:** Shows the 'Interfaces' section with tabs for Ethernet, VLAN, Loopback, Tunnel, and Cellular.

**Zones Screenshot:** Shows the 'Zones (7)' table with columns for Name, Security Po..., Location, Type, Interfaces, Zone Protec..., Packet Buffe..., and USER-ID/DEVICE-ID sub-columns. The table lists two zones: 'zone-internal' and 'zone-to-hub', both of type 'layer3' and associated with 'Auto-VPN-Default-Snippet'.

	Name	Security Po...	Location	Type	Interfaces	Zone Protec...	Packet Buffe...	USER-ID			DEVICE-ID		
								Ena...	Inclu...	Exclu...	Ena...	Inclu...	Exclu...
<input type="checkbox"/>	zone-internal		Auto-VPN-Default-Snippet	layer3			<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>			
<input type="checkbox"/>	zone-to-hub		Auto-VPN-Default-Snippet	layer3			<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>			

**Routing Screenshot:** Shows the 'Routing' section with tabs for Routers and Profiles. The 'Routers (1)' table lists a single router named 'default' with interfaces '\$eth-local' and '\$eth-internet' and location 'All Firewalls'.

	Name	Interfaces	Location	General	BGP	Static	OSPF
<input type="checkbox"/>	default	\$eth-local \$eth-internet	All Firewalls				

# Variables

- Variables (name starts with '\$') are configuration components defined in a Folder/Snippet that provide flexibility and reusability to manage firewall configurations.

## Commercial Parent Level:

<input type="checkbox"/>	\$GUEST-GW		Commercial	\$AE1.99	ip-netmask	10.0.99.1/24
<input type="checkbox"/>	\$EMPLOYEE-GW		Commercial	\$AE1.90	ip-netmask	10.0.90.1/24
<input type="checkbox"/>	\$DIA1		Commercial	\$AE1.998	ip-netmask	None
<input type="checkbox"/>	\$DIA2		Commercial	\$AE1.999	ip-netmask	None

## Frankfurt Commercial Site Level:

<input type="checkbox"/>	\$GUEST-GW		Commercial	\$AE1.99	ip-netmask	10.0.99.1/24
<input type="checkbox"/>	\$EMPLOYEE-GW		Commercial	\$AE1.90	ip-netmask	10.0.90.1/24
<input type="checkbox"/>	\$DIA1		Frankfurt-Commercial		ip-netmask	132.146.175.130/29
<input type="checkbox"/>	\$DIA2		Frankfurt-Commercial		ip-netmask	132.146.175.138/29

<https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/manage-configuration-ngfw-and-prisma-access/configuration-scope/variables>

**Thank you**