Network Configuration Example

Configuring Authentication and Enforcement Using SRX Series Services Gateways and Aruba ClearPass Policy Manager

Modified: 2016-08-02

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Network Configuration Example Configuring Authentication and Enforcement Using SRX Series Services Gateways and Aruba ClearPass Policy Manager

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

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

CHAPTER 1

Integrating Juniper Networks SRX Services Gateways, EX Series Switches, and Aruba ClearPass Policy Manager to Provide Authentication, Enforcement, and Threat and Attack Detection and Prevention

About This Network Configuration Example

This network configuration example describes the LDP-over-RSVP feature and the benefits of using it. It also includes a step-by-step procedure for configuring an LDP-over-RSVP topology.

Use Case Overview

With the proliferation of mobile devices and cloud services, securing them has become a fundamental strategic part of enterprise cybersecurity. Use of company smartphones poses one of the biggest IT security risks to businesses. In a work environment that supports mobile devices, knowing the identity of the user whose device is associated with an attack or threat provides IT administrators with an improved advantage in identifying the source of the attack and stemming potential future attacks that follow the same strategy.

SRX Series Services Gateways are next-generation firewall and security services devices offering outstanding protection, performance, scalability, availability, and security service integration. SRX Series devices are designed for port density, with a high-performance security services architecture, and provide seamless integration of networking and security in a single platform.

Aruba ClearPass Policy Manager is a policy management platform that provides role-based and device-based network access control (NAC) for any user across any wired, wireless, and VPN infrastructure.

The integration of ClearPass with SRX Series Services Gateways for authentication and enforcement can protect against attacks and intrusions by allowing you to configure security policies that identify users by their usernames, or by the groups they belong to. SRX Series devices can identify threats and attacks perpetrated against your network environment, and provide this information to the ClearPass Policy Manager (CPPM) so that action can be taken against the attacker. As a network security administrator, you can better align your security enforcement to protect against future similar attacks.

Enterprises that also deploy EX Series switches in these environments can leverage the switches' extensive RADIUS capabilities to integrate with Aruba ClearPass. This integration enables enterprises to deploy consistent security policies across their wired and wireless infrastructure.

This network configuration example shows how to integrate Juniper Networks and Aruba ClearPass products to support two use cases:

- Authentication and enforcement—When a user initially joins the network, authentication information is typically not shared beyond the authentication server. Integration is needed so that ClearPass can share user authentication and identity information with SRX Series devices to enable "identity-awareness" in security policies.
- Threat and attack detection and notification—When security is limited to initial access authentication of endpoints, the network is effectively blind to events that happen later in the connection life cycle. A feedback loop is needed so that SRX Series devices can share information back to ClearPass, to enable additional action to be taken if and when required.

Related Documentation

- Technical Overview on page 7
- Example 1: Configuring Endpoint Authentication and Enforcement on page 11

- Example 2: Configuring the User Query Function on page 26
- Example 3: Configuring Threat and Attack Detection and Notification on page 33
- Junos OS Release 12.3X48 Feature Guide

Technical Overview

The SRX Series integrated ClearPass authentication and enforcement feature gives you granular control at the user level over access to protected resources and the Internet. As administrator of an SRX Series device, you can now leverage the user and role information in ClearPass Policy Manager (CPPM) by specifying it within the device configuration, effectively making security policies "identity-aware." You are no longer restricted to relying solely on the IP address of the device as a means of identifying the user. User-level (or group-level) awareness enhances your control over security enforcement.

In addition to providing the SRX Series device with authenticated user information, CPPM can map a device type to a role and assign users to that role. It can then send that role mapping to the SRX Series device. This capability allows you to control (through security policies) a user's access to resources when they are using a specific type of device.

The integration of SRX Series devices with ClearPass delivers a set of network protection services to defend against a wide range of attack strategies. In addition to protecting the company's network resources, the SRX Series device can make available to CPPM log records generated by these protective security features in response to attacks or attack threats.

Support for the SRX Series integrated ClearPass authentication and enforcement feature begins with the following software releases:

- Junos OS Release 12.3X48-D30, for SRX Series Services Gateways
- Aruba ClearPass Policy Manager (CPPM) 6.6

Authentication and Enforcement

SRX Series device security policies protect the company's resources and enforce access control at a fine-grain level, taking advantage of the user authentication and identity information sent to the device from CPPM. CPPM can act as the authentication source, using its own internal RADIUS server to authenticate users. It can also rely on an external authentication source, such as an external RADIUS server or Windows Active Directory LDAP server, to perform authentication.

CPPM authentication is triggered by requests from network access server (NAS) type devices, such as switches (including EX Series switches) and access controllers. CPPM then sends POST request messages containing authenticated user identity and device posture information to the SRX Series device.

Web API

The SRX Series device exposes its Web API daemon (webapi) interface to CPPM, which enables CPPM to efficiently send authenticated user identity information to the SRX Series device. In this scenario, the SRX Series Web API daemon acts as an HTTP(S) server and CPPM is a client.

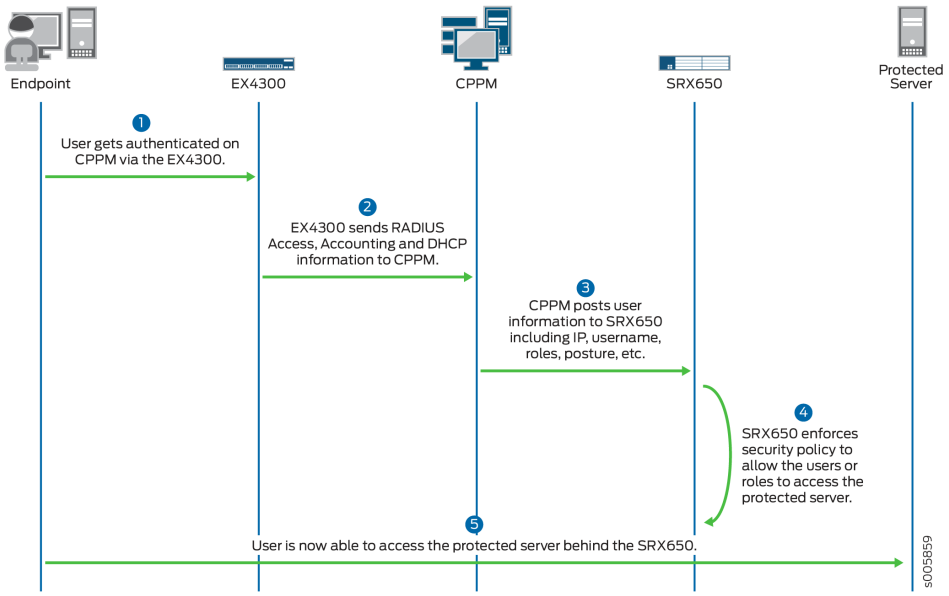
NOTE: For security reasons, we recommend using HTTPS.

ClearPass Authentication Table

When the SRX Series device receives information posted to it from CPPM, the device creates a ClearPass authentication table. The device extracts the user authentication and identity information, analyzes it, and generates an entry in the table for the authenticated user. When the SRX Series device receives an access request from a user, it can check its ClearPass authentication table to verify that the user is authenticated, and then apply the appropriate security policy to match the traffic from the user.

Figure 1 on page 8 illustrates the interworking of the network elements under normal conditions, as a user attempts to access a protected server. The EX4300 switch, CPPM, and SRX650 device work together to authenticate the user and provide access to the server. The devices also maintain awareness of the user, in case enforcement measures are required later in the user session.

Figure 1: Integrated Authentication and Enforcement - Normal Behavior



User Query Function

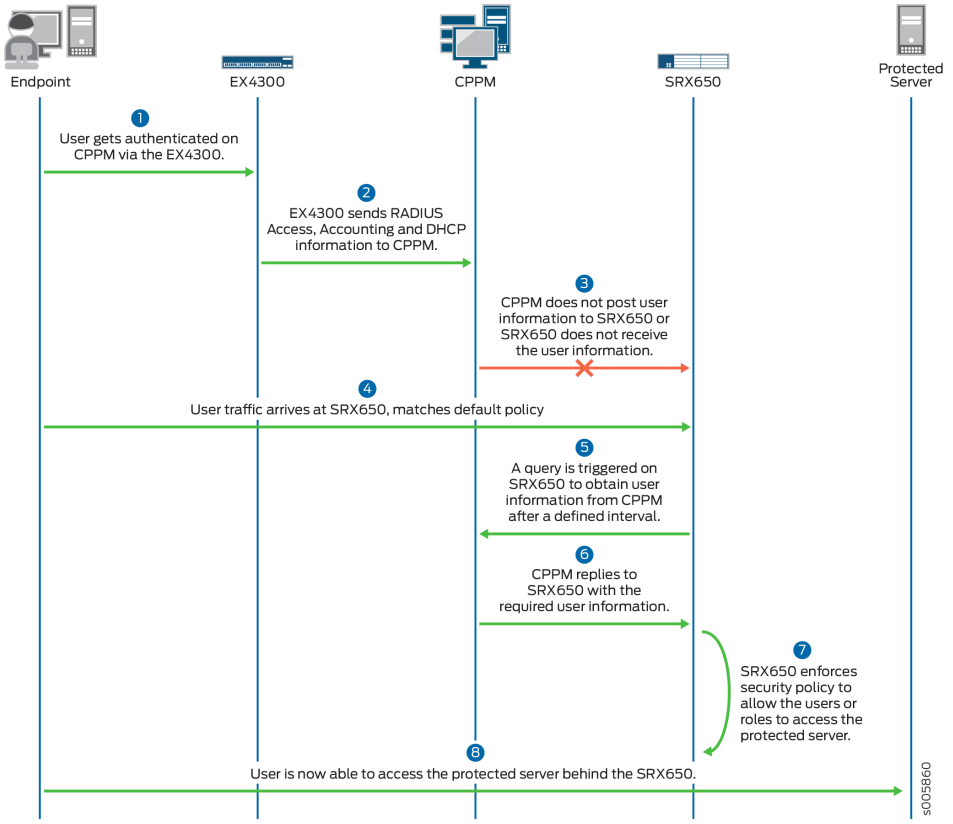
In rare cases, it may happen that an SRX Series device loses a user's authentication information, or does not receive it from CPPM. When this occurs, and user traffic arrives at the SRX Series device, the device does not have the identity awareness to recognize and authenticate the user. To protect against this scenario, you can configure the SRX

Series device's query function, which enables it to query the ClearPass server for authentication information for a user. The SRX Series device bases the query on the IP address of the user's device (which it obtained from the incoming user traffic).

When the user query function is configured, the query process is triggered automatically when the SRX Series device receives traffic from a user but does not find an entry for the user in its ClearPass authentication table.

Figure 2 on page 9 illustrates the interworking of the networks elements in a case where the SRX Series device does not have a user's authentication information. In this case, when the user's traffic arrives at the SRX650, the device sends a query to CPPM to obtain the necessary information. When the SRX650 device receives the user information, it creates an entry for the user in its ClearPass authentication table, authenticates the user, and grants access to the server.

Figure 2: Integrated Authentication and Enforcement - User Query Function



Threat and Attack Detection and Notification

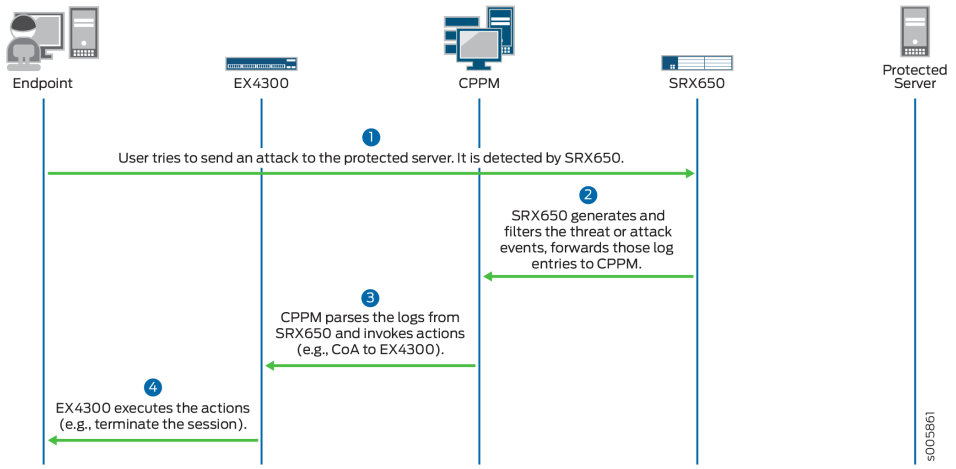
As noted earlier, the SRX Series integrated ClearPass authentication and enforcement feature enables not only the ability to use user information from CPPM to make the SRX Series device "identity-aware," it also enables the SRX Series device to send attack and threat event logs to CPPM for further action on existing users.

When an SRX Series device detects threat and attack events, they are recorded in the device's event log. The SRX Series device uses syslog to forward the logs to CPPM, which can evaluate the logs and take action based on configured matching conditions.

NOTE: SRX Series devices can provide CPPM with information on any kind of security threat event that can be sent though syslog. This includes core services such as SCREEN options, IDP, and UTM, as well as extended services such as Sky Advanced Threat Prevention, and so on.

Figure 3 on page 10 illustrates the interworking of the networks elements in a case where an authenticated user attempts to attack the protected server. The SRX650 device detects the attack and sends log information to CPPM. Based on this information, CPPM sends a RADIUS disconnect request message to the EX4300, which terminates the session and disconnects the user.

