centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1442

Procedimiento de empleo seguro
Cortafuegos Juniper SRX

Agosto de 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.09.04 13:26:30 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-095-0.
Fecha de Edición: agosto de 2023

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

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

1. El presente documento pretende servir de guía para establecer una configuración segura para las plataformas cortafuegos SRX.
2. Los dispositivos SRX con Junos OS son sistemas completos de enrutamiento y cortafuegos de capa 7, que soportan variedad de interfaces de alta velocidad (hasta 100 Gbps) para redes y aplicaciones de red. Estos dispositivos están físicamente autocontenidos y albergan el *software, firmware* y *hardware* necesario para desarrollar las funciones de conmutación, enrutamiento y seguridad.
3. La familia SRX soporta numerosos estándares de enrutamiento para asegurar flexibilidad y escalabilidad, así como protocolos de seguridad en Internet como 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 accesos IPSec, SNMP v3 o el protocolo SSH.
4. Además, los dispositivos soportan funcionalidades de detección y prevención de amenazas, 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.
5. Estos dispositivos constan de tres (3) componentes arquitectónicos principales:
   - **Plano de Control o Motor de enrutamiento (RE):** ejecuta el sistema operativo Junos OS y se encarga del aprendizaje y control de capa 2 y capa 3, y administración del dispositivo para todas las operaciones necesarias desde la configuración a la operación del dispositivo y control el flujo de información que llega al equipo o lo atraviesa.
   - **Plano de reenvío de paquetes o Motor de encaminamiento de paquetes (PFE):** proporciona todas las operaciones necesarias para la conmutación y el encaminamiento de paquetes que atraviesan el equipo.
   - **Plano de servicios.** El plano de servicios se puede considerar como una extensión opcional de la PFE para realizar funciones de seguridad stateful o cualquier servicio que no sea nativo de la PFE. Proporciona todas las funcionalidades de seguridad.
6. Estos dispositivos de seguridad son capaces de realizar 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.
7. El motor de enrutamiento y el motor de reenvío de paquetes realizan sus tareas principales de forma independiente, mientras se comunican constantemente a través de un enlace interno de alta velocidad. Esta disposición proporciona un control de enrutamiento y reenvío optimizado y la capacidad de ejecutar redes a escala de Internet a altas velocidades.
8. Estos productos han sido cualificados e incluidos en el Catálogo de Producto y Servicios STIC (CPTSIC) en la familia "*Cortafuegos*".

2. OBJETO Y ALCANCE

9. En la presente guía se recoge el procedimiento de empleo seguro para los cortafuegos SRX Branch (SRX300, SRX320, SRX340, SRX345 y SRX380) con Junos OS 20.4R1 o superiores y los cortafuegos SRX Mid-Range (SRX1500, SRX4100, SRX4200 y SRX4600) con Junos OS 19.2R1 o superiores. Esta guía incluye funciones de IPS, cortafuegos y VPN.

10. En la siguiente tabla se muestran, en detalle, los chasis de las series:

Familia	Modelo	Puertos de red
Cortafuegos SRX Branch	**SRX300**	Todos los modelos de la familia con la siguiente configuración: ▪ 1GbE RJ45: 6 puertos con soporte MACSEC ▪ 1GbE SFP: 2 puertos con soporte MACSEC ▪ Fuente de alimentación en AC
	SRX320	Todos los modelos de la familia con la siguiente configuración: ▪ 1GbE RJ45: 6 puertos con soporte PoE y MACSEC ▪ 1GbE SFP: 8 puertos con soporte MACSEC ▪ 2 slots Mini-PIM (módulos interfaces WAN o WIFI) ▪ Fuente de alimentación en AC.
	SRX340	Todos los modelos de la familia con la siguiente configuración: ▪ 1GbE RJ45: 8 puertos con soporte MACSEC ▪ 1GbE SFP: 8 puertos con soporte MACSEC ▪ 4 slots Mini-PIM (módulos interfaces WAN o WIFI) ▪ Puerto de gestión fuera de banda ▪ Fuente de alimentación en AC, y DC
	SRX345	Todos los modelos de la familia con la siguiente configuración: ▪ 1GbE RJ45: 8 puertos con soporte MACSEC ▪ 1GbE SFP: 8 puertos con soporte MACSEC ▪ 4 slots Mini-PIM (módulos interfaces WAN o WIFI) ▪ Puerto de gestión fuera de banda ▪ Versiones con una o dos fuentes de alimentación en AC, y una en DC
	SRX380	Todos los modelos de la familia con la siguiente configuración: ▪ 1GbE RJ45: 16 puertos con soporte PoE y MACSEC ▪ 1/10GbE SFP/SFP+: 4 puertos ▪ 4 slot Mini-PIM (módulos interfaces WAN o WIFI) ▪ Puerto de gestión fuera de banda ▪ Versiones con una y doble fuente de alimentación en AC

Familia	Modelo	Puertos de red
	SRX1500	Todos los modelos de la familia con la siguiente configuración: ▪ 1GbE RJ45: 12 puertos. ▪ 1GbE SFP: 4 puertos. ▪ 1/10GbE SFP/SFP+: 4 puertos ▪ HA 1GbE SFP: 1 puerto dedicado para alta disponibilidad ▪ Puerto de gestión fuera de banda
Cortafuegos SRX Mid-Range	**SRX4100**	Todos los modelos de la familia con la siguiente configuración: ▪ 1/10GbE SFP+: 8 puertos ▪ HA 1/10GbE SFP/SFP+: 2 puertos dedicados para alta disponibilidad ▪ Puerto de gestión fuera de banda
	SRX4200	Todos los modelos de la familia con la siguiente configuración: ▪ 1/10GbE SFP+: 8 puertos ▪ HA 1/10GbE SFP/SFP+: 2 puertos dedicados para alta disponibilidad ▪ Puerto de gestión fuera de banda
	SRX4600	Todos los modelos de la familia con la siguiente configuración: ▪ 1/10GbE SFP+: 8 puertos ▪ 40/100GbE QSFP+/QSFP28: 4 puertos ▪ HA Control 1/10GbE SFP/SFP+: 2 puertos dedicados para alta disponibilidad ▪ HA Data 1/10GbE SFP/SFP+: 2 puertos dedicados para alta disponibilidad ▪ Puerto de gestión fuera de banda

Tabla 1 – Chasis series SRX1500, SRX4100, SRX4200 y SRX4600

11. 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

12. El presente documento se divide en cuatro partes fundamentales, de acuerdo con distintas fases que componen el ciclo de vida del producto:

    a) **Apartado 4.** En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

    b) **Apartado 5.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

    c) **Apartado 6.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

    d) **Apartado 7.** En este apartado se recogen las tareas recomendadas para la fase de operación y mantenimiento del producto.

    e) **Apartado 8.** Incluye un listado de la documentación que ha sido referenciada a lo largo del documento.

    f) **Apartado 9.** Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

13. Durante el proceso de entrega deberán llevarse a cabo una serie de tareas de comprobación para garantizar que el producto recibido no haya sido manipulado indebidamente:

    a) **Etiqueta de envío:** deberá comprobarse que la etiqueta de envío identifica correctamente el nombre del cliente, 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.

14. En caso de identificarse algún problema durante la inspección, el cliente 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.

15. 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 contacto 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://support.juniper.net/support/ para ver el estado del pedido.

4.2 ENTORNO DE INSTALACIÓN SEGURO

16. 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.
17. Para ello, la sala en la que se ubica el CPD estará dotada de un sistema de control de acceso que asegure que únicamente el personal autorizado puede acceder al dispositivo (incluido fuera del horario laboral).
18. Deberán seguirse las recomendaciones indicadas en este Procedimiento de Empleo Seguro y en la documentación de los dispositivos SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200 y SRX4600. Otros servicios deberán ser realizados únicamente por el personal autorizado.
19. Antes de instalar el dispositivo, deben revisarse las condiciones para la infraestructura necesaria, indicadas en la documentación de los dispositivos SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200 y SRX4600, y así asegurarse de que el área de despliegue cumpla con los requisitos de energía, ambientales y de espacio libre para el cortafuegos.
20. Antes de conectar el dispositivo a una fuente de alimentación, revisar las instrucciones de instalación en la documentación de los SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200 y SRX4600.
21. Si el bastidor o armario dispone de dispositivos estabilizadores se deben instalar en el bastidor antes de montar el cortafuegos.

4.3 COMPONENTES DEL DISPOSITIVO Y DEL ENTORNO DE OPERACIÓN

22. Los dispositivos **SRX300, SRX320, SRX340, SRX345 y SRX380** deben ejecutar el firmware Junos OS 20.4R1 y los **SRX1500, SRX4100, SRX4200 y SRX4600** deben ejecutar el firmware Junos OS 19.2R1.
23. Para los equipos SRX Branch (**SRX300, SRX320, SRX340, SRX345 y SRX380)**, dentro de la frontera física de los dispositivos, se observan los componentes del equipo entre los que se incluyen el motor de enrutamiento (Routing Engine) donde se ejecuta el sitema operativo del equipo, y los ASICs (hardware de propósito específico) que consisten en lo que se llama el motor de reenvío de paquetes (Packet Forwarding Engine).

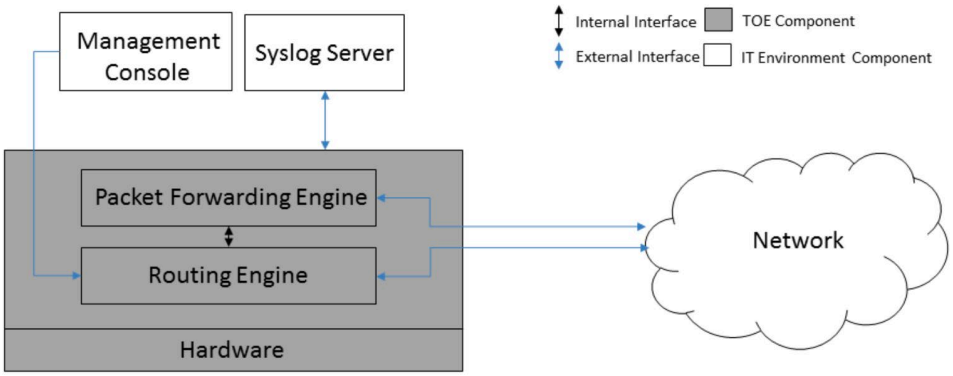

Figura 1- Arquitectura Física de dispositivos SRX300, SRX320, SRX340, SRX345 y SRX380

24. Para los equipos SRX Mid-Range (**SRX1500, SRX4100, SRX4200 y SRX4600)**, dentro de la frontera física de los dispositivos, además de la Routing Engine y la Packet Forwarding Engine, se incluye un hipervisor KVM, que proporciona la capa de virtualización en la que se ejecuta una Junos OS VM, como se muestra en la figura a continuación.

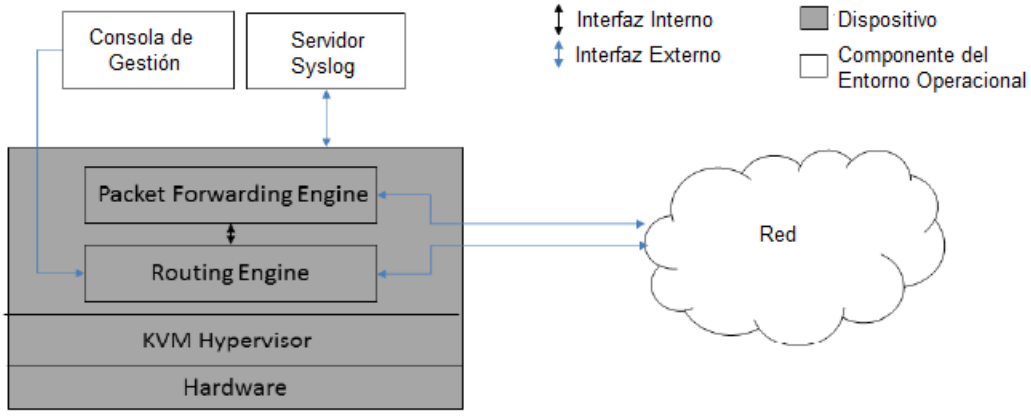

Figura 2- Arquitectura Física de dispositivos SRX1500, SRX4100, SRX4200 y SRX460

25. Los dispositivos requieren interfaces de red RJ-45, SFP/SFP + (como se detalla en la Tabla 1) para operar y comunicarse con la red conectada.

