CIS Juniper SRX Services Gateway VPN STIG Benchmark

v1.0.0 – 10-27-2022

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

Juniper SRX Services Gateway VPN Secure Technical Implementation Guide (STIG)
Version: 2 Release: 2 Benchmark
Date: 27 Oct 2022

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Juniper SRX Services Gateway VPN and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Juniper SRX Services Gateway VPN

Recommendations

1 STIG RULES

Juniper Firewall

Juniper SRX Services Gateway VPN Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 27 Oct 2022

CLASSIFICATION unclassified

1.1 JUSX-VN-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must limit the number of concurrent sessions for user accounts to one (1) and administrative accounts to three (3), or set to an organization-defined number.

```
GROUP ID: V-214668
RULE ID: SV-214668r382774
```

Rationale:

Network element management includes the ability to control the number of users and user sessions that utilize a network element. Limiting the number of allowed users and sessions per user is helpful in limiting risks related to DoS attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based upon mission needs and the operational environment for each system.

The intent of this policy is to ensure the number of concurrent sessions is deliberately set to a number based on the site's mission and not left unlimited.

Audit:

Verify the VPN Internet Key Exchange (IKE) gateway limits concurrent sessions.
[edit]
show security ike
View the value for the connections-limit.
If the VPN IKE gateway does not limit the number of concurrent sessions for user accounts to one (1) and administrative accounts to three (3), or is set to an organization-defined number, this is a finding.

Remediation:

Configure the VPN IKE gateway to limit concurrent sessions. The following is an example.
[edit]
set security ike gateway <VPN-GATEWAY> dynamic connections-limit 1
[edit]
set security ike gateway <VPN-GATEWAY> dynamic connections-limit 3

Additional Information:

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

- NIST SP 800-53::AC-10
- NIST SP 800-53A::AC-10.1 (ii)
- NIST SP 800-53 Revision 4::AC-10
- NIST SP 800-53 Revision 5::AC-10

1.2 JUSX-VN-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must renegotiate the IPsec security association after 8 hours or less.

```
GROUP ID: V-214669
RULE ID: SV-214669r856572
```

Rationale:

The IPsec SA and its corresponding key will expire either after the number of seconds or amount of traffic volume has exceeded the configured limit. A new SA is negotiated before the lifetime threshold of the existing SA is reached to ensure that a new SA is ready for use when the old one expires. The longer the lifetime of the IPsec SA, the longer the lifetime of the session key used to protect IP traffic. The SA is less secure with a longer lifetime because an attacker has a greater opportunity to collect traffic encrypted by the same key and subject it to cryptanalysis. However, a shorter lifetime causes IPsec peers to renegotiate Phase II more often resulting in the expenditure of additional resources.

Audit:

Review all IPsec security associations configured globally or within IPsec profiles on the VPN gateway and examine the configured idle time. The default is 3600.
[edit]
show security ipsec proposal
View the value of the lifetime-seconds option.
If the IPsec proposal lifetime-seconds are not renegotiated after 8 hours or less of idle time, this is a finding.
If the IPsec proposal lifetime-seconds is not configured, this is a finding.

Remediation:

Set the lifetime (in seconds) of the IPsec proposal to 8 hours or less.
Example:
[edit]
set security ipsec proposal <P2-PROPOSAL-NAME> lifetime-seconds 28800

Additional Information:

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

1.3 JUSX-VN-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must renegotiate the IKE security association after 24 hours or less.

```
GROUP ID: V-214670
RULE ID: SV-214670r856574
```

Rationale:

When a VPN gateway creates an IPsec Security Association (SA), resources must be allocated to maintain the SA. These resources are wasted during periods of IPsec endpoint inactivity, which could result in the gateway's inability to create new SAs for other endpoints, thereby preventing new sessions from connecting. The Internet Key Exchange (IKE) idle timeout may also be set to allow SAs associated with inactive endpoints to be deleted before the SA lifetime has expired, although this setting is not recommended at this time. The value of one hour or less is a common best practice.

Audit:

Review all IPsec security associations configured globally or within IPsec profiles on the VPN gateway and examine the configured idle time. The idle time value must be one hour or less. If idle time is not configured, determine the default used by the gateway. The default value is 28800 seconds which is compliant.
[edit]
show security ike proposal
View the value of the lifetime-seconds option.
If the IKE security associations are not renegotiated after 24 hours or less of idle time, this is a finding.

Remediation:

Specify the lifetime (in seconds) of an IKE security association (SA). When the SA expires, it is replaced by a new SA, the security parameter index (SPI), or terminated if the peer cannot be contacted for renegotiation.
Example:
[edit]
set security ike proposal <P1-PROPOSAL-NAME> lifetime-seconds 86400

Additional Information:

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

1.4 JUSX-VN-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN device also fulfills the role of IDPS in the architecture, the device must inspect the VPN traffic in compliance with DoD IDPS requirements.

```
GROUP ID: V-214671
RULE ID: SV-214671r382780
```

Rationale:

Remote access devices, such as those providing remote access to network devices and information systems, which lack automated, capabilities increase risk and makes remote user access management difficult at best.

Remote access is access to DoD non-public information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network.

Automated monitoring of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, from a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

Audit:

Obtain documentation from the site representative that the Juniper SRX is configured in compliance with the Juniper SRX Services Gateway IDPS STIG.
If the device has not been configured to comply with DoD IDPS requirements, this is a finding.

Remediation:

Perform a security review using the Juniper SRX Services Gateway IDPS STIG.

Additional Information:

CCI-000067 Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53::AC-17 (1)
- NIST SP 800-53A::AC-17 (1).1
- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

1.5 JUSX-VN-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Juniper SRX Services Gateway VPN must use AES encryption for the IPsec proposal to protect the confidentiality of remote access sessions.

```
GROUP ID: V-214672
RULE ID: SV-214672r382783
```

Rationale:

Without confidentiality protection mechanisms, unauthorized individuals may gain access to sensitive information via a remote access session. The Advance Encryption Standard (AES) encryption is critical to ensuring the privacy of the IPsec session; it is imperative that AES is used for encryption operations.

Remote access is access to DoD-non-public information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include broadband and wireless connections.

