ordr

Ordr and Palo Alto Networks: Integration Guide

ORDR INTEGRATION GUIDE

An Introduction to Ordr Systems Control Engine

Digital transformation across healthcare, manufacturing, retail, transportation, and logistics is accelerating the hyper-connectedness of enterprise systems powered by IoT and connected OT devices. The enterprise IT network is now the melting pot for a highly eclectic mix of devices that businesses must manage and protect or face an immediate security risk.

The Ordr Systems Control Engine allows organizations to rapidly inventory every thing in your domain, classify it based on device type and business function, and assess it for risk. It learns behaviors and creates device flow genomes, so you'll know what each device or group of devices should be talking to. When combined with Palo Alto Networks next-generation firewalls, customers can quickly deploy Zero Trust policy enforcement and microsegmentation to isolate groups or individual devices from non-essential access while protecting them from attack and compromise.

This guide describes in detail how Ordr Systems Control Engine integrates with Palo Alto Networks industry-leading Next-Generation Firewalls including centralized management with Panorama to deliver unparalleled visibility and protection through advanced IoT/OT device discovery, classification, and the automation of secure access control and microsegmentation policy to all networked users and devices across the enterprise campus, industrial zones, data center, and internet edge.

Table of Contents

Introduction

The combination of Ordr Systems Control Engine and Palo Alto Networks Next-Generation Firewalls enables customers to keep pace with explosive growth of Internet of Things (IoT) and Operational Technology (OT) devices on the network. IoT/OT spans a wide range of devices including media/entertainment, building automation, manufacturing control, healthcare services, financial transactions, office equipment, power generation, and location/tracking. Virtually any device including a coffee maker or refrigerator can be connected to the network to offer unprecedented automation, management, monitoring, and data sharing.

IoT and OT devices present unique challenges to access control. Most have no user associated with the device and offer no means to authenticate themselves to the network or the firewall. To reduce costs and simplify network connectivity, IoT devices often run rudimentary or minimized versions of legacy operating systems. Most are closed systems with minimal or no patching capabilities to defend themselves. The installation of posture or other device management agents is rarely an option. Direct scanning or interrogation by profiling and security assessment tools are often restricted due to the fragile nature of the device's operating system or networking stack. This leaves critical devices vulnerable to service disruption, data theft, or compromise to serve as a launchpad for other attacks.

The most effective means to protect IoT and digital OT devices is through microsegmentation and strict Zero Trust policies that limit access to only that required for a device to properly function while protecting it from unauthorized access and attack. Ordr SCE monitors all device communications to automatically establish the flow genome—a baseline of normal and approved behavior—by device and device group. The flow genome serves as the basis for anomalous behavior detection as well as the generation of access and microsegmentation policy.

To deploy granular policies at scale for the multitude of IoT/OT devices requires powerful enforcement solutions. Rapid device discovery and accurate classification must also scale to the diverse and meteoric growth of IoT/OT devices that continuously appear on the network. Manual processes cannot keep pace, so it is crucial that organizations deploy automated solutions to simplify and streamline network security operations.

The Ordr and Palo Alto Networks solution combines the industry's most scalable IoT discovery, classification, and automated policy engine from Ordr with the industry's most advanced and powerful firewalls from Palo Alto Networks to deliver world-class IoT device security and protection.

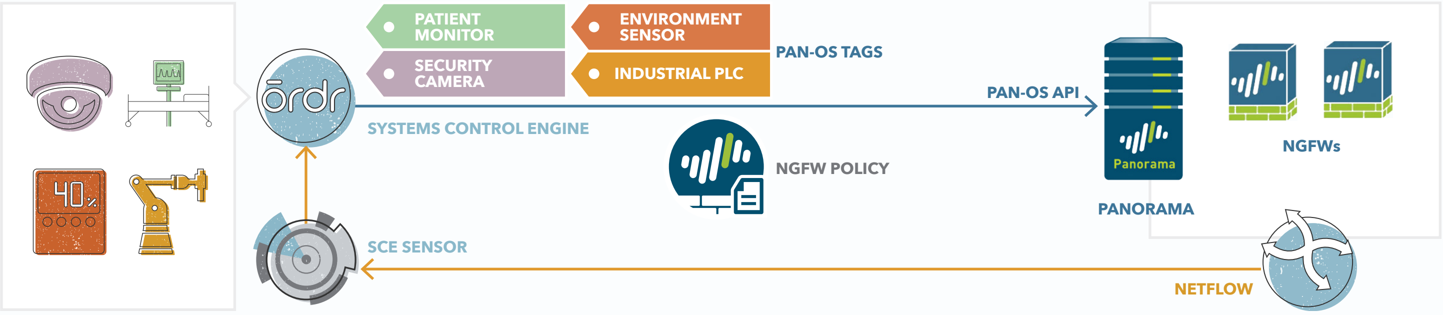
Ordr and Palo Alto Networks Use Cases

Ordr Systems Control Engine (SCE) complements and enhances the power of Palo Alto Networks (PAN) Next-Generation Firewall (NGFW) through the following use cases:

1. Automatic mapping of IoT/OT devices to PAN-OS Tags for simplified policy definition
2. Dynamic security policy rule generation based on PAN-OS Tags
3. Automatic downgrade of security threats subsequently blocked by NGFW
4. Enhancing flow visibility using NetFlow export in NGFW

The diagram provides a high-level overview of the integration. First, Ordr SCE discovers, classifies and groups all devices such as medical IOT, manufacturing OT, and building automation. Groups are populated into NGFW as PAN-OS Tags and, in turn, into Dynamic Address Groups using the native PAN-OS API. Security Policy is then generated automatically in NGFW based on Ordr SCE baselines. Administrations may optionally choose to manually enter security policy rules into NGFW based on Ordr prescriptive guidance. Ordr SCE can be integrated with a standalone NGFW or to Panorama for comprehensive tag and policy automation for all your NGFWs.

In the example, different classes of IoT and OT devices are categorized and automatically mapped to tags within the NGFWs. Zero Trust security policy rules are generated and deployed automatically within NGFW modules to restrict device communications only to trusted peers, protocols, and applications (by App-ID, i.e. DICOM, BACnet, and Modbus). Finally, Ordr can consume flow information from NGFW to enhance visibility into device communications for traffic that may not pass directly through SCE Sensors. Example scenarios include a remote branch using an NGFW for local Internet access or firewalls used to microsegment traffic between servers in the data center or manufacturing devices within an industrial zone.



The remainder of this guide provides details on how to configure integration between Ordr SCE and Palo Alto Networks Next-Generation Firewalls as well as integration details for each of the above use cases.

Basic Setup and Configuration

Setup is a simple two-step process. Ordr SCE can integrate either directly with a standalone NGFW or with Panorama for seamless management of multiple NGFWs and firewall device groups. When integrated with Panorama, you can choose which device groups in Panorama receive dynamic tag and security policy updates.

Step 1: Configure Ordr SCE with PAN-OS API credentials

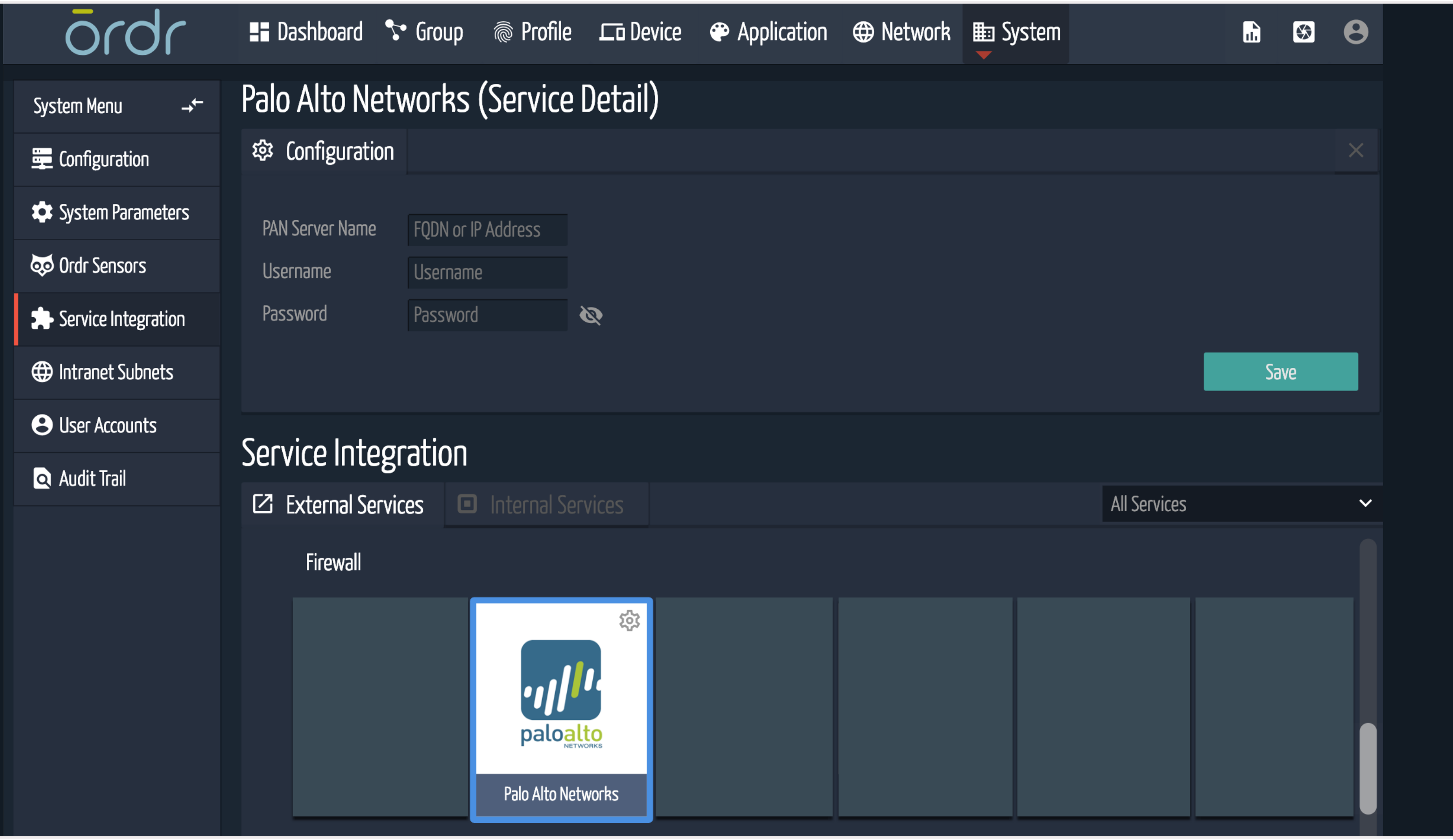
a. Login to the Ordr SCE administrative interface and navigate to **System** > **Service Integration** > **External Services**.

b. Under the **Firewall** section, select **Palo Alto Networks**.

c. Enter the **FQDN** or **IP address** of the Panorama Server. If not using Panorama, enter the FQDN or IP address of the standalone NGFW.

d. Enter the PAN-OS API **Username** and **Password**.

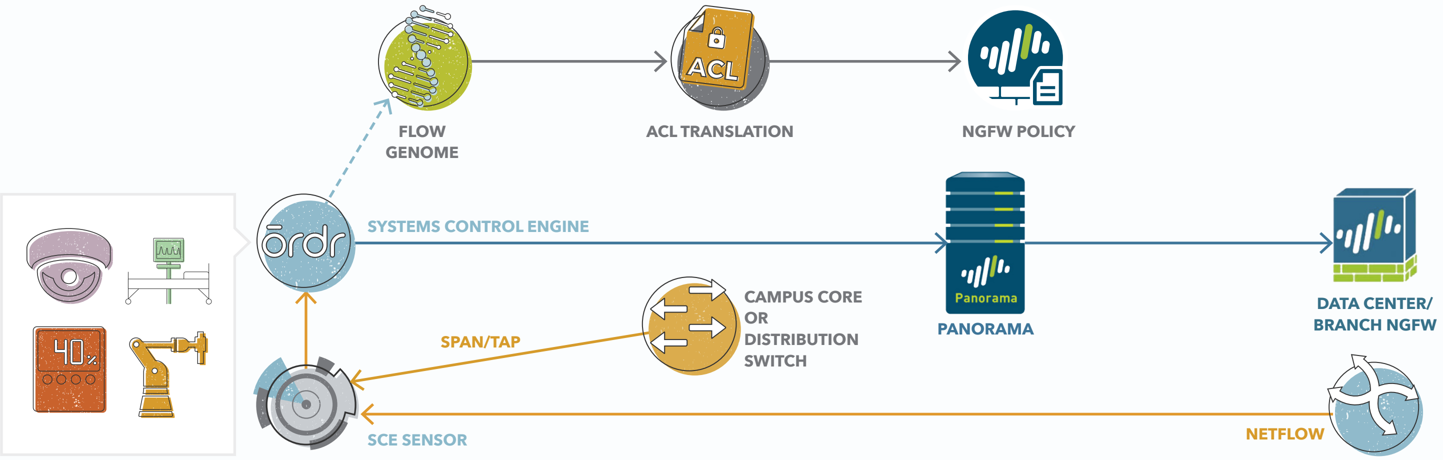
e. Click **Save** to commit the changes.



PAN Server Name: FQDN or IP Address
Username: Username
Password: Password

Step 2: Configure Panorama to send NetFlow to the SCE Sensor(s) [OPTIONAL]

This is an optional step for cases where traffic passing through an NGFW is not directly visible to SCE Sensors. Enabling NetFlow export to SCE Sensors allows NGFWs to act as mini-Sensors that augment the Device Flow Genome. The Device Flow Genome is the learned behavior for all devices and device profiles and is used to establish baselines for all normal and safe behavior. The Flow Genome serves as the basis for Anomaly Behavior Detection as well as dynamic policy generation.



The diagram above illustrates the SCE Sensor receiving direct flow information for traffic in the campus core or distribution but may not have visibility into some localized flows in the data center. Visibility of these localized flows can be learned from an NGFW in the data center through NetFlow. The flow data is used to augment the Flow Genome in Ordr SCE. This information is used to detect anomalous server traffic as well as to augment the ACL enforcement policy for inter-server traffic. The policy is then pushed to the NGFW to enforce both North-South traffic as well as lateral East-West traffic in the data center.

