centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1301

Procedimiento de empleo seguro
GigaVUE de GIGAMON

Abril 2023

MINISTERIO DE DEFENSA

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

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
2024.02.08 17:01:28 +01'00'

NIPO: 083-23-121-4.
Fecha de Edición: Abril de 2023
GIGAMON ha participado en la realización y modificación del presente documento y sus anexos.

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

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. **Gigamon** desarrolla y comercializa equipos y *software* de *Network Packet Brokering* (NPB), denominados **GigaVUE**, destinados a la captura de tráfico en interfaces de red físicos (en cobre fibra) o virtuales (en *clouds* públicas y privadas) para su posterior filtrado y manipulación y ulterior entrega a herramientas de seguridad y monitorización. El sistema operativo sobre el que funcionan los equipos de Gigamon se denomina GigaVUE-OS.
2. El propósito de este documento es detallar las configuraciones de seguridad en GigaVUE para proteger un dispositivo y que este opere de acuerdo a unas garantías mínimas de seguridad.
3. A modo de aclaración, los NPB implementan una variedad de herramientas de monitoreo para acceder y analizar el tráfico de una red. En pocas palabras, los NPB funcionan como "*intermediarios*" (o administradores) del tráfico de red. El NPB recopila el tráfico de múltiples enlaces de red, filtra y distribuye cada paquete individual a la herramienta de monitoreo de red correcta. Al hacerlo, los NPB garantizan una mayor eficacia de las herramientas de seguridad y supervisión de la red.
4. Mientras que un NPB tradicional puede ayudar a garantizar una mayor efectividad de las herramientas de monitoreo, un NPB de próxima generación asegura que se envía el tráfico a las herramientas de prevención en línea y fuera de banda adecuadas.
5. GigaVUE implementan las siguientes funciones:
    - Prevención de amenazas.
    - Balanceo de carga.
    - Alta resistencia de las herramientas de seguridad de red en línea.
    - Gran cantidad de herramientas de detección de amenazas fuera de banda.
    - Precisión de las herramientas de monitoreo de red.
    - Análisis del rendimiento de la red.
    - Agregación de TAP de red de alta velocidad.
6. Este documento está destinado a un público familiarizado con la configuración de GigaVUE-OS y no pretende sustituir a la Guía del Usuario, que puede descargarse del portal de la comunidad Gigamon o accederse en línea en el siguiente enlace:

    https://docs.gigamon.com/doclib59/5900-gigadoc.html.

2. CONVENCIONES UTILIZADAS EN EL PRESENTE DOCUMENTO

7. Este documento se centra en la configuración del dispositivo GigaVUE a través de la Interfaz de Línea de Comando (CLI). La mayoría de las recomendaciones que se comentan más abajo pueden realizarse también a través de la Gestión de Interfaz Gráfica (GUI) pero la manera de hacerlo puede variar de una versión a otra y es por eso que este documento se basa solo en la CLI. Para realizarlo por la GUI consultar la guía de usuario (REF1) adjunta.

8. El *prompt* para configurar el equipo GigaVUE cambia dependiendo del modo de funcionamiento: *Standard*, *Enable* y *Configure*. Los tres (3) modos que existen permiten:

    - *Standard*: Modo de acceso básico. Permite revisar los aspectos más básicos de la configuración como licencias, versiones, conectividad del equipo y estadísticas de puertos.
    - *Enable*: Permite el acceso completo a la monitorización del equipo, pudiendo ver toda la configuración, puertos, mapas, estadísticas, etc. También permite la gestión de actualizaciones.
    - *Configure*: Permite el acceso completo al sistema.

9. En los ejemplos utilizados en este documento, el nombre de *host* del dispositivo GigaVUE será *"gigavue-appliance*", que precederá a cada uno de los *prompts*. Comenzando con el modo *Standard* (indicado por el símbolo '>') y seguido del modo *Enable* (indicado por el símbolo '#') y el modo *Configure* (indicado por el prefijo *'(config) #*') estos se indican como:

```
gigavue-appliance > enable
gigavue-appliance # configure terminal
gigavue-appliance (config) #
```

Figura 1. Cambio de modos para aumentar privilegios

10. A continuación, se ilustra cómo retroceder de los modos anteriores:

```
gigavue-appliance (config) # exit
gigavue-appliance # disable
gigavue-appliance >
```

Figura 2. Cambio de modos para disminuir privilegios

11. Para la sintaxis CLI, los comandos introducidos por el usuario se muestran en naranja con *prompts* y salidas estándar (*stdout*) marcadas en negro:

```
gigavue-appliance > enable
gigavue-appliance # configure terminal
gigavue-appliance (config) # show clock
Time: 15:18:00
Date: 2020/03/23
Time zone:  Europe Western London
            (Europe/London)
UTC offset: same as UTC
gigavue-appliance (config) #
```

Figura 3. Ejemplo de comando input

12. Las variables introducidas por el usuario se muestran en azul:

```
gigavue-appliance > enable
gigavue-appliance # configure terminal
gigavue-appliance (config) # logging 192.168.1.10
gigavue-appliance (config) #
```

Figure 4. Ejemplo de comando input de variable

13. Los errores son señalados con color rojo (notar el uso del símbolo %):

```
gigavue-appliance > enable
gigavue-appliance # configure terminal
gigavue-appliance (config) # logging 300.300.300.300
% Invalid syslog server hostname/ipv4/ipv6 address:
300.300.300.300
gigavue-appliance (config) #
```

Figure 5. Ejemplo de error stdout

14. Los resultados de especial interés se marcarán en verde:

```
gigavue-appliance > enable
gigavue-appliance # show users
  USERNAME     REMOTE USERNAME       LINE     HOST              IDLE
* admin                             pts/0    192.168.1.2       0d  0h  0m  0s
  osheridan                         pts/1    192.168.1.3       0d  0h  0m 40s
gigavue-appliance #
```

Figure 6. Ejemplo de stdout de especial interés

15. Cabe señalar que la ejecución del comando *"write memory"* para garantizar que sus comandos permanecen persistentes a través de los reinicios se requiere y **se asume para cada ejemplo**.

3. VISIÓN GENERAL

16. **Los elementos GigaVUE-OS pueden ser configurados para mejorar la seguridad del propio dispositivo y de su entorno**.

17. **Se debe consultar el Catálogo de Productos y Servicios de Seguridad (CPSTIC) del Centro Criptológico Nacional para determinar qué modelos y qué versiones son los cualificados.**

18. Este documento se concentra en IPv4 al ser la versión más utilizada del Protocolo de Internet. Algunas de las configuraciones aquí recogidas también son válidas para IPv6. Para más información, se recomienda consultar la Guía de Usuario [REF1].

4. CONTROLES FÍSICOS

19. El acceso físico a cualquier dispositivo puede dar lugar a que se manipule el equipo, tanto en tránsito como una vez desplegado. Hay una gran cantidad de diferentes vectores de amenaza asociados a los ataques físicos, por lo que es conveniente seguir algunos pasos para asegurarse de que el dispositivo en cuestión no ha sido manipulado antes de su instalación.

4.1 COMPROBACIÓN DE MANIPULACIONES

20. Los dispositivos GigaVUE se envían desde fábrica en una caja sellada. Es conveniente inspeccionar la caja antes de su instalación para asegurarse de que no ha sido abierta y, por tanto, manipulada durante el transporte.

4.2 PEGATINAS ANTI-MANIPULACIÓN

21. La manipulación del dispositivo GigaVUE puede detectarse mediante las pegatinas anti-manipulación que Gigamon proporciona con los equipos. Estas aseguran que cualquier intrusión física en el chasis del dispositivo puede ser fácilmente detectada.

22. Las instrucciones para la correcta colocación de los adhesivos anti-manipulación se proporcionan con los adhesivos, de modo que no se cubran los orificios de aire que pueden afectar negativamente al flujo de aire necesario para enfriar el dispositivo.

Figura 7. Pegatinas anti-manipulación de Gigamon

4.3 DESACTIVACIÓN DEL INTERFAZ SERIE

23. Lo más frecuente es que la instalación de un dispositivo GigaVUE esté alojada en un entorno físicamente seguro; sin embargo, hay situaciones en las que puede resultar necesario desactivar la interfaz en serie cuando el acceso físico no está protegido.

24. Debe tenerse en cuenta que con la interfaz serie activada, aunque el acceso físico es posible, el inicio de sesión en GigaVUE-OS sigue estando sujeto al método de autenticación configurado (es decir, local / TACACS+ / RADIUS).

25. Una de las razones por las que se puede decidir deshabilitar la interfaz serie es que no se puede monitorizar si está conectada o no de la misma manera que se puede monitorizar el puerto de gestión de Ethernet. Este puerto de gestión estará conectado a un conmutador que a su vez puede enviar *Traps SNMP* y/o mensajes *Syslog* para alertarle de cualquier cambio en la conectividad (como por ejemplo que alguien desenchufe el puerto de gestión y conecte un portátil directamente).

26. Otra razón es que una sesión en serie no se cierra cuando se desconecta un puerto en serie. Sin embargo, se puede configurar un tiempo de espera, véase la sección 5.9 CONTROLES DE SESIÓN.

27. Se debe considerar cuidadosamente si es apropiado deshabilitar la interfaz serie. Si se hace y se pierden las credenciales de acceso al dispositivo GigaVUE-OS, no se podrá reiniciar el dispositivo de fábrica y requerirá un *Return Material Authorization* (RMA) que no tendrá costes asociados si se dispone de un contrato de mantenimiento con el fabricante. El procedimiento de RMA permite la solicitud de reemplazo de un equipo por avería, malfuncionamiento o pérdida de prestaciones, como sería este caso según los niveles de servicio descritos aquí.

28. Para deshabilitar el interfaz serie, se usa el comando *"**no serial enable**"*. Al introducir el comando se requiere confirmar el cambio introduciendo 'YES':

```
gigavue-appliance > enable
gigavue-appliance # configure terminal
gigavue-appliance (config) # no serial enable
Disable serial console will make serial connection unusable.
Only use this config command when you have available telnet/ssh
connections.
Enter 'YES' to confirm this operation: YES
Serial Console disabled.
gigavue-appliance (config) #
```

Figura 8. Deshabilitar el interfaz serie

29. El puerto serie estaría ahora deshabilitado. Se puede habilitar de nuevo en cualquier momento usando el mismo comando sin el prefijo "*no*":

```
gigavue-appliance (config) # serial enable
Serial Console enabled.
gigavue-appliance (config) #
```

Figura 9. Habilitar el interfaz serie

30. Más adelante en el documento se recogen las opciones del *IP Filter Firewall* para la interfaz de administración. Se recomienda tener el puerto serie disponible durante esta prueba, ya que puede bloquearse la interfaz de administración si se configura incorrectamente. Si deshabilitar la interfaz serie es un requerimiento, se sugiere que se posponga hasta que haya completado la configuración *del IP Filter Firewall.*

5. CONTROLES DE RED

5.1 REDUCCIÓN DE LA SUPERFICIE DE ATAQUE CON UN FILTRO IP

31. El dispositivo GigaVUE-OS proporciona características del cortafuegos *Linux Netfilter* (alias *'iptables'*) que permite al administrador eliminar las conexiones de red no deseadas recibidas en la interfaz de gestión. Esta configuración no tiene ninguna relación con las conexiones del plano del usuario (es decir, los puertos de red, de herramientas, en línea, etc.), pero proporciona un medio para evitar el acceso no autorizado a la interfaz y desde ella.

5.1.1 BREVE DESCRIPCIÓN DE LOS ELEMENTOS DEL FILTRO IP

32. Aunque el objetivo de este documento no es proporcionar una visión general del cortafuegos de Linux *Netfilter*, es importante comprender algunos principios clave de *Netfilter* en lo que respecta a la función de filtro IP Gigamon.

33. El filtro IP se compone de varias cadenas. Sin embargo, a los efectos de la implementación de Gigamon, solo se utilizan las cadenas *FORWARD*, *INPUT* y *OUTPUT*. Cada una de ellas se utiliza en las siguientes situaciones:

    - ***FORWARD*** se utiliza para el tráfico que se reenvía de una interfaz a otra. En el funcionamiento normal esta cadena no se utiliza. La política por defecto para esta cadena es *DROP*.
    - ***INPUT*** se utiliza para el tráfico que llega a la interfaz y se destina al dispositivo GigaVUE. Este será el foco de la configuración. La política por defecto para esta cadena es *DROP*.
    - ***OUTPUT*** se utiliza para el tráfico que se envía desde el dispositivo GigaVUE. Esto puede ser útil si se desea restringir los sistemas remotos a los que el dispositivo GigaVUE puede acceder (por ejemplo, servidores de *Syslog* remotos o la conexión a servidores *SCP/FTP/HTTP*). La política por defecto para esta cadena es *ACCEPT*.

