paloalto NETWORKS | Cybersecurity Partner of Choice

Palo Alto Networks

SCM Config Management

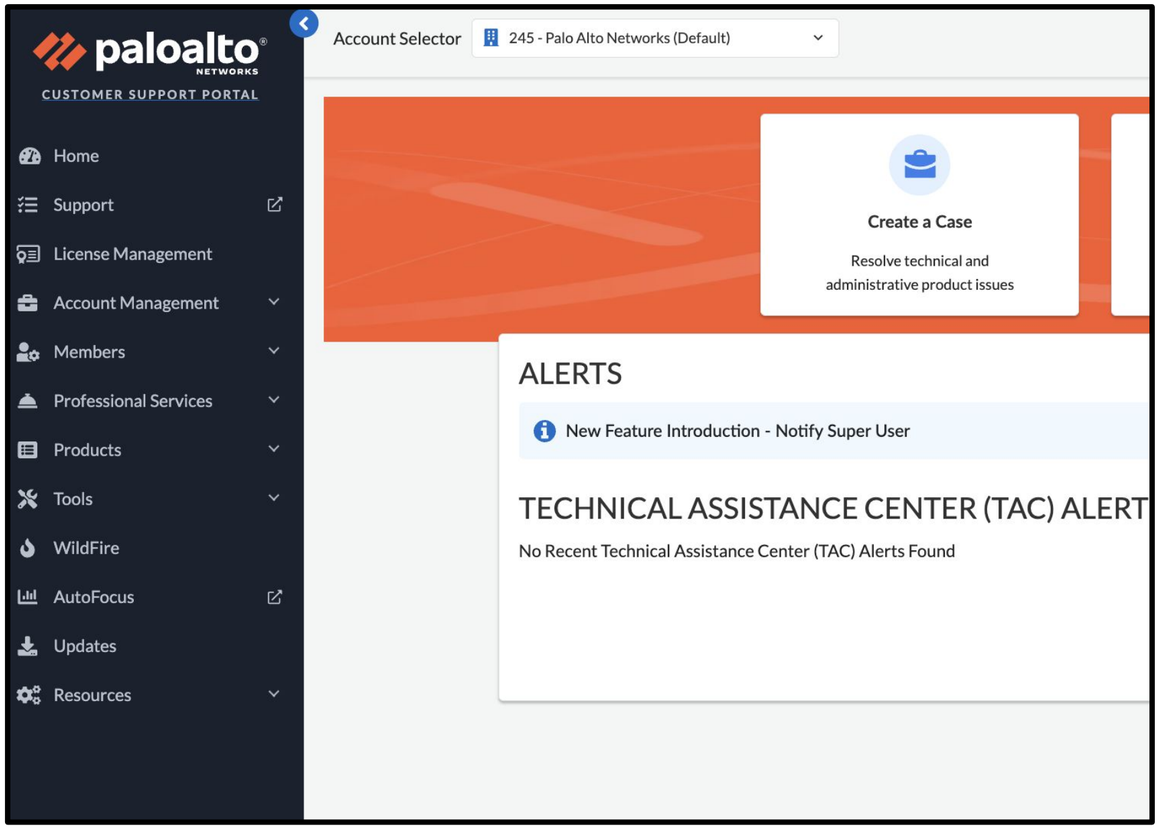
Deep Dive

Bingjun Wang
Technical Marketing Engineer

CSP vs Tenant

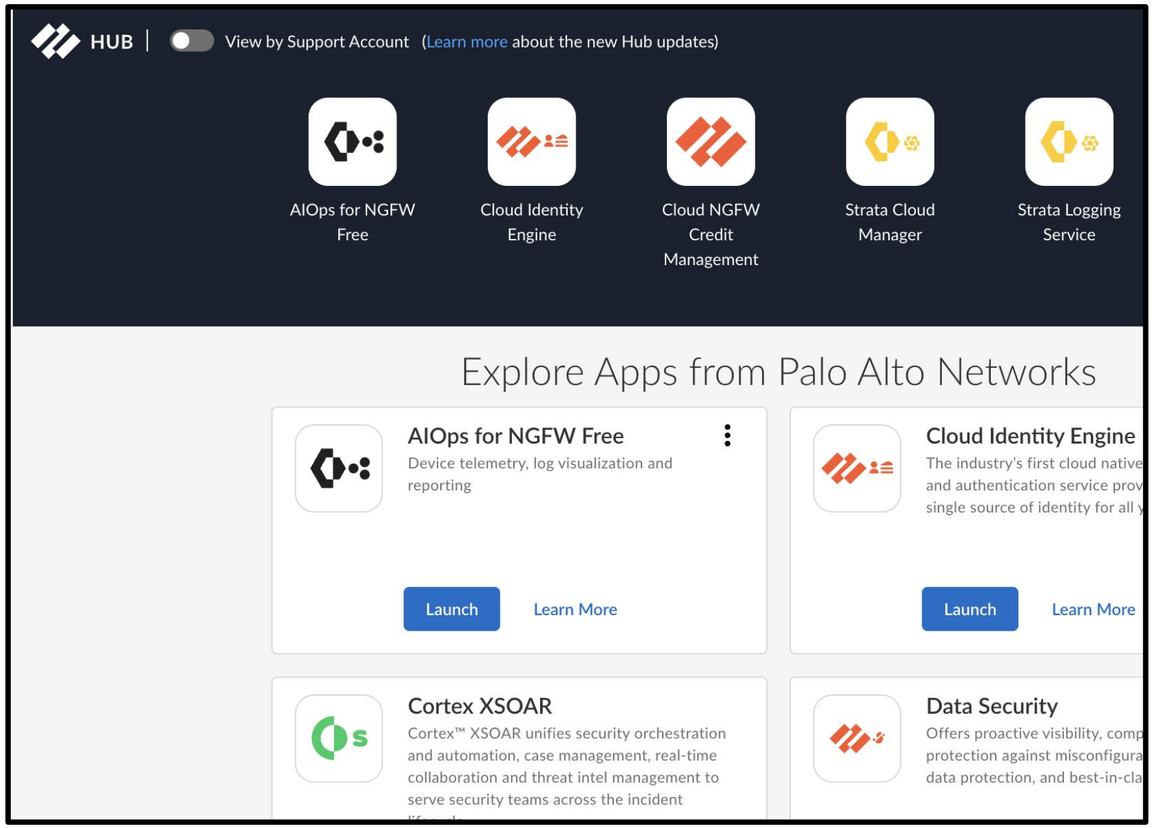
Customer Support Portal and Tenant

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

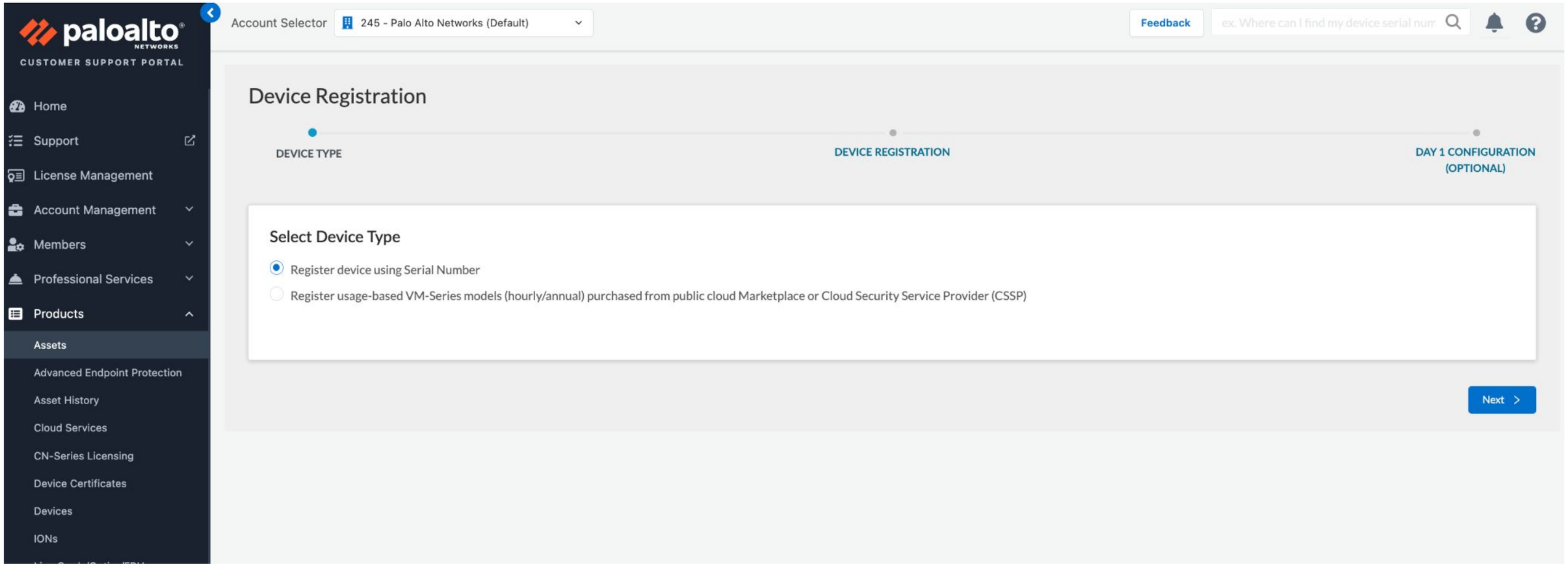
Hardware firewall Onboard to SCM Process

CSP/TSG

NGFW

