

# Junos<sup>®</sup> OS Release 12.3X48 Feature Guide

Junos OS Release 12.3X48  
2 May 2016  
Revision 3

This feature guide accompanies Junos OS Release 12.3X48-D30. This guide contains detailed information about new or enhanced functionality introduced in Junos OS Release 12.3X48-D30, Junos OS Release 12.3X48-D20, and Junos OS Release 12.3X48-D15 that is summarized in the Release Notes.

## Contents

New Features in Junos OS Release 12.3X48-D30 . . . . .	3
Integrated ClearPass Authentication and Enforcement . . . . .	3
Understanding SRX Series Integrated ClearPass Authentication and Its Component Functions . . . . .	3
Integrated ClearPass Authentication and Enforcement Examples . . . . .	25
Integrated ClearPass Authentication and Enforcement CLI Configuration Statements . . . . .	64
Integrated ClearPass Authentication and Enforcement CLI Operational Commands . . . . .	184
New Features in Junos OS Release 12.3X48-D20 . . . . .	205
Interfaces and Routing . . . . .	205
CLI Enhancement for Interfaces Operational Command . . . . .	205
Screens . . . . .	206
Logging and Trapping . . . . .	206
System Log Message . . . . .	210
Security Policies . . . . .	210
Setting TCP MSS per Policy . . . . .	211
VPNs . . . . .	220
AutoVPN Spokes and Auto Discovery VPN (ADVPN) Partners on High-End SRX Series Devices . . . . .	221
IKEv2 AES-GCM for Branch SRX Series and SRX5600 and SRX5800 Devices With Next-Generation Services Processing Card . . . . .	243
New Features in Junos OS Release 12.3X48-D15 . . . . .	252
Application Layer Gateways (ALGs) . . . . .	252
Scaling BLF Support for the UDP-Based SIP ALG . . . . .	252
464XLAT ALG Traffic Support . . . . .	253
Building Blocks . . . . .	259
Security Policies . . . . .	259

Intrusion Detection and Prevention . . . . .	262
Pattern Matching Engine . . . . .	262
System Log Message . . . . .	266
Documentation Feedback . . . . .	266
Requesting Technical Support . . . . .	267
Self-Help Online Tools and Resources . . . . .	267
Opening a Case with JTAC . . . . .	267
Revision History . . . . .	268

## New Features in Junos OS Release 12.3X48-D30

---

Junos OS Release 12.3X48-D30 introduces the integrated ClearPass authentication and enforcement feature.

- [Integrated ClearPass Authentication and Enforcement on page 3](#)

### Integrated ClearPass Authentication and Enforcement

Coverage of the new integrated ClearPass authentication and enforcement feature is organized into the following sections in this guide:

- [Understanding SRX Series Integrated ClearPass Authentication and Its Component Functions on page 3](#)
- [Integrated ClearPass Authentication and Enforcement Examples on page 25](#)
- [Integrated ClearPass Authentication and Enforcement CLI Configuration Statements on page 64](#)
- [Integrated ClearPass Authentication and Enforcement CLI Operational Commands on page 184](#)

### Understanding SRX Series Integrated ClearPass Authentication and Its Component Functions

---

- [Understanding the SRX Series Integrated ClearPass Authentication and Enforcement Feature on page 4](#)
- [SRX Series Supported Platforms for the Integrated ClearPass Authentication and Enforcement Feature on page 6](#)
- [Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API on page 7](#)
- [Understanding Enforcement of ClearPass User and Group Authentication on the SRX Series Devices on page 10](#)
- [Understanding the Integrated ClearPass Authentication and Enforcement User Query Function on page 19](#)
- [Understanding How the Integrated ClearPass Feature Detects Threats and Attacks and Notifies the CPPM on page 21](#)
- [SRX Series Threat and Attack Logs Sent to Aruba ClearPass on page 23](#)

***Understanding the SRX Series Integrated ClearPass Authentication and Enforcement Feature***

This topic introduces the SRX Series integrated ClearPass authentication and enforcement feature in which the SRX Series device and Aruba ClearPass collaborate to protect your network resources by enforcing security at the user identity level and controlling user access to the Internet. The ClearPass Policy Manager (CPPM) can authenticate users across wired, wireless, and VPN infrastructures. The integrated ClearPass feature allows the CPPM and the SRX Series device to collaborate in multiple environments in which they are deployed together.

- [Why You Need to Protect Your Environment With the SRX Series Integrated ClearPass Authentication and Enforcement Feature on page 4](#)
- [How the SRX Series Integrated ClearPass Authentication and Enforcement Feature Can Protect Your Network Environment on page 5](#)

***Why You Need to Protect Your Environment With the SRX Series Integrated ClearPass Authentication and Enforcement Feature***

The proliferation of mobile devices and cloud services and 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. The integrated ClearPass feature protects against malicious intrusions introduced through use of mobile devices and multiple concurrently connected devices.

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 improved advantage in identifying the source of the attack and stemming future potential attacks that follow the same strategy.

Attackers can gain access to nearby company-owned mobile devices and install malware on them that they can then use to capture data at any time. Whether reconnaissance or malicious, attacks against network resources are commonplace in today's computing environment. Attackers can launch information-gathering ventures, stop business activity, and steal sensitive corporate data.

Today's network environments are more open to attacks of various kinds because they support *anywhere, anytime, any device* access, to a greater or lesser degree, and they allow a user to use multiple concurrently network-connected devices.

The SRX Series integrated ClearPass authentication and enforcement feature can protect you against attacks and intrusions by allowing you to configure security policies that identify users by their usernames or by the groups that they belong to. It also identifies threats and attacks perpetrated against your network environment and provides this information to the CPPM. As administrator of the CPPM, you can better align your security enforcement to protect against possible future attacks of the same kind. If a user is logged in to the network with more than one device, you can keep track of their activity based on their identity, not only by their devices, and you can more easily control their network access and any egregious activity on their behalf, whether intended or not.

***How the SRX Series Integrated ClearPass Authentication and Enforcement Feature Can Protect Your Network Environment***

The SRX Series integrated ClearPass authentication and enforcement feature gives you granular control at the user level, not the device's IP address, over user access to protected resources and the Internet. As administrator of the SRX Series device, you can now specify in the source-identity parameter of *identity-aware* security policies a username or a role (group) name that the CPPM posts to the SRX Series device. You are no longer restricted to relying solely on the IP address of the device as a means of identifying the user. Honing in on the user of the device, rather than only the device, enhances your control over security enforcement.

In addition to providing the SRX Series device with authenticated user information, the 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*.

For example, suppose that the administrator of the CPPM configured a role called marketing-company-device and mapped to that role both company devices and members of the Marketing department. As administrator of the SRX Series device, you could specify that role in a security policy as if it were a group. The security policy would then apply to all users mapped to the role, inherently controlling their network activity when they use that type of device type.

The SRX Series integrated ClearPass feature delivers the protection of the SCREENS, IDP and UTM features to defend your network against a wide range of attack strategies. In addition to protecting the company's network resources, the SRX Series device can make available to the CPPM log records generated by these protective security features in response to attack or attack threats. Knowing about threats and specific attacks that have already occurred can help IT departments to identify noncompliant systems and exposed areas of the network. With this information, they can harden their security by enforcing device compliance and strengthening protection of their resources.

SRX Series 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 the CPPM. The CPPM acts as the authentication source. It uses its own internal RADIUS server to authenticate users. It can also rely on an external authentication source to perform the authentication for it, such as an external RADIUS server or Active Directory.

The CPPM authentication is triggered by requests from NAS devices such as switches and access controllers. The CPPM uses the XML portion of the RESTful Web services that the SRX Series device exposes to it to send in POST request messages to the SRX Series device authenticated user identity and device posture information.

The SRX Series device and Aruba ClearPass simplify the complex and complicated security tasks required to safeguard company resources and enforce Internet access policy for mobile devices. This security is essential in a network environment that supports the mobile experience and that gives the user latitude to use a wide range of devices, including their own systems, smartphones, and tablets.

- Related Documentation**
- [Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API on page 7](#)
  - [Understanding Enforcement of ClearPass User and Group Authentication on the SRX Series Devices on page 10](#)
  - [Example: Configuring the SRX Series Integrated ClearPass Feature to Allow the Device to Receive User Authentication Data from ClearPass on page 25](#)
  - [Example: Enforcing SRX Series Security Policies Using Aruba ClearPass as the Authentication Source on page 34](#)

***SRX Series Supported Platforms for the Integrated ClearPass Authentication and Enforcement Feature***

The integrated ClearPass authentication and enforcement feature is supported on the following SRX Series devices:

- SRX100H2, SRX110H2, SRX210H2
- SRX220H2, SRX240H2
- SRX550, SRX650
- SRX1400
- SRX3400, SRX3600
- SRX5400, SRX5600, SRX5800

- Related Documentation**
- [Understanding the SRX Series Integrated ClearPass Authentication and Enforcement Feature on page 4](#)
  - [Example: Configuring the SRX Series Integrated ClearPass Feature to Allow the Device to Receive User Authentication Data from ClearPass on page 25](#)
  - [Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API on page 7](#)
  - [Understanding Enforcement of ClearPass User and Group Authentication on the SRX Series Devices on page 10](#)

### ***Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API***

The integrated ClearPass authentication and enforcement feature enables the SRX Series device and Aruba ClearPass to collaborate in protecting your company's resources by enforcing security at the user identity level in environments in which they are deployed together. The ClearPass Policy Manager (CPPM) can authenticate users across wired, wireless, and VPN infrastructures and post that information to the SRX Series device, which, in turn, uses it to authenticate users requesting access to your protected resources and to the internet. The SRX Series device can provide the CPPM with threat and attack logs associated users' devices so that you can better harden your security at the ClearPass end.

- [Web API on page 7](#)
- [ClearPass Authentication Table on page 7](#)
- [Using HTTPS or HTTP for the Connection Protocol Between ClearPass and the SRX Series Device on page 8](#)
- [Ensuring the Integrity of Data Sent from ClearPass to the SRX Series Device on page 8](#)
- [Data Size Restrictions and Other Constraints on page 8](#)
- [Posture States and the Posture Group on page 9](#)

#### **Web API**

The SRX Series device exposes to the CPPM its Web API daemon (webapi) interface that enables the CPPM to integrate with it and efficiently send authenticated user identity information to the SRX Series device. The SRX Series Web API daemon acts as an HTTP server in that it implements part of the RESTful Web services that supports concurrent HTTP and HTTPS requests. In this relationship, the CPPM is the client. The Web API daemon is restricted to processing only HTTP/HTTPS requests. Any other type of request it receives generates an error message.



**WARNING:** If you are deploying the integrated ClearPass Web API function and Web-management at the same time, you must ensure that they use different HTTP or HTTPS service ports.

However, for security considerations, we recommend that you use HTTPS instead of HTTP. HTTP is supported primarily for debugging purposes.

The Web API daemon runs on the master Routing Engine in a chassis cluster environment. After an HA switchover, the daemon will start automatically on the new master Routing Engine. It has no effect on the Packet Forwarding Engine.

#### **ClearPass Authentication Table**

After the SRX Series device receives information posted to it from the CPPM, the SRX Series device extracts the user authentication and identity information, analyzes it, and distributes it to the appropriate processes for handling. The SRX Series device creates a ClearPass authentication table on the Packet Forwarding Engine side to hold this user information. When the SRX Series device receives the information sent to it from

ClearPass, the SRX Series device generates entries in the ClearPass authentication table for the authenticated users. 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 security policy that matches the traffic from the user.

#### ***Using HTTPS or HTTP for the Connection Protocol Between ClearPass and the SRX Series Device***

When you configure the SRX Series Web API, you specify a certificate key if you are using HTTPS as the connection protocol. To ensure security, the HTTPS default certificate key size is 2048 bytes. If you do not specify a certificate size, the default size is assumed. There are three methods that you can use to specify a certificate:

- Default certificate
- Certificate generated by PKI
- Custom certificate and certificate key

The SRX Series Web API supports only the Privacy-Enhanced Mail (PEM) format for the certificate and certificate key configuration.

If you enable the Web API on the default ports—HTTP (8080) or HTTPS (8443)—you must enable host inbound traffic on the ports. If you enable it on any other TCP port, you must enable host inbound traffic specifying the parameter **any-service**. For example:

```
user@host# set security zones security-zone trust host-inbound-traffic system-services  
any-service
```

#### ***Ensuring the Integrity of Data Sent from ClearPass to the SRX Series Device***

The following requirements ensure that the data sent from the CPPM is not compromised:

- The Web API implementation is restricted to processing only HTTP/HTTPS POST requests. Any other type of request that it receives generates an error message.
- The Web API daemon analyzes and processes HTTP/HTTPS requests from only the following dedicated URL:  
`/api/userfw/v1/post-entry`
- The HTTP/HTTPS content that the CPPM posts to the SRX Series device must be consistently formatted correctly. The correct XML format indicates a lack of compromise, and it ensures that user identity information is not lost.

#### ***Data Size Restrictions and Other Constraints***

The following data size restrictions and limitations apply to the CPPM:

- The CPPM must control the size of the data that it posts. Otherwise the Web API daemon is unable to process it. Presently the Web API can process a maximum of 2 megabytes of data.
- The following limitations apply to XML data for role and device posture information. The Web API daemon discards XML data sent to it that exceeds these amounts (that is, the overflow data):
  - The SRX Series device can process a maximum of 209 roles.



- The SRX Series device supports only one type of posture with six possible posture tokens, or values. Identity information for an individual user can have only one posture token.



**NOTE:** The CPPM checks the health and posture of a device and it can send that information to the SRX Series device as part of the user information that it posts. You cannot define posture on the SRX Series device. Also, the SRX Series device does not check posture information that it receives.

### ***Posture States and the Posture Group***

User, role, and posture token fields are distinct in the context of the CPPM. Each set of user identity information contains user and role (group) identity and a posture token. Because the SRX Series device supports only user and role (group) fields, the posture token value is mapped to a role by adding the prefix **posture-**. You can then use that role in a security policy as a group and that policy will be applied to all traffic that matches the policy.

The predefined posture identity states are:

- posture-healthy (HEALTHY)
- posture-checkup (CHECKUP)
- posture-transition (TRANSITION)
- posture-quarantine (QUARANTINE)
- posture-infected (INFECTED)
- posture-unknown (UNKNOWN)

#### **Related Documentation**

- [Understanding the SRX Series Integrated ClearPass Authentication and Enforcement Feature on page 4](#)
- [Understanding Enforcement of ClearPass User and Group Authentication on the SRX Series Devices on page 10](#)
- [Example: Enforcing SRX Series Security Policies Using Aruba ClearPass as the Authentication Source on page 34](#)
- [Understanding the Integrated ClearPass Authentication and Enforcement User Query Function on page 19](#)

***Understanding Enforcement of ClearPass User and Group Authentication on the SRX Series Devices***

This topic describes how the SRX Series device enforces user and group authentication when a user attempts to access a resource. It also explains how the SRX Series device handles information in the ClearPass authentication table user entries when a security policy that references a group in a user entry is removed. Understanding that process will help you troubleshoot issues related to group identity and give you insight into changes in the ClearPass authentication table user entries.

- [Understanding How the SRX Series Device Manages the ClearPass Authentication Table on page 10](#)
- [User Authentication Entries in the ClearPass Authentication Table on page 10](#)
- [Communication Between ClearPass and the SRX Series Device on page 13](#)
- [Understanding Domains and Interested Groups on page 15](#)
- [When a User Has Already Been Authenticated By Another Source on page 18](#)

***Understanding How the SRX Series Device Manages the ClearPass Authentication Table***

The integrated ClearPass authentication and enforcement feature enables the SRX Series device and the Aruba ClearPass Policy Manager (CPPM) to collaborate in protecting your company's resources. It enables the SRX Series device to apply firewall security policies to user traffic and to control user access to protected resources based on user or group identity. To ensure the identity of the user, the SRX Series device relies on authenticated user information that it receives from the CPPM.

It is useful to understand how the SRX Series device gets authenticated user identity information from the CPPM, generates entries in its ClearPass authentication table, and manages those entries in relation to security policies and user events. Understanding these processes will help you to quickly identify and resolve related problems.

This topic focuses on:

- How the SRX Series device obtains user identity information from the CPPM and manages it, and how you can use this information in security policies.
- How security policies that reference a group as the source (source-identity) have bearing on the groups listed in user entries in the ClearPass authentication table. Groups that are referenced by security policies are referred to as *interested groups*.

***User Authentication Entries in the ClearPass Authentication Table***

In their collaboration, ClearPass acts as the authentication source for the SRX Series device. The CPPM sends to the SRX Series device identity information about users that it has authenticated. The UserID daemon process in the SRX Series device receives this information, processes it, and synchronizes it to the Packet Forwarding Engine side in the independent ClearPass authentication table that is generated for this purpose.

As administrator of the SRX Series device, you can use the authenticated user identity information in security policies to control access to your protected resources and the Internet.

The collection of user identity information that the SRX Series device obtains from the CPPM and uses to create entries in its global routing engine authentication table that is synchronized to its individual ClearPass authentication table is referred to as a mapping, or, more commonly, an IP-user mapping because the username and the related group list are mapped to the IP address of the user's device.



**NOTE:** For each user authentication entry in the ClearPass authentication table, a group list identifies the groups that a user belongs to in addition to other information such as the posture token which indicates state of the device, such as whether it is healthy.

You can use a username or a group name in security policies to identity a user and not rely directly on the IP address of the device used, because the IP address of the device is tied to the username and its groups in the ClearPass authentication table entry.



**NOTE:** For each user entry, the number of groups, or roles, in the entry cannot exceed 200. After the capacity is reached, additional roles are discarded and the following syslog message is sent.

```
userid_get_and_check_adauth_num: src_ip ip-address user domain:user  
dropped.record numrecord-number has arrived max num of db
```

The CPPM posts user information to the SRX Series device in the following format. The SRX Series device does not use all of this information.

```
<userfw-entries>  
  <userfw-entry>  
    <source>Aruba ClearPass</source>  
    <timestamp>2016-01-29T03:18:10Z</timestamp>  
    <operation>login</operation>  
    <IP>4.0.0.110</IP>  
    <domain>my-company-domain</domain>  
    <user>user1</user>  
    <role-list>  
      <role>human-resources-grp</role>  
      <role>[User Authenticated],/role>  
    </role-list>  
    <posture>HEALTHY</posture>  
    <device_category>Computer</device_category>  
  </userfw-entry>  
</userfw-entries>
```

Here is the format for a ClearPass authentication table entry for a user, followed by an example entry and a description of its components.

*IP-address, domain, user, user-group-list*

In the following example, the user belongs to two groups, the human-resources-grp group and the posture-healthy group. The SRX Series device converts the posture information from the CPPM to a group name. You might configure a security policy that allows all users access to the marketing server if their devices belong to the posture-healthy group (role).

192.168.0.2, my-company-domain, lin, human-resources-grp, posture-healthy

- IP address

This is the IP address of the device used.

- The name of the domain that the user belongs to.

In this example, the domain name is "my-company-domain." The default domain name GLOBAL is used if a domain name is not provided.

- The username

The username is the user's login name used to connect to the network, which, in this example, is lin.

This name is constant regardless of the device used.

When you configure a security policy whose source-identity tuple identifies the source of the traffic by username or group name, not by the IP address of the device used, it is as if the security policy were device independent; it applies to the user's activity regardless of the device used.

- One or more groups that a user belongs to

It is here where the concept of *interested groups* and their relationship to security policies comes into play. An interested group is a group that is referenced in a security policy. The concept of interested groups is covered later in this topic.

Note that if a user is connected to the network using multiple devices, there might be more than one IP-user mapping for that user. Each mapping would have its own set of values—that is, domain name and group-list—in conjunction with the username and IP address.

For example, the following three IP address-to-username mappings might exist for the user abe who is connected to the network using three separate devices:

110.208.132.23 abe, marketing-grp, posture-healthy

192.168.1.1 abe, marketing-grp, posture-transition

202.38.11.33 abe, marketing-grp, posture-unknown

Assume that the SRX Series device receives a logout message for 110.208.132.23, abe.

The following partial user authentication entry shows that the user abe is now logged in to the network using only two devices:

192.168.1.1 abe, marketing-grp, posture-transition

202.38.11.33 abe, marketing-grp, posture-unknown

### Communication Between ClearPass and the SRX Series Device

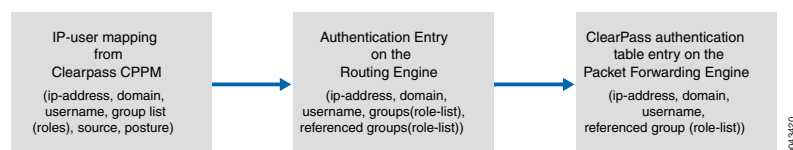
Here is a summary of how the SRX Series device and ClearPass communicate:

- A user joins the company network via a wired or wireless LAN.
- The CPPM authenticates the user.
- The CPPM initiates a secure connection with the SRX Series device using the integrated Web API.
- The SRX Series UserID daemon gets the full IP-user mapping from the CPPM. For each authenticated user, the UserID daemon generates an entry in the Routing Engine authentication table.

The Routing Engine authentication table is common in that it holds authentication entries based on information from other authentication sources in addition to ClearPass. For example, it might also hold entries for users authenticated by Microsoft Active Directory.

- The UserID daemon synchronizes the user authentication information from the Routing Engine authentication table to the ClearPass authentication table on the Packet Forwarding Engine. The ClearPass authentication table is dedicated to holding only ClearPass authentication information. See [Figure 1 on page 13](#).

**Figure 1: User Information from the CPPM to the SRX Series Device Routing Engine Synchronized to the ClearPass Authentication Table**



The SRX Series device uses the authenticated user identity information in the following process. When a user attempts to access an internal, protected resource or the Internet, the SRX Series device:

- Checks the traffic generated by the user for a matching security policy. The source traffic must match all of the tuples specified in the security policy. The match includes the source-identity field, which specifies a username or a group name.

To identify a match, the SRX Series device compares the username or the group name with the source-identity specification that is configured in a security policy, along with all other security policy values.

- Checks the ClearPass authentication table for an authentication entry for the user, if a security policy match was found.

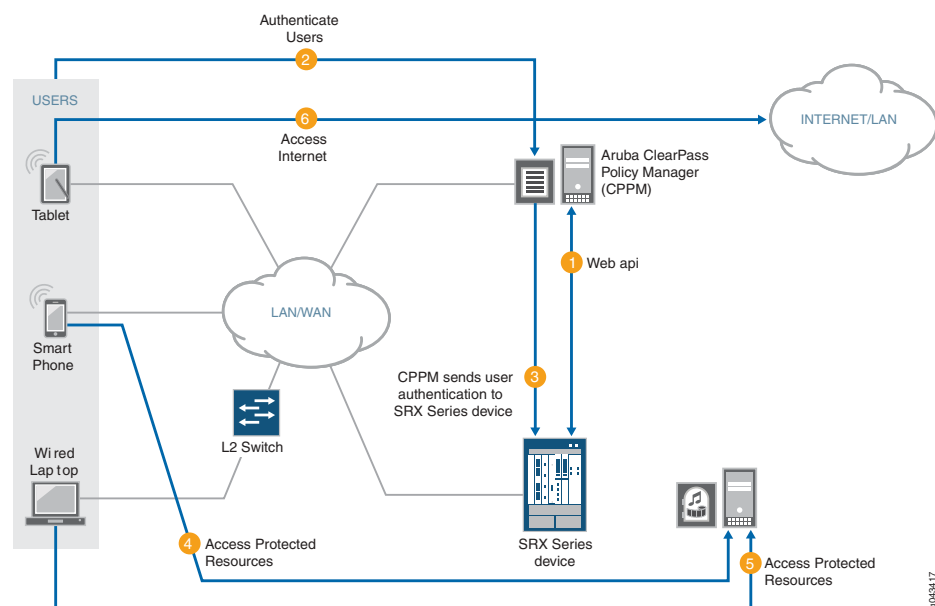
If it does not find an entry in the ClearPass authentication table, the SRX Series device checks other local authentication tables, in the order that you specified, until a match is found. However, it does not check other local authentication tables if the user query function is configured. See [“Understanding the Integrated ClearPass Authentication and Enforcement User Query Function” on page 19](#).



**NOTE:** The SRX Series device can query the CPPM for individual user information, under certain circumstances, when it has not already received that information from the CPPM. This feature is referred to as user query.

Figure 2 on page 14 illustrates the connection and communication between the SRX Series device and the CPPM. It also shows the paths entailed in authenticating users and allowing them access to the Internet and internal, protected resources.

**Figure 2: ClearPass and SRX Series Device Communication and User Authentication Process**



As Figure 2 on page 14 depicts, the following activity takes place:

1. The CPPM initiates a secure connection with the SRX Series device using the Web API.
2. Three users join the network and are authenticated by the CPPM.
  - A tablet user joins the network across the corporate WAN.
  - A smartphone user joins the network across the corporate WAN.
  - A wireless laptop user joins the network from a wired laptop connected to a Layer 2 switch that is connected to the corporate LAN.
3. The CPPM sends the user authentication and identity information for the users who are logged in to the network to the SRX Series device in POST request messages using the Web API.

When traffic from a user arrives at the SRX Series device, the SRX Series device:

- Identifies a security policy that the traffic matches.

- Locates an authentication entry for the user in the ClearPass authentication table.
  - Applies the security policy to the traffic after authenticating the user.
4. Traffic from the smartphone user who is requesting access to an internal, protected resource arrives at the SRX Series device. Because all of the conditions identified in Step 3 are met and the security policy permits it, the SRX Series device allows the user connection to the protected resource.
  5. Traffic from the wired laptop user who is requesting access to a protected resource arrives at the SRX Series device. Because all of the conditions identified in Step 3 are met and the security policy permits it, the SRX Series device allows the user connection to the resource.
  6. Traffic from the tablet user who is requesting access to the Internet arrives at the SRX Series device. Because all of the conditions identified in Step 3 are met and the security policy permits it, the SRX Series device allows the user connection to the Internet.

### ***Understanding Domains and Interested Groups***

How the user identity group information is managed on the SRX Series device is dominated by two concepts:

- Domain group

The SRX Series device follows the usual course in regard to how it handles usernames in domain namespaces. It makes use of the namespace to distinguish names that are the same—such as **admin**—but that are from different sources and are in different domains. Because they belong to different domains, the names are not in conflict.

Any group that is part of an IP-user mapping will always belong to a domain, whether that domain is a specific domain or the GLOBAL domain. If a domain name is not specified in the IP-user mapping, then the GLOBAL domain is assumed.

[Table 1 on page 15](#) illustrates how the domain for a group is determined, based on the IP-user mapping information obtained from the CPPM.

**Table 1: Assigning a Domain to a Group**

Does the IP-User Mapping Contain a Domain Name?	What Domain Is Applied to the Group?
<p>No</p> <p>For example:</p> <p>IP, , user1, group-list</p> <p>The second comma serves as a placeholder for the domain name and the GLOBAL domain is applied.</p>	<p>Groups included in group-list belong to the GLOBAL domain.</p>

Table 1: Assigning a Domain to a Group (*continued*)

Does the IP-User Mapping Contain a Domain Name?	What Domain Is Applied to the Group?
<p>Yes</p> <p>For example:</p> <p>IP, domain1, user1, group-list</p> <p><b>NOTE:</b> In this example, the IP-user mapping specifies the domain name as domain1.</p>	<p>The domain name, domain1, is included in the IP-user mapping from the CPPM, and it is used. It is retained in the entry for the authenticated user in the ClearPass authentication table on the Packet Forwarding Engine.</p>

- Interested group

A group qualifies as an *interested group* if it is referenced by a security policy—that is, if it is specified in a policy's source-identity field. On the Routing Engine authentication table, each user entry contains a group referenced by a policy list that identifies the names of the groups for which a security policy exists. If a group included in a user entry is not currently used in a security policy, it is not included in this list. A group can move in and out of the groups referenced by a policy list.

- Interested group lists

An interested group list, or a list of groups referenced by policies, is a subset of overall groups. It is the intersection of the group list in a user authentication entry and the source-identity list for security policies. That is, any group included in a ClearPass authentication table user entry qualifies as an interested group. The Routing Engine synchronizes to the user entry in the ClearPass authentication table on the Packet Forwarding Engine only those groups that are referenced by security policies.

Here is how it works:

- The UserID daemon gets the full IP-user role (group) mapping from the CPPM.
- For each group, the UserID daemon identifies whether it is an interested group by determining if there is a security policy that references it. Any qualifying groups are included in the groups referenced by a policy list on the Routing Engine. The UserID daemon synchronizes to the user entry in the ClearPass authentication table on the Packet Forwarding Engine interested groups along with the rest of the user authentication and identity information.

The interested groups list for a user entry on the Routing Engine can change, based on the following events:

- A new security policy is configured that references a group included in the user entry on the Routing Engine but that is not already in the entry's referenced groups list.
- A currently configured security policy that references a group in its source-identity is deleted.



Consider the following example:

- Assume that the CPPM posted the following information for two users to the SRX Series device:

```
10.1.1.1, abe, group1, group2, group3, group4, healthy
10.4.8.1, john, group1, group5, healthy
```

- After the SRX Series device maps the posture, defining it as a group, the two user entries in the SRX Series device Routing Engine authentication table appear as follows:

```
10.1.1.1, abe, group1, group2, group3, group4, posture-healthy
10.4.8.1, john, group1, group5, posture-healthy
```

- Assume that several security policies include source-identity fields that reference one of the following: group1, group3, posture-healthy.

The intersection of the preceding sets—the original group list and the list of security policies that refer to the groups—results in the following interested groups list:

- For the user john, the groups referenced by policy list includes group1 and posture-healthy.
- For the user abe, the groups referenced by policy list includes group1, group3, and posture-healthy.

Now suppose that the security policy whose source-identity field specified group1 was deleted. The groups referenced by policy lists for the user authentication entries for the two users—john and abe—would be changed, producing the following results:

- For the user John, the list would include only posture-healthy.
- For the user Abe, the list would include group3 and posture-healthy.

Table 2 on page 17 shows how a security policy that references a group affects the ClearPass authentication table. It also shows the effect on the ClearPass authentication table when a group is *not* referenced by a security policy, and therefore is not an interested group.

**Table 2: Interested Groups: Effect on the ClearPass Authentication Table**

Security Policies Configuration and Modification	Resulting Effect on ClearPass Authentication Table Packet Forwarding Engine Entries
<b>Case 1:</b>	
The SRX Series device gets the IP-user mapping for a user from the CPPM.	
None of the groups in the user mapping are referenced by security policies.	
IP-user mapping from the CPPM:	The user authentication entry written to the ClearPass authentication table in the Packet Forwarding Engine for this user does not contain any groups.
12.1.1.1, ,user1, g1, g2, g3, g4	12.1.1.1, ,user1

**Table 2: Interested Groups: Effect on the ClearPass Authentication Table  
(continued)**

Security Policies Configuration and Modification	Resulting Effect on ClearPass Authentication Table Packet Forwarding Engine Entries
<b>Case 2:</b>  The SRX Series device gets the IP-user mapping for a user from the CPPM. It checks the groups list against the security policies list and finds that two of the groups are referenced by security policies.	
IP-user mapping on the Routing Engine:  12.1.1.2, domain1, user2, g1, g2, g3, g4	The user authentication entry written to the ClearPass authentication table on the Packet Forwarding Engine for this user includes the following groups that are included in the groups referenced by the policy list on the Routing Engine:  12.1.1.2, domain1, user2, g2, g4

***When a User Has Already Been Authenticated By Another Source***

It can happen that the SRX Series device Routing Engine authentication table and the individual Packet Forwarding Engine Microsoft Active Directory table, for example, contain an entry for a user who was authenticated by Active Directory. As usual, the CPPM sends the IP-user mapping for the user to the SRX Series device. The SRX Series device must resolve the problem because its Routing Engine authentication table is common to both Active Directory and ClearPass.

Here is how the SRX Series device handles the situation:

- On the Routing Engine authentication table:
  - The SRX Series device overwrites the Active Directory authentication entry for the user in its common Routing Engine authentication table with the newly generated one from the IP-user mapping for the user from the CPPM.

There is now no IP address or username conflict.
- On the Packet Forwarding Engine:
  - The SRX Series device deletes the existing Active Directory authentication entry for the user from the Active Directory authentication table.

This will delete active sessions associated with the IP address.

  - The SRX Series device generates a new entry for the CPPM-authenticated user in the Packet Forwarding Engine ClearPass authentication table.

Traffic associated with the IP-user mapping entry will initiate new sessions based on user authentication in the ClearPass authentication table.

**Related  
Documentation**

- [Understanding the SRX Series Integrated ClearPass Authentication and Enforcement Feature on page 4](#)

- [Example: Enforcing SRX Series Security Policies Using Aruba ClearPass as the Authentication Source on page 34](#)
- [Example: Configuring the Integrated ClearPass Authentication and Enforcement User Query Function on page 52](#)

### ***Understanding the Integrated ClearPass Authentication and Enforcement User Query Function***

This topic focuses on how you can obtain user authentication and identity information for an individual user when that information is not posted directly to the SRX Series device by the ClearPass Policy Manager (CPPM).

The SRX Series integrated ClearPass authentication and enforcement feature allows the SRX Series device and Aruba ClearPass to control access to protected resources and the Internet from wireless and wired devices. For this to occur, ClearPass sends user authentication and identity information to the SRX Series device. The SRX Series device stores the information in its ClearPass authentication table. To send this information, usually the CPPM uses the Web API (webapi) services implementation, which allows it to make HTTP or HTTPS POST requests to the SRX Series device.

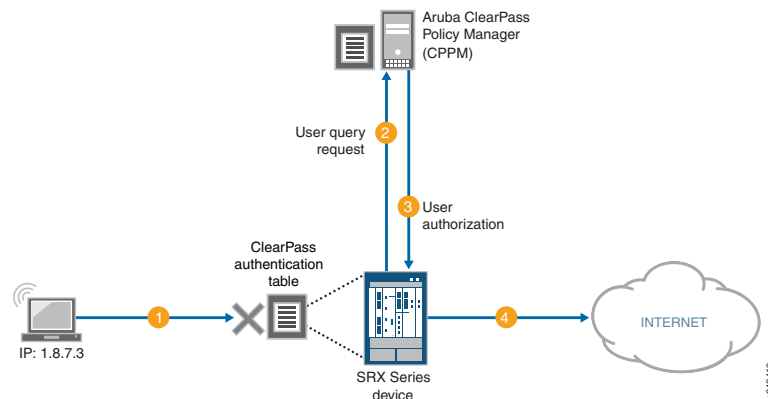
It can happen that the CPPM does not send user authentication information for a user, for various reasons. When traffic from that user arrives at the SRX Series device, the device cannot authenticate the user. If you configure the SRX Series device to enable the user query function, it can query the ClearPass webserver for authentication information for an individual user. The SRX Series device bases the query on the IP address of the user's device, which it obtains from the user's access request traffic.

If the user query function is configured, the query process is triggered automatically when the SRX Series device does not find an entry for the user in its ClearPass authentication table when it receives traffic from that user requesting access to a resource or the Internet. The SRX Series device does not search its other authentication tables. Rather, it sends a query to the CPPM requesting authentication information for the user.

[Figure 3 on page 20](#) depicts the user query process. In this example:

1. A user attempts to access a resource. The SRX Series device receives the traffic requesting access. The SRX Series device searches for an entry for the user in its ClearPass authentication table, but none is found.
2. The SRX Series device requests authentication for the user from the CPPM.
3. The CPPM authenticates the user and returns the user authentication and identity information to the SRX Series device.
4. The SRX Series device creates an entry for the user in its ClearPass authentication table, and grants the user access to the Internet.

Figure 3: The SRX Series ClearPass Integration User Query Function



You can control when the SRX Series device sends its requests automatically by configuring the following two mechanisms:

- The **delay-query-time** parameter

To determine the value to set for the **delay-query-time** parameter, it helps to understand the events and duration involved in how user identity information is transferred to the SRX Series device from ClearPass, and how the **delay-query-time** parameter influences the query process.

A delay is incurred from when the CPPM initially posts user identity information to the SRX Series device using the Web API to when the SRX Series device can update its local ClearPass authentication table with that information. The user identity information must first pass through the ClearPass device's control plane and the control plane of the SRX Series device. In other words, this process can delay when the SRX Series device can enter the user identity information in its ClearPass authentication table.

While this process is taking place, traffic might arrive at the SRX Series device that is generated by an access request from a user whose authentication and identity information is in transit from ClearPass to the SRX Series device.

Rather than allow the SRX Series device to respond automatically by sending a user query *immediately*, you can set a **delay-query-time** parameter, specified in seconds, that allows the SRX Series device to wait for a period of time before sending the query.

After the delay timeout expires, the SRX Series device sends the query to the CPPM and creates a pending entry in the Routing Engine authentication table. During this period, the traffic matches the default policy and is dropped or allowed, depending on the policy configuration.



**NOTE:** If there are many query requests in the queue, the SRX Series device can maintain multiple concurrent connections to ClearPass to increase throughput. However, to ensure that ClearPass is not stressed by these connections, the number of concurrent connections is constrained to no more than 20 ( $\leq 20$ ). You cannot change this value.

- A default policy, which is applied to a packet if the SRX Series device does not find an entry for the user associated with the traffic in its ClearPass authentication table.

The system default policy is configured to drop packets. You can override this action by configuring a default policy that specifies a different action to apply to this traffic.

Table 3 on page 21 shows the effect on the user query function in regard to whether or not Active Directory is enabled.

**Table 3: Relationship Between User Query Function and Active Directory Authentication as Processed by the CLI**

Active Directory Is Configured	ClearPass User Query Function Is Enabled	CLI Check Result
No	No	Pass
No	Yes	Pass
Yes	No	Pass
Yes	Yes	Fail

To avoid the failure condition reflected in the bottom row of the table, you must disable either Active Directory or the user query function. If both are configured, the system displays the following error message:

The priority of CP auth source is higher than AD auth source, and the CP user-query will shadow all AD features. Therefore, please choose either disabling CP user-query or not configuring AD.

#### Related Documentation

- [Example: Configuring the Integrated ClearPass Authentication and Enforcement User Query Function on page 52](#)
- [Understanding the SRX Series Integrated ClearPass Authentication and Enforcement Feature on page 4](#)
- [Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API on page 7](#)
- [Example: Configuring the SRX Series Integrated ClearPass Feature to Allow the Device to Receive User Authentication Data from ClearPass on page 25](#)

#### ***Understanding How the Integrated ClearPass Feature Detects Threats and Attacks and Notifies the CPPM***

The integrated ClearPass authentication and enforcement feature allows you to integrate your SRX Series device with the ClearPass Policy Manager (CPPM) to obtain authenticated user identity information. It also allows the SRX Series device to send attack and threat logs to the CPPM. This topic focuses on sending attack and threat logs to the CPPM.

When the SRX Series device features detect threat and attack events, the event is recorded in the SRX Series device event log. The SRX Series device uses syslog to forward the logs to the CPPM. The CPPM can evaluate the logs and take action based on matching

conditions. As administrator of ClearPass, you can use the information from the SRX Series device and define appropriate actions on the CPPM to harden your security.

Junos OS on the SRX Series device generates over 100 different types of log entries issued by more than 10 of its modules. Among the SRX Series device features that generate threat and attack logs are SCREENS, IDP, and UTM. To avoid overburdening the SRX Series device and the log server, the integrated ClearPass feature allows you to configure the SRX Series device to send to the CPPM only attack and threat log entries that were written to the event log in response to activity detected by the SCREENS, IDP, and UTM security features.

You can set the following conditions to control the log transmission:

- A log stream filter to ensure that only threat and attack logs are sent.
- A rate limiter to control the transmission volume. The SRX Series device log transmission will not exceed the rate-limiting conditions that you set.

For the CPPM to analyze the log information that the SRX Series sends to it, the content must be formatted in a standard, structured manner. The SRX Series log transmission follows the syslog protocol, which has a message format that allows vendor-specific extensions to be provided in a structured way.

Here is an example of an attack log generated by IDP:

```
<14>1 2014-07-24T13:16:58.362+08:00 bjsolar RT_IDP - IDP_ATTACK_LOG_EVENT
[junos@2636.1.1.1.2.86 epoch-time="1421996988" message-type="SIG"
source-address="4.0.0.1" source-port="32796" destination-address="5.0.0.1"
destination-port="21" protocol-name="TCP" service-name="SERVICE_IDP"
application-name="NONE" rule-name="1" rulebase-name="IPS" policy-name="idpengine"
export-id="4641"repeat-count="0" action="NONE" threat-severity="MEDIUM"
attack-name="FTP:USER:ROOT" nat-source-address="0.0.0.0" nat-source-port="0"
nat-destination-address="0.0.0.0" nat-destination-port="0" elapsed-time="0"
inbound-bytes="0" outbound-bytes="0" inbound-packets="0" outbound-packets="0"
source-zone-name="untrust" source-interface-name="ge-0/0/1.0"
destination-zone-name="trust" destination-interface-name="ge-0/0/7.0"
packet-log-id="0" alert="no" username="N/A" roles="N/A" message="-"]
```

[Table 4 on page 22](#) uses the content of this example IDP attack log to identify the parts of an attack log entry. See [“SRX Series Threat and Attack Logs Sent to Aruba ClearPass” on page 23](#) for further details on types of attack and threat logs.

**Table 4: Attack Log Fields Using Example Log**

Log Entry Component	Meaning	Format	Example
Priority	pri = LOG_USER + severity. Version is always 1	pri version	<14>1
Time and Time Zone	When the log was recorded and in what time zone.	y-m-dTh:m:s.ms+time zone <ul style="list-style-type: none"> <li>• y = year</li> <li>• m=month</li> <li>• d = day</li> <li>• T+hours</li> </ul>	2014-07-24T13:16:58.362+08:00

Table 4: Attack Log Fields Using Example Log (*continued*)

Log Entry Component	Meaning	Format	Example
Device/Host Name	Name of the device from which the event log was sent. This value is configured by the user.	string, <i>hostname</i>	bjsolar
Service Name	SRX Series feature that issued the event log.	string <i>service</i>	SERVICE_IDP
Application Name	Application that generated the log entry.	string <i>application-name</i>	NONE
PID	Process ID.  The process ID is not meaningful in this context, so <i>pid</i> is replaced by "-".  The value "-" is a placeholder for process ID.	<i>pid</i>	-
Errmsg Tag	Log ID name, error message tag.	string, <i>log-name and tag</i>	IDP_ATTACK_LOG_EVENT
Errmsg Tag Square Bracket	Log content enclosed in square brackets.	[ ]	-
OID	Product ID provided by the chassis daemon (chassisd).	junos@oid	junos@2636.1.1.1.2.86
Epoch Time	The time when the log was generated after the epoch.	<i>number</i>	1421996988

- Related Documentation**
- [SRX Series Threat and Attack Logs Sent to Aruba ClearPass on page 23](#)
  - [Understanding the SRX Series Integrated ClearPass Authentication and Enforcement Feature on page 4](#)
  - [Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API on page 7](#)
  - [Example: Configuring the Integrated ClearPass Authentication and Enforcement User Query Function on page 52](#)

#### ***SRX Series Threat and Attack Logs Sent to Aruba ClearPass***

The SRX Series integrated ClearPass authentication and enforcement feature collaborates with Aruba ClearPass in protecting a company's resources against potential and actual attacks through use of attack and threat event logs. These logs that are generated by the SRX Series SCREENS, IDP, and UTM components clearly identify the types of attacks and threats that threaten a company's network security.

The SRX Series device filters from the overall log entries the logs that report on threat and attack events, and it forwards these log entries to the ClearPass Policy Manager (CPPM) to be used in assessing and enforcing the company's security policy. The SRX Series device transmits the logs in volumes determined by the rate-limiting conditions that you set.

[Table 5 on page 24](#) identifies the types of threat and attack log entries and the events that they represent.

**Table 5: Threat and Attack Log Entries Generated by SRX Series Components**

Log Type	Description
RT_SCREEN_ICMP	ICMP attack
RT_SCREEN_ICMP_LS	
RT_SCREEN_IP	IP attack
RT_SCREEN_IP_LS	
RT_SCREEN_TCP	TCP attack
RT_SCREEN_TCP_LS	
RT_SCREEN_TCP_DST_IP	TCP destination IP attack
RT_SCREEN_TCP_DST_IP_LS	
RT_SCREEN_TCP_SRC_IP	TCP source IP attack
RT_SCREEN_TCP_SRC_IP_LS	
RT_SCREEN_UDP	UDP attack
RT_SCREEN_UDP_LS	
AV_VIRUS_DETECTED_MT	Virus infection
AV_VIRUS_DETECTED_MT_LS	A virus was detected by the antivirus scanner.
ANTISPAM_SPAM_DETECTED_MT	spam
ANTISPAM_SPAM_DETECTED_MT_LS	The identified e-mail was detected to be spam.
IDP_APPDDOS_APP_ATTACK_EVENT	Application-level distributed denial of Service (AppDDoS) attack
IDP_APPDDOS_APP_ATTACK_EVENT_LS	The AppDDoS attack occurred when the number of client transactions exceeded the user-configured connection, context, and time binding thresholds.



Table 5: Threat and Attack Log Entries Generated by SRX Series Components (*continued*)

Log Type	Description
IDP_APPDDOS_APP_STATE_EVENT	AppDDoS attack
IDP_APPDDOS_APP_STATE_EVENT_LS	The AppDDoS state transition occurred when the number of application transactions exceeded the user-configured connection or context thresholds.
IDP_ATTACK_LOG_EVENT	Attack discovered by IDP
IDP_ATTACK_LOG_EVENT_LS	IDP generated a log entry for an attack.

**Related Documentation**

- [Understanding the SRX Series Integrated ClearPass Authentication and Enforcement Feature on page 4](#)
- [Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API on page 7](#)

### Integrated ClearPass Authentication and Enforcement Examples

- [Example: Configuring the SRX Series Integrated ClearPass Feature to Allow the Device to Receive User Authentication Data from ClearPass on page 25](#)
- [Example: Enforcing SRX Series Security Policies Using Aruba ClearPass as the Authentication Source on page 34](#)
- [Example: Configuring the Integrated ClearPass Authentication and Enforcement User Query Function on page 52](#)
- [Example: Configuring Integrated ClearPass to Filter and Rate-limit Threat and Attack Logs on page 60](#)

#### ***Example: Configuring the SRX Series Integrated ClearPass Feature to Allow the Device to Receive User Authentication Data from ClearPass***

The SRX Series device and the ClearPass Policy Manager (CPPM) collaborate to control access to your protected resources and to the Internet. To carry this out, the SRX Series device must authenticate users in conjunction with applying security policies that match their requests. For the integrated ClearPass authentication and enforcement feature, the SRX Series device relies on ClearPass as its authentication source.

The Web API function, which this example covers, exposes to the CPPM an API that enables it to initiate a secure connection with the SRX Series device. The CPPM uses this connection to post user authentication information to the SRX Series device. In their relationship, the SRX Series device acts as an HTTPS server for the CPPM client.

- [Requirements on page 26](#)
- [Overview on page 26](#)
- [Configuration on page 30](#)

### Requirements

This section defines the software and hardware requirements for the topology for this example. See [Figure 5 on page 30](#) for the topology design.