34. La cadena aplicada a un paquete está determinada por su origen y destino, de modo que, por ejemplo, un usuario que se conecte al dispositivo GigaVUE por SSH tendrá la cadena INPUT (y sus reglas) aplicada a la sesión. Un usuario conectado al Dispositivo GigaVUE que realiza una conexión desde el dispositivo a un sistema remoto (como la transferencia de un archivo desde el dispositivo a un servidor SFTP por ejemplo) tendría la cadena OUTPUT (y sus reglas) aplicada a la sesión.

35. Por lo tanto, para resumir:

    - ***FORWARD:*** Reenvío de paquetes entre redes (no se utiliza).
    - ***INPUT:*** Paquetes destinados al puerto de gestión del dispositivo.
    - ***OUTPUT:*** Paquetes originados en el puerto de gestión del dispositivo.

36. Cada una de las cadenas anteriores tiene un conjunto de reglas que se procesan en orden (de la regla con menor número a la regla con mayor número), como es estándar en una Lista de Control de Acceso (ACL). A veces se hace referencia a esto como una arquitectura de reglas de "*secuencia ordenada*". Cuando un paquete coincide con la regla apropiada dentro de una cadena se aplica el objetivo configurado; este objetivo determina si el paquete será aceptado (*ACCEPT*) o descartado (*DROP*).

37. Por último, hay una política asociada a cada cadena, que puede ser configurada como *ACCEPT* o *DROP*. Esto dicta el comportamiento del Filtro IP en caso de que no se encuentre ninguna coincidencia dentro de las reglas de la cadena y para nuestros propósitos se puede pensar en la "*Regla por defecto*". Por ejemplo, si la política se establece en *DROP*, si no hay coincidencias para los paquetes entrantes en las reglas de la cadena, el paquete será eliminado. Por el contrario, si la política se establece en *ACEPTAR*, si no hay coincidencias para los paquetes entrantes en las reglas de la cadena, el paquete será aceptado.

38. Se debe aplicar una política de denegación (DROP) por defecto para las tres (3) cadenas comentadas anteriormente y posteriormente permitir las comunicaciones deseadas.

5.1.2 ANTES DE EMPEZAR

39. Si no tiene la opción de conectarse al Dispositivo GigaVUE por serie con el propósito de escribir y probar una política, puede determinar desde qué IP se está conectando utilizando el comando mostrar usuarios (***"show users"***), por ejemplo:

```
gigavue-appliance (config) # show users
  USERNAME     REMOTE USERNAME      LINE     HOST              IDLE
* admin                            pts/0    192.168.58.119    0d  0h  0m  0s
gigavue-appliance (config) #
```

Figura 10: Usuarios conectados en el momento

40. En la figura anterior se puede ver que el usuario *admin* está conectado desde la dirección IP 192.168.58.119 (el usuario con el que se ha conectado se indica con el símbolo *), por lo que es prudente verificar la existencia de una norma que permita el tráfico de este usuario. Esta regla puede y debe ser eliminada una vez finalizadas las pruebas. Por ejemplo, para permitir todo el tráfico de esta IP (con fines de prueba) utilizamos el siguiente comando:

```
gigavue-appliance (config) # ip filter chain INPUT rule append tail
target ACCEPT source-addr 192.168.58.119 /32
gigavue-appliance (config) #
```

Figura 11. Aceptar todo el tráfico de la IP del administrador para pruebas

5.1.3 VISUALIZACIÓN DE LA CONFIGURACIÓN ACTUAL DEL FILTRO IP

41. Para mostrar la configuración básica actual (la figura 12 a continuación, muestra el valor por defecto) del Filtro IP se puede utilizar el comando *"**show ip filter configured**"*:

```
gigavue-appliance (config) # show ip filter configured
Packet filtering for IPv4: DISABLED
Apply filters to bridges: no
IPv4 configuration (ignored until filtering is enabled):

Chain 'INPUT'
  #  Target  Proto   Source              Destination         Other
  1  ACCEPT  icmp    all                 all
  2  ACCEPT  igmp    all                 all
  3  ACCEPT  all     all                 all                 state ESTABLISHED,RELATED
  4  ACCEPT  all     all                 all                 inb lo
  5  ACCEPT  all     12.19.148.0/24      all
  6  ACCEPT  all     all                 12.19.148.0/24
Policy: DROP

Chain 'OUTPUT'
  No rules.
Policy: ACCEPT

Chain 'FORWARD'
  No rules.
Policy: DROP
gigavue-appliance (config) #
```

Figura 12. Política de filtro IP por defecto

42. En este caso, la cadena de entrada *INPUT* tiene una política establecida en *DROP*, por lo que, si no hay coincidencia en las reglas anteriores para el paquete, el paquete se eliminará. Hay seis reglas en esta cadena, la función de cada una se describe como:

    1. Acepta todos los paquetes ICMP desde cualquier fuente a cualquier destino.
    2. Acepta todos los paquetes IGMP desde cualquier fuente a cualquier destino.
    3. Acepta todos los paquetes donde haya una sesión establecida o relacionada. Un ejemplo de esto sería la aceptación de paquetes en ambas direcciones de un flujo (por ejemplo, cliente SSH a dispositivo GigaVUE o dispositivo GigaVUE a cliente SSH).
    4. Permite todas las comunicaciones para la interfaz de *loopback* (lo).
    5. Acepta todas las comunicaciones de la subred 12.19.148.0/24 a cualquier destino (el propósito de esta regla se examinará más adelante).
    6. Acepta todas las comunicaciones a la subred 12.19.148.0/24 desde cualquier destino (el propósito de esta regla se examinará más adelante).

43. Las reglas 5 y 6 permiten conexiones desde la subred 12.19.148.0/24, la cual se utiliza internamente dentro del dispositivo GigaVUE para permitir que la consola de administración se comunique con los módulos internos del equipo (otras tarjetas de puertos y la tarjeta GigaSMART). Al ser tráfico interno del equipo nunca alcanzará las interfaces externas con otros sistemas de red.

44. La cadena de salida *OUTPUT* tiene una política establecida para aceptar y, dado que no hay reglas específicas, el paquete será remitido.

45. La cadena *FORWARD* tiene una política establecida para *DROP* y, como no hay reglas específicas, el paquete será descartado.

5.1.4 HABILITAR Y DESHABILITAR LA POLÍTICA DE FILTRO IP

46. En la Figura 12, se observa que la política de Filtros IP está DESHABILITADA, por lo que actualmente permite todas las conexiones y la configuración es la predeterminada.

47. Durante la configuración de la política de filtrado IP es útil activar y desactivar el filtro IP. Para habilitar y deshabilitar el filtro IP, se deben utilizar los siguientes comandos:

```
gigavue-appliance (config) # ip filter enable
WARNING!! Enabling the ipv4/ipv6 filter may impact mgmt and clustering
ports and operations!!.
Enter 'YES' to confirm this operation: YES
gigavue-appliance (config) # no ip filter enable
gigavue-appliance (config) #
```

Figura 13. Habilitar y deshabilitar la política de filtro IP

48. Habilitar y deshabilitar la política es una característica conveniente al escribir y/o probar una política, ya que le permite resolver rápidamente cualquier problema de conectividad; como se ha dicho anteriormente, es prudente tener una sesión de consola en serie abierta, ya que esto evitará que se bloquee el acceso al dispositivo *GigaVUE Appliance*.

5.1.5 AÑADIR UNA REGLA A LA CADENA

49. Para añadir una regla a una cadena, hay tres (3) opciones: "*añadir*", "*insertar*" y "*establecer*".

50. La opción *"añadir"* nos permite añadir una regla al final de la cadena seleccionada, siendo esta la última regla que se evaluará antes de que se aplique la política global de la cadena (por ejemplo, una política establecida en DROP).

51. En la mayoría de los casos, la opción de inserción será adecuada cuando se añadan reglas, ya que permite insertar la regla configurada antes de una regla específica.

52. Por ejemplo, al insertar una regla antes de la regla número 1, la regla se coloca en la parte superior de la cadena y se convierte en la primera regla en ser evaluada por la política. Por ejemplo, si se necesita insertar una regla para permitir SSH (tcp/22) en la parte superior de la cadena INPUT, introduciríamos el siguiente comando:

```
gigavue-appliance (config) # ip filter chain INPUT rule insert 1
target ACCEPT protocol tcp dest-port 22
gigavue-appliance (config) #
```

Figura 14. Insertar una regla en una cadena de filtro IP

53. Por último, la opción "*set*" proporciona un medio para sobrescribir eficazmente la regla existente, lo que resulta útil en caso de que haya que corregir algún error en la configuración de la regla.

54. Por ejemplo, se ha proporcionado accidentalmente acceso a tcp/444 en lugar de tcp/443 para la regla #2, se puede corregir fácilmente de la siguiente manera:

```
gigavue-appliance (config) # ip filter chain INPUT rule set 2 target
ACCEPT protocol tcp dest-port 443
gigavue-appliance (config) #
```

Figura 15. Corregir una regla en una cadena de filtro IP

5.1.6 ELIMINAR UNA REGLA DE UNA CADENA

55. Para eliminar una regla de una cadena, se debe utilizar el prefijo "*no*" para eliminar la regla en cuestión.

56. Por ejemplo, si se quisiera eliminar la regla #1 de la cadena *INPUT*, se utilizaría el siguiente comando:

```
gigavue-appliance (config) # no ip filter chain INPUT rule 1
gigavue-appliance (config) #
```

Figura 16. Eliminar una regla de una cadena

5.1.7 EJEMPLO: RESTRINGIR EL ACCESO A SSH A UNA SUBRED ESPECÍFICA

57. Para dar un ejemplo de la configuración de una política de Filtro IP, se va a restringir el acceso a SSH para permitir sólo las conexiones de la subred "192.168.1.0/24".

58. La configuración inicial es la siguiente:

```
gigavue-appliance (config) # show ip filter configured
Packet filtering for IPv4: DISABLED
Apply filters to bridges: no
IPv4 configuration (ignored until filtering is enabled):

Chain 'INPUT'
  #  Target  Proto   Source            Destination    Other
  1  ACCEPT  icmp    all               all
  2  ACCEPT  igmp    all               all
  3  ACCEPT  all     all               all            state ESTABLISHED,RELATED
  4  ACCEPT  all     all               all            inb lo
  5  ACCEPT  all     12.19.148.0/24    all
  6  ACCEPT  all     all               12.19.148.0/24
Policy: DROP

Chain 'OUTPUT'
  No rules.
Policy: ACCEPT

Chain 'FORWARD'
  No rules.
Policy: DROP
gigavue-appliance (config) #
```

Figura 17. Filtro IP configurado actualmente

59. Se desea añadir una regla a la cadena "*INPUT*" para permitir las conexiones en el puerto 22 de la subred configurada:

```
gigavue-appliance (config) # ip filter chain INPUT rule append
tail target ACCEPT protocol tcp dest-port 22 source-addr
192.168.1.0 /24
gigavue-appliance (config) #
```

Figura 18. Anadir regla para permitir tcp/22 desde 192.168.1.0/24

60. La configuración del Filtro IP quedaría de la siguiente forma:

```
gigavue-appliance (config) # show ip filter configured
Packet filtering for IPv4: DISABLED
Apply filters to bridges: no
IPv4 configuration (ignored until filtering is enabled):
Chain 'INPUT'
  #  Target  Proto   Source              Destination         Other
  1  ACCEPT  icmp    all                 all
  2  ACCEPT  igmp    all                 all
  3  ACCEPT  all     all                 all                 state
ESTABLISHED,RELATED
  4  ACCEPT  all     all                 all                 inb lo
  5  ACCEPT  all     12.19.148.0/24      all
  6  ACCEPT  all     all                 12.19.148.0/24
  7  ACCEPT  tcp     192.168.1.0/24      all                 dpt 22
Policy: DROP
Chain 'OUTPUT'
  No rules.
Policy: ACCEPT
Chain 'FORWARD'
  No rules.
Policy: DROP
gigavue-appliance (config) #
```

