centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 1404

# Procedimiento de Empleo Seguro
# Plataformas SRX de Juniper

Abril 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA


NIPO: 083-19-007-1

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.04.11 17:22:01 +02'00'

Fecha de Edición: abril de 2019
Juniper Networks ha participado en la realización y modificación del presente documento y sus anexos.

**LIMITACIÓN DE RESPONSABILIDAD**

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

**AVISO LEGAL**

# PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Abril de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

# ÍNDICE

# 1. INTRODUCCIÓN

1. Los dispositivos con Junos OS para plataformas SRX son un sistema completo de enrutamiento que soportan variedad de interfaces de alta velocidad (hasta 10 Gbps) para redes y aplicaciones de red. Estos dispositivos están físicamente auto-contenidos y albergan el software, firmware y hardware necesario para desarrollar las funciones de enrutamiento.
2. Los enrutadores soportan numerosos estándares de enrutamiento para asegurar flexibilidad y escalabilidad, así como protocolos IPSec. Estas funciones pueden ser gestionadas a través del software de Junos, desde una consola en un terminal o vía conexión de red. La gestión de red puede ser securizada utilizando IPSec, SNMP v3 y protocolos SSH.
3. Además, los dispositivos soportan funcionalidades de detección y prevención, que permiten detectar y reaccionar ante ataques potenciales en tiempo real. El componente de IPS puede estar basado en firmas de ataque que especifican las características del tráfico potencialmente malicioso basadas en una variedad de atributos de datos de paquetes. También soportan detección anómala basada en las desviaciones del tráfico monitorizado con respecto a los valores esperados.
4. Estos dispositivos de seguridad realizan el enrutado mediante procesos denominados *Virtual Router* (VR). Un dispositivo de seguridad divide su componente de enrutamiento en dos o más VRs, cada una de las cuales mantiene su propia lista de redes conocidas en forma de tabla de enrutamiento, lógica de enrutamiento y zonas de seguridad asociadas.
5. Los dispositivos se gestionan y configuran vía interfaz de línea de comandos utilizando conexiones IPSec y no dependen de protocolos como FTP o SSL para operar correctamente.

## 2. OBJETO Y ALCANCE

6. En la presente guía se recoge el procedimiento de empleo seguro para las plataformas Junos 15.1X49D-60 y Junos 12.3X48-D30 para SRX, para las funciones de IPS, cortafuegos y VPN.

7. Aunque todas las plataformas presentan diferentes opciones de configuración, los algoritmos criptológicos utilizados en esta guía cumplen con los requisitos estipulados en la CCN-STIC-807 Criptología de empleo en el ENS para la Categoría Alta.

## 3. ORGANIZACIÓN DEL DOCUMENTO

8. El presente documento se divide en tres partes fundamentales, de acuerdo a distintas fases que componen el ciclo de vida del producto:

    a) Apartado 4. En este apartado se recogen los requisitos o recomendaciones asociadas a la fase de **despliegue e instalación** física del producto.

    b) Apartado 5. En este apartado se recogen requisitos o recomendaciones asociadas a la fase de **configuración segura** del producto.

    c) Apartado 6. En este apartado se recogen requisitos o recomendaciones relativas a las tareas de mantenimiento durante la fase de **operación y mantenimiento** del producto.

## 4. FASE DE DESPLIEGUE E INSTALACIÓN

### 4.1 Entrega segura del producto

9. Durante el proceso de entrega deberán llevarse a cabo una serie tareas de comprobación, de cara a garantizar que el producto recibido no se ha manipulado indebidamente:

    a) Etiqueta de envío. Deberá comprobarse que la etiqueta de envío identifica correctamente el nombre del usuario, su dirección y el dispositivo.

    b) Embalaje externo. Deberá inspeccionarse la caja de envío externa y la cinta adhesiva. Se comprobará que la cinta adhesiva no esté cortada ni se haya deteriorado en ningún punto. Así mismo, la caja no deberá presentar cortes ni daños que permitan acceder al dispositivo.

    c) Embalaje interno. Deberá inspeccionarse la bolsa de plástico y el sistema de sellado. La bolsa no deberá presentar cortes ni haber sido extraída. El sistema de sellado deberá estar intacto.

10. En caso de identificarse algún problema durante la inspección, el usuario deberá ponerse en contacto inmediatamente con el proveedor, al que se le indicará el número de pedido, el número de seguimiento y una descripción del problema.
11. Además, es necesario realizar una serie de comprobaciones para garantizar que la caja recibida la envió Juniper Networks y no existe una suplantación de identidad:
    a) Verificar la existencia de un pedido de compra al fabricante, dado que Juniper Networks nunca envía dispositivos sin pedido de compra.
    b) Comprobar que se ha recibido la notificación de envío de Juniper Networks en la dirección de correo electrónico que se indicó cuando se realizó el pedido. Este mensaje deberá incluir la siguiente información:
        i. Número de pedido de compra.
        ii. Número de pedido de Juniper Networks utilizado para hacer un seguimiento del envío.
        iii. Número de seguimiento del transportista utilizado para hacer un seguimiento del envío.
        iv. Lista de artículos enviados, incluidos los números de serie.
        v. Dirección y contactos del proveedor y del cliente.
    c) Verificar que el envío lo inició Juniper Networks. Para ello, sería necesario:
        i. Comparar el número de seguimiento de pedido del transportista que aparece en la notificación de envío de Juniper Networks con el número de seguimiento en el paquete recibido.
        ii. Iniciar sesión en el portal de ayuda al cliente en línea de Juniper Networks en la dirección:

            https://www.juniper.net/customers/csc/management

            para ver el estado del pedido.
        iii. Comparar el número de seguimiento del transportista o el número de pedido de Juniper Networks que aparece en la notificación de envío de Juniper Networks con el número de seguimiento en el paquete recibido.

## 4.2 Instalación segura

12. Los dispositivos deberán instalarse dentro de un Centro de Proceso de Datos (CPD), cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa.

13. Para ello, la sala en la que se ubica el CPD estará dotada de un sistema de control que asegure que únicamente dichas personas pueden acceder al dispositivo (incluido fuera del horario laboral).

# 5. FASE DE CONFIGURACIÓN

## 5.1 Administración del producto

14. El equipo se configurará de acuerdo a los principios de mínima funcionalidad y mínimo privilegio, es decir, se tratará que los usuarios administradores sean los mínimos posibles y que el conjunto de usuarios en general no disponga de más privilegios que los que necesita.
15. Las actualizaciones de firmware del dispositivo, así como la configuración de funciones de seguridad importantes del sistema operativo, solo podrán ser realizadas por un número reducido de administradores/administradores de seguridad.
16. La administración del dispositivo podrá realizarse de manera local o remota, aunque la primera opción siempre será preferible a la segunda, especialmente en el caso en que el dispositivo se utilice como DPP (Dispositivo de Protección de Perímetro):
    a) Administración local. Podrá realizarse desde un terminal utilizando la interfaz de línea de comandos (CLI). Para ello, deberá configurarse el puerto de consola RJ-45 situado en el panel posterior del dispositivo como equipo de terminal de datos (DTE) RS-232.
    b) Administración remota. Podrá realizarse a través de cualquier interfaz Ethernet. Aunque el dispositivo permite utilizar diversos protocolos para realizar la gestión remota, como J-Web y Telnet, el único permitido en este caso es SSHv2, que está habilitado por defecto en el dispositivo. Además, este canal para administración remota deberá encapsularse en una VPN IPSec, tal como se describirá más adelante.
17. Para la administración del dispositivo deberá utilizarse una interfaz dedicada de solo gestión. Esta interfaz solamente podrá aceptar o responder tráfico cuyo destino sea el propio dispositivo (administración fuera de banda).

## 5.2 Configuración de contraseñas asociadas para un administrador autorizado

18. El administrador autorizado va asociado a una clase de inicio de sesión predefinida en la que se le asignan todos los permisos. Los datos se almacenan de manera local para autenticar las contraseñas fijas.
19. A la hora de seleccionar contraseñas para las cuentas de administrador autorizadas, deberán seguirse las siguientes directrices y opciones de configuración:

a) Deberán ser fáciles de recordar, de modo que los usuarios no se sientan tentados a escribirlas. En caso de que sea necesario guardar una copia física de la contraseña, se hará en un contenedor seguro.

b) Deberán ser privadas y no compartirse con nadie.

c) Deberán cambiarse periódicamente, con un período no superior a 180 días.

d) No deberá permitirse la repetición de al menos las 5 últimas contraseñas utilizadas.

e) No deberá realizarse un nuevo cambio de contraseña en los 4 días posteriores al último cambio.

f) Deberán ser de 9 caracteres como mínimo.

**[edit] administrator@host# set system login password minimum-length 9**

g) Deberán incluir caracteres alfanuméricos y caracteres especiales como "!", "@", "#", "$", "%", "^", "&", "*", "(" y ")", al menos una letra en mayúscula y otra en minúscula, un número o más, y un signo de puntuación o más.

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

h) Deberán contener un número mínimo de juegos de caracteres o de cambios en el juego de caracteres. El número mínimo de juegos de caracteres necesario en contraseñas de texto sin formato en Junos es dos.

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

i) El algoritmo de autenticación para las contraseñas de texto sin formato se debe configurar como SHA-256.