Figure 3: Integrated Authentication and Enforcement - Threat/Attack Detection



NOTE: For more detailed information on these scenarios, and the SRX Series integrated ClearPass authentication and enforcement feature, see the Junos OS Release 12.3X48 Feature Guide.

Related Documentation

- Configuring 802.1X PEAP and MAC RADIUS Authentication with EX Series Switches and Aruba ClearPass Policy Manager
- Device Profiling with EX Series Switches and Aruba ClearPass Policy Manager

Example 1: Configuring Endpoint Authentication and Enforcement

This configuration example illustrates how to configure and integrate an SRX Services Gateway, an EX Series switch, and Aruba ClearPass Policy Manager to enable user-level access control to protected resources on the network.

This topic covers:

Requirements

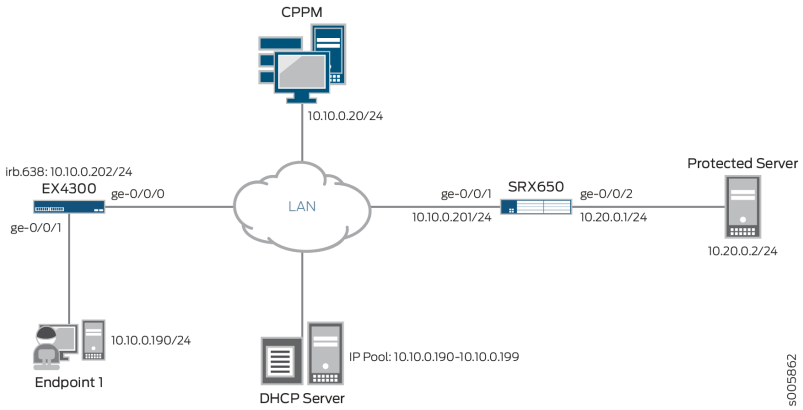
This example uses the following hardware and software components:

- An SRX650 device running Junos OS Release 12.3X48-D30 or later
- An EX4300 switch running Junos OS Release 15.1R3 or later
- Aruba ClearPass Policy Manager (CPPM) 6.6 on a CP-VA-500 platform

Overview and Topology

This network configuration example uses the topology shown in Figure 4 on page 11.

Figure 4: Solution Topology for SRX Series Integration with ClearPass



NOTE: All the examples in this document use the same topology.

In this example, user test1 sits at PC Endpoint 1 and wants to access the protected server. User test1 belongs to the QA group. The EX4300 switch has 802.1X authentication enabled on interface ge-0/0/1 and uses CPPM as its RADIUS server. On the SRX650 device, a

security policy is defined to allow only users from the QA group to access the protected server.

When the user tries to connect to the protected server, the EX4300 switch authenticates the user using 802.1X authentication. The user is verified against the CPPM user database and is allowed access to the network. CPPM then posts the user's identity information to the SRX650 device, which can then enforce security policies based on the username or group information to allow or deny the user access to the protected servers.

A DHCP server is used in this example to allocate IP addresses to the authenticated endpoints. As CPPM uses DHCP options to profile the endpoint's device type, OS info, and so on, the EX4300 switch forwards DHCP packets from the endpoint to CPPM in addition to the DHCP server.

Task Overview

The following tasks are performed in this example:

On the SRX650 device:

- Configure interfaces and zones
- Configure a security policy that includes the **source-identity** statement to allow access control based on a username or group
- Configure the Web API service to enable communication with CPPM

On the EX4300 switch:

- Configure interfaces and VLANs.
- Configure 802.1X authentication and RADIUS settings (specify CPPM as the RADIUS server)
- Configure DHCP relay to forward DHCP packets to CPPM for device profiling

On CPPM:

- Add the EX4300 switch as a network device
- Define the CPPM server's basic configuration, including enabling the Insight database
- Add the SRX650 device as an Endpoint Context Server (ECS)
- Define Context Server Actions for the SRX650 device
- Add an enforcement profile and policy
- Add a local user and map it to a role
- Bind the role mapping and enforcement policy into the 802.1X wired service

Configuration

This section provides instructions for:

Configuring the SRX650 Device

Step-by-Step Procedure

To configure the SRX650 device:

1. Configure interfaces and zones.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 10.10.0.201/24
user@host# set interfaces ge-0/0/2 unit 0 family inet address 10.20.0.1/24
user@host# set security zones security-zone untrust interfaces ge-0/0/1.0
host-inbound-traffic system-services any-service
user@host# set security zones security-zone untrust interfaces ge-0/0/1.0
host-inbound-traffic protocols all
user@host# set security zones security-zone trust interfaces ge-0/0/2.0
host-inbound-traffic system-services any-service
user@host# set security zones security-zone trust interfaces ge-0/0/2.0
host-inbound-traffic protocols all
```

2. Configure a security policy, and include the **source-identity** statement to allow users belonging to the QA group to access the protected server.

```
[edit]
user@host# set security address-book servers-zone-addresses address protected-server
10.20.0.2/32
user@host# set security policies from-zone untrust to-zone trust policy policy1 match
source-address any
user@host# set security policies from-zone untrust to-zone trust policy policy1 match
destination-address protected-server
user@host# set security policies from-zone untrust to-zone trust policy policy1 match
application any
user@host# set security policies from-zone untrust to-zone trust policy policy1 match
source-identity QA ## an "interested group"
user@host# set security policies from-zone untrust to-zone trust policy policy1 then permit
```

NOTE: CPPM can interwork with various authentication servers. When CPPM uses a Windows Active Directory (AD) LDAP server as the authentication source, the user information sent to the SRX Series device will include the username (or role name) *and* a domain name. This variation requires adjusting the configuration to support the additional information. The domain name must be added to the username (or role name) identified in the configuration using the format *domain\role*. For example, for the configuration setting used above, source-identity QA, identifies the role name as QA and is the correct format for local authentication; when using Windows AD, this statement must be adjusted to source-identity juniper\QA, to accommodate the domain name (in this case, juniper).

3. Configure the Web API service to communicate with Aruba ClearPass.

```
[edit]
user@host# set system services webapi user srx
user@host# set system services webapi user password <password>
user@host# set system services webapi client 10.10.0.20
user@host# set system services webapi http port 8080 ## default port
user@host# set system services webapi https port 443 ## default port is 8443
user@host# set system services webapi https default-certificate
```

NOTE: The username, password, and ports defined for the Web API service, must match what is defined in the Endpoint Context Server (ECS) section of CPPM.

Configuring the EX4300 Switch

Step-by-Step Procedure

To configure the EX4300 switch:

1. Configure interfaces and VLANs.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members
cppm-vlan
user@host# set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members
cppm-vlan
user@host# set vlans cppm-vlan vlan-id 638
user@host# set vlans cppm-vlan l3-interface irb.638
user@host# set interfaces irb unit 638 family inet address 10.10.0.202/24
```

2. Configure 802.1X authentication and RADIUS settings. Assign CPPM as the RADIUS server.

```
[edit]
user@host# set protocols dot1x authenticator interface ge-0/0/1.0 supplicant single
user@host# set protocols dot1x authenticator authentication-profile-name cp-pf1
user@host# set access radius-server 10.10.0.20 secret <password> ## IP address of
CPPM
user@host# set access radius-server 10.10.0.20 source-address 10.10.0.202
user@host# set access profile cp-pf1 authentication-order radius
user@host# set access profile cp-pf1 radius authentication-server 10.10.0.20
user@host# set access profile cp-pf1 radius accounting-server 10.10.0.20
user@host# set access profile cp-pf1 radius options nas-port-type ethernet ethernet
user@host# set access profile cp-pf1 radius-server 10.10.0.20 secret <password>
user@host# set access profile cp-pf1 radius-server 10.10.0.20 source-address 10.10.0.202
user@host# set access profile cp-pf1 accounting order radius
user@host# set access profile cp-pf1 accounting accounting-stop-on-access-deny
user@host# set access profile cp-pf1 accounting coa-immediate-update
user@host# set access profile cp-pf1 accounting address-change-immediate-update
```

NOTE: The RADIUS shared secret must match what is defined in CPPM.

3. Configure DHCP relay to forward DHCP packets to CPPM for device profiling.

```
[edit]
user@host# set forwarding-options dhcp-relay server-group cppm 10.10.0.20
user@host# set forwarding-options dhcp-relay active-server-group cppm
user@host# set forwarding-options dhcp-relay group cppm-dhcp interface ge-0/0/0.0
user@host# set forwarding-options dhcp-relay group cppm-dhcp interface irb.638
user@host# set vlans cppm-vlan forwarding-options dhcp-security group dhcp-group
overrides trusted
user@host# set vlans cppm-vlan forwarding-options dhcp-security group dhcp-group
interface ge-0/0/0.0
user@host# set vlans cppm-vlan forwarding-options dhcp-security option-82
```

NOTE: As the DHCP server is in the same subnet as Endpoint 1, the switch will broadcast the DHCP packets to the DHCP server, even with DHCP relay configured.

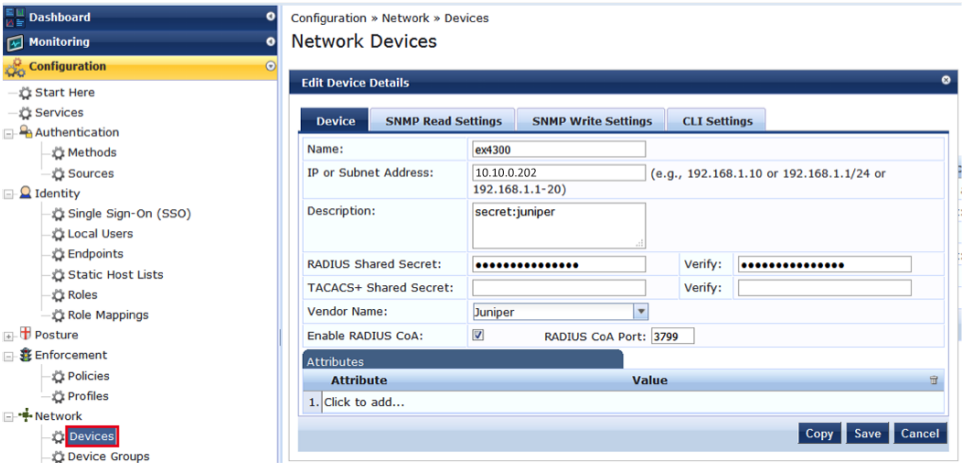
Configuring Aruba ClearPass Policy Manager

Step-by-Step Procedure

To configure CPPM interworking with the EX4300 switch and SRX650 device:

1. Add the EX4300 switch as a network device.

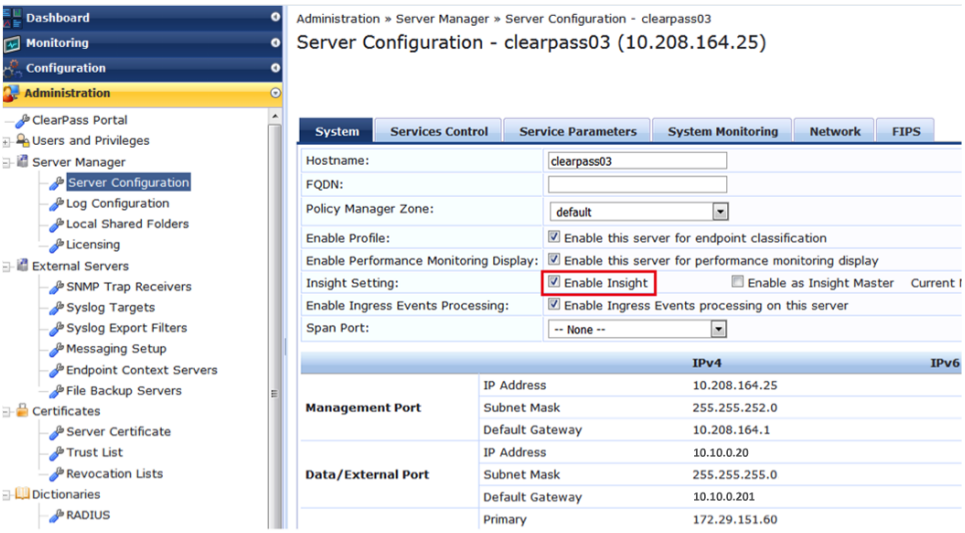
   Navigate to Configuration > Network > Devices and add the EX4300 switch on the Network Devices page.



NOTE: The RADIUS shared secret must match what is defined on the EX4300 switch.