The hardware and software components are:

- Aruba ClearPass (CPPM). The CPPM is configured to use its local authentication source to authenticate users.



**NOTE:** It is assumed that the CPPM is configured to provide the SRX Series device with user authentication and identity information, including the username, a list of the names of any groups that the user belongs to, the IP addresses of the devices used, and the device posture token.

- SRX Series device running Junos OS that includes the integrated ClearPass feature.  
See [“SRX Series Supported Platforms for the Integrated ClearPass Authentication and Enforcement Feature” on page 6](#).
- A server farm composed of six servers, all in the servers-zone:
  - marketing-server-protected (1.2.3.4)
  - human-resources-server (1.3.4.5)
  - accounting-server (1.4.5.6)
  - public-server (1.5.6.7)
  - corporate-server (1.6.7.8)
  - sales-server (1.7.8.9)
- AC 7010 Aruba Cloud Services Controller running ArubaOS.
- Aruba AP wireless access controller running ArubaOS.  
The Aruba AP is connected to the AC7010.  
Wireless users connect to the CPPM through the Aruba AP.
- Juniper Networks EX4300 switch used as the wired 802.1 access device.  
Wired users connect to the CPPM using the EX4300 switch.
- Six end-user systems:
  - Three wired network-connected PCs running Microsoft OS
  - Two BYOD devices that access the network through the Aruba AP access device
  - One wireless laptop running Microsoft OS

### Overview

You can configure identity-aware security policies on the SRX Series device to control a user's access to resources based on username or group name, not the IP address of the

Figure 4 on page 27 illustrates the communication cycle between the SRX Series device and the CPPM, including user authentication.



1. The CPPM initiates a secure connection with the SRX Series device using Web API.
2. Three users join the network and are authenticated by the CPPM.
  - A tablet user joins the network across the corporate WAN.
  - A smartphone user joins the network across the corporate WAN.
  - A wireless laptop user joins the network from a wired laptop connected to a Layer 2 switch that is connected to the corporate LAN.
3. The CPPM sends the user authentication and identity information for the users who are logged in to the network to the SRX Series device in POST request messages using the Web API.

- Identifies a security policy that the traffic matches.

- Locates an authentication entry for the user in the ClearPass authentication table.
  - Applies the security policy to the traffic after authenticating the user.
4. Traffic from the smartphone user who is requesting access to an internal, protected resource arrives at the SRX Series device. Because all of the conditions identified in Step 3 are met and the security policy permits it, the SRX Series device allows the user connection to the protected resource.
  5. Traffic from the wired laptop user who is requesting access to a protected resource arrives at the SRX Series device. Because all of the conditions identified in Step 3 are met and the security policy permits it, the SRX Series device allows the user connection to the resource.
  6. Traffic from the tablet user who is requesting access to the Internet arrives at the SRX Series device. Because all of the conditions identified in Step 3 are met and the security policy permits it, the SRX Series device allows the user connection to the Internet.

The Web API daemon is not enabled by default for security reasons. When you start up the Web API daemon, by default it opens either the HTTP (8080) or the HTTPS (8443) service port. You must ensure that one of these ports is configured, depending on which version of the HTTP protocol you want to use. We recommend that you use HTTPS for security reasons. Opening these ports makes the system more vulnerable to service attacks. To protect against service attacks that might use these ports, the Web API daemon will start up only after you enable it.

The Web API is a RESTful Web services implementation. However, it does not fully support the RESTful Web services. Rather, it acts as an HTTP or HTTPS server that responds to requests from the ClearPass client.



**NOTE:** The Web API connection is initialized by the CPPM using the HTTP service port (8080) or HTTPS service port (8443). For ClearPass to be able to post messages, you must enable and configure the Web API daemon.

---

To mitigate abuse and protect against data tampering, the Web API daemon:

- Requires ClearPass client authentication by HTTP or HTTPS basic user account authentication.
- Allows data to be posted to it only from the IP address configured as the client source. That is, it allows HTTP or HTTPS POST requests only from the ClearPass client IP address, which in this example is 10.208.111.177.
- Requires that posted content conforms to the established XML data format. When it processes the data, the Web API daemon ensures that the correct data format was used.



**NOTE:** Note that if you deploy Web management and the SRX Series device together, they must run on different HTTP or HTTPS service ports.

---

See [“Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API”](#) on page 7 for further information on how this feature protects against data tampering.

The SRX Series UserID daemon processes the user authentication and identity information and synchronizes it to the ClearPass authentication table on the Packet Forwarding Engine. The SRX Series device creates the ClearPass authentication table to be used for information received only from the CPPM. The ClearPass authentication table does not contain user authentication information from other authentication sources. The SRX Series device checks the ClearPass authentication table to authenticate users attempting to access protected network resources on the Internet using wired or wireless devices and local network resources.

For the CPPM to connect to the SRX Series device and post authentication information, it must be certified using HTTPS authentication. The Web API daemon supports three methods that can be used to refer to an HTTPS certificate: a default certificate, a PKI local certificate, and a customized certificate implemented through the certificate and certificate-key configuration statements. These certificate methods are mutually exclusive.

This example uses HTTPS for the connection between the CPPM and the SRX Series device. To ensure security, the integrated ClearPass feature default certificate key size is 2084 bits.

Whether you use any method—the default certificate, a PKI-generated certificate, or a custom certificate—for security reasons, you must ensure that the certificate size is 2084 bits or greater.

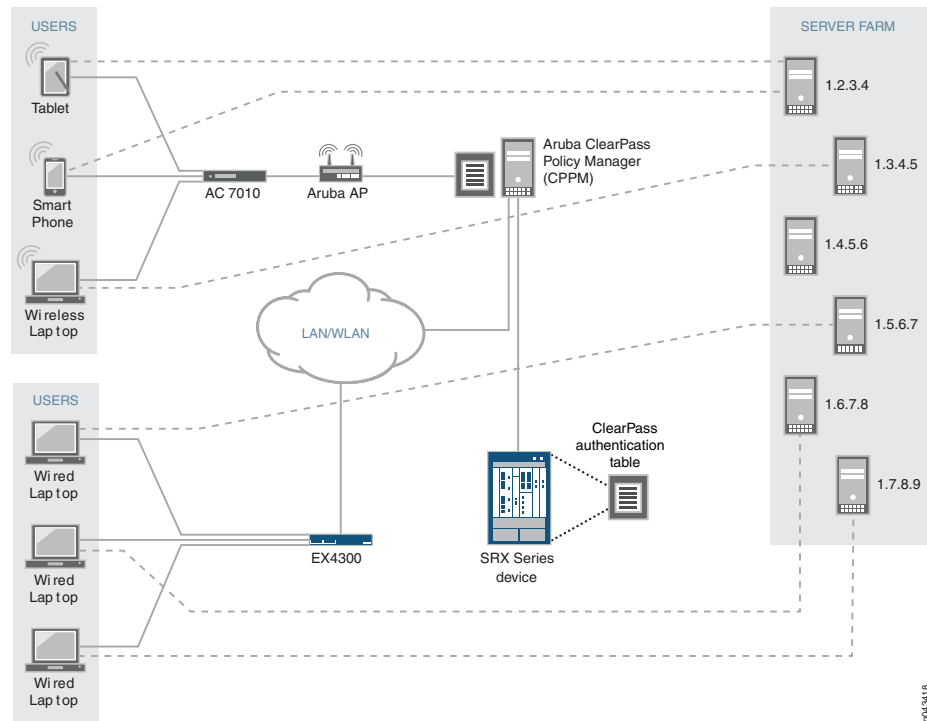
The following example shows how to generate a certificate and key using PKI:

```
user@host>request security pki generate-key-pair certificate-id aruba size 2048
user@host>request security pki local-certificate generate-self-signed certificate-id aruba
domain-name mycompany.net email jxchan@mycompany.net ip-address 1.1.1.1 subject
"CN=John Doe,OU=Sales,O=mycompany.net,L=MyCity,ST=CA,C=US"
```

### **Topology**

[Figure 5 on page 30](#) shows the topology used for the integrated ClearPass deployment examples.

**Figure 5: Integrated ClearPass Authentication and Enforcement Deployment Topology**



### Configuration

This section covers how to enable and configure the SRX Series Web API.



**NOTE:** You must enable the Web API. It is not enabled by default.

- [Configuring the SRX Series Web API Daemon on page 31](#)
- [Configuring the ClearPass Authentication Table Entry Timeout and Priority on page 33](#)

### CLI Quick Configuration

To quickly configure this example, copy the following statements, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the statements into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system services webapi user sunny password i4%rgd
set system services webapi client 10.208.111.177
set system services webapi https port 8443
set system services webapi https default-certificate
set system services webapi debug-level alert
set interfaces ge-0/0/3.4 vlan-id 340 family inet address 10.1.5.4
set security zones security-zone trust interfaces ge-0/0/3.4 host-inbound-traffic
system-services webapi-ssl
set security user-identification authentication-source aruba-clearpass priority 110
set security user-identification authentication-source local-authentication-table priority
120
```

```
set security user-identification authentication-source active-directory-authentication-table
priority 125
```

```
set security user-identification authentication-source firewall-authentication priority 150
set security user-identification authentication-source unified-access-control priority 200
```

### Configuring the SRX Series Web API Daemon

**Step-by-Step Procedure** Configuring the Web API allows the CPPM to initialize a connection to the SRX Series device. No separate connection configuration is required.

It is assumed that the CPPM is configured to provide the SRX Series device with authenticated user identity information, including the username, the names of any groups that the user belongs to, the IP addresses of the devices used, and a posture token.

Note that the CPPM might have configured role mappings that map users or user groups to device types. If the CPPM forwards the role mapping information to the SRX Series device, the SRX Series device treats the role mappings as groups. The SRX Series device does not distinguish them from other groups.

**Step-by-Step Procedure** To configure the Web API daemon:

1. Configure the Web API daemon (webapi) username and password for the account.

This information is used for the HTTPS certification request.

```
[edit system services]
user@host# set webapi user sunny password i4%rgd
```

2. Configure the Web API client address—that is—the IP address of the ClearPass webserver's data port.

The SRX Series device accepts information from this address only.



**NOTE:** The ClearPass webserver data port whose address is configured here is the same one that is used for the user query function, if you configure that function.

```
[edit system services]
user@host# set webapi client 10.208.111.177
```

3. Configure the Web API daemon HTTPS service port.

If you enable the Web API service on the default TCP port 8080 or 8443, you must enable host inbound traffic on that port.

In this example, the secure version of the Web API service is used (webapi-ssl), so you must configure the HTTPS service port, 8443.

```
[edit system services]
user@host# set webapi https port 8443
```

4. Configure the Web API daemon to use the HTTPS default certificate.

```
[edit system services]
user@host# set webapi https default-certificate
```

5. Configure the trace level for the Web API daemon.

The supported trace levels are notice, warn, error, crit, alert, and emerg. The default value is error.

```
[edit system services]
user@host# webapi debug-level alert
```

6. Configure the interface to use for host inbound traffic from the CPPM.

```
user@host# set interfaces ge-0/0/3.4 vlan-id 340 family inet address 10.1.5.4
```

7. Enable the Web API service over HTTPS host inbound traffic on TCP port 8443.

```
[edit security zones]
user@host# set security-zone trust interfaces ge-0/0/3.4 host-inbound-traffic
system-services webapi-ssl
```

**Results** From configuration mode, confirm your Web API configuration by entering the **show system services webapi** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user {
  sunny;
  password "$9$2B4JDqmf3n/k.F/9A1l"; ## SECRET-DATA
}
client {
  10.208.111.177;
}
https {
  port 8443;
  default-certificate;
}
debug-level {
  alert;
}
```

From configuration mode, confirm the configuration for the interface used for host inbound traffic from the CPPM by entering the **show interfaces ge-0/0/3.4** command. If the output does not display the intended configuration, repeat the verification process in this example to correct it.

```
vlan-id 340;
family inet {
  address 10.1.5.4/32;
}
```

From configuration mode, confirm your security zone configuration that allows host-inbound traffic from the CPPM using the secure Web API service (web-api-ssl) by entering the **show security zones security-zone trust** command. If the output does not display the intended configuration, repeat the verification process in this example to correct it.

```
interfaces {
  ge-0/0/3.4 {
```



```

host-inbound-traffic {
  system-services {
    webapi-ssl;
  }
}
}
}

```

If you are done configuring the device, enter **commit** from configuration mode.

### *Configuring the ClearPass Authentication Table Entry Timeout and Priority*

#### **Step-by-Step Procedure**

This procedure configures the following information:

- The timeout parameter that determines when to age out idle authentication entries in the ClearPass authentication table.
  - The ClearPass authentication table as the first authentication table in the lookup order for the SRX Series device to search for user authentication entries. If no entry is found in the ClearPass authentication table and there are other authentication tables configured, the SRX Series device will search them, based on the order that you set.
1. Set the timeout value that is used to expire idle authentication entries in the ClearPass authentication table to 20 minutes.

[edit services user-identification]

```

user@host# set authentication-source aruba-clearpass authentication-entry-timeout
20

```

The first time that you configure the SRX Series device to integrate with an authentication source, you must specify a timeout value to identify when to expire idle entries in the ClearPass authentication table. If you do not specify a timeout value, the default value is assumed.

- default = 30 minutes
  - range = If set, the timeout value should be within the range [10,1440 minutes]. A value of 0 means that the entry will never expire.
2. Set the authentication table priority order to direct the SRX Series device to search for user authentication entries in the ClearPass authentication table first. Specify the order in which other authentication tables are searched if an entry for the user is not found in the ClearPass authentication table.



**NOTE:** You need to set this value if the ClearPass authentication table is *not* the only authentication table on the Packet Forwarding Engine.

[edit security user-identification]

```

user@host# set authentication-source aruba-clearpass priority 110
user@host# set authentication-source local-authentication-table priority 120
user@host# set authentication-source active-directory-authentication-table priority
125
user@host# set authentication-source firewall-authentication priority 150
user@host# set authentication-source unified-access-control priority 200

```

The default priority value for the ClearPass authentication table is 110. You must change the local authentication table entry from 100 to 120 to direct the SRX Series device to check the ClearPass authentication table first if there are other authentication tables on the Packet Forwarding Engine. [Table 6 on page 34](#) shows the new authentication table search priority.

**Table 6: SRX Series Device Authentication Tables Search Priority Assignment**

SRX Series Authentication Tables	Set Value
ClearPass authentication table	110
Local authentication table	120
Active Directory authentication table	125
Firewall authentication table	150
UAC authentication table	200

**Results** From configuration mode, confirm that the timeout value set for aging out ClearPass authentication table entries is correct. Enter the **show services user-identification** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
authentication-source aruba-clearpass {
  authentication-entry-timeout 20;
}
```

- Related Documentation**
- [Understanding the SRX Series Integrated ClearPass Authentication and Enforcement Feature on page 4](#)
  - [Example: Enforcing SRX Series Security Policies Using Aruba ClearPass as the Authentication Source on page 34](#)
  - [Understanding How the Integrated ClearPass Feature Detects Threats and Attacks and Notifies the CPPM on page 21](#)
  - [Example: Configuring Integrated ClearPass to Filter and Rate-limit Threat and Attack Logs on page 60](#)

***Example: Enforcing SRX Series Security Policies Using Aruba ClearPass as the Authentication Source***

This example covers how to configure security to protect your resources and control access to the internet using the SRX Series device integrated ClearPass authentication and enforcement feature, which relies on the Aruba ClearPass Policy Manager as its authentication source. The SRX Series integrated ClearPass feature allows you to configure security policies that control access to company resources and the internet by identifying users by username, group name, or the name of a role that ties together a group of users and a device type.

Today's network environments are more open to attacks of various kinds because they support *anywhere, anytime, any device* access, to a greater or lesser degree, and they allow a user to use multiple concurrently network-connected devices. Because it allows you identify the user by username, the integrated ClearPass authentication and enforcement feature narrows the security gap that these capabilities introduce.

For details on how user authentication and identity information is conveyed from the CPPM to the SRX Series device, see the following topics:

- [Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API on page 7](#)
- [Understanding the Integrated ClearPass Authentication and Enforcement User Query Function on page 19](#)

The example covers the following processes:

- How to control access at the user level based on username or group name, not device IP address.

You can use the source-identity parameter in a security policy to specify the name of a user or the name of a group of users whose authentication is provided by the CPPM. The policy is applied to traffic generated by the users when they attempt to access a protected resource or the Internet regardless of the device used. The access control is tied to the user's name, and not directly to the IP address of the user's device.



**NOTE:** You can configure different security policies for a single user that specify different actions, differentiated by the zones and the destination addresses specified or a group that the user belongs to.

- How to display and interpret the contents of the ClearPass authentication table.

The SRX Series device creates the ClearPass authentication table to contain user authentication and identity information that it receives from the CPPM. The device refers to the table to authenticate a user who requests access to a resource.

The ClearPass authentication table contents are dynamic. They are modified to reflect user activity in response to various events and also in regard to security policies that reference groups.

For example, when a user logs out of the network or in to the network, the ClearPass authentication table is modified, as is the case when a user is removed from a group or a referenced security policy that specifies a group that the user belongs to is deleted. In the latter case, the user entry no longer shows the user as belonging to that group.

In this example, the ClearPass authentication table contents are displayed to depict changes made because of two events. The content for the users is displayed:

- Before and after a specific user logs out of the network
- Before and after a referenced security policy is deleted

The entry for the user who belonged to the group referenced by the security policy is displayed before and after the policy is deleted.

- [Requirements on page 36](#)
- [Overview on page 37](#)
- [Configuration on page 40](#)
- [Verification on page 49](#)

### **Requirements**

This section defines the software and hardware requirements for the topology for this example. See [Figure 5 on page 30](#) for the topology design.

The hardware and software components are:

- Aruba ClearPass. The ClearPass Policy Manager (CPPM) is configured to use its local authentication source to authenticate users.



**NOTE:** It is assumed that the CPPM is configured to provide the SRX Series device with user authentication and identity information, including the username, a list of the names of any groups that the user belongs to, the IP addresses of the devices used, and the device posture token.

- SRX Series device running Junos OS that includes the integrated ClearPass feature.  
See [“SRX Series Supported Platforms for the Integrated ClearPass Authentication and Enforcement Feature” on page 6](#).
- A server farm composed of six servers, all in the servers-zone:
  - marketing-server-protected (1.2.3.4)
  - human-resources-server (1.3.4.5)
  - accounting-server (1.4.5.6)
  - public-server (1.5.6.7)
  - corporate-server (1.6.7.8)
  - sales-server (1.7.8.9)
- AC 7010 Aruba Cloud Services Controller running ArubaOS.
- Aruba AP wireless access controller running ArubaOS.  
The Aruba AP is connected to the AC7010.  
Wireless users connect to the CPPM through the Aruba AP.
- Juniper Networks EX4300 switch used as the wired 802.1 access device.  
Wired users connect to the CPPM using the EX4300 switch.
- Six end-user systems:

- Three wired network-connected PCs running Microsoft OS
- Two BYOD devices that access the network through the Aruba AP access device
- One wireless laptop running Microsoft OS

### Overview

In its capacity as the authentication source for the integrated ClearPass feature, the CPPM posts to the SRX Series device user authentication and identity information. When it receives this information, the SRX Series UserID daemon processes it and generates entries for the authenticated users in the Routing Engine authentication table and then synchronizes that information to the ClearPass authentication table on the Packet Forwarding Engine side.

The SRX Series device requires the user authentication and identity information to verify that a user is authenticated when the user makes an access request and the traffic generated from the user's device arrives at the SRX Series device. If a security policy exists that specifies in the source-identity parameter the username or the name of a group that the user belongs to, the SRX Series device searches the contents of its ClearPass authentication table for an entry for that user.

If it does not find an entry for the user in its ClearPass authentication table, the SRX Series device can search its other authentication tables, if you have configured a search order that includes them. See [“Example: Configuring the SRX Series Integrated ClearPass Feature to Allow the Device to Receive User Authentication Data from ClearPass” on page 25](#) for information about the authentication table search order.

The integrated ClearPass feature allows you to create identity-aware security policies configured to match traffic issued by users based on their username or the name of a group that they belong to.



**NOTE:** You configure role mappings on the CPPM, not on the SRX Series device.

For example, a device type role mapping might tie user identities to company-owned computers. You could specify this role as a group in a security policy configured to apply to all users who are mapped to the rule. In this case, the conditions set by CPPM for the rule—use of company-owned computer—would apply to all users mapped to the rule. The SRX Series device does not consider the conditions, but rather accepts the rule from the CPPM.

The following configurations included in this example cover security policies that are applicable based on the type of device used as defined by the CPPM through rule mappings. It is assumed that the CPPM posted to the SRX Series device the following mapped rules that are used as groups in security policies:

- marketing-access-for-pcs-limited-group  
Maps jxchan to the device type PC.

The policy that specifies marketing-access-for-pcs-limited-group in its source-identity field allows jxchan, and other users who are mapped to it, access to the marketing-server-protected server using their PC, whether it is company owned or not.

- accounting-grp-and-company-device

Maps users who belong to accounting groups using company devices. The CPPM sends the role accounting-grp-and-company-device to the SRX Series device. The mapping is done on the CPPM by role mapping rules.

The policy that specifies accounting-grp-and-company-device in its source identity field allows users who are mapped to the rule to access protected resources on the accounting-server. The group accounting-grp is mapped to the rule. Therefore the mapped rule applies to the members of accounting-grp.

The user viki2 belongs to accounting-grp. If all conditions apply—that is, if viki2 is using a company-owned device and the policy permits access—she is allowed access to the resources on accounting-server. But, recall that the SRX Series device does not analyze the rule. Rather it applies it to all users who are mapped to it by the CPPM.

- guest-device-byod

Maps the guest group to the device type byod—that is, any user-owned device brought to the network.

The policy that specifies guest-device-byod in its source identity field denies users who are mapped to the rule access to all servers in the server zone if they are using smartphones or other user-owned devices. The username guest2 is mapped to this rule by the CPPM.

For all cases, if the users are allowed or denied access according to the security policy conditions, you can assume that the following conditions exist:

- The CPPM posted the correct authentication information for the users and groups to the SRX Series device.
- The SRX Series device processed the authenticated user information correctly and generated entries for the users and groups in its ClearPass authentication table.

[Table 7 on page 38](#) summarizes the users, their groups, and the zones to which they belong. All users belong to the default GLOBAL domain.

**Table 7: Authenticated User Information for Security Policy Example**

User	Group	Zone
Abe (abew1)	<ul style="list-style-type: none"> <li>• marketing-access-limited-grp</li> </ul>	marketing-zone
John (jxchan)	<ul style="list-style-type: none"> <li>• posture-healthy</li> <li>• marketing-access-for-pcs-limited-group</li> <li>• marketing-general</li> <li>• sales-limited</li> <li>• corporate-limited</li> </ul>	marketing-zone

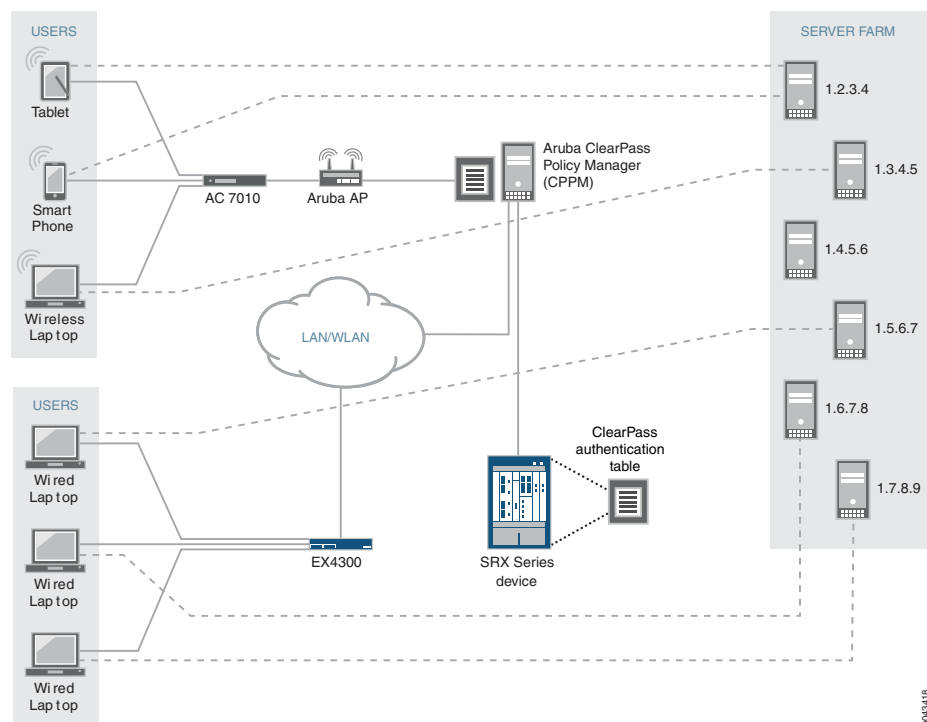
Table 7: Authenticated User Information for Security Policy Example (*continued*)

User	Group	Zone
Lin (lchen1)	<ul style="list-style-type: none"> <li>posture-healthy</li> <li>human-resources-grp</li> <li>accounting-limited</li> <li>corporate-limited</li> </ul>	human-resources-zone
Viki (viki2)	<ul style="list-style-type: none"> <li>posture-healthy</li> <li>accounting-grp</li> <li>accounting-grp-and-company-device</li> <li>corporate-limited</li> </ul>	accounting-zone
guest1	<ul style="list-style-type: none"> <li>posture-healthy</li> <li>guest</li> </ul>	public-zone
guest2	<ul style="list-style-type: none"> <li>posture-healthy</li> <li>guest-device-byod</li> </ul>	public-zone

**Topology**

Figure 6 on page 39 shows the topology for this example.

Figure 6: Topology for the Integrated ClearPass Authentication Enforcement Through Security Policies Example



### Configuration

This section covers how to configure the SRX Series device to include security policies that match traffic issued by users authenticated by the CPPM.

- [Configuring Interfaces, Zones, and an Address Book on page 42](#)
- [Configuring Identity-Aware Security Policies to Control User Access to Company Resources on page 45](#)
- [Results on page 47](#)

#### CLI Quick Configuration

To quickly configure this example, copy the following statements, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the statements into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/3 vlan-tagging
set interfaces ge-0/0/3.0 vlan-id 300 family inet address 1.0.0.1/24
set interfaces ge-0/0/3.1 vlan-id 310 family inet address 6.0.0.1/24
set interfaces ge-0/0/3.2 vlan-id 320 family inet address 7.0.0.1/24
set interfaces ge-0/0/4 vlan-tagging
set interfaces ge-0/0/4.0 vlan-id 400 family inet address 5.0.0.3/24
set interfaces ge-0/0/4.1 vlan-id 410 family inet address 8.0.0.1/24
set security zones security-zone marketing-zone interfaces ge-0/0/3.0
  host-inbound-traffic system-services all
set security zones security-zone marketing-zone interfaces ge-0/0/3.0
  host-inbound-traffic protocols all
set security zones security-zone accounting-zone interfaces ge-0/0/3.1
  host-inbound-traffic system-services all
set security zones security-zone accounting-zone interfaces ge-0/0/3.1
  host-inbound-traffic protocols all
set security zones security-zone human-resources-zone interfaces ge-0/0/3.2
  host-inbound-traffic system-services all
set security zones security-zone human-resources-zone interfaces ge-0/0/3.2
  host-inbound-traffic protocols all
set security zones security-zone public-zone interfaces ge-0/0/4.0 host-inbound-traffic
  system-services all
set security zones security-zone public-zone interfaces ge-0/0/4.0 host-inbound-traffic
  protocols all
set security zones security-zone servers-zone interfaces ge-0/0/4.1 host-inbound-traffic
  system-services all
set security zones security-zone servers-zone interfaces ge-0/0/4.1 host-inbound-traffic
  protocols all
set security address-book servers-zone-addresses address marketing-server-protected
  1.2.3.4
set security address-book servers-zone-addresses address human-resources-server
  1.3.4.5
set security address-book servers-zone-addresses address accounting-server 1.4.5.6
set security address-book servers-zone-addresses address corporate-server 1.6.7.8
set security address-book servers-zone-addresses address public-server 1.8.9.1
set security address-book servers-zone-addresses attach zone servers-zone
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p1
  match source-address any destination-address any
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p1
  match application any
```



```
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p1
  match source-identity "global\marketing-access-for-pcs-limited-group"
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p1
  then permit
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p2
  match source-address any destination address marketing-zone-protected
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p2
  match application any
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p2
  match source-identity "global\abew1"
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p2
  then permit
set security policies from-zone accounting-zone to-zone servers-zone policy acct-cp-device
  match source-address any destination address accounting-server
set security policies from-zone accounting-zone to-zone servers-zone policy acct-cp-device
  match application any
set security policies from-zone accounting-zone to-zone servers-zone policy acct-cp-device
  match source-identity "global\accounting-grp-and-company-device"
set security policies from-zone accounting-zone to-zone servers-zone policy acct-cp-device
  then permit
set security policies from-zone human-resources-zone to-zone servers-zone policy
  human-resources-p1 match source-address any destination address corporate-server
set security policies from-zone human-resources-zone to-zone servers-zone policy
  human-resources-p1 match application any
set security policies from-zone human-resources-zone to-zone servers-zone policy
  human-resources-p1 match source-identity "global\corporate-limited"
set security policies from-zone human-resources-zone to servers-zone policy
  human-resources-p1 then permit
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p0
  match source-address any destination address corporate-server
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p0
  match application any
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p0
  match source-identity "global\marketing-access-limited-grp"
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p0
  then permit
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p3
  match source-address any destination address human-resources-server
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p3
  match application any
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p3
  match source-identity "global\sales-limited-group"
set security policies from-zone marketing-zone to-zone servers-zone policy marketing-p3
  then permit
set security policies from-zone public-zone to-zone servers-zone policy guest-allow-access
  match source-address any destination address public-server
set security policies from-zone public-zone to-zone servers-zone policy guest-allow-access
  match application any
set security policies from-zone public-zone to-zone servers-zone policy guest-allow-access
  match source-identity "global\guest"
set security policies from-zone public-zone to-zone servers-zone policy guest-allow-access
  then permit
set security policies from-zone public-zone to-zone servers-zone policy guest-deny-access
  match source-address any destination address any
set security policies from-zone public-zone to-zone servers-zone policy guest-deny-access
  match application any
```

```
set security policies from-zone public-zone to-zone servers-zone policy guest-deny-access
match source-identity "global\guest-device-byod"
set security policies from-zone public-zone to-zone servers-zone policy guest-deny-access
then deny
```

### *Configuring Interfaces, Zones, and an Address Book*

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instruction on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

Configure the following interfaces and assign them to zones:

- ge-0/0/3.0 > marketing-zone
- ge-0/0/3.1 > human-resources-zone
- ge-0/0/3.2 > accounting-zone
- ge-0/0/4.0 > public-zone
- ge-0/0/4.1 > servers-zone

Because this example uses logical interfaces, you must configure VLAN tagging.

1. Configure interfaces for the SRX Series device:

```
[edit interfaces]
set ge-0/0/3 vlan-tagging
set ge-0/0/3.0 vlan-id 300 family inet address 1.0.0.1/24
set ge-0/0/3.1 vlan-id 310 family inet address 6.0.0.1/24
set ge-0/0/3.2 vlan-id 320 family inet address 7.0.0.1/24
set ge-0/0/4 vlan-tagging
set ge-0/0/4.0 vlan-id 400 family inet address 5.0.0.3/24
set ge-0/0/4.1 vlan-id 410 family inet address 8.0.0.1/24
```

2. Configure zones.

```
[edit security zones]
user@host#set security-zone marketing-zone interfaces ge-0/0/3.0
host-inbound-traffic system-services all
user@host#set security-zone marketing-zone interfaces ge-0/0/3.0
host-inbound-traffic protocols all
user@host#set security-zone accounting-zone interfaces ge-0/0/3.1
host-inbound-traffic system-services all
user@host#set security-zone accounting-zone interfaces ge-0/0/3.1
host-inbound-traffic protocols all
user@host#set security-zone human-resources-zone interfaces ge-0/0/3.2
host-inbound-traffic system-services all
user@host#set security-zone human-resources-zone interfaces ge-0/0/3.2
host-inbound-traffic protocols all
user@host#set security-zone public-zone interfaces ge-0/0/4.0 host-inbound-traffic
system-services all
user@host#set security-zone public-zone interfaces ge-0/0/4.0 host-inbound-traffic
protocols all
user@host#set security-zone servers-zone interfaces ge-0/0/4.1 host-inbound-traffic
system-services all
```

```
user@host#set security-zone servers-zone interfaces ge-0/0/4.1 host-inbound-traffic
protocols all
```

3. Configure an address book containing the IP addresses of the servers to use as destination addresses in security policies.

```
[edit security address-book servers-zone-addresses]
user@host# set address marketing-server-protected 1.2.3.4
user@host# set address human-resources-server 1.3.4.5
user@host# set address accounting-server 1.4.5.6
user@host# set address corporate-server 1.6.7.8
user@host# set address public-server 1.8.9.1
```

4. Attach the servers-zone-addresses address book to servers-zone.

```
[edit security address-book]
user@host# set servers-zone-addresses attach zone servers-zone
```

**Results** From configuration mode, confirm your configuration for interfaces by entering the **show interfaces** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
|
ge-0/0/3 {
  unit 0 {
    vlan-id 300;
    family inet {
      address 1.0.0.1/24;
    }
  }
  unit 1 {
    vlan-id 310;
    family inet {
      address 6.0.0.1/24;
    }
  }
  unit 2 {
    vlan-id 320;
    family inet {
      address 7.0.0.1/24;
    }
  }
}
ge-0/0/4 {
  vlan-tagging;
  unit 0 {
    vlan-id 400;
    family inet {
      address 5.0.0.3/24;
    }
  }
  unit 1 {
    vlan-id 410;
    family inet {
      address 8.0.0.1/24;
    }
  }
}
```

```
}  
}
```

From configuration mode, confirm your configuration for zones by entering the **show security zones** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
security-zone human-resources-zone {  
  interfaces {  
    ge-0/0/3.2 {  
      host-inbound-traffic {  
        system-services {  
          all;  
        }  
        protocols {  
          all;  
        }  
      }  
    }  
  }  
}  
security-zone accounting-zone {  
  interfaces {  
    ge-0/0/3.1 {  
      host-inbound-traffic {  
        system-services {  
          all;  
        }  
        protocols {  
          all;  
        }  
      }  
    }  
  }  
}  
security-zone marketing-zone {  
  interfaces {  
    ge-0/0/3.0 {  
      host-inbound-traffic {  
        system-services {  
          all;  
        }  
        protocols {  
          all;  
        }  
      }  
    }  
  }  
}  
security-zone servers-zone {  
  interfaces {  
    ge-0/0/4.1 {  
      host-inbound-traffic {  
        system-services {  
          all;  
        }  
      }  
    }  
  }  
}
```

```

        protocols {
            all;
        }
    }
}
}
security-zone public-zone {
    interfaces {
        ge-0/0/4.0 {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
        }
    }
}
}

```

From configuration mode, confirm your configuration for the address book by entering the **show security address-book** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```

servers-zone-addresses {
    address marketing-zone-protected 1.2.3.4/32;
    address human-resources-server 1.3.4.5/32;
    address accounting-server 1.4.5.6/32;
    address corporate-server 1.6.7.8/32;
    address public-server 1.8.9.1/32;
    attach {
        zone servers-zone;
    }
}

```

### *Configuring Identity-Aware Security Policies to Control User Access to Company Resources*

**Step-by-Step Procedure** This task entails configuring security policies that apply to a user's access to resources based on username or group name, and not the IP address of the device used.

Note that all users belong to the default GLOBAL domain.

1. Configure a security policy that specifies marketing-access-for-pcs-limited-group as the source-identity. It allows the user jxchan, who belongs to this group, access to any of the servers in the servers-zones when he is using a PC, whether it is a personal device or a company-owned device. The username jxchan is mapped by the CPPM to the rule marketing-access-for-pcs-limited-group.

[edit security policies]

```

user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p1
match source-address any destination address any

```

```

user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p1
match application any

```

```
user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p1
match source-identity "global\marketing-access-for-pcs-limited-group"
user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p1
then permit
```

2. Configure a security policy that allows the user abew1 access to the marketing-zone-protected server (IP address 1.2.3.4) in the servers-zone regardless of the device that he uses.

```
[edit security policies]
user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p2
match source-address any destination address marketing-zone-protected
user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p2
match application any
user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p2
match source-identity "global\abew1"
user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p2
then permit
```

3. Configure a security policy that allows the user viki2 access to the accounting-server (IP address 1.4.5.6) in the servers-zone when she is using a company-owned device. The user viki2 belongs to accounting-grp which is mapped to the company-owned-device rule (accounting-grp-and-company-device) by the CPPM.

```
[edit security policies]
user@host# set from-zone accounting-zone to-zone servers-zone policy
acct-cp-device match source-address any destination-address accounting-server
user@host# set from-zone accounting-zone to-zone servers-zone policy
acct-cp-device match application any
user@host# set from-zone accounting-zone to-zone servers-zone policy
acct-cp-device match source-identity
"global\accounting-grp-and-company-device"
user@host# set from-zone accounting-zone to-zone servers-zone policy
acct-cp-device then permit
```

4. Configure a security policy that allows users who belong to the corporate-limited group limited access to the corporate-server server (IP address 1.6.7.8) in the servers-zone when they are initiating a request from the human-resources zone.

If the source-address were specified as "any", the policy would apply to other users who also belong to the corporate-limited group.

```
[edit security policies]
user@host# set from-zone human-resources-zone to-zone servers-zone policy
human-resources-p1 match source-address any destination-address
corporate-server
user@host# set from-zone human-resources-zone to-zone servers-zone policy
human-resources-p1 match application any
user@host# set from-zone human-resources-zone to-zone servers-zone policy
human-resources-p1 match source-identity "global\corporate-limited"
user@host# set from-zone human-resources-zone to servers-zone policy
human-resources-p1 then permit
```

5. Configure a security policy that allows the user abew1 access to the corporate-server (IP address 1.6.7.8) server in the servers-zone. The user abew1 belongs to marketing-access-limited-grp to which the security policy applies.

```
[edit security policies]
```

```

user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p0
match source-address any destination-address corporate-server
user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p0
match application any
user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p0
match source-identity "global\marketing-access-limited-grp"
user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p0
then permit

```

6. Configure a security policy that allows users who belong to the sales-limited-group access to the human-resources-server (IP address 1.7.8.9) server when they initiate a request from the marketing-zone. The user jxchan belongs to sales-limited-group.

```

[edit security policies]
user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p3
match source-address any destination-address human-resources-server
user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p3
match application any
user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p3
match source-identity "global\sales-limited-group"
user@host# set from-zone marketing-zone to-zone servers-zone policy marketing-p3
then permit

```

7. Configure a security policy that allows users who belong to the guest group access to the public-server (IP address 1.8.9.1) in the servers-zone.

```

[edit security policies]
user@host# set from-zone public-zone to-zone servers-zone policy
guest-allow-access match source-address any destination address public-server
user@host# set from-zone public-zone to-zone servers-zone policy
guest-allow-access match application any
user@host# set from-zone public-zone to-zone servers-zone policy
guest-allow-access match source-identity "global\guest"
user@host# set from-zone public-zone to-zone servers-zone policy
guest-allow-access then permit

```

8. Configure a security policy that denies users who belong to the guest-device-byod group access to any servers in the servers-zone when they use their own devices.

```

[edit security policies]
user@host# set from-zone public-zone to-zone servers-zone policy
guest-deny-access match source-address any destination-address any
user@host# set from-zone public-zone to-zone servers-zone policy
guest-deny-access match application any
user@host# user@host# set from-zone public-zone to-zone servers-zone policy
guest-deny-access match source-identity "global\guest-device-byod"
user@host# set from-zone public-zone to-zone servers-zone policy
guest-deny-access then deny

```

### Results

From configuration mode, confirm your security policies configuration for integrated ClearPass by entering the **show security policies** command.

If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
from-zone marketing-zone to-zone servers-zone {
  policy marketing-p1 {
    match {
      source-address any;
      destination-address any;
      application any;
      source-identity "global\marketing-access-for-pcs-limited-group";
    }
    then {
      permit;
    }
  }
  policy marketing-p2 {
    match {
      source-address any;
      destination-address marketing-zone-protected;
      application any;
      source-identity "global\abew1";
    }
    then {
      permit;
    }
  }
  policy marketing-p0 {
    match {
      source-address any;
      destination-address corporate-server;
      application any;
      source-identity "global\marketing-access-limited-grp";
    }
    then {
      permit;
    }
  }
  policy marketing-p3 {
    match {
      source-address any;
      destination-address human-resources-server;
      application any;
      source-identity "global\sales-limited-group";
    }
    then {
      permit;
    }
  }
}
from-zone accounting-zone to-zone servers-zone {
  policy acct-cp-device {
    match {
      source-address any;
      destination-address accounting-server;
      application any;
      source-identity "global\accounting-grp-and-company-device";
    }
    then {
      permit;
    }
  }
}
```



```

    }
  }
}
from-zone human-resources-zone to-zone servers-zone {
  policy human-resources-p1 {
    match {
      source-address any;
      destination-address corporate-server;
      application any;
      source-identity "global\corporate-limited";
    }
    then {
      permit;
    }
  }
}
from-zone public-zone to-zone servers-zone {
  policy guest-allow-access {
    match {
      source-address any;
      destination-address public-server;
      application any;
      source-identity "global\guest";
    }
    then {
      permit;
    }
  }
  policy guest-deny-access {
    match {
      source-address any;
      destination-address any;
      application any;
      source-identity "global\guest-device-byod";
    }
    then {
      deny;
    }
  }
}
}

```

### Verification

This section verifies the ClearPass authentication table contents after certain events occur that cause some of its user authentication entries to be modified. It also shows how to ensure that the ClearPass authentication table has been deleted successfully after you issue the delete command. It includes the following parts:

- [Displaying the ClearPass Authentication Table Contents Before and After an Authenticated User Logs Out of the Network on page 50](#)
- [Displaying the Authentication Table Contents Before and After a Referenced Security Policy Is Deleted on page 50](#)

***Displaying the ClearPass Authentication Table Contents Before and After an Authenticated User Logs Out of the Network***

**Purpose** Display the ClearPass authentication table contents when a specific, authenticated user is logged in to the network and after the user logs out.

**Action** Enter the **show services user-identification authentication-table authentication-source authentication-source** command for the ClearPass authentication table, which is referred to as aruba-clearpass. Notice that the ClearPass authentication table includes an entry for the user viki2.

```
show services user-identification authentication-table authentication-source
aruba-clearpass
Domain: GLOBAL
Total entries: 6
Source IP      Username      groups(Ref by policy)      state
10.0.0.1       viki2         accounting-grp-and-company-dev Valid
20.0.0.1       abew1         marketing-access-limited-grp Valid
30.0.0.1       jxchan        marketing-access-for-pcs-limit Valid
40.0.0.1       lchen1        corporate-limited          Valid
50.0.0.1       guest1        corporate-limited          Valid
50.0.0.2       guest2        corporate-limited          Valid
```

Enter the same command again after viki2 logs out of the network. Notice that the ClearPass authentication table no longer contains an entry for viki2.

```
Domain: GLOBAL
Total entries: 6
Source IP      Username      groups(Ref by policy)      state
20.0.0.1       abew1         marketing-access-limited-grp Valid
30.0.0.1       jxchan        marketing-access-for-pcs-limit Valid
40.0.0.1       lchen1        corporate-limited          Valid
50.0.0.1       guest1        corporate-limited          Valid
50.0.0.2       guest2        corporate-limited          Valid
```

***Displaying the Authentication Table Contents Before and After a Referenced Security Policy Is Deleted***

**Purpose** Display the ClearPass authentication table contents for a specific user—lchen1—who belongs to a group that is referenced by a security policy. Delete that security policy, then display the entry for that user again.

**Action** Enter the **show service user-identification authentication-table authentication-source user *user-name*** command to display the ClearPass authentication table entry for a specific user, lchen1. Notice that it includes the group corporate-limited.

```
show service user-identification authentication-table authentication-source user lchen1
Domain: GLOBAL
Source IP      Username      groups(Ref by policy)      state
40.0.0.1       lchen1        corporate-limited          Valid
```

The human-resources-p1 security policy source-identity field refers to the group corporate-limited. As shown above in the ClearPass authentication entry for him, the user lchen1 belongs to that group. Here is the configuration for the human-resources-p1 referenced security policy:

```
from-zone human-resources-zone to-zone servers-zone {
  policy human-resources-p1 {
    match {
      source-address any;
      destination-address corporate-server;
      application any;
      source-identity "global\corporate-limited";
    }
    then {
      permit;
    }
  }
}
```

After you delete the human-resources-p1 security policy, whose source-identity parameter refers to the group called corporate-limited, enter the same command again. Notice that the authentication entry for lchen1 does not contain the corporate-limited group.

```
show service user-identification authentication-table authentication-source aruba-clearpass
user lchen1
Domain: GLOBAL
Source IP      Username      groups(Ref by policy)      state
40.0.0.1       lchen1                          Valid
```

Take a different approach in verifying the ClearPass authentication table state after the modification. Display the entire table to verify that the group—corporate-limited—is not included in any of the user entries. Note that if more than one user belonged to the corporate-limited group, authentication entries for all of the affected users would not show that group name.

From operational mode, enter the **show services user-identification authentication-table authentication-source aruba-clearpass** command.

```
show services user-identification authentication-table authentication-source
aruba-clearpass
Domain: GLOBAL
Total entries: 6
Source IP      Username      groups(Ref by policy)      state
10.0.0.1       viki2         accounting-grp-and-company-dev Valid
20.0.0.1       abew1         marketing-access-limited-grp Valid
30.0.0.1       jxchan        marketing-access-for-pcs-limit Valid
40.0.0.1       lchen1                          Valid
50.0.0.1       guest1         Valid
50.0.0.2       guest2         Valid
```

**Related Documentation**

- [Understanding the SRX Series Integrated ClearPass Authentication and Enforcement Feature on page 4](#)
- [Understanding Enforcement of ClearPass User and Group Authentication on the SRX Series Devices on page 10](#)
- [Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API on page 7](#)
- [SRX Series Supported Platforms for the Integrated ClearPass Authentication and Enforcement Feature on page 6](#)

***Example: Configuring the Integrated ClearPass Authentication and Enforcement User Query Function***

This example covers how to configure the SRX Series device to enable it to query Aruba ClearPass automatically for user authentication and identity information for an individual user when that information is not available.



**NOTE:** The user query function is supplementary to the Web API method of obtaining user authentication and identity information, and it is optional.

---

- [Requirements on page 52](#)
- [Overview on page 53](#)
- [Configuration on page 55](#)
- [Verification on page 58](#)

***Requirements***

This section defines the software and hardware requirements for the overall topology that includes user query requirements. See [Figure 8 on page 55](#) for the topology. For details on the user query process, see [Figure 7 on page 54](#).

The hardware and software components are:

- Aruba ClearPass (CPPM). The CPPM is configured to use its local authentication source to authenticate users.