26. El entorno operativo debe proporcionar los siguientes elementos:

- Servidor syslog que admite conexiones SSHv2 para enviar registros de auditoría.
- Cliente SSHv2 para administración remota.
- Cliente de conexión en serie para administración local.

5. FASE DE INSTALACIÓN

27. Una vez instalado el cortafuegos, es necesario realizar la configuración inicial:

    a) Conecte el puerto de consola a una computadora portátil o PC utilizando un cable RJ-45 y el adaptador RJ-45 a DB-9 suministrados. El puerto de consola (CON) se encuentra en el panel de puertos del dispositivo.

    b) Inicie sesión como root. Inicialmente no se requiere contraseña. Si el software se inicia antes de conectarse al puerto de consola, se debe presionar la tecla Intro para que aparezca el mensaje:

    login: root

    c) Iniciar la interfaz de línea de comandos (CLI) y entrar al modo de configuración:

    root@% cli

    root> configure

    d) Crear una contraseña para el usuario root (ver apartado 6.2.3.3 ROOT):

    [edit]

    root@# set system root-authentication plain-text-password

    New password: password

    Retype new password: password

    e) (Opcional) Configurar el nombre del cortafuegos. Si el nombre incluye espacios, escribirlo entre comillas.

    [edit]

    root@# set system host-name nombre_del_cortafuegos

    f) Configurar el Gateway por defecto:

    [edit]

    root@# set routing-options static route default next-hop DirIPdelGateway

    g) Configurar la interfaz de gestión fuera de banda para la administración remota (dirección IP y la máscara de red):

    [edit]

    root@# set interfaces fxp0 unit 0 family inet address direcciónIP/mascara

    h) (Opcional) Configure las rutas estáticas hacia las redes remotas con acceso a la interfaz de gestión:

    [edit]

    root@# set routing-options static route DirIP_remota/máscara next-hop DirIPpasarela retain no-readvertise

    i) Habilitar el servicio SSH para poder realizar la gestión remota del dispositivo:

    [edit]

    root@# set system services ssh

j) Ejecutar el comando commit para aplicar la configuración al cortafuegos:

[edit]

root@# commit

28. Una vez finalizada la configuración inicial, es necesario **comprobar que la versión de Junos instalada es la esperada** (en este caso Junos OS 20.4R1 para SRX Branch o Junos OS 19.2R1 para SRX Mid-range). Para ello:

a) Conecte el puerto de consola a una computadora portátil o PC utilizando un cable RJ-45 y el adaptador RJ-45 a DB-9 suministrados. El puerto de consola (CON) se encuentra en el panel de puertos del dispositivo.

b) Inicie sesión como root con la contraseña añadida anteriormente. Si el software se inicia antes de conectarse al puerto de consola, se debe presionar la tecla Intro para que aparezca el mensaje:

login: root

c) Iniciar la interfaz de línea de comandos (CLI) y entrar al modo de configuración:

root@% cli

d) Ejecutar el comando para confirmar la versión de Junos OS instalada:

root@hostname> show versión

e) Localizar en la salida del comando la versión instalada:

Hostname: lab

Model: srx4100

Junos: 19.2R1.8

JUNOS OS Kernel 64-bit [20190517.f0321c3_builder_stable_11]

[…]

29. Si la versión instalada no es la adecuada (Junos OS 20.4R1 para SRX Branch o Junos OS 19.2R1 para SRX Mid-range), es necesario descargar dicha versión:

a) Acceder a la web de descargas de software de Juniper y hacer login con la cuenta que tenga asociado el número de serie del equipo que se está instalando. (https://support.juniper.net/support/downloads/)

b) En la pestaña “Downloads” buscar el producto para el que queremos descargar la versión de Junos.

c) Una vez localizado el producto, localizar la versión el tipo de OS y la versión a descargar (Junos OS 20.4R1 para SRX Branch o Junos OS 19.2R1 para SRX Mid-range).

d) Elegir la versión correspondiente y hacer click en el enlace de descarga.

e) Sebe comprobar la integridad del software descargado con los “*checksum*” SHA256 o SHA512 que aparecen en la página, estando estos asociados a la descarga seleccionada.

f) Aceptar el EULA y seleccionar la opción *proceed.*

g) Descargar la versión deseada en el equipo local y alojarla en un servidor alcanzable por el cortaguegos a instalar.

30. Con la versión de Junos alojada en el servidor, hacer la instalación desde el cortafuegos:

a) Acceder al modo de configuración del equipo.

root@hostname> configure

b) Ejecutar el comando *request system software* add *<pathname><source>* reboot para instalar (Junos OS 20.4R1 para SRX Branch o Junos OS 19.2R1 para SRX Mid-range):

root@hostname> request system software add scp://hostname/pathname/junos-srxmr-x86-64-19.2R1.8.tgz reboot

Para usar autenticación, puede usarse el comando del siguiente modo:

scp://<username>:<password>@hostname/pathname/junos-srxmr-x86-64-19.2R1.8.tgz

c) Una vez que el equipo se ha reiniciado, comprobar que la nueva versión se ha instalado correctamente.

root@hostname> show version

d) Localizar en la salida del comando la versión instalada:

Hostname: lab

Model: srx4100

Junos: 19.2R1.8

JUNOS OS Kernel 64-bit [20190517.f0321c3_builder_stable_11]

[…]

5.1 REGISTRO Y LICENCIAS

31. Para poder instalar la licencia esta deberá haberse adquirido previamente y se debe disponer de una conexión CLI con el dispositivo. Todas las licencias instaladas en el dispositivo se almacenarán en el directorio */config/license*.

32. Existen dos formas de instalar la licencia: usando sentencias del modo configuración, o a través de comandos operacionales (ver apartado 6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA para información sobre la interfaz de comandos).

- La sentencia del modo configuración *set system license keys key*, que permite añadir o borrar licencias directamente o desde un fichero de configuración.
- El comando operacional *request system license add*, que instala la licencia a través de una URL o utilizando un fichero de licencias.

33. Instalación de licencia desde el modo configuración directamente con la sentencia:

set system license keys key name.

34. El parámetro *name* incluye el ID de la licencia y la clave de licencia. Tras ejecutar la sentencia, al estar en el modo de configuración, debe ejecutar el comando `commit` para hacer efectivos los cambios.

user@device#configure

[edit]

user@device# set system license keys key "JUNOS_TEST_LIC_FEAT xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx"

user@device# commit

commit complete

35. Instalación de licencia desde el modo configuración usando un fichero de configuración con sentencias *set system license keys key file* .

36. Se creará un fichero de configuración (por ejemplo: "*license.conf*") que contenga la sentencia *set system license keys key file* (o varias, si se quieren instalar varias licencias).

user@device# cat > license.conf

37. El contenido de "license.conf" será, por ejemplo:

```
system {
   license {
      keys {
        key "JUNOS_TEST_LIC_FEAT xxxxxx xxxxxx";
      }
   }
}
```

38. En el modo configuración, cargamos y ejecutamos el fichero de configuración y hacemos efectivos los cambios:

user@device# load merge license.conf

load complete

user@device# commit

commit complete

39. Instalación de licencia desde el modo operación usando el comando operacional

request system license add filename | url.

40. Al ser un comando operacional, el cambio se aplica de forma inmediata tras ejecutar el comando. Como parámetro se le puede pasar un fichero de licencia o la URL donde se encuentre la licencia.

41. Para mostrar las licencias se utilizará el comando operacional *show system license*.

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

42. El modo de operación seguro debe ser activado para que el dispositivo funcione con la configuración acorde a unos requisitos de seguridad determinados y, por tanto, funcione de acuerdo con las garantías de seguridad requeridas.

43. 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.

44. Cuando el modo de operación seguro está habilitado, el dispositivo realiza las siguientes tareas:

    - Realiza auto chequeos de las funciones criptográficas en el arranque del dispositivo.
    - Realiza auto chequeos continuos de la generación de números aleatorios y claves.
    - No permite el establecimiento de conexiones de gestión que no estén correctamente cifradas.
    - Obliga a que las contraseñas se almacenen protegidas con algoritmos unidireccionales sólidos (funciones hash). En el apartado 6.2.2.1 AUTENTICACIÓN CON NOMBRE DE USUARIO Y CONTRASEÑA, en la configuración de la política de contraseñas se puede definir la función hash que será utilizada (se recomienda el uso de SHA521)
    - Obliga a que las contraseñas de administrador tengan 10 caracteres como mínimo.

45. Todas las funciones y algoritmos criptográficos implementados por el dispositivo se implementan a través de los módulos: OpenSSL (OpenSSH), LibMD y Kernel.

    - El módulo OpenSSL (OpenSSH) se utiliza para implementar los algoritmos y funciones criptográficas del protocolo SSHv2 que utiliza el dispositivo para la administración remota, y para la conexión con servidores syslog.
    - La generación de valores aleatorios utiliza HMAC_DRBG implementado en los módulos Kernel y OpenSSL.
    - Adicionalmente, las funciones SHA256 y SHA512 son implementadas en el módulo LibMD que es utilizado por el demonio Junos MGD para el password hashing.

46. En modo de operación seguro se deshabilitan los algoritmos criptográficos débiles, como el estándar de cifrado DES y el algoritmo hash MD5, y únicamente se permite el uso de algoritmos y funciones criptográficas seguras. En la siguiente tabla se indican los algoritmos criptográficos que se implementan en modo de operación seguro:

Módulo criptográfico	Función	Algoritmos criptográficos
OpenSSL (OpenSSH)	Cifrado / Descifrado	AES-CBC (128, 192, 256) [no recomendado] AES-CTR (128, 192, 256)
	Message Digest Generation	SHA1 [no recomendado], SHA2-256, SHA2-384, SHA2-512

Módulo criptográfico	Función	Algoritmos criptográficos
	Autenticación de mensajes	HMAC-SHA1 , HMAC-SHA2-256, HMAC-SHA2-512
	Generación de claves Generación y verificación de firma	ECDSA (P-256 / SHA-256) ECDSA (P-384 / SHA-384) ECDSA (P-521 / SHA-521) RSA (2048/3072) [RSA 2048 no recomendado] / SHA256
	Random Bit Generation	DRBG (HMAC-SHA-2-256)
LibMD	Message Digest Generation	SHA1 [no recomendado], SHA2-256, SHA2-512
	Message Authentication	HMAC-SHA1, HMAC-SHA2-256
Kernel	Message Digest Generation	SHA1 [no recomendado], SHA2-256, SHA2-384, SHA2-512
	Message Authentication	HMAC-SHA1, HMAC-SHA2-256
	Random Bit Generation	DRBG (HMAC-SHA-2-256)

Tabla 2 – Algoritmos y funciones criptográficas en modo de operación seguro

47. En el modo de operación seguro se establece una frontera alrededor de los módulos criptográficos, de forma que ningún parámetro crítico de seguridad (CSP) puede cruzar esta frontera en texto plano, sino que deberá estar cifrado con uno de los algoritmos y funciones criptográficas aprobadas en el modo de operación seguro e indicadas en la tabla anterior. Los parámetros críticos de seguridad (CSPs) que maneja el dispositivo, son los siguientes:

CSP	Descripción	Funciones y algoritmos criptográficos empleados
SSH Host Key Privada	Claves SSH utilizadas para identificar el dispositivo como servidor SSH. Se generan en la configuración inicial del equipo.	ECDSA P-256 SSH-RSA [no recomendado]
SSH Session Key	Claves de sesión SSH usadas para el cifrado, autenticación de mensajes y *Key Establisment*.	Claves de cifrado AES 128/256 [AES 128 no recomendado] Claves HMAC-SHA1, HMAC-SHA2-256 y HMAC-SHA2-512 Claves privadas DH Group 14 [no recomendado] o ECDH-P256/P-384/P-512

CSP	Descripción	Funciones y algoritmos criptográficos empleados
Contraseñas de usuarios	Contraseñas en texto plano introducidas por los usuarios para su autenticación.	Las contraseñas se almacenan cifradas con un hash (SHA-256, SHA-512)
DRBG	Estado interno y "*seed key*" del DRBG	DRBG (HMAC-SHA-2-256)

Tabla 3 – Parámetros Críticos de Seguridad (CSPs)

48. En las tablas anteriores se incluyen las indicaciones de los mecanismos criptográficos que no deben ser utilizados ([no recomendado]) dado que no presentan la fortaleza de seguridad suficiente.

