JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

Common Criteria Guide for vSRX3.0

Published
2024-02-09

RELEASE
22.2R2

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, 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.

Junos® OS Common Criteria Guide for vSRX3.0
22.2R2
Copyright © 2024 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About This Guide

Use this guide to configure and evaluate vSRX3.0 for Common Criteria (CC) compliance. Common Criteria for information technology is an international agreement signed by several countries that permit the evaluation of security products against a common set of standards.

RELATED DOCUMENTATION

- Common Criteria and FIPS Certifications

CHAPTER 1

Overview

Understanding the Common Criteria Evaluated Configuration

IN THIS SECTION

This document describes the steps required to duplicate the configuration of the device running Junos OS when the device is evaluated. This is referred to as the evaluated configuration. The following list describes the standards to which the device has been evaluated:

- Collaborative Protection Profile for Network Devices, NDcPPv2.2e—https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.2E.pdf.

  PP modules for NDcPP are as follows:

  - MOD_FW_CPP v1.4e –https://www.niap-ccevs.org/MMO/PP/MOD_CPP_FW_v1.4e.pdf
  - MOD_IPS_V1.0 –https://www.niap-ccevs.org/MMO/PP/MOD_IPS_v1.0.pdf
  - VPNGW_MOD v1.2 – https://www.niap-ccevs.org/MMO/PP/MOD_VPNGW_v1.2.pdf

- Network Device Collaborative Protection Profile (NDcPPv2.2)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, Version 2.2, 22 March 2020 (VPNEP)
- Collaborative Protection Profile for Stateful Traffic Filter Firewalls, version 2.0, 14 March 2018 (FWcPP)https://www.commoncriteriaportal.org/files/ppfiles/CPP_FW_V2.0E.pdf
- Collaborative Protection Profile for Network Devices or Collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), (IPSEP)
- FIPS—https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

These documents are available at https://www.niap-ccevs.org/Profile/PP.cfm.

NOTE: On vSRX3.0, Junos OS Release 22.2R2 is certified for Common Criteria with FIPS mode enabled on the devices.

Understanding Common Criteria

Common Criteria for information technology is an international agreement signed by several countries that permits the evaluation of security products against a common set of standards. In the Common Criteria Recognition Arrangement (CCRA) at http://www.commoncriteriaportal.org/ccra/, the participants agree to mutually recognize evaluations of products performed in other countries. All evaluations are performed using a common methodology for information technology security evaluation.

For more information on Common Criteria, see http://www.commoncriteriaportal.org/.

Supported Platforms for vSRX Virtual Firewall

For the features described in this document, the following platforms are supported: • vSRX3.0 instances

The evaluated configuration for Common Criteria certification includes the following components:

- HP ProLiant DL380p Gen9 with Intel Xeon E5 with 3 to 8 NICs (at least as many as the number of configured virtual NICs (vNIC) in vSRX3.0)
- VMWare ESXi 7.0 Hypervisor
- Junos OS Release 22.2R2 for vSRX3.0 software installed as an ESXi Virtual Machine (VM)
- Pacstar 451 Model with 4 CPUs x Intel(R) Xeon(R) E-2254ML CPU @ 1.70GHz

NOTE: No other VMs may be installed on the ESXi instance. Each vNIC in vSRX3.0 must be mapped to a different physical NIC in the appliance or ESXi.

For more information on vSRX deployment over ESXi, see vSRX Virtual Firewall Deployment Guide for Private and Public Cloud Platforms.

Understanding Junos OS in FIPS Mode of Operation

IN THIS SECTION

Federal Information Processing Standards (FIPS) 140-3 defines security levels for hardware and software that perform cryptographic functions. Junos-FIPS is a version of the Junos operating system (Junos OS) that complies with Federal Information Processing Standard (FIPS) 140-3.

Operating vSRX Virtual Firewall 3.0 in a FIPS 140-3 Level 1 environment requires enabling and configuring FIPS mode of operation on the device from the Junos OS command-line interface (CLI).

The *Cryptographic Officer* enables FIPS mode of operation in Junos OS Release 22.2R2 and sets up keys and passwords for the system and other *FIPS users* who can view the configuration. Both user types can also perform normal configuration tasks on the device (such as modify interface types) as individual user configuration allows.

The cryptographic module is defined as multiple-chip standalone software module. The module executes Junos FIPS software on a VMware ESXi Hypervisor on the hardware platforms.

Table 1: Cryptographic Module Tested Configurations

Model	Software Version	Processor	HypervisorESXi	Hardware Platform
vSRX Virtual Firewall 3.0	Junos OS 22.2R2S2	Intel Xeon E5	ESXi 7.0	HP ProLiant DL380 Gen9 Server
vSRX Virtual Firewall 3.0	Junos OS 22.2R2S2	Intel Corei5	ESXi 7.0	PacStar 451 Server

About the Cryptographic Boundary on Your Device

FIPS 140-3 compliance requires a defined *cryptographic boundary* around each *cryptographic module* on a device. Junos OS in FIPS mode of operation prevents the cryptographic module from running any software that is not part of the FIPS-certified distribution, and allows only FIPS-approved cryptographic algorithms to be used. No critical security parameters (CSPs), such as passwords and keys, can cross the cryptographic boundary of the module by, for example, being displayed on a console or written to an external log file.

How FIPS Mode of Operation Differs from Non-FIPS Mode of Operation

Unlike Junos OS in non-FIPS mode of operation, Junos OS in FIPS mode of operation is a *nonmodifiable operational environment*. In addition, Junos OS in FIPS mode of operation differs in the following ways from Junos OS in non-FIPS mode of operation:

- Self-tests of all cryptographic algorithms are performed at startup.
- Self-tests of random number and key generation are performed continuously.
- Weak cryptographic algorithms such as Data Encryption Standard (DES) and MD5 are disabled.
- Weak or unencrypted management connections must not be configured.
- Passwords must be encrypted with strong one-way algorithms that do not permit decryption.
- Junos-FIPS administrator passwords must be at least 10 characters long.
- Cryptographic keys must be encrypted before transmission.

NOTE: In all other ways, Junos-FIPS behaves identically to the standard Junos OS image.

The FIPS 140-3 standard is available for download from the National Institute of Standards and Technology (NIST) at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf.

Validated Version of Junos OS in FIPS Mode of Operation

Juniper Networks submits one Junos OS release per year—Junos OS Release 22.2R2S2, for example—to the National Institute of Standards and Technology (NIST) for validation. To determine whether a Junos

OS release is NIST-validated, see the software download page on the Juniper Networks Web site (https://www.juniper.net/) or the National Institute of Standards and Technology site.

Understanding FIPS Mode of Operation Terminology and Supported Cryptographic Algorithms

IN THIS SECTION

Use the definitions of FIPS terms and supported algorithms to help you understand Junos OS in FIPS mode of operation.

FIPS Terminology

Critical security parameter (CSP)	Security-related information—for example, secret and private cryptographic keys and authentication data such as passwords and personal identification numbers (PINs)—whose disclosure or modification can compromise the security of a cryptographic module or the information it protects.
Cryptographic module	The set of hardware, software, and firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. SRX Series devices are certified at FIPS 140-3 Level 2.
Security Administrator	Person with appropriate permissions who is responsible for securely enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode of operation on a device.
ESP	Encapsulating Security Payload (ESP) protocol. The part of the IPsec protocol that guarantees the confidentiality of packets through encryption. The protocol ensures

	that if an ESP packet is successfully decrypted, and no other party knows the secret key the peers share, the packet was not wiretapped in transit.
FIPS	Federal Information Processing Standards. FIPS 140-3 specifies requirements for security and cryptographic modules. Junos OS in FIPS mode of operation complies with FIPS 140-3 Level 2.
IKE	The Internet Key Exchange (IKE) is part of IPsec and provides ways to securely negotiate the shared private keys that the authentication header (AH) and ESP portions of IPsec need to function properly. IKE employs Diffie-Hellman key-exchange methods and is optional in IPsec. (The shared keys can be entered manually at the endpoints.)
IPsec	The IP Security (IPsec) protocol. A standard way to add security to Internet communications. An IPsec security association (SA) establishes secure communication with another FIPS cryptographic module by means of mutual authentication and encryption.
KATs	Known answer tests. System self-tests that validate the output of cryptographic algorithms approved for FIPS and test the integrity of some Junos OS modules.
SA	Security association (SA). A connection between hosts that allows them to communicate securely by defining, for example, how they exchange private keys. As Security Administrator, you must manually configure an internal SA on devices running Junos OS in FIPS mode of operation. All values, including the keys, must be statically specified in the configuration.
SPI	Security parameter index (SPI). A numeric identifier used with the destination address and security protocol in IPsec to identify an SA. Because you manually configure the SA for Junos OS in FIPS mode of operation, the SPI must be entered as a parameter rather than derived randomly.
SSH	A protocol that uses strong authentication and encryption for remote access across a nonsecure network. SSH provides remote login, remote program execution, file copy, and other functions. It is intended as a secure replacement for `rlogin`, `rsh`, and `rcp` in a UNIX environment. To secure the information sent over administrative connections, use SSHv2 for CLI configuration. In Junos OS, SSHv2 is enabled by default, and SSHv1, which is not considered secure, is disabled.
Zeroization	Erasure of all CSPs and other user-created data on a device before its operation as a FIPS cryptographic module—or in preparation for repurposing the device for non-FIPS operation. The Security Administrator can zeroize the system with a CLI operational command.

Supported Cryptographic Algorithms

Each implementation of an algorithm is checked by a series of known answer test (KAT) self-tests. Any self-test failure results in a FIPS error state.

> **BEST PRACTICE**: For FIPS 140-3 compliance, use only FIPS-approved cryptographic algorithms in Junos OS in FIPS mode of operation.

The following cryptographic algorithms are supported in FIPS mode of operation. Symmetric methods use the same key for encryption and decryption, while asymmetric methods (preferred) use different keys for encryption and decryption.

AES The Advanced Encryption Standard (AES), defined in FIPS PUB 197. The AES algorithm uses keys of 128, 192, or 256 bits to encrypt and decrypt data in blocks of 128 bits.

Diffie-Hellman A method of key exchange across a nonsecure environment (such as the Internet). The Diffie-Hellman algorithm negotiates a session key without sending the key itself across the network by allowing each party to pick a partial key independently and send part of that key to the other. Each side then calculates a common key value. This is a symmetrical method, and keys are typically used only for a short time, discarded, and regenerated.

ECDH Elliptic Curve Diffie-Hellman. A variant of the Diffie-Hellman key exchange algorithm that uses cryptography based on the algebraic structure of elliptic curves over finite fields. ECDH allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. The shared secret can be used either as a key or to derive another key for encrypting subsequent communications using a symmetric key cipher.

ECDSA Elliptic Curve Digital Signature Algorithm. A variant of the Digital Signature Algorithm (DSA) that uses cryptography based on the algebraic structure of elliptic curves over finite fields. The bit size of the elliptic curve determines the difficulty of decrypting the key. The public key believed to be needed for ECDSA is about twice the size of the security level, in bits. ECDSA using the P-256, P-384, or the P-521 curve can be configured under OpenSSH.

HMAC Defined as “Keyed-Hashing for Message Authentication” in RFC 2104, HMAC combines hashing algorithms with cryptographic keys for message authentication. For Junos OS in FIPS mode of operation, HMAC uses the iterated cryptographic hash function SHA-1 (designated as HMAC-SHA1) along with a secret key.

Configuring the Time and Date

To configure a system date and time, use the following command:

```
[edit]
user@host# set date YYY YMMDDHHMM.ss
```

Configuring the User Session Idle Timeout

To configure the idle timeout for a user session, use the following command:

```
[edit]
      user@host# set system login idle-timeout minutes
```

Understanding Management Interfaces

The following management interfaces can be used in the evaluated configuration:

- Local Management Interfaces—The RJ-45 console port on the front panel of a device is configured as RS-232 data terminal equipment (DTE). Administrators can use the command-line interface (CLI) over this port to configure the device from a terminal.
- Remote Management Protocols—The device can be remotely managed over any Ethernet interface. SSHv2 is the only permitted remote management protocol that can be used in the evaluated configuration. The remote management protocols J-Web and Telnet are not available for use on the device.

RELATED DOCUMENTATION

Understanding the Common Criteria Evaluated Configuration

CHAPTER 2

Configuring Administrative Credentials and Privileges

Understanding the Associated Password Rules for an Authorized Administrator

The authorized administrator is associated with a defined login class, and the administrator is assigned with all permissions. Data is stored locally for fixed password authentication.

NOTE: We recommend that you not use control characters in passwords.

Use the following guidelines and configuration options for passwords and when selecting passwords for authorized administrator accounts. Passwords should be:

- Easy to remember so that users are not tempted to write it down.
- Changed periodically.
- Private and not shared with anyone.
- Contain a minimum of 10 characters. The minimum password length is 10 characters.

```
[ edit ]
administrator@host# set system login password minimum-length 10
```

- Include both alphanumeric and punctuation characters, composed of any combination of upper and lowercase letters, numbers, and special characters such as, “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)” and all other standard ASCII, extended ASCII and Unicode Characters. There should be at least a change in one case, one or more digits, and one or more punctuation marks.
- Contain character sets. Valid character sets include uppercase letters, lowercase letters, numbers, punctuation, and other special characters.

```
[ edit ]
administrator@host# set system login password change-type character-sets
```

- Contain the minimum number of character sets or character set changes. The minimum number of character sets required in plain-text passwords in Junos FIPS is 2.

```
[ edit ]
administrator@host# set system login password minimum-changes 2
```

NOTE: The authentication algorithm for plain-text passwords must be configured as sha256.

```
[ edit ]
administrator@host# set system login password format sha256
```

Weak passwords are:

- Words that might be found in or exist as a permuted form in a system file such as **/etc/passwd**.
- The hostname of the system (always a first guess).
- Any words appearing in a dictionary. This includes dictionaries other than English, and words found in works such as Shakespeare, Lewis Carroll, Roget's Thesaurus, and so on. This prohibition includes common words and phrases from sports, sayings, movies, and television shows.
- Permutations on any of the above. For example, a dictionary word with vowels replaced with digits (for example f00t) or with digits added to the end.
- Any machine-generated passwords. Algorithms reduce the search space of password-guessing programs and so should not be used.

Strong reusable passwords can be based on letters from a favorite phrase or word, and then concatenated with other, unrelated words, along with additional digits and punctuation. If the limit on the consecutive invalid password is reached, the user account is locked. The account automatically unlocks after the configured lockout time expires, or the account can be manually unlocked using the following command:

```
[ edit ]
administrator@host# clear system login lockout user username
```

NOTE: Passwords should be changed periodically.

Configuring a Common Criteria Authorized Administrator

An account for `root` is always present in a configuration and is not intended for use in normal operation. In the evaluated configuration, the `root` account is restricted to the initial installation and configuration of the evaluated device.

A Common Criteria authorized administrator must have all permissions, including the ability to change the router configuration.

To configure an authorized administrator:

1. Create a login class named security-admin with all permissions.

```
[edit]
root@host# set system login class security-admin permissions all
```

2. Define your common criteria user authorized administrator.

```
[edit]
root@host# set system login user NDcPP2.2e-user full-name Common Criteria NDcPP2.2e
Authorized Administrator class security-admin authentication encrypted-password <password>
```

3. Configure the authentication algorithm for plain-text passwords as sha256.

```
[edit]
root@host# set system login password format sha256
```

4. Commit the changes.

```
[edit]
root@host# commit
```

NOTE: The root password should be reset following the change to sha256 for the password storage format. This ensures the new password is protected using a sha256 hash, rather than the

default password hashing algorithm. To reset the root password, use the `set system login user root password` *`password`* command, and confirm the new password when prompted.

3

CHAPTER

Configuring Network Time Protocol

Configuring Network Time Protocol

The device can be configured to sync with a Network Time Protocol (NTP) server. This device supports time updates using NTP version 4 and NTP version 3. The device authentications updates using an administrator configured symmetric key, SHA-1 and SHA-256. The device rejects broadcast and multicast time updates. The device does not place a limit on the number of NTP time sources that can be configured.

To configure the device in client mode, include the server statement and other optional statements at the `[edit system ntp]` hierarchy level:

```
[edit system ntp]
server address <key key-number> <version value> <prefer>;
authentication-key key-number type type value password;
trusted-key[key-numbers];
```

Specify the address of the system acting as the time server. One specify an address, not a hostname.

To include an authentication key in all messages sent to the time server, include the `key` option. The key corresponds to the key number specified in the authentication-key statement.

By default, the device sends NTP version 4 packets to the time server. To set the NTP version level to 3, include the version option.

If more than one time server is configured, one server can be marked as preferred by including the *prefer* option.

The following example shows how to configure the device to operate in client mode:

```
[edit system ntp]
authentication-key 12 type sha256 value "$9$TQFn/9t0OIcywY4oGU9At"; ## SECRET-DATA
server 10.1.1.1 key 12 prefer;
trusted-key 12;
```

By default, NTP operates in an entirely unauthenticated manner. If a malicious attempt to influence the accuracy of a router or switch's clock succeeds, it could have negative effects on system logging, make troubleshooting and intrusion detection more difficult, and impede other management functions.

The following sample configuration synchronizes all the routers or switches in the network to a single time source. For common criteria compliance, use trusted authentication using SHA1 or SHA256 as the message digest algorithm(s) to make sure that the NTP peer is trusted. The `server` statement identifies the NTP server used for periodic time synchronization. The `source-address` statement enables the

administrator to specify one source address per family for each routing instance, The `authentication-key` statement specifies that a Sha256 scheme should be used to hash the key value for authentication, which prevents the router or switch from synchronizing with an attacker's host posing as the time server.

```
[edit]
system {
    ntp {
        authentication-key 12 type sha256 value " $9$TQFn/9t0OIcywY4oGU9At"; ## SECRET-DATA
        server 10.1.4.2 key 12;
        source-address 10.1.4.3;
        trusted key 12;
    }
}
```

For IP version 4 (IPv4), you can specify that if the NTP server configured at the `[edit system ntp]` hierarchy level is contacted on one of the loopback interface addresses, the reply always uses a specific source address. This is useful for controlling which source address NTP will use to access your network when it is either responding to an NTP client request from your network or when it itself is sending NTP requests to your network.

To configure the specific source address that the reply will always use, and the source address that requests initiated by NTP server will use, include the source-address statement at the `[edit system ntp]` hierarchy level. The source-address is a valid IP address configured on one of the router or switch interfaces.

```
[edit system ntp]
user@host#set source-address source-address
```

For example:

```
[edit system ntp]
user@host# set source-address 10.1.4.3
```

CHAPTER 4

Configuring Roles and Authentication Methods

Understanding Roles and Services for Junos OS in FIPS Mode of Operation

IN THIS SECTION

The Juniper Networks Junos operating system (Junos OS) running in non-FIPS mode of operation allows a wide range of capabilities for users, and authentication is identity-based. In contrast, the FIPS 140-3 standard defines two user roles: *Security Administrator* and *FIPS user*. These roles are defined in terms of Junos OS user capabilities.

Administrative users (Security Administrator) must provide unique identification and authentication data before any administrative access to the system is granted.

All other user types defined for Junos OS in FIPS mode of operation (operator, administrative user, and so on) must fall into one of the two categories: Security Administrator or FIPS user. For this reason, user authentication in FIPS mode of operation is role-based rather than identity-based.

In addition to their FIPS roles, both user types can perform normal configuration tasks on the device as individual user configuration allows.

Security Administrators and FIPS users perform all FIPS-related configuration tasks and issue all statements and commands for Junos OS in FIPS mode of operation. Security Administrator and FIPS user configurations must follow the guidelines for Junos OS in FIPS mode of operation.

Security Administrator Role and Responsibilities

The Security Administrator is the person responsible for enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode of operation on a device. The Security Administrator securely installs Junos OS on the device, enables FIPS mode of operation, establishes keys and passwords for other users and software modules, and initializes the device before network connection. The Security Administrator can configure and monitor the module through a console or SSH connection.

BEST PRACTICE: We recommend that the Security Administrator administer the system in a secure manner by keeping passwords secure and checking audit files.

The permissions that distinguish the Security Administrator from other FIPS users are `secret`, `security`, `maintenance`, and `control`. For FIPS compliance, assign the Security Administrator to a login class that contains all of these permissions. A user with the Junos OS maintenance permission can read files containing critical security parameters (CSPs).

NOTE: Junos OS in FIPS mode of operation does not support the *FIPS 140-3 maintenance role*, which is different from the Junos OS maintenance permission.

Among the tasks related to Junos OS in FIPS mode of operation, the Security Administrator is expected to:

- Set the initial root password.
- Reset user passwords for FIPS-approved algorithms during upgrades from Junos OS.
- Set up manual IPsec SAs for configuration with dual Routing Engines.
- Examine log and audit files for events of interest.
- Erase user-generated files and data on (zeroize) the device.

FIPS User Role and Responsibilities

All FIPS users, including the Security Administrator, can view the configuration. Only the user assigned as the Security Administrator can modify the configuration.

The permissions that distinguish Security Administrators from other FIPS users are `secret`, `security`, `maintenance`, and `control`. For FIPS compliance, assign the FIPS user to a class that contains *none* of these permissions.

FIPS users configure networking features on the device and perform other tasks that are not specific to FIPS mode of operation. FIPS users who are not Security Administrators can perform reboots and view status output.

What Is Expected of All FIPS Users

All FIPS users, including the Security Administrator, must observe security guidelines at all times.

All FIPS users must:

- Keep all passwords confidential.
- Store devices and documentation in a secure area.
- Deploy devices in secure areas.
- Check audit files periodically.
- Conform to all other FIPS 140-3 security rules.
- Follow these guidelines:
  - Users are trusted.
  - Users abide by all security guidelines.
  - Users do not deliberately compromise security.
  - Users behave responsibly at all times.

Loading Firmware on the Device

The Junos OS 22.2R2 FIPS images only accept the firmware signed with ECDSA and rejects any firmware signed with RSA + SHA1. You cannot downgrade to images that are signed with RSA + SHA1 from ECDSA signed only images. In this scenario, the vSRX device does not load the firmware. The load also fails if the embedded certificates in the firmware image are not valid.

RELATED DOCUMENTATION

Understanding FIPS Mode of Operation Terminology and Supported Cryptographic Algorithms | 6

Understanding Zeroization to Clear System Data for FIPS Mode of Operation | 31

Understanding Services for Junos OS in FIPS Mode of Operation

IN THIS SECTION

All services implemented by the module are listed in the tables that follow.

Understanding Authenticated Services

Table 2 on page 22 lists the authenticated services on the device running Junos OS.

Table 2: Authenticated services

Authenticated Services	Description	Security Administrator	User (read-only)	User (network)
Configure security	Security relevant configuration	x	–	–
Configure	Non-security relevant configuration	x	–	–
Secure traffic	IPsec protected routing	–	–	x
Status	Display the status	x	x	–

Table 2: Authenticated services *(Continued)*

Authenticated Services	Description	Security Administrator	User (read-only)	User (network)
Zeroize	Destroy all critical security parameters (CSPs)	x	–	–
SSH connect	Initiate SSH connection for SSH monitoring and control (CLI)	x	x	–
IPsec connect	Initiate IPsec connection (IKE)	x	–	x
Console access	Console monitoring and control (CLI)	x	x	–
Remote reset	Software-initiated reset	x	–	–

Table 3: Unauthenticated traffic

Service	Description
Local reset	Hardware reset or power cycle
Traffic	Traffic requiring no cryptographic services

Critical Security Parameters

Critical security parameters (CSPs) are security-related information such as cryptographic keys and passwords that can compromise the security of the cryptographic module or the security of the information protected by the module if they are disclosed or modified.

Zeroization of the system erases all traces of CSPs in preparation for operating the device as a cryptographic module.

"Critical Security Parameters" on page 23 lists the CSP access rights within services.

Table 4: CSP Access Rights Within Services

Service	CSPs					
	DRBG_Seed	DRBG_State	SSH PHK	SSH DH	SSH-SEK	ESP-SEK
Configure security	–	E	G, W	–	–	–
Configure	–	–	–	–	–	–
Secure Traffic	–	–	–	–	–	E
Status	–	–	–	–	–	–
Zeroize	Z	Z	Z	Z	Z	Z
SSH connect	–	E	E	G, E	G, E	–
IPSec connect	–	E	–	–	–	G
Console access	–	–	–	–	–	–
Remote reset	G, E	G	–	Z	Z	Z
Local Reset	G, E	G	–	Z	Z	Z
Traffic	–	–	–	–	–	–

Table 4: CSP Access Rights Within Services *(Continued)*

Keys/CSPs	CSPs					
	DRBG_Seed	DRBG_State	SSH PHK	SSH DH	SSH-SEK	ESP-SEK
Configure security	–	E	G, W	–	–	–
Configure	–	–	–	–	–	–
Secure Traffic	–	–	–	–	–	E
Status	–	–	–	–	–	–
Zeroize	Z	Z	Z	Z	Z	Z
SSH connect	–	E	E	G, E	G, E	–
IPSec connect	–	E	–	–	–	G
Console access	–	–	–	–	–	–
Remote reset	G, E	G	–	Z	Z	Z
Local Reset	G, E	G	–	Z	Z	Z
Traffic	–	–	–	–	–	–

Here:

- G = Generate: The device generates the CSP.
- E = Execute: The device runs using the CSP.
- W = Write: The CSP is updated or written to the device.
- Z = Zeroize: The device zeroizes the CSP.

Table 5: Cryptographic Key Destruction

Service	Purpose	Storage Location	Method of Zeroization
SSH Private Host Key	Generated with the random number generator when the SSH is first set up. Used to identify the host. ecdsa-sha2-nistp256 (ECDSA P-256, ECDSA P-384, ECDSA P-521) and/or ssh-rsa (RSA 2048)	Plaintext on the virtual disk.	When the TOE is recommissioned, the config files (including CSP files) are removed using the Linux shred command to wipe the persistent storage media.
SSH Private Host Key	Loaded into memory to complete session establishment	Plaintext in volatile memory.	The TOE calls `bzero()` at session termination. The hypervisor erases the released memory before it is placed in the free pool.
SSH Session Key	Session keys used with SSH, AES 128, 256, hmac-sha-1, hmac-sha2-256 or hmac-sha2-512 key (160, 256 or 512), DH Private Key (2048 or elliptic curve 256/384/521-bits)	Plaintext in volatile memory	The TOE calls `bzero()` at session termination. The hypervisor erases the released memory before it is placed in the free pool.
RNG state	Internal state and seed key of the RNG	Plaintext in volatile memory	Handled by kernel, overwritten with zeros at reboot.

Table 5: Cryptographic Key Destruction *(Continued)*

Service	Purpose	Storage Location	Method of Zeroization
IKE Private Host Key	Private authentication key used in IKE. RSA 2048, ECDSA P-256, ECDSA P-384	Plaintext in virtual disc or in flash memory	Erased by the Administrator issuing `clear security IKE security-association` command or zeroized at rebooting the TOE. Private keys stored in flash are not zeroized unless an explicit `request system zeroize` command is executed
IKE-SKEYID	IKE master secret used to derive IKE and IPsec ESP session keys	Plaintext in volatile memory	Erased by the Administrator issuing `clear security IKE security-association` command or zeroized at rebooting the TOE.
IKE Session Key	IKE Session keys. AES, HMAC	Plaintext in volatile memory	Erased by the Administrator issuing `clear security IKE security-association` command or zeroized at rebooting the TOE.

Table 5: Cryptographic Key Destruction *(Continued)*

Service	Purpose	Storage Location	Method of Zeroization
ESP Session Key	ESP Session Keys. AES, HMAC	Plaintext in volatile memory	Erased by the Administrator issuing `clear security ipsec security-association` command or zeroized at rebooting the TOE.
IKE-DH Private Exponent	Ephemeral DH private exponent used in IKE. DH N = 224 bit, ECDH P-256, or ECDH P-384	Plaintext in volatile memory	Erased by the Administrator issuing `clear security IKE security-association` command or zeroized at rebooting the TOE.
IKE-PSK	Pre-shared authentication key used in IKE	Hashed in virtual disc or flash memory	Erased by Administrator issuing a `clear security IKE security-association` command or zeroized at rebooting the TOE. Keys stored in flash are not zeroized unless an Administrator issues a `request system zeroize` command.

Table 5: Cryptographic Key Destruction *(Continued)*

Service	Purpose	Storage Location	Method of Zeroization
ecdh private keys	Loaded into memory to complete key exchange in session establishment	Plaintext in volatile memory	The TOE calls `bzero()` at session termination. The hypervisor erases the released memory before it is placed in the free pool.

RELATED DOCUMENTATION

Understanding Zeroization to Clear System Data for FIPS Mode of Operation | 31

Understanding FIPS Authentication Methods | 38

Downloading Software Packages from Juniper Networks (FIPS Mode)

To operate in Junos OS in FIPS mode, the device must have the following software packages installed. You can download the following Junos OS software packages from the Juniper Networks website:

- Junos OS for vSRX3.0 instances, Release 22.2R2.
- Junos FIPS mode, Release 22.2R2.

Before you begin to download the software, ensure that you have a Juniper Networks Web account and a valid support contract. To obtain an account, complete the registration form at the Juniper Networks website: https://www.juniper.net/registration/Register.jsp.

To download software packages from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks webpage. https://www.juniper.net/support/downloads/junos.html

2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Download the software. See Downloading Software

RELATED DOCUMENTATION

Installation and Upgrade Guide

Installing Junos Software Packages

SRX Series devices can provide the security defined by Federal Information Processing Standards (FIPS) 140-3 Level 2 if these devices are operated in the Junos OS in FIPS mode.

NOTE: Junos OS is delivered in signed packages that contain digital signatures to ensure the Juniper Networks software is running. When installing the software packages, Junos OS validates the signatures and the public key certificates used to digitally sign the software packages. If the signature or certificate is found to be invalid (for example, when the certificate validity period has expired or cannot be verified against the root CA stored in the Junos OS internal store), the installation process fails. Some functionalities might be impacted during the reboot following the software upgrade and not during the upgrade.

To install these software packages, perform the following tasks:

1. Download the Junos OS package and the Junos FIPS mode package from https://support.juniper.net/support/downloads/. See Downloading Software.
2. Install the Junos OS on your device using a TFTP server, see Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server or install Junos OS on your device using the following CLI command: `request system software add /<image-path>/<junos package> no-copy no-validate reboot`.

   Published Hash verification:

   To obtain Published hash, go to following link:

   https://support.juniper.net/support/downloads/?p=vsrx.

   To compute file hash and verify with published hash, below command is to be used:

   `user@host>` **file checksum sha1 software-package-name.tgz**

```
user@host> file checksum sha-256 software-package-name.tgz
```

RELATED DOCUMENTATION

Installation and Upgrade Guide

Understanding Zeroization to Clear System Data for FIPS Mode of Operation

IN THIS SECTION

Zeroization completely erases all configuration information on the device, including all plaintext passwords, secrets, and private keys for SSH, local encryption, local authentication, and IPsec. To exit the FIPS mode you need to zeroize the device.

The cryptographic module provides a non-approved mode of operation in which non-approved cryptographic algorithms are supported. When moving from the non-approved mode of operation to the approved mode of operation, the security administrator must zeroize the non-approved mode critical security parameters (CSPs).

