centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1456

Procedimiento de Empleo Seguro
Juniper Networks MX routers

Marzo 2025

MINISTERIO DE DEFENSA

cpage.mpr.gob.es

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2025

NIPO: 083-25-199-X
Fecha de Edición: marzo de 2025

CCN 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
2026.01.16 07:43:12 +01'00'

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1 INTRODUCCIÓN

1. El presente documento pretende servir de guía para establecer una configuración segura para los routers de Juniper Networks de la familia **MX** que ejecutan el sistema operativo **referenciado en el Catálogo de Productos y Servicios TIC (CPSTIC).**
2. Estos routers son dispositivos seguros de red, con una interfaz de gestión limitada y protegida, y un sistema operativo de propósito especial que no proporciona ninguna capacidad de propósito general, sino únicamente funciones de gestión y control, y de conmutación de paquetes Ethernet e IP.
3. El dispositivo MX son router altamente flexibles y de alto rendimiento, que proporcionan un conjunto diverso de opciones de implementación que permite a los operadores de los centros de datos y redes de altas prestaciones, construir redes automatizadas, protegidas y escalables que se adapten a sus necesidades de implementación, y que evolucionen fácilmente a medida que los requisitos cambian con el tiempo.
4. Los dispositivos son físicamente autónomos y albergan el software, el firmware y el hardware necesarios para realizar todas las funciones de conmutación y enrutado de paquetes.
5. Los dispositivos constan de los dos componentes arquitectónicos principales siguientes:
6. **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.
7. **Motor de encaminamiento de paquetes (PFE):** proporciona todas las operaciones necesarias para la conmutación y el encaminamiento de paquetes que atraviesan el equipo.
8. 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.
9. Esta familia de producto ha sido cualificada e incluida en el CPTSIC en la familia de *“Enrutadores”, “Switches” y “Redes privadas virtuales: IPSEC”.*

2 OBJETO Y ALCANCE

10. En la presente guía se recoge el procedimiento de empleo seguro para los **routers MX incluidos en el catálogo**.

11. En la siguiente tabla se muestran, en detalle, los chasis de las diferentes series dentro de la familia MX:

Familia	Modelo	Puertos de red
Router MX Gama MX10000	MX10003	Equipo completamente modular y redundante de hasta dos tarjetas de línea MX10K-LC2103 por chasis. Densidad de puertos por tarjeta de línea de hasta 72 10GbE (SFP+), 18 40GbE (QSFP+), o 12 100GbE (QSFP28) por chasis.
	MX10004	Equipo completamente modular y redundante de hasta cuatro tarjetas de línea MX10K-LC480 o MX10K-LC9600 por chasis. Densidad de puertos por tarjeta de línea MX10K-LC480 de hasta 48 1GbE, 48 10GbE por slot. Densidad de puertos por tarjeta de línea MX10K-LC9600 de hasta 96 10GbE (SFP+), 24 40GbE (QSFP+), 24 100GbE (QSFP28) o 24 400GbE (QSFP56DD) por slot. Densidad de puertos por tarjeta de línea MX10K-LC4800 de hasta 48 puertos de 100GbE (SFP56-DD Y QSFP56-DD en modo breakout), o 32 100GbE (SFP56-DD) y 4 puertos 400GbE por slot.

Familia	Modelo	Puertos de red
	MX10008	Equipo completamente modular y redundante de hasta ocho tarjetas de línea MX10K-LC480 o MX10K-LC9600 por chasis. Densidad de puertos por tarjeta de línea MX10K-LC480 de hasta 48 1GbE (SFP), 48 10GbE (SFP+) por slot. Densidad de puertos por tarjeta de línea MX10K-LC9600 de hasta 96 10GbE (SFP+), 24 40GbE (QSFP+), 24 100GbE (QSFP28) o 24 400GbE por slot. Densidad de puertos por tarjeta de línea MX10K-LC4800 de hasta 48 puertos de 100GbE (SFP56-DD Y QSFP56-DD en modo breakout), o 32 100GbE (SFP56-DD) y 4 puertos 400GbE por slot.

Tabla 1 – Chasis modular MX10000

Familia	Modelo	Puertos de red
Router MX Gama Media	MX240	Equipo completamente modular y redundante de hasta dos tarjetas de línea MPC10, MPC7, MPC5, MPC2E-NG o MPC3E-NG por chasis. Densidad de puertos por chasis de hasta 80 10GbE, o 30 100GbE, o 24 40GbE
	MX480	Equipo completamente modular y redundante de hasta seis tarjetas de línea MPC10, MPC7, MPC5, MPC2E-NG o MPC3E-NG por chasis. Densidad de puertos por chasis de hasta 240 10GbE, o 60 100GbE, o 72 40GbE
	MX960	Equipo completamente modular y redundante de hasta once tarjetas de línea MPC10, MPC7, MPC5, MPC2E-NG, MPC3E-NG por chasis. Densidad de puertos por chasis de hasta 440 10GbE, o 120 100GbE, o 132 40GbE

Tabla 2 – Chasis modular MX Universal

Familia	Modelo	Puertos de red
Router MX Gama Compacta	MX304	Equipo modular y redundante de hasta tres tarjetas de línea MX304-LMIC16 por chasis, o dos si se incorpora una segunda tarjeta supervisora. Densidad de puertos por tarjeta de línea de hasta 32 10GbE (Ópticas Breakout), 8 40GbE(QSFP+), o 16 100GbE(QSFP28) o 4 400GbE (QSFP56-DD) por chasis.
	MX204	Equipo compacto no modular y reudante a nivel de fuentes de alimentación de hasta 20 10GbE (SFP+ y ópticas Breakout), 4 40GbE(QSFP+), o 4 100GbE(QSFP28)

Tabla 3 – Chasis compactos MX

3 ORGANIZACIÓN DEL DOCUMENTO

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 0. 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 0. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

e) Apartado 9. Incluye un listado de la documentación que ha sido referenciada a lo largo del documento.

f) Apartado 10. Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

12. 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.