**NOTE:** It is assumed that the CPPM is configured to provide the SRX Series device with user authentication and identity information, including the username, a list of the names of any groups that the user belongs to, the IP addresses of the devices used, and the device posture token.

---

- SRX Series device running Junos OS that includes the integrated ClearPass feature.  
See [“SRX Series Supported Platforms for the Integrated ClearPass Authentication and Enforcement Feature” on page 6](#).
- A server farm composed of six servers, all in the servers-zone:

- marketing-server-protected (1.2.3.4)
- human-resources-server (1.3.4.5)
- accounting-server (1.4.5.6)
- public-server (1.5.6.7)
- corporate-server (1.6.7.8)
- sales-server (1.7.8.9)
- AC 7010 Aruba Cloud Services Controller running ArubaOS.
- Aruba AP wireless access controller running ArubaOS.

The Aruba AP is connected to the AC7010.

Wireless users connect to the CPPM through the Aruba AP.

- Juniper Networks EX4300 switch used as the wired 802.1 access device.

Wired users connect to the CPPM using the EX4300 switch.

- Six end-user systems:
  - Three wired network-connected PCs running Microsoft OS
  - Two BYOD devices that access the network through the Aruba AP access device
  - One wireless laptop running Microsoft OS

### Overview

You can configure the user query function to enable the SRX Series device to obtain authenticated user identity information from the CPPM for an individual user when the SRX Series device's ClearPass authentication table does not contain an entry for that user. The SRX Series device bases the query on the IP address of the user's device that generated the traffic issuing from the access request.

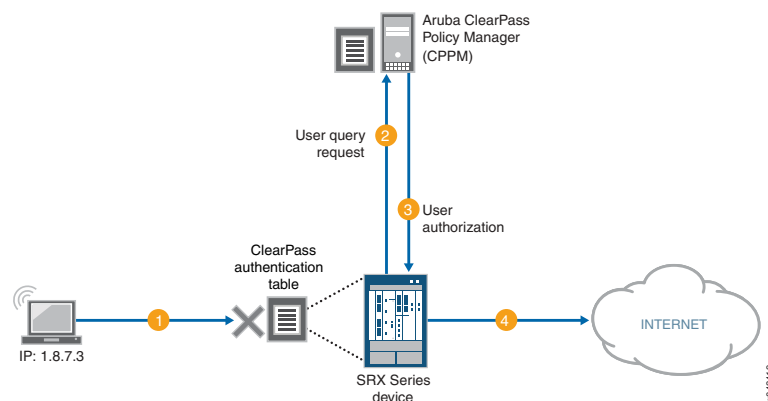
There are a number of reasons why the SRX Series device might not already have authentication information from the CPPM for a particular user. For example, it can happen that a user has not already been authenticated by the CPPM. This condition could occur if a user joined the network through an access layer that is not on a managed switch or WLAN.

The user query function provides a means for the SRX Series device to obtain user authentication and identity information from the CPPM for a user for whom the CPPM did not post that information to the SRX Series device using the Web API. When the SRX Series device receives an access request from a user for which there is not an entry in its ClearPass authentication table, it will automatically query the CPPM for it if this function is configured.

[Figure 7 on page 54](#) shows the user query flow process, which encompasses the following steps:

1. A user attempts to access a resource. The SRX Series device receives the traffic requesting access. The SRX Series device searches for an entry for the user in its ClearPass authentication table, but none is found.
2. The SRX Series device requests authentication for the user from the CPPM.
3. The CPPM authenticates the user and returns the user authentication and identity information to the SRX Series device.
4. The SRX Series device creates an entry for the user in its ClearPass authentication table, and grants the user access to the Internet.

**Figure 7: User Query Function Process**



For details on the parameters that you can use to control when the SRX Series device issues the query, see [“Understanding the Integrated ClearPass Authentication and Enforcement User Query Function”](#) on page 19.



**NOTE:** You can also manually query the CPPM for authentication information for an individual user when this feature is configured.

The ClearPass endpoint API requires use of OAuth (RFC 6749) to authenticate and authorize access to it. For the SRX Series device to be able to query the CPPM for individual user authentication and authorization information, it must acquire an access token. For this purpose, the SRX Series device uses the Client Credentials access token grant type, which is one of the two types that ClearPass supports.

As administrator of the ClearPass Policy Manager (CPPM), you must create an API client on the CPPM with the `grant_type` set to “client\_credentials”. You can then configure the SRX Series device to use that information to obtain an access token. Here is an example of the message format for doing this:

```
curl https://{Server}/api/oauth --insecure --data
"grant_type=client_credentials&client_id=Client2&client_secret=
m2Tvcklsi9je0kH9UTwuXQwlutKLC2obaDL54/fC2DzC"
```

A successful request from the SRX Series device to obtain an access token results in a response that is similar to the following example:

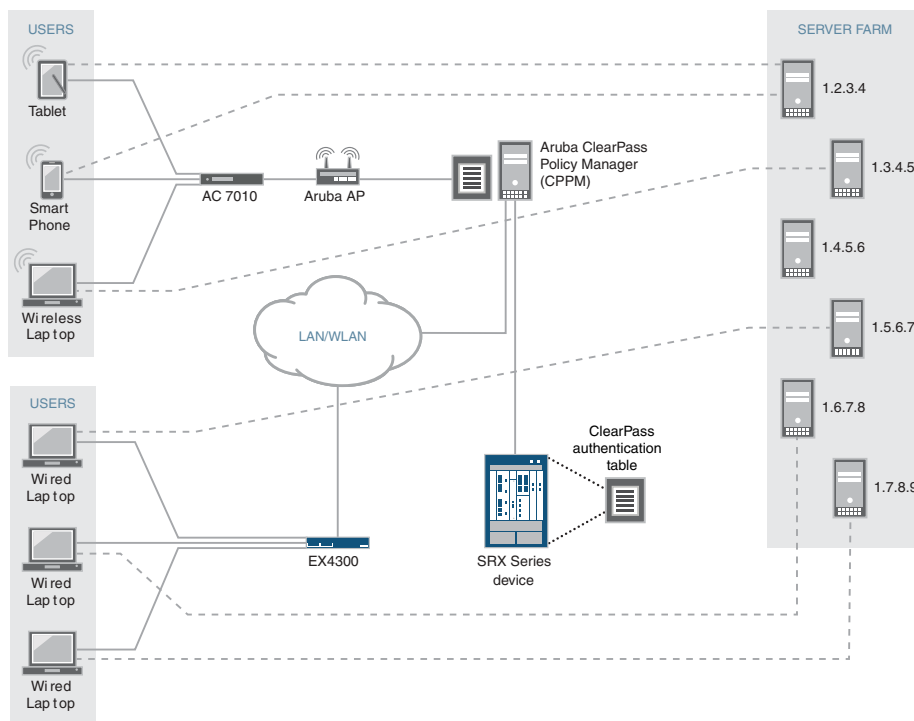
```
{
  "access_token": "ae79d980adf83ecb8e0eaca6516a50a784e81a4e",
  "expires_in": 2880,
  "token_type": "Bearer",
  "scope": "nu";
}
```

Before the access token expires, the SRX Series device can obtain a new token using the same message.

### Topology

Figure 8 on page 55 shows the overall topology for this deployment, which encompasses the user query environment.

**Figure 8: Topology for the Overall Deployment that Includes User Query**



### Configuration

To enable and configure the user query function, perform these tasks:

- [Configure the User Query Function \(Optional\) on page 56](#)
- [Manually Issuing a Query to the CPPM for Individual User Authentication Information \(Optional\) on page 58](#)

### CLI Quick Configuration

To quickly configure this example, copy the following statements, paste them into a text file, remove any line breaks, change any details necessary to match your network

configuration, copy and paste the statements into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set services user-identification authentication-source aruba-clearpass user-query
  web-server cp-webserver address 10.208.111.177
set services user-identification authentication-source aruba_clearpass user-query
  ca-certificate RADUISServerCertificate.crt
set services user-identification authentication-source aruba-clearpass user-query client-id
  client-1
set services user-identification authentication-source aruba-clearpass user-query
  client-secret 7cTr13#
set services user-identification authentication-source aruba-clearpass user-query token-api
  "api/aouth"
set services user-identification authentication-source aruba-clearpass user-query IP
  address"api/vi/insight/endpoint/ip/$IP$"
```

### *Configure the User Query Function (Optional)*

#### **Step-by-Step Procedure**

Configure the user query function to allow the SRX Series device to connect automatically to the ClearPass client to make requests for authentication information for individual users.

The user query function supplements input from the CPPM sent using the Web API. The Web API daemon does not need to be enabled for the user query function to work. For the user query function, the SRX Series device is the HTTP client. By default it sends HTTPS requests to the CPPM on port 443.

To enable the SRX Series device to make individual user queries automatically:

1. Configure Aruba ClearPass as the authentication source for user query requests, and configure the ClearPass webserver name and its IP address. The SRX Series device requires this information to contact the ClearPass webserver.



**NOTE:** You must specify aruba-clearpass as the authentication source.

```
[edit services user-identification]
```

```
user@host# set authentication-source aruba-clearpass user-query web-server
  cp-webserver address 10.208.111.177
```



**NOTE:** You can configure only one ClearPass webserver.

Optionally, configure the port number and connection method, or accept the following default values for these parameters. This example assumes the default values.

- connect-method (default is HTTPS)
- port (by default, the SRX Series device sends HTTPS requests to the CPPM on port 443)



However, if you were to explicitly configure the connection method and port, you would use these statements:

```
set services user-identification authentication-source aruba-clearpass user-query
web-server cp-webserver connect method <https/http>
set services user-identification authentication-source aruba-clearpass user-query
web-server cp-webserver port port-number
```

2. (Optional) Configure the ClearPass CA certificate file for the SRX Series device to use to verify the ClearPass webserver. (The default certificate is assumed if none is configured.)

```
[edit services user-identification]
user@host# set authentication-source aruba-clearpass user-query ca-certificate
RADUIServerCertificate.crt
```

The ca-certificate enables the SRX Series device to verify the authenticity of the ClearPass webserver and that it is trusted.

Before you configure the certificate, as administrator of the ClearPass device you must take the following actions:

- Export the ClearPass webserver's certificate from CPPM and import the certificate to the SRX Series device.
- Configure the ca-certificate as the path, including its CA filename, as located on the SRX Series device. In this example, the following path is used:

```
/var/tmp/RADUIServerCertificate.crt
```

3. Configure the client ID and the secret that the SRX Series device requires to obtain an access token required for user queries.

```
[edit services user-identification]
user@host# set authentication-source aruba-clearpass user-query client-id client-1
user@host# set authentication-source aruba-clearpass user-query client-secret
7cTr13#
```

The client ID and the client secret are required values. They must be consistent with the client configuration on the CPPM.



**TIP:** When you configure the client on the CPPM, copy the client ID and secret to use in the SRX Series device configuration.

4. Configure the token API that is used in generating the URL for acquiring an access token.



**NOTE:** You must specify the token API. It does not have a default value.

```
[edit services user-identification]
user@host# set authentication-source aruba-clearpass user-query
token-api "api/oauth"
```

In this example, the token API is `api/oauth`. It is combined with the following information to generate the complete URL for acquiring an access token `https://10.208.111.177/api/oauth`

- The connection method is HTTPS.
- In this example, the IP address of the ClearPass webserver is 10.208.111.177.

5. Configure the query API to use for querying individual user authentication and identity information.

```
[edit services user-identification]
user@host# set authentication-source aruba-clearpass user-query query-api
'api/vi/insight/endpoint/ip/$IP$'
```

In this example, the query-api is `api/vi/insight/endpoint/ip/$IP$`. It is combined with the URL `https://10.208.111.177/api/oauth` resulting in `https://10.208.111.177/api/oauth/api/vi/insight/endpoint/ip/$IP$`.

The `$IP` variable is replaced with the IP address of the end-user's device for the user whose authentication information the SRX Series is requesting.

6. Configure the amount of time in seconds to delay before the SRX Series device sends the individual user query.

```
[edit services user-identification]
user@host# set authentication-source aruba-clearpass user-query delay-query-time
10
```

#### ***Manually Issuing a Query to the CPPM for Individual User Authentication Information (Optional)***

##### **Step-by-Step Procedure**

- Configure the following statement to manually request authentication information for the user whose device's IP address is 1.2.3.6.

```
root@device>request service user-identification authentication-source
aruba-clearpass user-query address 1.2.3.6
```

#### ***Verification***

Use the following procedures to verify that the user query function is behaving as expected:

- [Verifying That the ClearPass Webserver Is Online on page 59](#)
- [Enabling Trace and Checking the Output on page 59](#)
- [Determining If the User Query Function Is Executing Normally on page 59](#)
- [Determining If a Problem Exists by Relying on User Query Counters on page 59](#)

***Verifying That the ClearPass Webserver Is Online***

**Purpose** Ensure that the ClearPass webserver is online, which is the first mean of verifying that the user query request can complete successfully.

**Action** Enter the **show service user-identification authentication-source authentication-source user-query status** command to verify that ClearPass is online.

```
show service user-identification authentication-source aruba-clearpass user-query status
```

```
Authentication source: aruba-clearpass
Web server Address: 10.208.111.177
Status: Online
Current connections: 0
```

***Enabling Trace and Checking the Output***

**Purpose** Display in the trace log any error messages generated by the user query function.

**Action** Set the trace log file name and enable trace using the following commands:

```
set system services webapi debug-log trace-log-1
set services user-identification authentication-source aruba-clearpass traceoptions flag user-query
```

***Determining If the User Query Function Is Executing Normally***

**Purpose** Determine if there is a problem with user query function behavior.

**Action** Check syslog messages to determine if the user query request failed.

If it failed, the following error message is reported:

```
LOG1: sending user query for IP <ip-address> to ClearPass web server failed.
:reason
```

The reason might be “server unconnected” or “socket error”.

***Determining If a Problem Exists by Relying on User Query Counters***

**Purpose** Display the user query counters to home in on the problem, if one exists, by entering the **show service user-identification authentication-source authentication-source user-query counters** command.

**Action** `show service user-identification authentication-source aruba-clearpass user-query counters`

Authentication source: aruba-clearpass

Web server Address: Address: *ip-address*  
Access token: *token-string*  
RE quest sent number: *counter*  
Routing received number: *counter*  
Time of last response: *timestamp*

- Related Documentation**
- [Understanding the Integrated ClearPass Authentication and Enforcement User Query Function on page 19](#)
  - [Understanding the SRX Series Integrated ClearPass Authentication and Enforcement Feature on page 4](#)
  - [Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API on page 7](#)

#### ***Example: Configuring Integrated ClearPass to Filter and Rate-limit Threat and Attack Logs***

The SRX Series device can dynamically send to the ClearPass Policy Manager (CPPM) information about threats and attacks identified by its security modules that protect network resources. It detects attack and attack threats that pertain to the activity of specific devices and their users, and it generates corresponding logs. To control this transmission, you must configure the type of logs to be sent and the rate at which they are sent. You can then use this information in setting policy rules on the CPPM to harden your network security.

This example shows how to configure the SRX Series integrated ClearPass authentication and enforcement feature to filter and transmit only threat and attack logs to the CPPM and to control the volume and rate at which the SRX Series device transmits them.

- [Requirements on page 60](#)
- [Overview on page 61](#)
- [Configuration on page 62](#)

#### ***Requirements***

The topology for this example uses the following hardware and software components:

- Aruba CPPM implemented in a virtual machine (VM) on a server. The CPPM is configured to use its local authentication source to authenticate users.
- SRX Series device running Junos OS that includes the integrated ClearPass feature. The SRX Series device is connected to the Juniper Networks EX4300 switch and to the Internet. The SRX Series device communicates with ClearPass over a secure connection.

- Juniper Networks EX4300 switch used as the wired 802.1 access device. The EX4300 Layer 2 switch connects the endpoint users to the network. The SRX Series device is connected to the switch.
- Wired, network-connected PC running Microsoft OS. The system is directly connected to the EX4300 switch.

Threat and attack logs are written for activity from these devices triggered by events that the security features catch and protect against.

### Overview

The SRX Series integrated ClearPass authentication and enforcement feature participates with Aruba ClearPass in protecting your company's resources against actual and potential attacks. The SRX Series device informs the CPPM about threats to your network resources and attacks against them through logs that it sends. You can then use this information to assess configuration of your security policy on the CPPM. Based on this information, you can harden your security in regard to individual users or devices.

To control the behavior of this feature, you must configure the SRX Series device to filter for attack and threat log entries and set rate-limiting conditions.

You can tune the behavior of this function in the following ways:

- Set a filter to direct the SRX Series device to send only threat and attack logs to the CPPM. This filter allows you to ensure that the SRX Series device and the log server do not need to handle irrelevant logs.
- Establish rate limit conditions to control the volume of logs that are sent.

You set the rate-limit parameter to control the volume and rate that logs are sent. For example, you can set the rate-limit parameter to 1000 to specify that a maximum of 1000 logs are sent to ClearPass in 1 second. In this case, if there is an attempt to send 1015 logs, the number of logs over the limit—15 logs, in this case—would be dropped. The logs are not queued or buffered.

You can configure a maximum of three log streams with each individual log defined by its destination, log format, filter, and rate limit. Log messages are sent to all configured log streams. Each stream is individually rate-limited.



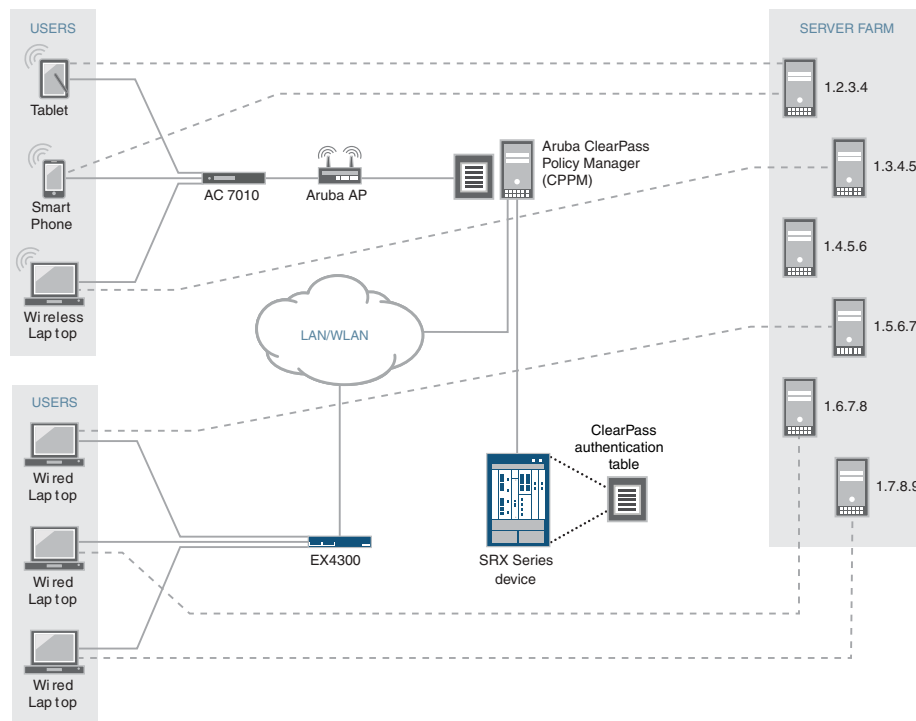
**NOTE:** To support rate-limiting on high-end platforms, log messages are sent out from the device's local SPU at a divided rate. In the configuration process, the Routing Engine assigns a divided rate to each SPU. The divided rate is equal to the configured rate divided by the number of SPUs on the device:

$$\text{divided-rate} = \text{configured-rate} / \text{number-of-SPUs}$$

### Topology

Figure 9 on page 62 shows the topology for this example.

**Figure 9: Integrated ClearPass Authentication and Enforcement Deployment Topology**



### Configuration

This example covers how to configure a filter to select threat and attack logs to be sent to ClearPass. It also covers how to set a rate limiter to control the volume of logs sent during a given period. It includes these parts:

- [Configuring Integrated ClearPass Authentication and Enforcement to Filter for Threat and Attack Logs Sent to the CPPM on page 63](#)
- [Results on page 63](#)

### CLI Quick Configuration

To quickly configure this example, copy the following statements, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the statements into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security log stream threat-attack-logs host 12.1.4.5
set security log mode stream
set security log source-interface ge-0/0/1.0
set security log stream to_clearpass format sd-syslog
set security log stream to_clearpass filter threat-attack
set security log stream to_clearpass rate-limit 1000
```

**Configuring Integrated ClearPass Authentication and Enforcement to Filter for Threat and Attack Logs Sent to the CPPM****Step-by-Step Procedure**

1. Specify CPPM as the destination for the log stream by setting the host IP address of the ClearPass device. Specify the predefined filter threat-attack to control the type of logs that are sent to it.  
  
[edit security]  
user@host# set log stream threat-attack host 12.1.4.5
2. Set the log mode to stream.  
  
[edit security]  
user@host# set log mode stream
3. Set the host source interface number.  
  
[edit security]  
user@host# set log source-interface ge-0/0/1.0
4. Set the log stream to use the structured syslog format for sending logs to ClearPass through syslog.  
  
[edit security]  
user@host# set log stream to\_clearpass format sd-syslog
5. Specify the type of events to be logged.  
  
[edit security]  
user@host# set log stream to\_clearpass filter threat-attack



**NOTE:** This configuration is mutually exclusive in relation to the current category set for the filter.

6. Set rate limiting for this stream. The range is from 1 through 65,535.  
  
This example specifies that up to 1000 logs per second can be sent to ClearPass. When the maximum is reached, any additional logs are dropped.  
  
[edit security]  
user@host# set log stream to\_clearpass rate-limit 1000

**Results**

From configuration mode, confirm your configuration for interfaces by entering the **show interfaces** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
mode stream;
source-interface ge-0/0/1.0;
stream threat-attack-logs {
  host {
    12.1.4.5;
  }
}
stream to_clearpass {
```

```
format sd-syslog;  
filter threat-attack;  
rate-limit {  
    1000;  
}  
}
```

**Related  
Documentation**

- [Understanding How the Integrated ClearPass Feature Detects Threats and Attacks and Notifies the CPPM on page 21](#)
- [SRX Series Threat and Attack Logs Sent to Aruba ClearPass on page 23](#)
- [Understanding the SRX Series Integrated ClearPass Authentication and Enforcement Feature on page 4](#)
- [Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API on page 7](#)

**Integrated ClearPass Authentication and Enforcement CLI Configuration  
Statements**

---

- [Security Configuration Statement Hierarchy on page 65](#)
- [Services Configuration Statement Hierarchy on page 108](#)
- [System Configuration Statement Hierarchy on page 114](#)
- [\[edit security log\] Hierarchy Level on page 146](#)
- [\[edit services user-identification\] Hierarchy Level on page 147](#)
- [\[edit system services\] Hierarchy Level on page 147](#)
- [address \(Services User Identification\) on page 157](#)
- [authentication-entry-timeout \(Services User Identification\) on page 157](#)
- [authentication-source \(Security User Identification\) on page 158](#)
- [authentication-source \(Services User Identification\) on page 159](#)
- [ca-certificate \(Services User Identification\) on page 160](#)
- [certificate \(System Services\) on page 161](#)
- [certificate-key \(System Services\) on page 162](#)
- [client \(System Services\) on page 162](#)
- [client-id \(Services User Identification\) on page 163](#)
- [client-secret \(Services User Identification\) on page 163](#)
- [connect-method \(Services User Identification\) on page 164](#)
- [debug-level \(System Services\) on page 164](#)
- [debug-log \(System Services\) on page 165](#)
- [default-certificate \(System Services\) on page 165](#)
- [delay-query-time \(Services User Identification\) on page 166](#)
- [file \(Services User Identification\) on page 167](#)
- [filter threat-attack \(Security\) on page 168](#)



- [http \(Services User Identification\) on page 168](#)
- [http \(System Services\) on page 169](#)
- [https \(Services User Identification\) on page 170](#)
- [https \(System Services\) on page 172](#)
- [level \(Services User Identification\) on page 173](#)
- [no-remote-trace \(Services User Identification\) on page 173](#)
- [no-user-query \(Services User Identification\) on page 174](#)
- [password \(System Services\) on page 174](#)
- [pki-local-certificate \(Services\) on page 175](#)
- [port \(Services User Identification\) on page 175](#)
- [port \(System Services\) on page 176](#)
- [priority \(Security User Identification\) on page 177](#)
- [query-api \(Services User Identification\) on page 178](#)
- [rate-limit \(Security Log\) on page 179](#)
- [token-api \(Services User Identification\) on page 180](#)
- [traceoptions \(Services User Identification\) on page 181](#)
- [webapi \(System Services\) on page 182](#)
- [webapi-clear-text \(Security\) on page 183](#)
- [webapi-ssl \(Security\) on page 183](#)
- [web-server \(Services\) on page 183](#)

### ***Security Configuration Statement Hierarchy***

For the integrated ClearPass authentication and enforcement feature, use the statements in the **security** hierarchy for the following purposes:

- To set the authentication source priority for Aruba ClearPass, if required, to ensure that the system checks the ClearPass authentication table for user authentication information before other authentication tables.
- To set the threat-attack filter and the rate limit and to control which logs are sent from the SRX Series device to the CPPM and the rate at which they are sent.

The security hierarchy also allows you to configure aspects of many other features, including, certificates, dynamic virtual private networks, firewall authentication, flow, forwarding options, group VPNs, Internet Key Exchange (IKE), Internet Protocol Security (IPsec), Intrusion Detection Prevention (IDP), logging, Network Address Translation (NAT), policies, public key infrastructure (PKI), resource manager, rules, SCREENS, secure shell known hosts, trace options, Unified Threat Management (UTM), user identification, and zones.

```
security {  
  address-book (book-name | global) {  
    address address-name {  
      ip-prefix {  
        description text;
```

```
    }
    description text;
    dns-name domain-name {
        ipv4-only;
        ipv6-only;
    }
    range-address lower-limit to upper-limit;
    wildcard-address ipv4-address/wildcard-mask;
}
address-set address-set-name {
    address address-name;
    address-set address-set-name;
    description text;
}
attach {
    zone zone-name;
}
description text;
}
alarms {
    audible {
        continuous;
    }
    potential-violation {
        authentication failures;
        cryptographic-self-test;
        decryption-failures {
            threshold value;
        }
        encryption-failures {
            threshold value;
        }
        idp;
        ike-phase1-failures {
            threshold value;
        }
        ike-phase2-failures {
            threshold value;
        }
        key-generation-self-test;
        non-cryptographic-self-test;
        policy {
            application {
                duration interval;
                size count;
                threshold value;
            }
            destination-ip {
                duration interval;
                size count;
                threshold value;
            }
            policy match {
                duration interval;
                size count;
                threshold value;
            }
        }
    }
}
```

```

    }
    source-ip {
        duration interval;
        size count;
        threshold value;
    }
}
replay-attacks {
    threshold value;
}
security-log-percent-full percentage;
}
}
alg {
    alg-manager {
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    alg-support-lib {
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
}
dns {
    disable;
    doctoring (none | sanity-check);
    maximum-message-length number;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
ftp {
    allow-mismatch-ip-address;
    disable;
    ftps-extension;
    line-break-extension;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
h323 {
    application-at a {
        message-flood {
            gatekeeper {
                threshold rate;
            }
        }
    }
}

```

```
        unknown-message {
            permit-nat-applied;
            permit-routed;
        }
    }
    disable;
    dscp-rewrite {
        code-point string;
    }
    endpoint-registration-timeout value-in-seconds;
    media-source-port-any;
    traceoptions {
        flag flag <detail | extensive | terse>;
    }
}
ike-esp-nat {
    enable;
    esp-gate-timeout value-in-seconds;
    esp-session-timeout value-in-seconds;
    state-timeout value-in-seconds;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
mgcp {
    application-screen {
        connection-flood {
            threshold rate;
        }
        message-flood {
            threshold rate;
        }
        unknown-message {
            permit-nat-applied;
            permit-routed;
        }
    }
    disable;
    dscp-rewrite {
        code-point string;
    }
    inactive-media-timeout value-in-seconds;
    maximum-call-duration value-in-minutes;
    traceoptions {
        flag flag <extensive>;
    }
    transaction-timeout value-in-seconds;
}
msrpc {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

```
    }
  }
  ptp {
    disable;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
}
real {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
rsh {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
rtsp {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
sccp {
  application-screen {
    call-flood {
      threshold rate;
    }
    unknown-message {
      permit-nat-applied;
      permit-routed;
    }
  }
  disable;
  dscp-rewrite {
    code-point string;
  }
  inactive-media-timeout value-in-seconds;
  traceoptions {
    flag flag <extensive>;
  }
}
sip {
  application-screen {
    protect {
```

```
deny {
  all {
    timeout value-in-seconds;
  }
  destination-ip address;
  timeout value-in-seconds;
}
}
unknown-message {
  permit-nat-applied;
  permit-routed;
}
}
c-timeout value-in-minutes;
disable;
dscp-rewrite {
  code-point string;
}
inactive-media-timeout value-in-seconds;
maximum-call-duration value-in-minutes;
retain-hold-resource;
t1-interval value-in-milliseconds;
t4-interval value-in-seconds;
traceoptions {
  flag flag <detail | extensive | terse>;
}
}
sql {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
sunrpc {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
talk {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
tftp {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

```

    }
  }
}
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    (no-world-readable | world-readable);
    size maximum-file-size;
  }
  level (brief | detail | extensive | verbose);
  no-remote-trace;
}
}
analysis no-report;
application-firewall {
  rule-sets rule-set-name {
    rule rule-name {
      default-rule (deny | permit);
      match {
        dynamic-application [system-application];
        dynamic-application-groups [system-application-group];
      }
      then (deny | permit);
    }
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      (no-world-readable | world-readable);
      size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
  }
}
application-tracking {
  disable;
  first-update | (first-update-interval first-update-interval);
  session-update-interval session-update-interval;
}
certificates {
  cache-size bytes;
  cache-timeout-negative seconds;
  certification-authority profile-name {
    ca-name name;
    crl filename;
    encoding (binary | pem);
    enrollment-url url;
    file filename;
    ldap-url url;
  }
  enrollment-retry number;
}

```

```
local name {
    certificate;
    load-key-file url;
}
maximum-certificates number;
path-length length;
}
datapath-debug {
    action-profile profile-name {
        event (jexec | lbt | lt-enter | lt-leave | mac-egress | mac-ingress | np-egress |
            np-ingress | pot) {
            count;
            packet-dump;
            packet-summary;
            trace;
        }
        module {
            flow {
                flag {
                    all;
                }
            }
        }
        preserve-trace-order;
        record-pic-history;
    }
    capture-file {
        filename;
        files files-number;
        format pacp-format;
        (no-world-readable | world-readable);
        size maximum-file-size;
    }
    maximum-capture-size value;
    packet-filter packet-filter-name {
        action-profile (profile-name | default);
        destination-port (port-range | protocol-name);
        destination-prefix destination-prefix;
        interface logical-interface-name;
        protocol (protocol-number | protocol-name);
        source-port (port-range | protocol-name);
        source-prefix source-prefix;
    }
    trace-options {
        file {
            filename;
            files files-number;
            match regular-expression;
            (no-world-readable | world-readable);
            size maximum-file-size;
        }
        no-remote-trace;
    }
}
dynamic-vpn {
    access-profile profile-name;
```



```

clients configuration-name {
    ipsec-vpn vpn-name;
    remote-exceptions ip-address/mask;
    remote-protected-resources ip-address/mask;
    user username;
}
force-upgrade;
}
firewall-authentication {
    traceoptions {
        flag flag;
    }
}
flow {
    aging {
        early-ageout seconds;
        high-watermark percent;
        low-watermark percent;
    }
    allow-dns-reply;
    bridge {
        block-non-ip-all;
        bpdv-vlan-flooding;
        bypass-non-ip-unicast;
        no-packet-flooding {
            no-trace-route;
        }
    }
}
force-ip-reassembly;
pending-sess-queue-length (high | moderate | normal);
route-change-timeout seconds;
syn-flood-protection-mode (syn-cookie | syn-proxy);
tcp-mss {
    all-tcp mss value;
    gre-in {
        mss value;
    }
    gre-out {
        mss value;
    }
    ipsec-vpn {
        mss value;
    }
}
tcp-session {
    no-sequence-check;
    no-syn-check;
    no-syn-check-in-tunnel;
    rst-invalidate-session;
    rst-sequence-check;
    strict-syn-check;
    tcp-initial-timeout seconds;
    time-wait-state {
        (session-ageout | session-timeout seconds);
    }
}
}

```

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    (no-world-readable | world-readable);
    size maximum-file-size;
  }
  flag flag;
  no-remote-trace;
  packet-filter filter-name {
    destination-port port-identifier;
    destination-prefix address;
    interface interface-name;
    protocol protocol-identifier;
    source-port port-identifier;
    source-prefix address;
  }
  rate-limit rate-limit;
}
}
forwarding-options {
  family {
    inet6 {
      mode (drop | flow-based | packet-based);
    }
    iso {
      mode packet-based;
    }
    mpls {
      mode packet-based;
    }
  }
}
forwarding-process {
  application-services {
    maximize-alg-sessions;
    maximize-cp-sessions;
    maximize-idp-sessions {
      inline-tap;
      weight (equal | firewall | idp);
    }
    session-distribution-mode {
      hash-based;
    }
  }
}
}
gprs {
  gtp {
    enable;
    profile profile-name {
      apn pattern-string {
        mcc-mnc mcc-mnc-number {
          action {
            drop;
            pass;
          }
        }
      }
    }
  }
}
```

```
        selection (ms|net|vrf);
    }
}
drop {
    aa-create-pdp (0 | 1 | 2 | all);
    aa-delete-pdp (0 | 1 | 2 | all);
    bearer-resource (0 | 1 | 2 | all);
    change-notification (0 | 1 | 2 | all);
    config-transfer (0 | 1 | 2 | all);
    context (0 | 1 | 2 | all);
    create-bearer (0 | 1 | 2 | all);
    create-data-forwarding (0 | 1 | 2 | all);
    create-pdp (0 | 1 | 2 | all);
    create-session (0 | 1 | 2 | all);
    create-tnl-forwarding (0 | 1 | 2 | all);
    cs-paging (0 | 1 | 2 | all);
    data-record (0 | 1 | 2 | all);
    delete-bearer (0 | 1 | 2 | all);
    delete-command (0 | 1 | 2 | all);
    delete-data-forwarding (0 | 1 | 2 | all);
    delete-pdn (0 | 1 | 2 | all);
    delete-pdp (0 | 1 | 2 | all);
    delete-session (0 | 1 | 2 | all);
    detach (0 | 1 | 2 | all);
    downlink-notification (0 | 1 | 2 | all);
    echo (0 | 1 | 2 | all);
    error-indication (0 | 1 | 2 | all);
    failure-report (0 | 1 | 2 | all);
    fwd-access (0 | 1 | 2 | all);
    fwd-relocation (0 | 1 | 2 | all);
    fwd-srns-context (0 | 1 | 2 | all);
    g-pdu (0 | 1 | 2 | all);
    identification (0 | 1 | 2 | all);
    mbms-sess-start (0 | 1 | 2 | all);
    mbms-sess-stop (0 | 1 | 2 | all);
    mbms-sess-update (0 | 1 | 2 | all);
    modify-bearer (0 | 1 | 2 | all);
    modify-command (0 | 1 | 2 | all);
    node-alive (0 | 1 | 2 | all);
    note-ms-present (0 | 1 | 2 | all);
    pdu-notification (0 | 1 | 2 | all);
    ran-info (0 | 1 | 2 | all);
    redirection (0 | 1 | 2 | all);
    release-access (0 | 1 | 2 | all);
    relocation-cancel (0 | 1 | 2 | all);
    resume (0 | 1 | 2 | all);
    send-route (0 | 1 | 2 | all);
    sgsn-context (0 | 1 | 2 | all);
    stop-paging (0 | 1 | 2 | all);
    supported-extension (0 | 1 | 2 | all);
    suspend (0 | 1 | 2 | all);
    trace-session (0 | 1 | 2 | all);
    update-bearer (0 | 1 | 2 | all);
    update-pdn (0 | 1 | 2 | all);
    update-pdp (0 | 1 | 2 | all);
}
```

```
        ver-not-supported (0 | 1 | 2 | all);
    }
    gtp-in-gtp-denied;
    log {
        forwarded (basic | detail);
        prohibited (basic | detail);
        rate-limited {
            (basic | detail);
            frequency-number number;
        }
        state-invalid (basic | detail);
    }
    max-message-length number;
    min-message-length number;
    rate-limit limit;
    remove-ie {
        version v1 {
            number ie-number;
            release (R6 | R7 | R8 | R9);
        }
    }
    restart-path (all | create | echo);
    timeout (value);
}
traceoptions {
    file {
        filename;
        files number;
        matchregular-expression;
        (no-world-readable | world-readable);
        size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
}
}
sctp {
    log {
        configuration;
        decoding-error;
        dropped-packet;
        exceeding-rate-limit;
    }
    profile profile-name {
        association-timeout time-in-minutes;
        drop {
            m3ua-service {
                isup;
                sccp;
                tup;
            }
            payload-protocol {
                all;
                asap;
                bicc;
                ddp-segment;
            }
        }
    }
}
```

```

        ddp-stream;
        dua;
        enrp;
        h248;
        h323;
        iua;
        m2pa;
        m2ua;
        m3ua;
        qipc;
        reserved;
        simco;
        sua;
        tali;
        v5ua;
    }
}
handshake-timeout time-in-seconds;
limit {
    rate {
        address ip-address {
            sccp rate-limit;
            ssp rate-limit;
            sst rate-limit;
        }
        sccp rate-limit;
        ssp rate-limit;
        sst rate-limit;
    }
}
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
        size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
}
}
}
group-vpn {
    co-location;
    member {
        ike {
            gateway gateway-name {
                address [ip-address-or-hostname];
                ike-policy policy-name;
                local-address ip-address;
                local-identity {
                    (distinguished-name | hostname hostname | inet ipv4-ip-address |
                     user-at-hostname e-mail-address);
                }
            }
        }
    }
}

```

```

}
policy policy-name {
  certificate {
    local-certificate certificate-id;
    peer-certificate-type [pkcs7 | x509-signature];
    trusted-ca (ca-index | use-all);
  }
  description description;
  mode (aggressive | main);
  pre-shared-key (ascii-text key | hexadecimal key);
  proposal-set (basic | compatible | standard);
  proposals [proposal-name];
}
proposal proposal-name {
  authentication-algorithm (md5 | sha-256 | sha1);
  authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
  description description;
  dh-group (group1 | group14 | group2 | group5);
  encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
    des-cbc);
  lifetime-seconds seconds;
}
}
ipsec {
  vpn vpn-name {
    group id;
    group-vpn-external-interface interface;
    heartbeat-threshold number;
    ike-gateway gateway-name;
  }
}
}
server {
  group name {
    activation-time-delay seconds;
    anti-replay-time-window seconds;
    description description;
    group-id number;
    ike-gateway gateway-name;
    ipsec-sa name {
      match-policy policy-name {
        destination ip-address/netmask;
        destination-port number;
        protocol number;
        source ip-address/netmask;
        source-port number;
      }
      proposal proposal-name;
    }
  }
  no-anti-replay;
  server-address ip-address;
  server-member-communication {
    certificate certificate-id;
    communication-type (multicast | unicast);
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
      des-cbc);
  }
}

```

```

        heartbeat seconds;
        lifetime-seconds seconds;
        multicast-group address;
        multicast-outgoing-interface interface;
        number-of-retransmission number;
        retransmission-period seconds;
        sig-hash-algorithm (md5 | sha1);
    }
}
ike {
    gateway gateway-name {
        address (ip-address | hostname);
        dynamic {
            (distinguished-name <container container-string> <wildcard wildcard-string>
             | hostname domain-name | inet ip-address | user-at-hostname
             e-mail-address);
        }
        ike-policy policy-name;
        local-identity {
            (distinguished-name | hostname hostname | inet ip-address | user-at-hostname
             e-mail-address);
        }
    }
}
policy policy-name {
    certificate {
        local-certificate certificate-id;
        peer-certificate-type [pkcs7 | x509-signature];
        trusted-ca (ca-index | use-all);
    }
    description description;
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposal-set (basic | compatible | standard);
    proposals [proposal-name];
}
proposal proposal-name {
    authentication-algorithm (md5 | sha-256 | sha1);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group14 | group2 | group5);
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
        des-cbc);
}
}
ipsec {
    proposal proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
        description description;
        encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
            des-cbc);
        lifetime-seconds seconds;
    }
}
traceoptions {
    file {
        filename;
    }
}

```

```

        files number;
        match regular-expression;
        (no-world-readable | world-readable);
        size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
}
}
}
idp {
    active-policy policy-name;
    custom-attack attack-name {
        attack-type {
            anomaly {
                direction (any | client-to-server | server-to-client);
                service service-name;
                shellcode (all | intel | no-shellcode | sparc);
                test test-condition ;
            }
            chain {
                expression boolean-expression;
                member member-name {
                    attack-type {
                        (anomaly | signature);
                    }
                }
            }
            order;
            protocol-binding {
                application application-name;
                icmp;
                ip {
                    protocol-number transport-layer-protocol-number ;
                }
                rpc {
                    program-number rpc-program-number ;
                }
                tcp {
                    minimum-port port-number maximum-port port-number ;
                }
                udp {
                    minimum-port port-number maximum-port port-number;
                }
            }
            reset;
            scope (session | transaction);
        }
        signature {
            context context-name;
            direction (any | client-to-server | server-to-client);
            negate;
            pattern signature-pattern;
            protocol {
                icmp {
                    code {
                        match (equal | greater-than | less-than | not-equal);
                    }
                }
            }
        }
    }
}

```



```

        value code-value;
    }
    data-length {
        match (equal | greater-than | less-than | not-equal);
        value data-length;
    }
    identification {
        match (equal | greater-than | less-than | not-equal);
        value identification-value;
    }
    sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number;
    }
    type {
        match (equal | greater-than | less-than | not-equal);
        value type-value;
    }
}
ip {
    destination {
        match (equal | greater-than | less-than | not-equal);
        value hostname;
    }
    identification {
        match (equal | greater-than | less-than | not-equal);
        value identification-value;
    }
    ip-flags {
        (df | no-df);
        (mf | no-mf);
        (rb | no-rb);
    }
    protocol {
        match (equal | greater-than | less-than | not-equal);
        value transport-layer-protocol-id;
    }
    source {
        match (equal | greater-than | less-than | not-equal);
        value hostname;
    }
    tos {
        match (equal | greater-than | less-than | not-equal);
        value type-of-service-in-decimal;
    }
    total-length {
        match (equal | greater-than | less-than | not-equal);
        value total-length-of-ip-datagram;
    }
    ttl {
        match (equal | greater-than | less-than | not-equal);
        value time-to-live;
    }
}
tcp {
    ack-number {

```

```
        match (equal | greater-than | less-than | not-equal);
        value acknowledgement-number ;
    }
    data-length {
        match (equal | greater-than | less-than | not-equal);
        value tcp-data-length;
    }
    destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port;
    }
    header-length {
        match (equal | greater-than | less-than | not-equal);
        value header-length;
    }
    mss {
        match (equal | greater-than | less-than | not-equal);
        value maximum-segment-size ;
    }
    option {
        match (equal | greater-than | less-than | not-equal);
        value tcp-option;
    }
    sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number;
    }
    source-port {
        match (equal | greater-than | less-than | not-equal);
        value source-port;
    }
    tcp-flags {
        (ack | no-ack);
        (fin | no-fin);
        (psh | no-psh);
        (r1 | no-r1);
        (r2 | no-r2);
        (rst | no-rst);
        (syn | no-syn);
        (urg | no-urg);
    }
    urgent-pointer {
        match (equal | greater-than | less-than | not-equal);
        value urgent-pointer;
    }
    window-scale {
        match (equal | greater-than | less-than | not-equal);
        value window-scale-factor;
    }
    window-size {
        match (equal | greater-than | less-than | not-equal);
        value window-size;
    }
}
udp {
    data-length {
```

```

        match (equal | greater-than | less-than | not-equal);
        value data-length;
    }
    destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port;
    }
    source-port {
        match (equal | greater-than | less-than | not-equal);
        value source-port;
    }
}
protocol-binding {
    application application-name;
    icmp;
    ip {
        protocol-number transport-layer-protocol-number;
    }
    rpc {
        program-number rpc-program-number;
    }
    tcp {
        minimum-port port-number maximum-port port-number;
    }
    udp {
        minimum-port port-number maximum-port port-number;
    }
}
regexp regular-expression;
shellcode (all | intel | no-shellcode | sparc);
}
}
recommended-action (close | close-client | close-server | drop |
drop-packet | ignore | none);
severity (critical | info | major | minor | warning);
time-binding {
    count count-value;
    scope (destination | peer | source);
}
}
custom-attack-group custom-attack-group-name {
    group-members [attack-group-name | attack-name];
}
dynamic-attack-group dynamic-attack-group-name {
    filters {
        category {
            values [list-of-values];
        }
    }
    direction {
        expression [and | or];
        values [any | client-to-server | exclude-any | exclude-client-to-server |
exclude-server-to-client | server-to-client];
    }
    false-positives {
        values [frequently | occasionally | rarely | unknown];
    }
}

```

```

    }
    performance {
        values [fast | normal | slow | unknown];
    }
    products {
        values [list-of-values];
    }
    recommended;
    service {
        values [list-of-values];
    }
    severity {
        values [critical | info | major | minor | warning];
    }
    type {
        values [anomaly | signature];
    }
}
}
idp-policy policy-name {
    rulebase-ddos {
        rule rule-name {
            description text;
            match {
                application (application-name | any | default);
                application-ddos {
                    (application-name | adp);
                }
                destination-address [ any names ];
                destination-except [ names ];
                from-zone (zone-name | any);
                source-address [ names ];
                source-except [ names ];
                to-zone zone-name;
            }
            then {
                action {
                    (close-server | drop-connection | drop-packet | no-action);
                }
                ip-action {
                    (ip-block | ip-close | ip-connection-rate-limit connections-per-second |
                     ip-notify);
                    log;
                    log-create;
                    refresh-timeout;
                    timeout seconds;
                }
                notification {
                    log-attacks {
                        alert;
                    }
                }
            }
        }
    }
}
}
rulebase-exempt {
    rule rule-name {

```

```

description text;
match {
  application [application-name];
  attacks {
    custom-attacks [attack-name];
    predefined-attack-groups [attack-name];
    predefined-attacks [attack-name];
  }
  destination-address [address-name];
  destination-except [address-name];
  from-zone zone-name ;
  source-address [address-name];
  source-except [address-name];
  to-zone zone-name ;
}
}
}
rulebase-ips {
  rule rule-name {
    description text;
    match {
      attacks {
        custom-attacks [attack-name];
        predefined-attack-groups [attack-name];
        predefined-attacks [attack-name];
      }
      destination-address [address-name];
      destination-except [address-name];
      from-zone zone-name ;
      source-address [address-name];
      source-except [address-name];
      to-zone zone-name ;
    }
    terminal;
    then {
      action {
        (close-client | close-client-and-server | close-server |
        drop-connection | drop-packet | ignore-connection |
        mark-diffserv value | no-action | recommended);
      }
      ip-action {
        (ip-block | ip-close | ip-notify);
        log;
        log-create;
        refresh-timeout;
        target (destination-address | service | source-address |
        source-zone | zone-service);
        timeout seconds;
      }
      notification {
        log-attacks {
          alert;(
        }
      }
      severity (critical | info | major | minor | warning);
    }
  }
}

