



Pulse Policy Secure

PPS Integration with Palo Alto Networks Firewall

Deployment Guide

Pulse Secure, LLC
2700 Zanker Road, Suite 200
San Jose, CA 95134
<https://www.pulsesecure.net>

© 2019 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <https://www.pulsesecure.net/support/eula>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA

Revision History

The following table lists the revision history for this document.

Document Version	Change (Add/Update/Remove)	Published Date	Effective Release	Notes
1.1	Included Screenshot for configuring security policies	August 2019		
1.0	Initial Version	February 2019		

Contents

Purpose of this Guide	6
Prerequisites	6
Enforcement using Palo Alto Networks Firewall	7
Overview.....	7
Deployment of PPS using PAN Firewall	7
Deploying PPS with a PAN firewall for a Small Enterprise	8
Deploying multiple PPS with PAN firewall	9
Deploying PPS with PAN firewall for a Large Enterprise.....	9
Specification for deploying PPS and PAN Appliances.....	10
Configuring PPS with PAN Firewall.....	11
Configuring PAN Intranet Enforcer in PPS	11
Configuring Auth Table Mapping Policies.....	12
Configuring Palo Alto Networks Firewall	14
Configuring User Identification on Security Zones	14
Configuring Dynamic Address Groups	15
Configuring Security Policies	16
Configuring PAN Device Certificates.....	17
Troubleshooting	19
Unsupported Features	20
Related Documentation.....	20
Provisioning PCS sessions to PAN Firewall.....	21
Overview.....	21
Deployment of PPS/PCS using PAN Next Generation Firewall	21
IF-MAP Configuration	22
Configuring IF-MAP Server.....	23
Configuring IF-MAP Client	25
Viewing the Federated Session Details.....	26
Alert Based Admission Control using PAN Next Generation Firewall	27
Overview.....	27
Deployment of PPS using PAN Next Generation Firewall.....	27
Configuring PPS with PAN Next Generation Firewall	28
Admission Control Template.....	29

Admission Control Policies	30
Admission Control Client.....	31
Configuring PAN Next Generation Firewall	31
Troubleshooting	34
IoT Policy Provisioning.....	35
Overview.....	35
Benefits.....	35
Deployments	35
Configuring IoT Policy Provisioning.....	36
Pre-Requisite.....	37
Summary of Configuration	37
Basic Configurations	37
Configuring IoT Access Policy	39
Viewing Devices in Enforcer Policy Report.....	39
Configuring IoT Access Policy using Palo Alto Networks Firewall	40
Configuring Additional Device Category/Profile Groups	43
Configuring Profiler Groups	44
Troubleshooting	45
Event Logs	45
References	47
Technical Support	48

Purpose of this Guide

This guide describes the following information:

- How to deploy and configure Pulse Policy Secure (PPS) with Palo Alto Networks (PAN) firewall.
- Provisioning PCS/PPS user sessions to PAN firewall through IF-MAP server.
- How to deploy and configure Pulse Policy Secure (PPS) with Palo Alto Networks (PAN) Next Generation firewall.

Prerequisites

This guide assumes you are familiar with the use of the following products and their related terminology.

- Pulse Policy Secure at version 9.0R3

Identity Management

This chapter includes the following information:

- Overview
- Deployment of PPS using PAN Firewall
- Configuring PPS with PAN Firewall
- Configuring Palo Alto Networks Firewall
- Troubleshooting

Overview

PPS delivers layer 3 network access control solution when deployed with Palo Alto Networks next-generation firewalls. PPS authenticates users, ensures that the endpoints meet security policies, and then dynamically updates the firewall enforcement point with the resulting user session information. Upon successful user authentication with PPS, the access to protected resources behind the firewall is based on the user identity, IP address, and user role information provided by PPS.

The PPS and PAN integration provides identity enabled layer 3 enforcement for BYOD and guests as well as enterprise employees, with the end authentication and comprehensive compliance checks from PPS.

Deployment of PPS using PAN Firewall

This section describes the integration of PPS with Palo Alto Networks next-generation firewall. The PPS and PAN firewall integration allows users to enforce role-based access to network resources and web applications and ensures endpoint compliance. The integrated solution provides policy enforcement for end to end protection of sensitive corporate data from unauthenticated access and attacks.

PPS combines user identity and device security state information with network location to create a unique, session specific access control policy for each user. The Palo Alto Networks firewall provides a feature called User Identification (User-ID) that creates policies and performs reporting based on users and groups rather than individual IP addresses. PPS uses the User-ID XML API to send the IP address to user and IP address to Group (Role) mapping information to the Palo Alto Networks firewall. PAN firewall enables the flexibility to apply different rules to the same server based on tags. A tag is a metadata element, which defines its role on the network, the operating system, or the different kinds of traffic it processes.

The Palo Alto Networks firewall compares the user information against the tag that is associated to a security rule. If the User Role name matches the tag, then traffic is either allowed or denied based on the configuration. When a user logs in, Pulse Policy Secure provisions their user ID, IP address of the endpoint, and role information to the Palo Alto Networks firewall; that enables firewall policies based on any of these attributes to be enforced.

Similarly, when a user logs out, the user ID, IP address of the endpoint, and role information is removed from the firewall. More importantly, when a user's role changes, the role change information is dynamically updated on the firewall, so that access based on the updated roles is automatically changed based on the policy matched by the new information.

With Palo Alto Networks firewall integration, all users' role changes, which includes compliance check

failure or unauthorized behavior are dynamically updated on the firewall. The access is based on user roles and not merely on source IP addresses.

PPS is the policy decision point that determines which users and endpoints can access protected resources. Palo Alto Networks Next Gen firewalls serve as the policy enforcement points to provide the ultimate protection to ensure that network assets are secured.

Palo Alto Networks integration with Pulse Policy Secure leverages dynamic role information provisioned to the firewall upon user session establishment and for the duration of the session. Pulse Policy Secure also communicates user information to the Palo Alto Networks firewall when users log in or log out from their device.

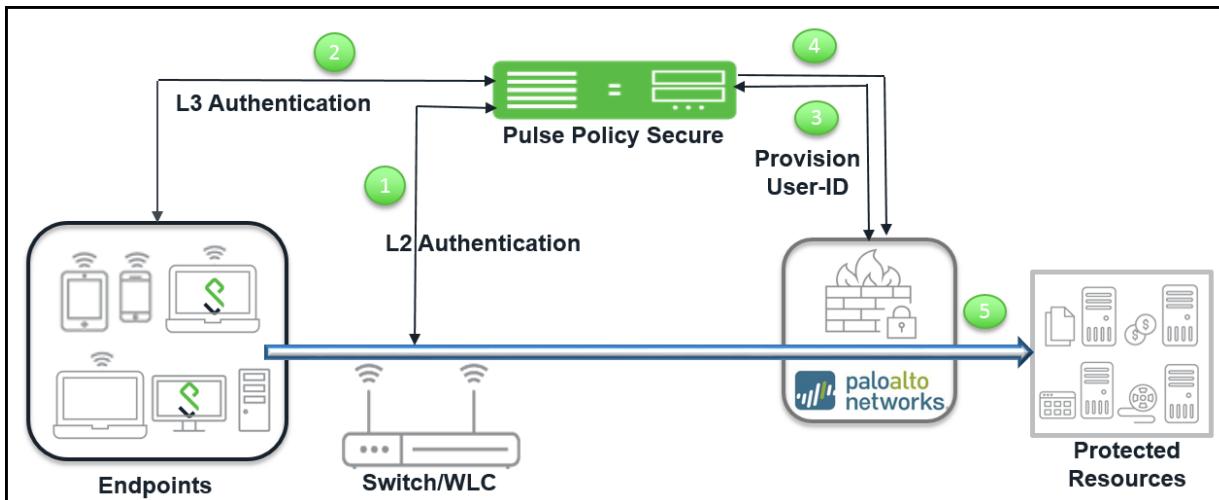
This section covers the following deployment scenarios:

- Deploying PPS with a PAN firewall for a Small Enterprise
- Deploying multiple PPS with PAN firewall
- Deploying PPS with PAN firewall for a Large Enterprise

Deploying PPS with a PAN firewall for a Small Enterprise

PPS and PAN integration can be used for role-based layer 3 access control. For small scale enterprise deployment, you can use a single PPS and PAN firewall as it involves less number of users. For example, employees, contractors and guest users. A single PPS device provisioning to a PAN firewall can handle up to 30,000 user sessions. The following is a sample deployment with a PPS device along with a PAN firewall.

Figure 1: Single PPS Deployment



The authentication process is described below:

1. The endpoints connect to switch/WLAN and performs the layer 2 authentication with PPS.
2. PPS performs the layer 3 authentication and performs compliance check on the endpoint and detects for any unauthorized behavior.
3. PPS provisions the auth table entries on the PAN firewall.
4. PPS provisions the auth table with changes in role information if any on PAN firewall. The user role changes, which includes any unauthorized behavior are dynamically updated on the firewall. The

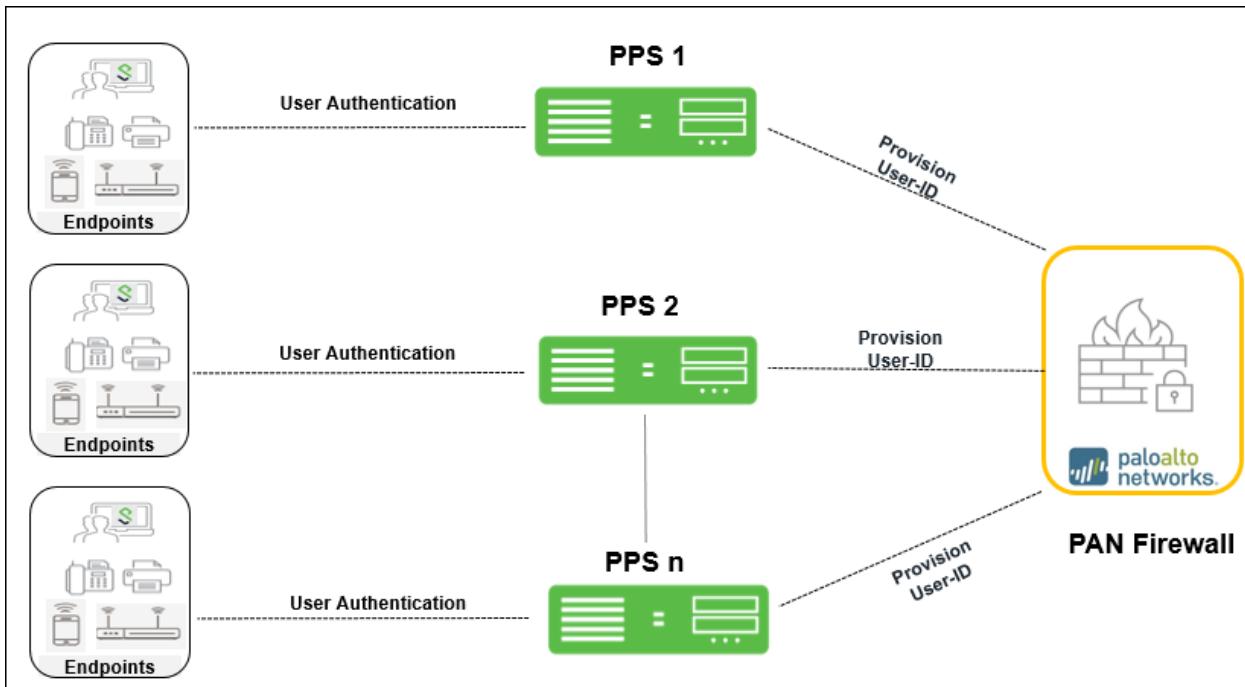
access is based on roles, rather than only on source IP addresses.

- The PAN firewall applies policies to allow or block user access to protected resources.

Deploying multiple PPS with PAN firewall

The deployment example describes an enterprise environment with multiple PPS servers where different users are authenticated using different PPS servers. For such deployments, multiple PPS servers can be configured to communicate with a single PAN firewall. The multiple PPS servers sends user-ID entries to a single PAN firewall.

Figure 2: Deploying multiple PPS with a PAN Firewall

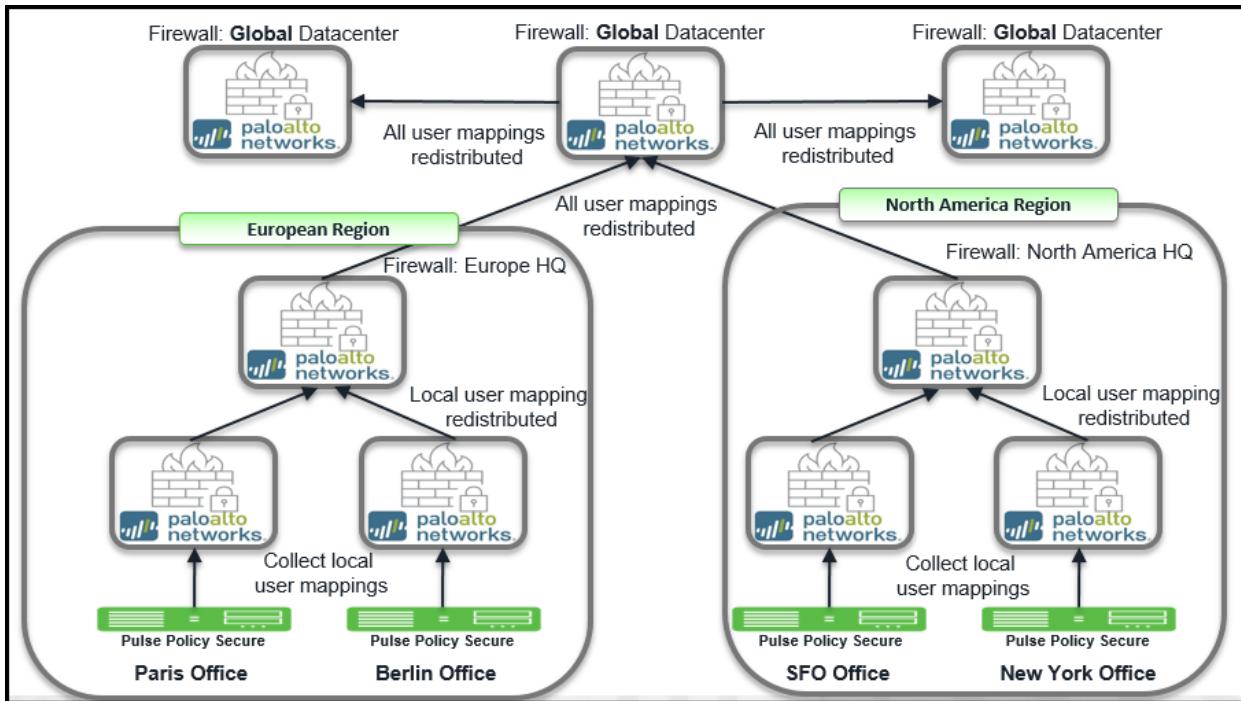


Deploying PPS with PAN firewall for a Large Enterprise

A large-scale enterprise network uses multiple firewalls to enforce policies. You can reduce the resources that the firewalls and information sources use in the querying process by configuring some firewalls to acquire mapping information. You can enable the firewall to enforce user-based policies when users rely on local sources for authentication (for example, regional directory services) but need access to remote resources (for example, global data center applications).