13. 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.

14. 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:

        1. Número de pedido de compra.
        2. Número de pedido de Juniper Networks, utilizado para hacer un seguimiento del envío.
        3. Número de seguimiento del transportista, utilizado para hacer un seguimiento del envío.
        4. Lista de artículos enviados, incluidos los números de serie.
        5. Dirección y contacto del proveedor y del cliente.

    c) Verificar que el envío lo inició Juniper Networks. Para ello, sería necesario:

        6. 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.

7. 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

15. 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.
16. 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).
17. Deberán seguirse las recomendaciones indicadas en este Procedimiento de Empleo Seguro y en la documentación de los dispositivos MX10003, MX10004, MX10008, MX240, MX480, MX960, MX304, MX204. Otros servicios deberán ser realizados únicamente por el personal autorizado.
18. Antes de instalar el dispositivo, deben revisarse las condiciones para la infraestructura necesaria, indicadas en la documentación de los dispositivos MX10003, MX10004, MX10008, MX240, MX480, MX960, MX304, MX204 y así asegurarse de que el área de despliegue cumpla con los requisitos de energía, ambientales y de espacio libre para el router.
19. Antes de conectar el dispositivo a una fuente de alimentación, revisar las instrucciones de instalación en la documentación de los MX10003, MX10004, MX10008, MX240, MX480, MX960, MX304, MX204.
20. Si el bastidor o armario dispone de dispositivos estabilizadores se deben instalar en el bastidor antes de montar el router.

4.3 REGISTRO Y LICENCIAS

21. 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*.
22. Existen dos formas de instalar la licencia: usando sentencias del modo configuración, o a través de comandos operacionales (ver apartado 6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA para información sobre la interfaz de comandos).
    a) La sentencia del modo configuración `set system license keys key`, que permite añadir o borrar licencias directamente o desde un fichero de configuración.
    b) El comando operacional `request system license add`, que instala la licencia a través de una URL o utilizando un fichero de licencias.

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

```
set system license keys key name.
```

24. 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 xxxxxx"
user@device# commit
commit complete
```

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

    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
```

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

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

    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
```

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

```
request system license add filename | url.
```

    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.

27. Para mostrar las licencias se utilizará el comando operacional `show system license`.

4.4 CONSIDERACIONES PREVIAS

28. En el apartado 4 FASE PREVIA A LA INSTALACIÓN de este documento se detallan las consideraciones previas que han de tenerse en cuenta previo a la instalación y configuración de los equipos de la familia MX.
29. En los sistemas MX de tipo modular se tiene la posibilidad de implementar dos motores de enrutamiento redundantes, o tarjetas procesadoras, sobre el mismo chasis. Una funciona como principal, mientras que la otra se mantiene como una copia de seguridad en caso de que falle el motor de enrutamiento principal. En las plataformas con procesadora redundante, la convergencia de red se lleva a cabo más rápido que en plataformas con un solo motor de enrutamiento. De forma predeterminada, Junos OS usa **re0** como motor de enrutamiento principal y **re1** como motor de enrutamiento de respaldo, a menos que se especifique lo contrario.
30. En los equipos con procesadoras redundantes, siempre y cuando se requiera que en ambos elementos tengan la misma programación, se deberá configurar el siguiente comando para que cada vez que se realice un cambio de configuración en el motor de enrutamiento principal este se propague automáticamente al motor secundario:

```
set system commit synchronize
```

31. Dada la flexibilidad a la hora de configurar el comportamiento de los mecanismos de redundancia del plano de control y plano de reenvio de paquetes del equipo se recomienda revisar el documento Junos OS *High Availability User Guide* que se puede ser encontrada en el apartado 9 REFERENCIAS *se pueden* consultar las diferentes opciones de configuración para la alta disponibilidad..

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

32. Los dispositivos **MX** deben ejecutar el firmware Junos OS **22.2R1, 22.3R1 y 22.4R2** en los chasis indicados en las siguientes tablas: *Tabla 1, Tabla 2, Tabla 3.*
33. Dentro de la frontera física de los dispositivos 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.

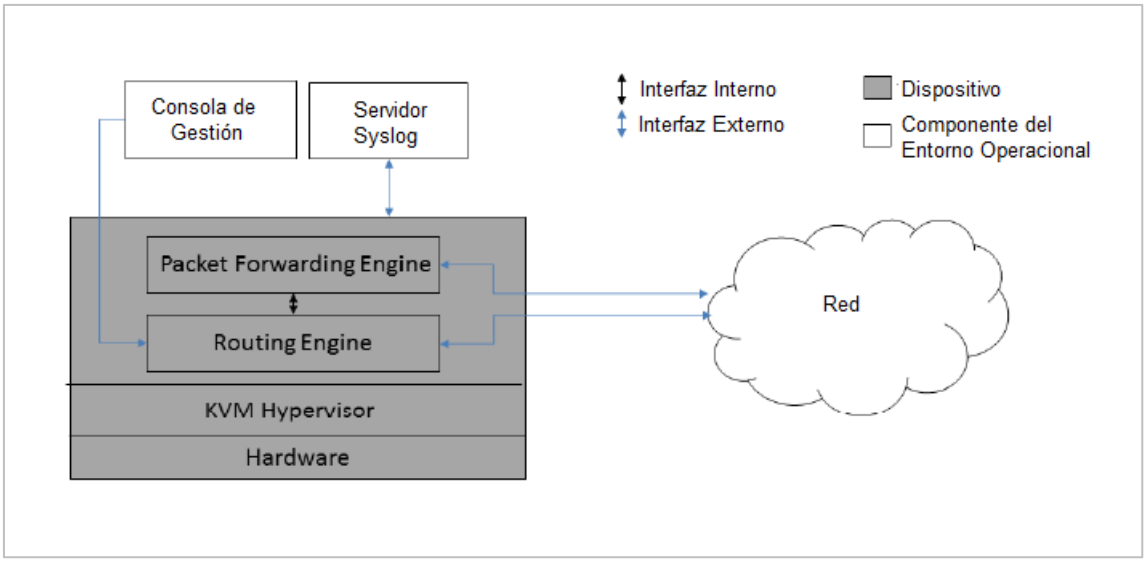

Figura 1- Arquitectura Física del dispositivo MX

34. Los dispositivos requieren interfaces de red RJ-45, SFP/SFP+, SFP28, SFP56-DD QSFP+/QSFP28, o QSFP56DD (como se detalla en las siguientes tablas: *Tabla 1, Tabla 2, Tabla 3)* para operar y comunicarse con la red conectada.

35. El entorno operativo debe proporcionar los siguientes elementos:

    a) Servidor syslog que admite conexiones SSHv2 para enviar registros de auditoría.

    b) Cliente SSHv2 para administración remota.

    c) Cliente de conexión en serie para administración local.

5 FASE DE INSTALACIÓN

36. Una vez instalado el router, 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 6.3.2.1 ROOT):

```
[edit]
root@# set system root-authentication plain-text-password
New password: password
Retype new password: password
```

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

```
[edit]
root@# set system host-name nombre_del_router
```

f) Configurar el Gateway por defecto:

```
[edit]
root@# set routing-options static route default next-hop
DirIPdelGateway
```

g) Configurar la interfaz de gestión (dirección IP y la máscara de red):

```
[edit]
root@# set interfaces em0 unit 0 family inet address
direcciónIP/máscara
```

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 router:

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

37. Una vez finalizada la configuración inicial, es necesario **comprobar que la versión de Junos instalada es la esperada**. 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 version
    ```

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

    ```
    Hostname: lab
    Model: mx10003
    Junos: 22.2R1.9
    JUNOS OS Kernel 64-bit  [20210529.2f59a40_builder_stable_12]
       […]
    ```

38. Si la versión instalada no es la adecuada (aquella que se encuentre **cualificada en el CPSTIC**), será necesario descargar la versión adecuada:

    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.

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

    e) Se debe 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 router a instalar.

39. Con la versión de Junos alojada en el servidor, hacer la instalación desde el router:

    a) Acceder al modo de configuración del equipo.

```
root@lab> configure
```

b) Ejecutar el comando `request vmhost software add <pathname><source> reboot` para instalar Junos de la Plataforma.

```
root@lab> request vmhost software add scp://hostname/pathname/junos-
vmhost-install-mx-x86-64-22.2R1.9.tgz reboot
```

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

```
scp://<username>:<password>@hostname/pathname/junos-vmhost-install-
mx-x86-64-22.2R1.9.tgz
```

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

```
root@lab> show version
```

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

```
Hostname: lab
Model: mx204
Junos: 22.2R1.9
JUNOS OS Kernel 64-bit [20200908.87c9d89_builder_stable_11]
[…]
```

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

40. 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.

41. 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 6.2.1 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 SHA1 con software Junos-FIPS).
    - Obliga a que las contraseñas de administrador tengan 10 caracteres como mínimo.

42. 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 SHA1, SHA256 y SHA512 son implementadas en el módulo LibMD que es utilizado por el demonio Junos MGD para el password hashing.

43. 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, 256) AES-CTR (128, 256)
	Message Digest Generation	SHA1, SHA2-256, SHA2-384, SHA2-512
	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 (2048/3072/4098) w/ SHA-256/512
	Random Bit Generation	DRBG (HMAC-SHA-2-256)
LibMD	Message Digest Generation	SHA1, SHA2-256, SHA2-512
	Message Authentication	HMAC-SHA1, HMAC-SHA2-256
Kernel	Message Digest Generation	SHA1, SHA2-256, SHA2-384, SHA2-512
	Message Authentication	HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-512
	Random Bit Generation	HMAC-DRBG (HMAC-SHA-2-256)

Tabla 4 – Algoritmos y funciones criptográficas en modo de operación seguro

44. 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

CSP	Descripción	Funciones y algoritmos criptográficos empleados
SSH Session Key	Claves de sesión SSH usadas para el cifrado, autenticación de mensajes y Key Establisment.	Claves de cifrado AES 128/256 Claves MAC HMAC-SHA1, HMAC-SHA2-256 y HMAC-SHA2-512 Claves privadas DH Group 14 o ECDH-P256/P-384/P-521
Contraseñas de usuarios	Contraseñas en texto plano introducidas por los usuarios para su autenticación.	Las contraseñas se almacenan cifradas con un hash (HMAC-SHA-256 o SHA-512)
DRBG	Estado interno y "seed key" del DRBG	DRBG (HMAC-SHA-2-256)

Tabla 5 – Parámetros Críticos de Seguridad (CSPs)

45. Para obtener información adicional sobre el proceso de configuración del modo de operación seguro se puede consultar las guías de configuración Common Criteria incluidas en el apartado 9 REFERENCIAS. A continuación, se muestran los pasos resumidos para configurar el modo de operación seguro desde Junos OS CLI:

    a) Acceder como usuario root, y ejecutar la sentencia `request system software add optional://fips-mode.tgz` y la sentancia `request system software add optional://jpfe-fips.tgz`. Estos paquetes no están instalados por defecto y son necesario para habilitar el modo FIPS.

    b) Configurar el dispositivo para funcionar en modo FIPS. El dispositivo solo dispone del "level 1", y para activa todas las características se ejecutará la sentencia `set system fips level 1`:

```
root@host>configure
Entering configuration mode
[edit]
root@host# set system fips level 1
```

    c) Confirmar el cambio y reiniciar el dispositivo:

```
root@host# commit
configuration check succeeds
[edit]
     'system'
     reboot is required to transition to FIPS level 1
commit complete
[edit]
root@host# run request vmhost reboot
Reboot the system ? [yes,no] (no) yes
```

46. Cuando el dispositivo se reinicia tras la activación del modo seguro, se realizan los auto-chequeos de arranque (ver apartado 6.9 AUTO-CHEQUEOS). Una vez

finalizan los auto chequeos, debe reiniciarse de nuevo el dispositivo para activar el RBG (HMAC-DRBG).

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

```
[edit]
root@host#show system
fips {
    level 1;
}
```

6.2 AUTENTICACIÓN

48. 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+.
49. Estos dos últimos servidores de autenticación se configuran según está detallado en el apartado 6.6 SERVIDORES DE AUTENTICACIÓN.
50. Se recomienda hacer uso de la autenticación local mediante nombre de usuario/contraseña de acrode a lo indicado en la siguiente sección, o claves públicas.

6.2.1 AUTENTICACIÓN CON NOMBRE DE USUARIO Y CONTRASEÑA

51. 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 MX es SHA512, y SHA256 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, o SHA256 con software Junos-FIPS, en los dispositivos MX.

```
[edit system login user username]
user@host# set authentication encrypted-password "$ABC123"
```

52. 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 6.3.2.5 CONFIGURACIÓN DE LOS PARAMETROS DE SESION**¡Error! No se encuentra el origen de la referencia.**). 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.

6.2.2 AUTENTICACIÓN CON CLAVE PÚBLICA SSH

53. 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).

54. 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.

55. 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 DH Group 14 – sha1	ECDSA P-256 RSA	AES CTR 128 AES CTR 256 AES CBC 128 AES CBC 256	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512

Tabla 6 – Funciones y Algoritmos SSHv2

56. 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: Diffie-Hellman Group 14 con SHA1, ECDH sobre las curvas nistp256, nistp384 y nistp521.
  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, 192, 256 bits.

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

root@host# set system services ssh ciphers aes128-ctr
root@host# set system services ssh ciphers aes256-ctr
```

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

- Acceder a la Shell del equipo como usuario root.

```
root@host# start shell user root
Password:
root@host%
```

- 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
```

  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 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

58. 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 están disponibles en el equipo una vez se activa el modo de empleo seguro (FIPS).

59. 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 en el apartado 9 REFERENCIAS.

60. 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.

61. 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.

62. 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*".

63. 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).

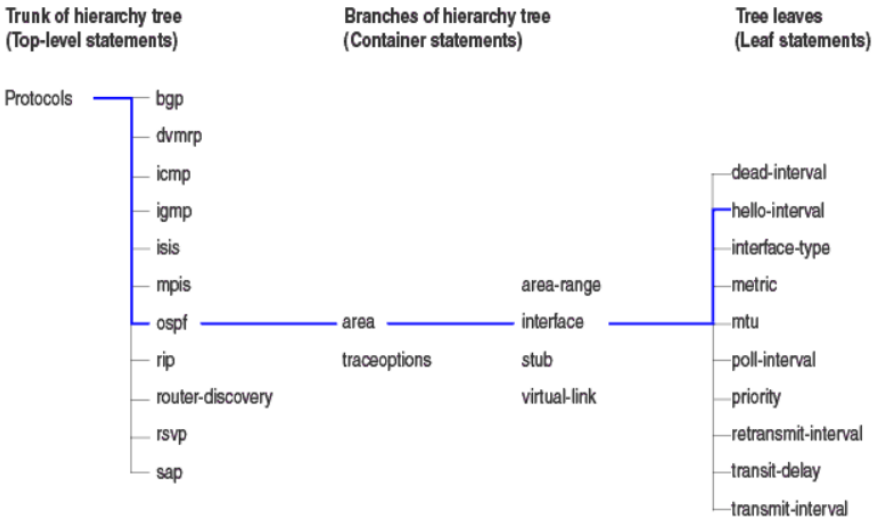

Figura 2 - Ejemplo de jerarquía de sentencias de configuración

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

6.3.2.1 ROOT

64. 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.

65. 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>;
}
```

