



Zero Trust Secure Access with Pulse Policy Secure and Pulse Connect Secure

Integration Guide

Published

August 2020

Document Version

1.0

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

© 2020 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.

Zero Trust Secure Access with Pulse Policy Secure and Pulse Connect Secure

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 <http://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 changes made to this document:

Document Revision	Release	Date	Feature	Changes
1.0	9.1R8	17/8/20	PCS PPS Integration Guide	

PURPOSE OF THIS GUIDE	1
PREREQUISITES	1
USE CASES	1
VISIBILITY AND ENFORCEMENT WITH REMOTE PROFILER	3
ALLOW ADMINISTRATOR ACCESS TO REST APIs	3
CONFIGURING REMOTE PROFILER ON PCS	4
CONFIGURING ROLE-MAPPING RULES FOR PROFILED DEVICES ON PCS	5
END-TO-END ZERO TRUST SECURE ACCESS	8
OVERVIEW	8
IF-MAP FEDERATION USE CASES	8
ACCESS CONTROL IN THE FEDERATED ENTERPRISE	8
SESSION MIGRATION ACROSS PCS AND PPS USING IF-MAP	9
IF-MAP CONFIGURATION	13
CONFIGURING IF-MAP SERVER	13
CONFIGURING IF-MAP CLIENT	15
CONFIGURING IF MAP POLICIES	17
ACTIVE FEDERATED SESSION DETAILS	20
IMPORTED SESSION DETAILS	21
EXPORTED SESSION DETAILS	21
FEDERATED SESSION DETAILS	22
TROUBLESHOOTING	22
APPENDIX	23
CLUSTERING IN A FEDERATED DEPLOYMENT	23
REPLICA IF-MAP SERVER	24
COORDINATED THREAT CONTROL IN A FEDERATED ENVIRONMENT	26
PERFORMANCE AND SCALABILITY	27
IOT ACCESS	30
IOT POLICY PROVISIONING	30
OVERVIEW	30
BENEFITS	30
DEPLOYMENTS	31
CONFIGURING IOT POLICY PROVISIONING	32
CONFIGURING IOT ACCESS POLICY	36
CONFIGURING ADDITIONAL DEVICE CATEGORY/PROFILE GROUPS	43
CONFIGURING PROFILER GROUPS	44
TROUBLESHOOTING	45

- PROVISIONING PCS SESSIONS TO PAN/CHECK POINT/FORTIGATE FIREWALL48
 - OVERVIEW.....48
 - DEPLOYMENT OF PPS/PCS USING PAN/CHECK POINT/ FORTIGATE NEXT GENERATION FIREWALL 48
 - IF-MAP CONFIGURATION49
 - STEP1: CONFIGURING IF-MAP SERVER50
 - STEP 2: CONFIGURING IF-MAP CLIENT.....52
 - STEP 3: VIEWING THE FEDERATED SESSION DETAILS.....52
 - ONE-TO-ONE NETWORK ADDRESS TRANSLATION (NAT)54
 - OVERVIEW54
 - ONE-TO-ONE NAT DEPLOYMENT54
 - CONFIGURING ONE-TO-ONE NAT54
 - REQUESTING TECHNICAL SUPPORT.....56
 - SELF-HELP ONLINE TOOLS AND RESOURCES56
 - OPENING A CASE WITH PSGSC.....56

Purpose of this Guide

This guide describes how Pulse Policy Secure (PPS) and Pulse Connect Secure (PCS) can provide end-to-end secure access with visibility, access control and compliance for remote users and devices. There are multiple use cases from having a complete visibility through Pulse Secure Profiler, to fully applying compliance checks using Host Checker (HC) and having granular access control. Depending on the requirements different approaches can be taken to control the VPN access.

Prerequisites

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

- *Pulse Policy Secure (PPS)*
- *Pulse Connect Secure (PCS)*

Use Cases

The following use cases are supported with PPS and PCS integration:

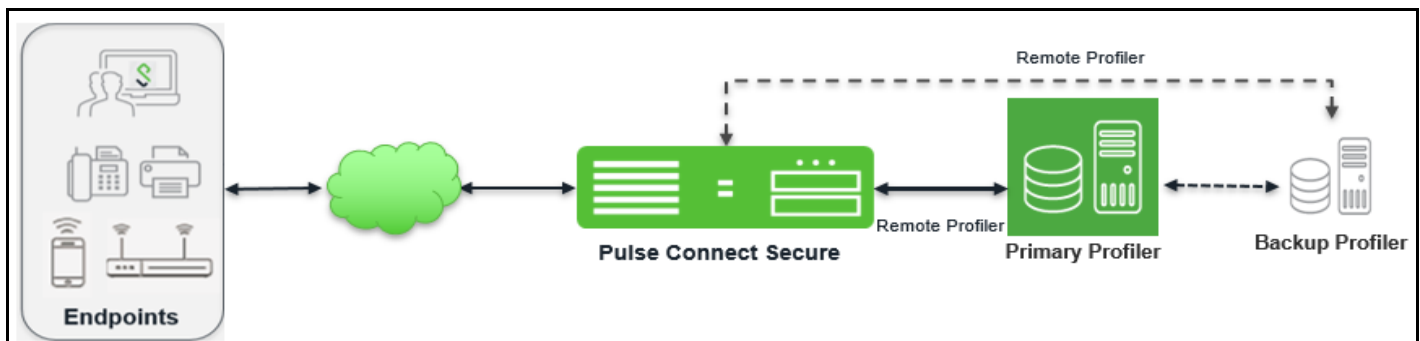
- Visibility and Enforcement with Remote Profiler- PCS needs to be configured with Remote Profiler, which will send endpoint contextual information to PPS/Profiler. PCS Sessions will be leveraged for endpoint visibility. Based on Profiler device attributes, PCS sessions can be assigned roles. Providing visibility for remote endpoints with contextual information helps to achieve overall endpoint visualization and enforcement based on endpoint attributes applied for pre and post admission control. This feature provides a single pane of glass to visualize all endpoints inside and outside the network, Remote users connecting through desktop clients can be assigned roles based on profiler attributes. Remote mobile clients can also be assigned roles based on device profiles and attributes through MDM integration (MobileIron, AirWatch, and Pulse Workspace (PWS)).
- Seamless access from remote to local with SSO functionality - Remote session can be migrated to PPS as an on-premises session, acting as a single entity to access resources with Single-sign-on capability. Whenever, end-users visit office premises, they don't have to authenticate to PPS again.
- PPS can provision access security policies by leveraging the profiler IoT discovery. This feature can be extended to other device categories.
- PCS user-identity provisioning to Palo Alto Networks and Check Point Next Generation Firewalls. Using Identity-based integration, PCS user-identity information (user-name & user-role) can be pushed to Palo Alto Networks and Check Point Next Generation firewalls so that these firewalls can employ granular level of policies at the perimeter to access protected resources.
- PCS user-identity provisioning to Juniper SRX Firewalls. Integration with Junos SRX firewalls using identity based integration so that remote users can securely access the resources behind Junos SRX firewalls.

Visibility and Enforcement with Remote Profiler

A Remote Profiler is useful in the following cases:

- Profile devices that are outside the enterprise network and connected through PCS.
- Access control of remote users based on device profile.

Figure 1 Visibility and enforcement with Remote Profiler



When user connects to a remote PCS and starts a session:

1. Information such as hostname and IP address, device IP address and MAC address, session identifier, user-agent are retrieved by the session and sent to the Profiler.
2. The Profiler uses the information to profile the devices.
3. Based on the device attributes, PCS assigns the user roles.

The following sections describe the steps to configure a Remote Profiler:

1. **Set up the Profiler:** To set up the profiler, see *Pulse Policy Secure Profiler Administration Guide*.
2. **Allow administrator access to REST APIs:** See [Allow Administrator Access to REST APIs](#).
3. **Set up backup profiler** (optional) - To set up sebackup profiler, see *Pulse Policy Secure Profiler Administration Guide*.

Allow Administrator Access to REST APIs

1. Log in to the Profiler.
2. Select **Authentication > Auth. Servers**.
3. Click on the **Administrator** link.
4. Select the **Users** tab.

5. Select the corresponding administrator user link, then select **Allow access to REST APIs** and Save Changes.

Note: REST API access to the Profiler can be enabled only for local administrators.

Figure 2 Allow Access to the Profiler

Auth Servers > Administrators > Update Administrator admin

Update Administrator admin

Full Name: Platform Administrator

Authenticate using: Administrators

Password: *****

Confirm Password: *****

Start Time: [Calendar Icon]

End Time: [Calendar Icon]

Time Zone: (GMT-08:00) Pacific Time (US & Canada), Tijuana

☐ One-time use (disable account after the next successful sign in)
☐ Allow console access
☒ Allow access to profiler using REST APIs
☒ Enabled
☐ Disabled
☐ Quarantined
☐ Require user to change password at next sign in

Note: You must also configure password management on the Authentication server Settings with Allow users to change their password option enabled. Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities.

Save Changes

Configuring Remote Profiler on PCS

Ensure you configure Remote Profiler on PCS, use the following procedure:

1. Select **Authentication > Auth. Servers**.
2. Select **Remote Profiler** from the server type drop-down list and click **New Server**.
3. Enter a name for the Authentication server.
4. Enter the FQDN name or IP address for the Remote Primary Profiler and the Backup Profiler.

Note: Do not include http:// or https:// before the IP address.

Figure 3 New Remote Profiler

Pulse Secure System Authentication Administrators Users Maintenance Wizards

Pulse Connect Secure

Auth Servers > New Remote Profiler

New Remote Profiler

Retrieved API key

*Name: Remote Profiler Label to reference this server.

*Remote Profiler: 10.96.65.125 Fully qualified domain name (FQDN) or IP address

*API Key: Get API Key ***** Auto-completed when API key is retrieved

Backup Remote Profiler: 10.204.88.35 Fully qualified domain name (FQDN) or IP address

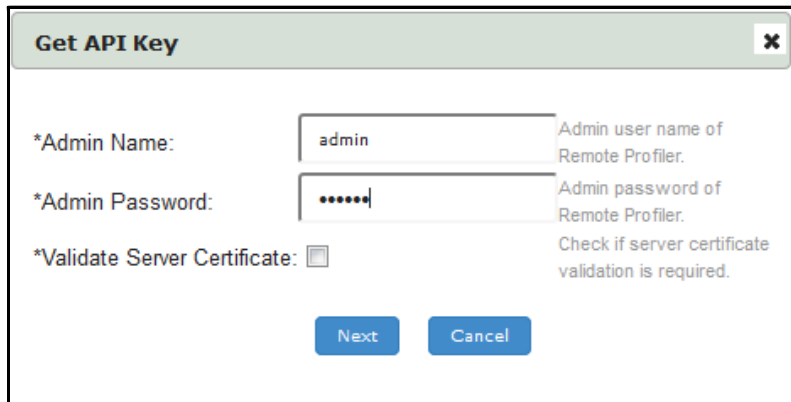
API Key: Get API Key ***** Auto-completed when API key is retrieved

Save Changes Reset

* Indicates required field

5. Click **Get API Key**. In the Get API Key window, provide the credentials of valid administrator on PPS/ Profiler server and click **Next**. The API key generates and displays in the API Key field.

Figure 4 Get API Key



The 'Get API Key' dialog box contains the following fields and controls:

- *Admin Name:** A text input field containing 'admin'. A tooltip on the right reads: 'Admin user name of Remote Profiler.'
- *Admin Password:** A password input field with masked characters. A tooltip on the right reads: 'Admin password of Remote Profiler.'
- *Validate Server Certificate:** An unchecked checkbox. A tooltip on the right reads: 'Check if server certificate validation is required.'
- Buttons:** 'Next' and 'Cancel' buttons at the bottom.

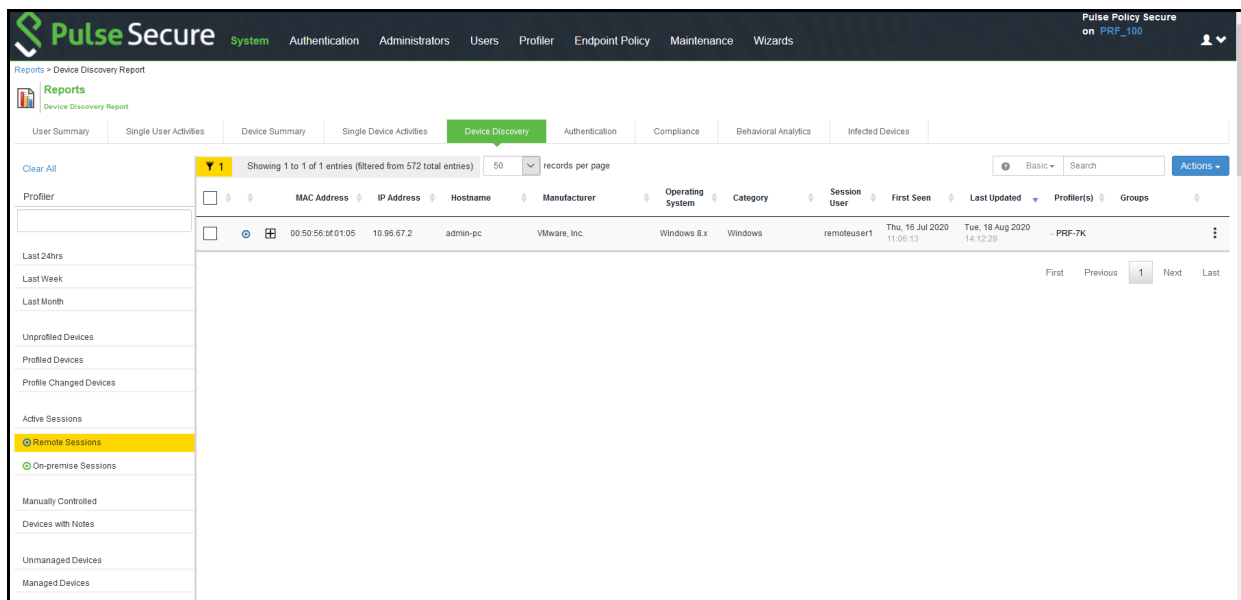
Note:

- If you already have the API key, you can enter it in the API Key field instead of clicking the **Get API Key** button.
- To enable trusted Root CA certificate validation, select the **Validate Server Certificate**.
- If trusted Root CA is not enabled, automatic role re-evaluation does not trigger on PCS when device profile changes.

6. **Save** changes.

Once created, communication is established between PCS and the Remote Profiler. You can view device profile data in the Device Discovery Report table of the Profiler.

Figure 5 Device Discovery Report table showing remote sessions



The screenshot shows the Pulse Secure interface with the 'Device Discovery Report' table. The table has the following columns: Profiler, MAC Address, IP Address, Hostname, Manufacturer, Operating System, Category, Session User, First Seen, Last Updated, Profiler(s), and Groups. The table displays one entry for a remote session.

Profiler	MAC Address	IP Address	Hostname	Manufacturer	Operating System	Category	Session User	First Seen	Last Updated	Profiler(s)	Groups
	00:50:56:0f:01:05	10.96.67.2	admin-pc	VMware, Inc.	Windows 8.x	Windows	remoteuser1	Thu, 16 Jul 2020 11:00:13	Tue, 18 Aug 2020 14:12:28	PRF-7K	

The interface also includes a left sidebar with navigation options like 'Unprofiled Devices', 'Profiled Devices', 'Active Sessions', and 'Remote Sessions' (which is highlighted). The top navigation bar includes 'System', 'Authentication', 'Administrators', 'Users', 'Profiler', 'Endpoint Policy', 'Maintenance', and 'Wizards'.

Configuring Role-Mapping Rules for Profiled Devices on PCS

After creating the Profiler, you can use device attributes from the Profiler in the role mapping rules for 802.1X realms for policy enforcement.