Figura 19. Mostrar la regla añadida para permitir tcp/22 desde 192.168.1.0/24

61. Ahora se añade una regla para eliminar el tráfico del puerto 22 que no está en esta subred:

```
gigavue-appliance (config) # ip filter chain INPUT rule append tail target DROP protocol tcp dest-port 22
gigavue-appliance (config) #
```

Figura 20. Anadir una regla *DROP* para todas las otras conexiones tcp/22

62. Ahora la configuración del Filtro IP quedaría de la siguiente forma:

```
gigavue-appliance (config) # show ip filter configured
Packet filtering for IPv4: DISABLED
Apply filters to bridges: no
IPv4 configuration (ignored until filtering is enabled):
Chain 'INPUT'
  #  Target  Proto   Source           Destination   Other
  1  ACCEPT  icmp    all              all
  2  ACCEPT  igmp    all              all
  3  ACCEPT  all     all              all           state
ESTABLISHED,RELATED
  4  ACCEPT  all     all              all           inb lo
  5  ACCEPT  all     12.19.148.0/24   all
  6  ACCEPT  all     all              12.19.148.0/24
  7  ACCEPT  tcp     192.168.1.0/24   all           dpt 22
  8  DROP    tcp     all              all           dpt 22
Policy: DROP
Chain 'OUTPUT'
  No rules.
Policy: ACCEPT
Chain 'FORWARD'
  No rules.
```

```
Policy: DROP
gigavue-appliance (config) #
```

Figura 21. Mostrar la configuración de filtro IP con la regla para descartar el resto de conexiones tcp/22

63. En la configuración detallada en la Figura 21, el filtrado de paquetes para IPv4 está deshabilitado por lo que el último paso sería habilitar la política:

```
gigavue-appliance (config) # ip filter enable
WARNING!! Enabling the ipv4/ipv6 filter may impact mgmt and
clustering ports and operations!!.
Enter 'YES' to confirm this operation: YES
gigavue-appliance (config) #
```

Figura 22. Habilitar la política

64. La política configurada quedaría de la siguiente forma:

```
gigavue-appliance (config) # show ip filter configured
Packet filtering for IPv4: enabled
Apply filters to bridges: no
IPv4 configuration:
Chain 'INPUT'
  #  Target  Proto   Source              Destination         Other
  1  ACCEPT  icmp    all                 all
  2  ACCEPT  igmp    all                 all
  3  ACCEPT  all     all                 all                 state
ESTABLISHED,RELATED
  4  ACCEPT  all     all                 all                 inb lo
  5  ACCEPT  all     12.19.148.0/24      all
  6  ACCEPT  all     all                 12.19.148.0/24
  7  ACCEPT  tcp     192.168.1.0/24      all                 dpt 22
  8  DROP    tcp     all                 all                 dpt 22
Policy: DROP
Chain 'OUTPUT'
  No rules.
Policy: ACCEPT
Chain 'FORWARD'
  No rules.
Policy: DROP
gigavue-appliance (config) #
```

Figura 23. Política de filtro IP habilitada

65. Como se ha mencionado anteriormente, es importante que cualquier regla adicional se coloque después de la regla #3 (como puede verse en el ejemplo de la Figura 23) ya que esto permite que las conexiones establecidas continúen. Sin embargo, recomendamos que todas las reglas adicionales se coloquen después de la política por defecto (es decir, la política tal como existe antes de cualquier edición).

5.2 SECURE SHELL (SSH)

66. Se utiliza SSHv2 para la administración remota de los dispositivos a través del CLI.

67. El uso de un par de claves públicas/privadas de SSH proporciona una alternativa a que el usuario utilice una contraseña para autenticarse y, siempre que la clave

privada se maneje de forma segura, facilita una mayor seguridad a la hora de autenticar a los usuarios.

68. Telnet ya no está soportado por GigaVUE-OS y fue desactivado en la versión 5.7.00.

5.2.1 ESTABLECER UN PAR DE CLAVES PUBLICA/PRIVADA

69. Esta sección detalla las formas en que se puede configurar un par de claves públicas/privadas para su uso con el protocolo SSH y se explican los métodos en Windows y Mac/Linux.

70. Los equipos de Gigamon permiten dos niveles de seguridad, el estándar y el de Criptografía Segura. **Se debe utilizar el modo Criptografía Segura.** En el apartado "5.10 HABILITAR EL MODO DE CRIPTOGRAFÍA SEGURA**"** se muestran los certificados disponibles para cada modo de seguridad.

71. A continuación, se va a detallar un ejemplo en el que se va utilizar la *suite* de código abierto *PuTTY*. Los componentes útiles para para este propósito son:

    - ***PuTTY***: Cliente SSH.
    - ***PuTTYgen***: Generador de parejas de claves SSH Publica/Privada.
    - ***Pageant***: Agente de autenticación SSH para PuTTY.

72. En *PuTTYgen*, se debe seleccionar en el cuadro *Parameters*, una de las siguientes opciones:

    - Tipo de clave a generar **RSA**, con una longitud de clave de **3072** bits o superior.
    - Tipo de clave a generar **ECDSA**, con una longitud de clave de **256 bits** o superior. En caso de habilitar el modo de Criptografía Segura, esta es la única opción posible.

73. Con *PuTTYgen* abierto, seleccionar el botón '*Generar*' de la siguiente manera:

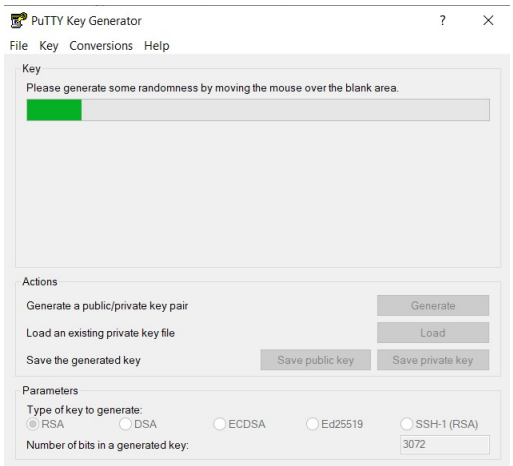

Figura 24. Generación de una clave desde el cliente *PuTTYgen*

74. Esto genera el par de claves SSH, como se muestra en el texto de la siguiente manera:

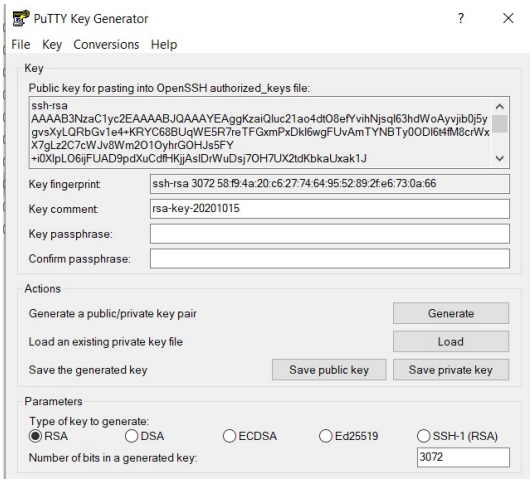

Figura 25. Un par de claves SSH generadas por *PuTTYgen*

75. **Se debe aplicar una contraseña a la clave**, de modo que esta sea requerida para poder utilizar la clave privada de SSH. También existe la opción de añadir un comentario de clave, que es prudente cuando se determina el motivo de la creación de la clave (en este ejemplo se ha utilizado la clave de ejemplo de un dispositivo *gigavue*).

76. Es importante que guardemos la clave pública y, sobretodo, la clave privada utilizando los botones asociados en alguna ubicación donde no puedan ser accedidas por personas no autorizadas.

77. Con la ventana de la figura 25 aún abierta, es nesario copiar la representación de texto de la clave pública para introducirla en la configuración del dispositivo GigaVUE, lo cual se muestra más adelante, en la sección *"5.2.2* AÑADIR UNA CLAVE PUBLICA SSH AL EQUIPO GIGAVUE*"* en el dispositivo GigaVUE.

5.2.1.1 CONFIGURACIÓN APPLE MAC/LINUX

78. El *software* necesario para generar un par de claves públicas/privadas SSH está instalado, por defecto, en una máquina Mac/Linux y se ejecuta emitiendo el comando ***"ssh-keygen"*** en una ventana de terminal. Este comando permite especificar otras opciones como:

    - algoritmo a utilizar: *"**ssh-keygen -t [rsa|dsa|ecdsa]**"*
    - longitud de la clave para rsa: **"ssh-keygen -b [numero de bits]". Se debe hacer uso de una longitud de clave de 3072 o superior.**

79. El siguiente ejemplo se ha seguido en un *Apple Macbook* (las instrucciones son las mismas para los sistemas Linux ya que tanto Mac como Linux usan *OpenSSH*):

```
macbook:~ osheridan$ ssh-keygen –b 3072
Generating public/private rsa key pair.
Enter file in which to save the key
(/Users/osheridan/.ssh/id_rsa):
```

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in
/Users/osheridan/.ssh/id_rsa.
Your public key has been saved in
/Users/osheridan/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:E7mR82fLqI+9gw/dhWZ2S0iauIDmBM3c7OwQh/7rI1U
osheridan@macbook
The key's randomart image is:
+---[RSA 3072]----+
|                 |
|   + +   o       |
|  . * + *   .    |
|   o *  EB + o   |
|    * +.S + O +  |
|   + +.. + X = . |
|    ..o o.o + .  |
|    . ...=.      |
|     oo.oo=o     |
+----[SHA256]-----+
macbook:~ osheridan$
```

Figura 26. Generación de par de claves publica/privada en un equipo Apple Macbook

80. Como se puede observar en la figura 26, el comando permite la posibilidad de introducir una contraseña para asegurar la clave privada de SSH si desea hacerlo. **Debe configurarse la utilización de una contraseña para la protección de la clave privada SSH.**

81. La clave pública se almacenará (si se aceptan los valores predeterminados) en el archivo *~/.ssh/id_rsa.pub.* Esta puede visualizarse utilizando el comando *"cat"*:

```
macbook:~ osheridan$ cat ~/.ssh/id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDE5qJBPDHVNvtLCYUasKodyTh3i0sR7HWhwmlGl91GE
amxwTM5xD21IIdgZY7jJ4Prew7UnFT73+vA8n56cGWdPMq11rXuqtMWUBQEDXTDDAMnj4Qrvi
NQWaS6/qU0+WoQ+Ss/dx6yhv3FQTsPVeChI5Zorw0orqdO9V5dCIPaAI2rZv8B1NXwOFXS8Oq
ejJC0ThV7PkFVkT0VDXlHOfWHOIk30BvTgU+06l/niiTN3DjcyHcfQfFxUAF+Yhm5h5l/FlFD
lERjfWJx+AKK9O8MqKb1l3p3hvxBW8lz4gf3q4mwDXsDN4rUkqnRc8ZghsXgi3svAiLgYoZ4x
DCijvzR osheridan@macbook
macbook:~ osheridan$
```

Figura 27. Mostrar la clave pública SSH en un *Apple Macbook*

82. Es necesario dar de alta esta cadena en el dispositivo GigaVUE, como se detalla en la siguiente sección.

5.2.2 AÑADIR UNA CLAVE PUBLICA SSH AL EQUIPO GIGAVUE

83. Se hace uso del siguiente comando para añadir la clave pública al usuario "*admin*":

```
gigavue-appliance (config) # ssh client user admin authorized-key sshv2
"ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAi5q9749zQt04ZpaaaGUy0lN5+sF+KVsONKdwWMez4YQtF
nsmgMFdQd1mdR7x412w42YI/ZLdwqJh5fXN/vskRje7qlBoQLLUvhiVxM5vh1SJdmsFeG+gWR
MJYO+hiH8sObju8VlwMgGTM+5lPe5VIY61RJKd/mPs+wwOzLY1a3b1mdUDzvmDnQpkPT7Xwxx
8uu+89302DpnjRzhopiXw927S6TNXOP4DDF42wbFwV8Pwdtbra6FGCO5FW8N/jcUClSLqH77B
```