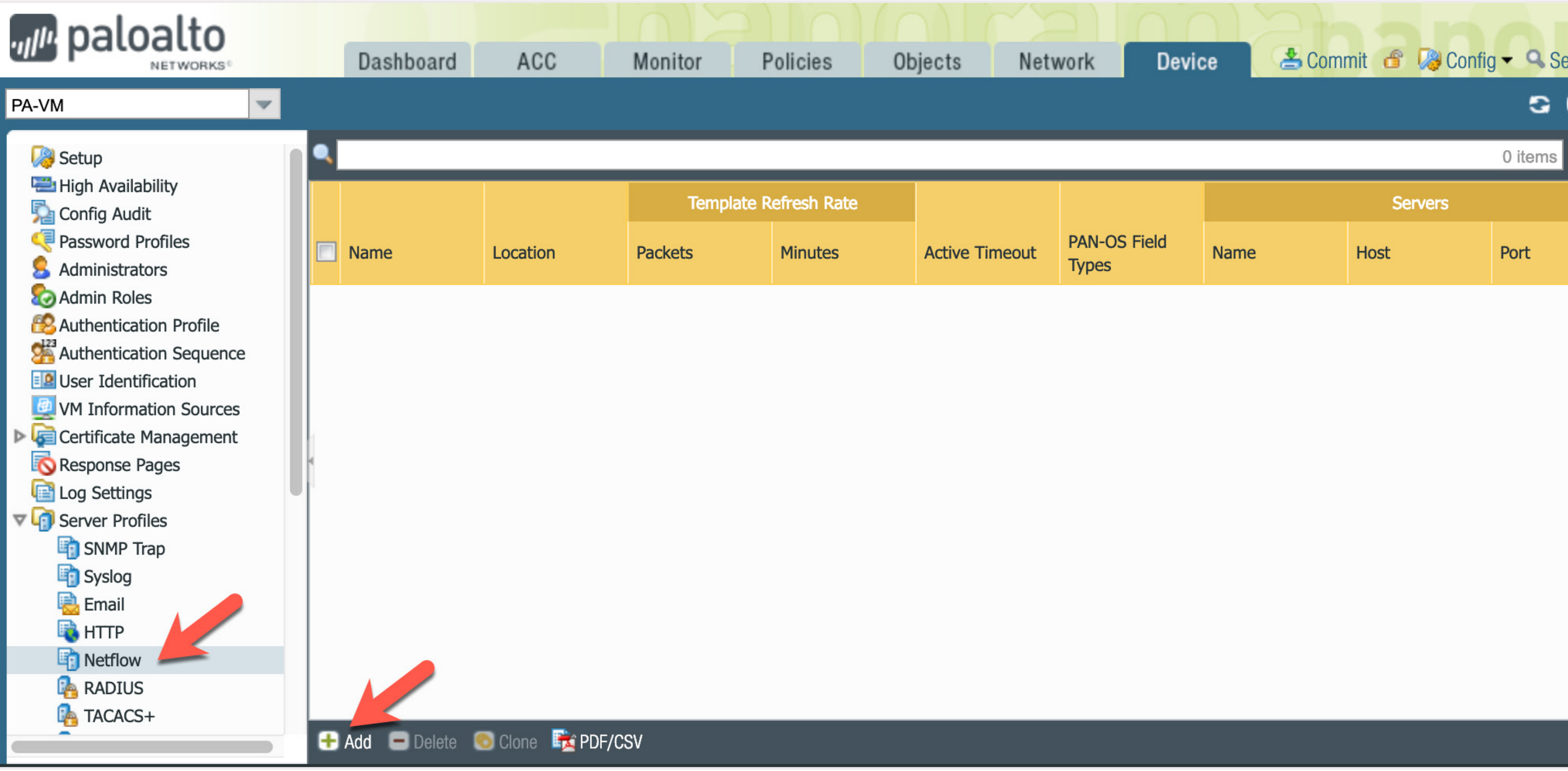
a. Login to the Panorama management server (or directly to specific firewall management interface) and navigate to **Device** > **Service Profiles** > **Netflow**.

b. From Panorama, change the Context to the specific NGFW where NetFlow is to be configured.

NOTE

It is generally recommended that each firewall send NetFlow to the closest SCE Sensor on the network.

c. Click **Add** from the bottom menu.



		Template Refresh Rate				Servers		
□ Name	Location	Packets	Minutes	Active Timeout	PAN-OS Field Types	Name	Host	Port

d. Enter the NetFlow Server Profile **Name**.

e. The Template Refresh Rate determines how often the template refreshes with its peers based on the number of minutes or packet count. Target systems cannot process NetFlow until the template received, so it is recommended to change Minutes from the default value of 30 to **1** to minimize gaps whenever NetFlow services restart.

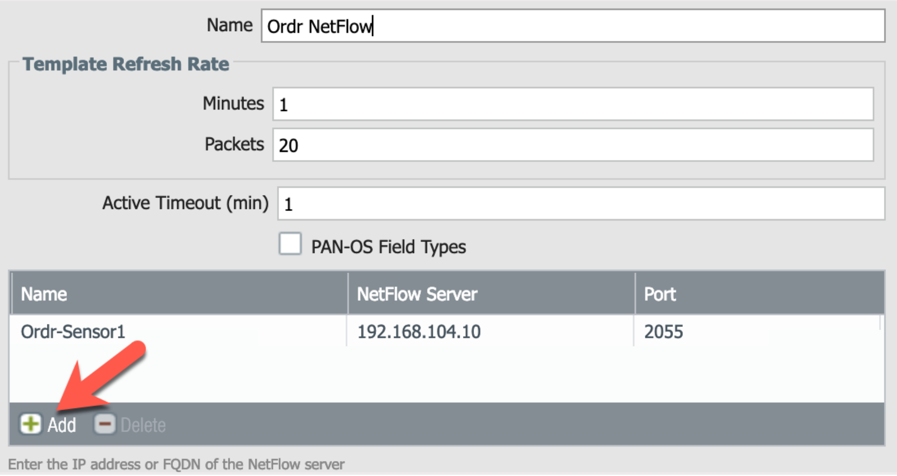
f. The Active Timeout determines the time after which flows are exported. To avoid excessively large bursts, it is recommended to change the default value of 5 minutes to **1** minute.

g. Click **Add** at the bottom left of the form to add the SCE Sensor as a NetFlow target.

h. Enter the **Name**, **FQDN** or **IP address**, and **Port** of the target SCE Sensor.

NOTE

By default, SCE Sensors support NetFlow collection on UDP ports 9995 and 2055. It is possible to add multiple targets to a single profile, but it is generally recommended to limit NetFlow export to a single SCE Sensor.



Name: Ordr NetFlow

Template Refresh Rate

Minutes: 1

Packets: 20

Active Timeout (min): 1

□ PAN-OS Field Types

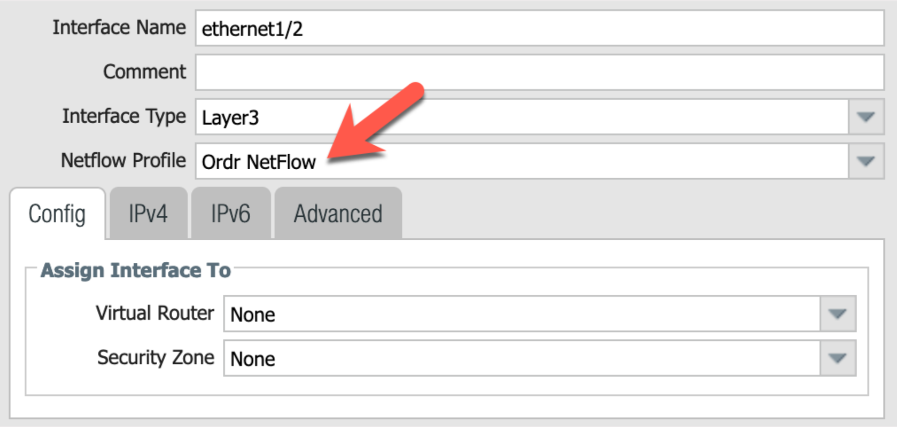
Name	NetFlow Server	Port
Ordr-Sensor1	192.168.104.10	2055

Enter the IP address or FQDN of the NetFlow server

i. Click **OK** when finished.

j. Navigate to **Network** > **Interfaces** > **Ethernet** and select the interface where device traffic enters the firewall. NetFlow Server Profiles are supported on Layer 3, Layer 2, virtual wire, tap, VLAN, loopback, and tunnel interfaces. For an Aggregate Ethernet (AE) Interface, you can export records for the aggregate group but not for individual interfaces within the group.

k. Select the **Netflow Profile** from the drop-down field.



Interface Name: ethernet1/2

Comment:

Interface Type: Layer3

Netflow Profile: Ordr NetFlow

Assign Interface To

Virtual Router: None

Security Zone: None

l. Click **OK** when finished.

m. Repeat the previous steps for each interface where flow data should be captured.

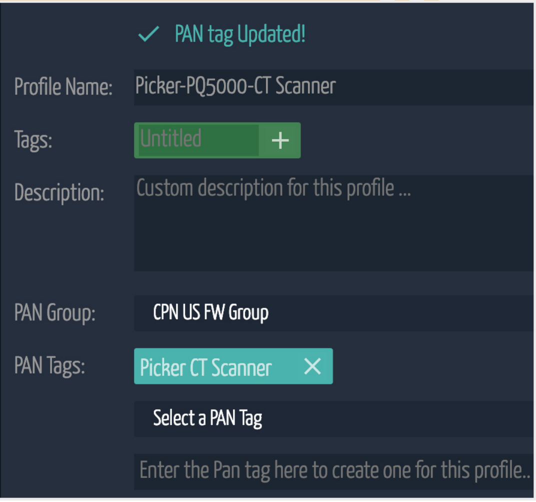
n. Remember to **Commit** and **Push** changes to Panorama and the device groups (or **Commit** on standalone NGFW) to activate the new configuration.

High-Level Overview of Ordr SCE and Palo Alto Networks NGFW Integration Steps

This guide provides detailed configuration steps as well as background explanations behind each of the use cases to integrate Ordr Systems Control Engine with Panorama and NGFW. However, the actual integration process is extremely simple and entails the following two key steps:

1. Assign PAN-OS Tags to Ordr SCE Device Profiles

STEP 1



✓ PAN tag Updated!

Profile Name: Picker-PQ5000-CT Scanner

Tags: Untitled +

Description: Custom description for this profile ...

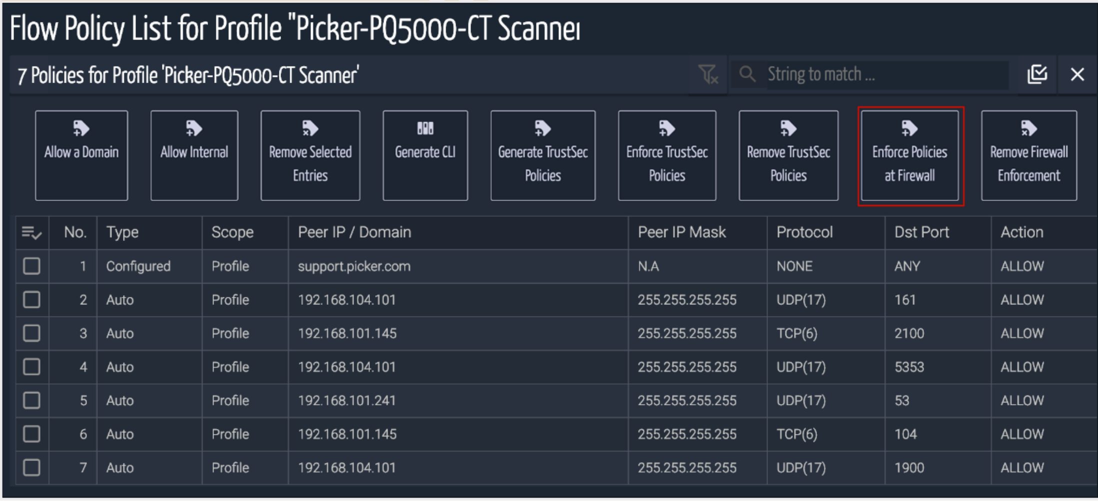
PAN Group: CPN US FW Group

PAN Tags: Picker CT Scanner ×

Select a PAN Tag

Enter the Pan tag here to create one for this profile..

STEP 2



Flow Policy List for Profile "Picker-PQ5000-CT Scanne

7 Policies for Profile 'Picker-PQ5000-CT Scanner'

String to match ...
Allow a Domain
Allow Internal
Remove Selected Entries
Generate CLI
Generate TrustSec Policies
Enforce TrustSec Policies
Remove TrustSec Policies
Enforce Policies at Firewall
Remove Firewall Enforcement

	No.	Type	Scope	Peer IP / Domain	Peer IP Mask	Protocol	Dst Port	Action
□	1	Configured	Profile	support.picker.com	N.A	NONE	ANY	ALLOW
□	2	Auto	Profile	192.168.104.101	255.255.255.255	UDP(17)	161	ALLOW
□	3	Auto	Profile	192.168.101.145	255.255.255.255	TCP(6)	2100	ALLOW
□	4	Auto	Profile	192.168.104.101	255.255.255.255	UDP(17)	5353	ALLOW
□	5	Auto	Profile	192.168.101.241	255.255.255.255	UDP(17)	53	ALLOW
□	6	Auto	Profile	192.168.101.145	255.255.255.255	TCP(6)	104	ALLOW
□	7	Auto	Profile	192.168.104.101	255.255.255.255	UDP(17)	1900	ALLOW

2. Enforce Firewall Policy for the Ordr SCE Device Profile

That is essentially all there is to it. Everything else is completely automated by Ordr Systems Control Engine!

The remainder of this document provides in-depth configuration steps and integration details.

Automatic mapping of IoT/OT devices to PAN-OS Tags for simplified policy definition

Palo Alto Networks Next-Generation Firewalls allow administrators to assign tags to address objects, address groups (static and dynamic), zones, services, service groups and security policy rules. Tags greatly simplify firewall management and policy enforcement by associating devices with business relevant labels and group assignments. Traditional firewall policy based on IP addresses inhibits mobility, obfuscates security policy (business intent is not obvious based on IP addresses alone), and often increases overhead and time to deploy changes as device changes (adds, moves, deletions) require updates to security policy rules to account for IP address changes.