To configure role-mapping rules:

1. Select **Users > User Realms**.
2. Select the realm name.
3. Select the Remote Profiler as Device Attributes Server.

Figure 6 Device Attributes

The screenshot shows the Pulse Secure web interface. The top navigation bar includes 'System', 'Authentication', 'Administrators', 'Users' (highlighted), 'Maintenance', and 'Wizards'. Below this, there are tabs for 'General', 'Authentication Policy', and 'Role Mapping'. The 'General' tab is active, showing a form for configuring a user realm. The 'Name' field is set to 'Users'. The 'Description' field contains the text 'Default authentication realm for users'. There is a checkbox labeled 'When editing, start on the Role Mapping page'. Below this, there is a section titled 'Servers' with a description: 'Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.' This section contains four rows of configuration: 'Authentication' set to 'System Local', 'User Directory/Attribute' set to 'None', 'Accounting' set to 'None', and 'Device Attributes' set to 'Remote Profiler'. To the right of these dropdowns are four lines of explanatory text: 'Specify the server to use for authenticating users.', 'Specify the server to use for authorization.', 'Specify the server to use for Radius accounting.', and 'Specify the server to use for device authorization.'

4. Click the **Role Mapping** tab.
5. Click **New Rule**.
6. Set **Rule based on** to "Device Attribute" and click **Update**.
7. Enter a name for the rule (if creating a new one).
8. Create the new role mapping rules. Select the attributes based on the new device attributes that are now available in the attributes drop-down field. When setting the attribute value, make sure the value you enter is an exact match for the value displayed in the Device Discovery Report table. Wildcards (* and ?) can be used in the attribute value.

Figure 7 Creating New Role Mapping Rule

Role Mapping Rule

Rule based on: Device attribute Update

* Name:

▼ Rule: If device has any of the following attribute values...

Attribute: (Select an attribute) Attributes...

☐ is

☒ is equal to LDAP attribute IdapServer is configured as LDAP Server in Authentication Server Local Profiler.

▼ then assign

Available Roles: Guest Guest Administrator Guest Sponsor Guest Wired Users

Selected Roles: (none)

☐ Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

9. Assign the roles and click **Save Changes**.

End-to-End Zero Trust Secure Access

• Overview	8
• IF-MAP Federation Use Cases	8
• IF-MAP Configuration	13
• Active Federated Session Details	20
• Troubleshooting	22
• Appendix	23

Overview

The federation allows users to connect to a PPS or PCS appliance and then access resources that are protected by the firewall connected to different PPS without re-authentication. For example, users in large campus sites and in branch offices connect to the corporate network from campus, branch, or private home offices and access the resources distributed across locations. The federation eliminates redundant log ins and host checks and provides seamless access to protected resources. The federation uses IF-MAP protocol to share information about user sessions between PCS and PPS over the distributed network.

For more information about IF-MAP, see http://www.trustedcomputinggroup.org/wp-content/uploads/TNC_gMAP_v1_1_r5.pdf

IF-MAP Federation Use Cases

This section describes the various IF-MAP use cases. Using IF-MAP federation the users can seamlessly access with a single log in to corporate resources protected by the firewall. It provisions seamless access between the user sessions of PCS and PPS.

This section describes the following uses cases:

- “Access Control in the Federated Enterprise” on page 8
- “Session Migration across PCS and PPS using IF-MAP” on page 9

Access Control in the Federated Enterprise

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

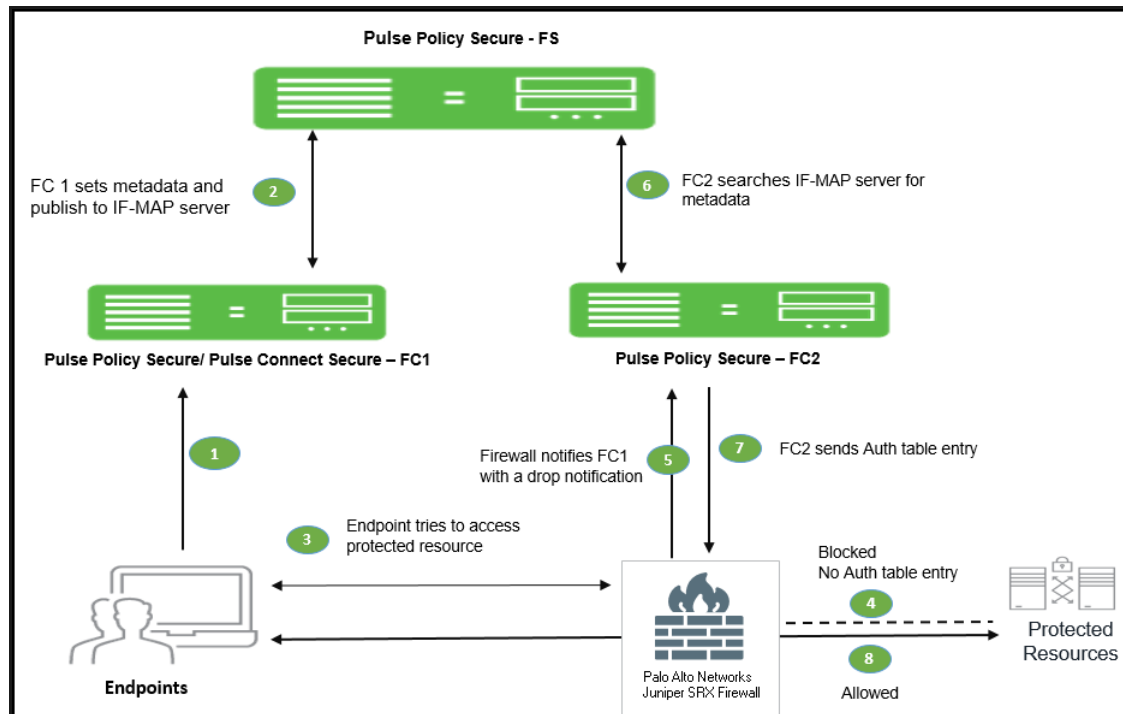
The federation requires dynamic auth table provisioning on the SRX firewall and allows access to the protected resource based on the resource access policies that are configured on PPS.

The access solution serves the following objectives:

- Ensures that the employees can access the corporate network and can access resources and data in both local and remote locations without having to specify their authentication credentials at each security policy enforcement point.

- Enhances security by enforcing role or policy based access control.

Figure 8 Access Control in the federated enterprise using IF-MAP



The session federation work flow is described below:

- The user connects to network and authenticates with PPS/PCS (FC1).
- Authentication information such as IP address, MAC address, username, and roles are published to the IF-MAP server.
- The user tries to access protected resource from the branch office.
- The firewall blocks the access.
- The firewall requests PPS (FC2) for session details such as user roles. PPS device subscribes to session information and other endpoint data based on the originating IP address.
- The federation server sends the search result based on the search request from PPS (FC2).
- PPS (FC2) send roles and policy information to the firewall.
- The firewall allows or denies traffic based on the resource access policies received from FC2.

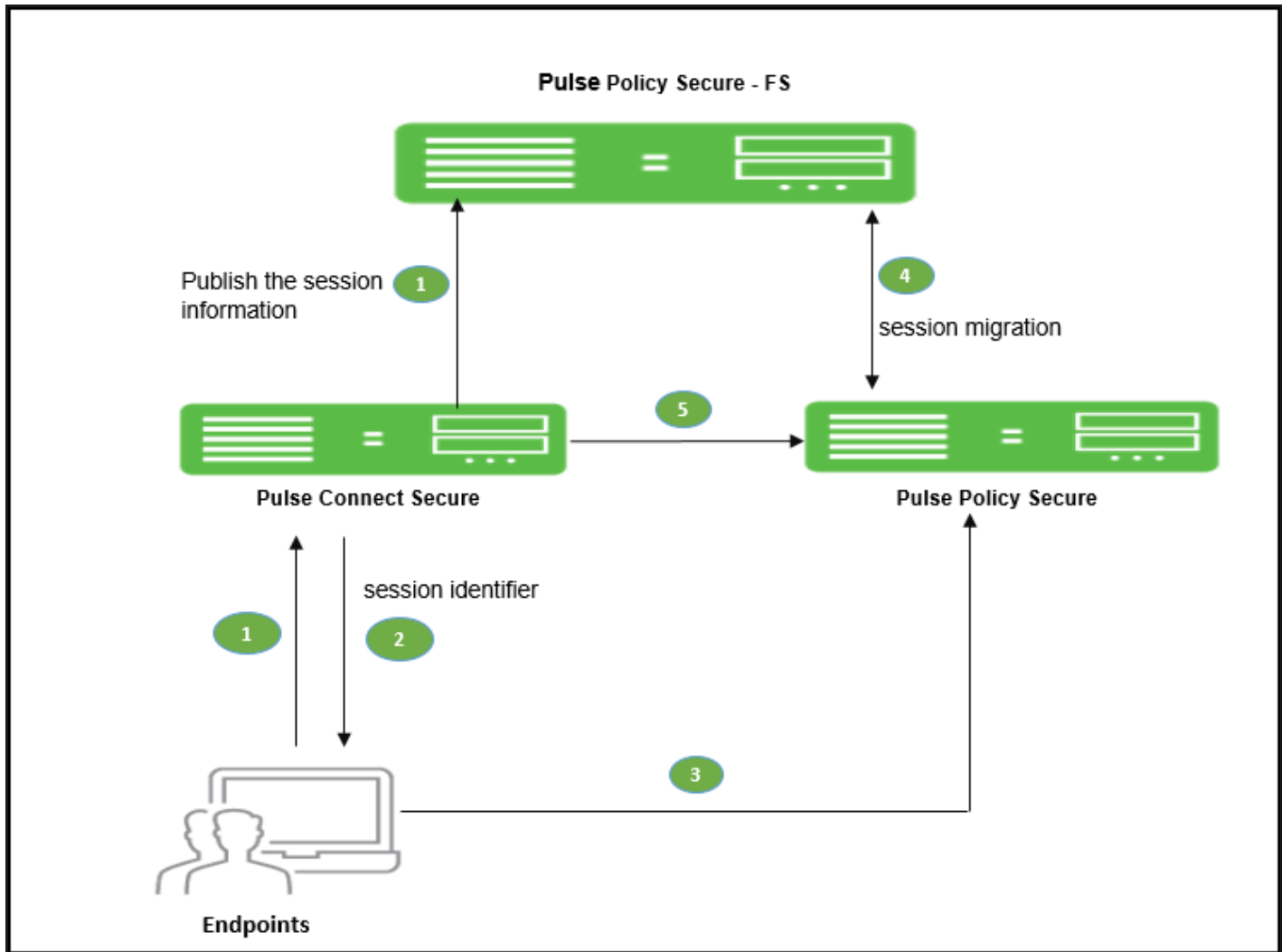
Session Migration across PCS and PPS using IF-MAP

IF-MAP federation allows seamless access to the users connected through remote access and on premise network without re-authenticating. For example, a user can connect from home through PCS and then arrive at work and connect through PPS without logging in again. The session migration also enables users to access different resources within the network that are protected by Pulse Secure devices without repeatedly providing credentials.

When a session is migrated, realm role-mapping rules determine user access capabilities. You can import user attributes when a session is migrated, or you can configure a dedicated directory server to look up attributes for migrated user sessions. To ensure that session migration retains user sessions, configure a limited access remediation role that does not require a Host Checker policy. This role is necessary because the Host Checker timeout can be exceeded if an endpoint is in hibernation or asleep. With the new remediation role, the user's session is maintained. The session migration works only with same authentication group.

If additional Host Checker policies are configured on a role or realm to which a migrated session applies, the policies are performed before allowing the user to access the role or realm. Administrators of different Pulse servers should ensure that Host Checker policies are appropriately configured for endpoint compatibility.

Figure 9 Session Migration across PCS and PPS



The session migration workflow is as follows:

1. User connects to PCS and the information is published to the federation server, which includes session identifier.
2. The session identifier information is also communicated to Pulse client.

3. When user connect to PPS in the same authentication group after arriving at office network using Pulse client.
4. The Pulse client sends session identifier to PPS.
5. PPS appliance uses the session identifier to look up the session information in the IF-MAP server and request to migrate the session from PCS to PPS.
6. PPS create a local session for the endpoint.

To permit session migration for users with the Pulse client, perform the following tasks:

1. Configure location awareness rules within a client connection set to specify locations included in the scope of session migration for users. For example, configure location awareness rules for a corporate PPS server connection and a PCS server connection.
2. Configure an IF-MAP federated network, with the applicable Pulse servers as IF-MAP Federation clients of the same IF-MAP Federation server.
3. Ensure that user entries are configured on the authentication server for each gateway.
4. Ensure that user roles are configured for all users on each gateway.
5. Define a remediation role with no Host Checker policies to allow user sessions to be maintained when an endpoint is sleeping or hibernating.
6. Configure role-mapping rules that permit users to access resources on each gateway.
7. Enable and configure session migration from the User Realms page of the admin console.
8. Distribute the Pulse client to users.

Configuring Session Migration for Pulse Client

Ensure that all of the PPS and PCS servers for which you want to enable session migration are IF-MAP Federation clients of the same IF-MAP Federation server. Additionally, make sure that each gateway is configured according to the procedures outlined in this section.

To configure session migration:

1. In the admin console, select **Users > User Realms**.
2. Select an existing realm, or create a new realm.
3. On the General page, select the **Session Migration** check box. Additional options appear.
4. In the Authentication Group box, enter a string that is common to all of the gateways
5. that provision session migration for users. The authentication group is used as an
6. identifier.
7. Select for either the **Use Attributes from IF-MAP** option button or the **Lookup Attributes using Directory Server** option.

Note: Select Lookup Attributes using Directory Server only if you are using an LDAP server. Attributes are served faster with an LDAP server.

Figure 10 Configuring Session Migration for Pulse Client

User Realms > Cert Auth > General

General | Authentication Policy | Role Mapping

* Name: Cert Auth

Description: System created authentication realm for Certificate Authentication.

☒ When editing, start on the Role Mapping page

▼ Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: Certificate Authentication ▼

User Directory/Attribute: None ▼

Accounting: None ▼

Device Attributes: None ▼

▼ Additional Authentication Server

☐ Enable additional authentication server

▼ Dynamic policy evaluation

☐ Enable dynamic policy evaluation

▼ Session Migration

☒ Session Migration

Session migration allows Pulse Secure clients to maintain a session across different Pulse Policy Secure and Pulse Connect Secure devices without requiring reauthentication.

Authentication Group: Auth_Group A string that determines which sessions may be migrated or shared

Inbound Sessions:

☒ Use Attributes from IF-MAP

☐ Lookup Attributes using Directory Server

▼ Other Settings

Authentication Policy: Certificate restrictions
Password restrictions
No Rules

Role Mapping:

[Save Changes](#)

* indicates required field

Authentication Server Support

The behavior of session migration depends to some extent on the authentication server on the inbound side.

The following list provides a summary of authentication server support:

- Local authentication server-Migration succeeds if the username is valid on the local authentication server.
- LDAP server-Migration succeeds if the LDAP authentication server can resolve the username to a distinguished name (DN).
- NIS server-Migration succeeds if the NIS authentication server can find the username on the NIS server.
- ACE server-Migration always succeeds.
- RADIUS server-Migration always succeeds. If you select Lookup Attributes using Directory Server, no attributes are present in the user context data.
- Active Directory-Migration always succeeds. The Lookup Attributes using Directory Server option may not work, depending on your configuration.
- Certificate-Migration succeeds if the certificate is valid.
- SAML-Migration always succeeds because Identity provider is external server.
- Anonymous-No support for migrating sessions because sessions are not authenticated.
- Siteminder-No support for migrating sessions because Siteminder SSO is used instead.