```
xGU9G4ips8mxUdYnRCcclOO7l3XOZDc3ja7oguGk1cwA+V8lmpuzf3Jf/qmrKP1tGAN05Xrxe
MlXZw== gigavue-appliance example key"
gigavue-appliance (config) #
```

Figura 28. Añadir clave SSH al equipo

84. Debido a los espacios en la clave pública de SSH, la cadena está entrecomillada. La cadena incluida es la obtenida y copiada en el apartado 5.2.1 ESTABLECER UN PAR DE CLAVES PUBLICA/PRIVADA.

5.2.3 MOSTRAR LAS CLAVES PÚBLICAS SSH

85. Para mostrar todas las claves públicas SSH, se puede usar el comando ***"show ssh client",*** tal como se muestra a continuación:

```
gigavue-appliance (config) # show ssh client
SSH client Strict Hostkey Checking: ask
No SSH global known hosts configured.
No SSH user identities configured.
SSH authorized keys:
  User admin:
    Key 1: ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAi5q9749zQt04ZpaaaGUy0lN5+sF+KVsONKdwWMez4YQtF
nsmgMFdQd1mdR7x412w42YI/ZLdwqJh5fXN/vskRje7qlBoQLLUvhiVxM5vh1SJdmsFeG+gWR
MJYO+hiH8sObju8VlwMgGTM+5lPe5VIY61RJKd/mPs+wwOzLY1a3b1mdUDzvmDnQpkPT7Xwxx
8uu+89302DpnjRzhopiXw927S6TNXOP4DDF42wbFwV8Pwdtbra6FGCO5FW8N/jcUClSLqH77B
xGU9G4ips8mxUdYnRCcclOO7l3XOZDc3ja7oguGk1cwA+V8lmpuzf3Jf/qmrKP1tGAN05Xrxe
MlXZw== gigavue-appliance example key
gigavue-appliance (config) #
```

Figura 29. Mostrar las claves públicas SSH

5.2.4 REVOCAR/ELIMINAR UNA CLAVE PUBLICA DEL EQUIPO GIGAVUE

86. Las claves públicas SSH también puede ser eliminadas de un equipo. A continuación, se muestra un ejemplo de revocación de la clave de *admin@linux* (key 1):

```
gigavue-appliance (config) # no ssh client user admin authorized-key
sshv2 1
gigavue-appliance (config) # show ssh client
SSH client Strict Hostkey Checking: ask
No SSH global known hosts configured.
No SSH user identities configured.
SSH authorized keys:
  User admin:
    Key 2:
AAAAB3NzaC1yc2EAAAADAQABAAABAQD32742EFYNsKTRZtGBmd6VT+/tFG/j2fM3UDGWDnhzw
e68LzDNCO0tWDzXVqiZc9Gf1TIFK8qEq2vuSi4evvLjTrvbdyqjmv4GX1DiOYhyUYnw77DqcM
RS7Jnf4py5DBZRHPsdUIp6xKpqvRs6PEXIK8CET09IXirHRKDmfDfgHo8KEhbdvBlLuUVFrWP
ZQLjea9iZlRUf+CdHrda1GI0OKdE6Ad3Xsc38loN1bMq9ka+5zaquWUrwhLZQeT/FUgpj58Ns
gebvBD8PcilvekvrbEmL7HlnEnoQGFUKQiFHXetJk7sW2PBvz5o/uN2ZtWrwgKRslRGrFocue
Sc675NH osheridan@workstation
gigavue-appliance (config) #
```

Figura 30. Eliminar una clave SSH autorizada

87. Cuando se eliminan claves, los números de las claves no se renumeran. Es decir, la clave 2 no se convierte en la clave 1 cuando se borra la clave 1.

5.2.5 INSTALAR CLAVES SSH PARA ACCEDER A OTROS RECURSOS SSH/SCP/SFTP

88. Cuando se descarga una imagen para actualizar un dispositivo GigaVUE (ver apartado 5.12 ACTUALIZACIÓN DEL PRODUCTO) hay varios protocolos que pueden utilizarse para este fin, a saber:

    - *HTTP*
    - *HTTPS*
    - *FTP*
    - *TFTP*
    - *SCP*
    - *SFTP*

89. **No se debe hacer uso de los protocolos HTTP, FTP y TFTP por considerarse inseguros.**

90. Par evitar su uso, se puede utilizar el IP, como se describe en la sección anterior 5.1 REDUCCIÓN DE LA SUPERFICIE DE ATAQUE CON UN FILTRO IP.

91. Cuando se utiliza SCP o SFTP se debe utilizar pares de claves públicas/privadas.

92. Tenga en cuenta que también se utilizan los pares de claves públicas/privadas SSH si desea cifrar los datos del *syslog*. Este procedimiento se detalla en el apartado "6.3.1 ENVÍO DE LOGS A UN SERVIDOR *SYSLOG* REMOTO A TRAVÉS DE UN CANAL SEGURO.".

5.2.6 GENERACIÓN DE UNA CLAVE PÚBLICA DE IDENTIDAD

93. La criptografía asimétrica es el método criptográfico que usa un par de claves para el envío de información. Las dos claves están relacionadas matemáticamente y son necesarias ambas para poder cifrar y descifrar las comunicaciones. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. La ventaja de este sistema es que la información cifrada con la clave privada solo podrá descifrarse con la clave pública y la cifrada con la clave pública a su vez solo podrá descifrarse con la privada.

94. Para generar una clave pública de identidad, utilizada para las **conexiones salientes del Dispositivo GigaVUE**, donde la clave privada (interna del Dispositivo GigaVUE) debe utilizarse para autenticar la conexión, se utiliza el comando ***"ssh client user admin identity rsa2 generate".***

```
se-reading-hc1-01 (config) # ssh client user admin identity rsa2 generate
se-reading-hc1-01 (config) # show ssh client
SSH client Strict Hostkey Checking: ask
No SSH global known hosts configured.
User Identities:
```

```
  User admin:
    RSAv2 Public key:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDFDXa1pgt1jbM+ovyBWs8AGPPlZRm4Nksg1jKUDsDSn
+bPomeH9HoxJ8Wrp7gGcCyAvkjadskd/z3jQALJikKIYfYu5DYsRdCdLuuFN3hr9OEcf4Sotd
eIkr8dBbHV8SMqN4CNf3GN4ROHnlxOPqYD/NnP9m70nvM4JquTqIqmjE7VPrgWqq4ufn+c/Gk
Y4BaAMGvlD8zeapuOsXV3nnkbu4TJOASyPW0GkOzMMN+sIKzqZXqtQMNJP12BxHOt2boamqAG
RODOqu1euh5SY71jnQdR+PeiiD3nvvvveg4q1DuRhoYiEnyEbxnzZxs32/Wv4qE2zb9BTHOKr
PqIg2kJ
    RSAv2 Private key:
********
    Passphrase:
********

SSH authorized keys:
  User admin:
    Key 1: ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQD3/bVlsAltZJvjfvU2sZGGZk9dJw74q4YlHQtPwD8F5
H4MYtV6Cieb5wp2bGtNZuDAfIampQPA4HZWWTyvekbdba8IgTfIUgmeydX91J0JuPKspxUHIW
eUS2O2yJxRjJ9r2rqs2sFHZfxu8Cf51wusTiE+xJydBCfv+TIU12345678rJueADrxDpwb1gQ
6EG3PS6bc7+k2PGOJP+GaI9HbhcjxlKLIcP5FsdPHnbptS1TQPljXN0QJTuWBIdE7QiFZBXWI
HD1QRqhqK5WJZ6S1C++bUXvQFmqBd4B4LEQu0Yyllwx3zxzo6lkOMGkjKHU6Lmwb+0iDyvD5Q
87+c8RH admin@remote
se-reading-hc1-01 (config) #
```

Figura 31. Muestra de clave de identidad SSH para el usuario *admin*

95. En la Figura 31 se muestra la clave pública RSAv2 para el usuario *admin*. Esta información es necesaria para añadir a las claves autorizadas en el sistema remoto, que para la mayoría de los sistemas será el archivo *~username/.ssh/authorized_keys* en el directorio principal del usuario.

96. En dicha Figura también se observa la existencia de una sección de claves autorizadas (*SSH authorized keys*) que **se utilizan para autenticar al dispositivo GigaVUE**.

5.3 TRANSPORT LAYER SECURITY (TLS)

97. Se utiliza TLS, por defecto, para proteger cualquier interfaz de gestión con sistemas externos, siendo estos:

    - Interfaz de gestión Web (HTTPS).
    - Interfaz de SNMP. Si se utiliza, **se debe utilizar SNMPv3.**
    - Interfaz de LDAP. Si se utiliza, se **debe utilizar *secureLDAP*.**

98. Cabe señalar que esto no se relaciona con la configuración de iSSL (descifrado SSL en línea) o SSL fuera de banda (descifrado SSL pasiva fuera de banda) y hace referencia específicamente a la gestión del dispositivo GigaVUE-OS.

99. La configuración de las características iSSL y SSL fuera de banda GigaSMART están fuera del alcance de este documento.

5.3.1 INSTALAR SU PROPIO CERTIFICADO

100. Para instalar su propio certificado, hay dos (2) métodos:

    1. Instalar un certificado y clave privada ya creados.
    2. Instalar un certificado en base a una petición de firma de certificado, *Certification Signing Request (CSR).*

5.3.1.1 INSTALACIÓN DE UN CERTIFICADO Y CLAVE PRIVADA EXISTENTES

101. Si ya se dispone de un certificado y una clave privada, se puede instalar en el dispositivo GigaVUE de la siguiente manera (la sección eliminada se indica con [TRUNCATED]):

```
gigavue-appliance (config) # crypto certificate name gigavue-appliance
public-cert pem "
> -----BEGIN CERTIFICATE-----
> MIIEdjCCA16gAwIBAgIIa6thcUvlstEwDQYJKoZIhvcNAQELBQAwgbYxCzAJBgNV
[TRUNCATED]
> ZrT24HNNYaVhz2ExbJ3gOKrLil1aArvYcVDJ0EIZ7j9SGleE/seLwHW8
> -----END CERTIFICATE-----"
Successfully installed certificate with name 'se-reading-hc1-01'
gigavue-appliance (config) #
```

Figura 32. Aplicar un certificado ya existente

102. A continuación, se añade la clave privada al dispositivo GigaVUE de la siguiente manera (la sección eliminada se indica con [TRUNCATED]):

```
gigavue-appliance (config) # crypto certificate name gigavue-appliance
private-key pem "
> -----BEGIN RSA PRIVATE KEY-----
> MIIEogIBAAKCAQEA3KQVZvo00RiEY0QMYgH4BKttV8Z4D46FE5pOVsJ44WzJq1Bd
[TRUNCATED]
> rRQX8b+0k1IXVHfAihBv3LuFMGM1mknagKdBJwrtybKZdoX5V+A=
> -----END RSA PRIVATE KEY-----"
Enter private key passphrase (if required):
gigavue-appliance (config) #
```

Figura 33. Introducción de clave privada en el alta de un certificado ya existente

103. A continuación, se activa el certificado:

```
gigavue-appliance (config) # web https certificate name se-reading-hc1-
01
gigavue-appliance (config) #
```

Figura 34. Activación del certificado

104. Para ver los certificados cargados, se puede hacer uso del comando "***show cryto certificate***":

```
gigavue-appliance (config) # show crypto certificate
Certificate with name 'se-reading-hc1-01'
    Private Key:                    present
    Serial Number:                  0x6bab61714be5b2d1
    SHA-1 Fingerprint:
1b2d5977897b76dc59fb1b2c2ea4f058af1f818b
```

```
    Validity:
        Starts:                     2019/06/11 14:35:00
        Expires:                    2020/06/10 14:35:00
    Subject:
        Common Name:                se-reading-hc1-01
        Country:                    UK
        State or Province:          Berkshire
        Locality:                   Reading
        Organization:               Gigamon UK Ltd.
        Organizational Unit:        SE Reading Lab
        E-mail Address:             ollie.sheridan@gigamon.com
    Issuer:
        Common Name:                SE-READING-LAB-INTERMEDIATE-CA
        Country:                    UK
        State or Province:          Berkshire
        Locality:                   Reading
        Organization:               Gigamon UK Ltd.
        Organizational Unit:        SE Reading Lab
        E-mail Address:             ollie.sheridan@gigamon.com