While there is much debate about the security and performance of AES, there is a consensus that AES is significantly more secure than other algorithms currently supported by IPsec implementations. AES is available in three key sizes: 128, 192, and 256 bits, versus the 56 bit DES. Therefore, there are approximately 1021 times more AES 128-bit keys than DES 56-bit keys. In addition, AES uses a block size of 128 bits—twice the size of DES or 3DES.

Audit:

Verify all Internet Key Exchange (IKE) proposals are set to use the AES encryption algorithm.
[edit]
show security ipsec
View the value of the encryption algorithm for each defined proposal.
If the value of the encryption algorithm for any IPsec proposal is not set to use an AES algorithm, this is a finding.

Remediation:

The following example commands configure the IPsec (phase 2) proposals. The option may also be configured to use the aes-128-cbc, aes-192-cbc, or aes-256-cbc algorithms.
[edit]
set security ipsec proposal <IPSEC-PROPOSAL-NAME> encryption-algorithm aes-256-cbc

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.6 JUSX-VN-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Juniper SRX Services Gateway VPN must use AES encryption for the Internet Key Exchange (IKE) proposal to protect the confidentiality of remote access sessions.

```
GROUP ID: V-214673
RULE ID: SV-214673r382783
```

Rationale:

Without confidentiality protection mechanisms, unauthorized individuals may gain access to sensitive information via a remote access session. The Advance Encryption Standard (AES) algorithm is critical to ensuring the privacy of the IKE session responsible for establishing the security association and key exchange for an IPsec tunnel. AES is used for encryption operations.

Remote access is access to DoD-non-public information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include broadband and wireless connections.

While there is much debate about the security and performance of AES, there is a consensus that AES is significantly more secure than other algorithms currently supported by IPsec implementations. AES is available in three key sizes: 128, 192, and 256 bits, versus the 56 bit DES. Therefore, there are approximately 1021 times more AES 128-bit keys than DES 56-bit keys. In addition, AES uses a block size of 128 bits—twice the size of DES or 3DES.

Audit:

Verify all IKE proposals are set to use the AES encryption algorithm.
[edit]
show security ike
View the value of the encryption algorithm for each defined proposal.
If the value of the encryption algorithm for any IKE proposal is not set to use an AES algorithm, this is a finding.

Remediation:

The following example commands configure the IKE (phase 1) proposals. The option may also be configured to use the aes-128-cbc, aes-192-cbc, or aes-256-cbc algorithms.
[edit]
set security ike proposal <IKE-PROPOSAL-NAME> encryption-algorithm aes-256-cbc

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.7 JUSX-VN-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must implement a FIPS-140-2 validated Diffie-Hellman (DH) group.

```
GROUP ID: V-214674
RULE ID: SV-214674r382783
```

Rationale:

Use of an approved DH algorithm ensures the Internet Key Exchange (IKE) (phase 1) proposal uses FIPS-validated key management techniques and processes in the production, storage, and control of private/secret cryptographic keys. The security of the DH key exchange is based on the difficulty of solving the discrete logarithm in which the key was derived from. Hence, the larger the modulus, the more secure the generated key is considered to be.

Audit:

Verify all IKE proposals are set to use a FIPS-validated dh-group.
[edit]
show security ike <P1-PROPOSAL-NAME>
View the IKE options dh-group option.
If the IKE option is not set to a FIPS-140-2 validated dh-group, this is a finding.

Remediation:

The following command is an example of how to configure the IKE (phase 1) proposals.
The following groups are allowed for use in DoD:
DH Groups 14 (2048-bit MODP)

- 19 (256-bit Random ECP), 20 (384-bit Random ECP), 5 (1536-bit MODP), 24 (2048-bit MODP with 256-bit POS).

Example:
[edit]
set security ike proposal <P1-PROPOSAL-NAME> dh-group group14

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.8 JUSX-VN-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must be configured to use IPsec with SHA1 or greater to negotiate hashing to protect the integrity of remote access sessions.

```
GROUP ID: V-214675
RULE ID: SV-214675r382846
```

Rationale:

Without strong cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access VPN provides access to DoD non-public information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network.

Audit:

Verify all IPSec proposals are set to use the sha-256 hashing algorithm.
[edit]
show security ipsec proposal <IPSEC-PROPOSAL-NAME>
View the value of the encryption algorithm for each defined proposal.
If the value of the encryption algorithm option for all defined proposals is not set to use SHA1 or greater, this is a finding.

Remediation:

The following example commands configure the IPSec proposal.
set security ipsec proposal <IPSEC-PROPOSAL-NAME> authentication-algorithm <hmac-sha-256-128 | hmac-sha-256-96 | hmac-sha1-96>

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.9 JUSX-VN-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must ensure inbound and outbound traffic is configured with a security policy in compliance with information flow control policies.

```
GROUP ID: V-214676
RULE ID: SV-214676r382735
```

Rationale:

Remote access devices, such as those providing remote access to network devices and information systems, which lack automated, capabilities increase risk and makes remote user access management difficult at best.

Remote access is access to DoD non-public information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network.

Automated monitoring of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, from a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

In phase-2, another negotiation is performed, detailing the parameters for the IPsec connection. New keying material using the Diffie-Hellman key exchange established in phase-1 is used to provide session keys used to protecting the VPN data flow. If Perfect-Forwarding-Secrecy (PFS) is used, a new Diffie-Hellman exchange is performed for each phase-2 negotiation. While this is slower, it makes sure that no keys are dependent on any other previously used keys; no keys are extracted from the same initial keying material. This is to make sure that, in the unlikely event that some key was compromised; no subsequent keys can be derived.

Audit:

Verify an IPsec policy is configured and used to control the VPN information flow.
[edit]
show security ipsec
Inspect the security policy.
If VPN traffic is not configured and controlled using an IPsec policy, this is a finding.

Remediation:

The following example command is an example of an IPsec policy.
[edit]
set security ipsec policy <IPSEC-POLICY> perfect-forward-secrecy keys group14
set security ipsec policy <IPSEC-POLICY> proposals <IPSEC-PROPOSAL>
The following command is an example of how to define an IPsec VPN using the IPsec policy and a secure tunnel interface. Alternatively, administrators can configure on-traffic tunnel establishment.
[edit]
set security ipsec vpn <VPN> bind-interface st0.0
set security ipsec vpn <VPN> ike gateway <IKE-PEER>
set security ipsec vpn <VPN> ike ipsec-policy <IPSEC-POLICY>
set security ipsec vpn <VPN> establish-tunnels immediately
For site-to-site VPN implementation, the SRX device is configured to route traffic over the IPsec VPN's secure tunnel interface by establishing a route with the next-hop specified as the secure tunnel interface. The following commands configure an IPv4 and IPv6 static route for their respective secure tunnels.
set routing-options static route <IPv4 network/netmask> next-hop st0.0
set routing-options rib inet6.0 static route <IPv6 network/netmask> next-hop st0.1

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

1.10 JUSX-VN-000011 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

If IDPS inspection is performed separately from the Juniper SRX Services Gateway VPN device, the VPN must route sessions to an IDPS for inspection.

```
GROUP ID: V-214678
RULE ID: SV-214678r864169
```

Rationale:

Remote access devices, such as those providing remote access to network devices and information systems, which lack automated, capabilities increase risk and makes remote user access management difficult at best.

Remote access is access to DoD non-public information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network.

Automated monitoring of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, from a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

Audit:

Inspect the Juniper SRX configuration or the site's architecture drawings to verify all inbound VPN traffic is routed to the site's intrusion detection system.
If all inbound VPN traffic is not inspected by the site's IDPS prior to being routed to its destination, this is a finding.

Remediation:

Configure the Juniper SRX to route traffic to the port attached to intrusion detection system or configure to route all inbound traffic to the sites intrusion detection system using the IP address of the IPS/IDS.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.11 JUSX-VN-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Juniper SRX Services Gateway VPN must use Internet Key Exchange (IKE) for IPsec VPN Security Associations (SAs).

```
GROUP ID: V-214677
RULE ID: SV-214677r385561
```

Rationale:

Without IKE, the SPI is manually specified for each security association. IKE peers will negotiate the encryption algorithm and authentication or hashing methods as well as generate the encryption keys.

An IPsec SA is established using either Internet Key Exchange (IKE) or manual configuration. When using IKE, the security associations are established when needed and expire after a period of time or volume of traffic threshold. If manually configured, they are established as soon as the configuration is complete at both end points and they do not expire. When using IKE, the Security Parameter Index (SPI) for each security association is a pseudo-randomly derived number.

With manual configuration of the IPsec security association, both the cipher key and authentication key are static. Hence, if the keys are compromised, the traffic being protected by the current IPsec tunnel can be decrypted as well as traffic in any future tunnels established by this SA. Furthermore, the peers are not authenticated prior to establishing the SA, which could result in a rogue device establishing an IPsec SA with either of the VPN end points.

IKE provides primary authentication to verify the identity of the remote system before negotiation begins. This feature is lost when the IPsec security associations are manually configured, which results in a non-terminating session using static pre-shared keys.

Audit:

Verify the IKE protocol is specified for all IPsec VPNs.
[edit]
show security ipsec vpn
If the IKE protocol is not specified as an option on all VPN gateways, this is a finding.

Remediation:

The following example commands configure an IPsec VPN to use the IKE gateway information.
[edit]
set security ipsec vpn <VPN-GWY-NAME> ike gateway <IKE-PEER-NAME>

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.12 JUSX-VN-000012 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Juniper SRX Services Gateway VPN must not accept certificates that have been revoked when using PKI for authentication.

```
GROUP ID: V-214679
RULE ID: SV-214679r385561
```

Rationale:

Situations may arise in which the certificate issued by a Certificate Authority (CA) may need to be revoked before the lifetime of the certificate expires. For example, the certificate is known to have been compromised.

To achieve this, a list of certificates that have been revoked, known as a Certificate Revocation List (CRL), is sent periodically from the CA to the IPsec gateway. When an incoming Internet Key Exchange (IKE) session is initiated for a remote client or peer whose certificate is revoked, the CRL will be checked to see if the certificate is valid; if the certificate is revoked, IKE will fail and an IPsec security association will not be established for the remote endpoint.

Audit:

Examine the CA trust point defined on the VPN gateway to determine if it references a CRL and that revocation check has been enabled. An alternate mechanism for checking the validity of a certificate is the use of the Online Certificate Status Protocol (OCSP). Unlike CRLs, which provide only periodic certificate status checks, OCSP can provide timely information regarding the status of a certificate.
If revoked certificates are accepted for PKI authentication, this is a finding.

Remediation:

Configure the CA trust point to enable certificate revocation check by referencing a CRL or via OCSP.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.13 JUSX-VN-000013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must specify Perfect Forward Secrecy (PFS).

```
GROUP ID: V-214680
RULE ID: SV-214680r385561
```

Rationale:

PFS generates each new encryption key independently from the previous key. Without PFS, compromise of one key will compromise all communications.

The phase 2 (Quick Mode) Security Association (SA) is used to create an IPsec session key. Hence, its rekey or key regeneration procedure is very important. The phase 2 rekey can be performed with or without Perfect Forward Secrecy (PFS). With PFS, every time a new IPsec Security Association is negotiated during the Quick Mode, a new Diffie-Hellman (DH) exchange occurs. The new DH shared secret will be included with original keying material (SYKEID_d, initiator nonce, and responder nonce from phase 1) for generating a new IPsec session key. If PFS is not used, the IPsec session key will always be completely dependent on the original keying material from the Phase-1. Hence, if an older key is compromised at any time, it is possible that all new keys may be compromised.

The DH exchange is performed in the same manner as was done in phase 1 (Main or Aggressive Mode). However, the phase 2 exchange is protected by encrypting the phase 2 packets with the key derived from the phase 1 negotiation. Because DH negotiations during phase 2 are encrypted, the new IPsec session key has an added element of secrecy.

Audit:

Examine all IPsec profiles to verify PFS is enabled.
[edit]
show security ipsec policy
If PFS is not configured, this is a finding.