```

```
    }
  }
}
security-package {
  automatic {
    enable;
    interval hours;
    start-time start-time;
  }
  url url-name;
}
sensor-configuration {
  application-identification {
    max-packet-memory value;
    max-tcp-session-packet-memory value;
    max-udp-session-packet-memory value;
  }
  detector {
    protocol-name protocol-name {
      tunable-name tunable-name {
        tunable-value protocol-value;
      }
    }
  }
}
flow {
  (allow-icmp-without-flow | no-allow-icmp-without-flow);
  (log-errors | no-log-errors);
  max-timers-poll-ticks value;
  reject-timeout value;
  (reset-on-policy | no-reset-on-policy);
}
global {
  (enable-all-qmodules | no-enable-all-qmodules);
  (enable-packet-pool | no-enable-packet-pool);
  (policy-lookup-cache | no-policy-lookup-cache);
}
high-availability {
  no-policy-cold-synchronization;
}
ips {
  detect-shellcode;
  ignore-regular-expression;
  log-supercede-min minimum-value;
  pre-filter-shellcode;
  process-ignore-s2c;
  process-override;
  process-port port-number;
}
log {
  cache-size size;
  suppression {
    disable;
    include-destination-address;
    max-logs-operate value;
    max-time-report value;
    start-log value;
  }
}
```

```

    }
  }
  re-assembler {
    ignore-memory-overflow;
    ignore-reassembly-memory-overflow;
    ignore-reassembly-overflow;
    max-flow-mem value ;
    max-packet-mem value ;
  }
}
traceoptions {
  file filename {
    <files number >;
    <match regular-expression >;
    <size maximum-file-size >;
    <world-readable | no-world-readable>;
  }
  flag all;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
}
ike {
  gateway gateway-name {
    address [ip-address-or-hostname];
    dead-peer-detection {
      always-send;
      interval seconds;
      threshold number;
    }
    dynamic {
      connections-limit number;
      (distinguished-name <container container-string> <wildcard wildcard-string> |
        hostname domain-name | inet ip-address | inet6 ipv6-address | user-at-hostname
        e-mail-address);
      ike-user-type (group-ike-id | shared-ike-id);
    }
  }
  external-interface external-interface-name;
  general-ikeid;
  ike-policy policy-name;
  local-identity {
    (distinguished-name | hostname hostname | inet ip-address | inet6 ipv6-address
    | user-at-hostname e-mail-address);
  }
  nat-keepalive seconds;
  no-nat-traversal;
  remote-identity {
    (distinguished-name <container container-string> <wildcard wildcard-string> |
      hostname hostname | inet ip-address | inet6 ipv6-address | user-at-hostname
      e-mail-address);
  }
  version (v1-only | v2-only);
  xauth {
    access-profile profile-name;
  }
}
}

```

```
policy policy-name {
  certificate {
    local-certificate certificate-id;
    peer-certificate-type (pkcs7 | x509-signature);
    trusted-ca (ca-index | use-all);
  }
  description description;
  mode (aggressive | main);
  pre-shared-key (ascii-text key | hexadecimal key);
  proposal-set (basic | compatible | standard);
  proposals [proposal-name];
}
proposal proposal-name {
  authentication-algorithm (md5 | sha-256 | sha1);
  authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
  description description;
  dh-group (group1 | group14 | group2 | group5);
  encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
  lifetime-seconds seconds;
}
respond-bad-spi <max-responses>;
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    (no-world-readable | world-readable);
    size maximum-file-size;
  }
  flag flag;
  no-remote-trace;
  rate-limit messages-per-second;
}
}
ipsec {
  policy policy-name {
    description description;
    perfect-forward-secrecy keys (group1 | group14 | group2 | group5);
    proposal-set (basic | compatible | standard);
    proposals [proposal-name];
  }
  proposal proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
    description description;
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    lifetime-kilobytes kilobytes;
    lifetime-seconds seconds;
    protocol (ah | esp);
  }
  traceoptions {
    flag flag;
  }
}
vpn vpn-name {
  bind-interface interface-name;
  df-bit (clear | copy | set);
  establish-tunnels (immediately | on-traffic);
}
```



```

ike {
    gateway gateway-name;
    idle-time seconds;
    install-interval seconds;
    ipsec-policy ipsec-policy-name;
    no-anti-replay;
    proxy-identity {
        local ip-prefix;
        remote ip-prefix;
        service (any | service-name);
    }
}
manual {
    authentication {
        algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
    }
    encryption {
        algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
        key (ascii-text key | hexadecimal key);
    }
    external-interface external-interface-name;
    gateway ip-address;
    protocol (ah | esp);
    spi spi-value;
}
vpn-monitor {
    destination-ip ip-address;
    optimized;
    source-interface interface-name;
}
}
vpn-monitor-options {
    interval seconds;
    threshold number;
}
}
key-protection;
log {
    cache {
        exclude exclude-name {
            destination-address destination-address;
            destination-port destination-port;
            event-id event-id;
            failure;
            interface-name interface-name;
            policy-name policy-name;
            process process-name;
            protocol protocol;
            source-address source-address;
            source-port source-port;
            success;
            user-name user-name;
        }
        limit value;
    }
}

```

```
disable;
event-rate rate;
file {
    files max-file-number;
    name file-name;
    path binary-log-file-path;
    size maximum-file-size;
}
format (binary | sd-syslog | syslog);
mode (event | stream);
source-address source-address;
stream stream-name {
    category (all | content-security);
    filter threat-attack
    format (binary | sd-syslog | syslog | welf);
    host {
        ip-address;
        port port-number;
    }
    rate-limit log-server-limit
    severity (alert | critical | debug | emergency | error | info | notice | warning);
}
traceoptions {
    file {
        file-name;
        files max-file-number;
        match regular-expression;
        (no-world-readable | world-readable);
        size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
}
utc-time-stamp;
}
nat {
    destination {
        pool pool-name {
            address ip-address {
                (port port-number | to ip-address);
            }
            description text;
            routing-instance routing-instance-name;
        }
        rule-set rule-set-name {
            description text;
            from {
                interface [interface-name];
                routing-instance [routing-instance-name];
                zone [zone-name];
            }
            rule rule-name {
                description text;
                match {
                    (destination-address <ip-address> | destination-address-name
                     <address-name>);
```

```

        destination-port port-number;
        protocol [protocol-name-or-number];
        source-address [ip-address];
        source-address-name [address-name];
    }
    then {
        destination-nat (off | pool pool-name);
    }
}
}
}
proxy-arp {
    interface interface-name {
        address ip-address {
            to ip-address;
        }
    }
}
proxy-ndp {
    interface interface-name {
        address ip-address {
            to ip-address;
        }
    }
}
source {
    address-persistent;
    interface {
        port-overloading {
            off;
        }
    }
    pool pool-name {
        address ip-address {
            to ip-address;
        }
        description text;
        host-address-base ip-address;
        overflow-pool (interface | pool-name);
        port {
            (no-translation | port-overloading-factor number | range port-low <to port-high>);
        }
        routing-instance routing-instance-name;
    }
    pool-default-port-range lower-port-range to upper-port-range;
    pool-utilization-alarm {
        clear-threshold value;
        raise-threshold value;
    }
    port-randomization {
        disable;
    }
    rule-set rule-set-name {
        description text;
        from {
            interface [interface-name];

```

```

        routing-instance [routing-instance-name];
        zone [zone-name];
    }
    rule rule-name {
        description text;
        match {
            (destination-address <ip-address> | destination-address-name
              <address-name>);
            destination-port port-number;
            protocol [protocol-name-or-number];
            source-address [ip-address];
            source-address-name [address-name];
        }
        then {
            source-nat {
                interface {
                    persistent-nat {
                        address-mapping;
                        inactivity-timeout seconds;
                        max-session-number value;
                        permit (any-remote-host | target-host | target-host-port);
                    }
                }
                off;
                pool {
                    persistent-nat {
                        address-mapping;
                        inactivity-timeout seconds;
                        max-session-number number;
                        permit (any-remote-host | target-host | target-host-port);
                    }
                    pool-name;
                }
            }
        }
    }
    to {
        interface [interface-name];
        routing-instance [routing-instance-name];
        zone [zone-name];
    }
}
static {
    rule-set rule-set-name {
        description text;
        from {
            interface [interface-name];
            routing-instance [routing-instance-name];
            zone [zone-name];
        }
        rule rule-name {
            description text;
            match {
                (destination-address ip-address | destination-address-name address-name);
            }

```



```
    }
    disable;
  }
  routing-instance routing-instance-name;
}
traceoptions {
  file filename {
    files number;
    match regular-expression;
    (no-world-readable | world-readable);
    size maximum-file-size;
  }
  flag flag;
  no-remote-trace;
}
}
policies {
  default-policy (deny-all | permit-all);
  from-zone zone-name to-zone zone-name {
    policy policy-name {
      description description;
      match {
        application {
          [application];
          any;
        }
        destination-address {
          [address];
          any;
          any-ipv4;
          any-ipv6;
        }
        source-address {
          [address];
          any;
          any-ipv4;
          any-ipv6;
        }
        source-identity {
          [role-name];
          any;
          authenticated-user;
          unauthenticated-user;
          unknown-user;
        }
      }
    }
  }
  scheduler-name scheduler-name;
  then {
    count {
      alarm {
        per-minute-threshold number;
        per-second-threshold number;
      }
    }
    deny;
    log {
```

```

    session-close;
    session-init;
  }
  permit {
    application-services {
      application-firewall {
        rule-set rule-set-name;
      }
      application-traffic-control {
        rule-set rule-set-name;
      }
      gprs-gtp-profile profile-name;
      gprs-sctp-profile profile-name;
      idp;
      redirect-wx | reverse-redirect-wx;
      ssl-proxy {
        profile-name profile-name;
      }
      uac-policy {
        captive-portal captive-portal;
      }
      utm-policy policy-name;
    }
    destination-address {
      drop-translated;
      drop-untranslated;
    }
    firewall-authentication {
      pass-through {
        access-profile profile-name;
        client-match user-or-group-name;
        web-redirect;
      }
      web-authentication {
        client-match user-or-group-name;
      }
    }
    services-offload;
    tcp-options {
      sequence-check-required;
      syn-check-required;
    }
    tunnel {
      ipsec-group-vpn group-vpn;
      ipsec-vpn vpn-name;
      pair-policy pair-policy;
    }
  }
  reject;
}
}
global {
  policy policy-name {
    description description;
    match {

```

```
application {
    [application];
    any;
}
destination-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
}
source-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
}
source-identity {
    [role-name];
    any;
    authenticated-user;
    unauthenticated-user;
    unknown-user;
}
}
scheduler-name scheduler-name;
then {
    count {
        alarm {
            per-minute-threshold number;
            per-second-threshold number;
        }
    }
    deny;
    log {
        session-close;
        session-init;
    }
    permit {
        application-services {
            application-firewall {
                rule-set rule-set-name;
            }
            application-traffic-control {
                rule-set rule-set-name;
            }
            gprs-gtp-profile profile-name;
            gprs-sctp-profile profile-name;
            idp;
            redirect-wx | reverse-redirect-wx;
            ssl-proxy {
                profile-name profile-name;
            }
            uac-policy {
                captive-portal captive-portal;
            }
            utm-policy policy-name;
        }
    }
}
```



```

    }
    destination-address {
        drop-translated;
        drop-untranslated;
    }
    firewall-authentication {
        pass-through {
            access-profile profile-name;
            client-match user-or-group-name;
            web-redirect;
        }
        web-authentication {
            client-match user-or-group-name;
        }
    }
    services-offload;
    tcp-options {
        sequence-check-required;
        syn-check-required;
    }
    }
    reject;
    }
    }
    policy-rematch;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            (no-world-readable | world-readable);
            size maximum-file-size;
        }
        flag flag;
        no-remote-trace;
    }
    }
    resource-manager {
        traceoptions {
            flag flag;
        }
    }
    screen {
        ids-option screen-name {
            alarm-without-drop;
            description text;
            icmp {
                flood {
                    threshold number;
                }
                fragment;
                ip-sweep {
                    threshold number;
                }
            }
            large;
        }
    }

```

```
    ping-death;
  }
  ip {
    bad-option;
    block-frag;
    loose-source-route-option;
    record-route-option;
    security-option;
    source-route-option;
    spoofing;
    stream-option;
    strict-source-route-option;
    tear-drop;
    timestamp-option;
    unknown-protocol;
  }
  limit-session {
    destination-ip-based number;
    source-ip-based number;
  }
  tcp {
    fin-no-ack;
    land;
    port-scan {
      threshold number;
    }
    syn-ack-ack-proxy {
      threshold number;
    }
    syn-fin;
    syn-flood {
      alarm-threshold number;
      attack-threshold number;
      destination-threshold number;
      source-threshold number;
      timeout seconds;
      white-list name {
        destination-address destination-address;
        source-address source-address;
      }
    }
  }
  syn-frag;
  tcp-no-flag;
  tcp-sweep {
    threshold threshold number;
  }
  winnuke;
}
udp {
  flood {
    threshold number;
  }
  udp-sweep {
    threshold threshold number;
  }
}
```

```

    }
  }
  traceoptions {
    file filename {
      files number;
      match regular-expression;
      (no-world-readable | world-readable);
      size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
  }
}
softwires {
  softwire-name name {
    softwire-concentrator ipv6-address;
    softwire-type IPv4-in-IPv6;
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      (no-world-readable | world-readable);
      size maximum-file-size;
    }
    flag (all | configuration | flow);
    no-remote-trace;
  }
}
ssh-known-hosts {
  fetch-from-server server-name;
  host hostname {
    dsa-key dsa-key;
    ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key;
    ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key;
    ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key;
    rsa-key rsa-key;
    rsa1-key rsa1-key;
  }
  load-key-file key-file;
}
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    (no-world-readable | world-readable);
    size maximum-file-size;
  }
  flag flag;
  no-remote-trace;
  rate-limit messages-per-second;
}
user-identification {
  authentication-source {

```

```
        active-directory-authentication-table ( priority priority);
        aruba-clearpass (priority priority);
        local-authentication-table ( priority priority);
        unified-access-control ( priority priority);
    }
}
utm {
    application-proxy {
        traceoptions {
            flag flag;
        }
    }
    custom-objects {
        custom-url-category object-name {
            value [value];
        }
        filename-extension object-name {
            value [value];
        }
        mime-pattern object-name {
            value [value];
        }
        protocol-command object-name {
            value [value];
        }
        url-pattern object-name {
            value [value];
        }
    }
    feature-profile {
        anti-spam {
            address-blacklist list-name;
            address-whitelist list-name;
            sbl {
                profile profile-name {
                    custom-tag-string [string];
                    (no-sbl-default-server | sbl-default-server);
                    spam-action (block | tag-header | tag-subject);
                }
            }
            traceoptions {
                flag flag;
            }
        }
        anti-virus {
            juniper-express-engine {
                pattern-update {
                    email-notify {
                        admin-email email-address;
                        custom-message message;
                        custom-message-subject message-subject;
                    }
                    interval value;
                    no-autoupdate;
                    proxy {
```

```

    password password-string;
    port port-number;
    server address-or-url;
    username name;
  }
  url url;
}
profile profile-name {
  fallback-options {
    content-size (block | log-and-permit);
    default (block | log-and-permit);
    engine-not-ready (block | log-and-permit);
    out-of-resources (block | (log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  notification-options {
    fallback-block {
      administrator-email email-address;
      allow-email;
      custom-message message;
      custom-message-subject message-subject;
      display-host;
      (no-notify-mail-sender | notify-mail-sender);
      type (message | protocol-only);
    }
    fallback-non-block {
      custom-message message;
      custom-message-subject message-subject;
      (no-notify-mail-recipient | notify-mail-recipient);
    }
    virus-detection {
      custom-message message;
      custom-message-subject message-subject;
      (no-notify-mail-sender | notify-mail-sender);
      type (message | protocol-only);
    }
  }
}
scan-options {
  content-size-limit value;
  (intelligent-prescreening | no-intelligent-prescreening);
  timeout value;
}
trickling {
  timeout value;
}
}
kaspersky-lab-engine {
  pattern-update {
    email-notify {
      admin-email email-address;
      custom-message message;
      custom-message-subject message-subject;
    }
    interval value;
  }
}

```

```
no-autoupdate;
proxy {
  password password-string;
  port port-number;
  server address-or-url;
  username name;
}
url url;
}
profile profile-name {
  fallback-options {
    content-size (block | log-and-permit);
    corrupt-file (block | log-and-permit);
    decompress-layer (block | log-and-permit);
    default (block | log-and-permit);
    engine-not-ready (block | log-and-permit);
    out-of-resources (block | log-and-permit);
    password-file (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  notification-options {
    fallback-block {
      administrator-email email-address;
      allow-email;
      custom-message message;
      custom-message-subject message-subject;
      display-host;
      (no-notify-mail-sender | notify-mail-sender);
      type (message | protocol-only);
    }
    fallback-non-block {
      custom-message message;
      custom-message-subject message-subject;
      (no-notify-mail-recipient | notify-mail-recipient);
    }
    virus-detection {
      custom-message message;
      custom-message-subject message-subject;
      (no-notify-mail-sender | notify-mail-sender);
      type (message | protocol-only);
    }
  }
}
scan-options {
  content-size-limit value;
  decompress-layer-limit value;
  (intelligent-prescreening | no-intelligent-prescreening);
  scan-extension filename;
  scan-mode (all | by-extension);
  timeout value;
}
trickling {
  timeout value;
}
}
```

```

mime-whitelist {
  exception listname;
  list listname {
    exception listname;
  }
}
sophos-engine {
  pattern-update {
    email-notify {
      admin-email email-address;
      custom-message message;
      custom-message-subject message-subject;
    }
    interval value;
    no-autoupdate;
    proxy {
      password password-string;
      port port-number;
      server address-or-url;
      username name;
    }
    url url;
  }
}
profile <name> {
  fallback-options {
    content-size (block | log-and-permit | permit);
    default (block | log-and-permit | permit);
    engine-not-ready (block | log-and-permit | permit);
    out-of-resources (block | log-and-permit | permit);
    timeout (block | log-and-permit | permit);
    too-many-requests (block | log-and-permit | permit);
  }
  notification-options {
    fallback-block {
      administrator-email email-address;
      allow-email;
      custom-message message;
      custom-message-subject message-subject;
      display-host;
      (no-notify-mail-sender | notify-mail-sender);
      type (message | protocol-only);
    }
    fallback-non-block {
      custom-message message;
      custom-message-subject message-subject;
      (no-notify-mail-recipient | notify-mail-recipient);
    }
    virus-detection {
      custom-message message;
      custom-message-subject message-subject;
      (no-notify-mail-sender | notify-mail-sender);
      type (message | protocol-only);
    }
  }
}
scan-options {
  content-size-limit value;
}

```

```
(no-uri-check | uri-check);
    timeout value;
}
trickling {
    timeout value;
}
}
sxl-retry value;
sxl-timeout seconds;
}
traceoptions {
    flag flag;
}
type (juniper-express-engine | kaspersky-lab-engine | sophos-engine);
url-whitelist listname;
}
content-filtering {
    profile profile-name {
        block-command protocol-command-list;
        block-content-type (activex | exe | http-cookie | java-applet | zip);
        block-extension extension-list;
        block-mime {
            exception list-name;
            list list-name;
        }
        notification-options {
            custom-message message;
            (no-notify-mail-sender | notify-mail-sender);
            type (message | protocol-only);
        }
        permit-command protocol-command-list;
    }
    traceoptions {
        flag flag;
    }
}
web-filtering {
    juniper-enhanced {
        cache {
            size value;
            timeout value;
        }
        profile profile-name {
            block-message {
                type {
                    custom-redirect-url;
                }
                url url;
            }
            category customurl-list name {
                action (block | log-and-permit | permit);
            }
            custom-block-message value;
            default (block | log-and-permit | permit);
            fallback-settings {
                default (block | log-and-permit);
            }
        }
    }
}
```



```

        server-connectivity (block | log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
    }
    no-safe-search;
    site-reputation-action {
        fairly-safe (block | log-and-permit | permit);
        harmful (block | log-and-permit | permit);
        moderately-safe (block | log-and-permit | permit);
        suspicious (block | log-and-permit | permit);
        very-safe (block | log-and-permit | permit);
    }
    timeout value;
}
server {
    host host-name;
    port number;
}
}
juniper-local {
    profile profile-name {
        custom-block-message value;
        default (block | log-and-permit | permit);
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        timeout value;
    }
}
surf-control-integrated {
    cache {
        size value;
        timeout value;
    }
    profile profile-name {
        category customurl-list name {
            action (block | log-and-permit | permit);
        }
        custom-block-message value;
        default (block | log-and-permit | permit);
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        timeout value;
    }
    server {
        host host-name;
        port number;
    }
}
}

```

```
traceoptions {
  flag flag;
}
type (juniper-enhanced | juniper-local | surf-control-integrated |
  websense-redirect);
url-blacklist listname;
url-whitelist listname;
websense-redirect {
  profile profile-name {
    account value;
    custom-block-message value;
    fallback-settings {
      default (block | log-and-permit);
      server-connectivity (block | log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
    server {
      host host-name;
      port number;
    }
    sockets value;
    timeout value;
  }
}
}
}
ipc {
  traceoptions {
    flag flag;
  }
}
traceoptions {
  flag flag;
}
utm-policy policy-name {
  anti-spam {
    smtp-profile profile-name;
  }
  anti-virus {
    ftp {
      download-profile profile-name;
      upload-profile profile-name;
    }
    http-profile profile-name;
    imap-profile profile-name;
    pop3-profile profile-name;
    smtp-profile profile-name;
  }
}
content-filtering {
  ftp {
    download-profile profile-name;
    upload-profile profile-name;
  }
  http-profile profile-name;
  imap-profile profile-name;
```

```

    pop3-profile profile-name;
    smtp-profile profile-name;
  }
  traffic-options {
    sessions-per-client {
      limit value;
      over-limit (block | log-and-permit);
    }
  }
  web-filtering {
    http-profile profile-name;
  }
}
zones {
  functional-zone {
    management {
      description text;
      host-inbound-traffic {
        protocols protocol-name {
          except;
        }
        system-services service-name {
          except;
        }
      }
    }
    interfaces interface-name {
      host-inbound-traffic {
        protocols protocol-name {
          except;
        }
        system-services service-name {
          except;
        }
      }
    }
    screen screen-name;
  }
}
security-zone zone-name {
  address-book {
    address address-name {
      ip-prefix {
        description text;
      }
      description text;
      dns-name domain-name {
        ipv4-only;
        ipv6-only;
      }
      range-address lower-limit to upper-limit;
      wildcard-address ipv4-address/wildcard-mask;
    }
    address-set address-set-name {
      address address-name;
      address-set address-set-name;
    }
  }
}

```

```

        description text;
    }
}
application-tracking;
description text;
host-inbound-traffic {
    protocols protocol-name {
        except;
    }
    system-services service-name {
        except;
    }
}
interfaces interface-name {
    host-inbound-traffic {
        protocols protocol-name {
            except;
        }
        system-services service-name {
            except;
        }
    }
}
screen screen-name;
tcp-rst;
}
}

```

### Services Configuration Statement Hierarchy

Use the statements in the **services** configuration hierarchy to configure the following parts of the integrated ClearPass authentication and enforcement feature:

- The authentication source and its characteristics, including setting the expiration time for user entries in the ClearPass authentication table.
- The user query function and its parameters to allow the SRX Series device to connect to and query the ClearPass Policy Manager (CPPM) for individual user authentication information.
- Trace options for activity pertaining to the authentication source, the CPPM.

The **services** hierarchy encompasses many other sub-hierarchies that cover different features and functions.

```

services {
    application-identification {
        application application-name {
            address-mapping address-name {
                filter {
                    ip ip-address-and-prefix-length;
                    port-range {
                        tcp [port];
                        udp [port];
                    }
                }
            }
        }
    }
}

```

```

    }
  }
  cacheable;
  description;
  icmp-mapping {
    code number;
    type number;
  }
  ip-protocol-mapping {
    protocol number;
  }
  order number;
  over protocol-type ;
  priority [high | low];
  application-group group-name {
    application-groups application-group-name;
    applications application-name;
  }
  application-system-cache-timeout value;
  download {
    automatic {
      interval hours;
      start-time MM-DD.hh:mm;
    }
    url url;
  }
  enable-performance-mode max-packet-threshold number;
  no-application-identification;
  no-application-system-cache;
  statistics {
    interval minutes;
  }
  traceoptions {
    file {
      filename ;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    level [all | error | info | notice | verbose | warning]
    no-remote-trace;
  }
}
captive-portal {
  authentication-profile-name authentication-profile-name;
  custom-options {
    banner-message string;
    footer-bgcolor hex-color-value;
    footer-message string;
    footer-text-color hex-color-value;
    form-header-bgcolor hex-color-value;
    form-header-message string;
    form-header-text-color hex-color-value;
    form-reset-label label name;
  }
}

```

```
    form-submit-label label name;  
    header-bgcolor hex-color-value;  
    header-logo filename;  
    header-message string;  
    header-text-color hex-color-value;  
    post-authentication-url url-string;  
  }  
  interface (all | interface-name) {  
    quiet-period seconds;  
    retries number-of-retries;  
    server-timeout seconds;  
    session-expiry seconds;  
    supplicant (multiple | single | single-secure);  
  }  
  secure-authentication (http | https);  
  traceoptions {  
    file {  
      filename ;  
      files number;  
      match regular-expression;  
      size maximum-file-size;  
      (world-readable | no-world-readable);  
    }  
    flag flag;  
  }  
}  
flow-monitoring {  
  version9 {  
    template template-name {  
      flow-active-timeout seconds;  
      flow-inactive-timeout seconds;  
      ipv4-template;  
      ipv6-template;  
      option-refresh-rate {  
        packets packets;  
        seconds seconds;  
      }  
      template-refresh-rate {  
        packets packets;  
        seconds seconds;  
      }  
    }  
  }  
}  
}  
ip-monitoring {  
  policy policy-name {  
    match {  
      rpm-probe [probe-name];  
    }  
    no-preempt ;  
    then {  
      interface interface-name (disable | enable);  
      preferred-route {  
        route destination-address {  
          next hop next-hop;  
          preferred-metric metric;  
        }  
      }  
    }  
  }  
}
```

```

        }
        routing-instances name;
    }
}
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}
rpm {
    bgp {
        data-fill data;
        data-size size;
        destination-port port;
        history-size size;
        logical-system logical-system-name <routing-instances routing-instance-name>;
        moving-average-size number-of-samples;
        probe-count count;
        probe-interval seconds;
        probe-type type;
        routing-instances {
            routing-instance-name;
        }
        test-interval seconds;
    }
    probe owner {
        test test-name {
            data-fill data;
            data-size size;
            destination-interface interface-name;
            destination-port port;
            dscp-code-point dscp-bits;
            hardware-timestamp;
            history-size size;
            inet6-options {
                source-address address;
            }
            moving-average-size number;
            next-hop next-hop;
            one-way-hardware-timestamp;
            probe-count count;
            probe-interval seconds;
            probe-type type;
            routing-instance instance-name;
            source-address address;
            target {
                address ipv4-address;
                url url;
            }
        }
    }
}

```

```
        inet6-address ipv6-address;  
        inet6-url url;  
    }  
    test-interval interval;  
    thresholds {  
        egress-time microseconds;  
        ingress-time microseconds;  
        jitter-egress microseconds;  
        jitter-ingress microseconds;  
        jitter-rtt microseconds;  
        rtt microseconds;  
        std-dev-egress microseconds;  
        std-dev-ingress microseconds;  
        std-dev-rtt microseconds;  
        successive-loss count;  
        total-loss count;  
    }  
    traps [ trap-names];  
}  
}  
probe-limit number;  
probe-server {  
    icmp {  
        destination-interface interface-name;  
    }  
    tcp {  
        destination-interface interface-name;  
        port port-number;  
    }  
    udp {  
        destination-interface interface-name;  
        port port-number;  
    }  
}  
service-device-pools {  
    pool pool-name {  
        interface service-device-name;  
    }  
}  
service-interface-pools {  
    pool pool-name {  
        interface service-interface-name;  
    }  
}  
ssl {  
    initiation {  
        profile profile-name {  
            actions {  
                ignore-server-auth-failure;  
            }  
            client-certificate;  
            custom-ciphers [ cipher];  
            enable-flow-tracing;  
            enable-session-cache;  
            preferred-ciphers (custom | medium | strong | weak);  
            protocol-version (all | tls1);
```



```

        trusted-ca (all | [ca-profile] );
    }
}
proxy {
    global-config {
        session-cache-timeout seconds;
    }
    profile profile-name {
        actions {
            crl{
                disable{
                    always;
                }
                if-no-crl;
                disable-session-resumption;
                ignore-server-auth-failure;
                logs {
                    all;
                    errors;
                    info;
                    sessions-allowed;
                    sessions-dropped;
                    sessions-ignored;
                    sessions-whitelisted;
                    warning;
                }
                renegotiation {
                    (allow | allow-secure | drop);
                }
            }
        }
        custom-ciphers [cipher];
        enable-flow-tracing;
        preferred-ciphers (custom | medium | strong | weak);
        root-ca root-certificate;
        trusted-ca (all | [ca-profile] );
        whitelist [global-address-book-addresses];
    }
}
termination {
    profile profile-name {
        custom-ciphers [cipher];
        enable-flow-tracing;
        enable-session-cache;
        preferred-ciphers (custom | medium | strong | weak);
        protocol-version (all | tls1);
        server-certificate certificate-identifier;
    }
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
}

```

```
        level [brief | detail | extensive | verbose];
        no-remote-trace;
    }
}
unified-access-control {
    captive-portal redirect-policy-name {
        redirect-traffic (all | unauthenticated);
        redirect-url redirect-url;
    }
    certificate-verification [ optional | required | warning ];
    infranet-controller host-name {
        address ip-address;
        ca-profile [ca-profile];
        interface interface-name;
        password password;
        port port-number;
        server-certificate-subject subject;
    }
    interval seconds;
    test-only-mode;
    timeout seconds;
    timeout-action (close | no-change | open);
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
}
}
wireless-wan {
    adapter adapter-name {
        adapter-type cx-bridge;
        ip-address ip-address;
        modem {
            usb1 description description;
            usb2 description description;
            usb3 description description;
        }
    }
}
}
```

### **System Configuration Statement Hierarchy**

You use the statements in the **system** configuration hierarchy to configure system management functions overall.

```
system {
    accounting {
        destination {
```

```
radius {
  server server-address {
    accounting-port port-number;
    max-outstanding-requests number;
    port number;
    retry number;
    secret password;
    source-address address;
    timeout seconds;
  }
}
tacplus {
  server server-address {
    port port-number;
    secret password;
    single-connection;
    source-address source-address;
    timeout seconds;
  }
}
}
events [change-log interactive-commands login];
traceoptions {
  file {
    filename;
    files number;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
}
allow-v4mapped-packets;
archival {
  configuration {
    archive-sites url {
      password password;
    }
    transfer-interval interval;
    transfer-on-commit;
  }
}
arp {
  aging-timer minutes;
  gratuitous-arp-delay seconds;
  gratuitous-arp-on-ifup;
  interfaces {
    interface name {
      aging-timer minutes;
    }
  }
  passive-learning;
  purging;
}
authentication-order [password radius tacplus];
```

```
auto-configuration {
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
}
auto-snapshot;
autoinstallation {
  configuration-servers {
    url {
      password password;
    }
  }
  interfaces {
    interface-name {
      bootp;
      rarp;
    }
  }
  usb {
    disable;
  }
}
auto-snapshot;
backup-router {
  address;
  destination [network];
}
commit {
  server {
    commit-interval seconds;
    days-to-keep-error-logs days;
    maximum-aggregate-pool number;
    maximum entries number;
    traceoptions {
      file {
        filename;
        files number;
        microsecond-stamp;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      no-remote-trace;
    }
  }
}
synchronize;
}
```

```

compress-configuration-files;
default-address-selection;
diag-port-authentication {
    encrypted-password passsword;
    plain-text-password;
}
domain-name domain-name;
domain-search [domain-list];
donot-disable-ip6op-ondad;
dump-device (boot-device | compact-flash | usb);
dynamic-profile-options {
    versioning;
}
encrypt-configuration-files;
extensions {
    providers {
        provider-id {
            license-type license deployment-scope [deployments];
        }
    }
    resource-limits {
        package package-name {
            resources {
                cpu {
                    priority number;
                    time seconds;
                }
                file {
                    core-size bytes;
                    open number;
                    size bytes;
                }
                memory {
                    data-size mbytes;
                    locked-in mbytes;
                    resident-set-size mbytes;
                    socket-buffers mbytes;
                    stack-size mbytes;
                }
            }
        }
    }
}
process process-ui-name {
    resources {
        cpu {
            priority number;
            time seconds;
        }
        file {
            core-size bytes;
            open number;
            size bytes;
        }
        memory {
            data-size mbytes;
            locked-in mbytes;
            resident-set-size mbytes;
        }
    }
}

```

```

        socket-buffers mbytes;
        stack-size mbytes;
    }
}
}
fips {
    level (0 | 1 | 2 | 3 | 4);
}
host-name hostname;
inet6-backup-router {
    address;
    destination destination;
}
Internet-options {
    icmpv4-rate-limit {
        bucket-size seconds;
        packet-rate packets-per-second;
    }
    icmpv6-rate-limit {
        bucket-size seconds;
        packet-rate packets-per-second;
    }
    (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
    ipv6-duplicate-addr-detection-transmits number;
    (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
    ipv6-path-mtu-discovery-timeout minutes;
    no-tcp-reset (drop-all-tcp | drop-tcp-with-syn-only);
    no-tcp-rfc1323;
    no-tcp-rfc1323-paws;
    (path-mtu-discovery | no-path-mtu-discovery);
    source-port upper-limit upper-limit;
    (source-quench | no-source-quench);
    tcp-drop-synfin-set;
    tcp-mss bytes;
}
kernel-replication;
license {
    autoupdate {
        url url;
        password password;
    }
    renew {
        before-expiration number;
        interval interval-hours;
    }
    traceoptions {
        file {
            filename ;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
    }
}

```

```

        no-remote-trace;
    }
}
location {
    altitude feet;
    building name;
    country-code code;
    floor number;
    hcoord horizontal-coordinate;
    lata service-area;
    latitude degrees;
    longitude degrees;
    npa-nxx number;
    postal-code postal-code;
    rack number;
    vcoord vertical-coordinate;
}
login {
    announcement text;
    class class-name {
        access-end hh:mm;
        access-start hh:mm;
        allow-commands regular-expression;
        allow-configuration regular-expression;
        allow-configuration-regexps [regular-expression];
        allowed-days [day];
        deny-commands regular-expression;
        deny-configuration regular-expression;
        deny-configuration-regexps [regular-expression];
        idle-timeout minutes;
        logical-system logical-system;
        login-alarms;
        login-script script;
        login-tip;
        permissions [permissions ];
        security-role (audit-administrator | crypto-administrator | ids-administrator |
            security-administrator);
    }
    deny-sources {
        address [address-or-hostname];
    }
    message text;
}
password {
    change-type (character-set | set-transitions);
    format (des | md5 | sha1);
    maximum-length length;
    minimum-changes number;
    minimum-length length;
}
retry-options {
    backoff-factor seconds;
    backoff-threshold number;
    lockout-period time;
    maximum-time seconds;
    minimum-time seconds;
}

```

```
    tries-before-disconnect number;
  }
  user username {
    authentication {
      encrypted-password password;
      load-key-file url;
      plain-text-password;
      ssh-dsa public-key;
      ssh-rsa public-key;
    }
    class class-name;
    full-name complete-name;
    uid uid-value;
  }
}
log-vital {
  interval minutes;
  files days;
  storage-limit percentage;
  file-size Mbytes;
  add oid{
    comment comment;
  }
  group {
    operating;
    idp;
    storage;
    cluster-counter;
    screen zone-name;
    spu spu-name;
  }
}
max-configuration-rollback number;
max-configurations-on-flash number;
mirror-flash-on-disk;
name-server ip-address;
nd-maxmcast-solicit value;
nd-retransmit-timer value;
no-compress-configuration-files;
no-debugger-on-alt-break;
no-multicast-echo;
no-neighbor-learn;
no-ping-record-route;
no-ping-time-stamp;
no-redirects;
no-saved-core-context;
ntp {
  authentication-key key-number {
    type md5;
    value password;
  }
  boot-server address;
  broadcast broadcast-address {
    key key;
    ttl value;
    version version;
  }
}
```



```

    }
    broadcast-client;
    multicast-client {
        address;
    }
    peer peer-address {
        key key;
        prefer;
        version version;
    }
    server server-address {
        key key;
        prefer;
        version version;
    }
    source-address source-address;
    trusted-key [key-number];
}
pic-console-authentication {
    encrypted-password password;
    plain-text-password;
}
ports {
    auxiliary {
        disable;
        insecure;
        type (ansi | small-xterm | vt100 | xterm);
    }
    console {
        disable;
        insecure;
        log-out-on-disconnect;
        type (ansi | small-xterm | vt100 | xterm);
    }
}
processes {
    802.1x-protocol-daemon {
        command binary-file-path;
        disable;
    }
    adaptive-services {
        command binary-file-path;
        disable;
        failover (alternate-media | other-routing-engine);
    }
    alarm-control {
        command binary-file-path;
        disable;
        failover (alternate-media | other-routing-engine);
    }
    application-identification {
        command binary-file-path;
        disable;
        failover (alternate-media | other-routing-engine);
    }
    application-security {

```

```
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
audit-process {  
    command binary-file-path;  
    disable;  
}  
auto-configuration {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
bootp {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
chassis-control {  
    disable;  
    failover alternate-media;  
}  
class-of-service {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
craft-control {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
database-replication {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
datapath-trace-service {  
    disable;  
    traceoptions {  
        file {  
            filename ;  
            files number;  
            match regular-expression;  
            size maximum-file-size;  
            (world-readable | no-world-readable);  
        }  
        flag flag;  
        level (all | error | info | notice | verbose | warning);  
        no-remote-trace;  
    }  
}  
dhcp {  
    command binary-file-path;  
    disable;  
}
```

```
dhcp-service {
  disable;
  failover (alternate-media | other-routing-engine);
  interface-traceoptions {
    file {
      filename ;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
  traceoptions {
    file {
      filename ;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
}
dialer-services {
  disable;
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
diameter-service {
  disable;
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
}
```

```
}
disk-monitoring {
    command binary-file-path;
    disable;
}
dynamic-flow-capture {
    command binary-file-path;
    disable;
}
ecc-error-logging {
    command binary-file-path;
    disable;
}
ethernet-connectivity-fault-management {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
ethernet-link-fault-management {
    command binary-file-path;
    disable;
}
ethernet-switching {
    command binary-file-path;
    disable;
}
event-processing {
    command binary-file-path;
    disable;
}
fipsd {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
firewall {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
firewall-authentication-service {
    disable;
}
forwarding {
    command binary-file-path;
    disable;
}
general-authentication-service {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
    }
}
```

```
    }
    flag flag;
    no-remote-trace;
  }
}
gprs-process {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
group-key-member {
  disable;
}
group-key-server {
  disable;
}
idp-policy {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
ilmi {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
inet-process {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
init {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
interface-control {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
ipmi {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
ipsec-key-management {
  (disable | enable);
}
jsrp-service {
  disable;
}
jtasktest {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
```

```
}
kernel-replication {
    command binary-file-path;
    disable;
}
l2-learning {
    command binary-file-path;
    disable;
}
l2cpd-service {
    command binary-file-path;
    disable;
}
lACP {
    command binary-file-path;
    disable;
}
lldpd-service {
    command binary-file-path;
    disable;
}
logical-system-mux {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
logical-system-service {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
mib-process {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
mobile-ip {
    command binary-file-path;
    disable;
}
mountd-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
mspd {
    command binary-file-path;
```

```
    disable;
    failover (alternate-media | other-routing-engine);
}
multicast-snooping {
    command binary-file-path;
    disable;
}
named-service {
    disable;
    failover (alternate-media | other-routing-engine);
}
neighbor-liveness {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
network-security {
    disable;
}
network-security-trace {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
nfsd-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
ntp {
    disable;
    failover (alternate-media | other-routing-engine);
}
ntpd-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
peer-selection-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
periodic-packet-services {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
pgcp-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
pgm {
    command binary-file-path;
    disable;
```

```
    failover (alternate-media | other-routing-engine);
  }
pic-services-logging {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
ppp {
  command binary-file-path;
  disable;
}
pppoe {
  command binary-file-path;
  disable;
}
process-monitor {
  disable;
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
}
profilerd {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
r2cp {
  command binary-file-path;
  disable;
}
redundancy-interface-process {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
remote-operations {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
resource-cleanup {
  disable;
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
    }
  }
}
```



```

        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
}
routing {
    disable;
    failover (alternate-media | other-routing-engine);
}
sampling {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
sbc-configuration-process {
    disable;
    failover (alternate-media | other-routing-engine);
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
}
sdk-service {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        level (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
}
}
secure-neighbor-discovery {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
}
security-log {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}

```

```
}
send {
  disable;
}
service-deployment {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
shm-rtssdbd {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
simple-mail-client-service {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
smtpd-service {
  disable;
}
snmp {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
static-subscribers {
  disable;
}
statistics-service {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
subscriber-management {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
subscriber-management-helper {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
system-health-management {
  disable;
}
system-log-vital {
  disable;
}
tunnel-oamd {
  command binary-file-path;
  disable;
}
uac-service {
```

```

    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
usb-control {
    command binary-file-path;
    disable;
}
virtualization-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
vrrp {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
wan-acceleration {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
watchdog {
    enable;
    disable;
    timeout value;
}
webapi {
    client ip-address;
    (http port port-number | https
    {
        certificate local-file-system-certificate-filename;
        certificate-key local-certificate-key;
        default-certificate;
        pki-local-certificate certificate-name;
        port port-number;
    }
    )
    user {
        name;
        password password;
    }
    debug-level [crit | emerg | error | notice | warn];
    debug-log filename;
}
web-management {

```

```
    disable;
    failover (alternate media | other-routing-engine);
  }
  webapi {
    client ip-address;
    (http port port-number | https
    {
      certificate local-file-system-certificate-filename;
      certificate-key local-certificate-key;
      default-certificate;
      pki-local-certificate certificate-name;
      port port-number;
    }
  )
  user {
    name;
    password password;
  }
  debug-level [crit | emerg | error | notice | warn];
  debug-log filename;
}
wireless-lan-service {
  disable;
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
wireless-wan-service {
  disable;
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
proxy {
  password password;
  port port-number;
  server url;
  username user-name;
}
radius-options {
```

```

    attributes {
        nas-ip-address nas-ip-address;
    }
    password-protocol mschap-v2;
}
radius-server server-address {
    accounting-port number;
    max-outstanding-requests number;
    port number;
    retry number;
    secret password;
    source-address source-address;
    timeout seconds;
}
root-authentication {
    encrypted-password password;
    load-key-file url;
    plain-text-password;
    ssh-dsa public-key {
        <from pattern-list>;
    }
    ssh-rsa public-key {
        <from pattern-list>;
    }
}
saved-core-context;
saved-core-files number;
scripts {
    commit {
        allow-transients;
        direct-access;
        file filename {
            checksum (md5 | sha-256 | sha1);
            optional;
            refresh;
            refresh-from url;
            source url;
        }
        refresh;
        refresh-from url;
        traceoptions {
            file {
                filename;
                files number;
                size maximum-file-size;
                (world-readable | no-world-readable);
            }
            flag flag;
            no-remote-trace;
        }
    }
}
load-scripts-from-flash;
op {
    file filename {
        arguments name {
            description text;

```

```
    }
    checksum (md5 | sha-256 | sha1);
    command filename-alias;
    description cli-help-text;
    refresh;
    refresh-from url;
    source url;
  }
  no-allow-url;
  refresh;
  refresh-from url;
  traceoptions {
    file {
      filename;
      files number;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
security-profile security-profile-name {
  address-book {
    maximum amount;
    reserved amount;
  }
  appfw-profile {
    maximum amount;
    reserved amount;
  }
  appfw-rule {
    maximum amount;
    reserved amount;
  }
  appfw-rule-set {
    maximum amount;
    reserved amount;
  }
  auth-entry {
    maximum amount;
    reserved amount;
  }
  cpu {
    reserved percent;
  }
  dslite-software-initiator {
    maximum amount;
    reserved amount;
  }
  flow-gate {
    maximum amount;
    reserved amount;
  }
  flow-session {
    maximum amount;
```

```
    reserved amount;
}
idp-policy idp-policy-name;
logical-system logical-system-name;
nat-cone-binding {
    maximum amount;
    reserved amount;
}
nat-destination-pool {
    maximum amount;
    reserved amount;
}
nat-destination-rule {
    maximum amount;
    reserved amount;
}
nat-interface-port-ol {
    maximum amount;
    reserved amount;
}
nat-nopat-address {
    maximum amount;
    reserved amount;
}
nat-pat-address {
    maximum amount;
    reserved amount;
}
nat-pat-portnum {
    maximum amount
    reserved amount
}
nat-port-ol-ipnumber {
    maximum amount;
    reserved amount;
}
nat-rule-referenced-prefix {
    maximum amount;
    reserved amount;
}
nat-source-pool {
    maximum amount;
    reserved amount;
}
nat-source-rule {
    maximum amount;
    reserved amount;
}
nat-static-rule {
    maximum amount;
    reserved amount;
}
policy {
    maximum amount;
    reserved amount;
}
```

```

    policy-with-count {
        maximum amount;
        reserved amount;
    }
    root-logical-system;
    scheduler {
        maximum amount;
        reserved amount;
    }
    zone {
        maximum amount;
        reserved amount;
    }
}
security-profile-resources {
    cpu-control;
    cpu-control-target percent;
}
services {
    database-replication {
        traceoptions {
            file {
                filename ;
                files number;
                match regular-expression;
                size maximum-file-size;
                (world-readable | no-world-readable);
            }
            flag flag;
            no-remote-trace;
        }
    }
}
dhcp {
    boot-file filename;
    boot-server (address | hostname);
    default-lease-time (infinite | seconds);
    domain-name domain-name;
    domain-search dns-search-suffix;
    maximum-lease-time (infinite | seconds);
    name-server ip-address;
    next-server ip-address;
    option option-identifier-code array type-name [ type-values ] | byte 8-bit-value | flag
        (false | off | on | true) | integer signed-32-bit-value | ip-address address | short
        signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
        unsigned-short 16-bit-value);
    pool subnet-ip-address/mask {
        address-range {
            high address;
            low address;
        }
        boot-file filename;
        boot-server (address | hostname);
        default-lease-time (infinite | seconds);
        domain-name domain-name;
        domain-search dns-search-suffix;
        exclude-address ip-address;
    }
}