The deployment example describes how a global datacenter resources is distributed across the branches and shared across the local offices. It also shows how you can organize the redistribution sequence in layers, where each layer has one or more firewalls. In this example, bottom-layer firewalls in local offices rely on PPS for authentication and then redistribute the mapping information to middle-layer firewalls in regional offices, which redistribute to one top-layer firewall in a global data center. The data center firewall redistributes the mapping information to other data center firewalls so that they can enforce global policies for all users.

Figure 3: Large Scale Deployment



Specification for deploying PPS and PAN Appliances

The firewall provides access to resources based on the user role. You can use the IP role mapping on the PAN firewall for role-based access. The maximum number of IP addresses that can be registered for each PAN device is different. The following table describes the specifics for different PAN firewall appliances and the recommended PPS appliance for your deployment.

Table 1: Recommendations for deploying PPS and PAN firewall

PAN Appliance	Maximum number of dynamically registered IP addresses	IP Address Tag	Recommended PPS Appliance
PA 500	1000	32	PSA 5000
PA 3020	5000	32	PSA 5000
PA 5020	20000	32	SM 360, PSA 7000
PA 7000	44000	32	PSA 7000

Note:

- The IP role mapping scale limit or the maximum number of dynamically registered IP addresses for a unique endpoint is based on the PAN appliance.
- The maximum number of IP address tags supported is also based on the PAN appliance.

The IP Address tag is a metadata element or attribute-value pair that is registered on the firewall. For example, IP1 {tag1, tag2,....tag32}, where the IP address and the associated tags are maintained as a list; each registered IP address can have up to 32 tags such as the operating system, the datacenter or the switch to which it belongs.

Configuring PPS with PAN Firewall

This section covers the configuration of PPS for adding PAN firewall as an Infranet Enforcer.

The following are the configuration steps:

1. Configuring PAN Infranet Enforcer in PPS
2. Configuring Auth Table Mapping Policies

Configuring PAN Infranet Enforcer in PPS

The PPS configuration requires defining a new Palo Alto Networks Firewall Infranet Enforcer instance on PPS and then fetching the API key from the firewall. The API key is used to communicate between the Palo Alto Networks firewall and PPS. The standard user authentication / authorization configurations such as Auth Table Mapping Policies should also be created and associated with the required roles.

To configure a Palo Alto Networks Firewall Infranet Enforcer in PPS:

1. Select **Endpoint Policy > Infranet Enforcer**.

Figure 4: Infranet Enforcer

2. Click New Infranet Enforcer and select Palo Alto Networks Firewall in the Platform drop down.

Figure 5: Palo Alto Networks Firewall

The screenshot shows the Pulse Secure Endpoint Policy interface. The top navigation bar includes links for System, Authentication, Administrators, Users, Endpoint Policy (which is highlighted in green), Maintenance, and Wizards. The main content area is titled "Infranet Enforcer > Connection > New Infranet Enforcer". A sub-section titled "New Infranet Enforcer" is expanded, showing a form for "Infranet Enforcer". The form fields include:

- Platform:** Palo Alto Networks Firewall (selected from a dropdown menu)
- Name:** (Required field, empty input field)
- IP Address:** (Required field, empty input field)
- API Key:** (Input field containing "Get API Key")
- Server Certificate Validation:** (checkbox, unchecked)

Below the form is a "Save Changes" button and a note: "* indicates required field".

- Enter the **Name** and **IP Address** of the Palo Alto Networks firewall and then click **Get API Key** which opens a new page:

Figure 6: API Key

The screenshot shows the Pulse Secure Endpoint Policy interface. The top navigation bar includes links for System, Authentication, Administrators, Users, Endpoint Policy (highlighted in green), Maintenance, and Wizards. The main content area is titled "Infranet Enforcer > Connection > New Infranet Enforcer". A sub-section titled "New Infranet Enforcer" is expanded, showing a form for "Retrieve API Key". The form fields include:

- Enforcer Username:** admin (input field)
- Enforcer Password:** (input field showing masked password)

Below the form are "Retrieve" and "Cancel" buttons.

- Enter the **Admin Username** and **Admin Password** of the Palo Alto Networks firewall and then Click **Retrieve**. This enables PPS to fetch the API key of the firewall. Once the API key is retrieved, the page automatically redirects back to the New Infranet Enforcer page as shown above and updates the API Key Field.

See Configuring PAN Device Certificates for understanding the validation procedure.

- Click **Save Changes**.

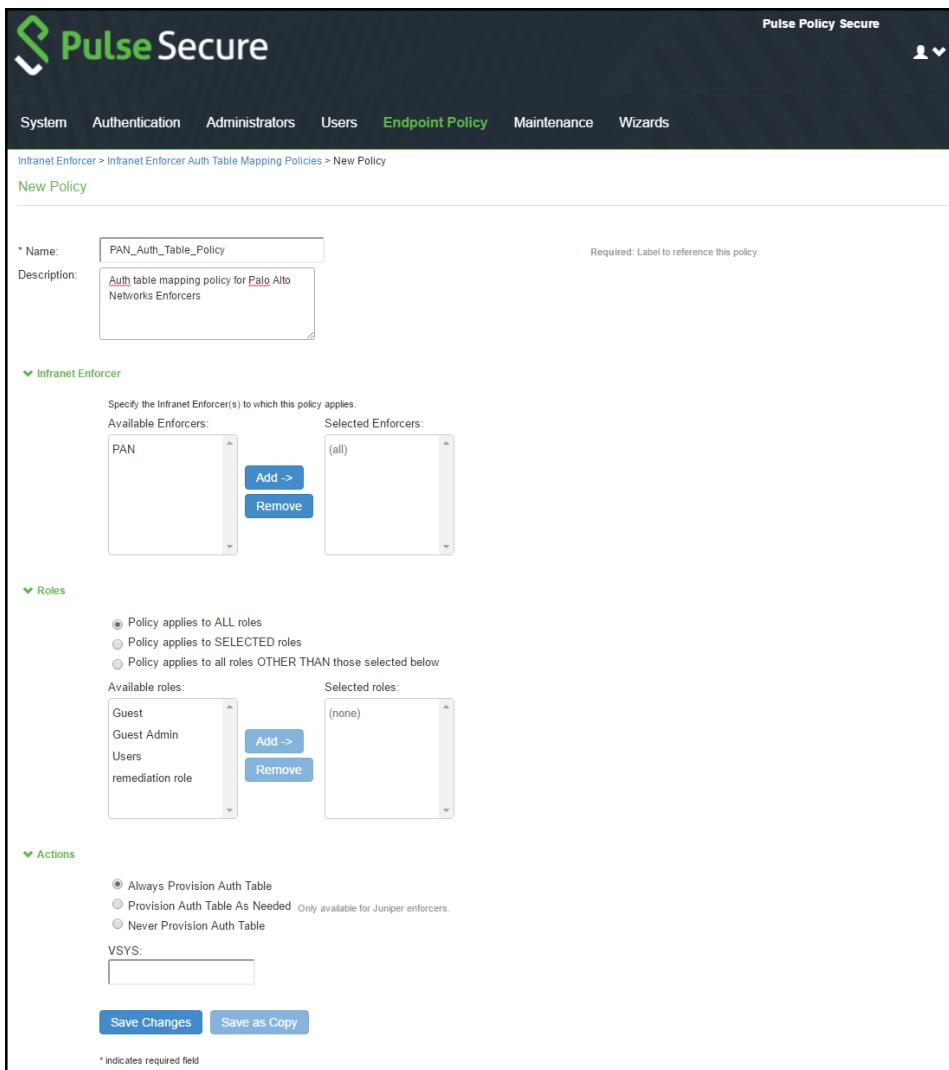
Configuring Auth Table Mapping Policies

An auth table entry consists of the user's name, a set of roles, and the IP address of the wired, wireless, or virtual adapter. An auth table mapping policy specifies which enforcer device can be used for each user role. These policies prevent the PPS from creating unnecessary auth table entries on all connected enforcer devices.

PPS's default configuration includes only one default auth table mapping policy. When the default auth table mapping policy is enabled, PPS pushes one auth table entry for each authenticated user to all Palo Alto Networks firewalls configured as Infranet Enforcers in PPS.

To configure an Auth Table Mapping Policy:

- Select Endpoint Policy > Infranet Enforcer > Auth Table Mapping and click New Policy.

Figure 7: Palo Alto Networks Firewall Configuration

2. On the New Policy page:
 - a. For Name, enter a name to label the auth table mapping policy.
 - b. (Optional) For Description, enter a description.
 - c. In the Enforcer section, specify the Intranet Enforcer firewall(s) to which you want to apply the auth table mapping policy.
 - d. In the Roles section, specify:
 - Policy applies to ALL roles—Select this option to apply the auth table mapping policy to all users.
 - Policy applies to SELECTED roles—Select this option to apply the auth table mapping policy only to users who are mapped to roles in the SELECTED roles list. You can add roles to this list from the available roles list.
 - Policy applies to all roles OTHER THAN those selected below—Select this option to apply the auth table mapping policy to all users except for those who map to the roles in the SELECTED roles list. You can add roles to this list from the available roles list.

- list.
- e. In the Action section, specify auth table mapping rules for the specified Infranet Enforcer.
 - Always Provision Auth Table—Select this option to automatically provision auth table entries for chosen roles on the specified Infranet Enforcer.
 - Provision Auth Table as Needed—Select this option to provision auth table entries only when a user with a chosen role attempts to access a resource behind the specified Infranet Enforcer. This option is greyed out for Palo Alto Networks Firewall Enforcers since it is not supported.
 - Never Provision Auth Table—Select this option to prevent chosen roles from accessing resources behind the specified Infranet Enforcer.
 3. You must delete the Default Policy if you configure any custom auth table mapping policies. PPS's default configuration includes this default auth table mapping policy that allows all source IP endpoints to use all Infranet Enforcers.
 4. Click **Save Changes**.

Configuring Palo Alto Networks Firewall

Palo Alto Networks firewall detects traffic from an endpoint that matches a configured security policy using the endpoint's auth table entry. It determines the role(s) associated with that user, and allows or denies the traffic based on the actions configured in the security policy.

The configuration on the Palo Alto Networks firewall includes:

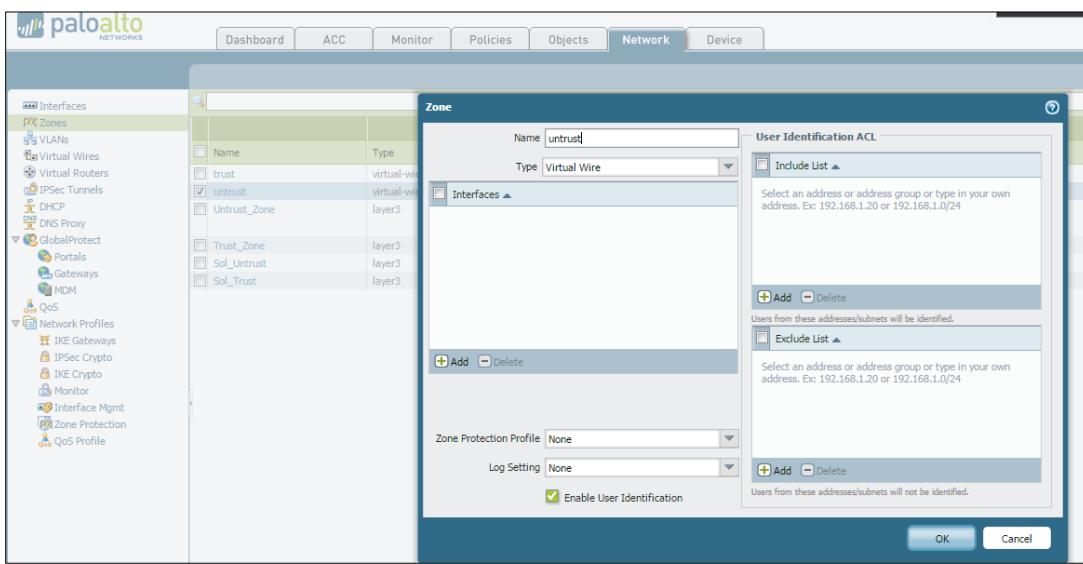
- Configuring User Identification on Security Zones
- Configuring Dynamic Address Groups
- Configuring Security Policies
- Configuring PAN Device Certificates

Configuring User Identification on Security Zones

Policy rules on the firewall use security zones to identify the source and the destination of the traffic. The data traffic flows freely within a zone and not between different zones until you define a security policy rule that allows it. To enable User-ID enforcement, you must enable User Identification on both inbound and outbound zones traversed by the end-user traffic.