Certificate with name 'system-self-signed' (default-cert)
    Comment:                        system-generated self-signed
certificate
    Private Key:                    present
    Serial Number:                  0x545bb39fcf477301d578279ee4c91727
    SHA-1 Fingerprint:
66fb98bea3effd3a1ce96d658c25a28bc21077d5

    Validity:
        Starts:                     2020/06/27 08:48:38
        Expires:                    2021/06/27 08:48:38

    Subject:
        Common Name:                se-reading-hc1-01
        Country:                    US
        State or Province:          California
        Locality:                   Santa Clara
        Organization:               Gigamon Inc.
        Organizational Unit:        Gigamon Network Visibility Systems
        E-mail Address:             admin@gigamon.com

    Issuer:
        Common Name:                se-reading-hc1-01
        Country:                    US
        State or Province:          California
        Locality:                   Santa Clara
        Organization:               Gigamon Inc.
        Organizational Unit:        Gigamon Network Visibility Systems
        E-mail Address:             admin@gigamon.com
```

Figura 35. Ejemplo de muestra información sobre los certificados cargados en el equipo

5.3.1.2 CREACIÓN DE UN CSR PARA CERTIFICADOS INCORPORADOS Y CLAVES PRIVADAS

105. En lugar de utilizar un certificado y una clave privada generados previamente, hay ocasiones en que es preferible generar una solicitud de firma de certificado (CSR). Cabe señalar que cada vez que se genera una CSR, se crea una nueva clave privada.

106. Para crear y cargar un certificado a través de CSR:

```
gigavue-appliance (config) # crypto cert-req-msg generate upload
scp://seadmin@10.60.20.67/home/seadmin/
Password (if required): ************
Enter private key passphrase (if required):
Successfully uploaded certificate signing request with name 'cert-req-
ZhWICv.csr'
Successfully uploaded private key with name 'cert-req-ZhWICv.key'
gigavue-appliance (config) #
```

Figura 36. Creación de un CSR

107. El procedimiento anterior carga tanto el CSR como la clave privada, por lo que debe asegurarse de que el sistema receptor de la solicitud es lo suficientemente seguro antes de realizar este procedimiento.

108. De este modo, el administrador del certificado dispondrá de la información necesaria para elaborar un certificado firmado por su entidad certificadora, que podrá aplicarse al dispositivo Gigamon según las instrucciones de la sección anterior.

109. Hay más opciones disponibles para un CSR. Para consultarlas, se puede acceder a la Guía del Usuario (REF1).

5.3.2 CONFIGURACIÓN DE VERSIÓN DE TLS PARA EL INTERFAZ DE GESTIÓN

110. **Se debe utilizar TLS1.2 en la interfaz de gestión GUI**. Las versiones anteriores se consideran inseguras.

```
gigavue-appliance (config) # web server ssl min-version ?
tls1            Require TLSv1 or higher
tls1.1          Require TLSv1.1 or higher
tls1.2          Require TLSv1.2 or higher
gigavue-appliance (config) #
```

Figura 37. Opciones para establecer la versión mínima de TLS

111. Para configurar el dispositivo Gigamon para que utilice una versión mínima de TLS1.2, se debe introducir el siguiente comando:

```
gigavue-appliance (config) # web server ssl min-version tls1.2
gigavue-appliance (config) #
```

Figura 38. Establecimiento de la versión mínima de TLS a TLS1.2

5.4 BANNERS

112. Los equipos de Gigamon permiten configurar un banner que se mostrará durante el proceso de acceso a los equipos, siendo esto posible a través de:

- Terminal.
- SSH.
- Web (GUI).

5.5 BANNER PRE-LOGIN (POR DEFECTO)

113. **Se debe configurar un *banner* previo al inicio de sesión que suministre información sobre las políticas de seguridad definidas en la organización**.

114. El *banner* aparece en la pantalla de inicio de sesión:

- Para accesos de línea de comandos (Terminal y SSH) esto será después de que se haya introducido el nombre de usuario, pero antes de que se introduzca la contraseña. Esto se debe tener en cuenta para no incluir en el banner información sensible sobre el dispositivo o la red en el que está desplegado.
- Para accesos WEB, será justo después de la pantalla de inicio mediante un pop-up.

115. En el texto del *banner* se pueden utilizar varias líneas y la cadena se encapsula entre comillas:

```
gigavue-appliance (config) # banner login "Property of Gigamon,
authorised users only"
```

Figura 39. Añadir un banner *pre-login*

5.5.1 BANNER LOCAL

116. Este tipo de banner sustituye al *banner* por defecto y se mostrará solo para accesos locales (terminal).

117. De nuevo, el banner puede estar formado por varias líneas. La cadena debe estar encapsulada entre comillas, como en el siguiente ejemplo:

```
gigavue-appliance (config) # banner login-local "Property of Gigamon,
authorised users only"
```

Figura 40. Añadir un *banner login* local

5.5.2 BANNER REMOTE

118. Este tipo de *banner* sustituye al *banner* por defecto y se mostrará solo para accesos remotos (ssh y web).

119. Igual que en los casos anteriores, puede estar compuesto por varias líneas y la cadena debe estar encapsulada entre comillas, como en el siguiente ejemplo:

```
gigavue-appliance (config) # banner login-remote "Property of Gigamon,
authorised users only"
```

Figura 41. Añadir un *banner remote* local

5.5.3 BANNER POST LOGIN

120. Se debe configurar un *banner* de acceso al equipo que proporcione detalles adicionales de los que se desee informar a los usuarios **después de que hayan entrado** en el sistema.

121. Se pueden utilizar varias líneas, de la misma manera que con el *banner* de Pre-entrada.

```
gigavue-appliance (config) # banner motd "Please observe change
control processes"
```

Figura 42. Anadir un banner *post login*

5.6 CONTROL DE ACCESO BASADO EN ROLES

122. Gigamon proporciona opciones granulares para el Control de Acceso Basado en Roles (RBAC) en el dispositivo GigaVUE. Los pasos necesarios para configurar el RBAC pueden resumirse en:

- Crear un usuario.
- Crear roles.
- Asignar roles a usuarios específicos.
- Usar los roles para permitir accesos y privilegios. Estos aplican a:
  - Puertos: cada una de las interfaces del equipo.
  - Mapas: cada una de las reglas de filtrado de tráfico existentes en uno o varios puertos.

123. Se recomienda, antes de configurar los roles y aplicarlos a los usuarios, puertos y mapas, tener una idea clara de lo que se desea conseguir aplicando RBAC.

5.6.1 NIVELES DE ACCESO A PUERTOS

124. El acceso a los puertos del dispositivo GigaVUE se divide en cinco (5) niveles, que se describen en el siguiente cuadro:

Permisos	Nivel1	Nivel2	Nivel 3	Nivel 4	Admin
Ver Puerto	✔	✔	✔	✔	✔
Ver mapas asociados a un Puerto de red	✔	✔	✔	✔	✔
Crear/Editar Mapas asociados a un puerto	✘	✔	✔	✔	✔

Crear *tool-mirror* a/desde un Puerto	✗	✓	✓	✓	✓
Cambiar filtros de salida	✗	✓	✓	✓	✓
Editar parámetros de puertos	✗	✗	✓	✓	✓
Crear pares de puertos	✗	✗	✓	✓	✓
Cambiar tipo de puerto	✗	✗	✗	✓	✓

Figura 43. Tabla detallada de niveles de acceso a puertos

125. Los niveles de acceso a los puertos dictan los diferentes permisos disponibles para los roles cuando se aplican a una configuración de puertos. En la creación de un rol se podrá especificar el acceso a cada puerto por separado o un subconjunto de los cinco niveles. De esta manera se podría definir exactamente el acceso a cada uno de los puertos del equipo. A modo de ejemplo se podría definir:

- Rol_1 -> Acceso Nivel 1 a los puertos 1/1/x1 y 1/1/x2 y acceso *admin* a los puertos 1/1/x3 y 1/1/x4
- Rol_2 -> Acceso *admin* a los puertos 1/1/x1 y 1/1/x2 y acceso Nivel1 a los puertos 1/1/x3 y 1/1/x4

126. Con esta configuración el Rol_1 sería el administrador de los puertos 1/1/x3 y 1/1/x4 pero no podría configurar nada en los puertos 1/1/x1 y 1/1/x2. Por otro lado, el Rol_2 sería el administrador de los puertos 1/1/x1 y 1/1/x2 pero no podría cambiar nada en los puertos 1/1/x3 y 1/1/x4.

5.6.2 MAP BASED ACCESS LEVELS

127. El acceso a los mapas del dispositivo GigaVUE se divide en cuatro (4) niveles, que se describen en la siguiente tabla:

Permisos	Solo lectura *"view_roles"*	Escucha *"listen_roles"*	Leer/Escribir *"edit_roles"*	Leer/Escribir/Propietario *"owner_roles"*
Ver Mapa	✓	✓	✓	✓
Añadir puerto de herramienta	✗	✓	✓	✓
Eliminar puerto de herramienta	✗	✓	✓	✓
Eliminar puerto de red	✗	✗	✓	✓
Añadir puerto de red	✗	✗	✓	✓
Eliminar/Editar Mapa	✗	✗	✓	✓
Compartir mapa	✗	✗	✓	✓

Figura 44. Tabla detallada de niveles de acceso a mapas.

128. Estos niveles de acceso basados en el mapa dictan los diferentes permisos disponibles para los roles cuando se aplican a una configuración del mapa.

129. La lógica a aplicar es la descrita en el apartado anterior respecto a los niveles de los puertos, pero aplicado a los mapas.

5.6.3 ENTENDER LOS ROLES

130. Los roles permiten agrupar a los usuarios para aplicar privilegios globales a los mapas y puertos. Los roles configurados por defecto son:

    - ***Admin***: los usuarios asignados a este rol tienen un acceso completo a la configuración. Este rol provee acceso a todos los modos de comando, incluyendo *Estándar*, *Habilitar* y *Configurar* y también a todos los comandos y puertos. Pueden ser considerados como miembros de todos los roles.
    - ***Monitor***: Los usuarios asignados a este rol sólo tienen acceso de vista a los puertos y configuraciones.
    - ***Default***: Este rol también proporciona acceso a todos los modos de comando. Los usuarios con este rol no tienen acceso a los puertos no asignados. Los nuevos usuarios se crean automáticamente con este rol.

131. Estos roles y sus características vienen configurados por defecto y no pueden ser eliminados o modificados.

132. Para listar los usuarios de un sistema y su estado, se puede utilizar el comando ***"show usernames"***:

```
gigavue-appliance (config) # show usernames
USERNAME     FULL NAME                ACCOUNT STATUS
admin        Administrator            Password set
monitor      System Monitor           Account locked out
operator     System Operator          Account locked out
osheridan    Ollie Sheridan           Password set
pmortimer    Paul Mortimer            Password set
gigavue-appliance (config) #
```

Figura 45. Mostrar usuarios

133. A continuación, a modo de ejemplo, se desea añadir un usuario *osheridan* al rol de seguridad (mediante el rol *Security*) y el usuario *pmortimer* al rol de gestor de red (mediante un rol *Network*). Se asume que estos usuarios ya han sido creados.

    – En primer lugar, se visualiza el listado de roles actualmente asignados, usando el comando "***show roles assignment all***":

```
gigavue-appliance (config) # show roles assignment all

 Role                    : monitor
 Type                    : normal
 Users                   : monitor,osheridan,pmortimer
 Level-1 Port(s)         : -
 Level-2 Port(s)         : -
 Level-3 Port(s)         : -
 Level-4 Port(s)         : -
```

```
 Role                    : admin
 Type                    : admin
 Users                   : admin,osheridan,pmortimer
 Level-1 Port(s)         : -
 Level-2 Port(s)         : -
 Level-3 Port(s)         : -
 Level-4 Port(s)         : -

 Role                    : Default
 Type                    : normal
 Users                   : -
 Level-1 Port(s)         : -
 Level-2 Port(s)         : -
 Level-3 Port(s)         : -
 Level-4 Port(s)         : -
gigavue-appliance (config) #
```

Figura 46. Mostrar los roles configurados

– En la figura anterior, también se proporciona información sobre los niveles asignados a cada usuario. Otra forma de mostrar los roles en un formato conciso es usar el comando ***"show roles":***

```
gigavue-appliance (config) # show roles
================================================
Role          Description                User(s)
------------------------------------------------
monitor                                  monitor,osheridan,pmortimer
admin                                    admin,osheridan,pmortimer
Default                                  -
gigavue-appliance (config) #
```

Figura 47. Mostrar los roles en formato conciso

– Se puede observar que es necesario crear los roles deseados ("*Network*" y "*Security*"). Para esto, se hace uso del comando ***"aaa authorization roles role":***

```
gigavue-appliance (config) # aaa authorization roles role
Network description "Networking Team"
gigavue-appliance (config) # aaa authorization roles role
Security description "Security Team"
gigavue-appliance (config) # show roles
================================================
Role          Description                User(s)
------------------------------------------------
monitor
monitor,osheridan,pmortimer
admin
admin,fmadmin,osheridan,pmo...
Security      Security Team              -
Default                                  -
Network       Networking Team            -
gigavue-appliance (config) #
```

Figura 48. Añadir los roles de red y seguridad

– Una vez agregados los roles, se deben asociar a los usuarios.