IF-MAP Configuration

The IF-MAP configuration involves configuring the PPS device as an IF-MAP client or an IF-MAP server. You can configure the PCS device as an IF-MAP client for an IF-MAP server. A device configured as an IF-MAP server is automatically a client of itself. An IF-MAP server can function as a fully functional PPS device and any endpoint sessions with an IP address created on an IF-MAP server are automatically published to that IF-MAP server.

This section covers the following information:

- [“Configuring IF-MAP Server” on page 13](#)
- [“Configuring IF-MAP Client” on page 15](#)
- [“Configuring IF MAP Policies” on page 17](#)

Configuring IF-MAP Server

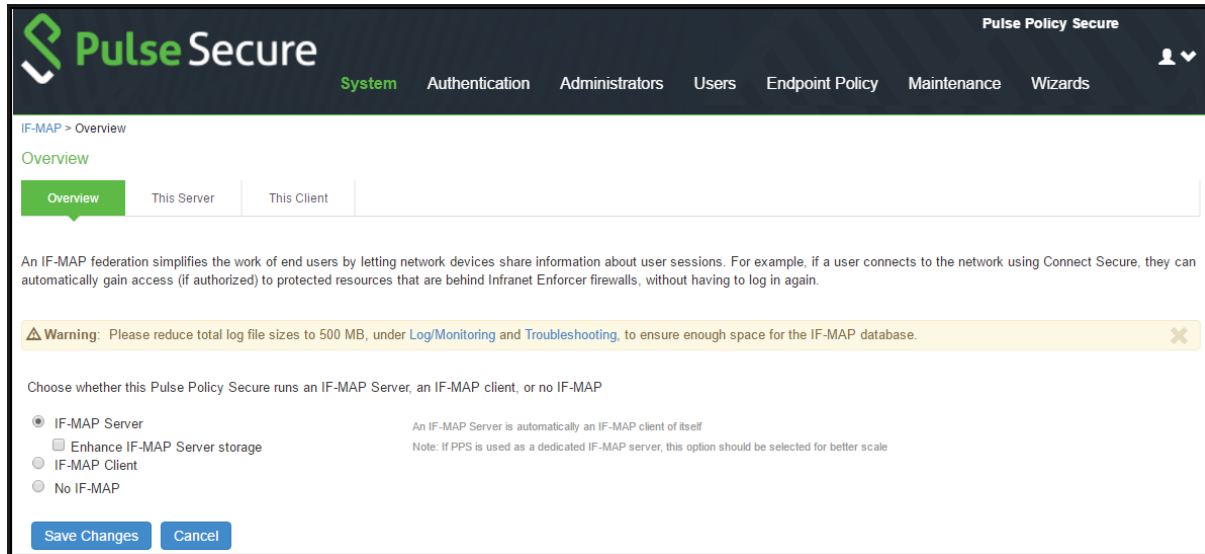
An IF-MAP server is a repository for IF-MAP clients, which is used for publishing information regarding an activity on the network. To deploy PPS as an IF-MAP server, you must configure PPS as an IF-MAP server and then add PPS/PCS as IF-MAP clients. A PPS device can be deployed as a dedicated IF-MAP server for better scale and performance. If you opt for this configuration it consumes most of the virtual memory available on appliance, which results in performance degradation of other PPS services.

Note: Currently, only Active/Passive cluster mode for IF-MAP server is supported.

To configure IF-MAP server on the PPS:

1. Select **System > IF-MAP Federation > Overview**.

Figure 11 IF-MAP Federation Overview



2. Select **IF-MAP Server** option
(Optional) Select **Enhance IF-MAP server storage** for using the appliance as a dedicated federation server for high scalability.
3. Click **Save Changes**.

Adding IF-MAP Clients

The IF-MAP client must be added for subscribing the session information on an IF-MAP server. You configure an entry for each IF-MAP client on the IF-MAP server.

To add IF-MAP client:

1. Select **System > IF-MAP Federation > This Server > Clients**.
2. Click **New IF-MAP Client**.

Figure 12 IF-MAP Client

3. Under IF-MAP Client,
 - a. Enter name and optionally a description for client.
 - b. Enter one or more IP addresses of the client.
 - If the client is connected to multiple data links on the same network or different network, then list all of its physical network interfaces.
 - If the client is a PPS cluster, then list the internal and external network interfaces of all nodes. You must enter all of the IP addresses for all of the interfaces because equipment failures may cause traffic between the IF-MAP client and the IF-MAP server to be re-routed through a different network interface. Listing all of the IP addresses maximizes the probability that IF-MAP Federation still works in the event of a failure.
4. Under Authentication, select the Client Authentication Method: **Basic** or **Certificate**.
 - a. If you select **Basic**, enter a Username and Password. The same information should be added to the IF-MAP server.
 - b. If you select **Certificate**, choose which Certificate Authority (CA) to use to verify the certificate for this client. Optionally, specify certificate attributes or restrictions to require values for certain client certificate attributes.
5. Click **Save Changes**.

Configuring IF-MAP Client

The IF-MAP client publishes the basic session information, which includes IP address, usernames, and roles. The IF-MAP server stores the information as metadata. Other IF-MAP clients in the network can poll the server for metadata information when the endpoint tries to access the protected resource. A PCS or PPS device can be deployed as an IF-MAP client. The PPS device connected to firewall is always added as an IF-MAP client. You must import the trusted root CA certificate of the federation sever device certificate issuing cert store in to IF-MAP client for secure connection. You can trust the certificate issued by CA of server's device certificate by importing the root certificate of the issuing authority.

To configure the IF-MAP client:

1. Select **System > IF-MAP Federation > Overview**.
2. Select **IF-MAP Client**.

Figure 13 IF-MAP Federation

Pulse Secure Pulse Policy Secure

System Authentication Administrators Users Endpoint Policy Maintenance Wizards

IF-MAP > 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 Infranet 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://ic/dana-ws/soap/idsifmap

✓ **Authentication**

☒ Basic

* Username:

* Password:

☐ Certificate

Save Changes Cancel

3. Enter **IF-MAP server IP address** or complete IF-MAP server URL. For IF-MAP server in cluster mode use the virtual IP address (VIP).
4. Select the Client Authentication Method: **Basic** or **Certificate**.
 - a. Select **Basic authentication**, and enter the **username** and **password**. This is the same as the information that you entered on the IF-MAP server.
 - b. Select Certificate, select the Device Certificate to use.
 1. Ensure that the certificate of the CA that signed the IF-MAP server certificate is added from the **System > Configuration > Certificates > Trusted Server CA page**.
 2. Ensure that the hostname in the IF-MAP URL on the client machine matches the hostname of the server certificate on the IF-MAP server and that the CA that signed the server certificate is configured as trusted server CA on the IF-MAP client.
5. Click **Save Changes**.

The status light on the server's IF-MAP Federation > This Server > Clients page is green when the client and server are successfully connected.

Configuring IF MAP Policies

The IF-MAP policies allows you to perform the data synchronization operations between the IF-MAP server and IF-MAP clients. This section covers the following information:

- “Session Export Policies” on page 17
- “Session Import Policies” on page 19

Session Export Policies

The session export policy specifies how to transform Pulse Secure client session data into IF-MAP standard data. It allows IF-MAP clients to translate outgoing session information into IF-MAP data and incoming IF-MAP data into session information. These translations enable sessions to be shared between PCS and PPS even if the devices sharing sessions have different role configurations.

To configure a session export policy:

1. Select **System > IF-MAP Federation > Session-Export Policies**.
2. Click **New** to create a new policy.

Figure 14 IF-MAP Session Export Policies

The screenshot displays the Pulse Secure web interface for configuring a Session Export Policy. The top navigation bar includes the Pulse Secure logo and a user profile icon. Below the navigation bar, a menu bar shows options: System, Authentication, Administrators, Users, Endpoint Policy, Maintenance, and Wizards. The main content area is titled "Policy Type: Session Export". It includes input fields for "Policy Name:" and "Policy Description:". Below these, there are two columns: "Available Roles:" and "Selected Roles:". The "Available Roles:" column lists roles: Engg, Guest, Guest Admin, OnboardRole, remed, Remediation, and Users. There are "Add ->" and "Remove" buttons between the columns. Below the role selection, there is a section titled "Policy Actions" with a checkbox "Set IF-MAP Capabilities". Under this checkbox, there are three radio button options: "Copy matching roles" (selected), "Copy ALL roles", and "Set capabilities specified below". A text box is provided for specifying capabilities. At the bottom, there is a link "View Advanced Actions" and a checkbox "Stop processing policies when this policy matches." with "Save Changes" and "Cancel" buttons.

3. Enter a policy name and, optionally, a description.

4. Select role and add if the policy needs to be applied to selected roles only, otherwise by default is to apply policy for all roles.
5. Under Policy Actions, select **Set IF-MAP Capabilities** and select the applicable option:
 - **Copy Matching Roles**-Copies all of the user roles that match the roles specified in the Roles section of this policy into the IF-MAP capabilities data.
 - **Copy all Roles**-Copies all of the roles from the user session to the IF-MAP capabilities data.
 - **Set capabilities specified below**-Enter capabilities, one per line.

To configure advanced options:

1. Select the **View Advanced Actions** link to display additional options.
2. Select **Set IF-MAP Identity** and configure identity settings:
 - **Identity Type** -Select an element used to specify identity. Options include aik-name, distinguished-name, dns-name, email-address, kerberos-principal, trusted-platform-model, username, sip-uri, tel-uri, and other. For example, for a regular employee named Bob Smith you can select username as the Identity Type and enter the Identity as username bsmith.
 - **Identity**-Identity is normally specified as <NAME>, which assigns the user's log in name. Any combination of literal text and context variables may be specified. If you select other for Identity Type, enter a unique Identity Type in the text box.
 - **Administrative Domain**-This optional information is applied to identity and MAC address data. One example for using this field is in a large network environment with several domains in which a username could be duplicated. By supplying the domain, you ensure that the correct user is identified.
 - **Other**-This field is provided for advanced use cases when none of the predefined options are applicable.
3. Select **Set IF-MAP Roles** and select the applicable option:
 - **Copy Matching Roles**-Copies all of the user roles that match the roles specified in the Roles section of this policy into the IF-MAP capabilities data.
 - **Copy all Roles**-Copies all of the roles from the user session to the IF-MAP capabilities data.
 - **Set capabilities specified below**-Enter capabilities, one per line.
4. Select **Set IF-MAP Device Attributes**. Device attributes represent a passed Host Checker policy on PPPSPS or PCS. Select the applicable option:
 - **Copy Host Checker policy names**-The name of each Host Checker policy that passed for the session is copied to a device attribute.
 - **Set Device Attributes**-Enter device attributes, one per line.
5. Select **Stop processing policies when this policy matches** to specify that when this policy is matched, no more Session-Export policies should be applied.
6. Select **Save Changes** or continue to configure advanced actions.

Session Import Policies

The session import policies specify how the device derives a username and a set of roles based on IF-MAP data that it receives from the IF-MAP server. The import policies are similar to role mapping rules on a realm. You must be precise when you configure Import policies, otherwise roles cannot be assigned properly.

To configure session-import policies:

1. Select **System > IF-MAP > Session-Import Policies**.
2. Click **New** to create a new policy.

Figure 15 IF-MAP Session Import Policies

The screenshot shows the Pulse Secure web interface for configuring a Session-Import Policy. The breadcrumb trail is: IF-MAP > This Client > IF-MAP session import policies > Session-Import Policy. The page title is 'Session-Import Policy'. The 'Policy Type' is set to 'Session Import'. There are input fields for 'Policy Name' and 'Policy Description'. Under 'Conditions when Policy Applies', the 'Match IF-MAP Capabilities' checkbox is selected. A note states: 'Makes this policy apply only when a federation-wide session has particular capabilities. IF-MAP capabilities are similar to Pulse Policy Secure roles'. A link 'View Advanced Conditions' is available. Under 'Assign these roles', the 'Copy IF-MAP Capabilities' checkbox is checked, and the 'All capabilities' radio button is selected. There is an empty text input field for specifying capabilities. A link 'View Advanced Assignment Option' is present. At the bottom, the 'Stop processing policies when this policy matches' checkbox is unchecked, and there are 'Save Changes' and 'Cancel' buttons.

3. Type a policy name and, optionally, a description.
4. Under Conditions when Policy Applies, select **Match IF-MAP Capabilities**.
You can use the wildcard characters * and % to match IF-MAP capabilities.
5. Enter IF-MAP capabilities exactly as they appear in the corresponding session-export policy. For example, if you assigned the value “engineering” to an IF-MAP capability in the session-export policy, enter “engineering” here.
6. Under “Assign these roles,” select **Use these roles** and select the roles for which the policy applies.
7. Alternatively, select **Copy IF-MAP Capabilities**. If you select this check box, IF-MAP session capabilities on the IF-MAP server are converted to PPS roles with the same name. You can use this option if PPS roles and IF-MAP capabilities have the same name. This option is typically not required for PPS deployments.

8. Select **Stop processing policies** when this policy matches to specify that when this policy is matched, no more Session-Export policies should be applied.
9. Select **Save Changes**, or continue to configure Advanced Conditions.

You can configure advanced options that would further require that Identity, Role, or Device Attributes in the IF-MAP data for a session must match before applying the role matching. The advanced options are not required for most PPS IF-MAP deployments.

To configure advanced options:

1. Select the **View Advanced Conditions** link to additional options.
2. Select one or more of the following check boxes to specify which IF-MAP criteria to use for assigning roles:

You can use the wildcard characters * and % to match IF-MAP capabilities.

- If you select **Match IF-MAP Identity**, complete the following settings:
 - **Identity Type**-Select an element used to specify identity. Options include aik-name, distinguished-name, dns-name, email-address, kerberos-principal, trusted-platform-model, username, sip-uri, tel-uri, and other. For example, for a regular employee named Bob Smith you can select username as the Identity Type and enter the Identity as username bsmith.
 - **Identity**-Identity is normally specified as <NAME>, which assigns the user's log in name. Any combination of literal text and context variables may be specified. If you select other for Identity Type, enter a unique Identity Type in the text box.
 - **Administrative Domain**-This optional information is applied to identity and MAC address data. One example for using this field is in a large network environment with several domains in which a username could be duplicated. By supplying the domain, you ensure that the correct user is identified.
 - **Other**-This field is provided for advanced use cases when none of the predefined options are applicable.
 - **Match IF-MAP Roles**-Enter individual roles in the provided text box.
 - **Match IF-MAP Device Attributes**-Enter individual device attributes in the provided text box.
3. Click **Save Changes**.

Active Federated Session Details

The federated session details of all the active users can be viewed on both the IF-MAP client and the IF-MAP server.

This section covers the following information:

- [“Imported Session Details” on page 21](#)
- [“Exported Session Details” on page 21](#)
- [“Federated Session Details” on page 22](#)

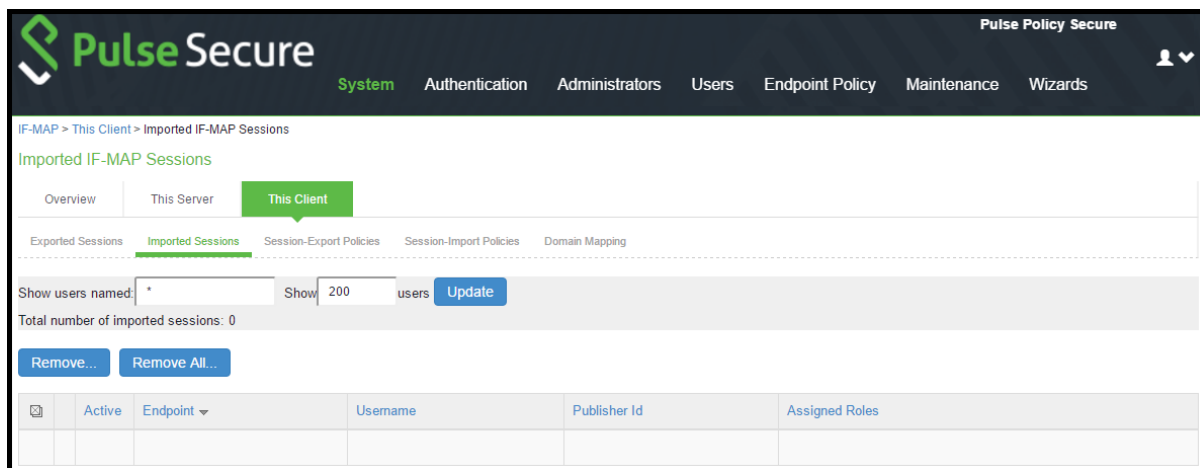
Imported Session Details

The session details from PPS, which are provisioned to SRX firewall can be viewed on an IF-MAP client.