Remediation:

Configure the VPN gateway to ensure PFS is enabled. The following commands configure an IPsec policy, enabling PFS using Diffie-Hellman group 14 and associates the IPsec proposal configured in the previous example.
[edit]
set security ipsec policy <IPSEC-POLICY> perfect-forward-secrecy keys group14
set security ipsec policy <IPSEC-POLICY> proposals <IPSEC-PROPOSAL>

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.14 JUSX-VN-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must use Encapsulating Security Payload (ESP) in tunnel mode.

```
GROUP ID: V-214681
RULE ID: SV-214681r385561
```

Rationale:

ESP provides confidentiality, data origin authentication, integrity, and anti-replay services within the IPsec suite of protocols. ESP in tunnel mode ensures a secure path for communications for site-to-site VPNs and gateway to endpoints, including header information.

ESP can be deployed in either transport or tunnel mode. Transport mode is used to create a secured session between two hosts. It can also be used when two hosts simply want to authenticate each IP packet with IPsec authentication header (AH). With ESP transport mode, only the payload (transport layer) is encrypted, whereas with tunnel mode, the entire IP packet is encrypted and encapsulated with a new IP header. Tunnel mode is used to encrypt traffic between secure IPsec gateways or between an IPsec gateway and an end-station running IPsec software. Hence, it is the only method to provide a secured path to transport traffic between remote sites or end-stations and the central site.

Audit:

Review all IPsec profiles and zones to verify ESP tunnel mode has been specified.
[edit]
show security ipsec proposal
show security zones security-zone untrust
If all IPsec proposals are not configured for the ESP protocol, this is a finding.
If an Internet Key Exchange (IKE) is not bound to an external host-inbound service to direct all inbound VPN traffic to the VPN interface configured for IKE, this is a finding.

Remediation:

Configure Phase 2 for ESP and allow IKE as a host-inbound service within the security zone associated with the IKE gateway's external interface configuration. Any traffic that you wish to encrypt is routed to this tunnel interface.
Example:
[edit
set security ipsec proposal IPSEC-PROPOSAL protocol esp
Assumes the external interface is associated with the "untrust" zone.
[edit]
set security ike gateway <IKE-PEER> external-interface <EXTERNAL-INTERFACE-NAME>
set security zones security-zone untrust host-inbound-traffic system-services ike

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.15 JUSX-VN-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway must disable or remove unnecessary network services and functions that are not used as part of its role in the architecture.

```
GROUP ID: V-214682
RULE ID: SV-214682r382903
```

Rationale:

Network devices are capable of providing a wide variety of functions (capabilities or processes) and services. Some of these functions and services are installed and enabled by default. The organization must determine which functions and services are required to perform the content filtering and other necessary core functionality for each component of the SRX. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Services that may be related security-related, but based on the role of the device in the architecture do not need to be installed. For example, the Juniper SRX can have an Antivirus, Web filter, IDS, or ALG license. However, if these functions are not part of the documented role of the SRX in the enterprise or branch architecture, then these the software and licenses should not be installed on the device. This mitigates the risk of exploitation of unconfigured services or services that are not kept updated with security fixes. If left unsecured, these services may provide a threat vector.

Only remove unauthorized services. This control is not intended to restrict the use of Juniper SRX devices with multiple authorized roles.

Audit:

Review the documentation and architecture for the device.

If unneeded services and functions are installed on the device, but are not part of the documented role of the device, this is a finding.

Remediation:

Remove unnecessary services and functions. From operational mode, display the licenses available to be deleted and enter the following commands.
request system license delete license-identifier-list ?
request system license delete
Note: Only remove unauthorized services. This control is not intended to restrict the use of Juniper SRX devices with multiple authorized roles.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.16 JUSX-VN-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must use IKEv2 for IPsec VPN security associations.

```
GROUP ID: V-214683
RULE ID: SV-214683r385486
```

Rationale:

Use of IKEv2 leverages DoS protections because of improved bandwidth management and leverages more secure encryption algorithms.

Audit:

Verify only IKEv2 is used for the IKE security configuration on all configured gateways.
Use of IKEv1 mitigates the risk to a CAT III finding.
Show security ike gateway <VPN-GATEWAY>
If IKEv2 is not used for IKE associations, this is a finding.

Remediation:

For site-to-site VPNs, configure the Juniper SRX to use IKEv2 only.
[edit]
set security ike gateway <VPN-GATEWAY> address <GW-IP-ADDRESS>
set security ike gateway <VPN-GATEWAY> version v2-only

Additional Information:

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

1.17 JUSX-VN-000017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the PPSM CAL and vulnerability assessments.

```
GROUP ID: V-214684
RULE ID: SV-214684r385486
```

Rationale:

In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types); organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

DoD continually assesses the ports, protocols, and services that can be used for network communications. Some ports, protocols or services have known exploits or security weaknesses. Network traffic using these ports, protocols, and services must be prohibited or restricted in accordance with DoD policy. The PPSM CAL and vulnerability assessments provide an authoritative source for ports, protocols, and services that are unauthorized or restricted across boundaries on DoD networks.

The Juniper SRX must be configured to prevent or restrict the use of prohibited ports, protocols, and services throughout the network by filtering the network traffic and disallowing or redirecting traffic as necessary. Default and updated policy filters from the vendors will disallow older version of protocols and applications and will address most known non-secure ports, protocols, and/or services.

Audit:

Entering the following commands from the configuration level of the hierarchy.
[edit]
show security services
If functions, ports, protocols, and services identified on the PPSM CAL are not disabled, this is a finding.

Remediation:

Ensure functions, ports, protocols, and services identified on the PPSM CAL are not used for system services configuration.
[edit]
show security services
Compare the services that are enabled, including the port, services, protocols, and functions.
Consult the Juniper knowledge base and configuration guides to determine the commands for disabling each port, protocols, services, or functions that is not in compliance with the PPSM CAL and vulnerability assessments.

Additional Information:

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

1.18 JUSX-VN-000018 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).

```
GROUP ID: V-214685
RULE ID: SV-214685r385489
```

Rationale:

To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and any processes acting on behalf of users) must be uniquely identified and authenticated for all accesses except the following.

(i) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

(ii) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN or proxy capability). This does not apply to authentication for the purpose of configuring the device itself (i.e., device management).

Audit:

Ask the site to identify the VPN access profile. Verify the access profile uses LDAP, not password configuration, for user remote access to the network. Ask the site representative if group accounts are allowed or configured.
[edit]
show security access profile <VPN-LDAP-PROFILE-NAME>
If an access profile that uses LDAP is not configured as the first option in the authentication order, this is a finding.
If group accounts are allowed for VPN logon, this is a finding.

Remediation:

Configure the LDAP access profile. The LDAP server must use DoD PKI for authentication of users.
[edit]
set access profile <VPN-LDAP-PROFILE-NAME> authentication-order ldap
set access profile <VPN-LDAP-PROFILE-NAME> address-assignment pool dyn-vpn-pool
set access profile <VPN-LDAP-PROFILE-NAME> ldap-options base-distinguished-name CN=Users, DC=firewall, DC=com (Location from where LDAP will start searching for users)
set access profile <VPN-LDAP-PROFILE-NAME> ldap-options search search-filter sAMAccountName=
set access profile <VPN-LDAP-PROFILE-NAME> ldap-options search admin-search distinguished-name CN=Administrator, CN=Users, DC=firewall, DC=com (User who is authorized to search the ldap tree)
set access profile <VPN-LDAP-PROFILE-NAME> ldap-options search admin-search password <Administrator Password>
set access profile <VPN-LDAP-PROFILE-NAME> ldap-server <AD Server IP address> port 389/636
set access firewall-authentication pass-through default-profile <VPN-LDAP-PROFILE-NAME>
set access firewall-authentication web-authentication default-profile <VPN-LDAP-PROFILE-NAME>
Note: To find the user or administrator base DN, use any LDAP browser. On an Internet search engine, search for ldp.exe, which is a very basic LDAP browser.
When using LDAP groups to authenticate a user, or a user belonging to a group in the active directory, include the following statement:
set access profile <VPN-LDAP-PROFILE-NAME> session-options client-group
Note: Without the above statement, users are not searched based on the group name or group string.
The IP address pool configuration is as follows (the user will be assigned the IP from this pool):

set access address-assignment pool dyn-vpn-pool family inet network <IP Network for Dynamic-VPN User> (e.g.. 192.168.100.0/24)
set access address-assignment pool dyn-vpn-pool family inet range dyn-vpn-pool-range low <Starting IP address for Dynamic-VPN User> (e.g.. 192.168.100.1)
set access address-assignment pool dyn-vpn-pool family inet range dyn-vpn-pool-range high <ending IP address for Dynamic-VPN User> (e.g.. 192.168.100.100)
Note: The IP network used for dynamic VPN users should be different from the IP network of the external interface used in the IKE configuration.
The access profile is linked to the xauth of the gateway for dynamic VPN.
set security ike gateway <VPN-GATEWAY> xauth access-profile <VPN-LDAP-PROFILE-NAME>
Under security >> dynamic-vpn, add all the users that are going to use the dynamic VPN. The command is as follows:
set security dynamic-vpn clients all user
Note: For users who are going to use dynamic VPN, this will be the AD user logon name for each user.

Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

1.19 JUSX-VN-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Juniper SRX Services Gateway VPN must use multifactor authentication (e.g., DoD PKI) for network access to non-privileged accounts.

```
GROUP ID: V-214686
RULE ID: SV-214686r385492
```

Rationale:

To assure accountability and prevent unauthenticated access, non-privileged users must utilize multifactor authentication to prevent potential misuse and compromise of the system.

Multifactor authentication uses two or more factors to achieve authentication. Use of password for user remote access for non-privileged account is not authorized.

Factors include: (i) Something you know (e.g., password/PIN); (ii) Something you have (e.g., cryptographic identification device, token); or (iii) Something you are (e.g., biometric).

A non-privileged account is any information system account with authorizations of a non-privileged user.

Network access is any access to an application by a user (or process acting on behalf of a user) where said access is obtained through a network connection.

The DoD CAC with DoD-approved PKI is an example of multifactor authentication.

Audit:

Ask the site to identify the VPN access profile. Verify the access profile uses LDAP, not password configuration, for user remote access to the network. Ask the site if the LDAP server used authenticates users through PKI authentication.
[edit]
show security access profile
If an access profile that uses LDAP is not configured as the first option in the authentication order, this is a finding.
If password access is configured for VPN user access, this is a finding.
If the LDAP server used does not use PKI authentication, this is a finding.

Remediation:

Configure multifactor authentication by configuring an access profile for an authentication server or services to authenticate VPN users upon logon using DoD PKI.
Example:
[edit]
set access profile dyn-vpn-ldap-xauth authentication-order ldap
set access profile dyn-vpn-ldap-xauth address-assignment pool dyn-vpn-pool
set access profile dyn-vpn-ldap-xauth ldap-options base-distinguished-name CN=Users, DC=firewall, DC=com (Location from where LDAP will start searching for users)
set access profile dyn-vpn-ldap-xauth ldap-options search search-filter sAMAccountName=
set access profile dyn-vpn-ldap-xauth ldap-options search admin-search distinguished-name CN=Administrator, CN=Users, DC=firewall, DC=com (User who is authorized to search the ldap tree)
set access profile dyn-vpn-ldap-xauth ldap-options search admin-search password <Administrator Password>
set access profile dyn-vpn-ldap-xauth ldap-server <AD Server IP address> port 389/636
set access firewall-authentication pass-through default-profile dyn-vpn-ldap-xauth
set access firewall-authentication web-authentication default-profile dyn-vpn-ldap-xauth
The access profile is linked to the xauth of the gateway for dynamic VPN.
set security ike gateway dyn-vpn-local-gw xauth access-profile dyn-vpn-ldap-xauth
Note: Under security >> dynamic-vpn, add all the users that are going to use the dynamic VPN. The command is as follows:
set security dynamic-vpn clients all user
Note: For users who are going to use dynamic VPN, this will be the AD user logon name for each user.