```
gigavue-appliance (config) # username osheridan roles add
Security
gigavue-appliance (config) # username pmortimer roles replace
Network
gigavue-appliance (config) # show roles
================================================
Role          Description                 User(s)
------------------------------------------------
monitor                                  monitor,osheridan
admin                                    admin,osheridan
Security      Security Team              osheridan
Default                                  -
Network       Networking Team            pmortimer
```

Figura 49. Añadir usuarios a sus respectivos roles

– En la Figura 49 se han usado las opciones de comando:

- ***roles add:*** para el usuario *osheridan*. Esta opción añade el rol deseado al usuario, sin modificar los otros roles ya asignados a dicho usuario.
- ***roles replace*****:** para el usuario *pmortimer*. Esta opción sobrescribe los roles asignados al usuario, quedando asignado de esta forma solo al rol indicado.

134. Al crear un mapa dentro del dispositivo GigaVUE, es importante entender que el mapa tendrá definido, dentro del campo "roles", todos los roles que tenga el usuario que creó el mapa, a menos que se especifique lo contrario en el campo ***"owner_role"*** del mapa. Por ejemplo, el usuario *osheridan* crea un mapa:

```
gigavue-appliance (config) # map alias SECURITY_ROLE_RULE
gigavue-appliance (config map alias SECURITY_ROLE_RULE) # from 1/1/g1
gigavue-appliance (config map alias SECURITY_ROLE_RULE) # to 1/1/x1
gigavue-appliance (config map alias SECURITY_ROLE_RULE) # rule add
pass vlan 123
gigavue-appliance (config map alias SECURITY_ROLE_RULE) # exit
gigavue-appliance (config) # show run map alias SECURITY_ROLE_RULE
##
## Running database "RBAC_Example"
## Generated at 2020/07/04 09:24:47 +0100
## Software version on which this output was taken: GigaVUE-OS 5.9.00
172922 2020-04-01 08:03:25
## Hostname: se-reading-hc1-01
##
## Traffic map connection configurations
##
map alias SECURITY_ROLE_RULE
  type regular byRule
  roles replace Security,admin,monitor to owner_roles
  rule add pass vlan 123
  to 1/1/x1
  from 1/1/g1
  exit
```

Figura 50. El usuario *osheridan* crea un mapa. Roles aplicados por defecto

135. Se observa que el mapa se ha creado con éxito, con todos los roles que tiene el usuario *osheridan* (*Security, Admin* y *Monitor).*

136. Si se deseara crear un mapa con el usuario *pmortimer (*miembro del rol de *Network* exclusivamente*)* no se podría ya que no se puede crear un mapa que contenga puertos a los que el rol asignado no tenga acceso.

```
gigavue-appliance (config) # map alias NETWORK_ROLE_RULE
gigavue-appliance (config map alias NETWORK_ROLE_RULE) # from 1/1/g1
gigavue-appliance (config map alias NETWORK_ROLE_RULE) # to 1/1/x1
gigavue-appliance (config map alias NETWORK_ROLE_RULE) # rule add pass
vlan 321
gigavue-appliance (config map alias NETWORK_ROLE_RULE) # exit
% Insufficient authorization to make change:
[Create Map] Required level 2+ for port(s): '1/1/g1'.
Command failed.
gigavue-appliance (config) #
```

Figura 51. Creación de un mapa con un usuario sin rol de administrador

137. Es importante destacar que un mapa tiene dos (2) tipos de puertos. Por un lado, están los puertos de entrada llamados **"Puertos de Red"** y por otro lado los puertos de salida llamados **"Puertos de Herramientas".**

138. Para que el usuario *pmortimer* cree un mapa, se deben realizar las siguientes acciones:

- Verificar que tiene los permisos suficientes para ambos puertos: el de Red y el de Herramientas. En primer lugar, se verifica el puerto de red (en este ejemplo 1/1/g1). Para ello, consultando los Controles de Acceso a los Puertos (ver sección anterior con la tabla asociada, figura 43), se puede determinar que, como mínimo, se requiere el Nivel 2 para *"Crear/Editar Mapas asociados a un puerto"*. Por lo tanto, será necesario añadir permisos de, al menos, Nivel 2, al rol *Network* para el puerto 1/1/g1.

- Como el usuario *osheridan* (que tiene el rol de administrador asignado) se puede hacer este cambio. Se añade al rol *Network* al Nivel 2 para el puerto 1/1/g1, lo que permitirá la creación/edición del mapa asociado a dicho puerto a los usuarios con rol *Network*:

```
gigavue-appliance (config) # port 1/1/g1 assign role Network level 2
gigavue-appliance (config) # show port assignment port-list 1/1/g1

 Port                  : 1/1/g1
 Level-1 Role(s)       : -
 Level-2 Role(s)       : Network
 Level-3 Role(s)       : -
 Level-4 Role(s)       : -
 Lock                  : -
 Lock Description      : -
 Lock-Share(s)         :
```

Figura 52. El usuario *osheridan* cambia el rol asignado sobre el puerto 1/1/g1

- De nuevo, el usuario *pmortimer* intenta configurar el mapa:

```
gigavue-appliance (config) # map alias NETWORK_ROLE_RULE
gigavue-appliance (config map alias NETWORK_ROLE_RULE) # from 1/1/g1
```

```
gigavue-appliance (config map alias NETWORK_ROLE_RULE) # to 1/1/x1
gigavue-appliance (config map alias NETWORK_ROLE_RULE) # rule add pass vlan
321
gigavue-appliance (config map alias NETWORK_ROLE_RULE) # exit
% Insufficient authorization to make change:
[Create Map] Required level 2+ for port(s): '1/1/x1'.
Command failed.
```

Figura 53. El usuario *pmortimer* intenta de nuevo añadir un mapa

– En la Figura 53, se observa que se ha vuelto a denegar la acción. Esta vez es debido a que no hay suficientes derechos en el puerto de herramientas, 1/1/x1. Por lo tanto, el usuario *osheridan* vuelve a cambiar los derechos:

```
gigavue-appliance (config) # port 1/1/x1 assign role Network level 2
gigavue-appliance (config) # show port assignment port-list 1/1/x1

 Port                    : 1/1/x1
 Level-1 Role(s)         : -
 Level-2 Role(s)         : Network
 Level-3 Role(s)         : -
 Level-4 Role(s)         : -
 Lock                    : -
 Lock Description        : -
 Lock-Share(s)           :
```

Figura 54. Asignación de privilegios de nivel 2 al rol de *Network* sobre el puerto 1/1/g1

– El usuario *pmortimer* ya puede crear el mapa con éxito, ya que pertenece al rol *Network*, el cual tiene ahora Nivel 2 en ambos puertos:

```
gigavue-appliance (config) # map alias NETWORK_ROLE_RULE
gigavue-appliance (config map alias NETWORK_ROLE_RULE) # from 1/1/g1
gigavue-appliance (config map alias NETWORK_ROLE_RULE) # to 1/1/x1
gigavue-appliance (config map alias NETWORK_ROLE_RULE) # rule add pass vlan
321
gigavue-appliance (config map alias NETWORK_ROLE_RULE) # exit
gigavue-appliance (config) #
```

Figura 55. Configuración exitosa del mapa por el usuario *pmortimer*

139. El establecimiento de roles y la autorización de funciones y servicios a los usuarios debe realizarse de acuerdo al **principio de mínimo privilegio**, ya que así se evitaría la supervisión no autorizada del tráfico de la red.

5.7 DISMINUCIÓN DE LOS PRIVILEGIOS DE LA CUENTA ADMIN

140. Aunque no es posible eliminar la cuenta de administrador en un dispositivo GigaVUE, sí es posible reducir los privilegios de esta cuenta.

141. **Se deben limitar los privilegios siempre que sea posible**. Se debe verificar que existen otras cuentas que tienen asignado el papel de administrador antes de dar este paso ya que sino se podría perder acceso completo al sistema al no haber ninguna cuenta con este rol disponible. Al eliminar el rol de administrador se desconectará la cuenta de administrador.

142. Para asociar la cuenta de administrador al rol de "*Monitor*", teniendo en cuenta la advertencia anterior, se pueden utilizar los siguientes comandos:

```
gigavue-appliance (config) # username admin roles replace monitor
```

```
gigavue-appliance (config) # show roles
=================================================
Role          Description                 User(s)
-------------------------------------------------
monitor                                   admin,monitor,osheridan,pmo...
admin                                     osheridan,pmortimer
Default                                         -
gigavue-appliance (config) #
```

Figura 56. Asignar el rol de monitor a la cuenta *admin*

143. Se puede ver en la figura anterior que el usuario *admin* ha sido asociado al rol "*Monitor*". Como evidencia de este cambio, se accede al dispositivo GigaVUE y se intenta cambiar el banner y añadir un mapa:

```
Using username "admin".
Pre-authentication banner message from server:
|
| Gigamon GigaVUE-OS
|
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Last login: Sat Jul  4 07:58:59 2020 from 192.168.58.133
Gigamon GigaVUE-OS

Logged in with monitor role. Access will be limited.
The username admin's admin privilege has been revoked.

Software Version: GigaVUE-OS 5.9.00 172922 2020-04-01 08:03:25
System in classic mode.
gigavue-appliance > enable
gigavue-appliance # configure terminal
gigavue-appliance (config) # banner "Trying to change this"
% Unrecognized command "banner".
Type "?" for help.
gigavue-appliance (config) # map alias TRYING_TO_ADD_A_MAP
% Unrecognized command "map".
Type "?" for help.
gigavue-appliance (config) #
```

Figura 57. La cuenta de administración después de asociarla al rol *monitor*

144. Como se puede ver en la Figura 57, el usuario *admin* no ha podido hacer ningún cambio en el banner ni ha podido añadir un nuevo mapa.

5.8 PROTECCIÓN FRENTE A ATAQUES DE INICIO DE SESIÓN POR FUERZA BRUTA

145. La cuenta de administrador y/u otras, pueden ser objeto de ataques de fuerza bruta por lo que se deben establecer mecanismos para protegerla.

146. Existen dos métodos de restricción temporal para inicios de sesión fallido. Se puede configurar un tiempo de bloqueo para un usuario tras cada inicio de sesión fallido (valores entre 0[desactivado] y 1410065408 segundos):

```
gigavue-appliance (config) # aaa authentication attempts lockout lock-time 30
gigavue-appliance (config) # show aaa authentication attempts configured
Configuration for authentication failure tracking and locking:
   Track authentication failures:                  yes
   Lock accounts based on authentication failures:  yes
   Override treatment of 'admin' user:             (none)
   Override treatment of unknown usernames:        hash-usernames

Configuration for lockouts based on authentication failures:
   Lock account after consecutive auth failures:    5
   Allow retry on locked accounts (unlock time):    never
   Temp lock after each auth failure (lock time):   for 30 second(s)
```

Figura 58. Asignar un tiempo entre accesos fallidos

147. Además, se puede especificar un número de intentos de inicio de sesión fallidos (*attemts lockout max-fail*) y el tiempo (*attemts lockout time*) que esta cuenta se bloqueará en segundos.

- *unlock-time*: entre 0[desactivado] y 2147483647 segundos.
- *max-fail*: entre 0[desactivado] y 4294967295 intentos.