66. 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
```

67. 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.**

6.3.2.2 ADMINISTRADOR DE SEGURIDAD

68. 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:

a) Administración local (vía consola) y remota (vía SSHv2) del dispositivo.

b) Consultar la versión actual del firmware e iniciar actualizaciones manuales del mismo (verificando que la firma digital del paquete es correcta).

c) 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.

d) Crear, modificar o borrar cuentas de otros administradores y usuarios, incluyendo los parámetros relacionados con los intentos fallidos de autenticación (retry-options, ver apartado 6.3.2.5 CONFIGURACIÓN DE LOS PARAMETROS DE SESION**¡Error! No se encuentra el origen de la referencia.**), el reseteo de sus contraseñas o el desbloqueo de cuentas.

e) Generar las claves de autenticación SSH.

f) Configurar parámetros de sesión, como el banner de acceso o los tiempos máximos de inactividad.

g) Importar certificados al almacén seguro del dispositivo.

h) Configurar el servidor SSH del dispositivo, incluidas las funciones criptográficas.

i) Configurar la fecha y hora del dispositivo.

69. Para crear el Administrador de Seguridad:

    1. 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
```

    2. 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
```

6.3.2.3 LOGIN CLASSES Y PERMISOS

70. 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 en el apartado 9 REFERENCIAS.

71. 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.

72. 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*).

73. 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]`).

En la Tabla 2 (página 4) del documento ***¡Error! No se encuentra el origen de la referencia.*** se pueden consultar todos los Permission Bits existentes. Cabe destacar los siguientes:

c) ***Admin:*** puede ver la información de cuentas de usuario en el modo configuración, y con el comando `show configuration`.

d) ***Admin-control*:** puede ver las cuentas de usuario y configurarlas (en el nivel de jerarquía `[edit system login]`).

e) ***All:*** todos los permisos.

f) ***Clear*:** puede borrar información aprendida de la red, que se almacena en varias bases de datos de la red (utilizando los comandos clear).

g) ***Network:*** puede acceder a la red con comandos ping, ssh, telnet y traceroute.

h) ***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]`).

i) ***Trace*:** puede ver la configuración de los "traces files" en los modos de configuración y operacional.

j) ***Secret:*** puede ver contraseñas y otras claves de autenticación en la configuración.

k) *Secret-control*: puede ver contraseñas y otras claves de autenticación, y **las puede modificar en el modo configuración.**

l) ***View*:** puede usar varios comandos para visualizar parámetros del sistema, tabla de enrutamiento, valores de protocolos y estadísticas.

m) ***Security*:** puede ver la configuración de seguridad en el modo configuración y usando el comando show configuration del modo operacional.

n) ***Security-control*:** puede ver y configurar la información de seguridad (en el nivel de jerarquía `[edit security]`).

74. Todos los usuarios que accedan al router, deben encontrarse en una login class. Existen cuatro 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 7 – Login classes predefinidas en Junos OS

75. 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 3 - Configuración de "edit system login".

6.3.2.4 CONFIGURACIÓN DE POLITICA SEGURA DE CONTRASEÑA

76. 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;
}
```

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

b) `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.**

c) `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.`

d) `minimum-character-changes`: mínimo número de caracteres que deben cambiar entre una contraseña y la anterior.

e) `format (sha1 | sha256 | sha512):` Función hash con la que Junos OS cifrará la contraseña. En los dispositivos MX es SHA512 por defecto (las contraseñas empiezan por 6). Se recomienda usar SHA512 con software Junos-FIPS.

f) `maximum-length / mínimum-length`: longitudes máxima y mínima de la contraseña. **Se recomiendan 12 caracteres mínimo**.

g) `maximum-lifetime days`: máxima duración de la contraseña en días. **Se recomienda configurar un tiempo máximo de 60 días o menos.**

h) `minimum-lifetime days`: mínimo número de días que debe durar la contraseña antes de poder cambiarla. **Se recomienda configurar no menos de 4 días.**

i) `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.

j) `minimum-reuse`: mínimo número de contraseñas antiguas que no deben coincidir con la nueva contraseña. **Se recomienda configurar, al menos, 5.**

77. 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 en el apartado 9 REFERENCIAS.

6.3.2.5 CONFIGURACIÓN DE LOS PARAMETROS DE SESION

78. Los parámetros de intento de sesión que deben configurarse 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, que es el valor por defecto**.
- `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:

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

   ii. 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.

c) **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.

d) **Tiempo máximo de inactividad de sesión (*idle timeout*):** como se ha comentado en el apartado 6.3.2.3 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.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

79. Se recomiendo desactivar las interfaces de red no utilizadas:

```
[edit interfaces]
user@host# set interface-name disable
```

80. (Opcional) Agregar una descripción a los puertos utilizados y no utilizados:

Para interfaces utilizados:

```
[edit interfaces]
user@host# set interface-name description "---descripción---"
```

Para interfaces no utilizados:

```
[edit interfaces]
user@host# set interface-name description "---no utilizada---"
```

81. No se recomienda habilitar LLDP a nivel general y solo deberá activarse en aquellas interfaces estrictamente necesarias

```
[edit protocols lldp]
user@host# set interface interface-name
```

6.5 GESTIÓN DE CERTIFICADOS

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

83. 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).

84. 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 (issued) por uno de ellos.

6.6 SERVIDORES DE AUTENTICACIÓN

85. 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 en el apartado 9 REFERENCIAS, sección Radius Authentication.

86. 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
```

87. 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.

88. 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
```

- Aplicar la configuración.