- Register Device to CSP

CSP Registration



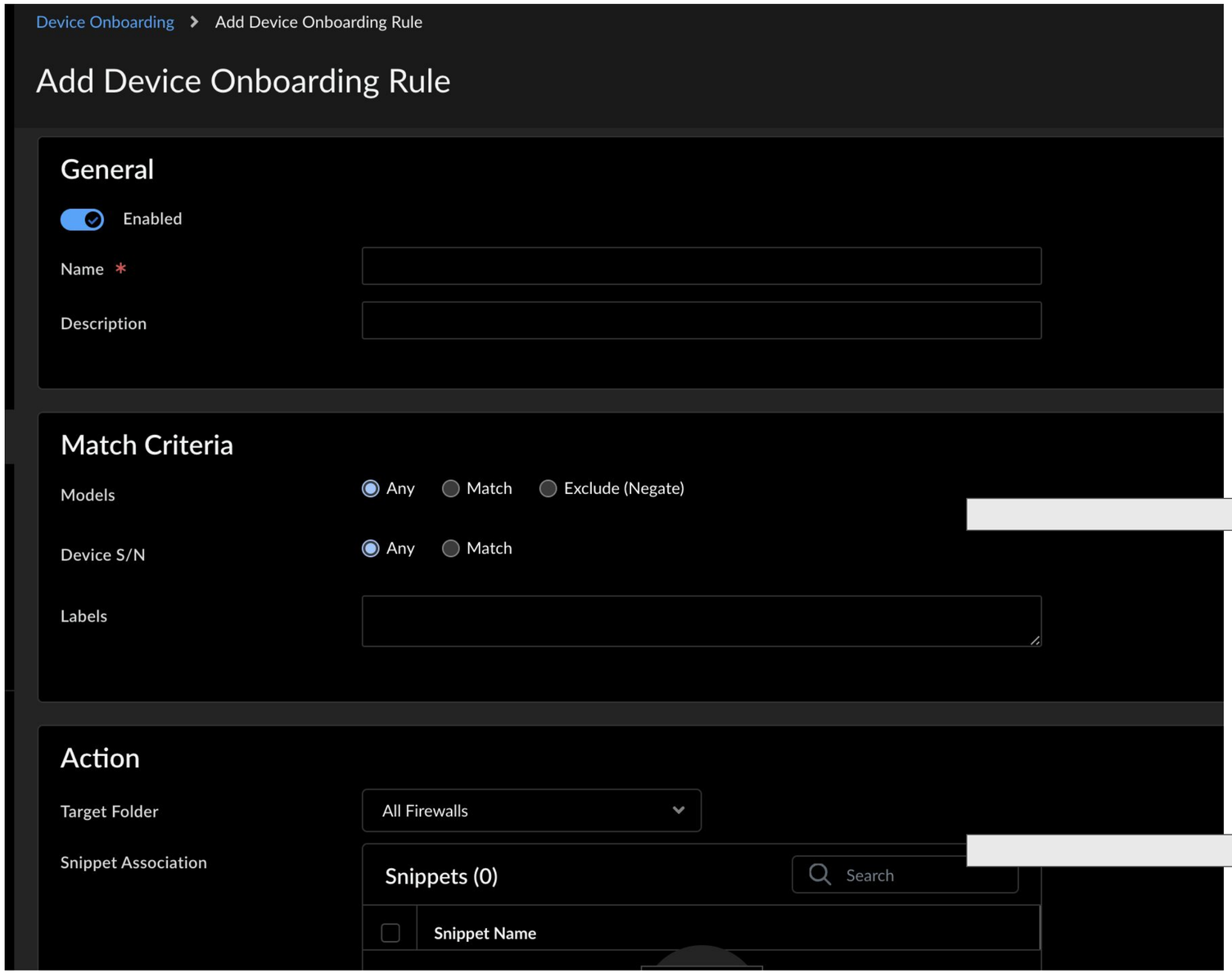
Hardware firewall Onboard to SCM Process

CSP/TSG

NGFW

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

Firewall Onboarding Rule (Optional)



Firewall can be matched with Model and/or Serial Number

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

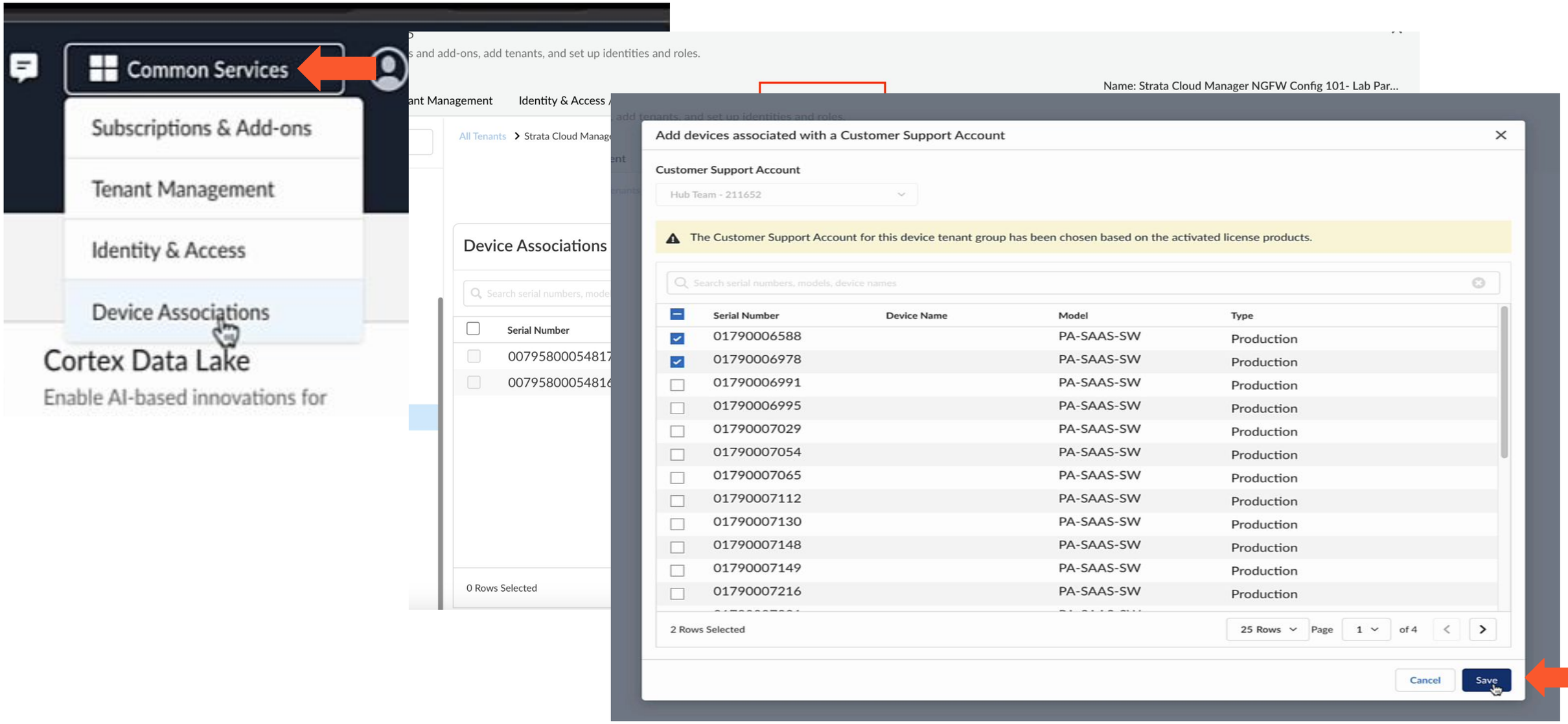
Hardware firewall Onboard to SCM Process