```
gigavue-appliance (config) aaa authentication attempts lockout unlock-time 3600
gigavue-appliance (config) aaa authentication attempts lockout max-fail 10
gigavue-appliance (config) # show aaa authentication attempts configured
Configuration for authentication failure tracking and locking:
   Track authentication failures:                  yes
   Lock accounts based on authentication failures:  yes
   Override treatment of 'admin' user:             (none)
   Override treatment of unknown usernames:        hash-usernames

Configuration for lockouts based on authentication failures:
   Lock account after consecutive auth failures:    10
   Allow retry on locked accounts (unlock time):    after 3600 second(s)
   Temp lock after each auth failure (lock time):   nonesecond(s)
```

Figura 59. Asignar un tiempo entre accesos fallidos

5.9 CONTROLES DE SESIÓN

148. **Se recomienda asignar un valor de tiempo máximo de inactividad, tras el cual se procederá al bloqueo de sesiones de CLI y *WebUI*.**

149. La gestión de un dispositivo GigaVUE se lleva a cabo a través de la interfaz de usuario Web (WebUI) o la Interfaz de Línea de Comandos (que abarca las sesiones SSH y Serial).

150. **Se recomienda que el tiempo de cierre de sesión sea el mínimo posible que permita una operación funcional del dispositivo. El tiempo de espera puede desactivarse utilizando el valor 0; sin embargo, como ajuste permanente no se recomienda.**

5.9.1 WEBUI *TIMEOUTS*

151. Para los usuarios de la *WebUI*, se puede aplicar la siguiente configuración:

```
gigavue-appliance (config) # web auto-logout 10
```

Figura 60: Configuración del cierre de sesión automático de la interfaz de usuario de la web

152. En el ejemplo anterior, se han configurado 10 minutos, pero se puede ajustar a cualquier valor entre 0,25 minutos (15 segundos) y 35791 minutos (596 horas y 31 minutos).

5.9.2 CLI *TIMEOUTS*

153. Hay dos (2) opciones para la configuración de este tiempo de espera; una por sesión y otra de forma permanente.

154. Para establecer el tiempo de espera de la sesión actual utilice la siguiente sintaxis:

```
gigavue-appliance (config) # cli session auto-logout 10
gigavue-appliance (config) #
```

Figura 61. Configurar el cierre de sesión automático de la interfaz de usuario de la CLI

155. En la Figura 61, se ha fijado el periodo a 10 minutos. Se puede ajustar a cualquier valor entre 0,25 minutos (15 segundos) y 35791 minutos (596 horas y 31 minutos). **Este ajuste no es permanente**, solo afecta a la sesión existente.

156. Para establecerlo de forma permanente (recordando emitir el comando *write memory* para mantener la configuración de forma persistente) se puede utilizar la siguiente sintaxis:

```
gigavue-appliance (config) # cli default auto-logout 10
gigavue-appliance (config) #
```

Figura 62. Configuración del interfaz CLI de auto *logout*

157. Como en el ejemplo anterior, se han configurado 10 minutos. Sin embargo, se puede ajustar a cualquier valor entre 0,25 minutos (15 segundos) y 35791 minutos (596 horas y 31 minutos).

158. El tiempo de espera puede ser desactivado utilizando un valor de 0; sin embargo, no se recomienda.

5.10 HABILITAR EL MODO DE CRIPTOGRAFÍA SEGURA

159. Un dispositivo GigaVUE puede configurarse en modo de criptografía segura para mejorar la seguridad de la interfaz de gestión. En el modo de criptografía segura, se desactivan los algoritmos débiles de cifrado/descifrado y *hashing*, utilizados para proteger las comunicaciones.

160. Los *ciphers* permitidos en el modo seguro son:

Figura 63. Ciphers Seguros

161. Los *ciphers* permitidos en el modo no seguro son:

Normal Cryptography Mode		
GVCCV2	**Other PowerPC Platforms**	**Intel Platforms**
AES128-CTR AES192-CTR AES256-CTR	AES128-CTR AES192-CTR AES256-CTR	AES128-CTR AES192-CTR AES256-CTR AES128-CBC AES256-CBC

Figura 64. *Ciphers* no seguros

162. Los algoritmos criptográficos permitidos en el modo seguro:

SSH Host Key Algorithm	SSH Key Exchange	Encryption Algorithms	Hash-based Message Authentication Code
ECDSA	Diffie-Hellman-group14-sha1	AES128-CBC, AES256-CBC	HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-512

Figura 65. Algoritmos de cifrado seguros

163. **Se debe habilitar el modo de Criptografía Segura (*Secure Cryptography Mode)*.**

164. El dispositivo GigaVUE utiliza, por defecto el modo clásico. Para activar y desactivar el Modo de Criptografía Segura, se utilizan los siguientes comandos:

```
gigavue-appliance (config) # system security crypto enhanced
! Notice: HTTPS minimum TLS version will be set to TLSv1.2 !
! Please reload system to activate PENDING cryptography mode change !
gigavue-appliance (config) # no system security crypto enhanced
gigavue-appliance (config) #
```

Figura 66. Habilitar y deshabitar el modo de criptografía segura

165. Se destaca que es necesario reiniciar el sistema cuando se activa o desactiva el modo de criptografía segura. Se puede utilizar el comando "*reload*" para reiniciar el dispositivo y completar el cambio.

166. También se recomienda realizar este cambio a través de una conexión en serie y asegurar que el navegador web y/o el cliente SSH puedan conectarse con éxito al dispositivo GigaVUE.

167. Si al habilitar el modo seguro, el cliente no soporta los cifrados especificados en las tablas anteriores, la comunicación puede bloquearse (esto pasa hoy en día con algunos navegadores obsoletos y no actualizados).

5.11 POLÍTICA DE CONTRASEÑAS DE USUARIO

168. **Se debe establecer una política de fortaleza de contraseñas**, que deberá estar en consonancia con la política de contraseñas de la organización, y aplicarla por defecto a todas las cuentas de administración. Los parámetros a definir, serán los siguientes:

    a) Número máximo de sesiones concurrentes.

b) Tiempo máximo de inactividad de sesión.

c) Número máximo de intentos fallidos de autenticación y acciones a realizar cuando se supera el umbral. Este número no debería ser superior a 5 intentos.

d) Inhabilitación automática de cuentas inactivas.

e) Requisitos de vigencia, expiración y fortaleza de contraseñas. Deberán seguirse las siguientes directrices y opciones de configuración:

- No deberá permitirse la repetición de al menos las 5 últimas contraseñas utilizadas.
- No deberá realizarse un nuevo cambio de contraseña en los 4 días posteriores al último cambio.
- Deberán ser de 9 caracteres como mínimo, aunque se recomienda una longitud de 15 caracteres.
- Deberán incluir caracteres alfanuméricos y caracteres especiales como “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“ y “)”, al menos una letra en mayúscula y otra en minúscula, un número o más, y un signo de puntuación o más.
- Deberán contener un número mínimo de juegos de caracteres o de cambios en el juego de caracteres.

f) Además, a la hora de seleccionar contraseñas para las cuentas de administrador autorizadas, conviene seguir las siguientes recomendaciones de seguridad.

- Deberán ser fáciles de recordar, de modo que los usuarios no se sientan tentados a escribirlas. En caso de que sea necesario guardar una copia física de la contraseña, se hará en un contenedor seguro.
- Deberán ser privadas y no compartirse con nadie.
- Deberán cambiarse periódicamente, con un período no superior a 180 días.
- Son contraseñas poco seguras:
  i. Las palabras que puedan estar en o que existan como forma permutada en un archivo de sistema.
  ii. El nombre de host del sistema (siempre lo primero que se intenta).
  iii. Cualquier palabra que aparezca en un diccionario, incluidos también diccionarios de otros idiomas distintos al inglés o al castellano, palabras que puedan aparecer en obras de autores

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

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

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

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

169. La configuración de la longitud mínima de contraseñas permite establecer entre 8-30 caracteres (8 es el valor predeterminado). **Se debe utilizar una longitud mínima de 12 caracteres.** Para ello, se puede usar el comando ***"system security passwords":***

```
gigavue-appliance (config) # system security passwords enhanced
gigavue-appliance (config) # system security passwords min-length 12
gigavue-appliance (config) #
```

Figura 67. Determinar la longitud mínima de *password* de 12 caracteres

170. Aunque **no se debe permitir**, un usuario administrador puede usar el parámetro '*login-blank*' para permitir el acceso sin contraseña. Aunque está desactivado por defecto, puede ser específicamente desactivado de la siguiente forma:

```
(config) # no system security passwords login-blank
```

Figura 68. Deshabilitar el *password blank login* del usuario administrador

171. Para más información en relación a la configuración de contraseñas, se puede consultar la guía de usuario (REF1).

5.12 ACTUALIZACIÓN DEL PRODUCTO

172. El proceso para actualizar el producto consta de tres (3) fases.

173. En primer lugar, es necesario descargar la versión de *software* en el propio equipo. Los protocolos disponibles para importar las imágenes son:

- HTTP
- HTTPS
- FTP
- TFTP
- SCP
- SFTP

174. **No se debe hacer uso de los protocolos HTTP, FTP y TFTP por considerarse inseguros**

175. El comando sería:

```
gigavue-appliance (config) # image fetch
scp://forsola@192.168.167.1/Users/forsola/Downloads/hc1_5100101.img
Password (if required): *********
100.0%
[##############################################################################
##############################################################################
############################]
```

Figura 69. Descarga de actualizaciones de software

176. Una vez descargado el *software,* se debe verificar que está disponible para su instalación:

```
gigavue-appliance (config)# show images
Installed images:

  Partition 1:
  GigaVUE-OS 5.9.00 Build 172922 2020-04-01 08:03:57 x86_64 gihc1
root@jenkins-slave022:git:ba83fe15c6c6

  Partition 2:
  GigaVUE-OS 5.9.00 Build 172922 2020-04-01 08:03:57 x86_64 gihc1
root@jenkins-slave022:git:ba83fe15c6c6

Last boot partition: 1
Next boot partition: 1

Images available to be installed:

  hc1_5100101.img
  GigaVUE-OS 5.10.01.01 Build 211011 2020-09-30 08:58:05 x86_64 gihc1
root@jenkins-slave004:git:cebb63b43c01

Serve image files via HTTP/HTTPS: no

No image install currently in progress.

No boot manager password is set.

Image signing: trusted signature always required
Admin require signed images: no (not active)

Settings for next boot only:
   Fallback reboot on configuration failure: yes (default)
```

Figura 70. Listado de versiones de *software* instaladas y disponibles

177. Para proceder a la instalación de la imagen disponible se debe hacer uso del siguiente comando:

```
gigavue-appliance (config)# image install hc1_5100101.img
Step 1 of 4: Verify Image
100%
[##############################################################################]
Step 2 of 4: Uncompresses
Image
100%
[##############################################################################]
Step 3 of 4: Create Filesystem
```

```
100%
[##############################################################################]
Step 4 of 4: Install Image
100%
[##############################################################################]
```

Figura 71. Proceso de instalación de actualizaciones

178. Por último, se debe verificar que la actualización se ha instalado y reiniciar:

```
gigavue-appliance (config)# show images
Installed images:
  Partition 1:
  GigaVUE-OS 5.9.00 Build 172922 2020-04-01 08:03:57 x86_64 gihc1
root@jenkins-slave022:git:ba83fe15c6c6
  Partition 2:
  GigaVUE-OS 5.10.01.01 Build 211011 2020-09-30 08:58:05 x86_64 gihc1
root@jenkins-slave004:git:cebb63b43c01
Last boot partition: 1
Next boot partition: 1
Images available to be installed:
hc1_5100101.img
GigaVUE-OS 5.10.01.01 Build 211011 2020-09-30 08:58:05 x86_64 gihc1
root@jenkins-slave004:git:cebb63b43c01
Serve image files via HTTP/HTTPS: no
No image install currently in progress.
No boot manager password is set.
Image signing: trusted signature always required
Admin require signed images: no (not active)
Settings for next boot only:
Fallback reboot on configuration failure: yes (default)
gigavue-appliance (config)# image boot location 2
```

Figura 73. Forzar reinicio en la partición con la nueva actualización

5.13 COPIAS DE SEGURIDAD

179. Los equipos pueden tener muchas configuraciones guardadas y tener cargada la deseada en cada momento. Se podrá disponer de tantos archivos de configuración como se desee.

180. El sistema trabaja con una configuración que reside en memoria y que es volátil. Es decir que, de no ser salvada, se perderá tras cada reinicio del equipo.

181. Para guardar la configuración que está en memoria en disco:

```
gigavue-appliance (config) # configuration write
gigavue-appliance (config) #
```

Figura 74. Guardar configuración en disco

182. Para guardar la configuración en otro archivo de configuración:

```
gigavue-appliance (config) # configuration write to my_config
gigavue-appliance (config) #
```

Figura 75. Guardar configuración en otro archivo de configuración.

183. Si se desea que este nuevo archivo de configuración no sea el activo se puede modificar el comando con el parámetro **"*no-switch*":**

```
gigavue-appliance (config) # configuration write to my_config no-switch
gigavue-appliance (config) #
```

Figura 76. Guardar configuración en otro archivo de configuración.

184. También se puede listar todas las configuraciones salvadas anteriormente:

```
gigavue-appliance (config) #  show configuration files

        initial
        initial.bak
        my_config
        my_confug (active)
        snapdb.tms
```

Figura 77. Listado de configuraciones existentes

185. Una vez modificada la configuración, se podrá volver a cargar la última configuración guardada a través del siguiente comando:

```
gigavue-appliance (config) # configuration revert saved
gigavue-appliance (config) #
```

Figura 78. Recuperar la última configuración guardada.

186. O bien cargar cualquier otra configuración salvada anteriormente con otro nombre:

```
gigavue-appliance (config) # configuration switch-to initial
gigavue-appliance (config) #
```

Figura 79. Recuperar cualquier configuración anterior.

187. También es posible exportar cualquier configuración a un sistema externo mediante los siguientes protocolos:

- FTP
- TFTP
- SCP
- SFTP

188. **No se debe hacer uso de los protocolos FTP y TFTP por considerarse inseguros.**

189. El comando a usar sería:

```
gigavue-appliance (config) # configuration upload active
scp://mylogin:abc123@192.168.51.41/pre-upgrade
gigavue-appliance (config) #
```

Figura 80. Exportar configuraciones

6. CONTROLES DE LOGGING Y AUDITORÍA

6.1 DETERMINAR LA ZONA HORARIA A UTC

190. Para fijar la zona horaria a UTC, se puede usar el comando '*clock time zone UTC*' (nótese que UTC debe ir en mayúsculas):

```
gigavue-appliance (config) # clock timezone UTC
gigavue-appliance (config) # show clock
Time:       07:14:10
Date:       2020/07/04
Time zone:  UTC
            (Etc/UTC)
UTC offset: same as UTC
gigavue-appliance (config) #
```

Figura 81. Fijar la zona horaria UTC y mostrar la hora

6.2 CONFIGURAR NTP

191. Para garantizar que las marcas de tiempo sean exactas, **se recomienda configurar la sincronización con un servidor NTP (*Network Time Protocol*).** Para ello, se puede hacer uso del siguiente comando:

```
gigavue-appliance (config) # ntp server 10.60.20.67
gigavue-appliance (config) # show ntp configured
NTP enabled: yes
NTP authentication enabled: no
No NTP peers configured.
NTP server 10.60.20.67
  Enabled: yes
  NTP version: 3
  Key Enabled: no
  Key Number: 1
gigavue-appliance (config) #
```

Figura 82. Fijar y mostrar la configuración de NTP

192. Es posible configurar las claves para la comunicación con el servidor NTP. Para obtener más información al respecto, se puede consultar la Guía del Usuario (REF1). Los servidores NTP pueden usar claves para implementar la autenticación. Sin el uso de esta clave cuando un equipo haga una petición NTP sobre un servidor autenticado, este no responderá. En caso de tener que usar un servidor NTP autenticado tendremos que especificar la clave que espera el otro extremo.

6.3 *LOGGING* Y *SYSLOG* REMOTOS

193. Se recomienda que todos los eventos registrados sean transportados a un servidor externo.

194. El nivel de auditoría por defecto ("*NOTICE*") proporciona el registro de todos los comandos introducidos por los usuarios. De esta forma, se proporciona información de auditoría para cualquier cambio de configuración.

195. El nivel de auditoría especifica la **severidad mínima** de un comando para ser incluido en los logs. Existen los siguientes niveles de auditoría:

Nivel de Auditoria	Descripción
emergency	Emergencia: el sistema no se puede utilizar. El nivel de gravedad con el menor registro: solo se registran los eventos / comandos de nivel de emergencia.
alert	Se deben tomar medidas de inmediato.
critical	Condiciones críticas.
error	Condiciones de error.
warning	Condiciones de advertencia.
notice	Condiciones normales pero significativas.
info	Mensajes informativos.
debug	Mensajes de nivel de depuración. Autorizado para uso exclusivo en fábrica.

196. En un entorno controlado, puede ser que se desee y/o se requiera el envío a través de la red de datos *Syslog* no cifrados**. Sin embargo, se recomienda que los datos se envíen por un canal cifrado.** Para ello, se debe consultar el apartado 6.3.1 ENVÍO DE LOGS A UN SERVIDOR *SYSLOG* REMOTO A TRAVÉS DE UN CANAL SEGURO.

197. A continuación, se recoge un ejemplo en el que se van a enviar datos *Syslog* a un servidor con dirección IP 192.168.1.10. Para habilitar el registro en un servidor *Syslog* remoto se utiliza el siguiente comando (se recuerda que la conexión entre el dispositivo y el servidor no está cifrada):

```
gigavue-appliance (config) # logging 192.168.1.10
gigavue-appliance (config) # logging 192.168.1.10 trap notice
gigavue-appliance (config) # logging level audit mgmt info
```

Figura 83. Habilitar *logging* en un equipo GigaVUE

198. El ejemplo anterior, se enviarán al servidor configurado todos los comandos introducidos por los usuarios que utilizan el dispositivo GigaVUE (con nivel de "*NOTICE*").

199. Es importante resaltar que cuando el producto se configura para el envío de los registros de auditoría a un servidor externo, si la comunicación se interrumpe, los ficheros de auditoría generados durante ese tiempo se almacenan localmente. Una vez que se restablece la conexión, el envío de ficheros se inicia de nuevo, pero no se envían aquellos ficheros generados durante la interrupción. Es necesario que el administrador descargue esos ficheros de forma manual para que no sean sobrescritos cuando el *log* de auditoría se llene.

6.3.1 ENVÍO DE LOGS A UN SERVIDOR *SYSLOG* REMOTO A TRAVÉS DE UN CANAL SEGURO.

200. **Se recomienda enviar los registros a un servidor de *Syslog* a través de una conexión SSH cifrada**. Los pasos necesarios para completar esta tarea son:

- Crear una clave pública SSH (ver sección 5.2.6 GENERACIÓN DE UNA CLAVE PÚBLICA DE IDENTIDAD).
- Copiar la clave en la máquina remota de *Linux* en *~username/.ssh/authorized_keys.* Para ello, es necesario tener permisos sobre el directorio.
- Configurar la máquina remota de *Linux* para aceptar *syslog* en *tcp.*
- Configurar el dispositivo GigaVUE para enviar el syslog a la máquina remota sobre TCP.

201. En el ejemplo que se recoge a continuación, se va a usar la clave pública creada en la sección anterior y se configura el envío de los logs a un servidor *CentOS 8.1* ejecutando *rsyslog*. Se usa el usuario remoto "*sysloguser*" en la máquina Linux remota.

202. En el servidor *LINUX,* se debe configurar *rsyslog* para aceptar conexiones en tcp/514 (se puede usar cualquier puerto). Esto se consigue cambiando las siguientes líneas (quitando el comentario "#", para habilitar las líneas) de */etc/rsyslog.conf*:

```
#module(load="imtcp") # needs to be done just once
#input(type="imtcp" port="514")
```

Figura 84. Configuración por defecto de rsyslog.conf

A:

```
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")
```

Figura 85. Cambio de configuración de rsyslog.conf

203. Se debe reiniciar el servicio. *CentOS 8.1* usa *systemd* pero en otra distribución puede ser diferente.

```
# systemctl restart rsyslog.service
```

Figura 86. Reinicio del servicios rsyslog comos root)

204. Por último, se necesita configurar la auditoría en el dispositivo GigaVUE:

```
gigavue-appliance (config) # logging 10.60.20.220 tcp 514 ssh username
sysloguser
The authenticity of host '10.60.20.220' can't be established.
The ssh key finger print is  (ECDSA)
65:93:5f:15:0b:ed:b6:2f:72:35:c8:7c:a7:46:ff:1b [MD5].
Are you sure you want to send log (yes/no)? [no] yes
gigavue-appliance (config) #
```

Figura 87. Configuración del equipo GigaVUE para enviar syslog cifrado al servidor remoto

205. En CentOS 8.1, los registros aparecerán en el archivo */var/log/messages*. Sin embargo, si se utiliza una distribución diferente, la ruta puede variar. En Ubuntu 20.04 LTS, por ejemplo, los registros se almacenan en */var/log/syslog.*

6.4 *SIMPLE NETWORK MANAGEMENT PROTOCOL* (SNMP)

206. SNMP es un protocolo útil para supervisar la actividad de los dispositivos de red. Sin embargo, **no se deben usar SNMPv1 y SNMPv2** porque utiliza autenticación mediante contraseñas en texto plano.

207. **Se debe utilizar, por tanto, SNMPv3** que aporta mejoras de seguridad. Para más información sobre la configuración de SNMPv3:

https://docs.gigamon.com/doclib59/5900-gigadoc.html#GV-OS-CLI/_snmp_server.html

7. FASE DE OPERACIÓN

208. Durante la fase de operación del producto se recomienda llevar a cabo, al menos, las siguientes tareas para una gestión segura del producto:

a) Revisar las alertas que genera el sistema, tanto en la consola GUI como en el servidor que recibe los eventos de *syslog*.

b) Mirar los parámetros de carga del sistema, CPU, RAM y espacio en disco, con el fin de anticiparse a situaciones límites. El sistema genera alarmas automáticas al alcanzar los valores máximos configurados.

c) Revisar que las copias de seguridad automáticas se realizan correctamente para los datos y los archivos de configuración.

d) Revisar periódicamente los logs de auditoría. Comprobar el límite de almacenamiento y eliminar (y si fuese oportuno, almacenando en una ubicación alternativa) los logs más antiguos para evitar que el sistema los sobrescriba.

e) Controlar el acceso a la información de auditoría, de tal forma que únicamente el personal designado pueda acceder a ella.

f) Comprobar si hay nuevas actualizaciones de *software* disponibles, mediante acceso al portal de clientes, con el objetivo de mantener el sistema actualizado siempre a la última versión.

8. ABREVIATURAS

ACL	Lista de control de acceso.
CLI	Interfaz de Línea de Comando
CSR	Petición de firma de certificado
FTP	Protocolo de tranaferencia de ficherosl
GUI	Interfaz gráfico de usuario
HTTP	Protocolo de transferencia de hypertexto
HTTPS	Protocolo de transferencia de hypertexto Seguro
IP	Protocolo Internet
NPB	*Network Packet Brokering*
NTP	Protocolo de tiempo de red
RADIUS	Servicio de autenticación remota de usuario Dial-In
RBAC	Control de Acceso Basado en Roles
RMA	Autorización de retorno de material
SCP	Protocolo de copia segura
SFTP	Protocolo de transferencia segura de ficheiros
SNMP	Protocolo de gestión de red simple
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
SSL	Capa de Sockets Seguros
Syslog	Protocolo de registro de sistema
TACACS	Sistema de Control de Acceso Mediante Control del Acceso desde Terminales
TLS	Segurdad en capa de transporte
UTC	Tiempo Universal Coordinado

9. REFERENCIAS

REF1 *GigaVUE-OS 5.9.00 – Guía de usuario*
https://docs.gigamon.com/doclib59/5900-gigadoc.html.

REF2 *Certificación Common Criteria de la tecnología Giga-VUE OS de Gigamon*
Common Criteria on GigaVUE

REF3 *Certificación FIPS 140-2 de la tecnología Giga-VUE OS de Gigamon*
FIPS 140-2 Compliance on GigaVUE-OS

REF4 *Certificación UC APL de la tecnología Giga-VUE OS de Gigamon*
GigaVUE-OS Unified Capabilities Approved Products List (UC APL) compliancy

PUBLICACIONES DE DEFENSA

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