To enable User Identification:

1. Select Palo Alto Networks > Network > Zones.
2. For each zone that serves as an inbound or outbound zone for enforced traffic, click the zone name (For example, trust, untrust, and so on).
3. Select Enable User Identification and click OK.

Figure 8: Enabling User Identification on a Zone

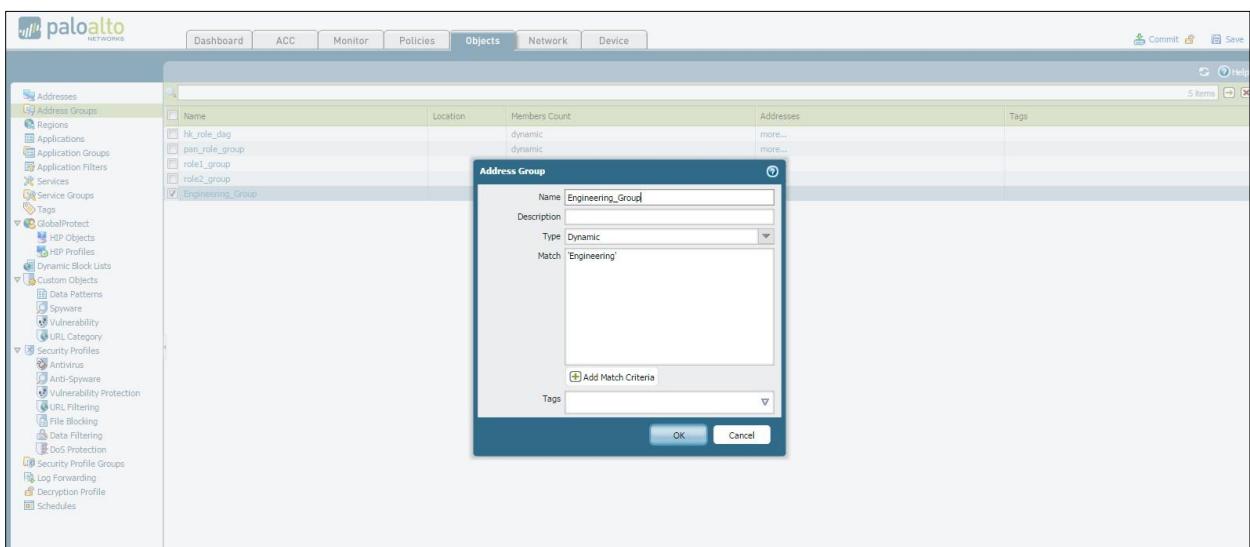
Note: Provisioning of Resource Access Policies from PPS to the Palo Alto Networks Firewall Enforcer is not supported. You must configure the required security policies on the firewall.

Configuring Dynamic Address Groups

Dynamic address groups allow you to create policy that automatically adapts to changes—adds, moves, or deletions of servers. It also enables the flexibility to apply different rules to the same server based on its role on the network or the different kinds of traffic it processes.

To configure a dynamic address group:

1. Select Palo Alto Networks > Objects > Address Groups.

Figure 9: Address Groups

2. Click Add and enter a Name and a Description for the address group.
3. Select Type as **Dynamic**. Define the match criteria. You can select dynamic and static tags as the

match criteria to populate the members of the group.

4. Enter the role name of the users. The role name in the Match section should match the roles that are configured in PPS.
5. Click **OK**.



Note: Dynamic discovery of users and their roles is not supported on the Palo Alto Networks firewall.

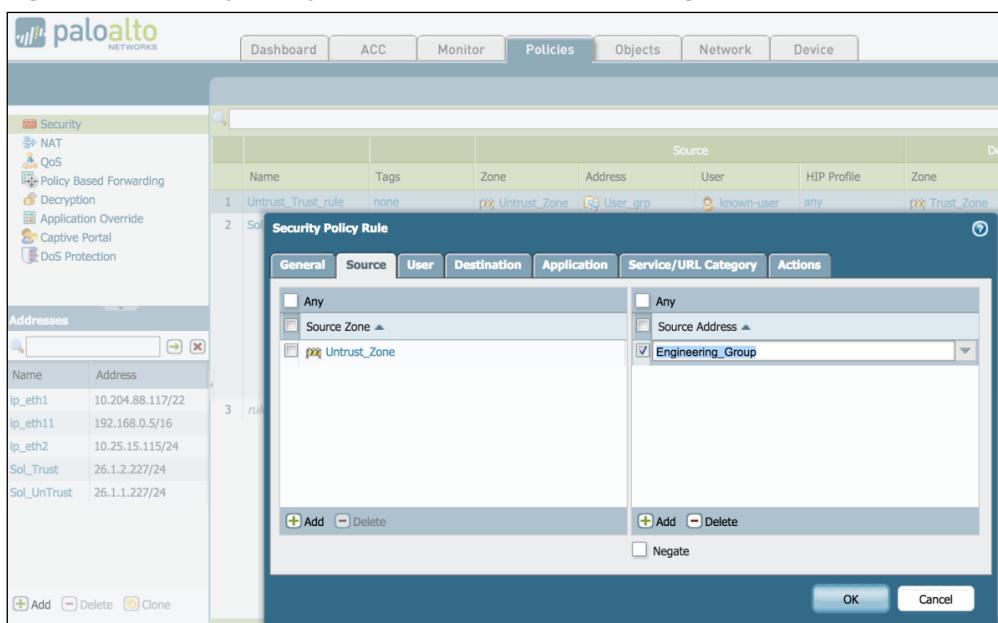
Configuring Security Policies

Security policies protect network assets from threats and disruptions and aid in optimally allocating network resources for enhancing productivity and efficiency in business processes. On the Palo Alto Networks firewall, security policies determine whether to block or allow a session based on traffic attributes such as the source and destination security zone, the source and destination IP address, the application, user, and the service.

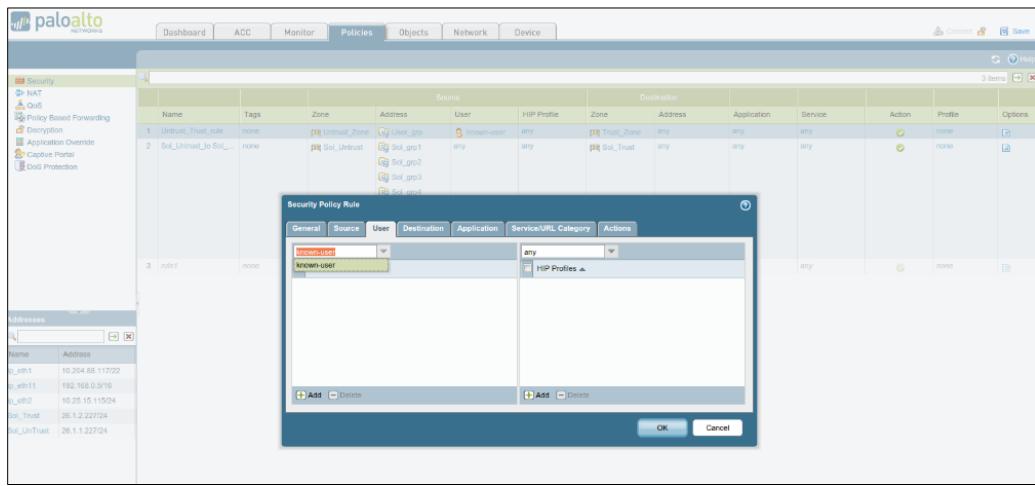
To configure security policies associated with dynamic address groups:

1. Select Palo Alto Networks > Policies > Security.
2. Click Add to create a new security policy rule. In the Source Address tab, select the previously-configured address group, as shown in figure.

Figure 10: Security Policy Rule - Source Address Configuration

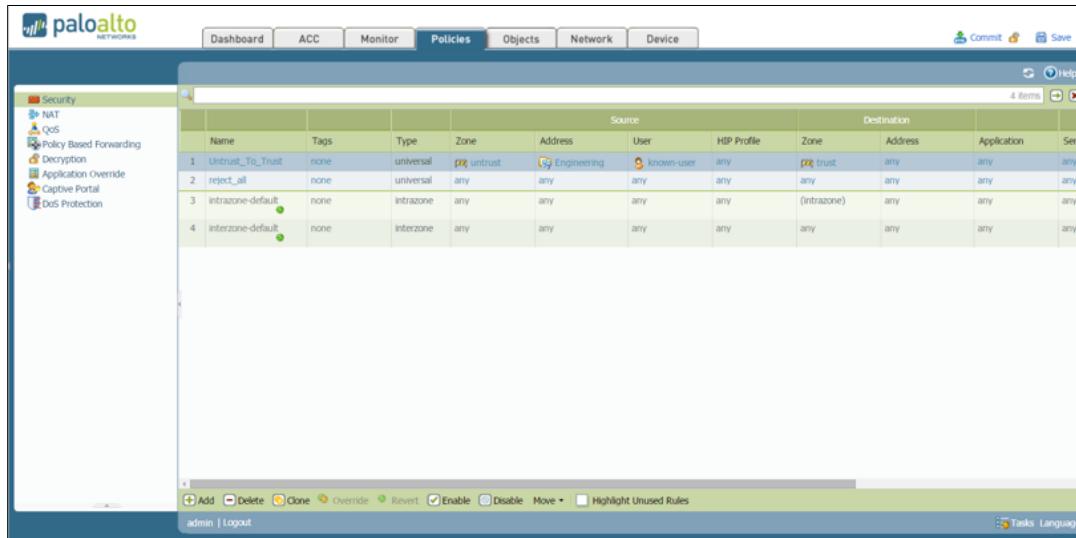


3. In the User tab, enable **known-user**.

Figure 11: Security Policy Rule - User Configuration

i Note: When the known-user is enabled, the resource access is revoked immediately once the user disconnects from PPS.

- Configure the other options to meet your security requirements. Traffic from the endpoint is allowed or blocked based on the action chosen under the Action tab.
- Click **Commit** to complete the configuration. The completed security configuration on the Palo Alto Networks firewall is shown below.

Figure 12: Completed Security Policy Rule

Configuring PAN Device Certificates

PAN device certificate validation enhances the security between PPS and the PAN device. It allows PPS to verify whether the server certificate is from a trusted source. This topic describes how to configure the PPS for validating device certificates, creating certificates on PAN, and checking the validity of the certificate.

This section covers the following configuration:

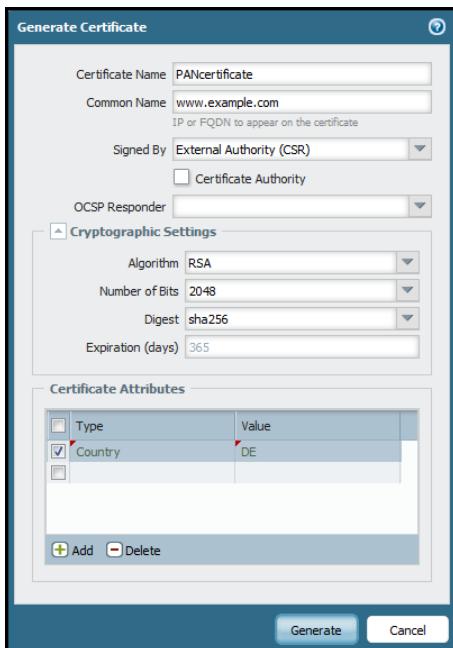
- Creating a Certificate Signing Request (PAN 6.0 and later)
- Exporting the CSR and Importing the Signed Request
- Importing the Certificate on PPS
- Adding PAN Device to PPS

Creating a Certificate Signing Request (PAN 6.0 and later)

To create a Certificate Signing Request (CSR) for sending to public third-party Certificate Authority (like Verisign, Globalsign, Entrust, and so on). For more information, see <https://www.paloaltonetworks.com/documentation/60/pan-os/pan-os/certificate-management/obtain-certificates>

1. Select **Device > Certificate Management > Certificates > Device Certificates**.

Figure 13: Certificate Signing Request



2. Enter a **Certificate Name** (save this name for later).
3. In the Common Name field, enter the IP address of the interface where you will configure the service that will use this certificate.
4. Select the **Certificate Authority** (CA) check box for self-signed root CA certificate. Exporting the CSR and Importing the Signed Certificate are not applicable for self-signed certificates.

Note: Uncheck the Certificate Authority check box if you are using enterprise CA, or trusted third-party CA certificates.

5. Complete the remaining details such as Country, Organization, and so on. Check with the Certificate Authority (CA) about their requirements for Certificate Attribute formatting and criteria.
6. Click Generate.

Note: Ensure that the SSL/TLS service profile is enabled while creating the server certificate.

Exporting the CSR and Importing the Signed Request

Once the CSR is created, you must export the CSR to a third-party CA for signature.

To export the CSR:

1. Click the check box next to the Certificate Name.
2. Click **Export** and save the file.
3. Send the exported CSR to a third-party Certificate Authority. The CA will respond with a signed certificate.

Once the CA responds with the signed certificate, you must import the signed certificate from the certificate authority.

To import the signed certificate:

1. Note the name, including capitalization, of the certificate to import. (This must match the CSR request from above.)
2. Click **Import**.
3. In the Import Certificate dialog, type the name of the pending certificate. It must match exactly.
4. Go to the signed certificate received from the Certificate Authority and click OK.
5. Do not click the **Import Private Key** check box.
6. Depending on the certificate authority used, it may be necessary to chain the intermediate certificate with the server certificate and import it before completing this step.
7. Click **OK**.