CSP/TSG

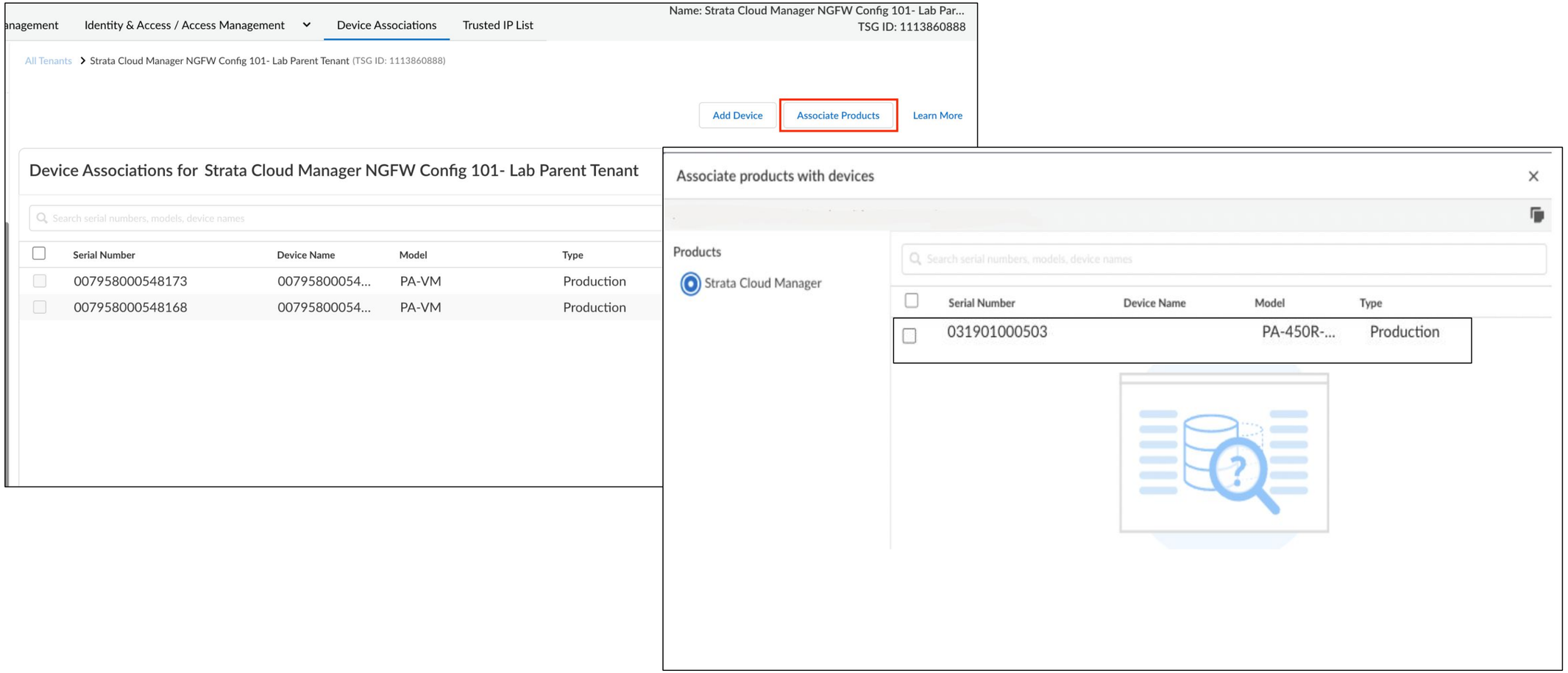
NGFW

- 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



Associate SCM Product to Device



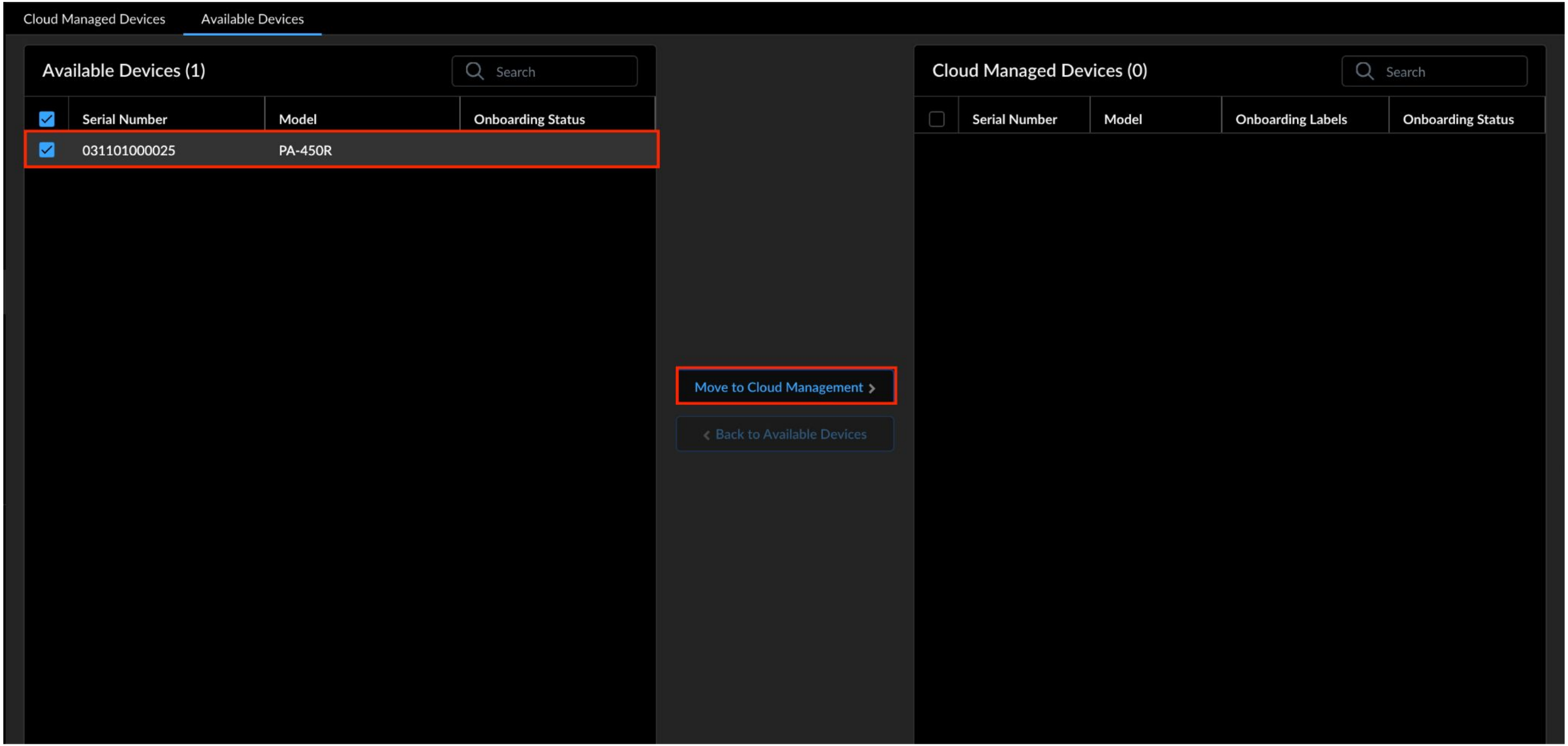
Hardware firewall Onboard to SCM Process