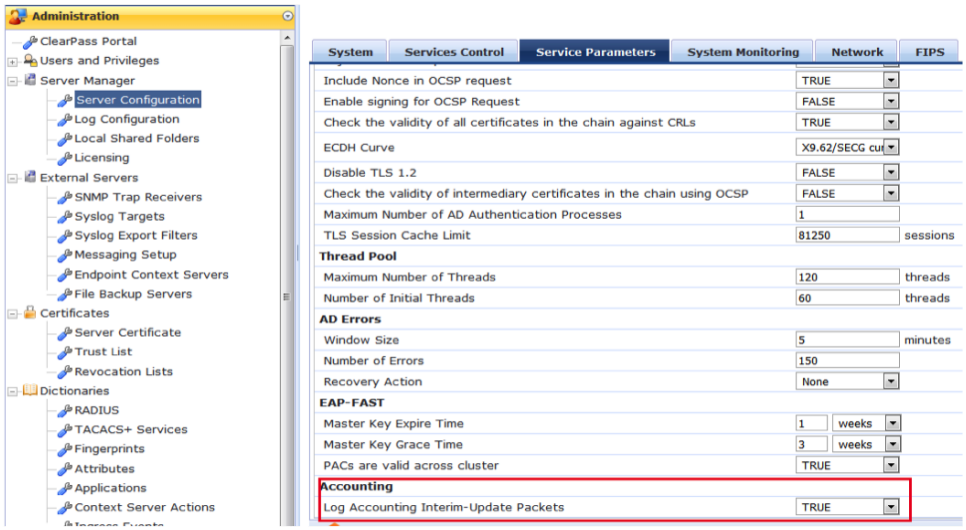
2. Define the CPPM server's basic configuration.

   a. Navigate to Administration > Server Manager > Server Configuration. On the System tab, click the **Enable Insight** check box. and configure IP addressing for the Data/External Port.



NOTE: The Insight database must be enabled, otherwise CPPM will not post any information to the SRX650 device.

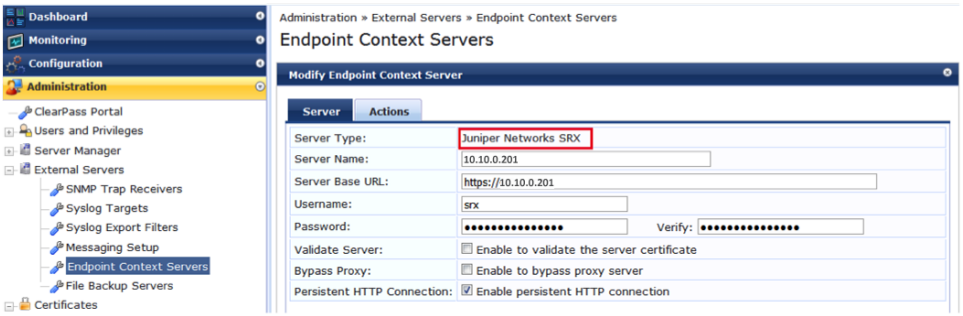
b. On the Service Parameters tab, under RADIUS Server Service, set Log Accounting Interim-Update Packets to **TRUE**.



3. Add the SRX650 device as the Endpoint Context Server.

NOTE: For more detailed information on this step, see Integrating ClearPass with Juniper Networks SRX in the CPPM User Guide.

Navigate to Administration > External Servers > Endpoint Context Servers, and on the Server tab set the Server Type to **Juniper Networks SRX**.

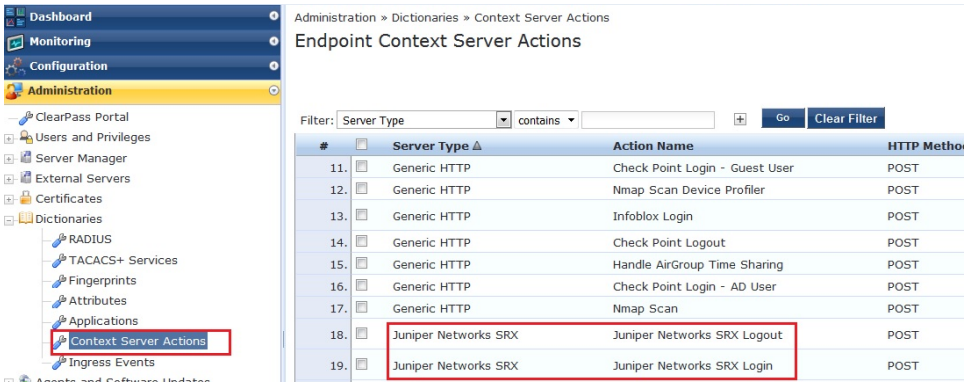


NOTE: By default, CPPM uses HTTPS port 443 to send user information to the SRX Series device. To change the port number, adjust the Server Base URL field using the format *https://<ip address>:<port>*, for example **https://10.10.0.201:8443**.

The username and password must match what is defined in the SRX Series device's Web API configuration.

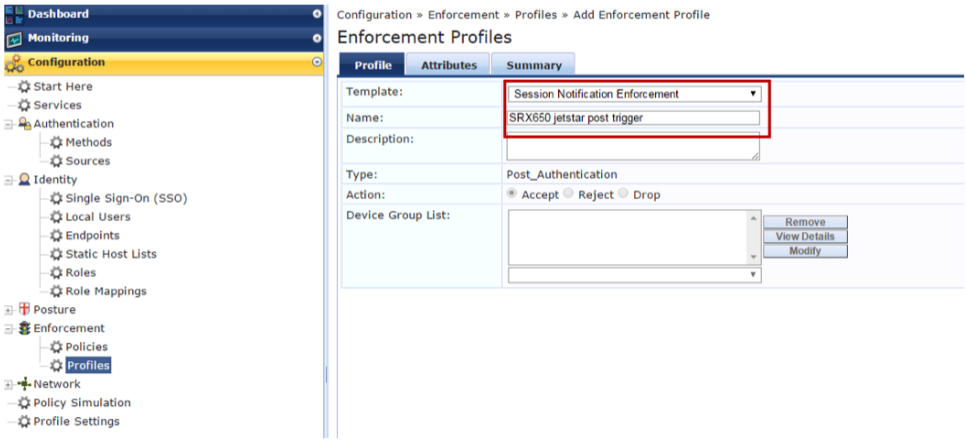
4. Define Context Server actions for the SRX650 device.

   Navigate to Administration > Dictionaries > Context Server Actions, and verify that the two entries with Server Type **Juniper Networks SRX** exist.



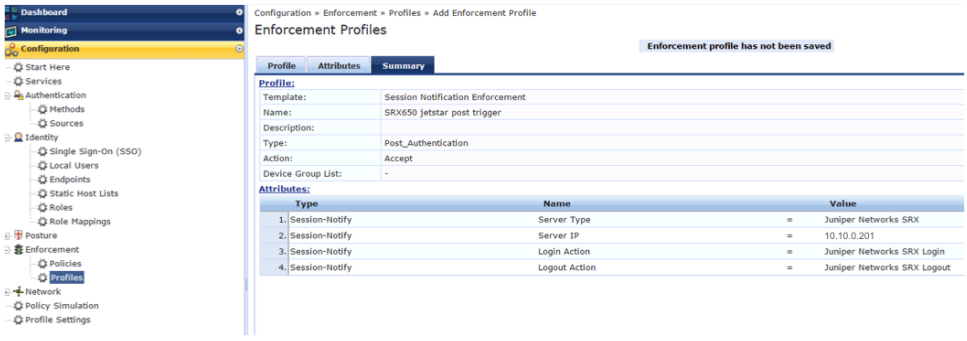
5. Add an enforcement profile and policy.

a. Navigate to Configuration > Enforcement > Profiles, and on the Profile tab select the Template **Session Notification Enforcement**, this triggers CPPM to send a notification on user login or logout.

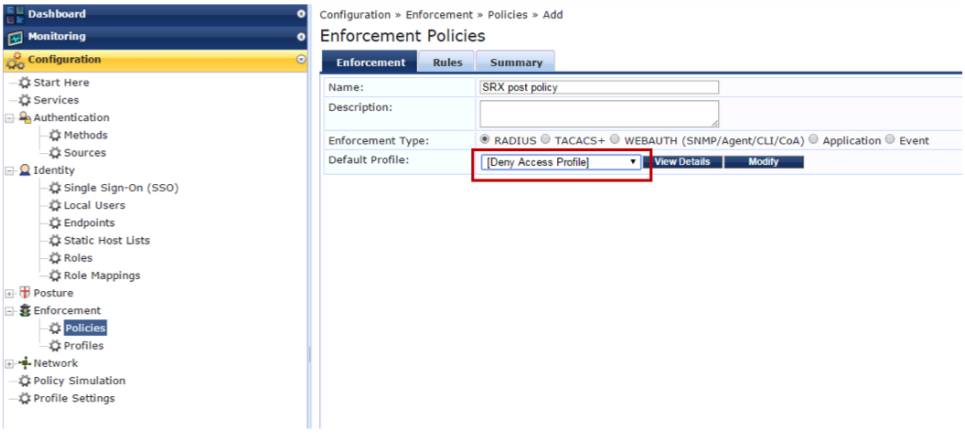


b. On the Attributes tab, add (or edit) the attribute values for the profile, as shown below.

c. On the Summary tab, review and save the configuration.

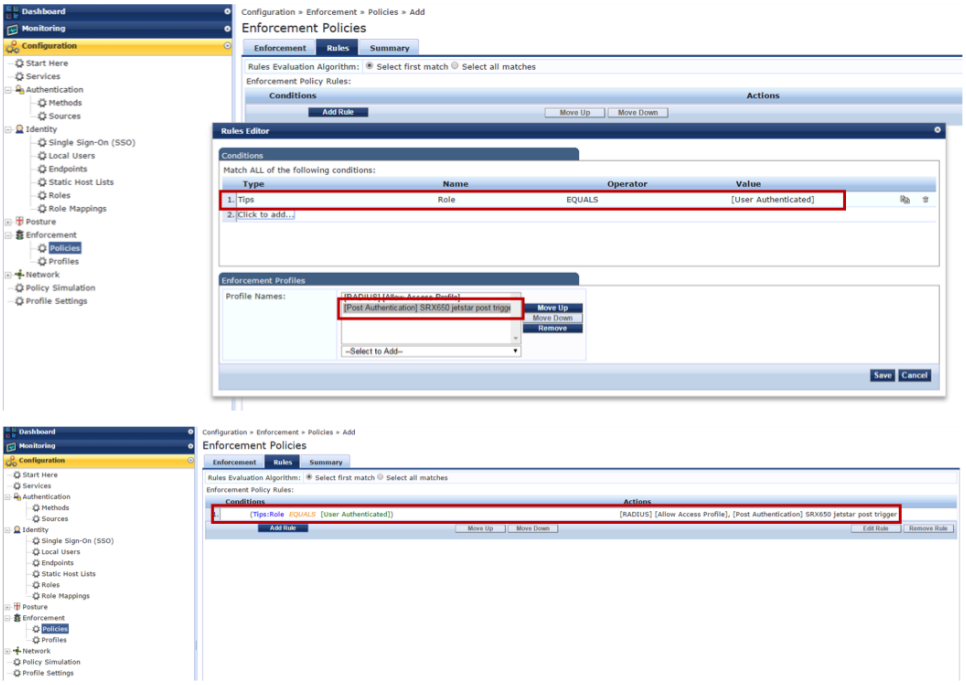


d. Navigate to Configuration > Enforcement > Policies, and on the Enforcement tab select the Default Profile **[Deny Access Profile]**.

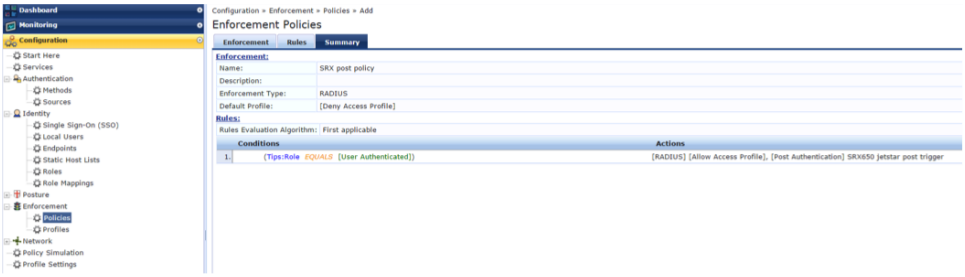


e. On the Rules tab, click **Add Rule** and add a new rule.

   Configure the rule so that if the condition matches the role **User Authenticated** (i.e. the role assigned by CPPM when a user authenticates successfully), then the profile **SRX650 jetstar post profile** profile (created earlier) is enforced.



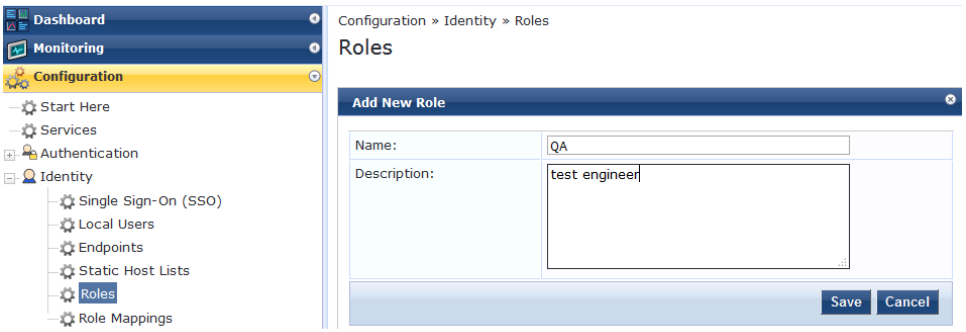
f. On the Summary tab, review and save the configuration.