49. Para obtener información adicional sobre el proceso de configuración del modo de operación seguro se puede consultar la guía Junos® OS Common Criteria Guide for SRX345 and SRX380 Devices [**REF3**] o la guía Junos® OS Common Criteria Evaluated Configuration Guide for SRX1500, SRX4100, SRX4200, and SRX4600 devices [**REF4**]. A continuación, se muestran los pasos resumidos para configurar el modo de operación seguro desde Junos OS CLI:

    a) Como usuario root, entrar al modo configuración y ejecutar la sentencia *set system fips level nivel_FIPS*, el dispositivo solo dispone del "*level 1*" lo cual activa todas las características indicadas:

    root@host>configure

    Entering configuration mode

    [edit]

    root@host# set system fips level 2

    b) Confirmar el cambio y reiniciar el dispositivo:

    root@host# commit

    configuration check succeeds

    [edit]

    'system'

    reboot is required to transition to FIPS level 2

    commit complete

    [edit]

    root@host# run request system reboot

    Reboot the system ? [yes,no] (no) yes

50. Cuando el dispositivo se reinicia tras la activación del modo seguro, se realizan los auto-chequeos de arranque (ver apartado 6.7 AUTO-CHEQUEOS). Una vez finalizan los auto chequeos, debe reiniciarse de nuevo el dispositivo para activar el RBG (HMAC-DRBG).

51. Para verificar que el dispositivo está en modo FIPS, ejecutar el comando operacional *show system*:

    [edit]

```
root@host#show system
fips {
    level 2;
}
```

6.2 ADMINISTRACIÓN DEL PRODUCTO

6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

52. La interfaz de línea de comandos (CLI) de Junos OS es la interfaz de software que se utiliza para acceder al dispositivo y configurarlo, supervisar sus operaciones y ajustar la configuración según sea necesario. Se deberá acceder a ella a través de:

    a) ***Interfaces de gestión local*:** el puerto de consola RJ-45 en el panel trasero del dispositivo está configurado como equipo terminal de datos (DTE) RS-232. Se puede utilizar la interfaz de línea de comandos (CLI) en este puerto para configurar el dispositivo desde un terminal.

    b) ***Protocolos de gestión remota*:** el dispositivo puede gestionarse en remoto mediante cualquier interfaz Ethernet. **El protocolo SSHv2 es el único protocolo de gestión remota recomendado**. Telnet y J-Web no se usarán para gestionar los dispositivos y no deberán estar habilitados.

53. 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.

54. A continuación, se explican unos conceptos necesarios para entender otros apartados de este documento. Se puede obtener más información sobre la operativa de Junos OS CLI y sus comandos, en la guía CLI User Guide **[REF2]**.

55. Junos OS CLI tiene dos (2) modos:

    a) **Modo Operacional**. En el modo operacional se utilizan comandos para monitorizar y solucionar problemas (troubleshooting) y para mostrar el estado actual del dispositivo. Comandos de ejemplo: *monitor, ping, show, test y traceroute.*

    b) **Modo Configuración**. Este modo permite configurar el dispositivo. En este modo, se ejecutarán sentencias (*configuration statements*) para configurar todas las propiedades del dispositivo, incluidos interfaces, enrutamiento, acceso de usuarios, y varias propiedades del sistema y del hardware.

56. Cuando se accede al modo configuración, en realidad se están haciendo los cambios sobre un archivo llamado *candidate configuration*. Este archivo permite realizar cambios de configuración sin provocar cambios en la configuración activa. El dispositivo no implementará los cambios añadidos al archivo *candidate configuration* hasta que se confirmen mediante un *commit*, lo que activa la nueva configuración en el dispositivo.

57. Cuando se configura, opera o monitoriza un dispositivo, es habitual estar cambiando de un modo a otro. Aunque existen varias formas para hacer esto, lo más sencillo para cambiar a modo configuración desde modo operación, es ejecutar "*configure*". Y para salir del modo de configuración al de operación, teclear "*exit*".

58. Los comandos CLI están organizados en **jerarquías**:

    a) En el modo operacional, los comandos que realizan una función similar se agrupan bajo el mismo nivel de jerarquía. Por ejemplo, todos los comandos que muestran información sobre el sistema se agrupan bajo el comando *show system*, y todos los comandos que muestran información sobre la tabla de enrutamiento se agrupan bajo el comando *show route*. Para ejecutar un comando determinado, se debe teclear el nombre completo del comando comenzando en el nivel superior de la jerarquía. Por ejemplo, para mostrar una vista breve de las rutas, se usaría el comando *show route brief*.

    b) En el modo configuración, la jerarquía de sentencias de configuración (*configuration statements*) tiene dos tipos de sentencias: sentencias contenedor (*container statements*) que contienen otras sentencias, y sentencias finales (*leaf statements*) que no contienen otras sentencias. La siguiente figura muestra un ejemplo del árbol de jerarquía. La sentencia *protocols* es una sentencia "top" que forma parte del tronco del árbol de jerarquías. Las sentencias *ospf*, *area* e *interface* son sentencias contenedoras subordinadas (son ramas del árbol de jerarquía), y la sentencia *hello-interval* es una sentencia final (una hoja en el árbol de jerarquía).

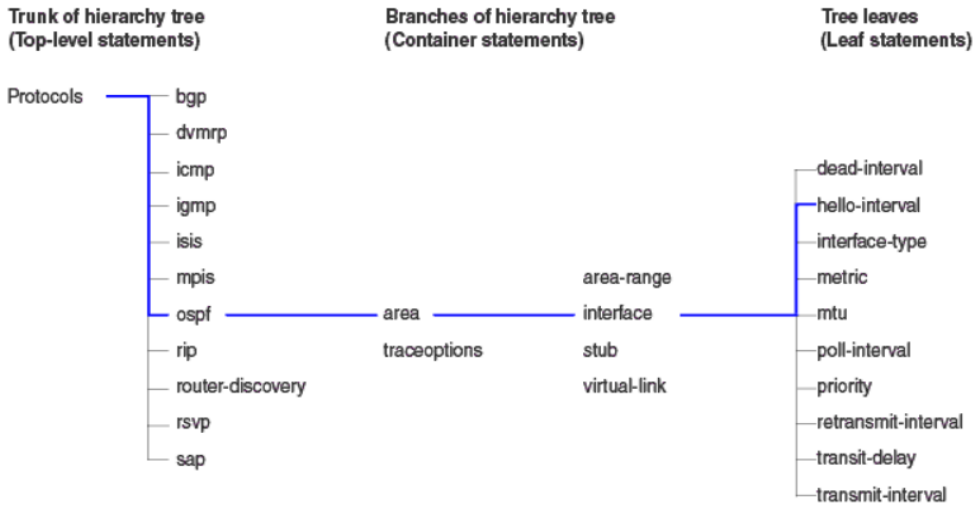

Figura 3- Ejemplo de jerarquía de sentencias de configuración

6.2.2 AUTENTICACIÓN

59. La autenticación de los usuarios puede ser de varios tipos:

    a) Autenticación con nombre de usuario y contraseña (para accesos al dispositivo a través de consola y SSH).

    b) Autenticación con nombre de usuario y clave pública (para accesos al dispositivo a través de SSH).

    c) Autenticación con RADIUS.

    d) Autenticación con TACACS+.

60. Estos dos últimos servidores de autenticación se configuran según está detallado en el apartado 6.3 AUTENTICACIÓN CON SERVIDORES EXTERNOS

61. Se recomienda hacer uso de la autenticación local mediante nombre de usuario/contraseña o claves públicas.

6.2.2.1 AUTENTICACIÓN CON NOMBRE DE USUARIO Y CONTRASEÑA

62. Cuando se crea una cuenta de usuario, uno de los parámetros que se indican es el método de autenticación (authentication). En caso de utilizar contraseña, esta podrá especificarse:

    a) En texto plano (*plain-text password*). Esta contraseña será protegida en el almacenamiento por Junos OS mediante el cifrado con funciones hash. El algoritmo usado por defecto en los dispositivos SRX es SHA512, con software Junos-FIPS, y no se recomienda modificarlo. Se recomienda hacer uso de esta modalidad, ya que permite la definición de una política de contraseñas para asegurar el uso de contraseñas seguras.

- En caso de especificar este método de autenticación, el dispositivo solicitará la introducción y confirmación de la contraseña:

  [edit system login user username]

  user@host# set authentication plain-text-password

  New password: type password here

  Retype new password: retype password here

    b) Cifrada (*encrypted-password*). Se introduce directamente la contraseña cifrada, y es lo que directamente almacena Junos OS. El algoritmo de cifrado por defecto es la función hash SHA 512, y sha1 con software Junos-FIPS, en los dispositivos SRX.

  [edit system login user username]

  user@host# set authentication encrypted-password "$ABC123"

63. En la autenticación por contraseña, el dispositivo fuerza un mecanismo de acceso con retardo. Para ello se deben configurar una serie de parámetros, como el número máximo de intentos fallidos de autenticación y tiempos de retardo (ver apartado 6.2.4 PARÁMETROS DE SESIÓN (*LOGIN SETTINGS*)). Si, por ejemplo, los primeros dos intentos de introducir la contraseña correcta fallan, no se aplica ningún retardo. Cuando el usuario introduce la contraseña por tercera vez, el dispositivo fuerza un retardo de 5 segundos. A cada intento fallido desde entonces, se suman 5 segundo más de retardo respecto al intento fallido anterior.

64. **Política de contraseñas**: el método de autenticación de contraseña en texto plano, permite definir una política de contraseñas a través de la sentencia de configuración *password* en el nivel de jerarquía *[edit system login]:*

```
[edit system login]
password {
    change-type (set-transitions | character-set);
    format (sha1 | sha256 | sha512);
    maximum-length length;
    maximum-lifetime days
    minimum-changes number;
```

minimum-character-changes number

minimum-length length;

minimum-lifetime days

minimum-lower-cases number;

minimum-numerics number;

minimum-reuse number

minimum-punctuations number;

minimum-upper-cases number;

}

- *change-type*: establece los requisitos para utilizar conjuntos de caracteres en la contraseña.

- *character-sets*: la contraseña puede usar sets de caracteres. Los 5 sets de caracteres admitidos en Junos OS son: mayúsculas, minúsculas, números, ¡signos de puntuación y caracteres especiales (! @ # $ % ^ & * , +< > : ;). **Se recomienda configurar el uso de, al menos, 4 conjuntos de caracteres.**
- *set-transitions*: número de transiciones entre los conjuntos de caracteres. Este parámetro se usa en combinación con *minimum-changes*. Si *change-type* es character-sets, entonces el número de sets de caracteres incluidos en la contraseña, se chequea contra el número especificado en *minimum-changes*. Si *change-type* es *set-transitions*, entonces el número de cambios en los sets de caracteres incluidos en la contraseña, se cheque contra el número especificado en *minimum-changes*.
- *minimum-character-changes*: mínimo número de caracteres que deben cambiar entre una contraseña y la anterior.
- *format (sha1 | sha256 | sha512):* Función hash con la que Junos OS cifrará la contraseña. En los dispositivos SRX es SHA512 por defecto (las contraseñas empiezan por 6). *Se recomienda usar SHA512.*
- *maximum-length / mínimum-length*: longitudes máxima y mínima de la contraseña. **Se recomiendan 12 caracteres mínimo**.
- *maximum-lifetime days*: máxima duración de la contraseña en días. **Se recomienda configurar un tiempo máximo de 60 días o menos.**
- *minimum-lifetime days*: mínimo número de días que debe durar la contraseña antes de poder cambiarla. **Se recomienda configurar no menos de 4 días.**
- *minimum-lower-cases / minimum-numerics / minimum-punctuations / minimum-upper-cases*: mínimo número de caracteres de cada tipo, que debe contener la contraseña. **Se recomienda que, al menos, contenga 1 carácter de cada tipo.**
- *minimum-reuse*: mínimo número de contraseñas antiguas que no deben coincidir con la nueva contraseña. **Se recomienda configurar, al menos, 5.**

65. A la hora de crear las contraseñas, deberán observarse y tenerse en cuenta las recomendaciones expuestas en la guía CCN-STIC 821, Apéndice V: Normas de Creación y Uso de Contraseñas NP40 [**REF5**].