Additional Information:

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

1.20 JUSX-VN-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must use FIPS 140-2 compliant mechanisms for authentication to a cryptographic module.

```
GROUP ID: V-214687
RULE ID: SV-214687r385516
```

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified, and therefore cannot be relied upon to provide confidentiality or integrity and DoD data may be compromised.

Network elements utilizing encryption are required to use FIPS compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements.

Audit:

Verify IPsec is defined and configured using FIPS-complaint protocols.
[edit]
show security ipsec vpn
If the IPSEC policy and VP are not configured to use FIPS 140-2 compliant mechanisms for authentication to a cryptographic module, this is a finding.

Remediation:

After configuring the Internet Key Exchange (IKE) gateway and IPsec policy, the following commands configure an IPsec policy, enabling Perfect Forward Secrecy (PFS) using Diffie-Hellman group
14 and associating the IPsec proposal configured in the previous example.
set security ipsec policy IPSEC-POLICY perfect-forward-secrecy keys group14
set security ipsec policy IPSEC-POLICY proposals IPSEC-PROPOSAL
The following commands define an IPsec VPN using a secure tunnel interface, specifying the IKE gateway information, IPsec policy, and tunnel establishment policy. Alternatively, administrators can configure on-traffic tunnel establishment.
[edit]
set security ipsec vpn VPN bind-interface st0.0
set security ipsec vpn VPN ike gateway IKE-PEER
set security ipsec vpn VPN ike ipsec-policy IPSEC-POLICY
set security ipsec vpn VPN establish-tunnels immediately

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

1.21 JUSX-VN-000021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).

```
GROUP ID: V-214688
RULE ID: SV-214688r385519
```

Rationale:

Lack of authentication and identification enables non-organizational users to gain access to the network or possibly a network element that provides opportunity for intruders to compromise resources within the network infrastructure.

This requirement only applies to components where this is specific to the function of the device or has the concept of a non-organizational user.

Audit:

Verify that groups are not used for authentication.
[edit]
show security access profile
If LDAP is not configured as the first authentication-order, this is a finding.

Remediation:

Configure the LDAP access profile. The LDAP server must use DoD PKI for authentication of users.
[edit]
set access profile <VPN-LDAP-PROFILE-NAME> authentication-order ldap
set access profile <VPN-LDAP-PROFILE-NAME> address-assignment pool dyn-vpn-pool
set access profile <VPN-LDAP-PROFILE-NAME> ldap-options base-distinguished-name CN=Users, DC=firewall, DC=com (Location from where LDAP will start searching for users)
set access profile <VPN-LDAP-PROFILE-NAME> ldap-options search search-filter sAMAccountName=
set access profile <VPN-LDAP-PROFILE-NAME> ldap-options search admin-search distinguished-name CN=Administrator, CN=Users, DC=firewall, DC=com (User who is authorized to search the ldap tree)
set access profile <VPN-LDAP-PROFILE-NAME> ldap-options search admin-search password <Administrator Password>
set access profile <VPN-LDAP-PROFILE-NAME> ldap-server <AD Server IP address> port 389/636
set access firewall-authentication pass-through default-profile <VPN-LDAP-PROFILE-NAME>
set access firewall-authentication web-authentication default-profile <VPN-LDAP-PROFILE-NAME>
Note: To find the user or administrator base DN, use any LDAP browser. On an Internet search engine, search for ldp.exe, which is a very basic LDAP browser.
When using LDAP groups to authenticate a user, or a user belonging to a group in the active directory, include the following statement:
set access profile <VPN-LDAP-PROFILE-NAME> session-options client-group
Note: Without the above statement, users are not searched based on the group name or group string.
The IP address pool configuration is as follows (the user will be assigned the IP from this pool):
set access address-assignment pool dyn-vpn-pool family inet network <IP Network for Dynamic-VPN User> (e.g.. 192.168.100.0/24)

set access address-assignment pool dyn-vpn-pool family inet range dyn-vpn-pool-range low <Starting IP address for Dynamic-VPN User> (e.g.. 192.168.100.1)
set access address-assignment pool dyn-vpn-pool family inet range dyn-vpn-pool-range high <ending IP address for Dynamic-VPN User> (e.g.. 192.168.100.100)
Note: The IP network used for dynamic VPN users should be different from the IP network of the external interface used in the IKE configuration.
The access profile is linked to the xauth of the gateway for dynamic VPN.
set security ike gateway <VPN-GATEWAY> xauth access-profile <VPN-LDAP-PROFILE-NAME>
Under security >> dynamic-vpn, add all the users that are going to use the dynamic VPN. The command is as follows:
set security dynamic-vpn clients all user
Note: Users who are going to use dynamic VPN. This will be the AD user logon name for each user.

Additional Information:

CCI-000804 Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

- NIST SP 800-53::IA-8
- NIST SP 800-53A::IA-8.1
- NIST SP 800-53 Revision 4::IA-8
- NIST SP 800-53 Revision 5::IA-8

1.22 JUSX-VN-000022 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Juniper SRX Services Gateway VPN must terminate all network connections associated with a communications session at the end of the session.

```
GROUP ID: V-214689
RULE ID: SV-214689r695324
```

Rationale:

Idle TCP sessions can be susceptible to unauthorized access and hijacking attacks. By default, routers do not continually test whether a previously connected TCP endpoint is still reachable. If one end of a TCP connection idles out or terminates abnormally, the opposite end of the connection may still believe the session is available. These “orphaned” sessions use up valuable router resources and can also be hijacked by an attacker. To mitigate this risk, routers must be configured to send periodic keep alive messages to check that the remote end of a session is still connected. If the remote device fails to respond to the TCP keep alive message, the sending router will clear the connection and free resources allocated to the session.

The TCP keep-alive for remote access is implemented in the Juniper SRX Firewall STIG.

Audit:

Ask the site representative which proposal implements Suite B.
[edit]
show security ike gateway
View the configured options.
If the dead-peer-detection is not configured, this is a finding.