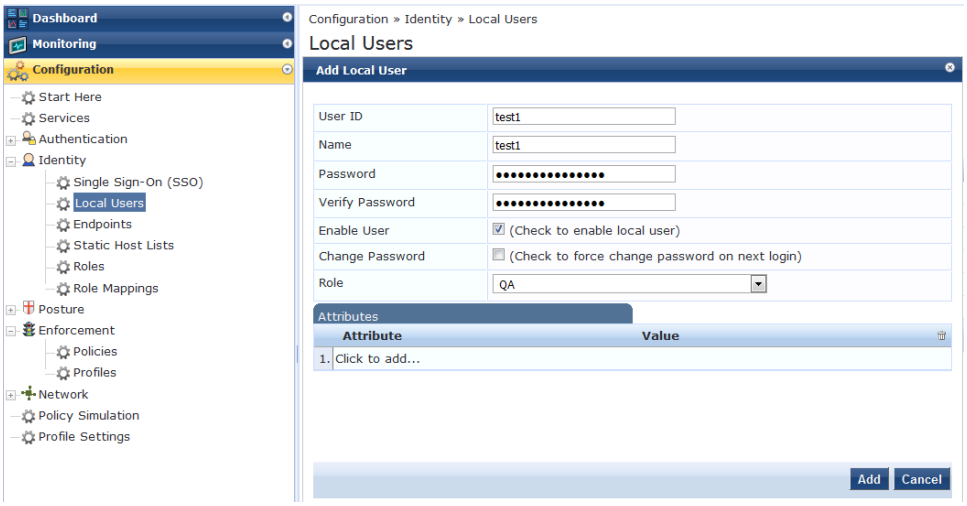
6. Add a local user and map the user to a role.

   a. Navigate to Configuration > Identity > Roles and define a new role.

      For this example, the role is called **QA**.

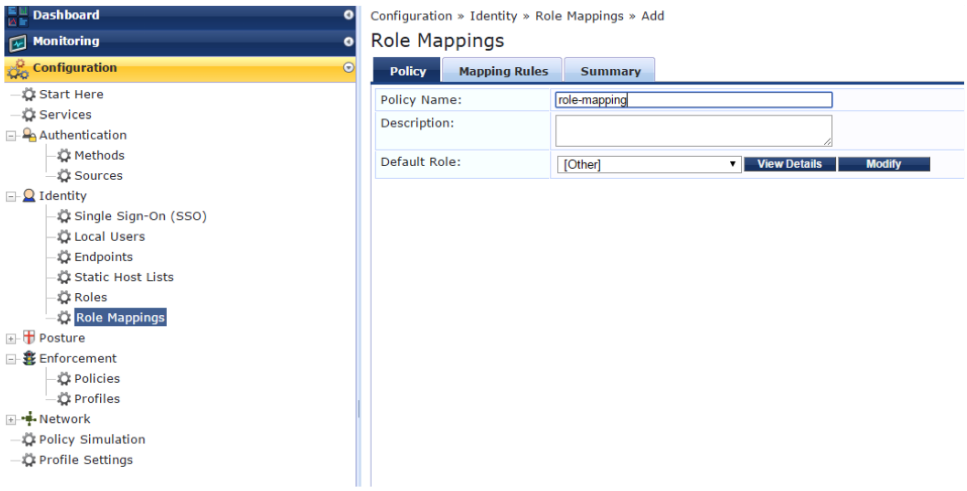


   b. Navigate to Configuration > Identity > Local users, and enter a User ID (in this case, **test1**), Password, and select the **QA** Role, as shown below.



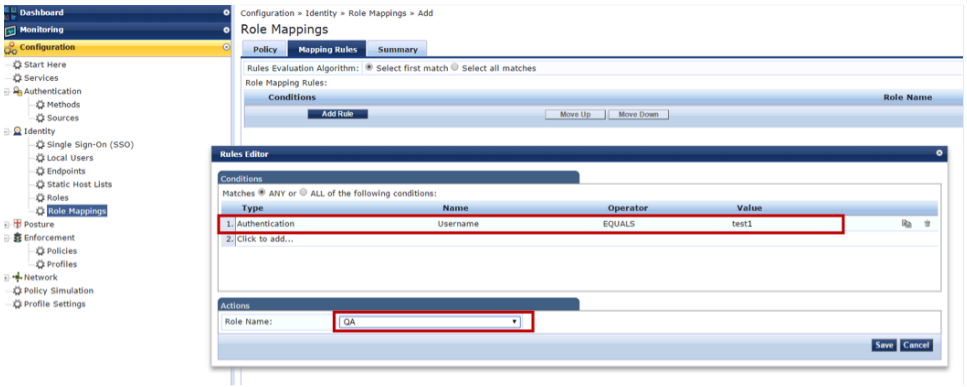
NOTE: The value selected in the Role field must match the value used in the source-identity statement of the SRX650 device configuration.

c. Navigate to Configuration > Identity > Role Mapping, and add a new role mapping.

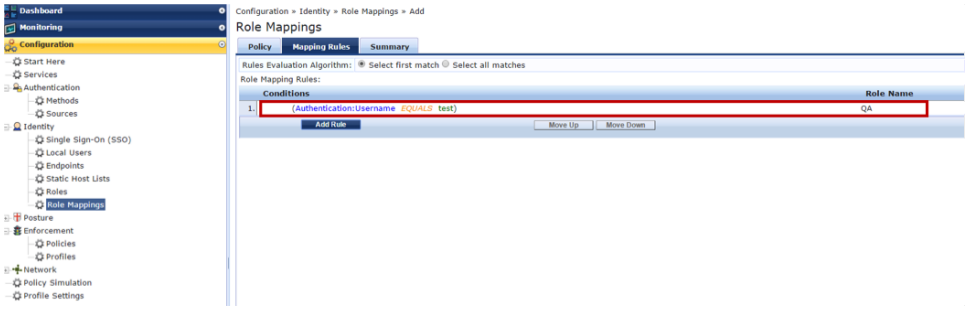


d. On the Mapping Rules tab, click **Add Rule** to assign a role to a specific user.

Configure the rule so that if the condition matches the username **test1**, assign the role **QA**.



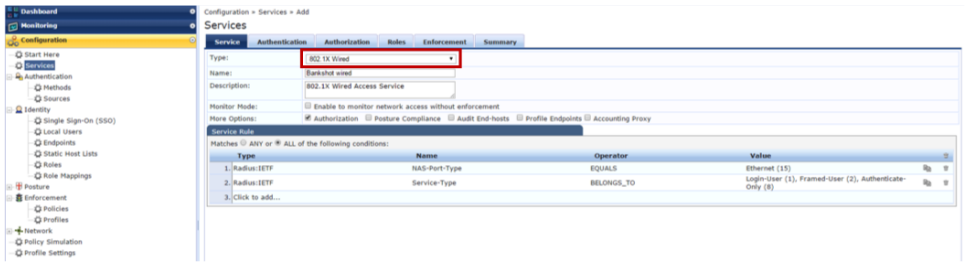
NOTE: This sub-step facilitates CPPM pushing role information to the SRX device.



e. On the Summary tab, review and save the configuration.

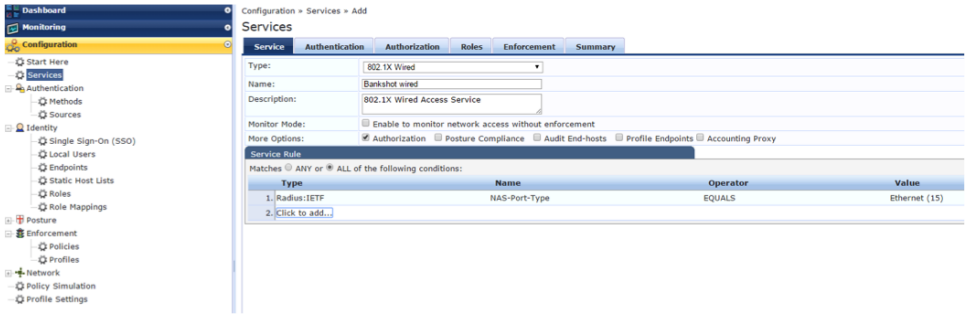
7. Bind the role mapping and enforcement policy into the 802.1X wired service.

a. Navigate to Configuration > Services, and add a new service. On the Service tab, specify the Type as **802.1X Wired**.

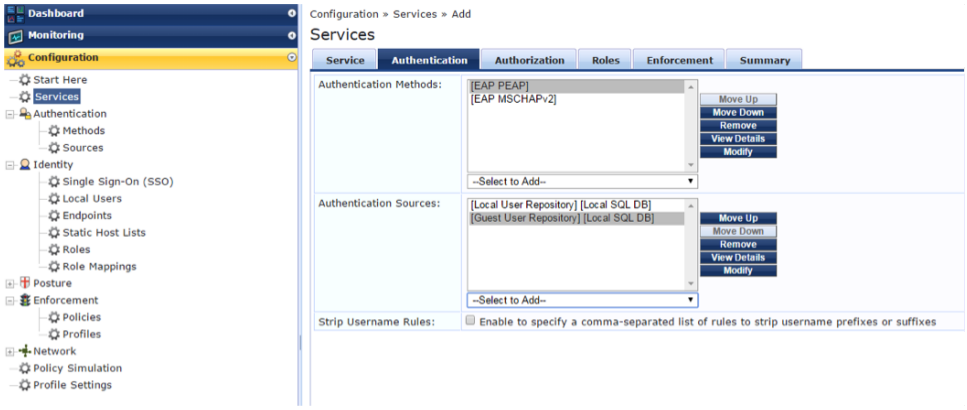


b. On the same page, remove the Service Rule named **Service-Type**.

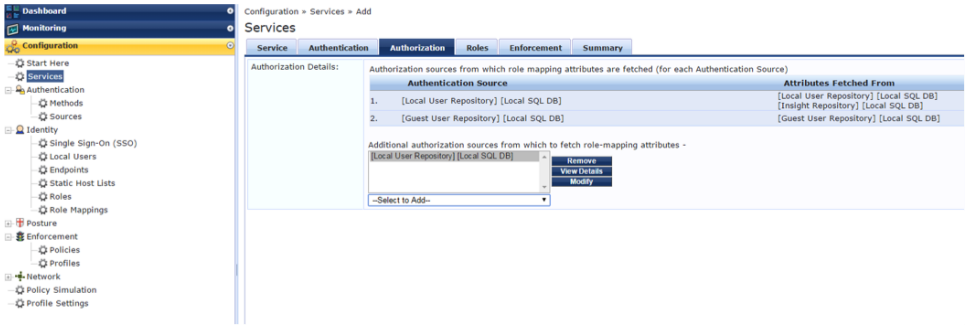
NOTE: **This rule is not needed, and if kept will cause the scenario to not work properly.**



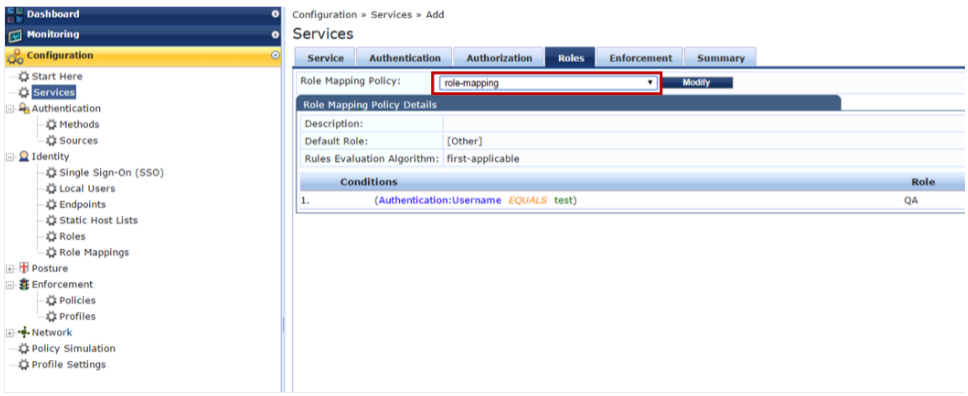
c. On the Authentication tab, arrange the Authentication Methods and Authentication Sources as shown below.



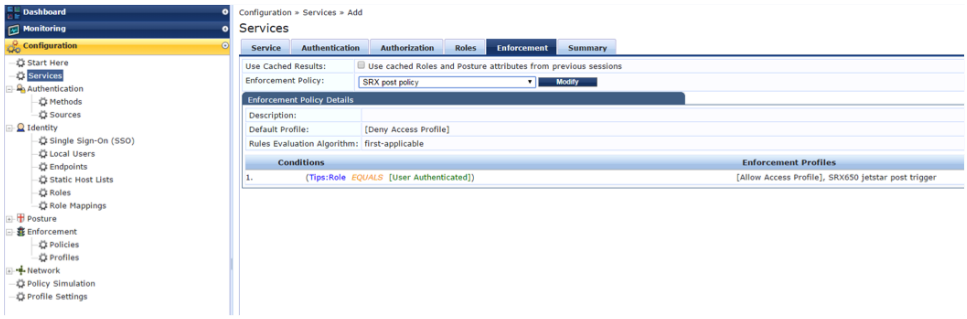
d. On the Authorization tab, add the two Authentication Sources as shown below.