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



Hardware firewall Onboard to SCM Process

CSP/TSG

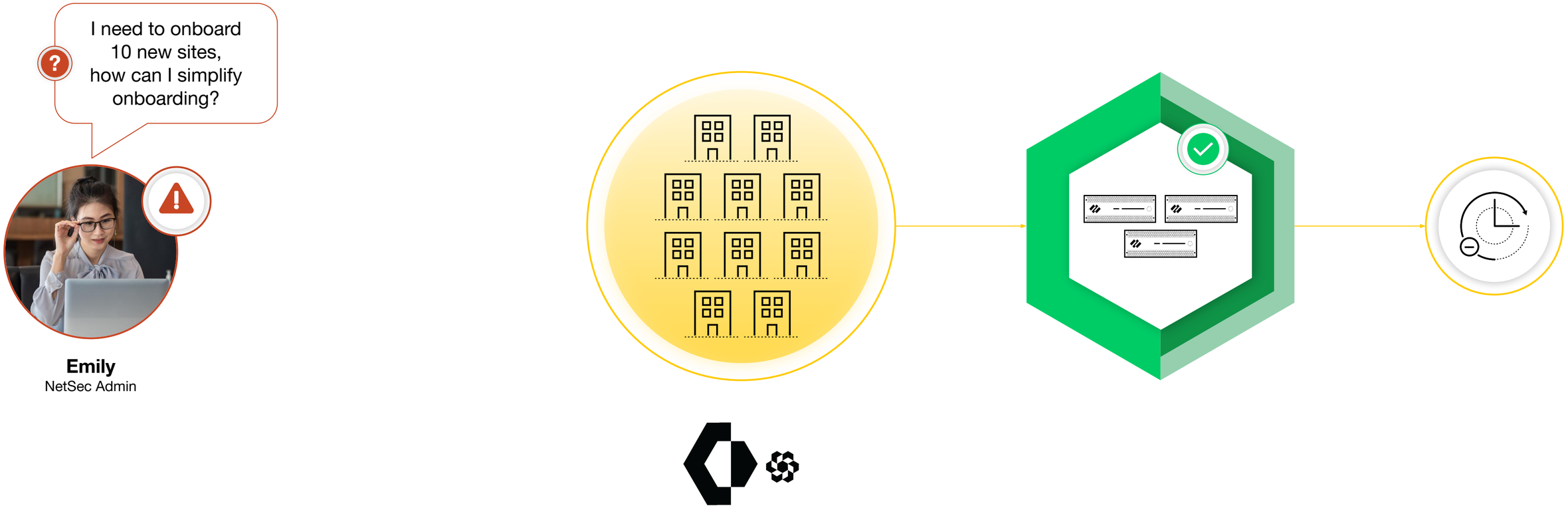
- Register Device to CSP
- Create Onboarding Rules (Optional) on Strata Cloud Manager
- Associate Device to the TSG and Associate with the App (AIOPs Premium / SCM Pro)
- Move Device from Available Device to Cloud Manage