Importing the Certificate on PPS

You can use the Trusted Server CAs page to import the trusted root certificate.

To configure device certificate verification:

1. Select System > Trusted Server CAs > Import Trusted Server CA.
2. Click Browse and select the certificate file.
3. Click Import Certificate. The Trusted Server CA page appears.
4. Verify if the certificate is imported successfully and click Done.
5. Click Configuration > Certificates > Trusted Server CAs and verify that the certificate is from a trusted source.

Adding PAN Device to PPS

For complete information on configuration, see Configuring PAN Infranet Enforcer in PPS.

 **Note:** If the server certificate is not valid the user will see the following error message.

Error: Failed to Retrieve API Key. Peer Certificate cannot be authenticated with known CA certificates.

Troubleshooting

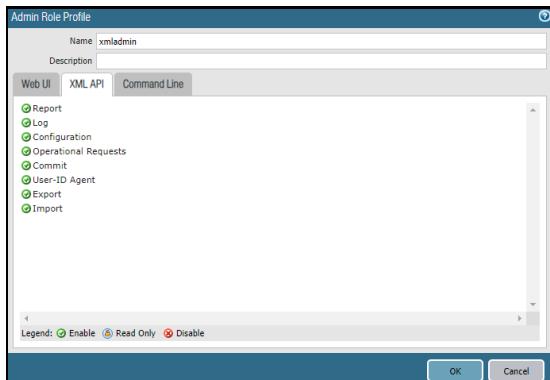
You can use the following CLI commands on the Palo Alto Networks firewall for troubleshooting:

- *show user ip-user-mapping all*— Displays the table of user identities mapped to IP addresses.
- *show object registered-address all* — Displays the table of addresses with user

information associated.

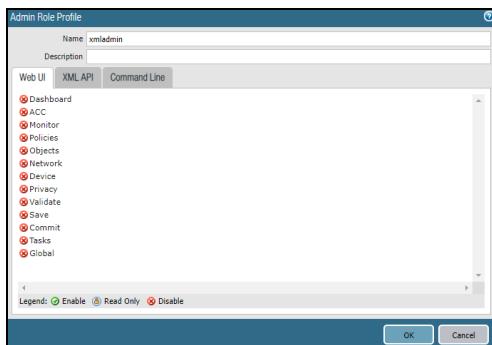
For identity management using Palo Alto Networks firewall only minimum Admin role permissions are sufficient. Ensure that the XML API rights on the Palo Alto Networks UI is enabled as shown in the below screenshot.

Figure 14: XML API



Admin can choose to disable other options from the Web UI tab of the Palo Alto Networks UI as per the security requirement.

Figure 15: Web UI



Unsupported Features

The following features are not supported:

- Captive portal
- IPsec Enforcement
- Virtual Systems (VSYs)
- Enforcement for endpoints behind Network Address Translation (NAT)
- Dynamic Auth Table Allocation

Related Documentation

- For federated access across multiple policy servers / firewall enforcers federated single sign-on for Pulse Connect Secure tunneled traffic, see Provisioning PCS sessions to PAN Firewall.

- For information on Alert based Admission Control, see Alert Based Admission Control

Provisioning PCS sessions to PAN Firewall

This chapter provides an overview of provisioning PCS/PPS user sessions to PAN firewall through IF-MAP server. It includes the following information:

- Overview
- Deployment of PPS/PCS using PAN Next Generation Firewall
- IF-MAP Configuration

Overview

Pulse Policy Secure (PPS) integrates with Palo Alto Network's (PAN) Next Generation Firewall to provision user's identity information (user name, roles and IP address) to PAN/firewall.

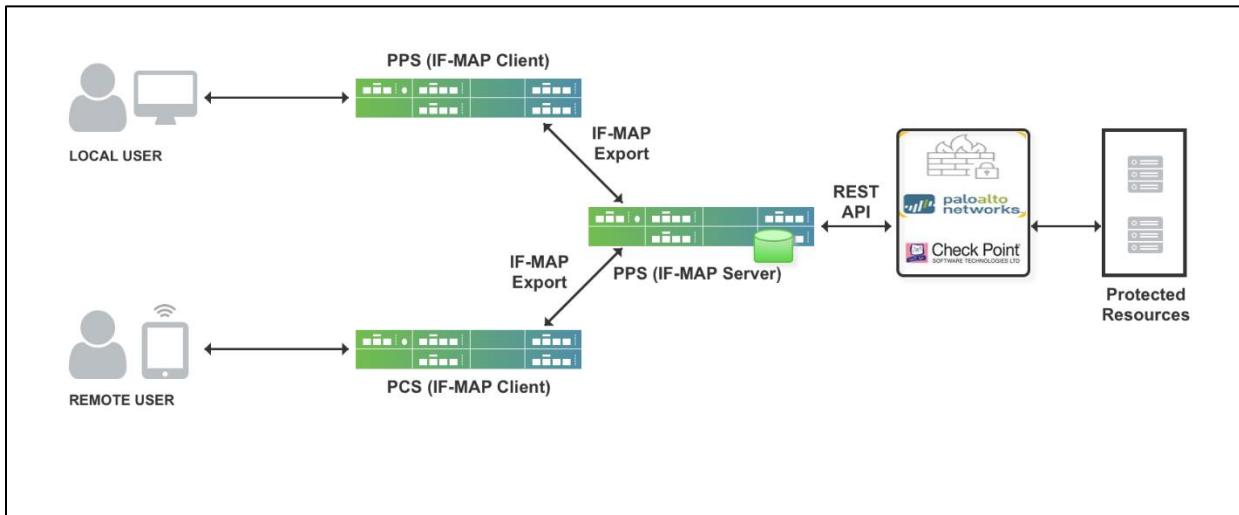
This section focuses on provisioning Pulse Connect Secure (PCS) /PPS user's identity information to PAN firewall using IF-MAP server. Using this solution access control can be provided for PCS/PPS users for accessing resources protected by Firewall.

Deployment of PPS/PCS using PAN Next Generation Firewall

In a federated enterprise, a user can log in to a PPS or PCS device (remote access) for authentication and access the resource protected by the PAN Firewall. The session information is shared across PPS or PCS device using IF-MAP protocol through IF-MAP server.

The PAN Firewall controls the PPS and PCS user's access to protected resources based on the policy settings. The IF-MAP server receives the session information of multiple PPS and PCS and provisions user identity information to Firewall. The federation requires provisioning of user's information on the PAN Firewall and allows access to the protected resource based on the resource access policies that are configured on PPS.

Figure 16: Deploying PPS/PCS using PAN Next Generation Firewall



The authentication process is described below:

1. The remote user establishes VPN tunnel using Pulse Client and the role is granted to the user based on policy configured on PCS.
 - a. PCS session is exported to IF-MAP server.
 - b. IF-MAP server provisions user identity details to PAN Firewall.
2. The remote user tries to access PAN firewall protected resource. PAN Firewall allows access to protected resource if the user is authorized.
3. User's role changes while logged in (for example, when Host Check compliance change causes role(s) to change). In this case, user's new role(s) are sent to PAN Firewall.
4. User logs out of PCS. In this case, all information associated with the user from that endpoint is removed from the Firewall. User is denied access to protected resources by Firewall.



Note: The same workflow applies to local users connecting through PPS.

IF-MAP Configuration

A high-level overview of the configuration steps needed to set up and run the integration:

- The Administrator configures IF-MAP clients (PPS, PCS) on IF-MAP server admin UI from System > IF-MAP Federation.
- Install the Device certificates and Trusted Server CA from System > Configuration > certificates on both IF-MAP Server and IF-MAP client.
- From IF-MAP Server admin UI, admin configures PAN Firewall device by entering the following:
 - Name for the PAN Firewall.
 - IP address of the PAN Firewall.
 - API Key for PAN
 - Administrator configures the Infranet Enforcer Auth Table Mapping Policies.

When the PPS or PCS session is exported to IF-MAP server, IF-MAP server provisions user identity details to configured PAN Firewall based on the configured Auth Table Mapping Policies.

This section covers the following topics:

- Configuring IF-MAP Server
- Configuring IF-MAP Client
- Viewing the Federated Session Details

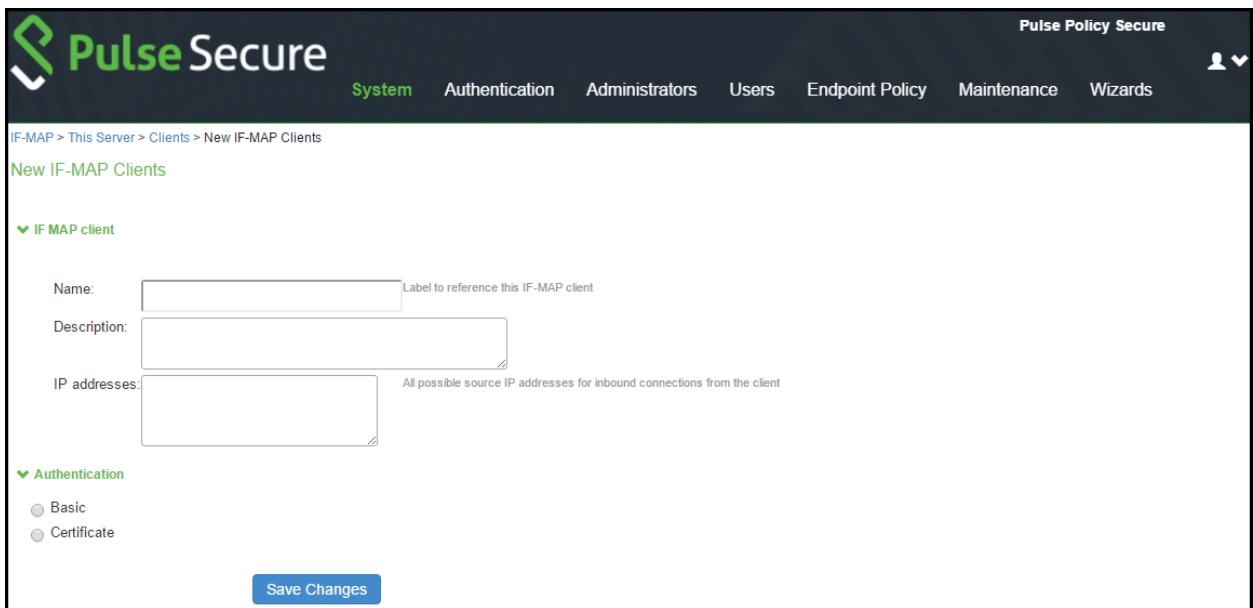
Configuring IF-MAP Server

To configure IF-MAP server on the PPS:

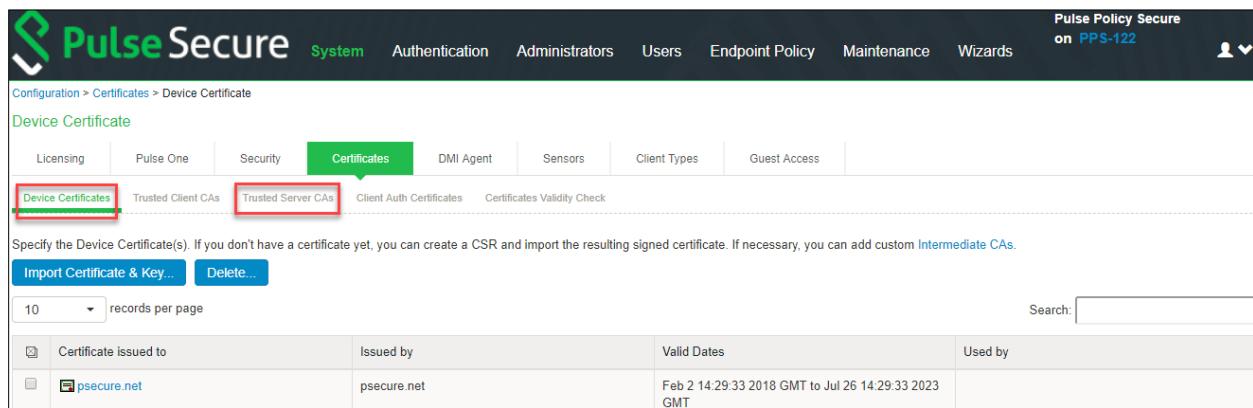
1. Select **System > IF-MAP Federation > Overview**.
2. Select **IF-MAP Server**.
3. Click **Save Changes**.

Figure 17: Overview

4. Select **IF-MAP > This Server > Clients > New Client** and add PPS/PCS as IF-MAP client.

Figure 18: Add IF-MAP Client

5. Install the Device certificates and Trusted Server CA from **System > Configuration > Certificates** on both IF-MAP Server.

Figure 19: Certificates

6. If the client is added successfully the status turns to green color.

Figure 20: This Server

IF-MAP > This Server > Clients

Clients

Overview This Server This Client

Clients Replicas Federation-Wide Sessions

New client... Duplicate... Enable Disable Delete...

10 records per page Search:

Name	IP Addresses	Enabled	Status	Detail
PCS-90.250	10.204.90.250	✓	●	

Configuring IF-MAP Client

To configure the IF-MAP client:

1. Select **System > IF-MAP Federation > Overview**.
2. Select **IF-MAP Client**.
3. Enter the IF-MAP server IP address or the complete server URL.

Figure 21: Overview

IF-MAP > Overview

Overview

Overview This Client

An IF-MAP federation simplifies the work of end users by letting network devices share information about user sessions. For example, if a user connects to the network using Connect Secure, they can automatically gain access (if authorized) to protected resources that are behind Intranet Enforcer firewalls, without having to log in again.