6.2.2.2 AUTENTICACIÓN CON CLAVE PÚBLICA SSH

66. Con la autenticación mediante clave pública SSH, el usuario introduce el nombre de usuario y demuestra que posee la clave privada que corresponde a la clave pública que el dispositivo tiene almacenada para ese usuario.

67. Las claves SSH podrán ser ECDSA P-256 o RSA. La configuración de SSH y de las claves de autenticación, se puede consultar en el apartado 6.2.5 CONFIGURACIÓN DE SSH.

6.2.3 CONFIGURACIÓN DE USUARIOS

6.2.3.1 LOGIN CLASSES Y PERMISOS

68. En este apartado se indican los conceptos clave que utiliza Junos OS en relación con las cuentas de usuario y la autenticación, y se describen los pasos básicos para la creación de usuarios y cuentas. No obstante, se puede obtener más información al respecto en *Junos OS User Access and Authentication Administration Guide* **[REF1].**

69. Junos OS asocia los usuarios a **login classes** las cuales tendrán asignados ciertos privilegios de acceso. En función de ellos, se determinará qué comandos CLI se pueden ejecutar y qué configuración se puede ver y/o modificar.

70. A cada cuenta de usuario individual se le asocia una login class, determinando con ello los permisos y privilegios del usuario. Cada login class, además, lleva configurado un tiempo máximo de inactividad de sesión (*idle timeout*).

71. Los permisos y privilegios se asignan utilizando lo que se llaman *Permission Bits*, que dan acceso a lectura y/o escritura de las funcionalidades del dispositivo. Los hay de dos tipos:

    a) Los que llevan la coletilla "-control", que proporcionan lectura y escritura de la funcionalidad.

    b) Los que no llevan la coletilla "-control", que solo proporcionan capacidad de lectura sobre la funcionalidad. Por ejemplo:

        - ***access*:** permite visualizar la configuración de acceso en el modo configuración, usando el comando del modo operacional *show configuration.*
        - ***access-control*:** permite visualizar y configurar la información de acceso (en el nivel de jerarquía del modo configuración *[edit access]).*

    c) En la Tabla 2 (página 4) del documento [**REF1**] se pueden consultar todos los *Permission Bits* existentes. Cabe destacar los siguientes:

        - ***Admin:*** puede ver la información de cuentas de usuario en el modo configuración, y con el comando *show configuration*.
        - ***Admin-control*:** puede ver las cuentas de usuario y configurarlas (en el nivel de jerarquía *[edit system login]).*
        - ***All**:* todos los permisos.
        - ***Clear*:** puede borrar información aprendida de la red, que se almacena en varias bases de datos de la red (utilizando los comandos *clear*).
        - ***Network:*** puede acceder a la red con comandos ping, ssh, telnet y traceroute.

- ***Reset*:** puede reiniciar los procesos software utilizando el comando restart, y puede configurar si los procesos software están o no habilitados (en el nivel de jerarquía *[edit system processes]).*
- ***Trace*:** puede ver la configuración de los "traces files" en los modos de configuración y operacional.
- ***Secret:*** puede ver contraseñas y otras claves de autenticación en la configuración.
- ***Secret-control*:** puede ver contraseñas y otras claves de autenticación, y las puede modificar en el modo configuración.
- ***View*:** puede usar varios comandos para visualizar parámetros del sistema, tabla de enrutamiento, valores de protocolos y estadísticas.
- ***Security*:** puede ver la configuración de seguridad en el modo configuración y usando el comando show configuration del modo operacional.
- ***Security-control*:** puede ver y configurar la información de seguridad (en el nivel de jerarquía *[edit security]).*

72. Todos los usuarios que accedan al cortafuegos, deben encontrarse en una *login c*lass. Existen cuatro (4) *login classes* predefinidas y que no pueden ser modificadas:

Login Class	*Permission bits*
Operator	*Clear, network, reset, trace, and view*
Read-only	*View*
Super-user	*All*
Unauthorized	*None*

Tabla 4 – Login classes predefinidas en Junos OS

73. Se pueden crear nuevas *login classes* personalizadas para realizar diferentes combinaciones de permisos. A continuación, se muestra un ejemplo en el que se crean 3 *login classes*: la primera se llama *observation*, y solo permite ver estadísticas y configuración, no permite modificar ninguna configuración. La segunda clase se llama *operation* y permite ver y modificar la configuración. La tercera se llama *engineering* y permite ilimitado acceso y control. Las tres clases utilizan el mismo tiempo máximo de inactividad de sesión (*idle timeout*) de 5 minutos. Para definir una *login class*, se incluirá la sentencia de configuración *class*, en el nivel de jerarquía *[edit system login]:*

```
[edit system login]
    class observation {
        idle-timeout 5;
        permissions [ view ];
    }
    class operation {
        idle-timeout 5;
        permissions [ admin clear configure interface interface-control network
        reset routing routing-control snmp snmp-control trace-control
        firewall-control rollback ];
    }
    class engineering {
        idle-timeout 5;
        permissions all;
    }
```

Figura 4. Configuración de "*edit system login*"

6.2.3.2 CREACIÓN DE CUENTAS DE USUARIO

74. Las cuentas de usuarios se configuran para permitir a los usuarios acceder al dispositivo. Para cada cuenta se define el nombre de usuario (*login name*), la contraseña y, de forma opcional, otros parámetros y metadatos del usuario. Una vez creada la cuenta, se crea automáticamente el directorio home del usuario.

75. Para cada cuenta de usuario, se pueden definir los siguientes parámetros:

    - ***Username*** (requerido): nombre que identifica al usuario. Debe ser único en el dispositivo. No debe incluir espacios, dos puntos, ni comas. Tiene un tamaño máximo de 64 caracteres.
    - ***User's full name*** (opcional): nombre completo del usuario. Si incluye espacios, debe ir entre comillas. No incluir dos puntos ni comas.
    - ***User identifier*** (UID) (opcional): identificador numérico que se asocia a la cuenta de usuario. No se recomienda configurar un UID manual, ya que el software automáticamente le asignará uno. Si se configura manualmente debe ser único en el dispositivo y en un rago entre 100 y 64000.
    - ***User's access privilege*** (requerido): login class asignada al usuario.
    - **Authentication** (requerido): método de autenticación (plain-text password, encrypted-password, SSH key) y contraseña (si procede) que el usuario utilizará para el acceso.

6.2.3.3 ROOT

76. Cuando se instala Junos OS en el dispositivo, y este está encendido, ya está listo para configurarse. Al principio, se iniciará sesión como usuario root sin contraseña.

77. Posteriormente a esta conexión inicial, el administrador debe configurar la contraseña de root. Para ello, debe seleccionar un método de autenticación de los anteriormente indicados. Esto

se hace con la sentencia de configuración *root-authentication* en el nivel de jerarquía *[edit system]:*

```
[edit system]
root-authentication {
   encrypted-password "password"| plain-text-password;
   load-key-file URL filename;
   ssh-ecdsa “public-key” <from hostname>;
   ssh-rsa “public-key” <from hostname>;
}
```

78. Para habilitar el acceso de root a través de SSH, se debe configurar a través de la sentencia del modo configuración:

```
set system services ssh root-login allow
```

79. El producto dispone de distintas acciones a nivel de *Shell* que solo se pueden llevar a cabo con el nivel de acceso *root*. Por tanto, la cuenta root no debe utilizarse durante el funcionamiento normal, deberá estar restringida a la instalación inicial y a la configuración del dispositivo

6.2.3.4 ADMINISTRADOR DE SEGURIDAD

80. Como se ha comentado anteriormente, la cuenta root debe utilizarse únicamente en la instalación y configuración inicial del equipo. Para la operativa normal, se recomienda la creación de un **Administrador de Seguridad** con los permisos para poder llevar a cabo, al menos, las siguientes tareas:

- Administración local (vía consola) y remota (vía SSHv2) del dispositivo.
- Consultar la versión actual del firmware e iniciar actualizaciones manuales del mismo (verificando que la firma digital del paquete es correcta).
- Configurar la auditoría: tanto el envío de registros a un servidor syslog externo, como los parámetros del almacenamiento local de los registros. Únicamente el administrador de seguridad podrá leer o borrar el fichero de auditoría activo o los archivados.
- Crear, modificar o borrar cuentas de otros administradores y usuarios, incluyendo los parámetros relacionados con los intentos fallidos de autenticación (retry-options, ver apartado 6.2.4 PARÁMETROS DE SESIÓN (*LOGIN SETTINGS*), el reseteo de sus contraseñas o el desbloqueo de cuentas.
- Generar las claves de autenticación SSH.
- Configurar parámetros de sesión, como el banner de acceso o los tiempos máximos de inactividad.
- Importar certificados al almacén seguro del dispositivo.
- Configurar el servidor SSH del dispositivo, incluidas las funciones criptográficas.
- Configurar la fecha y hora del dispositivo.

81. Para crear el Administrador de Seguridad:

a) Crear una *login class* llamada "*security-admin*" y asignarle el *Permissions Bit* "All":

[edit]

user@host# set system login security-admin permissions all

user@host# commit

b) Crear el Adminitrador de Seguridad utilizando la sentencia de configuración *edit system login user*, asignándoles la *login class*, los datos del usuario y el método de autenticación.

[edit]

*user@host# set system login user Admin_Seguridad class security-admin authentication encrypted-password "*****"*

user@host# commit

6.2.4 PARÁMETROS DE SESIÓN (*LOGIN SETTINGS*)

82. Los parámetros de intento de sesión que deben conigurarse en estos dispositivos son los siguientes:

a) **Intentos fallidos de autenticación (*retry-options*)**: los parámetros relacionados con el comportamiento del dispositivo frente a los intentos fallidos de autenticación de usuarios se configuran con la sentencia de configuración *retry-options* en el nivel de jerarquía *[edit system login]:*

[edit]

user@host# set system login retry-options

tries-before-disconnect number;

backoff-threshold number;

backoff-factor seconds;

maximum-time seconds

minimum-time seconds;

con los siguientes campos:

- *tries-before-disconnect*: umbral de intentos fallidos de autenticación superado el cual, la conexión se cierra. **Se recomienda establecer un valor de tres (3) intentos fallidos**.
- *backoff-threshold*: umbral de intentos fallidos de autenticación superado el cual, se inicia un retardo antes de que el usuario pueda introducir de nuevo la contraseña. Se permiten valores de 1 a 3, siendo el valor por defecto 2. El retardo se especifica en el parámetro *backoff-factor*, que permite valores de 5 a 10 segundos, siendo 5 el valor por defecto. Con cada intento, el retardo aumenta en el valor configurado. Por ejemplo, si se configura *backoff-factor* a 5 segundos, cuando se superan los intentos fallidos el retardo es de 5 segundos. Si se vuelve a introducir la contraseña incorrecta, el retardo es de 10 segundos, si la introduce de nuevo incorrecta, el retardo es de 15 segundos, etc.

- *maximum-time(seconds):* tiempo máximo que la conexión permanece abierta a la espera de que el usuario introduzca las credenciales de usuario y contraseña. El rango es de 20 a 300 segundos y por defecto está configurado a 120 segundos.
- *minimum-time (seconds):* tiempo mínimo que la conexión permanece abierta mientras el usuario intenta introducir la contraseña. El rango es de 20 a 60 segundos y por defecto está configurado a 20 segundos.

  Se recomienda limitar el número de intentos fallidos de autenticación, para evitar los ataques de fuerza bruta.

  Una vez el usuario ha superado el número máximo de intentos fallidos de autenticación, y comienza el retardo, el administrador puede manualmente desbloquear al usuario y sacarlo de este estado. Para ello se utiliza el comando *clear system login lockout username*.