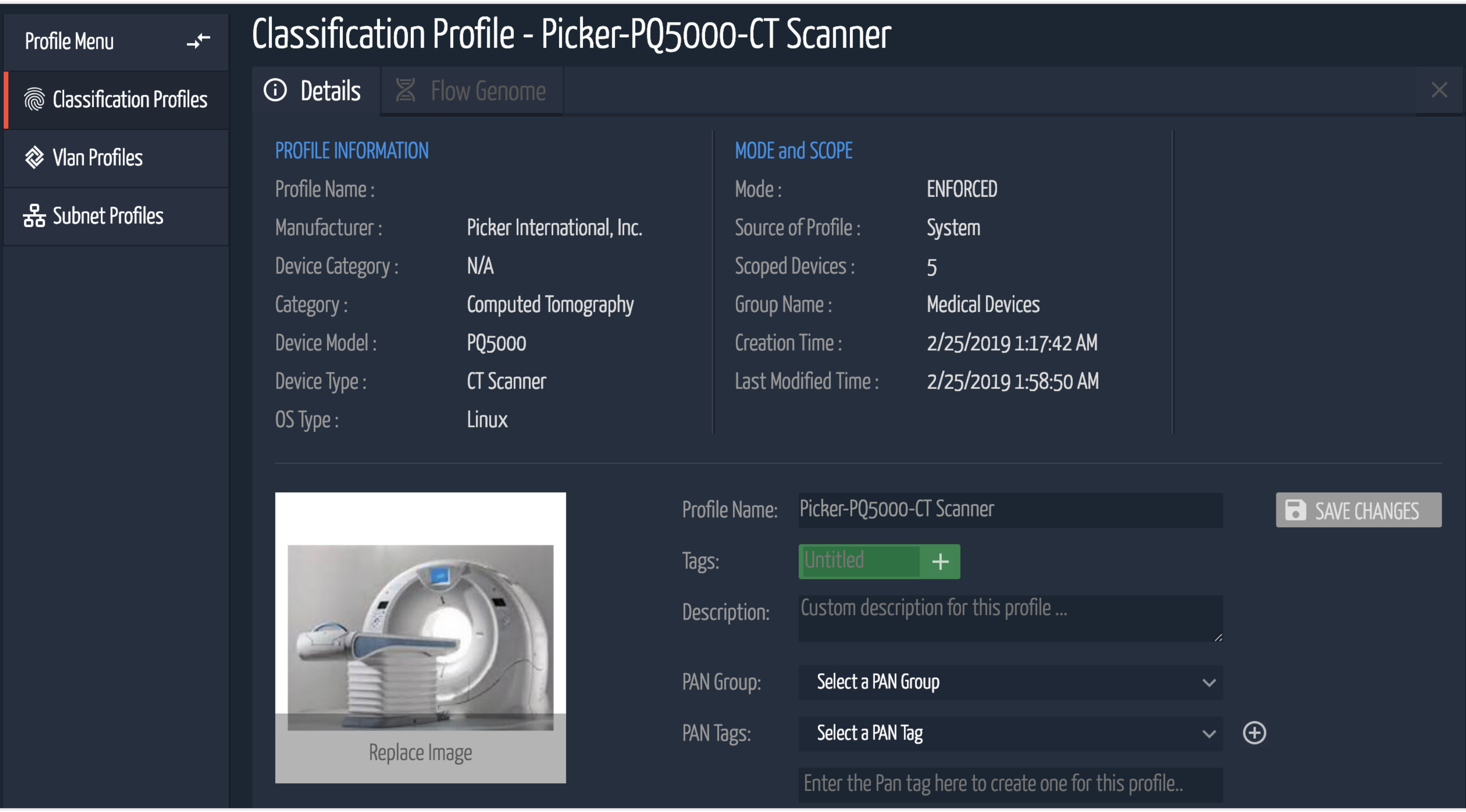
Rather than statically assigning a group of IoT devices such as network cameras or medical devices like CT Scanners to specific IP addresses then basing security policy on the static IP addresses, Dynamic Address Groups (DAGs) can be associated with a tag such as Network-Cameras or CT-Scanners and policy built on meaningful device types and roles. When changes occur to the group membership—even an IP address change for a group member—the security policy itself does not change, only the IP addresses of devices associated with the group, or tag. An added benefit in using Dynamic Address Groups is they allow the administrator to create a policy that automatically adapts to changes in membership—adds, moves, deletions—without the need to perform a commit to recognize changes.

Ordr SCE simplifies tag assignments in NGFW through auto-discovery, high-definition classification and grouping of devices, and dynamic update of tags and Dynamic Address Group membership. The resulting tags and matching Dynamic Address Groups can then be used to define Panorama and NGFW security policy rules. When assigning Ordr Classification Profiles to tags, the tags themselves can be preconfigured, or can be dynamically registered by Ordr SCE. Additionally, Ordr SCE allows administrators to choose which firewall device groups receive updates.

Step 1: Assign Ordr Classification Profiles to PAN Tags

a. Login to the Ordr SCE administrative interface and go to **Profiles** > **Classification Profiles**.

b. Navigate to the **Details** tab of the profile to be mapped to a tag. The profile for Picker-PQ5000-CT Scanners has been selected in the example below.



Classification Profile - Picker-PQ5000-CT Scanner

PROFILE INFORMATION

Profile Name :	
Manufacturer :	Picker International, Inc.
Device Category :	N/A
Category :	Computed Tomography
Device Model :	PQ5000
Device Type :	CT Scanner
OS Type :	Linux

MODE and SCOPE

Mode :	ENFORCED
Source of Profile :	System
Scoped Devices :	5
Group Name :	Medical Devices
Creation Time :	2/25/2019 1:17:42 AM
Last Modified Time :	2/25/2019 1:58:50 AM

Profile Name: Picker-PQ5000-CT Scanner

Tags: Untitled +

Description: Custom description for this profile ...

PAN Group: Select a PAN Group

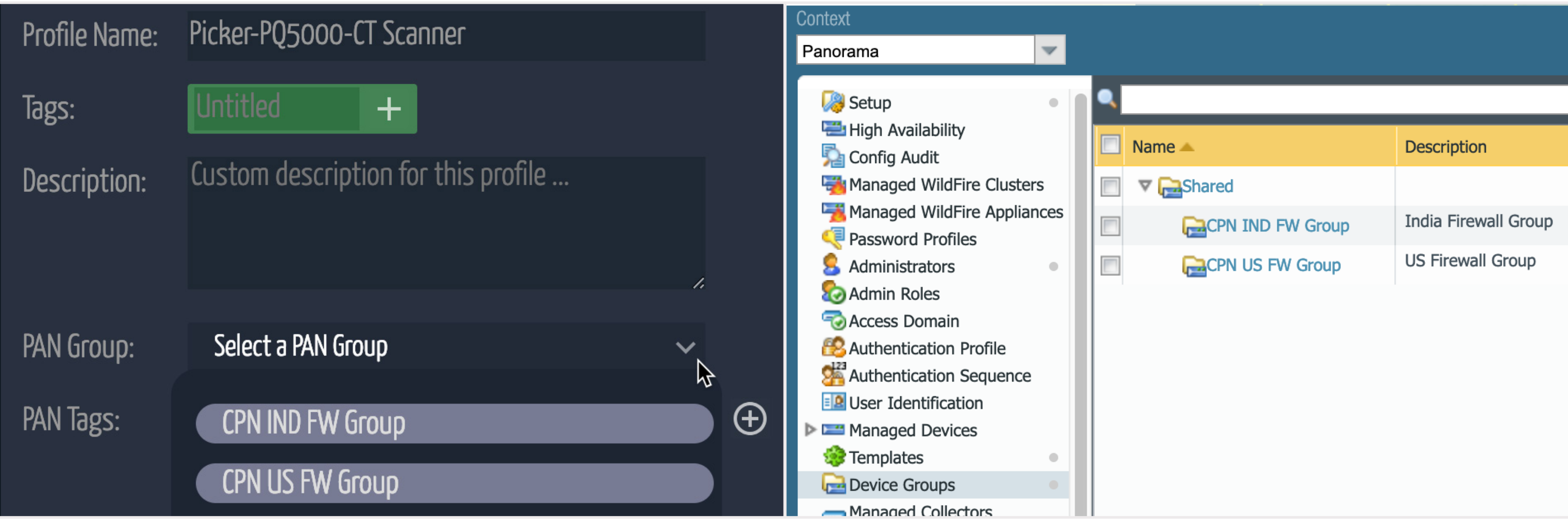
PAN Tags: Select a PAN Tag

Enter the Pan tag here to create one for this profile..

c. Under the PAN Group field (lower portion of the profile Details), select the appropriate firewall device group from the drop-down list. The list is automatically populated with the list of device groups configured in Panorama as shown in the example on the next page.

NOTE

If integrating Ordr SCE with a standalone NGFW, it is not necessary to specify a device group.



Profile Name: Picker-PQ5000-CT Scanner

Tags: Untitled +

Description: Custom description for this profile ...

PAN Group: Select a PAN Group

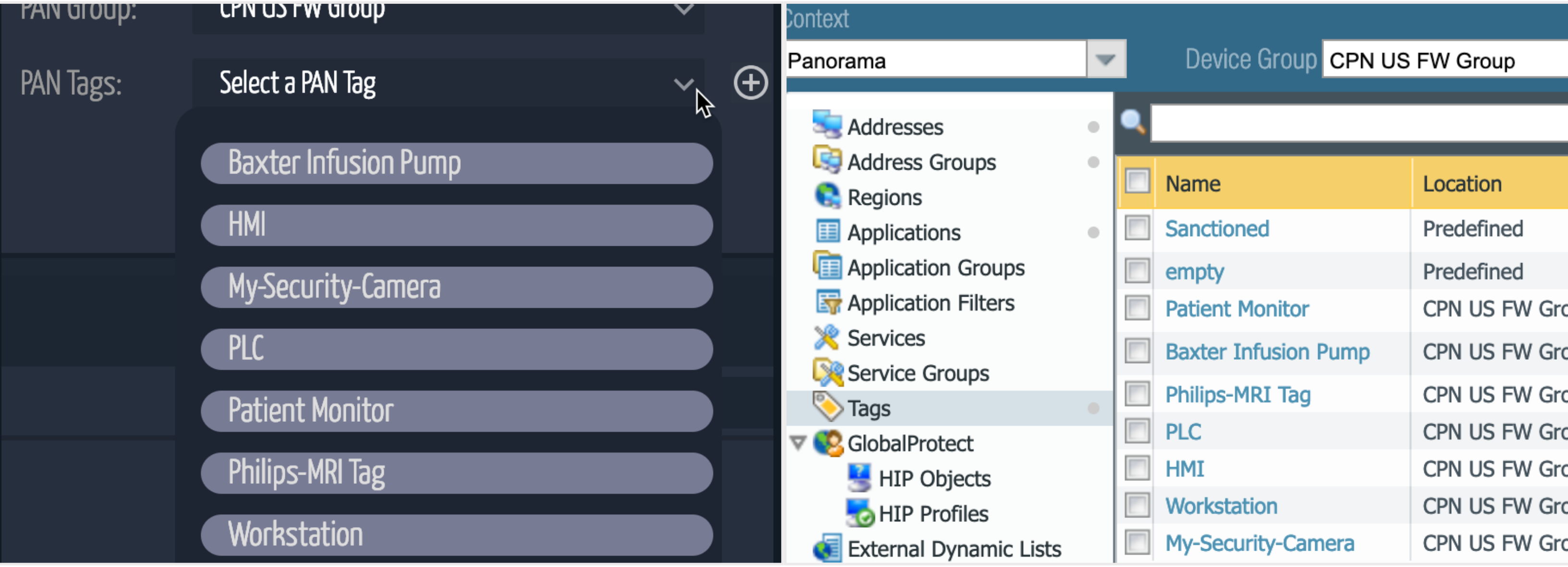
PAN Tags:

- CPN IND FW Group
- CPN US FW Group

Context: Panorama

□	Name	Description
□	Shared	
□	CPN IND FW Group	India Firewall Group
□	CPN US FW Group	US Firewall Group

d. Under the PAN Tags field, either select the name of an existing tag or enter a new tag name. The list of tags is automatically populated with the list of tags already configured in Panorama as shown in the example.



PAN Group: CPN US FW Group

PAN Tags: Select a PAN Tag

- Baxter Infusion Pump
- HMI
- My-Security-Camera
- PLC
- Patient Monitor
- Philips-MRI Tag
- Workstation

Context: Panorama

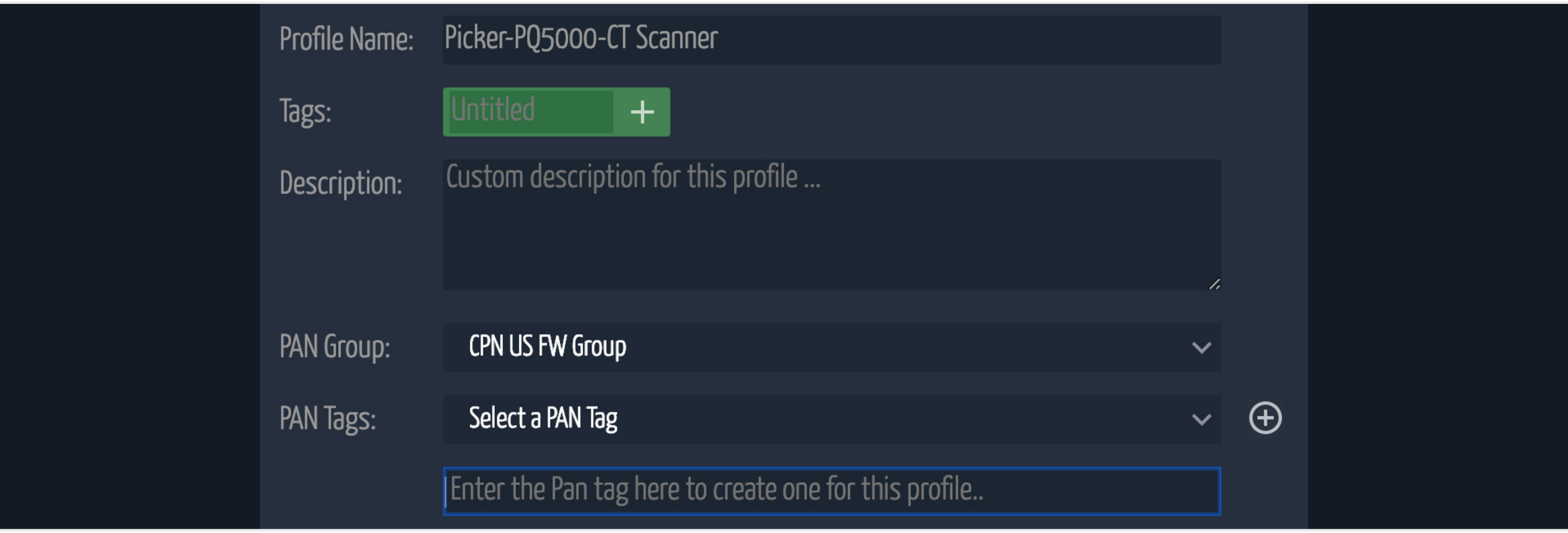
Device Group: CPN US FW Group

□	Name	Location
□	Sanctioned	Predefined
□	empty	Predefined
□	Patient Monitor	CPN US FW Gro
□	Baxter Infusion Pump	CPN US FW Gro
□	Philips-MRI Tag	CPN US FW Gro
□	PLC	CPN US FW Gro
□	HMI	CPN US FW Gro
□	Workstation	CPN US FW Gro
□	My-Security-Camera	CPN US FW Gro

NOTE

⊕ It is possible to assign multiple PAN Tags to each Classification Profile by selecting the tag from the drop-down list and using the **Add** icon. Additional details on multiple tag assignment provided at the end of this section.

If creating a new tag, enter the name to be populated in Panorama under the designated field.



Profile Name: Picker-PQ5000-CT Scanner

Tags: Untitled +

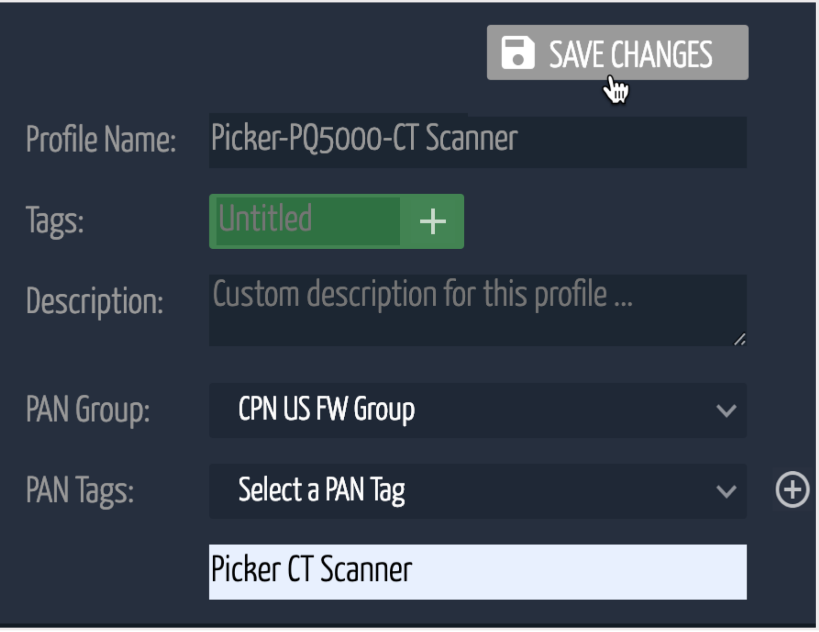
Description: Custom description for this profile ...