Choose whether this Pulse Policy Secure runs an IF-MAP Server, an IF-MAP client, or no IF-MAP

IF-MAP Server An IF-MAP Server is automatically an IF-MAP client of itself

IF-MAP Client

No IF-MAP

Server URL

* Server URL: Example: https://lc/dana-ws/soapidsifmap

Authentication

Basic

* Username:

* Password:

Certificate

Save Changes Cancel

After completing the IF-MAP server and IF-client configurations, configure the IF-MAP Policies. For more

information, see Configuring Session Export Policies.

Note: This use case supports configuring only Session-Export policies.

Viewing the Federated Session Details

1. Select **System > IF-MAP > This Server > Federation-wide Sessions**.

Figure 22: Federation-wide Sessions

User	Capabilities	IF-MAP Roles	Device Attributes	Signin Time	Events	Signed in IP Address	Signed in MAC Address	Publisher ID
user1	LimitedAccess_Role			2018-01-12 09:37:40		10.0.0.110.5		1CsxZeQ/PCS-90 250

Alert Based Admission Control

This chapter provides an overview of enforcement using PAN Next Generation Firewall. It includes the following information:

- Overview
- Deployment of PPS using PAN Next Generation Firewall
- Configuring PPS with PAN Next Generation Firewall
- Configuring PAN Next Generation Firewall
- Troubleshooting

Overview

PPS integration with PAN next generation firewall provide user access control based on the threats identified by the network security devices. The network security device provides intelligence driven detection of threats based on the intrusion prevention system. This helps in detecting the unknown threats and reduces the false alarms. The PAN Next Generation Firewall uses the syslog events to notify the other devices regarding the network threats. PPS also supports dynamically changing the access to the user based on the information received from the PAN Next Generation Firewall.

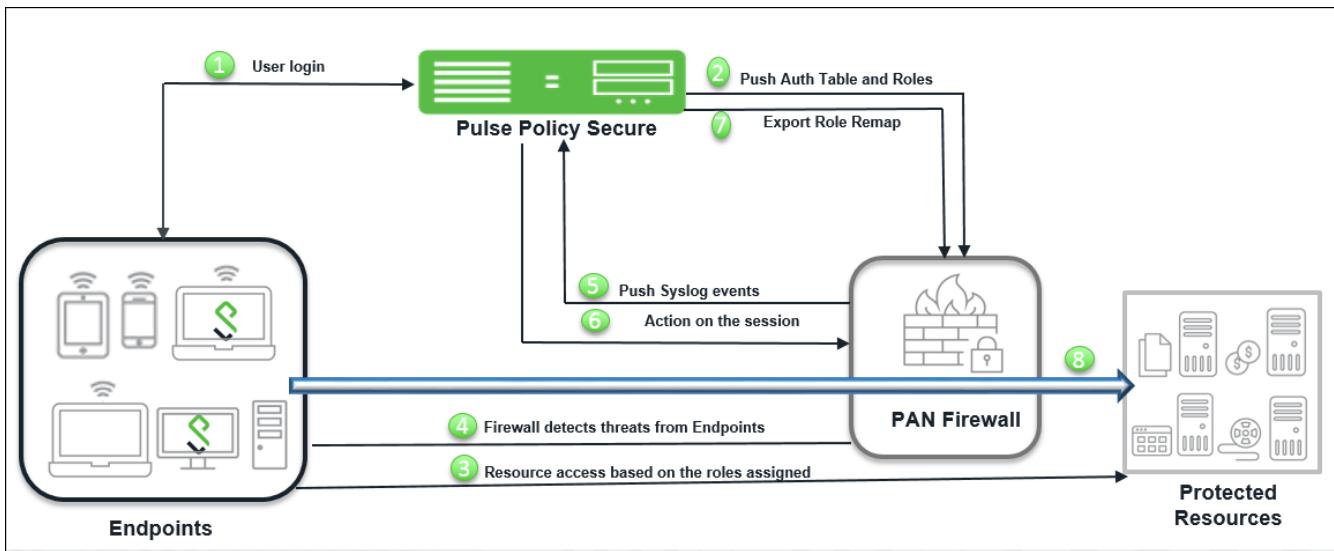
The admission control user flow is as follows:

1. The user logs into the PPS and a corresponding session is created on PPS.
2. The user starts accessing the resources and tries to access a restricted website or application.
3. The PAN Next Generation Firewall identifies it as threat and generates a corresponding syslog event and sent to PPS.
4. PPS receives the threat information and based on the policies configured it modifies the user access. For example, changing user access, terminating user access and so on.

Deployment of PPS using PAN Next Generation Firewall

This section describes the integration of PPS with PAN Next Generation Firewall. PPS integrates with PAN Next Generation Firewall syslog notification mechanism to receive the threat alert information from Palo Alto Networks and takes an action based on the admin configured policies.

Figure 23: Deployment using PAN Next Generation Firewall



The authentication process is described below:

1. User is authenticated on PPS after validating the Host Checker policy.
2. The user sessions are exported to PAN through enforcement configuration, which uses REST APIs for updating the session details.
3. The PAN Next Generation firewall obtains session information from REST APIs and creates an IP to username mapping. The firewall can use this information to either allow or block traffic based on the configured policy.
4. PAN Next Generation Firewall Monitors the end user flow and activity and detects attacks/malicious activity at the end user session
5. PAN Next Generation Firewall sends a syslog message to PPS if any suspicious traffic or activity is detected from end user.
6. PPS will process the received syslog message and based on the configured policies, actions will be taken for the end user session.
7. PPS will update PAN Next Generation firewall with updated session information.
8. The PAN Next Generation Firewall changes access to the user based on the updated session information obtained from PPS.



Note: The enforcement of the user is also updated on the firewall.

Configuring PPS with PAN Next Generation Firewall

The network security devices are configured with PPS for admission access control. A high-level overview of the configuration steps needed to set up and run the integration is described below:

- The Administrator configures the PAN syslog client on PPS Admin UI.

The network security device acts as a syslog client on which syslog forwarding is enabled and PPS receives the forwarded syslog messages.

- The Administrator then configures a set of policies that define what actions are to be

taken on user sessions, based on the data in the threat events.

The actions on sessions supported are

- Ignore - Logs and ignores the syslog message.
- Terminate session - Removes the user session.
- Disable - Removes the user session and disables the user.
- Change role - Update the user session with limited role specified. The role change can also be marked as permanent or only for that session.
 - The user templates are used to identify events supported by the security device. It also provides the pattern match for collecting values for predefined variables which are used for acting on a session. The predefined variable used are source IP, source user, event and severity.

This section covers the following topics:

- Admission Control Template
- Admission Control Policies
- Admission Control Client

Admission Control Template

The admission control template provides the list of possible events that can be received from the network security device along with regular expression to parse the message. The template also provides possible actions that can be taken for an event.

PPS is loaded with default templates for Fortigate, Fortianalyzer and PAN next generation firewall. Admin can create templates for other security devices and can upload to templates.

You can view the list of configured integration templates that provides the list of network security devices and the supported protocol type using Endpoint Policy > Admission Control > Templates.

To view the admission control templates:

Select **Endpoint Policy > Admission Control > Templates**.

Figure 24: Existing Template

Admission Control > Templates																																									
Templates																																									
		Configure		Templates																																					
New Template...		Delete...		Restore Factory Default...																																					
10 records per page		Search: <input type="text"/>																																							
<table border="1"> <thead> <tr> <th>Q</th><th>Name</th><th>File Name</th><th>Protocol Type</th><th>Vendor</th><th>Device Type</th></tr> </thead> <tbody> <tr> <td>1</td><td>paloaltonetworksfw-ietf.1tmpl</td><td>paloaltonetworksfw-ietf.1tmpl</td><td>Syslog</td><td>PaloAlto Networks</td><td>Firewall</td></tr> <tr> <td>2</td><td>fortigate-text.1tmpl</td><td>fortigate-text.1tmpl</td><td>Syslog</td><td>Fortinet</td><td>Firewall</td></tr> <tr> <td>3</td><td>fortianalyzer-text.1tmpl</td><td>fortianalyzer-text.1tmpl</td><td>Syslog</td><td>Fortinet</td><td>Analyzer</td></tr> <tr> <td>4</td><td>fortianalyzer-cef.1tmpl</td><td>fortianalyzer-cef.1tmpl</td><td>Syslog</td><td>Fortinet</td><td>Analyzer</td></tr> <tr> <td>5</td><td>fortigate-cef.1tmpl</td><td>fortigate-cef.1tmpl</td><td>Syslog</td><td>Fortinet</td><td>Firewall</td></tr> </tbody> </table>						Q	Name	File Name	Protocol Type	Vendor	Device Type	1	paloaltonetworksfw-ietf.1tmpl	paloaltonetworksfw-ietf.1tmpl	Syslog	PaloAlto Networks	Firewall	2	fortigate-text.1tmpl	fortigate-text.1tmpl	Syslog	Fortinet	Firewall	3	fortianalyzer-text.1tmpl	fortianalyzer-text.1tmpl	Syslog	Fortinet	Analyzer	4	fortianalyzer-cef.1tmpl	fortianalyzer-cef.1tmpl	Syslog	Fortinet	Analyzer	5	fortigate-cef.1tmpl	fortigate-cef.1tmpl	Syslog	Fortinet	Firewall
Q	Name	File Name	Protocol Type	Vendor	Device Type																																				
1	paloaltonetworksfw-ietf.1tmpl	paloaltonetworksfw-ietf.1tmpl	Syslog	PaloAlto Networks	Firewall																																				
2	fortigate-text.1tmpl	fortigate-text.1tmpl	Syslog	Fortinet	Firewall																																				
3	fortianalyzer-text.1tmpl	fortianalyzer-text.1tmpl	Syslog	Fortinet	Analyzer																																				
4	fortianalyzer-cef.1tmpl	fortianalyzer-cef.1tmpl	Syslog	Fortinet	Analyzer																																				
5	fortigate-cef.1tmpl	fortigate-cef.1tmpl	Syslog	Fortinet	Firewall																																				
<table border="1"> <tr> <td>← Previous</td><td>1</td><td>Next →</td></tr> </table>						← Previous	1	Next →																																	
← Previous	1	Next →																																							

Admission Control Policies

The admission control policies define the list of actions to be performed on PPS for the user sessions. The actions are based on the event and the severity information received from the network security device.

To view and add the new integration policy:

1. Select **Endpoint Policy > Admission Control > Policies**.

Figure 25: Configuration Policies

	Name	Protocol Type	Vendor	Device Type	Event	Severity	Action	Applies to
1	URL Policy	Syslog	PaloAlto Networks	Firewall	url	Any	terminateSession	All
2	Flood	Syslog	PaloAlto Networks	Firewall	flood	Any	terminateSession	All
3	Vulnerability	Syslog	PaloAlto Networks	Firewall	vulnerability	Critical	terminateSession	All
4	AntiSpyware	Syslog	PaloAlto Networks	Firewall	spyware	Critical	terminateSession	All
5	Wildfire	Syslog	PaloAlto Networks	Firewall	wildfire	Any	terminateSession	All
6	Data	Syslog	PaloAlto Networks	Firewall	file	Critical	terminateSession	All

2. Click New Policy.
3. Enter the policy name.
4. Select PaloAlto Networks-Firewall-Syslog-text as a template.
5. Under Rule on Receiving, select the event type and the severity level. The event types and the severity level are based on the selected template.

Figure 26: Adding New Configuration Policy

6. Under Count these many times, enter the number between 1-256.

7. Under **then perform this action**, select the desired action.
 - Ignore (log the event) —Received syslog event details are logged on the PPS and no specific action is taken.
 - Terminate user session— Terminates the user session on the PPS for the received messages.
 - Disable user account— Terminates the user session and disables the user on the PPS for the received messages.
 - Replace user role with this role— Changes the roles assigned to the user on PPS so that restriction/privileges for the user can be changed.
 - Specify whether to apply the role assignment permanently or only for the session.
8. Under **Roles**, specify:
 - Policy applies to ALL roles—To apply the policy to all users.
 - Policy applies to SELECTED roles—To apply this policy only to users who are mapped to roles in the Selected roles list. You must add roles to this list from the Available roles list.
 - Policy applies to all roles OTHER THAN those selected below—To apply this policy to all users except for those who map to the roles in the Selected roles list. You must add roles to this list from the Available roles list.
9. Click Save changes.

Admission Control Client

The admission control clients are the network security devices on which the syslog forwarding is enabled. The messages are received by the syslog server module running on PPS.

To add a client:

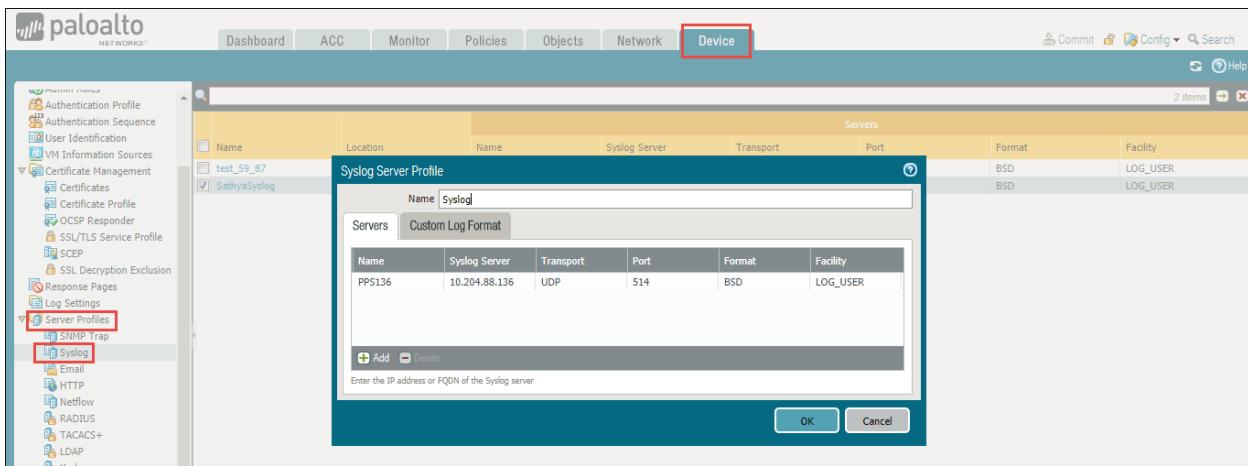
1. Select Endpoint Policy > Admission Control > Clients.
2. Click New Client.
3. Enter the name of the client that will be added in the PPS.
4. Enter the description.
5. Enter the IP address of the client.
6. Select the template used by the client.
 - PaloAlto Networks-Firewall-Syslog-text
7. Click Save Changes.