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

- 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
```

89. 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 en el apartado 9 REFERENCIAS, sección *TACACS+ Authentication*.

90. 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
```

91. 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
```

- Aplicar la configuración.

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

- 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
```

6.7 SINCRONIZACIÓN

92. 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
```

93. Los routers MX 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.

94. 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>
```

95. **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"
```

96. 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.

97. 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
```

- Aplicar la configuración.

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

- 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
```

6.8 ACTUALIZACIONES

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

99. 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.

100. El procedimiento de actualización es el mismo que el descrito en el apartado 5 FASE DE INSTALACIÓN. Este proceso incluye como realizar una instalación vía protocolo seguro SCP.

101. El paquete instalable de firmware para los routers **MX** 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.

102. 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.

103. 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.

104. 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.

6.9 AUTO-CHEQUEOS

105. 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 SHA1 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 correctamente utilizando /opt/sbin/kats/cannot-exec.real.
- **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.

6.10 ALTA DISPONIBILIDAD

106. Dada la flexibilidad a la hora de configurar el comportamiento de los mecanismos de redundancia del plano de control y plano de reenvio de paquetes del equipo se recomienda revisar el documento Junos OS *High Availability User Guide* que se puede ser encontrada en el apartado 9 REFERENCIAS *se pueden* consultar las diferentes opciones de configuración para la alta disponibilidad..

6.11 AUDITORÍA

107. 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.
108. 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 Message) en el apartado 9* REFERENCIAS.

6.11.1 REGISTRO DE EVENTOS

109. 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.

110. 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]`.

111. 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 router1 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.	Router1

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 8 – Estructura de los mensajes de auditoría

112. 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

Tipo	Mensaje de auditoría generado
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 9 – Ejemplo de mensajes de auditoría

6.11.2 ALMACENAMIENTO LOCAL

113. 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]`.

114. 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 (hasta 1Gb) o el número de archivos de auditoría que se irán almacenando (10 por defecto).

115. 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.

116. 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.

117. 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 10 – 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.

Severity Level	Tipo de mensajes
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 11 – Valores para Severity Level

118. 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
```

119. 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 6.3.2.2 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 6.3.2.3 LOGIN CLASSES Y PERMISOS).

6.11.3 ALMACENAMIENTO REMOTO

120. 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.

121. 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 2048 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)`.

122. 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
```

123. 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”
```

124. Configurar el protocolo NETCONF con SSH.

- Incluir una de las siguientes declaraciones en el nivel de jerarquía de configuración indicado

  a. 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
  ```

  b. 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
  ```

  c. 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
```

- (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 veces que el número de que se pueden perder antes de desencadenan una desconexión.

```
[edit system services]
user@host# set netconf ssh client-alive-interval 10
user@host# set netconf ssh client-alive-count-max 3
```

- 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.

125. 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
```

126. 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
```

127. 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>
```

128. 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.

6.12 BACKUP

129. **Se debe realizar una copia de seguridad de la configuración de los equipos**. Para realizarlo, utilizar el siguiente comando:

```
user@host> request system software configuration-backup path
```

130. Este comando operativo guarda la configuración actualmente activa y cualquier parámetro específico esta. La dirección especificada es el disco local del equipo. Se recomienda almacenar las copias de seguridad en un servidor externo mediante SCP o SFP.

```
user@host> request system configuration rescue save
```

131. 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
```

132. 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
```

- Aplicar la configuración.

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

- 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
```

133. 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.

7 CONFIGURACIÓN DE VPNS

7.1 CONFIGURACIÓN DE VPN

134. La configuración de VPN aplica a MX240, MX480 y MX960 cuando incorporA en el chasis la tarjeta de servicios MX-SPC3.

135. Para utilizar las funcionalidades de VPN seguras a través del protocolo IPSE se debe añadir un paquete adicional en el equipo identificado como jpfe-spc3*, en ambas procesadoras del equipo

136. De forma previa a la instalado el nuevo software y reiniciado el equipo, se deberá habilitar el modo unified-services en amba procesadoras. Este comando requiere el reinicio del equipo, que realizaremos tras la instalación del software jpfe-spc3* que veremos en el siguiente apartado:

```
request system enable unified-services
```

137. Se debe proceder a la instalación del paquete jpfe-spc3* en ambas procesadoras del equipo. Para instalar el paquete se deberán seguir las instrucciones dadas en el apartado 5 FASE DE INSTALACIÓN para la instalación del software. Se recomienda revisar el documento Next Gen Services Interfaces User Guide for Routing Devices que se puede ser encontrada en el apartado 9 REFERENCIAS *para más detalle.*

138. Todas las VPN deberán configurarse de forma que se utilicen algoritmos de cifrado con una fortaleza criptológica de 128 bits o superior, de acuerdo con lo estipulado en la guía CCN-STIC-807 para el ENS Categoría Alta. Los algoritmos de cifrado IKE e IPSEC disponibles son los siguientes:

Algoritmo	Descripción
aes-128-cbc	*AES-CBC 128-bit encryption algorithm*
aes-128-gcm	*AES-GCM 128-bit encryption algorithm*
aes-192-cbc	*AES-CBC 192-bit encryption algorithm*
*aes-192-gcm**	*AES-GCM 192-bit encryption algorithm*
aes-256-cbc	*AES-CBC 256-bit encryption algorithm*
aes-256-gcm	*AES-GCM 256-bit encryption algorithm*

**Solo soportado para IPSEC*

Tabla 12 – Algoritmos de cifrado IKE e IPSEC

139. 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.

7.1.1 CONFIGURACIÓN DE VPN EN UN DISPOSITIVO CON SO JUNOS

140. 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.

141. 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.

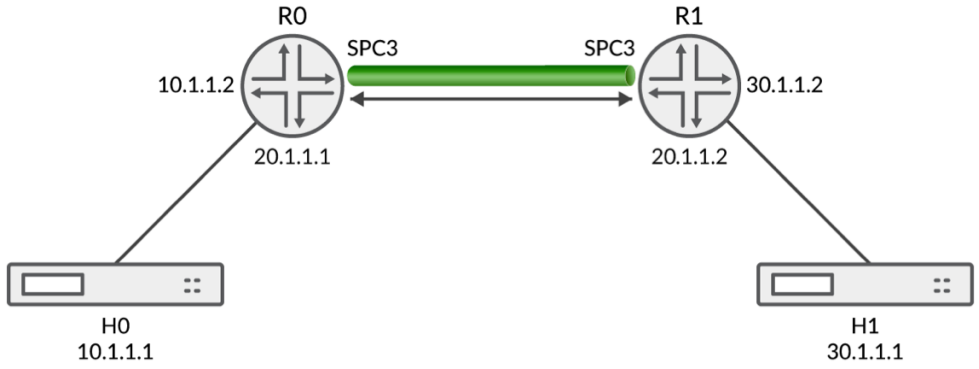

Figura 4. Topología de VPN

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

143. 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, ECDSA-SIGNATURES-521
Algoritmo de autenticación	SHA-256, SHA-384, SHA-512
Grupo DH	19, 20, 21 y 24
Algoritmo de cifrado	AES-128-CBC, AES-128-GCM, AES-192-CBC, AES-256-CBC, AES-256-GCM
PROPUESTA EN FASE 2 (P2, IPSEC)	
Protocolo IKE	IKEv2
Algoritmo de autenticación	HMAC-SHA-256-128, HMAC-SHA-384, HMAC-SHA-512
Grupo DH	19, 20, 21 y 24
Método de cifrado	ESP
Algoritmo de cifrado	AES-128-CBC, AES-128-GCM, AES-192-CBC, AES-192-GMC, AES- 256-CBC, AES-256-GCM

Tabla 13 - Listado de algoritmos permitidos para una VPN

144. 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`.

7.1.2 CONFIGURACIÓN DE UNA VPN CON IPSEC CON UNA FIRMA ECDSA PARA AUTENTICACIÓN IKE

145. 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 14 - Autenticación y cifrado IKE o IPSec

7.1.3 CONFIGURACIÓN DE UNA VPN IPSEC CON FIRMA ECDSA PARA AUTENTICACIÓN IKE EN EL INICIADOR

146. 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/vpn-ipsec/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]

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

```
user@host# set set security ike proposal ike-proposal1 dh-group
group19
user@host# set security ike proposal ike-proposal1
authentication-algorithm sha384
user@host# set security ike 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]
user@host# set security ike policy ike-policy1 mode main
user@host# set security ike policy ike-policy1 proposals ike-
proposal1
user@host# set security ike policy ike-policy1 certificate
local-certificate cert1
```

h) Configurar la propuesta IPSec.

```
[edit]

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

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

i) Configurar la política IPSec.

```
[edit]

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

user@host# set security ike gateway gw1 ike-policy ike-policy1
user@host# set security ike gateway gw1 address 20.1.1.2
user@host# set security ike gateway gw1 local-identity inet
20.1.1.1
user@host# set security ike gateway gw1 external-interface xe-
0/0/2
user@host# set security ike gateway gw1 version v2-only
```

Donde **gw1** es el nombre de una puerta de enlace IKE, 20.1.1.2 es la IP del extremo remoto de la VPN, 20.1.1.1 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 security ipsec vpn vpn1 establish-tunnels
immediately
```

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

l) Configurar la jerarquía service-set:

```
[edit]
user@host# set services service-set IPSEC_SS_SPC3 next-hop-
service inside-service-interface vms-5/0/0.1
user@host# set services service-set IPSEC_SS_SPC3 next-hop-
service outside-service-interface vms-5/0/0.2
user@host# set services service-set IPSEC_SS_SPC3 ipsec-vpn vpn1
```

m) Configurar las ingerfaces las opciones de routing:

```
[edit]
user@host# set interfaces xe-0/0/2 unit 0 family inet address
20.1.1.1/24
user@host# set interfaces vms-5/0/0 unit 0 family inet
user@host# set interfaces vms-5/0/0 unit 1 family inet
user@host# set interfaces vms-5/0/0 unit 1 family inet6
user@host# set interfaces vms-5/0/0 unit 1 service-domain inside
user@host# set interfaces vms-5/0/0 unit 2 family inet
user@host# set interfaces vms-5/0/0 unit 2 family inet6
user@host# set interfaces vms-5/0/0 unit 2 service-domain
outside
user@host# set interfaces st0 unit 1 family inet
user@host# set interfaces st0 unit 1 family inet6
user@host# set interfaces st0 unit 2 family inet
user@host# set interfaces st0 unit 2 family inet6
user@host# set routing-options static route 30.1.1.0/24 next-hop
st0.0
```

n) Confirmar la configuración.