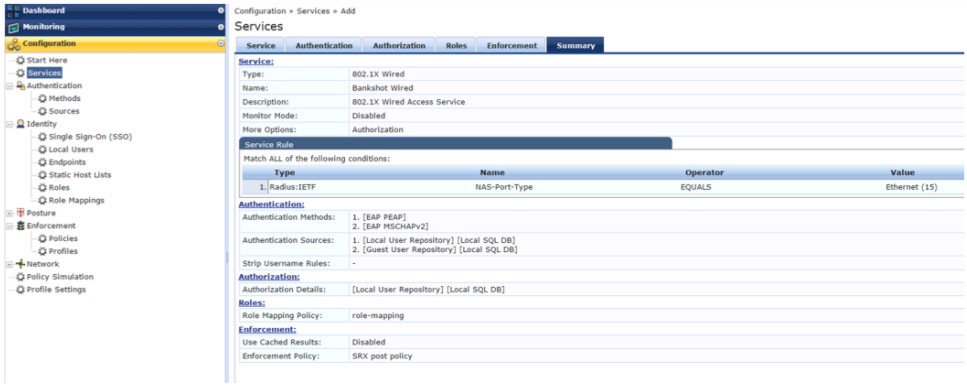
e. On the Roles tab, select **role-mapping** from the Role Mapping Policy drop-down list to bind the role mapping rule created earlier to this service.



f. On the Enforcement tab, select **SRX post-policy** from the Enforcement Policy drop-down list to bind the policy created earlier to this service.



g. On the Summary tab, review and save the configuration.



Verification

Confirm that the configuration is working properly.

- Verifying User Authentication on page 24
- Verifying User Access to the Protected Server on page 26

Verifying User Authentication

Purpose Verify that user test1 on Endpoint 1 has successfully authenticated with the various network elements.

Action

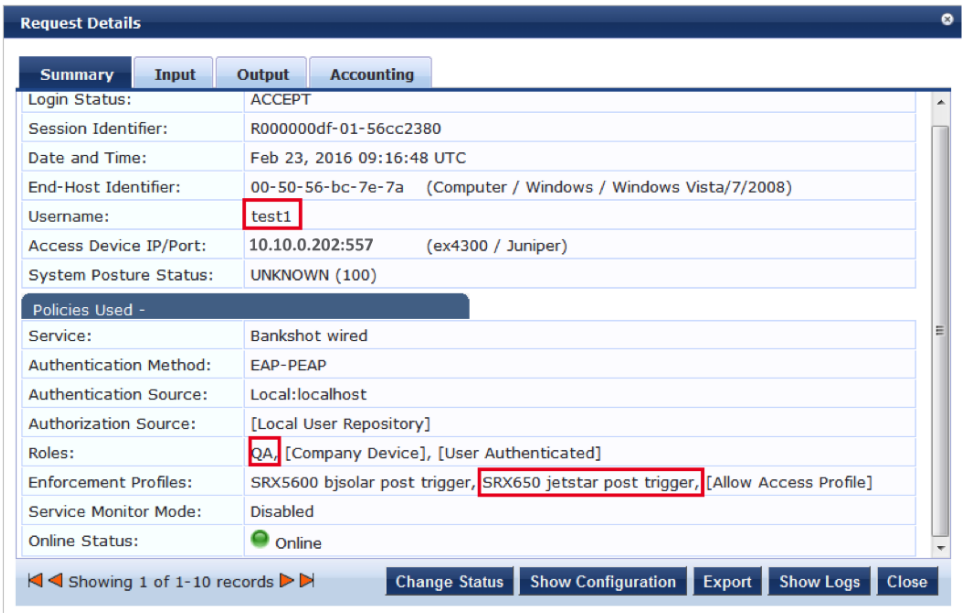
1. On the EX4300 switch, verify that user test1 is authenticated through 802.1X.

```
user@host> show dot1x interface ge-0/0/1
802.1X Information:
Interface      Role           State          MAC address        User
ge-0/0/1.0     Authenticator  Authenticated  00:50:56:BC:7E:7A  test1
```

2. In CPPM, verify that user test1 is authenticated.

   a. Navigate to Monitoring > Live Monitoring > Access Tracker, find the relevant RADIUS event and verify that user test1 has Login Status of **ACCEPT**.

   b. Click on the RADIUS event, and on the Summary tab that appears, verify that user **test1** with role **QA** has Login Status of **ACCEPT** and Online Status of **Online**. Note also that CPPM has enforced the **SRX650 jetstar post trigger** profile, which will send (post) the user information to the SRX650 device.



3. On the SRX650 device, verify that user test1's authentication information has been received from CPPM.

```
user@host> show services user-identification authentication-table authentication-source
aruba-clearpass extensive
Domain: GLOBAL
Total entries: 1
  Source-ip: 10.10.0.190
    Username: test1
    Groups:posture-unknown, qa, [employee], [user authenticated]
    Groups referenced by policy:qa
    State: Valid
    Source: Aruba ClearPass
    Access start date: 2000-01-01
```

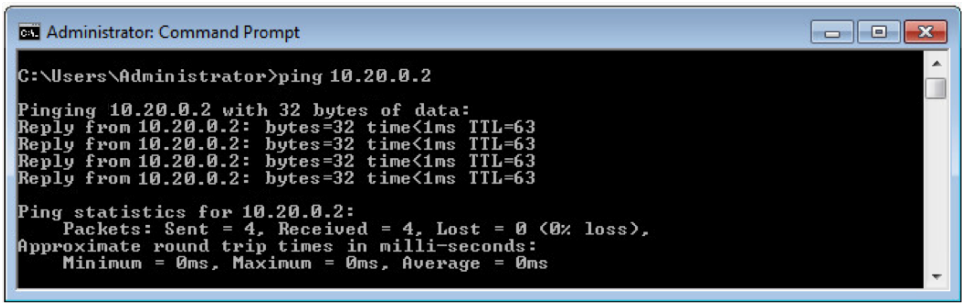
```
Access start time: 14:21:50
Last updated timestamp: 2016-02-26 14:25:28
Age time: 27
```

Meaning The user has successfully authenticated with all network elements.

Verifying User Access to the Protected Server

Purpose Verify that user test1 on Endpoint 1 can access the protected server.

Action From Endpoint 1, ping the protected server (10.20.0.2).



Meaning The user can successfully reach the protected server.

Related Documentation

- Use Case Overview on page 6
- Technical Overview on page 7
- Example 2: Configuring the User Query Function on page 26
- Example 3: Configuring Threat and Attack Detection and Notification on page 33

Example 2: Configuring the User Query Function

This configuration example illustrates how to protect against the rare case where an SRX Series device loses a user's authentication information, or does not receive it from the Aruba ClearPass server. This example shows how to configure the SRX Services Gateway and ClearPass Policy Manager so that the device can query the server for user authentication information when required.

This topic covers:

- Requirements on page 26
- Overview and Topology on page 27
- Configuration on page 28
- Verification on page 30

Requirements

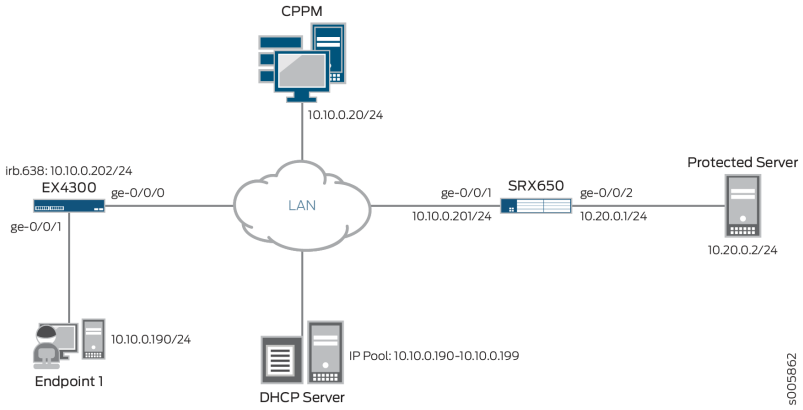
This example uses the following hardware and software components:

- An SRX650 device running Junos OS Release 12.3X48-D30 or later
- An EX4300 switch running Junos OS Release 15.1R3 or later
- Aruba ClearPass Policy Manager (CPPM) 6.6 on a CP-VA-500 platform

Overview and Topology

This network configuration example uses the topology shown in Figure 4 on page 11.

Figure 5: Solution Topology for SRX Series Integration with ClearPass



NOTE: All the examples in this document use the same topology.

This example uses the same general setup as "Example 1: Configuring Endpoint Authentication and Enforcement" on page 11. User test1 sits at PC Endpoint 1 and wants to access the protected server. User test1 belongs to the QA group. The EX4300 switch has 802.1X authentication enabled on interface ge-0/0/1 and uses CPPM as its RADIUS server. On the SRX650 device, a security policy is defined to allow only users from the QA group to access the protected server.

In this example, user test1 is authenticated by CPPM; however, the SRX650 device has not received the user information from CPPM (you will delete user test1's authentication table entry on the SRX650 device to simulate this scenario). When traffic from user test1 arrives at the SRX650 device, the first packet is assessed by the device's security policy; however, when the device checks its local ClearPass authentication table, it does not find an entry for the user.

With the user query function configured, the SRX650 device automatically sends a query to CPPM to obtain the needed information. The SRX650 device receives the information and adds the authentication table entry for user test1. The security policy now functions as expected, and subsequent packets from the user to the protected server are now permitted.

Task Overview

This example continues from "Example 1: Configuring Endpoint Authentication and Enforcement" on page 11. The following new tasks are performed:

On the SRX650 device:

- Enable the user query function

On the EX4300 switch:

- No additional configuration is required

On CPPM:

- Use ClearPass Guest to create an OAuth token
- Create an OAuth2 API client

Configuration

This section provides instructions for:

Configuring the SRX650 Device

Step-by-Step Procedure

To configure the SRX650 device:

1. Perform the SRX650 configuration steps from the Example 1 section "Configuring the SRX650 Device" on page 13.
2. Enable the user query function.

   The user query function allows the SRX650 device to query CPPM for user authentication and identity information when it does not receive this information from CPPM through the Web API daemon (webapi).

```
[edit]
user@host# set services user-identification authentication-source aruba-clearpass user-query client-id Client3
user@host# set services user-identification authentication-source aruba-clearpass user-query client-secret <password>
user@host# set services user-identification authentication-source aruba-clearpass user-query token-api api/oauth
user@host# set services user-identification authentication-source aruba-clearpass user-query query-api "api/v1/insight/endpoint/ip/$IP$"
user@host# set services user-identification authentication-source aruba-clearpass user-query web-server bankshot-cppm-sim
user@host# set services user-identification authentication-source aruba-clearpass user-query web-server address 10.10.0.20
user@host# set services user-identification authentication-source aruba-clearpass user-query web-server port 443
user@host# set services user-identification authentication-source aruba-clearpass user-query delay-query-time 0
```

NOTE: The client ID and secret must match the values entered in CPPM on the Create API Client page.

The ClearPass endpoint API requires use of OAuth (RFC 6749) to authenticate and authorize SRX Series device access.

Configuring the EX4300 switch

Step-by-Step Procedure

This section uses the same EX4300 configuration steps as the Example 1 section "Configuring the EX4300 Switch" on page 14. If you have not yet performed these steps, do so now.

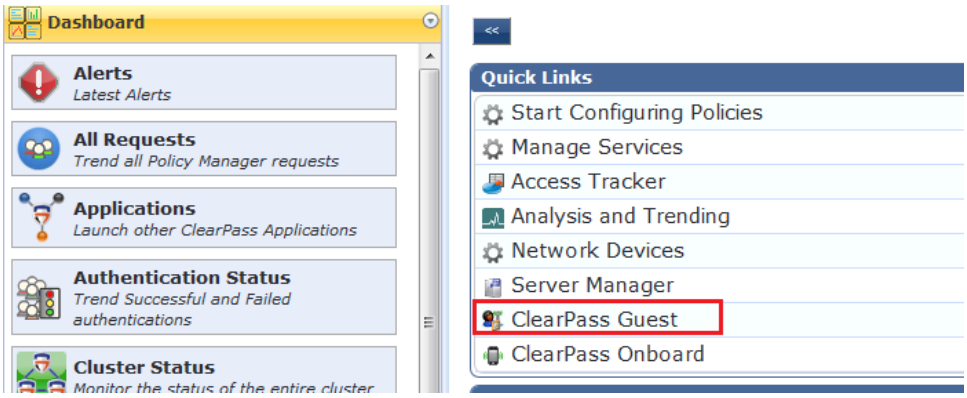
Configuring Aruba ClearPass Policy Manager

Step-by-Step Procedure

To configure CPPM to allow the SRX650 device to query its Insight database:

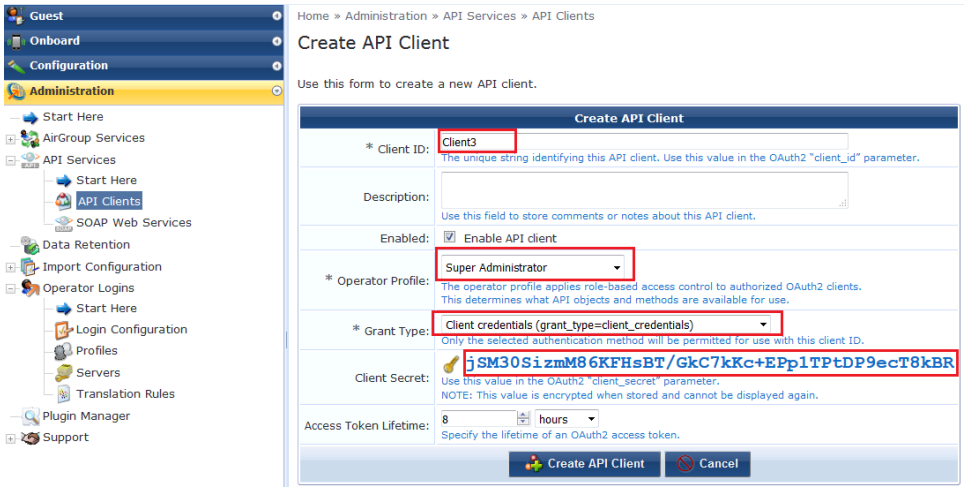
1. Perform the CPPM configuration steps from the Example 1 section "Configuring Aruba ClearPass Policy Manager" on page 15.
2. Use ClearPass Guest to create an OAuth token.