To view, remove, or remove all the current sessions on an IF-MAP client:

1. Select **System > IF-MAP Federation > This Client**.
2. Select **Imported Sessions**.

Figure 16 Imported Sessions



3. Select **Remove** or **Remove All** to remove the imported federated session(s) from the device and the associated authentication table entries.

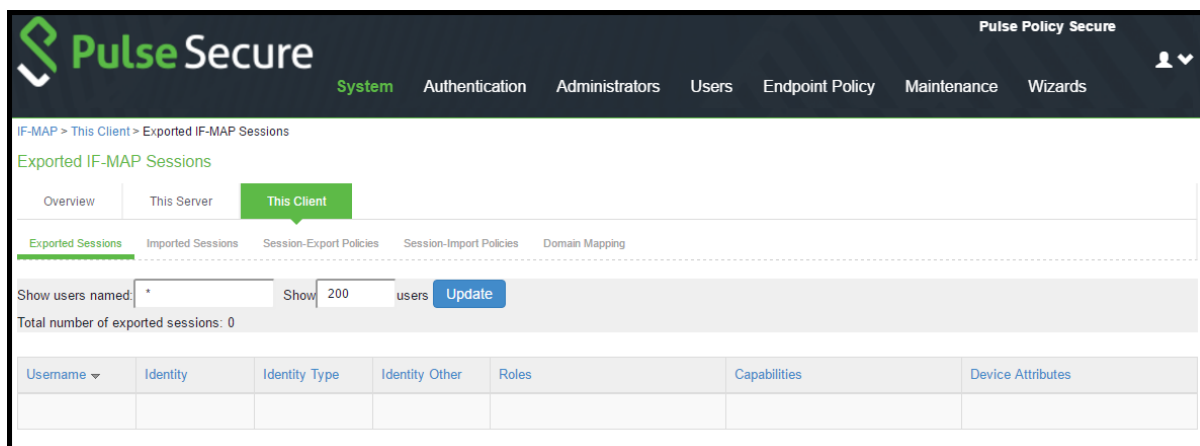
Exported Session Details

On an IF-MAP client, you can view all sessions from other PPS appliances that are currently published to firewall.

To view the exported sessions:

1. Select **System > IF-MAP Federation > This Client**.
2. Select **Exported Sessions**.

Figure 17 Exported Sessions



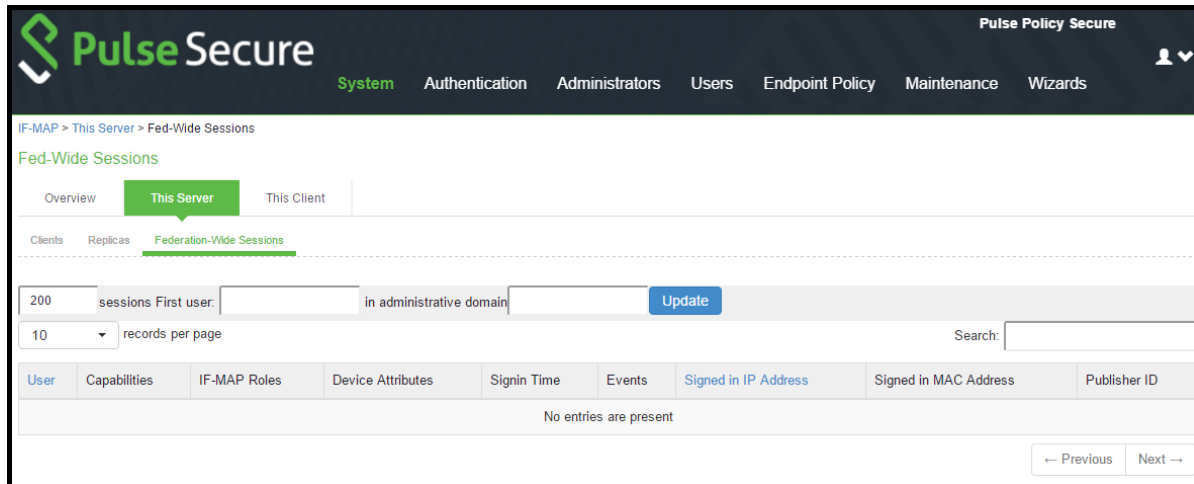
Federated Session Details

The federated sessions published to the server can be viewed on an IF-MAP server. The IF-MAP server purges sessions about 3.5 minutes after the client disconnects. The exceptions are if the server is currently involved in a purge or immediately after the server starts. It takes several minutes to scan the database before a purge can begin.

To view details about users and their sessions, and perform detailed searches:

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

Figure 18 IF-MAP Fed Wise Sessions



2. Enter users and administrative domain and click Update to search for specific session information.
3. Sort users on the page by selecting User or Signed in IP Address.

Note: The maximum number of session entries displayed in the Federation-Wide Sessions table or returned by the query to the table is 5,000 entries.

Note: You can also view IF-MAP session-export details by selecting the IF-MAP check box at Troubleshooting > User Sessions > Policy Tracing in the admin console.

Troubleshooting

The following diagnostic tools on PPS can assist you in troubleshooting the federated network:

- **IF-MAP Client User Messages**-On the IF-MAP client, logs information that is published to and removed from the IF-MAP server. Enable IF-MAP Client User Messages by selecting Log/Monitoring > User Access > Settings on the PPS IF-MAP client.
- **IF-MAP Server Trace**-On the IF-MAP server, logs the XML for all IF-MAP requests and responses. Enable the IF-MAP Server Trace by selecting Log/Monitoring > Events > Settings on the IF-MAP server. IF-MAP Server Trace should only be enabled for troubleshooting purposes, because running this diagnostic incurs a large performance impact.
- **Debuglog** - Select Troubleshooting > Monitoring > Debug Log, use event code dsfederate for debugging logs.

The admin logs help to debug the configuration issues. Ensure that the server root CA certificate is imported to avoid configuration issues.

If the IF-MAP server loses the connectivity due to hard failures and reconnects back within 3 minutes, then the access to protected resources is not affected. If the connection is lost for more than 3 minutes the access to protected resource is suspended till the users tries to access the resource.

Appendix

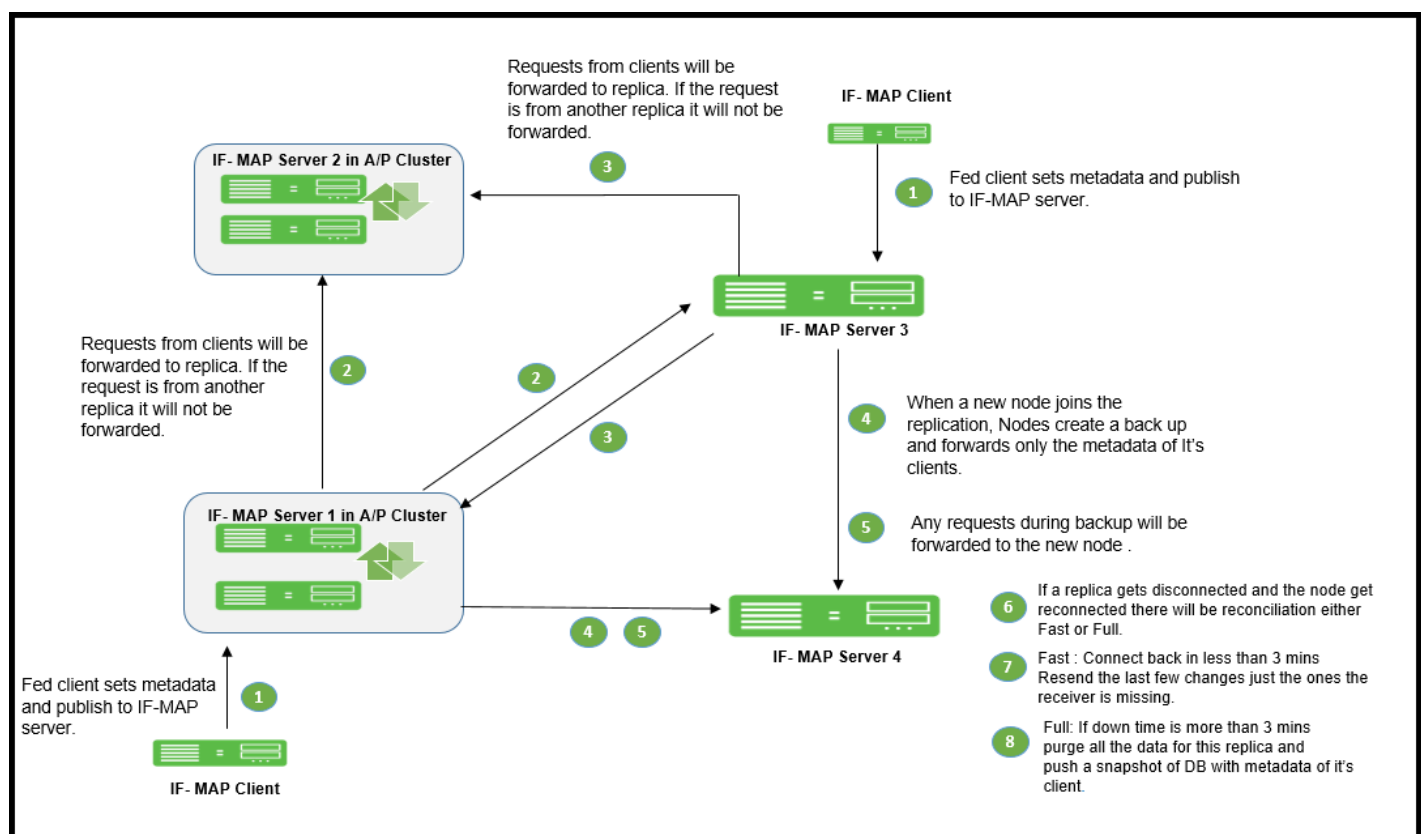
Clustering in a Federated Deployment

You can deploy clustered PPS appliance as IF-MAP servers or IF-MAP clients. You can configure IF-MAP servers in an Active Passive cluster. IF-MAP clients must be configured with the cluster's virtual IP (VIP) and must communicate with only the active node.

The session changes in federation cluster networks are propagated rapidly. The clients can access resources without experiencing delays, and there is no single point of failure. If any single device fails, the passive node recovers in seconds. You can configure IF-MAP client in Active/Active or Active/Passive cluster.

You can also use clustered PPS appliances as server replicas. [Figure 19](#) illustrates a complex network of clustered and standalone PPS appliance.

Figure 19 IF-MAP Server Clustering



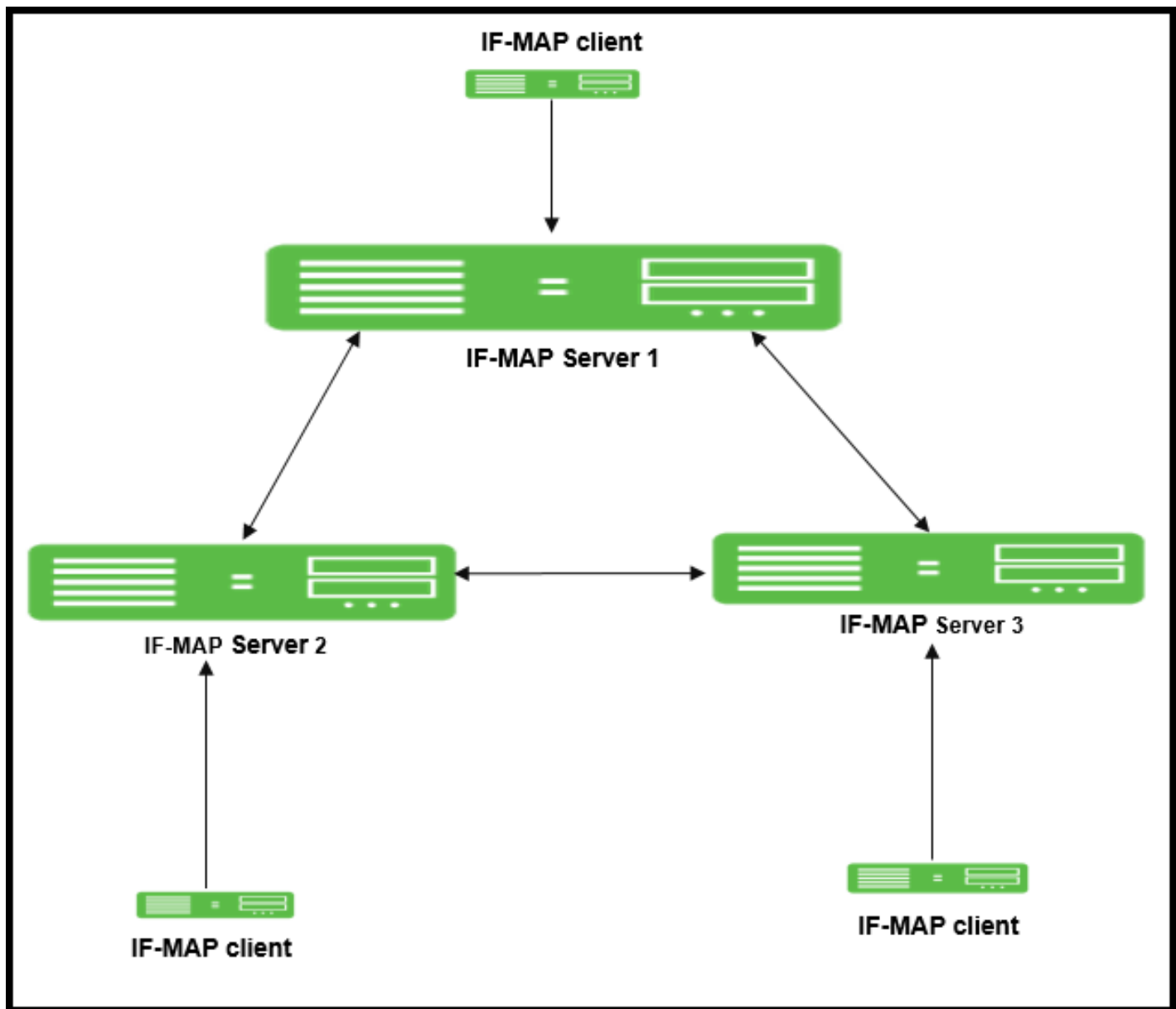
Replica IF-MAP Server

The IF-MAP server has the capability to replicate all of its IF-MAP data to other IF-MAP servers. For example, if you have a network in Boston and a network in London, you can run IF-MAP servers in both places and configure the IF-MAP servers in both locations to replicate data to one another. An endpoint that accesses PPS or PCS can access protected resources behind any of the PPS devices connected to local or replica IF-MAP server.