Configuring PAN Next Generation Firewall

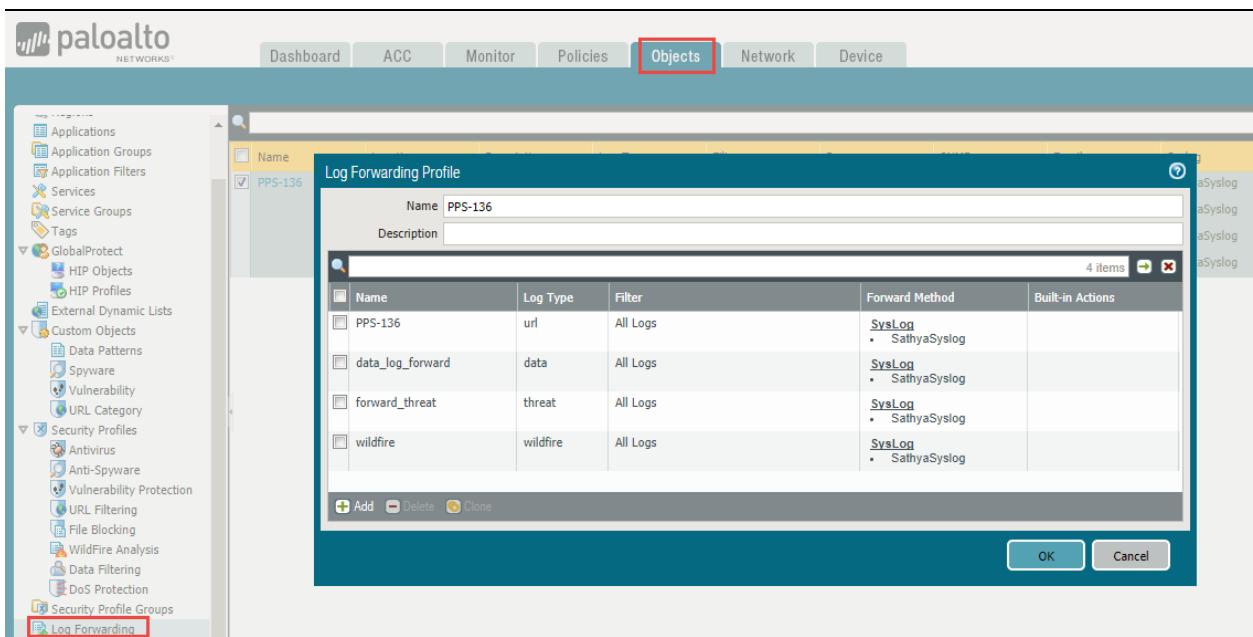
The PPS device must be added as a syslog server while configuring the PAN Next Generation Firewall for sending the logging information. You must add PAN Next Generation Firewall as syslog client on PPS.

To configure PAN firewall:

1. Select **Device > Service Profiles > Syslog** and create a syslog server. Enter the IP address of PPS.

Figure 27: Syslog Server

2. Create a log forwarding profile. Select **Objects > Log Forwarding**. Enable PAN to forward the syslog message.

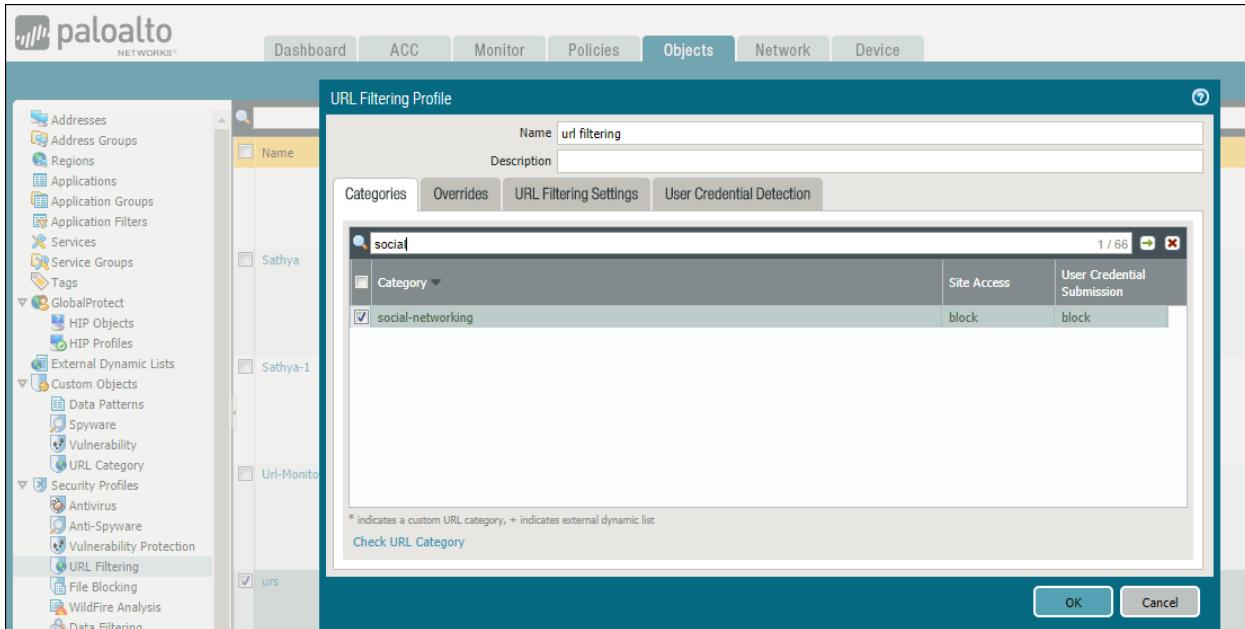
Figure 28: Log Forwarding

Note: On PAN Next Generation Firewall, configure the security policy – network trust, untrust zone and apply the policy to desired ports.

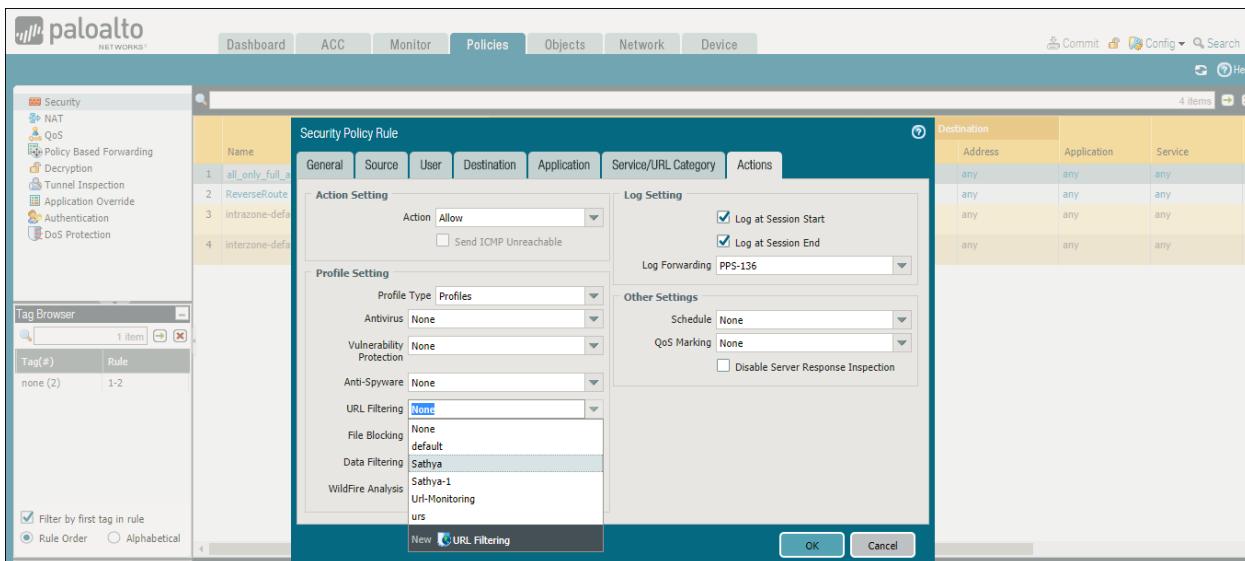
3. Select **Objects > Security Profiles** and create a security profile. The following security profiles are available:

- URL Filtering
- Anti Spyware
- Vulnerability Protection
- File Blocking

- Wildfire Analysis
 - DoS Protection
4. The following is an example of configuring a URL filtering policy.

Figure 29: URL Filtering Profile

5. Select **Policies > Security**, click the policy add the created objects to Security Policy Rule.

Figure 30: Security Policy Rule

Troubleshooting

When the network security device detects threats, the syslogs are forwarded to PPS.

For example, to monitor the URL filtering logs on PAN Next Generation Firewall, select Monitor > URL Filtering and view the logs.

Figure 31: Events Log

The screenshot shows the Palo Alto Networks Monitor interface. The top navigation bar includes Dashboard, ACC, Monitor (which is highlighted with a red box), Policies, Objects, Network, and Device. On the left, a sidebar menu under the Logs section is expanded, showing Traffic, Threat, and URL Filtering (which is also highlighted with a red box). Other items in the sidebar include WildFire Submissions, Data Filtering, HIP Match, User-ID, Tunnel Inspection, Configuration, System, Alarms, Authentication, Unified, Packet Capture, and App Scope. The main pane displays a table of URL filtering logs with the following columns: Receive Time, Category, URL, From Zone, To Zone, Source, Source User, Destination, Application, and Action. The logs show multiple entries for Facebook URLs being blocked from trust to untrust zones.

Receive Time	Category	URL	From Zone	To Zone	Source	Source User	Destination	Application	Action
01/21 11:05:12	social-networking	www.facebook.c...	trust	untrust	10.25.15.102		157.240.21.35	facebook-base	block- url
01/21 10:35:12	social-networking	www.facebook.c...	trust	untrust	10.25.15.102		157.240.21.35	facebook-base	block- url
01/21 10:05:12	social-networking	www.facebook.c...	trust	untrust	10.25.15.102		157.240.21.35	facebook-base	block- url
01/21 09:35:11	social-networking	www.facebook.c...	trust	untrust	10.25.15.102		157.240.21.35	facebook-base	block- url
01/21 09:05:10	social-networking	www.facebook.c...	trust	untrust	10.25.15.102		157.240.21.35	facebook-base	block- url
01/21 08:35:10	social-networking	www.facebook.c...	trust	untrust	10.25.15.102		157.240.21.35	facebook-base	block- url
01/21 08:05:10	social-networking	www.facebook.c...	trust	untrust	10.25.15.102		157.240.21.35	facebook-base	block- url
01/21 07:35:09	social-networking	www.facebook.c...	trust	untrust	10.25.15.102		157.240.21.35	facebook-base	block- url

To verify the event logs on PPS, select System > Log/Monitoring > Events.

Figure 32: Events

The screenshot shows the Pulse Secure Log/Monitoring interface. The top navigation bar includes System, Authentication, Administrators, Users, Endpoint Policy, Maintenance, and Wizards. Below the navigation bar, it says "Log/Monitoring > Events > Logs". The main pane is titled "Logs" and has tabs for Events (which is selected and highlighted with a green box), User Access, Admin Access, Sensors, Client Logs, SNMP, Statistics, and Advanced Settings. Under the Events tab, there are buttons for Log, Settings, and Filters. A "View by filter:" dropdown is set to "Standard:Standard (default)" and a "Show" dropdown is set to "200 items". There is a "Edit Query:" input field with "Update", "Reset Query", and "Save Query..." buttons. Below these are "Save Log As...", "Clear Log", "Save All Logs", and "Clear All Logs" buttons. A "Filter:Standard (default)" section shows "Date:Oldest to Newest" and "Query:". An "Export Format:Standard" section is present. The bottom part of the screen displays a table of log entries with columns: Severity, ID, and Message. Two log entries are shown:

Severity	ID	Message
Info	INT31545	2018-01-21 08:48:07 - [127.0.0.1] System[0] - Syslog Message received from Client: 10.96.70.1 Message: <14>Jan 23 14:46:18 PA-VM 1.2018/01/23 14:46:18.007951000021073.SYSTEM.url-filtering.0,2018/01/23 14:46:18.,upgrade-url-database-success,,0,general,informational,PAN-DB was upgraded to version 20180122.40111,146008.0x0,0,0,0,PA-VM
Info	INT31545	2018-01-21 08:43:12 - [127.0.0.1] System[0] - Syslog Message received from Client: 10.96.70.1 Message: <14>Jan 23 14:41:17 PA-VM 1.2018/01/23 14:41:17.007951000021073.SYSTEM.url-filtering.0,2018/01/23 14:41:17.,upgrade-url-database-success,,0,general,informational,PAN-DB was upgraded to version 20180122.40110,146007.0x0,0,0,0,PA-VM

IoT Policy Provisioning

This chapter provides an overview of IoT device enforcement using PAN firewall. It includes the following information:

- Overview
- Deployments
- Configuring IoT Policy Provisioning

Overview

As we increasingly connect devices to the Internet, new opportunities to exploit potential security vulnerabilities grow. Any unknown devices including IoT devices could serve as entry points for cyberattack by allowing malicious individuals to re-program a device or cause it to malfunction. The IoT devices are being added to corporate networks with or without the knowledge of IT administrator and they may communicate using the corporate IP network. These devices may have limited security controls leaving them open to be used as an attack vector. To improve security posture of IoT devices in corporate network, visibility and Role Based Access Control play a key role. Hence, it's extremely important to detect and classify what's there on the network.