   On the CPPM Dashboard page, in the Quick Links section, select ClearPass Guest.



3. Create an OAuth2 API client.

   Navigate to Administration > API Services > API Clients and create an API client using the information shown below.



NOTE: The values used in the Client ID and the Client Secret fields must match the OAuth2 client configuration on the SRX650 device.

Verification

Confirm that the configuration is working properly.

- Verifying User Authentication on page 30
- Verifying User Access to the Protected Server on page 32

Verifying User Authentication

Purpose Verify that user test1 on Endpoint 1 has successfully authenticated with the various network elements.

Action

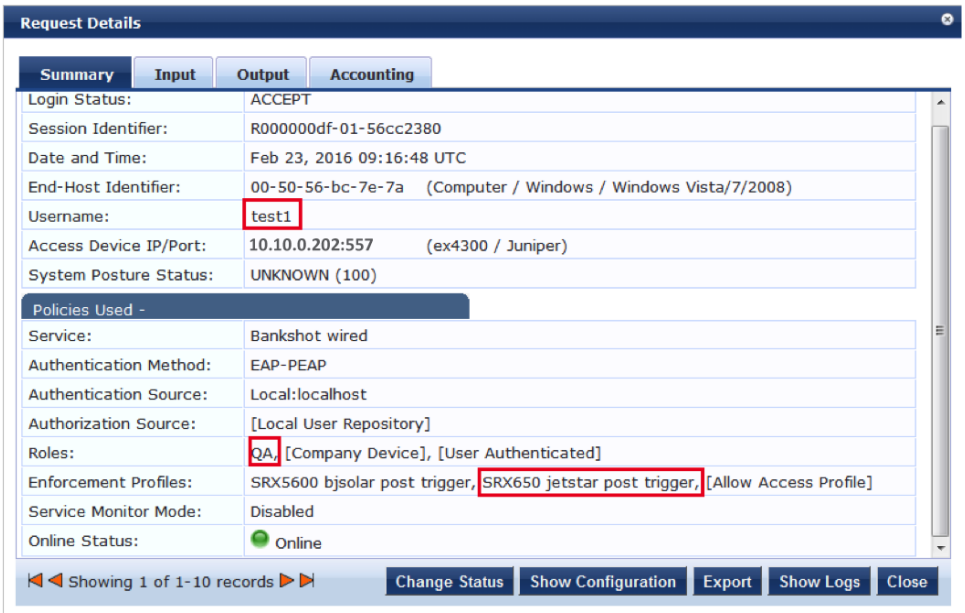
1. On the EX4300 switch, verify that user test1 is authenticated through 802.1X.

```
user@host> show dot1x interface ge-0/0/1
802.1X Information:
Interface      Role           State          MAC address        User
ge-0/0/1.0     Authenticator  Authenticated  00:50:56:BC:7E:7A  test1
```

2. In CPPM, verify that user test1 is authenticated.

   a. Navigate to Monitoring > Live Monitoring > Access Tracker, find the relevant RADIUS event and verify that user test1 has Login Status of **ACCEPT**.

   b. Click on the RADIUS event, and on the Summary tab that appears, verify that user **test1** with role **QA** has Login Status of **ACCEPT** and Online Status of **Online**. Note also that CPPM has enforced the **SRX650 jetstar post trigger** profile, which will send (post) the user information to the SRX650 device.



3. On the SRX650 device, verify that user test1's authentication information has been received from CPPM.

```
user@host> show services user-identification authentication-table authentication-source
aruba-clearpass
Domain: GLOBAL
Total entries: 1
Source IP       Username       groups(Ref by policy)          state
10.10.0.190       test1          qa                             Valid
```

Meaning The user has successfully authenticated with all network elements.

Verifying User Access to the Protected Server

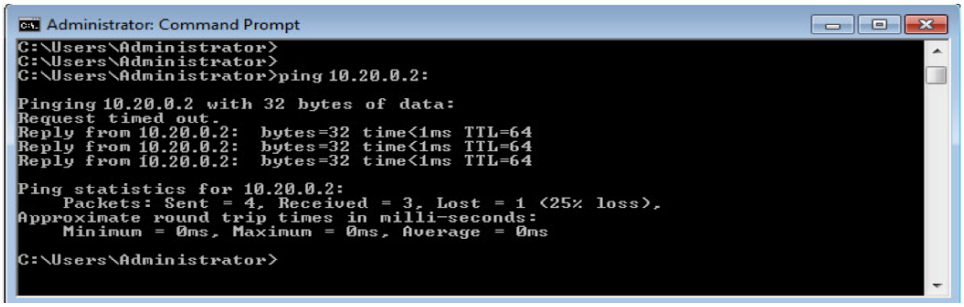
Purpose Verify that when the SRX650 device does not have a user's authentication information, it can collaborate with CPPM to permit user test1 on Endpoint 1 to access the protected server.

Action

1. On the SRX650 device, clear the ClearPass authentication table entry for user test1.

```
user@host> clear services user-identification authentication-table authentication-source
aruba-clearpass
warning: "There is no authentication-table entry."
```

2. From Endpoint 1, ping the protected server (10.20.0.2).



NOTE: Because the SRX650 device had no authentication entry for user test1, the first ping matched the default (deny) policy and timed out. In the meantime, that first ping triggered a user query to obtain user test1's information from CPPM. With the authentication entry again in the SRX650 device's authentication table, the remaining pings are successful.

3. On the SRX650 device, verify that user test1's authentication information has been received from CPPM and added to the ClearPass authentication table.

```
user@host> show services user-identification authentication-table authentication-source
aruba-clearpass
Domain: GLOBAL
Total entries: 1
Source IP       Username       groups(Ref by policy)          state
10.10.0.190       test1          qa                             Valid
```

Meaning The user can successfully reach the protected server due to the interworking between the SRX650 device and CPPM.

Related Documentation

- Use Case Overview on page 6
- Technical Overview on page 7
- Example 1: Configuring Endpoint Authentication and Enforcement on page 11
- Example 3: Configuring Threat and Attack Detection and Notification on page 33

Example 3: Configuring Threat and Attack Detection and Notification

This configuration example illustrates how to configure and integrate an SRX Services Gateway, an EX Series switch, and Aruba ClearPass Policy Manager to be able to take action in response to attacks or attack threats on network resources.

This topic covers:

Requirements

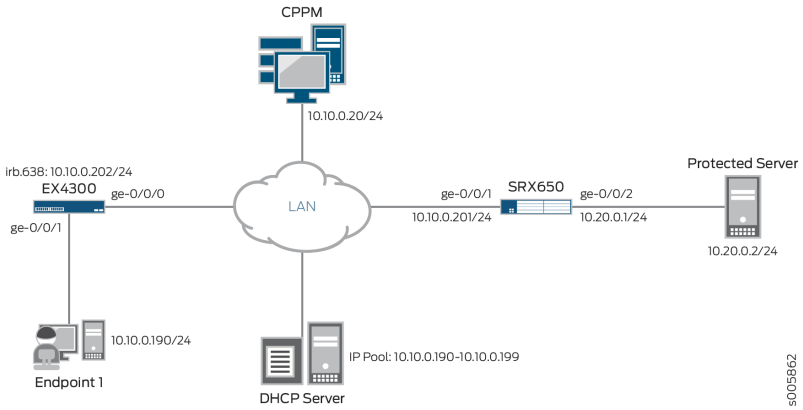
This example uses the following hardware and software components:

- An SRX650 device running Junos OS Release 12.3X48-D30 or later
- An EX4300 switch running Junos OS Release 15.1R3 or later
- Aruba ClearPass Policy Manager (CPPM) 6.6 on a CP-VA-500 platform

Overview and Topology

This network configuration example uses the topology shown in Figure 4 on page 11.

Figure 6: Solution Topology for SRX Series Integration with ClearPass



NOTE: **All the examples in this document use the same topology.**

This example uses the same general setup as "Example 1: Configuring Endpoint Authentication and Enforcement" on page 11. However, in this case user test1, sitting at PC Endpoint 1, has been already granted access to the protected server and is now using fragmented IP packets to attack it. User test1 belongs to the QA group. The EX4300

switch has 802.1X authentication enabled on interface ge-0/0/1 and uses CPPM as its RADIUS server. On the SRX650 device, in addition to having a security policy defined to allow only users from the QA group to access the protected server, a SCREEN option is also configured to block IP fragments. The SRX650 device is also configured to forward threat event logs to CPPM.

When the SRX650 device receives the fragmented IP packets from Endpoint 1, it detects and blocks the packets. The device generates a threat event log and forwards it to CPPM. On CPPM, the event log service enforces the policy and triggers a request to the EX4300 switch to terminate the user session.

Task Overview

This example continues from "Example 1: Configuring Endpoint Authentication and Enforcement" on page 11 and "Example 2: Configuring the User Query Function" on page 26.

NOTE: The features used in "Example 1: Configuring Endpoint Authentication and Enforcement" on page 11 and "Example 2: Configuring the User Query Function" on page 26 are not required for this scenario; threat and attack detection and notification can be enabled as its own feature. However, it is typical to implement all these features together, and so for this scenario the functionality is added into the existing environment.

The following new tasks are performed:

On the SRX650 device:

- Configure a SCREEN option to block IP fragments
- Configure the log stream filter to transmit only threat and attack logs to CPPM

On the EX4300 switch:

- No additional configuration is required

On CPPM:

- Enable ingress event processing and select an ingress events dictionary
- Adjust the batch processing interval
- Add the SRX650 device as an event source
- Create an enforcement policy to monitor incoming log events from the SRX650 device (and take action when certain conditions are met)
- Create a new event service and bind the enforcement policy to the service

Configuration

This section provides instructions for:

Configuring the SRX650 Device

Step-by-Step Procedure

To configure the SRX650 device:

1. Perform the SRX650 configuration steps from the Example 1 section "Configuring the SRX650 Device" on page 13 and the Example 2 section "Example 2: Configuring the User Query Function" on page 26.
2. Configure a SCREEN option to block IP fragments, and apply it to the untrust zone.

```
[edit]
user@host# set security screen ids-option jscreen ip block-frag
user@host# set security zones security-zone untrust screen jscreen
```

3. Configure the log stream filter to transmit only threat and attack logs to CPPM.

```
[edit]
user@host# set security log mode stream
user@host# set security log source-address 10.10.0.201
user@host# set security log stream to_cppm filter threat-attack
user@host# set security log stream to_cppm host 10.10.0.20
```

Configuring the EX4300 switch

Step-by-Step Procedure

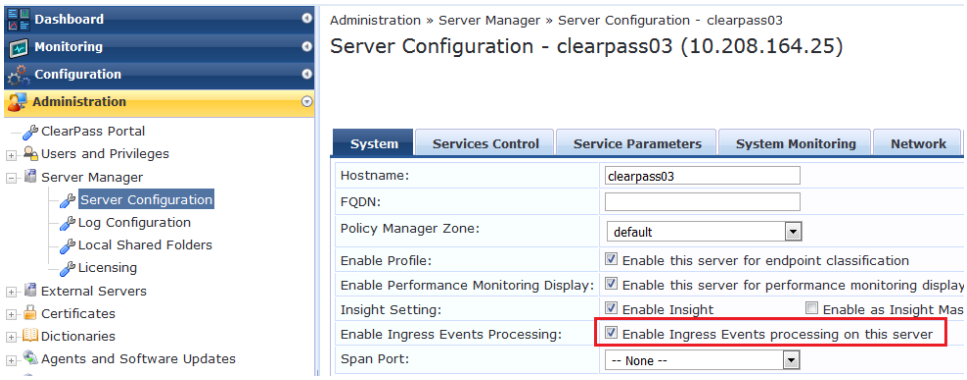
This section uses the same EX4300 configuration steps as the Example 1 section "Configuring the EX4300 Switch" on page 14. If you have not yet performed these steps, do so now.

Configuring Aruba ClearPass Policy Manager

Step-by-Step Procedure

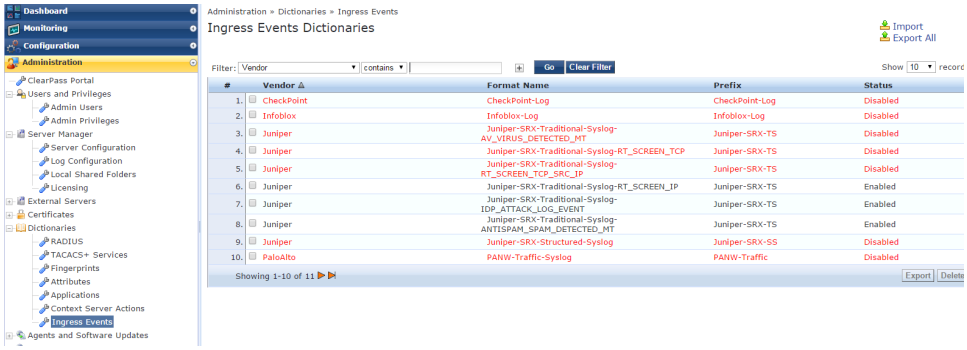
To configure CPPM to receive and process threat events from the SRX650 device:

1. Perform the CPPM configuration steps from the Example 1 section "Configuring Aruba ClearPass Policy Manager" on page 15 and the Example 2 section "Example 2: Configuring the User Query Function" on page 26.
2. Enable ingress event processing and select an ingress events dictionary.
   a. Navigate to Administration > Server Manager > Server Configuration, and on the System tab select the **Enable Ingress Events processing on this server** check box.