Zeroization can be time-consuming. Although all configurations are removed in a few seconds, the zeroization process goes on to overwrite all media, which can take considerable time depending on the size of the media.

Why Zeroize?

Your device is not considered a valid FIPS cryptographic module until all CSPs have been entered—or reentered—while the device is in FIPS mode of operation.

BEST PRACTICE: For FIPS 140-2 compliance, we recommend that you zeroize the device to exit the FIPS mode.

When to Zeroize?

The cryptographic module provides a non-approved mode of operation in which non-approved cryptographic algorithms are supported. When transitioning between the non-approved mode of operation and the approved mode of operation, the Cryptographic Officer must zeroize the approved mode CSPs. This is achieved by removing the vSRX Virtual Firewall virtual machine from the datastore by following the below steps on VMWare vSphere:

1. Power off the vSRX Virtual Firewall virtual machine.
2. Ensure that another virtual machine is not sharing the disk. If two virtual machines are sharing the same disk, the disk files are not deleted.
3. Right click the virtual machine and select All vCenter Actions > Delete from Disk.
4. Click OK.

As a security administrator, perform zeroization in the following situations:

- **Before FIPS operation**—To prepare your device for operation as a FIPS cryptographic module, perform zeroization to remove the non-approved mode critical security parameters (CSPs) and enable FIPS mode on the device.
- **Before non-FIPS operation**—To begin repurposing your device for non-FIPS operation, perform zeroization before disabling FIPS mode of operation on the device or loading Junos OS packages that do not include FIPS mode of operation.

NOTE: Juniper Networks does not support installing non-FIPS software in a FIPS mode of operation, but doing so might be necessary in certain test environments. Be sure to zeroize the system first.

RELATED DOCUMENTATION

Understanding FIPS Self-Tests | 268

How to Enable and Configure Junos OS in FIPS Mode of Operation

You, as security administrator, can enable and configure Junos OS in FIPS mode of operation on your device.

To enable the Junos OS in FIPS mode of operation, perform the following steps:

1. Enable the FIPS mode on the device.

   ```
   user@host# set system fips level 2
   ```

2. Commit and reboot the device.

   ```
   user@host# commit
   ```

3. Run integrity and self-tests on powering on the device when the module is operating in FIPS mode.

4. Configure IKEv2 when AES-GCM is used for encryption of IKE and/or IPSec.

```
root@host# set security ike proposal <ike_proposal_name> encryption-algorithm ?
Possible completions:
aes-128-cbc
aes-128-gcm
aes-192-cbc
aes-256-cbc
aes-256-gcm
AES-CBC 128-bit encryption algorithm
AES-GCM 128-bit encryption algorithm
AES-CBC 192-bit encryption algorithm
AES-CBC 256-bit encryption algorithm
AES-GCM 256-bit encryption algorithm
root@host# set security ike proposal <ike_proposal_name> encryption-algorithm aes-256-gcm
root@host# set security ipsec proposal <ipsec_proposal_name> encryption-algorithm ?
Possible completions:
aes-128-cbc
aes-128-gcm
aes-192-cbc
aes-192-gcm
aes-256-cbc
aes-256-gcm
AES-CBC 128-bit encryption algorithm
```

```
AES-GCM 128-bit encryption algorithm
AES-CBC 192-bit encryption algorithm
AES-GCM 192-bit encryption algorithm
AES-CBC 256-bit encryption algorithm
AES-GCM 256-bit encryption algorithm
root@host# set security ipsec proposal <ipsec_proposal_name> encryption-algorithm aes-128-gcm
root@host# set security ike gateway <gateway_name> version ?
Possible completions:
v1-only The connection must be initiated using IKE version 1
v2-only The connection must be initiated using IKE version 2
root@host# set security ike gateway <gateway_name> version v2-only
root@host# commit
commit complete
```

5. Ensure that the backup image of the firmware is also a JUNOS-FIPS image by issuing the `request system snapshot` command.

NOTE: The `show configuration security ike` and `show configuration security ipsec` commands display the approved and configured IKE/IPsec configuration for the device operating in FIPS-approved mode.

```
root@fipscc-vsrx3-c:fips> show version
Hostname: fipscc-vsrx3-c
Model: vSRX
Junos: 22.2R2.10
JUNOS OS Kernel 64-bit  [20220817.0361d5f_builder_stable_12_222]
JUNOS OS libs [20220817.0361d5f_builder_stable_12_222]
JUNOS OS runtime [20220817.0361d5f_builder_stable_12_222]
JUNOS OS time zone information [20220817.0361d5f_builder_stable_12_222]
JUNOS network stack and utilities [20221105.194720_builder_junos_222_r2]
JUNOS libs [20221105.194720_builder_junos_222_r2]
JUNOS OS libs compat32 [20220817.0361d5f_builder_stable_12_222]
JUNOS OS 32-bit compatibility [20220817.0361d5f_builder_stable_12_222]
JUNOS libs compat32 [20221105.194720_builder_junos_222_r2]
JUNOS runtime [20221105.194720_builder_junos_222_r2]
JUNOS Simple Package [18.4I20180626_1521_tmfink]
JUNOS py extensions [20221105.194720_builder_junos_222_r2]
JUNOS py base [20221105.194720_builder_junos_222_r2]
JUNOS OS vmguest [20220817.0361d5f_builder_stable_12_222]
JUNOS OS crypto [20220817.0361d5f_builder_stable_12_222]
JUNOS OS boot-ve files [20220817.0361d5f_builder_stable_12_222]
```

```
JUNOS na telemetry [22.2R2.10]
JUNOS Web Management Platform Package [20221105.194720_builder_junos_222_r2]
JUNOS vsrx modules [20221105.194720_builder_junos_222_r2]
JUNOS publish subscribe base [20221105.194720_builder_junos_222_r2]
JUNOS srx libs compat32 [20221105.194720_builder_junos_222_r2]
JUNOS srx runtime [20221105.194720_builder_junos_222_r2]
JUNOS srx platform support [20221105.194720_builder_junos_222_r2]
JUNOS common platform support [20221105.194720_builder_junos_222_r2]
JUNOS vsrx runtime [20221105.194720_builder_junos_222_r2]
JUNOS Routing mpls-oam-basic [20221105.194720_builder_junos_222_r2]
JUNOS Routing lsys [20221105.194720_builder_junos_222_r2]
JUNOS Routing 32-bit Compatible Version [20221105.194720_builder_junos_222_r2]
JUNOS Routing aggregated [20221105.194720_builder_junos_222_r2]
JUNOS probe utility [20221105.194720_builder_junos_222_r2]
JUNOS pppoe [20221105.194720_builder_junos_222_r2]
JUNOS Openconfig [22.2R2.10]
JUNOS mtx network modules [20221105.194720_builder_junos_222_r2]
JUNOS modules [20221105.194720_builder_junos_222_r2]
JUNOS srx libs [20221105.194720_builder_junos_222_r2]
JUNOS L2 RSI Scripts [20221105.194720_builder_junos_222_r2]
JUNOS hsm [20221105.194720_builder_junos_222_r2]
JUNOS srx Data Plane Crypto Support [20221105.194720_builder_junos_222_r2]
JUNOS daemons [20221105.194720_builder_junos_222_r2]
JUNOS srx daemons [20221105.194720_builder_junos_222_r2]
JUNOS cloud libs [20221105.194720_builder_junos_222_r2]
JUNOS cloud init [20221105.194720_builder_junos_222_r2]
JUNOS SRX TVP AppQos Daemon [20221105.194720_builder_junos_222_r2]
JUNOS Extension Toolkit [20221105.194720_builder_junos_222_r2]
JUNOS Juniper Malware Removal Tool (JMRT) [1.0.0+20221105.194720_builder_junos_222_r2]
JUNOS Juniper Malware Removal Tool (JMRT) Test [1.0.0+20221105.194720_builder_junos_222_r2]
JUNOS J-Insight [20221105.194720_builder_junos_222_r2]
JUNOS jfirmware [20220922.092606_builder_junos_222_r2]
JUNOS Online Documentation [20221105.194720_builder_junos_222_r2]
JUNOS jail runtime [20220817.0361d5f_builder_stable_12_222]
JUNOS FIPS mode utilities [20221105.194720_builder_junos_222_r2]
JUNOS dsa dsa [22.2R2.10]
Junos debug agent [20221105.194720_builder_junos_222_r2]
```

The `fips` keyword next to the `hostname` in the output indicates that the module is operating in FIPS mode for Junos Software Release 22.2R2.

```
user@host-vSRX3.0:fips> show configuration security ike
proposal ike-proposal1 {
    authentication-method pre-shared-keys;
    dh-group group14;
    encryption-algorithm aes-256-gcm;
}
policy ike-policy1 {
    mode main;
    proposals ike-proposal1;
    pre-shared-key ascii-text "$9$Hq.5zF/tpBUj9Au0IRdbwsaZ"; ## SECRET-DATA
}
gateway gw1 {
    ike-policy ike-policy1;
    address 198.51.100.0;
    local-identity inet 203.0.113.0;
    external-interface ge-0/0/3;
    version v2-only;
}


user@host-vSRX3.0:fips> show configuration security ipsec
proposal ipsec-proposal1 {
    protocol esp;
    encryption-algorithm aes-128-gcm;
}
policy ipsec-policy1 {
    perfect-forward-secrecy {
        keys group14;
    }
    proposals ipsec-proposal1;
}
vpn vpn1 {
    bind-interface st0.0;
    ike {
        gateway gw1;
        ipsec-policy ipsec-policy1;
    }
}
```

5
CHAPTER

Configuring SSH and Console Connection

Understanding FIPS Authentication Methods

IN THIS SECTION

The Juniper Networks Junos operating system (Junos OS) running in FIPS mode of operation allows a wide range of capabilities for users, and authentication is role-based. The following types of role-based authentication are supported in the FIPS mode of operation:

- "Username and Password Authentication over the Console and SSH" on page 38
- "Username and Public Key Authentication over SSH" on page 39

Username and Password Authentication over the Console and SSH

In this authentication method, the user is requested to enter the username and password. The device enforces the user to enter a minimum of 10 characters password that is chosen from the 96 human-readable ASCII characters.

NOTE: The maximum password length is 20 characters.

In this method, the device enforces a timed access mechanism—for example, first two failed attempts to enter the correct password (assuming 0 time to process), no timed access is enforced. When the user enters the password for the third time, the module enforces a 5 second delay. Each failed attempt thereafter results in an additional 5 second delay above the previous failed attempt. For example, if the fourth failed attempt is a 10 second delay, then the fifth failed attempt is a 15 second delay, the sixth failed attempt is a 20 second delay, and the seventh failed attempt is a 25 second delay.

Therefore, this leads to a maximum of seven possible attempts in a 1 minute period for each getty active terminal. So, the best approach for the attacker would be to disconnect after 4 failed attempts, and wait for a new getty to be spawned. This would allow the attacker to perform roughly 9.6 attempts per minute (576 attempts per hour or 60 minutes). This would be rounded off to 9 attempts per minute, because there is no such thing as 0.6 attempts. Thus the probability of a successful random attempt is

1/9610, which is less than 1/1 million. The probability of a success with multiple consecutive attempts in a 1 minute period is 9/(9610), which is less than 1/100,000.

Username and Public Key Authentication over SSH

In SSH public key authentication, you provide the username and validate the ownership of the private key corresponding to the public key stored on the server. The device supports ECDSA (P-256, P-384, and P-521) and RSA (2048, 3072, and 4092 modulus bit length) key-types. The probability of a success with multiple consecutive attempts in a 1-minute period is 5.6e7/(2128).

NOTE: The ssh-rsa authentication method is one of the allowed algorithms in FIPS mode.

Configuring a System Login Message and Announcement

A system login message appears before the user logs in and a system login announcement appears after the user logs in. By default, no login message or announcement is displayed on the device. The administrator is required to configure a login message and announcement for Common Criteria compliance.

To configure a system login message, use the following command:

```
[edit]
user@host# set system login message login-message-banner-text
```

To configure system announcement, use the following command:

```
[edit]
user@host# set system login announcement  system-announcement-text
```

NOTE:

- If the message text contains any spaces, enclose it in quotation marks.
- You can format the message using the following special characters:
  - \n—New line
  - \t—Horizontal tab
  - \'—Single quotation mark
  - \"—Double quotation mark
  - \\—Backslash

Limiting the Number of User Login Attempts for SSH Sessions

A remote administrator may login to a device through SSH. Administrator credentials are stored locally on the device. If the remote administrator presents a valid username and password, access to the TOE is granted. If the credentials are invalid, the TOE allows the authentication to be retried after an interval that starts after 1 second and increases exponentially. If the number of authentication attempts exceed the configured maximum, no authentication attempts are accepted for a configured time interval. When the interval expires, authentication attempts are again accepted.

You can configure the device to limit the number of attempts to enter a password while logging through SSH. Using the following command, the connection can be terminated if a user fails to login after a specified number of attempts:

```
[edit system login]
user@host# set retry-options  tries-before-disconnect <number>
```

Here, `tries-before-disconnect` is the number of times a user can attempt to enter a password when logging in. The connection closes if a user fails to log in after the number specified. The range is from 1 through 10, and the default value is 10.

You can also configure a delay, in seconds, before a user can try to enter a password after a failed attempt.

```
[edit system login]
user@host# set retry-options  backoff-threshold  <number>
```

Here, `backoff-threshold` is the threshold for the number of failed login attempts before the user experiences a delay in being able to enter a password again. Use the `backoff-factor` option to specify the length of the delay in seconds. The range is from 1 through 3, and the default value is 2 seconds.

In addition, the device can be configured to specify the threshold for the number of failed attempts before the user experiences a delay in entering the password again.

```
[edit system login]
user@host# set retry-options  backoff-factor  <number>
```

Here, `backoff-factor` is the length of time, in seconds, before a user can attempt to log in after a failed attempt. The delay increases by the value specified for each subsequent attempt after the threshold. The range is from 5 through 10, and the default value is 5 seconds.

You can control user access through SSH. By configuring ssh root-login deny, the administrator can ensure the root account remains active and continues to have local administrative privileges to the TOE even if other remote users are logged off.

```
[edit system login]
user@host# set services ssh root-login deny
```

The SSH2 protocol provides secure terminal sessions utilizing the secure encryption. The SSH2 protocol enforces running the key-exchange phase and changing the encryption and integrity keys for the session. Key exchange is done periodically, after specified seconds or after specified bytes of data have passed over the connection. Thresholds for SSH rekeying can be configured. The TSF ensures that within the SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of the transmitted data. When either of the thresholds are reached, a rekey must be performed.

```
[edit system login]
user@host# set services ssh rekey time-limit number
```

Time limit before renegotiating session keys is 1 through 1440 minutes.

```
[edit system login]
user@host# set services ssh rekey data-limit number
```

Data limit before renegotiating session keys is 51200 through 4294967295 byte.

Configuring SSH on the Evaluated Configuration

SSH is an allowed remote management interface in the evaluated configuration. This topic describes how to configure SSH on the device.

1. Before you begin, log in with your root account on the device running Junos OS Release 22.2R2 and edit the configuration.

NOTE: The commands shown configure SSH to use all of the allowed cryptographic algorithms.

NOTE: You can enter the configuration commands in any order and commit all the commands at once.

To configure SSH on the TOE:

1. Specify the permissible SSH host-key algorithms.

```
[edit system services ssh]
user@host# set hostkey-algorithm ssh-ecdsa
```

NOTE: For Common Criteria compliance, use below host key algorithms : ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, and ecdsa-sha2-nistp521.

2. Specify the command to disable rsa-sha2-512 and rsa-sha2-256 hostkey algorithms.

```
[edit system services ssh]
user@host# set hostkey-algorithm no-ssh-rsa
```

> **NOTE**: The set system services ssh hostkey-algorithm no-ssh-rsa command will disable the rsa-sha2-512, rsa-sha2-256, and ssh-rsa hostkey algorithms.

3. Specify the SSH key-exchange algorithms.

```
[edit system services ssh]
user@host#set key-exchange [ ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 Diffie-
hellman-group14-sha1 ]
```

4. Specify all the permissible message authentication code algorithms.

```
[edit system services ssh]
user@host#set macs [ hmac-sha1 hmac-sha2-256 hmac-sha2-512 ]
```

5. Specify the ciphers allowed for protocol version 2.

```
[edit system services ssh]
user@host#set ciphers [ aes128-cbc aes128-ctr aes192-cbc aes192-ctr aes256-cbc aes256-ctr ]
```

6. (Optional step) Specify the number of minutes or maximum amount of data, before a rekey is forced on a session. The time limit must not be set greater than one hour and the data limit must not be set greater than one gigabyte.

```
[edit system services ssh]
user@host#set rekey time-limit minutes
user@host#set rekey data-limit bytes
```

RELATED DOCUMENTATION

Understanding FIPS Authentication Methods | 38

How to Enable and Configure Junos OS in FIPS Mode of Operation | 33

6
CHAPTER

Configuring the Remote Syslog Server

Sample Syslog Server Configuration on a Linux System

IN THIS SECTION

Sample Syslog Server Configuration on a Linux System Overview

A secure Junos OS environment requires auditing of events and storing them in a local audit file. The recorded events are simultaneously sent to an external syslog server. A syslog server receives the syslog messages streamed from the device. The syslog server must have an SSH client with NETCONF support configured to receive the streamed syslog messages.

The NDcPP2.2e logs capture the events, few of them are listed below:

- Committed changes
- Login and logout of users
- Failure to establish an SSH session
- Establishment or termination of an SSH session
- Changes to the system time

The following procedure is an example to show how to configure a syslog server on a Linux platform using the StrongSwan configuration to provide IPsec. Before you begin, the Linux-based syslog server must be configured with the IP address and gateway, and the StrongSwan IPsec client must be installed on the syslog server to initiate a VPN connection with the Junos OS device.

To setup a StrongSwan configuration on the remote syslog server to provide IPsec VPN capability:

1. Modify the */etc/ipsec.secrets* settings in accordance with the Junos OS device configuration.

```
root@host# vi /etc/ipsec.secrets 192.168.1.2 192.168.1.1 : PSK “12345”
```

2. Modify the */etc/ipsec.conf* settings in accordance with the Junos OS device configuration.

```
root@host# vi /etc/ipsec.conf
config setup
                charondebug="ike 4, cfg 4, chd 4, enc 1, net 4, knl 4, dmn 4"
conn %default
              ikelifetime=240
                keylife=300
                rekeymargin=10s
                keyingtries=%forever
                mobike=no
conn home
              keyexchange=ikev1
                authby=psk
                ike=aes128-sha256-modp2048!
                esp=aes128-sha1-modp2048!
                left=192.168.1.2 # self if
                leftsubnet=203.0.113.1/24 # self net for proxy id
                leftid=192.168.1.2 # self id
                right=192.168.1.1 # peer if
                rightsubnet=192.168.2.0/24 # peer net for proxy id
                rightid=192.168.1.1 # peer id
                auto=add
                leftfirewall=yes
                dpdaction=restart
                dpddelay=10
                dpdtimeout=120
                rekeyfuzz=10%
                reauth=no
```

NOTE: Here `conn home` specifies the name of the IPSec tunnel connection to be established between a Junos OS device and Strongswan VPN Client on Syslog server, `ike=aes-sha256-modp2048` specifies the IKE encryption and authentication algorithms and DH Group to be used for the connection, and`esp=aes128-sha1` specifies the ESP encryption and authentication algorithms to be used for the connection.

3. Activate IPsec service by using `ipsec up <being-established-ipsec-tunnel-name>` command. For example,

```
[root@host]# ipsec up home
002 "home" #3: initiating Main Mode
104 "home" #3: STATE_MAIN_I1: initiate
010 "home" #3: STATE_MAIN_I1: retransmission; will wait 20s for response
```

4. Restart the IPsec StrongSwan service.

```
root@host# ipsec restart
```

5. Check for syslog encrypted traffic.

```
root@host# tcpdump -I eth1 -vv -s 1500 -c 10 -o /var/tmp/Syslog_Traffic.pcap
```

6. Copy **/var/log/syslog to /var/tmp/syslog_verify** file on the syslog server to validate the syslog from the Junos OS device.

```
root@host# cp /var/log/syslog /var/tmp/syslog_verify
```

Configuring Event Logging to a Local File

You can configure storing of audit information to a local file and the level of detail to be recorded with the `syslog` statement. This example stores logs in a file named **Audit_file**

```
[edit system]
syslog {
    file Audit_file;
}
```

Configuring Event Logging to a Remote Server

Configure the export of audit information to a secure, remote server by setting up an event trace monitor that sends event log messages by using NETCONF over SSH to the remote system event logging server. The following procedures show the configuration needed to send system log messages to a secure external server by using NETCONF over SSH.

Configuring Event Logging to a Remote Server when Initiating the Connection from the Remote Server

The following procedure describes the steps to configure event logging to a remote server when the SSH connection to the TOE is initiated from the remote system log server.

1. Generate an RSA public key on the remote syslog server.

```
$ ssh-keygen -b 2048 -t rsa -C 'syslog-monitor key pair' -f ~/.ssh/syslog-monitor
```

   You will be prompted to enter the desired passphrase. The storage location for the `syslog-monitor` key pair is displayed.

2. On the TOE, create a class named `monitor` that has permission to trace events.

```
[edit]
user@host# set system login class monitor permissions trace
```

3. Create a user named `syslog-mon` with the class monitor, and with authentication that uses the `syslog-monitor` key pair from the key pair file located on the remote syslog server.

```
[edit]
user@host# set system login user syslog-mon class monitor authentication ssh-rsa “ssh-rsa
xxxxx syslog-monitor key pair”
```

4. Set up NETCONF with SSH.

```
[edit]
user@host# set system services netconf ssh
```

5. Configure syslog to log all the messages at */var/log/messages*.

```
[edit]
user@host# set system syslog file Audit_file any any
user@host# commit
```

6. On the remote system log server, start up the SSH agent. The start up is required to simplify the handling of the syslog-monitor key.

```
$ eval `ssh-agent`
```

7. On the remote syslog server, add the `syslog-monitor` key pair to the SSH agent.

```
$ ssh-add ~/.ssh/syslog-monitor
```

You will be prompted to enter the desired passphrase. Enter the same passphrase used in Step 1.

8. After logging in to the `external_syslog_server` session, establish a tunnel to the device and start NETCONF.

```
$ ssh syslog-mon@NDcPP_TOE -s netconf > test.out
```

9. After NETCONF is established, configure a system log events message stream. This RPC will cause the NETCONF service to start transmitting messages over the SSH connection that is established.

```
<rpc><get-syslog-events><stream>messages</stream></get-syslog-events></rpc>
```

10. The examples for syslog messages are listed below. Monitor the event log generated for admin actions on TOE as received on the syslog server. Examine the traffic that passes between the audit server and the TOE, observing that these data are not viewed during this transfer, and that they are successfully received by the audit server. Match the logs between local event and the remote event logged in a syslog server and record the particular software (such as name, version, and so on) used on the audit server during testing.

The following output shows test log results for syslog server.

```
host@ssh-keygen -b 2048 -t rsa -C 'syslog-monitor key pair' -f ~/.ssh/syslog-monitor
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

```
Your identification has been saved in /home/host/.ssh/syslog-monitor.
Your public key has been saved in /home/host/.ssh/syslog-monitor.pub.
The key fingerprint is:
ef:75:d7:68:c5:ad:8d:6f:5e:7a:7e:9b:3d:f1:4d:3f syslog-monitor key pair
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|                 |
|                 |
|               ..|
|        S       +|
|         .     Bo|
|          . . *.X|
|         . . o E@|
|          .   .BX|
+-----------------+
[host@linux]$ cat /home/host/.ssh/syslog-monitor.pub
ssh-rsa
 AAAAB3NzaC1yc2EAAAADAQABAAABAQCrUREJUBpjwAoIgRrGy9zgt+
D2pikk3Q/Wdf8I5vr+njeqJhCx2bUAkrRbYXNILQQAZbg7kLfi/8TqqL
eon4HOP2e6oCSorKdx/GrOTzLONL4fh0EyuSAk8bs5JuwWNBUokV025
gzpGFsBusGnlj6wqqJ/sjFsMmfxyCkbY+pUWb8m1/A9YjOFT+6esw+9S
tF6Gbg+VpbYYk/Oday4z+z7tQHRFSrxj2G92aoliVDBLJparEMBc8w
LdSUDxmgBTM2oadOmm+kreBUQjrmr6775RJn9H9YwIxKOxGm4SFnX/Vl4
R+lZ9RqmKH2wodIEM34K0wXEHzAzNZ01oLmaAVqT
syslog-monitor key pair
[host@linux]$ eval `ssh-agent`
Agent pid 1453
[host@linux]$ ssh-add ~/.ssh/syslog-monitor
Enter passphrase for /home/host/.ssh/syslog-monitor:
Identity added: /home/host/.ssh/syslog-monitor (/home/host/.ssh/syslog-monitor)
```

```
host@linux]$ ssh syslog-mon@starfire -s netconf > test.out
host@linux]$ cat test.out
this is NDcPP test device

<!-- No zombies were killed during the creation of this user interface --
<!-- user syslog-mon, class j-monitor -><hello>
  <capabilities>
    <capability>urn:ietf:params:xml:ns:netconf:base:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:candidate:1.0</capability>
```

```
    <capability>urn:ietf:params:xml:ns:netconf:capability:confirmed-commit:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:validate:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:url:1.0?protocol=http,ftp,file</
capability>
    <capability>http://xml.juniper.net/netconf/junos/1.0</capability>
    <capability>http://xml.juniper.net/dmi/system/1.0</capability>
  </capabilities>
  <session-id4129/session-id>
</hello>
]]>]]>
```

The following output shows event logs generated on the TOE that are received on the syslog server.

```
Jan 20 17:04:51  starfire sshd[4182]: error: Could not load host key: /etc/ssh/ssh_host_dsa_key
Jan 20 17:04:51  starfire sshd[4182]: error: Could not load host key: /etc/ssh/ssh_host_ecdsa_key
Jan 20 17:04:53  starfire sshd[4182]: Accepted password for sec-admin from 10.209.11.24 port
55571 ssh2
Jan 20 17:04:53  starfire mgd[4186]: UI_AUTH_EVENT: Authenticated user 'sec-admin' at permission
level 'j-administrator'
Jan 20 17:04:53  starfire mgd[4186]: UI_LOGIN_EVENT: User 'sec-admin' login, class 'j-
administrator' [4186], ssh-connection '10.209.11.24 55571 10.209.14.92 22', client-mode 'cli'
```

The following output shows that the local syslogs and remote syslogs received are similar.

```
Local : an 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress:
Redundancy interface management process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/rdd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/rdd', PID 4317,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Dynamic
flow capture service checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/dfcd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/dfcd', PID 4318,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress:
Connectivity fault management process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/cfmd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/cfmd', PID 4319,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Layer 2
address flooding and learning process checking new configuration
```

```
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/l2ald'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/l2ald', PID 4320,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Layer 2
Control Protocol process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/l2cpd'
Jan 20 17:09:30  starfire l2cp[4321]: Initializing PNAC state machines
Jan 20 17:09:30  starfire l2cp[4321]: Initializing PNAC state machines complete
Jan 20 17:09:30  starfire l2cp[4321]: Initialized 802.1X module and state machinesJan 20
17:09:30  starfire l2cp[4321]: Read acess profile () config
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/l2cpd', PID 4321,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Multicast
Snooping process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/mcsnoopd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/mcsnoopd', PID
4325, status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: commit
wrapup...
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress:
activating '/var/etc/ntp.conf'
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: start ffp
activate
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/ffp'
Jan 20 17:09:30  starfire ffp[4326]: "dynamic-profiles": No change to
profiles.....................................
```

```
Remote : an 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress:
Redundancy interface management process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/rdd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/rdd', PID 4317,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Dynamic
flow capture service checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/dfcd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/dfcd', PID 4318,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress:
Connectivity fault management process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/cfmd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/cfmd', PID 4319,
```

```
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Layer 2
address flooding and learning process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/l2ald'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/l2ald', PID 4320,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Layer 2
Control Protocol process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/l2cpd'
Jan 20 17:09:30  starfire l2cp[4321]: Initializing PNAC state machines
Jan 20 17:09:30  starfire l2cp[4321]: Initializing PNAC state machines complete
Jan 20 17:09:30  starfire l2cp[4321]: Initialized 802.1X module and state machinesJan 20
17:09:30  starfire l2cp[4321]: Read acess profile () config
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/l2cpd', PID 4321,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Multicast
Snooping process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/mcsnoopd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/mcsnoopd', PID
4325, status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: commit
wrapup...
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress:
activating '/var/etc/ntp.conf'
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: start ffp
activate
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/ffp'
Jan 20 17:09:30  starfire ffp[4326]: "dynamic-profiles": No change to profiles ..............
```

If the connections used by the device is unintentionally broken, the security administrator needs to restart the connection, or the device will try to re-connect with the audit server.

CHAPTER 7

Configuring Audit Log Options

Configuring Audit Log Options in the Evaluated Configuration

IN THIS SECTION

Configuring Audit Log Options for vSRX3.0

The following section describes how to configure audit log options in the evaluated configuration. To configure audit log options for vSRX3.0 instances:

1. Specify the number of files to be archived in the system logging facility.

```
[edit system syslog]
root@host# set archive files 2
```

2. Specify the file in which to log data.

```
[edit system syslog]
root@host# set file syslog any any
```

3. Specify the size of files to be archived.

```
[edit system syslog]
root@host# set file syslog archive size 10000000
```

4. Log system messages in a structured format.

```
[edit system syslog]
          root@host# set file syslog structured-data
```

5. Specify how security logs need to be processed and exported.

```
[edit]
root@host#set security log mode event
```

RELATED DOCUMENTATION

Sample Code Audits of Configuration Changes | 57

Sample Code Audits of Configuration Changes

IN THIS SECTION

This sample code audits all changes to the configuration secret data and sends the logs to a file named Audit-File:

```
[edit system]
    syslog {
    file Audit-File {
    authorization info;
    change-log info;
    interactive-commands info;
    }
      }
```

This sample code expands the scope of the minimum audit to audit all changes to the configuration, not just secret data, and sends the logs to a file named Audit-File:

```
[edit system]
    syslog
```

```
{
    file Audit-File
    {
    any any;
    51
    authorization info;
    change-log any;
    interactive-commands info;
    kernel info;
    pfe info;
    }
}
```

Example: System Logging of Configuration Changes

This example shows a sample configuration and makes changes to users and secret data. It then shows the information sent to the audit server when the secret data is added to the original configuration and committed with the load command.

```
[edit system]
    location {
    country-code US;
    building B1;
    }
    ...
    login {
    message "UNAUTHORIZED USE OF THIS ROUTER\n\tIS STRICTLY PROHIBITED!";
   user admin {
    uid 2000;
    class super-user;
    authentication {
    encrypted-password “$ABC123”;
    # SECRET-DATA
    }
    }
    password {
    format sha256;
   }
    }
```

```
    radius-server 192.0.2.15 {
    secret “$ABC123” # SECRET-DATA
    }
    services {
    ssh;
    }
    syslog {
    user *{
    52
    any emergency;
    }
    file messages {
    any notice;
    authorization info;
    }
    file interactive-commands {
    interactive-commands any;
    }
    }
    ...
    ...
```

The new configuration changes the secret data configuration statements and adds a new user.