Each replica IF-MAP server communicates in a bidirectional way with all the connected IF-MAP server replicas. The data on each IF-MAP server is available on every server and enhances the system performance. A 3-way replica in mesh topology in which all the servers are connected to each other is supported.

Figure 20 depicts one possible deployment replica scenario.

Figure 20 IF-MAP Server Replica



Bandwidth issues determine the effectiveness of the entire IF-MAP Federation's operation. A key to timeliness is that IF-MAP servers should generally be placed geographically close to IF-MAP clients to ensure the most efficient operation. Replicas in an IF-MAP federated network allow user session data to be shared over greater distance. For example, the user in Boston can connect with servers in London through the replicated IF-MAP server in London.

To configure IF-MAP server replicas to communicate:

1. Select **System > IF-MAP Federation > This Server**.
2. Click the **Replicas** tab and then select **New IF-MAP replica to configure Replica settings**.

Figure 21 IF-MAP Server Replica

3. Type a Name for the replica IF-MAP server.
4. (Optional) Enter a Description for the replica or replica network.
5. For **Hostname**, enter the hostname that exactly matches the replica's device certificate. This is used when this IF-MAP server initiates a connection to the replica. Use the fully qualified domain name (FQDN) of the replica's internal or external interface should be used; for a cluster, use the FQDN of the internal or external VIP.
6. After **IP addresses**, provide one or more IP addresses from which the replica can initiate connections to this server. If the replica is standalone, for survivability list both the internal and external network interfaces. If the replica is a cluster, for survivability list the internal and external network interfaces of both cluster nodes.
7. Select the Authentication method: **Basic** or **Certificate**.
8. For **Basic**, enter a username and password.
9. For **Certificate**, select the CA that issued the IF-MAP replica's certificate. Enter restrictions, one per line. If any restrictions match, (for example CN=ic.example.com), the certificate is accepted.
10. Click **Save Changes** to create the connection for the replica.

Coordinated Threat Control in a Federated Environment

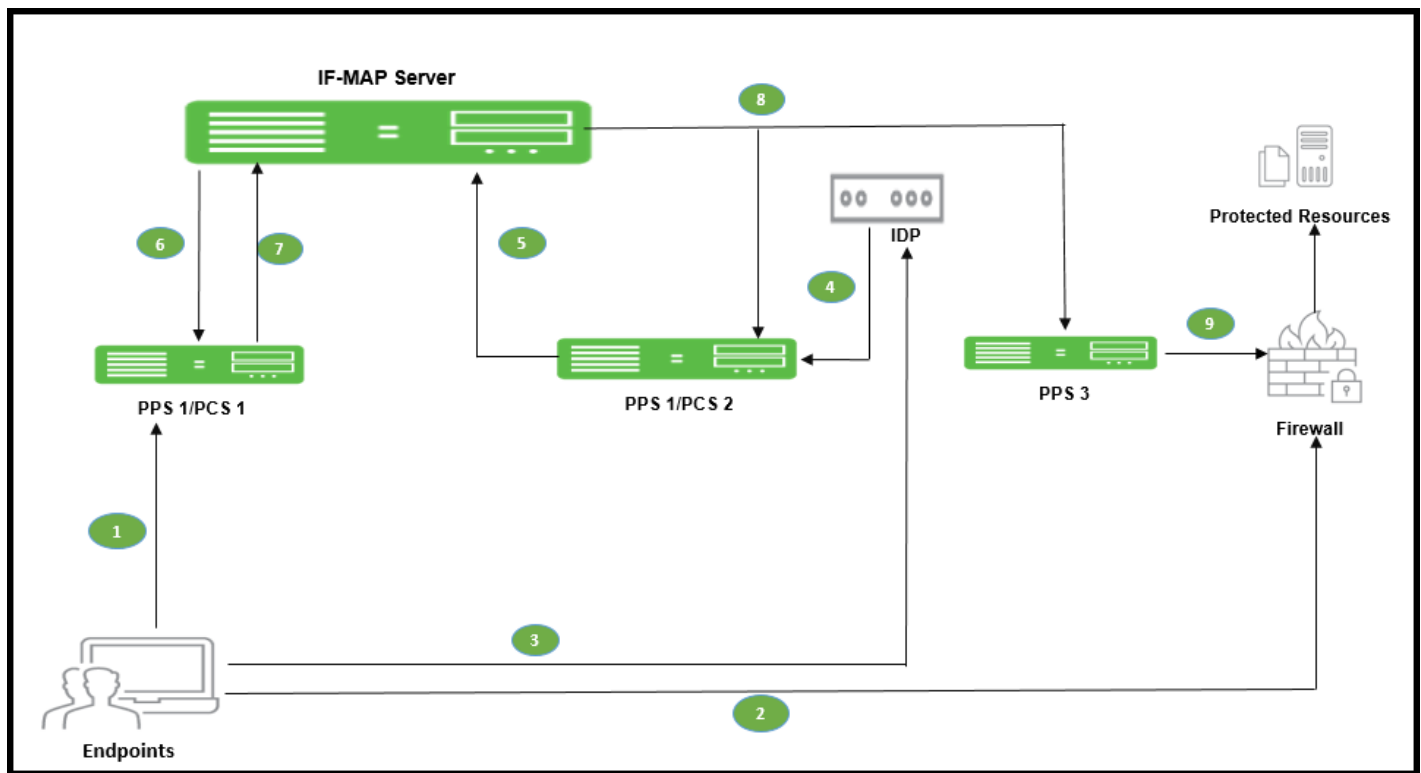
You can use Juniper Networks IDP Series Intrusion Detection and Prevention Appliance with Federation to detect attacks from within the network. Any endpoint that is on any connected PPS device or PCS can be monitored for suspicious activity. IF-MAP clients can work together to provide coordinated threat control across all attached enforcement points.

Endpoints that access PCS can be monitored by standalone IDP. Endpoints that access PPS device can be monitored by either standalone IDP, Integrated Security Gateway Intrusion Detection and Prevention ISG-IDP, or SRX Series Services Gateway IDP.

The IDP device reports attacks to the PPS or PCS to which it is connected. The PPS or PCS configured as an IF-MAP client reports the user's activity to the IF-MAP server using IF-MAP. The IF-MAP server notifies the authenticating PPS or PCS about the attack, and the authenticating device applies its IDP sensor policies. If new roles or restrictions are imposed on the endpoint based on policies configured on the device, the PPS or PCS publishes the new session information for the endpoint to the IF-MAP server.

When any other PPS or PCS polls the IF-MAP server, the newly published session information for the user determines the protected resources that the user can access. [Figure 22](#) shows a deployment with IDP.

Figure 22 IF-MAP with IDP



The following steps summarize the interaction with IDP in an IF-MAP federated network.

1. The endpoint successfully accesses PPS or PCS 1 and publishes session data to the IF-MAP server through Session-Export policies.
2. The endpoint attempts to access protected resources behind the SRX firewall, which is connected to PPS 3. PPS 3 uses IF-MAP to query the IF-MAP server for session information about the endpoint. After receiving session information, PPS 3 uses Session-Import policies to determine roles and then provisions an auth table entry on the SRX firewall. PPS 3 subscribes to updates about the endpoint's session data.
3. After the endpoint is successfully connected to resources behind the SRX firewall, IDP detects an attack originating from the endpoint.
4. IDP notifies PPS 2 of the attack. (If IDP is standalone IDP, PPS 2 could also be an PCS. If IDP is an SRX firewall with the ISG-IDP security module, PPS 2 cannot be a PCS, because the PCS does not communicate with the SRX firewall.)
5. PPS 2 updates the endpoint session data on the IF-MAP server with information about the attack.
6. The IF-MAP server notifies PPS or PCS 1 (the original authenticating device) about the attack. The authenticating PPS or PCS is responsible for consuming the attack.
7. The authenticating PPS or PCS applies its sensor policies to the endpoint and updates the endpoint's session according to actions specified in the sensor policies. For example, the endpoint must be assigned a more restrictive role. The PPS or PCS publishes the new session information to the IF-MAP server, and the new information replaces the old data.
8. The IF-MAP server notifies any PPS that subscribe to updates about the endpoint. This includes PPS 3, which is connected to the SRX firewall.
9. PPS 3 applies Session-Import policies to the new session data for the endpoint and pushes the resulting roles to the SRX firewall.
10. If the new set of roles denies access to the protected resources, access is denied.

Performance and Scalability

The IF-MAP server is supported on both hardware and virtual platforms.

The scalability of the IF-MAP server depends on:

- Type of platform- Hardware or VM image
- If the IF-MAP server is used as a dedicated IF-MAP server and the virtual memory available. You must configure PPS as dedicated only when you want it to be fully used as an IF-MAP server and not for other processes such as authentication.
- Number of roles and attributes
- For example, PSA 7000 has no impact of dedicated IF-MAP server setting option due to kernel memory limit of process. With single role for session, scale limit is up to 300K fed-wide sessions.
- PSA5000/SM360/PSA3000, the scale limit is 150K fed-wide session on dedicated IF-MAP appliance.
- For virtual platform (VM image), scalability is limited and based on the size of virtual memory.

The performance on IF-MAP server is described below:

- The IF-MAP server supports 24 export/import requests together per second.
- The time interval required to access the resource protected by the firewall after the user log in is 20 seconds.
- Latency and bandwidth between IF-MAP replicas affect the amount of time taken to replicate large amounts of data during heavy IF-MAP server utilization.
- The IF-MAP federation replica is supported over transatlantic link, however we might face issues due to WAN connection and latency between the devices.
- For clustering or replication, there is no impact on the scalability.

IoT Access

• IoT Policy Provisioning	30
• Troubleshooting	45

IoT Policy Provisioning

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

- [“Overview” on page 30](#)
- [“Deployments” on page 31](#)
- [“Configuring IoT Policy Provisioning” on page 32](#)

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:

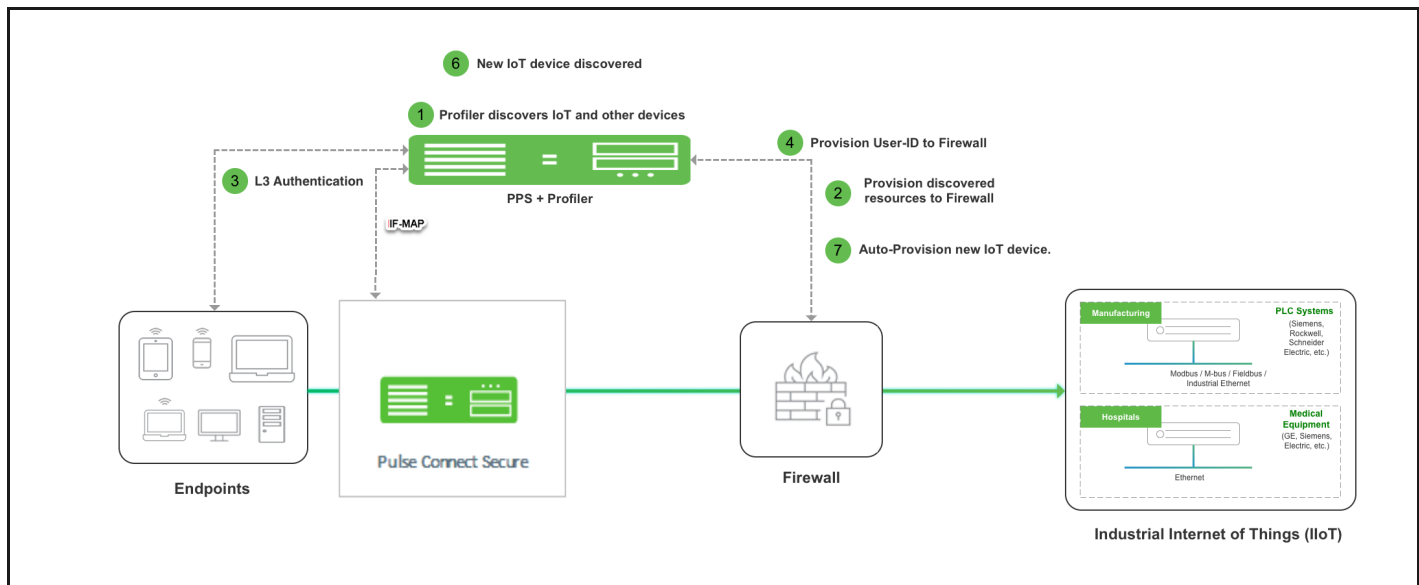
- Discover and profile IoT devices using Profiler. Profiler enables you to continuously monitor the network and discover new devices such as security cameras, sensors, Industrial IoT devices (IIoT), medical sensors, and so on.
- PPS provides IoT access control using the IoT Access Policies, which are 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 SRX/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.

When a contractor would like to access IoT or IIoT device for troubleshooting or maintenance purpose, they can access IoT device from anywhere (remote or local). PCS can share session information with PPS and PPS can enforce firewall policies based on role-based access for specific contractor to access specific IoT/IIoT machine.

Figure 23 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. Authorised users (based on roles) are allowed to access IoT devices. Access to IoT devices by unauthorised 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 SRX/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” on page 44.](#)

Configuring IoT Policy Provisioning

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

- [“Basic Configurations” on page 32](#)
- [“Configuring IoT Access Policy” on page 36](#)
- [“Configuring Additional Device Category/Profile Groups” on page 43](#)

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.

Step 1: Configure Profiler

Step 2: Configure SRX/PAN Enforcer

Step 3: [“Configuring IoT Access Policy” on page 36](#)

Step 3.1: [“Viewing Devices in Enforcer Policy Report” on page 36](#)

Step 3.2: [“Configuring IoT Access Policy using Juniper SRX Firewall” on page 37](#)

Step 4: Configuring Additional Device Category/Profile Groups

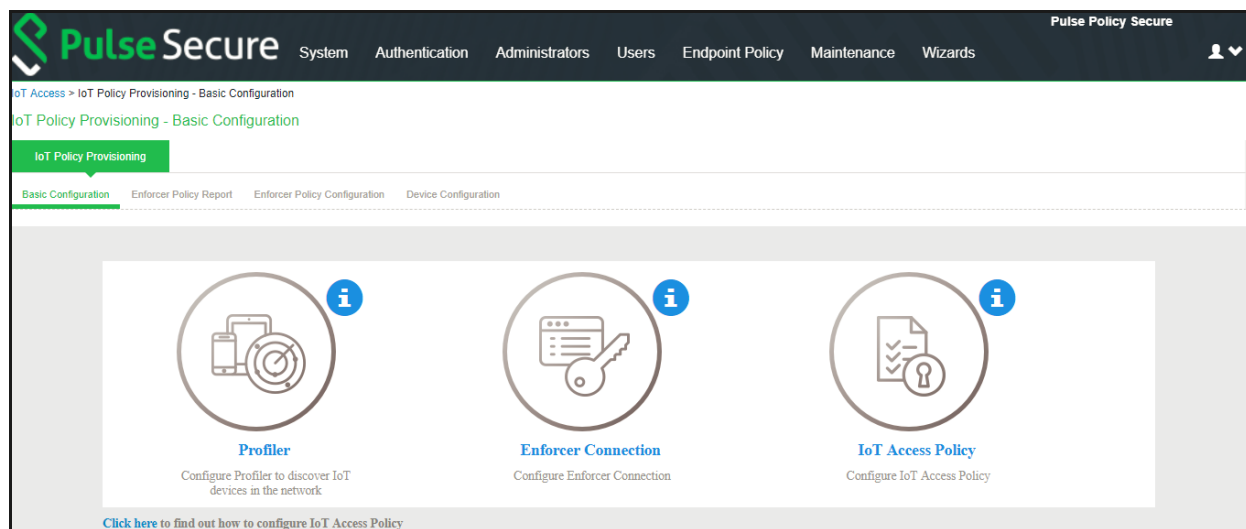
Basic Configurations

- 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 24 Policy Provisioning- Basic Configurations



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 has to be configured.