PAN Group: CPN US FW Group

PAN Tags: Select a PAN Tag

Enter the Pan tag here to create one for this profile..

SAVE CHANGES



Profile Name: Picker-PQ5000-CT Scanner

Tags: Untitled +

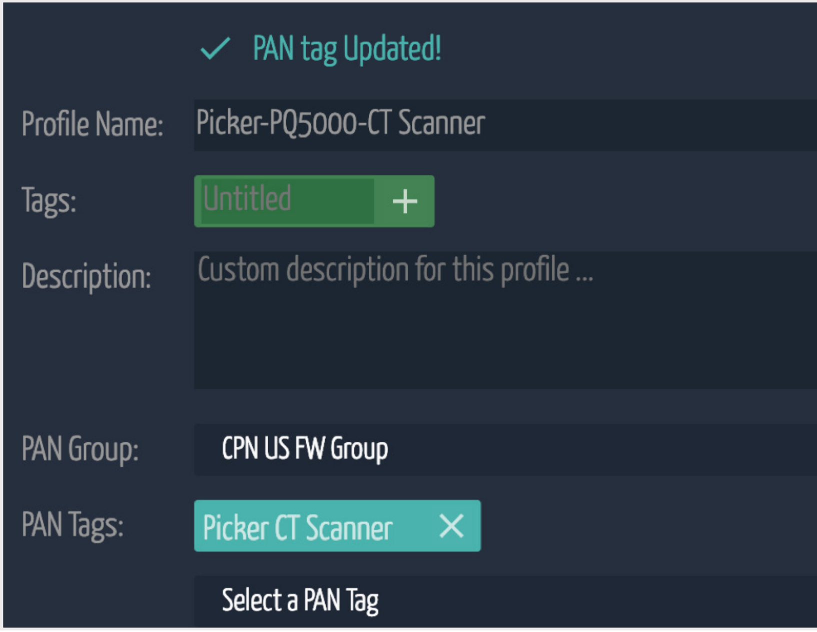
Description: Custom description for this profile ...

PAN Group: CPN US FW Group

PAN Tags: Select a PAN Tag

Picker CT Scanner

UPDATED PAN TAG



✓ PAN tag Updated!

Profile Name: Picker-PQ5000-CT Scanner

Tags: Untitled +

Description: Custom description for this profile ...

PAN Group: CPN US FW Group

PAN Tags: Picker CT Scanner ✕

Select a PAN Tag

e. A new PAN Tag labeled Picker CT Scanner is shown in the example above. Click **Save Changes** when finished updating the PAN Group and PAN Tags. A message will appear if update is successful as shown in the above example.

NOTE: REMOVING TAGS

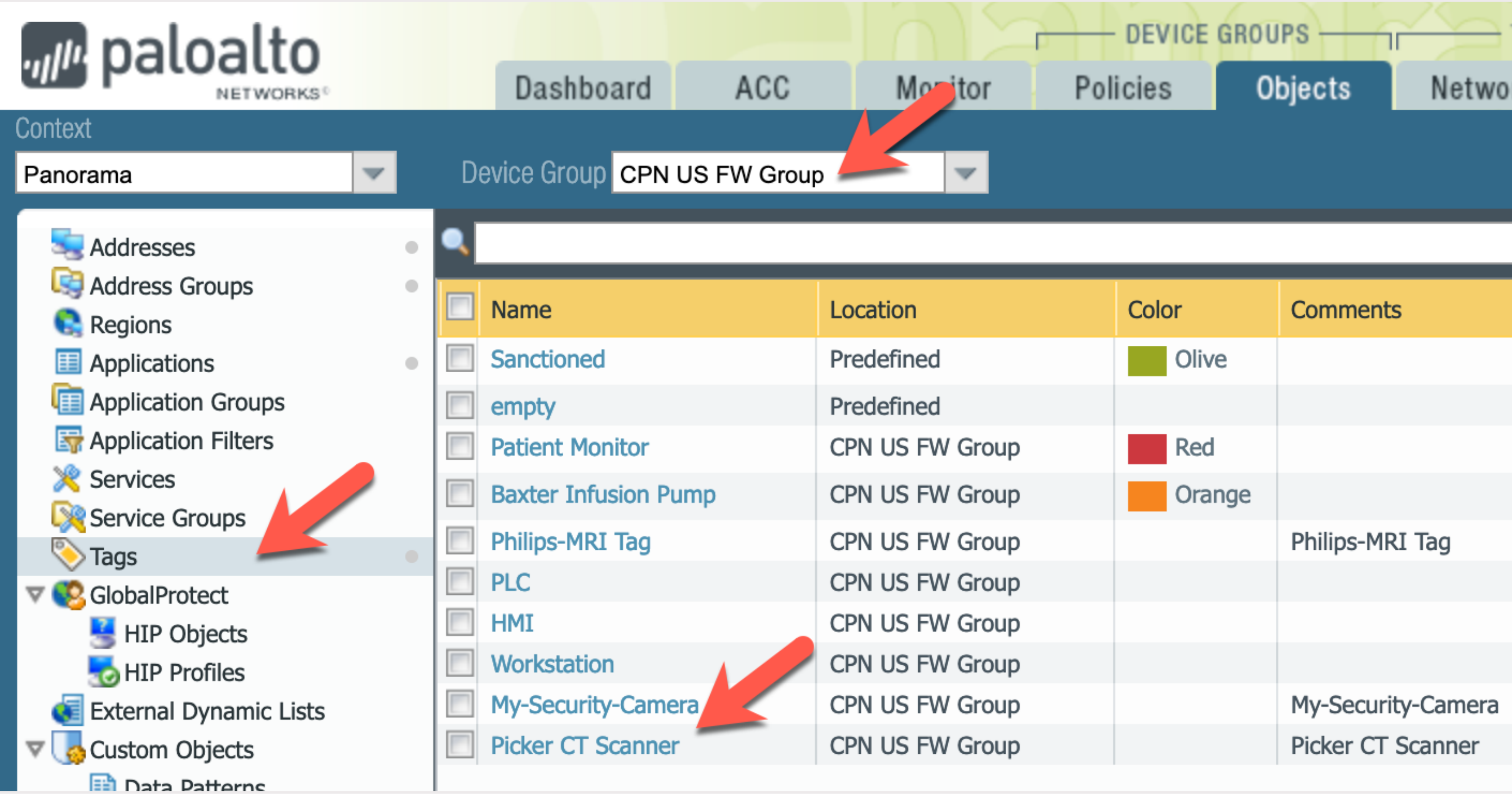
To remove the assigned tag, click the X next to the tag name under the PAN Tags field. This will also automatically remove any associations of member devices to the tag in Panorama.

If Firewall Policy is enforced using tags, be sure to remove the Firewall Policy Enforcement before removing the tag assignments. Additional information is provided in the policy enforcement section of this guide.

Step 2: Verify dynamic update to PAN-OS Tags

a. Verify changes made in Panorama (or standalone NGFW) by accessing the Panorama or NGFW web management interface and navigating to **Objects** > **Tags**.

b. Verify the correct Context and Device Group are selected. In the example below, the new Picker CT Scanner tag was defined for the CPN US FW Group.



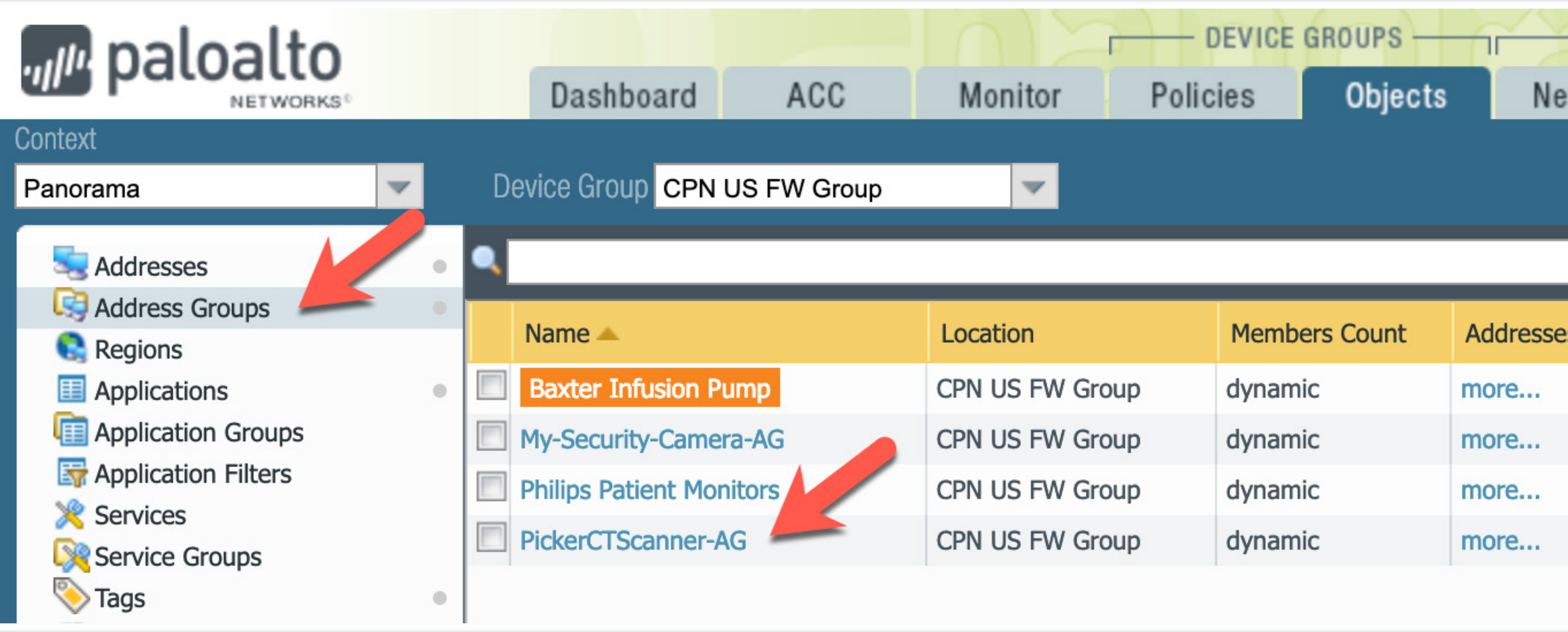
Context: Panorama

Device Group: CPN US FW Group

□	Name	Location	Color	Comments
□	Sanctioned	Predefined	🟩 Olive	
□	empty	Predefined		
□	Patient Monitor	CPN US FW Group	🟥 Red	
□	Baxter Infusion Pump	CPN US FW Group	🟧 Orange	
□	Philips-MRI Tag	CPN US FW Group		Philips-MRI Tag
□	PLC	CPN US FW Group		
□	HMI	CPN US FW Group		
□	Workstation	CPN US FW Group		
□	My-Security-Camera	CPN US FW Group		My-Security-Camera
□	Picker CT Scanner	CPN US FW Group		Picker CT Scanner

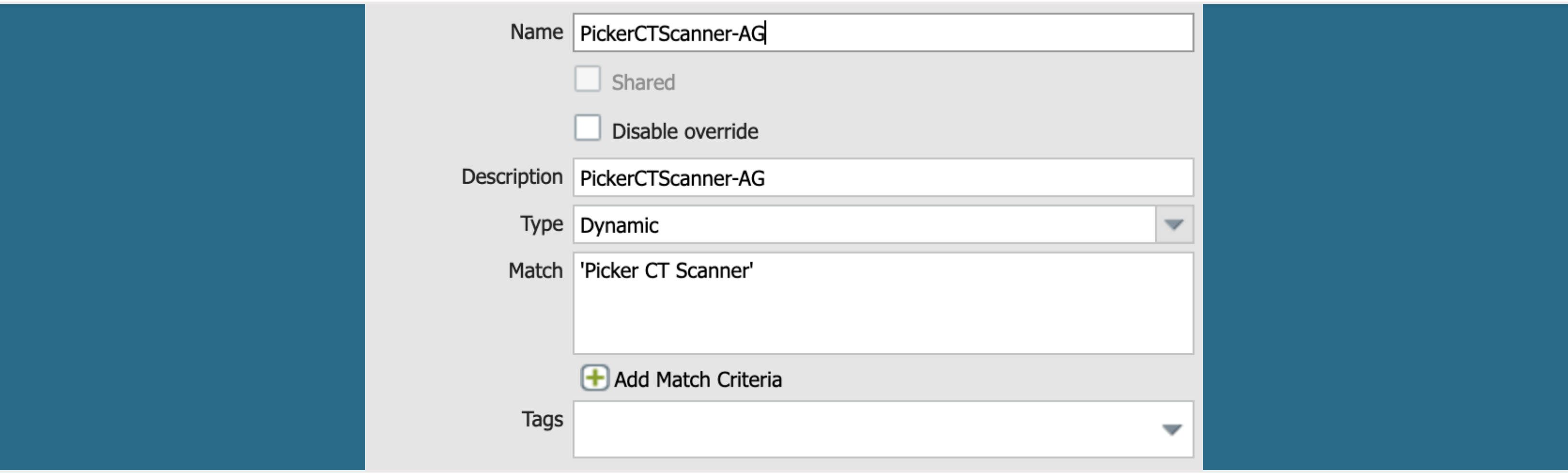
Step 3: Verify dynamic update to PAN Address Groups

a. Go to **Objects** > **Address Groups** to display the list of address groups. Confirm the existence of an address group that matches the new or updated tag. In the example, PickerCTScanner-AG was automatically created by Ordr SCE to match devices associated with tag "Picker CT Scanner."



	Name	Location	Members Count	Addresse
□	Baxter Infusion Pump	CPN US FW Group	dynamic	more...
□	My-Security-Camera-AG	CPN US FW Group	dynamic	more...
□	Philips Patient Monitors	CPN US FW Group	dynamic	more...
□	PickerCTScanner-AG	CPN US FW Group	dynamic	more...

b. Click on the Name of the new address group and verify the mapping between the tag and address group. In the example below, Address Group "PickerCTScanner-AG" is matched to Tag "Picker CT Scanner." The value for Type should be set to "Dynamic."