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



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

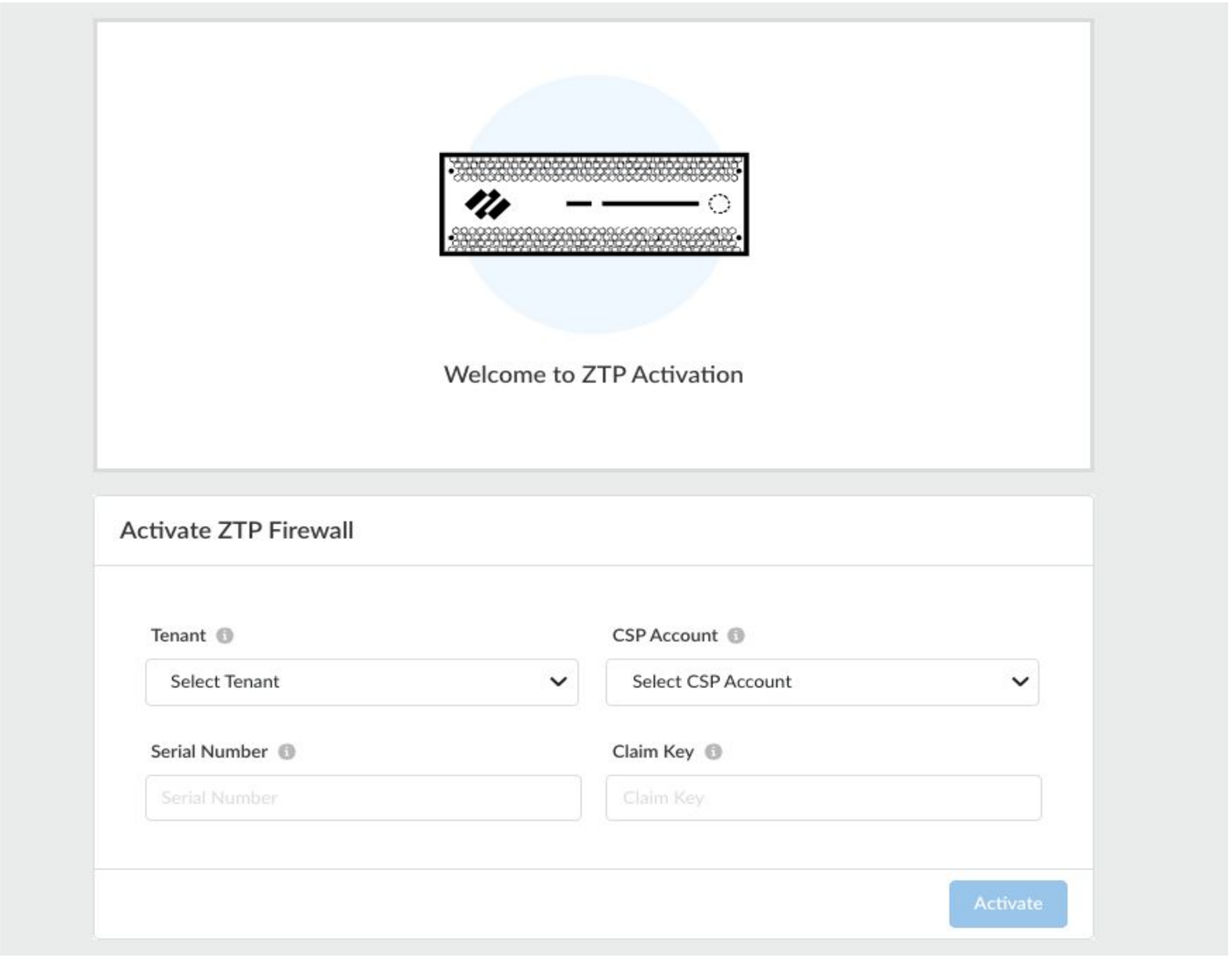
CSP/TSG

- ZTP Activation

NGFW

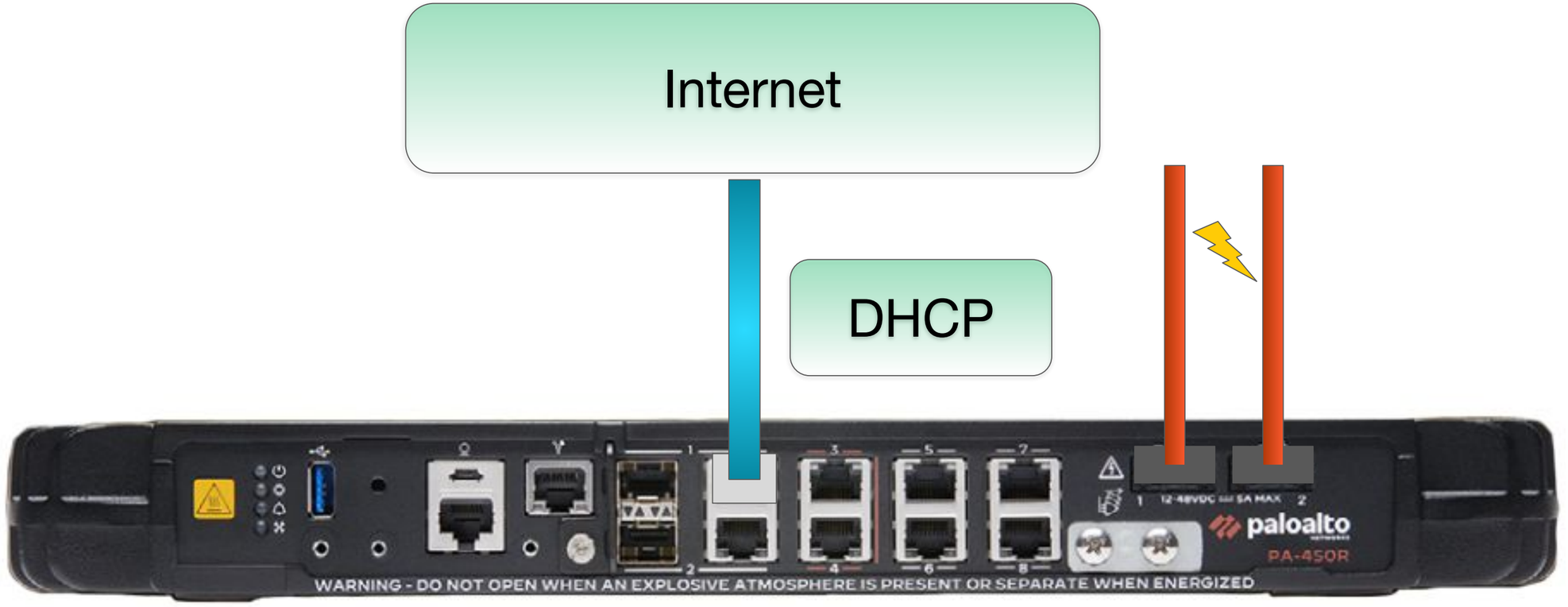
- Cabling the firewall and power up

ZTP Hardware firewall



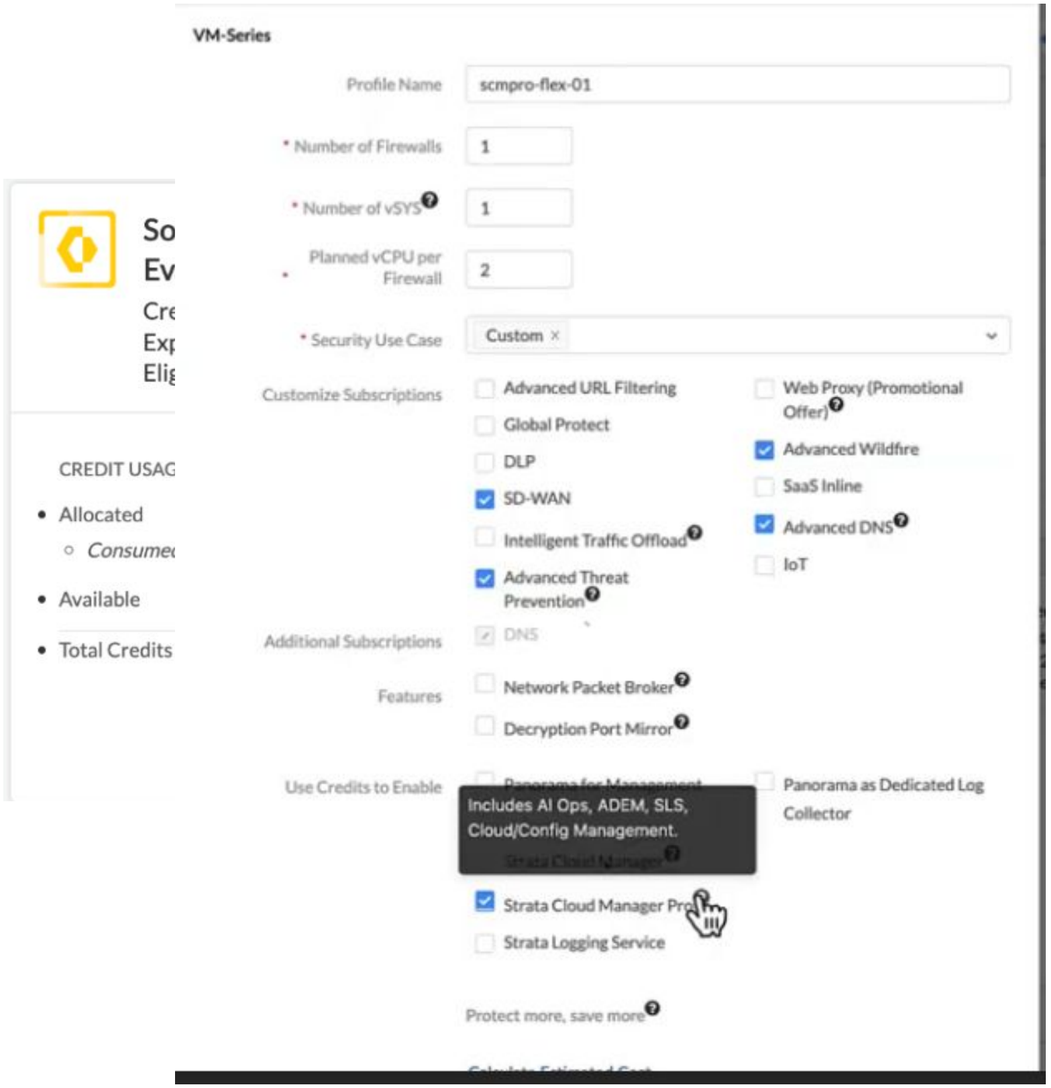
- CSP Registration
- TSG Device/SCM Association

https://strataclоudmanager.paloaltonetworks.com/ztpdeviceactivation



Factory Default State

VM-Flex Credit Pool



- 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)