  El administrador puede también ver qué usuarios se encuentran bloqueados y en periodo de retardo, con el comando *show system login lockout*. Si es el administrador el que se encuentra bloqueado, para salir de este estado deberá conectarse al puerto consola, que ignora los parámetros de bloqueo.

b) **Login Banner**: Junos OS permite configurar banners que se muestran a los usuarios autorizados cuando inician sesión. Hay dos tipos:

c) Mensaje de inicio de sesión (*login message*) que aparece antes de que el usuario inicie sesión.

d) Mensaje de anuncio de inicio de sesión (*login announcement*) que aparece después de que el usuario inicie sesión.

Ambos mensajes se configuran con sentencias de configuración:

[edit]

user@host# set system login message login-message-banner-text

[edit]

user@host# set system login announcement system-announcement-text

Si el texto del mensaje contiene algún espacio, deberá encerrarse entre comillas. Se puede dar formato al mensaje con los siguientes caracteres especiales: *\n Nueva línea, \t Tabulador horizontal, \' Comilla simple, \" Comilla doble, \\ Backslash.*

Dichos *banners* deben configurarse de forma que avisen al usuario de la sensibilidad de la información manejada en los equipos, pero no deben dar detalles que puedan facilitar un posible ataque

e) **Restricción de acceso por fechas y horas.** Se puede restringir el acceso de un usuario a ciertos días a ciertas horas, a través de la login class que tenga asignada. Son las propiedades: `allowed-days, access-start, access-end`. Como ejemplo, se define la login class *operador-turnos* con restricción de acceso solo lunes, miércoles y viernes de 8.30 a 15.30h.

[edit system]

login {

class operador-turnos {

allowed-days [monday wednesday friday];

access-start 0830;

access-end 1530;

}

}

Se deben crear y asignar las *login class* para que el acceso de los usuarios esté limitado a su jornada laboral. Cualquier acceso fuera de dicho horario deberá estar restringido y aprobado de forma excepcional, en caso de ser necesario.

f) **Tiempo máximo de inactividad de sesión (*idle timeout*):** como se ha comentado en el apartado 6.2.3.1 LOGIN CLASSES Y PERMISOS, cada *login class* lleva asociado el tiempo máximo de inactividad de sesión, a través del parámetro *idle-timeout*. Ese parámetro define el tiempo máximo en minutos, que podrá permanecer inactiva la sesión de un usuario. Inactiva quiere decir, sin recibir entrada de teclado. Transcurrido ese tiempo, la sesión se desconecta de forma automática. Se recomienda establecer un tiempo de inactividad de cinco (5) minutos antes de que la sesión cierre automáticamente.

[edit system login class class-name*]*

idle-timeout minutes*;*

5 minutos antes de que cumpla el tiempo de inactividad, se irán mostrando mensajes al usuario en la CLI:

user@host# Session will be closed in 5 minutes if there is no activity.

Warning: session will be closed in 1 minute if there is no activity

Warning: session will be closed in 10 seconds if there is no activity

Idle timeout exceeded: closing session

El idle-timeout no puede configurar para las login class predefinidas (operator, read-only, super-user).

Los usuarios pueden finalizar sus sesiones (locales y remotas). Un usuario puede cerrar una sesión existente escribiendo *logout*, y Junos OS hará que el contenido actual de la sesión sea ilegible después de que el usuario inicie la terminación de sesión. No podrá tener lugar ninguna actividad del usuario hasta que se vuelva a identificar y se autentique.

6.2.5 CONFIGURACIÓN DE SSH

83. El dispositivo utiliza el protocolo SSHv2 para la administración remota, y para la conexión con servidores remotos de auditoría (syslog). En ambos casos, el dispositivo actúa como Servidor SSH, utilizando las funciones y algoritmos criptográficos implementados por módulo criptográfico OpenSSL (OpenSSH).
84. La siguiente tabla indica las funciones y algoritmos que pueden configurarse para SSHv2, cuando el producto opera en modo de operación seguro.

Establecimiento de claves (Key Exchange)	Autenticación (Authentication)	Cifrado (Cipher)	Autenticación de Mensajes (Message Auth)
ECDH-sha2-nistp256 ECDH-sha2-nistp384 ECDH-sha2-nistp521	ECDSA P-256 RSA [no recomendado]	AES CTR 128 AES CTR 256 AES CBC 128 [no recomendado] AES CBC 256 [no ecomendado]	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512

85. La configuración de SSH debe hacerse con el usuario *root*, en el modo configuración, y con el comando *set system services ssh*. Los pasos son los siguientes:

- Especificar los algoritmos para autenticación SSH. Los algoritmos de clave pública compatible son: ECDSA y RSA. Se recomienda seleccionar ECDSA. En caso de seleccionar RSA, la SSH Host Key generada deberá ser de, al menos, 3072 bits.

  [edit]

  root@host# set system services ssh hostkey-algorithm ssh-ecdsa

- Especificar los métodos de Key Exchange. Los métodos de Key Exchange compatibles son ECDH sobre las curvas nistp256, nistp384, nistp512 y SHA2. Se recomienda seleccionar ECDH:

  [edit]

  root@host# set system services ssh key-exchange ecdh-sha2-nistp256

  root@host# set system services ssh key-exchange ecdh-sha2-nistp384

  root@host# set system services ssh key-exchange ecdh-sha2-nistp521

- Especificar los algoritmos de autenticación de mensajes. Los algoritmos compatibles son: HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-512. **Se recomienda seleccionar SHA2-256 o SHA2-512:**

  [edit]

  root@host# set system services ssh macs hmac-sha2-256

  root@host# set system services ssh macs hmac-sha2-512

- Especificar los algoritmos de cifrado. Los algoritmos compatibles son AES en modos CBC y CTR y claves de 128, 256 bits. **Se recomienda CTR**.

  [edit]

  root@host# set system services ssh ciphers aes128-ctr

  root@host# set system services ssh ciphers aes256-ctr

86. Una vez finalizada la configuración, es posible crear una SSH Host Key:

a) Acceder a la Shell del equipo como usuario root.

root@host# start shell user root

Password:

root@host%

b) Regenerar las Host Keys.

root@host% ssh-keygen -t ecdsa -b 384 -f /etc/ssh/ssh_host_dsa_key

root@host% ssh-keygen -t rsa -b 3072 -f /etc/ssh/ssh_host_rsa_key

87. Estos comandos pueden solicitar una clave, pero se dejará en blanco ya que no se usa para conexiones salientes. Es posible que aparezca un mensaje indicando que la clave ya existe, en este caso hay que sobrescribirla.

6.3 AUTENTICACIÓN CON SERVIDORES EXTERNOS

88. Para usar la autenticación RADIUS en el dispositivo, es necesario configurar la información sobre uno o más servidores RADIUS en la red. El dispositivo consulta los servidores RADIUS en el orden en que están configurados. Si el servidor primario (el primero configurado) no está disponible, el dispositivo intenta contactar a cada servidor en la lista hasta que recibe una respuesta. El detalle de configuración de RADIUS se puede consultar en la guía *Junos OS User Access and Authentication Administration Guide* [**REF1**], en el apartado *RADIUS Authentication*

89. Para configurar un servidor RADIUS:

90. Para configurar un servidor RADIUS:

- Configurar la dirección IP del servidor RADIUS de autenticación.

  [edit access radius-server]

  user@host# set server-address

- (Opcional) Configurar la IP de origen de las peticiones que se envían al servidor RADIUS.

  [edit access radius-server server-address]

  user@host# set source-address source-address

- Configure la contraseña secreta compartida que utiliza el dispositivo de red para autenticarse con el servidor RADIUS.

  [edit access radius-server server-address]

  user@host# set secret password

  - La contraseña configurada debe coincidir con la contraseña configurada en el servidor RADIUS. Si la contraseña contiene espacios, debe escribirse entre comillas.

- (Opcional) Especificar el puerto por el que se contactará con el servidor RADIUS si es diferente del puerto por defecto (1812)

  [edit access radius-server server-address]

  user@host# set port port-number

- (Opcional) Configurar la cantidad de veces que el dispositivo intenta comunicarse con el servidor RADIUS y la cantidad de tiempo que el dispositivo espera para recibir una respuesta del servidor.

  [edit access radius-server server-address]

  user@host# set retry number

  user@host# set timeout seconds

- Especificar el orden de la autenticación incluyendo la opción de RADIUS.

  [edit system]

  user@host# set authentication-order [authentication-methods]

- Asignar una clase de inicio de sesión a los usuarios autenticados por RADIUS que no tengan una cuenta de usuario definida localmente.

  [edit system login]

  user@host# set user remote class class

91. De forma predeterminada, Junos OS encamina los paquetes de autenticación, autorización y contabilidad para RADIUS a través de la instancia de enrutamiento predeterminada. También puede encaminar paquetes RADIUS a través de una interfaz de administración en una instancia VRF no predeterminada.

92. Para encaminar paquetes RADIUS a través de la instancia de administración *mgmt_junos*:

- Habilitar la instancia de administración mgmt_junos.

  [edit system]

  user@host# set management-instance

- Configurar la instrucción mgmt_junos de la instancia de enrutamiento para el servidor de autenticación RADIUS y el servidor de contabilidad RADIUS, si está configurado.

  [edit system]

  user@host# set radius-server server-address routing-instance mgmt_junos

  user@host# set accounting destination radius server server-address routing-instance mgmt_junos

93. Al igual que ocurre con la autenticación RADIUS, para usar la autenticación TACACS+ en el dispositivo, es necesario configurar la información el servidor TACACS+ en la red. El detalle de configuración de configuración de TACACS+ se puede consultar en la guía Junos OS User Access and Authentication Administration Guide [**REF1**], en el apartado *TACACS+ Authentication*.

94. Para configurar un servidor TACACS+:

- Configurar el orden de autenticación eligiendo TACACS+ como primera opción.

  [edit groups global system]

  user@host# set authentication-order [authentication-methods]

- Configurar la IP y puerto del servidor TACACS+.

  [edit groups global system]

  user@host# set tacplus-server 10.1.110.150 port 49

- Configurar la clave compartida con el ACS (Access Control System):

  [edit groups global system]

  user@host# set tacplus-server 10.1.110.150 secret "secret"

- Configurar el tiempo en el que la autenticación pasará a la base de datos local si no hay respuesta del TACACS+.

[edit groups global system]

user@host# set tacplus-server 10.1.110.150 timeout 5

- Definir la Management IP de origen hacia el ACS:

  [edit groups global system]

  user@host# set tacplus-server 10.1.110.150 source-address 10.96.105.208

- Habilitar el accounting para eventos específicos:

  [edit groups global system]

  user@host #set accounting events login

  user@host #set accounting events change-log

  user@host #set accounting events interactive-commands

- Configurar la IP del servidor de accounting ACS:

  [edit groups global system]

  user@host #set accounting destination tacplus server 10.1.110.150 secret "secret"

- Configurar la IP de origen del servidor de accounting ACS hacia la IP de gestión del equipo

  [edit groups global system]

  user@host #set accounting destination tacplus server 10.1.110.150 source-address 10.96.105.208

95. Para encaminar paquetes TACACS+ a través de la instancia de administración *mgmt_junos*:

- Habilitar la instancia de administración mgmt_junos.

  [edit system]

  user@host# set management-instance

- Configurar la instrucción *mgmt_junos* de la instancia de enrutamiento para el servidor de autenticación TACACS+ y el servidor de contabilidad TACACS+, si está configurado.

  [edit system]

  user@host# set tacplus-server server-address routing-instance mgmt_junos

  user@host# set accounting destination tacplus server server-address routing-instance mgmt_junos

6.4 GESTIÓN DE CERTIFICADOS

96. Junos OS utiliza certificados X.509 v3 para verificar los paquetes de actualización de firmware.

97. Estos paquetes llevan una firma digital (tipo ECDSA P-256 con SHA256) junto con el certificado ECDSA, que debe ser validado. Junos OS valida la ruta del certificado (*certificate path*) mediante la construcción de una cadena de certificados basada en el vínculo entre el emisor (*issuer*) y el sujeto (*subject*). Si algún certificado de la cadena falla en la validación, la validación falla en su totalidad. Las cadenas de certificados se validarán hasta el último certificado (root CA).

98. El último certificado de la cadena (root CA) debe coincidir con uno de los certificados guardados en el almacenamiento de confianza (*trust store*) del dispositivo o, al menos, debe haber sido emitido (*issu ed*) por uno de ellos.