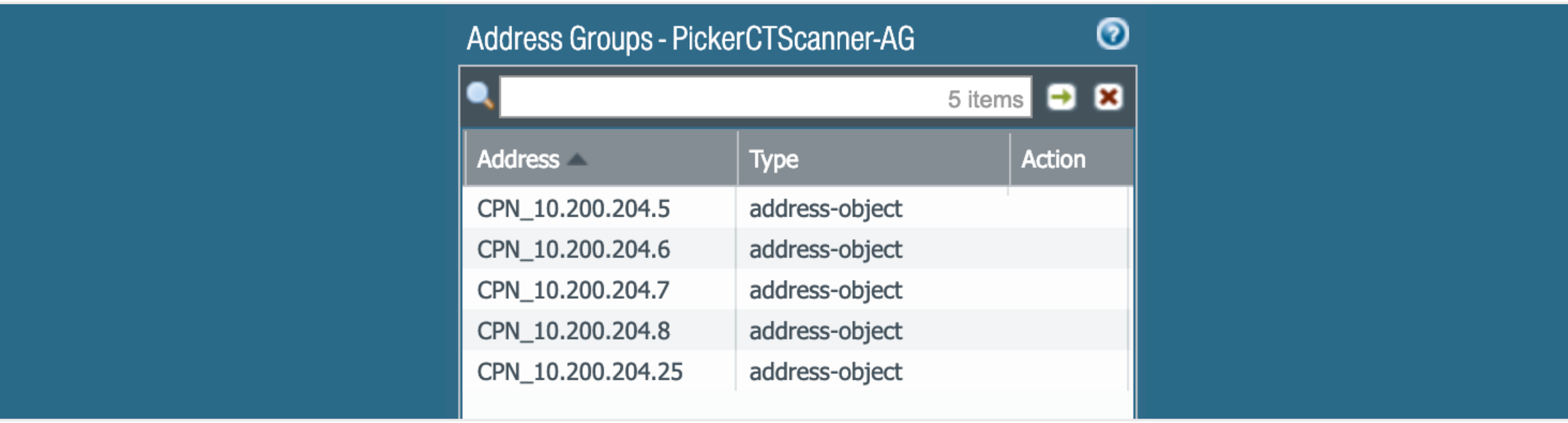


Name	PickerCTScanner-AG
	□ Shared
	□ Disable override
Description	PickerCTScanner-AG
Type	Dynamic
Match	'Picker CT Scanner'
	Add Match Criteria
Tags	

Step 4: Verify dynamic update of device membership in Dynamic Address Groups and Tags

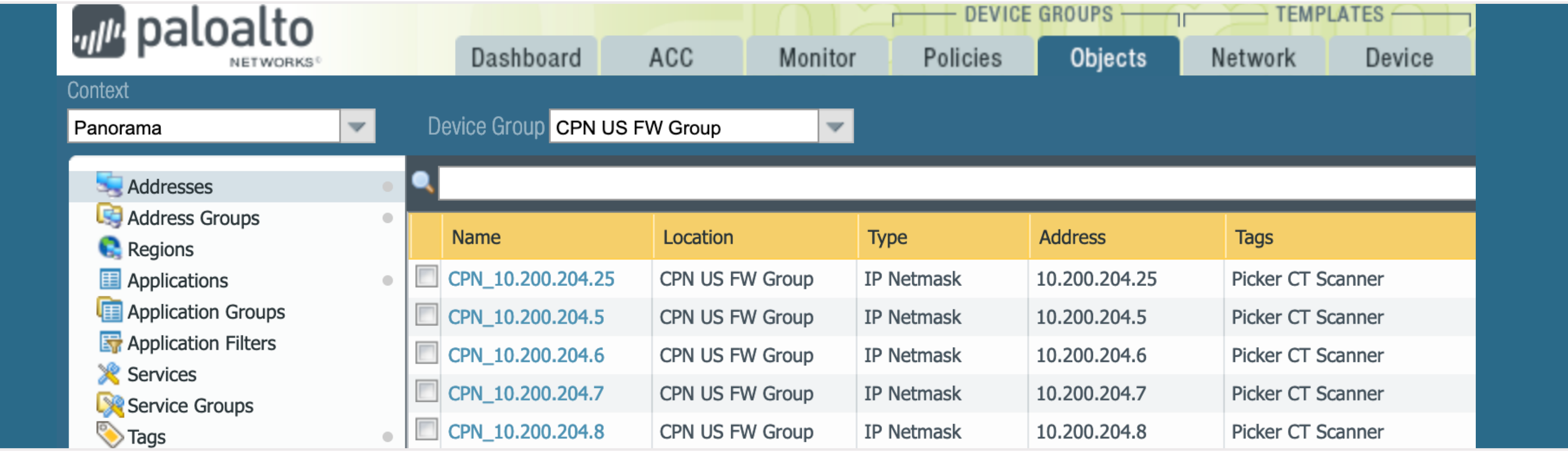
Each device matching a Classification Profile in Ordr SCE is automatically associated with its assigned PAN-OS Tag which, in turn, automatically populates the Dynamic Address Group member list.

a. Under **Objects** > **Address Groups**, click **more…** under the Addresses column for the newly updated address group.


Address Groups - PickerCTScanner-AG

Address	Type	Action
CPN_10.200.204.5	address-object	
CPN_10.200.204.6	address-object	
CPN_10.200.204.7	address-object	
CPN_10.200.204.8	address-object	
CPN_10.200.204.25	address-object	

b. Navigate to **Objects** > **Addresses** and view the IP addresses associated with the “Picker CT Scanner” tag.



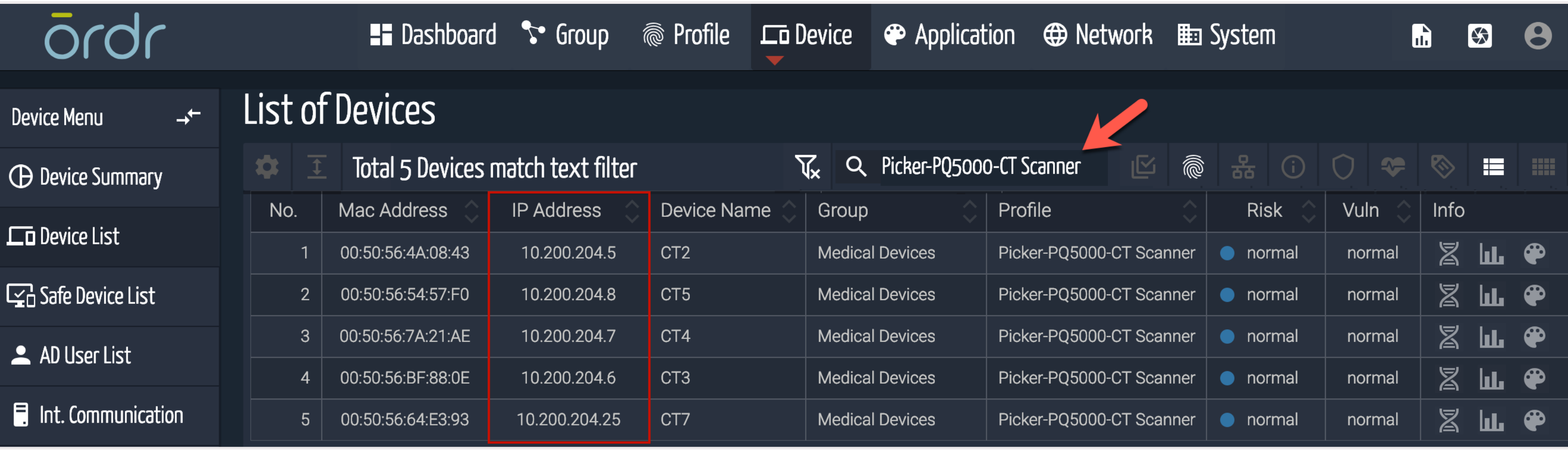
Context: Panorama

Device Group: CPN US FW Group

	Name	Location	Type	Address	Tags
□	CPN_10.200.204.25	CPN US FW Group	IP Netmask	10.200.204.25	Picker CT Scanner
□	CPN_10.200.204.5	CPN US FW Group	IP Netmask	10.200.204.5	Picker CT Scanner
□	CPN_10.200.204.6	CPN US FW Group	IP Netmask	10.200.204.6	Picker CT Scanner
□	CPN_10.200.204.7	CPN US FW Group	IP Netmask	10.200.204.7	Picker CT Scanner
□	CPN_10.200.204.8	CPN US FW Group	IP Netmask	10.200.204.8	Picker CT Scanner

c. The list of IP addresses above precisely matches the devices classified as Picker-PQ5000-CT Scanner in Ordr SCE as seen in the graphic on the next page, i.e. the Classification Profile mapped to the “Picker

CT Scanner" tag in our example.



No.	Mac Address	IP Address	Device Name	Group	Profile	Risk	Vuln	Info
1	00:50:56:4A:08:43	10.200.204.5	CT2	Medical Devices	Picker-PQ5000-CT Scanner	● normal	normal	
2	00:50:56:54:57:F0	10.200.204.8	CT5	Medical Devices	Picker-PQ5000-CT Scanner	● normal	normal	
3	00:50:56:7A:21:AE	10.200.204.7	CT4	Medical Devices	Picker-PQ5000-CT Scanner	● normal	normal	
4	00:50:56:BF:88:0E	10.200.204.6	CT3	Medical Devices	Picker-PQ5000-CT Scanner	● normal	normal	
5	00:50:56:64:E3:93	10.200.204.25	CT7	Medical Devices	Picker-PQ5000-CT Scanner	● normal	normal	

As new network devices are discovered and classified in the same Classification Profile, they are automatically added to the list of IP addresses for the matching tag in the firewalls. Furthermore, when Ordr SCE detects IP changes for existing member devices, the entries are automatically reflected in Panorama and updated to the NGFWs. Any devices reclassified or removed from the Ordr SCE Classification Profile are deleted from the PAN-OS Tag and its associated Dynamic Address Group.

Step 5: Assign multiple PAN-OS Tags to an Ordr SCE Classification Profile

Ordr SCE and Palo Alto Networks NGFWs support the assignment of multiple tags to the same IP address. It can often be useful to associate the same group of devices with different tags. Each tag can represent a different grouping such as device type, business function, ownership, department, location, or hierarchy. In addition to supporting the assignment of multiple tags to the same Ordr Classification Profile, it is also possible to assign multiple profiles to the same tag.

Different security policies can be assigned to members of a group based on their tag assignment. For example, a granular microsegmentation policy can be assigned to CT Scanners for a specific vendor or type, but a global policy assigned to all CT Scanners regardless of vendor/type, or one policy that applies to all Medical Imaging devices.

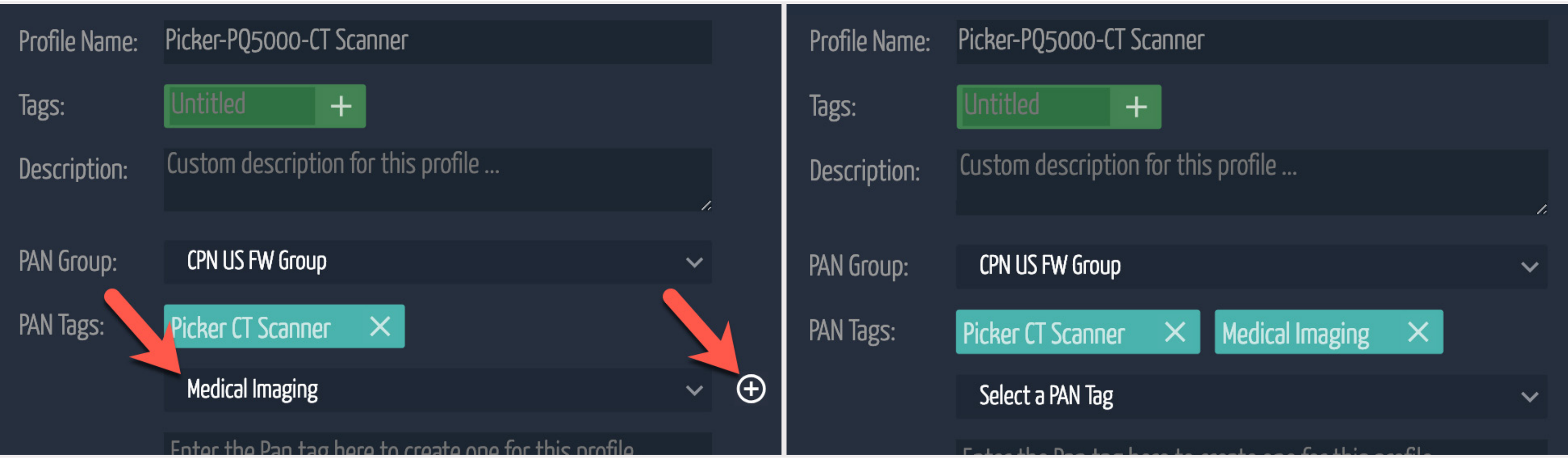
a. From the Ordr SCE administrative interface go to **Profiles** > **Classification Profiles**.

b. Navigate to the **Details** tab of the profile to be mapped to multiple PAN Tags.

c. Under the PAN Group field (lower portion of the profile Details), select the appropriate firewall device group from the drop-down list.

d. Under the PAN Tags field, select the additional tag or tags to assign. This list is automatically populated from tags already configured in Panorama or NGFW. Click the **Add** icon after each new tag selection.

e. Using the original example, the bottom (left) graphic shows that the "Picker-PQ5000-CT Scanner" profile was previously mapped to the "Picker CT Scanner" tag. A second PAN Tag labeled "Medical Imaging" is also selected. Once selected, the Add icon is clicked to add the new tag to the list.



Profile Name: Picker-PQ5000-CT Scanner
Tags: Untitled +
Description: Custom description for this profile ...
PAN Group: CPN US FW Group
PAN Tags: Picker CT Scanner ×
Medical Imaging
Enter the Pan tag here to create one for this profile

Profile Name: Picker-PQ5000-CT Scanner
Tags: Untitled +
Description: Custom description for this profile ...
PAN Group: CPN US FW Group
PAN Tags: Picker CT Scanner × Medical Imaging ×
Select a PAN Tag
Enter the Pan tag here to create one for this profile

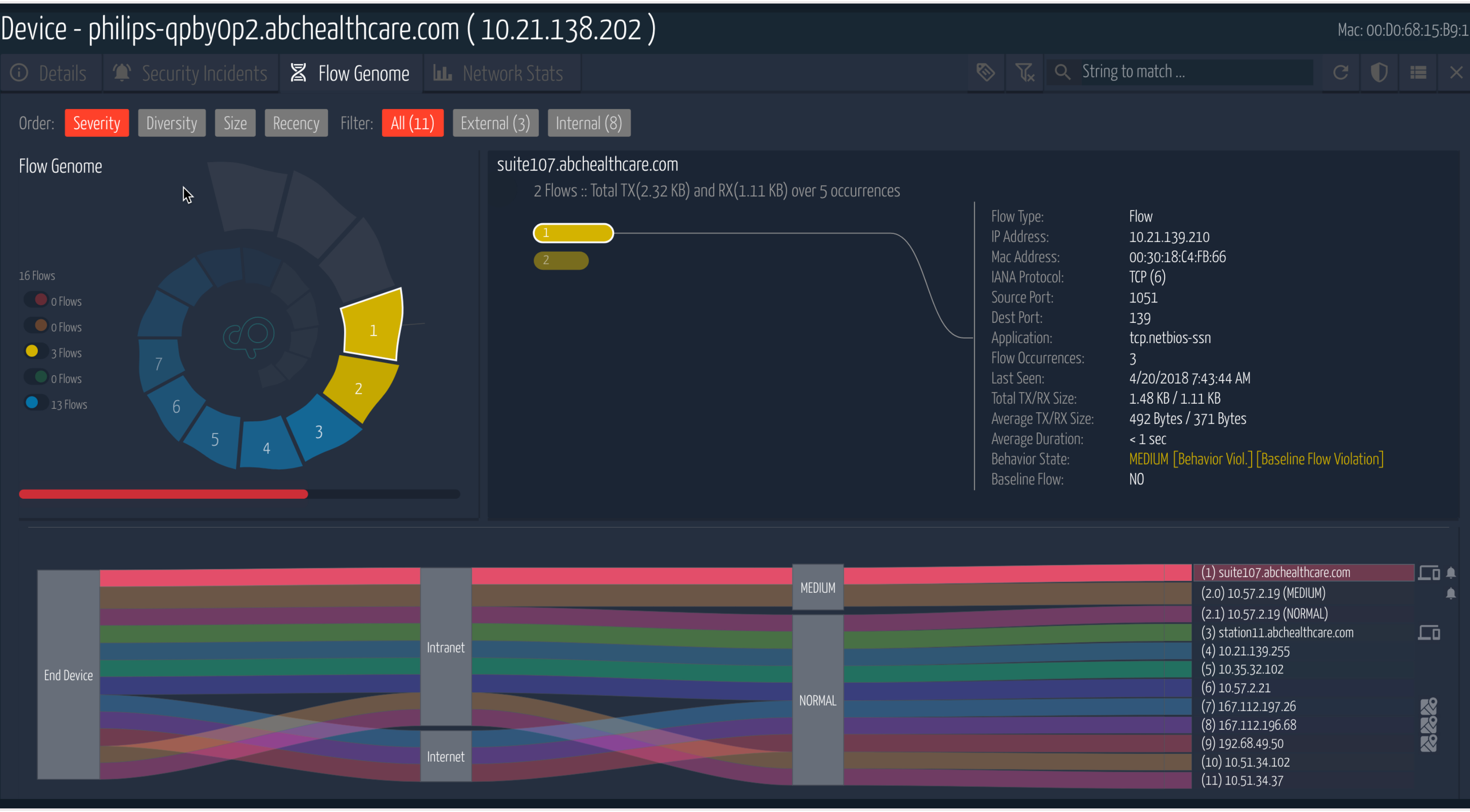
f. Additional tags can be assigned at the same time or later as needed. To commit the tag assignments to Panorama/NGFW, be sure to click **Save Changes** when finished.

g. Verify changes made in Panorama (or standalone NGFW) by accessing the Panorama or NGFW web management interface and navigating to **Objects** > **Addresses**. All members of the Classification Profile will be listed with their multiple tag mappings.