Remediation:

For site-to-site VPN, configure an Internet Key Exchange (IKE) gateway that includes dead-peer-detection parameters such as in the following example.
set security ike gateway IKE-PEER ike-policy IKE-POLICY
set security ike gateway IKE-PEER address <Peer IP Address>
set security ike gateway IKE-PEER dead-peer-detection always-send
set security ike gateway IKE-PEER dead-peer-detection interval 10
set security ike gateway IKE-PEER dead-peer-detection threshold 2
set security ike gateway IKE-PEER local-identity inet <IPv4 Address in Certificate>
set security ike gateway IKE-PEER remote-identity inet <IPv4 Address in Remote Certificate>
set security ike gateway IKE-PEER external-interface
set security ike gateway IKE-PEER version v2-only
For dynamic (remote access) VPN, the TCP keep-alive for remote access is implemented in the Juniper SRX Firewall STIG.

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

1.23 JUSX-VN-000023 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Juniper SRX Services Gateway VPN Internet Key Exchange (IKE) must use cryptography that is compliant with Suite B parameters when transporting classified traffic across an unclassified network.

```
GROUP ID: V-214690
RULE ID: SV-214690r856575
```

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The network element must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

RFC 6379 Suite B Cryptographic Suites for IPsec defines four cryptographic user interface suites for deploying IPsec. Each suite provides choices for Encapsulating Security Payload (ESP) and IKE. The four suites are differentiated by the choice of IKE authentication and key exchange, cryptographic algorithm strengths, and whether ESP is to provide both confidentiality and integrity or integrity only. The suite names are based on the Advanced Encryption Standard (AES) mode and AES key length specified for ESP. Two suites are defined for transporting classified information up to SECRET level—one for both confidentiality and integrity and one for integrity only. There are also two suites defined for transporting classified information up to TOP SECRET level.

Audit:

Ask the site representative which proposal implements Suite B.
[edit]
show security ike
View the configured options.
If the value of the authentication-method and other options are not set for Suite B compliance, this is a finding.

Remediation:

The following example commands configure the IKE (phase 1) Suite B proposal. Note that SRX must have Junos 12.1X46 or later to support SuiteB.
[edit]
set security ike proposal suiteb-proposal
set ike proposal suiteb-proposal authentication-method ecdsa-signatures-384
set ike proposal suiteb-proposal dh-group group20
set ike proposal suiteb-proposal authentication-algorithm sha-384
set ike proposal suiteb-proposal encryption-algorithm aes-256-cbc

Additional Information:

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

1.24 JUSX-VN-000024 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN IKE must use NIST FIPS-validated cryptography to implement encryption services for unclassified VPN traffic.

```
GROUP ID: V-214691
RULE ID: SV-214691r856576
```

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The network element must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Audit:

Verify all Internet Key Exchange (IKE) proposals are set to use the AES encryption algorithm.
[edit]
show security ike
View the value of the encryption algorithm for each defined proposal.
If the value of the authentication method and other options are not set to use FIPS-compliant values, this is a finding.

Remediation:

The following example commands configure the IKE (phase 1) proposal.
[edit]
set security ike proposal <P1-PROPOSAL> authentication-method rsa-signatures
set security ike proposal p1-proposal dh-group group14
set security ike proposal p1-proposal authentication-algorithm sha-256
set security ike proposal p1-proposal encryption-algorithm aes-256-cbc
set security ike proposal p1-proposal lifetime-seconds 86400

Additional Information:

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

1.25 JUSX-VN-000025 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Juniper SRX Services Gateway VPN must configure Internet Key Exchange (IKE) with SHA1 or greater to protect the authenticity of communications sessions.

```
GROUP ID: V-214692
RULE ID: SV-214692r383107
```

Rationale:

Authenticity protection provides protection against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.

This requirement focuses on communications protection for the application session rather than for the network packet and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Depending on the required degree of confidentiality and integrity, web services/SOA will require the use of mutual authentication (two-way/bidirectional).

An IPsec Security Associations (SA) is established using either IKE or manual configuration.

Audit:

View all IKE proposals using in the VPN configuration.
[edit]
show security ike proposal
If the authentication algorithm in all IKE proposals is not set to SHA1 or higher, this is a finding.

Remediation:

Include the SHA1 or higher authentication algorithm in the IKE proposal. The following is an example command.
[edit]
set security ike proposal <P1-PROPOSAL-NAME> authentication-algorithm sha-256

Additional Information:

CCI-001184 Protect the authenticity of communications sessions.

- NIST SP 800-53::SC-23
- NIST SP 800-53A::SC-23.1
- NIST SP 800-53 Revision 4::SC-23
- NIST SP 800-53 Revision 5::SC-23

1.26 JUSX-VN-000026 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must only allow the use of DoD PKI established certificate authorities for verification of the establishment of protected sessions.

```
GROUP ID: V-214693
RULE ID: SV-214693r856577
```

Rationale:

Untrusted certificate authorities (CA) can issue certificates, but they may be issued by organizations or individuals that seek to compromise DoD systems or by organizations with insufficient security controls. If the CA used for verifying the certificate is not a DoD-approved CA, trust of this CA has not been established.

The DoD will only accept PKI certificates obtained from a DoD-approved internal or external certificate authority. Reliance on CAs for the establishment of secure sessions includes, for example, the use of Internet Key Exchange (IKE) authentication certificates.

This requirement focuses on communications protection for the application session rather than for the network packet. Network elements that perform these functions must be able to identify which session identifiers were generated when the sessions were established.

Audit:

Verify the all IKE proposals are set to use the AES encryption algorithm.
[edit]
show security ike
View the value of the authentication-method for each defined proposal.
If the value of the authentication-method for each defined proposal is not set to use AES, this is a finding.

Remediation:

The following example commands configure the IKE (phase 1) proposals. Use certificates instead of pre-shared keys to establish the IKE phase 1 tunnel.
This proposal requires AES 256-bit encryption
set security ike proposal p1-proposal authentication-method rsa-signatures

Additional Information:

CCI-002470 Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

- NIST SP 800-53 Revision 4::SC-23 (5)
- NIST SP 800-53 Revision 5::SC-23 (5)

1.27 JUSX-VN-000027 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must only allow incoming VPN communications from organization-defined authorized sources routed to organization-defined authorized destinations.

```
GROUP ID: V-214694
RULE ID: SV-214694r856578
```

Rationale:

Unrestricted traffic may contain malicious traffic which poses a threat to an enclave or to other connected networks. Additionally, unrestricted traffic may transit a network, which uses bandwidth and other resources.