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

j) El uso de caracteres de control en las contraseñas no está recomendado.

k) Son contraseñas poco seguras:

   i. Las palabras que puedan estar en o que existan como forma permutada en un archivo de sistema, como /etc/passwd.

   ii. El nombre de host del sistema (siempre lo primero que se intenta).

   iii. Cualquier palabra que aparezca en un diccionario, incluidos también diccionarios de otros idiomas distintos al inglés o al castellano, palabras que puedan aparecer en obras de autores

famosos, palabras y frases habituales del mundo de los deportes, dichos, películas y series televisivas, etc.

iv. Permutaciones de todo lo anterior. Por ejemplo, una palabra del diccionario cuyas vocales se hayan sustituido por números (por ejemplo f00t) o a la que se añadan números al final.

v. Palabras generadas por máquinas. Los algoritmos reducen el espacio de búsqueda de los programas de adivinación de contraseñas, por lo que no conviene usarlos.

vi. Una contraseña fuerte y reutilizable puede basarse en letras de una frase o una palabra favorita que vaya después concatenada con otras palabras no relacionadas junto con números y signos de puntuación adicionales.

## 5.3 Configuración de un administrador autorizado

20. Las cuentas raíz se encuentran siempre pre-configuradas de fábrica. Su uso debe restringirse a la instalación y configuración inicial del dispositivo. Nunca deberán utilizarse en la operación normal del equipo.

21. El administrador autorizado deberá tener todos los permisos, incluido el de cambiar la configuración del dispositivo.

22. Para configurar un administrador autorizado se deberá:

    a) Crear una clase de inicio de sesión llamada “security-admin” con todos los permisos.

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

    b) Definir su usuario administrador autorizado “CPSTIC-usuario”.

    **[edit] root@host# set system login user CPSTIC-usuario full-name “<Administrador Autorizado>” class security-admin authentication encrypted-password <contraseña>**

    c) Configurar el algoritmo de autenticación SHA-256 para las contraseñas sin cifrar.

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

    Esto garantiza que la nueva contraseña va protegida con un hash SHA-256 en lugar de con el algoritmo de hash de contraseña por defecto. Para reiniciar la contraseña, es posible utilizar el comando:

    **[edit] root@host# set system login user CPSTIC-usuario authentication encrypted-password <contraseña>**

    y confirmarla cuando se solicite.

    d) Confirmar los cambios.

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

## 5.4 Configuración de SSH y conexión de la consola

### 5.4.1 Configuración de un anuncio y un mensaje de inicio de sesión en el sistema

23. El mensaje de inicio de sesión en el sistema aparece antes de que el usuario inicie sesión y el anuncio de inicio de sesión en el sistema aparece después de que el usuario inicie sesión. En el dispositivo no aparece por defecto ningún mensaje, por lo que deberá configurarse.
24. Antes del establecimiento de una sesión en el Sistema deberá aparecer un mensaje advirtiendo de que **solo los usuarios autorizados pueden acceder al Sistema y que toda la actividad será supervisada para verificar el cumplimiento de la política de seguridad**. En dicho mensaje no se facilitará información del Sistema que pueda identificarlo o caracterizarlo ante un atacante.
25. Deberá utilizarse el siguiente comando para configurar un mensaje de inicio de sesión en el sistema:

    **[edit] user@host# set system login message "<Mensaje de inicio de sesión en el sistema>"**

26. En el caso de que se desee configurar también un anuncio de inicio de sesión deberá utilizarse el siguiente comando:

    **[edit] user@host# set system login announcement “<Anuncio de inicio de session>”**

27. Si el texto del mensaje contiene algún espacio, deberá encerrarse entre comillas. Puede dar formato al mensaje con los siguientes caracteres especiales:

    a) \n Nueva línea.

    b) \t Tabulador horizontal.

    c) \’ Comilla simple.

    d) \” Comilla doble.

    e) \\ Backslash.

### 5.4.2 Limitación del número de intentos de inicio de sesión de usuario para sesiones SSH

28. Los administradores remotos pueden iniciar sesión en un dispositivo utilizando para ello el protocolo SSH. Si el administrador remoto introduce un nombre de usuario y una contraseña válidos, se concede el acceso al dispositivo. Si, por el contrario, las credenciales no son válidas, el dispositivo permite que se vuelta a intentar la autenticación tras un intervalo de tiempo que comienza después de un segundo y va aumentando exponencialmente.

29. Si el número de intentos de autenticación sobrepasa el máximo configurado (no superior a 5), no se aceptarán más intentos de autenticación durante el intervalo de tiempo determinado. Una vez venza este intervalo se aceptarán nuevos intentos de autenticación.

30. Mediante la opción "tries-before-disconnect" se indica el número de veces que un usuario puede intentar introducir una contraseña para iniciar sesión. A partir de ese número de intentos la conexión se cerrará. El comando sería el siguiente:

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

    El valor por defecto es el 10 aunque, como ya se ha indicado anteriormente, no deberá ser mayor de 5 intentos.

31. Mediante la opción "backopff-threshold" es posible configurar un retardo, en segundos, antes de que el usuario pueda volver a intentar introducir la contraseña tras un intento fallido.

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

    En este caso, <numero> es el umbral para el número de intentos fallidos antes de que el usuario tenga que esperar un retardo para volver a introducir la contraseña de nuevo.

32. Por último, es posible utilizar la opción "backoff-factor" para especificar la longitud del retardo en segundos. El rango es de 1 a 3, y el valor por defecto es 2.

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

    El retardo se incrementa con el valor especificado por cada intento después de haber alcanzado el umbral. El rango va de 5 a 10, y el valor por defecto es 5 segundos.

## 5.5 Configuración de algoritmos criptográficos SSH

33. Como ya se indicó anteriormente, SSH a través de IPsec es la única interfaz de gestión remota que debe usarse en esta configuración del dispositivo.

34. Para configurarlo, es necesario iniciar sesión con la cuenta raíz en el dispositivo y editar la configuración, para lo que se llevarán a cabo los siguientes pasos, teniendo en cuenta que pueden introducirse en cualquier orden y confirmarse todos a la vez:

    a) Especificar los algoritmos SSH host-key permitidos para los servicios del sistema (SSH-ECDSA).

       **[edit] root@host# set system services ssh hostkey-algorithm ssh-ecdsa**

    b) Especificar el valor SSH key-exchange de las claves Diffie-Hellman para los servicios del sistema (ECDH-SHA2-NISTP256).

**[edit] root@host#set system services ssh key-exchange ecdh-sha2-nistp256**

c) Especificar todos los algoritmos de autenticación de mensajes permitidos para SSHv2 (HMAC-SHA1).

**[edit] root@host#set system services ssh macs hmac-sha1**

d) Especificar los algoritmos de cifrado permitidos (AES-128-CBC).

**[edit] root@host#set system services ssh ciphers aes128-cbc**

e) Confirmar los cambios.

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

## 5.6 Configuración de un canal seguro para el Syslog

### 5.6.1 Creación de un canal seguro para el Syslog

35. Para establecer la conexión con el servidor de Syslog deberá configurarse un canal seguro. Para ello, se creará un túnel VPN IPSec entre el dispositivo y el servidor de almacenamiento externo.

36. Las tablas que se muestran a continuación recogen un listado de los algoritmos considerados en esta configuración VPN con IPSec. El resto de opciones de configuración que permite el dispositivo no se considera adecuado, ya que utilizan algoritmos que no reúnen la fortaleza necesaria para un nivel alto de seguridad (min. 128 bits).

| ALGORITMOS VPN IPSEC – IKE EN FASE 1 | |
|---|---|
| **Método de autenticación** | *ECDSA-signatures-256*, *ECDSA-signatures-384* |
| **Algoritmos de autenticación** | SHA-256, SHA-384 |
| **Grupo DH** | 19, 20 |
| **Algoritmo de cifrado** | AES-128-GCM, AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-256-GCM |

**Tabla 1 Algoritmos IKE Fase 1**

| ALGORITMOS VPN IPSEC – IKE EN FASE 2 | |
|---|---|
| **Método de autenticación** | HMAC-SHA1-96, HMAC-SHA-256-128 |
| **Grupo DH** | 19, 20 |
| **Método de cifrado** | ESP |
| **Algoritmo de cifrado** | AES-128-GCM, AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-256-GCM |

**Tabla 2 Algoritmos IKE Fase 2**

### 5.6.2 Ejemplo de configuración de un canal seguro con un servidor de almacenamiento externo remoto

37. En este ejemplo, el servidor de almacenamiento externo remoto es un servidor de Syslog basado en Linux donde el túnel VPN con IPSec finaliza en la interfaz de salida Eth1. Los datos de registro transferidos desde el dispositivo se envían a la interfaz de finalización de Syslog Eth2 y la aplicación StrongSwan proporciona la funcionalidad VPN con IPSec.

38. La siguiente tabla muestra los datos del túnel VPN con IPSec que se utilizan en este ejemplo.

| PROPUESTA EN EN FASE 1 (P1, IKE) | |
|---|---|
| **Método de autenticación** | ECDSA-signatures-256 |
| **Algoritmo de autenticación** | SHA-256 |
| **Grupo-DH** | 19 |
| **Algoritmo de cifrado** | AES-128-CBC |
| **PROPUESTA EN EN FASE 2 (P2, IPSEC)** | |
| **Algoritmo de autenticación** | HMAC-SHA1-96 |
| **Grupo-DH** | 19 |
| **Método de cifrado** | ESP |
| **Algoritmo de cifrado** | AES-128-CBC |

**Tabla 3 Parámetros de configuración VPN para conexión con servidor de Syslog**

39. La siguiente figura muestra el esquema de comunicación que se configura en el ejemplo. Se establece un túnel con IPSec entre una interfaz de salida de dispositivos (Intf-1) y una interfaz de salida del servidor de Syslog remoto (Eth1). Los datos se reenvían después de forma interna en el servidor de almacenamiento externo remoto desde su interfaz de salida Eth1; es decir, el extremo VPN a Eth2.