```
user@host# show | compare
      [edit system login user admin authentication]
      - encrypted-password “$ABC123”; # SECRET-DATA
      + encrypted-password “$ABC123”; # SECRET-DATA
      [edit system login]
      + user admin2 {
      + uid 2001;
      + class operator;
      + authentication {
      + encrypted-password “$ABC123”;
      # SECRET-DATA
      + }
      + }
      [edit system radius-server 192.0.2.15]
      - secret “$ABC123”; # SECRET-DATA
      + secret “$ABC123”; # SECRET-DATA
```

Table 6: Audit Records for all Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FAU_GEN.1	None	None	
FAU_STG.1	None	None	
FAU_STG_EXT.1	None	None	
FCS_CKM.1	None	None	
FCS_CKM.2	None	None	
FCS_CKM.4	None	None	
FCS_COP.1/ DataEncryption	None	None	
FCS_COP.1/SigGen	None	None	
FCS_COP.1/Hash	None	None	
FCS_COP.1/KeyedHash	None	None	

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.	<27>1 2022-07-25T07:40:00.019Z Proliant_Node0 kmd 20805 - - IKE negotiation failed with error: No proposal chosen. IKE Version: 2, VPN: ike-vpn-devices Gateway: gw-b, Local: 10.1.5.129/500, Remote: 10.1.5.29/500, Local IKE-ID: Not-Available, Remote IKE-ID: Not-Available, VR-ID: 0: Role: Initiator <27>1 2022-07-25T07:40:00.020Z Proliant_Node0 kmd 20805 - - IPSec negotiation failed with error: No proposal chosen. IKE Version: 2, VPN: ike-vpn-devices Gateway: gw-b, Local: 10.1.5.129/500, Remote: 10.1.5.29/500, Local IKE-ID: Not-Available, Remote IKE-ID: Not-Available, VR-ID: 0

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity of new/removed time server	<182>1 2023-02-22T14:23:37.828Z Proliant_Node0 mgd 12129 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[system ntp server 10.1.1.160\]" delimiter="" value=""] User 'acumensec' set: [system ntp server 10.1.1.160] <182>1 2023-02-22T14:24:54.508Z Proliant_Node0 mgd 12129 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="delete" pathname="[system ntp server 10.1.1.160\]" delimiter="" value=""] User 'acumensec' delete: [system ntp server 10.1.1.160]
FCS_RBG_EXT.1	None	None	

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure	<35>1 2021-09-27T09:41:37.763Z VSRX_TOE sshd 70783 - - error: PAM: Authentication error for acumensec from 10.1.2.146 <37>1 2021-09-27T09:41:37.763Z VSRX_TOE sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.129 username="acumensec" source-address="10.1.2.146"] Login failed for user 'acumensec' from host '10.1.2.146'
FDP_RIP.2	None	None	
FFW_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface	Time of Log: 2022-11-29 10:25:35 UTC, Filter: pfe, Filter action: discard, Name of interface: reth1.0 Name of protocol: TCP, Packet Length: 40, Source address: 10.1.1.146:20, Destination address: 10.1.3.161:1035

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FFW_RUL_EXT.2	Dynamical definition of rule Establishment of a session	None	**Dynamical definition of rule** <182>1 2023-02-22T07:12:41.900Z Proliant_Node0 mgd 13150 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter TCP-ports term allow from protocol tcp\]" delimiter="" value=""] User 'acumensec' set: [firewall filter TCP-ports term allow from protocol tcp] <182>1 2023-02-22T07:12:41.901Z Proliant_Node0 mgd 13150 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter TCP-ports term allow from port 0-1024\]" delimiter="" value=""] User 'acumensec' set: [firewall filter TCP-ports term allow from port 0-1024] <182>1 2023-02-22T07:12:49.599Z Proliant_Node0 mgd 13150 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			username="acumensec" action="set" pathname="[firewall filter TCP-ports term allow then\]" delimiter="" data="unconfigured" value="accept"] User 'acumensec' set: [firewall filter TCP-ports term allow then] unconfigured -- "accept" <182>1 2023-02-22T07:12:49.600Z Proliant_Node0 mgd 13150 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter TCP-ports term allow then\]" delimiter="" data="unconfigured" value="log"] User 'acumensec' set: [firewall filter TCP-ports term allow then] unconfigured -- "log" <182>1 2023-02-22T07:13:26.841Z Proliant_Node0 mgd 13150 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter TCP-ports term deny from protocol tcp\]" delimiter="" value=""]

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			User 'acumensec' set: [firewall filter TCP-ports term deny from protocol tcp] <182>1 2023-02-22T07:13:26.841Z Proliant_Node0 mgd 13150 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter TCP-ports term deny from port 1025-65535\]" delimiter="" value=""] User 'acumensec' set: [firewall filter TCP-ports term deny from port 1025-65535] <182>1 2023-02-22T07:13:33.651Z Proliant_Node0 mgd 13150 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter TCP-ports term deny then discard\]" delimiter="" value=""] User 'acumensec' set: [firewall filter TCP-ports term deny then discard] <182>1 2023-02-22T07:13:36.999Z Proliant_Node0 mgd 13150

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter TCP-ports term deny then \]" delimiter="" data="unconfigured" value="log"] User 'acumensec' set: [firewall filter TCP-ports term deny then] unconfigured -- "log" **Establishment of a session** Time of Log: 2022-09-14 06:03:10 UTC, Filter: pfe, Filter action: accept, Name of interface: reth1.0 Name of protocol: TCP, Packet Length: 52, Source address: 10.1.1. 146:38452, Destination address: 10.1.3.161:1023 Time of Log: 2022-09-14 06:11:57 UTC, Filter: pfe, Filter action : discard, Name of interface: reth1.0 Name of protocol: TCP, Packet Length: 60, Source address: 10.1.1 .146:58594, Destination address: 10.1.3.161:1025

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address)	<37>1 2021-09-29T10:45:55.798Z VSRX_TOE sshd 14027 LIBJNX_LOGIN_ACCOUNT_LOCKED [junos@2636.1.1.1.2.129 username="acumensec"] Account for user 'acumensec' has been locked out from logins <38>1 2021-09-29T10:45:55.799Z VSRX_TOE sshd 14027 - - Failed password for acumensec from 10.1.2.146 port 33362 ssh2 <37>1 2021-09-29T10:46:20.818Z VSRX_TOE sshd - SSHD_LOGIN_ATTEMPTS_THRESHOLD [junos@2636.1.1.1.2.129 limit="5" username="acumensec"] Threshold for unsuccessful authentication attempts (5) reached by user 'acumensec' <38>1 2021-09-29T10:46:20.818Z VSRX_TOE sshd 14028 - - Disconnecting authenticating user acumensec 10.1.2.146 port 33362: Too many

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			password failures for acumensec
FIA_PMG_EXT.1	None	None	

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FIA_UIA_EXT.1	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)	**Local Successful Login** <37>1 2021-09-29T12:39:25.733Z VSRX_TOE login 20829 - - Login attempt for user acumensec from host [unknown] <38>1 2021-09-29T12:39:31.884Z VSRX_TOE login 20829 LOGIN_INFORMATION [junos@2636.1.1.1.2.129 username="acumensec" hostname="[unknown\]" tty-name="ttyv0"] User acumensec logged in from host [unknown] on device ttyv0 <190>1 2021-09-29T12:39:32.226Z VSRX_TOE mgd 20847 UI_AUTH_EVENT [junos@2636.1.1.1.2.129 username="acumensec" authentication-level="j-super-user"] Authenticated user 'acumensec' assigned to class 'j-super-user' <190>1 2021-09-29T12:39:32.226Z VSRX_TOE mgd 20847 UI_LOGIN_EVENT [junos@2636.1.1.1.2.129 username="acumensec" class-name="j-super-user" local-peer=""

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			pid="20847" ssh-connection="" client-mode="cli"] User 'acumensec' login, class 'j-super-user' [20847], ssh-connection '', client-mode 'cli' **Local Unsuccessful Login** <37>1 2021-09-29T12:33:50.765Z VSRX_TOE login 20513 - - Login attempt for user acumensec from host [unknown] <35>1 2021-09-29T12:33:56.858Z VSRX_TOE login 20513 LOGIN_PAM_AUTHENTICATION_ERROR [junos@2636.1.1.1.2.129 username="acumensec"] Failed password for user acumensec <37>1 2021-09-29T12:33:56.859Z VSRX_TOE login 20513 LOGIN_FAILED [junos@2636.1.1.1.2.129 username="acumensec" source-address="ttyv0"] Login failed for user acumensec from host ttyv0 **Remote Successful Password-Based Login**

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			<38>1 2021-09-29T12:45:01.580Z VSRX_TOE sshd 21135 - - Accepted keyboard-interactive/pam for acumensec from 10.1.2.146 port 33504 ssh2 <190>1 2021-09-29T12:45:01.915Z VSRX_TOE mgd 21148 UI_AUTH_EVENT [junos@2636.1.1.1.2.129 username="acumensec" authentication-level="j-super-user"] Authenticated user 'acumensec' assigned to class 'j-super-user' <190>1 2021-09-29T12:45:01.915Z VSRX_TOE mgd 21148 UI_LOGIN_EVENT [junos@2636.1.1.1.2.129 username="acumensec" class-name="j-super-user" local-peer="" pid="21148" ssh-connection="10.1.2.146 33504 10.1.2.129 22" client-mode="cli"] User 'acumensec' login, class 'j-super-user' [21148], ssh-connection '10.1.2.146 33504 10.1.2.129 22', client-mode 'cli' **Remote Unsuccessful Password-Based Login**

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			<35>1 2021-09-29T12:43:19.559Z VSRX_TOE sshd 21040 - - error: PAM: Authentication error for acumensec from 10.1.2.146 <37>1 2021-09-29T12:43:19.559Z VSRX_TOE sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.129 username="acumensec" source-address="10.1.2.146"] Login failed for user 'acumensec' from host '10.1.2.146' **Remote Successful Public Key-Based Login** <38>1 2021-10-07T11:03:56.574Z VSRX_TOE sshd 35243 - - Accepted publickey for tester from 10.1.2.146 port 60712 ssh2: ECDSA SHA256:i2HeKO8gDAEyR1gz0JRv4Pqi/OCoXLzcj8calZLBxW4 <190>1 2021-10-07T11:03:56.931Z VSRX_TOE mgd 35247 UI_AUTH_EVENT [junos@2636.1.1.1.2.129 username="tester" authentication-level="j-super-user"]

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			Authenticated user 'tester' assigned to class 'j-super-user' <190>1 2021-10-07T11:03:56.931Z VSRX_TOE mgd 35247 UI_LOGIN_EVENT [junos@2636.1.1.1.2.129 username="tester" class-name="j-super-user" local-peer="" pid="35247" ssh-connection="10.1.2.146 60712 10.1.2.129 22" client-mode="cli"] User 'tester' login, class 'j-super-user' [35247], ssh-connection '10.1.2.146 60712 10.1.2.129 22', client-mode 'cli' **Remote Unsuccessful Public Key-Based Login** <35>1 2021-10-07T10:59:02.307Z VSRX_TOE sshd 34503 - - error: PAM: Authentication error for tester from 10.1.2.146 <37>1 2021-10-07T10:59:02.308Z VSRX_TOE sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.129 username="tester" source-address="10.1.2.146"] Login failed for user

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			'tester' from host '10.1.2.146'

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FIA_UAU_EXT.2	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)	**Local Successful Login** <37>1 2021-09-29T12:39:25.733Z VSRX_TOE login 20829 - - Login attempt for user acumensec from host [unknown] <38>1 2021-09-29T12:39:31.884Z VSRX_TOE login 20829 LOGIN_INFORMATION [junos@2636.1.1.1.2.129 username="acumensec" hostname="[unknown\]" tty-name="ttyv0"] User acumensec logged in from host [unknown] on device ttyv0 <190>1 2021-09-29T12:39:32.226Z VSRX_TOE mgd 20847 UI_AUTH_EVENT [junos@2636.1.1.1.2.129 username="acumensec" authentication-level="j-super-user"] Authenticated user 'acumensec' assigned to class 'j-super-user' <190>1 2021-09-29T12:39:32.226Z VSRX_TOE mgd 20847 UI_LOGIN_EVENT [junos@2636.1.1.1.2.129 username="acumensec" class-name="j-super-user" local-peer=""

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			pid="20847" ssh-connection="" client-mode="cli"] User 'acumensec' login, class 'j-super-user' [20847], ssh-connection '', client-mode 'cli' **Local Unsuccessful Login** <37>1 2021-09-29T12:33:50.765Z VSRX_TOE login 20513 - - Login attempt for user acumensec from host [unknown] <35>1 2021-09-29T12:33:56.858Z VSRX_TOE login 20513 LOGIN_PAM_AUTHENTICATION_ERROR [junos@2636.1.1.1.2.129 username="acumensec"] Failed password for user acumensec <37>1 2021-09-29T12:33:56.859Z VSRX_TOE login 20513 LOGIN_FAILED [junos@2636.1.1.1.2.129 username="acumensec" source-address="ttyv0"] Login failed for user acumensec from host ttyv0 **Remote Successful Login** <38>1 2021-09-29T12:45:01.58

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			0Z VSRX_TOE sshd 21135 - - Accepted keyboard-interactive/pam for acumensec from 10.1.2.146 port 33504 ssh2 <190>1 2021-09-29T12:45:01.915Z VSRX_TOE mgd 21148 UI_AUTH_EVENT [junos@2636.1.1.1.2.129 username="acumensec" authentication-level="j-super-user"] Authenticated user 'acumensec' assigned to class 'j-super-user' <190>1 2021-09-29T12:45:01.915Z VSRX_TOE mgd 21148 UI_LOGIN_EVENT [junos@2636.1.1.1.2.129 username="acumensec" class-name="j-super-user" local-peer="" pid="21148" ssh-connection="10.1.2.146 33504 10.1.2.129 22" client-mode="cli"] User 'acumensec' login, class 'j-super-user' [21148], ssh-connection '10.1.2.146 33504 10.1.2.129 22', client-mode 'cli' **Remote Unsuccessful Login** <35>1 2021-09-29T12:43:19.55

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			9Z VSRX_TOE sshd 21040 - - error: PAM: Authentication error for acumensec from 10.1.2.146 <37>1 2021-09-29T12:43:19.559Z VSRX_TOE sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.129 username="acumensec" source-address="10.1.2.146"] Login failed for user 'acumensec' from host '10.1.2.146' **Remote Successful Public Key-Based Login** <38>1 2021-10-07T11:03:56.574Z VSRX_TOE sshd 35243 - - Accepted publickey for tester from 10.1.2.146 port 60712 ssh2: ECDSA SHA256:i2HeKO8gDAEyR1gz0JRv4Pqi/OCoXLzcj8calZLBxW4 <190>1 2021-10-07T11:03:56.931Z VSRX_TOE mgd 35247 UI_AUTH_EVENT [junos@2636.1.1.1.2.129 username="tester" authentication-level="j-super-user"] Authenticated user 'tester' assigned to class 'j-super-user'

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			<190>1 2021-10-07T11:03:56.931Z VSRX_TOE mgd 35247 UI_LOGIN_EVENT [junos@2636.1.1.1.2.129 username="tester" class-name="j-super-user" local-peer="" pid="35247" ssh-connection="10.1.2.146 60712 10.1.2.129 22" client-mode="cli"] User 'tester' login, class 'j-super-user' [35247], ssh-connection '10.1.2.146 60712 10.1.2.129 22', client-mode 'cli' **Remote Unsuccessful Public Key-Based Login** <35>1 2021-10-07T10:59:02.307Z VSRX_TOE sshd 34503 - - error: PAM: Authentication error for tester from 10.1.2.146 <37>1 2021-10-07T10:59:02.308Z VSRX_TOE sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.129 username="tester" source-address="10.1.2.146"] Login failed for user 'tester' from host '10.1.2.146'
FIA_UAU.7	None	None	

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement, or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	**Unsuccessful attempt to validate a certificate** <27>1 2022-12-07T07:13:12.436Z Proliant_Node0 pkid 20720 PKID_CRL_CERTIFICATE_REVOKED [junos@2636.1.1.1.2.129 argument1="/C=US/O=Acumen/OU=CC/CN=AcumenICA" argument2="6b92a1eaeb70ca59"] Certificate /C=US/O=Acumen/OU=CC/CN=AcumenICA with serial number 0x6b92a1eaeb70ca59 is revoked <27>1 2022-12-07T07:13:12.437Z Proliant_Node0 kmd 85673 KMD_PEER_CERT_VERIFY_FAILED [junos@2636.1.1.1.2.129 gateway-name="gw-b" local-address="10.1.5.129" local-port="500" remote-address="10.1.5.251" remote-port="500" name="10.1.5.129" peer-name="10.1.5.251" vrrp-group-id="0"] Failed peer certificate verification for Gateway: gw-b, Local: 10.1.5.129/500, Remote: 10.1.5.251/500, Local

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			IKE-ID: 10.1.5.129, Remote IKE-ID: 10.1.5.251, VR id: 0 **Addition of trust anchor** <182>1 2023-02-22T07:21:57.600Z Proliant_Node0 mgd 13150 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security pki ca-profile AcumenCA ca-identity\]" delimiter="" data="unconfigured" value="AcumenCA"] User 'acumensec' set: [security pki ca-profile AcumenCA ca-identity] unconfigured -- "AcumenCA" <29>1 2023-02-22T07:22:24.769Z Proliant_Node0 pkid 11250 PKID_PV_CERT_LOAD [junos@2636.1.1.1.2.129 type-string="AcumenCA"] Certificate AcumenCA has been successfully loaded **Removal of trust anchor** <182>1 2023-02-22T07:24:47.471Z Proliant_Node0 mgd 13150 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			username="acumensec" action="delete" pathname="[security pki ca-profile AcumenCA\]" delimiter="" value=""] User 'acumensec' delete: [security pki ca-profile AcumenCA] <29>1 2023-02-22T07:24:56.433Z Proliant_Node0 pkid 11250 PKID_PV_CERT_DEL [junos@2636.1.1.1.2.129 type-string="AcumenCA"] Certificate deletion has occurred for AcumenCA
FIA_X509_EXT.2	None	None	
FIA_X509_EXT.3	None	None	
FMT_MOF.1/Functions	None	None	

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None	<190>1 2023-02-17T11:08:28.481Z Proliant_Node0 mgd 5002 UI_CHILD_START [junos@2636.1.1.1.2.129 command="/usr/libexec/ui/package"] Starting child '/usr/libexec/ui/package' <29>1 2023-02-17T11:08:28.484Z Proliant Node0 mgd 9302 - - /usr/libexec/ui/package -X update -reboot /var/home/acumensec/junos-install-vsrx3-x86-64-22.2R1.9.tgz
FMT_MOF.1/Services	None	None	
FMT_MTD.1/CoreData	None	None	
FMT_MTD.1/CryptoKeys	None	None	

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FMT_SMF.1 FMT_SMF.1/VPN FMT_SMF.1/FFW	All management activities of TSF data (including creation, modification and deletion of firewall rules).	None	**Ability to administer the TOE locally and remotely** Local <37>1 2021-09-29T12:39:25.733Z VSRX_TOE login 20829 - - Login attempt for user acumensec from host [unknown] <38>1 2021-09-29T12:39:31.884Z VSRX_TOE login 20829 LOGIN_INFORMATION [junos@2636.1.1.1.2.129 username="acumensec" hostname="[unknown\]" tty-name="ttyv0"] User acumensec logged in from host [unknown] on device ttyv0 <190>1 2021-09-29T12:39:32.226Z VSRX_TOE mgd 20847 UI_AUTH_EVENT [junos@2636.1.1.1.2.129 username="acumensec" authentication-level="j-super-user"] Authenticated user 'acumensec' assigned to class 'j-super-user' <190>1 2021-09-29T12:39:32.226Z VSRX_TOE mgd 20847 UI_LOGIN_EVENT [junos@2636.1.1.1.2.129

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			username="acumensec" class-name="j-super-user" local-peer="" pid="20847" ssh-connection="" client-mode="cli"] User 'acumensec' login, class 'j-super-user' [20847], ssh-connection '', client-mode 'cli' Remote <38>1 2021-09-29T12:45:01.580Z VSRX_TOE sshd 21135 - - Accepted keyboard-interactive/pam for acumensec from 10.1.2.146 port 33504 ssh2 <190>1 2021-09-29T12:45:01.915Z VSRX_TOE mgd 21148 UI_AUTH_EVENT [junos@2636.1.1.1.2.129 username="acumensec" authentication-level="j-super-user"] Authenticated user 'acumensec' assigned to class 'j-super-user' <190>1 2021-09-29T12:45:01.915Z VSRX_TOE mgd 21148 UI_LOGIN_EVENT [junos@2636.1.1.1.2.129 username="acumensec" class-name="j-super-user" local-peer=""

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			pid="21148" ssh-connection="10.1.2.146 33504 10.1.2.129 22" client-mode="cli"] User 'acumensec' login, class 'j-super-user' [21148], ssh-connection '10.1.2.146 33504 10.1.2.129 22', client-mode 'cli' **Ability to configure the access banner** <182>1 2021-10-01T10:58:24.632Z VSRX_TOE mgd 54807 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[system login message\]" delimiter="\"" data="Login message: Only Authorized Users Allowed" value="This is a login message. Warning: Only authorized users allowed !"] User 'acumensec' set: [system login message] "Login message: Only Authorized Users Allowed -- "This is a login message. Warning: Only authorized users allowed !" <182>1 2021-10-01T10:59:15.045Z VSRX_TOE mgd 54807 UI_CFG_AUDIT_SET

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			[junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[system login announcement\]" delimiter="\"" data="This is MOTD banner." value="This is an MOTD banner. \\n This is EXEC banner. \\n"] User 'acumensec' set: [system login announcement] "This is MOTD banner. -- "This is an MOTD banner. \n This is EXEC banner. \n" **Ability to configure the session inactivity time before session termination or locking** <182>1 2021-10-01T09:50:49.070Z VSRX_TOE mgd 48114 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[system login class security-admin idle-timeout\]" delimiter="" data="unconfigured" value="1"] User 'acumensec' set: [system login class security-admin idle-timeout] unconfigured -- "1" <14>1 2021-10-01T09:52:56.15

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			0Z VSRX_TOE -cli - UI_CLI_IDLE_TIMEOUT [junos@2636.1.1.1.2.129 username="acumensec"] Idle timeout for user 'acumensec' exceeded and session terminated **Ability to update the TOE, and to verify the updates using digital signature and [published hash] capability prior to installing those updates** <190>1 2023-02-17T11:08:28.481Z Proliant_Node0 mgd 5002 UI_CHILD_START [junos@2636.1.1.1.2.129 command="/usr/libexec/ui/package"] Starting child '/usr/libexec/ui/package' <29>1 2023-02-17T11:08:28.484Z Proliant Node0 mgd 9302 - - /usr/libexec/ui/package -X update -reboot /var/home/acumensec/junos-install-vsrx3-x86-64-22.2R1.9.tgz <118>1 2023-02-17T11:16:15.726Z Proliant_Node0 kernel - - - Verified os-kernel-prd-x86-64-20220607 signed by PackageProductionECP25

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			6_2022 method ECDSA256+SHA256 <118>1 2023-02-17T11:16:15.726Z Proliant_Node0 kernel - - - Verified os-libs-12-x86-64-20220607 signed by PackageProductionECP256_2022 method ECDSA256+SHA256 <118>1 2023-02-17T11:16:15.726Z Proliant_Node0 kernel - - - Verified os-runtime-x86-64-20220607 signed by PackageProductionECP256_2022 method ECDSA256+SHA256 <118>1 2023-02-17T11:16:15.726Z Proliant_Node0 kernel - - - Verified jail-runtime-x86-32-20220607 signed by PackageProductionECP256_2022 method ECDSA256+SHA256 <118>1 2023-02-17T11:16:15.726Z Proliant_Node0 kernel - - - Verified dsa-x86-64-22.9 signed by PackageProductionECP256_2022 method ECDSA256+SHA256

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			<118>1 2023-02-17T11:16:15.726Z Proliant_Node0 kernel - - - Verified fips-mode-x86-64-20220617 signed by PackageProductionECP256_2022 method ECDSA256+SHA256 **Ability to configure the authentication failure parameters for FIA_AFL.1** <182>1 2023-02-22T10:37:08.552Z Proliant_Node0 mgd 12191 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[system login retry-options tries-before-disconnect\]" delimiter="" data="unconfigured" value="5"] User 'acumensec' set: [system login retry-options tries-before-disconnect] unconfigured -- "5" <182>1 2023-02-22T10:37:08.553Z Proliant_Node0 mgd 12191 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[system login

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			retry-options lockout-period\]" delimiter="" data="unconfigured" value="1"] User 'acumensec' set: [system login retry-options lockout-period] unconfigured -- "1" **Definition of packet filtering rules** <182>1 2023-02-22T07:12:41.900Z Proliant_Node0 mgd 13150 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter TCP-ports term allow from protocol tcp\]" delimiter="" value=""] User 'acumensec' set: [firewall filter TCP-ports term allow from protocol tcp] <182>1 2023-02-22T07:12:49.599Z Proliant_Node0 mgd 13150 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter TCP-ports term allow then\]" delimiter="" data="unconfigured" value="accept"] User

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			'acumensec' set: [firewall filter TCP-ports term allow then] unconfigured -- "accept” **Association of packet filtering rules to network interfaces** <182>1 2023-02-22T10:46:34.748Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[interfaces reth1 unit 0 family inet filter input\]" delimiter="" data="unconfigured" value="TCP_filter"] User 'acumensec' set: [interfaces reth1 unit 0 family inet filter input] unconfigured -- "TCP_filter" **Ordering of packet filtering rules by priority** <182>1 2023-02-22T11:16:15.344Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall family inet filter dst-allow term allow then\]" delimiter=""

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			data="unconfigured" value="accept"] User 'acumensec' set: [firewall family inet filter dst-allow term allow then] unconfigured -- "accept" <182>1 2023-02-22T11:16:39.401Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall family inet filter dst-allow term deny then discard\]" delimiter="" value=""] User 'acumensec' set: [firewall family inet filter dst-allow term deny then discard] **Ability to configure firewall rules** <182>1 2023-02-22T07:12:41.900Z Proliant_Node0 mgd 13150 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter TCP-ports term allow from protocol tcp\]" delimiter="" value=""] User 'acumensec' set: [firewall filter TCP-ports term allow from protocol tcp]

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			<182>1 2023-02-22T07:12:49.599Z Proliant_Node0 mgd 13150 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter TCP-ports term allow then\]" delimiter="" data="unconfigured" value="accept"] User 'acumensec' set: [firewall filter TCP-ports term allow then] unconfigured -- "accept" **Enable, disable signatures applied to sensor interfaces, and determine the behavior of IPS functionality** Signature enabled <14>1 2022-08-02T11:50:20.785Z Proliant_Node0 RT_FLOW - RT_FLOW_SESSION_CREATE [junos@2636.1.1.1.2.129 source-address="10.1.1.146" source-port="22362" destination-address="10.1.5.29" destination-port="1" connection-tag="0" service-name="icmp" nat-source-

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			address="10.1.1.146" nat-source-port="22362" nat-destination-address="10.1.5.29" nat-destination-port="1" nat-connection-tag="0" src-nat-rule-type="N/A" src-nat-rule-name="N/A" dst-nat-rule-type="N/A" dst-nat-rule-name="N/A" protocol-id="1" policy-name="vpn-bypass" source-zone-name="trust" destination-zone-name="untrust" session-id="348283" username="N/A" roles="N/A" packet-incoming-interface="reth1.0" application="UNKNOWN" nested-application="UNKNOWN" encrypted="UNKNOWN" application-category="N/A" application-sub-category="N/A" application-risk="-1" application-characteristics="N/A" src-vrf-grp="N/A" dst-vrf-grp="N/A" tunnel-inspection="Off" tunnel-inspection-policy-set="root" source-tenant="N/A" destination-service="N/A"] session created

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			10.1.1.146/22362->10.1.5.29/1 0x0 icmp 10.1.1.146/22362->10.1.5.29/1 0x0 N/A N/A N/A N/A 1 vpn-bypass trust untrust 348283 N/A(N/A) reth1.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1 N/A N/A N/A Off root N/A N/A <14>1 2022-08-02T11:50:20.786Z Proliant_Node0 RT_IDP - IDP_ATTACK_LOG_EVENT [junos@2636.1.1.1.2.129 epoch-time="1659440989" message-type="SIG" source-address="10.1.1.146" source-port="22355" destination-address="10.1.5.29" destination-port="25" protocol-name="ICMP" service-name="SERVICE_IDP" application-name="NONE" rule-name="1" rulebase-name="IPS" policy-name="IDP_Source" export-id="1048576" repeat-count="2" action="DROP" threat-severity="INFO" attack-name="IPv4_source" nat-

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			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="trust" source-interface-name="reth1.0" destination-zone-name="untrust" destination-interface-name="reth2.0" packet-log-id="0" alert="yes" username="N/A" roles="N/A" xff-header="N/A" cve-id="N/A" session-id="348238" message="-"] IDP: at 1659440989, SIG Attack log <10.1.1.146/22355->10.1.5.29/25> for ICMP protocol and service SERVICE_IDP application NONE by rule 1 of rulebase IPS in policy IDP_Source. attack: id=1048576, repeat=2, action=DROP, threat-severity=INFO, name=IPv4_source, NAT <0.0.0.0:0->0.0.0.0:0>, time-elapsed=0, inbytes=0, outbytes=0, inpackets=0, outpackets=0,

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			intf:trust:reth1.0->untrust:reth2.0, packet-log-id: 0, alert=yes, username=N/A, roles=N/A, xff-header=N/A, cve-id=N/A, session-id=348238 and misc-message - <14>1 2022-08-02T11:50:20.786Z Proliant_Node0 RT_IDP - IDP_ATTACK_LOG_EVENT [junos@2636.1.1.1.2.129 epoch-time="1659440989" message-type="SIG" source-address="10.1.1.146" source-port="22355" destination-address="10.1.5.29" destination-port="25" protocol-name="ICMP" service-name="SERVICE_IDP" application-name="NONE" rule-name="1" rulebase-name="IPS" policy-name="IDP_Source" export-id="1048576" repeat-count="2" action="DROP" threat-severity="INFO" attack-name="IPv4_source" nat-source-address="0.0.0.0" nat-source-port="0" nat-destination-

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			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="trust" source-interface-name="reth1.0" destination-zone-name="untrust" destination-interface-name="reth2.0" packet-log-id="0" alert="yes" username="N/A" roles="N/A" xff-header="N/A" cve-id="N/A" session-id="348238" message="-"] IDP: at 1659440989, SIG Attack log <10.1.1.146/22355->10.1.5.29/25> for ICMP protocol and service SERVICE_IDP application NONE by rule 1 of rulebase IPS in policy IDP_Source. attack: id=1048576, repeat=2, action=DROP, threat-severity=INFO, name=IPv4_source, NAT <0.0.0.0:0->0.0.0.0:0>, time-elapsed=0, inbytes=0, outbytes=0, inpackets=0, outpackets=0, intf:trust:reth1.0->untrust:reth2.0, packet-log-id: 0, alert=yes,

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			username=N/A, roles=N/A, xff-header=N/A, cve-id=N/A, session-id=348238 and misc-message - Signature disabled <14>1 2022-08-02T14:24:46.700Z Proliant_Node0 RT_FLOW - RT_FLOW_SESSION_CREATE [junos@2636.1.1.1.2.129 source-address="10.1.1.146" source-port="22796" destination-address="10.1.5.29" destination-port="1" connection-tag="0" service-name="icmp" nat-source-address="10.1.1.146" nat-source-port="22796" nat-destination-address="10.1.5.29" nat-destination-port="1" nat-connection-tag="0" src-nat-rule-type="N/A" src-nat-rule-name="N/A" dst-nat-rule-type="N/A" dst-nat-rule-name="N/A" protocol-id="1" policy-name="vpn-bypass" source-zone-name="trust" destination-zone-name="untrust" session-id="357681" username="N/A" roles="N/A" packet-

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			incoming-interface="reth1.0" application="UNKNOWN" nested-application="UNKNOWN" encrypted="UNKNOWN" application-category="N/A" application-sub-category="N/A" application-risk="-1" application-characteristics="N/A" src-vrf-grp="N/A" dst-vrf-grp="N/A" tunnel-inspection="Off" tunnel-inspection-policy-set="root" source-tenant="N/A" destination-service="N/A"] session created 10.1.1.146/22796->10.1.5.29/1 0x0 icmp 10.1.1.146/22796->10.1.5.29/1 0x0 N/A N/A N/A N/A 1 vpn-bypass trust untrust 357681 N/A(N/A) reth1.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1 N/A N/A N/A Off root N/A N/A **Modify these parameters that define the network traffic to be collected and analyzed:**

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			• **Source IP addresses (host address and network address)** <182>1 2023-02-22T11:44:10.082Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack IPv4-src attack-type signature protocol ipv4 source match\]" delimiter="" data="unconfigured" value="equal"] User 'acumensec' set: [security idp custom-attack IPv4-src attack-type signature protocol ipv4 source match] unconfigured -- "equal" <182>1 2023-02-22T11:44:10.083Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set"

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			pathname="[security idp custom-attack IPv4-src attack-type signature protocol ipv4 source value\]" delimiter="" data="unconfigured" value="10.1.1.146"] User 'acumensec' set: [security idp custom-attack IPv4-src attack-type signature protocol ipv4 source value] unconfigured -- "10.1.1.146" • **Destination IP addresses (host address and network** <182>1 2023-02-22T11:49:26.089Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack IPv4-dst attack-type signature protocol ipv4 destination value \]" delimiter="" data="unconfigured" value="10.1.3.161"] User 'acumensec' set: [security idp custom-

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			attack IPv4-dst attack-type signature protocol ipv4 destination value] unconfigured -- "10.1.3.161" • **Source port (TCP and UDP)** <182>1 2023-02-22T11:52:32.476Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack TCP-src attack-type signature protocol tcp source-port value\]" delimiter="" data="unconfigured" value="1026"] User 'acumensec' set: [security idp custom-attack TCP-src attack-type signature protocol tcp source-port value] unconfigured -- "1026" <182>1 2023-02-22T11:54:44.137Z

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack UDP-src attack-type signature protocol udp source-port value\]" delimiter="" data="unconfigured" value="1035"] User 'acumensec' set: [security idp custom-attack UDP-src attack-type signature protocol udp source-port value] unconfigured -- "1035" • **Destination port (TCP and UDP)** <182>1 2023-02-22T11:58:07.093Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack TCP-dst attack-type

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			signature protocol tcp destination-port value \]" delimiter="" data="unconfigured" value="1025"] User 'acumensec' set: [security idp custom-attack TCP-dst attack-type signature protocol tcp destination-port value] unconfigured -- "1025" <182>1 2023-02-22T11:59:43.020Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack UDP-dst attack-type signature protocol udp destination-port value \]" delimiter="" data="unconfigured" value="1036"] User 'acumensec' set: [security idp custom-attack UDP-dst attack-type signature protocol udp destination-port value] unconfigured -- "1036"

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			• **• Protocol (IPv4 and IPv6)** <182>1 2023-02-22T12:13:46.343Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack Proto-IPv4 attack-type signature protocol ipv4 protocol value\]" delimiter="" data="unconfigured" value="4"] User 'acumensec' set: [security idp custom-attack Proto-IPv4 attack-type signature protocol ipv4 protocol value] unconfigured -- "4" <182>1 2023-02-22T12:20:32.925Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			idp custom-attack Proto-IPv6 attack-type signature protocol ipv6 next-header value\]" delimiter="" data="unconfigured" value="41"] User 'acumensec' set: [security idp custom-attack Proto-IPv6 attack-type signature protocol ipv6 next-header value] unconfigured -- "41" • **ICMP type and code** <182>1 2023-02-22T12:26:20.596Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack ICMP-type attack-type signature protocol icmp type value\]" delimiter="" data="unconfigured" value="8"] User 'acumensec' set: [security idp custom-attack ICMP-type attack-type signature

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			protocol icmp type value] unconfigured -- "8" <182>1 2023-02-22T12:27:37.168Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack ICMP-code attack-type signature protocol icmp code value\]" delimiter="" data="unconfigured" value="1"] User 'acumensec' set: [security idp custom-attack ICMP-code attack-type signature protocol icmp code value] unconfigured -- "1" **Update (import) signatures** <182>1 2022-08-03T07:29:40.597Z Proliant_Node0 mgd 44488 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			screen ids-option Pre-existing\]" delimiter="" data="unconfigured" value="alarm-without-drop"] User 'acumensec' set: [security screen ids-option Pre-existing] unconfigured -- "alarm-without-drop" <182>1 2022-08-03T07:29:44.111Z Proliant_Node0 mgd 44488 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security screen ids-option Pre-existing ip\]" delimiter="" data="unconfigured" value="tear-drop"] User 'acumensec' set: [security screen ids-option Pre-existing ip] unconfigured -- "tear-drop" **Create custom signatures** <182>1 2022-08-05T12:45:03.832Z Proliant_Node0 mgd 150 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack IPv4-version severity\]" delimiter="" data="unconfigured"

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			value="info"] User 'acumensec' set: [security idp custom-attack IPv4-version severity] unconfigured -- "info" <182>1 2022-08-05T12:45:03.832Z Proliant_Node0 mgd 150 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack IPv4-version attack-type signature context\]" delimiter="" data="unconfigured" value="packet"] User 'acumensec' set: [security idp custom-attack IPv4-version attack-type signature context] unconfigured -- "packet" <182>1 2022-08-05T12:45:03.832Z Proliant_Node0 mgd 150 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack IPv4-version attack-type signature direction\]" delimiter="" data="unconfigured" value="any"] User 'acumensec' set: [security idp custom-attack IPv4-

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			version attack-type signature direction] unconfigured -- "any" <182>1 2022-08-05T12:45:03.833Z Proliant_Node0 mgd 150 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack IPv4-version attack-type signature protocol ipv4 protocol match\]" delimiter="" data="unconfigured" value="equal"] User 'acumensec' set: [security idp custom-attack IPv4-version attack-type signature protocol ipv4 protocol match] unconfigured -- "equal" <182>1 2022-08-05T12:45:03.833Z Proliant_Node0 mgd 150 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack IPv4-version attack-type signature protocol ipv4 protocol value\]" delimiter="" data="unconfigured" value="4"] User 'acumensec' set: [security

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			idp custom-attack IPv4-version attack-type signature protocol ipv4 protocol value] unconfigured -- "4" **Configure anomaly detection** <182>1 2022-08-03T07:37:10.470Z Proliant_Node0 mgd 44488 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall policer policer-throughput\]" delimiter="" data="unconfigured" value="filter-specific"] User 'acumensec' set: [firewall policer policer-throughput] unconfigured -- "filter-specific" <182>1 2022-08-03T07:37:10.471Z Proliant_Node0 mgd 44488 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall policer policer-throughput if-exceeding \]" delimiter="" value=""] User 'acumensec' set: [firewall policer policer-throughput if-exceeding]

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			<182>1 2022-08-03T07:37:10.471Z Proliant_Node0 mgd 44488 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall policer policer-throughput if-exceeding bandwidth-limit\]" delimiter="" data="unconfigured" value="32k"] User 'acumensec' set: [firewall policer policer-throughput if-exceeding bandwidth-limit] unconfigured -- "32k" <182>1 2022-08-03T07:37:10.471Z Proliant_Node0 mgd 44488 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall policer policer-throughput if-exceeding burst-size-limit\]" delimiter="" data="unconfigured" value="1500"] User 'acumensec' set: [firewall policer policer-throughput if-exceeding burst-size-limit] unconfigured -- "1500"

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			<182>1 2022-08-03T07:37:21.158Z Proliant_Node0 mgd 44488 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall policer policer-throughput then\]" delimiter="" data="unconfigured" value="discard"] User 'acumensec' set: [firewall policer policer-throughput then] unconfigured -- "discard" **Enable and disable actions to be taken when signature or anomaly matches are detected** <182>1 2023-02-22T13:04:26.115Z Proliant_Node0 mgd 12129 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall policer policer-throughput then\]" delimiter="" data="unconfigured" value="discard"] User 'acumensec' set: [firewall policer policer-throughput then] unconfigured -- "discard"

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			<182>1 2023-02-22T13:05:22.198Z Proliant_Node0 mgd 12129 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="delete" pathname="[firewall policer policer-throughput then\]" delimiter="\"" value="discard"] User 'acumensec' delete: [firewall policer policer-throughput then] "discard **Modify thresholds that trigger IPS reactions** <182>1 2022-08-04T12:41:57.552Z Proliant_Node0 mgd 32710 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[services rpm probe owner test threshold-test target address\]" delimiter="" data="unconfigured" value="10.1.3.28"] User 'acumensec' set: [services rpm probe owner test threshold-test target address] unconfigured --"10.1.3.28" <182>1 2022-08-04T12:42:00.64

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			6Z Proliant_Node0 mgd 32710 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[services rpm probe owner test threshold-test thresholds rtt\]" delimiter="" data="unconfigured" value="50"] User 'acumensec' set: [services rpm probe owner test threshold-test thresholds rtt] unconfigured -- "50" **Modify the duration of traffic blocking actions** <182>1 2023-02-22T13:11:01.830Z Proliant_Node0 mgd 12129 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[schedulers scheduler schedule-tuesday tuesday start-time 16:00 stop-time 16:30\]" delimiter="" value=""] User 'acumensec' set: [schedulers scheduler schedule-tuesday tuesday start-time 16:00 stop-time 16:30] <182>1 2023-02-22T13:11:15.28

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			2Z Proliant_Node0 mgd 12129 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security policies from-zone trust to-zone untrust policy vpn-deny scheduler-name \]" delimiter="" data="unconfigured" value="schedule-tuesday"] User 'acumensec' set: [security policies from-zone trust to-zone untrust policy vpn-deny scheduler-name] unconfigured -- "schedule-tuesday" **Modify the known-good and known-bad lists (of IP addresses or address ranges)** <182>1 2023-02-22T13:15:58.34 2Z Proliant_Node0 mgd 12129 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security address-book book3 address known-good\]" delimiter="" data="unconfigured" value="10.1.1.146/32"] User 'acumensec' set: [security address-book

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			book3 address known-good] unconfigured -- "10.1.1.146/32" <182>1 2022-08-04T13:06:56.602Z Proliant_Node0 mgd 32710 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security address-book book3 address known-bad\]" delimiter="" data="unconfigured" value="10.1.3.161/32"] User 'acumensec' set: [security address-book book3 address known-bad] unconfigured -- "10.1.3.161/32" **Configure the known-good and known-bad lists to override signature-based IPS policies** <14>1 2022-08-05T10:14:49.398Z Proliant_Node0 RT_FLOW - RT_FLOW_SESSION_DENY [junos@2636.1.1.1.2.129 source-address="10.1.1.146" source-port="0" destination-address="10.1.3.161" destination-port="0"

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			connection-tag="0" service-name="icmp" protocol-id="1" icmp-type="8" policy-name="known-bad-policy" source-zone-name="trust" destination-zone-name="untrust" application="UNKNOWN" nested-application="UNKNOWN" username="N/A" roles="N/A" packet-incoming-interface="reth1.0" encrypted="No" reason="Denied by policy" session-id="163556" application-category="N/A" application-sub-category="N/A" application-risk="-1" application-characteristics="N/A" src-vrf-grp="N/A" dst-vrf-grp="N/A" source-tenant="N/A" destination-service="N/A"] session denied 10.1.1.146/0->10.1.3.161/0 0x0 icmp 1(8) known-bad-policy trust untrust UNKNOWN UNKNOWN N/A(N/A) reth1.0 No Denied by policy 163556 N/A N/A -1 N/A N/A N/A N/A N/A <14>1 2022-08-05T10:55:54.40

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			3Z Proliant_Node0 RT_FLOW - RT_FLOW_SESSION_CREATE [junos@2636.1.1.1.2.129 source-address="10.1.3.161" source-port="0" destination-address="10.1.1.146" destination-port="0" connection-tag="0" service-name="icmp" nat-source-address="10.1.3.161" nat-source-port="0" nat-destination-address="10.1.1.146" nat-destination-port="0" nat-connection-tag="0" src-nat-rule-type="N/A" src-nat-rule-name="N/A" dst-nat-rule-type="N/A" dst-nat-rule-name="N/A" protocol-id="1" policy-name="known-good-policy" source-zone-name="untrust" destination-zone-name="trust" session-id="168100" username="N/A" roles="N/A" packet-incoming-interface="reth2.0" application="UNKNOWN" nested-application="UNKNOWN" encrypted="UNKNOWN" application-

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			category="N/A" application-sub-category="N/A" application-risk="-1" application-characteristics="N/A" src-vrf-grp="N/A" dst-vrf-grp="N/A" tunnel-inspection="Off" tunnel-inspection-policy-set="root" source-tenant="N/A" destination-service="N/A"] session created 10.1.3.161/0->10.1.1.146/0 0x0 icmp 10.1.3.161/0->10.1.1.146/0 0x0 N/A N/A N/A N/A 1 known-good-policy untrust trust 168100 N/A(N/A) reth2.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1 N/A N/A N/A Off root N/A N/A **Ability to manage the trusted public keys database** <182>1 2023-11-29T07:39:02.630Z Proliant_Node0 mgd 69627 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[system login user tester authentication ssh-ecdsa /* SECRET-DATA */\]" delimiter=""

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			value=""] User 'acumensec' set: [system login user tester authentication ssh-ecdsa /* SECRET-DATA */] **Ability to manage the cryptographic keys** <38>1 2023-02-22T13:21:52.110Z Proliant_Node0 ssh-keygen 13377 - - Generated SSH key file /etc/ssh/fips_ssh_host_ecdsa_key.pub with fingerprint SHA256:QwCmhn5oD41IhNSSFGmjSIq0EKmubD6K71wlPtO+hEw **Ability to configure the cryptographic functionality** <190>1 2021-10-01T09:05:59.503Z VSRX_TOE mgd 46513 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.129 username="acumensec" command="set system services ssh ciphers aes128-cbc "] User 'acumensec', command 'set system services ssh ciphers aes128-cbc ' **Ability to configure the lifetime for IPsec SAs**

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			<182>1 2023-02-22T13:59:57.731Z Proliant_Node0 mgd 12129 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security ipsec proposal ipsec-devices-proposal lifetime-seconds\]" delimiter="" data="unconfigured" value="28800"] User 'acumensec' set: [security ipsec proposal ipsec-devices-proposal lifetime-seconds] unconfigured -- "28800" **Ability to import X.509v3 certificates to the TOE's trust store** <29>1 2022-12-07T09:45:49.144Z Proliant_Node0 pkid 20720 PKID_PV_CERT_LOAD [junos@2636.1.1.1.2.129 type-string="AcumenICA"] Certificate AcumenICA has been successfully loaded **Ability to start and stop services** <190>1 2021-09-30T10:31:50.410Z VSRX_TOE mgd

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			82886 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.129 username="acumensec" command="set system services ssh "] User 'acumensec', command 'set system services ssh ' **Ability to modify the behavior of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full** <182>1 2023-02-22T14:07:52.135Z Proliant_Node0 mgd 12129 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[system services netconf ssh\]" delimiter="" value=""] User 'acumensec' set: [system services netconf ssh] <182>1 2023-02-22T14:05:18.020Z Proliant_Node0 mgd 12129 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set"

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			pathname="[system syslog file auditlog archive size\]" delimiter="" data="unconfigured" value="65536"] User 'acumensec' set: [system syslog file auditlog archive size] unconfigured -- "65536" <182>1 2023-02-22T14:05:18.020Z Proliant_Node0 mgd 12129 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[system syslog file auditlog archive files\]" delimiter="" data="unconfigured" value="3"] User 'acumensec' set: [system syslog file auditlog archive files] unconfigured -- "3" **Ability to configure thresholds for SSH rekeying** <182>1 2023-02-22T14:11:10.922Z Proliant_Node0 mgd 12129 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[system services ssh rekey data-limit\]" delimiter=""

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			data="unconfigured" value="6553600"] User 'acumensec' set: [system services ssh rekey data-limit] unconfigured -- "6553600" **Ability to re-enable an Administrator account** <37>1 2021-10-11T12:47:25.700Z VSRX_TOE sshd 9848 LIBJNX_LOGIN_ACCOUNT_UNLOCKED [junos@2636.1.1.1.2.129 username="acumensec"] Account for user 'acumensec' has been unlocked for logins **Ability to set the time which is used for time-stamps** <190>1 2021-10-05T06:21:00.970Z VSRX_TOE mgd 21760 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.129 username="acumensec" command="run set date 202110050630.00 "] User 'acumensec', command 'run set date 202110050630.00 ' <190>1 2021-10-05T06:21:00.989Z VSRX_TOE mgd 21760 UI_CHILD_START

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			[junos@2636.1.1.1.2.129 command="/bin/date"] Starting child '/bin/date' <37>1 2021-10-05T06:30:00.000Z VSRX_TOE date 21937 - - date set by root <190>1 2021-10-05T06:30:00.002Z VSRX_TOE mgd 21760 UI_CHILD_STATUS [junos@2636.1.1.1.2.129 command="/bin/date" pid="21937" status-code="512"] Cleanup child '/bin/date', PID 21937, status 0x200 <29>1 2021-10-05T06:30:00.002Z VSRX_TOE mgd 21760 UI_CHILD_EXITED [junos@2636.1.1.1.2.129 pid="21937" return-value="2" core-dump-status="" command="/bin/date"] Child exited: PID 21937, status 2, command '/bin/date' <30>1 2021-10-05T06:30:00.015Z VSRX_TOE nsd 23326 NSD_SYS_TIME_CHANGE - System time has changed. **Ability to configure NTP**

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			<182>1 2023-02-22T14:23:37.828Z Proliant_Node0 mgd 12129 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[system ntp server 10.1.1.160\]" delimiter="" value=""] User 'acumensec' set: [system ntp server 10.1.1.160] <182>1 2023-02-22T14:24:54.508Z Proliant_Node0 mgd 12129 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="delete" pathname="[system ntp server 10.1.1.160\]" delimiter="" value=""] User 'acumensec' delete: [system ntp server 10.1.1.160] **Ability to configure the reference identifier for the peer** <182>1 2023-11-29T07:29:05.116Z Proliant_Node0 mgd 69627 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set"

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			pathname="[security ike gateway gw-b remote-identity inet\]" delimiter="" data="unconfigured" value="10.1.5.251"] User 'acumensec' set: [security ike gateway gw-b remote-identity inet] unconfigured -- "10.1.5.251" **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors** <182>1 2023-02-22T07:21:57.600Z Proliant_Node0 mgd 13150 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security pki ca-profile AcumenCA ca-identity\]" delimiter="" data="unconfigured" value="AcumenCA"] User 'acumensec' set: [security pki ca-profile AcumenCA ca-identity] unconfigured -- "AcumenCA" <29>1 2023-02-22T07:22:24.769Z Proliant_Node0 pkid 11250 PKID_PV_CERT_LOAD [junos@2636.1.1.1.2.129

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			type-string="AcumenCA"] Certificate AcumenCA has been successfully loaded

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FMT_SMF.1/IPS	Modification of an IPS policy element.	Identifier or name of the modified IPS policy element (e.g. which signature, baseline, or known- good/known-bad list was modified).	<182>1 2023-02-22T11:44:10.082Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack IPv4-src attack-type signature protocol ipv4 source match\]" delimiter="" data="unconfigured" value="equal"] User 'acumensec' set: [security idp custom-attack IPv4-src attack-type signature protocol ipv4 source match] unconfigured -- "equal" <182>1 2023-02-22T11:44:10.083Z Proliant_Node0 mgd 12723 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp custom-attack IPv4-src attack-type signature protocol ipv4 source value\]" delimiter="" data="unconfigured" value="10.1.1.146"] User 'acumensec' set: [security idp custom-attack IPv4-src attack-type signature protocol ipv4 source

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			value] unconfigured -- "10.1.1.146"
FMT_SMR.2	None	None	
FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol	Time of Log: 2022-11-29 10:25:35 UTC, Filter: pfe, Filter action: discard, Name of interface: reth1.0 Name of protocol: TCP, Packet Length: 40, Source address: 10.1.1.146:20, Destination address: 10.1.3.161:1035
FPT_SKP_EXT.1	None	None	
FPT_APW_EXT.1	None	None	
FPT_TST_EXT.1	None	None	

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	<190>1 2021-10-05T06:21:00.970Z VSRX_TOE mgd 21760 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.129 username="acumensec" command="run set date 202110050630.00 "] User 'acumensec', command 'run set date 202110050630.00 ' <190>1 2021-10-05T06:21:00.989Z VSRX_TOE mgd 21760 UI_CHILD_START [junos@2636.1.1.1.2.129 command="/bin/date"] Starting child '/bin/date' <37>1 2021-10-05T06:30:00.000Z VSRX_TOE date 21937 - - date set by root <190>1 2021-10-05T06:30:00.002Z VSRX_TOE mgd 21760 UI_CHILD_STATUS [junos@2636.1.1.1.2.129 command="/bin/date" pid="21937" status-code="512"] Cleanup child '/bin/date', PID 21937, status 0x200 <29>1 2021-10-05T06:30:00.002Z VSRX_TOE mgd

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			21760 UI_CHILD_EXITED [junos@2636.1.1.1.2.129 pid="21937" return-value="2" core-dump-status="" command="/bin/date"] Child exited: PID 21937, status 2, command '/bin/date' <30>1 2021-10-05T06:30:00.015Z VSRX_TOE nsd 23326 NSD_SYS_TIME_CHANGE - System time has changed.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None	<190>1 2023-02-17T11:08:28.481Z Proliant_Node0 mgd 5002 UI_CHILD_START [junos@2636.1.1.1.2.129 command="/usr/libexec/ui/package"] Starting child '/usr/libexec/ui/package' <29>1 2023-02-17T11:08:28.484Z Proliant Node0 mgd 9302 - - /usr/libexec/ui/package -X update -reboot /var/home/acumensec/junos-install-vsrx3-x86-64-22.2R1.9.tgz

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FTA_SSL.3	The termination of a remote session by the session locking mechanism	None	<14>1 2021-10-01T09:52:56.150Z VSRX_TOE -cli - UI_CLI_IDLE_TIMEOUT [junos@2636.1.1.1.2.129 username="acumensec"] Idle timeout for user 'acumensec' exceeded and session terminated <190>1 2021-10-01T09:52:56.158Z VSRX_TOE mgd 49989 UI_LOGOUT_EVENT [junos@2636.1.1.1.2.129 username="acumensec"] User 'acumensec' logout
FTA_SSL.4	The termination of an interactive session	None	<190>1 2021-10-01T10:08:16.234Z VSRX_TOE mgd 51170 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.129 username="acumensec" command="exit "] User 'acumensec', command 'exit ' <190>1 2021-10-01T10:08:16.235Z VSRX_TOE mgd 51170 UI_LOGOUT_EVENT [junos@2636.1.1.1.2.129 username="acumensec"] User 'acumensec' logout

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism	None	<14>1 2021-10-01T10:37:08.360Z VSRX_TOE -cli - UI_CLI_IDLE_TIMEOUT [junos@2636.1.1.1.2.129 username="acumensec"] Idle timeout for user 'acumensec' exceeded and session terminated <190>1 2021-10-01T10:37:08.360Z VSRX_TOE mgd 53004 UI_LOGOUT_EVENT [junos@2636.1.1.1.2.129 username="acumensec"] User 'acumensec' logout
FTA_TAB.1	None	None	

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FTP_ITC.1	Initiation of the trusted channel Termination of the trusted channel Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channels establishment attempt	**Initiation** <38>1 2021-09-27T09:25:13.032Z VSRX_TOE sshd 70000 - - Accepted keyboard-interactive/pam for acumensec from 10.1.2.146 port 59010 ssh2 <190>1 2021-09-27T09:25:13.361Z VSRX_TOE mgd 70011 UI_AUTH_EVENT [junos@2636.1.1.1.2.129 username="acumensec" authentication-level="j-super-user"] Authenticated user 'acumensec' assigned to class 'j-super-user' <190>1 2021-09-27T09:25:13.362Z VSRX_TOE mgd 70011 UI_LOGIN_EVENT [junos@2636.1.1.1.2.129 username="acumensec" class-name="j-super-user" local-peer="" pid="70011" ssh-connection="10.1.2.146 59010 10.1.2.129 22" client-mode="cli"] User 'acumensec' login, class 'j-super-user' [70011], ssh-connection '10.1.2.146 59010 10.1.2.129 22', client-mode 'cli' **Failure**

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			<35>1 2021-09-27T09:41:37.763Z VSRX_TOE sshd 70783 - - error: PAM: Authentication error for acumensec from 10.1.2.146 <37>1 2021-09-27T09:41:37.763Z VSRX_TOE sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.129 username="acumensec" source-address="10.1.2.146"] Login failed for user 'acumensec' from host '10.1.2.146' <35>1 2021-09-27T09:41:41.966Z VSRX_TOE sshd 70783 - - error: PAM: Authentication error for acumensec from 10.1.2.146 <37>1 2021-09-27T09:41:41.966Z VSRX_TOE sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.129 username="acumensec" source-address="10.1.2.146"] Login failed for user 'acumensec' from host '10.1.2.146' <35>1 2021-09-27T09:41:50.81

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			2Z VSRX_TOE sshd 70783 - - error: PAM: Authentication error for acumensec from 10.1.2.146 <37>1 2021-09-27T09:41:50.812Z VSRX_TOE sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.129 username="acumensec" source-address="10.1.2.146"] Login failed for user 'acumensec' from host '10.1.2.146' **Termination** <37>1 2021-09-29T10:45:55.798Z VSRX_TOE sshd 14027 LIBJNX_LOGIN_ACCOUNT_LOCKED [junos@2636.1.1.1.2.129 username="acumensec"] Account for user 'acumensec' has been locked out from logins <38>1 2021-09-29T10:45:55.799Z VSRX_TOE sshd 14027 - - Failed password for acumensec from 10.1.2.146 port 33362 ssh2 <37>1 2021-09-29T10:46:20.818Z VSRX_TOE sshd -

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			SSHD_LOGIN_ATTEMPTS_THRESHOLD [junos@2636.1.1.1.2.129 limit="5" username="acumensec"] Threshold for unsuccessful authentication attempts (5) reached by user 'acumensec' <38>1 2021-09-29T10:46:20.818Z VSRX_TOE sshd 14028 - - Disconnecting authenticating user acumensec 10.1.2.146 port 33362: Too many password failures for acumensec <38>1 2021-09-29T10:46:20.819Z VSRX_TOE sshd 14027 - - Disconnecting authenticating user acumensec 10.1.2.146 port 33362: Too many password failures for acumensec [preauth]

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FTP_TRP.1/Admin	Initiation of the trusted path Termination of the trusted path. Failure of the trusted path functions.	None	**Initiation** <38>1 2021-10-01T11:07:41.592Z VSRX_TOE sshd 55853 - - Accepted keyboard-interactive/pam for acumensec from 10.1.2.146 port 35880 ssh2 <190>1 2021-10-01T11:07:41.942Z VSRX_TOE mgd 55864 UI_AUTH_EVENT [junos@2636.1.1.1.2.129 username="acumensec" authentication-level="j-super-user"] Authenticated user 'acumensec' assigned to class 'j-super-user' <190>1 2021-10-01T11:07:41.942Z VSRX_TOE mgd 55864 UI_LOGIN_EVENT [junos@2636.1.1.1.2.129 username="acumensec" class-name="j-super-user" local-peer="" pid="55864" ssh-connection="10.1.2.146 35880 10.1.2.129 22" client-mode="cli"] User 'acumensec' login, class 'j-super-user' [55864], ssh-connection '10.1.2.146 35880 10.1.2.129 22', client-mode 'cli' **Failure**

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			<35>1 2021-09-27T09:41:37.763Z VSRX_TOE sshd 70783 - - error: PAM: Authentication error for acumensec from 10.1.2.146 <37>1 2021-09-27T09:41:37.763Z VSRX_TOE sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.129 username="acumensec" source-address="10.1.2.146"] Login failed for user 'acumensec' from host '10.1.2.146' <35>1 2021-09-27T09:41:41.966Z VSRX_TOE sshd 70783 - - error: PAM: Authentication error for acumensec from 10.1.2.146 <37>1 2021-09-27T09:41:41.966Z VSRX_TOE sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.129 username="acumensec" source-address="10.1.2.146"] Login failed for user 'acumensec' from host '10.1.2.146' <35>1 2021-09-27T09:41:50.81

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			2Z VSRX_TOE sshd 70783 - - error: PAM: Authentication error for acumensec from 10.1.2.146 <37>1 2021-09-27T09:41:50.812Z VSRX_TOE sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.129 username="acumensec" source-address="10.1.2.146"] Login failed for user 'acumensec' from host '10.1.2.146' **Termination** <37>1 2021-09-29T10:45:55.798Z VSRX_TOE sshd 14027 LIBJNX_LOGIN_ACCOUNT_LOCKED [junos@2636.1.1.1.2.129 username="acumensec"] Account for user 'acumensec' has been locked out from logins <38>1 2021-09-29T10:45:55.799Z VSRX_TOE sshd 14027 - - Failed password for acumensec from 10.1.2.146 port 33362 ssh2 <37>1 2021-09-29T10:46:20.818Z VSRX_TOE sshd -

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			SSHD_LOGIN_ATTEMPTS_THRESHOLD [junos@2636.1.1.1.2.129 limit="5" username="acumensec"] Threshold for unsuccessful authentication attempts (5) reached by user 'acumensec' <38>1 2021-09-29T10:46:20.818Z VSRX_TOE sshd 14028 - - Disconnecting authenticating user acumensec 10.1.2.146 port 33362: Too many password failures for acumensec <38>1 2021-09-29T10:46:20.819Z VSRX_TOE sshd 14027 - - Disconnecting authenticating user acumensec 10.1.2.146 port 33362: Too many password failures for acumensec [preauth]
IPS Logs			

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FMT_SMF.1/IPS	Modification of an IPS policy element.	Identifier or name of the modified IPS policy element (e.g. which signature, baseline, or known-good/known-bad list was modified).	<182>1 2022-08-05T12:47:47.327Z Proliant_Node0 mgd 150 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security idp idp-policy deny-policy rulebase-ips rule rule1 match from-zone\]" delimiter="" data="unconfigured" value="any"] User 'acumensec' set: [security idp idp-policy deny-policy rulebase-ips rule rule1 match from-zone] unconfigured -- "any"

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
IPS_ABD_EXT.1	Inspected traffic matches an anomaly-based IPS policy.	Source and destination IP addresses. The content of the header fields that were determined to match the policy. TOE interface that received the packet Aspect of the anomaly-based IPS policy rule that triggered the event (e.g. throughput, time of day, frequency, etc.). Network-based action by the TOE (e.g. allowed, blocked, sent reset to source IP, sent blocking notification to firewall).1	<14>1 2022-08-04T10:58:34.276Z Proliant_Node0 RT_FLOW - RT_FLOW_SESSION_DENY [junos@2636.1.1.1.2.129 source-address="2001:10:1:3:0:0:0:28" source-port="0" destination-address="2001:10:1:1:0:0:0:128" destination-port="0" connection-tag="0" service-name="icmpv6" protocol-id="58" icmp-type="128" policy-name="schedule" source-zone-name="untrust" destination-zone-name="trust" application="UNKNOWN" nested-application="UNKNOWN" username="N/A" roles="N/A" packet-incoming-interface="reth2.0" encrypted="No" reason="Denied by policy" session-id="21108" application-category="N/A" application-sub-category="N/A" application-risk="-1" application-characteristics="N/A" src-vrf-grp="N/A" dst-vrf-

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			grp="N/A" source-tenant="N/A" destination-service="N/A"] session denied 2001:10:1:3:0:0:0:28/0->2001:10:1:1:0:0:0:128/0 0x0 icmpv6 58(128) schedule untrust trust UNKNOWN UNKNOWN N/A(N/A) reth2.0 No Denied by policy 21108 N/A N/A -1 N/A N/A N/A N/A N/A

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
IPS_IPB_EXT.1	Inspected traffic matches a list of known-good or known-bad addresses applied to an IPS policy.	Source and destination IP addresses (and, if applicable, indication of whether the source and/or destination address matched the list). TOE interface that received the packet. Network-based action by the TOE (e.g. allowed, blocked, sent reset).	<14>1 2022-08-05T10:55:54.403Z Proliant_Node0 RT_FLOW - RT_FLOW_SESSION_CREATE [junos@2636.1.1.1.2.129 source-address="10.1.3.161" source-port="0" destination-address="10.1.1.146" destination-port="0" connection-tag="0" service-name="icmp" nat-source-address="10.1.3.161" nat-source-port="0" nat-destination-address="10.1.1.146" nat-destination-port="0" nat-connection-tag="0" src-nat-rule-type="N/A" src-nat-rule-name="N/A" dst-nat-rule-type="N/A" dst-nat-rule-name="N/A" protocol-id="1" policy-name="known-good-policy" source-zone-name="untrust" destination-zone-name="trust" session-id="168100" username="N/A" roles="N/A" packet-incoming-interface="reth2.0" application="UNKNOWN" nested-application="UNKNOWN

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			" encrypted="UNKNOWN" application-category="N/A" application-sub-category="N/A" application-risk="-1" application-characteristics="N/A" src-vrf-grp="N/A" dst-vrf-grp="N/A" tunnel-inspection="Off" tunnel-inspection-policy-set="root" source-tenant="N/A" destination-service="N/A"] session created 10.1.3.161/0->10.1.1.146/0 0x0 icmp 10.1.3.161/0->10.1.1.146/0 0x0 N/A N/A N/A N/A 1 known-good-policy untrust trust 168100 N/A(N/A) reth2.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1 N/A N/A N/A Off root N/A N/A <14>1 2022-08-05T10:14:49.398Z Proliant_Node0 RT_FLOW - RT_FLOW_SESSION_DENY [junos@2636.1.1.1.2.129 source-address="10.1.1.146" source-port="0" destination-address="10.1.3.161"

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			destination-port="0" connection-tag="0" service-name="icmp" protocol-id="1" icmp-type="8" policy-name="known-bad-policy" source-zone-name="trust" destination-zone-name="untrust" application="UNKNOWN " nested-application="UNKNOWN " username="N/A" roles="N/A" packet-incoming-interface="reth1.0" encrypted="No" reason="Denied by policy" session-id="163556" application-category="N/A" application-sub-category="N/A" application-risk="-1" application-characteristics="N/A" src-vrf-grp="N/A" dst-vrf-grp="N/A" source-tenant="N/A" destination-service="N/A"] session denied 10.1.1.146/0->10.1.3.161/0 0x0 icmp 1(8) known-bad-policy trust untrust UNKNOWN UNKNOWN N/A(N/A) reth1.0 No Denied by policy 163556 N/A N/A -1 N/A N/A N/A N/A N/A

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
IPS_NTA_EXT.1	Modification of which IPS policies are active on a TOE interface. Enabling/disabling a TOE interface with IPS policies applied. Modification of which mode(s) is/are active on a TOE interface.	Identification of the TOE interface. The IPS policy and interface mode (if applicable).	Modification of which IPS policies are active on a TOE interface. <182>1 2023-09-27T10:12:14.782Z Proliant_Node0 mgd 39458 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security zones security-zone trust interfaces reth1.0\]" delimiter="" value=""] User 'acumensec' set: [security zones security-zone trustinterfaces reth1.0] <182>1 2023-09-27T10:12:41.394Z Proliant_Node0 mgd 39458 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[security policies from-zone trust to-zone untrust policy bypass then permit application-services idp-policy\]" delimiter="" data="unconfigured" value="IDP_src"] User 'acumensec' set: [security policies from-zone trust to-zone untrust policy bypass then permit

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			application-services idp-policy] unconfigured -- "IDP_src" Enabling/disabling a TOE interface with IPS policies applied. <182>1 2023-09-27T10:16:32.546Z Proliant_Node0 mgd 39458 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[interfaces reth1 unit 0\]" delimiter="" data="unconfigured" value="disable"] User 'acumensec' set: [interfaces reth1 unit 0] unconfigured -- "disable" Modification of which mode(s) is/are active on a TOE interface. <182>1 2023-09-27T10:19:04.627Z Proliant_Node0 mgd 39458 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[interfaces reth1\]" delimiter="" data="unconfigured" value="promiscuous-mode"] User 'acumensec'

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			set: [interfaces reth1] unconfigured -- "promiscuous-mode"

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
IPS_SBD_EXT.1	Inspected traffic matches a signature-based IPS rule with logging enabled.	Name or identifier of the matched signature Source and destination IP addresses The content of the header fields that were determined to match the signature. TOE interface that received the packet Network-based action by the TOE (e.g. allowed, blocked, sent reset)	<14>1 2022-08-05T13:05:12.092Z Proliant_Node0 RT_IDP - IDP_ATTACK_LOG_EVENT [junos@2636.1.1.1.2.129 epoch-time="1659704712" message-type="SIG" source-address="10.1.1.146" source-port="1" destination-address="10.1.3.161" destination-port="1" protocol-name="IPIP" service-name="SERVICE_IDP" application-name="NONE" rule-name="1" rulebase-name="IPS" policy-name="deny-policy" export-id="1048576" repeat-count="0" action="DROP" threat-severity="INFO" attack-name="IPv4-version" 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="trust" source-

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			interface-name="reth1.0" destination-zone-name="untrust" destination-interface-name="reth2.0" packet-log-id="0" alert="yes" username="N/A" roles="N/A" xff-header="N/A" cve-id="N/A" session-id="181445" message="-"] IDP: at 1659704712, SIG Attack log <10.1.1.146/1->10.1.3.161/1> for IPIP protocol and service SERVICE_IDP application NONE by rule 1 of rulebase IPS in policy deny-policy. attack: id=1048576, repeat=0, action=DROP, threat-severity=INFO, name=IPv4-version, NAT <0.0.0.0:0->0.0.0.0:0>, time-elapsed=0, inbytes=0, outbytes=0, inpackets=0, outpackets=0, intf:trust:reth1.0->untrust:reth2.0, packet-log-id: 0, alert=yes, username=N/A, roles=N/A, xff-header=N/A, cve-id=N/A, session-id=181445 and misc-message –
VPNGW Logs			
FAU_GEN.1/VPN	No events specified.	N/A	N/A

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FCS_CKM.1/IKE	No events specified.	N/A	N/A
FIA_PSK_EXT.1	None.	None.	N/A
FIA_PSK_EXT.2	None.	None.	N/A

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FMT_SMF.1/VPN	All administrative actions	No additional information.	• **Definition of packet filtering rules:** <182>1 2023-02-01T11:31:10.142Z Proliant_Node0 mgd 81936 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall family inet filter SRC_DENY term drop from source-address 10.1.1.146/32\]" delimiter="" value=""] User 'acumensec' set: [firewall family inet filter SRC_DENY term drop from source-address 10.1.1.146/32] <182>1 2023-02-01T11:31:43.123Z Proliant_Node0 mgd 81936 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall family inet filter

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			SRC_DENY term drop then discard\]" delimiter="" value=""] User 'acumensec' set: [firewall family inet filter SRC_DENY term drop then discard] <182>1 2023-02-01T11:31:47.137Z Proliant_Node0 mgd 81936 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall family inet filter SRC_DENY term drop then\]" delimiter="" data="unconfigured" value="log"] User 'acumensec' set: [firewall family inet filter SRC_DENY term drop then] unconfigured -- "log" • **Association of packet filtering rules to network interfaces** <182>1 2023-02-01T11:37:19.068Z Proliant_Node0 mgd 81936 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			129 username="acumensec" action="set" pathname="[interfaces st0 unit 0 family inet filter output\]" delimiter="" data="unconfigured" value="SRC_DENY"] User 'acumensec' set: [interfaces st0 unit 0 family inet filter output] unconfigured -- "SRC_DENY" • Ordering of packet filtering rules by priority <182>1 2023-02-01T11:41:01.701Z Proliant_Node0 mgd 81936 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter DEST_PERMIT term permit from destination-address 10.1.3.161/32\]" delimiter="" value=""] User 'acumensec' set: [firewall filter DEST_PERMIT term permit from

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			destination-address 10.1.3.161/32] <182>1 2023-02-01T11:41:07.196Z Proliant_Node0 mgd 81936 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter DEST_PERMIT term permit then\]" delimiter="" data="unconfigured" value="accept"] User 'acumensec' set: [firewall filter DEST_PERMIT term permit then] unconfigured -- "accept" <182>1 2023-02-01T11:41:09.880Z Proliant_Node0 mgd 81936 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter DEST_PERMIT term permit then\]" delimiter=""

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			data="unconfigured" value="log"] User 'acumensec' set: [firewall filter DEST_PERMIT term permit then] unconfigured -- "log" <182>1 2023-02-01T11:41:21.622Z Proliant_Node0 mgd 81936 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter DEST_PERMIT term drop from destination-address 10.1.3.161/32\]" delimiter="" value=""] User 'acumensec' set: [firewall filter DEST_PERMIT term drop from destination-address 10.1.3.161/32] <182>1 2023-02-01T11:41:31.951Z Proliant_Node0 mgd 81936 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.129

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			username="acumensec" action="set" pathname="[firewall filter DEST_PERMIT term drop then discard\]" delimiter="" value=""] User 'acumensec' set: [firewall filter DEST_PERMIT term drop then discard] <182>1 2023-02-01T11:41:34.822Z Proliant_Node0 mgd 81936 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.129 username="acumensec" action="set" pathname="[firewall filter DEST_PERMIT term drop then\]" delimiter="" data="unconfigured" value="log"] User 'acumensec' set: [firewall filter DEST_PERMIT term drop then] unconfigured -- "log"

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport layer protocol	{primary:node0}[edit] acumensec@Proliant_Node0:fips# run show firewall log detail Time of Log: 2022-11-29 10:16:39 UTC, Filter: pfe, Filter action: accept, Name of interface: reth1.0 Name of Protocol: TCP, Packet Length: 40, Source address: 10.1.1.146:1300, Destination address: 10.1.3.161:80 Time of Log: 2022-11-29 10:16:39 UTC, Filter: pfe, Filter action: accept, Name of interface: reth1.0 Name of Protocol: TCP, Packet Length: 40, Source address: 10.1.1.146:1300, Destination address: 10.1.3.161:80 Time of Log: 2022-11-29 10:16:39 UTC, Filter: pfe, Filter action: accept, Name of interface: reth1.0 Name of Protocol: TCP, Packet Length: 40, Source address: 10.1.1.146:1300, Destination address: 10.1.3.161:80

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			Time of Log: 2022-11-29 10:16:36 UTC, Filter: pfe, Filter action: discard, Name of interface: reth1.0 Name of Protocol: TCP, Packet Length: 40, Source address: 10.1.1.146:1200, Destination address: 10.1.3.161:80 Time of Log: 2022-11-29 10:16:36 UTC, Filter: pfe, Filter action: discard, Name of interface: reth1.0 Name of Protocol: TCP, Packet Length: 40, Source address: 10.1.1.146:1200, Destination address: 10.1.3.161:80 Time of Log: 2022-11-29 10:16:36 UTC, Filter: pfe, Filter action: discard, Name of interface: reth1.0 Name of Protocol: TCP, Packet Length: 40, Source address: 10.1.1.146:1200, Destination address: 10.1.3.161:80
FPT_FLS.1/SelfTest	No events specified.	N/A	N/A
FPT_TST_EXT.3	No events specified.	N/A	N/A

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FTP_ITC.1/VPN	Initiation of the trusted channel	No additional information.	***Initiation*** <14>1 2022-07-15T07:32:37.658Z Proliant_Node0 RT_FLOW - RT_FLOW_SESSION_CREATE [junos@2636.1.1.1.2.129 source-address="10.1.1.146" source-port="11276" destination-address="10.1.3.28" destination-port="1" connection-tag="0" service-name="icmp" nat-source-address="10.1.1.146" nat-source-port="11276" nat-destination-address="10.1.3.28" nat-destination-port="1" nat-connection-tag="0" src-nat-rule-type="N/A" src-nat-rule-name="N/A" dst-nat-rule-type="N/A" dst-nat-rule-name="N/A" protocol-id="1" policy-name="vpn-allow" source-zone-name="trust" destination-zone-name="vpnzone" session-id="3802" username="N/A" roles="N/A" packet-incoming-interface="reth1.0" application="UNKNOWN" nested-application="UNKNOWN

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			" encrypted="UNKNOWN" application-category="N/A" application-sub-category="N/A" application-risk="-1" application-characteristics="N/A" src-vrf-grp="N/A" dst-vrf-grp="N/A" tunnel-inspection="Off" tunnel-inspection-policy-set="root" source-tenant="N/A" destination-service="N/A"] session created 10.1.1.146/11276->10.1.3.28/1 0x0 icmp 10.1.1.146/11276->10.1.3.28/1 0x0 N/A N/A N/A N/A 1 vpn-allow trust vpnzone 3802 N/A(N/A) reth1.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1 N/A N/A N/A Off root N/A N/A

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FTP_ITC.1/VPN	Termination of the trusted channel	No additional information.	***Termination*** <14>1 2022-07-15T13:17:56.130Z Proliant_Node0 RT_FLOW - RT_FLOW_SESSION_DENY [junos@2636.1.1.1.2.129 source-address="10.1.1.146" source-port="57642" destination-address="10.1.3.28" destination-port="22" connection-tag="0" service-name="junos-ssh" protocol-id="6" icmp-type="0" policy-name="vpn-deny" source-zone-name="trust" destination-zone-name="vpnzone" application="UNKNOWN" nested-application="UNKNOWN" username="N/A" roles="N/A" packet-incoming-interface="reth1.0" encrypted="No" reason="Denied by policy" session-id="41942" application-category="N/A" application-sub-category="N/A" application-risk="-1" application-characteristics="N/A" src-vrf-grp="N/A" dst-vrf-

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			grp="N/A" source-tenant="N/A" destination-service="N/A"] session denied 10.1.1.146/57642->10.1.3.28/22 0x0 junos-ssh 6(0) vpn-deny trust vpnzone UNKNOWN UNKNOWN N/A(N/A) reth1.0 No Denied by policy 41942 N/A N/A -1 N/A N/A N/A N/A N/A <14>1 2022-07-15T13:17:58.129Z Proliant_Node0 RT_FLOW - RT_FLOW_SESSION_DENY [junos@2636.1.1.1.2.129 source-address="10.1.1.146" source-port="57642" destination-address="10.1.3.28" destination-port="22" connection-tag="0" service-name="junos-ssh" protocol-id="6" icmp-type="0" policy-name="vpn-deny" source-zone-name="trust" destination-zone-name="vpnzone" application="UNKNOWN" nested-application="UNKNOWN" username="N/A" roles="N/A" packet-incoming-interface="reth1.0"

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			encrypted="No" reason="Denied by policy" session-id="41943" application-category="N/A" application-sub-category="N/A" application-risk="-1" application-characteristics="N/A" src-vrf-grp="N/A" dst-vrf-grp="N/A" source-tenant="N/A" destination-service="N/A"] session denied 10.1.1.146/57642->10.1.3.28/22 0x0 junos-ssh 6(0) vpn-deny trust vpnzone UNKNOWN UNKNOWN N/A(N/A) reth1.0 No Denied by policy 41943 N/A N/A -1 N/A N/A N/A N/A N/A

Table 6: Audit Records for all Auditable Events *(Continued)*

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FTP_ITC.1/VPN	Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channel establishment attempt	***Failure*** <27>1 2022-07-25T07:32:45.548Z Proliant_Node0 kmd 20805 - - IKE negotiation failed with error: No proposal chosen. IKE Version: 1, VPN: ike-vpn-devices Gateway: gw-b, Local: 10.1.5.129/500, Remote: 10.1.5.29/500, Local IKE-ID: Not-Available, Remote IKE-ID: Not-Available, VR-ID: 0: Role: Initiator <27>1 2022-07-25T07:32:46.554Z Proliant_Node0 kmd 20805 - - IKE negotiation failed with error: No proposal chosen. IKE Version: 1, VPN: ike-vpn-devices Gateway: gw-b, Local: 10.1.5.129/500, Remote: 10.1.5.29/500, Local IKE-ID: Not-Available, Remote IKE-ID: Not-Available, VR-ID: 0: Role: Initiator

8
CHAPTER

Configuring Event Logging

Event Logging Overview

The evaluated configuration requires the auditing of configuration changes through the system log.

In addition, Junos OS can:

- Send automated responses to audit events (syslog entry creation).
- Allow authorized managers to examine audit logs.
- Send audit files to external servers.
- Allow authorized managers to return the system to a known state.

The logging for the evaluated configuration must capture the following events:

- Changes to secret key data in the configuration.
- Committed changes.
- Login/logout of users.
- System startup.
- Failure to establish an SSH session.
- Establishment/termination of an SSH session.
- Changes to the (system) time.
- Termination of a remote session by the session locking mechanism.
- Termination of an interactive session.

In addition, Juniper Networks recommends that logging also:

- Capture all changes to the configuration.
- Store logging information remotely.

Interpreting Event Messages

The following output shows a sample event message.

```
Jul 24 17:43:28  router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system radius-
server 1.2.3.4 secret]
```

Table 7 on page 175 describes the fields for an event message. If the system logging utility cannot determine the value in a particular field, a hyphen (-) appears instead.

Table 7: Fields in Event Messages

Field	Description	Examples
timestamp	Time when the message was generated, in one of two representations: • *MMM-DD HH:MM:SS.MS+/-HH:MM,* is the month, day, hour, minute, second and millisecond in local time. The hour and minute that follows the plus sign (+) or minus sign (-) is the offset of the local time zone from Coordinated Universal Time (UTC). • *YYYY-MM-DDTHH:MM:SS.MSZ* is the year, month, day, hour, minute, second and millisecond in UTC.	`Jul 24 17:43:28` is the timestamp expressed as local time in the United States. `2012-07-24T09:17:15.719Z` is `9:17 AM UTC on 24 July 2012.`
hostname	Name of the host that originally generated the message.	`router1`
process	Name of the Junos OS process that generated the message.	`mgd`
processID	UNIX process ID (PID) of the Junos OS process that generated the message.	`4153`
TAG	Junos OS system log message tag, which uniquely identifies the message.	`UI_DBASE_LOGOUT_EVENT`

Table 7: Fields in Event Messages *(Continued)*

Field	Description	Examples
username	Username of the user initiating the event.	"admin"
message-text	English-language description of the event .	set: [system radius-server 1.2.3.4 secret]

Logging Changes to Secret Data

The following are examples of audit logs of events that change the secret data.

Load Merge

When a `load merge` command is issued to merge the contents of the example Common Criteria configuration with the contents of the original configuration, the following audit logs are created concerning the secret data:

```
Jul 24 17:43:28  router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system radius-
server 1.2.3.4 secret]
Jul 24 17:43:28  router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system login
user admin authentication encrypted-password]
Jul 24 17:43:28  router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system login
user admin2 authentication encrypted-password]
```

Load Replace

When a `load replace` command is issued to replace the contents of the example Common Criteria configuration with the contents of the original configuration, the following audit logs are created concerning the secret data:

```
Jul 24 18:29:09  router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' replace: [system
radius-server 1.2.3.4 secret]
Jul 24 18:29:09  router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' replace: [system login
user admin authentication encrypted-password]
```

```
Jul 24 18:29:09  router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' replace: [system login
user admin authentication encrypted-password]
```

Load Override

When a `load override` command is issued to override the contents of the example Common Criteria configuration with the contents of the original configuration, the following audit logs are created concerning the secret data:

```
Jul 25 14:25:51  router1 mgd[4153]: UI_LOAD_EVENT: User 'admin' is performing a 'load override'
Jul 25 14:25:51  router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' override: CC_config2.txt
Jul 25 14:25:51  router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system radius-
server 1.2.3.4 secret]
Jul 25 14:25:51  router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system login
user admin authentication encrypted-password]
Jul 25 14:25:51  router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system login
user admin authentication encrypted-password]
```

Load Update

When a `load update` command is issued to update the contents of the example Common Criteria configuration with the contents of the original configuration, the following audit logs are created concerning the secret data:

```
Jul 25 14:31:03  router1 mgd[4153]: UI_LOAD_EVENT: User 'admin' is performing a 'load update'
Jul 25 14:31:03  router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' update: CC_config2.txt
Jul 25 14:31:03  router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system radius-
server 1.2.3.4 secret]
Jul 25 14:31:03  router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' deactivate: [system radius-
server 1.2.3.4 secret] ""
Jul 25 14:31:03  router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system login
user admin authentication encrypted-password]
Jul 25 14:31:03  router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' deactivate: [system login
user admin authentication encrypted-password] ""
Jul 25 14:31:03  router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system login
user test authentication encrypted-password]
Jul 25 14:31:03  router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' deactivate: [system login
user test authentication encrypted-password] ""
```

For more information about configuring parameters and managing log files, see the *Junos OS System Log Messages Reference*.

RELATED DOCUMENTATION

Interpreting Event Messages | 175

Login and Logout Events Using SSH

System log messages are generated whenever a user successfully or unsuccessfully attempts SSH access. Logout events are also recorded. For example, a logout event for both remote and local sessions can be triggered due to the user issuing an *exit* or *quit* command or by the inactivity timer triggering the termination of a session. The following logs are the result of two failed authentication attempts, then a successful one, and finally a logout:

```
Dec 20 23:17:35  bilbo sshd[16645]: Failed password for op from 172.17.58.45 port 1673 ssh2
Dec 20 23:17:42  bilbo sshd[16645]: Failed password for op from 172.17.58.45 port 1673 ssh2
Dec 20 23:17:53  bilbo sshd[16645]: Accepted password for op from 172.17.58.45 port 1673 ssh2
Dec 20 23:17:53  bilbo mgd[16648]: UI_AUTH_EVENT: Authenticated user 'op' at permission level
                                   'j-operator'
Dec 20 23:17:53  bilbo mgd[16648]: UI_LOGIN_EVENT: User 'op' login, class 'j-operator' [16648]
Dec 20 23:17:56  bilbo mgd[16648]: UI_CMDLINE_READ_LINE: User 'op', command 'quit '
Dec 20 23:17:56  bilbo mgd[16648]: UI_LOGOUT_EVENT: User 'op' logout
```

RELATED DOCUMENTATION

Interpreting Event Messages | 175

Logging of Audit Startup

The audit information logged includes startups of Junos OS. This in turn identifies the startup events of the audit system, which cannot be independently disabled or enabled. For example, if Junos OS is restarted, the audit log contains the following information:

```
Dec 20 23:17:35  bilbo syslogd: exiting on signal 14
Dec 20 23:17:35  bilbo syslogd: restart
Dec 20 23:17:35  bilbo syslogd /kernel: Dec 20 23:17:35 init: syslogd (PID 19128) exited with
```

```
status=1
Dec 20 23:17:42  bilbo /kernel:
Dec 20 23:17:53  init: syslogd (PID 19200) started
```

9

CHAPTER

Configuring VPNs

Configuring VPN on a Device Running Junos OS

IN THIS SECTION

This section describes sample configurations of an IPsec VPN on a Junos OS device using the following IKE authentication methods:

- "Configuring an IPsec VPN with a Preshared Key for IKE Authentication" on page 183
- "Configuring an IPsec VPN with an RSA Signature for IKE Authentication" on page 191
- "Configuring an IPsec VPN with an ECDSA Signature for IKE Authentication" on page 196

Figure 1 on page 181 illustrates the VPN topology used in all the examples described in this section. Here, H0 and H1 are the host PCs, R0 and R2 are the two endpoints of the IPsec VPN tunnel, and R1 is a router to route traffic between the two different networks.

NOTE: The router R1 can be a Linux-based router, a Juniper Networks device, or any other vendor router.

Figure 1: VPN Topology

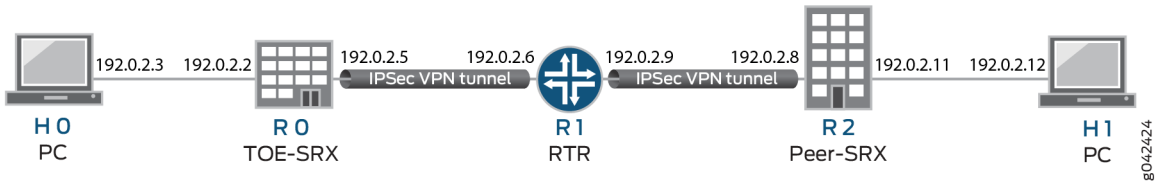

Table 8 on page 182 provides a complete list of the supported IKE protocols, tunnel modes, Phase 1 negotiation mode, authentication method or algorithm, encryption algorithm, DH groups supported for the IKE authentication and encryption (Phase1, IKE Proposal), and for IPsec authentication and

encryption (Phase2, IPsec Proposal). The listed protocols, modes, and algorithms are supported and required for 22.2R2 Common Criteria.

Table 8: VPN Combination Matrix

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 1 Proposal (P1, IKE)			
			Authentication Method	Authentication Algorithm	DH Group	Encryption Algorithm
IKEv1	Main	Route	pre-shared-keys	sha-256	group14	
IKEv2			rsa-signatures-2048	sha-384	group19	aes-128-cbc
			ecdsa-signatures-256		group20	aes-128-gcm
			ecdsa-signatures-384		group24	aes-192-cbc
						aes-256-cbc
						aes-256-gcm

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 2 Proposal (P2, IPsec)			
			Authentication Algorithm	DH Group (PFS)	Encryption Method	Encryption Algorithm
IKEv1	Main	Route	hmac-sha1-96	group14	ESP	
IKEv2			hmac-sha-256-128	group19		aes-128-cbc
				group20		aes-128-gcm
				group24		aes-192-cbc

(Continued)

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 2 Proposal (P2, IPsec)			
			Authentication Algorithm	DH Group (PFS)	Encryption Method	Encryption Algorithm
						aes-192-gcm
						aes-256-cbc
						aes-256-gcm

NOTE: The following sections provide sample configurations of IKEv1 IPsec VPN examples for selected algorithms. Authentication algorithms can be replaced in the configurations to accomplish the user's desired configurations. Use `set security ike gateway <gw-name> version v2-only` command for IKEv2 IPsec VPN.

Configuring an IPsec VPN with a Preshared Key for IKE Authentication

In this section, instructions are provided to configure devices running Junos OS for IPsec VPN using a preshared key as the IKE authentication method. The algorithms used in IKE or IPsec authentication or encryption is shown in Table 9 on page 183

Table 9: IKE or IPsec Authentication

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 1 Proposal (P1, IKE)			
			Authentication Method	Authentication Algorithm	DH Group	Encryption Algorithm
IKEv1	Main	Route	pre-shared-keys	sha-256	group14	aes-256-cbc

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 2 Proposal (P2, IPsec)			
			Authentication Algorithm	DH Group (PFS)	Encryption Method	Encryption Algorithm
IKEv1	Main	Route	hmac-sha-256-128	group14	ESP	aes-256-cbc

NOTE: A device running Junos OS uses certificate-based authentication or preshared keys for IPsec. TOE accepts ASCII preshared or bit-based keys up to 255 characters (and their binary equivalents) that contain uppercase and lowercase letters, numbers, and special characters such as !, @, #, $, %, ^, &, *, (, and). The device accepts the preshared text keys and converts the text string into an authentication value as per RFC 2409 for IKEv1 or RFC 4306 for IKEv2, using the PRF that is configured as the hash algorithm for the IKE exchanges. The Junos OS does not impose minimum complexity requirements for preshared keys. Hence, users are advised to carefully choose long preshared keys of sufficient complexity.

Configuring IPsec VPN with Preshared Key as IKE Authentication on the Initiator

To configure the IPsec VPN with preshared key IKE authentication on the initiator:

1. Configure the IKE proposal.

```
[edit security ike]
user@host# set proposal ike-proposal1 authentication-method pre-shared-keys
user@host# set proposal ike-proposal1 dh-group group14
user@host# set proposal ike-proposal1 authentication-algorithm sha256
user@host# set proposal ike-proposal1 encryption-algorithm aes-256-cbc
```

NOTE: Here, `ike-proposal1` is the IKE proposal name given by the authorized administrator.

2. Configure the IKE policy.

```
[edit]
user@host# set security ike policy ike-policy1 mode main
user@host# set security ike policy ike-policy1 proposals ike-proposal1
```

NOTE: Here, `ike-policy1` is the IKE policy name and `ike-proposal1` is the IKE proposal name given by the authorized administrator.

```
user@host# prompt security ike policy ike-policy1 pre-shared-key ascii-text
New ascii-text (secret):(secret)
Retype new ascii-text (secret):(secret)
```

NOTE: You must enter and reenter the preshared key when prompted. For example, the preshared key can be *CertSqa@jnpr2014*.

NOTE: The preshared key can alternatively be entered in hexadecimal format. For example:

```
[edit]
root@host# prompt security ike policy ike-policy1 pre-shared-key hexadecimal
New hexadecimal (secret):(secret)
Retype new hexadecimal (secret):(secret)
```

Enter the hexadecimal preshared key value.

3. Configure the IPsec proposal.

```
[edit security ipsec]
user@host# set security proposal ipsec-proposal1 protocol esp
user@host# set security proposal ipsec-proposal1 authentication-algorithm hmac-sha-256-128
user@host# set security proposal ipsec-proposal1 encryption-algorithm aes-256-cbc
```

NOTE: Here, `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

4. Configure the IPsec policy.

```
[edit security ipsec]
user@host# set security policy ipsec-policy1 perfect-forward-secrecy keys group14
user@host# set security policy ipsec-policy1 proposals ipsec-proposal1
```

NOTE: Here, `ipsec-policy1` is the IPsec policy name and `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

5. Configure the IKE.

```
[edit security ike]
user@host# set gateway gw1 ike-policy ike-policy1
user@host# set gateway gw1 address 192.0.2.8
user@host# set gateway gw1 local-identity inet 192.0.2.5
user@host# set gateway gw1 external-interface ge-0/0/2
```

NOTE: Here, `gw1` is an IKE gateway name, `192.0.2.8` is the peer VPN endpoint IP, `192.0.2.5` is the local VPN endpoint IP, and `ge-0/0/2` is a local outbound interface as the VPN endpoint. The following additional configuration is also needed in the case of IKEv2

```
[edit security ike]
user@host# set gateway gw1 version v2-only
```

6. Configure the VPN.

```
[edit]
user@host# set security ipsec vpn vpn1 ike gateway gw1
user@host# set security ipsec vpn vpn1 ike ipsec-policy ipsec-policy1
user@host# set security ipsec vpn vpn1 bind-interface st0.0
user@host# set routing-options static route 192.0.2.10/24 qualified-next-hop st0.0 preference
1
```

NOTE: A secure tunnel interface (st0) is an internal interface that is used by route-based VPNs to route cleartext traffic to an IPsec VPN tunnel. For more information on secure tunnel interface, see Secure Tunnel Interface in a Virtual Router.

NOTE: Here, `vpn1` is the VPN tunnel name given by the authorized administrator.

7. Configure the outbound flow policies.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application any
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then session-close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

8. Configure the inbound flow policies.

```
[edit security policies]
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match source-address
untrustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match destination-
address trustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match application any
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then permit
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-init
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

9. Commit your configuration.

```
user@host# commit
```

Configuring IPsec VPN with Preshared Key as IKE Authentication on the Responder

To configure the IPsec VPN with preshared key IKE authentication on the responder:

1. Configure the IKE proposal.

```
[edit security ike]
user@host# set proposal ike-proposal1 authentication-method pre-shared-keys
user@host# set proposal ike-proposal1 dh-group group14
user@host# set proposal ike-proposal1 authentication-algorithm sha256
user@host# set proposal ike-proposal1 encryption-algorithm aes-128-cbc
```

NOTE: Here, `ike-proposal1` is the IKE proposal name given by the authorized administrator.

2. Configure the IKE policy.

```
[edit]
user@host# set security ike policy ike-policy1 mode main
user@host# set security ike policy ike-policy1 proposals ike-proposal1
```

NOTE: Here, `ike-policy1` is the IKE policy name and `ike-proposal1` is the IKE proposal name given by the authorized administrator.

```
user@host# prompt security ike policy ike-policy1 pre-shared-key ascii-text
New ascii-text (secret):(secret)
Retype new ascii-text (secret):(secret)
```

NOTE: You must enter and reenter the preshared key when prompted. For example, the preshared key can be *CertSqa@jnpr2014*.

NOTE: The pre-share key could alternatively be entered in hexadecimal format. For example,

```
user@host# prompt security ike policy ike-policy1 pre-shared-key hexadecimal
New hexadecimal (secret):
Retype new hexadecimal (secret):
```

Here, the hexadecimal preshared key can be `cc2014bae9876543`.

3. Configure the IPsec proposal.

```
[edit security ipsec]
user@host# set proposal ipsec-proposal1 protocol esp
user@host# set proposal ipsec-proposal1 authentication-algorithm hmac-sha-256-128
user@host# set proposal ipsec-proposal1 encryption-algorithm aes-128-cbc
```

NOTE: Here, `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

4. Configure the IPsec policy.

```
[edit security ipsec]
user@host# set policy ipsec-policy1 perfect-forward-secrecy keys group14
user@host# set policy ipsec-policy1 proposals ipsec-proposal1
```

NOTE: Here, `ipsec-policy1` is the IPsec policy name and `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

5. Configure the IKE.

```
[edit security ike]
user@host# set gateway gw1 ike-policy ike-policy1
user@host# set gateway gw1 address 192.0.2.5
```

```
user@host# set gateway gw1 local-identity inet 192.0.2.8
user@host# set gateway gw1 external-interface ge-0/0/2
```

NOTE: Here, `gw1` is an IKE gateway name, `192.0.2.5` is the peer VPN endpoint IP, `192.0.2.8` is the local VPN endpoint IP, and `ge-0/0/2` is a local outbound interface as the VPN endpoint. The following additional configuration is also needed in the case of IKEv2.

```
[edit security ike]
user@host# set gateway gw1 version v2-only
```

6. Configure the VPN.

```
[edit]
user@host# set security ipsec vpn vpn1 ike gateway gw1
user@host# set security ipsec vpn vpn1 ike ipsec-policy ipsec-policy1
user@host# set security ipsec vpn vpn1 bind-interface st0.0
user@host# set routing-options static route 192.0.2.7/24 qualified-next-hop st0.0 preference 1
```

NOTE: Here, `vpn1` is the VPN tunnel name given by the authorized administrator.

7. Configure the outbound flow policies.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application any
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then session-close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

8. Configure the inbound flow policies.

```
[edit security policies]
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match source-address
untrustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match destination-
address trustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match application any
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then permit
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-init
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

9. Commit your configuration.

```
user@host# commit
```

Configuring an IPsec VPN with an RSA Signature for IKE Authentication

The following section provides an example to configure Junos OS devices for IPsec VPN using RSA Signature as IKE Authentication method, whereas, the algorithms used in IKE/IPsec authentication/ encryption is as shown in the following table. In this section, you configure devices running Junos OS for IPsec VPN using an RSA signature as the IKE authentication method. The algorithms used in IKE or IPsec authentication or encryption is shown in Table 9 on page 183 .

The TOE checks the validity of X.509 certificates each time a certificate is presented for IPsec authentication. To validate certificates, the TOE extracts the subject, issuer, subject's public key, signature, basic Constraints and validity period fields. If any fields are not present, the validation fails. The issuer is looked up in the PKI database. If the issuer is not present, or if the issuer certificate does not have the CA:true flag in the basicConstraints section, the validation fails. The TOE verifies the validity of the signature. If the signature is not valid, the validation fails. It then confirms that the current date and time is within the valid time period specified in the certificate if the TOE has been configured to perform a revocation check using CRL (as specified in RFC 5280 Section 6.3). If the CRL fails to download, the certificate is considered to have failed validation, unless the option to skip CRL checking on download failure has been enabled.

Table 10: IKE/IPsec Authentication and Encryption

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 1 Proposal (P1, IKE)			
			Authentication Method	Authentication Algorithm	DH Group	Encryption Algorithm
IKEv1	Main	Route	rsa-signatures-2048	sha-256	group19	aes-128-cbc

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 2 Proposal (P2, IPsec)			
			Authentication Algorithm	DH Group (PFS)	Encryption Method	Encryption Algorithm
IKEv1	Main	Route	hmac-sha-256-128	group19	ESP	aes-128-cbc

Configuring IPsec VPN with RSA Signature as IKE Authentication on the Initiator or Responder

To configure the IPsec VPN with RSA signature IKE authentication on the initiator:

1. Configure the PKI. See Example: Configuring PKI.
2. Generate the RSA key pair. See Example: Generating a Public-Private Key Pair.
3. Generate and load the CA certificate. See Example: Loading CA and Local Certificates Manually.
4. Load the CRL. See Example: Manually Loading a CRL onto the Device .
5. Generate and load a local certificate. See Example: Loading CA and Local Certificates Manually.
6. Configure the IKE proposal.

```
[edit security ike]
user@host# set proposal ike-proposal1 authentication-method rsa-signatures
user@host# set proposal ike-proposal1 dh-group group19
user@host# set proposal ike-proposal1 authentication-algorithm sha-256
user@host# set proposal ike-proposal1 encryption-algorithm aes-128-cbc
```

NOTE: You can use the disable option to disable the revocation check or select the crl option toconfigure the CRL attributes. Using the `set security pki ca-profile <profilename>revocation-check crl disable` on-download-failure command disable the on-downloadfailure option to allow the sessions matching the CA profile, when CRL download failed for a CA profile. The sessions will be allowed only if no old CRL is present in the same CA profile."Here, ike-proposal1 is the name given by the authorized administrator.

7. Configure the IKE policy.

```
[edit security ike]
user@host# set policy ike-policy1 mode main
user@host# set policy ike-policy1 proposals ike-proposal1
user@host# set policy ike-policy1 certificate local-certificate cert1
```

NOTE: Here, `ike-policy1` IKE policy name given by the authorized administrator.

8. Configure the IPsec proposal.

```
[edit security ipsec]
user@host# set proposal ipsec-proposal1 protocol esp
user@host# set proposal ipsec-proposal1 authentication-algorithm hmac-sha-256-128
user@host# set proposal ipsec-proposal1 encryption-algorithm aes-128-cbc
```

NOTE: Here, `ipsec-proposal1` is the name given by the authorized administrator.

9. Configure the IPsec policy.

```
[edit security ipsec]
user@host# set policy ipsec-policy1 perfect-forward-secrecy keys group19
user@host# set policy ipsec-policy1 proposals ipsec-proposal1
```

NOTE: Here, `ipsec-policy1` is the name given by the authorized administrator.

10. Configure the IKE.

```
[edit security ike]
user@host# set gateway gw1 ike-policy ike-policy1
user@host# set gateway gw1 address 192.0.2.8
user@host# set gateway gw1 local-identity inet 192.0.2.5
user@host# set gateway gw1 external-interface fe-0/0/1
```

NOTE: Here, `192.0.2.8` is the peer VPN endpoint IP, `192.0.2.5` is the local VPN endpoint IP, and `fe-0/0/1` is the local outbound interface as VPN endpoint. The following configuration is also needed for IKEv2.

```
[edit security ike]
user@host# set gateway gw1 version v2-only
```

11. Configure VPN.

```
[edit security ipsec]
user@host# set vpn vpn1 ike gateway gw1
user@host# set vpn vpn1 ike ipsec-policy ipsec-policy1
user@host# set vpn vpn1 bind-interface st0.0
```

NOTE: Here, `vpn1` is the VPN tunnel name given by the authorized administrator.

```
[edit]
user@host# set routing-options static route 192.0.2.10/24 qualified-next-hop st0.0
preference 1
```

12. Configure the outbound flow policies.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
```

```
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application any
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zone and `trustLan` and `untrustLan` are preconfigured network addresses.

13. Configure the inbound flow policies.

```
[edit security policies]
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match source-address
untrustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match destination-
address trustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match application any
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then permit
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-init
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-
close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

14. Commit the configuration.

```
[edit]
user@host# commit
```

A web server (Example Apache 2) can be used to host the CRL files on the CRL server which the device can then retrieve via HTTP.

Configuring an IPsec VPN with an ECDSA Signature for IKE Authentication

In this section, you configure devices running Junos OS for IPsec VPN using an ECDSA signature as the IKE authentication method. The algorithms used in IKE or IPsec authentication or encryption are shown in Table 9 on page 183 .

Table 11: IKE or IPsec Authentication and Encryption

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 1 Proposal (P1, IKE)			
			Authentication Method	Authentication Algorithm	DH Group	Encryption Algorithm
IKEv1	Main	Route	ecdsa-signatures-256	sha-384	group14	aes-256-cbc

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 2 Proposal (P2, IPsec)			
			Authentication Algorithm	DH Group (PFS)	Encryption Method	Encryption Algorithm
IKEv1	Main	Route	No Algorithm	group14	ESP	aes-256-gcm

Configuring IPsec VPN with ECDSA signature IKE authentication on the Initiator

To configure the IPsec VPN with ECDSA signature IKE authentication on the initiator:

1. Configure the PKI. See, Example: Configuring PKI.
2. Generate the ECDSA key pair. See Example: Generating a Public-Private Key Pair.
3. Generate and load CA certificate. See Example: Loading CA and Local Certificates Manually.
4. Load CRL. See Example: Manually Loading a CRL onto the Device .
5. Generate and load a local certificate. See Example: Loading CA and Local Certificates Manually.

6. Configure the IKE proposal.

```
[edit security ike]
user@host# set proposal ike-proposal1 authentication-method ecdsa-signatures-256
user@host# set proposal ike-proposal1 dh-group group14
user@host# set proposal ike-proposal1 authentication-algorithm sha-384
user@host# set proposal ike-proposal1 encryption-algorithm aes-256-cbc
```

NOTE: Here, `ike-proposal1` is the IKE proposal name given by the authorized administrator.

7. Configure the IKE policy.

```
[edit security ike]
user@host# set policy ike-policy1 mode main
user@host# set policy ike-policy1 proposals ike-proposal1
user@host# set policy ike-policy1 certificate local-certificate cert1
```

8. Configure the IPsec proposal.

```
[edit security ipsec]
user@host# set proposal ipsec-proposal1 protocol esp
user@host# set proposal ipsec-proposal1 encryption-algorithm aes-256-gcm
```

NOTE: Here, `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

9. Configure the IPsec policy.

```
[edit security ipsec]
user@host# set policy ipsec-policy1 perfect-forward-secrecy keys group14
user@host# set policy ipsec-policy1 proposals ipsec-proposal1
```

NOTE: Here, `ipsec-policy1` is the IPsec policy name and `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

10. Configure IKE.

```
[edit security ike]
user@host# set gateway gw1 ike-policy ike-policy1
user@host# set gateway gw1 address 192.0.2.8
user@host# set gateway gw1 local-identity inet 192.0.2.5
user@host# set gateway gw1 external-interface ge-0/0/2
```

NOTE: Here, `gw1` is an IKE gateway name, `192.0.2.8` is the peer VPN endpoint IP, `192.0.2.5` is the local VPN endpoint IP, and `ge-0/0/2` is a local outbound interface as the VPN endpoint. The following configuration is also needed for IKEv2.

```
[edit security ike]
user@host# set gateway gw1 version v2-only
```

11. Configure the VPN.

```
[edit]
user@host# set security ipsec vpn vpn1 ike gateway gw1
user@host# set security ipsec vpn vpn1 ike ipsec-policy ipsec-policy1
user@host# set security ipsec vpn vpn1 bind-interface st0.0
user@host# set routing-options static route 192.0.2.10/24 qualified-next-hop st0.0
preference 1
```

NOTE: Here, `vpn1` is the VPN tunnel name given by the authorized administrator.

12. Configure the outbound flow policies.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
```

```
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application any
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-
close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

13. Configure the inbound flow policies.

```
[edit security policies]
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match source-address
untrustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match destination-
address trustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match application any
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then permit
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-init
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-
close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

14. Commit your configuration.

```
user@host# commit
```

Configuring IPsec VPN with ECDSA signature IKE authentication on the Responder

To configure IPsec VPN with ECDSA signature IKE authentication on the responder:

1. Configure the PKI. See, Example: Configuring PKI.

2. Generate the ECDSA key pair. See Example: Generating a Public-Private Key Pair.
3. Generate and load CA certificate. See Example: Loading CA and Local Certificates Manually.
4. Load the CRL. See Example: Manually Loading a CRL onto the Device .
5. Configure the IKE proposal.

```
[edit security ike]
user@host# set proposal ike-proposal1 authentication-method ecdsa-signatures-256
user@host# set proposal ike-proposal1 dh-group group14
user@host# set proposal ike-proposal1 authentication-algorithm sha-384
user@host# set proposal ike-proposal1 encryption-algorithm aes-256-cbc
```

NOTE: Here, `ike-proposal1` is the IKE proposal name given by the authorized administrator.

6. Configure the IKE policy.

```
[edit security ike]
user@host# set policy ike-policy1 mode main
user@host# set policy ike-policy1 proposals ike-proposal1
user@host# set policy ike-policy1 certificate local-certificate cert1
```

7. Configure the IPsec proposal.

```
[edit security ipsec]
user@host# set proposal ipsec-proposal1 protocol esp
user@host# set proposal ipsec-proposal1 encryption-algorithm aes-256-gcm
```

NOTE: Here, `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

8. Configure the IPsec policy.

```
[edit security ipsec]
user@host# set policy ipsec-policy1 perfect-forward-secrecy keys group14
user@host# set policy ipsec-policy1 proposals ipsec-proposal1
```

NOTE: Here, `ipsec-policy1` is the IPsec policy name and `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

9. Configure the IKE.

```
[edit security ike]
user@host# set gateway gw1 ike-policy ike-policy1
user@host# set gateway gw1 address 192.0.2.5
user@host# set gateway gw1 local-identity inet 192.0.2.8
user@host# set gateway gw1 external-interface ge-0/0/1
```

NOTE: Here, `gw1` is an IKE gateway name, `192.0.2.5` is the peer VPN endpoint IP, `192.0.2.8` is the local VPN endpoint IP, and `ge-0/0/1` is a local outbound interface as the VPN endpoint. The following configuration is also needed for IKEv2.

```
[edit security ike]
user@host# set gateway gw1 version v2-only
```

10. Configure the VPN.

```
[edit]
user@host# set security ipsec vpn vpn1 ike gateway gw1
user@host# set security ipsec vpn vpn1 ike ipsec-policy ipsec-policy1
user@host# set security ipsec vpn vpn1 bind-interface st0.0
user@host# set routing-options static route 192.0.2.1/24 qualified-next-hop st0.0
preference 1
```

NOTE: Here, `vpn1` is the VPN tunnel name given by the authorized administrator.

11. Configure the outbound flow policies.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application any
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-
close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

12. Configure the inbound flow policies.

```
[edit security policies]
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match source-address
untrustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match destination-
address trustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match application any
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then permit
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-init
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-
close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

13. Commit your configuration.

```
user@host# commit
```

Configuring the Lifetime for an IKE SA

The IKE lifetime sets the lifetime of an IKE SA. When the IKE SA expires, it is replaced by a new SA (and SPI) or is terminated. The default value IKE lifetime is 3600 seconds.

To configure the IKE lifetime, include the lifetime-seconds statement and specify the number of seconds (180 through 86,400) at the `[edit security ike proposal ike-proposal-name]` hierarchy level:

```
[edit security ike proposal ike-proposal-name]
lifetime-seconds seconds;
```

Configuring the Lifetime for an IPsec SA

The IPsec lifetime option sets the lifetime of an IPsec SA. When the IPsec SA expires, it is replaced by a new SA (and SPI) or is terminated. A new SA has new authentication and encryption keys, and SPI; however, the algorithms may remain the same if the proposal is not changed. If lifetime is not configured and a lifetime is not sent by a responder, the lifetime is 28,800 seconds.

To configure the IPsec lifetime, include the lifetime-seconds statement and specify the number of seconds (180 through 28,800) at the `[edit security ipsec proposal ipsec-proposal-name]` hierarchy level:

```
[edit security ipsec proposal ike-proposal-name]
lifetime-seconds seconds;
```

To configure the IPsec lifetime by number of bytes, include the lifetime-kilobytes and Specify the lifetime (in kilobytes) of an IPsec security association (SA). If this statement is not configured, the number of kilobytes used for the SA lifetime is unlimited.

Range: 64 through 4,294,967,294 kilobytes at the `[edit security ipsec proposal ipsec-proposal-name]` hierarchy level:

```
[edit security ipsec proposal ipsec-proposal-name]
lifetime-kilobytes kilobytes;
```

Configuring Remote IKE IDs

By default, the IKE ID received from the peer is validated with the IP address configured for the IKE gateway. In certain network setups, the IKE ID received from the peer (the IKE ID can be an IPv4 or IPv6 address, email id, fully qualified domain name (FQDN), or a distinguished name) does not match the IKE gateway configured on the device. This can lead to a Phase 1 validation failure.

To configure the IKE ID perform the following steps:

1. Configure the remote-identity statement at the set security ike gateway gateway-name hierarchy

   level to match the IKE ID that is received from the peer. The IKE ID values can be an IPv4 address or an IPv6 address, email id, FQDN, or a distinguished name.

2. On the peer device, ensure that the IKE ID is the same as the remote-identity configured on the device. If the peer device is a Junos OS device, configure the local-identity statement at the set security ike gateway gateway-name hierarchy level. The IKE ID values can be an IPv4 address or an IPv6 address, email id, FQDN, or a distinguished name.

RELATED DOCUMENTATION

- Public Key Infrastructure Feature Guide for Security Devices

10

CHAPTER

Configuring Security Flow Policies

Understanding a Security Flow Policy on a Device Running Junos OS

IN THIS SECTION

You can define a security flow policy on a device running Junos OS to inspect and process network packets. The device can permit, deny, and log operations to be associated with each policy. Each of these policies are associated to zones on which distinct network interfaces are bound.

The following modes can be defined for a security flow policy to determine how a device directs traffic:

- Bypass—The `Permit` option directs the traffic traversing the device through the stateful firewall inspection, but not through the IPsec VPN tunnel.
- Discard—The `Deny` option inspects and drops all packets that do not match any `Permit` policies.
- Protect—The traffic is routed through an IPsec tunnel based on the combination of route lookup and `Permit` policy inspection.
- Log—This option logs traffic and session information for all the modes mentioned above.

The following sections describe how to configure a security policy for each of these modes:

- "Configuring a Security Flow Policy in Firewall Bypass Mode" on page 206
- "Configuring a Security Policy in Firewall Discard Mode" on page 207
- "Configuring a Security Flow Policy in IPsec Protect Mode" on page 208

Configuring a Security Flow Policy in Firewall Bypass Mode

To configure a security flow policy for firewall bypass mode:

- Configure the security policies.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application any
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then session-close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses. `junos-ssh` is an example of a Junos OS default predefined application that can be configured in a security policy to enforce SSH traffic.

Configuring a Security Policy in Firewall Discard Mode

To configure a security flow policy for firewall discard mode:

- Configure the security policies.

```
[edit security policies]
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match source-address
untrustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match destination-
address trustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match application junos-
telnet
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then deny
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-init
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then session-close
```

NOTE: Here, `trustZone` and `untrustZone` are the preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses. `junos-telnet` is an example of a Junos OS

default predefined application that can be configured in a security policy to enforce Telnet traffic.

Configuring a Security Flow Policy in IPsec Protect Mode

To configure a security flow policy for IPSec protect mode:

1. Configure the VPN.

```
[edit]
user@host# set security ipsec vpn vpn1 ike gateway gw1
user@host# set security ipsec vpn vpn1 ike ipsec-policy ipsec-policy1
user@host# set security ipsec vpn vpn1 bind-interface st0.0
user@host# set routing-options static route 198.51.100.14/24 qualified-next-hop st0.0
preference 1
```

NOTE: Here, `gw1` and `ipsec-policy1` are preconfigured IKE and IPsec policies.

2. Configure the security policies.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application any
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then session-close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

For more information on stateful session behavior, see Traffic Processing on SRX Series Devices Overview.

For more information on how to configure known good and bad lists, see Configuring Security Policies.

For more information on scheduling security policies, see Scheduling Security Policies and Policer Implementation Overview.

RELATED DOCUMENTATION

Configuring VPN on a Device Running Junos OS

Configuring VPN on a Device Running Junos OS | **181**

CHAPTER 11

Configuring Traffic Filtering Rules

Overview

By default, the TOE denies all traffic through an SRX Series Firewall. In fact, an implicit default security policy exists that denies all packets. You can change this behavior by configuring a standard security policy that permits certain types of traffic. The implicit default policy can be changed to permit all traffic with the `set security policies default-policy` command; however, this is not recommended.

The security policy rule set is an ordered list of security policy entries enforced by the firewall rules, each of which contains the specification of a network flow and an action:

- Source IP address and network mask
- Destination IP address and network mask
- Protocol
- Source port
- Destination port
- Action: permit, deny, drop silently, log

Each packet is compared against entries in the security policy rule set in sequential order until one is found that matches the specification in the policy, or until the end of the rule set is reached, in which case the implicit default policy is implemented and the packet is discarded.

RELATED DOCUMENTATION

Reordering Security Policies

Understanding Protocol Support

Devices running Junos OS can be configured to perform stateful network traffic filtering on network packets using network traffic protocols and network fields as described in Table 12 on page 212 .

Table 12: Network Traffic Protocols and Fields

Protocol or RFC	Fields
ICMPv4 - RFC 792, Internet Control Message Protocol version 4	• Type • Code
ICMPv6 - RFC 4443, Internet Control Message Protocol version 6	• Type • Code
IPv4 - RFC 791, Internet Protocol	• Source address • Destination address • Transport Layer Protocol
IPv6 - RFC 8200, Internet Protocol	• Source address • Destination address • Transport Layer Protocol
TCP - RFC 793, Transmission Control Protocol	• Source port • Destination port
UDP - RFC 768, User Datagram Protocol	• Source port • Destination port

The following protocols are also supported on devices running Junos OS and are a part of this evaluation.

- IPsec
- IKE
- SSH

The following protocols are supported on devices running Junos OS but are not included in the scope of this evaluation.

- OSPF
- BGP
- RIP

The firewall filter terms are evaluated in the order in which they are configured. To configure the order of rule processing, see Firewall Filter Terms.

RELATED DOCUMENTATION

Configuring Traffic Filter Rules | 213

Configuring Traffic Filter Rules

Traffic filter rules can be configured on a device to enforce validation against protocols attributes and direct traffic accordingly to the configured attributes. These rules are based on zones on which network interfaces are bound.

The following procedure describes how to configure traffic filter rules to direct FTP traffic from source `trustZone` to destination `untrustZone` and from source network `trustLan` to destination network `untrustLan`. Here, traffic is traversing from the devices interface A on `trustZone` to interface B on `untrustZone`.

1. Configure a zone and its interfaces.

```
[edit]
user@host# set security zones security-zone trustLan interfaces ge-0/0/0
```

2. Configure the security policy in the specified zone-to-zone direction and specify the match criteria.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application ftp
```

3. Configure the security policy in the specified zone-to-zone direction and specify the action to take when a packet matches a criteria.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then session-close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

Configuring Default Deny-All and Reject Rules

By default, security devices running Junos OS deny traffic unless rules are explicitly created to allow it using the following command:

```
[edit]
user@host#set security policies default-policy deny-all
```

You can configure your security devices running Junos OS to enforce the following default reject rules with logging on all network traffic:

- Invalid fragments
- Fragmented IP packets that cannot be reassembled completely
- Where the source address is equal to the address of the network interface
- Where the source address does not belong to the networks associated with the network interface
- Where the source address is defined as being on a broadcast network
- Where the source address is defined as being on a multicast network
- Where the source address is defined as being a loopback address
- Where the source address is a multicast packet
- Where the source or destination address is a link-local address

- Where the source or destination address is defined as being an address “reserved for future use” as specified in RFC 5735 for IPv4
- Where the source or destination address is defined as an “unspecified address” or an address “reserved for future definition and use” as specified in RFC 3513 for IPv6
- With the IP option Loose Source Routing, Strict Source Routing, or Record Route is specified

Logging the Dropped Packets Using Default Deny-all Option

The evaluated configuration device drops all IPv6 traffic by default. This topic describes how to log packets dropped by this default deny-all option.

1. Before you begin, log in with your root account on a Junos OS device running Junos OS Release 22.2R2 and edit the configuration.

> **NOTE**: You can enter the configuration commands in any order and commit all the commands at once.

To log packets dropped by the default deny-all option:

1. Configure a network security policy in a global context and specify the security policy match criteria.

```
[edit security policy]
user@host# set global policy always-last-default-deny-and-log match source-address any
destination-address any application any
```

2. Specify the policy action to take when the packet matches the criteria.

```
[edit security policy]
user@host# set global policy always-last-default-deny-and-log then deny
```

3. Configure the security policy to enable logs at the session initialization time.

```
[edit security policy]
user@host# set global policy always-last-default-deny-and-log then log session-init
```

NOTE: This procedure might capture a very large amount of data until you have configured the other policies.

To permit all IPv6 traffic into an SRX Series Firewall, configure the device with flow-based forwarding mode. While the default policy in flow-based forwarding mode is still to drop all IPv6 traffic, you can now add rules to permit selected types of IPv6 traffic.

```
user@host# set security forwarding-options family inet6 mode flow-based
```

Configuring Mandatory Reject Rules for Invalid Fragments and Fragmented IP Packets

This topic describes how to configure mandatory reject rules for invalid fragments and fragmented IP packets that cannot be reassembled.

1. Before you begin, log in with your root account on a Junos OS device running Junos OS Release 22.2R2 and edit the configuration.

NOTE: You can enter the configuration commands in any order and commit all the commands at once.

To configure mandatory reject rules:

1. Specify the flow configuration to forcefully reassemble the IP fragments.

```
[edit]
user@host# set security flow force-ip-reassembly
```

2. Delete the screen ID and the IDS options and enable the ICMP fragment IDS option.

```
[edit]
user@host# delete security screen ids-option trustScreen icmp fragment
```

3. Delete the IP layer IDS option and enable the IP fragment blocking IDS option.

```
[edit]
user@host# delete security screen ids-option trustScreen ip block-frag
```

Configuring Default Reject Rules for Source Address Spoofing

The following guidelines describe when to configure the default reject rules for source address spoofing:

- When the source address is equal to the address of the network interface where the network packet was received.
- When the source address does not belong to the networks associated with the network interface where the network packet was received.
- When the source address is defined as being on a broadcast network.

1. Before you begin, log in with your root account on a Junos OS device running Junos OS Release 22.2R2 and edit the configuration.

NOTE: You can enter the configuration commands in any order and commit all the commands at once.

To configure default reject rules to log source address spoofing:

1. Configure the security screen features and enable the IP address spoofing IDS option.

```
[edit]
user@host# set security screen ids-option trustScreen ip spoofing
```

2. Specify the name of the security zone and the IDS option object applied to the zone.

```
[edit]
user@host# set security zones security-zone trustZone screen trustScreen
```

Configuring Default Reject Rules with IP Options

This topic describes how to configure default reject rules with IP options. The IP options enable the device to either block any packets with loose or strict source route options or detect such packets and then record the event in the counters list for the ingress interface.

1. Before you begin, log in with your root account to an SRX Series Firewall running Junos OS Release 22.2R2.

> **NOTE**: You can enter the configuration commands in any order and commit all the commands at once.

To configure the default reject rules with IP options:

1. Configure the screen features to enable IP options.

```
[edit security screen ids-option trustScreen]
user@host# set ip source-route-option
user@host# set ip loose-source-route-option
user@host# set ip strict-source-route-option
user@host# set ip record-route-option
```

2. Specify the name of the security zone and the IDS option object applied to the zone.

```
[edit]
user@host# set security zones security-zone trustZone screen trustScreen
```

Configuring Default Reject Rules

The following guidelines describe when to configure the default reject rules:

- Source address is defined on a multicast network, a loopback address, or a multicast address.
- The source or destination address of a packet is a link-local address, an address “reserved for future use” as specified in RFC 5735 for IPv4, an “unspecified address” or an address “reserved for future definition and use” as specified in RFC 3513 for IPv6.
- An illegal or out-of-sequence TCP packet is received.

1. Before you begin, log in with your root account on a Junos OS device running Junos OS Release 22.2R2 and edit the configuration.

   NOTE: You can enter the configuration commands in any order and commit all the commands at once.

To configure default reject rules:

1. Configure the security screen features and enable the IP address spoofing IDS option.

```
[edit]
user@host# set security screen ids-option trustScreen ip spoofing
```

2. Configure the security flow feature to log the dropped illegal packets.

```
[edit]
user@host# set security flow log dropped-illegal-packet
```

3. Specify the name of the security zone and the IDS option object applied to the zone.

```
[edit]
user@host# set security zones security-zone trustZone screen trustScreen
```

4. Configure the mandatory TCP reject rule.

```
[edit]
user@host# set security flow tcp-session strict-syn-check
```

12
CHAPTER

Configuring Network Attacks

Configuring IP Teardrop Attack Screen

This topic describes how to configure detection of an IP teardrop attack.

Teardrop attacks exploit the reassembly of fragmented IP packets. In the IP header, one of the field is the fragment offset fields, which indicates the starting position, or offset of the data contained in a fragmented packet, relative to the data of the original unfragmented packet. When the sum of the offset and size of one fragmented packet differs from that of the next fragmented packet, the packets overlap and the server attempting to reassemble the packet might crash.

To enable detection of a teardrop attack:

1. Configure interfaces and assign IP addresses to the interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones **trustZone** and **untrustZone** and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from **untrustZone** to **trustZone**.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
```

```
permit
user@host# set security policies default-policy deny-all
```

4. Configure the security screen option and attach it to the **untrustZone**.

```
[edit]
user@host# set security screen ids-option untrustScreen ip tear-drop
user@host# set security zones security-zone untrustZone screen untrustScreen
user@host# set security screen ids-option untrustScreen alarm-without-drop
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog explicit-priority
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

```
[edit]
user@host# commit
```

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

Attack Detection and Prevention User Guide for Security Devices

Configuring TCP Land Attack Screen

This topic describes how to configure detection of a TCP land attack.

Land attacks occur when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and the source IP address.

To enable detection of a TCP land attack:

1. Configure interfaces and assign IP addresses to the interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones **trustZone** and **untrustZone** and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from **untrustZone** to **trustZone**.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to **untrustZone**.

```
[edit]
user@host# set security screen ids-option untrustScreen tcp land
user@host# set security zones security-zone untrustZone screen untrustScreen
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog explicit-priority
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

```
[edit]
user@host# commit
```

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

Attack Detection and Prevention User Guide for Security Devices

Configuring ICMP Fragment Screen

This topic describes how to configure detection of an ICMP fragment attack.

If an ICMP packet is large, then it must be fragmented. When the ICMP fragment protection screen option is enabled, the Junos OS blocks any ICMP packet that has many fragment flags set or that has an offset value indicated in the offset field.

To enable detection of an ICMP fragment IDS attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones **trustZone** and **untrustZone** and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from **untrustZone** to **trustZone**.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to **untrustZone**.

```
[edit]
user@host# set security screen ids-option untrustScreen icmp fragment
user@host# set security zones security-zone untrustZone screen untrustScreen
user@host# set security screen ids-option untrustScreen alarm-without-drop
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog explicit-priority
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

```
[edit]
user@host# commit
```

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

Attack Detection and Prevention User Guide for Security Devices

Configuring Ping-Of-Death Attack Screen

This topic describes how to configure detection of ping-of-death attack.

The IP datagram with the protocol field of the IP header is set to 1 (ICMP), the last fragment bit is set, and (IP offset * 8) + (IP data length) > 65535. The IP offset (which represents the starting position of this fragment in the original packet, and which is in 8-byte units) plus the rest of the packet is greater than the maximum size for an IP packet.

To enable detection of a ping-of-death IDP attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones **trustZone** and **untrustZone** and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from **untrustZone** to **trustZone**.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to **untrustZone**.

```
[edit]
user@host# set security screen ids-option untrustScreen icmp ping-death
user@host# set security zones security-zone untrustZone screen untrustScreen
user@host# set security screen ids-option untrustScreen alarm-without-drop
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog explicit-priority
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

```
[edit]
user@host# commit
```

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

Attack Detection and Prevention User Guide for Security Devices

Configuring tcp-no-flag Attack Screen

This topic describes how to configure detection of a `tcp-no-flag` attack.

A TCP segment with no control flags set is an anomalous event causing various responses from the recipient. When the TCP no-flag is enabled, the device detects the TCP segment headers with no flags set, and drops all TCP packets with missing or malformed flag fields.

To enable detection of a `tcp-no-flag` option:

1. Configure interfaces and assign an IP address to the interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones **trustZone** and **untrustZone** and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from **untrustZone** to **trustZone**.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to **untrustZone**.

```
[edit]
user@host# set security screen ids-option untrustScreen tcp tcp-no-flag
user@host# set security zones security-zone untrustZone screen untrustScreen
user@host# set security screen ids-option untrustScreen alarm-without-drop
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog explicit-priority
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

```
[edit]
user@host# commit
```

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

Attack Detection and Prevention User Guide for Security Devices

Configuring TCP SYN-FIN Attack Screen

This topic describes how to configure detection of a TCP SYN-FIN attack.

A TCP header with the SYN and FIN flags set is anomalous TCP behavior causing various responses from the recipient, depending on the OS. Blocking packets with SYN and FIN flags helps prevent the OS system probes.

To enable detection of TCP SYN-FIN bits:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones **trustZone** and **untrustZone** and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from **untrustZone** to **trustZone**.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to **untrustZone**.

```
[edit]
user@host# set security screen ids-option untrustScreen tcp syn-fin
user@host# set security zones security-zone untrustZone screen untrustScreen
user@host# set security screen ids-option untrustScreen alarm-without-drop
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog explicit-priority
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

```
[edit]
user@host# commit
```

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

Attack Detection and Prevention User Guide for Security Devices

Configuring TCP fin-no-ack Attack Screen

This topic describes how to configure detection of TCP `fin-no-ack` attack. A TCP header with the FIN flag set but not the ACK flag is anomalous TCP behavior.

To enable detection of FIN bits with no ACK bit IDS option:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones **trustZone** and **untrustZone** and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from **untrustZone** to **trustZone**.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to **untrustZone**.

```
[edit]
user@host# set security screen ids-option untrustScreen tcp fin-no-ack
user@host# set security zones security-zone untrustZone screen untrustScreen
user@host# set security screen ids-option untrustScreen alarm-without-drop
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog explicit-priority
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
```

```
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

```
[edit]
user@host# commit
```

RELATED DOCUMENTATION

- IDP Extended Package Configuration Overview | 249
- Attack Detection and Prevention User Guide for Security Devices

Configuring UDP Bomb Attack Screen

If the UDP length specified is less than the IP length specified then the malformed packet type is associated with a denial-of-service attempt. By default, SRX drops these packets. No configuration is required.

RELATED DOCUMENTATION

- IDP Extended Package Configuration Overview | 249
- Attack Detection and Prevention User Guide for Security Devices

Configuring UDP CHARGEN DoS Attack Screen

This topic describes how to configure protection from a UDP CHARGEN DoS attack.

NOTE: UDP packet is detected with a source port of 7 and a destination port of 19 is an attack.

To enable detection of a UDP CHARGEN DoS attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones `trustZone` and `untrustZone` and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from `untrustZone` to the `trustZone` with the Junos OS predefined application `junos-chargen`.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application junos-chargen
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
deny
user@host# set security policies default-policy permit-all
```

4. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog explicit-priority
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
```

```
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

5. To allow the packet to reach the destination, change the policy configuration from `deny` to `permit`.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
```

6. Commit the configuration.

```
[edit]
user@host# commit
```

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

Attack Detection and Prevention User Guide for Security Devices

Configuring TCP SYN and RST Attack Screen

This topic describes how to configure TCP packet when the SYN and RST flags are set.

To enable detection of a TCP SYN and RST attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones `trustZone` the `untrustZone` and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
```

```
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure the IDP custom-attack signatures.

```
[edit]
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 match from-zone any
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 match source-address any
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 match to-zone any
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 match destination-
address any
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 match application default
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 match attacks custom-
attacks syn_rst
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 then action no-action
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 then notification log-
attacks
user@host# set security idp active-policy idpengine
user@host# set security idp custom-attack syn_rst severity info
user@host# set security idp custom-attack syn_rst attack-type signature context packet
user@host# set security idp custom-attack syn_rst attack-type signature pattern
user@host# set security idp custom-attack syn_rst attack-type signature direction any
user@host# set security idp custom-attack syn_rst attack-type signature protocol tcp tcp-
flags rst
user@host# set security idp custom-attack syn_rst attack-type signature protocol tcp tcp-
flags syn
```

4. Configure security policies from `untrustZone` to `trustZone`.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
```

```
permit application-services idp
user@host# set security policies default-policy deny-all
```

5. Configure security `tcp-session` option in flow.

```
[edit]
user@host# set security flow tcp-session no-syn-check
user@host# set security flow tcp-session no-sequence-check
```

6. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog explicit-priority
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

7. To allow the traffic to reach the destination, configure the `tcp-session` option.

```
[edit]
user@host# set security flow tcp-session relax-check
```

8. Commit the configuration.

```
[edit]
user@host# commit
```

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

Attack Detection and Prevention User Guide for Security Devices

Configuring ICMP Flood Attack Screen

This topic describes how to configure detection of an ICMP flood attack.

An ICMP flood typically occurs when an ICMP echo request overloads the victim with many requests such that the ICMP echo request spends all its resources responding until it can no longer process valid network traffic. When enabling the ICMP flood protection feature, you can set a threshold that, once exceeded, invokes the ICMP flood attack protection feature.

To enable detection of an ICMP flood attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones `trustZone` and `untrustZone` and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from `untrustZone` to `trustZone`.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to untrustZone.

```
[edit]
user@host# set security screen ids-option untrustScreen icmp flood
user@host# set security screen ids-option untrustScreen alarm-without-drop
user@host# set security zones security-zone untrustZone screen untrustScreen
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog explicit-priority
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

```
[edit]
user@host# commit
```

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

Attack Detection and Prevention User Guide for Security Devices

Configuring TCP SYN Flood Attack Screen

This topic describes how to configure detection of a TCP SYN flood attack.

A SYN flood occurs when a host is so overwhelmed by SYN segments initiating incomplete connection requests that it can no longer process legitimate connection requests.

To enable detection of a TCP SYN flood attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones trustZone and untrustZone and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from untrustZone to trustZone.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to untrustZone.

```
[edit]
user@host# set security screen ids-option untrustScreen tcp syn-flood
user@host# set security screen ids-option untrustScreen alarm-without-drop
user@host# set security zones security-zone untrustZone screen untrustScreen
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog explicit-priority
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

```
[edit]
user@host# commit
```

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

Attack Detection and Prevention User Guide for Security Devices

Configuring TCP Port Scan Attack Screen

This topic describes how to configure detection of a TCP port scan attack.

A port scan occurs when one source IP address sends an IP packet containing TCP SYN segments to a defined number of different ports at the same destination IP address within a defined interval.

To enable detection of a TCP port scan attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones trustZone and untrustZone and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from untrustZone to trustZone.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to untrustZone.

```
[edit]
user@host# set security screen ids-option untrustScreen tcp port-scan
user@host# set security screen ids-option untrustScreen alarm-without-drop
user@host# set security zones security-zone untrustZone screen untrustScreen
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog explicit-priority
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
```

```
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

```
[edit]
user@host# commit
```

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

Attack Detection and Prevention User Guide for Security Devices

Configuring UDP Port Scan Attack Screen

This topic describes how to configure detection of a UDP port scan attack.

These attacks scan the target IP addresses for open, listening, or responsive services by targeting multiple protocols or ports on one or more target IP address using obvious (sequentially numbered) patterns of the target protocol or port numbers. The patterns are derived by randomizing the protocol or port numbers and randomizing the time delays between the transmissions.

To enable detection of a UDP port scan attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones `trustZone` and `untrustZone` and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
```

```
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from `untrustZone` to `trustZone`.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to `untrustZone`.

```
[edit]
user@host# set security screen ids-option untrustScreen udp port-scan
user@host# set security screen ids-option untrustScreen alarm-without-drop
user@host# set security zones security-zone untrustZone screen untrustScreen
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog explicit-priority
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

```
[edit]
user@host# commit
```

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

Attack Detection and Prevention User Guide for Security Devices

Configuring IP Sweep Attack Screen

This topic describes how to configure detection of an IP sweep attack.

An address sweep occurs when one source IP address sends a defined number of ICMP packets to different hosts within a defined time interval (5000 microseconds is the default value). The purpose of this attack is to send ICMP packets—typically echo requests—to various hosts in the hope that at least one replies, thus uncovering an address to target.

To enable detection of an IP sweep attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones `trustZone` and `untrustZone` and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from `untrustZone` to `trustZone`.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
```

```
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to untrustZone.

```
[edit]
user@host# set security screen ids-option untrustScreen icmp ip-sweep
user@host# set security screen ids-option untrustScreen alarm-without-drop
user@host# set security zones security-zone untrustZone screen untrustScreen
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog explicit-priority
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

```
[edit]
user@host# commit
```

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

Attack Detection and Prevention User Guide for Security Devices

13

CHAPTER

Configuring the IDP Extended Package

IDP Extended Package Configuration Overview

The Junos OS Intrusion Detection and Prevention (IDP) policy enables you to selectively enforce various attack detection and prevention techniques on network traffic passing through an IDP-enabled device. It allows you to define policy rules to match a section of traffic based on a zone, network, and application, and then take active or passive preventive actions on that traffic.

An IDP policy defines how your device handles the network traffic. It allows you to enforce various attack detection and prevention techniques on traffic traversing your network.

A policy is made up of rule bases, and each rule base contains a set of rules. You define rule parameters, such as traffic match conditions, action, and logging requirements, then add the rules to rule bases. After you create an IDP policy by adding rules in one or more rule bases, you can select that policy to be the active policy on your device.

To configure the IDP extended package (IPS-EP) perform the following steps:

1. Enable IPS in a security policy. See Configuring IDP Policy Rules and IDP Rulebases.
2. Configure IDP policy rules, IDP rule bases, and IDP rule actions. See Configuring IDP Policy Rules and IDP Rulebases .
3. Configure IDP custom signatures. SeeUnderstanding IDP Signature-Based Attacks
4. Update the IDP signature database. SeeIntrusion Detection and Prevention Feature Guide for Security Devices.

RELATED DOCUMENTATION

- Intrusion Detection and Prevention Feature Guide for Security Devices

14

CHAPTER

Configuring Cluster Mode

Understanding Cluster Mode

The Administrator of the TOE can set up the Cluster Mode for High Availability (HA) by connecting HA control port em0 on node 0 to the HA control port em0 on node 1 as described in the article - https://kb.juniper.net/KB34608.

The factory-default configuration does not include HA configuration. To enable HA, if the physical interfaces used by HA have some configurations, these configurations need to be removed. The two hosts constituting a chassis cluster must have identical configuration except for one being configured to node 0 and the other to node 1.

The TOE has a dedicated fxp0 interface for the HA management of the TOE. The interface for HA control link must be between em0 on each device. The fabric interface may be defined by the Administrator. After the cluster has been defined and set up by the Administrator, the two devices constituting a chassis cluster have identical cluster-id but difference node ID as one host most be node 0 and the other one node 1. For vSRX Virtual Firewall instances the ge-0/0/1 interface on node1 changes to ge-7/0/1.

The node 1 renumbers its interfaces by adding the total number of system FPCs to the original FPC number of the interface. The fabric interface remains Administrator-defined.

With L2 HA link encryption tunnel, any Security Sensitive Parameters (Critical Security Parameters) exchanged over the control link between the two chassis in cluster mode are protected using IPsec. The configuration information and IKE HA messages that pass through the chassis cluster link from the primary node to the secondary node are protected from active and passive eavesdropping by using IPsec for internal communication between nodes. An attacker cannot gain privilege access or observe traffic, without the internal IPsec key.

Configuring L2 HA Link Encryption tunnel

Physically connect the two devices and ensure that they are the same models. Connect the dedicated control ports on node 0 and node 1. Connect the user defined fabricated ports on node 0 and node 1. To configure two chassis in cluster mode, follow the below steps:

1. Zeroize both the SRX Series Firewalls before you use for cluster. If the devices are already in cluster mode please make sure you disable them before the zeroize process. For information on how to disable chassis cluster, see Disabling a Chassis Cluster. Zeroize is achieved by removing the vSRX Virtual Firewall virtual machine from the datastore as mentioned in "Understanding Zeroization" on page 31 .

2. Delete the web management services.

```
user@host# delete system services web-management
```

3. Configure FIPS mode and bring up the devices in FIPS mode.

```
[edit]
     user@host# set groups global system fips level 2
    [edit]
     user@host# set groups global system root-authentication plain-textpassword
     New password: type password here
     Retype new password: retype password here
    [edit]
     user@host# commit
     user@host> request system reboot
```

4. Configure device 1 with standard cluster commands for operating in cluster mode as node0 with control port configuration. See Chassis Cluster Control Plane Interfaces.

```
[edit]
user@host# set groups node0 system host-name node0-host-name
user@host# set groups node0 system backup-router gateway-address
user@host# set groups node0 system backup-router destination value
user@host# set groups node0 interfaces fxp0 unit 0 family inet address node0-ip-address
user@host# set groups node1 system host-name node1-host-name
user@host# set groups node1 system backup-router gateway-address
user@host# set groups node1 system backup-router destination value
user@host# set groups node1 interfaces fxp0 unit 0 family inet address node1-ip-address
user@host# set apply-groups global
user@host# set apply-groups "$(node)"
user@host# delete apply-groups re0
user@host# set system ports console log-out-on-disconnect
user@host# set chassis cluster reth-count 5
user@host# set chassis cluster redundancy-group 0 node 0 priority 254
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
user@host# commit
user@host> set chassis cluster cluster-id 1 node 0 reboot
```

5. After the device 1 is up, configure HA link encryption as shown in sample configuration below, commit and reboot. Device 1 needs to be configured with both node0 and node1 HA link encryption configuration before commit and reboot.

```
[edit]
user@host# set groups node0 security ike traceoptions file ikelog
user@host# set groups node0 security ike traceoptions file size 100m
user@host# set groups node0 security ike traceoptions flag all
user@host# set groups node0 security ike traceoptions level 15
user@host# set groups node0 security ike proposal IKE_PROP_PSK authentication-method pre-
shared-keys
user@host# set groups node0 security ike proposal IKE_PROP_PSK dh-group group20
user@host# set groups node0 security ike proposal IKE_PROP_PSK authentication-algorithm
sha-256
user@host# set groups node0 security ike proposal IKE_PROP_PSK encryption-algorithm aes-256-
cbc
user@host# set groups node0 security ike policy IKE_POL_PSK proposals IKE_PROP_PSK
user@host# prompt groups node0 security ike policy IKE_POL_PSK pre-shared-key ascii-text New
ascii-text (secret): juniper
Retype new ascii-text (secret): juniper
user@host# set groups node0 security ike gateway S2S_GW ike-policy IKE_POL_PSK
user@host# set groups node0 security ike gateway S2S_GW version v2-only
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK protocol esp
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK authentication-algorithm
hmac-sha1-96
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK encryption-algorithm
aes-256-cbc
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK lifetime-seconds 200
user@host# set groups node0 security ipsec policy IPSEC_POL_PSK perfect-forward-secrecy keys
group20
user@host# set groups node0 security ipsec policy IPSEC_POL_PSK proposal IPSEC_PROP_PSK
user@host# set groups node0 security ipsec vpn S2S_VPN ha-link-encryption
user@host# set groups node0 security ipsec vpn S2S_VPN ike gateway S2S_GW
user@host# set groups node0 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PSK
user@host# set groups node1 security ike traceoptions file ikelog
user@host# set groups node1 security ike traceoptions file size 100m
user@host# set groups node1 security ike traceoptions flag all
user@host# set groups node1 security ike traceoptions level 15
user@host# set groups node1 security ike proposal IKE_PROP_PSK authentication-method pre-
shared-keys
user@host# set groups node1 security ike proposal IKE_PROP_PSK dh-group group20
user@host# set groups node1 security ike proposal IKE_PROP_PSK authentication-algorithm
```

```
sha-256
user@host# set groups node1 security ike proposal IKE_PROP_PSK encryption-algorithm aes-256-
cbc
user@host# set groups node1 security ike policy IKE_POL_PSK proposals IKE_PROP_PSK
user@host# prompt groups node1 security ike policy IKE_POL_PSK pre-shared-key ascii-text New
ascii-text(secret): juniper
Retype new ascii-text (secret): juniper
user@host# set groups node1 security ike gateway S2S_GW ike-policy IKE_POL_PSK
user@host# set groups node1 security ike gateway S2S_GW version v2-only
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK protocol esp
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK authentication-algorithm
hmac-sha1-96
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK encryption-algorithm
aes-256-cbc
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK lifetime-seconds 200
user@host# set groups node1 security ipsec policy IPSEC_POL_PSK perfect-forward-secrecy keys
group20
user@host# set groups node1 security ipsec policy IPSEC_POL_PSK proposals IPSEC_PROP_PSK
user@host# set groups node1 security ipsec vpn S2S_VPN ha-link-encryption
user@host# set groups node1 security ipsec vpn S2S_VPN ike gateway S2S_GW
user@host# set groups node1 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PSK
user@host# set groups global interfaces fab0 fabric-options member-interfaces ge-0/0/3
user@host# set groups global interfaces fab1 fabric-options member-interfaces ge-7/0/3
user@host# commit
user@host> request system reboot
```

6. To proceed further with device 2 configuration and commit, you need to ensure device 1 and device 2 are not reachable to each other. One way to achieve this is to power off device 1 at this point.
7. Configure device 2 with standard cluster commands for operating in cluster mode as node1 with control port configuration. See Chassis Cluster Control Plane Interfaces.

```
[edit]
user@host# set groups node0 system host-name node0-host-name
user@host# set groups node0 system backup-router gateway-address
user@host# set groups node0 system backup-router destination value
user@host# set groups node0 interfaces fxp0 unit 0 family inet address node0-ip-address
user@host# set groups node1 system host-name node1-host-name
user@host# set groups node1 system backup-router gateway-address
user@host# set groups node1 system backup-router destination value
user@host# set groups node1 interfaces fxp0 unit 0 family inet address node1-ip-address
user@host# set apply-groups global
```

```
user@host# set apply-groups "$(node)"
user@host# delete apply-groups re0
user@host# set system ports console log-out-on-disconnect
user@host# set chassis cluster reth-count 5
user@host# set chassis cluster redundancy-group 0 node 0 priority 254
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
user@host# commit
user@host> set chassis cluster cluster-id 1 node 1 reboot
```

8. After the device 2 is up, configure HA link encryption as shown in sample configuration below on device 2. Device 2 needs to be configured with both node0 and node1 HA link encryption configuration. Commit on node1 (device 2), and finally reboot node1 (device 2).

```
[edit]
user@host# set groups node0 security ike traceoptions file ikelog
user@host# set groups node0 security ike traceoptions file size 100m
user@host# set groups node0 security ike traceoptions flag all
user@host# set groups node0 security ike traceoptions level 15
user@host# set groups node0 security ike proposal IKE_PROP_PSK authentication-method pre-
shared-keys
user@host# set groups node0 security ike proposal IKE_PROP_PSK dh-group group20
user@host# set groups node0 security ike proposal IKE_PROP_PSK authentication-algorithm
sha-256
user@host# set groups node0 security ike proposal IKE_PROP_PSK encryption-algorithm aes-256-
cbc
user@host# set groups node0 security ike policy IKE_POL_PSK proposals IKE_PROP_PSK
user@host# prompt groups node0 security ike policy IKE_POL_PSK pre-shared-key ascii-text
New ascii-text (secret): juniper
Retype new ascii-text (secret): juniper
user@host# set groups node0 security ike gateway S2S_GW ike-policy IKE_POL_PSK
user@host# set groups node0 security ike gateway S2S_GW version v2-only
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK protocol esp
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK authentication-algorithm
hmac-sha1-96
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK encryption-algorithm
aes-256-cbc
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK lifetime-seconds 200
user@host# set groups node0 security ipsec policy IPSEC_POL_PSK perfect-forward-secrecy keys
group20
user@host# set groups node0 security ipsec policy IPSEC_POL_PSK proposal IPSEC_PROP_PSK
user@host# set groups node0 security ipsec vpn S2S_VPN ha-link-encryption
user@host# set groups node0 security ipsec vpn S2S_VPN ike gateway S2S_GW
```

```
user@host# set groups node0 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PSK
user@host# set groups node1 security ike traceoptions file ikelog
user@host# set groups node1 security ike traceoptions file size 100m
user@host# set groups node1 security ike traceoptions flag all
user@host# set groups node1 security ike traceoptions level 15
user@host# set groups node1 security ike proposal IKE_PROP_PSK authentication-method pre-
shared-keys
user@host# set groups node1 security ike proposal IKE_PROP_PSK dh-group group20
user@host# set groups node1 security ike proposal IKE_PROP_PSK authentication-algorithm
sha-256
user@host# set groups node1 security ike proposal IKE_PROP_PSK encryption-algorithm aes-256-
cbc
user@host# set groups node1 security ike policy IKE_POL_PSK proposals IKE_PROP_PSK
user@host# prompt groups node1 security ike policy IKE_POL_PSK pre-shared-key ascii-text
New ascii-text(secret): juniper
Retype new ascii-text (secret): juniper
user@host# set groups node1 security ike gateway S2S_GW ike-policy IKE_POL_PSK
user@host# set groups node1 security ike gateway S2S_GW version v2-only
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK protocol esp
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK authentication-algorithm
hmac-sha1-96
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK encryption-algorithm
aes-256-cbc
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK lifetime-seconds 200
user@host# set groups node1 security ipsec policy IPSEC_POL_PSK perfect-forward-secrecy keys
group20
user@host# set groups node1 security ipsec policy IPSEC_POL_PSK proposals IPSEC_PROP_PSK
user@host# set groups node1 security ipsec vpn S2S_VPN ha-link-encryption
user@host# set groups node1 security ipsec vpn S2S_VPN ike gateway S2S_GW
user@host# set groups node1 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PSK
user@host# set groups global interfaces fab0 fabric-options member-interfaces ge-0/0/3
user@host# set groups global interfaces fab1 fabric-options member-interfaces ge-7/0/3
user@host# commit
user@host> request system reboot
```

Configuring PKI Based L2HA Link Encryption

- Physically connect the two devices and ensure that they are the same models.

- Connect the dedicated control ports on node 0 and node 1.
- Connect the user defined fabricated ports on node 0 and node 1.

To configure two chassis in cluster mode, follow the below steps:

1. Zeroize both the SRX Series Firewalls before you use for cluster. If the devices are already in cluster mode please ensure you disable them before zeroize. For information on how to disable chassis cluster, see Disabling a Chassis Cluster.
2. Delete the web management services.

   user@host# **delete system services web-management https**
3. Configure FIPS mode and bring up the devices in FIPS mode.

```
[edit]
user@host# set groups global system fips level 2
[edit]
user@host# set groups global system root-authentication plain-textpassword
New password: type password here
Retype new password: retype password here
[edit]
user@host# commit
user@host> request system reboot
```

4. Configure device 1 with standard cluster commands for operating in cluster mode as node0. This requires a reboot.

```
[edit]
user@host# set groups node0 system host-name node0-host-name
user@host# set groups node0 system backup-router gateway-address
user@host# set groups node0 system backup-router destination value
user@host# set groups node0 interfaces fxp0 unit 0 family inet address node0-ip-address
user@host# set groups node1 system host-name node1-host-name
user@host# set groups node1 system backup-router gateway-address
user@host# set groups node1 system backup-router destination value
user@host# set groups node1 interfaces fxp0 unit 0 family inet address node1-ip-address
user@host# set apply-groups global
user@host# set apply-groups "$(node)"
user@host# delete apply-groups re0
user@host# set system ports console log-out-on-disconnect
user@host# set chassis cluster reth-count 5
user@host# set chassis cluster redundancy-group 0 node 0 priority 254
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
user@host# commit
```

```
user@host> set chassis cluster cluster-id 1 node 0 reboot
```

See https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster-verification.html

5. After the device 1 is up, configure HA link encryption as shown in sample configuration below, commit and reboot. device 1 needs to be configured with both node0 and node1 HA link encryption configuration before commit and reboot.

```
[edit]
user@host# set groups node0 security ike traceoptions file ikelog
user@host# set groups node0 security ike traceoptions file size 100m
user@host# set groups node0 security ike traceoptions flag all
user@host# set groups node0 security ike traceoptions level 15
user@host# set groups node0 security pki traceoptions file pkilog
user@host# set groups node0 security pki traceoptions file size 100m
user@host# set groups node0 security pki traceoptions flag all
user@host# set groups node0 security ike proposal IKE_PROP_PKI authentication-method rsa-
signatures
user@host# set groups node0 security ike proposal IKE_PROP_PKI dh-group group20
user@host# set groups node0 security ike proposal IKE_PROP_PKI authentication-algorithm
sha-256
user@host# set groups node0 security ike proposal IKE_PROP_PKI encryption-algorithm aes-256-
cbc
user@host# set groups node0 security ike policy IKE_POL_PKI mode main
user@host# set groups node0 security ike policy IKE_POL_PKI proposals IKE_PROP_PKI
user@host# set groups node0 security ike policy IKE_POL_PKI certificate local-certificate
pkicert
user@host# set groups node0 security ike gateway S2S_GW ike-policy IKE_POL_PKI
user@host# set groups node0 security ike gateway S2S_GW version v2-only
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI protocol esp
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI authentication-algorithm
hmac-sha1-96
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI encryptionalgorithm
aes-128-cbc
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI lifetime-seconds 200
user@host# set groups node0 security ipsec policy IPSEC_POL_PKI perfect-forward-secrecy
keys group20
user@host# set groups node0 security ipsec policy IPSEC_POL_PKI proposals IPSEC_PROP_PKI
user@host# set groups node0 security ipsec vpn S2S_VPN ha-link-encryption
user@host# set groups node0 security ipsec vpn S2S_VPN ike gateway S2S_GW
user@host# set groups node0 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PKI
```

```
user@host# set groups node0 security pki ca-profile S2S_PKI ca-identity S2S_PKI_CA1
user@host# set groups node0 security pki ca-profile S2S_PKI enrollment url <Enrollment URL
of certificate authority>
user@host# set groups node0 security pki ca-profile S2S_PKI revocation-check crl url <CRL
distribution point for certificate authority>
user@host# set groups node0 security pki ca-profile S2S_PKI revocation-check disable
user@host# set groups node0 interfaces st0 unit 0 family inet
user@host# set groups node1 security ike traceoptions file ikelog
user@host# set groups node1 security ike traceoptions file size 100m
user@host# set groups node1 security ike traceoptions flag all
user@host# set groups node1 security ike traceoptions level 15
user@host# set groups node1 security pki traceoptions file pkilog
user@host# set groups node1 security pki traceoptions file size 100m
user@host# set groups node1 security pki traceoptions flag all
user@host# set groups node1 security ike proposal IKE_PROP_PKI authentication-method rsa-
signatures
user@host# set groups node1 security ike proposal IKE_PROP_PKI dh-group group20
user@host# set groups node1 security ike proposal IKE_PROP_PKI authentication-algorithm
sha-256
user@host# set groups node1 security ike proposal IKE_PROP_PKI encryption-algorithm aes-256-
cbc
user@host# set groups node1 security ike policy IKE_POL_PKI mode main
user@host# set groups node1 security ike policy IKE_POL_PKI proposals IKE_PROP_PKI
user@host# set groups node1 security ike policy IKE_POL_PKI certificate local-certificate
pkicert
user@host# set groups node1 security ike gateway S2S_GW ike-policy IKE_POL_PKI
user@host# set groups node1 security ike gateway S2S_GW version v2-only
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PKI protocol esp
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PKI authenticationalgorithm
hmac-sha1-96
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PKI encryptionalgorithm
aes-128-cbc
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PKI lifetime-seconds 200
user@host# set groups node1 security ipsec policy IPSEC_POL_PKI perfect-forward-secrecy
keys group20
user@host# set groups node1 security ipsec policy IPSEC_POL_PKI proposals IPSEC_PROP_PKI
user@host# set groups node1 security ipsec vpn S2S_VPN ha-link-encryption
user@host# set groups node1 security ipsec vpn S2S_VPN ike gateway S2S_GW
user@host# set groups node1 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PKI
user@host# set groups node1 security pki ca-profile S2S_PKI ca-identity S2S_PKI_CA1
user@host# set groups node1 security pki ca-profile S2S_PKI enrollment url <Enrollment URL
of certificate authority>
user@host# set groups node1 security pki ca-profile S2S_PKI revocation-check crl url <CRL
```

```
distribution point for certificate authority>
user@host# set groups node1 security pki ca-profile S2S_PKI revocation-check disable
user@host# set groups node1 interfaces st0 unit 0 family inet
user@host# set groups global interfaces fab0 fabric-options member-interfaces ge-0/0/3
user@host# set groups global interfaces fab1 fabric-options member-interfaces ge-7/0/3
user@host# commit
user@host> clear security pki node-local local-certificate all
user@host> clear security pki node-local certificate-request all
user@host> clear security pki node-local key-pair all
user@host> clear security pki crl all
user@host> clear security pki ca-certificate all
user@host> request security pki node-local generate-key-pair certificate-id pkicert type
rsa size 2048
```

```
root@vm# curl "http://<PKI-Server-IP>/certsrv/certnew.cer?
ReqID=CACert=0=bin" -o /tmp/dut_ca.cer
root@vm# scp /tmp/dut_ca.cer root@node0-host-name:/var/tmp
user@host> request security pki ca-certificate load ca-profile S2S_PKI filename/var/tmp/
dut_ca.cer
user@host> show security pki ca-certificate
```

```
root@vm# curl "http://PKI-Server-IP/certsrv/certcrl.crl?Renewal=0=bin"
-o /tmp/dut.crl
root@vm# scp /tmp/dut.crl root@node0-host-name:/var/tmp
user@host> request security pki crl load ca-profile S2S_PKI filename /var/tmp/dut.crl
user@host> show security pki crl
user@host> request security pki node-local generate-certificate-request certificate-id
pkicert subject
 CN=testdut,OU=QA,O=JuniperNetworks,L=CNRD,ST=Beijing,C=CN domainname dut.juniper.net
 ip-address 129.16.0.1 email dut@juniper.net
```

```
root@vm# rm -rf /cert
root@vm# mkdir /cert
root@vm# chmod 777 /cert
root@vm# echo -----BEGIN CERTIFICATE REQUEST-----copy-generatedkey-----END CERTIFICATE
REQUEST----- /cert/dsakey
root@vm# cat /cert/dsakey
root@vm# chmod 777 /cert/dsakey
```

```
root@vm# chmod o+w /tftpboot
root@vm# rm -f /etc/xinetd.d/tftp.org
root@vm# cp /etc/xinetd.d/tftp /etc/xinetd.d/tftp.org
root@vm# sed -e 's/server_args.*/server_args = -s \/tftpboot -c/g' /etc/xinetd.d/tftp  /etc/
xinetd.d/tftp.mdf
root@vm# mv -f /etc/xinetd.d/tftp.mdf /etc/xinetd.d/tftp
root@vm# systemctl enable tftp.service
root@vm# /bin/systemctl restart xinetd.service
root@vm# mv -f /etc/xinetd.d/tftp.org /etc/xinetd.d/tftp
root@vm# dir /tftpboot/pki.tcl
root@vm# /bin/cp /tftpboot/pki.tcl /cert/
root@vm# chmod 775 /cert/pki.tcl
root@vm# /cert/pki.tcl PKI-Server-IP /cert/dsakey /cert/dut.cer
root@vm# scp /cert/dut.cer root@node0-host-name:/var/tmp
```

6. To proceed further with device 2 configuration and commit, you need to ensure device1 and device 2 are not reachable to each other. One way to achieve this is to power off device 1 at this point.
7. Configure device 2 with standard cluster command for operating in cluster mode as node1. This requires a reboot.

   [edit]

   user@host# set groups node0 system host-name node0-host-name

   user@host# set groups node0 system backup-router gateway-address

   user@host# set groups node0 system backup-router destination value

   user@host# set groups node0 interfaces fxp0 unit 0 family inet address node0-ip-address

   user@host# set groups node1 system host-name node1-host-name

   user@host# set groups node1 system backup-router gateway-address

   user@host# set groups node1 system backup-router destination value

   user@host# set groups node1 interfaces fxp0 unit 0 family inet address node1-ip-address

   user@host# set apply-groups global

   user@host# set apply-groups “$(node)”

   user@host# delete apply-groups re0

   user@host# set system ports console log-out-on-disconnect

   user@host# set chassis cluster reth-count 5

   user@host# set chassis cluster redundancy-group 0 node 0 priority 254

user@host# set chassis cluster redundancy-group 0 node 1 priority 1

user@host# commit

user@host> set chassis cluster cluster-id 1 node 1 reboot

See https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster-verification.html

8. After the device 2 is up, configure HA link encryption as shown in sample configuration below on device 2. Device 2 needs to be configured with both node0 and node1 HA link encryption configuration. Commit on node1 (device 2), and finally reboot node1 (device 2).

   [edit]

   user@host# set groups node0 security ike traceoptions file ikelog

   user@host# set groups node0 security ike traceoptions file size 100m

   user@host# set groups node0 security ike traceoptions flag all

   user@host# set groups node0 security ike traceoptions level 15

   user@host# set groups node0 security pki traceoptions file pkilog

   user@host# set groups node0 security pki traceoptions file size 100m

   user@host# set groups node0 security pki traceoptions flag all

   user@host# set groups node0 security ike proposal IKE_PROP_PKI authentication-method

   rsa-signatures

   user@host# set groups node0 security ike proposal IKE_PROP_PKI dh-group group20

   user@host# set groups node0 security ike proposal IKE_PROP_PKI authentication-algorithm sha-256

   user@host# set groups node0 security ike proposal IKE_PROP_PKI encryption-algorithm aes-256-cbc

   user@host# set groups node0 security ike policy IKE_POL_PKI mode main

   user@host# set groups node0 security ike policy IKE_POL_PKI proposals IKE_PROP_PKI

   user@host# set groups node0 security ike policy IKE_POL_PKI certificate local-certificate pkicert

   user@host# set groups node0 security ike gateway S2S_GW ike-policy IKE_POL_PKI

   user@host# set groups node0 security ike gateway S2S_GW version v2-only

   user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI protocol esp

user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI authenticationalgorithm hmac-sha1-96

user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI encryptionalgorithm aes-128-cbc

user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI lifetime-seconds 200

user@host# set groups node0 security ipsec policy IPSEC_POL_PKI perfect-forwardsecrecy keys group20

user@host# set groups node0 security ipsec policy IPSEC_POL_PKI proposals IPSEC_PROP_PKI

user@host# set groups node0 security ipsec vpn S2S_VPN ha-link-encryption

user@host# set groups node0 security ipsec vpn S2S_VPN ike gateway S2S_GW

user@host# set groups node0 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PKI

user@host# set groups node0 security pki ca-profile S2S_PKI ca-identity S2S_PKI_CA1

user@host# set groups node0 security pki ca-profile S2S_PKI enrollment url <Enrollment URL of certificate authority>

user@host# set groups node0 security pki ca-profile S2S_PKI revocation-check crl url <CRL distribution point for certificate authority>

user@host# set groups node0 security pki ca-profile S2S_PKI revocation-check disable

user@host# set groups node0 interfaces st0 unit 0 family inet

user@host# set groups node1 security ike traceoptions file ikelog

user@host# set groups node1 security ike traceoptions file size 100m

user@host# set groups node1 security ike traceoptions flag all

user@host# set groups node1 security ike traceoptions level 15

user@host# set groups node1 security pki traceoptions file pkilog

user@host# set groups node1 security pki traceoptions file size 100m

user@host# set groups node1 security pki traceoptions flag all

user@host# set groups node1 security ike proposal IKE_PROP_PKI authentication-method rsa-signatures

user@host# set groups node1 security ike proposal IKE_PROP_PKI dh-group group20

user@host# set groups node1 security ike proposal IKE_PROP_PKI authentication-algorithm sha-256

user@host# set groups node1 security ike proposal IKE_PROP_PKI encryption-algorithm aes-256-cbc

user@host# set groups node1 security ike policy IKE_POL_PKI mode main

user@host# set groups node1 security ike policy IKE_POL_PKI proposals IKE_PROP_PKI

user@host# set groups node1 security ike policy IKE_POL_PKI certificate local-certificate pkicert

user@host# set groups node1 security ike gateway S2S_GW ike-policy IKE_POL_PKI

user@host# set groups node1 security ike gateway S2S_GW version v2-only

user@host# set groups node1 security ipsec proposal IPSEC_PROP_PKI protocol esp

user@host#set groups node1 security ipsec proposal IPSEC_PROP_PKI authenticationalgorithm hmac-sha1-96

user@host> set groups node1 security ipsec proposal IPSEC_PROP_PKI encryptionalgorithm aes-128-cbc

user@host# set groups node1 security ipsec proposal IPSEC_PROP_PKI lifetime-seconds 200

user@host# set groups node1 security ipsec policy IPSEC_POL_PKI perfect-forward-secrecy keys group20

user@host# set groups node1 security ipsec policy IPSEC_POL_PKI proposals IPSEC_PROP_PKI

user@host# set groups node1 security ipsec vpn S2S_VPN ha-link-encryption

user@host# set groups node1 security ipsec vpn S2S_VPN ike gateway S2S_GW

user@host# set groups node1 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PKI

user@host# set groups node1 security pki ca-profile S2S_PKI ca-identity S2S_PKI_CA1

user@host# set groups node1 security pki ca-profile S2S_PKI enrollment url <Enrollment URL of certificate authority>

user@host# set groups node1 security pki ca-profile S2S_PKI revocation-check crl url <CRL distribution point for certificate authority>

user@host# set groups node1 security pki ca-profile S2S_PKI revocation-check disable

user@host# set groups node1 interfaces st0 unit 0 family inet

user@host# set groups global interfaces fab0 fabric-options member-interfaces ge-0/0/3

user@host# set groups global interfaces fab1 fabric-options member-interfaces ge-7/0/3

user@host# commit

user@host> clear security pki node-local local-certificate all

user@host> clear security pki node-local certificate-request all

user@host> clear security pki node-local key-pair all

user@host> clear security pki crl all

user@host> clear security pki ca-certificate all

user@host> request security pki node-local generate-key-pair certificate-id pkicert type rsa size 2048

```
root@vm# curl "http://PKI-Server-IP/certsrv/certnew.cer?
ReqID=CACert=0=bin" -o /tmp/aux_ca.cer
root@vm# scp /tmp/aux_ca.cer root@node1-host-name:/var/tmp
```

user@host> request security pki ca-certificate load ca-profile S2S_PKI filename/var/tmp/aux_ca.cer

user@host> show security pki ca-certificate

```
root@vm# curl "http://PKI-Server-IP/certsrv/certcrl.crl?Renewal=0=bin"
-o /tmp/aux.crl
root@vm# scp /tmp/aux.crl root@node1-host-name:/var/tmp
```

user@host> request security pki crl load ca-profile S2S_PKI filename /var/tmp/aux.crl

user@host> show security pki crl

user@host> request security pki node-local generate-certificate-request certificate-id pkicert subject

CN=testaux,OU=QA,O=JuniperNetworks,L=CNRD,ST=Beijing,C=CN domainname aux.juniper.net

ip-address 130.16.0.1 email aux@juniper.net

```
root@vm# rm -rf /cert
root@vm# mkdir /cert
```

```
root@vm# chmod 777 /cert
root@vm# echo -----BEGIN CERTIFICATE REQUEST-----copy-generatedkey-----
END CERTIFICATE REQUEST-----  /cert/dsakey
root@vm# cat /cert/dsakey
root@vm# chmod 777 /cert/dsakey
root@vm# chmod o+w /tftpboot
root@vm# rm -f /etc/xinetd.d/tftp.org
root@vm# cp /etc/xinetd.d/tftp /etc/xinetd.d/tftp.org
root@vm# sed -e 's/server_args.*/server_args = -s \/tftpboot -c/g' /etc/
xinetd.d/tftp  /etc/xinetd.d/tftp.mdf
root@vm# mv -f /etc/xinetd.d/tftp.mdf /etc/xinetd.d/tftp
root@vm# systemctl enable tftp.service
root@vm# /bin/systemctl restart xinetd.service
root@vm# mv -f /etc/xinetd.d/tftp.org /etc/xinetd.d/tftp
root@vm# dir /tftpboot/pki.tcl
root@vm# /bin/cp /tftpboot/pki.tcl /cert/
root@vm# chmod 775 /cert/pki.tcl
root@vm# /cert/pki.tcl PKI-Server-IP /cert/dsakey /cert/aux.cer
root@vm# scp /cert/aux.cer root@node1-host-name:/var/tmp
```

```
user@host> clear security pki node-local local-certificate all
         user@host> request security pki node-local local-certificate load filename
           /var/tmp/aux.cer
         certificate-id pkicert
         user@host> request system reboot
```

9. Power ON node0 (device 1).
10. Both the nodes will be in cluster mode with HA link encryption enabled.

NOTE: To enable HA link encryption on node1 in step 6, the other node must be in lost state for the commit to go through. Hence, manage the timing correctly, else step 6 must be redone until enabling HA link encryption on node1 commit goes through.

15
CHAPTER

Performing Self-Tests on a Device

Understanding FIPS Self-Tests

IN THIS SECTION

The cryptographic module enforces security rules to ensure that a device running the Juniper Networks Junos operating system (Junos OS) in FIPS mode of operation meets the security requirements of FIPS 140-3 Level 2. To validate the output of cryptographic algorithms approved for FIPS and test the integrity of some system modules, the device performs the following series of known answer test (KAT) self-tests:

- `md_kats`—KAT for libmd and libc
- `quicksec_7_0_kats`—KAT for Quicksec_7_0 Toolkit cryptographic implementation
- `openssl_kats`—KAT for OpenSSL cryptographic implementation
- `openssl-102_kats` - KAT for OpenSSL v1.0.2 cryptographic information
- `kernel_kats`—KAT for kernel cryptographic routines
- `srxpfe_kats`— KAT for SRX packet forwarding engine

The KAT self-tests are performed automatically at startup and reboot when FIPS mode of operation is enabled on the device. Conditional self-tests are also performed automatically to verify digitally signed software packages, generated random numbers, RSA and ECDSA key pairs, and manually entered keys.

If the KATs are completed successfully, the system log (syslog) file is updated to display the tests that were executed.

If the device fails a KAT, the device writes the details to a system log file, enters FIPS error state (panic), and reboots.

There may be instances where the device ends up not booting correctly. It can be a result of a POST test failure, or other things. The administrators are advised to refer to this guidance document to look for solution and if the issues are not resolved, contact support team.

The `file show /var/log/messages` command displays the system log.

DRBG does not require any configuration, and initialized on startup.

Performing Power-On Self-Tests on the Device

Each time the cryptographic module is powered on, the module tests that the cryptographic algorithms still operate correctly and that sensitive data has not been damaged. Power-on self-tests are performed on demand by power cycling the module.

On powering on or resetting the device, the module performs the following self-tests. All KATs must be completed successfully prior to any other use of cryptography by the module. If one of the KATs fail, the module enters the Critical Failure error state.

The module displays the following status output for vSRX3.0 devices while running the power-on self-tests:

```
<118>1 2022-09-13T23:30:18.193-07:00 fipscc-vsrx3-g kernel - - - Initializing Verified Exec:
<2>1 2022-09-13T23:30:18.193-07:00 fipscc-vsrx3-g kernel - - - random:
randomdev_wait_until_seeded unblock wait
<2>1 2022-09-13T23:30:18.193-07:00 fipscc-vsrx3-g kernel - - - random: Entropy start-up health
tests performed on 1024 samples passed.
<2>1 2022-09-13T23:30:18.193-07:00 fipscc-vsrx3-g kernel - - - random: unblocking device.
<118>1 2022-09-13T23:30:18.193-07:00 fipscc-vsrx3-g kernel - - - FIPS veriexec ECDSA Verify
Known Answer Test: Passed
<118>1 2022-09-13T23:30:18.193-07:00 fipscc-vsrx3-g kernel - - - Verified os-kernel-prd-
x86-64-20220607 signed by PackageProductionECP256_2022 method ECDSA256+SHA256

<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: Running FIPS Self-tests
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: Testing kernel KATS:
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: NIST 800-90 HMAC DRBG
Known Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: DES3-CBC Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA1 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-256 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: SHA-2-384 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: SHA-2-512 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES128-CMAC Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES-CBC Known Answer Test:
Passed
```

```
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: Testing MACSec KATS:
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES128-CMAC Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES256-CMAC Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES-ECB Known Answer Test:
Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES-KEYWRAP Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: KBKDF Known Answer Test:
Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: Testing libmd KATS:
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA1 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-256 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: SHA-2-512 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: Testing OpenSSL v1.0.2
KATS:
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: NIST 800-90 HMAC DRBG
Known Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: FIPS ECDSA Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: FIPS ECDH Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: FIPS RSA Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: DES3-CBC Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA1 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-224 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-256 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-384 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-512 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES-CBC Known Answer Test:
Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES-GCM Known Answer Test:
```

```
Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: ECDSA-SIGN Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: KDF-IKE-V1 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: KDF-SSH-SHA256 Known
Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: KAS-ECC-EPHEM-UNIFIED-NOKC
Known Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: KAS-FFC-EPHEM-NOKC Known
Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: Testing OpenSSL KATS:
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: NIST 800-90 HMAC DRBG
Known Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: FIPS ECDSA Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: FIPS ECDH Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: FIPS RSA Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: DES3-CBC Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA1 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-224 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-256 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-384 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-512 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES-CBC Known Answer Test:
Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES-GCM Known Answer Test:
Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: ECDSA-SIGN Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: KDF-IKE-V1 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: KDF-SSH-SHA256 Known
Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: KAS-ECC-EPHEM-UNIFIED-NOKC
```

```
Known Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: KAS-FFC-EPHEM-NOKC Known
Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: Testing QuickSec 7.0 KATS:
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: NIST 800-90 HMAC DRBG
Known Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: DES3-CBC Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA1 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-224 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-256 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-384 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-512 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES-CBC Known Answer Test:
Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES-GCM Known Answer Test:
Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: SSH-RSA-ENC Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: SSH-RSA-SIGN Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: SSH-ECDSA-SIGN Known
Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: KDF-IKE-V1 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: KDF-IKE-V2 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: Testing QuickSec KATS:
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: NIST 800-90 HMAC DRBG
Known Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: DES3-CBC Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA1 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-224 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-256 Known Answer
Test: Passed
```

```
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-384 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-512 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES-CBC Known Answer Test:
Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES-GCM Known Answer Test:
Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: SSH-RSA-ENC Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: SSH-RSA-SIGN Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: KDF-IKE-V1 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: KDF-IKE-V2 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: Testing SSH IPsec KATS:
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: NIST 800-90 HMAC DRBG
Known Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: DES3-CBC Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA1 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: HMAC-SHA2-256 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: AES-CBC Known Answer Test:
Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: SSH-RSA-ENC Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: SSH-RSA-SIGN Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: KDF-IKE-V1 Known Answer
Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: Testing file integrity:
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: File integrity Known
Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: Testing crypto integrity:
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: Crypto integrity Known
Answer Test: Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: Expect an exec
Authentication error...
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: /sbin/kats/run-tests: /
sbin/kats/cannot-exec: Authentication error
```

```
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: FIPS Self-tests Passed
<118>1 2022-09-13T23:30:18.194-07:00 fipscc-vsrx3-g kernel - - - mgd: commit complete
```

NOTE: The module implements cryptographic libraries and algorithms that are not utilized in the approved mode of operation.

RELATED DOCUMENTATION

How to Enable and Configure Junos OS in FIPS Mode of Operation | 33

16
CHAPTER

Configuration Statements

checksum-validate

IN THIS SECTION

Syntax

```
checksum-validate {
    match (equal | greater-than | less-than | not-equal);
    value checksum-value;
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol ipv4]
[edit security idp custom-attack attack-name attack-type signature protocol tcp]
[edit security idp custom-attack attack-name attack-type signature protocol udp]
[edit security idp custom-attack attack-name attack-type signature protocol icmp]
[edit security idp custom-attack attack-name attack-type signature protocol icmpv6]
```

Description

Allow IDP to validate checksum field against the calculated checksum.

Options

match (equal | greater-than | less-than | not-equal)

Match an operand.

value *checksum-value*

Match a decimal value.

- **Range:** 0 through 65,535

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

code

IN THIS SECTION

Syntax

```
code {
    match (equal | greater-than | less-than | not-equal);
    value code-value;
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol icmpv6]
```

Description

Specify the secondary code that identifies the function of the request/reply within a given type.

Options

- `match` (`equal` | `greater-than` | `less-than` | `not-equal`)—Match an operand.
- `value` *`code-value`*—Match a decimal value.
- **Range:** 0 through 255

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

data-length

IN THIS SECTION

Syntax

```
data-length {
    match (equal | greater-than | less-than | not-equal);
    value data-length;
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol udp]
[edit security idp custom-attack attack-name attack-type signature protocol icmp]
[edit security idp custom-attack attack-name attack-type signature protocol icmpv6]
[edit security idp custom-attack attack-name attack-type signature protocol tcp]
```

Description

Specify the number of bytes in the data payload. In the TCP header, for SYN, ACK, and FIN packets, this field should be empty.

Options

- `match` (`equal` | `greater-than` | `less-than` | `not-equal`)—Match an operand.
- `value` *`data-length`*—Match the number of bytes in the data payload.
- **Range:** 0 through 65,535

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 9.3.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

destination-option

IN THIS SECTION

Syntax

```
destination-option {
    home-address {
        match (equal | greater-than | less-than | not-equal);
        value header-value;
```

```
    }
    option-type {
        match (equal | greater-than | less-than | not-equal);
        value header-value;
    }
}
```

Hierarchy Level

```
[edit  set security idp custom-attack attack-name attack-type signature protocol ipv6 extension-
header]
```

Description

Specify the IPv6 destination option for the extension header. The `destination-option` option inspects the header option type of `home-address` field in the `extension header` and reports a custom attack if a match is found. The `destination-option` supports the `home-address` field type of inspection.

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

extension-header

IN THIS SECTION

Syntax

```
extension-header {
    destination-option {
        home-address {
            match (equal | greater-than | less-than | not-equal);
            value header-value;
        }
            option-type {
                match (equal | greater-than | less-than | not-equal);
                value header-value;
            }
    }
    routing-header {
        header-type {
            match (equal | greater-than | less-than | not-equal);
            value header-value;
            }
        }
}
```

Hierarchy Level

```
[edit  set security idp custom-attack attack-name attack-type signature protocol ipv6]
```

Description

Specify the IPv6 extension header.

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

header-type

IN THIS SECTION

Syntax

```
header-type {
    match (equal | greater-than | less-than | not-equal);
    value header-value;
}
```

Hierarchy Level

```
[edit  set security idp custom-attack attack-name attack-type signature protocol ipv6 extension-header routing-header]
```

Description

Specify the IPv6 routing header type.

Options

match (equal | greater-than | less-than | not-equal)

Match an operand.

value

Match a decimal value.

- **Range:** 0 through 255

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

home-address

IN THIS SECTION

Syntax

```
home-address {
    match (equal | greater-than | less-than | not-equal);
```

```
    value value;
}
```

Hierarchy Level

```
[edit  set security idp custom-attack attack-name attack-type signature protocol ipv6 extension-
header destination-option]
```

Description

Specify the IPv6 home address of the mobile node.

Options

match (equal | greater-than | less-than | not-equal)	Match an operand.
value	Match a decimal value.

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

identification

IN THIS SECTION

Syntax

```
identification {
    match (equal | greater-than | less-than | not-equal);
    value identification-value;
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol icmpv6]
```

Description

Specify a unique value used by the destination system to associate requests and replies.

Options

- `match` (`equal` | `greater-than` | `less-than` | `not-equal`)—Match an operand.
- `value` *`identification-value`*—Match a decimal value.
- **Range:** 0 through 65,535

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

icmpv6 (Security IDP Custom Attack)

IN THIS SECTION

Syntax

```
icmpv6 {
    checksum-validate {
        match (equal | greater-than | less-than | not-equal);
        value checksum-value;
    }
    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;
    }
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol]
```

Description

Allow IDP to match the attack for the specified ICMPv6.

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

ihl (Security IDP Custom Attack)

IN THIS SECTION

Syntax

```
ihl {
    match (equal | greater-than | less-than | not-equal);
    value ihl-value;
}
```

Hierarchy Level

```
[edit  set security idp custom-attack ipv4_custom attack-type signature protocol ipv4]
```

Description

Specify the IPv4 header length in words.

Options

match (equal | greater-than | less-than | not-equal)

Match an operand.

value

Match a decimal value.

- **Range:** 0 through 15

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

option-type

IN THIS SECTION

Syntax

```
option-type {
    match (equal | greater-than | less-than | not-equal);
    value header-value;
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol ipv6 extension-
header destination-option]
```

Description

Specify the type of option for destination header type.

Options

match (equal | greater-than | less-than | not-equal)

Match an operand.

value

Match a decimal value.

- **Range:** 0 through 255

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

reserved (Security IDP Custom Attack)

IN THIS SECTION

Syntax

```
reserved {
    match (equal | greater-than | less-than | not-equal);
```

```
    value reserved-value;
}
```

Hierarchy Level

```
[edit security idp custom-attack ipv4_custom attack-type signature protocol tcp]
```

Description

Specify the three reserved bits in the TCP header field.

Options

match (equal | greater-than | less-than | not-equal)

Match an operand.

value

Match a decimal value.

- **Range:** 0 through 7

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

routing-header

IN THIS SECTION

Syntax

```
routing-header {
    header-type {
        match (equal | greater-than | less-than | not-equal);
        value header-value;
    }
}
```

Hierarchy Level

```
[edit  set security idp custom-attack attack-name attack-type signature protocol ipv6 extension-
header]
```

Description

Specify the IPv6 routing header type. The `routing-header` option inspects the routing-header type field and reports a custom attack if a match with the specified value is found. The `routing-header` option supports the following routing header types: `routing-header-type0`, `routing-header-type1`, and so on.

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

sequence-number (Security IDP ICMPv6 Headers)

IN THIS SECTION

Syntax

```
sequence-number {
    match (equal | greater-than | less-than | not-equal);
    value sequence-number;
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol icmpv6]
```

Description

Specify the sequence number of the packet. This number identifies the location of the request/reply in relation to the entire sequence.

Options

- `match` (`equal` | `greater-than` | `less-than` | `not-equal`)—Match an operand.
- `value` *`sequence-number`*—Match a decimal value.
- **Range:** 0 through 65,535

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview

type (Security IDP ICMPv6 Headers)

IN THIS SECTION

Syntax

```
type {
    match (equal | greater-than | less-than | not-equal);
    value type-value;
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol icmpv6]
```

Description

Specify the primary code that identifies the function of the request/reply.

Options

`match` (`equal` | `greater-than` | `less-than` | `not-equal`)—Match an operand.

`value` *`type-value`*—Match a decimal value.

- **Range:** 0 through 255

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 249

CHAPTER 17

Junos-FIPS Configuration Restrictions

Unsupported Junos-FIPS Configuration Statements

The following configuration statements are not supported on Junos-FIPS:

Statement	Description
`set system services { ftp | finger | telnet | web-management | xnm-clear-text | tftp}`	Junos-FIPS does not allow an unencrypted or weakly encrypted or a connection that relies on a vulnerable key establishment protocol.
`set system services ssh protocol-version`	Junos-FIPS allows the SSHv2 setting only.
`set system login password format { des | md5 }`	You must encrypt administrator passwords using strong algorithms, such as Secure Hash Algorithm (sha-256 and sha-512).
`set system ike policy` *`policy name`* `proposal-set`	Junos-FIPS does not support preconfigured proposal sets. You must configure an IKE proposal explicitly.

`set system ike proposal` *`proposal name`* `authentication-algorithm md5`
 	
`set system ipsec proposal` *`proposal name`* `authentication-algorithm hmac-md5-96`
	Junos-FIPS does not support Message Digest 5 (MD5). However it does support (sha-256 and sha-384).

`set system ike proposal` *`proposal name`* `encryption-algorithm des-cbc`
 	
`set system ipsec proposal` *`proposal name`* `encryption-algorithm des-cbc`
	Junos-FIPS does not support Data Encryption Standard (DES). However it does support Advanced Encryption Standard (AES).

`set system ike proposal` *`proposal name`* `protocol ah`	Authentication Header (AH) protocol provides authentication but not encryption. Enhanced Security Protocol (ESP) is required.
`set system ike proposal` *`proposal name`* `dh-group {group1 | group2}`	Junos-FIPS does not support Diffie-Hellman (DH) groups 1 and 2. However, DH-groups 14, 19 and 20 are supported on Junos-FIPS.

Unsupported Junos-FIPS Operational Commands

The following operating commands are not supported on Junos-FIPS:

Command	Description
`request system software reboot` *`at time in minutes`* `usb`	You must load the firmware image directly from the internal flash memory. Junos-FIPS does not support loading from an external source.
`set wlan`	Junos-FIPS does not support wireless configuration.
`request system software rollback`	You must upload a new version of the firmware explicitly. Junos-FIPS does not support the rollback to a previously saved version.
`request security pki ca-certificate enroll`	You must enroll the certificate authority enrollment manually. Simple Certificate Enrollment Protocol (SCEP) is disabled.

Supported Protocols

Range of IPv4/IPv6 protocols supported by the Device:

- For IPv4 supported protocol ID range is from 1 to 100
- For IPv6 supported protocol ID range is from 1 to 142 except for protocol ID 43, 44, 51, 60.