PPS along with Profiler enables you to secure and manage access to IoT devices. It allows you to configure IoT Access Policy based on discovered or profiled device category. It also allows you to dynamically configure resource access policies for newly discovered devices and map user's role-based access to specific category and manufacturer or profile group of IoT devices.

Benefits

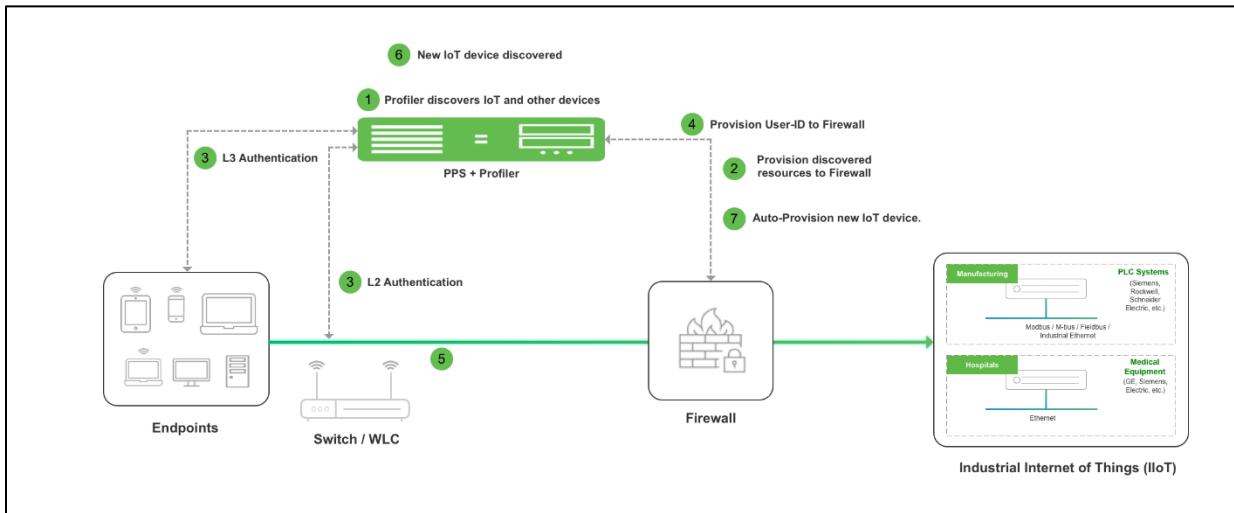
The IoT Policy Provisioning Page enables you to quickly configure IoT policy provisioning and provides the following benefits:

- Discover and profile IoT devices using Profiler. Profiler enables you to continuously monitor the network and discover new devices such as security cameras, sensors, Industrial IoT devices (IIoT), medical sensors, and so on.
- PPS provides IoT access control using the IoT Access Policies, which are created automatically based on profiled or newly discovered device information from Profiler.
- Reduce IoT/IIoT machine downtime by allowing authorised users to get a role-based access to specific IoT/IIoT device for troubleshooting/maintenance.
- Automatic access control for the newly discovered IoT devices.

Deployments

The below network diagram depicts how PPS, Profiler, and PAN Firewall can be deployed to protect access to IoT devices. For example, the manufacturing domain consists of different IoT devices to monitor and control the manufacturing process. The industrial IoT devices are separated and controlled behind the firewall. PPS enables you to define IoT Access Policy using the Profiler attributes (category and manufacturer or profile group) and provides secure and seamless access to IoT devices for authorized users.

Figure 33: IoT Device Deployment



The workflow is described below:

1. A local Profiler configured on PPS discovers devices including IoT devices connected to corporate network.
2. PPS leverages the list of IoT devices discovered using Profiler and based on device category and manufacturer or profile group and it enforces or controls the access to IoT devices protected by the firewall.
3. User authenticates to PPS and endpoint compliance is evaluated. The user session is created on PPS and appropriate role is assigned based on the compliance check and user ID.
4. User Identity details (AuthTable) are provisioned to firewall.
5. User tries to access IoT devices protected by firewall. Authorized users (based on roles) can access IoT devices. Access to IoT devices by unauthorized users is blocked.
6. A new IoT device is added to the corporate network and same is discovered by Profiler.
7. IoT Access Policy for the newly discovered IoT device is automatically pushed to PAN firewall.

Note:

- Only Local Profiler is currently supported.
- The Administrator can group the discovered devices based on any Profiler attributes. For more information see, Configuring Profiler Groups.

Configuring IoT Policy Provisioning

This section covers the procedure for configuring IoT Policy Provisioning on PPS.

- Basic Configurations
- Configuring IoT Access Policy
- Configuring Additional Device Category/Profile Groups

Pre-Requisite

IoT Policy Provisioning requires Profiler feature. You must install the Profiler license on PPS to enable it.

Summary of Configuration

A high-level overview of the configuration steps needed to set up IoT Policy Provisioning is shown below.

1. Configure Profiler
2. Configure PAN Enforcer
3. Configuring IoT Access Policy
 - a. Viewing Devices in Enforcer Policy Report
 - b. **Error! Reference source not found.**
 - c. Configuring Additional Device Category/Profile Groups

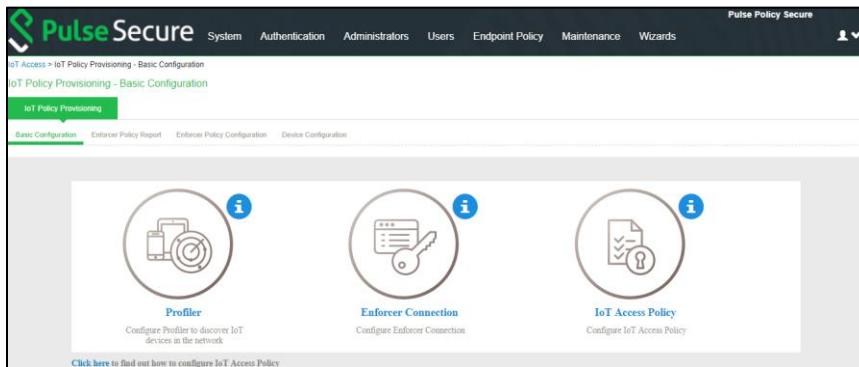
Basic Configurations

The basic configuration page enables you to configure Profiler to discover IoT devices in the network, Enforcer to push the user identity information to PPS, and IoT Access Policy for IoT devices.

To launch the configuration page:

1. Select **Endpoint Policy > IoT Access > IoT Policy Provisioning**.
2. Click **Basic Configuration**.

Figure 34: Policy Provisioning- Basic Configurations



- i Note:** If PPS is already configured with Profiler and Enforcer. The configurations will be reused.
3. Configure the Profiler used to discover the IoT devices in the network. Click **Profiler** and configure the local Profiler. See [Profiler Deployment Guide](#) for complete configuration.

The icons in the configuration page indicate the status of configuration.

- Green Tick mark refers that this section is configured correctly.
- If the configuration section is in grey color, it indicates that the section is not configured.
- Information icon refers that this section must be configured.

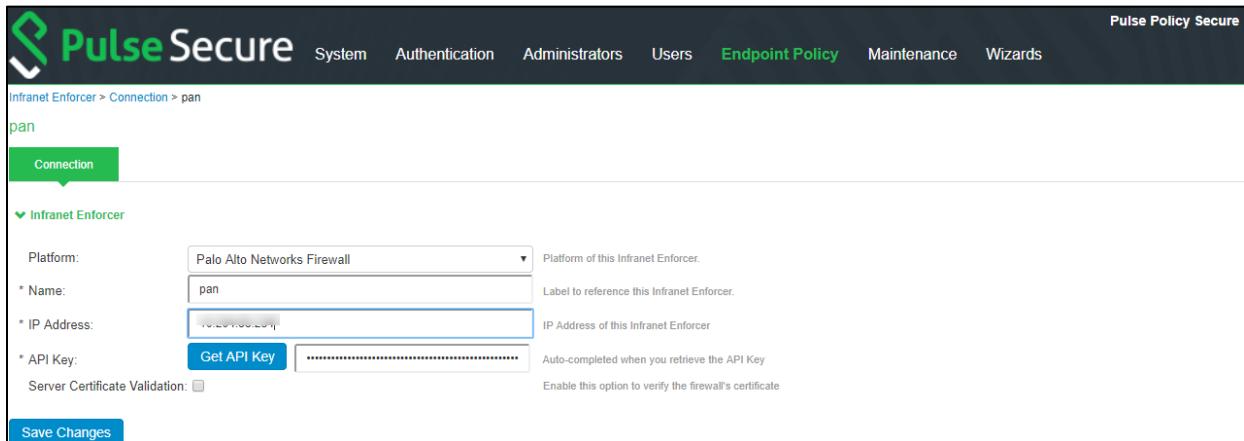
Figure 35: Profiler Settings

The screenshot displays the 'Profiler Settings' page within the Pulse Secure interface. Key sections include:

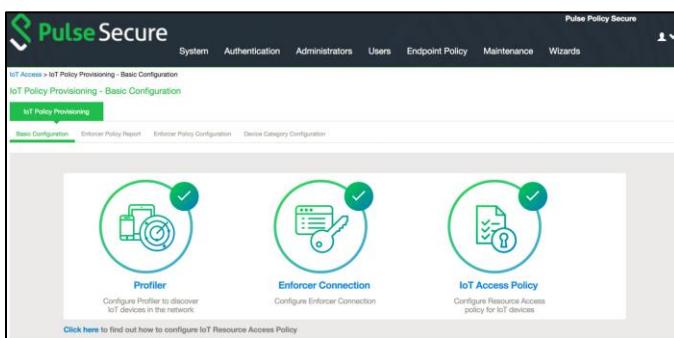
- Fingerprint Database file:** A file named 'fingerprint_db' was last uploaded on June 14, 2018.
- General Settings:** Poll Interval is set to 60 minutes. DHCP Sniffing mode is set to 'DHCP Helper (Internal port)'.
- Device Sponsoring:** Device categories triggering approval emails include BSD, Linux, Other OS, Routers and APs, and Video Conferencing. Approved devices also include Datacenter appliance, Macintosh, Physical Security, Smartphones/PDAs/Tablets, and VoIP Phones/Adapters.
- WMI Profiling:** Credential type is set to 'Configure WMI credentials' (User: admin, Password: redacted). Test Credentials button is present.
- SSH Profiling:** Authentication Method is set to 'Public key'. RSA key owner and RSA private key fields are shown.
- MDM Server:** An MDM server is specified for collecting additional endpoint attributes.

- Configure the PAN Enforcer. Click Enforcer Connection and add PAN as a New Enforcer.

Figure 36: PAN Enforcer



Once the configuration is complete and successful, the Administrator can see the configuration status as shown below.



Configuring IoT Access Policy

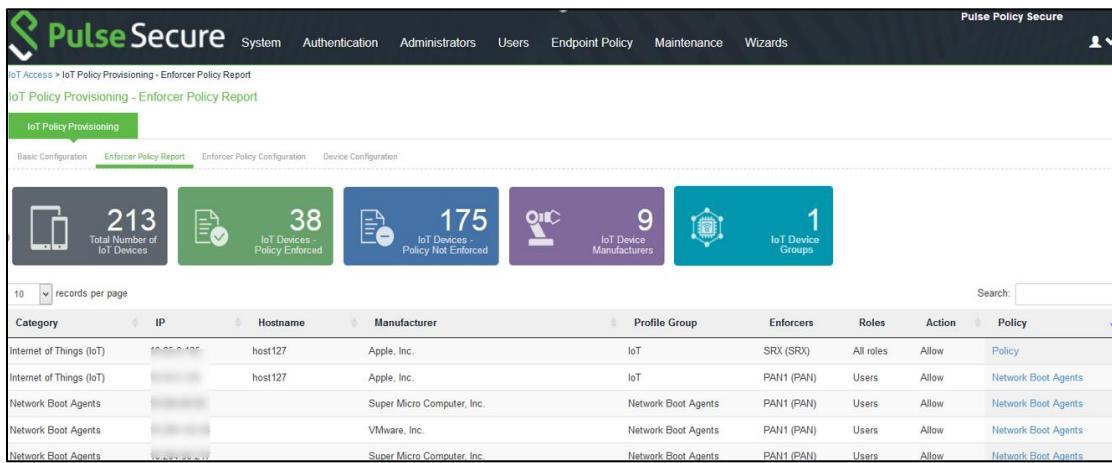
- Viewing Devices in Enforcer Policy Report
- Configuring IoT Access Policy using Palo Alto Networks Firewall

Viewing Devices in Enforcer Policy Report

This page provides details of discovered and connected IoT device's and firewall policies applied for IoT devices. You can view details such as total number of IoT devices, number of IoT devices enforced, number of IoT devices not enforced, and IoT device manufacturers.

To view the enforcer policy report:

- Select **Endpoint Policy > IoT Access > IoT Policy Provisioning**.
- Click **Enforcer Policy Report**.

Figure 37: Enforcer Policy Report

Configuring IoT Access Policy using Palo Alto Networks Firewall

The IoT access policy specifies which users are allowed or denied access to a set of protected resources. You can specify which users you want to allow or deny by choosing the roles for each IoT Access Policy. The IoT Access Policy page enables you to configure the policy based on device details using Profiler device attributes, such as device category and device manufacturer or Profile Group.