In the example below, all five members of the Picker CT Scanner profile are listed with their current IP address. Both the "Picker CT Scanner" and "Medical Imaging" tags are shown in the Tags column.

Dynamic security policy rule generation based on tags

Ordr SCE continually monitors all device communications through a SPAN mirror, network tap, or flow export (NetFlow, IPFIX, or sFlow). Communication baselines are established for each device and each group of like devices by profile. This learned behavior—refferred to as the Flow Genome—forms the basis of Ordr SCE's Anomaly Behavior Detection.



Device - philips-qpbyop2.abchealthcare.com (10.21.138.202)

Mac: 00:D0:68:15:B9:1

suite107.abchealthcare.com

2 Flows :: Total TX(2.32 KB) and RX(1.11 KB) over 5 occurrences

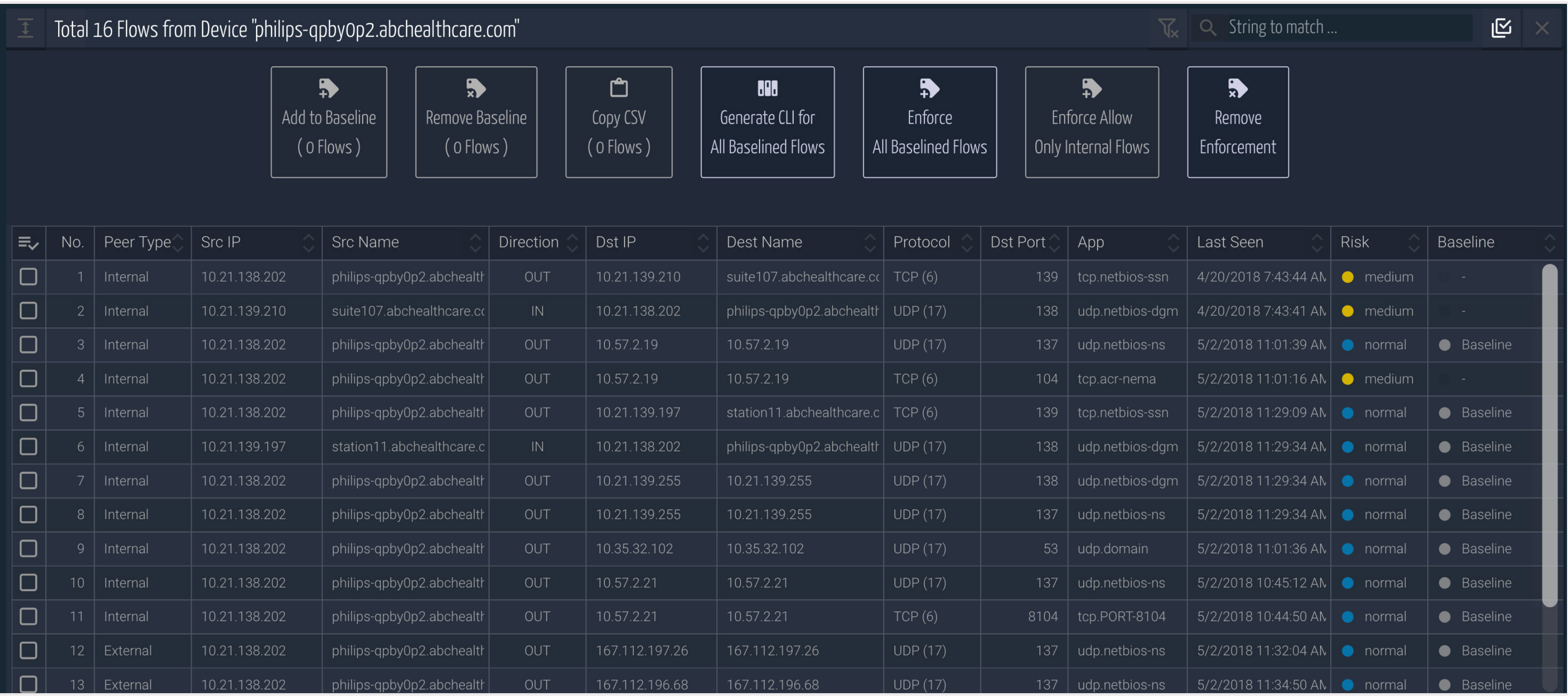
Flow Type: Flow
IP Address: 10.21.139.210
Mac Address: 00:30:18:C4:FB:66
IANA Protocol: TCP (6)
Source Port: 1051
Dest Port: 139
Application: tcp.netbios-ssn
Flow Occurrences: 3
Last Seen: 4/20/2018 7:43:44 AM
Total TX/RX Size: 1.48 KB / 1.11 KB
Average TX/RX Size: 492 Bytes / 371 Bytes
Average Duration: < 1 sec
Behavior State: MEDIUM [Behavior Viol.] [Baseline Flow Violation]
Baseline Flow: NO

(1) suite107.abchealthcare.com
(2.0) 10.57.2.19 (MEDIUM)
(2.1) 10.57.2.19 (NORMAL)
(3) station11.abchealthcare.com
(4) 10.21.139.255
(5) 10.35.32.102
(6) 10.57.2.21
(7) 167.112.197.26
(8) 167.112.196.68
(9) 192.68.49.50
(10) 10.51.34.102
(11) 10.51.34.37

As depicted above, the Flow Genome is represented using both a helical graph (top left) as well as a Sanky diagram (bottom half). In the helical graph, each wedge or step represents a different communication peer. Clicking on a wedge reveals all flows with that peer including time, port, protocol, application, and session, packet and byte TX/RX counts. Flows are color coded to easily visualize security risk rating. The Sanky diagram is an alternate way to view the same information where each peer on the right side is flagged as Internal or External. Internal peers are cross-linked to the device details in Ordr SCE while external peers are cross-linked to their geolocation.

It is generally recommended to allow Ordr SCE to monitor device communications and flows for a few days or weeks to ensure all normal communication patterns have been observed. Longer periods are warranted when devices may sit idle for extended periods or some communications only occur at major intervals (for example, a monthly policy or maintenance update from a manufacturer or patch server). Once the baseline for normal and safe communications is established, the Classification Profile can be moved from a Learning mode to an Enforcement mode.

Enforcement mode tracks communications outside of the established baseline and triggers Anomalous Behavior alerts. Enforcement mode also allows the generation of a Zero Trust security policy in Palo Alto Networks Next-Generation Firewalls based on the Flow Genome. In the example below, three flows have been deemed to be Anomalous and present Medium risk, and therefore not included as part of the default baseline.


Total 16 Flows from Device "philips-qpby0p2.abchealthcare.com"
String to match ...
Add to Baseline (0 Flows)
Remove Baseline (0 Flows)
Copy CSV (0 Flows)
Generate CLI for All Baselined Flows
Enforce All Baselined Flows
Enforce Allow Only Internal Flows
Remove Enforcement

	No.	Peer Type	Src IP	Src Name	Direction	Dst IP	Dest Name	Protocol	Dst Port	App	Last Seen	Risk	Baseline
□	1	Internal	10.21.138.202	philips-qpby0p2.abchealth	OUT	10.21.139.210	suite107.abchealthcare.cc	TCP (6)	139	tcp.netbios-ssn	4/20/2018 7:43:44 AM	● medium	-
□	2	Internal	10.21.139.210	suite107.abchealthcare.cc	IN	10.21.138.202	philips-qpby0p2.abchealth	UDP (17)	138	udp.netbios-dgm	4/20/2018 7:43:41 AM	● medium	-
□	3	Internal	10.21.138.202	philips-qpby0p2.abchealth	OUT	10.57.2.19	10.57.2.19	UDP (17)	137	udp.netbios-ns	5/2/2018 11:01:39 AM	● normal	● Baseline
□	4	Internal	10.21.138.202	philips-qpby0p2.abchealth	OUT	10.57.2.19	10.57.2.19	TCP (6)	104	tcp.acr-nema	5/2/2018 11:01:16 AM	● medium	-
□	5	Internal	10.21.138.202	philips-qpby0p2.abchealth	OUT	10.21.139.197	station11.abchealthcare.c	TCP (6)	139	tcp.netbios-ssn	5/2/2018 11:29:09 AM	● normal	● Baseline
□	6	Internal	10.21.139.197	station11.abchealthcare.c	IN	10.21.138.202	philips-qpby0p2.abchealth	UDP (17)	138	udp.netbios-dgm	5/2/2018 11:29:34 AM	● normal	● Baseline
□	7	Internal	10.21.138.202	philips-qpby0p2.abchealth	OUT	10.21.139.255	10.21.139.255	UDP (17)	138	udp.netbios-dgm	5/2/2018 11:29:34 AM	● normal	● Baseline
□	8	Internal	10.21.138.202	philips-qpby0p2.abchealth	OUT	10.21.139.255	10.21.139.255	UDP (17)	137	udp.netbios-ns	5/2/2018 11:29:34 AM	● normal	● Baseline
□	9	Internal	10.21.138.202	philips-qpby0p2.abchealth	OUT	10.35.32.102	10.35.32.102	UDP (17)	53	udp.domain	5/2/2018 11:01:36 AM	● normal	● Baseline
□	10	Internal	10.21.138.202	philips-qpby0p2.abchealth	OUT	10.57.2.21	10.57.2.21	UDP (17)	137	udp.netbios-ns	5/2/2018 10:45:12 AM	● normal	● Baseline
□	11	Internal	10.21.138.202	philips-qpby0p2.abchealth	OUT	10.57.2.21	10.57.2.21	TCP (6)	8104	tcp.PORT-8104	5/2/2018 10:44:50 AM	● normal	● Baseline
□	12	External	10.21.138.202	philips-qpby0p2.abchealth	OUT	167.112.197.26	167.112.197.26	UDP (17)	137	udp.netbios-ns	5/2/2018 11:32:04 AM	● normal	● Baseline
□	13	External	10.21.138.202	philips-qpby0p2.abchealth	OUT	167.112.196.68	167.112.196.68	UDP (17)	137	udp.netbios-ns	5/2/2018 11:34:50 AM	● normal	● Baseline

While not typically necessary, it is possible to override the established baseline by adding or removing entries. When ready to apply security policies, administrators can choose to simply copy the auto-generated policy for manual update into Panorama or standalone NGFW, or else “push” policy automatically through the native PAN-OS API.

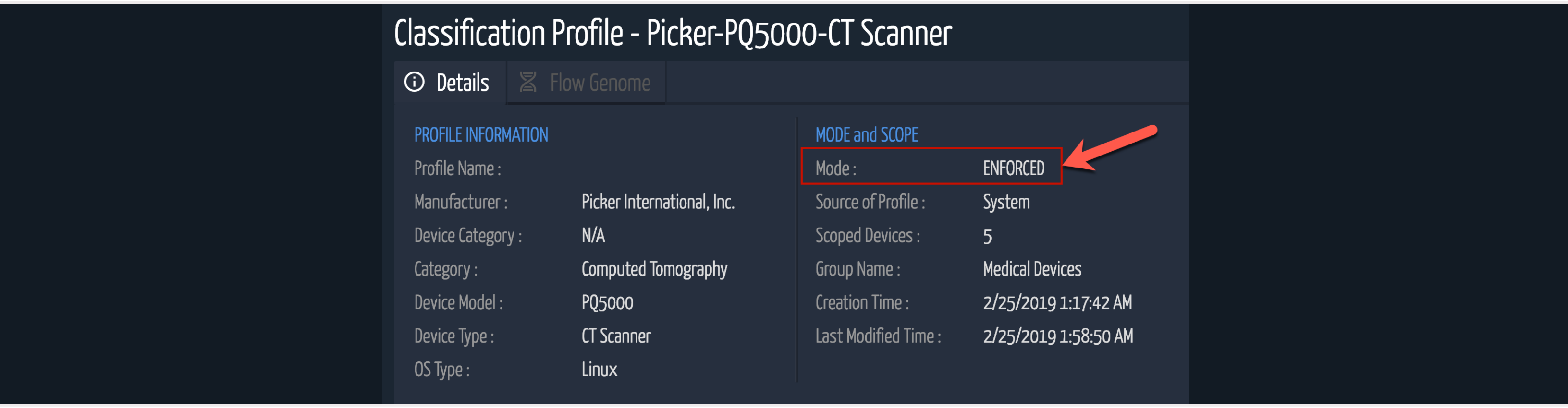
Once tags have been assigned to Ordr SCE profiles, security policy rules published into the NGFWs can be based on the tags and their corresponding address groups.

Step 1: Review the baseline for the device profile

The Picker CT Scanner example used to illustrate the use of tags will also be used to illustrate automated policy enforcement in Panorama.

a. Login to the Ordr SCE administrative interface and go to **Profiles** > **Classification Profiles**.

b. Navigate to the **Details** tab of the profile to be mapped to a PAN-OS Tag. The profile for "Picker-PQ5000-CT Scanners" is selected in the example below. Verify the Mode is set to **ENFORCED**.