```



```

maximum-lease-time (infinite | seconds);
name-server ip-address;
next-server ip-address;
option option-identifier-code array type-name [ type-values ] | byte 8-bit-value |
    flag (false | off | on | true) | integer signed-32-bit-value | ip-address address |
    short signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
    unsigned-short 16-bit-value);
propagate-ppp-settings interface-name;
propagate-settings interface-name;
router ip-address;
server-identifier dhcp-server;
sip-server {
    address ip-address;
    name sip-server-name;
}
wins-server ip-address;
}
propagate-ppp-settings interface-name;
propagate-settings interface-name;
router ip-address;
server-identifier dhcp-server;
sip-server {
    address ip-address;
    name sip-server-name;
}
static-binding mac-address;
traceoptions {
    file {
        filename ;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
wins-server ip-address;
}
dhcp-local-server {
    dhcpv6 {
        authentication {
            password password;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name;
                interface-name;
                logical-system-name;
                relay-agent-interface-id;
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix;
            }
        }
    }
}

```

```
    }
  }
  dynamic-profile {
    profile-name;
    aggregate-clients {
      merge;
      replace;
    }
    junos-default-profile;
    use-primary dynamic-profile-name;
  }
  group group-name {
    authentication {
      password password;
      username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name;
        interface-name;
        logical-system-name;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix;
      }
    }
  }
  dynamic-profile {
    profile-name;
    aggregate-clients {
      merge;
      replace;
    }
    junos-default-profile;
    use-primary dynamic-profile;
  }
  interface interface-name {
    dynamic-profile {
      profile-name;
      aggregate-clients {
        merge;
        replace;
      }
      junos-default-profile;
      use-primary dynamic-profile-name;
    }
    exclude;
    overrides {
      delegated-pool pool-name;
      interface-client-limit number;
      process-inform {
        pool pool-name;
      }
      rapid-commit ;
    }
  }
```

```

    service-profile service-profile-name
    trace ;
    upto interface-name;
  }
  liveness-detection {
    failure-action {
      clear-binding;
      clear-binding-if-interface-up;
      log-only;
    }
    method {
      bfd {
        detection-time {
          threshold milliseconds;
        }
        holddown-interval interval;
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        session-mode (automatic | multihop | single-hop);
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        version (0 | 1 | automatic);
      }
    }
  }
  overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    rapid-commit ;
  }
  reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
      radius-disconnect;
    }
  }
  service-profile service-profile-name;
}
liveness-detection {
  failure-action {
    clear-binding;
    clear-binding-if-interface-up;
    log-only;
  }
  method {
    bfd {

```

```

        detection-time {
            threshold milliseconds;
        }
        holddown-interval interval;
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        session-mode (automatic | multihop | single-hop);
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        version (0 | 1 | automatic);
    }
}
overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit ;
}
reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
}
service-profile service-profile-name;
}
group group-name {
    interface interface-name {
        exclude;
        upto upto-interface-name;
    }
}
}
dns {
    dns-proxy {
        cache hostname inet ip-address;
        default-domain domain-name {
            forwarders ip-address;
        }
        interface interface-name;
        propogate-setting (enable | disable);
        view view-name {
            domain domain-name {
                forward-only;
                forwarders ip-address;
            }
        }
    }
}

```

```

        match-clients subnet-address;
    }
}
}
dnssec {
    disable;
    dlv {
        domain-name domain-name trusted-anchor trusted-anchor;
    }
    secure-domains domain-name;
    trusted-keys (key dns-key | load-key-file url);
    forwarders {
        ip-address;
    }
    max-cache-ttl seconds;
    max-ncache-ttl seconds;
    traceoptions {
        category {
            category-type;
        }
        debug-level level;
        file {
            filename;
            files number;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        level (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
}
dynamic-dns {
    client hostname {
        agent agent-name;
        interface interface-name;
        password server-password;
        server server-name;
        username user-name;
    }
}
finger {
    connection-limit number;
    rate-limit number;
}
ftp {
    connection-limit number;
    rate-limit number;
}
netconf {
    ssh {
        connection-limit number;
        port port-number;
        rate-limit number;
    }
    traceoptions {

```

```
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
    on-demand;
}
}
outbound-ssh {
    client client-id {
        address {
            port port-number;
            retry number;
            timeout value;
        }
        device-id device-id;
        keep-alive {
            retry number;
            time-out value;
        }
        reconnect-strategy (in-order | sticky);
        secret secret;
        services {
            netconf;
        }
    }
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}
service-deployment {
    local-certificate certificate-name;
    servers server-address {
        port port-number;
        security-options {
            ssl3;
            tls;
        }
        user user-name;
    }
}
source-address source-address;
traceoptions {
    file {
        filename;
```

```

        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}
ssh {
    ciphers [cipher];
    client-alive-count-max number;
    client-alive-interval seconds;
    connection-limit number;
    hostkey-algorithm {
        (ssh-dss | no-ssh-dss);
        (ssh-ecdsa | no-ssh-ecdsa);
        (ssh-rsa | no-ssh-rsa);
    }
    key-exchange [algorithm];
    macs [algorithm];
    max-sessions-per-connection number;
    protocol-version {
        v1;
        v2;
    }
    rate-limit number;
    root-login (allow | deny | deny-password);
    (tcp-forwarding | no-tcp-forwarding);
}
subscriber-management {
    enforce-strict-scale-limit-license;
    gres-route-flush-delay;
    maintain-subscriber interface-delete;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
subscriber-management-helper {
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
    }
}

```

```
        no-remote-trace;
    }
}
telnet {
    connection-limit number;
    rate-limit number;
}
web-management {
    control {
        max-threads number;
    }
    http {
        interface [interface-name];
        port port-number;
    }
    https {
        interface [interface-name];
        local-certificate name;
        pki-local-certificate certificate-name;
        port port-number;
        system-generated-certificate;
    }
    management-url url;
    session {
        idle-timeout minutes;
        session-limit number;
    }
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        level (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
}
here
xnm-clear-text {
    connection-limit number;
    rate-limit number;
}
xnm-ssl {
    connection-limit number;
    local-certificate name;
    rate-limit number;
}
}
static-host-mapping hostname {
    alias [host-name-alias];
    inet [ip- address];
    inet6 [ipv6- address];
    sysid system-identifier;
```



```

}
syslog {
  allow-duplicates;
  archive {
    binary-data;
    files number;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  console {
    (any | facility) severity;
  }
  file filename {
    allow-duplicates;
    archive {
      archive-sites url {
        password password;
      }
      (binary-data | no-binary-data);
      files number;
      size maximum-file-size;
      start-time "YYYY-MM-DD.hh:mm";
      transfer-interval minutes;
      (world-readable | no-world-readable);
    }
    structure-data {
      brief;
    }
    (any | facility) severity;
  }
  host (hostname | other-routing-engine) {
    (any | facility) severity;
  }
  log-rotate-frequency minutes;
  source-address source-address;
  time-format {
    millisecond;
    year;
  }
  user (username | *) {
    (any | facility) severity;
  }
}
tacplus-options {
  (exclude-cmd-attribute | no-cmd-attribute-value);
  service-name service-name;
}
tacplus-server server-address {
  port port-number;
  secret password;
  single-connection;
  source-address source-address;
  timeout seconds;
}
time-zone (GMThour-offset | time-zone);
tracing {

```

```
destination-override {
  syslog {
    host address;
  }
}
use-imported-time-zones;
}
```

**[edit security log] Hierarchy Level**

```
log {
  cache {
    exclude exclude-name {
      destination-address destination-address;
      destination-port destination-port;
      event-id event-id;
      failure;
      interface-name interface-name;
      policy-name policy-name;
      process process-name;
      protocol protocol;
      source-address source-address;
      source-port source-port;
      success;
      user-name user-name;
    }
    limit value;
  }
  disable;
  event-rate rate;
  facility-override;
  file {
    files max-file-number;
    name file-name;
    path binary-log-file-path;
    size maximum-file-size;
  }
  format (binary | sd-syslog | syslog);
  mode (event | stream);
  rate-cap rate-cap-value;
  (source-address source-address | source-interface interface-name);
  stream stream-name {
    category (all | content-security);
    format (binary | sd-syslog | syslog | welf);
    filter threat-attack
    host {
      ip-address;
      port port-number;
    }
    rate-limit log-server-limit
    severity (alert | critical | debug | emergency | error | info | notice | warning);
  }
  traceoptions {
    file {
      filename;
    }
  }
}
```

```

    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
transport {
  protocol (udp | tcp | tls);
  tls-profile tls-profile-name;
  tcp-connections tcp-connections;
}
utc-time-stamp;
}

```

#### **[edit services user-identification] Hierarchy Level**

```

user-identification {
  authentication-source name {
    authentication-entry-timeout minutes;
    no-user-query;
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      level level ;
      no-remote-trace;
    }
  }
  user-query {
    ca-certificate ca-certificate-filename;
    client-id client-id;
    client-secret client-secret;
    delay-query-time delay-time-in-seconds;
    query-api user-query-api;
    token-api token-api-path
    web-server {
      server-name
      address (ip-address | hostname);
      connect-method (http | https) ;
      port web-server-port;
    }
  }
}

```

#### **[edit system services] Hierarchy Level**

```

services {
  database-replication {
    traceoptions {
      file {

```

```

        filename ;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}
dhcp {
    boot-file filename;
    boot-server (address | hostname);
    default-lease-time (infinite | seconds);
    domain-name domain-name;
    domain-search dns-search-suffix;
    maximum-lease-time (infinite | seconds);
    name-server ip-address;
    next-server ip-address;
    option option-identifier-code array type-name [ type-values ] | byte 8-bit-value | flag
        (false | off | on | true) | integer signed-32-bit-value | ip-address address | short
        signed-16-bit-value | string text-string | unsigned-integer 32-bit-value | unsigned-short
        16-bit-value);
    pool subnet-ip-address/mask {
        address-range {
            high address;
            low address;
        }
        boot-file filename;
        boot-server (address | hostname);
        default-lease-time (infinite | seconds);
        domain-name domain-name;
        domain-search dns-search-suffix;
        exclude-address ip-address;
        maximum-lease-time (infinite | seconds);
        name-server ip-address;
        next-server ip-address;
        option option-identifier-code array type-name [ type-values ] | byte 8-bit-value | flag
            (false | off | on | true) | integer signed-32-bit-value | ip-address address | short
            signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
            unsigned-short 16-bit-value);
        propagate-ppp-settings interface-name;
        propagate-settings interface-name;
        router ip-address;
        server-identifier dhcp-server;
        sip-server {
            address ip-address;
            name sip-server-name;
        }
        wins-server ip-address;
    }
    propagate-ppp-settings interface-name;
    propagate-settings interface-name;
    router ip-address;
    server-identifier dhcp-server;
    sip-server {

```

```

    address ip-address;
    name sip-server-name;
}
static-binding mac-address;
traceoptions {
    file {
        filename ;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
wins-server ip-address;
}
dhcp-local-server {
    dhcpv6 {
        authentication {
            password password;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name;
                interface-name;
                logical-system-name;
                relay-agent-interface-id;
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix;
            }
        }
    }
    dynamic-profile {
        profile-name;
        aggregate-clients {
            merge;
            replace;
        }
        junos-default-profile;
        use-primary dynamic-profile-name;
    }
    group group-name {
        authentication {
            password password;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name;
                interface-name;
                logical-system-name;
                relay-agent-interface-id;
            }
        }
    }
}

```

```
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix;
    }
}
dynamic-profile {
    profile-name;
    aggregate-clients {
        merge;
        replace;
    }
    junos-default-profile;
    use-primary dynamic-profile;
}
interface interface-name {
    dynamic-profile {
        profile-name;
        aggregate-clients {
            merge;
            replace;
        }
        junos-default-profile;
        use-primary dynamic-profile-name;
    }
    exclude;
    overrides {
        delegated-pool pool-name;
        interface-client-limit number;
        process-inform {
            pool pool-name;
        }
        rapid-commit ;
    }
    service-profile service-profile-name
    trace ;
    upto interface-name;
}
liveness-detection {
    failure-action {
        clear-binding;
        clear-binding-if-interface-up;
        log-only;
    }
    method {
        bfd {
            detection-time {
                threshold milliseconds;
            }
            holddown-interval interval;
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            session-mode (automatic | multihop | single-hop);
            transmit-interval {
```

```

        minimum-interval milliseconds;
        threshold milliseconds;
    }
    version (0 | 1 | automatic);
}
}
overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit ;
}
reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
}
service-profile service-profile-name;
}
liveness-detection {
    failure-action {
        clear-binding;
        clear-binding-if-interface-up;
        log-only;
    }
}
method {
    bfd {
        detection-time {
            threshold milliseconds;
        }
        holddown-interval interval;
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        session-mode (automatic | multihop | single-hop);
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        version (0 | 1 | automatic);
    }
}
}
overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
}

```

```

        rapid-commit ;
    }
    reconfigure {
        attempts number;
        clear-on-abort;
        strict;
        timeout number;
        token token-name;
        trigger {
            radius-disconnect;
        }
    }
    service-profile service-profile-name;
}
group group-name {
    interface interface-name {
        exclude;
        upto upto-interface-name;
    }
}
}
dns {
    dns-proxy {
        cache hostname inet ip-address;
        default-domain domain-name {
            forwarders ip-address;
        }
        interface interface-name;
        propogate-setting (enable | disable);
        view view-name {
            domain domain-name {
                forward-only;
                forwarders ip-address;
            }
            match-clients subnet-address;
        }
    }
}
}
dnssec {
    disable;
    dlv {
        domain-name domain-name trusted-anchor trusted-anchor;
    }
    secure-domains domain-name;
    trusted-keys (key dns-key | load-key-file url);
    forwarders {
        ip-address;
    }
    max-cache-ttl seconds;
    max-ncache-ttl seconds;
    traceoptions {
        category {
            category-type;
        }
        debug-level level;
        file {

```



```

        filename;
        files number;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
}
dynamic-dns {
    client hostname {
        agent agent-name;
        interface interface-name;
        password server-password;
        server server-name;
        username user-name;
    }
}
finger {
    connection-limit number;
    rate-limit number;
}
ftp {
    connection-limit number;
    rate-limit number;
}
netconf {
    ssh {
        connection-limit number;
        port port-number;
        rate-limit number;
    }
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
        on-demand;
    }
}
outbound-ssh {
    client client-id {
        address {
            port port-number;
            retry number;
            timeout value;
        }
        device-id device-id;
        keep-alive {
            retry number;

```

```
        time-out value;
    }
    reconnect-strategy (in-order | sticky);
    secret secret;
    services {
        netconf;
    }
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}
service-deployment {
    local-certificate certificate-name;
    servers server-address {
        port port-number;
        security-options {
            ssl3;
            tls;
        }
        user user-name;
    }
}
source-address source-address;
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}
ssh {
    ciphers [cipher];
    client-alive-count-max number;
    client-alive-interval seconds;
    connection-limit number;
    hostkey-algorithm {
        (ssh-dss | no-ssh-dss);
        (ssh-ecdsa | no-ssh-ecdsa);
        (ssh-rsa | no-ssh-rsa);
    }
    key-exchange [algorithm];
    macs [algorithm];
    max-sessions-per-connection number;
```

```

protocol-version {
  v1;
  v2;
}
rate-limit number;
root-login (allow | deny | deny-password);
(tcp-forwarding | no-tcp-forwarding);
}
subscriber-management {
  enforce-strict-scale-limit-license;
  gres-route-flush-delay;
  maintain-subscriber interface-delete;
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
subscriber-management-helper {
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
telnet {
  connection-limit number;
  rate-limit number;
}
webapi {
  client ip-address;
  (http port port-number | https
  {
    certificate local-file-system-certificate-filename;
    certificate-key local-certificate-key;
    default-certificate;
    pki-local-certificate certificate-name;
    port port-number;
  }
)
user {
  name;
  password password;
}

```

```
debug-level [crit | emerg | error | notice | warn];
debug-log filename;
}
web-management {
  control {
    max-threads number;
  }
  http {
    interface [interface-name];
    port port-number;
  }
  https {
    interface [interface-name];
    local-certificate name;
    pki-local-certificate certificate-name;
    port port-number;
    system-generated-certificate;
  }
  management-url url;
  session {
    idle-timeout minutes;
    session-limit number;
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
}
webapi {
  client ip-address;
  (http port port-number | https
  {
    certificate local-file-system-certificate-filename;
    certificate-key local-certificate-key;
    default-certificate;
    pki-local-certificate certificate-name;
    port port-number;
  }
)
  user {
    name;
    password password;
  }
  debug-level [crit | emerg | error | notice | warn];
  debug-log filename;
}
xnm-clear-text {
  connection-limit number;
```

```

        rate-limit number;
    }
    xnm-ssl {
        connection-limit number;
        local-certificate name;
        rate-limit number;
    }
}

```

## address (Services User Identification)

<b>Syntax</b>	<code>address (<i>ip-address</i>   <i>hostname</i>);</code>
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass user-query web-server]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	Configure for the integrated ClearPass authentication and enforcement feature the address of the ClearPass webserver that the SRX Series device communicates with. The SRX Series device requests user authentication and identity information for an individual user from the ClearPass webserver whose address is configured. If you configure the user query function, the SRX Series device can obtain this information for a specific user when it does not receive it from the ClearPass Policy Manager through Web API POST requests.
<b>Required Privilege Level</b>	services—To view this statement in the configuration services-control—To add this statement to the configuration.

## authentication-entry-timeout (Services User Identification)

<b>Syntax</b>	<code>authentication-entry-timeout <i>minutes</i>;</code>
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Configure for the integrated ClearPass authentication and enforcement feature the timeout interval after which idle entries in the ClearPass authentication table expire. The value is expressed in minutes. The timeout interval begins from when the user authentication entry is added to the ClearPass authentication table. The default value is 30 minutes.</p> <p>Default: 30 minutes</p> <p>Range: 10 through 1440 minutes. If a value of 0 is specified, the entries will never expire.</p>
<b>Required Privilege Level</b>	services—To view this statement in the configuration services-control—To add this statement to the configuration.

## authentication-source (Security User Identification)

---

<b>Syntax</b>	<pre>authentication-source {     active-directory-authentication-table (disable   priority <i>priority</i>);     aruba-clearpass (disable   priority <i>priority</i>);     local-authentication-table (disable   priority <i>priority</i>);     unified-access-control (disable   priority <i>priority</i>); }</pre>
<b>Hierarchy Level</b>	[edit security user-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Configure the authentication table priority order. Low number takes precedence. The SRX Series device searches the authentication tables for user authentication entries in the specified priority order. To ensure that it checks the ClearPass authentication table first, configure the lowest number for the ClearPass authentication table priority value, which is identified by <b>aruba-clearpass</b>.</p> <p>If an entry for the user is not found in the ClearPass authentication table, other authentication tables are searched in the specified priority.</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>

## authentication-source (Services User Identification)

```

Syntax authentication-source name {
    authentication-entry-timeout minutes;
    no-user-query;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable |no-world-readable);
        }
        flag flag;
        level level ;
        no-remote-trace;
    }
}

```

**Hierarchy Level** [edit services user-identification]

**Release Information** Statement introduced in Junos OS Release 12.3X48-D30.

**Description** Configure ClearPass as the authentication source for the integrated ClearPass authentication and enforcement feature. You must specify `aruba-clearpass` as the value of authentication source *name*, followed by its defining characteristics. You cannot specify the authentication source alone—that is, apart from its configuration parameters that qualify it.

The ClearPass Policy Manager (CPPM), as the authentication source and client of the SRX Series device HTTP server, initiates a connection to the SRX Series device using the Web API that the SRX Series device exposes to it. The CPPM sends user authentication and identity information to the SRX Series device across this connection using HTTP or HTTPS POST request messages.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.


## ca-certificate (Services User Identification)

---

<b>Syntax</b>	<code>ca-certificate <i>certificate-file</i>;</code>
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass user-query https]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Specify the certificate file that the SRX Series device uses to verify the ClearPass server's certificate for the SSL connection that is used for the user query function.</p> <p>As the ClearPass administrator, you must export the server's certificate from the ClearPass Policy Manager (CPPM) and import it to the SRX Series device. Afterward, you must configure the ca-certificate path and the certificate filename on the SRX Series device. Here is an example:</p> <pre>'/var/tmp/RADIUSServerCertificate.crt'</pre> <p>This configuration is part of the integrated ClearPass authentication and enforcement feature user query function. User query enables the SRX Series device to query the CPPM for authentication and identity information for an individual user under certain circumstance when it does not receive that information from the CPPM through the Web API POST request messages.</p>
<b>Required Privilege Level</b>	<p>services—To view this statement in the configuration.</p> <p>services-control—To add this statement to the configuration.</p>



## certificate (System Services)

<b>Syntax</b>	<code>certificate <i>certificate-filename</i>;</code>
<b>Hierarchy Level</b>	[edit system services webapi https]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Configure a custom certificate. A certificate is required when HTTPS is used for the Web API function (webapi), which allows the ClearPass Policy Manager (CPPM) to initiate a connection to the SRX Series device.</p> <p>The Web API daemon (webapi), which acts as an HTTP or HTTPS server, allows the CPPM, acting as a client, to send user authentication and identity information to the SRX Series device. The Web API function is part of the integrated ClearPass authentication and enforcement feature that uses Aruba ClearPass as its authentication source.</p> <p>When you configure the Web API daemon to use HTTPS, you can use the default certificate, a custom one, or a certificate generated by the public key infrastructure (PKI) local store.</p> <p>If you configure a custom certificate, you must configure a certificate key with it. Here is an example of how to configure a certificate and certificate key:</p> <pre>set system services webapi https certificate /var/tmp/certificate.crt set system services webapi https certificate-key /var/tmp/certificate.key</pre> <p> <b>NOTE:</b> The Web API function supports only the Privacy-Enhanced Mail (PEM) format for the custom certificate and certificate key.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

## certificate-key (System Services)

---

<b>Syntax</b>	<code>certificate-key <i>filename</i>;</code>
<b>Hierarchy Level</b>	[edit system services webapi https]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	Configure the filename of the certificate key to use with the specified custom certificate for the Web API function HTTPS configuration. A certificate key is required if a custom certificate file is used.



**NOTE:** The integrated ClearPass feature Web API function supports only the Privacy-Enhanced Mail (PEM) format for the custom certificate and certificate key.

---

If you configure a custom certificate, you must configure a certificate key with it. Here is an example of how to configure a certificate and certificate key:

```
set system services webapi https certificate /var/tmp/certificate.crt
set system services webapi https certificate-key /var/tmp/certificate.key
```

<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
---------------------------------	---

## client (System Services)

---

<b>Syntax</b>	<code>client <i>ip-address</i>;</code>
<b>Hierarchy Level</b>	[edit system services webapi]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Configure the IP address of the client. For the integrated ClearPass authentication and enforcement feature Web API daemon (webapi) configuration, the client is the ClearPass Policy Manager (CPPM). The CPPM initiates a connection to the Web API daemon, which acts as an HTTP or HTTPS server.</p> <p>The CPPM client sends POST request messages containing user authentication and identity information to the Web API daemon. The SRX Series device accepts information only from the configured address of the client.</p>
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## client-id (Services User Identification)

<b>Syntax</b>	client-id <i>client-id</i> ;
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass user-query]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Configure the client ID that the SRX Series device requires to obtain an access token for the integrated ClearPass authentication and enforcement user query function. The client ID must be consistent with the API client configured on the CPPM.</p> <p>The ClearPass endpoint API requires use of OAuth (RFC 6749) to authenticate and authorize the SRX Series device access. The SRX Series device uses the Client Credentials grant type access token, which is one of the two types that ClearPass supports.</p> <p>If it is configured, the user query function allows the SRX Series device to query the CPPM for authentication and identity information about individual users when it does not receive this information from the CPPM through the Web API.</p>
<b>Required Privilege Level</b>	<p>services—To view this statement in the configuration.</p> <p>services-control—To add this statement to the configuration.</p>

## client-secret (Services User Identification)

<b>Syntax</b>	client-secret <i>client-secret</i> ;
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass user-query]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Configure the client secret used with the client ID that the SRX Series device requires to obtain an access token for the integrated ClearPass authentication and enforcement user query function. The client secret must be consistent with the client secret configured on the ClearPass Policy Manager (CPPM).</p> <p>The ClearPass endpoint API requires use of OAuth (RFC 6749) to authenticate and authorize SRX Series device access. The SRX Series device uses the Client Credentials grant type access token, which is one of the two types that ClearPass supports.</p> <p>If it is configured, the user query function allows the SRX Series device to query the CPPM for authentication and identity information about individual users when it does not receive this information from the CPPM through the Web API daemon (webapi).</p>
<b>Required Privilege Level</b>	<p>services—To view this statement in the configuration.</p> <p>services-control—To add this statement to the configuration.</p>

## connect-method (Services User Identification)

---

<b>Syntax</b>	connect-method (http   https);
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass user-query web-server]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Configure the application protocol used for the SRX Series device connection to the ClearPass Policy Manager (CPPM) for user query requests. You identify the connection protocol as part of the configuration that identifies the CPPM server.</p> <p>The connect-method configuration is optional. If it is not configured, the default value of HTTPS is assumed.</p> <p>The user query function allows the SRX Series device to request from the CPPM user authentication and identity information for an individual user.</p>
<b>Required Privilege Level</b>	services—To view this statement in the configuration. services-control—To add this statement to the configuration.

## debug-level (System Services)

---

<b>Syntax</b>	debug-level <i>level</i> ;
<b>Hierarchy Level</b>	[edit system services webapi]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	Specify the trace level for the integrated ClearPass authentication and enforcement Web API daemon (webapi).
<b>Options</b>	<p><b>level</b>—A flag that specifies the type of logs to be written to the log file for the Web API daemon (webapi).</p> <p><b>alert</b>—Matches alert messages.</p> <p><b>crit</b>—Matches critical messages.</p> <p><b>emerg</b>—Matches emergency messages.</p> <p><b>error</b>—Matches error messages.</p> <p><b>notice</b>—Matches notification messages.</p> <p><b>warn</b>—Matches warning messages.</p>
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## debug-log (System Services)

---

<b>Syntax</b>	debug-log <i>filename</i> ;
<b>Hierarchy Level</b>	[edit system services webapi]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Specify the name of the log file to which trace messages for the integrated ClearPass authentication and enforcement Web API daemon (webapi) are written.</p> <p>The debug level flag determines the kind of logs that are written to this file. Possible values are:</p> <p>alert—Matches alert messages.</p> <p>crit—Matches critical messages.</p> <p>emerg—Matches emergency messages.</p> <p>error—Matches error messages.</p> <p>notice—Matches notification messages.</p> <p>warn—Matches warning messages.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

## default-certificate (System Services)

---

<b>Syntax</b>	default-certificate;
<b>Hierarchy Level</b>	[edit system services webapi https]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Specify that the default certificate is to be used for the integrated ClearPass authentication and enforcement Web API daemon (webapi) HTTPS configuration. To ensure security, the Junos OS default certificate key size is 2084 bits.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

## delay-query-time (Services User Identification)

---

<b>Syntax</b>	<code>delay-query-time <i>delay-time-in-seconds</i>;</code>
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass user-query]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Configure the amount of time for the SRX Series device to delay before sending queries to the Aruba ClearPass Policy Manager (CPPM) for authentication and identity information for individual users. If the CPPM does not send to the SRX Series device authentication and identity information for a particular user, the SRX Series device can request that information for the user if you configure the user query function.</p> <p>Delays can occur from when the CPPM initially posts user authentication information to the SRX Series device to when the SRX Series device updates its ClearPass authentication table with that information. In its transit, the user identity information must first pass through the CPPM device's control plane and the control plane of the SRX Series device.</p> <p>During that period, traffic might arrive at the SRX Series device that is generated by an access request from a user whose authentication and identity information is in transit from the CPPM to the SRX Series device. Rather than allow the SRX Series device to respond automatically by sending a user query request <i>immediately</i>, you can set the delay time parameter specifying in seconds how long the SRX Series device should wait before sending the request.</p> <p>After the delay timeout expires, the SRX Series device sends the query to the CPPM and creates a pending entry for the user in the Routing Engine authentication table. During this period, any arriving traffic matches the default policy whose action on the traffic you can configure.</p> <p>Range: 0 through 60</p>
<b>Required Privilege Level</b>	<p>services—To view this statement in the configuration.</p> <p>services-control—To add this statement to the configuration.</p>

## file (Services User Identification)

<b>Syntax</b>	<pre> file {     filename     files <i>number</i>;     match <i>regular-expression</i>;     size <i>maximum-file-size</i>;     (world-readable   no-world-readable); } </pre>
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass traceoptions]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	Configure the name of the trace log file and its characteristics to which messages for the behavior of the authentication source are logged. For the SRX Series device integrated ClearPass authentication and enforcement feature, the authentication source is the Aruba ClearPass Policy Manager (CPPM).
<b>Options</b>	<p><b>filename</b>—Name of the log file.</p> <p><b>files <i>max-number-of-files</i></b>—Specifies the maximum number of trace files. Range: 2 through 1000</p> <p><b>match <i>regular-expression</i></b>—Specifies a regular expression that determines which lines are logged.</p> <p><b>no-world-readable</b>—Denies users the ability to read the log file.</p> <p><b>size <i>max-file-size</i></b>—Specifies the trace file maximum file size. Range: 10,240 through 1,073,741,824.</p> <p><b>world-readable</b>—Allows users to read the log file.</p>
<b>Required Privilege Level</b>	<p>services—To view this statement in the configuration.</p> <p>services-control—To add this statement to the configuration.</p>


## filter threat-attack (Security)

---

<b>Syntax</b>	filter threat-attack;
<b>Hierarchy Level</b>	[edit security log stream <i>stream-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	Configure the log stream filter to transmit only threat and attack logs to the ClearPass Policy Manager (CPPM). The integrated ClearPass authentication and enforcement feature sends to the CPPM threat and attack logs detected by the SRX Series device security modules. You can use these reports to inform your approach to hardening the CPPM security policy. Setting the log stream filter to threat-attack ensures that the SRX Series device and the log server are not overburdened by irrelevant logs.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## http (Services User Identification)


---

<b>Syntax</b>	http port <i>port-number</i> ;
<b>Hierarchy Level</b>	[edit services user-identification authentication-source <i>name</i> user-query web-server <i>name</i> connect-method]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Configure HTTP as the connection protocol to use for the SRX Series integrated ClearPass authentication and enforcement feature's connection to the ClearPass Policy Manager (CPPM) webserver for individual user authentication queries. You identify the connection protocol as part of the configuration that identifies the CPPM webserver (mutually exclusive with HTTPS).</p> <p>If a value for the connection method is not configured, the default value of HTTPS is assumed.</p> <p>If the SRX Series devices does not find an authentication entry for a user in its local ClearPass authentication table, it can query the Aruba ClearPass webserver for this information.</p>
<div> <b>NOTE:</b> This configuration assumes that aruba-clearpass is specified as the authentication source.</div>	
<b>Required Privilege Level</b>	services—To view this statement in the configuration. services-control—To add this statement to the configuration.




## http (System Services)

---

<b>Syntax</b>	http port <i>port-number</i> ;
<b>Hierarchy Level</b>	[edit system services webapi]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Specify HTTP as the communication protocol for the Web API function of the SRX Series integrated ClearPass authentication and enforcement feature.</p> <p>The SRX Series device exposes to the ClearPass Policy Manager (CPPM) the Web API for it to use to initiate a connection and then use that connection to send to the SRX Series device user authentication and identity information.</p> <p>This statement also specifies the port number to use for the HTTP connection. The port number is optional. If it is not specified, the default port of 8080 is used.</p>
	<p>.....</p> <div>  <p><b>NOTE:</b> If you deploy HTTP along with a Web management application, you must ensure that they run on different service ports.</p> </div> <p>.....</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

## https (Services User Identification)

<b>Syntax</b>	<pre>https (   certificate <i>local-certificate</i>;   certificate-key <i>local-certificate-key</i>;   default-certificate;   pki-local-certificate <i>certificate-name</i>;   port <i>port-number</i>; )</pre>
<b>Hierarchy Level</b>	[edit services user-identification authentication-source <i>name</i> user-query web-server <i>name</i> connect-method]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Configure HTTPS as the connection protocol used for the SRX Series connection to the ClearPass Policy Manager (CPPM) for user query requests. You identify the connection protocol as part of the configuration that identifies the CPPM webserver.</p> <p>The integrated ClearPass authentication and enforcement user query function allows the SRX Series device to request from the CPPM user authentication and identity information for an individual when the SRX Series ClearPass authentication table does not contain that information.</p> <p>The connect-method configuration is optional. If it is not configured, a default value of HTTPS is assumed.</p>
	<div>  <p><b>NOTE:</b> This configuration assumes that aruba-clearpass is specified as the authentication source.</p> </div>
<b>Options</b>	<p><b>https</b>—Specifies use of the encrypted HTTPS protocol. (Mutually exclusive with HTTP.)</p> <p><b>default-certificate</b>—Configures the Web API daemon (webapi) to use the default HTTPS certificate.</p> <p>For security reasons, the HTTPS default-certificate key size 2048.</p> <p><b>certificate <i>filename</i></b>—Configures the Web API daemon to use a specified, custom certificate file.</p> <p>The Web API supports only the Privacy-Enhanced Mail (PEM) format for the custom certificate and certificate key configuration.</p> <p><b>certificate-key <i>local-certificate-key</i></b>—Configures the Web API daemon service certificate key. This parameter is required if a custom service certificate file is configured.</p> <p><b>pki-local-certificate <i>pki-certificate</i></b>—Configures the Web API daemon to use the local X.509 PKI certificate.</p> <p><b>port <i>port-number</i></b>—Configures the HTTPS service port. The default port is 8443.</p>

Range: 1 through 65535

**Required Privilege  
Level**

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

## https (System Services)

---

**Syntax**    `https (  
          certificate local-certificate;  
          certificate-key local-certificate-key;  
          default-certificate;  
          pki-local-certificate certificate-name;  
          port port-number;  
          )`

**Hierarchy Level**    `[edit system services webapi connect-method]`

**Release Information**    Statement introduced in Junos OS Release 12.3X48-D30.

**Description**    Specify use of HTTPS as the communication protocol for the Web API function of the SRX Series integrated ClearPass authentication and enforcement feature. When you configure HTTPS, you specify the service certificate and certificate key. You can also specify the port to be used.

The Web API daemon, acting as an HTTPS server, allows the ClearPass Policy Manager (CPPM), acting as the client, to send POST request messages to it. The CPPM, which is the authentication source for this feature, sends to the SRX Series device user authentication and identity information.



**NOTE:** If you deploy HTTPS with a Web management application, you must ensure that they run on different service ports.

---

**Options**    **https**—Specifies use of the encrypted HTTPS protocol. (Mutually exclusive with HTTP.)

**default-certificate**—Configures the Web API daemon (webapi) to use the default HTTPS certificate.

      For security reasons, the HTTPS default-certificate key size 2048.

**certificate *filename***—Configures the Web API daemon to use the specified, custom certificate file.

      For certificate and certificate key configuration, the Web API function supports only the Privacy-Enhanced Mail (PEM) format.

**certificate-key *local-certificate-key***—Configures the Web API daemon service certificate key. This parameter is required if a custom service certificate file is configured.

**pki-local-certificate *pki-certificate***—Configures the Web API daemon to use the local X.509 PKI certificate.

**port *port-number***—Configures the HTTPS service port. The default port is 8443. Range: 1 through 65,535.

<b>Required Privilege Level</b>	system—To view this statement in the configuration.
	system-control—To add this statement to the configuration.

---

## level (Services User Identification)

---

<b>Syntax</b>	level (brief   detail   extensive   verbose);
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass traceoptions]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	Configure the level of messages o be written to the trace log file about authentication source behavior.
	For the integrated ClearPass authentication enforcement feature, the authentication source is Aruba ClearPass.
<b>Options</b>	<b>all</b> —Matches all levels.
	<b>error</b> —Matches error conditions.
	<b>info</b> —Matches informational messages.
	<b>notice</b> —Matches conditions that require special handling.
	<b>verbose</b> —Matches verbose messages.
	<b>warning</b> —Matches warning messages.
<b>Required Privilege Level</b>	services—To view this statement in the configuration.
	services-control—To add this statement to the configuration.

---

## no-remote-trace (Services User Identification)

---

<b>Syntax</b>	no-remote-trace;
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass traceoptions]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	Disable remote tracing.
<b>Required Privilege Level</b>	services—To view this statement in the configuration.
	services-control—To add this statement to the configuration.

## no-user-query (Services User Identification)

---

<b>Syntax</b>	no-user-query;
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Disable the integrated ClearPass authentication and enforcement user query function, if it is configured. You can use the no-user-query statement to turn off the user query function without having to delete the configuration.</p> <p>The user query function allows the SRX Series device to query the ClearPass webserver for authentication and identity information for an individual user whose information was not posted to the SRX Series device by ClearPass.</p>
<b>Required Privilege Level</b>	<p>services—To view this statement in the configuration.</p> <p>services-control—To add this statement to the configuration.</p>

## password (System Services)

---

<b>Syntax</b>	password <i>password</i> ;
<b>Hierarchy Level</b>	[edit system services webapi user]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Specify the password for the integrated ClearPass authentication and enforcement feature Web API daemon (webapi) user.</p> <p>Range: 1 through 128 characters.</p> <p>The Web API daemon, acting as an HTTP server, exposes to the Aruba ClearPass Policy Manager (CPPM) an API that allows the CPPM, acting as a client, to send POST request messages to it. The CPPM, which serves as the authentication source, initiates the session to the SRX Series device and sends it user authentication and identity information.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

## pki-local-certificate (Services)

---

<b>Syntax</b>	<code>pki-local-certificate <i>pki-certificate</i>;</code>
<b>Hierarchy Level</b>	[edit services webapi https]
<b>Release Information</b>	Statement introduced in Junos OS release 12.3X48-D30.
<b>Description</b>	For the SRX Series Integrated ClearPass Authentication and Enforcement feature, configures the webapi daemon to use the local X.509 PKI certificate.
<b>Required Privilege Level</b>	services—To view this statement in the configuration. services-control—To add this statement to the configuration.

## port (Services User Identification)

---

<b>Syntax</b>	<code>port <i>port-number</i></code>
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass user-query web-server]
<b>Release Information</b>	Statement introduced in Junos OS release 12.3X48-D30.
<b>Description</b>	<p>Specifies the ClearPass Policy Manager (CPPM) web server port used for the SRX Series Integrated and Enforcement user query function. Together with the CPPM web server IP address and connection method, the port identifies the web server to which the SRX Series device sends user query requests. The port number is optional. Default is 433.</p> <p>If the CPPM web server contact information is configured, the SRX Series device can query it under certain circumstances for authentication and identity information about individual users.</p>
<b>Required Privilege Level</b>	services—To view this statement in the configuration. services-control—To add this statement to the configuration.


## port (System Services)

---

<b>Syntax</b>	<code>port <i>port-number</i>;</code>
<b>Hierarchy Level</b>	[edit system services webapi http] [edit system services webapi https]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	Specify the SRX Series device TCP port to use for incoming HTTP or HTTPS connection requests initiated by the ClearPass Policy Manager (CPPM). The SRX Series device integrated ClearPass authentication and enforcement feature exposes its Web API (webapi) to the CPPM. The CPPM uses the Web API to establish a connection to the SRX Series device and send user authentication and identity information to it.
<b>Options</b>	<p><code>port <i>port-number</i></code>—For HTTP, the default service port is 8080. Range: 1 through 65535.</p> <p><code>port <i>port-number</i></code>—For HTTPS, the default service port is 8443. Range: 1 through 65535.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>



## priority (Security User Identification)


<b>Syntax</b>	<pre>authentication-source {   active-directory priority <i>priority</i>;   aruba-clearpass priority <i>priority</i>;   firewall-authentication priority <i>priority</i>;   local-authentication-table priority <i>priority</i>;   unified-access-control priority <i>priority</i>; }</pre>
<b>Hierarchy Level</b>	[edit security user-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Set the lookup priority to identify the order in which the SRX Series device checks its configured authentication tables for user authentication information. Authentication tables are searched in order based on their priority setting in which lowest value takes precedence.</p> <p>For the integrated ClearPass authentication and enforcement feature, the SRX Series device must be configured to search the ClearPass authentication table first.</p>
	<p> <b>NOTE:</b> Note that both the authentication source, Aruba ClearPass, and the SRX Series ClearPass authentication table are both referred to as <code>aruba-clearpass</code> in the CLI and its output.</p>
	<p>You need to set this value only if the local authentication table, whose default value is 100, also resides on the Packet Forwarding Engine. In that case, you must configure a higher priority value, such as 120, for the local authentication table.</p>
<b>Options</b>	<p><b><code>aruba-clearpass <i>priority</i></code></b>—By default, the authentication table search priority for the ClearPass authentication table is 110.</p> <p>Range: 1 through 65535.</p> <p>Default values for other authentication tables are:</p> <ul style="list-style-type: none"> <li>Local authentication table: 100</li> <li>Active Directory (AD) table: 125</li> <li>UAC authentication table: 150</li> <li>Firewall authentication table: 200</li> </ul>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>

## query-api (Services User Identification)

---

<b>Syntax</b>	<code>query-api query-api</code>
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass user-query]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Configure <b>query-api</b> to specify the path of the URL that the SRX Series device uses to query the ClearPass Policy Manager (CPPM) webserver for authentication and identity information for an individual user. For the SRX Series device to be able to make a request, you must have configured it to obtain an access token. See <a href="#">token-api (Services User Identification)</a>.</p> <p>The integrated ClearPass authentication and enforcement user query function supplements the Web API function (webapi) by allowing the SRX Series device to obtain from the CPPM authentication information for an individual user whose information does not already exist in the SRX Series ClearPass authentication table.</p> <p>Consider the following <b>query-api</b> example:</p> <pre>api/v1/insight/endpoint/ip/\$IP\$</pre> <p>The SRX Series device generates the complete URL for the user query request by combining the query-api string with the connection method (HTTPS) and the CPPM webserver IP address ({server}).</p> <pre>https://{server}/api/v1/insight/endpoint/ip/\$IP\$</pre> <p>In this example, the SRX Series device replaces the variables with the following values resulting in a specific URL request for the individual user:</p> <pre>https://10.17.4.12/api/v1/insight/endpoint/ip/10.17.4.12</pre> <p>Under normal circumstances, the ClearPass webserver sends user authentication information to the SRX Series device in POST request messages and the SRX Series device writes that information to its ClearPass authentication table. When the SRX Series device receives an access request from a user, it searches its ClearPass authentication table for an entry for that user.</p> <p>It can happen that the SRX Series device might not have received authentication for a user from the CPPM because the user has not yet been authenticated by the CPPM. For example, the user might have joined the network through an access layer not on a managed switch or WLAN. When the CPPM receives the user query from the SRX Series device, it authenticates the user and returns the authentication information to the device.</p>
<b>Required Privilege Level</b>	<p>services—To view this statement in the configuration.</p> <p>services-control—To add this statement to the configuration.</p>

## rate-limit (Security Log)

<b>Syntax</b>	<code>rate-limit <i>rate-limit</i>;</code>
<b>Hierarchy Level</b>	[edit security log stream <i>stream-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>The Integrated Authentication and Enforcement feature sends threat and attack logs generated by the SRX Series device security modules to the ClearPass Policy Manager (CPPM) to use in its security policy assessment.</p> <p>The logs are sent in stream mode. To avoid overburdening the SRX Series device and the log server, you can control the rate at which these logs are sent. By setting a rate-limit value, you can constrain the number of logs that are sent in 1 second. After the limit is reached, no more logs are sent.</p> <p>Range: 1 through 65,535.</p>
	<p> <b>NOTE:</b> For high-end multicore systems that use SPUs, the number of log messages sent per SPU is a divided rate:</p> $\text{rate} = \text{configured-rate} / \text{number-of-SPUs}$ <p>Rate limiting on high-end platforms is generally not as accurate as it is on low-end platforms, because the generation of logs is not entirely balanced between SPUs.</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>

## token-api (Services User Identification)

---

<b>Syntax</b>	<code>token-api <i>token-api</i></code>
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass user-query]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Configure the token API that is used in generating the URL for acquiring an access token. The token API is combined with the connection method and the IP address of the ClearPass webserver to produce the complete URL used for acquiring an access token.</p> <p>For example, if the token API is oauth, the connection method is HTTPS, and the IP address of the ClearPass webserver is 10.208.111.177, the complete URL for acquiring an access token would be https://10.208.111.177/api/oauth. This is a required parameter. There is no default value.</p> <p>The SRX Series device user query function requires an access token to be able to query the ClearPass webserver. If the user query function is configured, the SRX Series device can request from the ClearPass webserver user authentication and identity information for an individual user.</p>
<b>Required Privilege Level</b>	<p>services—To view this statement in the configuration.</p> <p>services-control—To add this statement to the configuration.</p>

---

## traceoptions (Services User Identification)

---

**Syntax**    traceoptions {  
              file {  
                  *filename*;  
                  files *number*;  
                  match *regular-expression*;  
                  size *maximum-file-size*;  
                  (world-readable | no-world-readable);  
              }  
              flag *flag*;  
              level *level* ;  
              no-remote-trace;  
          }

**Hierarchy Level**    [edit services user-identification authentication-source aruba-clearpass]

**Release Information**    Statement introduced in Junos OS Release 12.3X48-D30.

**Description**    Specify the name of the trace log file and its characteristics. Messages about the behavior of the authentication source are written to this log file. Aruba ClearPass Policy Manager (CPPM) is the authentication source for the SRX Series device integrated ClearPass authentication and enforcement feature.

**Required Privilege Level**    services—To view this statement in the configuration.  
                                  services-control—To add this statement to the configuration.