6.5 SINCRONIZACIÓN

99. Los equipos deben estar correctamente sincronizados. Para definir la fecha y hora del equipo, se debe ejecutar el siguiente comando en el modo operacional. Al ser un comando del modo operacional, no es necesario hacer el commit de la configuración

    root@host> set date YYYYMMDDhhmm.ss

100. Los equipos de la familia SRX pueden actuar como cliente de algunos servicios, como el Protocolo de tiempo de red (NTP), y se pueden configurar para obtener la hora del sistema de los servidores NTP que están conectados en la red.

101. El comando de configuración utilizado para configurar los equipos como cliente del servidor NTP externo es el siguiente:

    [edit]

    root@host# set system ntp server <ntp_server_ip>

102. **Se debe configurar autenticación en los servidores NTP mediante SHA-256** para asegurar que el peer NTP es confiable.

    [edit]

    root@host# set system ntp authentication-key 2 type sha256 value "key_value"

103. De forma predeterminada, Junos OS encamina los paquetes de NTP a través de la instancia de enrutamiento predeterminada. También puede encaminar paquetes NTP a través de una interfaz de administración en una instancia VRF no predeterminada.

104. Para encaminar paquetes NTP a través de la instancia de administración *mgmt_junos*:

- Habilitar la instancia de administración *mgmt_junos*.

    [edit system]

    user@host# set management-instance

- Configurar la instrucción *mgmt_junos* de la instancia de enrutamiento para el servidor NTP.

    [edit system]

    user@host# set ntp server <ntp_server_ip> routing-instance mgmt_junos

    user@host# set ntp source-address <ntp_server_ip> routing-instance mgmt_junos

6.6 ACTUALIZACIONES

105. El Administrador de Seguridad será capaz de verificar la versión actual del firmware del dispositivo utilizando el comando CLI: *show versión local* y, si existe una nueva versión disponible, podrá inicial la actualización manual.

106. Junos OS no proporciona actualizaciones parciales, sino versiones (*releases*) completas. No existe proceso de actualización automática, todas las actualizaciones deben llevarse a cabo de forma manual.

107. El procedimiento de actualización es el mismo que el descrito en el apartado 5 FASE DE INSTALACIÓN.

108. El paquete instalable de firmware para los cortafuegos SRX está firmado digitalmente (firma ECDSA P-256 con SHA256) y proporciona una cadena de certificados ECDSA que deben finalizar con el certificado de una CA interna. Cuando se procede a la instalación del paquete, Junos OS valida automáticamente las firmas y los certificados de la cadena usados para firmar el paquete. Si se determina que la firma o alguno de los certificados no son válidos (por ejemplo, cuando un certificado haya expirado el periodo de validez, o no se pueda verificar con la CA root almacenada en el dispositivo), el proceso de instalación falla.

109. El proceso de verificación del certificado utiliza una lista CRL (*Certificate Revocation List*) almacenada en el almacén de confianza (trust store) de la caché local del dispositivo. Durante una actualización de firmware, se carga una CRL actualizada, ya que está embebida en el binario de firmware. Si el certificado a validar no está presente en la lista de certificados revocados, la validación se realiza correctamente. Si la CRL no está disponible en la caché de Junos OS, la validación del certificado falla.

110. El Kernel de Junos OS mantiene una serie de huellas digitales (*fingerprints* SHA1) de los ficheros ejecutables y otros ficheros inmutables del sistema operativo. Estas huellas se encuentran en un fichero que se llama "*manifest file*". Este fichero, a su vez, se firma y verifica con la misma clave de firma del paquete de firmware.

111. Cuando se emite el comando para instalar una actualización, el *manifest file* de la actualización se verifica y almacena. A partir de las huellas incluidas en el *manifest file*, los archivos ejecutables y otros archivos inmutables se verifican antes de que se ejecuten. Si la verificación no es correcta, los archivos no podrán ejecutarse.

6.7 AUTO-CHEQUEOS

112. Junos OS ejecuta una serie de auto chequeos durante el arranque del dispositivo para verificar su correcta operación. Estos chequeos se llevan a cabo siempre, incluso si el dispositivo no está en modo de operación seguro habilitado. Los auto chequeos son los siguientes:

    - **Tests de arranque (*Power on tests*)**: determinan que el dispositivo de arranque (boot-device) responde, y realiza una verificación del tamaño de la memoria para confirmar la cantidad de memoria disponible.
    - **Tests de integridad de archivos (*File Integrity Tests*)**: verifican la integridad de todos los paquetes de software montados, para comprobar que los archivos del sistema no han sido alterados. Para probar la integridad del firmware, las huellas digitales (fingerprints) de los ejecutables y de otros archivos inmutables se validan con las huellas digitales contenidas en el *manifest file*.
    - **Tests de integridad criptográfica (*Crypto integrity tests*)**: verifican la integridad de los parámetros críticos de seguridad (CSPs), como las SSH Host Keys.
    - **Errores de autenticación (*Authentication errors*)**: verifica que "*veriexec*", el cual es un subsistema de integridad de archivos basado en el kernel que garantiza que solo se puedan ejecutar los binarios autorizados, está habilitado y funciona con el siguiente

comando en modo operacional, no es necesario hacer el commit de la configuración al ser un comando del modo operacional, no es necesario hacer el commit de la configuración.

root@host> request system malware-scan veriexec-check

- **Tests KAT (*Known Answer Tests*):** se realizan sobre los módulos criptográficos Kernel, LibMD y OpenSSL. Los tests KAT ejecutan cada algoritmo criptográfico con datos para los que ya se conoce la salida correcta (respuesta conocida). La salida calculada se compara con la respuesta conocida. Si no son idénticos, el test KAT falla.

113. Si los tests se completan con éxito, se actualizan los registros de auditoría con los resultados de las pruebas ejecutadas, y el dispositivo arranca correctamente.
114. Si, por el contrario, alguno de los test falla, se registra el error en los registros de auditoría y el dispositivo entra en estado de fallo y se reinicia, dejando de procesar el tráfico por los interfaces e impidiendo cualquier entrada de línea de comandos.
115. Cuando el dispositivo se reinicia, debe volver a pasar todos los auto chequeos.

6.8 AUDITORÍA

116. Para un entorno de Junos OS seguro es necesario auditar los eventos y almacenarlos en un archivo de auditoría local. Los eventos registrados se pueden enviar de manera simultánea a un servidor de syslog externo.
117. En este apartado se indica cómo configurar, en pasos generales, la función de auditoría del dispositivo. Se recomienda consultar más información en la guía *Junos OS Network Management and Monitoring Guide (Cap 11 – System Log Messages)* [**REF4**].

6.8.1 REGISTRO DE EVENTOS

118. Se recomienda configurar la auditoría en el dispositivo para que registre, al menos, los siguientes eventos:
    - Cambios de configuración sobre los datos secretos de claves.
    - Cambios confirmados (*commits*).
    - Inicio y cierre de sesiones de los usuarios.
    - Arranque del sistema.
    - Intentos fallidos se establecer una sesión SSH.
    - Establecimiento o finalización de una sesión SSH.
    - Cambios en la hora del sistema.
    - Finalización de una sesión remota por parte del mecanismo de bloqueo de sesión.
    - Finalización de una sesión interactiva.
    - Modificación o supresión de claves criptográficas.
    - Restablecimiento de contraseñas.
    - Todos los cambios de configuración.

119. Como se indica en el siguiente apartado, los eventos a registrar se especificarán mediante las sentencias *Facility* y *Severity Level* del nivel de jerarquía *[edit system syslog].*

120. La estructura de un mensaje de auditoría es la que se indica en la siguiente tabla. Para cada campo, se incluye como ejemplo su valor para el mensaje de auditoría:

Jul 24 17:43:28 host1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system radius-server 1.2.3.4 secret]

Campo	Descripción	Ejemplo
Timestamp	Fecha/Hora en la que se generó el mensaje, representada de una de las dos siguientes maneras: ▪ ***MMM-DD HH:MM:SS.MS+/-HH:MM*** corresponde al mes, día, hora, minuto, segundo y milisegundo en hora local. Las horas y los minutos que aparecen detrás del signo más (+) o del signo menos (-) representan la diferencia horaria entre la hora local y el Tiempo Universal Coordinado (UTC). ▪ ***YYYY-MM-DDTHH:MM:SS.MSZ*** corresponde al año, mes, día, hora, minuto, segundo y milisegundo en UTC.	Jul 24 17:43:28 es la marca de tiempo expresada en la hora local de Estados Unidos.
Hostname	Nombre del *host* que creó el mensaje original.	Host1
Process	Nombre del proceso de Junos OS que generó el mensaje.	mgd
ProcessID	ID del proceso (PID) UNIX Junos OS que generó el mensaje.	4163
TAG	Etiqueta del mensaje que identifica el mensaje unívocamente.	UI_CFG_AUDIT_SET_SECRET
username	Username del usuario que inició el evento.	«admin»
message-text	Descripción del evento.	set: [system radius-server 1.2.3.4 secret]

Tabla 5 – Estructura de los mensajes de auditoría

121. A continuación, se muestran algunos ejemplos de registros de auditoría:

Tipo	Mensaje de auditoría generado
Inicio y Fin de sesión SSH	*Los siguientes registros, son el resultado de un intento fallido de autenticación, seguido de un intento correcto y, finalmente, la finalización de la sesión.* *Dec 20 23:17:35 bilbo sshd[16645]: Failed password for op from 172.17.58.45 port 1673 ssh2* *Dec 20 23:17:53 bilbo sshd[16645]: Accepted password for op from 172.17.58.45 port 1673 ssh2* *Dec 20 23:17:53 bilbo mgd[16648]: UI_AUTH_EVENT: Authenticated user 'op' at permission level 'j-operator'* *Dec 20 23:17:53 bilbo mgd[16648]: UI_LOGIN_EVENT: User 'op' login, class 'j-operator' [16648]* *Dec 20 23:17:56 bilbo mgd[16648]: UI_CMDLINE_READ_LINE: User 'op', command 'quit '* *Dec 20 23:17:56 bilbo mgd[16648]: UI_LOGOUT_EVENT: User 'op' logout*
Reinicio del dispositivo y arranque de la función de auditoría	*Dec 20 23:17:35 bilbo syslogd: exiting on signal 14* *Dec 20 23:17:35 bilbo syslogd: restart* *Dec 20 23:17:35 bilbo syslogd /kernel: Dec 20 23:17:35 init: syslogd (PID 19128) exited with status=1* *Dec 20 23:17:42 bilbo /kernel:* *Dec 20 23:17:53 init: syslogd (PID 19200) started*

Tabla 6 – Ejemplo de mensajes de auditoría

6.8.2 ALMACENAMIENTO LOCAL

122. Los registros de auditoría se almacenan localmente en */var/log*. Para configurar el almacenamiento local de los registros de auditoría, se utiliza el usuario ***root***, con modo configuración y el nivel de jerarquía *[edit system syslog].*

123. A través de sentencias de configuración en este nivel de jerarquía, se especifican varios parámetros, como el nombre del archivo que almacenará los registros de auditoría (por ejemplo, *logfile*), el tamaño máximo de este archivo o el número de archivos de auditoría que se irán almacenando (10 por defecto).

124. Cuando un archivo de registro activo llamado, por ejemplo, *logfile*, alcanza el tamaño máximo configurado, la utilidad de *logging* cierra el archivo, lo comprime y lo renombra como logfile.0.gz. La utilidad de *logging* abre y escribe en un nuevo archivo activo *logfile*. Este proceso se conoce como **rotación de archivos**. Cuando el nuevo logfile alcanza el tamaño máximo configurado, logfile.0.gz es renombrado a logfile.1.gz, y logfile se cierra, comprime y renombra como logfile.0.gz. Se crearán tantos logfile.X.gz como se haya configurado (parámetro *archive file*). Cuando se alcanza este número máximo de archivos configurado, y cuando el tamaño del archivo activo (logfile) alcanza el tamaño máximo configurado, se sobrescribe el archivo almacenado más antiguo, con el archivo activo actual.

125. Otra de las sentencias de configuración a tener en cuenta dentro de la jerarquía *[edit system syslog] es log-rotate-frequency*, que configura cada cuánto tiempo la utilidad de logging comprobará el tamaño del archivo de registros (*logfile*). El intervalo puede ser de 1 a 59 minutos, siendo 15 minutos el valor por defecto.