Access control policies and access control lists implemented on devices, such as firewalls, that control the flow of network traffic, ensure the flow of traffic is only allowed from authorized sources to authorized destinations. Networks with different levels of trust (e.g., the Internet) must be kept separated.

Audit:

Request documentation of the Juniper SRX configuration drawings to determine which ports are configured for external/outbound traffic. Verify outbound interfaces have been configured with DoS screens.
[edit]
show security zones
If the VPN zone(s) is configured to allow unauthorized/untrusted traffic to unauthorized zones, this is a finding.

Remediation:

The SRX device will route traffic over the IPsec VPN's secure tunnel interface if there is a route with the next-hop specified as the secure tunnel interface. The following example commands configure an IPv4 and IPv6 static route for their respective secure tunnels.
set routing-options static route <IPv4 network/netmask> next-hop st0.0
set routing-options rib inet6.0 static route <IPv6 network/mask> next-hop st0.1
set security policies from-zone untrust to-zone trust policy group-sec-policy then permit tunnel ipsec-vpn groupvpn
Note: For the SRX device to transmit traffic over the IPsec tunnel, you must configure the secure tunnel interface (st0 in this case), associate it with a security zone, and create a static route entry for the remote network's address space.

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

1.28 JUSX-VN-000028 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must disable split-tunneling for remote clients VPNs.

```
GROUP ID: V-214695
RULE ID: SV-214695r856579
```

Rationale:

Split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information.

A VPN hardware or software client with split tunneling enabled provides an unsecured backdoor to the enclave from the Internet. With split tunneling enabled, a remote client has access to the Internet while at the same time has established a secured path to the enclave via an IPsec tunnel. A remote client connected to the Internet that has been compromised by an attacker in the Internet, provides an attack base to the enclave's private network via the IPsec tunnel. Hence, it is imperative that the VPN gateway enforces a no split-tunneling policy to all remote clients.

Traffic to the protected resource will go through the specified dynamic VPN tunnel and will therefore be protected by the Juniper SRX firewall's security policies.

Audit:

Verify split-tunneling is disabled.
[edit]
show security dynamic-vpn access-profile
If split-tunneling is not disabled, this is a finding.

Remediation:

Configure the VPN tunnel to control what is sent out in clear text. The "remote-protected-resources" command defines what is routed through the tunnel. The "remote-exceptions" command defines what traffic is sent out in clear text. The following is an example.
[edit]
set security dynamic-vpn access-profile
set security dynamic-vpn clients all ipsec-vpn
set security dynamic-vpn clients all remote-protected-resources <IP-address/mask>
set security dynamic-vpn clients all remote-exceptions 0.0.0.0/0

Additional Information:

CCI-002397 Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using organization-defined safeguards.

- NIST SP 800-53 Revision 4::SC-7 (7)
- NIST SP 800-53 Revision 5::SC-7 (7)

1.29 JUSX-VN-000031 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Juniper SRX Services Gateway VPN must use anti-replay mechanisms for security associations.

```
GROUP ID: V-214696
RULE ID: SV-214696r856580
```

Rationale:

Anti-replay is an IPsec security mechanism at a packet level which helps to avoid unwanted users from intercepting and modifying an ESP packet.

The SRX adds a sequence number to the ESP encapsulation which is verified by the VPN peer so packets are received within a correct sequence. This will cause issues if packets are not received in the order in which they were sent out.

By default the SRX has a replay window of 64 or 32, depending on the platform. The SRX drops packets received out of order that are not received within this window. However, this default may be overridden by setting the option no-anti-replay as follows: set security vpn name ike no-anti-replay.

Audit:

Verify anti-replay service is enabled.
[edit]
show security ipsec security-associations index 16384 detail
If anti-replay service is not enabled, this is a finding.

Remediation:

Remove the no-anti-replay Internet Key Exchange (IKE) option from the VPN configuration. By default the SRX has a replay window of 64 or 32, depending on the platform.
Example:
[edit]
delete security vpn name ike no-anti-replay

Additional Information:

CCI-001942 The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (9)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	JUSX-VN-000001 (Manual)	☐	☐
1.2	JUSX-VN-000002 (Manual)	☐	☐
1.3	JUSX-VN-000003 (Manual)	☐	☐
1.4	JUSX-VN-000004 (Manual)	☐	☐
1.5	JUSX-VN-000005 (Manual)	☐	☐
1.6	JUSX-VN-000006 (Manual)	☐	☐
1.7	JUSX-VN-000007 (Manual)	☐	☐
1.8	JUSX-VN-000008 (Manual)	☐	☐
1.9	JUSX-VN-000009 (Manual)	☐	☐
1.10	JUSX-VN-000011 (Manual)	☐	☐
1.11	JUSX-VN-000010 (Manual)	☐	☐
1.12	JUSX-VN-000012 (Manual)	☐	☐
1.13	JUSX-VN-000013 (Manual)	☐	☐
1.14	JUSX-VN-000014 (Manual)	☐	☐
1.15	JUSX-VN-000015 (Manual)	☐	☐
1.16	JUSX-VN-000016 (Manual)	☐	☐
1.17	JUSX-VN-000017 (Manual)	☐	☐
1.18	JUSX-VN-000018 (Manual)	☐	☐
1.19	JUSX-VN-000019 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	JUSX-VN-000020 (Manual)	☐	☐
1.21	JUSX-VN-000021 (Manual)	☐	☐
1.22	JUSX-VN-000022 (Manual)	☐	☐
1.23	JUSX-VN-000023 (Manual)	☐	☐
1.24	JUSX-VN-000024 (Manual)	☐	☐
1.25	JUSX-VN-000025 (Manual)	☐	☐
1.26	JUSX-VN-000026 (Manual)	☐	☐
1.27	JUSX-VN-000027 (Manual)	☐	☐
1.28	JUSX-VN-000028 (Manual)	☐	☐
1.29	JUSX-VN-000031 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 27, 2025	1.0.0	Initial CIS Release