## webapi (System Services)

---

**Syntax**

```
webapi {
  client ip-address;
  (
    http {
      port port-number;
    }
    https {
      certificate certificate-filename;
      certificate-key local-certificate-key;
      default-certificate
        pki-local-certificate;
      port port-number;
    }
    user {
      name;
      password password;
    }
    debug-log filename;
    debug-level level;
  }
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced in Junos OS Release 12.3X48-D30.

**Description** Configure the Web API function daemon (webapi) component of the integrated ClearPass authentication and enforcement feature. The Web API daemon acts as a HTTP or HTTPS server. The SRX Series device exposes to the Aruba ClearPass Policy Manager (CPPM) the Web API that allows the CPPM, as a client, to send POST request messages to it that provide the SRX Series device with user authentication and identity information. The CPPM serves as the user authentication source for the SRX Series device.

The Web API function (webapi) facilitates efficient transmission of user authentication and identity information from the CPPM to the SRX Series device. The CPPM, which is the client in this relationship, initiates a session with the SRX Series device Web API daemon, which is the server in this relationship. However, the CPPM can do this only if you have configured the Web API function on the SRX Series device. For security reasons, the Web API daemon is not enabled by default.

The configuring statements are explained separately. See the CLI Explorer.

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

## webapi-clear-text (Security)

<b>Syntax</b>	web-api-cleartext
<b>Hierarchy Level</b>	[edit security zones security-zone <i>zone</i> host-inbound-traffic system-services]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	Enable the Web API (webapi) service over HTTP host inbound traffic on TCP port 8080 for unencrypted data.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## webapi-ssl (Security)

<b>Syntax</b>	webapi-ssl
<b>Hierarchy Level</b>	[edit security zones security-zone <i>zone</i> host-inbound-traffic system-services]
<b>Release Information</b>	Statement introduced in Junos OS Routing Engine release 12.3X48-D30.
<b>Description</b>	Enable the Web API service over HTTPS host inbound traffic on TCP port 8443.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## web-server (Services)

<b>Syntax</b>	web-server <i>server-name</i> ;
<b>Hierarchy Level</b>	[edit services user-identification authentication-source aruba-clearpass user-query]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Specify the name of the webserver configuration on the SRX Series device used for the user query integrated ClearPass authentication and enforcement function. The webserver is the ClearPass server to which the SRX Series device connects to request authentication and identity information for an individual user.</p> <p>When information for the individual user is not posted to the SRX Series device by ClearPass through Web API POST request messages, the SRX Series device can request this information from the ClearPass Policy Manager (CPPM) under certain circumstances. You must enable the user query function by configuring it.</p>
<b>Required Privilege Level</b>	services—To view this statement in the configuration. services-control—To add this statement to the configuration.

### Integrated ClearPass Authentication and Enforcement CLI Operational Commands

The Integrated ClearPass Authentication and Enforcement CLI operational commands are:

- `clear services user-identification authentication-source aruba-clearpass user-query counters`
- `clear services user-identification authentication-table`
- `request services user-identification authentication-source aruba-clearpass user-query`
- `request services user-identification authentication-table delete`
- `show service user-identification authentication-source aruba-clearpass user-query counters`
- `show service user-identification authentication-source aruba-clearpass user-query status`
- `show services user-identification authentication-table`



## clear services user-identification authentication-source aruba-clearpass user-query counters

<b>Syntax</b>	clear services user-identification authentication-source aruba-clearpass user-query counters
<b>Release Information</b>	Command introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Clear the integrated ClearPass authentication and enforcement user query function counters. One counter records the number of queries sent from the SRX Series device to the ClearPass webserver requesting authentication information for individual users. The other counter shows the number of responses that the SRX Series device received from the ClearPass webserver. This command resets the counts, which begin again when the next request is sent.</p> <p>The user query function allows the SRX Series device to query the ClearPass webserver for authentication and identification information for a particular individual, identified by the IP address of their device. The SRX Series device can use this function only if you configure it. It is not enabled by default.</p> <p>After you issue the clear command, the counters are reset, and there is no CLI output.</p>
<b>Options</b>	<b>authentication-source</b> —For the SRX Series integrated ClearPass authentication and enforcement feature, you must specify the predefined value aruba-clearpass to indicate that ClearPass is the authentication source.
<b>Required Privilege Level</b>	clear
<b>List of Sample Output</b>	<a href="#">clear services user-identification authentication-source aruba-clearpass user-query counters on page 185</a>

### Sample Output

#### clear services user-identification authentication-source aruba-clearpass user-query counters

```
user@host> clear services user-identification authentication-source aruba-clearpass user-query counters
```

The clear command does not product output.

## clear services user-identification authentication-table

---

<b>Syntax</b>	<code>clear services user-identification authentication-table authentication-source authentication-source</code> (all   active-directory   aruba-clearpass)
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	Clear the contents of the ClearPass authentication table. The ClearPass authentication table, which is created by the SRX Series device on the Packet Forwarding Engine, is populated with user authentication and identity information received from Aruba ClearPass. Aruba ClearPass is the authentication source for the integrated ClearPass feature. You must <code>aruba-clearpass</code> as the authentication source.
<b>Options</b>	<b><i>authentication-source</i></b> —For the SRX Series integrated ClearPass feature, you must specify <code>aruba-clearpass</code> to indicate that ClearPass is the authentication source and that the authentication table relies on user information from the ClearPass Policy Manager.
<b>Additional Information</b>	The remaining statements are explained separately. See CLI Explorer.
<b>Required Privilege Level</b>	clear
<b>List of Sample Output</b>	<a href="#">clear services user-identification authentication-table authentication-source on page 186</a>
<b>Output Fields</b>	<p>If there are no entries in the ClearPass authentication table, the following warning message is displayed after you enter the <code>clear</code> command.</p> <p><b>There is no authentication-table entry.</b></p> <p>If there are entries in the ClearPass authentication table, no messages are displayed after you enter the <code>clear</code> command.</p>

## Sample Output

### clear services user-identification authentication-table authentication-source

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

## request services user-identification authentication-source aruba-clearpass user-query

<b>Syntax</b>	request services user-identification authentication-source <i>authentication-source</i> user-query address <i>ip-address</i>
<b>Release Information</b>	Command introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Manually send to the ClearPass website a request for user authentication and identity information for an individual user. The command specifies the IP address of the user's device to identify the user whose information you want to obtain. If the user query command executes successfully, an entry for the user (IP address) has been created in the ClearPass authentication table, and no output is displayed.</p> <p>The user query function is part of the SRX Series integrated ClearPass authentication and enforcement feature. The user query function, if configured, allows the SRX Series device to send requests for individual user information. This command also allows you to manually send requests. Normally administrators send query requests manually to troubleshoot issues.</p> <p>The user query function supplements use of the Web API function. The SRX Series device exposes to ClearPass a Web API that ClearPass uses to send POST request messages to the SRX Series device. These messages contain user authentication and identity information.</p>
<b>Options</b>	<i>ip-address</i> —The IP address of the user's device for whom you are manually requesting authentication information.
<b>Required Privilege Level</b>	maintenance
<b>List of Sample Output</b>	<a href="#">request services user-identification authentication-source authentication-source user-query address ip-address on page 187</a>

### Sample Output

[request services user-identification authentication-source authentication-source user-query address ip-address](#)

```
user@host> request services user-identification authentication-source aruba-clearpass user-query
address 40.0.0.1
```

## request services user-identification authentication-table delete

---

<b>Syntax</b>	<code>request services user-identification authentication-table delete (ip-address <i>ip-address</i>   authentication-source (all   active-directory   <i>authentication-source</i> (domain <i>domain-name</i>   group <i>group-name</i>   user <i>user-name</i>) )</code>
<b>Release Information</b>	Command introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	Delete entries from the ClearPass authentication table based on the IP address of the user's device, or on the authentication source and the name of a domain, a group, or a user. When only the authentication source is specified, the entire ClearPass authentication table is deleted. For the integrated ClearPass authentication and enforcement feature, the authentication source is always aruba-clearpass.
<b>Options</b>	<p><b><i>ip-address</i></b>—Deletes a user authentication entry from the ClearPass authentication table, and the Active Directory (AD) table, based on the IP address of the user's device.</p> <p><b><i>authentication-source</i></b> —Deletes user entries from the ClearPass authentication table. In the CLI, ClearPass as the authentication source is referred to by the value <code>aruba-clearpass</code> as is the ClearPass authentication table. To identify the user entries to be deleted, you specify a domain, a group, or a username.</p> <p><b><i>domain-name</i></b>—Deletes from the ClearPass authentication table user entries for users who belong to the specified domain.</p> <p><b><i>group group-name</i></b>—Deletes the entry entry from the ClearPass authentication table for users who belong to the group, regardless of whether they belong to other groups.</p> <p><b><i>user user-name</i></b>—Deletes the entry for the specified user from the ClearPass authentication table.</p>
<b>Required Privilege Level</b>	maintenance
<b>List of Sample Output</b>	<p><a href="#">request services user-identification authentication-table delete ip-address on page 189</a></p> <p><a href="#">request services user-identification authentication-table delete authentication-source aruba-clearpass domain on page 189</a></p> <p><a href="#">request services user-identification authentication-table delete authentication-source aruba-clearpass group on page 190</a></p> <p><a href="#">request services user-identification authentication-table delete authentication-source aruba-clearpass on page 192</a></p>
<b>Output Fields</b>	The following examples cover how to delete various user entries from the ClearPass authentication table based on the specified parameter. It also shows how to check to ensure that the user entries were deleted successfully.

## Sample Output

### request services user-identification authentication-table delete ip-address

The following command deletes the entry for the user whose device IP address is specified.

```
user@host> request services user-identification authentication-table delete ip-address 50.0.0.1
```

Before you delete the entry:

To ensure that the entry exists in the ClearPass authentication table, use the following command to display the entry for the user. Note that the ClearPass authentication table includes the user entry with the IP address 50.0.0.1.

```
user@host> show services user-identification authentication-table ip-address 50.0.0.1
```

Domain: GLOBAL

Source-ip: 50.0.0.1

Username: guest1

Groups:posture-healthy, guest, [user authenticated]

State: Valid

Source: Aruba ClearPass

Access start date: 2015-12-14

Access start time: 17:07:23

Last updated timestamp: 2015-12-22 05:50:47

Age time: 0

After you delete the user entry associated with the IP address, enter the command again to verify that the entry has been deleted.

```
user@host> show services user-identification authentication-table ip-address 50.0.0.1
```

warning: "This IP address isn't in authentication table."

### request services user-identification authentication-table delete authentication-source aruba-clearpass domain

The following command deletes the specified domain.

```
user@host> request services user-identification authentication-table delete authentication-source domain global
```

Before you delete the domain contents from the ClearPass authentication table, use the following command to display the domain information to ensure that it exists. Note that the ClearPass authentication table includes the global domain.

```
user@host> show services user-identification authentication-table authentication-source aruba-clearpass domain global extensive
```

Domain: GLOBAL

Total entries: 6

Source-ip: 10.0.0.1

Username: viki2

Groups:posture-healthy, accounting-grp, accounting-grp-and-company-device, corporate-limited, [user authenticated]

Groups referenced by policy:accounting-grp-and-company-device

State: Valid

Source: Aruba ClearPass

Access start date: 2016-03-08

Access start time: 17:20:30

Last updated timestamp: 2015-12-22 04:02:48

Age time: 0

Source-ip: 20.0.0.1

Username: abew1

Groups:posture-unknown, marketing-access-limited-grp, [user authenticated]

Groups referenced by policy:marketing-access-limited-grp

```
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:31:40
Last updated timestamp: 2015-12-22 04:18:48
Age time: 0
Source-ip: 30.0.0.1
Username: jxchan
Groups:posture-healthy, marketing-access-for-pcs-limited-group,
marketing-general, sales-limited, corporate-limited, [user authenticated]
Groups referenced by policy:marketing-access-for-pcs-limited-group
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:22:48
Last updated timestamp: 2015-12-22 05:46:21
Age time: 0
Source-ip: 40.0.0.1
Username: lchen1
Groups:posture-healthy, human-resources-grp, accounting-limited,
corporate-limited, [user authenticated]
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:21:37
Last updated timestamp: 2015-12-22 05:41:18
Age time: 0
Source-ip: 50.0.0.1
Username: guest1
Groups:posture-healthy, guest, [user authenticated]
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:23:10
Last updated timestamp: 2015-12-22 05:50:47
Age time: 0
Source-ip: 50.0.0.2
Username: guest2
Groups:posture-healthy, guest-device-byod, [user authenticated]
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:23:21
Last updated timestamp: 2015-12-22 05:52:44
Age time: 0
```

After you delete the domain, use the command again to verify that the domain and its user members was deleted.

```
user@host> show services user-identification authentication-table authentication-source
aruba-clearpass domain global
warning: "There is no related auth entry in authentication-table."
```

#### **request services user-identification authentication-table delete authentication-source aruba-clearpass group**

The following command deletes the entries for any users who belong to the group posture-healthy.

```
user@host> request services user-identification authentication-table delete authentication-source
aruba-clearpass group posture-healthy
```

Before you delete the group contents from the ClearPass authentication table, use the following command to display it to ensure that the group is used in some user entries. Notice that the appropriate user entries contain the posture-healthy group.

```
Domain: GLOBAL
Total entries: 6
Source-ip: 10.0.0.1
  Username: viki2
  Groups:posture-healthy, accounting-grp, accounting-grp-and-company-device,
  corporate-limited, [user authenticated]
  Groups referenced by policy:accounting-grp-and-company-device
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:20:30
  Last updated timestamp: 2015-12-22 04:02:48
  Age time: 0
Source-ip: 20.0.0.1
  Username: abew1
  Groups:posture-unknown, marketing-access-limited-grp, [user authenticated]
  Groups referenced by policy:marketing-access-limited-grp
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:31:40
  Last updated timestamp: 2015-12-22 04:18:48
  Age time: 0
Source-ip: 30.0.0.1
  Username: jxchan
  Groups:posture-healthy, marketing-access-for-pcs-limited-group,
  marketing-general, sales-limited, corporate-limited, [user authenticated]
  Groups referenced by policy:marketing-access-for-pcs-limited-group
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:22:48
  Last updated timestamp: 2015-12-22 05:46:21
  Age time: 0
Source-ip: 40.0.0.1
  Username: lchen1
  Groups:posture-healthy, human-resources-grp, accounting-limited,
  corporate-limited, [user authenticated]
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:21:37
  Last updated timestamp: 2015-12-22 05:41:18
  Age time: 0
Source-ip: 50.0.0.1
  Username: guest1
  Groups:posture-healthy, guest, [user authenticated]
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:23:10
  Last updated timestamp: 2015-12-22 05:50:47
  Age time: 0
Source-ip: 50.0.0.2
  Username: guest2
  Groups:posture-healthy, guest-device-byod, [user authenticated]
  State: Valid
```

```
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:23:21
Last updated timestamp: 2015-12-22 05:52:44
Age time: 0
```

Enter the **show services user-identification authentication-table authentication-source aruba-clearpass group posture-healthy** to display the entries for the users who belong to the group posture-healthy.

Notice that the group name does not show up in the column for groups referenced by policy because it is not one. Notice, too, that the output contains information for only those users who belong to the group. It does not include an entry for the user abewl, who does not belong to the group.

```
Domain: GLOBAL
Source IP      Username      groups(Ref by policy)      state
10.0.0.1       viki2         accounting-grp-and-company-dev Valid
30.0.0.1       jxchan        marketing-access-for-pcs-limit Valid
40.0.0.1       lchen1        corporate-limited          Valid
50.0.0.1       guest1                                 Valid
50.0.0.2       guest2                                 Valid
```

After you delete the group, use the command again to verify that it has been deleted.

```
user@host> show services user-identification authentication-table authentication-source
aruba-clearpass group posture-healthy
warning: "There is no related auth entry in authentication-table."
```

For further verification, you can use the following command to check the entry for one of the users who belonged to the group:

```
user@host> show services user-identification authentication-table authentication-source
aruba-clearpass user viki2
warning: "There is no related auth entry in authentication-table."
```

### **request services user-identification authentication-table delete authentication-source aruba-clearpass**

The following command deletes the ClearPass authentication table (aruba-clearpass).

```
user@host> request services user-identification authentication-table delete authentication-source
aruba-clearpass
```

Before you delete the ClearPass authentication table, use the following command to display it to ensure that the table exists.

```
user@host> show services user-identification authentication-table authentication-source
aruba-clearpass
Domain: GLOBAL
Total entries: 6
Source-ip: 10.0.0.1
Username: viki2
Groups: posture-healthy, accounting-grp, accounting-grp-and-company-device,
corporate-limited, [user authenticated]
Groups referenced by policy: accounting-grp-and-company-device
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
```



```

Access start time: 17:20:30
Last updated timestamp: 2015-12-22 04:02:48
Age time: 0
Source-ip: 20.0.0.1
Username: abew1
Groups:posture-unknown, marketing-access-limited-grp, [user authenticated]
Groups referenced by policy:marketing-access-limited-grp
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:31:40
Last updated timestamp: 2015-12-22 04:18:48
Age time: 0
Source-ip: 30.0.0.1
Username: jxchan
Groups:posture-healthy, marketing-access-for-pcs-limited-group,
marketing-general, sales-limited, corporate-limited, [user authenticated]
Groups referenced by policy:marketing-access-for-pcs-limited-group
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:22:48
Last updated timestamp: 2015-12-22 05:46:21
Age time: 0
Source-ip: 40.0.0.1
Username: lchen1
Groups:posture-healthy, human-resources-grp, accounting-limited,
corporate-limited, [user authenticated]
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:21:37
Last updated timestamp: 2015-12-22 05:41:18
Age time: 0
Source-ip: 50.0.0.1
Username: guest1
Groups:posture-healthy, guest, [user authenticated]
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:23:10
Last updated timestamp: 2015-12-22 05:50:47
Age time: 0
Source-ip: 50.0.0.2
Username: guest2
Groups:posture-healthy, guest-device-byod, [user authenticated]
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:23:21
Last updated timestamp: 2015-12-22 05:52:44
Age time: 0

```

To verify that you deleted the authentication table successfully, enter the command again:

```
user@host> show services user-identification authentication-table authentication-source
aruba-clearpass
```

```
warning: "There is no authentication-table entry."
```



## show service user-identification authentication-source aruba-clearpass user-query counters

<b>Syntax</b>	show service user-identification authentication-source aruba-clearpass user-query counters
<b>Release Information</b>	Command introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	<p>Display statistics on the counters maintained by the user query function. The output identifies the ClearPass webserver as the destination of the user query requests. It displays the number of requests sent from the SRX Series device to the ClearPass webserver and the number of responses that the SRX Series device received from it. You can use this command to identify that a problem exists—the number of responses received is less than the number of requests sent.—and then analyze and correct it.</p> <p>If there are no problems with the communication between the ClearPass Policy Manager (CPPM) and the SRX Series device, the number of requests sent is equal to the number of responses received and the number of error responses.</p> $\text{number-of-requests} = \text{number-of-responses} + \text{error-message-responses}$ <p>The user query function is part of the SRX Series integrated ClearPass authentication and enforcement feature. The SRX Series device can automatically send requests for individual user authentication and identity information to ClearPass in the event that ClearPass does not post that information to it. For this to occur, you must have configured the user query function.</p> <p>The SRX Series device exposes to ClearPass a Web API (webapi) that ClearPass uses to send POST request messages to it automatically. These messages contain user authentication and identity information.</p> <p>The user query function supplements use of the SRX Series Web API function.</p>
<b>Options</b>	<b>authentication-source</b> —Specify aruba-clearpass to identifies Aruba ClearPass as the authentication source.
<b>Required Privilege Level</b>	view
<b>Output Fields</b>	<ul style="list-style-type: none"> <li>• Webserver Address—The IP address of the ClearPass webserver.</li> <li>• Access token—The token string that the SRX Series device obtains from ClearPass which allows the SRX Series device to query the ClearPass webserver for an individual user's authentication and identity information.</li> <li>• Requests sent number—A counter that shows the number of individual user authentication information queries that the SRX Series device sent to the ClearPass webserver.</li> <li>• Total response received number—A counter that shows the number of returns from the ClearPass webserver in response to the individual user authentication information queries that the SRX Series device sent to it. The number of responses should match the number of requests unless an error occurred.</li> </ul>

- Error response received number—The number errors that occurred in relation to requests.
- Time of last response—A timestamp showing when the last response from the ClearPass webserver was received.

## Sample Output

**show service user-identification authentication-source aruba-clearpass user-query counters**

```
user@host> show service user-identification authentication-source aruba-clearpass user-query counters
```

```
Web server Address: 4.0.0.20
Access token: 433feffae5c3eb3ff8ffdc49f968b03437ca1ce5
Request sent number: 7
Total response received number: 7
Error response received number: 0
Time of last response: 2000-01-01 11:57:17
```

## show service user-identification authentication-source aruba-clearpass user-query status

---

<b>Syntax</b>	show service user-identification authentication-source <i>authentication-source</i> user-query status
<b>Release Information</b>	Command introduced in Junos OS Release 12.3X48-D30.
<b>Description</b>	Check to determine if the ClearPass webserver is online. The SRX Series device sends user query requests to the ClearPass webserver. The user query function is part of the SRX Series ClearPass Authentication and Enforcement feature.
<b>Options</b>	<b><i>authentication-source</i></b> —The value aruba-clearpass identifies Aruba ClearPass as the authentication source. For the integrated ClearPass feature, you must specify aruba-clearpass to determine if the ClearPass webserver is online.
<b>Required Privilege Level</b>	view
<b>List of Sample Output</b>	<a href="#">show service user-identification authentication aruba-clearpass user-query status on page 197</a>
<b>Output Fields</b>	Authentication source:—Identifies Aruba ClearPass as the authentication source.  Webserver Address—The IP address of the ClearPass webserver that the SRX Series devices sends the user query request to.  Status—Shows whether the ClearPass webserver is online.  Current connections—Number of active connections from the SRX Series device to the ClearPass server. Maximum number of connections is 20.

## Sample Output

### show service user-identification authentication aruba-clearpass user-query status

```
user@host>show service user-identification authentication-source aruba-clearpass status
Authentication source: aruba-clearpass

Web server Address: 10.208.111.177

Status: Online

Current Connections: 6
```

## show services user-identification authentication-table

---

**Syntax** `show services user-identification authentication-table ip-address ip-address | authentication-source authentication-source (brief | domain domain-name (<enter> | brief | extensive) | group group-name (<enter> | brief | extensive) | user user-name (<enter> | brief | extensive) ) all | active directory`

**Release Information** Command introduced in Junos OS release 12.3X48-D30.

**Description** Display the ClearPass authentication table contents for an individual user based on the IP address of the user's device, the entire ClearPass authentication table contents, users who belong to a domain, users who belong to a group, or a user's entry based on the user's name.

The ClearPass authentication table user entries include authentication and identity information that the SRX Series device obtains from the ClearPass Policy Manager (CPPM). ClearPass, which is the authentication source for the Integrated ClearPass Authentication and Enforcement feature, posts the user authentication information to the SRX Series device. The SRX Series device UserID daemon synchronizes the ClearPass user authentication information from the Routing Engine authentication table, which includes entries from other authentication sources, to the ClearPass authentication table on the Packet Forwarding Engine.

To supplement posting from the ClearPass authentication table, the SRX Series device supports a user query function that allows you to obtain authentication information for an individual user.

**Options** *ip-address*—Displays information for a user identified by the IP address of their device.

*authentication-source*—The authentication source for the Integrated ClearPass Authentication and Enforcement feature. For this feature, you must specify the value *aruba-clearpass*.

Specify the following identifiers to control the degree and kind of information to display:

**brief**—By default, the show command displays brief information for ClearPass authentication table user entries. For each domain, it displays the domain name and the number of users who belong to it. For each user, it shows the user's device IP address, username, groups that the user belongs to that are referenced by a security policy, and the state of the user entry.

**domain** —Specifies the name of domain whose user member information you want to view. You can specify *extensive* with *domain* to show extensive information for user entries for all of its members. By default, brief information is displayed.

**extensive**—Shows extensive information for the ClearPass authentication table user entries. For each domain, *extensive* displays the domain name and the number of users who belong to it. For each user, it shows the user's device IP address, username, the groups that the user belongs to, the groups that the user belongs to that are referenced by a security policy, the state of the user entry, the authentication source

(Aruba ClearPass), the access start date and time, a timestamp showing the last time the entry was updated, and the age after which time the entry expires.

You can specify `extensive` without a qualifying identifier to display extensive information for all of the table's user entries. You can specify it in conjunction with `domain`, `group`, or `user` to display extensive information for that category of users—that is, all members of the domain, all users who belong to the group, or an individual user identified by their username.

**group**—Specifies the name of the group whose member information you want to view. You can specify `extensive` with `group` to show extensive information for users who belong to the group. By default, brief information is displayed.

**user**—Specifies the name of the user whose information you want to view. You can specify `extensive` to show extensive information for that user.

**Required Privilege Level**

view

**List of Sample Output**

[show services user-identification authentication-table authentication-source aruba-clearpass on page 200](#)  
[show services user-identification authentication-table authentication-source aruba-clearpass domain on page 202](#)  
[show services user-identification authentication-table authentication-source aruba-clearpass group on page 203](#)  
[show services user-identification authentication-table authentication-source aruba-clearpass user on page 205](#)

Field Name	Field Description
Domain <b>Output Fields</b>	Name of the domain that the users belong to. If the CPPM does not send domain information to the SRX Series device for a user, the user belongs to the GLOBAL domain.
Total entries	Number of user entries in the ClearPass authentication table by domain.
For each entry:	
Source IP	The IP address of the user's device. If a user is logged in to the network with more than one device, a separate entry is created for the user for each device. It showing the devices IP address.
username	The name by which the user is logged in to the network.
Groups	A list of the groups that the user belongs to. The list can include a group that identifies the device posture.
State	<p>The state of the entry. There are four states for an authentication entry: initial, valid, invalid, and pending.</p> <ul style="list-style-type: none"> <li>• An initial state is a temporary state, and it can be created from either a valid or an invalid entry.</li> <li>• A valid state indicates that the authentication entry has a valid IP address, domain, and username.</li> <li>• An invalid state indicates that the entry does not have a valid IP address, domain, and username. This can happen when the SRX Series device does not receive a query response from the CPPM. If the entry is invalid, it is put in the null domain.</li> <li>• A pending state indicates that the entry was created after the user query was sent and before the response was received.</li> </ul>
Source	The name of the authentication source. For the Integrated ClearPass Authentication and Enforcement feature, this value is always aruba-clearpass.
Access start date	The date when the authentication entry was created by the SRX Series device.
Access start time	The time when the authentication entry was created by the SRX Series device.
Last updated timestamp	The time when ClearPass creates the user information. This value is taken from the timestamp field in the user information posted by ClearPass to the SRX Series device.
Age time:	The time after which the entry expires, as configured by the authentication-entry-timeout statement. If a value of 0 was specified, the entry never expires. When an expiration time is reached, the SRX Series device deletes the user entry from the ClearPass authentication table.

## Sample Output

**show services user-identification authentication-table authentication-source aruba-clearpass**

Note that in the following example, the output would show the same results whether or not you specified brief. The default behavior is to display brief output.



```
user@host> show services user-identification authentication-table authentication-source
aruba-clearpass brief
```

In this case, if there was more than one domain configured, the output would show the following kind of information for each domain.

```
Domain: GLOBAL
Total entries: 6
Source IP      Username      groups(Ref by policy)      state
10.0.0.1       viki2         accounting-grp-and-company-dev Valid
20.0.0.1       abew1         marketing-access-limited-grp Valid
30.0.0.1       jxchan        marketing-access-for-pcs-limit Valid
40.0.0.1       lchen1        corporate-limited           Valid
50.0.0.1       guest1                    Valid
50.0.0.2       guest2                    Valid
```

```
user@host> show services user-identification authentication-table authentication-source
aruba-clearpass extensive
```

```
Domain: GLOBAL
Total entries: 6
Source-ip: 10.0.0.1
Username: viki2
Groups:posture-healthy, accounting-grp, accounting-grp-and-company-device,
corporate-limited, [user authenticated]
Groups referenced by policy:accounting-grp-and-company-device,
corporate-limited
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:20:30
Last updated timestamp: 2015-12-22 04:02:48
Age time: 0
Source-ip: 20.0.0.1
Username: abew1
Groups:posture-unknown, marketing-access-limited-grp, [user authenticated]
Groups referenced by policy:marketing-access-limited-grp
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:31:40
Last updated timestamp: 2015-12-22 04:18:48
Age time: 0
Source-ip: 30.0.0.1
Username: jxchan
Groups:posture-healthy, marketing-access-for-pcs-limited-group,
marketing-general, sales-limited, corporate-limited, [user authenticated]
Groups referenced by policy:marketing-access-for-pcs-limited-group,
corporate-limited
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:22:48
Last updated timestamp: 2015-12-22 05:46:21
Age time: 0
Source-ip: 40.0.0.1
Username: lchen1
Groups:posture-healthy, human-resources-grp, accounting-limited,
corporate-limited, [user authenticated]
Groups referenced by policy:corporate-limited
```

```

State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:21:37
Last updated timestamp: 2015-12-22 05:41:18
Age time: 0
Source-ip: 50.0.0.1
Username: guest1
Groups:posture-healthy, guest, [user authenticated]
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:23:10
Last updated timestamp: 2015-12-22 05:50:47
Age time: 0
Source-ip: 50.0.0.2
Username: guest2
Groups:posture-healthy, guest-device-byod, [user authenticated]
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:23:21
Last updated timestamp: 2015-12-22 05:52:44
Age time: 0

```

#### show services user-identification authentication-table authentication-source aruba-clearpass domain

Note that in the following example the output would show the same results whether or not you specified brief. The default behavior is to display brief output.

```

user@host> show services user-identification authentication-table authentication-source
aruba-clearpass domain GLOBAL brief

```

```

Domain: GLOBAL
Total entries: 6

```

Source IP	Username	groups(Ref by policy)	state
10.0.0.1	viki2	accounting-grp-and-company-dev	Valid
20.0.0.1	abew1	marketing-access-limited-grp	Valid
30.0.0.1	jxchan	marketing-access-for-pcs-limit	Valid
40.0.0.1	lchen1	corporate-limited	Valid
50.0.0.1	guest1		Valid
50.0.0.2	guest2		Valid

```

user@host> show services user-identification authentication-table authentication-source
aruba-clearpass domain GLOBAL extensive

```

```

Domain: GLOBAL
Total entries: 6
Source-ip: 10.0.0.1
Username: viki2
Groups:posture-healthy, accounting-grp, accounting-grp-and-company-device,
corporate-limited, [user authenticated]
Groups referenced by policy:accounting-grp-and-company-device,
corporate-limited
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:20:30
Last updated timestamp: 2015-12-22 04:02:48
Age time: 0
Source-ip: 20.0.0.1
Username: abew1

```

```

Groups:posture-unknown, marketing-access-limited-grp, [user authenticated]
Groups referenced by policy:marketing-access-limited-grp
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:31:40
Last updated timestamp: 2015-12-22 04:18:48
Age time: 0
Source-ip: 30.0.0.1
Username: jxchan
Groups:posture-healthy, marketing-access-for-pcs-limited-group,
marketing-general, sales-limited, corporate-limited, [user authenticated]
Groups referenced by policy:marketing-access-for-pcs-limited-group,
corporate-limited
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:22:48
Last updated timestamp: 2015-12-22 05:46:21
Age time: 0
Source-ip: 40.0.0.1
Username: lchen1
Groups:posture-healthy, human-resources-grp, accounting-limited,
corporate-limited, [user authenticated]
Groups referenced by policy:corporate-limited
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:21:37
Last updated timestamp: 2015-12-22 05:41:18
Age time: 0
Source-ip: 50.0.0.1
Username: guest1
Groups:posture-healthy, guest, [user authenticated]
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:23:10
Last updated timestamp: 2015-12-22 05:50:47
Age time: 0
Source-ip: 50.0.0.2
Username: guest2
Groups:posture-healthy, guest-device-byod, [user authenticated]
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:23:21
Last updated timestamp: 2015-12-22 05:52:44
Age time: 0

```

#### show services user-identification authentication-table authentication-source aruba-clearpass group

Note that in the following example, the output would show the same results whether or not you specified brief. The default behavior is to display brief output.

```

user@host> show services user-identification authentication-table authentication-source
aruba-clearpass group posture-healthy brief

```

```

Domain: GLOBAL
Source IP      Username      groups(Ref by policy)      state
10.0.0.1      viki2        accounting-grp-and-company-dev Valid

```

30.0.0.1	jxchan	marketing-access-for-pcs-limit	Valid
40.0.0.1	lchen1	corporate-limited	Valid
50.0.0.1	guest1		Valid
50.0.0.2	guest2		Valid

user@host> show services user-identification authentication-table authentication-source  
aruba-clearpass group posture-healthy extensive

Domain: GLOBAL

Source-ip: 10.0.0.1

Username: viki2

Groups:posture-healthy, accounting-grp, accounting-grp-and-company-device,  
corporate-limited, [user authenticated]

Groups referenced by policy:accounting-grp-and-company-device,  
corporate-limited

State: Valid

Source: Aruba ClearPass

Access start date: 2016-03-08

Access start time: 17:20:30

Last updated timestamp: 2015-12-22 04:02:48

Age time: 0

Source-ip: 30.0.0.1

Username: jxchan

Groups:posture-healthy, marketing-access-for-pcs-limited-group,  
marketing-general, sales-limited, corporate-limited, [user authenticated]

Groups referenced by policy:marketing-access-for-pcs-limited-group,  
corporate-limited

State: Valid

Source: Aruba ClearPass

Access start date: 2016-03-08

Access start time: 17:22:48

Last updated timestamp: 2015-12-22 05:46:21

Age time: 0

Source-ip: 40.0.0.1

Username: lchen1

Groups:posture-healthy, human-resources-grp, accounting-limited,  
corporate-limited, [user authenticated]

Groups referenced by policy:corporate-limited

State: Valid

Source: Aruba ClearPass

Access start date: 2016-03-08

Access start time: 17:21:37

Last updated timestamp: 2015-12-22 05:41:18

Age time: 0

Source-ip: 50.0.0.1

Username: guest1

Groups:posture-healthy, guest, [user authenticated]

State: Valid

Source: Aruba ClearPass

Access start date: 2016-03-08

Access start time: 17:23:10

Last updated timestamp: 2015-12-22 05:50:47

Age time: 0

Source-ip: 50.0.0.2

Username: guest2

Groups:posture-healthy, guest-device-byod, [user authenticated]

State: Valid

Source: Aruba ClearPass

Access start date: 2016-03-08

Access start time: 17:23:21

Last updated timestamp: 2015-12-22 05:52:44

Age time: 0

## Sample Output

`show services user-identification authentication-table authentication-source aruba-clearpass user`

```
user@host> show services user-identification authentication-source aruba-clearpass user brief
abew1
```

```
Domain: GLOBAL
Source IP      Username      groups(Ref by policy)      state
20.0.0.1      abew1        marketing-access-limited-grp Valid
```

```
user@host> show services user-identification authentication-source aruba-clearpass user
extensive abew1
```

```
Domain: GLOBAL
Source-ip: 20.0.0.1
Username: abew1
Groups:posture-unknown, marketing-access-limited-grp, [user authenticated]
Groups referenced by policy:marketing-access-limited-grp
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:31:40
Last updated timestamp: 2015-12-22 04:18:48
Age time: 0
```

## New Features in Junos OS Release 12.3X48-D20

Junos OS Release 12.3X48-D20 introduces the following features:

- [Interfaces and Routing on page 205](#)
- [Screens on page 206](#)
- [Security Policies on page 210](#)
- [VPNs on page 220](#)

## Interfaces and Routing

This topic includes the following sections:

- [CLI Enhancement for Interfaces Operational Command on page 205](#)

### CLI Enhancement for Interfaces Operational Command

- [show interfaces terse zone](#)

## show interfaces terse zone

---

<b>Syntax</b>	show interfaces terse zone
<b>Release Information</b>	Command introduced in Junos OS Release 12.3X48-D20.
<b>Description</b>	Display summary information about zone interfaces.
<b>Options</b>	This command has no options.
<b>Required Privilege Level</b>	view

### Sample Output

#### show interface terse zone

```
user@host> show interface terse zone
Interface      Admin  Link  Proto  Local          Remote      Zone
ge-0/0/0.0     up     up    inet   1.4.253.251/16      trust
```

## Screens

---

This topic includes the following sections:

- [Logging and Trapping on page 206](#)
- [System Log Message on page 210](#)

### Logging and Trapping

- [\[edit security screen\] Hierarchy Level on page 206](#)
- [trap on page 209](#)
- [show security screen status](#)

#### **[edit security screen] Hierarchy Level**

```
security {
  screen {
    ids-option screen-name {
      alarm-without-drop;
      description text;
      icmp {
        flood {
          threshold number;
        }
        fragment;
        icmpv6-malformed;
        ip-sweep {
          threshold number;
        }
        large;
        ping-death;
      }
    }
  }
}
```

```

ip {
  bad-option;
  block-frag;
  ipv6-extension-header {
    AH-header;
    ESP-header;
    HIP-header;
    destination-header {
      ILNP-nonce-option;
      home-address-option;
      line-identification-option;
      tunnel-encapsulation-limit-option;
      user-defined-option-type <type-low> to <type-high>;
    }
    fragment-header;
    hop-by-hop-header {
      CALIPSO-option;
      RPL-option;
      SFM-DPD-option;
      jumbo-payload-option;
      quick-start-option;
      router-alert-option;
      user-defined-option-type <type-low> to <type-high>;
    }
    mobility-header;
    no-next-header;
    routing-header;
    shim6-header
    user-defined-option-type <type-low> to <type-high>;
  }
  ipv6-extension-header-limit limit;
  ipv6-malformed-header;
  loose-source-route-option;
  record-route-option;
  security-option;
  source-route-option;
  spoofing;
  stream-option;
  strict-source-route-option;
  tear-drop;
  timestamp-option;
  unknown-protocol;
  tunnel {
    gre {
      gre-4in4;
      gre-4in6;
      gre-6in4;
      gre-6in6;
    }
    ip-in-udp {
      teredo;
    }
  }
  ipip {
    ipip-4in4;
    ipip-4in6;
    ipip-6in4;
  }
}

```

```

        ipip-6in6;
        ipip-6over4;
        ipip-6to4relay;
        isatap;
        dslite;
    }
    bad-inner-header;
}
}
limit-session {
    destination-ip-based number;
    source-ip-based number;
}
tcp {
    fin-no-ack;
    land;
    port-scan {
        threshold number;
    }
    syn-ack-ack-proxy {
        threshold number;
    }
    syn-fin;
    syn-flood {
        alarm-threshold number;
        attack-threshold number;
        destination-threshold number;
        source-threshold number;
        timeout seconds;
        white-list name {
            destination-address destination-address;
            source-address source-address;
        }
    }
    syn-frag;
    tcp-no-flag;
    tcp-sweep {
        threshold threshold number;
    }
    winnuke;
}
udp {
    flood {
        threshold number;
    }
    udp-sweep {
        threshold threshold number;
    }
}
}
}
traceoptions {
    file filename {
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
    }
}

```



```

        size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
}
trap {
    interval trap interval;
}
}
}

```

- Related Documentation**
- *Attack Detection and Prevention Overview*
  - *Example: Configuring Multiple Screening Options*
  - *Security Configuration Statement Hierarchy*

## trap

<b>Syntax</b>	trap { interval trap interval; }
<b>Hierarchy Level</b>	[edit security screen trap]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D20.
<b>Description</b>	Configure trap interval.
<b>Options</b>	<b>interval</b> —The trap interval is 1 through 3600 seconds, and the default interval is 2 seconds.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Security Configuration Statement Hierarchy</i></li> </ul>

## show security screen status

---

Syntax	show security screen status
Release Information	Command introduced in Junos OS Release 12.3X48-D20.
Description	Show screen status data.
Required Privilege Level	view
List of Sample Output	<a href="#">show security screen status on page 210</a>

### Sample Output

#### show security screen status

```
user@host> show security screen status
Screen status:
  Screen trap interval : 2 second(s)
```

### System Log Message

#### RT\_SCREEN\_SESSION\_LIMIT

### RT\_SCREEN\_SESSION\_LIMIT

---

System Log Message	<i>attack-name</i> : (if not root-lsys): [ <i>lsys:logical-system-name</i> ] <i>sub-attack-name</i> !, source: <i>source-ip-address</i> : <i>source-port</i> or undefined, destination: <i>destination-ip-address</i> : <i>destination-port</i> or undefined, protocol-id: <i>protocol-id</i> , zone name: <i>attached-zone-name</i> , interface name: <i>interface-name</i> , action: <i>action</i>
Description	<p>Session limit category</p> <ul style="list-style-type: none"><li>• The message displays original source IP based session limit when the <b>source-ip-address</b> is configured.</li><li>• The message displays original destination IP based session limit when the <b>destination-ip-address</b> is configured.</li><li>• The source port number and destination port number displays <b>undefined</b> when there is no port traffic.</li></ul>
Type	Event: This message reports an event, not an error
Severity	error
Facility	LOG_PFE

### Security Policies

---

This topic includes the following sections:

- [Setting TCP MSS per Policy on page 211](#)

## Setting TCP MSS per Policy

- [initial-tcp-mss on page 211](#)
- [reverse-tcp-mss on page 212](#)
- [show security policies](#)

## initial-tcp-mss

<b>Syntax</b>	<code>initial-tcp-mss <i>mss-value</i>;</code>
<b>Hierarchy Level</b>	[edit security policies from-zone <i>zone-name</i> to-zone <i>zone-name</i> policy <i>policy-name</i> then permit tcp-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D20.
<b>Description</b>	<p>Configure the TCP maximum segment size (MSS) for packets that arrive at the ingress interface (initial direction), match a specific policy, and for which a session is created. The value you configure overrides the TCP MSS value in the incoming packet when the value in the packet is higher than the one you specify.</p> <p>The <b>initial-tcp-mss</b> value per policy takes precedence over a global <b>tcp-mss</b> value (<b>all-tcp</b>, <b>ipsec-vpn</b>, <b>gre-in</b>, <b>gre-out</b>), if one is configured. However, when the <b>syn-flood-protection-mode syn-proxy</b> statement at the [edit security flow] hierarchy level is used to enable SYN proxy defenses against SYN attacks, the TCP MSS value is not overridden.</p> <p>Because each policy has two directions, you can configure a value for both directions or for just one direction. To configure a TCP MSS value for the reverse session, use the <b>reverse-tcp-mss</b> option.</p>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>tcp-mss (Security Flow)</i></li> <li>• <i>syn-flood-protection-mode</i></li> </ul>

## reverse-tcp-mss

---

<b>Syntax</b>	<code>reverse-tcp-mss <i>mss-value</i>;</code>
<b>Hierarchy Level</b>	[edit security policies from-zone <i>zone-name</i> to-zone <i>zone-name</i> policy <i>policy-name</i> then permit tcp-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X48-D20.
<b>Description</b>	<p>Configure the TCP maximum segment size (MSS) for packets that match a specific policy and travel in the reverse direction of a session. The value you configure replaces the TCP MSS value when the value in the packet is higher than the one you specify.</p> <p>The <b>reverse-tcp-mss</b> value per policy takes precedence over a global <b>tcp-mss</b> value (<b>all-tcp</b>, <b>ipsec-vpn</b>, <b>gre-in</b>, <b>gre-out</b>), if one is configured. However, when the <b>syn-flood-protection-mode syn-proxy</b> statement at the [edit security flow] hierarchy level is used to enable SYN proxy defenses against SYN attacks, the TCP MSS value is not overridden.</p> <p>Because each policy has two directions, you can configure a value for both directions or for just one direction. To configure the TCP MSS value for the initial session, use the <b>initial-tcp-mss</b> option.</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>tcp-mss (Security Flow)</i></li><li>• <i>syn-flood-protection-mode</i></li></ul>

## show security policies

<b>Syntax</b>	<pre>show security policies &lt;detail&gt; &lt;none&gt; policy-name <i>policy-name</i> &lt;detail&gt; &lt;global&gt;</pre>
<b>Release Information</b>	<p>Command modified in Junos OS Release 9.2. Support for IPv6 addresses added in Junos OS Release 10.2. Support for IPv6 addresses in active/active chassis cluster configurations in addition to the existing support of active/passive chassis cluster configurations added in Junos OS Release 10.4. Support for wildcard addresses added in Junos OS Release 11.1. Support for global policy added in Junos OS Release 11.4. Support for services offloading added in Junos OS Release 11.4. Support for source-identities added in Junos OS Release 12.1. The <b>Description</b> output field added in Junos OS Release 12.1. Support for negated address added in Junos OS Release 12.1X45-D10. The output fields for Policy Statistics expanded, and the output fields for the <b>global</b> and <b>policy-name</b> options expanded to include from-zone and to-zone global match criteria in Junos OS Release 12.1X47-D10. Support for the <b>initial-tcp-mss</b> and <b>reverse-tcp-mss</b> options added in Junos OS Release 12.3X48-D20.</p>
<b>Description</b>	<p>Display a summary of all security policies configured on the device. If a particular policy is specified, display information particular to that policy.</p>
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>none</b>—Display basic information about all configured policies.</li> <li>• <b>detail</b>—(Optional) Display a detailed view of all of the policies configured on the device.</li> <li>• <b>policy-name <i>policy-name</i></b>—(Optional) Display information about the specified policy.</li> <li>• <b>global</b>—Display information about global policies.</li> </ul>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Security Policies Overview</i></li> <li>• <i>Understanding Security Policy Rules</i></li> <li>• <i>Understanding Security Policy Elements</i></li> <li>• <i>Building Blocks Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<p><a href="#">show security policies on page 216</a>  <a href="#">show security policies policy-name p1 detail on page 217</a>  <a href="#">show security policies (services-offload) on page 218</a>  <a href="#">show security policies detail on page 218</a>  <a href="#">show security policies detail (TCP Options) on page 219</a>  <a href="#">show security policies policy-name p1 (Negated Address) on page 219</a>  <a href="#">show security policies policy-name p1 detail (Negated Address) on page 220</a>  <a href="#">show security policies global on page 220</a></p>

**Output Fields** Table 8 on page 214 lists the output fields for the **show security policies** command. Output fields are listed in the approximate order in which they appear.

**Table 8: show security policies Output Fields**

Field Name	Field Description
<b>From zone</b>	Name of the source zone.
<b>To zone</b>	Name of the destination zone.
<b>Policy</b>	Name of the applicable policy.
<b>Description</b>	Description of the applicable policy.
<b>State</b>	Status of the policy: <ul style="list-style-type: none"> <li>• <b>enabled:</b> The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it.</li> <li>• <b>disabled:</b> The policy cannot be used in the policy lookup process, and therefore it is not available for access control.</li> </ul>
<b>Index</b>	Internal number associated with the policy.
<b>Sequence number</b>	Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, 4.
<b>Source addresses</b>	For standard display mode, the names of the source addresses for a policy. Address sets are resolved to their individual names.  For detail display mode, the names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs.
<b>Destination addresses</b>	Name of the destination address (or address set) as it was entered in the destination zone's address book. A packet's destination address must match this value for the policy to apply to it.
<b>Source addresses (excluded)</b>	Name of the source address excluded from the policy.
<b>Destination addresses (excluded)</b>	Name of the destination address excluded from the policy.
<b>Source identities</b>	One or more user roles specified for a policy.

Table 8: show security policies Output Fields (*continued*)

Field Name	Field Description
Applications	<p>Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time.</p> <ul style="list-style-type: none"> <li>• <b>IP protocol</b>: The Internet protocol used by the application—for example, TCP, UDP, ICMP.</li> <li>• <b>ALG</b>: If an ALG is explicitly associated with the policy, the name of the ALG is displayed. If <b>application-protocol ignore</b> is configured, ignore is displayed. Otherwise, 0 is displayed. However, even if this command shows ALG: 0, ALGs might be triggered for packets destined to well-known ports on which ALGs are listening, unless ALGs are explicitly disabled or when <b>application-protocol ignore</b> is not configured for custom applications.</li> <li>• <b>Inactivity timeout</b>: Elapsed time without activity after which the application is terminated.</li> <li>• <b>Source port range</b>: The low-high source port range for the session application.</li> </ul>
Destination Address Translation	<p>Status of the destination address translation traffic:</p> <ul style="list-style-type: none"> <li>• <b>drop translated</b>—Drop the packets with translated destination addresses.</li> <li>• <b>drop untranslated</b>—Drop the packets without translated destination addresses.</li> </ul>
Application Firewall	<p>An application firewall includes the following:</p> <ul style="list-style-type: none"> <li>• <b>Rule-set</b>—Name of the rule set.</li> <li>• <b>Rule</b>—Name of the rule. <ul style="list-style-type: none"> <li>• <b>Dynamic applications</b>—Name of the applications.</li> <li>• <b>Dynamic application groups</b>—Name of the application groups.</li> <li>• <b>Action</b>—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following: <ul style="list-style-type: none"> <li>• <b>permit</b></li> <li>• <b>deny</b></li> </ul> </li> </ul> </li> <li>• <b>Default rule</b>—The default rule applied when the identified application is not specified in any rules of the rule set.</li> </ul>
Action or Action-type	<ul style="list-style-type: none"> <li>• The action taken in regard to a packet that matches the policy's tuples. Actions include the following: <ul style="list-style-type: none"> <li>• <b>permit</b></li> <li>• <b>firewall-authentication</b></li> <li>• <b>tunnel ipsec-vpn <i>vpn-name</i></b></li> <li>• <b>pair-policy <i>pair-policy-name</i></b></li> <li>• <b>source-nat pool <i>pool-name</i></b></li> <li>• <b>pool-set <i>pool-set-name</i></b></li> <li>• <b>interface</b></li> <li>• <b>destination-nat <i>name</i></b></li> <li>• <b>deny</b></li> <li>• <b>reject</b></li> <li>• <b>services-offload</b></li> </ul> </li> </ul>
Session log	<p>Session log entry that indicates whether the <b>at-create</b> and <b>at-close</b> flags were set at configuration time to log session information.</p>

Table 8: show security policies Output Fields (*continued*)

Field Name	Field Description
<b>Scheduler name</b>	Name of a preconfigured scheduler whose schedule determines when the policy is active and can be used as a possible match for traffic.
<b>Policy statistics</b>	<ul style="list-style-type: none"> <li>• <b>Input bytes</b>—The total number of bytes presented for processing by the device. <ul style="list-style-type: none"> <li>• <b>Initial direction</b>—The number of bytes presented for processing by the device from the initial direction.</li> <li>• <b>Reply direction</b>—The number of bytes presented for processing by the device from the reply direction.</li> </ul> </li> <li>• <b>Output bytes</b>—The total number of bytes actually processed by the device. <ul style="list-style-type: none"> <li>• <b>Initial direction</b>—The number of bytes from the initial direction actually processed by the device.</li> <li>• <b>Reply direction</b>—The number of bytes from the reply direction actually processed by the device.</li> </ul> </li> <li>• <b>Input packets</b>—The total number of packets presented for processing by the device. <ul style="list-style-type: none"> <li>• <b>Initial direction</b>—The number of packets presented for processing by the device from the initial direction.</li> <li>• <b>Reply direction</b>—The number of packets presented for processing by the device from the reply direction.</li> </ul> </li> <li>• <b>Output packets</b>—The total number of packets actually processed by the device. <ul style="list-style-type: none"> <li>• <b>Initial direction</b>—The number of packets actually processed by the device from the initial direction.</li> <li>• <b>Reply direction</b>—The number of packets actually processed by the device from the reply direction.</li> </ul> </li> <li>• <b>Session rate</b>—The total number of active and deleted sessions.</li> <li>• <b>Active sessions</b>—The number of sessions currently present because of access control lookups that used this policy.</li> <li>• <b>Session deletions</b>—The number of sessions deleted since system startup.</li> <li>• <b>Policy lookups</b>—The number of times the policy was accessed to check for a match.</li> </ul> <p><b>NOTE:</b> Configure the Policy P1 with the <b>count</b> option to display policy statistics.</p>
<b>Per policy TCP Options</b>	Configured sync and sequence checks, and the configured TCP MSS value for the initial direction and /or the reverse direction.

## Sample Output

### show security policies

```

user@host> show security policies
From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Sequence number: 1
Source addresses:
sa-1-ipv4: 2.2.2.0/24
sa-2-ipv6: 2001:0db8::/32
sa-3-ipv6: 2001:0db6/24
sa-4-wc: 192.168.0.11/255.255.0.255
Destination addresses:
da-1-ipv4: 2.2.2.0/24
da-2-ipv6: 2400:0af8::/32

```



```

da-3-ipv6: 2400:0d78:0/24
da-4-wc: 192.168.22.11/255.255.0.255
Source identities: role1, role2, role4
Applications: any
Action: permit, application services, log, scheduled
Application firewall : my_ruleset1
Policy: p2, State: enabled, Index: 5, Sequence number: 2
Source addresses:
sa-1-ipv4: 2.2.2.0/24
sa-2-ipv6: 2001:0db8::/32
sa-3-ipv6: 2001:0db6/24
Destination addresses:
da-1-ipv4: 2.2.2.0/24
da-2-ipv6: 2400:0af8::/32
da-3-ipv6: 2400:0d78:0/24
Source identities: role1, role4
Applications: any
Action: deny, scheduled

```

### show security policies policy-name p1 detail

```

user@host> show security policies policy-name p1 detail
Policy: p1, action-type: permit, State: enabled, Index: 4
Description: The policy p1 is for the sales team
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses:
sa-1-ipv4: 2.2.2.0/24
sa-2-ipv6: 2001:0db8::/32
sa-3-ipv6: 2001:0db6/24
sa-4-wc: 192.168.0.11/255.255.0.255
Destination addresses:
da-1-ipv4: 2.2.2.0/24
da-2-ipv6: 2400:0af8::/32
da-3-ipv6: 2400:0d78:0/24
da-4-wc: 192.168.22.11/255.255.0.255
Source identities:
role1
role2
role4
Application: any
IP protocol: 0, ALG: 0, Inactivity timeout: 0
Source port range: [0-0]
Destination port range: [0-0]
Destination Address Translation: drop translated
Application firewall :
Rule-set: my_ruleset1
Rule: rule1
Dynamic Applications: junos:FACEBOOK, junos:YMSG
Dynamic Application groups: junos:web, junos:chat
Action: deny
Default rule: permit
Session log: at-create, at-close
Scheduler name: sch20
Per policy TCP Options: SYN check: No, SEQ check: No
Policy statistics:
Input bytes      : 18144      545 bps
Initial direction: 9072       272 bps
Reply direction  : 9072       272 bps
Output bytes     : 18144      545 bps
Initial direction: 9072       272 bps

```

Reply direction :	9072	272 bps
Input packets :	216	6 pps
Initial direction:	108	3 bps
Reply direction :	108	3 bps
Output packets :	216	6 pps
Initial direction:	108	3 bps
Reply direction :	108	3 bps
Session rate :	108	3 sps
Active sessions :	93	
Session deletions :	15	
Policy lookups :	108	

### show security policies (services-offload)

```

user@host> show security policies
Default policy: deny-all
From zone: trust, To zone: untrust
  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, services-offload, count
From zone: untrust, To zone: trust
  Policy: p2, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, services-offload

```

### show security policies detail

```

user@host> show security policies detail
Default policy: deny-all
Policy: p1, action-type: permit, services-offload:enabled , State: enabled, Index:
4, Scope Policy: 0
Policy Type: Configured
Description: The policy p1 is for the sales team
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Source identities:
  role1
  role2
  role4
Application: any
IP protocol: 0, ALG: 0, Inactivity timeout: 0
Source port range: [0-0]
Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No
Policy statistics:
  Input bytes      :      18144      545 bps
  Initial direction:      9072      272 bps
  Reply direction  :      9072      272 bps
  Output bytes     :      18144      545 bps

```

```

Initial direction:          9072          272 bps
Reply direction :          9072          272 bps
Input packets :            216           6 pps
Initial direction:          108           3 bps
Reply direction :          108           3 bps
Output packets :            216           6 pps
Initial direction:          108           3 bps
Reply direction :          108           3 bps
Session rate :             108           3 sps
Active sessions :           93
Session deletions :         15
Policy lookups :            108

Policy: p2, action-type: permit, services-offload:enabled , State: enabled, Index:
5, Scope Policy: 0
Policy Type: Configured
Description: The policy p2 is for the sales team
Sequence number: 1
From zone: untrust, To zone: trust
Source addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Source identities:
  role1
  role2
  role4
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
  Source port range: [0-0]
  Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No

```

#### show security policies detail (TCP Options)

```

user@host> show security policies policy-name policy1 detail
node0:
-----
Policy: policy1, action-type: permit, State: enabled, Index: 7, Scope Policy: 0
Policy Type: Configured
Sequence number: 2
From zone: trust, To zone: untrust
Source addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
  Source port range: [0-0]
  Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No
Per policy TCP MSS: initial: 800, reverse: 900

```

#### show security policies policy-name p1 (Negated Address)

```

user@host> show security policies policy-name p1
node0:
-----

```

```
From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
Source addresses(excluded): as1
Destination addresses(excluded): as2
Applications: any
Action: permit
```

#### show security policies policy-name p1 detail (Negated Address)

```
user@host>show security policies policy-name p1 detail
node0:
-----
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
Policy Type: Configured
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses(excluded):
  ad1(ad): 255.255.255.255/32
  ad2(ad): 1.1.1.1/32
  ad3(ad): 15.100.199.56 ~ 15.200.100.16
  ad4(ad): 15.100.196.0/22
  ad5(ad): 15.1.7.199 ~ 15.1.8.19
  ad6(ad): 15.1.8.0/21
  ad7(ad): 15.1.7.0/24
Destination addresses(excluded):
  ad13(ad2): 20.1.7.0/24
  ad12(ad2): 20.1.4.1/32
  ad11(ad2): 20.1.7.199 ~ 20.1.8.19
  ad10(ad2): 50.1.4.0/22
  ad9(ad2): 20.1.1.11 ~ 50.1.5.199
  ad8(ad2): 2.1.1.1/32
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
  Source port range: [0-0]
  Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No
```

#### show security policies global

```
user@host>show security policies global policy-name Pa
node0:
-----
Global policies:
Policy: Pa, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
From zones: zone1, zone2
To zones: zone3, zone4
Source addresses: any
Destination addresses: any
Applications: any
Action: permit
```

---

## VPNs

- [AutoVPN Spokes and Auto Discovery VPN \(ADVPN\) Partners on High-End SRX Series Devices on page 221](#)
- [IKEv2 AES-GCM for Branch SRX Series and SRX5600 and SRX5800 Devices With Next-Generation Services Processing Card on page 243](#)

## AutoVPN Spokes and Auto Discovery VPN (ADVPN) Partners on High-End SRX Series Devices

- [Understanding Auto Discovery VPN on page 221](#)
- [advpn on page 226](#)
- [show security ike security-associations](#)
- [show security ipsec security-associations](#)

### ***Understanding Auto Discovery VPN***

AutoVPN deployments can use the Auto Discovery VPN (ADVPN) protocol to dynamically establish spoke-to-spoke VPN tunnels. When passing traffic from one spoke to another spoke, the hub can suggest that the spokes establish a direct security association (SA), called a shortcut, between each other. Shortcuts can be established and torn down dynamically between spokes, resulting in better network resource utilization and less reliance on a centrally located hub.

- [ADVPN Protocol on page 221](#)
- [Establishing a Shortcut on page 221](#)
- [Shortcut Initiator and Responder Roles on page 223](#)
- [Shortcut Attributes on page 223](#)
- [Shortcut Termination on page 224](#)
- [ADVPN Configuration Limitations on page 225](#)

### ***ADVPN Protocol***

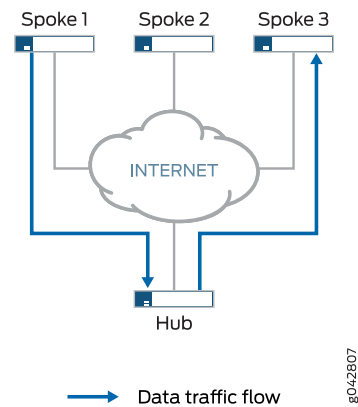
The ADVPN protocol is an extension of IKEv2 that allows a shortcut to be created between two VPN peers. Devices that support the ADVPN protocol send an ADVPN\_SUPPORTED notification in the IKEv2 Notify payload during the initial IKE exchange. A device that supports ADVPN can act as either a shortcut suggester or a shortcut partner, but not both. This shortcut capability information, along with the ADVPN version number, is also exchanged.

### ***Establishing a Shortcut***

An IPsec VPN gateway can act as a shortcut suggester when it notices that traffic is exiting a tunnel with one of its peers and entering a tunnel with another peer.

[Figure 10 on page 222](#) shows traffic from Spoke 1 to Spoke 3 passing through the hub.

Figure 10: Spoke-to-Spoke Traffic Passing Through Hub

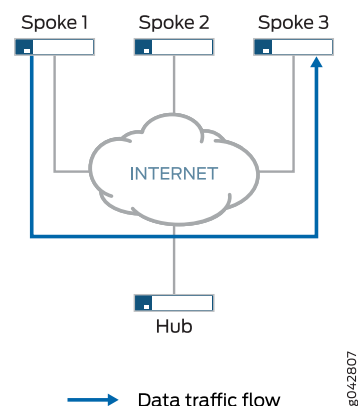


When ADVPN is configured on the devices, ADVPN shortcut capability information is exchanged between the hub and spokes. As long as Spokes 1 and 3 have previously advertised ADVPN shortcut partner capability to the hub, the hub can suggest that Spokes 1 and 3 establish a shortcut between each other.

The shortcut suggester uses its already established IKEv2 SAs with the peers to begin a shortcut exchange with one of the two peers. If the peer accepts the shortcut exchange, then the shortcut suggester begins a shortcut exchange with the other peer. The shortcut exchange includes information to allow the peers (referred to as shortcut partners) to establish IKE and IPsec SAs with each other. The creation of the shortcut between the shortcut partners starts only after both peers accept the shortcut exchange.

[Figure 11 on page 222](#) shows traffic passing through a shortcut between Spokes 1 and 3. Traffic from Spoke 1 to Spoke 3 does not need to traverse the hub.

Figure 11: Spoke-to-Spoke Traffic Passing Through Shortcut



### ***Shortcut Initiator and Responder Roles***

The shortcut suggester chooses one of the shortcut partners to act as the initiator for the shortcut; the other partner acts as the responder. If one of the partners is behind a NAT device, then the partner behind the NAT device is chosen as the initiator. If none of the partners is behind a NAT device, then the suggester randomly chooses one of the partners as the initiator; the other partner acts as the responder. If both partners are behind NAT devices, then a shortcut cannot be created between them; the suggester does not send a shortcut exchange to any of the peers.

The shortcut suggester begins the shortcut exchange with the responder first. If the responder accepts the shortcut suggestion, then the suggester notifies the initiator.

Using information contained in the shortcut suggester's notification, the shortcut initiator establishes an IKEv2 exchange with the responder, and a new IPsec SA is established between the two partners. On each partner, the route to the network behind its partner now points to the shortcut instead of to the tunnel between the partner and the suggester. Traffic originating behind one of the partners that is destined to a network behind the other shortcut partner flows over the shortcut.

If the partners decline the shortcut suggestion, then the partners notify the suggester with the reason for the rejection. In this case, traffic between the partners continues to flow through the shortcut suggester.

### ***Shortcut Attributes***

The shortcut receives some of its attributes from the shortcut suggester while other attributes are inherited from the suggester-partner VPN tunnel configuration.

[Table 9 on page 223](#) shows the parameters of the shortcut.

**Table 9: Shortcut Parameters**

Attributes	Received/Inherited From
ADVPN	Configuration
Antireplay	Configuration
Authentication algorithm	Configuration
Dead peer detection	Configuration
DF bit	Configuration
Encryption algorithm	Configuration
Establish tunnels	Suggester
External interface	Configuration
Gateway policy	Configuration

Table 9: Shortcut Parameters (*continued*)

Attributes	Received/Inherited From
General IKE ID	Configuration
IKE version	Configuration
Install interval	Configuration
Local address	Configuration
Local identity	Suggester
NAT traversal	Configuration
Perfect forward secrecy	Configuration
Protocol	Configuration
Proxy ID	Not applicable
Remote address	Suggester
Remote identity	Suggester
Respond bad SPI	Configuration
Traffic selector	Not applicable

**Shortcut Termination**

By default, the shortcut lasts indefinitely. Shortcut partners terminate the shortcut if traffic falls below a specified rate for a specified time. By default, the shortcut is terminated if traffic falls below 5 packets per second for 900 seconds; the idle time and idle threshold values are configurable for partners. The shortcut can be manually deleted on either shortcut partner with the **clear security ike security-association** or **clear security ipsec security-association** commands to clear the corresponding IKE or IPsec SA. Either of the shortcut partners can terminate the shortcut at any time by sending an IKEv2 delete payload to the other shortcut partner.

When the shortcut is terminated, the corresponding IKE SA and all child IPsec SAs are deleted. After the shortcut is terminated, the corresponding route is deleted on both shortcut partners and traffic between the two peers again flows through the suggester. Shortcut termination information is sent from a partner to the suggester.

The lifetime of a shortcut is independent of the tunnel between the shortcut suggester and shortcut partner. The shortcut is not terminated simply because the tunnel between the suggester and partner is terminated.



### ***ADVPN Configuration Limitations***

Note the following limitations when configuring ADVPN:

- Configuring an ADVPN partner is only allowed on site-to-site VPNs. Configuring an ADVPN suggester is only allowed on AutoVPN hubs.
- You cannot configure both suggester and partner roles on the same gateway. When ADVPN is enabled on a gateway, you cannot disable both suggester and partner roles on the gateway.
- As mentioned previously, you cannot create a shortcut between partners that are both behind NAT devices. The suggester can initiate a shortcut exchange if only one of the partners is behind a NAT device or if no partners are behind NAT devices.
- Only the OSPF dynamic routing protocol is supported with ADVPN; RIP and BGP are not supported.

The following configurations are not supported with ADVPN:

- IKEv1
- Policy-based VPN
- IKEv2 configuration payload
- Traffic selectors
- Preshared key
- Point-to-point secure tunnel interfaces

### **Related Documentation**

- *Understanding Traffic Routing with Shortcut Tunnels*
- *Example: Improving Network Resource Utilization with Auto Discovery VPN Dynamic Tunnels*
- *Enabling OSPF to Update Routes Quickly After ADVPN Shortcut Tunnels Are Established*

## advpn

```
Syntax  advpn {
        suggester {
            disable;
        }
        partner {
            connection-limit <number>;
            idle-threshold <packets/sec>;
            idle-time <seconds>;
            disable;
        }
    }
```

**Hierarchy Level** [edit security ike gateway *gateway-name*]

**Release Information** Statement introduced in Junos OS Release 12.3X48-D10. The range for the **idle-threshold** option and the range and default value for the **idle-time** option revised in Junos OS Release 12.3X48-D20.

**Description** Enable Auto Discovery VPN (ADVPN) protocol on the specified gateway.

**Options** **suggester**—VPN peer that can initiate a shortcut exchange to allow shortcut partners to establish dynamic security associations (SAs) with each other. Specify **disable** to disable this role on the gateway.



**NOTE:** Both **suggester** and **partner** roles are enabled if **advpn** is configured without explicitly configuring **suggester** or **partner** keywords. We do not support **suggester** and **partner** roles on the same gateway. You must explicitly configure **disable** with the **suggester** or **partner** keyword to disable that particular role. You cannot disable both **suggester** and **partner** roles on the same gateway.

**partner**—VPN peer that can receive a shortcut exchange suggesting that it should establish dynamic SAs with another peer. Specify **disable** to disable this role on the gateway. The following options can be configured for the **partner** role:

**connection-limit**—Maximum number of shortcut tunnels that can be created with different shortcut partners using a particular gateway. The maximum number, which is also the default, is platform-dependent.



**NOTE:** Reducing the configured **connection-limit** value causes all active shortcut tunnels to be brought down. For example, if **connection-limit** is configured as 100 and you later reconfigure the number to 80, all active shortcut tunnels are brought down. Increasing the configured **connection-limit** value does not cause shortcut tunnels to go down.

**idle-threshold**—Rate, in packets per second, below which the shortcut is brought down.

**Range:** 3 through 5,000 packets per second.

**Default:** 5 packets per second.

**idle-time**—Duration, in seconds, after which the shortcut is deleted if the traffic remains below the **idle-threshold** value.

**Range:** 60 through 86,400 seconds.

**Default:** 300 seconds.

<b>Required Privilege</b>	security—To view this statement in the configuration.
<b>Level</b>	security-control—To add this statement to the configuration.

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Understanding Auto Discovery VPN on page 221</a></li></ul>
------------------------------	--

## show security ike security-associations

---

**Syntax**    **show security ike security-associations**  
              *peer-address*  
              **brief** | **detail**  
              **family** (inet | inet6)  
              *fpc slot-number*  
              *index SA-index-number*  
              **kmd-instance** (all | *kmd-instance-name*)  
              *pic slot-number*  
              **sa-type** shortcut <detail>

**Release Information**    Command introduced in Junos OS Release 8.5. Support for the **fpc**, **pic**, and **kmd-instance** options added in Junos OS Release 9.3. Support for the **family** option added in Junos OS Release 11.1. Support for Auto Discovery VPN added in Junos OS Release 12.3X48-D10.

**Description**    Display information about Internet Key Exchange security associations (IKE SAs).

- Options**
- **none**—Display standard information about existing IKE SAs, including index numbers.
  - **peer-address**—(Optional) Display details about a particular SA based on the IPv4 or IPv6 address of the destination peer. This option and **index** provide the same level of output.
  - **brief**—(Optional) Display standard information about all existing IKE SAs. (Default)
  - **detail**—(Optional) Display detailed information about all existing IKE SAs.
  - **family**—(Optional) Display IKE SAs by family. This option is used to filter the output.
    - **inet**—IPv4 address family.
    - **inet6**—IPv6 address family.
  - **fpc slot-number**—(Optional) Display information about existing IKE SAs in this Flexible PIC Concentrator (FPC) slot. This option is used to filter the output.
  - **index SA-index-number**—(Optional) Display information for a particular SA based on the index number of the SA. For a particular SA, display the list of existing SAs by using the command with no options. This option and **peer-address** provide the same level of output.
  - **kmd-instance** —(Optional) Display information about existing IKE SAs in the key management process (in this case, it is KMD) identified by FPC *slot-number* and PIC *slot-number*. This option is used to filter the output.
    - **all**—All KMD instances running on the Services Processing Unit (SPU).
    - **kmd-instance-name**—Name of the KMD instance running on the SPU.
  - **pic slot-number** —(Optional) Display information about existing IKE SAs in this PIC slot. This option is used to filter the output.
  - **sa-type**—(Optional for ADVPN) Type of SA. **shortcut** is the only option for this release.

**Required Privilege Level** view

**Related Documentation**

- *Example: Configuring a Route-Based VPN Tunnel in a User Logical System*

**List of Sample Output** [show security ike security-associations \(IPv4\) on page 231](#)  
[show security ike security-associations \(IPv6\) on page 231](#)  
[show security ike security-associations detail \(Branch SRX Series Devices\) on page 232](#)  
[show security ike security-associations detail \(High-End SRX Series Devices\) on page 232](#)  
[show security ike security-associations family inet6 on page 233](#)  
[show security ike security-associations index 8 detail on page 233](#)  
[show security ike security-associations 1.1.1.2 on page 234](#)  
[show security ike security-associations fpc 6 pic 1 kmd-instance all \(SRX Series Devices\) on page 234](#)  
[show security ike security-associations detail \(ADVPN Enabled on Suggester Only\) on page 234](#)  
[show security ike security-associations detail \(ADVPN Enabled on Partner\) on page 234](#)  
[show security ike security-associations sa-type shortcut \(ADVPN\) on page 234](#)  
[show security ike security-associations sa-type shortcut detail \(ADVPN\) on page 234](#)

**Output Fields** [Table 10 on page 229](#) lists the output fields for the **show security ike security-associations** command. Output fields are listed in the approximate order in which they appear.

**Table 10: show security ike security-associations Output Fields**

Field Name	Field Description
<b>IKE Peer or Remote Address</b>	IP address of the destination peer with which the local peer communicates.
<b>Index</b>	Index number of an SA. This number is an internally generated number you can use to display information about a single SA.
<b>Gateway Name</b>	Name of the IKE gateway.
<b>Location</b>	<ul style="list-style-type: none"> <li>• <b>FPC</b>—Flexible PIC Concentrator (FPC) slot number.</li> <li>• <b>PIC</b>—PIC slot number.</li> <li>• <b>KMD-Instance</b>—The name of the KMD instance running on the SPU, identified by FPC <i>slot-number</i> and PIC <i>slot-number</i>. Currently, 4 KMD instances are running on each SPU, and any particular IKE negotiation is carried out by a single KMD instance.</li> </ul>
<b>Role</b>	Part played in the IKE session. The device triggering the IKE negotiation is the initiator, and the device accepting the first IKE exchange packets is the responder.
<b>State</b>	State of the IKE SAs: <ul style="list-style-type: none"> <li>• <b>DOWN</b>—SA has not been negotiated with the peer.</li> <li>• <b>UP</b>—SA has been negotiated with the peer.</li> </ul>
<b>Initiator cookie</b>	Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.

Table 10: show security ike security-associations Output Fields (*continued*)

Field Name	Field Description
<b>Responder cookie</b>	<p>Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.</p> <p>A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity.</p>
<b>Mode or Exchange type</b>	<p>Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between one another. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are:</p> <ul style="list-style-type: none"> <li>• <b>main</b>—The exchange is done with six messages. This mode or exchange type encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate.</li> <li>• <b>aggressive</b>—The exchange is done with three messages. This mode or exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected.</li> </ul> <p><b>NOTE:</b> IKEv2 protocol does not use the mode configuration for negotiation. Therefore, mode displays the version number of the security association.</p>
<b>Local</b>	Address of the local peer.
<b>Remote</b>	Address of the remote peer.
<b>Lifetime</b>	Number of seconds remaining until the IKE SA expires.
<b>Algorithms</b>	<p>IKE algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:</p> <ul style="list-style-type: none"> <li>• <b>Authentication</b>—Type of authentication algorithm used: <ul style="list-style-type: none"> <li>• <b>sha1</b>—Secure Hash Algorithm 1 authentication.</li> <li>• <b>md5</b>—MD5 authentication.</li> </ul> </li> <li>• <b>Encryption</b>—Type of encryption algorithm used: <ul style="list-style-type: none"> <li>• <b>aes-256-cbc</b>—Advanced Encryption Standard (AES) 256-bit encryption.</li> <li>• <b>aes-192-cbc</b>—AES 192-bit encryption.</li> <li>• <b>aes-128-cbc</b>—AES 128-bit encryption.</li> <li>• <b>3des-cbc</b>—3 Data Encryption Standard (DES) encryption.</li> <li>• <b>des-cbc</b>—DES encryption.</li> </ul> </li> </ul>
<b>Diffie-Hellman group</b>	Specifies the IKE Diffie-Hellman group.
<b>Traffic statistics</b>	<ul style="list-style-type: none"> <li>• <b>Input bytes</b>—Number of bytes received.</li> <li>• <b>Output bytes</b>—Number of bytes transmitted.</li> <li>• <b>Input packets</b>—Number of packets received.</li> <li>• <b>Output packets</b>—Number of packets transmitted.</li> </ul>

Table 10: show security ike security-associations Output Fields (*continued*)

Field Name	Field Description
Flags	<p>Notification to the key management process of the status of the IKE negotiation:</p> <ul style="list-style-type: none"> <li>• <b>caller notification sent</b>—Caller program notified about the completion of the IKE negotiation.</li> <li>• <b>waiting for done</b>—Negotiation is done. The library is waiting for the remote end retransmission timers to expire.</li> <li>• <b>waiting for remove</b>—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation.</li> <li>• <b>waiting for policy manager</b>—Negotiation is waiting for a response from the policy manager.</li> </ul>
IPSec security associations	<ul style="list-style-type: none"> <li>• <b>number created</b>: The number of SAs created.</li> <li>• <b>number deleted</b>: The number of SAs deleted.</li> </ul>
Phase 2 negotiations in progress	<p>Number of Phase 2 IKE negotiations in progress and status information:</p> <ul style="list-style-type: none"> <li>• <b>Negotiation type</b>—Type of Phase 2 negotiation. Junos OS currently supports quick mode.</li> <li>• <b>Message ID</b>—Unique identifier for a Phase 2 negotiation.</li> <li>• <b>Local identity</b>—Identity of the local Phase 2 negotiation. The format is <i>id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)</i>.</li> <li>• <b>Remote identity</b>—Identity of the remote Phase 2 negotiation. The format is <i>id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)</i>.</li> <li>• <b>Flags</b>—Notification to the key management process of the status of the IKE negotiation: <ul style="list-style-type: none"> <li>• <b>caller notification sent</b>—Caller program notified about the completion of the IKE negotiation.</li> <li>• <b>waiting for done</b>—Negotiation is done. The library is waiting for the remote end retransmission timers to expire.</li> <li>• <b>waiting for remove</b>—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation.</li> <li>• <b>waiting for policy manager</b>—Negotiation is waiting for a response from the policy manager.</li> </ul> </li> </ul>

## Sample Output

### show security ike security-associations (IPv4)

```

user@host> show security ike security-associations
Index Remote Address  State Initiator cookie  Responder cookie  Mode
8 1.1.1.2    UP  3a895f8a9f620198  9040753e66d700bb  Main
Index Remote Address  State Initiator cookie  Responder cookie  Mode
9 1.2.1.3    UP  5ba96hfa9f65067  1 70890755b65b80b  d Main

```

## Sample Output

### show security ike security-associations (IPv6)

```

user@host> show security ike security-associations
Index  State Initiator cookie  Responder cookie  Mode Remote Address
5      UP    e48efd6a444853cf  0d09c59aafb720be  Aggressive 1212::1112

```

## Sample Output

### show security ike security-associations detail (Branch SRX Series Devices)

```

user@host> show security ike security-associations detail
IKE peer 25.191.134.245, Index 2577565, Gateway Name: tropic
Role: Initiator, State: UP
Initiator cookie: b869b3424513340a, Responder cookie: 4cb3488cb19397c3
Exchange type: Main, Authentication method: Pre-shared-keys
Local: 25.191.134.241:500, Remote: 25.191.134.245:500
Lifetime: Expires in 169 seconds
Peer ike-id: 25.191.134.245
Xauth assigned IP: 0.0.0.0
Algorithms:
Authentication      : hmac-sha1-96
Encryption          : aes128-cbc
Pseudo random function: hmac-sha1
Diffie-Hellman group : DH-group-5
Traffic statistics:
Input bytes  :          1012
Output bytes :          1196
Input packets:           4
Output packets:          5
Flags: IKE SA is created
IPSec security associations: 1 created, 0 deleted
Phase 2 negotiations in progress: 0

Negotiation type: Quick mode, Role: Initiator, Message ID: 0
Local: 25.191.134.241:500, Remote: 25.191.134.245:500
Local identity: 25.191.134.241
Remote identity: 25.191.134.245
Flags: IKE SA is created

```

## Sample Output

### show security ike security-associations detail (High-End SRX Series Devices)

```

user@host> show security ike security-associations detail
IKE peer 1.1.1.2, Index 914039858, Gateway Name: tropic
Location: FPC 3, PIC 1, KMD-Instance 3
Role: Initiator, State: UP
Initiator cookie: 219a697652bdde37, Responder cookie: b49c30b229d36bcd
Exchange type: Aggressive, Authentication method: Pre-shared-keys
Local: 1.1.1.1:500, Remote: 1.1.1.2:500
Lifetime: Expires in 26297 seconds
Peer ike-id: 1.1.1.2
Xauth user-name: not available
Xauth assigned IP: 0.0.0.0
Algorithms:
Authentication      : hmac-sha1-96
Encryption          : 3des-cbc
Pseudo random function: hmac-sha1
Diffie-Hellman group : DH-group-5
Traffic statistics:
Input bytes  :          0
Output bytes :          0
Input packets:           0
Output packets:          0
IPSec security associations: 0 created, 0 deleted
Phase 2 negotiations in progress: 1

```



## Sample Output

### show security ike security-associations family inet6

```

user@host> show security ike security-associations family inet6
IKE peer 1212::1112, Index 5, Gateway Name: tropic
Role: Initiator, State: UP
Initiator cookie: e48efd6a444853cf, Responder cookie: 0d09c59aafb720be
Exchange type: Aggressive, Authentication method: Pre-shared-keys
Local: 1212::1111:500, Remote: 1212::1112:500
Lifetime: Expires in 19518 seconds
Peer ike-id: not valid
Xauth assigned IP: 0.0.0.0
Algorithms:
  Authentication      : sha1
  Encryption          : 3des-cbc
  Pseudo random function: hmac-sha1
  Diffie-Hellman group : DH-group-5
Traffic statistics:
  Input bytes  :          1568
  Output bytes :          2748
  Input packets:           6
  Output packets:         23
Flags: Caller notification sent
IPsec security associations: 5 created, 0 deleted
Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Initiator, Message ID: 2900338624
Local: 1212::1111:500, Remote: 1212::1112:500
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Flags: Caller notification sent, Waiting for done

```

## Sample Output

### show security ike security-associations index 8 detail

```

user@host> show security ike security-associations index 8 detail
IKE peer 1.1.1.2, Index 8, Gateway Name: tropic
Role: Responder, State:UP
Initiator cookie: 3a895f8a9f620198, Responder cookie: 9040753e66d700bb
Exchange type; main, Authentication method: Pre-shared-keys
Local: 1.1.1.1:500, Remote: 1.1.1.2:500
Lifetime: Expired in 381 seconds
Algorithms:
  Authentication:      md5
  Encryption:         3des-cbc
  Pseudo random function  hmac-md5
  Diffie-Hellman group   : DH-group-5
Traffic statistics:
  Input bytes:         11268
  Output bytes:        6940
  Input packets:       57
  Output packets:      57
Flags: Caller notification sent
IPsec security associations: 0 created, 0 deleted
Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Responder, Message ID: 1765792815
Local: 1.1.1.1:500, Remote: 1.1.1.2:500
Local identity: No Id

```

```
Remote identity: No Id
Flags: Caller notification sent, Waiting for remove
```

## Sample Output

### show security ike security-associations 1.1.1.2

```
user@host> show security ike security-associations 1.1.1.2
Index      State Initiator cookie Responder cookie Mode Remote Address
  8         UP    3a895f8a9f620198 9040753e66d700bb Main 1.1.1.2
```

## Sample Output

### show security ike security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices)

```
user@host> show security ike security-associations fpc 6 pic 1 kmd-instance all
Index Remote Address State Initiator cookie Responder cookie Mode
1728053250 1.1.1.2 UP fc959afd1070d10b bdeb7e8c1ea99483 Main
```

## Sample Output

### show security ike security-associations detail (ADVPN Enabled on Suggester Only)

```
user@host> show security ike security-associations detail
IKE peer 17.0.1.7, Index 8375028, Gateway Name: hub_gw
Auto Discovery VPN:
  Type: Static, Local Capability: Suggester, Peer Capability: Not Supported
Suggester Shortcut Suggestions Statistics:
  Suggestions sent      : 0
  Suggestions accepted: 0
  Suggestions declined: 0
Role: Responder, State: UP
```

## Sample Output

### show security ike security-associations detail (ADVPN Enabled on Partner)

```
user@host> show security ike security-associations detail
IKE peer 23.0.0.250, Index 1345685, Gateway Name: spoke_gw
Auto Discovery VPN:
  Type: Static, Local Capability: Partner, Peer Capability: Suggester
Partner Shortcut Suggestions Statistics:
  Suggestions received: 0
  Suggestions accepted: 0
  Suggestions declined: 0
Role: Responder, State: UP
```

## Sample Output

### show security ike security-associations sa-type shortcut (ADVPN)

```
user@host> show security ike security-associations sa-type shortcut
Index State Initiator cookie Responder cookie Mode Remote Address
3075266 UP e0368d95b3289c77 5a8e2e025abdf6e IKEv2 23.0.0.106
```

## Sample Output

### show security ike security-associations sa-type shortcut detail (ADVPN)

```
user@host> show security ike security-associations sa-type shortcut detail
```

IKE peer 23.0.0.111, Index 1345683, Gateway Name: spoke\_gw  
Auto Discovery VPN:  
Type: Shortcut, Local Capability: Partner, Peer Capability: Partner  
Role: Initiator, State: UP

## show security ipsec security-associations

---

**Syntax**    **show security ipsec security-associations**  
              **brief | detail**  
              **family (inet | inet6)**  
              **fpc slot-number**  
              **index SA-index-number**  
              **kmd-instance (all | kmd-instance-name)**  
              **pic slot-number>**  
              **sa-type shortcut**  
              **vpn-name vpn-name <traffic-selector traffic-selector-name>**

**Release Information**    Command introduced in Junos OS Release 8.5. Support for the **fpc**, **pic**, and **kmd-instance** options added in Junos OS Release 9.3. Support for the **family** option added in Junos OS Release 11.1. Support for the **vpn-name** option added in Junos OS Release 11.4R3. Support for the **traffic-selector** option and traffic selector field added in Junos OS Release 12.1X46-D10. Support for Auto Discovery VPN added in Junos OS Release 12.3X48-D10.

**Description**    Display information about the IPsec security associations (SAs).

- Options**
- **none**—Display information about all SAs.
  - **brief | detail**—(Optional) Display the specified level of output.
  - **family**—(Optional) Display SAs by family. This option is used to filter the output.
    - **inet**—IPv4 address family.
    - **inet6**—IPv6 address family.
  - **fpc slot-number**—(Optional) Display information about existing IPsec SAs in this Flexible PIC Concentrator (FPC) slot. This option is used to filter the output.
  - **index SA-index-number**—(Optional) Display detailed information about the specified SA identified by this index number. To obtain a list of all SAs that includes their index numbers, use the command with no options.
  - **kmd-instance**—(Optional) Display information about existing IPsec SAs in the key management process (in this case, it is KMD) identified by the FPC *slot-number* and PIC *slot-number*. This option is used to filter the output.
    - **all**—All KMD instances running on the Services Processing Unit (SPU).
    - **kmd-instance-name**—Name of the KMD instance running on the SPU.
  - **pic slot-number**—(Optional) Display information about existing IPsec SAs in this PIC slot. This option is used to filter the output.
  - **sa-type**—(Optional for ADVPN) Type of SA. **shortcut** is the only option for this release.
  - **vpn-name vpn-name**—Name of the VPN. If configured, **traffic-selector traffic-selector-name** can optionally be specified.

**Required Privilege Level** view

**Related Documentation**

- [clear security ipsec security-associations](#)
- [Example: Configuring a Route-Based VPN Tunnel in a User Logical System](#)

**List of Sample Output**

[show security ipsec security-associations \(IPv4\) on page 240](#)  
[show security ipsec security-associations \(IPv6\) on page 240](#)  
[show security ipsec security-associations index 5 on page 240](#)  
[show security ipsec security-associations brief on page 241](#)  
[show security ipsec security-associations detail on page 241](#)  
[show security ipsec security-associations family inet6 on page 241](#)  
[show security ipsec security-associations fpc 6 pic 1 kmd-instance all \(SRX Series Devices\) on page 242](#)  
[show security ipsec security-associations detail \(ADVPN Suggester, Static Tunnel\) on page 242](#)  
[show security ipsec security-associations detail \(ADVPN Partner, Static Tunnel\) on page 242](#)  
[show security ipsec security-associations sa-type shortcut \(ADVPN\) on page 243](#)  
[show security ipsec security-associations sa-type shortcut detail \(ADVPN\) on page 243](#)

**Output Fields** [Table 11 on page 237](#) lists the output fields for the **show security ipsec security-associations** command. Output fields are listed in the approximate order in which they appear.

**Table 11: show security ipsec security-associations**

Field Name	Field Description
<b>Total active tunnels</b>	Total number of active IPsec tunnels.
<b>ID</b>	Index number of the SA. You can use this number to get additional information about the SA.
<b>VPN name</b>	IPsec name for VPN.
<b>Gateway</b>	IP address of the remote gateway.
<b>Port</b>	If Network Address Translation (NAT) is used, this value is 4500. Otherwise, it is the standard IKE port, 500.
<b>Algorithm</b>	<p>Cryptography used to secure exchanges between peers during the IKE Phase 2 negotiations includes:</p> <ul style="list-style-type: none"> <li>• An authentication algorithm used to authenticate exchanges between the peers. Options are <b>hmac-md5-95</b>, <b>hmac-sha1-96</b>, or <b>ESP</b>.</li> <li>• An encryption algorithm used to encrypt data traffic. Options are <b>3des-cbc</b>, <b>aes-128-cbc</b>, <b>aes-192-cbc</b>, <b>aes-256-cbc</b>, or <b>des-cbc</b>.</li> </ul>

Table 11: show security ipsec security-associations (*continued*)

Field Name	Field Description
<b>SPI</b>	Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI. Each entry includes the name of the VPN, the remote gateway address, the SPIs for each direction, the encryption and authentication algorithms, and keys. The peer gateways each have two SAs, one resulting from each of the two phases of negotiation: Phase 1 and Phase 2.
<b>Life: sec/kb</b>	The lifetime of the SA, after which it expires, expressed either in seconds or kilobytes.
<b>Sta</b>	State has two options, <b>Installed</b> and <b>Not Installed</b> . <ul style="list-style-type: none"> <li>• <b>Installed</b>—The SA is installed in the SA database.</li> <li>• <b>Not Installed</b>—The SA is not installed in the SA database.</li> </ul> For transport mode, the value of State is always <b>Installed</b> .
<b>Mon</b>	The Mon field refers to VPN monitoring status. If VPN monitoring is enabled, then this field displays <b>U</b> (up) or <b>D</b> (down). A hyphen (-) means VPN monitoring is not enabled for this SA.
<b>vsys or Virtual-system</b>	The root system.
<b>Tunnel index</b>	Numeric identifier of the specific IPsec tunnel for the SA.
<b>Local gateway</b>	Gateway address of the local system.
<b>Remote gateway</b>	Gateway address of the remote system.
<b>Traffic selector</b>	Name of the traffic selector.
<b>Local identity</b>	Identity of the local peer so that its partner destination gateway can communicate with it. The value is specified as an IP address, fully qualified domain name, e-mail address, or distinguished name (DN).
<b>Remote identity</b>	IP address of the destination peer gateway.
<b>DF-bit</b>	State of the don't fragment bit: <b>set</b> or <b>cleared</b> .
<b>Bind interface</b>	The tunnel interface to which VPN is bound.
<b>Policy-name</b>	Name of the applicable policy.
<b>Location</b>	<b>FPC</b> —Flexible PIC Concentrator (FPC) slot number.  <b>PIC</b> —PIC slot number.  <b>KMD-Instance</b> —The name of the KMD instance running on the SPU, identified by FPC <i>slot-number</i> and PIC <i>slot-number</i> . Currently, 4 KMD instances running on each SPU, and any particular IPsec negotiation is carried out by a single KMD instance.
<b>Tunnel events</b>	Tunnel events and occurrences.

Table 11: show security ipsec security-associations (*continued*)

Field Name	Field Description
<b>Direction</b>	Direction of the SA; it can be inbound or outbound.
<b>AUX-SPI</b>	Value of the auxiliary security parameter index(SPI). <ul style="list-style-type: none"> <li>When the value is <b>AH</b> or <b>ESP</b>, <b>AUX-SPI</b> is always 0.</li> <li>When the value is <b>AH+ESP</b>, <b>AUX-SPI</b> is always a positive integer.</li> </ul>
<b>Mode</b>	Mode of the SA: <ul style="list-style-type: none"> <li><b>transport</b>—Protects host-to-host connections.</li> <li><b>tunnel</b>—Protects connections between security gateways.</li> </ul>
<b>Type</b>	Type of the SA: <ul style="list-style-type: none"> <li><b>manual</b>—Security parameters require no negotiation. They are static and are configured by the user.</li> <li><b>dynamic</b>—Security parameters are negotiated by the IKE protocol. Dynamic SAs are not supported in transport mode.</li> </ul>
<b>State</b>	State of the SA: <ul style="list-style-type: none"> <li><b>Installed</b>—The SA is installed in the SA database.</li> <li><b>Not Installed</b>—The SA is not installed in the SA database.</li> </ul> For transport mode, the value of State is always <b>Installed</b> .
<b>Protocol</b>	Protocol supported. <ul style="list-style-type: none"> <li>Transport mode supports Encapsulation Security Protocol (ESP) and Authentication Header (AH).</li> <li>Tunnel mode supports ESP and AH. <ul style="list-style-type: none"> <li><b>Authentication</b>—Type of authentication used.</li> <li><b>Encryption</b>—Type of encryption used.</li> </ul> </li> </ul>
<b>Soft lifetime</b>	The soft lifetime informs the IPsec key management system that the SA is about to expire. <p>Each lifetime of an SA has two display options, hard and soft, one of which must be present for a dynamic SA. This allows the key management system to negotiate a new SA before the hard lifetime expires.</p> <ul style="list-style-type: none"> <li><b>Expires in seconds</b>—Number of seconds left until the SA expires.</li> </ul>
<b>Hard lifetime</b>	The hard lifetime specifies the lifetime of the SA. <ul style="list-style-type: none"> <li><b>Expires in seconds</b>—Number of seconds left until the SA expires.</li> </ul>
<b>Lifesize Remaining</b>	The lifesize remaining specifies the usage limits in kilobytes. If there is no lifesize specified, it shows unlimited. <ul style="list-style-type: none"> <li><b>Expires in kilobytes</b>—Number of kilobytes left until the SA expires.</li> </ul>

Table 11: show security ipsec security-associations (*continued*)

Field Name	Field Description
Anti-replay service	State of the service that prevents packets from being replayed. It can be <b>Enabled</b> or <b>Disabled</b> .
Replay window size	Configured size of the antireplay service window. It can be 32 or 64 packets. If the replay window size is 0, the antireplay service is disabled.  The antireplay window size protects the receiver against replay attacks by rejecting old or duplicate packets.
Bind-interface	The tunnel interface to which the route-based VPN is bound.

## Sample Output

### show security ipsec security-associations (IPv4)

```

user@host> show security ipsec security-associations
Total active tunnels: 1
ID      Gateway      Port  Algorithm      SPI      Life:sec/kb  Mon vsys
 131075  11.0.28.241    500   ESP:3des/sha1  86758ff0  6918/ unlim  -   0
 131075  11.0.28.241    500   ESP:3des/sha1  3183ff26  6918/ unlim  -   0

```

## Sample Output

### show security ipsec security-associations (IPv6)

```

user@host> show security ipsec security-associations
Total active tunnels: 1
ID      Algorithm      SPI      Life:sec/kb  Mon vsys Port  Gateway
 131074  ESP:3des/sha1  14caf1d9  3597/ unlim  -   root  500   1212::1112
 131074  ESP:3des/sha1  9a4db486  3597/ unlim  -   root  500   1212::1112

```

## Sample Output

### show security ipsec security-associations index 5

```

user@host> show security ipsec security-associations index 5
ID: 131073 Virtual-system: root, VPN Name: tropic
Local gateway: 1.1.1.1, Remote gateway: 1.1.1.2
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0...7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear
Bind-interface: st0.3
Policy-name: my-policy

Direction: inbound, SPI: 494001027, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expired
Hard lifetime: Expired in 130 seconds
Lifesize Remaining: Unlimited

```



```

Anti-replay service: Enabled, Replay window size: 64

Direction: inbound, SPI: 1498711950, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 40 seconds
Hard lifetime: Expires in 175 seconds
Lifesize Remaining: Unlimited
Anti-replay service: Enabled, Replay window size: 64

Direction: outbound, SPI: 4038397695, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 40 seconds
Hard lifetime: Expires in 175 seconds
Lifesize Remaining: Unlimited
Anti-replay service: Enabled, Replay window size: 64

```

## Sample Output

### show security ipsec security-associations brief

```

user@host> show security ipsec security-associations brief
Total active tunnels: 2
ID Gateway Port Algorithm SPI Life:sec/kb Mon vsys
<16384 1.1.1.1 500 ESP:3des/sha1 af88baa 28795/unlim D 0
>16384 1.1.1.1 500 ESP:3des/sha1 f4e3e5f4 28795/unlim D 0

```

## Sample Output

### show security ipsec security-associations detail

```

user@host> show security ipsec security-associations detail
ID: 131073 Virtual-system: root, VPN Name: tropic
Local Gateway: 1.1.1.2, Remote Gateway: 1.1.1.1
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear
Bind-interface: st0.3
Direction: inbound, SPI: 184060842, AUX-SPI: 0
Hard lifetime: Expires in 28785 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expired
Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: DOWN
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Anti-replay service: enabled, Replay window size: 32

Direction: outbound, SPI: 4108576244, AUX-SPI: 0
Hard lifetime: Expires in 28785 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expired
Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: DOWN
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Anti-replay service: enabled, Replay window size: 32

```

## Sample Output

### show security ipsec security-associations family inet6

```

user@host> show security ipsec security-associations family inet6

```

```

Virtual-system: root
Local Gateway: 1212::1111, Remote Gateway: 1212::1112
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
DF-bit: clear
Direction: inbound, SPI: 14caf1d9, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 3440 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2813 seconds
Mode: tunnel, Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Anti-replay service: counter-based enabled, Replay window size: 64

Direction: outbound, SPI: 9a4db486, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 3440 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2813 seconds
Mode: tunnel, Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Anti-replay service: counter-based enabled, Replay window size: 64

```

## Sample Output

### show security ipsec security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices)

```

user@host> show security ipsec security-associations fpc 6 pic 1 kmd-instance all
Total active tunnels: 1

ID      Gateway      Port  Algorithm      SPI      Life:sec/kb  Mon vsys
<2      1.1.1.2      500   ESP:3des/sha1  67a7d25d  28280/unlim  -   0
>2      1.1.1.2      500   ESP:3des/sha1  a23cbcdc  28280/unlim  -   0

```

## Sample Output

### show security ipsec security-associations detail (ADVPN Suggester, Static Tunnel)

```

user@host> show security ipsec security-associations detail
ID: 268173314 Virtual-system: root, VPN Name: zth_hub_vpn
Local Gateway: 23.0.0.250, Remote Gateway: 23.0.0.111
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear, Bind-interface: st0.0
Port: 500, Nego#: 22, Fail#: 0, Def-Del#: 0 Flag: 0x608a29

```

## Sample Output

### show security ipsec security-associations detail (ADVPN Partner, Static Tunnel)

```

user@host> show security ipsec security-associations detail
ID: 268173314 Virtual-system: root, VPN Name: zth_spoke_vpn
Local Gateway: 17.0.1.7, Remote Gateway: 23.0.0.250
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear, Bind-interface: st0.0
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x8608a29

```

## Sample Output

### show security ipsec security-associations sa-type shortcut (ADVPN)

```
user@host> show security ipsec security-associations sa-type shortcut
Total active tunnels: 1
ID      Algorithm      SPI      Life:sec/kb  Mon  lsys Port  Gateway
<268173318 ESP:aes-cbc-256/sha1 6f164ee0 3580/ unlim - root 500 23.0.0.111
>268173318 ESP:aes-cbc-256/sha1 e6f29cb0 3580/ unlim - root 500 23.0.0.111
```

### show security ipsec security-associations sa-type shortcut detail (ADVPN)

```
user@host> show security ipsec security-associations sa-type shortcut detail
ID: 67108874 Virtual-system: root, VPN Name: spoke_vpn
Local Gateway: 17.0.1.7, Remote Gateway: 23.0.0.111
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Auto Discovery VPN:
  Type: Shortcut, Shortcut Role: Initiator
Version: IKEv2
```

## IKEv2 AES-GCM for Branch SRX Series and SRX5600 and SRX5800 Devices With Next-Generation Services Processing Card

- [encryption-algorithm \(Security IKE\) on page 244](#)
- [proposal-set \(Security IKE\) on page 246](#)
- [proposal-set \(Security IPsec\) on page 249](#)
- [Understanding Suite B and PRIME Cryptographic Suites on page 250](#)

## encryption-algorithm (Security IKE)

<b>Syntax</b>	encryption-algorithm (3des-cbc   aes-128-cbc   aes-128-gcm   aes-192-cbc   aes-256-cbc   aes-256-gcm   des-cbc);
<b>Hierarchy Level</b>	[edit security group-vpn member ike proposal <i>proposal-name</i> ] [edit security group-vpn server ike proposal <i>proposal-name</i> ] [edit security ike proposal <i>proposal-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. Support for <b>group-vpn</b> hierarchies added in Junos OS Release 10.2. Support for <b>aes-128-gcm</b> and <b>aes-256-gcm</b> options added in Junos OS Release 12.3X48-D20.
<b>Description</b>	Configure an encryption algorithm for an IKE proposal.



**NOTE:** The device does not delete existing IPsec SAs when you update the **encryption-algorithm** configuration in the IKE proposal.

<b>Options</b>	<p><b>3des-cbc</b>—Has a block size of 24 bytes; the key size is 192 bits long.</p> <p><b>aes-128-cbc</b>—Advanced Encryption Standard (AES) 128-bit encryption algorithm.</p> <p><b>aes-128-gcm</b>—AES 128-bit authenticated encryption algorithm supported with IKEv2 only. When this option is used, <b>aes-128-gcm</b> must be configured at the [edit security ipsec proposal <i>proposal-name</i>] hierarchy level, and the <b>authentication-algorithm</b> option must not be configured at the [edit security ike proposal <i>proposal-name</i>] hierarchy level. This option is not supported on Group VPN.</p> <p><b>aes-192-cbc</b>—AES 192-bit encryption algorithm.</p> <p><b>aes-256-cbc</b>—AES 256-bit encryption algorithm.</p> <p><b>aes-256-gcm</b>—AES 256-bit authenticated encryption algorithm supported with IKEv2 only. When this option is used, <b>aes-256-gcm</b> must be configured at the [edit security ipsec proposal <i>proposal-name</i>] hierarchy level, and the <b>authentication-algorithm</b> option must not be configured at the [edit security ike proposal <i>proposal-name</i>] hierarchy level. This option is not supported on Group VPN.</p> <p><b>des-cbc</b>—Has a block size of 8 bytes; the key size is 48 bits long.</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Dynamic VPN Overview</i></li> <li>• <i>Group VPN Overview</i></li> <li>• <i>IPsec VPN Overview</i></li> </ul>

- *Monitoring VPNs*

## proposal-set (Security IKE)

---

<b>Syntax</b>	<code>proposal-set (basic   compatible   prime-128   prime-256   standard   suiteb-gcm-128   suiteb-gcm-256);</code>
<b>Hierarchy Level</b>	<code>[edit security ike policy <i>policy-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. Support for <b>suiteb-gcm-128</b> and <b>suiteb-gcm-256</b> options added in Junos OS Release 12.1X45-D10. Support for <b>prime-128</b> and <b>prime-256</b> options added in Junos OS Release 12.3X48-D20.
<b>Description</b>	Specify a set of default Internet Key Exchange (IKE) proposals.



**NOTE:** The **prime-128** and **prime-256** proposal sets require IKE v2 and typically use certificate-based authentication.

---

- Options**
- basic**—Includes a basic set of two IKE proposals:
- Proposal 1—Preshared key, Data Encryption Standard (DES) encryption, and Diffie-Hellman (DH) group 1 and Secure Hash Algorithm 1 (SHA-1) authentication.
  - Proposal 2—Preshared key, DES encryption, and DH group 1 and Message Digest 5 (MD5) authentication.
- compatible**—Includes a set of four commonly used IKE proposals:
- Proposal 1—Preshared key, triple DES (3DES) encryption, and Gnutella2 and SHA-1 authentication.
  - Proposal 2—Preshared key, 3DES encryption, and DH group 2 and MD5 authentication.
  - Proposal 3—Preshared key, DES encryption, and DH group 2 and SHA-1 authentication.
  - Proposal 4—Preshared key, DES encryption, and DH group 2 and MD5 authentication.
- prime-128**—Provides the following proposal set (this option is not supported on Group VPNs):
- Authentication method—Elliptic Curve Digital Signature Algorithm (ECDSA) 256-bit signatures.
  - Diffie-Hellman Group—19.
  - Encryption algorithm—Advanced Encryption Standard (AES) 128-bit Galois/Counter Mode (GCM).
  - Authentication algorithm—None (AES-GCM provides both encryption and authentication).

When this option is used, **prime-128** should also be configured at the **[edit security ipsec policy *policy-name* proposal-set]** hierarchy level.

**prime-256**—Provides the following proposal set (this option is not supported on Group VPNs):

- Authentication method—ECDSA 384-bit signatures.
- Diffie-Hellman Group—20.
- Encryption algorithm—AES 256-bit GCM.
- Authentication algorithm—None (AES-GCM provides both encryption and authentication).

When this option is used, **prime-256** should also be configured at the **[edit security ipsec policy *policy-name* proposal-set]** hierarchy level.

**standard**—Includes a standard set of two IKE proposals:

- Proposal 1—Preshared key, 3DES encryption, and DH group 2 and SHA-1 authentication.
- Proposal 2—Preshared key, AES 128-bit encryption, and DH group 2 and SHA-1 authentication.

**suiteb-gcm-128**—Provides the following Suite B proposal set (this option is not supported on Group VPNs):

- Authentication method—ECDSA 256-bit signatures.
- Diffie-Hellman Group—19.
- Encryption algorithm—AES 128-bit cipher block chaining (CBC)



**NOTE:** CBC mode is used instead of GCM.

- Authentication algorithm—SHA-256.

**suiteb-gcm-256**—Provides the following Suite B proposal set (this option is not supported on Group VPNs):

- Authentication method—ECDSA 384-bit signatures.
- Diffie-Hellman Group—20.
- Encryption algorithm—AES 256-bit CBC.



**NOTE:** CBC mode is used instead of GCM.

- Authentication algorithm—SHA-384.

<b>Required Privilege</b>	security—To view this statement in the configuration.
<b>Level</b>	security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Dynamic VPN Overview</i></li><li>• <i>IPsec VPN Overview</i></li></ul>



## proposal-set (Security IPsec)

<b>Syntax</b>	<code>proposal-set (basic   compatible   prime-128   prime-256   standard   suiteb-gcm-128   suiteb-gcm-256);</code>
<b>Hierarchy Level</b>	<code>[edit security ipsec policy <i>policy-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4. Support for <b>suiteb-gcm-128</b> and <b>suiteb-gcm-256</b> options added in Junos OS Release 12.1X45-D10. Support for <b>prime-128</b> and <b>prime-256</b> options added in Junos OS Release 12.3X48-D20.
<b>Description</b>	Define a set of default IPsec proposals.

**Options** **basic**—nopfs-esp-des-sha and nopfs-esp-des-md5.

**compatible**—nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, and nopfs-esp-des-md5.

**prime-128**—Provides the following proposal set:

- Encapsulating Security Payload (ESP) protocol.
- Encryption algorithm—Advanced Encryption Standard Galois/Counter mode (AES-GCM)128-bit.
- Authentication algorithm—None (AES-GCM provides both encryption and authentication).



**NOTE:** This option is not supported on Group VPNs.

**prime-256**—Provides the following proposal set:

- ESP protocol.
- Encryption algorithm—AES-GCM 256-bit.
- Authentication algorithm—None (AES-GCM provides both encryption and authentication).



**NOTE:** This option is not supported on Group VPNs.

**standard**—g2-esp-3des-sha and g2-esp-aes128-sha.

**suiteb-gcm-128**—Provides the following Suite B proposal set:

- ESP protocol.
- Encryption algorithm— AES-GCM 128-bit.

- Authentication algorithm—None (AES-GCM provides both encryption and authentication).



**NOTE:** This option is not supported on Group VPNs.

**suiteb-gcm-256**—Provides the following Suite B proposal set:

- ESP protocol.
- Encryption algorithm—AES-GCM 256-bit.
- Authentication algorithm—None (AES-GCM provides both encryption and authentication).



**NOTE:** This option is not supported on Group VPNs.



**NOTE:** Perfect Forward Secrecy setting in IPsec policy will override the settings in proposal-sets in Junos OS Release 10.4 and later.

**Required Privilege Level**

security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- *Dynamic VPN Overview*
- *Group VPN Overview*
- *IPsec VPN Overview*

### ***Understanding Suite B and PRIME Cryptographic Suites***

Suite B is a set of cryptographic algorithms designated by the U.S. National Security Agency to allow commercial products to protect traffic that is classified at secret or top secret levels. Suite B protocols are defined in RFC 6379, *Suite B Cryptographic Suites for IPsec*. The Suite B cryptographic suites provide Encapsulating Security Payload (ESP) integrity and confidentiality and should be used when ESP integrity protection and encryption are both required. Protocol Requirements for IP Modular Encryption (PRIME), an IPsec profile defined for public sector networks in the United Kingdom, is based on the Suite B cryptographic suite, but uses AES-GCM rather than AES-CBC for IKEv2 negotiations.

The following cryptographic suites are supported:

- Suite-B-GCM-128

- ESP: Advanced Encryption Standard (AES) encryption with 128-bit keys and 16-octet integrity check value (ICV) in Galois Counter Mode (GCM).
- IKE: AES encryption with 128-bit keys in cipher block chaining (CBC) mode, integrity using SHA-256 authentication, key establishment using Diffie-Hellman (DH) group 19, and authentication using Elliptic Curve Digital Signature Algorithm (ECDSA) 256-bit elliptic curve signatures.
- Suite-B-GCM-256
  - ESP: AES encryption with 256-bit keys and 16-octet ICV in GCM for ESP.
  - IKE: AES encryption with 256-bit keys in CBC mode, integrity using SHA-384 authentication, key establishment using DH group 20, and authentication using ECDSA 384-bit elliptic curve signatures.
- PRIME-128
  - ESP: AES encryption with 128-bit keys and 16-octet ICV in GCM.
  - IKE: AES encryption with 128-bit keys in GCM, key establishment using DH group 19, and authentication using ECDSA 256-bit elliptic curve signatures.
- PRIME-256
  - ESP: AES encryption with 256-bit keys and 16-octet ICV in GCM for ESP.
  - IKE: AES encryption with 256-bit keys in GCM, key establishment using DH group 20, and authentication using ECDSA 384-bit elliptic curve signatures.

Suite-B cryptographic suites support IKEv1 and IKEv2. PRIME cryptographic suites only support IKEv2.



**NOTE:** Suite B and PRIME are not fully supported on SRX1400, SRX3400, and SRX3600 devices, and on SRX5600 and SRX5800 devices that do not have the next-generation SPC installed. You can configure IKE with Suite B options on these devices, but AES-GCM options are not supported. If you configure IKE with Suite B options on these devices, VPN establishment is slower because the devices do not have the hardware processors that can accelerate Suite B algorithm processing.



**NOTE:** Suite B and PRIME are not supported with the Group VPN feature.

CLI options support Suite B and PRIME compliance in IKE and IPsec proposal configuration.

- For IKE proposals configured at the `[edit security ike proposal proposal-name]` hierarchy level:
  - **authentication-algorithm** options include **sha-256** and **sha-384**.
  - **authentication-method** options include **ecdsa-signatures-256** and **ecdsa-signatures-384**.

- **dh-group** options include **group19** and **group20**.
- **encryption-algorithm** options for PRIME include **aes-128-gcm** and **aes-256-gcm**.
- For IPsec proposals configured at the [**edit security ipsec proposal *proposal-name***] hierarchy level, **encryption-algorithm** options include **aes-128-gcm**, **aes-192-gcm**, and **aes-256-gcm**.
- For IPsec policies configured at the [**edit security ipsec policy *policy-name***] hierarchy level, the **perfect-forward-secrecy keys** options include **group19** and **group20**.
- For convenience, predefined proposals that provide compliance with Suite B (**suiteb-gcm-128** and **suiteb-gcm-256**) and PRIME (**prime-128** and **prime-256**) are available at the [**edit security ike policy *policy-name***] and [**edit security ipsec policy *policy-name***] hierarchy levels.



**NOTE:** VPN monitoring and cryptographic configuration options **ecdsa-signatures-384** (for IKE authentication) and DH group 20 consume considerable CPU resources. If VPN monitoring and the **ecdsa-signatures-384** and **group20** options are used on an SRX Series device with a large number of tunnels configured, the SRX Series device must have the next-generation SPC installed.

**Related  
Documentation**

- [IPsec VPN Overview](#)
- [\[edit security ike\] Hierarchy Level](#)
- [\[edit security ipsec\] Hierarchy Level](#)

---

## New Features in Junos OS Release 12.3X48-D15

Junos OS Release 12.3X48-D15 introduces the following features:

- [Application Layer Gateways \(ALGs\) on page 252](#)
- [Building Blocks on page 259](#)
- [Intrusion Detection and Prevention on page 262](#)

---

### Application Layer Gateways (ALGs)

- [Scaling BLF Support for the UDP-Based SIP ALG on page 252](#)
- [464XLAT ALG Traffic Support on page 253](#)

#### Scaling BLF Support for the UDP-Based SIP ALG

- [Understanding Scaling Busy Lamp Field Support for the UDP-Based SIP ALG on page 252](#)

##### ***Understanding Scaling Busy Lamp Field Support for the UDP-Based SIP ALG***

Busy lamp field (BLF) is a light on an IP phone that indicates whether another extension connected to the same private branch exchange (PBX) is busy or not. You can manually

configure the BLF by using a Web interface. When BLF is configured, the phone subscribes to a resource list available on the IP PBX to be notified of status information for other extensions. BLF works through the Session Initiation Protocol (SIP) and uses the SUBSCRIBE and NOTIFY messages. Usually, the phone is the subscriber and the IP PBX is the notifier.

When a phone is registered to the IP PBX, the IP PBX notifies the phone of the state of the resource list. For example, if the resource list is huge, the body of the NOTIFY message will also be huge. Because the SIP ALG supports only 3000-byte SIP messages, it bypasses the huge NOTIFY message. If there are too many instances of BLF in the message body, the payload will not be changed and the gate will not be opened.

Starting with Junos OS Release 12.3X48-D15, the SIP ALG supports 65,000-byte SIP messages on the UDP protocol. In the scaling BLF application, if every instance is around 500 bytes, the SIP ALG supports 100 instances in one SIP UDP message.

BLF support for the UDP-based SIP ALG includes the following features:

- The device can send and receive 65,000-byte SIP messages.
- The SIP ALG can parse the 65,000-byte SIP messages and open the pinhole, if required.
- The SIP ALG regenerates the new jumbo SIP message if NAT is configured and the payload is changed.

#### Related Documentation

- *Understanding SIP ALG*

## 464XLAT ALG Traffic Support

- [Understanding 464XLAT ALG Traffic Support on page 253](#)
- [Understanding 464XLAT ALG Functionality on page 254](#)

### **Understanding 464XLAT ALG Traffic Support**

When you deploy IPv6 applications on mobile networks, be aware that some mobile operators cannot provide IPv6 support for their users, because some phone applications do not support an IPv6-only environment.

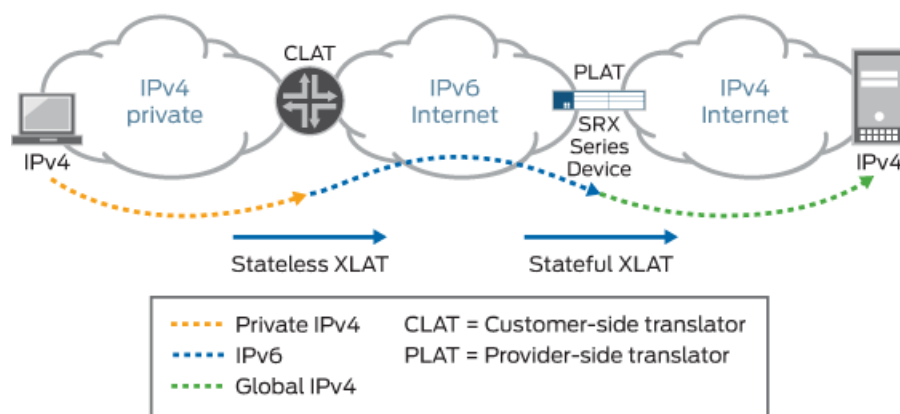
The solution is to use the NAT64 mechanism to access the IPv4-only content in the operator's network and to use 464XLAT traffic to enable IPv4-only applications to work on IPv6-only networks.

The 464XLAT architecture is a combination of stateless translation on the customer-side translator (CLAT) and stateful translation on the provider-side translator (PLAT). The 464XLAT architecture is used to translate the packet information of a device using the combination of stateless (translates private IPv4 address to global IPv6 addresses, and vice versa) and stateful (translates IPv6 addresses to global IPv4 addresses, and vice versa) translation.

[Figure 12 on page 254](#) illustrates the 464XLAT architecture, which provides IPv4 connectivity across an IPv6-only network by combining existing and well-known stateful protocol translation on PLAT in the core and stateless protocol on CLAT at the edge. The private

IPv4 host can reach global IPv4 hosts through both CLAT and PLAT translation. Conversely, the IPv6 host can directly reach other IPv6 hosts on the Internet without translation. This means that the customer premises equipment (CPE) can support CLAT and also operate as an IPv6 native router for native IPv6 traffic.

Figure 12: 464XLAT Architecture



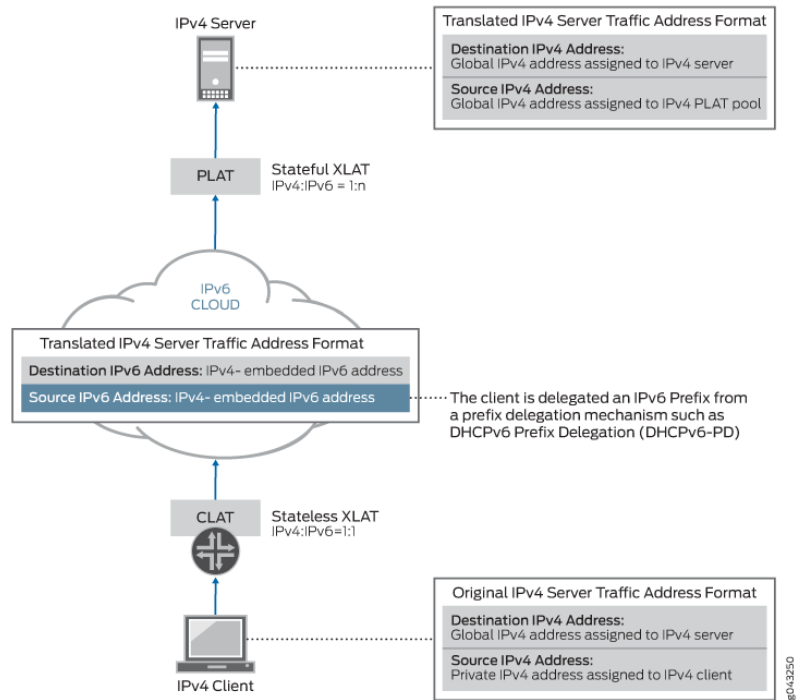
**Related Documentation**

- [Understanding 464XLAT ALG Functionality on page 254](#)

#### ***Understanding 464XLAT ALG Functionality***

Figure 13 on page 255 describes the address translation architecture and shows how packet information for a device is translated using a combination of stateful translation at the provider-side translator (PLAT) and stateless translation at the customer-side translator (CLAT). In this diagram, the client is delegated an IPv6 prefix from a prefix delegation mechanism such as DHCPv6 Prefix Delegation (DHCPv6-PD). Therefore, the client has a dedicated IPv6 prefix for translation.

Figure 13: 464XLAT ALG Functionality



The PPTP, RTSP, and FTP ALGs also support XLAT functionality.

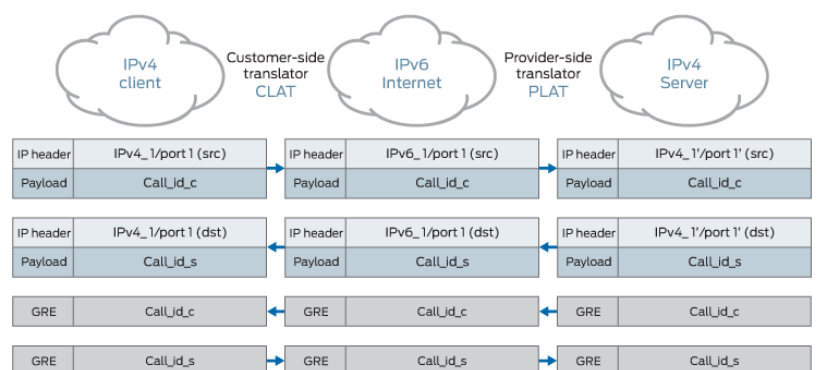
This following sections explain how the PPTP, RTSP, and FTP ALGs work when the device acts as PLAT:

- [How the PPTP ALG Supports the Device Acting As PLAT on page 256](#)
- [How the RTSP ALG Supports the Device Acting As PLAT on page 257](#)
- [How the FTP ALG Supports the Device Acting As PLAT on page 258](#)

#### **How the PPTP ALG Supports the Device Acting As PLAT**

[Figure 14 on page 256](#) describes the PPTP ALG XLAT functionality.

**Figure 14: PPTP ALG XLAT Functionality**



The PPTP ALG uses the call\_ID for destination port functionality.

1. **The client sends the outgoing call request (with PPTP Access Concentrator (PAC) call\_ID) to the server:**

CLAT: The source address/port is translated from Ipv4\_1/port1 to Ipv6\_1/port1. However, the payload call\_ID is not changed.

PLAT: The source address/port Ipv6\_1/port1 is translated to Ipv4\_1'/port1' and matches the NAT64 rule. However, the call\_ID in the payload is not changed. The PPTP ALG creates a gate such as server\_ip/0->Ipv4\_1'/call\_ID(Ipv6\_1/call\_ID).

**The first generic routing encapsulation (GRE) packet reaches the gate from the server side:** When the first GRE traffic reaches the gate, the GRE packet from the server side with destination Ipv4\_1'/call\_ID is translated to Ipv6\_1/call\_ID. Finally, the GRE packet reaches the client Ipv4\_1/call\_ID after CLAT.

#### **Another special case for call\_ID 0:**

CLAT: The source address/port is translated from Ipv4\_1/port1 to Ipv6\_1/port1. However, the payload call\_ID is not changed.

PLAT: The source address/port Ipv6\_1/port1 is translated to Ipv4\_1'/port1' and matches the NAT64 rule. However, the call\_ID 0 in the payload is manually translated to 65002. The PPTP ALG creates a gate such as server\_ip/0->Ipv4\_1'/65002(Ipv6\_1/0).

**The first GRE packet reaches the gate from the server side:** When the first GRE traffic reaches the gate, the GRE packet from the server side with destination Ipv4\_1'/65002



is translated to `Ipv6_1/0`. Finally, the GRE packet reaches the client `Ipv4_1/0` after CLAT.

2. **The server sends the outgoing call reply (with PPTP Network Server (PNS) and PAC call\_ID) to the client:**

PLAT: The source address/port `Ipv4_2/port2` is translated to `Ipv6_2/port2'` and matches the NAT64 rule. However, the `call_ID` in the payload is not changed, and the PPTP ALG creates a gate such as `client_v6/0->Ipv6_2/call_ID(Ipv4_2/call_ID)`.

CLAT: The source address/port is translated from `Ipv6_2/port2` to `Ipv4_2/port2`. However, the payload `call_ID` is not changed.

**The first GRE packet reaches the gate from the client side:** When the first GRE traffic reaches the gate, the GRE packet from the client side with destination `Ipv4_2'/call_ID` is translated to `Ipv6_2/call_ID` after CLAT and then it is translated to `Ipv4_2/call_ID`. Finally, the GRE packet reaches the server `Ipv4_2/call_ID` after PLAT.

**Another special case for call\_ID 0:**

PLAT: The source address/port `Ipv4_2/port2` is translated to `Ipv6_2/port2'` and matches the NAT64 rule. However, the `call_ID` in the payload is translated to 65002 and the PPTP ALG creates a gate such as `client_v6/0->Ipv6_2/65002(Ipv4_2/0)`.

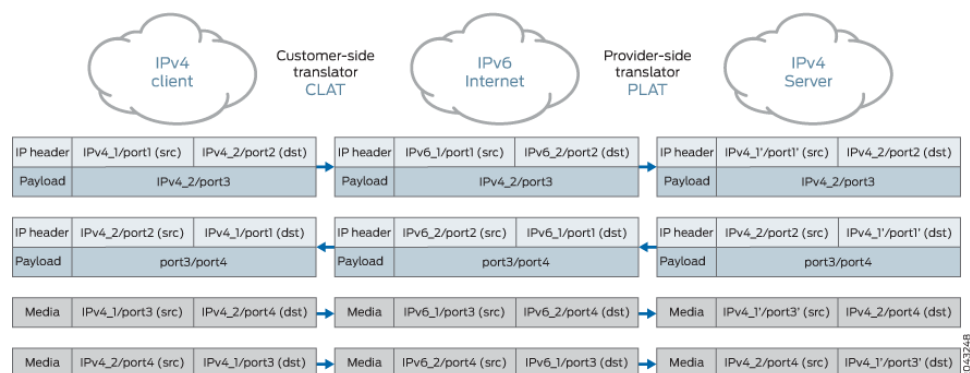
CLAT: The source address/port is translated from `Ipv6_2/port2` to `Ipv4_2/port2`. However, the payload `call_ID` is not changed.

**The first GRE packet reaches the gate from the client side:** When the first GRE traffic reaches the gate, the GRE packet from the client side with destination `Ipv4_2'/65002` is translated to `Ipv6_2/65002` after CLAT and then it is translated to `Ipv4_2/0`. Finally, the GRE packet reaches the server `Ipv4_2/0` after PLAT.

**How the RTSP ALG Supports the Device Acting As PLAT**

Figure 15 on page 257 describes the RTSP ALG XLAT functionality.

Figure 15: RTSP ALG XLAT Functionality



1. **The Windows Media Player on the Windows PC sends a SETUP message:**

CLAT: The source address/port is translated from Ipv4\_1/port1 to Ipv6\_1/port1. However, the payload Ipv4\_2/port3 is not changed.

PLAT: The source address/port Ipv6\_1/port1 is translated to Ipv4\_1'/port1' and matches the NAT64 rule, and the payload port3 is translated to port3'. However, the IP address in the payload ULR remains unchanged.

2. **The Windows Media Server on the Windows server sends a 200 OK message:**

PLAT: The source address/port Ipv4\_1'/port1' is translated to Ipv6\_1/port1 and matches the NAT64 rule. However, the port4 in the payload is not changed. The port3' is translated to port3. The RTSP ALG create gates such as c->s Ipv6\_1/port1->Ipv6\_2/port3 and s->c Ipv4\_2/port4->Ipv4\_1'/port3' over UDP media data sent from the server side with destination Ipv4\_1'/port1', then the IP header is translated to Ipv6\_1/port1 and reaches the gate.

CLAT: The source address/port is translated from Ipv6\_1/port1 to Ipv4\_1/port1. However, the payload port3/port4 is not changed.

3. **The server sends the Real-Time Transport Protocol (RTP) over UDP media data:**

PLAT: When the RTP over UDP media data is sent from the server side with destination Ipv4\_1'/port3, the IP header is translated to Ipv6\_1/port3 and reaches the gate.

CLAT: The IP header is translated from Ipv6\_1/port3 to Ipv4\_1/port3.

4. **The client sends the RTP over UDP media data:**

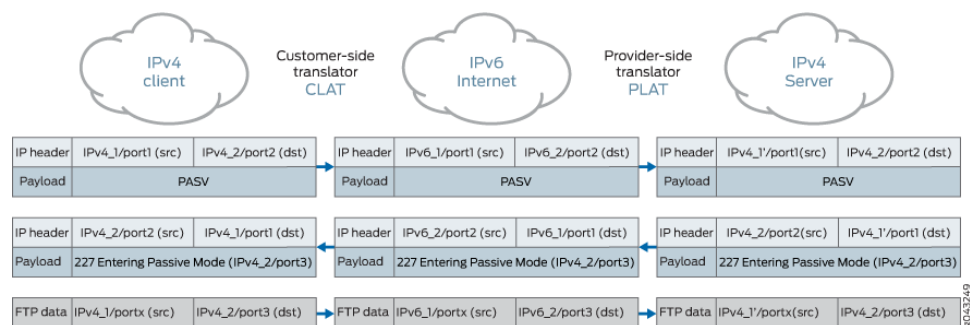
CLAT: The source address/port is translated from Ipv4\_1/port3 to Ipv6\_1/port3 and the destination address is translated from Ipv4\_2/port4 to Ipv6\_2/port4.

PLAT: The source address/port is translated from Ipv6\_1/port3 to Ipv4\_1'/port3 and the destination address is translated from Ipv6\_2/port4 to Ipv4\_2/port4.

**How the FTP ALG Supports the Device Acting As PLAT**

Figure 16 on page 258 and Figure 17 on page 259 describe the FTP ALG XLAT functionality in passive mode and port mode.

**Figure 16: FTP Passive mode:**



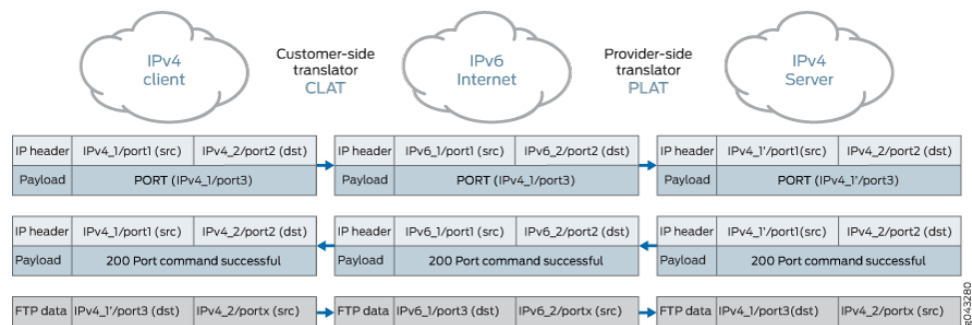
1. **A 227 message enters passive mode:**

CLAT: The source address/port is translated from Ipv4\_1/port1 to Ipv6\_1/port1. However, the payload does not contain IP or port information.

PLAT: The source address/port Ipv4\_1'/port1' is translated to Ipv6\_1/port1 and matches the NAT64 rule. However, the Ipv4\_2/port3 in the payload is not changed, and the FTP ALG creates a gate such as Ipv4\_1/0(Ipv6\_1/0)->Ipv4\_2/port3.

2. **The first packet reaches the gate from the client side:** When the traffic reaches the gate, the data packet from the client side with destination Ipv4\_2/port3 is translated to Ipv6\_2/port2. The IP header is translated to Ipv4\_2/port3 by NAT64 rule based on PLAT.

Figure 17: FTP Port Mode



1. **FTP port mode sends a PORT message:**

CLAT: The source address/port is translated from Ipv4/port1 to Ipv6/port1.

PLAT: The source address/port is Ipv6\_1/port1 is translated to Ipv4\_1'/port1' and matches the NAT64 rule. The Ipv4\_1/port2 in the payload is translated to Ipv4\_1'/port2' and the FTP ALG creates a gate such as Ipv4\_1'/port2'(Ipv4\_1/port2->server\_ip/server\_port).

2. **The first packet reaches the gate from the server side:** When the traffic reaches the gate, the first packet from the server side with destination Ipv4\_1'/port2' is translated to Ipv6\_1/port2. Finally, the packet reaches the client Ipv4\_1/port2 before CLAT.

#### Related Documentation

- [Understanding 464XLAT ALG Traffic Support on page 253](#)

## Building Blocks

This topic includes the following sections:

- [Security Policies on page 259](#)

## Security Policies

- [Best Practices for Defining Policies on High-End SRX Series Devices on page 260](#)

**Best Practices for Defining Policies on High-End SRX Series Devices**

A secure network is vital to a business. To secure a network, a network administrator must create a security policy that outlines all of the network resources within that business and the required security level for those resources. The security policy applies the security rules to the transit traffic within a context (from-zone to to-zone) and each policy is uniquely identified by its name. The traffic is classified by matching the source and destination zones, the source and destination addresses, and the application that the traffic carries in its protocol headers with the policy database in the data plane.

Table 12 on page 260 provides the policy limitations for high-end SRX Series devices.

**Table 12: Policy Limitations for High-End SRX Series Devices**

Policy Limitations	SRX1400	SRX3400 SRX3600	SRX5400 SRX5600 SRX5800
Address objects	1024	4096	4096
Application objects	3072	3072	3072
Security policies	40,000	40,000	80,000
Policy contexts (zone pairs)	4096	4096	8192
Policies per context	10240	40,000	80,000
Policies with counting enabled	1024	1024	1024



**NOTE:** The number of source and destination address objects allowed per firewall policy is 4096. The systemwide maximum allowed is 150,000 address objects.

Therefore, as you increase the number of addresses and applications in each rule, the amount of memory that is used by the policy definition increases, and sometimes the system runs out of memory with fewer than 80,000 policies.

To get the actual memory utilization of a policy on the Packet Forwarding Engine (PFE) and the Routing Engine (RE), you need to take various components of the memory tree into consideration. The memory tree includes the following two components:

- Policy context—Used to organize all policies in this context. Policy context includes variables such as source and destination zones.
- Policy entity—Used to hold the policy data. Policy entity calculates memory using parameters such as policy name, IP addresses, address count, applications, firewall authentication, WebAuth, IPsec, count, application services, and Junos Services Framework (JSF).

Additionally, the data structures used to store policies, rule sets, and other components use different memory on the Packet Forwarding Engine and on the Routing Engine. For example, address names for each address in the policy are stored on the Routing Engine, but no memory is allocated at the Packet Forwarding Engine level. Similarly, port ranges are expanded to prefix and mask pairs and are stored on the Packet Forwarding Engine, but no such memory is allocated on the Routing Engine.

Accordingly, depending on the policy configuration, the policy contributors to the Routing Engine are different from those to the Packet Forwarding Engine, and memory is allocated dynamically.

Memory is also consumed by the “deferred delete” state. In the deferred delete state, when an SRX Series device applies a policy change, there is transitory peak usage whereby both the old and new policies are present. So for a brief period, both old and new policies exist on the Packet Forwarding Engine, taking up twice the memory requirements.

Therefore, there is no definitive way to infer clearly how much memory is used by either component (Packet Forwarding Engine or Routing Engine) at any given point in time, because memory requirements are dependent on specific configurations of policies, and memory is allocated dynamically.

The following best practices for policy implementation enable you to better use system memory and to optimize policy configuration:

- Use single prefixes for source and destination addresses. For example, instead of using /32 addresses and adding each address separately, use a large subnet that covers most of the IP addresses you require.
- Use application “any” whenever possible. Each time you define an individual application in the policy, you can use an additional 52 bytes.
- Use fewer IPv6 addresses because IPv6 addresses consume more memory.
- Use fewer zone pairs in policy configurations. Each source or destination zone uses about 16,048 bytes of memory.
- The following parameters can change how memory is consumed by the bytes as specified:
  - Firewall authentication—About 16 bytes or more (unfixed)
  - Web authentication—About 16 bytes or more (unfixed)
  - IPsec—12 bytes
  - Application services—28 bytes
  - Count—64 bytes
- Check memory utilization before and after compiling policies.



**NOTE:** The memory requirement for each device is different. Some devices support 512,000 sessions by default, and the bootup memory is usually at 72 to 73 percent. Other devices can have up to 1 million sessions and the bootup memory can be up to 83 to 84 percent. In the worst-case scenario, to support about 80,000 policies in the SPU, the SPU should boot with a flowd kernel memory consumption of up to 82 percent, and with at least 170 megabytes of memory available.

---

**Related  
Documentation**

- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Global Address Books*
- *Global Policy Overview*
- *Example: Configuring a Global Policy with No Zone Restrictions*
- *Checking Memory Status*

---

## Intrusion Detection and Prevention

---

- [Pattern Matching Engine on page 262](#)
- [System Log Message on page 266](#)

### Pattern Matching Engine

- `show security idp policy-commit-status`
- `show security idp attack detail`

## show security idp policy-commit-status

<b>Syntax</b>	show security idp policy-commit-status
<b>Release Information</b>	Command introduced in JUNOS OS Release 10.4.
<b>Description</b>	<p>Display the IDP policy commit status. For example, status of policy compilation or load.</p> <p>Starting with Junos OS Release 12.3X48-D15, a new pattern matching engine is introduced for the SRX Series IDP feature. This scanning mechanism helps improve performance and policy loading. The new engine is 9.223 times faster than the existing DFA engine.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>show security idp status</i></li> <li>• <i>show security idp policy-commit-status clear</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp policy-commit-status on page 263</a>
<b>Output Fields</b>	When you enter this command, you are provided with the IDP policy commit status.

### Sample Output

#### show security idp policy-commit-status

```

user@host> show security idp policy-commit-status
IDP policy[/var/db/idpd/bins/test.bin.gz.v] and
detector[/var/db/idpd/sec-repository/installed-detector/libidp-detector.so.tgz.v]
loaded successfully.

The loaded policy size is:1735229 Bytes
PCRE converted patterns: 151 pcre:1 hw:0

```

## show security idp attack detail

<b>Syntax</b>	<b>show security idp attack detail <i>attack-name</i></b>
<b>Release Information</b>	Command introduced in Junos OS Release 11.4.
<b>Description</b>	Display details of a specified IDP attack.
<b>Options</b>	<ul style="list-style-type: none"> <li><b><i>attack-name</i></b> —IDP attack name.</li> </ul>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>clear security idp attack table</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp attack detail FTP:USER:ROOT on page 265</a> <a href="#">show security idp attack detail TROJAN:MISC:ROOTBEER-CLIENT on page 265</a>
<b>Output Fields</b>	Table 13 on page 264 lists the output fields for the <b>show security idp attack detail</b> command. Output fields are listed in the approximate order in which they appear.

**Table 13: show security idp attack detail Output Fields**

Field Name	Field Description
<b>Display Name</b>	Display name of the IDP attack.
<b>Severity</b>	Severity level of the IDP attack.
<b>Category</b>	IDP attack category.
<b>Recommended</b>	Specifies whether a default action for the IDP attack is recommended by Juniper Networks (true or false).
<b>Recommended Action</b>	Recommended action for the IDP attack.
<b>Type</b>	Type of IDP attack.
<b>Direction</b>	Direction of the IDP attack.
<b>False Positives</b>	Specifies whether the IDP attack produces a false positive on the network.
<b>Service</b>	IDP service configured for the IDP attack. If a service is configured for the IDP attack, the IDP service name is displayed. Otherwise, <b>Not available</b> is displayed.
<b>Member Name</b>	Name of the attack member in the IDP attack.
<b>Expression</b>	Specifies the Boolean expression of attack members. Used to identify the way (for example, OR, AND, or oAND) attack members should be matched.



Table 13: show security idp attack detail Output Fields (*continued*)

Field Name	Field Description
PCRE Expression	Specifies the Boolean expression of PCRE format-based attack members. Used to identify the way (for example, OR, AND, or oAND) attack members should be matched. If this field is not present, "Expression" is used as a Boolean expression for attack matching.
Shellcode	Signifies if the IDP attack is a shellcode attack.
Flow	Signifies the channel (control, data) of the IDP attack.
Context	Name of the context under which the IDP attack has to be matched.
Negate	Signifies if the signature in the IDP attack is a negate signature.
TimeBinding	Specifies count and scope under which the attack is valid.
Pattern	Specifies the regular expression in the IDP attack.
PCRE Pattern	Specifies the regular expression in PCRE format in the IDP attack.
Hidden Pattern	Specifies if the attack pattern is hidden.

## Sample Output

### show security idp attack detail FTP:USER:ROOT

```

user@host> run show security idp attack detail FTP:USER:ROOT
Display Name: FTP: "root" Account Login
Severity: Minor
Category: FTP
Recommended: false
Recommended Action: None
Type: signature
Direction: CTS
False Positives: unknown
Shellcode: no
Flow: control
Context: ftp-username
Negate: false
TimeBinding:
  Scope: none
  Count: 1
Hidden Pattern: False
Pattern: \[root\]

```

### show security idp attack detail TROJAN:MISC:ROOTBEER-CLIENT

```

user@host> show security idp attack detail TROJAN:MISC:ROOTBEER-CLIENT
Display Name: TROJAN: Digital Rootbeer Client Connect
Severity: Minor
Category: TROJAN
Recommended: false
Recommended Action: None

```

```
Type: chain
False Positives: unknown
Service: TCP/2600
Expression: m01 oAND m02
Order: no
Reset: no
Scope: session
TimeBinding:
Members:
  Member Name: m01
  Type: Signature
  Direction: CTS
  Flow: control
  Shellcode: no
  Context: stream256
  Negate: false
  Hidden Pattern: False
  Pattern: .*/QUE,who are you\.\.\.\?.*
  PCRE Pattern: ^(.)*\QUE,who are you\.\.\.\?

  Member Name: m02
  Type: Signature
  Direction: STC
  Flow: control
  Shellcode: no
  Context: stream256
  Negate: false
  Hidden Pattern: False
  Pattern: .*/QUE,billy the kid.*
  PCRE Pattern: ^(.)*\QUE,billy the kid
```

## System Log Message

### *IDP\_PATTERN\_CONVERSION\_FAILED*

---

#### IDP\_PATTERN\_CONVERSION\_FAILED

---

<b>System Log Message</b>	Conversion to the PCRE pattern failed <warning-message>.
<b>Description</b>	The IDP pattern conversion to PCRE format is failed for the attack details. Hence, the attacks were excluded from the active policy.
<b>Type</b>	Event: This message reports an event, not an error
<b>Severity</b>	warning
<b>Facility</b>	LOG_AUTH

---

## Documentation Feedback

---

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience.

Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.

- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net). Include the document or topic name, URL or page number, and software version (if applicable).

## Requesting Technical Support

---

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

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

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

## Revision History

---

1 July 2015—Revision 1, Junos OS Feature Guide for Junos OS Release 12.3X48-D15 Maintenance Release

10 November 2015—Revision 2, Junos OS Feature Guide for Junos OS Release 12.3X48-D20 Maintenance Release

2 May 2016—Revision 3, Junos OS Feature Guide for Junos OS Release 12.3X48-D30 Maintenance Release

Copyright © 2016, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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