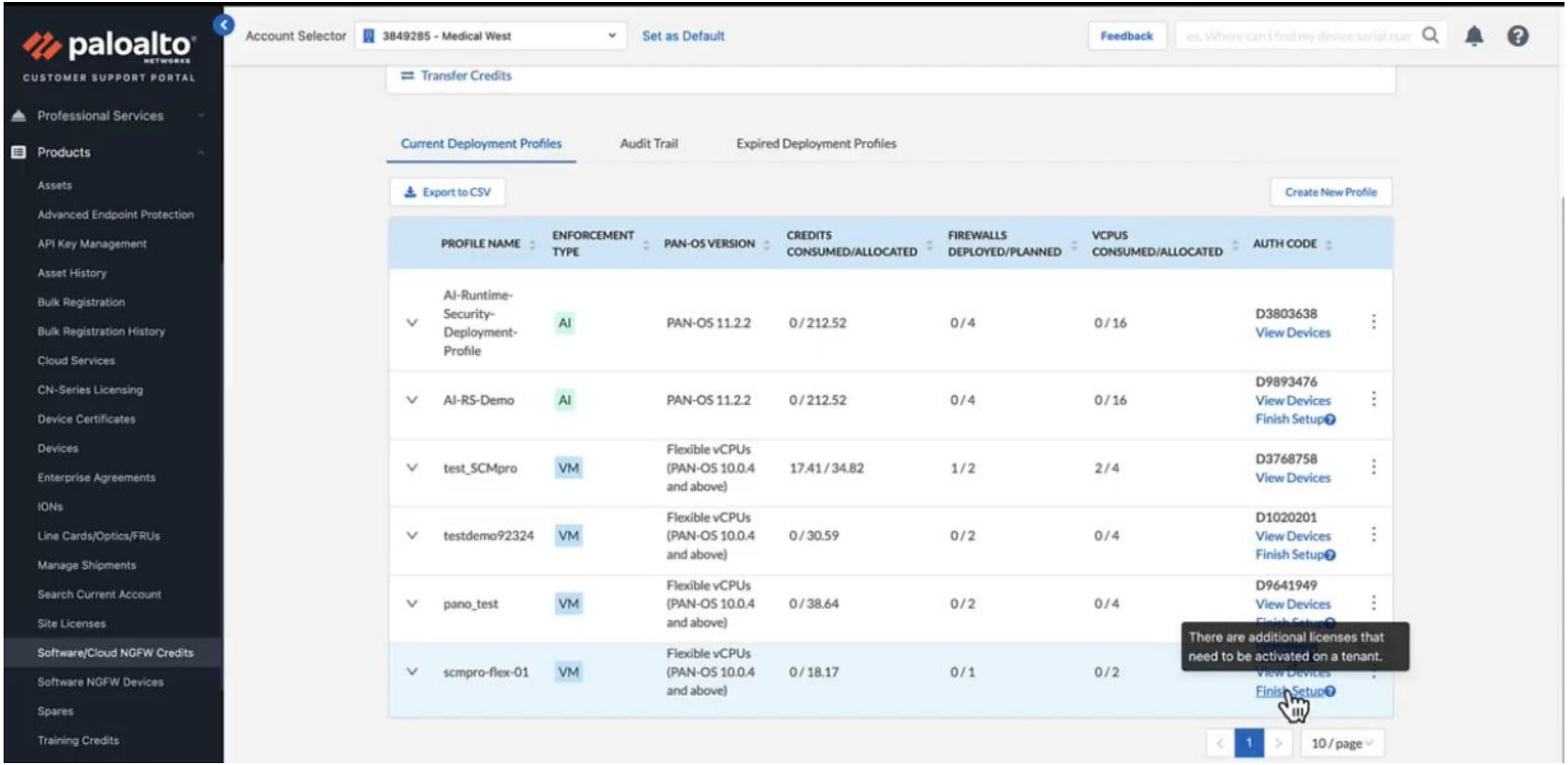
VM-Series firewall Onboard to SCM Process

CSP/TSG

NGFW

- Create Deployment Profile
- Associate Deployment Profile to TSG

Proceed to Finish Setup



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)

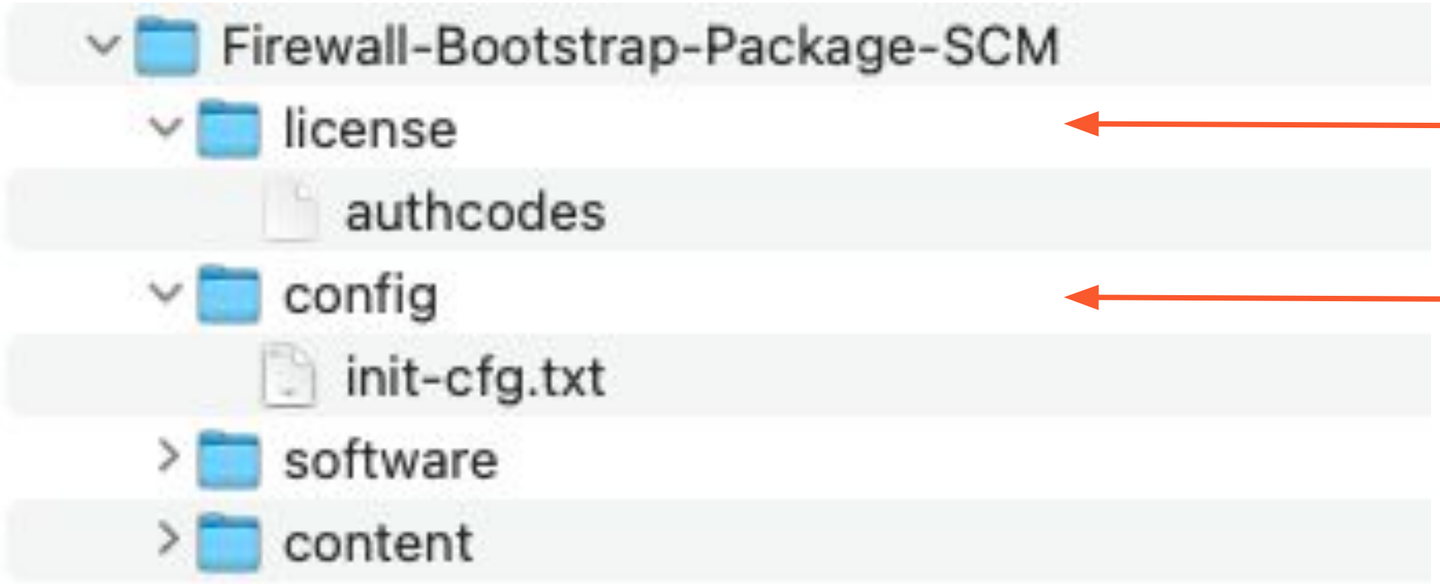
CSP/TSG

- 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:

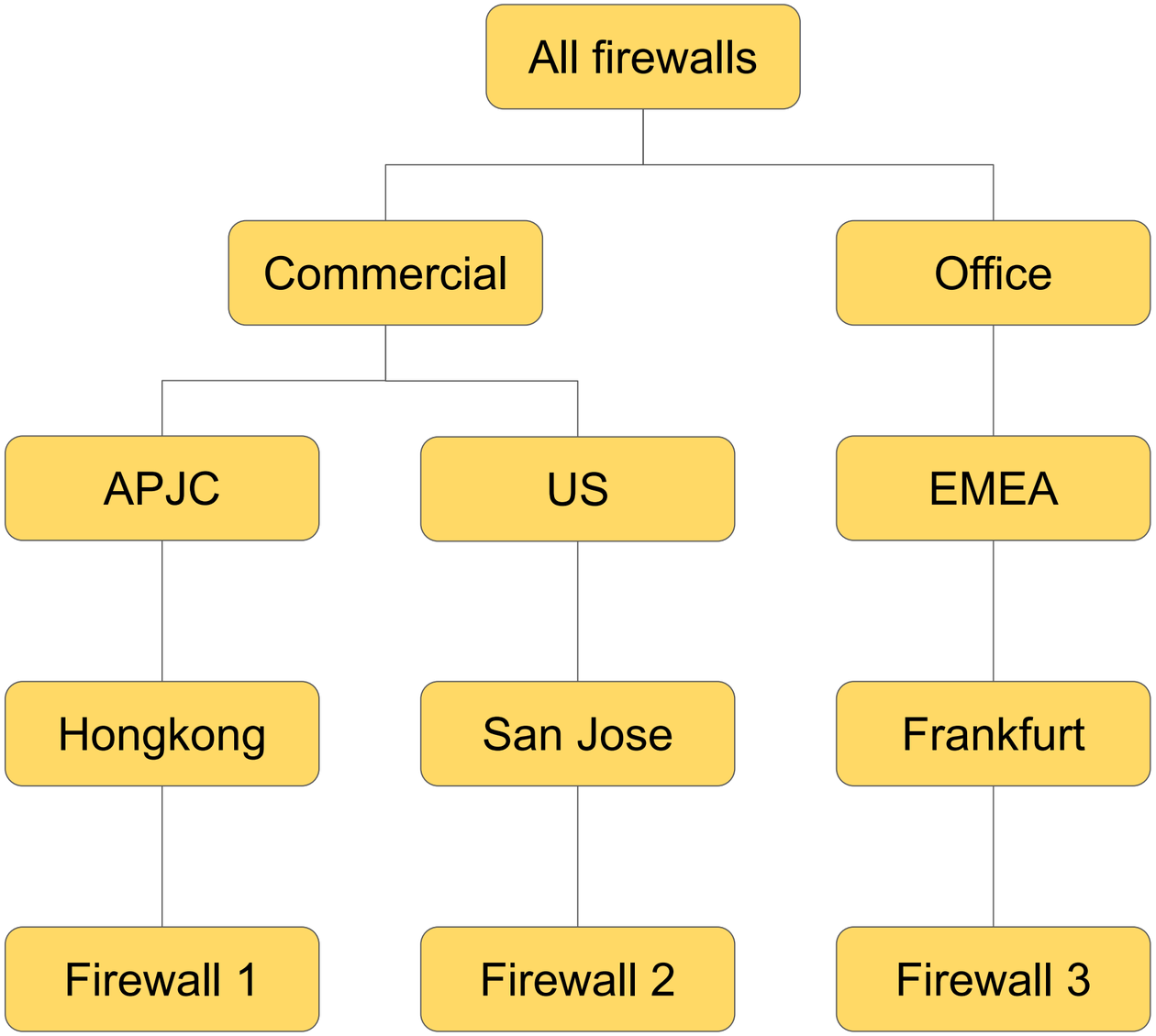
1. Join Webex meeting with your email address
2. Follow the lab instructions to use the authcode to generate the firewall serial number
3. Post the NGFW 1 and NGFW 2 Serial number into the chat with your Pod number and email address
4. Instructor will reply back with the OTP that you need for the next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

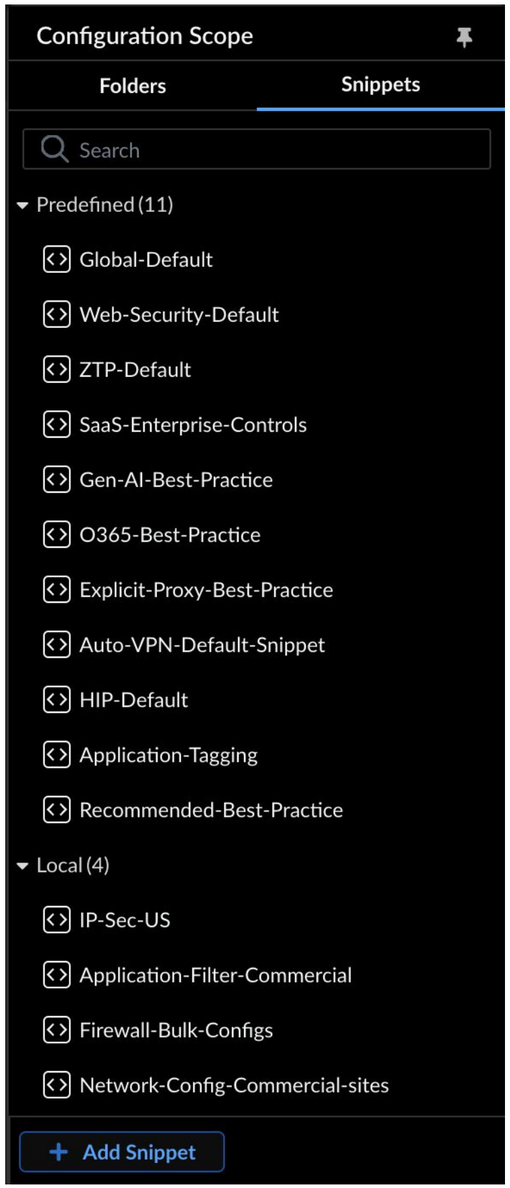
- Configuration Modifications
  The inherited configurations can be modified/overridden in the sub-folder level. The a inherited configuration ***cannot be deleted.*** *(can only be reverted back to inherited)*

- Folder Hierarchy Limits
  Four nested folder level under ***All Firewall*** *Folders*

Predefined Folders

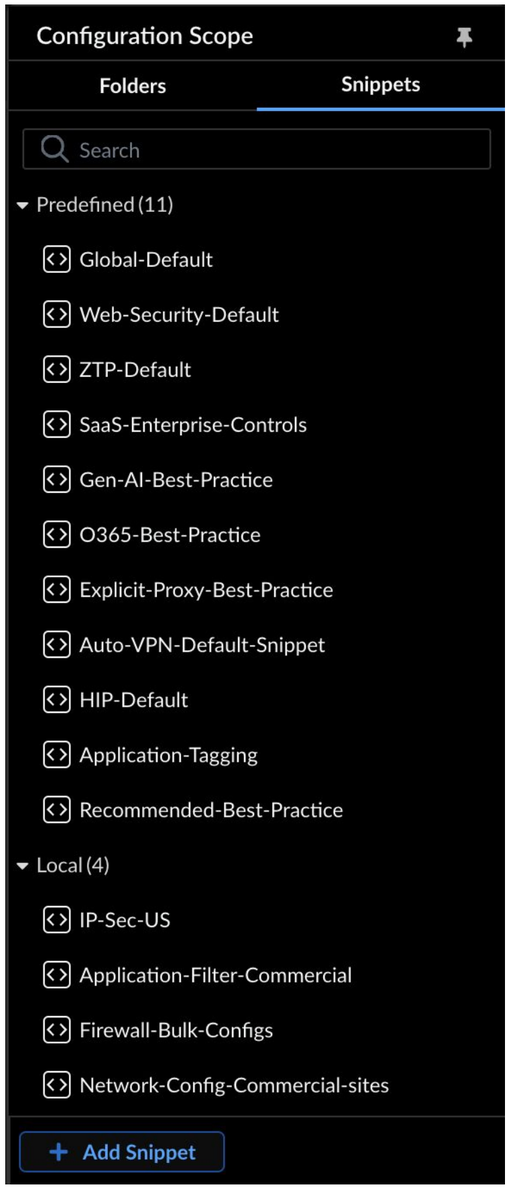
Global	The parent folder for all folders. Security rules added in this level will be applied to the entire Security Platform (Unified Security Configuration)
Prisma Access (Hierarchy)	Prisma Access Folder Hierarchy will appear only if you enabled Prisma Access. Prisma Access Folder Hierarchy will be 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.