Classification Profile - Picker-PQ5000-CT Scanner

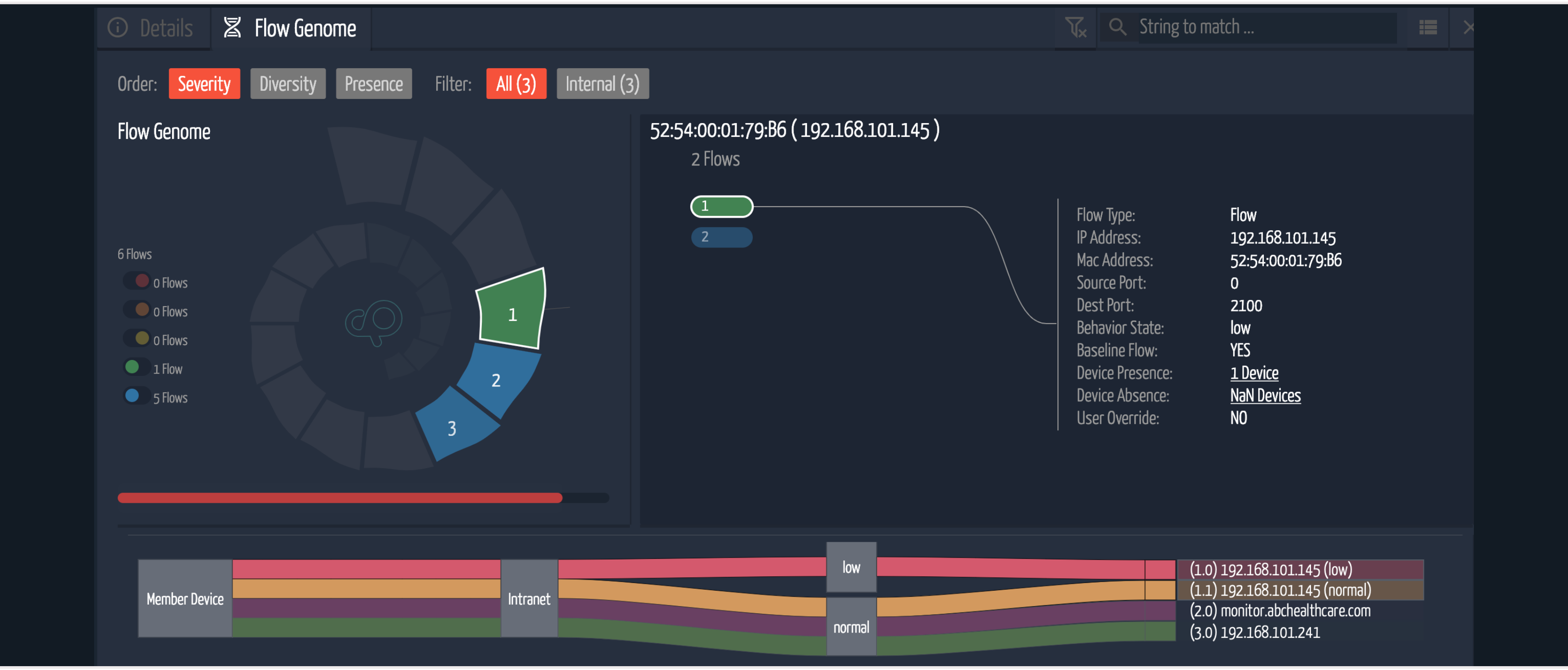
PROFILE INFORMATION

Profile Name :	
Manufacturer :	Picker International, Inc.
Device Category :	N/A
Category :	Computed Tomography
Device Model :	PQ5000
Device Type :	CT Scanner
OS Type :	Linux

MODE and SCOPE

Mode :	ENFORCED
Source of Profile :	System
Scoped Devices :	5
Group Name :	Medical Devices
Creation Time :	2/25/2019 1:17:42 AM
Last Modified Time :	2/25/2019 1:58:50 AM

c. Select the **Flow Genome** tab from the profile menu.



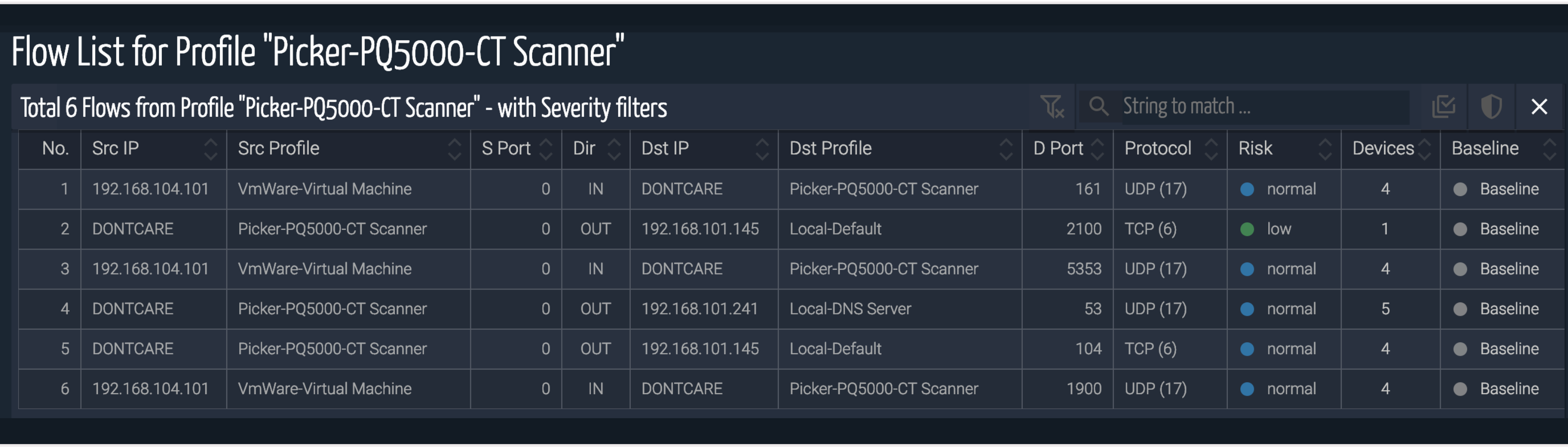
52:54:00:01:79:B6 (192.168.101.145)

Flow Type:	Flow
IP Address:	192.168.101.145
Mac Address:	52:54:00:01:79:B6
Source Port:	0
Dest Port:	2100
Behavior State:	low
Baseline Flow:	YES
Device Presence:	1 Device
Device Absence:	NaN Devices
User Override:	NO

(1.0) 192.168.101.145 (low)
(1.1) 192.168.101.145 (normal)
(2.0) monitor.abchealthcare.com
(3.0) 192.168.101.241

In the example on the previous page, all flows have been deemed Normal (blue) or Low risk (green). While still considered "safe" and part of the baseline, the single green entry is flagged low risk based on the fact that only a smaller subset of devices in the group exhibited this particular traffic behavior.

d. Click the **List** icon in the upper right corner in order to display the Flow List associated with this Flow Genome. The resulting list below represents all inbound and outbound communication peers, protocols, and ports to/from the selected group of devices in this profile.



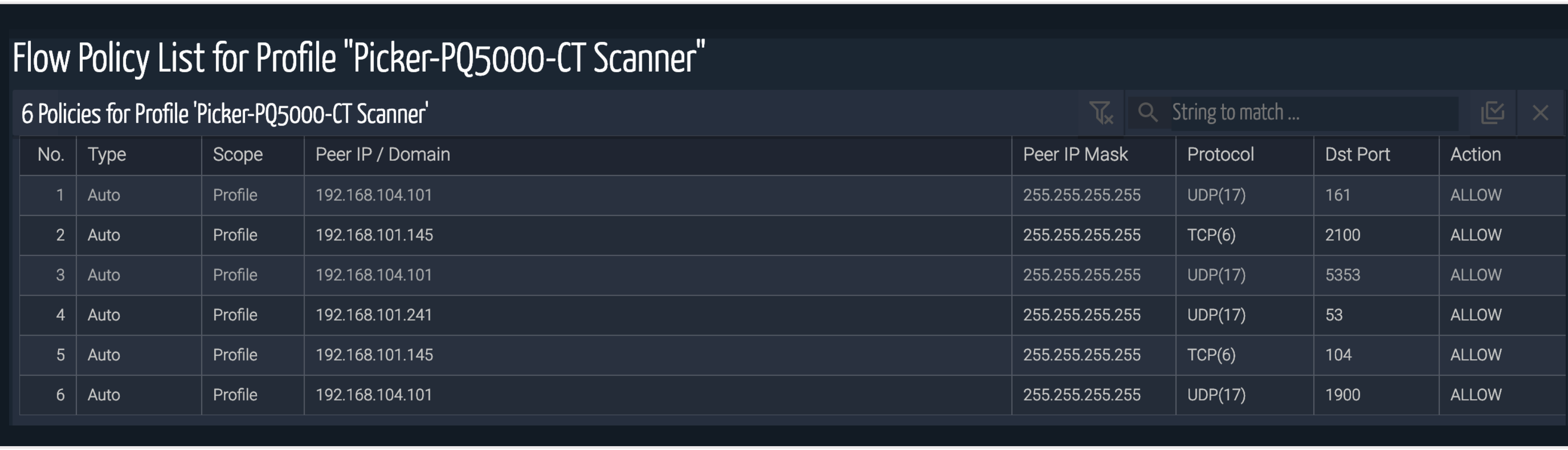
Flow List for Profile "Picker-PQ5000-CT Scanner"

Total 6 Flows from Profile "Picker-PQ5000-CT Scanner" - with Severity filters

No.	Src IP	Src Profile	S Port	Dir	Dst IP	Dst Profile	D Port	Protocol	Risk	Devices	Baseline
1	192.168.104.101	VmWare-Virtual Machine	0	IN	DONTCARE	Picker-PQ5000-CT Scanner	161	UDP (17)	● normal	4	● Baseline
2	DONTCARE	Picker-PQ5000-CT Scanner	0	OUT	192.168.101.145	Local-Default	2100	TCP (6)	● low	1	● Baseline
3	192.168.104.101	VmWare-Virtual Machine	0	IN	DONTCARE	Picker-PQ5000-CT Scanner	5353	UDP (17)	● normal	4	● Baseline
4	DONTCARE	Picker-PQ5000-CT Scanner	0	OUT	192.168.101.241	Local-DNS Server	53	UDP (17)	● normal	5	● Baseline
5	DONTCARE	Picker-PQ5000-CT Scanner	0	OUT	192.168.101.145	Local-Default	104	TCP (6)	● normal	4	● Baseline
6	192.168.104.101	VmWare-Virtual Machine	0	IN	DONTCARE	Picker-PQ5000-CT Scanner	1900	UDP (17)	● normal	4	● Baseline

e. Click on the **Bulk Actions** icon in the upper right corner to modify the baseline.

Or click the **Enforcement Policies** icon to view the enforcement Flow Policy List.



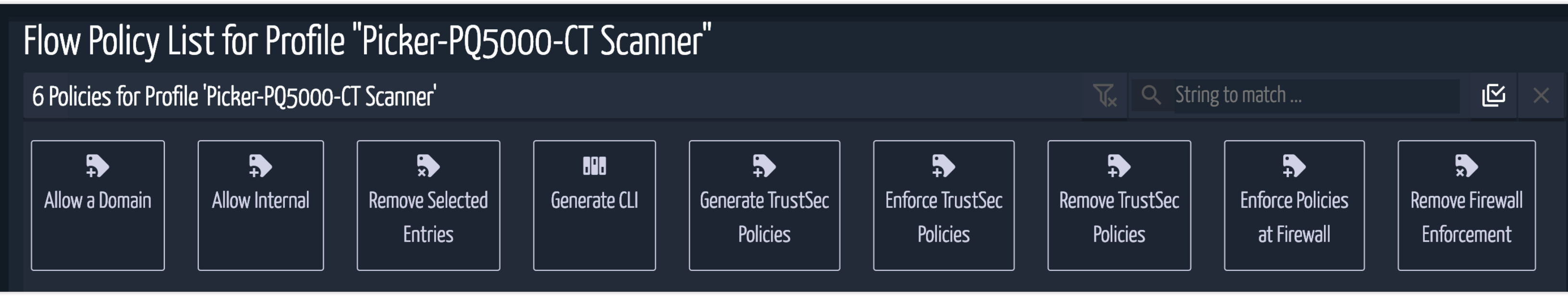
Flow Policy List for Profile "Picker-PQ5000-CT Scanner"

6 Policies for Profile 'Picker-PQ5000-CT Scanner'

No.	Type	Scope	Peer IP / Domain	Peer IP Mask	Protocol	Dst Port	Action
1	Auto	Profile	192.168.104.101	255.255.255.255	UDP(17)	161	ALLOW
2	Auto	Profile	192.168.101.145	255.255.255.255	TCP(6)	2100	ALLOW
3	Auto	Profile	192.168.104.101	255.255.255.255	UDP(17)	5353	ALLOW
4	Auto	Profile	192.168.101.241	255.255.255.255	UDP(17)	53	ALLOW
5	Auto	Profile	192.168.101.145	255.255.255.255	TCP(6)	104	ALLOW
6	Auto	Profile	192.168.104.101	255.255.255.255	UDP(17)	1900	ALLOW

The list represents an ACL-based policy which can be universally applied to all enforcement devices and policy servers.

f. Clicking on the **Bulk Actions** icon in the upper right corner of the Flow Policy List reveals policy enforcement actions.

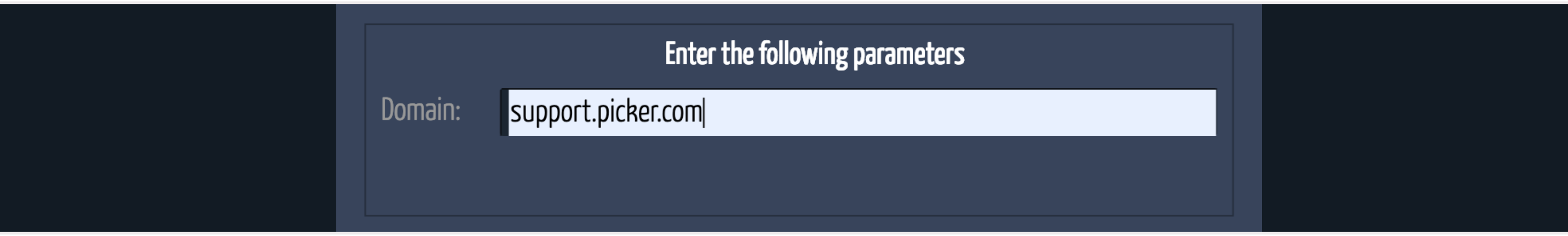


Flow Policy List for Profile "Picker-PQ5000-CT Scanner"

6 Policies for Profile 'Picker-PQ5000-CT Scanner'

String to match ...
Allow a Domain
Allow Internal
Remove Selected Entries
Generate CLI
Generate TrustSec Policies
Enforce TrustSec Policies
Remove TrustSec Policies
Enforce Policies at Firewall
Remove Firewall Enforcement

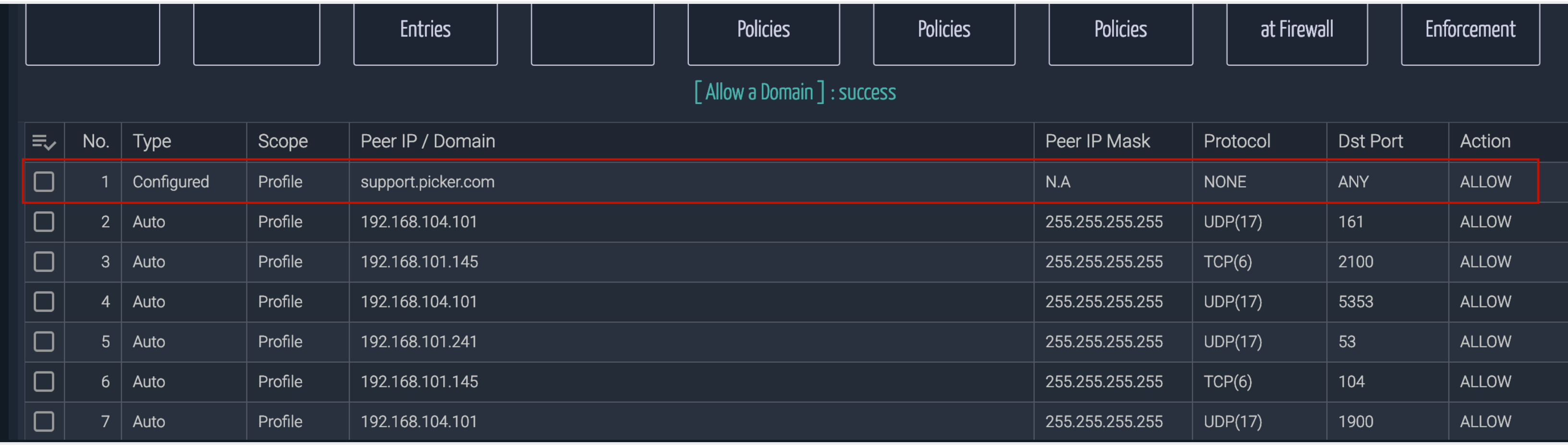
g. To optionally add domain-based permissions to the policy list, click the **Allow a Domain** entry and enter the domain to allow access at the PAN Firewall. In the example below, access to a vendor support site is illustrated.