When the network Administrator selects category and manufacturer or Profile Group information under device details the IP addresses of the corresponding discovered devices get automatically updated under Resources. Hence the Administrator can seamlessly create IoT Access Policy of profiled devices based on device category, device manufacturer attributes, or Profiler group. If the Administrator wants to have granular control over the IoT devices, further control can be achieved by providing specific port and protocol. The specified port and protocol configuration is applied to all the discovered devices of the selected category and manufacturers.

Follow the steps as mentioned below to configure IoT access policy:

1. Select **Endpoint Policy > IoT Access > IoT Policy Provisioning > Enforcer Policy Configuration**.
2. Click **New Policy**.
3. Enter the **Policy name**.
4. Enter a description.
5. Under Infranet Enforcer, select the Platform as **Palo Alto Networks Firewall**.
6. Under Security Zones, specify the firewall security zones (source zone/destination zone) for the policy. Multiple zones can be specified with comma separated values. If zones are not specified, then it applies to all zones.
7. Under Service, select any to allow all TCP and UDP ports (default) or select the service to specify the TCP or UDP port or port range. The policy port and protocol configuration remain same for all the resources.
8. Under **Device Details**, specify whether the policy should be applied based on device category and manufacturer or Profile group.
 - a. **Category and manufacturer**
 - Specify the category from the drop-down list. The values in the drop-down list is populated based on the Device category configuration (IoT Access > IoT Policy)

Provisioning - Device Configuration).

- Select the Device manufacturer from the Available Device Manufacturers.
- Specify the protocol (TCP/UDP) and Port/Range to be applied to the discovered devices.

b. **Profile Group**

- Configure the Profiler Group (IoT Access > IoT Policy Provisioning - Device Configuration). To configure Profiler Groups, see [Configuring Profiler Groups](#).
- Select the Profile Group from the Available Profile Groups.
- Specify the protocol (TCP/UDP) and Port/Range to be applied to the discovered devices.

i Note: Port ranges must be configured in dash-separated, comma-delimited, ascending, and non-overlapping order. Multiple port ranges must be separated by a comma. For example, the following examples show the delimiters that are used to enter port ranges:(80, 443, 1-1024, 1-100, 500-600).

The Port/Range entered will be applied to all the discovered devices.

- c. Select **Auto-Update Newly Discovered Devices** to automatically add IoT Access Policy for the newly discovered devices from the selected category and manufacturer or Profile Group.

For example, If a policy is created for IoT device category with manufacturer or Profile Group with **Auto-Update Newly Discovered Devices** enabled then for any new IoT device discovered with the selected manufacturer, a IoT Access Policy is automatically added to firewall. If port and protocol are specified in the "Device Details" panel, the policy for the newly discovered devices is applied for specified port and protocol.

9. Under **Resources**, the IoT devices will be auto populated using the Device details configuration described earlier. If the administrator wants to apply policies on different ports and protocols for different discovered devices, the port configuration can be edited. If the Admin selects multiple protocol (for example, TCP and UDP) then the device entries appear twice with protocol information in the Resources table. The Admin can choose whether to push the policies for the selected resource based on the IP address, Protocol, and Port information to enforcer by enabling/disabling the checkbox in the resources table.
10. Select the desired Roles for which the policy applies. For example, IoT Administrator.
11. Under **Actions**, select whether to allow access or deny access.
12. Click **Save Changes**.

Figure 38: Palo Alto Networks Firewall Enforcer Policy Configuration

The screenshot shows the 'New Policy' configuration page in the Pulse Secure interface. The policy is named 'IoT1'. Under the 'Intranet Enforcer' section, the platform is set to 'Palo Alto Networks Firewall'. Available enforcers include 'PAN_88_234 (PANNGFW)' and 'PAN-10.96.70.1 (PANNGFW)'. Under 'Security Zones', source and destination zones are both set to 'trust'. In the 'Device Details' section, a profile group 'iot-group1' is selected. The 'Resources' section lists 24 IP addresses from 10.204.88.72 to 10.209.114.193. Under 'Roles', the 'Policy applies to SELECTED roles' option is selected, and the 'Selected roles' dropdown contains 'FullAccess_Role'. The 'Actions' section has 'Allow access' selected. At the bottom, there are 'Save Changes' and 'Save as Copy' buttons.

Once the policy is successfully added, it can be viewed as shown below.

Figure 39: Policy

Policy	Category	Manufacturers	Profile Groups	Auto-Update	Enforcers	Roles	Resources	Action
IoT	Internet of Things (IoT)	AMERICAN POWER CONVERSION CORP	pan (PAN)	ON	Users		tcp://10.25.15.11:443 tcp://10.25.15.12:443 tcp://10.25.15.13:443 tcp://10.25.15.14:443 tcp://10.25.15.15:443 tcp://10.25.15.16:443 tcp://10.25.15.177:443 tcp://10.25.15.24:443 tcp://10.204.48.2:443	Allow
IoT_Group	IoT Group		IoT Group	ON	Users		tcp://10.204.48.241:443 tcp://10.204.49.21:443 tcp://10.204.49.243:443 tcp://10.204.48.217:443 tcp://10.204.49.122:443 tcp://10.204.49.187:443 tcp://10.204.49.59:443 tcp://10.204.49.30:443 tcp://10.204.49.28:443 tcp://10.204.49.39:443	Allow

Note: Resource Access Policy and IoT Policy Provisioning with Palo Alto Network's Firewall works only with default Virtual System "vsys1" and default device name "localhost.localdomain" configuration.

Configuring Additional Device Category/Profile Groups

The Internet of Things (IoT) device category is selected by default and hence it is visible by default on IoT policy enforcer report and Policy Configuration page. However, If the Administrator wants to use IoT Policy Provisioning feature for other Profiler supported categories such as Video Conferencing Devices, Printers/Scanners, Medical device, Storage device and so on additional categories can be configured on this page.

Under Profile Groups, Admin can select the groups that should be used with IoT Policy Provisioning feature. Only the selected Profile Groups are shown while creating IoT access policy using Profile Groups. If none of the Profile Groups are selected in Device Configuration tab, then no groups are shown in IoT access policy. To create IoT access policy using Profile Groups, the same needs to be selected in the Device Configuration tab.

Figure 40: Device Category Configuration

The screenshot shows the 'IoT Policy Provisioning - Device Configuration' section. The 'Device Configuration' tab is active. Under 'Device Category', there are several categories with checkboxes: BSD, Macintosh, Point of Sale devices, Switches, Datacenter appliance, Medical Device, Printers/Scanners, Thin Clients, Gaming Consoles, Monitoring Devices, Projectors, Video Conferencing, Home Audio/Video Equipment, Network Boot Agents, Routers and APs, VoIP Phones/Adapters, Internet of Things (IoT), Other OS, Smartphones/PDAs/Tablets, Linux, Physical Security, Storage Devices, and Windows. Under 'Profile Group', a group named 'IoT' is selected. A link to view or configure Profile Groups is provided. At the bottom is a 'Save Changes' button.

Configuring Profiler Groups

Administrator can create different Profile Groups by using different Profiler attributes (for example, group all IoT devices with manufacturer Schneider Electric and Operating System Linux) and combine discovered devices in a group. If an Admin wants to provision IoT Access policy using attributes other than Category and Manufacturer, a Profile Group can be created to group discovered devices and then IoT Policy Provisioning feature can be used for the resources belonging to Profile Group.

To configure Profiler Groups:

1. Select the Profiler server under Authentication > Auth. Servers.
2. Select Profile Groups tab, select the **New Profile Group**.
3. Enter the Group Name and Rule. The rules can be written with device attributes and suggested operators can be chosen from the list.
4. As an optional step, emails also can be configured which results in notifications for any group related changes.

Figure 41: New Profile Group

The screenshot shows the 'Edit Profile Group' interface. The group name is 'IoT'. The rule is set to 'category = "Internet of Things (IoT)"'. There is an unchecked checkbox for sending email notifications. Buttons for 'Save' and 'Delete this group' are at the bottom.

5. Click Save Changes.

Troubleshooting

The event and debug logs can be used for troubleshooting:

- The Event logs are generated whenever the policies are pushed to firewall.
- The Admin Logs are generated upon policy provisioning and auto updation of newly discovered devices.

You can also use **Maintenance > Troubleshooting > Monitoring > Debug Log** for debugging issues.

If the device is not discovered properly in the **IoT Policy Provisioning > Enforcer Policy Report** page check the Device Discovery Report page for the device category.

The PPS created policies on PAN firewall should not be modified by the PAN admin. The PPS created policies on Palo Alto Networks firewall are tagged as Pulse Secure Managed.

Figure 42: Debug log for debugging issues

Name	Tags	Type	Source			Destination			Application	Service	Action	Profile	Options
			Zone	Address	User	Zone	Address						
1 IoT1	Pulse Secure M	universal	pq untrust	Users	any	any	pq trust	10.25.15.60	any	IoT1_servic	Allow	none	Edit
2 IoT2	Pulse Secure M	universal	pq trust	Users	any	any	pq untrust	10.25.15.60	any	any	Deny	none	Edit
3 IoT3	Pulse Secure M	universal	pq trust	Users	any	any	pq untrust	10.25.15.60	any	IoT3_servic	Allow	none	Edit
4 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	none
5 interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none	none

Event Logs

To view the communication between PPS and Infranet Enforcer enable **Enforcer Command Trace** under **Events > Settings**.

Figure 43: Enforcer Command Trace

A sample event logs is shown below.

Figure 44: Sample Event Logs

Pulse Policy Secure													
System		Authentication		Administrators		Users							
Log/Monitoring > Events > Logs													
Logs													
Events	User Access	Admin Access	Sensors	Client Logs	SNMP	Statistics	Advanced Settings						
Log	Settings	Filters											
View by filter: Standard Standard (default) Show 200 items													
Edit Query: <input type="text"/>													
<button>Update</button>		<button>Reset Query</button>		<button>Save Query...</button>									
<button>Save Log As...</button>		<button>Clear Log</button>		<button>Save All Logs</button>		<button>Clear All Logs</button>							
Filter: Standard (default) Date: Oldest to Newest Query: Export Format: Standard													
Severity	ID	Message											
Info	GWT31691	2018-10-30 03:18:44 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) Commit success: Commit											
Info	GWT31691	2018-10-30 03:18:44 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) command b'<response status="success" code="19'><result><msg><line>Commit job enqueued with jobid 216</line></msg><job>216</job></result></response>											
Info	GWT31689	2018-10-30 03:18:45 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) type commit cmd <commit></commit>											
Info	GWT31691	2018-10-30 03:18:45 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) ADD policy success: IoT											
Info	GWT31691	2018-10-30 03:18:45 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) command b'<response status="success" code="20'><msg>command succeeded</msg></response>											
Info	GWT31689	2018-10-30 03:18:45 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) type config action set xpath:/config/devices/entry[@name='localhost.localdomain']/sys/entry[@name='vsys1']/rulebase/security/rules/entry[@name='IoT'] element <!-->member=Pulse Secure Managed</member><!-->source</member>users</member>/source</from>untrust</member>/from</to><member>trust</member></to></destination><member>10.25.15.11</member><member>10.25.15.12</member><member>10.25.15.13</member><member>10.25.15.14</member><member>10.25.15.15</member><member>10.25.15.16</member><member>10.25.15.17</member><member>10.25.15.24</member><member>10.204.48.2</member></destination><application><member>any</member></application><service><member>IoT_service_Icp</member></service><action>allow</action>											
Info	GWT31691	2018-10-30 03:18:42 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) Create source address success: Users											
Info	GWT31691	2018-10-30 03:18:42 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) command b'<response status="success" code="20'><msg>command succeeded</msg></response>											
Info	GWT31689	2018-10-30 03:18:42 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) type config action set xpath:/config/devices/entry[@name='localhost.localdomain']/sys/entry[@name='vsys1']/address-group/entry[@name='Users'] element <!-->dynamic</dynamic><filter><members><member>Pulse Secure Managed</member></members>											
Info	GWT31691	2018-10-30 03:18:42 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) Create service success: IoT_service_Icp											
Info	GWT31691	2018-10-30 03:18:42 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) command b'<response status="success" code="20'><msg>command succeeded</msg></response>											
Info	GWT31689	2018-10-30 03:18:42 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) type config action set xpath:/config/devices/entry[@name='localhost.localdomain']/sys/entry[@name='vsys1']/service/entry[@name='IoT_service_Icp'] element <!-->proto=tcp</proto><!-->port=443</port><!-->protocol=tcp</protocol><!-->member=Pulse Secure Managed</member></!-->											
Info	GWT31691	2018-10-30 03:18:42 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) Create tag success: Pulse Secure Managed											
Info	GWT31691	2018-10-30 03:18:42 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) command b'<response status="success" code="20'><msg>command succeeded</msg></response>											
Info	GWT31689	2018-10-30 03:18:41 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) type config action set xpath:/config/devices/entry[@name='localhost.localdomain']/sys/entry[@name='vsys1']/tag/entry[@name='Pulse Secure Managed'] element <!-->color=Color_1</color>											
Info	GWT31691	2018-10-30 03:18:41 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) command b'<response status="success" code="20'><msg><!-->tag</tag></msg></response>											
Info	GWT31689	2018-10-30 03:18:41 - ie - [127.0.0.1] System[] - Enforcer(pn 10.204.88.234) type config action get xpath:/config/devices/entry[@name='localhost.localdomain']/sys/entry[@name='vsys1']/rulebase/security/rules/entry[@name='IoT']											

References

This document complements the following Documents:

- Pulse Policy Secure Administration Guide

Technical Support

When you need additional information or assistance, you can contact “Pulse Secure Global Support Center (PSGSC):

- <https://www.pulsesecure.net/support>
- support@pulsesecure.net
- Call us at 1- 844-751-7629 (toll-free USA)

For more technical support resources, browse the support (<https://www.pulsesecure.net/support>).