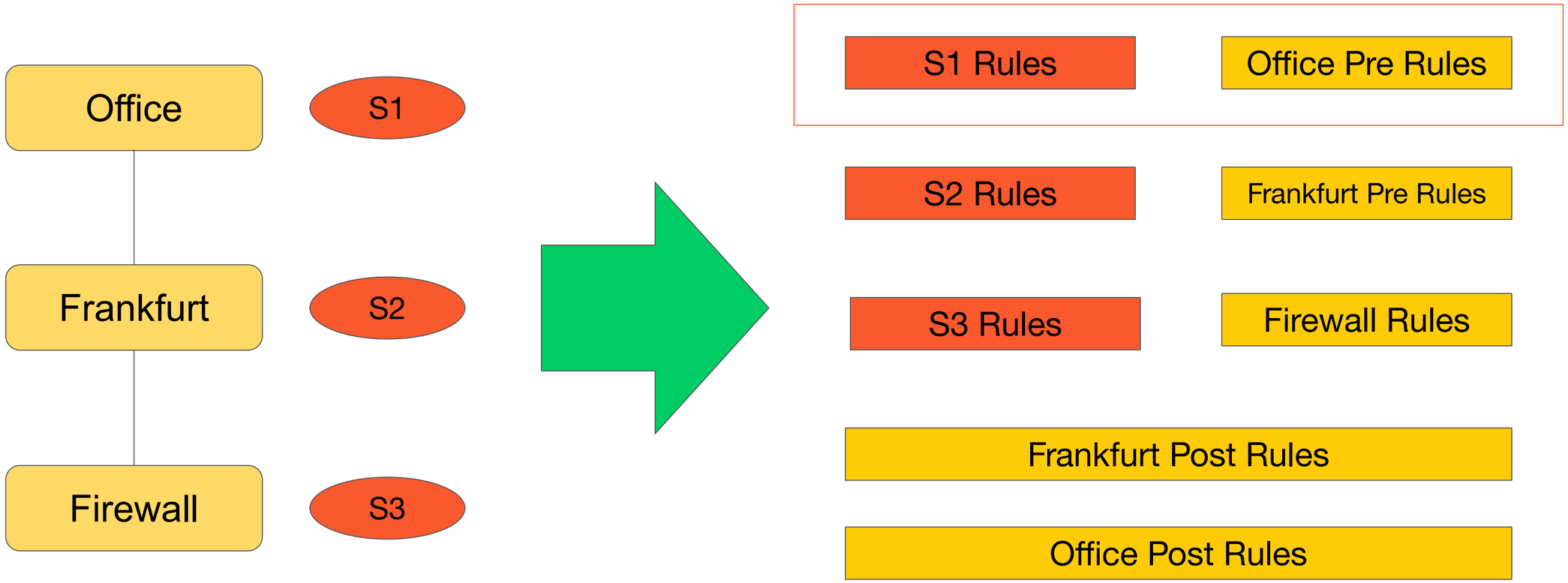
Snippets Use Case



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

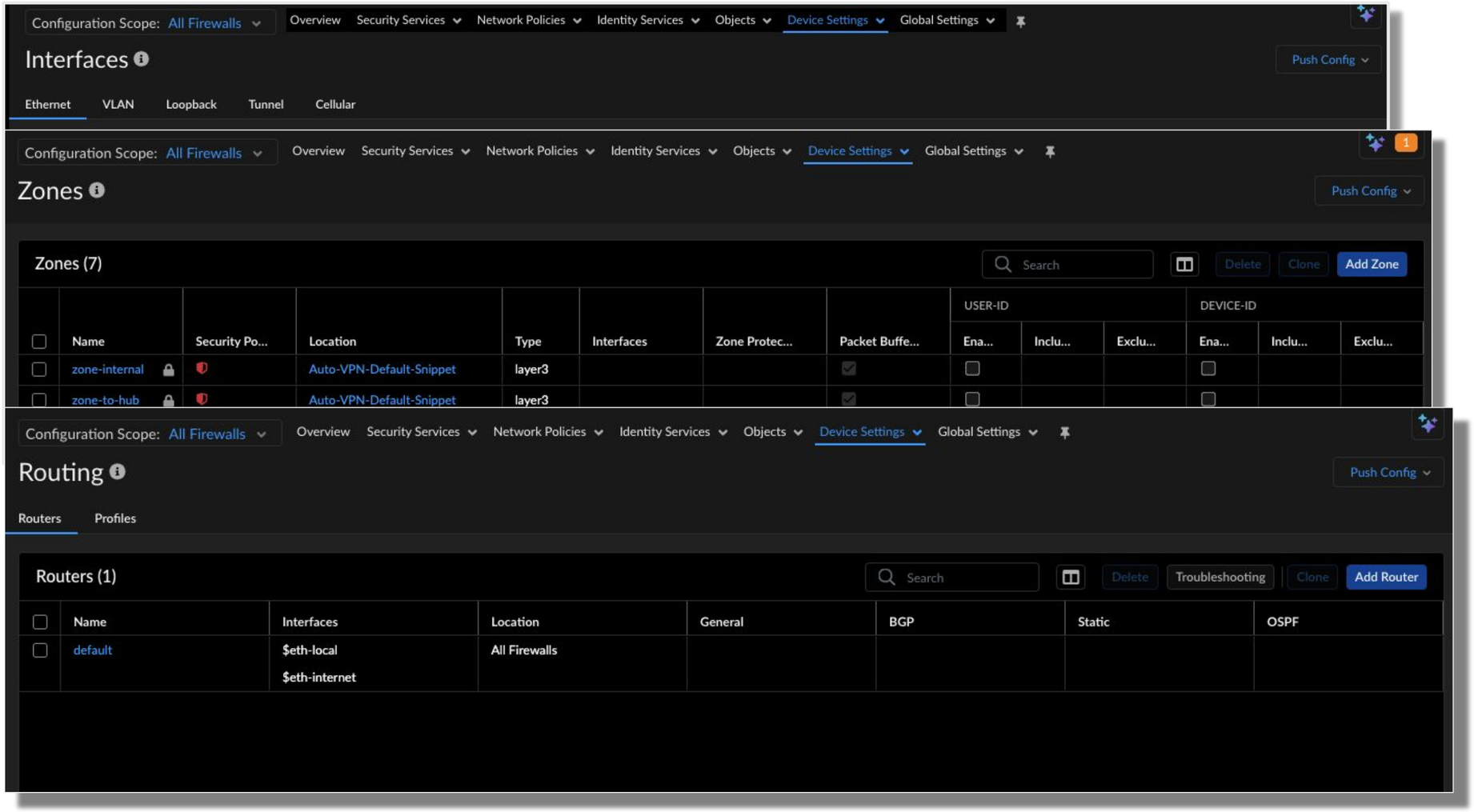
Security Rules Merge Logic (Folders + Snippets)

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)

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:

☐	$GUEST-GW		Commercial	$AE1.99	ip-netmask	10.0.99.1/24
☐	$EMPLOYEE-GW		Commercial	$AE1.90	ip-netmask	10.0.90.1/24
☐	$DIA1		Commercial	$AE1.998	ip-netmask	None
☐	$DIA2		Commercial	$AE1.999	ip-netmask	None

Frankfurt Commercial Site Level:

☐	$GUEST-GW		Commercial	$AE1.99	ip-netmask	10.0.99.1/24
☐	$EMPLOYEE-GW		Commercial	$AE1.90	ip-netmask	10.0.90.1/24
☐	$DIA1		Frankfurt-Commercial		ip-netmask	132.146.175.130/29
☐	$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