Enter the following parameters

Domain: support.picker.com

h. Click **Add** when finished. The Flow Policy List is updated with the new domain entry. Notice the entry is flagged as Type = Configured while the auto-generated entries are Type = Auto.

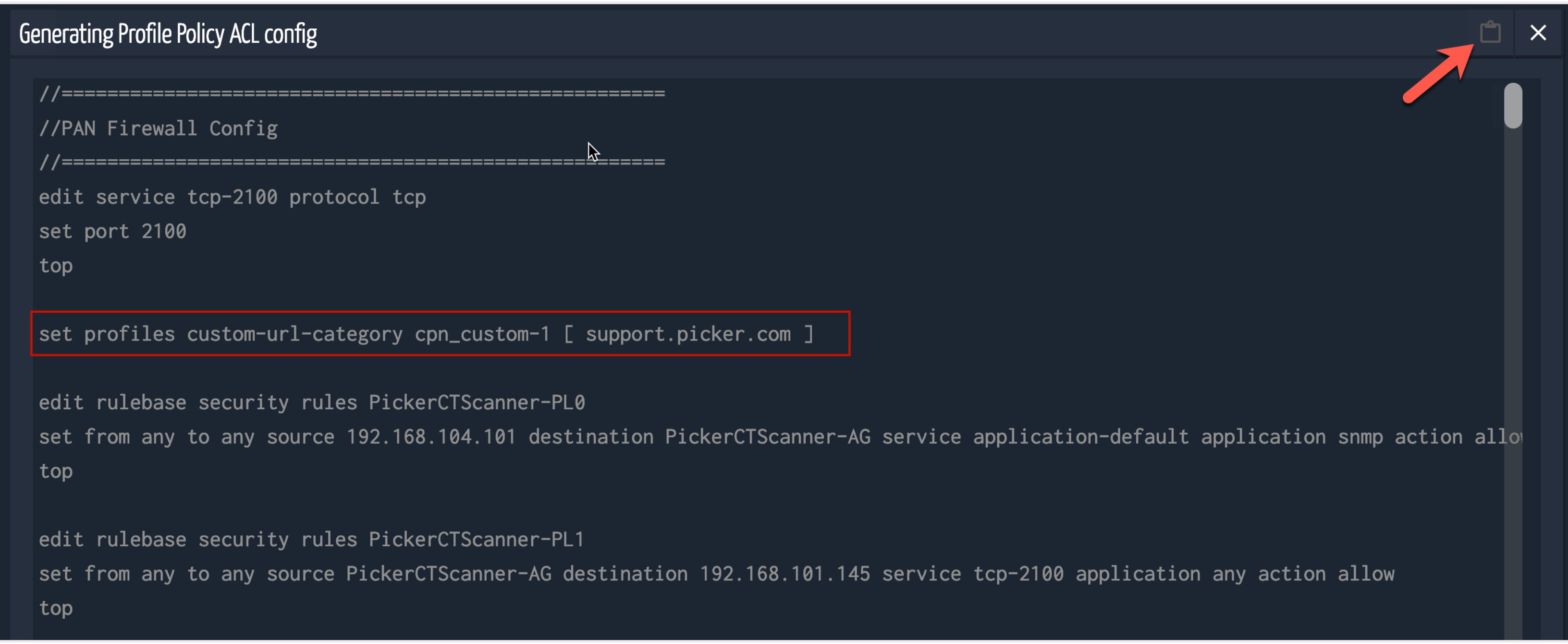


[Allow a Domain] : success

	No.	Type	Scope	Peer IP / Domain	Peer IP Mask	Protocol	Dst Port	Action
□	1	Configured	Profile	support.picker.com	N.A	NONE	ANY	ALLOW
□	2	Auto	Profile	192.168.104.101	255.255.255.255	UDP(17)	161	ALLOW
□	3	Auto	Profile	192.168.101.145	255.255.255.255	TCP(6)	2100	ALLOW
□	4	Auto	Profile	192.168.104.101	255.255.255.255	UDP(17)	5353	ALLOW
□	5	Auto	Profile	192.168.101.241	255.255.255.255	UDP(17)	53	ALLOW
□	6	Auto	Profile	192.168.101.145	255.255.255.255	TCP(6)	104	ALLOW
□	7	Auto	Profile	192.168.104.101	255.255.255.255	UDP(17)	1900	ALLOW

Step 2: Review and enforce NGFW security policy

a. Review the NGFW security policy to enforce the baseline for the selected profile by clicking the Generate CLI box. A text-based version of the ACL policy rules to be applied to the NGFWs is displayed.



```
//=====================================================
//PAN Firewall Config
//=====================================================
edit service tcp-2100 protocol tcp
set port 2100
top

set profiles custom-url-category cpn_custom-1 [ support.picker.com ]

edit rulebase security rules PickerCTScanner-PL0
set from any to any source 192.168.104.101 destination PickerCTScanner-AG service application-default application snmp action allo
top

edit rulebase security rules PickerCTScanner-PL1
set from any to any source PickerCTScanner-AG destination 192.168.101.145 service tcp-2100 application any action allow
top
```

The output includes all commands required to deploy the NGFW configuration including domain-based policy rules and policy objects.

b. 📋 To manually deploy the NGFW configuration, simply click the **Clipboard** icon in the upper right corner to copy the content of text output to the local computer's clipboard. The contents can then be pasted to the medium of choice such as a text file, email, or the CLI of the target device. Click **X** in the upper right corner to close the ACL Configuration window.

c. To automatically deploy the NGFW configuration, simply click the **Enforce Policy at Firewall** box.

d. The update push over PAN-OS API may take a few seconds to complete. When finished, the success message "**[Enforce Policies at Firewall]: Success**" should appear.

NOTE: REMOVING FIREWALL ENFORCEMENT

To remove the security policy applied to the NGFWs, select the **Remove Firewall Enforcement** box.

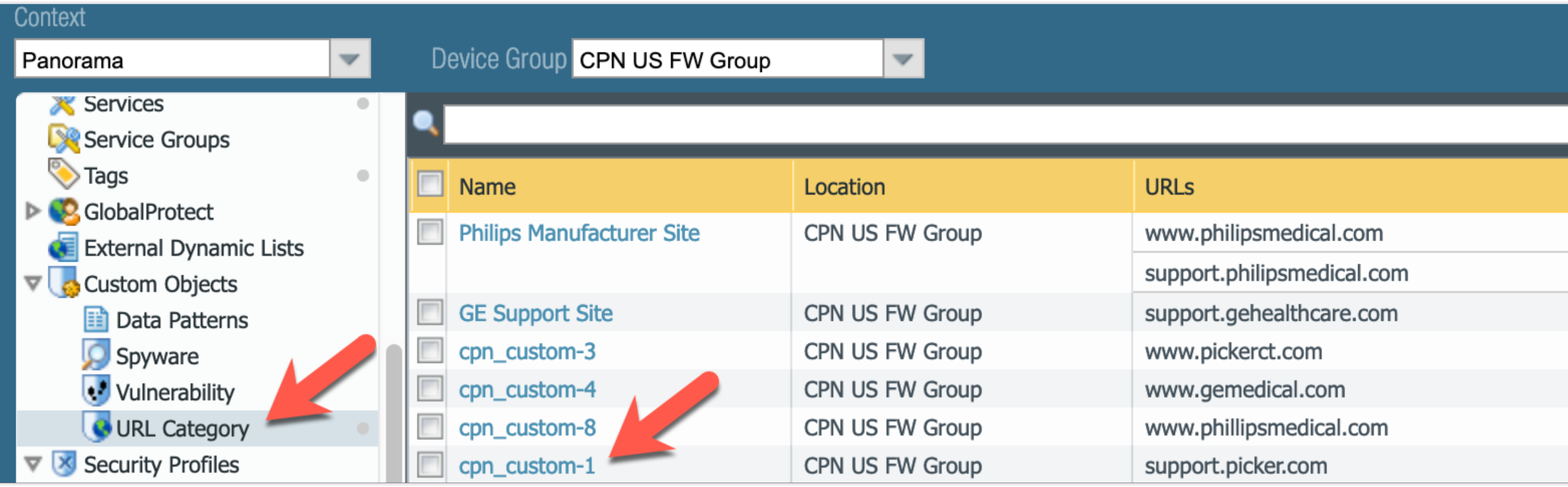
Step 3: Verify dynamic update of security policy to Panorama

a. Verify changes made in Panorama (or standalone NGFW) by accessing the Panorama or NGFW web management interface.

b. If domain-based policies were deployed as part of the Ordr SCE policy enforcement, navigating to **Objects** > **Custom Objects** > **URL Category**.

c. Verify the correct Context and Device Group are selected in Panorama.

In the example below, the URL Category object cpn_custom-1 has been successfully created per the ACL Configuration output shown in the Ordr SCE interface. It is mapped to the sample domain support.picker.com.

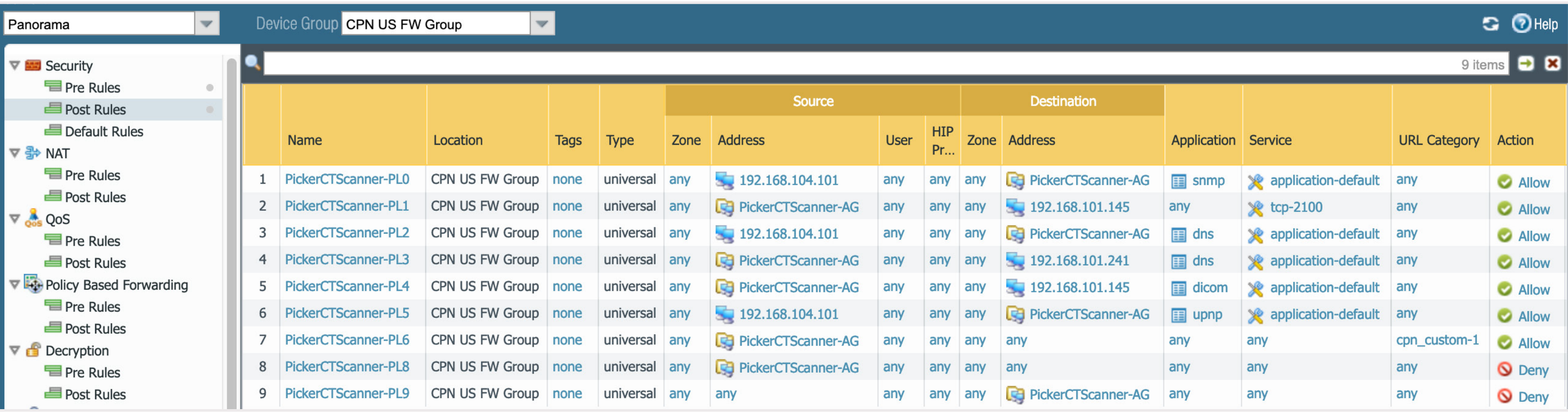


Context: Panorama

Device Group: CPN US FW Group

☐	Name	Location	URLs
☐	Philips Manufacturer Site	CPN US FW Group	www.philipsmedical.com support.philipsmedical.com
☐	GE Support Site	CPN US FW Group	support.gehealthcare.com
☐	cpn_custom-3	CPN US FW Group	www.pickerct.com
☐	cpn_custom-4	CPN US FW Group	www.gemedical.com
☐	cpn_custom-8	CPN US FW Group	www.phillipsmedical.com
☐	cpn_custom-1	CPN US FW Group	support.picker.com

d. Navigate to **Policies** > **Security** > **Post Rules** to display the security policy automatically pushed by Ordr SCE.



Panorama

Device Group: CPN US FW Group

					Source				Destination					
	Name	Location	Tags	Type	Zone	Address	User	HIP Pr...	Zone	Address	Application	Service	URL Category	Action
1	PickerCTScanner-PL0	CPN US FW Group	none	universal	any	192.168.104.101	any	any	any	PickerCTScanner-AG	snmp	application-default	any	Allow
2	PickerCTScanner-PL1	CPN US FW Group	none	universal	any	PickerCTScanner-AG	any	any	any	192.168.101.145	any	tcp-2100	any	Allow
3	PickerCTScanner-PL2	CPN US FW Group	none	universal	any	192.168.104.101	any	any	any	PickerCTScanner-AG	dns	application-default	any	Allow
4	PickerCTScanner-PL3	CPN US FW Group	none	universal	any	PickerCTScanner-AG	any	any	any	192.168.101.241	dns	application-default	any	Allow
5	PickerCTScanner-PL4	CPN US FW Group	none	universal	any	PickerCTScanner-AG	any	any	any	192.168.101.145	dicom	application-default	any	Allow
6	PickerCTScanner-PL5	CPN US FW Group	none	universal	any	192.168.104.101	any	any	any	PickerCTScanner-AG	upnp	application-default	any	Allow
7	PickerCTScanner-PL6	CPN US FW Group	none	universal	any	PickerCTScanner-AG	any	any	any	any	any	any	cpn_custom-1	Allow
8	PickerCTScanner-PL8	CPN US FW Group	none	universal	any	PickerCTScanner-AG	any	any	any	any	any	any	any	Deny
9	PickerCTScanner-PL9	CPN US FW Group	none	universal	any	any	any	any	any	PickerCTScanner-AG	any	any	any	Deny

Each of the line entries corresponds to a line entry in the Ordr SCE ACL Configuration. Additional entries are added to the bottom of the policy list to deny any additional traffic from or to the members of the Tag = Picker CT Scanner, which are mapped to Address Group = PickerCTScanner-AG.

e. The URL Category column (if enabled for display) includes any domain-based objects. In the example, full access is granted to cpn_custom-1 which is mapped to the domain support.picker.com. NGFWs will automatically resolve the domain to its current IP address(es).

Summary

The combination of Ordr Systems Control Engine (a next-generation IoT profile and enforcement policy engine) and Palo Alto Networks Next-Generation Firewalls offers customers a world-class solution to automatically detect, classify, and secure all IoT/OT devices on the network using scalable, tag-based microsegmentation.

ōrdr

take control.

info@ordr.net
www.ordr.net

2445 Augustine Drive Suite 601
Santa Clara, CA 95054