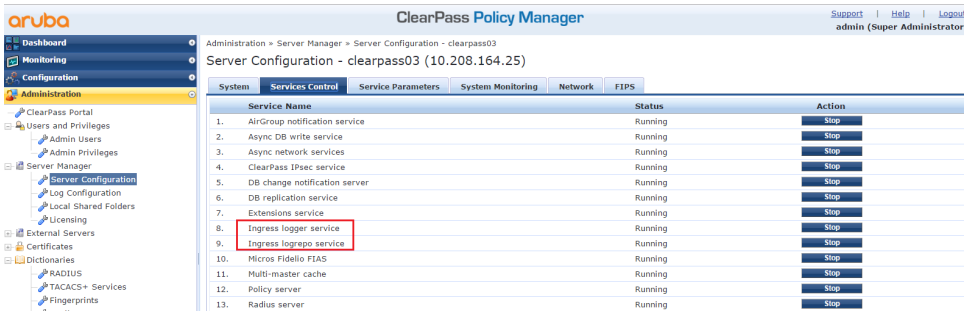


b. Navigate to Administration > Dictionaries > Ingress Events, and click on the relevant dictionary to enable it.

   For this example, select **Juniper-SRX-Traditional-Syslog-RT_SCREEN_IP**.



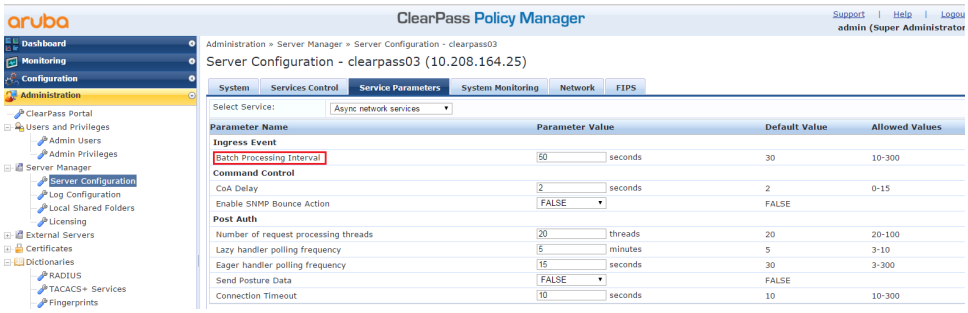
c. Navigate to Administration > Server Manager > Server Configuration, and on the Services Control tab ensure **Ingress logger service** and **Ingress logrepo service** are running.



3. Adjust the batch processing interval.

   Navigate to Administration > Server Manager > Server Configuration, and on the Service Parameters tab set the Batch Processing Interval value to **50** seconds.

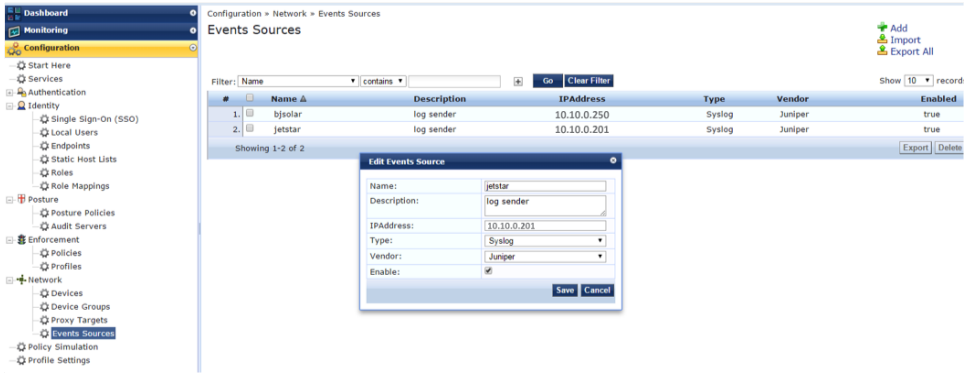
NOTE: The batch processing interval determines the frequency at which the Event Engine checks the event database for new entries. On older hardware, the default of 30 seconds might need to be increased (as has been done in this example).



4. Add the SRX650 device as an event source.

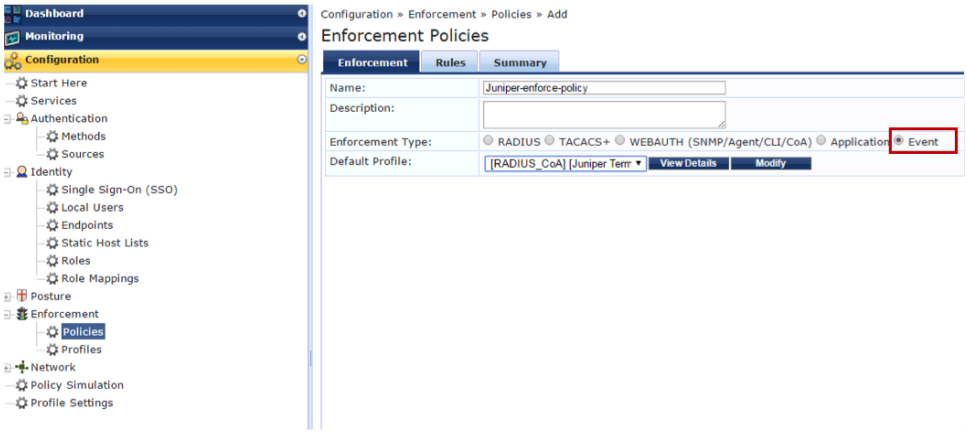
   Navigate to Configuration > Network > Event Sources, and configure an Events Source with the parameters as shown below.

   In this example, the log sender is **jetstar**. Select **Juniper** as the Vendor.

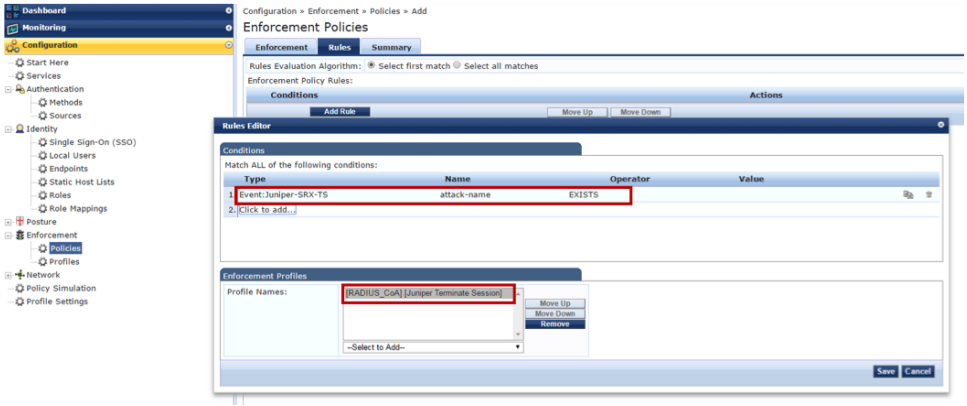


5. Create an enforcement policy to monitor incoming log events from the SRX650 device, and take specific action when certain conditions are met.

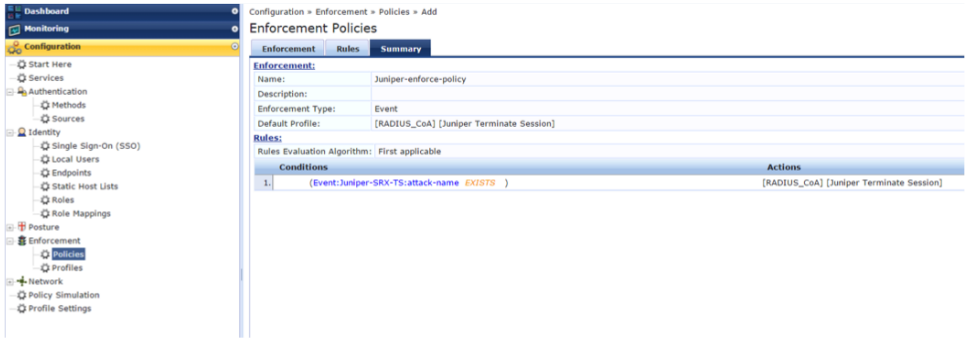
   a. Navigate to Configuration > Enforcement > Policies and add a new enforcement policy. On the Enforcement tab, set the Enforcement Type to **Event**.



b. On the Rules tab, click **Add Rule**. Create a Condition **Event:Juniper-SRX-TS:attack-name "EXISTS"** and select the Enforcement Profile **Juniper Terminate Session**.



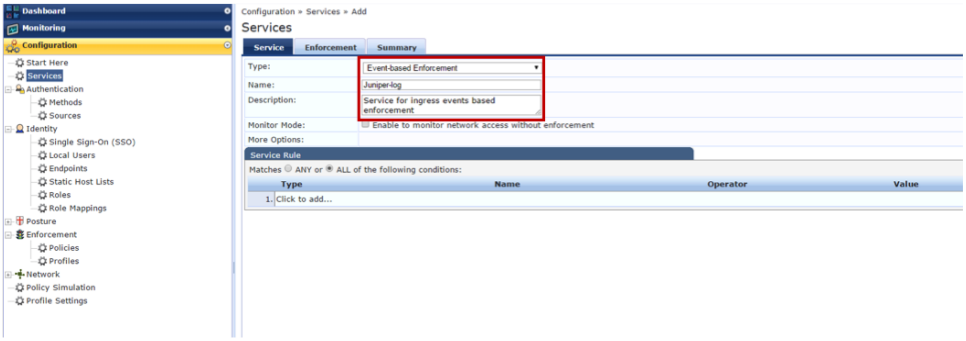
c. On the Summary tab, review and save the configuration.



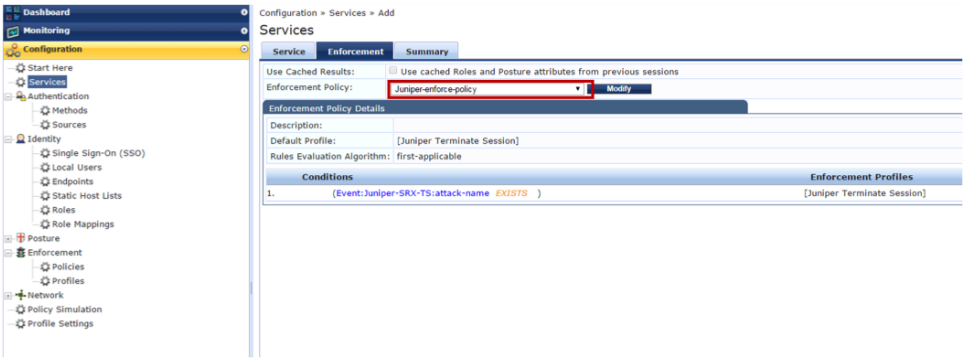
6. Create a new event service and bind the enforcement policy to the service.

a. Navigate to Configuration > Services, and on the Service tab add new a service with Type **Event-based Enforcement**.

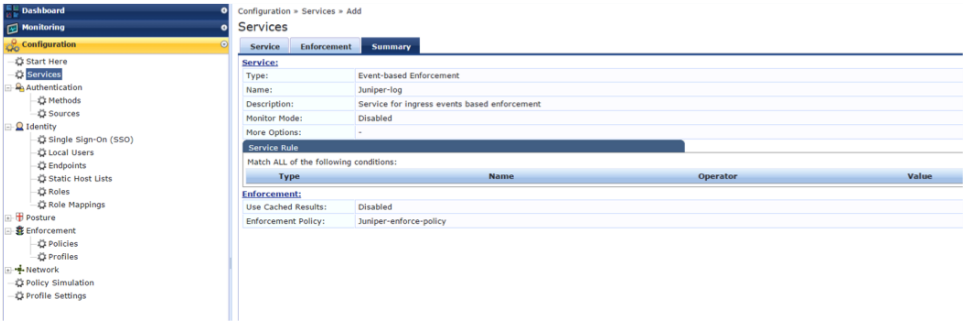
   In this example, the service is named **Juniper-log**.



b. On the Enforcement tab, select the Enforcement Policy **Juniper-enforce-policy** to bind it to the service.

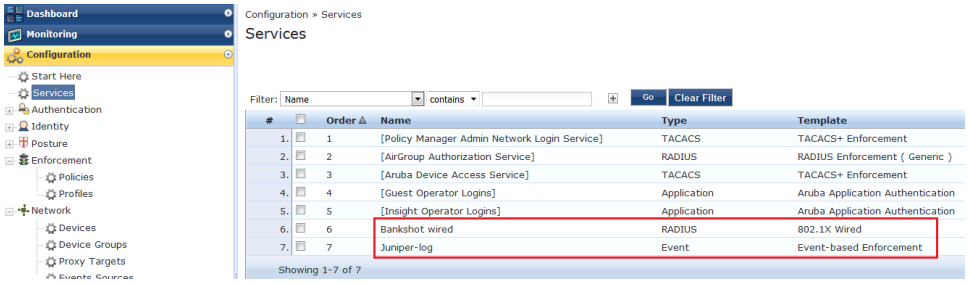


c. On the Summary tab, review and save the configuration.



d. Verify that the new service has been added to the system.