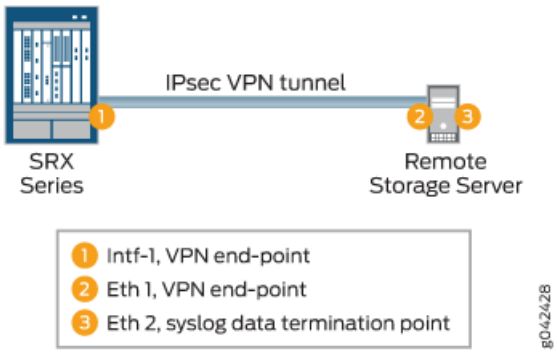


**Figura 1 Túnel VPN con IPSec**

40. La tabla que se muestra a continuación recoge los datos de la interfaz y la configuración IP utilizada.

| DISPOSITIVO JUNOS | |
|---|---|
| **Dirección IP** | Interfaz "Intf-2": GE-0/0/1 – Dirección IP: 198.51.100.2<br>Interfaz "Intf-1": GE/0/0/2 – Dirección IP: 198.51.100.1 |
| **Habilitar** | Registro de Syslog en servidor de Syslog remoto |
| **SERVIDOR DE ALMACENAMIENTO REMOTO** | |
| **Dirección IP** | Eth1: 198.51.100.3<br>Eth2: 203.0.113.1<br>Puerta de enlace Eth1: 198.51.100.1 |
| **Herramientas** | SSH y Strongswan (para VPN con IPSEC) |

**Tabla 4 Datos de la interfaz y configuración IP para la ruta de confianza**

41. Para configurar la ruta o el canal seguro con el servidor de almacenamiento externo remoto es necesario seguir los siguientes pasos:

    a) Habilitar registro de *streaming* para los registros del tráfico.

**[edit security]**

**user@host#set log cache**

**user@host#set log mode stream**

**user@host#set log source-address 198.51.100.2**

**user@host#set log stream STREAM category all**

**user@host#set log stream STREAM host 203.0.113.1**

Donde, 198.51.100.2 es la dirección IP de la interfaz de salida hacia el servidor de Syslog donde finaliza el túnel VPN con IPSec, y 203.0.113.1 es la dirección IP de la interfaz del servidor de Syslog de destino de los datos de registro.

b) Habilitar el Syslog en el dispositivo.

**[edit system]**

**user@host#set syslog user * any emergency**

**user@host#set syslog host 203.0.113.1 any any**

**user@host#set syslog file SYSLOG any any**

**user@host#set syslog file SYSLOG authorization info**

**user@host#set syslog file SYSLOG_COMMANDS interactive-commands error**

**user@host#set syslog file traffic-log any any**

**user@host#set syslog file traffic-log match RT_FLOW_SESSION**

**user@host#set syslog source-address 198.51.100.2**

c) Habilitar VPN en el dispositivo.

Configuración IKE:

**[edit security]**

**user@host#set ike proposal IKE_Proposal authentication-method ecdsa-signatures-256**

**user@host#set ike proposal IKE_Proposal dh-group group19**

**user@host#set ike proposal IKE_Proposal authentication-algorithm sha-256**

**user@host#set ike proposal IKE_Proposal encryption-algorithm aes-128-cbc**

**user@host#set ike policy IKE_Policy mode main**

**user@host#set ike policy IKE_Policy proposals IKE_Proposal**

**user@set ike policy IKE_Policy certificate local-certificate <certificado local>**

**set ike policy IKE_Policy certificate peer-certificate-type < pkcs7 | x509-signature>**

**user@host#set ike gateway GW ike-policy IKE_Policy**

**user@host#set ike gateway GW address 198.51.100.3**

**user@host#set ike gateway GW local-identity inet 198.51.100.1**

**user@host#set ike gateway GW external-interface ge-0/0/2**

**user@host#set ike gateway GW version v2-only**

Configuración IPsec:

**[edit security ipsec]**

**user@host#set proposal IPsec_Proposal protocol esp**

**root@host#set proposal IPsec_Proposal authentication-algorithm hmac-sha1-96**

**root@host#set proposal IPsec_Proposal encryption-algorithm aes-128-cbc**

**root@host#set policy IPsec_Policy perfect-forward-secrecy keys group19**

**root@host#set policy IPsec_Policy proposals IPsec_Proposal**

**root@host#set vpn VPN bind-interface st0.0**

**root@host#set vpn VPN ike gateway GW**

**root@host#set vpn VPN ike ipsec-policy IPsec_Policy**

**root@host#set vpn VPN establish-tunnels immediately**

d) Aplicar las siguientes configuraciones adicionales en el dispositivo.

Registro de IKE:

**[edit security ike]**

**root@host#set traceoptions file IKE_Trace**

**root@host#set traceoptions file size 10000000**

**root@host#set traceoptions flag all**

e) Seguimiento de flujo:

**[edit security flow]**

**root@host#set traceoptions file DEBUG**

**root@host#set traceoptions file size 1000000**

**root@host#set traceoptions flag all**

f) Opciones de ruta:

**[edit]**

**root@host#set routing-options static route 203.0.113.2/24 qualified-next-hop st0.0 preference 1**

g) Configuración de la libreta de direcciones:

**[edit security address-book]**

**root@host#set global address trustLAN 198.51.100.0/24**

**root@host#set global address unTrustLAN 198.51.100.3/24**

h) Configuración de zona:

**[edit security zones]**

**root@host#set security-zone trustZone host-inbound-traffic system-services all**

**root@host#set security-zone trustZone host-inbound-traffic protocols all**

**root@host#set security-zone trustZone interfaces ge-0/0/1.0**

**root@host#set security-zone unTrustZone host-inbound-traffic system-services all**

**root@host#set security-zone unTrustZone host-inbound-traffic protocols all**

**root@host#set security-zone unTrustZone interfaces st0.0**

**root@host#set security-zone unTrustZone interfaces ge-0/0/2.0**

i) Configuración de política:

**[edit security policies]**

**root@host#set from-zone trustZone to-zone unTrustZone policy Policy1 match source-address trustLAN**

**root@host#set from-zone trustZone to-zone unTrustZone policy Policy1 match destination-address unTrustLAN**

**root@host#set from-zone trustZone to-zone unTrustZone policy Policy1 match application any**

**root@host#set from-zone trustZone to-zone unTrustZone policy Policy1 then permit**

**root@host#set from-zone trustZone to-zone unTrustZone policy Policy1 then log session-init**

**root@host#set from-zone trustZone to-zone unTrustZone policy Policy1 then log session-close**

**root@host#set from-zone unTrustZone to-zone trustZone policy Policy1 match source-address unTrustLAN**

**root@host#set from-zone unTrustZone to-zone trustZone policy Policy1 match destination-address trustLAN**

**root@host#set from-zone unTrustZone to-zone trustZone policy Policy1 match application any**

**root@host#set from-zone unTrustZone to-zone trustZone policy Policy1 then permit**

**root@host#set from-zone unTrustZone to-zone trustZone policy Policy1 then log session-init**

**root@host#set from-zone unTrustZone to-zone trustZone policy Policy1 then log session-close**

## 5.7 Configuración de reglas de filtrado de tráfico

42. Un principio clave cuando se define una política de cortafuegos es seguir una aproximación basada en denegación por defecto, en la que selectivamente se permite sólo lo estrictamente necesario. Por el contrario, una aproximación de denegación selectiva se fundamenta en denegar todo aquello que no está permitido, práctica muy poco recomendable por su difícil gestión y porque deja una superficie de ataque mucho mayor.

43. El principio de denegación por defecto simplemente requiere que se habilite lo permitido y que el cortafuegos bloquee todo lo demás a través de las reglas rechazo y denegación total. En base a esta filosofía, deberán seguirse los siguientes pasos de configuración:

    a) Configuración de reglas de filtrado de tráfico. Donde se especificará qué tráfico se **permite** en base a unos determinados criterios basados en atributos de protocolos definidos por el usuario del sistema. Ver ejemplo 5.7.2.

    b) Configuración de reglas por defecto de rechazo y denegación total. En el caso en que el tráfico recibido no cumpla ninguno de los criterios definidos en el punto anterior se **denegará**, para lo cual deberá activarse la regla de rechazo por defecto. Ver 5.7.3.

    c) Configuración del registro de paquetes descartados mediante la opción por defecto de denegación total. Cada vez que se descarte un paquete por aplicación de la opción por defecto deberá guardarse un registro para que pueda ser revisado posteriormente. Ver 5.7.4

    d) Configuración reglas de rechazo por defecto y registro cuando se cumpla alguna de estas reglas:

        i. Se reciben fragmentos no válidos. Ver 5.7.5.

        ii. Se reciben paquetes IP fragmentados que no se pueden volver a ensamblar por completo. Ver 5.7.5.

        iii. La dirección origen es igual a la dirección de la interfaz de red. Ver 5.7.6.

iv. La dirección origen no pertenece a las redes asociadas con la interfaz de red. Ver 5.7.6.

v. La dirección origen está definida como perteneciente a una red de *broadcast*. Ver 5.7.6.

vi. Cuando se especifiquen las opciones IP Loose Source Routing, Strict Source Routing o Record Route. Ver 5.7.7

vii. La dirección origen está definida como perteneciente a una red *multicast*. Ver 5.7.8.

viii. La dirección origen está definida como dirección de *loopback*. Ver 5.7.8.

ix. Cuando la dirección origen es una dirección *multicast.* Ver 5.7.8.

x. La dirección origen o destino es una dirección de enlace-local.

xi. La dirección origen o destino se define como una dirección "reservada para uso futuro", tal y como se especifica en RFC 5735 para IPv4. Ver 5.7.8.

xii. La dirección origen o destino se define como una "dirección sin especificar" o una dirección "reservada para uso y definición futuros", tal y como se especifica en RFC 3513 para IPv6. Ver 5.7.8.

xiii. Se reciben paquetes IPv6 sin asignar.

### 5.7.1 Filtrado y protocolos soportados

44. Es posible configurar el dispositivo para filtrar tráfico de red por los campos especificados para los siguientes tipos de tráfico de paquetes de red:

| PROTOCOLO O RFC | CAMPOS |
|---|---|
| **ICMPv4 – RFC 792** | Tipo<br>Código |
| **ICMPv6 – RFC 4443** | Tipo<br>Código |
| **IPv4 – RFC 791** | Dirección de origen<br>Dirección de destino<br>Protocolo de capa de transporte |
| **IPv4 – RFC 2460** | Dirección de origen<br>Dirección de destino<br>Protocolo de capa de transporte |
| **TCP – RFC 793** | Puerto de origen<br>Puerto de destino |
| **UDP – RFC 768** | Puerto de origen<br>Puerto de destino |

45. Además, los siguientes protocolos son también compatibles con el dispositivo.
    - IPsec
    - IKE
    - OSPF
    - BGP

    **Solamente se permitirá utilizar SSH a través de un túnel IPSec.**

### 5.7.2 Configuración de reglas de filtrado de tráfico

46. Podrán configurarse reglas de filtrado de tráfico en el dispositivo para forzar la validación contra atributos de protocolos y dirigir el tráfico de acuerdo a dichos atributos. Estas reglas se basan en zonas a las que están vinculadas los interfaces de red.
47. El siguiente procedimiento describe un ejemplo de cómo configurar reglas de filtrado para dirigir tráfico FTP desde una zona de origen (trustZone) a una de destino (untrustZone) y desde una LAN de origen (trustLan) a una LAN destino (untrustLan). Aquí, el tráfico pasa de la interfaz de dispositivo A en trustZone a la interfaz B en untrustZone.
    a) Configurar una zona y sus interfaces.

    **[edit]**

**user@host# set security zones security-zone trustLan interfaces ge-0/0/0**

b) Configurar la política de seguridad que debe aplicarse en un determinado sentido del tráfico y especificar los criterios de coincidencia.

**[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**

c) Configurar la política de seguridad en un determinado sentido y especificar qué acción llevar a cabo cuando un paquete coincida con los criterios.

**[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**

Aquí, trustZone y untrustZone son zonas de seguridad preconfiguradas, y trustLan y untrustLan son direcciones de red preconfiguradas.

48. Para permitir que entre todo el tráfico IPv6 a un dispositivo de la serie SRX, debe configurarse el dispositivo con el modo de reenvío basado en flujo. Aunque la política por defecto en el modo de reenvío basado en flujo sea descartar todo el tráfico IPv6, es posible agregar reglas para permitir los tipos de tráfico IPv6 seleccionados.

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

### 5.7.3 Configuración de regla de denegación total por defecto

49. Para que el cortafuegos deniegue por defecto todo tipo de tráfico a menos que se creen reglas explícitamente para permitirlo, se utilizará el comando siguiente:

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

### 5.7.4 Configuración de registro de paquetes descartados mediante la opción denegación total por defecto

50. Para guardar el registro de paquetes que han sido descartados utilizando la opción de denegación total por defecto es necesario seguir los siguientes pasos, teniendo en cuenta que es posible introducir los comandos de configuración en cualquier orden y confirmarlos todos a la vez:

    a) Iniciar la sesión con la cuenta raíz en el dispositivo y editar la configuración.

    b) Configurar una política de seguridad de red en un contexto global y especificar los criterios de coincidencia de ésta.

    **[edit security policy]**

    **user@host# set global policy always-last-default-deny-and-log match source-address any destination-address any application any**

    c) Especificar la acción que debe llevarse a cabo cuando el paquete coincida con los criterios indicados.

    **[edit security policy]**

    **user@host# set global policy always-last-default-deny-and-log then deny**

    d) Configurar la política de seguridad para habilitar los registros en el momento de inicializar la sesión.

    **[edit security policy]**

    **user@host# set global policy always-last-default-deny-and-log then log session-init**

    Es importante tener en cuenta que este procedimiento puede capturar una gran cantidad de datos desde que se activa la política hasta que se configuran otras políticas de filtrado.

### 5.7.5 Configuración de opción de rechazo para fragmentos no válidos y paquetes IP fragmentados

51. En este punto se describe cómo configurar reglas de rechazo para fragmentos no válidos y paquetes IP fragmentados que no se pueden volver a ensamblar.

52. Para ello, deberán introducirse los siguientes comandos en cualquier orden y confirmarlos todos a la vez:

    a) Iniciar la sesión con la cuenta raíz en el dispositivo y editar la configuración.

    b) Especificar la configuración de flujo para forzar el reensamblado de los fragmentos IP.

**[edit]**

**user@host# set security flow force-ip-reassembly**

c) Eliminar las opciones de monitorización de ID y de IDS y habilitar la opción IDS de fragmentos ICMP.

**[edit]**

**user@host# delete security screen ids-option trustScreen icmp fragment**

d) Eliminar la opción IDS de la capa IP y habilitar la opción IDS de bloqueo de fragmentos IP.

**[edit]**

**user@host# delete security screen ids-option trustScreen ip block-frag**

### 5.7.6 Configuración opción de rechazo por defecto para suplantación (Spoofing) de direcciones origen

53. Deberán configurarse opciones de rechazo por defecto para *spoofing* de direcciones origen que contemplen los siguientes casos:

    a) La dirección de origen es igual que la dirección de la interfaz de red donde se ha recibido el paquete de red.

    b) La dirección de origen no pertenece a las redes asociadas con la interfaz de red donde se ha recibido el paquete de red.

    c) Cuando la dirección de origen se define como perteneciente a una red *broadcast.*

54. Para configurar reglas de rechazo por defecto para registrar la suplantación de direcciones origen es necesario seguir los pasos que se indican a continuación, teniendo en cuenta que es posible introducir los comandos en cualquier orden y confirmarlos todos a la vez:

    a) Iniciar la sesión con la cuenta raíz en el dispositivo y editar la configuración.

    b) Configurar las características de monitorización de seguridad y habilitar la opción IDS para suplantación de direcciones IP.

    **[edit]**

    **user@host# set security screen ids-option trustScreen ip spoofing**

    c) Especificar el nombre de la zona de seguridad y el objeto de la opción IDS aplicado a la zona.

    **[edit]**

    **user@host# set security zones security-zone trustZone screen trustScreen**

### 5.7.7 Configuración de opción de rechazo por defecto con opciones IP

55. Podrán configurarse reglas de rechazo por defecto con opciones IP. Las opciones IP permiten al dispositivo bloquear paquetes con opciones de ruta de origen estricta o flexible o detectar y registrar el evento en la lista de contadores para la interfaz de entrada.

56. Para ello, es necesario seguir los pasos que se indican a continuación, teniendo en cuenta que es posible introducir los comandos en cualquier orden y confirmarlos todos a la vez:

    a) Iniciar la sesión con la cuenta raíz en el dispositivo.

    b) Configurar las características monitorización para habilitar las opciones IP.

    **[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**

    c) Especificar el nombre de la zona de seguridad y el objeto de la opción IDS aplicado a la zona.

    **[edit]**

    **user@host# set security zones security-zone trustZone screen trustScreen**

### 5.7.8 Configuración de otras opciones de rechazo por defecto

57. Deberán configurarse reglas de rechazo por defecto para los siguientes casos:

    a) La dirección de origen se ha identificado como en una red *multicast*, una dirección de *loopback* o una dirección *multicast*.

    b) La dirección de origen o de destino de un paquete es una dirección de enlace-local, una dirección “reservada para uso futuro” tal y como se especifica en RFC 5735 para IPv4, una “dirección sin especificar” o una dirección “reservada para uso y definición futuros” tal y como se especifica en RFC 3513 para IPv6.

    c) Se ha recibido un paquete TCP ilegal o fuera de secuencia.

58. Para configurar reglas de rechazo por defecto es necesario seguir los pasos que se indican a continuación, teniendo en cuenta que es posible introducir los comandos en cualquier orden y confirmarlos todos a la vez:

    a) Iniciar la sesión con la cuenta raíz en el dispositivo y editar la configuración.

b) Configurar las características de monitorización de seguridad y habilitar la opción IDS para *spoofing* de direcciones IP.

**[edit]**

**user@host# set security screen ids-option trustScreen ip spoofing**

c) Configurar la función de flujo de seguridad para registrar los paquetes ilegales descartados.

**[edit]**

**user@host# set security flow log dropped-illegal-packet**

d) Especificar el nombre de la zona de seguridad y el objeto de la opción IDS aplicado a la zona.

**[edit]**

**user@host# set security zones security-zone trustZone screen trustScreen**

e) Configurar la regla de rechazo TCP obligatoria ante anomalías en las sesiones TCP.

**[edit]**

**user@host# set security flow tcp-session strict-syn-check**

### 5.7.9 Configuración del dispositivo para descartar paquetes IPv6 sin asignar

59. Deberá configurarse el dispositivo para descartar los paquetes IPv6 sin asignar. Para ello, es necesario comprobar previamente el estado de la configuración por defecto del dispositivo introduciendo el comando de configuración **show usp flow** desde el modo operativo.

60. En la salida, la opción avanzada **no_drop_unassigned_ipv6_address: disabled (default)** indica que el dispositivo descarta por defecto los paquetes IPv6 sin asignar.

61. Para que el dispositivo pueda descartar los paquetes IPv6 sin asignar, deberá utilizarse el siguiente comando:

**user@host# set security flow advanced-options no-drop-unassigned-ipv6-address**

**user@host# commit**

62. Para permitir a los usuarios volver a la configuración por defecto, deberá utilizarse el siguiente comando:

**user@host# delete security flow advanced-options no-drop-unassigned-ipv6-address**

**user@host# commit**

## 5.8 Configuración de políticas de seguridad de flujos

### 5.8.1 Definición de política de seguridad de flujos para un dispositivo con SO Junos

63. Es posible definir una política de flujo de seguridad en un dispositivo con SO Junos para inspeccionar y procesar paquetes de red. El dispositivo puede permitir, denegar y registrar operaciones que deberán asociarse a cada política. Todas estas políticas se asocian a zonas donde hay vinculadas interfaces de red diferentes.

64. Es posible definir los siguientes modos para determinar cómo una política de seguridad de flujos dirige el tráfico un dispositivo:

    a) ***Bypass***: la opción ***Permit*** dirige el tráfico que atraviesa el dispositivo a través de la inspección del cortafuegos sin pasar por la VPN.

    b) ***Discard***: la opción ***Deny*** inspecciona y descarta todos los paquetes que no coinciden con ninguna política ***Permit***.

    c) ***Protect***: el tráfico se enruta a través de un túnel IPSec basado en la combinación de tabla de rutas de rutas e inspección de políticas ***Permit***.

    d) ***Log***: esta opción registra tráfico e información de sesión para todos los modos mencionados arriba.

65. Los apartados siguientes describen cómo configurar una política de seguridad para cada uno de estos modos.

### 5.8.2 Configuración de una política de seguridad de flujos en modo *Bypass*

66. Para configurar una política de seguridad de flujos para el modo Bypass es necesario seguir los siguientes pasos:

    a) Configurar las políticas de seguridad:

    **[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 junos-ssh**

    **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**

67. Aquí, trustZone y untrustZone son zonas de seguridad pre-configuradas y trustLan y untrustLan son direcciones de red pre-configuradas. Junos-ssh es un ejemplo de una aplicación de SO Junos predefinida por defecto que se puede configurar en una política de seguridad para forzar el tráfico SSH.

### 5.8.3 Configuración de una política de seguridad en modo *Discard*

68. Para configurar una política de flujo de seguridad para el modo *Discard* es necesario seguir los siguientes pasos.

    a) Configurar las políticas de seguridad.

    **[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**

    Donde trustZone y untrustZone son zonas de seguridad pre-configuradas y trustLan y untrustLan son direcciones de red pre-configuradas. Junos-telnet es un ejemplo de una aplicación de SO Junos predefinida por defecto que se puede configurar en una política de seguridad para forzar el tráfico Telnet.

### 5.8.4 Configuración de una política de flujo de seguridad en modo *Protect*

69. Para configurar una política de flujo de seguridad para el modo protección IPSec es necesario seguir los siguientes pasos:

    a) Configurar la 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**

donde gw1 e ipsec-policy1 son políticas IKE e IPSec pre-configuradas.

b) Configurar las políticas de seguridad.

**[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**

Donde trustZone y untrustZone son zonas de seguridad pre-configuradas y trustLan y untrustLan son direcciones de red pre-configuradas.

## 5.9 Configuración de VPN

70. Todas las VPN deberán configurarse de forma que se utilicen algoritmos de cifrado con una fortaleza criptológica de 128 bits o superior, de acuerdo a lo estipulado en la guía CCN-STIC-807 para el ENS Categoría Alta.

71. Para ello, como regla general, deberán aplicarse las siguientes restricciones a las opciones de configuración que presenta el producto:

    a) Se seleccionará siempre IKEv2 en lugar de IKEv1 como protocolo de intercambio de claves.

    b) No deberán utilizarse Pre-Shared-Keys (PSK) como método de autenticación, dado que no es posible determinar *a priori* si la clave posee la fortaleza exigida para el ENS.

    c) No deberá utilizarse RSA-2048 como método de autenticación, dado que posee una fortaleza de 112 bits, por lo que incumple los requisitos mínimos establecidos para el ENS categoría Alta. Solamente se permitirá el uso del RSA-2048 cuando la VPN se establezca dentro de la red local para ofrecer un canal seguro con el administrador remoto o el servidor de autenticación.

d) No deberá seleccionarse el grupo Diffie Hellman 14 (DH group-14) para el establecimiento de secretos compartidos en la fase de intercambio de claves, dado que posee una fortaleza de 112 bits.

e) No deberá seleccionarse 3des-cbc como algoritmo de cifrado, dado que posee una fortaleza igual a 112 bits.

f) Deberá activarse la opción **perfect-forward-secrecy,** ya que, **aunque supone incrementos en coste computacional,** impide que se descifre el contenido de la comunicación aunque se comprometan las claves establecidas para las asociaciones de seguridad.

### 5.9.1 Configuración de VPN en un dispositivo con SO Junos

72. Este apartado muestra configuraciones de ejemplo de una VPN con IPSec en un dispositivo con SO Junos donde se utilizan los siguientes métodos de autenticación IKE:

    a) Configuración de una VPN con IPSec con una firma RSA para autenticación IKE.

    b) Configuración de una VPN con IPSec con una firma ECDSA para autenticación IKE.

73. La figura muestra la topología de VPN utilizada en todos los ejemplos que se describen en esta sección. Aquí H0 y H1 son los PC host, R0 y R2 son los dos extremos del túnel VPN con IPSec, y R1 es un enrutador para direccionar el tráfico entre las dos redes diferentes.

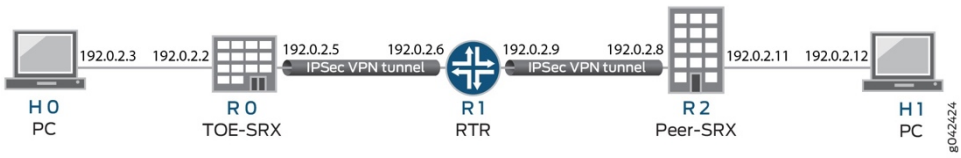


**Figura 2 Topología de VPN**

74. El dispositivo R1 puede tratarse de un enrutador basado en Linux o un dispositivo Juniper Networks o de cualquier otro fabricante.

75. La siguiente tabla muestra una lista completa de los protocolos, modos, algoritmos y fortaleza de claves recomendados para una configuración segura de VPN en este tipo de dispositivos.

| PROPUESTA EN FASE 1 (P1, IKE) | |
|---|---|
| **Protocolo IKE** | IKEv2 |
| **Método de autenticación** | ECDSA-SIGNATURES-256, ECDSA-SIGNATURES-384 |
| **Algoritmo de autenticación** | SHA-256, SHA-384 |
| **Grupo DH** | 19, 20, y 24 |
| **Algoritmo de cifrado** | AES-128-CBC, AES-128-GCM, AES-192-CBC, AES-256-CBC, AES-256-GCM |
| **PROPUESTA EN FASE 2 (P2, IPSEC)** | |
| **Protocolo IKE** | IKEv2 |
| **Algoritmo de autenticación** | HMAC-SHA1-96, HMAC-SHA-256-128 |
| **Grupo DH** | 19, 20, y 24 |
| **Método de cifrado** | ESP |
| **Algoritmo de cifrado** | AES-128-CBC, AES-128-GCM, AES-192-CBC, AES-256-CBC, AES-256-GCM |

**Tabla 5 Listado de algoritmos permitidos para una VPN**

76. Los apartados siguientes incluyen configuraciones de ejemplo de redes VPN con IPsec IKEv2 para los algoritmos seleccionados. Es posible utilizar cualquier combinación de ellos. Aunque el dispositivo también implementa el protocolo IKEv1, éste no se recomienda en una configuración segura. Por ello, deberá utilizarse el comando **set security ike gateway <nombre-gw> version v2-only**.

### 5.9.2 Configuración de una VPN con IPSec con una firma ECDSA para autenticación IKE

77. Este apartado detalla la configuración de un dispositivo para una VPN IPSec que utiliza ECDSA como método de autenticación IKE. La siguiente tabla muestra los algoritmos utilizados para la autenticación o el cifrado IKE o IPSec.

| PROPUESTA EN FASE 1 (P1, IKE) | |
|---|---|
| **Protocolo IKE** | IKEv2 |
| **Método de autenticación** | ECDSA-SIGNATURES-256 |
| **Algoritmo de autenticación** | SHA-384 |
| **Grupo DH** | 19 |
| **Algoritmo de cifrado** | AES-256-CBC |
| **PROPUESTA EN FASE 2 (P2, IPSEC)** | |
| **Protocolo IKE** | IKEv2 |
| **Grupo DH** | 19 |
| **Método de cifrado** | ESP |
| **Algoritmo de cifrado** | AES-256-GCM |

**Tabla 6 Autenticación y cifrado IKE o IPSec**

### 5.9.3 Configuración de una VPN IPsec con firma ECDSA para autenticación IKE en el iniciador

78. Para configurar una VPN con IPsec con autenticación con firma ECDSA en el iniciador deberán seguirse los siguientes pasos:

    a) Configurar la PKI. Consultar ejemplo en:

    http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/example/certificate-pki-configuring.html

    b) Generar el par de claves ECDSA. Consultar ejemplo en:

    http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/example/certificate-private-key-pair-generating-cli.html

    c) Generar y cargar el certificado CA. Consultar ejemplo en:

    http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/example/certificate-ca-local-manual-loading-cli.html

    d) Cargar la CRL. Consultar ejemplo en:

    http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/example/certificate-crl-manual-loading-cli.html

    e) Generar y cargar un certificado local. Consultar ejemplo en:

    http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/example/certificate-ca-local-manual-loading-cli.html

    f) Configurar la propuesta IKE.

**[edit security ike]**

**user@host# set proposal ike-proposal1 authentication-method ecdsa-signatures-256**

**user@host# set proposal ike-proposal1 dh-group group19**

**user@host# set proposal ike-proposal1 authentication-algorithm sha-384**

**user@host# set proposal ike-proposal1 encryption-algorithm aes-256-cbc**

Donde **ike-proposal1** es el nombre de propuesta IKE dado por el administrador autorizado.

g) Configurar la política IKE.

**[edit security IPsec]**

**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**

h) Configurar la propuesta IPSec.

**[edit security IPsec]**

**user@host# set proposal ipsec-proposal1 protocol esp**

**user@host# set proposal ipsec-proposal1 encryption-algorithm aes-256-gcm**

Donde **ipsec-proposal1** es el nombre de propuesta IPSec dado por el administrador autorizado.

i) Configurar la política IPSec.

**[edit security IPsec]**

**user@host# set policy ipsec-policy1 perfect-forward-secrecy keys group19**

**user@host# set policy ipsec-policy1 proposals ipsec-proposal1**

Donde **ipsec-policy1** es el nombre de la política IPSec e **ipsec-proposal1** es el nombre de la propuesta IPSec dado por el administrador autorizado.

j) Configurar 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**

**user@host# set gw1 version v2-o**

Donde **gw1** es el nombre de una puerta de enlace IKE, 192.0.2.8 es la IP del extremo remoto de la VPN, 192.0.2.5 es la IP del extremo local de la VPN y ge-0/0/2 es la interfaz de salida del extremo local de la VPN.

k) Configurar la 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**

**Donde vpn1 es el nombre del túnel VPN dado por el administrador autorizado.**

l) Configurar las políticas de flujo de salida

**[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 <nombre aplicación>**[1]

**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**

Donde trustZone y untrustZone son zonas de seguridad pre-configuradas y trustLan y untrustLan son direcciones de red pre-configuradas.

m) Configurar las políticas de flujo de entrada.

**[edit security policies]**

**user@host# set from-zone untrustZone to-zone trustZone policy policy1 match source-address untrustLan**

[1] Especificar las aplicaciones que se desean permitir, de acuerdo a lo establecido en el apartado 5.7.

**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**

Donde trustZone y untrustZone son zonas de seguridad pre-configuradas y trustLan y untrustLan son direcciones de red pre-configuradas

n) Confirmar la configuración.

**user@host# commit**

### 5.9.4 Configuración de una VPN IPSec con firma ECDSA como autenticación IKE en la respuesta

79. Para configurar una VPN con IPSec con autenticación con firma ECDSA en la respuesta deberán seguirse los siguientes pasos:

a) Configurar la PKI. Consultar ejemplo en:

http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/example/certificate-pki-configuring.html

b) Generar el par de claves ECDSA. Consultar ejemplo en:

http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/example/certificate-private-key-pair-generating-cli.html

c) Generar y cargar el certificado CA. Consultar ejemplo en:

http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/example/certificate-ca-local-manual-loading-cli.html

d) Cargar la CRL. Consultar ejemplo en:

http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/example/certificate-crl-manual-loading-cli.html

e) Configurar la propuesta IKE.

**[edit security ike]**

**user@host# set proposal ike-proposal1 authentication-method ecdsa-signatures-256**

**user@host# set proposal ike-proposal1 dh-group group19**

**user@host# set proposal ike-proposal1 authentication-algorithm sha-384**

**user@host# set proposal ike-proposal1 encryption-algorithm aes-256-cbc**

Donde **ike-proposal1** es el nombre de propuesta IKE dado por el administrador autorizado

f) Configurar la política IKE.

**[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**

g) Configurar la propuesta IPSec.

**[edit security ipsec]**

**user@host# set proposal ipsec-proposal1 protocol esp**

**user@host# set proposal ipsec-proposal1 encryption-algorithm aes-256-gcm**

Donde **ipsec-proposal1** es el nombre de propuesta IPSec dado por el administrador autorizado.

h) Configurar la política IPSec.

**[edit security ipsec]**

**user@host# set policy ipsec-policy1 perfect-forward-secrecy keys group19**

**user@host# set policy ipsec-policy1 proposals ipsec-proposal1**

Donde **ipsec-policy1** es el nombre de la política IPSec e **ipsec-proposal1** es el nombre de la propuesta IPSec dado por el administrador autorizado.

i) Configurar 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**

**user@host# set gw1 version v2-only**

Donde **gw1** es el nombre de una puerta de enlace IKE, 192.0.2.5 es la IP del extremo remoto de la VPN, 192.0.2.8 es la IP del extremo local de la VPN y ge-0/0/1 es una interfaz de salida del extremo local de la VPN.

j) Configurar 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**

Donde **vpn1** es el nombre del túnel VPN dado por el administrador autorizado.

k) Configurar las políticas de flujo de salida.

**[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**

Donde trustZone y untrustZone son zonas de seguridad pre-configuradas y trustLan y untrustLan son direcciones de red pre-configuradas.

l) Configurar las políticas de flujo de entrada.

**[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**

Donde trustZone y untrustZone son zonas de seguridad pre-configuradas y trustLan y untrustLan son direcciones de red pre-configuradas.

m) Confirmar la configuración.

**user@host# commit**

## 5.10 Configuración del servidor de Syslog remoto

### 5.10.1 Reenvío de registros al servidor de Syslog externo

80. Cuando el dispositivo que ejecuta el SO Junos está configurado para un servidor de Syslog externo, éste reenvía copias de registros locales al servidor de Syslog externo y conserva copias locales de todos los registros cuando se ha configurado en modo de registro de eventos. En el modo de registro de secuencias, todos los registros, salvo los de tráfico, se almacenan de manera local y se pueden reenviar a un servidor de Syslog externo, mientras que los registros de tráfico solo se pueden reenviar a un servidor de Syslog externo.

81. La conexión entre el dispositivo y el servidor de Syslog se establece por eventos, dependiendo de la configuración previa sobre el tipo de registros que se reenvían desde la ubicación local a la externa. Cuando se cumple la condición configurada, el dispositivo envía los registros locales al servidor de Syslog externo.

## 5.11 Configuración de opciones de registro de auditoría

### 5.11.1 Ejemplo de Configuración de opciones de registro de auditoría

82. Deberá configurarse el dispositivo para que realice un registro de auditoría. Para ello, es necesario seguir los siguientes pasos:

a) Especificar el número de archivos que se guardarán en el registro del sistema.

**[edit system syslog]**

**root@host#set archive files 2**

b) Especificar el archivo donde registrar los datos.

**[edit system syslog]**

**root@host#set file syslog any any**

c) Especificar el tamaño de los archivos.

[**edit system syslog**]

**root@host#set file syslog archive size 10000000**

d) Especificar la prioridad en los mensajes para el registro del sistema.

**[edit system syslog]**

**root@host#set file syslog explicit-priority**

e) Registrar los mensajes del sistema de manera estructurada.

**[edit system syslog]**

**root@host#set file syslog structured-data**

f) Especificar cómo deben procesarse y exportarse los registros de seguridad.

**[edit]**

**root@host#set security log mode stream**

### 5.11.2 Configuración de auditoria de cambios de configuración

83. Esta configuración permite auditar todos los cambios en los datos secretos de la configuración y enviar los registros a un archivo llamado Audit-File:

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

84. Este código amplía el ámbito de auditoría mínima y permite auditar todos los cambios en la configuración, no solo en los datos secretos, y envía los registros a un archivo llamado Audit-File:

```
[edit system]
syslog {
    file Audit-File {
        any any;
        authorization info;
```

```
                change-log any;
                interactive-commands info;
                kernel info;
                pfe info;
        }
}
```

85. El siguiente código realiza cambios en usuarios y en datos secretos. Después muestra la información enviada al servidor de auditoría cuando se añaden los datos secretos a la configuración original y se confirman con el comando load.

```
[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 “$ABC123”;
                        #SECRET-DATA
                }
        }
        Password{
                Format md5;
        }
}
radius-server 192.0.2.15 {
        secret “$ABC123” # SECRET-DATA
}
```

```
services {
        ssh;
}
syslog {
        user *{
                any emergency;
        }
        file messages {
                any notice;
                authorization info;
        }
        file interactive-commands {
                interactive-commands any;
        }
}
...
...
```

86. La nueva configuración cambia las instrucciones de configuración de los datos secretos y añade un nuevo usuario.

```
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**

## 5.12 Configuración de registro de eventos

### 5.12.1 El registro de eventos

87. El dispositivo deberá auditar los cambios de configuración a través del registro del sistema.
88. Además, el SO Junos tiene capacidad para realizar las siguientes acciones:
    a) Enviar respuestas automáticas para auditar eventos (creación de entradas de Syslog).
    b) Permitir a los administradores autorizados examinar registros de auditoría.
    c) Enviar archivos de auditoría a servidores externos.
    d) Permitir a los administradores autorizados devolver el sistema a un estado conocido.
89. Los eventos de configuración que deberán capturarse como mínimo serán:
    a) Cambios en datos clave secretos dentro de la configuración.
    b) Cambios confirmados.
    c) Inicio y cierre de sesión por parte de los usuarios.
    d) Inicio del sistema.
    e) Fallos al establecer una sesión de SSH.
    f) Establecimiento o finalización de una sesión de SSH.
    g) Cambios en la fecha y hora del sistema.
    h) Finalización de una sesión remota por medio del mecanismo de bloqueo de sesiones.
    i) Finalización de una sesión interactiva.
    j) Cambios en la configuración del sistema.
90. La información de auditoria estará protegida y se hará una copia de seguridad (no almacenada en el mismo sistema) que se guardará el período de tiempo especificado por la normativa de seguridad del sistema.

### 5.12.2 Configuración del registro de eventos en un archivo local

91. Es posible configurar el almacenamiento de la información de las auditorías en un archivo local con la instrucción syslog. Este ejemplo almacena los registros en un archivo llamado Audit-File:

```
[edit system]
syslog {
        file Audit-File;
}
```

## 5.13 Detección de ataques en red

92. El dispositivo deberá configurarse para que tenga la capacidad de detectar los siguientes ataques en red:

    a) **Ataque de Teardrop IP**. Los ataques de TearDrop aprovechan el reensamblaje de los paquetes IP fragmentados. Uno de los campos del encabezado IP es el campo de *offset* de fragmentos, que indica la posición de inicio o el *offset* en los datos contenidos en un paquete fragmentado en relación con los datos del paquete original no fragmentado. Cuando la suma del *offset* y el tamaño de un paquete fragmentado varía con respecto a la del siguiente paquete fragmentado, los paquetes se solapan y esto puede hacer que el servidor que intenta reensamblar el paquete se bloquee.

    b) **Ataque LAND TCP.** Los ataques LAND se producen cuando un atacante envía paquetes SYN falsificados en los que las direcciones IP origen y destino son la dirección de la víctima.

    c) **Ataque de fragmentos ICMP**. Si un paquete ICMP es de gran volumen, deberá ser fragmentado. Cuando está habilitada la opción de monitorización de protección de fragmentos ICMP, el SO Junos bloquea los paquetes ICMP que tengan definidos muchos marcadores de fragmento o que tengan un valor de *offset* indicado en el campo correspondiente.

    d) **Ataque de ping de la muerte**. El datagrama IP con el campo de protocolo del encabezado IP igual a 1 (ICMP), el bit del último fragmento es igual a 1 y (diferencia IP * 8) + (longitud de datos IP) > 65535. El *offset* IP (que representa la posición de inicio de este fragmento en el paquete original expresado en unidades de 8 bytes) más el resto del paquete es superior al tamaño máximo para un paquete IP.

    e) **Ataque TCP sin marcadores.** Los segmentos TCP que no tienen definidos marcadores de control son eventos anómalos que generan distintas respuestas del destinatario. Cuando se habilita la opción para detectar TCP sin marcadores, el dispositivo reconoce los encabezados de segmentos TCP sin marcadores definidos y elimina todos los paquetes TCP donde falten campos o que tengan marcadores formados erróneamente.

    f) **Ataque TCP SYN-FIN**. Los encabezados TCP con marcadores SYN y FIN definidos dan lugar a comportamientos TCP anómalos que generan

distintas respuestas del destinatario, dependiendo del SO. Bloquear los paquetes con marcadores SYN y FIN ayuda a prevenir sondeos del SO.

g) **Ataque TCP fin-no-ack.** Los encabezados TCP con marcadores FIN definidos pero sin marcadores ACK generan un comportamiento TCP anómalo.

h) **Ataque de bomba UDP.** Si la longitud UDP especificada es inferior a la longitud IP especificada, el paquete se considera malformado y se asocia con un ataque de denegación de servicio.

i) **Ataque DoS UDP Chargen.** Si el paquete UDP detectado posee un puerto de origen 7 y un puerto de destino 19, sería considerado como un ataque.

j) **Ataque TCP SYN y RST.** El dispositivo deberá detectar paquetes TCP que tengan definidos los marcadores SYN y RST.

k) **Ataque de desbordamiento ICMP.** Los ataques de desbordamiento ICMP generalmente se producen cuando la víctima debe procesar demasiadas solicitudes de eco ICMP, de tal forma que invierte todos sus recursos en responder hasta que ya no puede procesar el tráfico de red útil. Para evitar este tipo de ataques, el dispositivo invoca a una función de protección cada vez que un umbral establecido es sobrepasado.

l) **Ataque de desbordamiento TCP SYN.** Los ataques de desbordamiento SYN se producen cuando un host se ve tan desbordado por segmentos SYN que inician solicitudes de conexión incompletas que deja de poder procesar solicitudes de conexión legítimas.

m) **Ataque de escaneo de puerto TCP.** El escaneo del puerto se produce cuando una dirección IP de origen envía un paquete IP con segmentos TCP SYN a un número definido de puertos diferentes en la misma dirección IP de destino dentro de un intervalo concreto.

n) **Ataque de escaneo de puerto UDP.** Estos ataques escanean las direcciones IP objetivo para detectar los servicios que hay abiertos, a la escucha o respondiendo para atacar a varios protocolos o puertos en una dirección IP destino o más mediante patrones obvios (numerados secuencialmente) del protocolo o números de puerto. Los patrones se generan aleatorizando el protocolo o los números de puerto y aleatorizando los retardos entre las transmisiones.

o) **Ataque de barrido IP.** El barrido de direcciones se produce cuando una dirección IP origen envía un número definido de paquetes ICMP a diferentes hosts dentro de un intervalo de tiempo definido (el valor por defecto es 5000 microsegundos). El propósito de este ataque es enviar paquetes ICMP (generalmente solicitudes de eco) a distintos hosts con la esperanza de que al menos uno responda y así descubrir una dirección a la que atacar.

93. Esta configuración se aplicará a las zonas externas, dado que para zonas internas es importante asegurarse de que la configuración no impactará negativamente sobre ninguna herramienta de monitorización, que en muchas ocasiones utilizan técnicas similares a los escaneos para determinar si los servicios están operativos y funcionando según se espera.

94. Para llevar a cabo la configuración de estas opciones dentro del dispositivo, deberán haberse llevado a cabo con anterioridad los siguientes pasos:

    a) Configurar las interfaces y asignarles direcciones IP. Ej.:

    **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**

    b) Configurar las zonas de seguridad trustZone y untrustZone y asignarles las interfaces. Ej.:

    **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 interfaces ge-0/0/3.0**

    c) Configurar políticas de seguridad desde untrustZone a trustZone. Ver apartados 5.7 y 5.8.

### 5.13.1 Detección de ataque de Teardrop IP

95. Para habilitar la detección de un ataque de TearDrop es necesario llevar a cabo los siguientes pasos:

    a) Configurar la opción de monitorización de seguridad y asociarla a la untrustZone.

    **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**

    b) Configurar el Syslog.

    **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**

c) Confirmar la configuración.

**user@host# commit**

### 5.13.2 Detección del ataque LAND TCP

96. Para habilitar la detección de un ataque LAND TCP es necesario realizar los siguientes pasos:

a) Configurar opciones de monitorización de seguridad y vincularlas a una untrustZone.

**user@host# set security screen ids-option untrustScreen tcp land**

**user@host# set security zones security-zone untrustZone screen untrustScreen**

b) Configurar el Syslog.

**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 polici1 then log session-init**

**user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then log session-close**

c) Confirmar la configuración.

**user@host# commit**

### 5.13.3 Detección de ataque de fragmentos ICMP

97. Para habilitar la detección de un ataque IDS de fragmentos ICMP es necesario llevar a cabo los siguientes pasos:

a) Configurar opciones de monitorización de seguridad y vincularlas a una untrustZone.

**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**

b) Configurar el Syslog.

**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**

c) Confirmar la configuración.

**user@host# commit**

### 5.13.4 Detección de ataque de ping de la muerte

98. Para habilitar la detección de un ataque de ping de la muerte IDP es necesario llevar a cabo los siguientes pasos:

a) Configurar pantallas de seguridad y vincularlas a una untrustZone.

**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**

b) Configurar el Syslog.

**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**

c) Confirmar la configuración.

**user@host# commit**

### 5.13.5 Detección de ataque TCP sin marcadores

99. Para habilitar la opción de TCP sin marcadores es necesario llevar a cabo los siguientes pasos:

a) Configurar opciones de monitorización de seguridad y vincularlas a una untrustZone.

**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**

b) Configurar el Syslog.

**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**

c) Confirmar la configuración.

**user@host# commit**

### 5.13.6 Detección de ataque TCP SYN-FIN

100. Para habilitar la detección de bits TCP SYN-FIN deberán llevarse a cabo los siguientes pasos:

a) Configurar opciones de monitorización de seguridad y vincularlas a una untrustZone.

**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**

b) Configurar el Syslog.

**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**

c) Confirme la configuración.

user@host# commit

### 5.13.7 Detección de ataque TCP fin-no-ack

101. Para habilitar la detección de bits FIN sin opción IDS de bit ACK es necesario llevar a cabo los siguientes pasos:

a) Configurar las reglas de monitorización de seguridad y vincularlas a una untrustZone.

**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**

b) Configurar el Syslog.

**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**

c) Confirmar la configuración.

**user@host# commit**

### 5.13.8 Detección de ataque de bomba UDP

102. SRX elimina por defecto estos paquetes y no precisa ninguna configuración específica.

### 5.13.9 Detección de ataque DoS UDP CHARGEN

103. Para habilitar la detección de un ataque DoS UDP CHARGEN es necesario llevar a cabo los siguientes pasos:

a) Configurar las políticas de untrustZone a trustZone con la aplicación del SO Junos junos-chargen predefinida.

**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**

b) Configurar el Syslog.

**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**

c) Cambiar la configuración de la política de denegar a permitir para que el paquete llegue a su destino.

**user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then permit**

d) Confirmar la configuración.

**user@host# commit**

### 5.13.10 Detección de ataque TCP SYN y RST

104. Para la detección de ataques TCP SYN y RST, deberán llevarse a cabo los siguientes pasos:

a) Configurar las firmas de ataque personalizado IDP.

**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**

b) Configurar políticas de seguridad desde untrustZone a trustZone.

**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**

c) Configurar la opción de seguridad tcp-session en el flujo.

**user@host# set security flow tcp-session no-syn-check**

**user@host# set security flow tcp-session no-sequence-check**

d) Configurar el Syslog.

**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**

e) Para permitir que el tráfico llegue al destino, es necesario configurar la opción tcp-session.

**user@host# set security flow tcp-session relax-check**

f) Confirmar la configuración.

**user@host# commit**

### 5.13.11 Detección de ataque de desbordamiento ICMP

105. Para habilitar la detección de un ataque de desbordamiento ICMP es necesario llevar a cabo los siguientes pasos:

a) Configurar las opciones de monitorización de seguridad y vincularlas a una untrustZone.

**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**

b) Configurar el Syslog.

**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**

c) Confirmar la configuración.

**user@host# commit**

### 5.13.12 Detección de ataque de desbordamiento TCP SYN

106. Para habilitar la detección de un ataque de desbordamiento TCP SYN es necesario llevar a cabo los siguientes pasos:

a) Configurar las opciones de monitorización de seguridad y vincularlas a una untrustZone.

**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**

b) Configurar el Syslog.

**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**

c) Confirmar la configuración.

**user@host# commit**

### 5.13.13 Detección de ataque de escaneo de puerto TCP

107. Para habilitar la detección de un ataque de escaneo de puerto TCP es necesario llevar a cabo los siguientes pasos:

a) Configurar las opciones de monitorización de seguridad y vincularlas a una untrustZone.

**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**

b) Configurar el Syslog.

**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**

c) Confirmar la configuración.

**user@host# commit**

### 5.13.14 Detección de ataque de escaneo de puerto UDP

108. Para habilitar la detección de un ataque de escaneo de puerto UDP es necesario llevar a cabo los siguientes pasos:

a) Configurar opciones de monitorización de seguridad y vincularlas a una untrustZone.

**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**

b) Configurar el Syslog.

**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**

c) Confirmar la configuración.

**user@host# commit**

### 5.13.15 Detección de ataque de barrido IP

109. Para habilitar la detección de un ataque de barrido IP es necesario llevar a cabo los siguientes pasos:

a) Configurar pantallas de seguridad y vincularlas a una untrustZone.

**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**

b) Configurar el Syslog.

**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**

c) Confirmar la configuración.

**user@host# commit**

## 5.14 Configuración del paquete extendido IDP

110. Deberá habilitarse la política IPD (prevención y detección de intrusiones) del SO Junos, que permite aplicar de manera selectiva distintas técnicas de prevención y detección de ataques para el tráfico de red que pasa por el dispositivo.

111. Las políticas se componen de bases de reglas, cada una de las cuales contiene un conjunto de reglas. Primero se definen los parámetros de las reglas, como las condiciones de coincidencia del tráfico, la medida que tomar y los requisitos de registro, y después se agregan las reglas a las bases de reglas. Tras crear una política IDP agregando reglas a una o más bases de reglas, es posible seleccionar esa política para que sea la política activa en el dispositivo.

112. Para configurar el paquete ampliado IDP (IPS-EP) es necesario seguir los pasos que se indican a continuación:

a) Habilitar IPS en una política de seguridad. Esta configuración se describe en el tema sobre configuración de reglas de políticas IDP y bases de reglas IDP en la guía de funciones de prevención y detección de intrusiones para dispositivos de seguridad del SO Junos[2].

b) Configurar las reglas de la política IDP, las bases de reglas IDP y las medidas de acción para las reglas IDP. Esta configuración se describe el tema sobre configuración de reglas de políticas IDP y bases de reglas IDP en la guía de funciones de prevención y detección de intrusiones para dispositivos de seguridad del SO Junos[1].

c) Configurar las firmas personalizadas IDP. Esta configuración se describe en el tema que explica qué son los ataques basados en firmas IDP y el ejemplo sobre configuración de ataques basados en firmas IDP en la guía de funciones de prevención y detección de intrusiones para dispositivos de seguridad para el SO Junos[1].

d) Actualizar la base de datos de firmas IDP. Este proceso se describe en el tema sobre resumen de actualización de la base de datos de firmas IDP en la guía de funciones de prevención y detección de intrusiones para dispositivos de seguridad para el SO Junos[1].

## 6. FASE DE OPERACIÓN Y MANTENIMIENTO

113. Durante la fase de operación de los dispositivos, los administradores de seguridad deberán llevar a cabo las siguientes tareas de mantenimiento:

a) Comprobaciones periódicas del hardware y software para asegurar que no se ha introducido hardware o software no autorizado. El código fuente del código activo y su integridad deberá verificarse periódicamente y estará libre de software malicioso.

b) Aplicación regular de parches de seguridad y actualizaciones del firmware del sistema, de cara a mantener su configuración segura.

c) Mantenimiento de registros de auditoria incluyendo los eventos del sistema. Estos registros estarán protegidos de borrado y modificación no autorizada y solamente el personal de seguridad autorizado podrá acceder a ella. La información de auditoría se guardará en las condiciones establecidas en la normativa de seguridad.

d) Auditoría de al menos los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

e) Comprobación de que los ficheros de auditoria están protegidos del borrado y modificación no autorizada, incluso accidentales.

[2] https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/security/security-idp-policy.pdf

f) Control de acceso a la información de auditoria de forma que únicamente el personal de seguridad designado pueda acceder a ella.

g) Almacenamiento de la información de auditoria en las condiciones establecidas en la normativa de seguridad y por el período establecido.

## 7. REFERENCIAS


STIC.1 CCN-STIC-807 Criptografía de empleo en el ENS.

STIC.2 *Common Criteria Evaluated Configuration Guide for SRX Series Security Devices*

STIC.3 https://www.juniper.net/customers/csc/management

STIC.4 http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/example/certificate-pki-configuring.html

STIC.5 http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/example/certificate-private-key-pair-generating-cli.html

STIC.6 http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/example/certificate-ca-local-manual-loading-cli.html

STIC.7 http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/example/certificate-crl-manual-loading-cli.html

STIC.8 https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/security/security-idp-policy.pdf

## 8. ABREVIATURAS

| | |
|---|---|
| **AES** | *Advanced Encription Standard* |
| **BGP** | *Border Gateway Protocol* |
| **CBC** | *Cipher-Block Chaining* |
| **CCN** | *Centro Criptológico Nacional* |
| **CPSTIC** | *Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación* |
| **DH** | *Diffie-Hellman* |
| **DPP** | *Dispositivo de Protección de Perímetro* |
| **ECDSA** | *Elliptic Curve Digital Signature Algorithm* |
| **ENS** | *Esquema Nacional de Seguridad* |
| **FTP** | *File Transfer Protocol* |
| **GCM** | *Galois Counter Mode* |
| **HMAC** | *Hashed Message Authentication Code* |
| **ICMP** | *Internet Control Message Protocol* |
| **IKE** | *Internet Key Exchange* |
| **IP** | *Internet Protocol* |
| **IPS** | *Intrusion Prevention System* |
| **IPSec** | *Internet Protocol Security* |
| **LAN** | *Local Area Network* |
| **OSPF** | *Open Shortest Path First* |
| **PSK** | *Pre-Shared Keys* |
| **RSA** | *Rivest, Shamir y Adleman* |
| **SHA** | *Secure Hash Algorithm* |
| **SNMP** | *Simple Network Management Protocol* |
| **SO** | *Sistema Operativo* |
| **SSH** | *Secure Shell* |
| **SSL** | *Secure Sockets Layer* |
| **STIC** | *Seguridad de las Tecnologías de la Información y la Comunicación* |
| **VPN** | *Virtual Private Network* |