126. Para especificar el tipo de mensajes que se deben registrar, se utilizan los parámetros *facility* y *severity level* del nivel de jerarquía *[edit system syslog],* que pueden tomar los valores indicados en las siguientes tablas:

Facility	Tipo de mensajes
kernel	Acciones realizadas o errores encontrados por el kernel de Junos OS.
user	Acciones realizadas o errores encontrados por los procesos del espacio de usuarios.
daemon	Acciones realizadas o errores encontrados por los procesos del sistema.
authorization	Intentos de autenticación y autorización.
ftp	Acciones realizadas o errores encontrados por los procesos FTP.
ntp	Acciones realizadas o errores encontrados por los procesos NTP.
security	Eventos o errores relacionados con la seguridad.
dfc	Eventos relacionados con la captura dinámica de flujo.
external	Acciones realizadas o errores encontrados por las aplicaciones locales externas.
firewall	Acciones de filtrado de paquetes realizadas por el filtro del firewall.
pfe	Acciones realizadas o errores encontrados por el motor de reenvío de paquetes (Packet Forwarding Engine).
conflict-log	Cuando la configuración especificada no es válida para el tipo de dispositivo.
change-log	Cambios de la configuración de Junos OS.
interactive-commands	Comandos emitidos por CLI de Junos OS o por una aplicación cliente, como un protocolo XML de Junos o un cliente XML NETCONF.
any	Todas las *facilities*.

Tabla 7 – Valores para *Faciliy*

Severity Level	Tipo de mensajes
none	Deshabilita el logging de todos los mensajes de la facility seleccionada.
emergency	Panic del sistema o cualquier otra condición que cause que el dispositivo deje de funcionar.
alert	Condiciones que requieren corrección inmediata, como una base de datos del sistema dañada.
critical	Condiciones críticas, como errores hardware.
error	Condiciones de error que generalmente tienen consecuencias menos graves que los errores en los niveles de emergencia, alerta y crítico.
warning	Condiciones que requieren monitorización.
notice	Condiciones que no suponen un error, pero podrían necesitar un manejo especial.
info	Eventos o condiciones de interés, que no suponen un error.
any	Incluye todos los niveles de severidad.

Tabla 8 – Valores para *Severity Level*

127. A continuación, se incluye un ejemplo de cómo configurar la auditoría:

    - Especificar el número de archivos que almacenarán los eventos de auditoría:

      [edit system syslog]

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

    - Especificar el nombre del archivo de registros de auditoría y el tipo de eventos a registrar (todos):

      [edit system syslog]

      root@host#set file logfile any any

    - Especificar el tamaño del archivo de registros de auditoría:

      [edit system syslog]

      root@host#set file logfile archive size 1m

    - Especificar que se registre la prioridad (Facility y Severity Level) en los mensajes.

      [edit system syslog]

      root@host#set file logfile explicit-priority

    - Es recomendable registrar los mensajes del sistema de manera estructurada (formato de protocolo syslog especificado en la RFC 5424) en lugar de formato Junos OS. En este formato, la prioridad del mensaje se registra por defecto y el paso anterior no sería necesario.

      [edit system syslog]

      root@host#set file logfile structured-data

128. Deberá limitarse la capacidad de leer y borrar tanto el fichero activo, como los ficheros almacenados de registros de auditoría, al Administrador de Seguridad (ver apartado 6.2.3.4 ADMINISTRADOR DE SEGURIDAD). Esta capacidad corresponde al permiso "*maintenance*" de forma que la login class que se asigne al Administrador de Seguridad deberá disponer de este permiso (ver apartado 6.2.3.1 LOGIN CLASSES Y PERMISOS).

6.8.3 ALMACENAMIENTO REMOTO

129. Se recomienda configurar el dispositivo para el envío de los registros de auditoría a un servidor syslog remoto. Para ello se utilizará el protocolo NETCONF sobre SSH.

130. El servidor syslog remoto actuará de cliente SSH. Se debe generar una pareja de claves pública/privada SSH en el servidor syslog. **Se deben generar claves RSA de 3072 bits o superior, o claves ECDSA**. Por ejemplo:

    $ ssh-keygen -b 3072 -t rsa -C 'syslog-monitor key pair' -f ~/.ssh/syslog-monitor

    Se solicitará introducir una frase de contraseña. Se mostrará la ubicación del almacenamiento del par de claves *(syslog-monitor).*

131. En el dispositivo, crear una login class llamada, por ejemplo, monitor, con permisos para rastrear eventos (*permission bit: trace*):

[edit]

user@host# set system login class monitor permissions trace

132. Crear el usuario con el que el servidor *syslog* se conectará al dispositivo. El usuario se llamará "*syslog-mon*" y se asignará la *login class* creada (monitor). El tipo de autenticación será clave pública SSH y la clave será la generada en el servidor *syslog*.

[edit]

user@host# set system login user syslog-mon class monitor authentication ssh-rsa

"ssh-rsa xxxxx syslog-monitor key pair"

133. Configurar el protocolo NETCONF con SSH.

a) Incluir una de las siguientes declaraciones en el nivel de jerarquía de configuración indicado.

- Para habilitar el acceso al subsistema NETCONF SSH usando el puerto NETCONF-over-SSH predeterminado (830) como lo especifica RFC 4742, incluir la declaración netconf ssh en el nivel de jerarquía *[edit system services]:*

[edit system services]

user@host# set netconf ssh

- Para habilitar el acceso al subsistema NETCONF SSH usando un número de puerto específico, configurar la declaración de puerto con el número de puerto deseado en el nivel de jerarquía [edit system services]:

[edit system services]

user@host# set netconf ssh port port-number

- Para habilitar el acceso al subsistema NETCONF SSH usando el puerto SSH predeterminado (22), incluir la instrucción ssh en el nivel de jerarquía *[edit system services].* Esta configuración permite el acceso SSH al dispositivo para todos los usuarios y aplicaciones. La instrucción ssh se puede incluir en la configuración además de las instrucciones de configuración enumeradas anteriormente.

[edit system services]

user@host# set ssh

b) (Opcional) Habilitar Junos OS para desconectar a los clientes NETCONF que no responden especificando el intervalo de tiempo de espera (en segundos) después del cual, si no se han recibido datos del cliente, el proceso sshd solicita una respuesta, así como el umbral de cliente perdido activo. respuestas que desencadenan una desconexión.

[edit system services]

user@host# set netconf ssh client-alive-interval 10

user@host# set netconf ssh client-alive-count-max 10

- Aplicar la configuración.

[edit]

user@host# commit

- Repita los pasos anteriores en cada dispositivo que ejecute Junos OS donde la aplicación cliente establezca sesiones NETCONF.

134. En el servidor syslog remoto, iniciar el agente SSH y añadirle el par de claves generadas (syslog-monitor).

$ eval `ssh-agent`

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

135. En el servidor syslog remoto, iniciar la conexión NETCONF con el dispositivo, usando el usuario syslog-mon:

$ ssh syslog-mon@nombre_dispositivo -s netconf > Fichero_logs.out

136. Una vez la conexión NETCONF esté establecida, configurar la transmisión de mensajes de eventos. Esta RPC hará que el servicio NETCONF empiece a transmitir mensajes a través de la conexión SSH que se ha establecido.

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

137. Una vez finalizada la configuración, se recomienda:

- **Monitorizar el registro de eventos** que se genera en el dispositivo, por ejemplo, para las acciones de administración, y que recibe el servidor de syslog. Compararlos para verificar que son los mismos.
- **Examinar el tráfico entre el servidor syslog y el dispositivo**, para comprobar que no se puede acceder a estos datos durante la transferencia y que el servidor syslog los recibe bien.

6.9 COPIAS DE SEGURIDAD

138. Se debe realizar un backup de la configuración de los equipos. Para realizarlo, utilizar el siguiente comando:

user@host> request system software configuration-backup path

139. Este comando operativo guarda la configuración actualmente activa y cualquier parámetro específico de la instalación. La dirección especificada puede ser una ubicación local o un servidor externo. Se recomienda almacenar las copias de seguridad en un servidor externo mediante SCP o SFP, por ejemplo:

user@host> request system software configuration-backup scp://ftp.test.net/test

140. Es posible configurar la realización de copias periódicas de la configuración de forma local o enviarlas a un servidor externo. Para ello se debe añadir la siguiente configuración en la jerarquía *[edit system archival configuration]:*

- Especificar el destino de la copia de seguridad. El destino puede ser un directorio del equipo o un servidor remoto. En el caso de un servidor remoto debe usarse un protocolo seguro como SCP.

[edit system archival configuration]

user@host# set archive-sites scp://username@host<:port>/url-path | file://<path>/<filename>

- (Opcional) Configurar el intervalo en el cual se desea realizar las copias periódicas. Es posible configurar un intervalo entre 15 y 2880 minutos.

  [edit system archival configuration]

  user@host# transfer-interval interval

- (Opcional) Configurar si se desea realizar el envío de la copia de configuración cada vez que se aplica la configuración con el comando commit.

  [edit system archival configuration]

  user@host# set transfer-on-commit

141. Para realizar el envío de las copias de seguridad a través de una instancia de routing y administración diferente:

- Habilitar la instancia de administración *mgmt_junos*.

  [edit system]

  user@host# set management-instance

- Configurar la instrucción *mgmt_junos* de la instancia de enrutamiento para el archivo de configuraciones.

  [edit system archival configuration]

  user@host# set routing-instance mgmt_junos

142. Se resalta que estos comandos operativos, o de configuración, no guardan los logs. Para ello, sería necesario:

- Ingresar el siguiente comando para archivar el directorio */var/log*. Este comprimirá, en formato tar, la carpeta */var/log* y nombrará el archivo (LOGS.tar). También enviará el archivo comprimido a la carpeta de destino */var/tmp*:

  root@host> file archive source /var/log destination /var/tmp/LOGS

  root@host> file list /var/tmp

  /var/tmp:

  .snap/

  *LOCK_FILE**

  LOGS.tar <--Archivo creado

- Exportar los logs vía SCP o SFTP.

6.10 CONFIGURACIÓN DE REGLAS DE FILTRADO DE TRÁFICO

143. 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.

144. 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 6.10.2.

    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 6.10.3.

    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 6.10.4

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

        i. Se reciben fragmentos no válidos. Ver 6.10.5.

        ii. Se reciben paquetes IP fragmentados que no se pueden volver a ensamblar por completo. Ver 6.10.5.

        iii. La dirección origen es igual a la dirección de la interfaz de red. Ver 6.10.6.

        iv. La dirección origen no pertenece a las redes asociadas con la interfaz de red. Ver 6.10.6.

        v. La dirección origen está definida como perteneciente a una red de broadcast. Ver 6.10.6.

        vi. Cuando se especifiquen las opciones IP Loose Source Routing, Strict Source Routing o Record Route. Ver 6.10.7.

        vii. La dirección origen está definida como perteneciente a una red multicast. Ver 6.10.8.

        viii. La dirección origen está definida como dirección de loopback. Ver 6.10.8.

        ix. Cuando la dirección origen es una dirección multicast. Ver 6.10.8.

        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 6.10.8.

        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 6.10.8.

6.10.1 FILTRADO Y PROTOCOLOS SOPORTADOS

145. 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 Código
ICMPv6 – RFC 4443	Tipo Código
IPv4 – RFC 791	Dirección de origen Dirección de destino Protocolo de capa de transporte
IPv4 – RFC 2460	Dirección de origen Dirección de destino Protocolo de capa de transporte
TCP – RFC 793	Puerto de origen Puerto de destino
UDP – RFC 768	Puerto de origen Puerto de destino

146. Además, los siguientes protocolos son también compatibles con el dispositivo.

- IPsec
- IKE
- OSPF
- BGP

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

6.10.2 CONFIGURACIÓN DE REGLAS DE FILTRADO DE TRÁFICO

148. 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.

149. 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.

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 log session-close

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

150. 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

6.10.3 CONFIGURACIÓN DE REGLA DE DENEGACIÓN TOTAL POR DEFECTO

151. 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

6.10.4 CONFIGURACIÓN DE REGISTRO DE PAQUETES DESCARTADOS MEDIANTE LA OPCIÓN DENEGACIÓN TOTAL POR DEFECTO

152. 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

153. 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.