   On the Configuration > Services page, verify that the new **Juniper-log** service appears at the bottom of the services list.



NOTE: The **Bankshot wired** (802.1X Wired) service was configured in the Example 1 section "Configuring Aruba ClearPass Policy Manager" on page 15. It is required for this example, as CPPM needs to be aware of new user connections in order to be able to take action on them.

Verification

Confirm that the configuration is working properly.

Verifying User Authentication

Purpose Verify that user test1 on Endpoint 1 has successfully authenticated with the various network elements.

Action

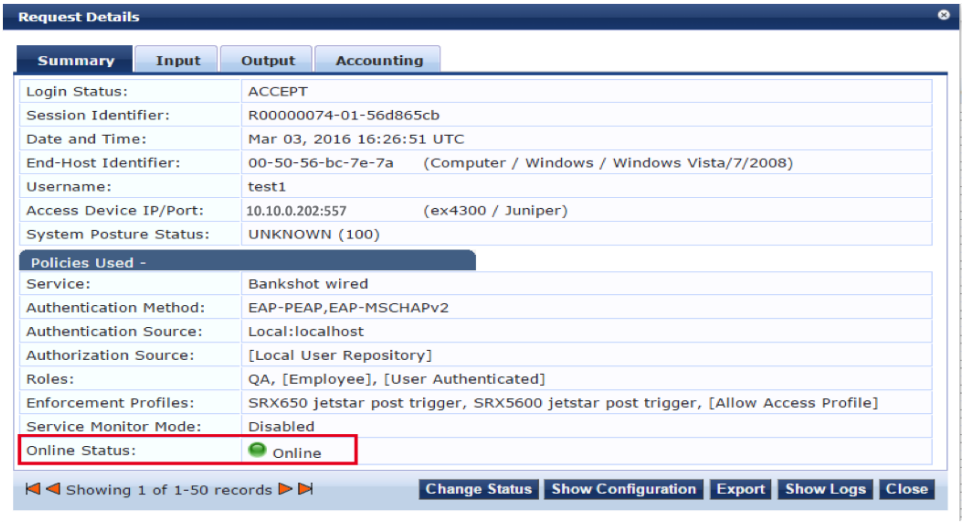
1. On the EX4300 switch, verify that user test1 is authenticated through 802.1X.

```
user@host> show dot1x interface ge-0/0/1
802.1X Information:
Interface     Role          State          MAC address          User
ge-0/0/1.0    Authenticator Authenticated  00:50:56:BC:7E:7A    test1
```

2. In CPPM, verify that user test1 is authenticated.

   a. Navigate to Monitoring > Live Monitoring > Access Tracker, find the relevant RADIUS event and verify that user test1 has Login Status of **ACCEPT**.

   b. Click on the RADIUS event, and on the Summary tab that appears, verify that user **test1** with role **QA** has Login Status of **ACCEPT** and Online Status of **Online**. Note also that CPPM has enforced the **SRX650 jetstar post trigger** profile, which will send (post) the user information to the SRX650 device.



3. On the SRX650 device, verify that user test1's authentication information has been received from CPPM.

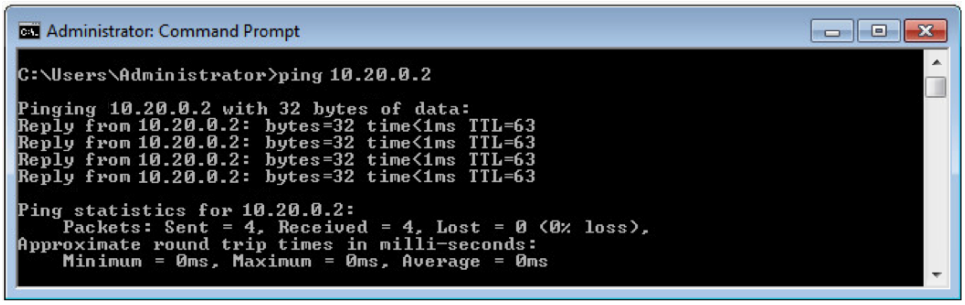
```
user@host> show services user-identification authentication-table authentication-source
aruba-clearpass extensive
Domain: GLOBAL
Total entries: 1
  Source-ip: 10.10.0.190
    Username: test1
    Groups:posture-unknown, qa, [employee], [user authenticated]
    Groups referenced by policy:qa
    State: Valid
    Source: Aruba ClearPass
    Access start date: 2000-01-01
    Access start time: 14:21:50
    Last updated timestamp: 2016-02-26 14:25:28
    Age time: 27
```

Meaning The user has successfully authenticated with all network elements.

Verifying User Access to the Protected Server

Purpose Verify that user test1 on Endpoint 1 can access the protected server under normal conditions.

Action From Endpoint 1, ping the protected server (10.20.0.2).



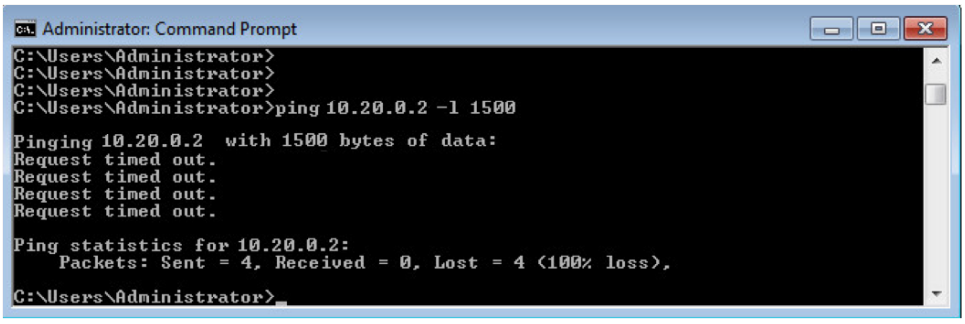
Meaning The user can successfully reach the protected server.

Verifying Detection and Protection of Unwanted Traffic

Purpose Verify that when user test1 on Endpoint 1 sends attack-type traffic towards the protected server, the network elements work together to protect the server.

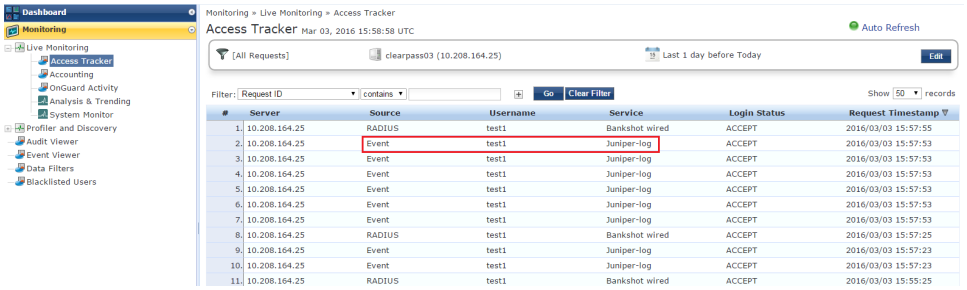
Action

1. From Endpoint 1, ping the protected server (10.20.0.2) again; however, this time specify a packet size large enough to cause the packets to be fragmented.

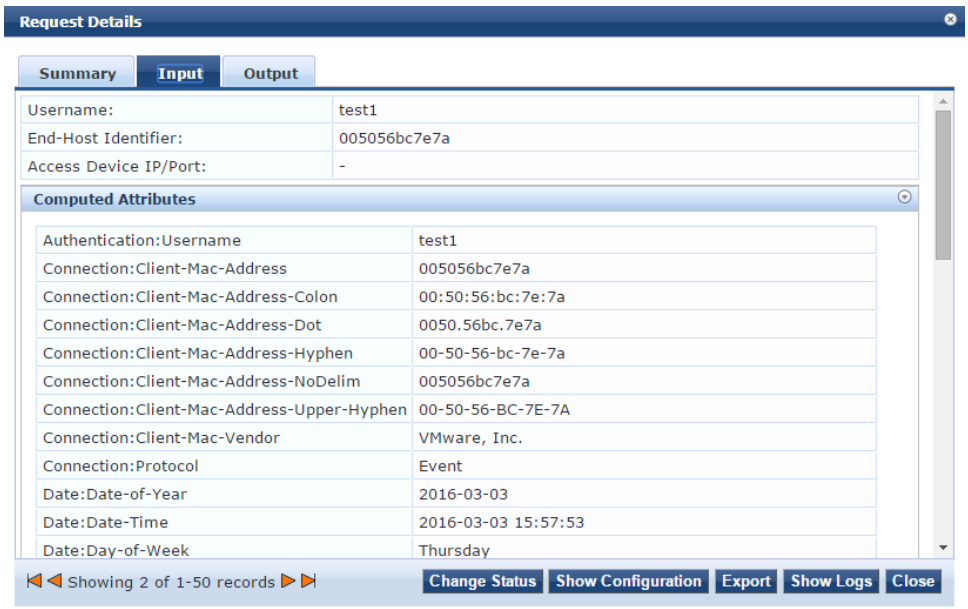


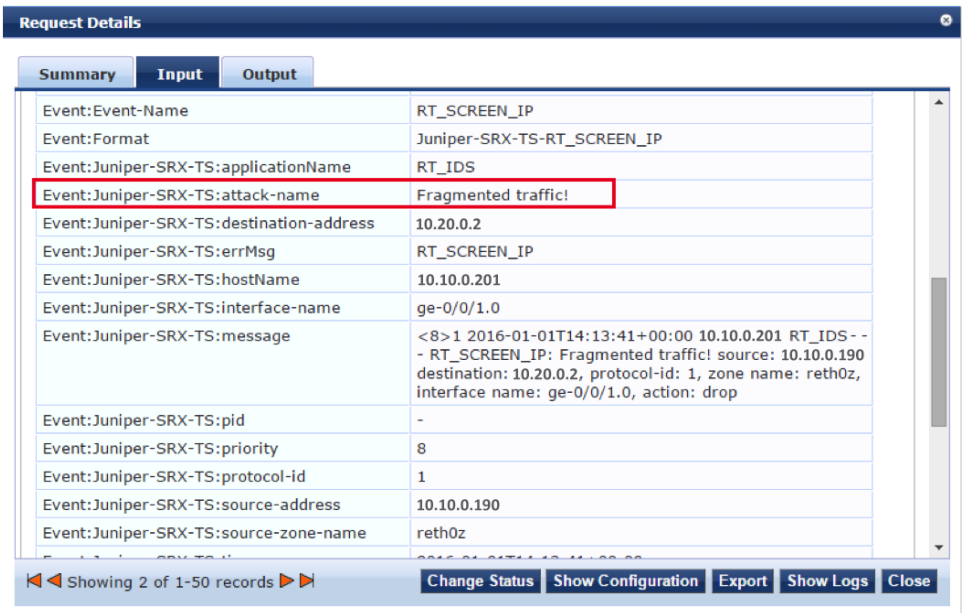
NOTE: Because the SRX650 device has a SCREEN option configured to detect and block IP fragments, the pings are timing out.

2. In CPPM, verify that the SRX650 device has detected the attack and sent event logs.
   a. Navigate to Monitoring > Access Tracker, and verify that CPPM has received the event.



b. Click on the event, and on the Input tab verify that the log information received from the SRX650 device includes information about fragmented packets.

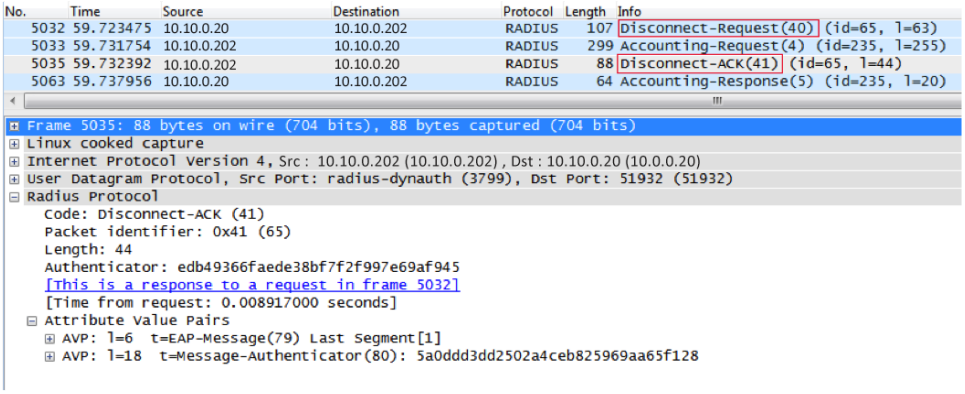




c. On the Summary tab for the event, verify that the Enforcement Profile now shows **Juniper Terminate Session**, and the user's Online Status now shows **Offline**.

NOTE: The Juniper Terminate Session profile triggers CPPM to send a request to the EX4300 switch to disconnect the user.

3. Using a packet capture tool, verify the exchange of RADIUS messages between the EX4300 switch and CPPM that result in the user being disconnecting from the network..



Meaning The SRX650 device, CPPM, and the EX4300 switch have communicated correctly to block and disconnect user test1 from the network.

Related Documentation

- Use Case Overview on page 6
- Technical Overview on page 7