Figure 25 Profiler Settings

Pulse Secure System **Authentication** Administrators Users Endpoint Policy Maintenance Wizards

Auth Servers > Profiler > Settings

Settings

Name: Profiler Label to reference this server.

Fingerprint Database file

No file chosen. [Browse](#) [Upload and Save](#)

Last uploaded version: 32 | Last imported on: Thu Jun 14 12:14:00 2018

General Settings

• Poll Interval: 60 Minutes. Specify the interval to check Switch for connected endpoints. Default=60 minimum=5. To discover devices, configure one or more switches under [Network Infrastructure Device](#).

• DHCP Sniffing mode: DHCP Helper (internal port) Select an option based on your DHCP forward mode.

Device Sponsoring

Select device categories that will trigger an email to the admin for approval. Create a role-mapping rule based on 'status' attribute to assign the device to the respective role before and after approval.

Note: Devices can be approved or unapproved from the [Device Discovery Report](#).

☐ BSD ☐ Datacenter appliance ☐ Gaming Consoles ☐ Home Audio/Video Equipment ☐ Internet of Things (IoT)
☐ Linux ☐ Macintosh ☐ Medical Device ☐ Monitoring Devices ☐ Network Boot Agents
☐ Other OS ☐ Physical Security ☐ Point of Sale devices ☐ Printers/Scanners ☐ Projectors
☐ Routers and APs ☐ Smartphones/PDAs/Tablets ☐ Storage Devices ☐ Switches ☐ Thin Clients
☐ Video Conferencing ☐ VoIP Phones/Adapters ☐ Windows

Approver's email address to send notifications. Multiple addresses can be separated by a semicolon(,).

SMTP server configuration is required for sending emails. Currently SMTP server is not enabled. [Click here to configure](#).

• URL for Device Discovery Report.

I will appear in the notification email as a link for quick access to the devices that need approval. Profiler hostname or IP address is needed to complete the URL.

[https://10.204.88.124/dana-admin/reporting/report_device_discovery.cgi](#)

Endpoints to scan using NMAP/WMI/SSH

Once devices are discovered using DHCP, SNMP or other mechanisms, more granular profiling is done only for those devices using NMAP, WMI and SSH active scan. Use the following subnet configuration to either allow, or disallow, such scans. Maximum 100 subnets.

Subnet	Include/Exclude	Collector	
	<input checked="" type="radio"/> Include <input type="radio"/> Exclude	<input checked="" type="checkbox"/> NMAP <input type="checkbox"/> WMI <input type="checkbox"/> SSH	Add

Subnets should be in valid CIDR format or individual IP or IP Range.

Example Subnets:
Valid CIDR Format:
192.168.1.0/24
10.200.0.0/16
IP or IP Range:
10.10.10.10
10.10.10.10-100
10.10.1.1-10.10.3.200

WMI Profiling

• ☒ Configure WMI credentials. • ☐ Use Active Directory server credentials.

*User: admin1 User or domain\user or user@domain.com for endpoints.

*Password: *****

[Test Credentials](#)

Endpoint IP or hostname on which credentials can be tested

SSH Profiling

Authentication Method: Public key

*User: RSA key owner

*Private key: RSA private key

passphrase: Passphrase used for generating key

[Test Credentials](#)

Endpoint IP or hostname on which credentials can be tested

MDM Server

MDM server: Specify an MDM server that the Profiler may contact to collect additional endpoint attributes

[Save Changes](#) [Reset](#)

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

Figure 26 SRX Enforcer

Pulse Secure System Authentication Administrators Users **Endpoint Policy** Maintenance Wizards Pulse Policy Secure on N1

Intranet Enforcer > Connection > SRX

SRX

Connection

▼ Intranet Enforcer

Platform: JUNOS SRX Platform of this Intranet Enforcer.

* Name: SRX Label to reference this Intranet Enforcer.

* Password: ***** Connection password.

* Serial number(s): CF1314AK0016 One per line.

Location Group: - No 802.1X - To manage groups, see the [Location Group](#)

▼ Coordinated Threat Control

Note that not all enforcer versions and platforms have an IDP module.

☐ Use IDP Module as Sensor

Save Changes

* indicates required field

Figure 27 PAN Enforcer

Pulse Secure System Authentication Administrators Users **Endpoint Policy** Maintenance Wizards Pulse Policy Secure

Intranet Enforcer > Connection > pan

pan

Connection

▼ Intranet Enforcer

Platform: Palo Alto Networks Firewall Platform of this Intranet Enforcer.

* Name: pan Label to reference this Intranet Enforcer.

* IP Address: 192.168.1.1 IP Address of this Intranet Enforcer

* API Key: [masked] Auto-completed when you retrieve the API Key

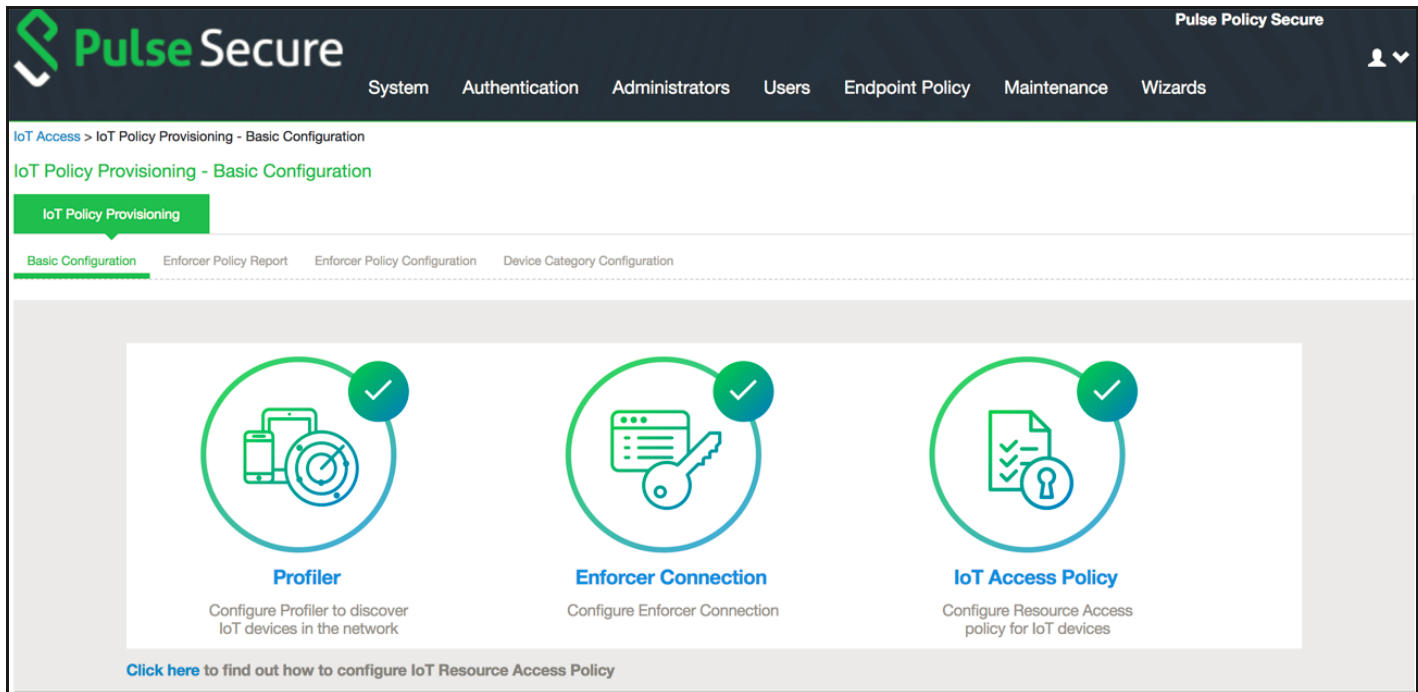
Get API Key

Server Certificate Validation: ☐ Enable this option to verify the firewall's certificate

Save Changes

Once the configuration is complete and successful, the Administrator can see the configuration status as shown in [Figure 28](#).

Figure 28 Basic Configuration



Configuring IoT Access Policy

- "Viewing Devices in Enforcer Policy Report" on page 36
- "Configuring IoT Access Policy using Juniper SRX Firewall" on page 37
- "Configuring IoT Access Policy using Palo Alto Networks Firewall" on page 40

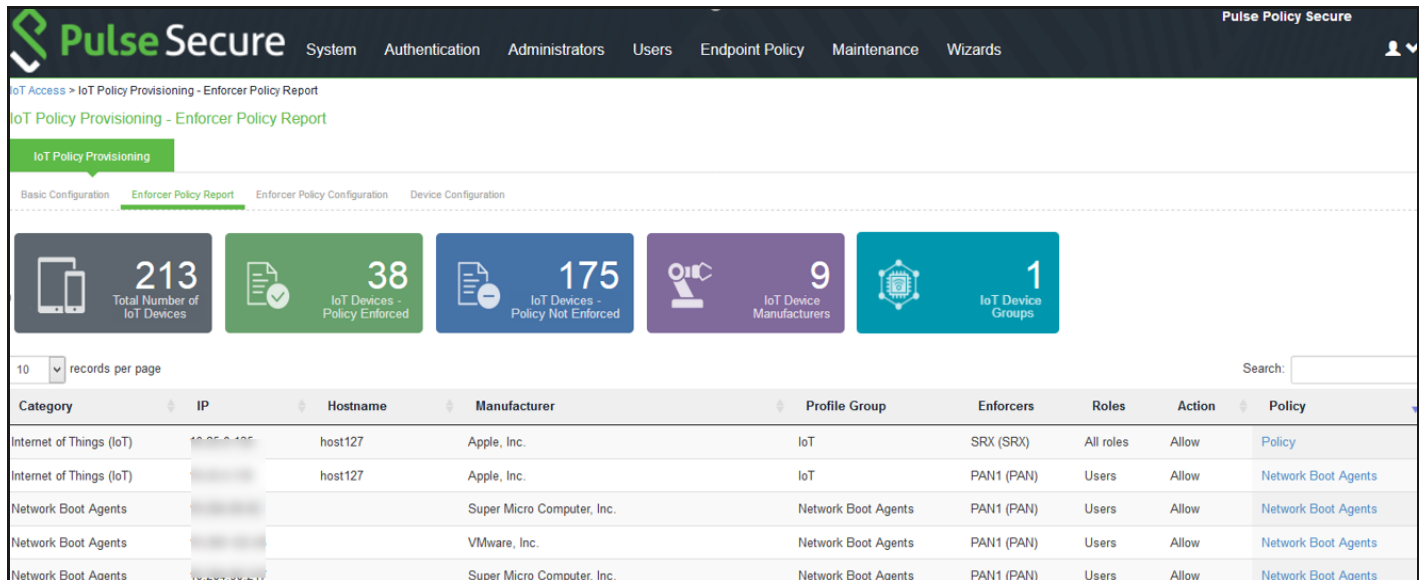
Viewing Devices in Enforcer Policy Report

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:

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

Figure 29 Enforcer Policy Report



Configuring IoT Access Policy using Juniper SRX 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 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.

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 **Junos SRX**.
6. Under **Device Details**, specify whether the policy should be applied based on device category and manufacturer or Profile group.
 - a. Category and manufacturer

1. 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).
 2. Select the Device manufacturer from the Available Device Manufacturers.
 3. Specify the protocol (TCP/UDP/ICMP) and Port/Range to be applied to the discovered devices.
- d. Profile Group
1. Configure the Profiler Group (IoT Access > IoT Policy Provisioning - Device Configuration). To configure Profiler Groups, [“Configuring Profiler Groups” on page 44.](#)
 2. Select the Profile Group from the Available Profile Groups.
 3. Specify the protocol (TCP/UDP/ICMP) and Port/Range to be applied to the discovered devices.

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. If you want to enter different port values, you can edit the port value under Resources table.

- e. 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.

7. 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 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.
8. Select the desired Roles for which the policy applies. For example, IoT Administrator.
9. Under Actions, select whether to allow access or deny access.
10. Click **Save Changes**.

Figure 30 Junos SRX Enforcer Policy Configuration

Pulse Secure System Authentication Administrators Users **Endpoint Policy** Maintenance Wizards

IoT Access > IoT Policy Provisioning > Enforcer Policy Configuration > iot-group

iot-group

General

* Name: iot-group Required: Label to reference this policy.

Description:

▼ Intranet Enforcer

Platform: ☒ JUNOS SRX ☐ Palo Alto Networks Firewall

Specify the Intranet Enforcer(s) to which this policy applies. (Applicable for only Juniper or Palo Alto Networks Firewalls.)

Available Enforcers: SRX_Cluster (SRX) **Add ->** **Remove**

Selected Enforcers: SRX650_89.109 (SRX)

▼ Device Details

Specify the filter for getting resources.

☐ Category and Manufacturer ☒ Profile Group

Click here to configure Device Category or Profile Group.

Select the profile group(s) for which this policy applies.

Available Profile Group(s): **Add ->** **Remove**

Selected Profile Group(s): iot-group1

Specify Protocol and Port/Range which will be applied to the discovered devices.

Protocol: ☒ TCP ☐ UDP ☐ ICMP

Port: Examples: 80 or 80-433 or 1-1024 or 8080, 1-1024,8082 or 1-1024,8080 or 1-100,500-600 etc.

☒ Auto-Update Newly Discovered Devices.

▼ Resources

Resources will be auto-populated using the configuration specified in Device Details panel; port field is editable. Policy for the selected resources will be pushed to enforce.

10 records per page Search:

IP	Protocol	Port	
10.204.88.72		<input type="text"/>	<input checked="" type="checkbox"/>
10.204.88.98		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.225		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.226		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.227		<input type="text"/>	<input checked="" type="checkbox"/>
10.204.88.160		<input type="text"/>	<input checked="" type="checkbox"/>
10.204.88.69		<input type="text"/>	<input checked="" type="checkbox"/>
10.204.88.158		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.228		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.193		<input type="text"/>	<input checked="" type="checkbox"/>

Showing 1 to 10 of 24 entries [Previous](#) [1](#) [2](#) [3](#) [Next](#)

▼ Roles

☐ Policy applies to ALL roles ☒ Policy applies to SELECTED roles ☐ Policy applies to all roles OTHER THAN those selected below

Available roles: Contractor_FullAccess_Role Contractor_LimitedAccess_Role FullAccess_Role Guest Guest Admin **Add ->** **Remove**

Selected roles: Blocked_Users_Role

▼ Actions

☐ Allow access ☒ Deny access

Deny / Reject Message: Short message displayed to users when traffic is denied or rejected. *{SOURCEIP}* *{DESTIP}* *{DESTPORT}* and *{PROTOCOL}* in the message are replaced with the source IP address, destination IP address, destination port, and protocol of the denied traffic. *{USER}* in the message is replaced with the name of the user.

NOTE: changes to this page will cause a slight interruption of service for Intranet Enforcer Resource Policies users.

Save Changes **Save as Copy**

Once the policy is successfully added, it can be viewed as shown in [Figure 31](#).

Figure 31 Junos SRX Enforcer Policy Configuration

Policy	Category	Manufacturers	Profile Groups	Auto-Update	Enforcers	Roles	Resources	Action
iot-group			iot-group1	ON	SRX650_89.109 (SRX)	Blocked_Users_Role	10.204.88.72:* 10.204.88.98:* 10.209.114.225:* 10.209.114.226:* 10.209.114.227:* 10.204.88.160:* 10.204.88.69:* 10.204.88.158:* 10.209.114.228:* 10.209.114.193:* More...	Deny
iot-cat	Smartphones/PDAs/Tablets	HUAWEI TECHNOLOGIES CO.,LTD		ON	SRX650_89.109 (SRX)	All roles	10.209.123.81:* 10.204.90.58:* 10.209.122.142:* 10.204.90.73:* 10.209.123.109:* 10.209.123.88:* 10.204.90.23:* 10.209.123.33:* 10.204.90.35:* 10.209.123.31:* More...	Allow

Note: The Device Details panel is only available when IoT Access Policy is created using IoT Policy Provisioning > Enforcer Policy Configuration.

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.

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 remains 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
 1. 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).
 2. Select the Device manufacturer from the Available Device Manufacturers.
 3. Specify the protocol (TCP/UDP) and Port/Range to be applied to the discovered devices.
 - b. Profile Group
 1. Configure the Profiler Group (IoT Access > IoT Policy Provisioning - Device Configuration). To configure Profiler Groups, see ["Configuring Profiler Groups" on page 44](#).
 2. Select the Profile Group from the Available Profile Groups.
 3. Specify the protocol (TCP/UDP) and Port/Range to be applied to the discovered devices.

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 32 Palo Alto Networks Firewall Enforcer Policy Configuration

IoT Access > IoT Policy Provisioning - Enforcer Policy Configuration > New Policy

New Policy

* Name:
IoT1

Description:

Required: Label to reference this policy.

Intranet Enforcer

Platform:

JUNOS SRX

Palo Alto Networks Firewall

Specify the Intranet Enforcer(s) to which this policy applies.
(Applicable for only Juniper and Palo Alto Networks Firewalls.)

Available Enforcers:

PAN-88.234 (PANNGFW)

Add ->

Remove

Selected Enforcers:

PAN-10.96.70.1 (PANNGFW)

Security Zones

Specify firewall security zones for this policy.
If security zone is not specified, then it applies to all zones i.e. any
Multiple zones can be specified with comma separated. Example: trust,mgmt

Source Zone:

untrust

Destination Zone:

trust

Device Details

Specify the filter for getting resources.

Category and Manufacturer

Profile Group

Click here to configure Device Category or Profile Group.

Select the profile group(s) for which this policy applies.

Available Profile Group(s):

Selected Profile Group(s):

iot-group1

Service:

any

Auto-Update Newly Discovered Devices.

Resources

Resources will be auto-populated using the configuration specified in Device Details panel, port field is editable.
Policy for the selected resources will be pushed to enforcer.

10 records per page

Search:

IP	Protocol	Port	
10.204.88.72			
10.204.88.98			
10.209.114.225			
10.209.114.226			
10.209.114.227			
10.204.88.160			
10.204.88.69			
10.204.88.158			
10.209.114.228			
10.209.114.193			

Showing 1 to 10 of 24 entries

Previous

1

2

3

Next

Roles

Policy applies to ALL roles

Policy applies to SELECTED roles

Policy applies to all roles OTHER THAN those selected below

Available roles:

Blocked_Users_Role

Contractor_FullAccess_Role

Contractor_LimitedAccess_Role

Guest

Guest Admin

Selected roles:

FullAccess_Role

Actions

Allow access

Deny access

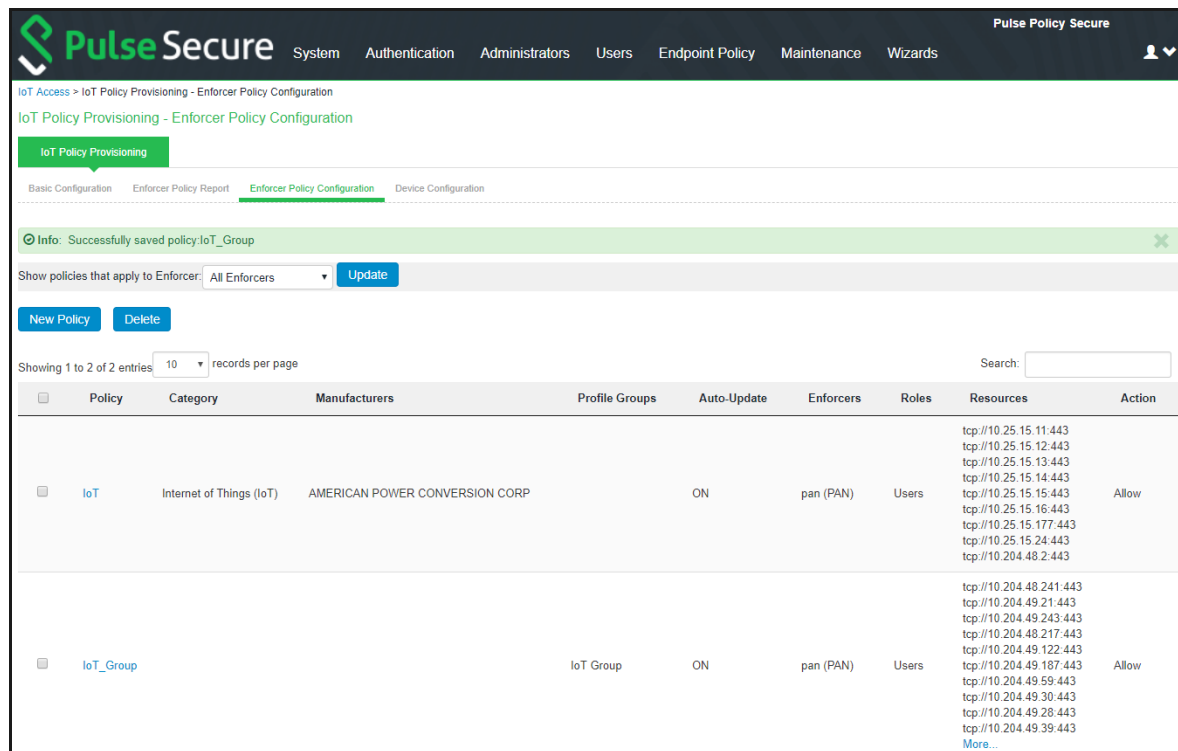
NOTE: changes to this page will cause a slight interruption of service for Intranet Enforcer Resource Policies users.

Save Changes

Save as Copy

Once the policy is successfully added, it can be viewed as shown in [Figure 33](#).

Figure 33 Palo Alto Networks Firewall Enforcer Policy Configuration



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 34 Device Category Configuration

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 35 Configuring Profiler Groups

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.

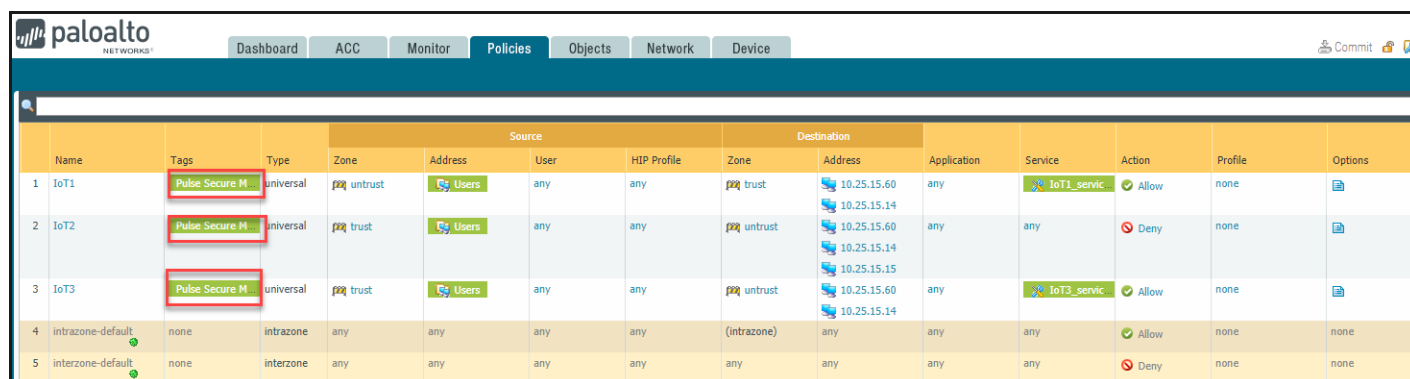
You can also use **Maintenance > Troubleshooting > Monitoring > Debug Log** for debugging issues.

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*.

Note: Selecting the option "Policy Applies to All Roles" for Resource Access Policy with PAN as Infranet Enforcer may not work as expected. Hence, it is recommended to use the option "Policy Applies to Selected Roles" instead.

Figure 36 PaloAlto Networks

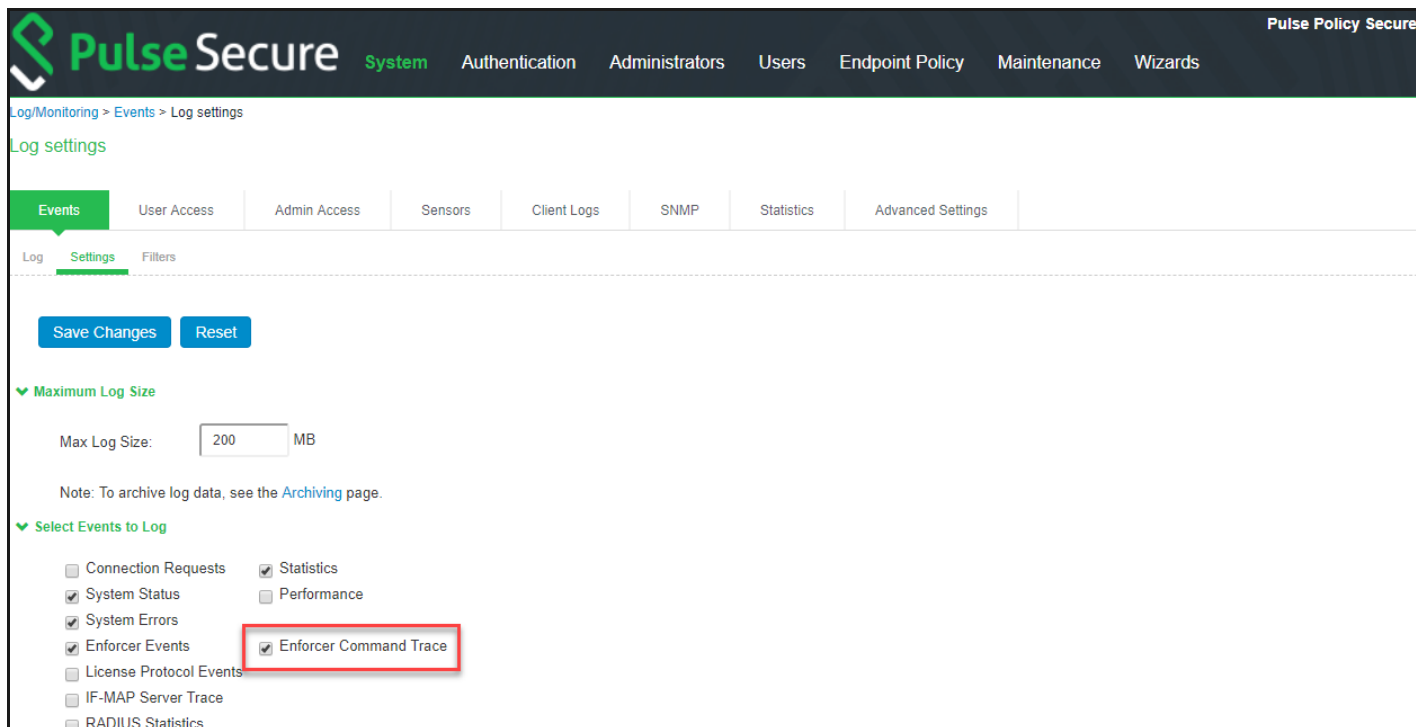


	Name	Tags	Type	Zone	Source	Destination	Application	Service	Action	Profile	Options
1	IoT1	Pulse Secure M	universal	untrust	Users	trust	any	IoT1_servic	Allow	none	
2	IoT2	Pulse Secure M	universal	trust	Users	untrust	any	any	Deny	none	
3	IoT3	Pulse Secure M	universal	trust	Users	untrust	any	IoT3_servic	Allow	none	
4	intrazone-default	none	intrazone	any	any	(intrazone)	any	any	Allow	none	none
5	interzone-default	none	interzone	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 37 Event Logs



Pulse Secure **System** Authentication Administrators Users Endpoint Policy Maintenance Wizards

Log/Monitoring > Events > Log settings

Log settings

Events User Access Admin Access Sensors Client Logs SNMP Statistics Advanced Settings

Log Settings Filters

Save Changes Reset

Maximum Log Size

Max Log Size: MB

Note: To archive log data, see the [Archiving](#) page.

Select Events to Log

<input type="checkbox"/> Connection Requests	<input checked="" type="checkbox"/> Statistics
<input checked="" type="checkbox"/> System Status	<input type="checkbox"/> Performance
<input checked="" type="checkbox"/> System Errors	
<input checked="" type="checkbox"/> Enforcer Events	<input checked="" type="checkbox"/> Enforcer Command Trace
<input type="checkbox"/> License Protocol Events	
<input type="checkbox"/> IF-MAP Server Trace	
<input type="checkbox"/> RADIUS Statistics	

A sample event logs is shown in [Figure 38](#).

Figure 38 Sample event Log

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:

Update Reset Query Save Query...

Save Log As... Clear Log Save All Logs Clear All Logs

Filter:Standard (default)
Date:Oldest to Newest
Query:
Export Format:Standard

Severity	ID	Message
Info	GWT31691	2018-10-30 03:18:44 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) Commit success: Commit
Info	GWT31691	2018-10-30 03:18:44 - ic - [127.0.0.1] System() - Enforcer:pan(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 03:18:43 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) type commit cmd: <commit></commit>
Info	GWT31691	2018-10-30 03:18:43 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) ADD policy success: IoT
Info	GWT31691	2018-10-30 03:18:43 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) command: b'<response status="success" code="20"><msg>command succeeded</msg></response>'
Info	GWT31689	2018-10-30 03:18:42 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) type config action: set xpath:/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/rulebase/security/rules/entry[@name='IoT'] element: <tag><member>Pulse Secure Managed</member></tag><source><member>Users</member></source><from><member>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_tcp</member></service><action>allow</action>
Info	GWT31691	2018-10-30 03:18:42 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) Create source address success: Users
Info	GWT31691	2018-10-30 03:18:42 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) command: b'<response status="success" code="20"><msg>command succeeded</msg></response>'
Info	GWT31689	2018-10-30 03:18:42 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) type config action: set xpath:/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/address-group/entry[@name='Users'] element: <dynamic><filter>'Users'</filter></dynamic><tag><member>Pulse Secure Managed</member></tag>
Info	GWT31691	2018-10-30 03:18:42 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) Create service success: IoT_service_tcp
Info	GWT31691	2018-10-30 03:18:42 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) command: b'<response status="success" code="20"><msg>command succeeded</msg></response>'
Info	GWT31689	2018-10-30 03:18:42 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) type config action: set xpath:/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/service/entry[@name='IoT_service_tcp'] element: <protocol><tcp><port>443</port></tcp></protocol><tag><member>Pulse Secure Managed</member></tag>
Info	GWT31691	2018-10-30 03:18:42 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) Create tag success: Pulse Secure Managed
Info	GWT31691	2018-10-30 03:18:42 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) command: b'<response status="success" code="20"><msg>command succeeded</msg></response>'
Info	GWT31689	2018-10-30 03:18:41 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) type config action: set xpath:/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/tag/entry[@name='Pulse Secure Managed'] element: <color>color13</color>
Info	GWT31691	2018-10-30 03:18:41 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) command: b'<response status="success" code="7"><result></response>'
Info	GWT31689	2018-10-30 03:18:41 - ic - [127.0.0.1] System() - Enforcer:pan(10.204.88.234) type config action: get xpath:/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/rulebase/security/rules/entry[@name='IoT']

Provisioning PCS sessions to PAN/Check Point/FortiGate Firewall

- [Overview](#) 48
- [Deployment of PPS/PCS using PAN/Check Point/ FortiGate Next Generation Firewall](#) ... 48
- [IF-MAP Configuration](#) 49

Overview

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

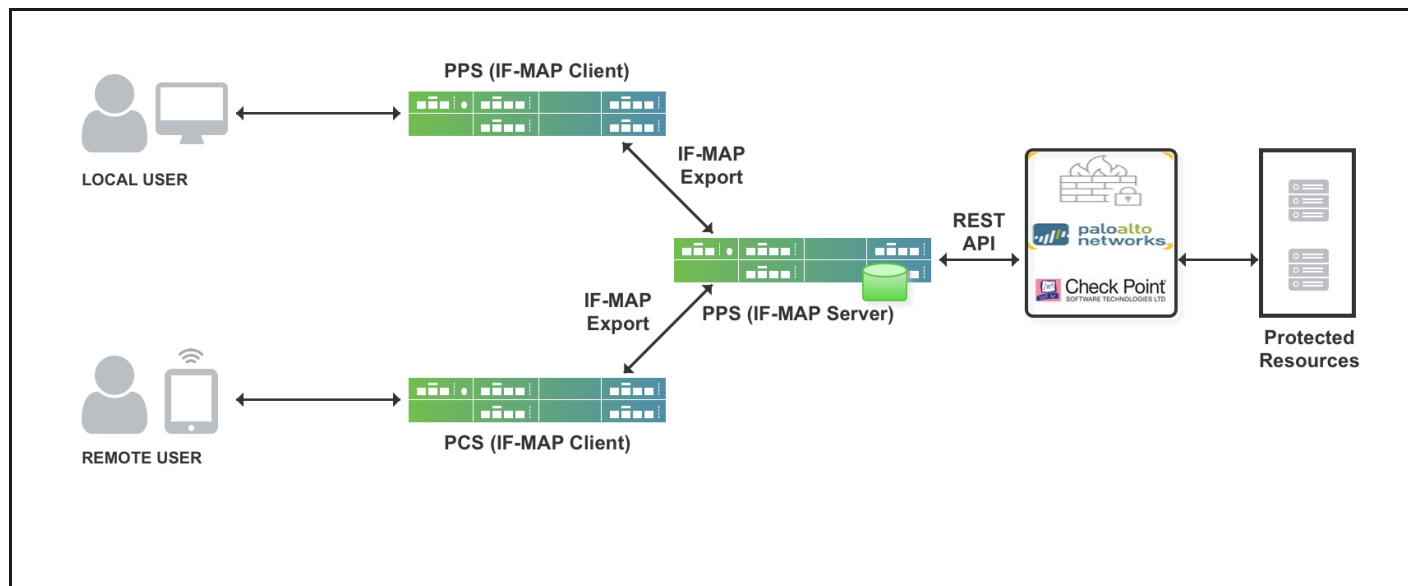
This section focuses on provisioning Pulse Connect Secure(PCS) /PPS user's identity information to PAN/Check Point/ FortiGate firewall using IF-MAP server. Using this solution access control can be provided for PCS/PPS users for accessing resources protected by Firewall.

Deployment of PPS/PCS using PAN/Check Point/ FortiGate 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/Check Point/ FortiGate Firewall. The session information is shared across PPS or PCS device using IF-MAP protocol through IF-MAP server.

The PAN/Check Point/ FortiGate 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/Check Point/ FortiGate Firewall and allows access to the protected resource based on the resource access policies that are configured on PPS.

Figure 39 The authentication process



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/Check Point/ FortiGate Firewall.
2. The remote user tries to access PAN firewall protected resource. PAN/Check Point/ FortiGate 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/Check Point/ FortiGate 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/Check Point/ FortiGate Firewall.
 - IP address of the PAN/Check Point/ FortiGate Firewall.

- API Key for PAN/ Shared Secret for Check Point/ FortiGate
- 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/Check Point/ FortiGate Firewall based on the configured Auth Table Mapping Policies.

This section covers the following topics:

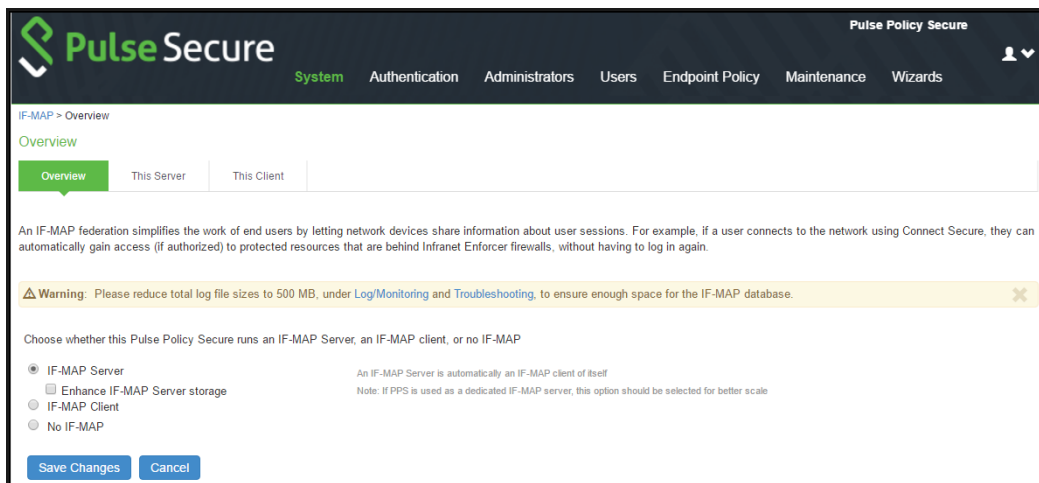
- “Step1: Configuring IF-MAP Server” on page 50
- “Step 2: Configuring IF-MAP Client” on page 52
- “Step 3: Viewing the Federated Session Details” on page 52

Step1: 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 40 Configuring IF-MAP Server Overview



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

Figure 41 Configuring IF-MAP Server New Client

Pulse Secure Pulse Policy Secure

System Authentication Administrators Users Endpoint Policy Maintenance Wizards

IF-MAP > This Server > Clients > New IF-MAP Clients

New IF-MAP Clients

IF MAP client

Name: Label to reference this IF-MAP client

Description:

IP addresses: All possible source IP addresses for inbound connections from the client

Authentication

☐ Basic

☐ Certificate

Save Changes

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

Pulse Secure Pulse Policy Secure on PPS-122

System Authentication Administrators Users Endpoint Policy Maintenance Wizards

Configuration > Certificates > Device Certificate

Device Certificate

Licensing Pulse One Security Certificates DMI Agent Sensors Client Types Guest Access

Device Certificates Trusted Client CAs Trusted Server CAs Client Auth Certificates Certificates Validity Check

Specify the Device Certificate(s). If you don't have a certificate yet, you can create a CSR and import the resulting signed certificate. If necessary, you can add custom [Intermediate CAs](#).

Import Certificate & Key... Delete...

10 records per page Search:

	Certificate issued to	Issued by	Valid Dates	Used by
<input type="checkbox"/>	psecure.net	psecure.net	Feb 2 14:29:33 2018 GMT to Jul 26 14:29:33 2023 GMT	

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

Figure 42 Configuring IF-MAP Server Delete

Pulse Secure Pulse Policy Secure on PPS-122

System Authentication Administrators Users Endpoint Policy Maintenance Wizards

Configuration > Certificates > Device Certificate

Device Certificate

Licensing Pulse One Security Certificates DMI Agent Sensors Client Types Guest Access

Device Certificates Trusted Client CAs Trusted Server CAs Client Auth Certificates Certificates Validity Check

Specify the Device Certificate(s). If you don't have a certificate yet, you can create a CSR and import the resulting signed certificate. If necessary, you can add custom [Intermediate CAs](#).

Import Certificate & Key... Delete...

10 records per page Search:

	Certificate issued to	Issued by	Valid Dates	Used by
<input type="checkbox"/>	psecure.net	psecure.net	Feb 2 14:29:33 2018 GMT to Jul 26 14:29:33 2023 GMT	

Step 2: 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 43 Configuring IF-MAP Client Overview

Pulse Secure Pulse Policy Secure

System Authentication Administrators Users Endpoint Policy Maintenance Wizards

IF-MAP > 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 Infranet 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://ic/dana-ws/soap/dsifmap

▼ 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.

Step 3: Viewing the Federated Session Details

To view the federated session details, select **System > IF-MAP > This Server > Federation-wide Sessions**.

Figure 44 Viewing the Federated Session Details

Pulse Secure

System Authentication Administrators Users Endpoint Policy Maintenance Wizards

IF-MAP > This Server > Fed-Wide Sessions

Fed-Wide Sessions

Overview This Server This Client

Clients Replicas Federation-Wide Sessions

200 sessions First user: in administrative domain Update

10 records per page Search:

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		10.200.112.5		1CsxZsQ/PCS-90.250

← Previous 1 Next →

One-to-One Network Address Translation (NAT)

- Overview 54
- One-to-One NAT Deployment 54
- Configuring one-to-one NAT 54

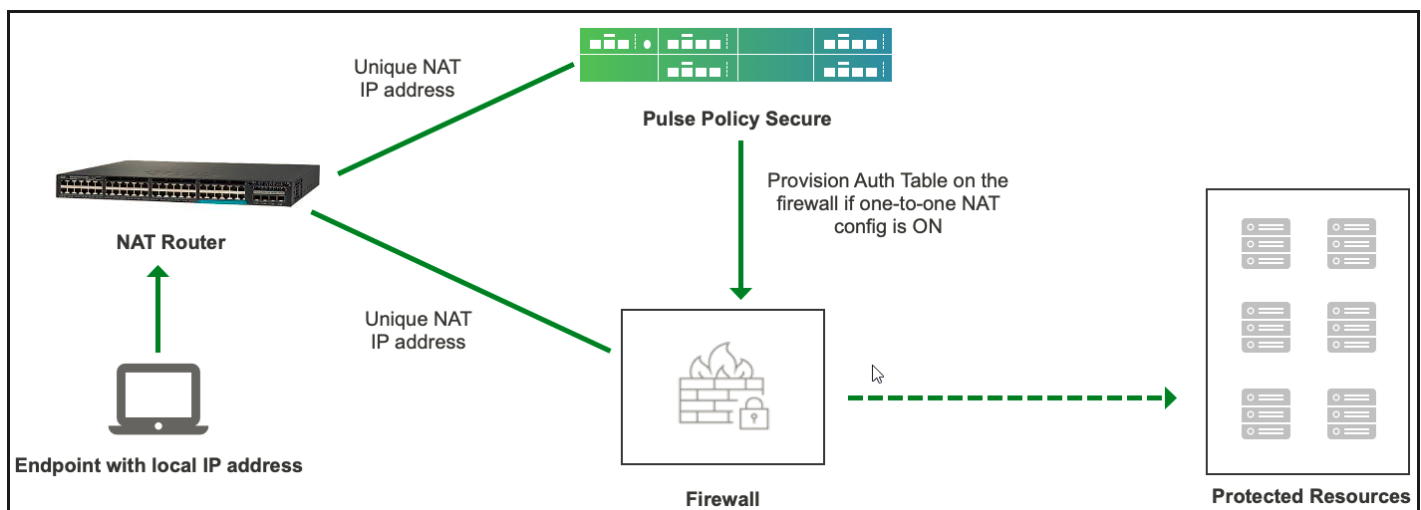
Overview

One-to-One NAT is the process that maps one internal private IP address to one external public IP address. This helps to protect the private IP addresses from any malicious attack or discovery as the private IP addresses are kept hidden. PPS allows admin to provision auth table entries for endpoints behind one-to-one NAT deployment.

One-to-One NAT Deployment

In this deployment, each end user is having their local address and they are assigned a unique NAT IP address. PPS labels the end user as behind NAT for this type of deployment. The resources are provisioned to firewall only if the Provision Auth table for endpoints behind one-to-one NAT deployment option is enabled on PPS.

Figure 45 One-to-One NAT Deployment



The authentication process is described below:

1. User behind one-to-one NAT logs in and the corresponding user role is assigned.
2. A matching auth table mapping policy is detected. If configuration for **Provision Auth table for one-to-one NAT Deployment** option is enabled in this policy, then authentication table for external public IP address for the user is pushed on the firewall.
3. User logs out and all the external public IP address information associated with the user from that endpoint is removed from the firewall.

Configuring one-to-one NAT

To configure one-to-one NAT on PPS:

1. Select **Endpoint Policy > Infranet Enforcer > Auth Table Mapping**.
2. Select **Provision Only User-IP Mapping to Palo Alto Networks Enforcer** to provision user name only to PAN enforcer to use the directory services.
3. Under One-One NAT deployment, enable the checkbox for **Provision Auth Table for one-to-one NAT deployment**.

Figure 46 Configuring one-to-one NAT

The screenshot shows the configuration page for the Default Policy under Infranet Enforcer Auth Table Mapping Policies. The page is divided into several sections:

- General:**
 - * Name: Default Policy (Required: Label to reference this policy)
 - Description: Allows auth table mapping to all Infranet Enforcers; remove this policy to restrict mapping to specific Infranet Enforcers.
- Infranet Enforcer:**
 - Specify the Infranet Enforcer(s) to which this policy applies.
 - Available Enforcers: PAN
 - Selected Enforcers: (all)
 - Buttons: Add ->, Remove
- Enforcement Settings:**
 - Enable this option to provision only IP-User mapping to Palo Alto Networks Enforcer. Applicable to Palo Alto Networks Enforcer only.
 - ☐ Provision only IP-User mapping to Palo Alto Networks Enforcer
- Roles:**
 - ☒ Policy applies to ALL roles
 - ☐ Policy applies to SELECTED roles
 - ☐ Policy applies to all roles OTHER THAN those selected below
 - Available roles: Guest, Guest Admin, Guest Sponsor, Guest Wired Restricted, Users
 - Selected roles: (none)
 - Buttons: Add ->, Remove
- Actions:**
 - ☒ Always Provision Auth Table
 - ☐ Provision Auth Table As Needed (Only available for Juniper enforcers)
 - ☐ Never Provision Auth Table
 - VSYS: [Empty field]
- One-to-one NAT Deployment:**
 - ☐ Provision Auth table for one-to-one NAT Deployment (Enable this option to provision Auth Table for one-to-one NAT Deployment)

Buttons at the bottom: Save Changes, Save as Copy. A note at the bottom left states: * indicates required field.

4. The Admin is redirected to a confirmation page with a warning message.

Note: This configuration option is recommended to use for one-to-one NAT Deployment. It is not recommended to use for many-to-one NAT Deployment. If used, it could allow multiple endpoints behind many-to-one NAT to access resources without authentication.

5. Click **Enable**.
6. Click **Save Changes**.

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, file a ticket with PSGSC.

- Product warranties—For product warranty information, visit <https://support.pulsesecure.net/product-service-policies/>

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure provides an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://support.pulsesecure.net>
- Search for known bugs: <https://support.pulsesecure.net>
- Find product documentation: <https://www.pulsesecure.net/techpubs>
- Download the latest versions of software and review release notes: <https://support.pulsesecure.net>
- Open a case online in the CSC Case Management tool: <https://support.pulsesecure.net>
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://support.pulsesecure.net>

For important product notices, technical articles, and to ask advice:

- Search the Pulse Secure Knowledge Center for technical bulletins and security advisories: <https://kb.pulsesecure.net>
- Ask questions and find solutions at the Pulse Community online forum: <https://community.pulsesecure.net>

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at <https://support.pulsesecure.net>.
- Call 1-844 751 7629 (Toll Free, US).
- For international or direct-dial options in countries without toll-free numbers, see <https://support.pulsesecure.net/support-support-contacts/>