```
user@host# commit
```

7.1.4 CONFIGURACIÓN DE UNA VPN IPSEC CON FIRMA ECDSA COMO AUTENTICACIÓN IKE EN LA RESPUESTA

147. 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/en_US/junos/topics/topic-map/security-revoking-digital-certificates.html#id-example-manually-loading-a-crl-onto-the-device

o) Configurar la propuesta IKE.

```
[edit]

user@host# set security ike proposal ike-proposal1
authentication-method ecdsa-signatures-256
user@host# set set security ike proposal ike-proposal1 dh-group
group19
user@host# set security ike proposal ike-proposal1
authentication-algorithm sha384
user@host# set security ike proposal ike-proposal1 encryption-
algorithm aes-256-cbc
```

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

p) Configurar la política IKE.

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

q) Configurar la propuesta IPSec.

```
[edit]

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

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

r) Configurar la política IPSec.

```
[edit]

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

s) Configurar IKE.

```
[edit]

user@host# set security ike gateway gw1 ike-policy ike-policy1
user@host# set security ike gateway gw1 address 20.1.1.1
user@host# set security ike gateway gw1 local-identity inet
20.1.1.2
user@host# set security ike gateway gw1 external-interface xe-
0/0/3
user@host# set security ike gateway gw1 version v2-only
```

Donde **gw1** es el nombre de una puerta de enlace IKE, 20.1.1.2 es la IP del extremo remoto de la VPN, 20.1.1.1 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.

t) 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 security ipsec vpn vpn1 establish-tunnels
immediately
```

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

u) Configurar la jerarquía service-set:

```
[edit]
user@host# set services service-set IPSEC_SS_SPC3 next-hop-
service inside-service-interface vms-4/0/0.1
user@host# set services service-set IPSEC_SS_SPC3 next-hop-
service outside-service-interface vms-4/0/0.2
user@host# set services service-set IPSEC_SS_SPC3 ipsec-vpn vpn1
```

v) Configurar las ingerfaces las opciones de routing:

```
[edit]
user@host# set interfaces xe-0/0/3 unit 0 family inet address
20.1.1.2/24
user@host# set interfaces vms-4/0/0 unit 0 family inet
user@host# set interfaces vms-4/0/0 unit 1 family inet
user@host# set interfaces vms-4/0/0 unit 1 family inet6
user@host# set interfaces vms-4/0/0 unit 1 service-domain inside
user@host# set interfaces vms-4/0/0 unit 2 family inet
user@host# set interfaces vms-4/0/0 unit 2 family inet6
user@host# set interfaces vms-4/0/0 unit 2 service-domain
outside
user@host# set interfaces st0 unit 1 family inet
user@host# set interfaces st0 unit 1 family inet6
user@host# set interfaces st0 unit 2 family inet
user@host# set interfaces st0 unit 2 family inet6
user@host# set routing-options static route 10.1.1.0/24 next-hop
st0.0
```

w) Confirmar la configuración.

```
user@host# commit
```

8 FASE DE OPERACIÓN Y MANTENIMIENTO

148. 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.

8.1 MONITORIZACIÓN DE LOS REGISTROS DE AUDITORÍA

149. 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.

150. 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.

151. 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.

152. Para consultar los registros de auditoría (con los permisos administrativos pertinentes) a través de CLI, ejecutar la siguiente sentencia:

```
user@host> show log filename
```

153. 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 un backup de los mismos antes de que sean sobrescritos (por alcanzar el máximo número de ficheros, o por falta de espacio de almacenamiento).

8.2 COPIAS DE SEGURIDAD

154. 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.

8.3 COMPROBACIÓN DE LA INTEGRIDAD Y ACTUALIZACIONES

155. 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.

156. 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.

9 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

REF 3 Junos®OS High Availability User Guide
https://www.juniper.net/documentation/us/en/software/junos/high-availability/high-availability.pdf

REF4 Junos® OS Common Criteria Evaluated Configuration Guide for MX10003 Devices
https://www.juniper.net/documentation/us/en/software/ccfips22.2/cc-routers-mx10003/cc-routers-mx10003.pdf

REF 5 Junos® OS Common Criteria Configuration Guide for MX240, MX480, and MX960 Devices with MX-SPC3 Services Card
https://www.juniper.net/documentation/us/en/software/ccfips22.2/cc-routers-mx240-480-960/cc-routers-mx240-480-960.pdf

REF 6 Junos® OS Common Criteria Evaluated Configuration Guide for MX304 Device with JNP304-LMIC16 Line Card
https://www.juniper.net/documentation/us/en/software/ccfips22.4/cc-routers-mx304/cc-routers-mx304.pdf

REF7 Junos® OS Network Management and Monitoring Guide
https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/index.html

REF8 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

REF9 Next Gen Services Interfaces User Guide for Routing Devices
https://www.juniper.net/documentation/us/en/software/junos/interfaces-next-gen-services/interfaces-next-gen-services.pdf

10 ABREVIATURAS

AES	Advanced Encryption Standard.
CLI	Commnad Line Interface.
CFP2-DCO	C-form factor pluggable 2- Digital Coherent Optics
DH	Diffie Hellman.
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.
HMAC	Keyed-Hash Authentication Code.
IKE	Internet Key Exchange
IPSEC	Internet Protocol Security
KVM	Kernel-Based Virtual Machine.
NTP	Network Time Protocol.
QSFP+	Quad small form-factor pluggable +
QSFP28	Quad small form-factor pluggable 28
SHA	Secure Hash Algorithm.
SSH	Secure Shell.
VRF	Virtual Routing and Forwarding.

PUBLICACIONES DE DEFENSA

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