6.10.5 RECHAZO PARA FRAGMENTOS NO VÁLIDOS Y PAQUETES IP FRAGMENTADOS

154. 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.

155. 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

6.10.6 RECHAZO POR DEFECTO PARA *SPOOFING* DE DIRECCIONES ORIGEN

156. 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.*

157. 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

6.10.7 CONFIGURACIÓN DE OPCIÓN DE RECHAZO POR DEFECTO CON OPCIONES IP

158. 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.

159. 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

6.10.8 CONFIGURACIÓN DE OTRAS OPCIONES DE RECHAZO POR DEFECTO

160. 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.

161. 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

6.11 CONFIGURACIÓN DE POLÍTICAS DE SEGURIDAD DE FLUJOS

6.11.1 DEFINICIÓN DE POLÍTICA DE SEGURIDAD DE FLUJOS

162. 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.

163. 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.

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

6.11.2 CONFIGURACIÓN DE UNA POLÍTICA DE FLUJOS EN MODO *BYPASS*

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

[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 log session-close

166. 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.

6.11.3 CONFIGURACIÓN DE UNA POLÍTICA DE SEGURIDAD EN MODO DISCARD

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

[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-telnet

user@host# set from-zone trustZone to-zone untrustZone policy policy1 then deny

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

168. 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.

6.11.4 CONFIGURACIÓN DE UNA POLÍTICA DE FLUJO DE SEGURIDAD EN MODO PROTECT

169. 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.

    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 log session-close

170. Donde trustZone y untrustZone son zonas de seguridad preconfiguradas y trustLan y untrustLan son direcciones de red preconfiguradas.

6.12 CONFIGURACIÓN DE VPN

171. 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.

172. 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.

6.12.1 CONFIGURACIÓN DE VPN EN UN DISPOSITIVO CON SO JUNOS

173. 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.

174. 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.

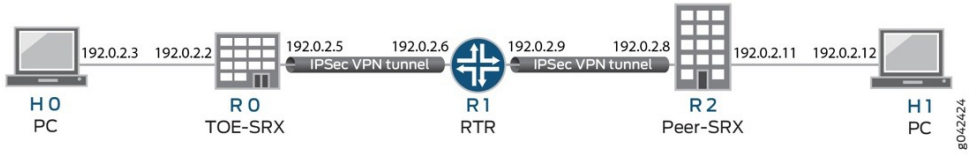

Figura 5. Topología de VPN

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

176. 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

PROPUESTA EN FASE 1 (P1, IKE)	
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 9 - Listado de algoritmos permitidos para una VPN

177. 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.*

6.12.2 VPN- IPSEC CON FIRMA ECDSA PARA AUTENTICACIÓN IKE

178. 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 10 - Autenticación y cifrado IKE o IPSec

6.12.3 VPN -IPSEC CON FIRMA ECDSA PARA AUTENTICACIÓN IKE EN EL INICIADOR

179. 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:

https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-digital-certificates-with-pki-overview.html#id-example-generating-a-public-private-key-pair

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

https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/topic-map/public-key-cryptography.html#d43e28

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

https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-configuring-ca-and-local-certificates.html#id-example-loading-ca-and-local-certificates-manually

d) Cargar la CRL manualmente. Consultar ejemplo en:

https://www.juniper.net/documentation/us/en/software/junos/vpnipsec/topics/topic-map/security-revoking-digital-certificates.html#id-example-manually-loading-a-crl-onto-the-device

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

https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-configuring-ca-and-local-certificates.html#id-example-loading-ca-and-local-certificates-manually

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

[1] Especificar las aplicaciones que se desean permitir, de acuerdo a lo establecido en el apartado 6.10.

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

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

6.12.4 VPN-IPSEC CON FIRMA ECDSA COMO AUTENTICACIÓN IKE EN LA RESPUESTA

180. 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: https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/example/certificate-pki-configuring.html

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

https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-digital-certificates-with-pki-overview.html#id-example-generating-a-public-private-key-pair

c) Generar y cargar el certificado CA. Consultar ejemplo en: https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-configuring-ca-and-local-certificates.html#id-example-loading-ca-and-local-certificates-manually

d) Cargar la CRL. Consultar ejemplo en: https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-revoking-digital-certificates.html#id-example-manually-loading-a-crl-onto-the-device

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 preconfiguradas y trustLan y

untrustLan son direcciones de red preconfiguradas.

m) Confirmar la configuración.

user@host# commit

6.13 DETECCIÓN DE ATAQUES EN RED

181. 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

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

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

i) **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.

j) **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.

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

l) **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.

m) **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.

n) **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.

o) **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.

p) **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.

182. 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.

183. 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 198.1.10.0/24

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 6.10 y 6.11.

6.13.1 DETECCIÓN DE ATAQUE DE TEARDROP IP

184. 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

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

b) Confirmar la configuración.

user@host# commit

6.13.2 DETECCIÓN DEL ATAQUE LAND TCP

185. 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 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

6.13.3 DETECCIÓN DE ATAQUE DE FRAGMENTOS ICMP

186. 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

6.13.4 DETECCIÓN DE ATAQUE DE PING DE LA MUERTE

187. 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

6.13.5 DETECCIÓN DE ATAQUE TCP SIN MARCADORES

188. 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

6.13.6 DETECCIÓN DE ATAQUE TCP SYN-FIN

189. 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

a) Confirme la configuración

c) user@host# commit

6.13.7 DETECCIÓN DE ATAQUE TCP FIN-NO-ACK

190. 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

6.13.8 DETECCIÓN DE ATAQUE DE BOMBA UDP

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

6.13.9 DETECCIÓN DE ATAQUE DOS UDP CHARGEN

192. 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

6.13.10 DETECCIÓN DE ATAQUE TCP SYN Y RST

193. 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 la jerarquía 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

6.13.11 DETECCIÓN DE ATAQUE DE DESBORDAMIENTO ICMP

194. 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

6.13.12 DETECCIÓN DE ATAQUE DE DESBORDAMIENTO TCP SYN

195. 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

6.13.13 DETECCIÓN DE ATAQUE DE ESCANEO DE PUERTO TCP

196. 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

6.13.14 DETECCIÓN DE ATAQUE DE ESCANEO DE PUERTO UDP

197. 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

6.13.15 DETECCIÓN DE ATAQUE DE BARRIDO IP

198. 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

6.14 CONFIGURACIÓN DEL PAQUETE EXTENDIDO IDP

199. 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.

200. 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.

201. 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[1].

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[2].

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].

[2] https://www.juniper.net/documentation/us/en/software/junos/idp-policy/idp-policy.pdf

7. FASE DE OPERACIÓN Y MANTENIMIENTO

202. El correcto funcionamiento del producto requiere de características que deben estar presentes en el entorno. Es la responsabilidad del administrador autorizado asegurar que el entorno operacional cumple con los requisitos enumerados a continuación:

    a) **El producto estará instalado y será mantenido en un entorno físico seguro**. Esto incluye un edificio seguro con control de acceso, o un entorno móvil controlado por el administrador.

    b) El producto no contendrá ninguna aplicación de uso general como compiladores o aplicaciones de usuario.

    c) Los administradores deben asegurar con otras medidas de seguridad complementarias el tráfico que atraviesa el producto, puesto que este no presenta ese tipo de funcionalidad.

    d) **Los administradores deben estar correctamente entrenados en el uso y la correcta operación del producto**, así como en las características del entorno seguro en que está presente. Al mismo tiempo, los administradores seguirán las guías e indicaciones presentes.

    e) Los administradores se asegurarán de que el producto cuenta con **las últimas actualizaciones de firmware y software** para preservar al mismo de amenazas y vulnerabilidades conocidas.

    f) Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.

    g) Los administradores deben **eliminar toda la información residual sensible** que pudiera quedar resultante de operar con el producto después de terminar la vida útil de este.

7.1 MONITORIZACIÓN DE LOS REGISTROS DE AUDITORÍA

203. El Administrador de Seguridad debe realizar un correcto seguimiento y mantenimiento de los registros de auditoría, asegurando que no son borrados, modificados ni accedidos por agentes no autorizados.

204. Del mismo modo, procesará la información que contienen con el fin de agilizar el proceso de respuesta y/o mitigación de potenciales problemas de seguridad. Entre los registros de mayor importancia se encuentran los relacionados con acciones administrativas, cambios de configuración, fallo de las funciones de seguridad y acceso al producto por cualquiera de sus vías. Para consultar los registros de auditoría (con los permisos administrativos pertinentes) a través de CLI, ejecutar la siguiente sentencia:

    user@host> show log filename

205. **La política de backup deberá tener en cuenta los registros de auditoría**. Considerando en número máximo de registros que se almacenan y su tamaño máximo, es recomendable realizar una copia de seguridad de los mismos antes de que sean sobrescritos (por alcanzar el máximo número de ficheros, o por falta de espacio de almacenamiento).

7.2 COPIAS DE SEGURIDAD

206. Se deben realizar copias de seguridad periódicas de forma automatizada y centralizada de la configuración actual del producto, y de la información sensible que pueda contener. Esto ayuda a garantizar, en la medida de lo posible, la respuesta a incidentes de disponibilidad y pérdida de información.

7.3 COMPROBACIÓN DE LA INTEGRIDAD Y ACTUALIZACIONES

207. Se debe comprobar periódicamente la integridad del hardware y del software que compone el producto con el fin de detectar y/o mitigar posibles problemas de seguridad derivados de la presencia de malware y/o técnicas de tampering.

208. Los Administradores de Seguridad se encargarán de la actualización regular del firmware, con el fin de solventar los problemas de seguridad presentes y potenciales conocidos. De la misma manera que el propio producto, las actualizaciones serán verificadas y siempre obtenidas por vías aceptadas y reconocidas por el fabricante.

8. REFERENCIAS

REF1 Junos® OS User Access and Authentication Administration Guide

https://www.juniper.net/documentation/us/en/software/junos/user-access/index.html

REF2 CLI User Guide

https://www.juniper.net/documentation/us/en/software/junos/cli/topics/topic-map/getting-started.html

REF3 Junos® OS Common Criteria Guide for SRX345 and SRX380 Devices

https://www.juniper.net/documentation/en_US/junos-cc20.4/information-products/pathway-pages/security/20.4r1-cc/20.4r1-security-cc-guide-srx380.pdf

REF4 Junos® OS Common Criteria Guide for SRX1500, SRX4100, SRX4200, and SRX4600 Devices

https://www.juniper.net/documentation/en_US/junos-cc19.2/information-products/pathway-pages/security/19.2r1-srx1500-4k-cc/19.2r1-srx1500-4k-cc-guide.html

REF5 Junos® OS Network Management and Monitoring Guide *https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/index.html*

REF6 Guía de Seguridad de las TIC CCN-STIC 821 APÉNDICE V: NORMAS DE CREACIÓN Y USO DE CONTRASEÑAS NP40

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/534-ccn-stic-821-normas-de-seguridad-en-el-ens-anexo-v/file.html

9. ABREVIATURAS

AES	Advanced Encryption Standard.
BGP	*Border Gateway Protocol*
CLI	Commnad Line Interface.
CBC	*Cipher-Block Chaining*
DH	Diffie Hellman.
DPP	*Dispositivo de Protección de Perímetro*
DRBG	Deterministic Random Bit Generator.
ECC	Elliptic Curve Cryptography.
ECDSA	Elliptic Curve Digital Signature Algorithm.
EULA	End User License Agreement.
ENS	Esquema Nacional de Seguridad.
GCM	*Galois Counter Mode*
HMAC	Keyed-Hash Authentication Code.
IKE	*Internet Key Exchange*
IPS	*Intrusion Prevention System*
IPSec	*Internet Protocol Security*
KVM	Kernel-Based Virtual Machine.
NTP	Network Time Protocol.
OSPF	*Open Shortest Path First*
PSK	*Pre-Shared Keys*
QSFP+	Quad small form-factor pluggable +.
QSFP28	Quad small form-factor pluggable 28
RSA	*Rivest, Shamir y Adleman*
SHA	Secure Hash Algorithm.
SSH	Secure Shell

SNMP	*Simple Network Management Protocol*
SFP+	Small form-factor pluggable +
VRF	Virtual Routing and Forwarding
VPN	*Virtual Private Network*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL