

Guía de Seguridad de las TIC

CCN-STIC 1301

Procedimiento de Empleo Seguro GigaVUE de GIGAMON



Mayo 2025



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

Edita:



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

NIPO: 083-25-178-0

Fecha de Edición: Mayo de 2025



CENTRO CRIPTOLOGICO
NACIONAL

cn=CENTRO CRIPTOLOGICO
NACIONAL, 2.5.4.97=VATES-
S2800155J, ou=CENTRO
CRYPTOLOGICO NACIONAL,
o=CENTRO CRIPTOLOGICO
NACIONAL, c=ES
2026.01.16 08:15:26 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

ÍNDICE

1 INTRODUCCIÓN	4
2 OBJETIVO Y ALCANCE.....	5
3 ORGANIZACIÓN DEL DOCUMENTO	6
4 FASE PREVIA A LA INSTALACIÓN.....	7
4.1 COMPROBACIÓN DE MANIPULACIONES	7
4.1.1 PEGATINAS ANTI-MANIPULACIÓN.....	7
4.2 CONSIDERACIONES PREVIAS.....	7
4.2.1 USO DE LA TERMINAL DE COMANDOS (CLI).....	7
4.2.2 DESACTIVACIÓN DEL INTERFAZ SERIE	10
5 FASE DE INSTALACIÓN.....	12
6 FASE DE CONFIGURACIÓN.....	14
6.1 HABILITAR EL MODO DE CRIPTOGRAFÍA SEGURA	14
6.2 AUTENTICACIÓN	15
6.2.1 POLÍTICA DE CONTRASEÑAS DE USUARIO	15
6.3 ADMINISTRACIÓN DEL PRODUCTO.....	16
6.3.1 CONTROL DE ACCESO BASADO EN ROLES	16
6.3.2 BLOQUEO DE SESIÓN	24
6.3.3 BANNERS.....	25
6.4 FILTRADO IP	26
6.4.1 BREVE DESCRIPCIÓN DE LOS ELEMENTOS DEL FILTRO IP.....	26
6.4.2 ANTES DE EMPEZAR.....	27
6.4.3 VISUALIZACIÓN DE LA CONFIGURACIÓN ACTUAL DEL FILTRO IP	27
6.4.4 HABILITAR Y DESHABILITAR LA POLÍTICA DE FILTRO IP	28
6.4.5 AÑADIR UNA REGLA A LA CADENA.....	29
6.4.6 ELIMINAR UNA REGLA DE UNA CADENA	29
6.4.7 EJEMPLO: RESTRINGIR EL ACCESO A SSH A UNA SUBRED ESPECÍFICA.....	29
6.5 SECURE SHELL (SSH)	32
6.5.1 ESTABLECER UN PAR DE CLAVES PUBLICA/PRIVADA.....	32
6.5.2 AÑADIR UNA CLAVE PUBLICA AL EQUIPO GIGAVUE	34
6.5.3 MOSTRAR LAS CLAVES PUBLICAS SSH	35
6.5.4 REVOCAR/ELIMINAR UNA CLAVE PUBLICA DEL EQUIPO GIGAVUE	35
6.5.5 INSTALAR CLAVES SSH PARA ACCEDER A OTROS RECURSOS SSH/SCP/SFTP	36
6.5.6 PAR EVITAR SU USO, SE PUEDE UTILIZAR LA IP, COMO SE DESCRIBE EN LA SECCIÓN ANTERIOR 6.2.1 POLÍTICA DE CONTRASEÑAS DE USUARIO	36
6.6 ADMINISTRACIÓN DEL PRODUCTO.....	37
6.6.1 CONTROL DE ACCESO BASADO EN ROLES	37
6.6.2 BLOQUEO DE SESIÓN	45
6.6.3 BANNERS.....	46
6.7 ADMINISTRACIÓN DEL PRODUCTO.....	47
6.7.1 CONTROL DE ACCESO BASADO EN ROLES	47
6.7.2 BLOQUEO DE SESIÓN	55
6.7.3 BANNERS.....	56
6.7.4 GENERACIÓN DE UNA CLAVE PÚBLICA DE IDENTIDAD	57
6.8 TRANSPORT LAYER SECURITY (TLS).....	58
6.8.1 INSTALAR CERTIFICADO	59
6.8.2 CONFIGURACIÓN DE VERSIÓN DE TLS PARA EL INTERFAZ DE GESTIÓN	61

6.9	ACTUALIZACIONES	62
6.10	BACKUP	63
6.11	AUDITORÍA	65
6.11.1	DETERMINAR LA ZONA HORARIA A UTC	65
6.11.2	EVENTOS DEL EQUIPO	65
6.11.3	EVENTOS DEL EQUIPO: ALMACENAMIENTO LOCAL.....	66
6.11.4	EVENTOS DEL EQUIPO: ALMACENAMIENTO REMOTO.....	67
6.11.5	ALMACENAMIENTO REMOTO	68
6.12	SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP).....	69
7	FASE DE OPERACIÓN	70
8	ABREVIATURAS.....	71
9	REFERENCIAS	72
10	ABREVIATURAS.....	73

1 INTRODUCCIÓN

1. Gigamon desarrolla y comercializa equipos y Software de Network Packet Brokering (NPB), 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-OS** para proteger un dispositivo y que este opere de acuerdo a unas garantías mínimas de seguridad.
3. Las instrucciones contenidas están asociadas a la **versión 6.5** del GigaVUE-OS, objeto de la última certificación de Common Criteria de Gigamon
4. A modo de introducción del Producto, un NPB es una tecnología que implementa una variedad de herramientas de monitoreo para acceder y analizar el tráfico (también conocido como "paquetes de red") a través de una red. En pocas palabras, los NPB funcionan como "intermediarios" (o administradores) del tráfico de la red. El NPB recopila el tráfico de múltiples enlaces de red, filtrando y distribuyendo 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, al proporcionar datos mejorados a través de la red.
5. Mientras que un NPB tradicional puede ayudar a garantizar una mayor efectividad de la herramienta, un NPB de próxima generación lleva las cosas más allá, asegurando que se envíe el tráfico correcto a las herramientas de prevención en línea y fuera de banda adecuadas. Ya sea que una configuración de red sea local, virtual o en la nube, un intermediario de paquetes de red inteligente proporciona la base de visibilidad perfecta. Compatibilidad con corredores de paquetes de red de próxima generación:
 - 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 OBJETIVO Y ALCANCE

7. Hay varios elementos de GigaVUE-OS (el sistema operativo común a todos los equipos Gigamon) que pueden ser configurados para mejorar la seguridad del propio dispositivo. Este documento cubre el endurecimiento de los siguientes dispositivos:

Nombre comercial	Modelo
HC3 AC Power	GVS-HC301
HC3 DC Power	GVS-HC302
HC2 AC Power	GVS-HC2A1
HC2 DC Power	GVS-HC2A2
HC1 AC Power	GVS-HC101
HC1 DC Power	GVS-HC102
TA25 (solo hardware) AC Power 48 puertos	GVS-TAX21-HW
TA25 (solo hardware) DC Power 48 puertos	GVS-TAX22-HW
TA25 (solo hardware) AC Power 24 puertos	GVS-TAX21A-HW
TA25 (solo hardware) DC Power 24 puertos	GVS-TAX22A-HW
TA200 (solo hardware) AC Power	GVS-TAC21
TA200 (solo hardware) DC Power	GVS-TAC22
GTAP Serie 2 Cobre	GTP-ATX21
GTAP Serie 2 SFP	GTP-ASF21

Tabla 1. Modelos

8. 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].
9. El producto GigaVUE ha sido cualificado en el catálogo CPSTIC para categoría ENS ALTA/MEDIA en la familia “Captura, Monitorización y Análisis de Tráfico”.

3 ORGANIZACIÓN DEL DOCUMENTO

10. El presente documento se organiza en los siguientes apartados:

- a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
- b) Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
- c) Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- d) Apartado **7**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de operación del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 COMPROBACIÓN DE MANIPULACIONES

11. 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.
12. 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.

4.1.1 PEGATINAS ANTI-MANIPULACIÓN

13. 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.
14. 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.



Ilustración 1. Pegatinas anti-manipulación de Gigamon

4.2 CONSIDERACIONES PREVIAS

4.2.1 USO DE LA TERMINAL DE COMANDOS (CLI)

15. 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.

16. El *prompt* para configurar el equipo GigaVUE cambia dependiendo del modo de funcionamiento: *Standard*, *Enable* y *Configure*. Los tres modos que existen permiten:
- *Standard*: Modo de acceso básico. Permite revisar los aspectos más básicos de la configuración como licencias, versiones y 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.
17. 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) #
```

Ilustración 2. Cambio de modos para aumentar privilegios

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

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

Ilustración 3. Cambio de modos para disminuir privilegios

19. 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) #
```

Ilustración 4. Ejemplo de comando input

20. 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) #
```

Ilustración 5. Ejemplo de comando input de variable

21. 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) #
```

Ilustración 6. Ejemplo de error stdout

22. 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 #
```

Ilustración 7. Ejemplo de stdout de especial interés

23. 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**.

4.2.2 DESACTIVACIÓN DEL INTERFAZ SERIE

24. 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.
25. 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).
26. 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).
27. 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 6.3.2 BLOQUEO DE SESIÓN.
28. Se debe considerar cuidadosamente si es apropiado deshabilitar la interfaz serie. Si lo hace y pierde las credenciales de acceso al dispositivo GigaVUE-OS, no 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](#).
29. Para deshabilitar el interfaz serie, usaremos 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) #
```

Ilustración 8. Deshabilitar el interfaz serie

30. 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) #
```

Ilustración 9. Habilitar el interfaz serie

31. 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 FASE DE INSTALACIÓN

32. Tras el primer login en el equipo, esté abligará a cambiar la contraseña. El administrador del sistema debe cambiar la contraseña de la cuenta de administrador predeterminada a través del script de inicio rápido. La contraseña predeterminada (admin123A!) ya no está permitida. La contraseña debe cumplir con los siguientes estándares:
- incluir de 8 a 64 caracteres
 - incluir al menos un número
 - incluir al menos una letra mayúscula
 - incluir al menos una letra minúscula
 - incluir al menos un carácter especial (por ejemplo, !, @, #, \$, %, ^, & o *ASCII 0x21,0x2F, 0x3A, 0x40, 0x5B, 0x5F, 0x7B, 0x7E)
 - No debe incluir el nombre de usuario ni partes del nombre completo.
33. Tras la puesta en marcha del equipo y para configurarlo desde cero se usará el comando “configuration jump-start”:

```
gigavue-appliance (config) # GigaVUE-OS configuration wizard

Step 1: Hostname? [TA25]
Step 2: Use DHCP on eth0 interface? [no]
Step 3: Use zeroconf on eth0 interface? [no]
Step 4: Primary IPv4 address and masklen? [10.60.126.23/17]
Step 5: Default gateway? [10.60.0.1]
Step 6: Primary DNS server? [8.8.8.8]
Step 7: Domain name?
Step 8: Enable IPv6? [yes]
Step 9: Enable IPv6 autoconfig (SLAAC) on eth0 interface? [no]
Step 10: Enable DHCPv6 on eth0 interface? [yes]
Step 11: Enable SNMP communities? [no]
Step 12: Enable secure cryptography? [no]
Step 13: Minimum password length? [8]
Step 14: Admin password (Enter to Leave unchanged)?
Step 15: Cluster enable? [yes]
Step 16: Cluster Interface <eth0> ? [eth0]
Step 17: Cluster id (Back-end may take time to proceed)? [AEAT-AA]
Step 18: Cluster name? [AEAT-AA]
Step 19: Cluster mgmt virtual IP address and masklen? [10.60
```

Ilustración 10. Habilitar y deshabitar el modo de criptografía segura

34. Siga las indicaciones del script de inicio rápido para configurar cada uno de los ajustes que se enumeran en la siguiente tabla.
35. NOTA: Si cambia de opinión sobre un ajuste en particular, tendrá la oportunidad de cambiarlo al final del script.
- **Nombre de host** El nombre de host aparece en el indicador del sistema y se utiliza para identificar el chasis en las trampas SNMP.
 - **Puerto de administración** Configuración de red. Utilice DHCP o especifique una dirección IP estática y una máscara de red. Si no utiliza DHCP, se le solicitará que configure las siguientes opciones adicionales:
 - a) Puerta de enlace predeterminada: Proporcione la dirección IP de la puerta de enlace predeterminada para el nodo.

- b) Servidor DNS: Proporcione la dirección IP del servidor DNS para el nodo. Se requiere un servidor DNS válido para el uso exitoso de TACACS+.
 - c) Nombre de dominio: Proporcione el nombre de dominio para el nodo (por ejemplo, mycompany.com).
 - **¿Habilitar IPv6?** Puede habilitar el uso de IPv6 para el puerto de administración. Se utiliza IPv6 además de IPv4 si habilita esta opción. Si habilita IPv6, tiene la opción de habilitar la configuración automática de IPv6 o especificar una dirección estática.
 - **Configuración de seguridad** Habilite las siguientes configuraciones de seguridad:
 - d) modo de criptografía segura
 - e) modo de contraseñas seguras
 - f) longitud mínima de contraseña
36. Consulte la Guía de referencia de la CLI de GigaVUE-OS para obtener información sobre seguridad.
- **Contraseña de administrador** La contraseña de la cuenta de administrador debe cambiarse a una contraseña que no sea la predeterminada.
 - **¿Habilitar clúster?** Habilite la compatibilidad con clústeres si este nodo formará parte de un clúster de nodos GigaVUE Serie H conectados. Si habilita la compatibilidad con clústeres, el script de inicio rápido le solicitará que suministre el ID de clúster, el nombre del clúster y la dirección IP virtual de administración de clúster. Puede unirse a un clúster existente si proporciona valores que coincidan con la configuración existente.
37. NOTA: Para los nodos agrupados en clústeres configurados para usar el puerto eth1 en una tarjeta de control como puerto de administración y de administración de clústeres, tenga en cuenta que NTP también se usa en el puerto de administración eth0 en el nodo GigaVUE Serie H de la Serie H. En un caso como este, solo puede usar uno o el otro.
- **Box ID:** para el nodo Proporcione un ID de caja numérico para el nodo. Este box id se utiliza para identificar los puertos de red/herramientas en el nodo; el formato es ID de caja/ID de ranura/ID de puerto. Se le solicitará un ID de caja solo si no se habilitó la agrupación en clústeres en el paso anterior.
38. Revise su configuración. Puede cambiar una configuración especificando su número de línea indicado y volviendo a ingresar la configuración.
39. Cuando esté satisfecho con su configuración, salga del script como se le solicite. GigaVUE H Series guarda automáticamente su configuración.
40. Reinicie el nodo con el comando reload.

6 FASE DE CONFIGURACIÓN

6.1 HABILITAR EL MODO DE CRIPTOGRAFÍA SEGURA

41. 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.

42. A nivel de Ciphers la diferencia:

- Ciphers permitidos en el modo seguro:

Secure Cryptography Mode	
All Platforms	
AES128-CBC	
AES256-CBC	

Ilustración 11. Ciphers Seguros

- Ciphers permitidos en el modo no seguro:

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

Ilustración 12. Ciphers no seguros

43. A nivel de algoritmos criptográficos:

- Algoritmos 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

Ilustración 13. Algoritmos de cifrado seguros

44. Se debe habilitar el modo de criptografía segura (*Secure Cryptography Mode*).

45. 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) #
```

Ilustración 14. Habilitar y deshabitar el modo de criptografía segura

46. Se destaca que es necesario reiniciar el sistema cuando se activa o desactiva el modo de criptografía segura. Se puede utilizar el comando “*reload*” en el modo de configuración para reiniciar el dispositivo y completar el cambio.
47. 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.
48. Si al habilitar el modo seguro resulta que el cliente no soporta los cifrados especificados en las tablas anteriores, puede bloquearse potencialmente fuera del dispositivo GigaVUE (esto pasa hoy en día con algunos navegadores obsoletos y no actualizados).

6.2 AUTENTICACIÓN

6.2.1 POLÍTICA DE CONTRASEÑAS DE USUARIO

49. **Se debe establecer una política de fortaleza de contraseñas.**
50. Por defecto las contraseñas deben incluir, al menos:
 - Un número.
 - Una letra minúscula.
 - Una letra mayúscula.
 - Un carácter especial (por ejemplo: !, @, #, \$, %, ^, &, or *)
51. La configuración de la longitud mínima de contraseñas permite establecer entre 8-30 caracteres (8 es el valor predeterminado).
52. Para fijar la longitud mínima, se debe 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) #
```

Ilustración 15. Determinar la longitud mínima de password de 12 caracteres

53. En la figura 67 se ha configurado una longitud de 12 caracteres, valor mínimo recomendado.
54. 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
```

Ilustración 16. Deshabilitar el *password blank login* del usuario administrador

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 CONTROL DE ACCESO BASADO EN ROLES

55. 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.

56. 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.

6.3.1.1 NIVELES DE ACCESO A PUERTOS

57. 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 maps asociados a un Puerto de red	✓	✓	✓	✓	✓
Crear/Editar Mapas asociados a un puerto	✗	✓	✓	✓	✓
Crear tool-mirror a/desde Puerto	✗	✓	✓	✓	✓
Cambiar filtros de salida	✗	✓	✓	✓	✓
Editar parámetros de puertos	✗	✗	✓	✓	✓
Crear pares de puertos	✗	✗	✓	✓	✓
Cambiar tipo de puerto	✗	✗	✗	✓	✓

Ilustración 17. Tabla detallada de niveles de acceso a puertos

58. 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 en conjunto de entre estos 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
59. 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. Y del modo contrario 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

6.3.1.2 MAP BASED ACCESS LEVELS

60. El acceso a los mapas del dispositivo GigaVUE se divide en cuatro 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	✗	✗	✓	✓

Ilustración 18. Tabla detallada de niveles de acceso a mapas

61. Estos niveles de acceso basados en el mapa dictan los diferentes permisos disponibles para los Roles cuando se aplican a una configuración del mapa.
62. La lógica aquí es la descrita en el apartado anterior respecto a los niveles de los puertos, pero aplicado a los mapas.

6.3.1.3 ENTENDER LOS ROLES

63. Los roles permiten agrupar a los usuarios para aplicar privilegios globales a los mapas y puertos.
64. Los roles configurados por defecto son:
- **Admin:** los usuarios asignados a esta función 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 a todos los puertos. Pueden ser considerados como miembros de todos los roles.
 - **Monitor:** Los usuarios asignados a esta función sólo tienen acceso de vista a los puertos y configuraciones.
 - **Default:** Esta función 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.

65. Los roles y sus características que vienen configurados por defecto no pueden ser eliminados o modificados.
66. En nuestro sistema de ejemplo tenemos varios usuarios, que pueden ser listados usando 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) #
```

Ilustración 19. Mostrar usuarios

67. Si se quiere, por ejemplo, añadir el usuario *osheridan* a la función de seguridad y el usuario *pmortimer* a la función de red (se asume que estos usuarios ya han sido añadidos). 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) #
```

Ilustración 20. Mostrar los roles configurados

68. En la Ilustración 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) #
```

Ilustración 21. Mostrar los roles en formato conciso

69. En primer lugar, es necesario crear los roles deseados ("Red" y "Seguridad") usando el 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
admin          admin, fadmin, osheridan, pmo...
Security      Security Team          -
Default
Network      Networking Team        -
gigavue-appliance (config) #
```

Ilustración 22. Añadir los roles de red y seguridad

70. Una vez agregados los roles, se deben aplicar 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
admin          admin, osheridan
Security      Security Team          osheridan
Default
Network      Networking Team        pmortimer
gigavue-appliance (config) #
```

Ilustración 23. Añadir usuarios a sus respectivos roles

71. En la Ilustración 23 se han usado las opciones de comando **"roles add"** para el usuario *osheridan* y opciones **"roles replace"** para el usuario *pmortimer*. Estos aumentan y reemplazan los roles para cada usuario respectivamente.
72. 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 creo el mapa, a menos que se especifique lo contrario en el campo **"owner_role"** del mapa. Por ejemplo, si el usuario *osheridan* ahora 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 2023/01/23 12:45:33 +0100
## Software version on which this output was taken: GigaVUE-OS 6.5.00
111224 2024-11-12 13:25:35
## Hostname: gigavue-appliance
##
##
## 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
gigavue-appliance (config) #
```

Ilustración 24. El usuario osheridan crea un mapa. Roles aplicados por defecto

73. En la Ilustración 24 se observa que esto se ha creado con éxito, y que el mapa se ha creado con todos los roles que tiene el usuario que creó el mapa.
74. Si ahora tratamos de crear una regla con el usuario pmortimer:

```
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) #
```

Ilustración 25. Creación de un mapa con un usuario sin rol de administrador

75. En la Ilustración 25 podemos ver que el usuario *pmortimer*, que es un miembro del rol de red exclusivamente, no puede crear un mapa. Esto se debe a que no es posible crear un mapa que contenga puertos a los que este rol no tenga acceso.
76. Es importante destacar que un Mapa tiene dos 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.”**
77. Así que habrá que verificar que el usuario *pmortimer* tenga permisos suficientes para ambos puertos el de Red y el de Herramientas.
78. Primero verificaremos el puerto de red (en este ejemplo 1/1/g1). Mirando los Controles de Acceso a los Puertos (ver sección anterior con la tabla asociada, Ilustración 17) podemos determinar que como mínimo se requiere el Nivel 2 para “Crear/Editar Mapas asociados a un puerto”.
79. Como usuario *osheridan* (que tiene el rol de administrador asignado) podemos hacer este cambio, añadiendo el rol *Network* como Nivel2 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)       :
gigavue-appliance (config) #

```

Ilustración 26. El usuario osheridan cambiando el rol asignado para el puerto 1/1/g1

80. Ahora intentamos configurar el mapa de nuevo como usuario *pmortimer*:

```

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.
gigavue-appliance (config) #

```

Ilustración 27. El usuario *pmortimer* intenta de nuevo añadir un mapa

81. En la Ilustración 27 se observa que se ha vuelto a denegar la acción 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)       :
gigavue-appliance (config) #

```

Ilustración 28. Asignar privilegios de nivel 2 al rol de Network

82. Con los permisos establecidos se puede ahora añadir en el mapa con éxito como usuario *pmortimer*, ya que pertenece al rol *Network*, el cual tiene ahora Nivel2 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) #

```

Ilustración 29. Configuración exitosa del mapa por el usuario *pmortimer*

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

6.3.1.4 DISMINUCIÓN DE LOS PRIVILEGIOS DE LA CUENTA ADMIN

84. Aunque no es posible eliminar la cuenta de administrador en un dispositivo GigaVUE, sí es posible cambiar los privilegios de esta cuenta a la categoría de "monitor" reduciendo sus privilegios en el sistema.
85. Se recomienda 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 perderíamos 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.
86. Para asociar la cuenta de administrador con la función 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) #
```

Ilustración 30. Asignar la función de Monitor a la cuenta admin

87. Se puede ver en la figura anterior que el usuario *admin* ha sido asociado al rol "Monitor". Como evidencia de este cambio, se puede acceder al dispositivo GigaVUE y se intenta cambiar el banner y añadir en 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 6.5.00 111224 2024-11-12 13:25:35
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) #
```

Ilustración 31. La cuenta de administración después de asociarla al rol Monitor

88. Se comprueba que efectivamente el usuario *admin* no ha podido hacer ningún cambio en la configuración.

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

89. La cuenta de administrador y/u otras, pueden ser objeto de ataques de fuerza bruta por lo que se deben establecer mecanismos para protegerla.
90. Existen dos métodos de restricción temporal para inicios de sesión fallido.
91. 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)
```

Ilustración 32. Asignar un tiempo entre accesos fallidos

92. Además, se puede especificar un número de intentos de inicio de sesión fallidos (*attempts lockout max-fail*) y el tiempo (*attempts lockout time*) que esta cuenta se bloqueará en segundos. Los rangos son:
- unlock-time: entre 0[desactivado] y 2147483647 segundos):
 - max-fail: entre 0[desactivado] y 4294967295. segundos):

```
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)
```

Ilustración 33. Asignar un tiempo entre accesos fallidos

6.3.2 BLOQUEO DE SESIÓN

93. Se recomienda asignar un valor de tiempo máximo de inactividad, tras el cual se procederá al bloqueo de sesiones de CLI y *WebUI*.
94. 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 (CLI, que abarca las sesiones SSH y Serial).
95. 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.

6.3.2.1 WEBUI TIMEOUTS

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

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

Ilustración 34. Configuración del cierre de sesión automático de la interfaz de usuario de la web

97. 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).

6.3.2.2 CLI TIMEOUTS

98. Hay dos (2) opciones para la configuración de este tiempo de espera; una por sesión y otra de forma permanente.
99. 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) #
```

Ilustración 35. Configurar el cierre de sesión automático de la interfaz de usuario de la CLI

100. En el ejemplo anterior se ha fijado el periodo a 10 minutos, pero 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.
101. 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) #
```

Ilustración 36. Configuración del interfaz CLI de auto logout

102. Como en el caso del tiempo de espera de la sesión, en el ejemplo anterior se utilizan 10 minutos y se puede ajustar a cualquier valor entre 0,25 minutos (15 segundos) y 35791 minutos (596 horas y 31 minutos).
103. Al igual que con los ajustes de la sesión, el tiempo de espera puede ser desactivado utilizando un valor de 0; sin embargo, no se recomienda.

6.3.3 BANNERS

104. Los equipos de Gigamon permiten configurar banner a mostrar durante el proceso de acceso a los equipos siendo esto posible por:

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

6.3.3.1 BANNER PRE-LOGIN (POR DEFECTO)

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

106. El *banner* aparece en la pantalla de inicio de sesión.

107. 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.

108. Para accesos WEB, será justo después de la pantalla de inicio mediante un pop-up.

109. En el texto del banner se pueden utilizar varias líneas, la cadena está encapsulada entre comillas:

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

Ilustración 37. Añadir un banner pre-login

6.3.3.1.1 BANNER LOCAL

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

111. De nuevo, se pueden utilizar varias líneas, la cadena está encapsulada entre comillas.

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

Ilustración 38. Añadir un banner login local

6.3.3.1.2 BANNER REMOTE

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

113. Se pueden utilizar varias líneas, la cadena está encapsulada entre comillas.

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

Ilustración 39. Añadir un banner remote local

6.3.3.1.3 BANNER POST LOGIN

114. También se recomienda configurar un *banner* de acceso al puesto que proporcione detalles adicionales de los que se desee informar a los usuarios después de que hayan entrado en el sistema.

115. 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"
```

Ilustración 40. Anadir un banner post login

6.4 FILTRADO IP

116. 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. Por ejemplo, es posible que desee restringir a qué servidores de *syslog* puede enviar registros un dispositivo GigaVUE.

6.4.1 BREVE DESCRIPCIÓN DE LOS ELEMENTOS DEL FILTRO IP

117. 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.
118. 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*.
119. 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.
120. 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.
121. 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) y será un concepto familiar para alguien que haya configurado previamente las ACLs de los routers. 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 el destino del paquete y puede ser aceptado (*ACCEPT*) o descartado (*DROP*).

122. 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.
123. Se debe aplicar una política de denegación (*DROP*) por defecto para las tres (3) cadenas comentadas anteriormente y posteriormente permitir las comunicaciones deseadas.

6.4.2 ANTES DE EMPEZAR

124. 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) #
```

Ilustración 41. Usuarios conectados en el momento

125. En la ilustración 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) #
```

Ilustración 42. Aceptar todo el tráfico de la IP del administrador para pruebas

6.4.3 VISUALIZACIÓN DE LA CONFIGURACIÓN ACTUAL DEL FILTRO IP

126. Para mostrar la configuración básica actual (la Ilustración 43 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) #

```

Ilustración 43. Política de filtro IP por defecto

127. A continuación, se detallan los ajustes por defecto para cada una de estas cadenas en secuencia.
128. La cadena de entrada *INPUT* tiene una política establecida en *DROP*, por lo que, si no hay coincidencia en las reglas 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 examina más adelante).
 6. Acepta todas las comunicaciones a la subred 12.19.148.0/24 desde cualquier destino (el propósito de esta regla se discute más adelante).
129. 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 este tráfico interno del equipo nunca alcanzara las interfaces externas con otros sistemas de red.
130. La cadena de salida *OUTPUT* tiene una política establecida para aceptar y dado que no hay reglas específicas, el paquete será remitido.
131. La cadena *FORWARD* tiene una política establecida para *DROP* y como no hay reglas específicas, el paquete será descartado.

6.4.4 HABILITAR Y DESHABILITAR LA POLÍTICA DE FILTRO IP

132. En la Ilustración 43, se observa que la política de Filtros IP está DESHABILITADA, por lo que actualmente permite todas las conexiones y la configuración es la predeterminada.
133. Durante la configuración de la política de filtrado IP es útil activar y desactivar el filtro IP mientras se soluciona el problema de la política, lo que se puede lograr de la siguiente manera:

```

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) #

```

Ilustración 44. Habilitar y deshabilitar la política de filtro IP

134. 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 la Consola en serie abierta, ya que esto evitará que se le bloquee el acceso al dispositivo GigaVUE Appliance.

6.4.5 AÑADIR UNA REGLA A LA CADENA

135. Para añadir una regla a una cadena, hay tres (3) opciones: “añadir”, “insertar(insert)” y “establecer(set)”.
136. 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).
137. 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. Por ejemplo, al insertar una regla antes de la 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 lo siguiente:

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

Ilustración 45. Insertar una regla en una cadena de filtro IP

138. 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. Por ejemplo, se ha proporcionado accidentalmente acceso a tcp/444 en lugar de tcp/443 para la regla #2, podemos corregir esto 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) #
```

Ilustración 46. Corregir una regla en una cadena de filtro IP

6.4.6 ELIMINAR UNA REGLA DE UNA CADENA

139. Para eliminar una regla de una cadena, se debe utilizar el prefijo “no” para eliminar la regla en cuestión. 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) #
```

Ilustración 47. Eliminar una regla de una cadena

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

140. 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”.

141. 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) #
```

Ilustración 48. Filtro IP configurado actualmente

142. Se desea añadir una regla a la cadena "INPUT" al final, (es decir, añadirla al final de la lista) 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) #
```

Ilustración 49. Anadir regla para permitir tcp/22 desde 192.168.1.0/24

143. 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) #
```

Ilustración 50. Mostrar la regla añadida para permitir tcp/22 desde 192.168.1.0/24

144. Ahora se añade una regla para eliminar el tráfico del puerto 22 que no está en esta subred, así que añadimos esto a lo siguiente:

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

Ilustración 51. Anadir una regla drop para todas las otras conexiones tcp/22

145. Ahora volvemos a listar la configuración del Filtro IP, anotando nuestros cambios:

```
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) #
```

Ilustración 52. Mostrar la configuración de filtro IP con la regla para descartar el resto de conexiones tcp/22

146. Esta configuración detallada arriba en la Ilustración 52, 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) #
```

Ilustración 53. Habilitar la política

147. 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) #					

Ilustración 54. Política de filtro IP habilitada

148. 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 Ilustración 54) 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).

6.5 SECURE SHELL (SSH)

149. Se utiliza SSHv2 para la administración remota de los dispositivos a través del CLI.
150. 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.
151. Telnet ya no está soportado por GigaVUE-OS y fue desactivado en la versión 5.7.00.

6.5.1 ESTABLECER UN PAR DE CLAVES PUBLICA/PRIVADA

152. 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.
153. Los equipos de Gigamon permiten dos niveles de seguridad, el estándar y el e Criptografía Segura. En el apartado [6.1 HABILITAR EL MODO DE CRIPTOGRAFÍA SEGURA](#) se muestran los certificados disponibles para cada modo de seguridad.
154. En este ejemplo, se va a utilizar la suite de código abierto *PuTTY*, para la que se supone que ya está instalada. Los elementos útiles para nuestros propósitos de esta *suite* son:
- **PuTTY**: Cliente SSH.
 - **PuTTYgen**: Generador de parejas de claves SSH Publica/Privada.
 - **Pageant**: Agente de autenticación SSH para PuTTY.
155. En *PuTTYgen*, 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.

156. Con *PuTTYgen* abierto, seleccionar el botón ‘Generar’ de la siguiente manera:

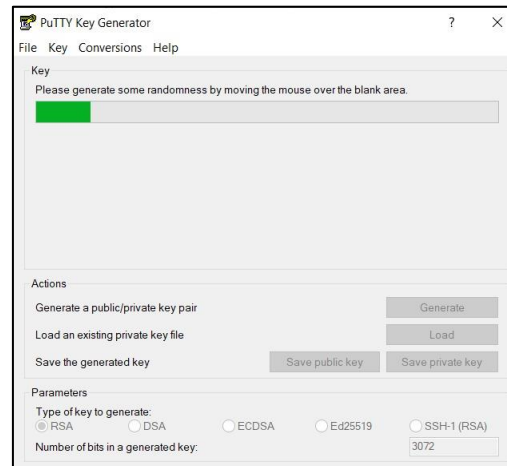


Ilustración 55. Generación de una clave desde el cliente PuTTYgen

157. Esto entonces produce el par de claves SSH, que se muestra en el texto de la siguiente manera:

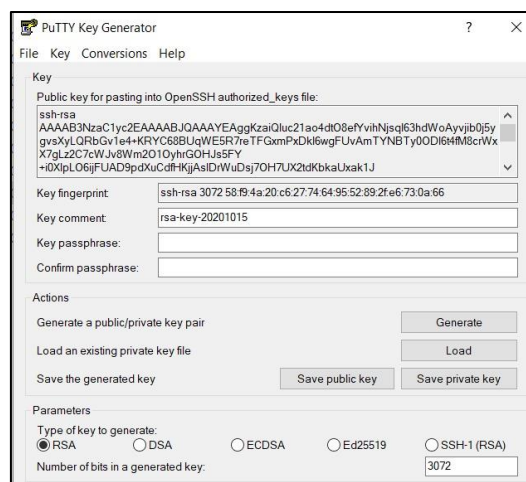


Ilustración 56. Un par de claves SSH generadas por PuTTYgen

158. Tal vez desee aplicar una contraseña a la clave, de modo que esta sea requerida para 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 he utilizado la clave de ejemplo de un dispositivo *gigavue*). Es importante que guardemos la clave pública y, sobretodo, la clave privada utilizando los botones asociados en algún lugar donde no puedan ser accedidas por personas no autorizadas.
159. Con la ventana de la Ilustración 56 aún abierta, se necesita copiar la representación de texto de la clave pública para introducirla en la configuración del dispositivo GigaVUE, lo cual se demuestra en la sección 6.5.2 AÑADIR UNA CLAVE PUBLICA AL EQUIPO GIGAVUE en el dispositivo GigaVUE.

6.5.1.1 CONFIGURACIÓN APPLE MAC/LINUX

160. 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]”

161. 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
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/dhWZ2S0iauIDmBM3c70wQh/7rI1U osheridan@macbook
The key's randomart image is:
+----[RSA 3072]-----+
|
|  + +  o
| . * + * .
| o * EB + o
| * +.S + O +
| + +.. + X = .
| ..o o.o + .
| . ...=.
| oo.o0=0
+-----[SHA256]-----+
macbook:~ osheridan$
```

Ilustración 57. Generación de par de claves publica/privada en un equipo *Apple Macbook*

162. Existe la posibilidad de introducir una contraseña para asegurar aún más la clave privada de SSH si desea hacerlo. Esto es recomendable.

163. La clave pública se almacenará (si se aceptan los valores predeterminados) en el archivo `~/.ssh/id_rsa.pub` y esto puede revelarse utilizando el comando “cat”:

```
macbook:~ osheridan$ cat ~/.ssh/id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDE5qJBPDHVNvtLCYUasKodyTh3i0sR7HWhwmLGL91GEa
mxwTM5xD21IIdgZY7jJ4Prew7UnFT73+vA8n56cGwdPMq11rXuqtMWUBQEDXTDDAmnj4QrviNQ
WaS6/qU0+WoQ+Ss/dx6yhv3FQTSpVeChI5Zorw0orqd09V5dCIPaAI2rZv8B1NXwOFXS80qeJJ
C0ThV7PkFVkt0VDXLH0fWHQIk30BvTgU+06L/niiTN3DjcyHcfQfFxUAF+Yhm5h5L/FLFDLERj
fWJx+AKK908MqKb1L3p3hvxBW8Lz4gf3q4mwDXsDN4rUkqnRc8ZghsXgi3svAiLgYoZ4xDCijv
zR osheridan@macbook
macbook:~ osheridan$
```

Ilustración 58. Mostrar la clave pública SSH en un *Apple Macbook*

164. Esta cadena de salida necesitaremos usarla cuando apliquemos la clave pública de SSH a la configuración del dispositivo GigaVUE, detallada en la siguiente sección.

6.5.2 AÑADIR UNA CLAVE PUBLICA AL EQUIPO GIGAVUE

165. Para este ejemplo, se utiliza el usuario “admin”:

```
gigavue-appliance (config) # ssh client user admin authorized-key sshv2
"ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAi5q9749zQt04ZpaaaGUy0LN5+sF+KVSONKdwwMez4YQtFn
smgMFdQd1mdR7x412w42YI/ZLdwqJh5fXN/vskRje7qLBoQLLUVhiVxM5vh1SJdmsFeG+gWRMJ
YO+hiH8sObju8VLwMgGTM+5LPe5VIY61RJKd/mPs+wwOzLY1a3b1mdUDzvmDnQpkPT7Xwx8uu
+89302DpnjRzhopiXw927S6TNXOP4DDF42wbFwV8Pwtdbra6FGC05FW8N/jcUCLSLqH77BxGU9
G4ips8mxUdYnRCccL007L3XOZDc3ja7oguGk1cwA+V8Lmpuzf3Jf/qmrKP1tGAN05XrxeMLXZw
== gigavue-appliance example key"
gigavue-appliance (config) #
```

Ilustración 59. Añadir clave SSH al equipo

166. Debido a los espacios en la llave pública de SSH, su cadena está encerrada entre dobles comillas. La cadena incluida es la obtenida y copiada en el apartado 6.5.1 ESTABLECER UN PAR DE CLAVES PUBLICA/PRIVADA.

6.5.3 MOSTRAR LAS CLAVES PUBLICAS SSH

167. Para mostrar todas las claves publicas SSH hay que usar el comando **"show ssh client"**:

```
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+KVSONKdwwMez4YQtFn
smgMFdQd1mdR7x412w42YI/ZLdwqJh5fXN/vskRje7qLBoQLLUVhiVxM5vh1SJdmsFeG+gWRMJ
YO+hiH8sObju8VLwMgGTM+5LPe5VIY61RJKd/mPs+wwOzLY1a3b1mdUDzvmDnQpkPT7Xwx8uu
+89302DpnjRzhopiXw927S6TNXOP4DDF42wbFwV8Pwtdbra6FGC05FW8N/jcUCLSLqH77BxGU9
G4ips8mxUdYnRCccL007L3XOZDc3ja7oguGk1cwA+V8Lmpuzf3Jf/qmrKP1tGAN05XrxeMLXZw
== gigavue-appliance example key
gigavue-appliance (config) #
```

Ilustración 60. Mostrar las claves públicas SSH

6.5.4 REVOCAR/ELIMINAR UNA CLAVE PUBLICA DEL EQUIPO GIGAVUE

168. Las claves públicas SSH también puede ser eliminadas de un equipo.
169. A continuación, se muestra un ejemplo de revocación de la llave de *osheridan@linux* (clave 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:
AAAAB3NzaC1yc2EAAAADAQABAAQDQ32742EFYNSKTRZtGBmd6VT+/tFG/j2fM3UDGWDnhzwe
68LzDNC00tWDZxVqiZc9Gf1TIFK8qEq2vuSi4evvLjTrvbdyqjmv4GX1Di0YhyUYnw77DqCMRS
7Jnf4py5DBZRHPsdUIp6xKpqvRs6PEXIK8CET09IXirHRKDMfdFgHo8KEhbdvBLLuUVFrWPZQL
jea9iZLRuf+CdHrda1GI0KdE6Ad3Xsc38LoN1bmQ9ka+5zaquwUrwhLZQeT/FUgpgj58Nsgebv
```

```
BD8PciIvekvrbEmL7HLnEnoQGFUKQiFHXetJk7sW2PBvz5o/uN2ZtWrwgKRSLRGrFocueSc675
NH osheridan@workstation
gigavue-appliance (config) #
```

Ilustración 61. Eliminar una clave SSH autorizada

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

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

171. Cuando se descarga una imagen para actualizar un dispositivo GigaVUE hay varios protocolos que pueden utilizarse para este fin, a saber:

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

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

6.5.6 PAR EVITAR SU USO, SE PUEDE UTILIZAR LA IP, COMO SE DESCRIBE EN LA SECCIÓN ANTERIOR 6.2.1 POLÍTICA DE CONTRASEÑAS DE USUARIO

173. **Se debe establecer una política de fortaleza de contraseñas.**

174. Por defecto las contraseñas deben incluir, al menos:

- Un número.
- Una letra minúscula.
- Una letra mayúscula.
- Un carácter especial (por ejemplo: !, @, #, \$, %, ^, &, or *)

175. La configuración de la longitud mínima de contraseñas permite establecer entre 8-30 caracteres (8 es el valor predeterminado).

176. Para fijar la longitud mínima, se debe 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) #
```

Ilustración 15. Determinar la longitud mínima de password de 12 caracteres

177. En la figura 67 se ha configurado una longitud de 12 caracteres, valor mínimo recomendado.

178. 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
```

Ilustración 16. Deshabilitar el *password blank login* del usuario administrador

6.6 ADMINISTRACIÓN DEL PRODUCTO

6.6.1 CONTROL DE ACCESO BASADO EN ROLES

179. 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.

180. 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.

6.6.1.1 NIVELES DE ACCESO A PUERTOS

181. 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 maps asociados a un Puerto de red	✓	✓	✓	✓	✓
Crear/Editar Mapas asociados a un puerto	✗	✓	✓	✓	✓
Crear tool-mirror a/desde Puerto	✗	✓	✓	✓	✓
Cambiar filtros de salida	✗	✓	✓	✓	✓
Editar parámetros de puertos	✗	✗	✓	✓	✓
Crear pares de puertos	✗	✗	✓	✓	✓
Cambiar tipo de puerto	✗	✗	✗	✓	✓

Ilustración 17. Tabla detallada de niveles de acceso a puertos

182. 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 en conjunto de entre estos 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

183. 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. Y del modo contrario 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

6.6.1.2 MAP BASED ACCESS LEVELS

184. El acceso a los mapas del dispositivo GigaVUE se divide en cuatro 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	✗	✗	✓	✓

Ilustración 18. Tabla detallada de niveles de acceso a mapas

185. Estos niveles de acceso basados en el mapa dictan los diferentes permisos disponibles para los Roles cuando se aplican a una configuración del mapa.
186. La lógica aquí es la descrita en el apartado anterior respecto a los niveles de los puertos, pero aplicado a los mapas.

6.6.1.3 ENTENDER LOS ROLES

187. Los roles permiten agrupar a los usuarios para aplicar privilegios globales a los mapas y puertos.
188. Los roles configurados por defecto son:
- **Admin:** los usuarios asignados a esta función 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 a todos los puertos. Pueden ser considerados como miembros de todos los roles.
 - **Monitor:** Los usuarios asignados a esta función sólo tienen acceso de vista a los puertos y configuraciones.

- **Default:** Esta función 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.
189. Los roles y sus características que vienen configurados por defecto no pueden ser eliminados o modificados.
190. En nuestro sistema de ejemplo tenemos varios usuarios, que pueden ser listados usando 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) #
```

Ilustración 19. Mostrar usuarios

191. Si se quiere, por ejemplo, añadir el usuario *osheridan* a la función de seguridad y el usuario *pmortimer* a la función de red (se asume que estos usuarios ya han sido añadidos). 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) #
```

Ilustración 20. Mostrar los roles configurados

192. En la Ilustración 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) #		

Ilustración 21. Mostrar los roles en formato conciso

193. En primer lugar, es necesario crear los roles deseados ("Red" y "Seguridad") usando el 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,osheridan,pmo...
Security      Security Team          -
Default       -                       -
Network       Networking Team         -
gigavue-appliance (config) #
```

Ilustración 22. Añadir los roles de red y seguridad

194. Una vez agregados los roles, se deben aplicar 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
gigavue-appliance (config) #
```

Ilustración 23. Añadir usuarios a sus respectivos roles

195. En la Ilustración 23 se han usado las opciones de comando **"roles add"** para el usuario *osheridan* y opciones **"roles replace"** para el usuario *pmortimer*. Estos aumentan y reemplazan los roles para cada usuario respectivamente.
196. 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 creo el mapa, a menos que se especifique lo contrario en el campo **"owner_role"** del mapa. Por ejemplo, si el usuario *osheridan* ahora 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 2023/01/23 12:45:33 +0100
## Software version on which this output was taken: GigaVUE-OS 6.5.00
111224 2024-11-12 13:25:35
## Hostname: gigavue-appliance
##
##
## 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
gigavue-appliance (config) #

```

Ilustración 24. El usuario osheridan crea un mapa. Roles aplicados por defecto

197. En la Ilustración 24 se observa que esto se ha creado con éxito, y que el mapa se ha creado con todos los roles que tiene el usuario que creó el mapa.
198. Si ahora tratamos de crear una regla con el usuario pmortimer:

```

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) #

```

Ilustración 25. Creación de un mapa con un usuario sin rol de administrador

199. En la Ilustración 25 podemos ver que el usuario *pmortimer*, que es un miembro del rol de red exclusivamente, no puede crear un mapa. Esto se debe a que no es posible crear un mapa que contenga puertos a los que este rol no tenga acceso.
200. Es importante destacar que un Mapa tiene dos 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.”**.
201. Así que habrá que verificar que el usuario *pmortimer* tenga permisos suficientes para ambos puertos el de Red y el de Herramientas.
202. Primero verificaremos el puerto de red (en este ejemplo 1/1/g1). Mirando los Controles de Acceso a los Puertos (ver sección anterior con la tabla asociada, Ilustración 17) podemos determinar que como mínimo se requiere el Nivel 2 para “Crear/Editar Mapas asociados a un puerto”.

203. Como usuario *osheridan* (que tiene el rol de administrador asignado) podemos hacer este cambio, añadiendo el rol *Network* como Nivel2 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)                    : -
gigavue-appliance (config) #
```

Ilustración 26. El usuario *osheridan* cambiando el rol asignado para el puerto 1/1/g1

204. Ahora intentamos configurar el mapa de nuevo como usuario *pmortimer*:

```
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.
gigavue-appliance (config) #
```

Ilustración 27. El usuario *pmortimer* intenta de nuevo añadir un mapa

205. En la Ilustración 27 se observa que se ha vuelto a denegar la acción 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)                    : -
gigavue-appliance (config) #
```

Ilustración 28. Asignar privilegios de nivel 2 al rol de *Network*

206. Con los permisos establecidos se puede ahora añadir en el mapa con éxito como usuario *pmortimer*, ya que pertenece al rol *Network*, el cual tiene ahora Nivel2 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) #
```

Ilustración 29. Configuración exitosa del mapa por el usuario *pmortimer*

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

6.6.1.4 DISMINUCIÓN DE LOS PRIVILEGIOS DE LA CUENTA ADMIN

208. Aunque no es posible eliminar la cuenta de administrador en un dispositivo GigaVUE, sí es posible cambiar los privilegios de esta cuenta a la categoría de “monitor” reduciendo sus privilegios en el sistema.
209. Se recomienda 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 perderíamos 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.
210. Para asociar la cuenta de administrador con la función 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                osherman,pmortimer
Default              -
gigavue-appliance (config) #
```

Ilustración 30. Asignar la función de Monitor a la cuenta admin

211. Se puede ver en la figura anterior que el usuario *admin* ha sido asociado al rol “Monitor”. Como evidencia de este cambio, se puede acceder al dispositivo GigaVUE y se intenta cambiar el banner y añadir en 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 6.5.00 111224 2024-11-12 13:25:35
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) #
```

Ilustración 31. La cuenta de administración después de asociarla al rol Monitor

212. Se comprueba que efectivamente el usuario *admin* no ha podido hacer ningún cambio en la configuración.

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

213. La cuenta de administrador y/u otras, pueden ser objeto de ataques de fuerza bruta por lo que se deben establecer mecanismos para protegerla.
214. Existen dos métodos de restricción temporal para inicios de sesión fallido.
215. 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)
```

Ilustración 32. Asignar un tiempo entre accesos fallidos

216. Además, se puede especificar un número de intentos de inicio de sesión fallidos (*attempts lockout max-fail*) y el tiempo (*attempts lockout time*) que esta cuenta se bloqueará en segundos. Los rangos son:

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

```
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)

```

Ilustración 33. Asignar un tiempo entre accesos fallidos

6.6.2 BLOQUEO DE SESIÓN

217. Se recomienda asignar un valor de tiempo máximo de inactividad, tras el cual se procederá al bloqueo de sesiones de CLI y *WebUI*.
218. 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 (CLI, que abarca las sesiones SSH y Serial).
219. 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.

6.6.2.1 WEBUI TIMEOUTS

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

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

Ilustración 34. Configuración del cierre de sesión automático de la interfaz de usuario de la web

221. 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).

6.6.2.2 CLI TIMEOUTS

222. Hay dos (2) opciones para la configuración de este tiempo de espera; una por sesión y otra de forma permanente.
223. 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) #
```

Ilustración 35. Configurar el cierre de sesión automático de la interfaz de usuario de la CLI

224. En el ejemplo anterior se ha fijado el periodo a 10 minutos, pero 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.
225. 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) #
```

Ilustración 36. Configuración del interfaz CLI de auto logout

226. Como en el caso del tiempo de espera de la sesión, en el ejemplo anterior se utilizan 10 minutos y se puede ajustar a cualquier valor entre 0,25 minutos (15 segundos) y 35791 minutos (596 horas y 31 minutos).

227. Al igual que con los ajustes de la sesión, el tiempo de espera puede ser desactivado utilizando un valor de 0; sin embargo, no se recomienda.

6.6.3 BANNERS

228. Los equipos de Gigamon permiten configurar banner a mostrar durante el proceso de acceso a los equipos siendo esto posible por:

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

6.6.3.1 BANNER PRE-LOGIN (POR DEFECTO)

229. Se debe configurar un **banner** previo al inicio de sesión que suministre información sobre las políticas de seguridad definidas en la organización.
230. El **banner** aparece en la pantalla de inicio de sesión.
231. 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.
232. Para accesos WEB, será justo después de la pantalla de inicio mediante un pop-up.
233. En el texto del banner se pueden utilizar varias líneas, la cadena está encapsulada entre comillas:

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

Ilustración 37. Añadir un banner pre-login

6.6.3.1.1 BANNER LOCAL

234. Este tipo de banner sustituye al banner por defecto y se mostrará solo para accesos locales (terminal).
235. De nuevo, se pueden utilizar varias líneas, la cadena está encapsulada entre comillas.

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

Ilustración 38. Añadir un banner login local

6.6.3.1.2 BANNER REMOTE

236. Este tipo de banner sustituye al banner por defecto y se mostrará solo para accesos remotos (ssh y web).
237. Se pueden utilizar varias líneas, la cadena está encapsulada entre comillas.

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

Ilustración 39. Añadir un banner remote local

6.6.3.1.3 BANNER POST LOGIN

238. También se recomienda configurar un *banner* de acceso al puesto que proporcione detalles adicionales de los que se desee informar a los usuarios después de que hayan entrado en el sistema.

239. 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"
```

Ilustración 40. Anadir un banner post login

240. POLÍTICA DE CONTRASEÑAS DE USUARIO

241. **Se debe establecer una política de fortaleza de contraseñas.**

242. Por defecto las contraseñas deben incluir, al menos:

- Un número.
- Una letra minúscula.
- Una letra mayúscula.
- Un carácter especial (por ejemplo: !, @, #, \$, %, ^, &, or *)

243. La configuración de la longitud mínima de contraseñas permite establecer entre 8-30 caracteres (8 es el valor predeterminado).

244. Para fijar la longitud mínima, se debe 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) #
```

Ilustración 15. Determinar la longitud mínima de password de 12 caracteres

245. En la figura 67 se ha configurado una longitud de 12 caracteres, valor mínimo recomendado.

246. 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
```

Ilustración 16. Deshabilitar el *password blank login* del usuario administrador

6.7 ADMINISTRACIÓN DEL PRODUCTO

6.7.1 CONTROL DE ACCESO BASADO EN ROLES

247. 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.

248. 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.

6.7.1.1 NIVELES DE ACCESO A PUERTOS

249. 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 maps asociados a un Puerto de red	✓	✓	✓	✓	✓
Crear/Editar Mapas asociados a un puerto	✗	✓	✓	✓	✓
Crear tool-mirroring a/desde Puerto	✗	✓	✓	✓	✓
Cambiar filtros de salida	✗	✓	✓	✓	✓
Editar parámetros de puertos	✗	✗	✓	✓	✓
Crear pares de puertos	✗	✗	✓	✓	✓
Cambiar tipo de puerto	✗	✗	✗	✓	✓

Ilustración 17. Tabla detallada de niveles de acceso a puertos

250. 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 en conjunto de entre estos 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

251. 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. Y del modo contrario 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

6.7.1.2 MAP BASED ACCESS LEVELS

252. El acceso a los mapas del dispositivo GigaVUE se divide en cuatro 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"
----------	------------------------------	---------------------------	-------------------------------	--

<i>Ver Mapa</i>	✓	✓	✓	✓
<i>Añadir puerto de herramienta</i>	✗	✓	✓	✓
<i>Eliminar puerto de herramienta</i>	✗	✓	✓	✓
<i>Eliminar puerto de red</i>	✗	✗	✓	✓
<i>Añadir puerto de red</i>	✗	✗	✓	✓
<i>Eliminar/Editar Mapa</i>	✗	✗	✓	✓
<i>Compartir mapa</i>	✗	✗	✓	✓

Ilustración 18. Tabla detallada de niveles de acceso a mapas

253. Estos niveles de acceso basados en el mapa dictan los diferentes permisos disponibles para los Roles cuando se aplican a una configuración del mapa.
254. La lógica aquí es la descrita en el apartado anterior respecto a los niveles de los puertos, pero aplicado a los mapas.

6.7.1.3 ENTENDER LOS ROLES

255. Los roles permiten agrupar a los usuarios para aplicar privilegios globales a los mapas y puertos.
256. Los roles configurados por defecto son:
- **Admin:** los usuarios asignados a esta función 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 a todos los puertos. Pueden ser considerados como miembros de todos los roles.
 - **Monitor:** Los usuarios asignados a esta función sólo tienen acceso de vista a los puertos y configuraciones.
 - **Default:** Esta función 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.
257. Los roles y sus características que vienen configurados por defecto no pueden ser eliminados o modificados.
258. En nuestro sistema de ejemplo tenemos varios usuarios, que pueden ser listados usando 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) #

```

Ilustración 19. Mostrar usuarios

259. Si se quiere, por ejemplo, añadir el usuario *osheridan* a la función de seguridad y el usuario *pmortimer* a la función de red (se asume que estos usuarios ya han sido añadidos). 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) #
```

Ilustración 20. Mostrar los roles configurados

260. En la Ilustración 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) #
```

Ilustración 21. Mostrar los roles en formato conciso

261. En primer lugar, es necesario crear los roles deseados ("Red" y "Seguridad") usando el 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) #

```

Ilustración 22. Añadir los roles de red y seguridad

262. Una vez agregados los roles, se deben aplicar 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
gigavue-appliance (config) #

```

Ilustración 23. Añadir usuarios a sus respectivos roles

263. En la Ilustración 23 se han usado las opciones de comando **“roles add”** para el usuario *osheridan* y opciones **“roles replace”** para el usuario *pmortimer*. Estos aumentan y reemplazan los roles para cada usuario respectivamente.
264. 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 creo el mapa, a menos que se especifique lo contrario en el campo **“owner_role”** del mapa. Por ejemplo, si el usuario *osheridan* ahora 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 2023/01/23 12:45:33 +0100
## Software version on which this output was taken: GigaVUE-OS 6.5.00
111224 2024-11-12 13:25:35
## Hostname: gigavue-appliance
##
##
## 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

```

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

Ilustración 24. El usuario osheridan crea un mapa. Roles aplicados por defecto

265. En la Ilustración 24 se observa que esto se ha creado con éxito, y que el mapa se ha creado con todos los roles que tiene el usuario que creó el mapa.
266. Si ahora tratamos de crear una regla con el usuario pmortimer:

```
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) #
```

Ilustración 25. Creación de un mapa con un usuario sin rol de administrador

267. En la Ilustración 25 podemos ver que el usuario *pmortimer*, que es un miembro del rol de red exclusivamente, no puede crear un mapa. Esto se debe a que no es posible crear un mapa que contenga puertos a los que este rol no tenga acceso.
268. Es importante destacar que un Mapa tiene dos 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.**”.
269. Así que habrá que verificar que el usuario *pmortimer* tenga permisos suficientes para ambos puertos el de Red y el de Herramientas.
270. Primero verificaremos el puerto de red (en este ejemplo 1/1/g1). Mirando los Controles de Acceso a los Puertos (ver sección anterior con la tabla asociada, Ilustración 17) podemos determinar que como mínimo se requiere el Nivel 2 para “Crear/Editar Mapas asociados a un puerto”.
271. Como usuario *osheridan* (que tiene el rol de administrador asignado) podemos hacer este cambio, añadiendo el rol *Network* como Nivel2 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)                    : -
gigavue-appliance (config) #
```

Ilustración 26. El usuario osheridan cambiando el rol asignado para el puerto 1/1/g1

272. Ahora intentamos configurar el mapa de nuevo como usuario *pmortimer*:

```
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.
gigavue-appliance (config) #

```

Ilustración 27. El usuario *pmortimer* intenta de nuevo añadir un mapa

273. En la Ilustración 27 se observa que se ha vuelto a denegar la acción 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)                    :
gigavue-appliance (config) #

```

Ilustración 28. Asignar privilegios de nivel 2 al rol de Network

274. Con los permisos establecidos se puede ahora añadir en el mapa con éxito como usuario *pmortimer*, ya que pertenece al rol *Network*, el cual tiene ahora Nivel2 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) #

```

Ilustración 29. Configuración exitosa del mapa por el usuario *pmortimer*

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

6.7.1.4 DISMINUCIÓN DE LOS PRIVILEGIOS DE LA CUENTA ADMIN

276. Aunque no es posible eliminar la cuenta de administrador en un dispositivo GigaVUE, sí es posible cambiar los privilegios de esta cuenta a la categoría de “monitor” reduciendo sus privilegios en el sistema.
277. Se recomienda 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 perderíamos 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.

278. Para asociar la cuenta de administrador con la función 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) #
```

Ilustración 30. Asignar la función de Monitor a la cuenta admin

279. Se puede ver en la figura anterior que el usuario *admin* ha sido asociado al rol “Monitor”. Como evidencia de este cambio, se puede acceder al dispositivo GigaVUE y se intenta cambiar el banner y añadir en 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 6.5.00 111224 2024-11-12 13:25:35
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) #
```

Ilustración 31. La cuenta de administración después de asociarla al rol Monitor

280. Se comprueba que efectivamente el usuario *admin* no ha podido hacer ningún cambio en la configuración.

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

281. La cuenta de administrador y/u otras, pueden ser objeto de ataques de fuerza bruta por lo que se deben establecer mecanismos para protegerla.
282. Existen dos métodos de restricción temporal para inicios de sesión fallido.

283. 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)
```

Ilustración 32. Asignar un tiempo entre accesos fallidos

284. Además, se puede especificar un número de intentos de inicio de sesión fallidos (*attempts lockout max-fail*) y el tiempo (*attempts lockout time*) que esta cuenta se bloqueará en segundos. Los rangos son:

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

```
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): none
```

Ilustración 33. Asignar un tiempo entre accesos fallidos

6.7.2 BLOQUEO DE SESIÓN

285. Se recomienda asignar un valor de tiempo máximo de inactividad, tras el cual se procederá al bloqueo de sesiones de CLI y *WebUI*.
286. 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 (CLI, que abarca las sesiones SSH y Serial).
287. 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.

6.7.2.1 WEBUI TIMEOUTS

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

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

Ilustración 34. Configuración del cierre de sesión automático de la interfaz de usuario de la web

289. 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).

6.7.2.2 CLI TIMEOUTS

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

291. 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) #
```

Ilustración 35. Configurar el cierre de sesión automático de la interfaz de usuario de la CLI

292. En el ejemplo anterior se ha fijado el periodo a 10 minutos, pero 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.

293. 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) #
```

Ilustración 36. Configuración del interfaz CLI de auto logout

294. Como en el caso del tiempo de espera de la sesión, en el ejemplo anterior se utilizan 10 minutos y se puede ajustar a cualquier valor entre 0,25 minutos (15 segundos) y 35791 minutos (596 horas y 31 minutos).

295. Al igual que con los ajustes de la sesión, el tiempo de espera puede ser desactivado utilizando un valor de 0; sin embargo, no se recomienda.

6.7.3 BANNERS

296. Los equipos de Gigamon permiten configurar banner a mostrar durante el proceso de acceso a los equipos siendo esto posible por:

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

6.7.3.1 BANNER PRE-LOGIN (POR DEFECTO)

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

298. El *banner* aparece en la pantalla de inicio de sesión.

299. 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.
300. Para accesos WEB, será justo después de la pantalla de inicio mediante un pop-up.
301. En el texto del banner se pueden utilizar varias líneas, la cadena está encapsulada entre comillas:

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

Ilustración 37. Añadir un banner pre-login

6.7.3.1.1 BANNER LOCAL

302. Este tipo de banner sustituye al banner por defecto y se mostrará solo para accesos locales (terminal).
303. De nuevo, se pueden utilizar varias líneas, la cadena está encapsulada entre comillas.

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

Ilustración 38. Añadir un banner login local

6.7.3.1.2 BANNER REMOTE

304. Este tipo de banner sustituye al banner por defecto y se mostrará solo para accesos remotos (ssh y web).
305. Se pueden utilizar varias líneas, la cadena está encapsulada entre comillas.

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

Ilustración 39. Añadir un banner remote local

6.7.3.1.3 BANNER POST LOGIN

306. También se recomienda configurar un *banner* de acceso al puesto que proporcione detalles adicionales de los que se desee informar a los usuarios después de que hayan entrado en el sistema.
307. 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"
```

Ilustración 40. Anadir un banner post login

308. Cuando se utiliza SCP o SFTP se debe utilizar pares de claves públicas/privadas.
309. 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 6.11.4
- EVENTOS DEL EQUIPO: ALMACENAMIENTO REMOTO

6.7.4 GENERACIÓN DE UNA CLAVE PÚBLICA DE IDENTIDAD

310. 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. Además, los métodos criptográficos garantizan que esa pareja de claves solo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves. 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.

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

```
gigavue-appliance (config) # ssh client user admin identity rsa2 generate
gigavue-appliance (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
AAAAB3NzaC1yc2EAAAADAQABAAQDFDXa1pgt1jbM+ovyBWs8AGPPLZRm4Nksg1jKUDsDSn
+bPomeH9HoxJ8Wrp7gGcCyAvkjadskd/z3jQALJikKIYfYu5DYsRdCdLuuFN3hr90Ec4Sotd
eIkr8dBbHV8SMqN4CNf3GN4ROHnLxOPqYD/NnP9m70nvM4JquTqIqmjE7VPrgWqq4ufn+c/Gk
Y4BaAMGvLD8zeapuOsXV3nnkbu4TJOASyPW0GkOzMMN+sIKzqZXqtQMNJP12BxH0t2boamqAG
ROD0qu1euh5SY71jnQdR+PeiiD3nvvvveg4q1DuRhoYiEnyEbxnzXxs32/Wv4qE2zb9BTHOKr
PqIg2kJ
  RSAv2 Private key:
*****
  Passphrase:
*****
SSH authorized keys:
  User admin:
    Key 1: ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQD3/bVLsAlTzJvjfvU2sZGGZk9dJw74q4YLHQtpWd8F5
H4MYtV6Cieb5wp2bGtNZuDAfIampQPA4HZWWTyvekdbba8IgTfIUgmeYdX91J0JuPKspXUHIW
eUS02yJxRjJ9r2rqs2sFHZfxu8Cf51wusTiE+xJydBCfv+TIU12345678rJueADrxDpwb1gQ
6EG3PS6bc7+k2PGOJP+GaI9HbhcjxLKLICP5FsdPHnbptS1TQPLjXN0QJTUwBIde7QiFZBXWI
HD1QRqhQK5WJZ6S1C++bUXvQFmqBd4B4LEQu0YyLLwx3zxzo6LkOMGkjKHU6Lmwb+0iDyvD5Q
87+c8RH admin@remote
gigavue-appliance (config) #
```

Ilustración 62. Muestra de clave de identidad SSH para el usuario admin

312. En la Ilustración 62 se muestra la clave pública RSAv2 para el usuario administrador. 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.
313. En dicha Figura también se observa la existencia de una sección de claves autorizadas que no deben confundirse; **éstas se utilizan para autenticar al dispositivo GigaVUE.**

6.8 TRANSPORT LAYER SECURITY (TLS)

314. 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 la versión 3 de este protocolo.
 - Interfaz de LDAP si se utiliza secureLDAP de este protocolo.
315. 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.
316. La configuración de las características iSSL y SSL Fuera de Banda GigaSMART están fuera del alcance de este documento.

6.8.1 INSTALAR CERTIFICADO

317. Para instalar su propio certificado, hay dos (2) métodos:
- Instalar un certificado y clave privada ya creados.
 - Instalar un certificado en base a una petición de firma de certificado, *Certification Signing Request (CSR)*.

6.8.1.1 INSTALACIÓN DE UN CERTIFICADO Y CLAVE PRIVADA EXISTENTES

318. Si ya se dispone de un certificado y una clave privada, se puede instalar en el dispositivo GigaVUE de la siguiente manera (teniendo en cuenta que no se proporciona el certificado completo. La sección eliminada se indica con [TRUNCATED]):

```
gigavue-appliance (config) # crypto certificate name gigavue-appliance
public-cert pem "
> -----BEGIN CERTIFICATE-----
> MIIEEjCCA16gAwIBAgIIa6thcUvlstEwDQYJKoZIhvcNAQELBQAwgBYxCzAJBgNV
[TRUNCATED]
> ZrT24HNNYyVhZ2ExbJ3gOKrLi1aArvYcVDJ0EIZ7j9SGLeE/seLwHW8
> -----END CERTIFICATE-----"
Successfully installed certificate with name 'gigavue-appliance'
gigavue-appliance (config) #
```

Ilustración 63. Aplicar un certificado existente previamente

319. A continuación, se añade la clave privada al dispositivo GigaVUE de la siguiente manera (teniendo en cuenta que no se proporciona la clave privada completa. La sección eliminada se indica con [TRUNCATED]):

```
gigavue-appliance (config) # crypto certificate name gigavue-appliance
private-key pem "
> -----BEGIN RSA PRIVATE KEY-----
> MIIIEogIBAAKCAQEAA3KQVZvo00RiEY0QMYgH4BKttV8Z4D46FE5pOVsJ44WzJq1Bd
[TRUNCATED]
> rRQX8b+0k1IXVHfAihBv3LuFMGM1mknagKdBJwrtYbKZdoX5V+A=
> -----END RSA PRIVATE KEY-----"
Enter private key passphrase (if required):
gigavue-appliance (config) #
```

Ilustración 64. Aplicar un certificado existente previamente

320. A continuación, se activa el certificado:

```
gigavue-appliance (config) # web https certificate name gigavue-appliance
gigavue-appliance (config) #
```

Ilustración 65. Activación del certificado

321. Para ver los certificados cargado, se puede hacer uso del comando **"show crypto certificate"**:

```

gigavue-appliance (config) # show crypto certificate
Certificate with name 'gigavue-appliance'
  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:               gigavue-appliance
    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:               gigavue-appliance
    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:               gigavue-appliance
    Country:                   US
    State or Province:         California
    Locality:                   Santa Clara
    Organization:               Gigamon Inc.
    Organizational Unit:        Gigamon Network Visibility Systems
    E-mail Address:             admin@gigamon.com
gigavue-appliance (config) #

```

Ilustración 66. Ejemplo de muestra de certificado desplegado

6.8.1.2 CREACIÓN DE UN CSR PARA CERTIFICADOS INCORPORADOS Y CLAVES PRIVADAS

322. 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.

323. Para crear y cargar una 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) #
```

Ilustración 67. Creación de un CSR

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

325. 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.

326. Hay más opciones disponibles para un CSR. Para consultarlas, se puede acceder a la Guía del Usuario [REF1] para más información tal y como se describe en la introducción de este documento.

6.8.2 CONFIGURACIÓN DE VERSIÓN DE TLS PARA EL INTERFAZ DE GESTIÓN

327. 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) #
```

Ilustración 68. Opciones para establecer la versión mínima de TLS

328. 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) #
```

Ilustración 69. Establecimiento de la versión mínima de TLS a TLS1.2

6.9 ACTUALIZACIONES

329. Los equipos no se actualizan automáticamente ni avisan de nuevas versiones disponibles. Sin embargo, Gigamon envía por mail notificaciones de nuevas versiones disponibles a todos sus clientes.
330. El proceso para actualizar el producto consta de tres fases.
331. Primero habrá que descargar la versión de software en el propio equipo. Los protocolos disponibles para importar las imágenes son:
- http
 - https
 - ftp
 - tftp
 - scp
 - sftp
332. 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%
[#####]
#####
#####]
```

Ilustración 70. Descarga de actualizaciones de software

333. Una vez descargado el software verificar que efectivamente está disponible para su instalación:

```
gigavue-appliance (config)# show images
Installed images:
  Partition 1:
    GigaVUE-OS 6.5.00 111224 2024-11-12 13:25:35 6x86_64 gihc1
root@jenkins-slave022:git:ba83fe15c6c6
  Partition 2:
    GigaVUE-OS 6.5.00 111224 2024-11-12 13:25:35 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)
```

Ilustración 71. Listado de versiones de software instaladas y disponibles

334. Ahora habrá que instalar la imagen disponible en la partición que no está activa ahora mismo. Como se observa en la imagen el primer paso de la instalación es una verificación de

que la imagen es válida y ha sido generada por Gigamon para eviar así la instalación de imágenes de terceros:

```
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%
[#####]
#####]
```

Ilustración 72. Proceso de instalación de actualizaciones

335. Verificar que la actualización se ha instalado y forzar el reinicio desde la otra partición:

```
gigavue-appliance (config)# show images
Installed images:
Partition 1:
GigaVUE-OS 6.5.00 111224 2024-11-12 13:25:35 x86_64 gihc1 root@jenkins-
slave022:git:ba83fe15c6c6
Partition 2:
GigaVUE-OS 6.5.00 111224 2024-11-12 13:25:35 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
```

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

6.10 BACKUP

336. Los equipos pueden tener muchas configuraciones guardadas y cargar la deseada en cada momento. Para ello se podrá generar tantos archivos de configuración como se desee.

337. El sistema además 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.

338. Para guardar la configuración que está en memoria en disco usar:

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

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

Ilustración 74. Guardar configuración en disco

339. Si se desea guardar la configuración en otro archivo de configuración usar:

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

Ilustración 75. Guardar configuración en otro archivo de configuración

340. Si se desea que este nuevo archivo de configuración no sea ahora 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) #
```

Ilustración 76. Guardar configuración en otro archivo de configuración

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

```
gigavue-appliance (config) # show configuration files
initial
initial.bak
my_config
my_config (active)
snapdb.tms
gigavue-appliance (config) #
```

Ilustración 77. Listado de configuraciones existentes

342. Una vez modificada la configuración se podrá volver a cargar la última configuración guardada mediante:

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

Ilustración 78. Recuperar la última configuración guardada

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

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

Ilustración 79. Recuperar cualquier configuración anterior

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

- FTP
- TFTP
- SCP
- SFTP

345. El commando a usar sería:

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

Ilustración 80. Exportar configuraciones

6.11 AUDITORÍA

6.11.1 DETERMINAR LA ZONA HORARIA A UTC

346. Para fijar la zona horaria a UTC, 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) #
```

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

6.11.1.1 CONFIGURAR NTP

347. 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) #
```

Ilustración 82. Fijar y mostrar la configuración de NTP

348. También es posible configurar las claves para el servidor NTP, ver la Guía del Usuario para más información. 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.

6.11.2 EVENTOS DEL EQUIPO

349. El nivel de auditoría por defecto ("*NOTICE*") proporciona el registro de todos los comandos introducidos por los usuarios, proporcionando así información de auditoría para cualquier cambio de configuración.

350. Existen los siguientes niveles de auditoría:

Nivel de Auditoría	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	Condición normal pero significativa.
info	Mensajes informativos.
debug	Mensajes de nivel de depuración. Autorizado para uso exclusivo en fábrica.

Tabla 2. Nivel de Auditoría

351. Se puede especificar de manera separada la criticidad para:

- Local: Eventos guardados en archivos locales del equipo.
- Traps: Nivel de eventos que se enviarán por SNMP en caso de estar configurado.
- Remotos: Eventos que se enviarán a un syslog remoto en caso de estar habilitado.

6.11.3 EVENTOS DEL EQUIPO: ALMACENAMIENTO LOCAL

352. Los eventos del equipo se almacenan automáticamente en una partición local independiente y su rotación es automática y cíclica.

353. Se pueden comprobar los eventos guardados con:

```
gigavue-appliance (config) # show Logs
```

Ilustración 83. Ver los logs guardados localmente

354. Se pueda cambiar la criticidad de los logs locales con

```
gigavue-appliance (config) # logging local
alert crit emerg err info none notice warning
```

Ilustración 84. Cambiar la criticidad de los logs locales

355. Se puede forzar la rotación de los logs:

```
gigavue-appliance (config) # logging files rotation force
```

Ilustración 84. Forzar la rotación de los logs locales

356. Se pueden ver los archivos existen en el sistema con el comando:

```
gigavue-appliance (config) show log files
1
2
3
4
```

Ilustración 85. Archivos de logs existentes

357. Se pueden borrar los logs con el comando logs:

```
gigavue-appliance (config) # logging files delete oldest/current
```

Ilustración 86. Eliminar logs del sistema local

358. Los logs se eliminan automáticamente cada 30 días.

6.11.4 EVENTOS DEL EQUIPO: ALMACENAMIENTO REMOTO

359. 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.

360. 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.

361. 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
```

Ilustración 87. Habilitar logging en un equipo GigaVUE

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

363. 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.

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

364. 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).
- 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 de *Linux* sobre *TCP*.

365. 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.

366. 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")
```

Ilustración 88. Configuración por defecto de rsyslog.conf

367. A:

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

Ilustración 89. Cambio de configuración de rsyslog.conf

368. El reinicio del servicio (CentOS 8.1 usa *systemd*. En otra distribución, puede ser diferente):

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

Ilustración 90. Reinicio del servicios rsyslog como root

369. 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) #
```

Ilustración 91. Configuración del equipo GigaVUE para enviar syslog cifrado al servidor remoto

370. 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*.

6.11.5 ALMACENAMIENTO REMOTO

371. Se recomienda que todos los eventos registrados sean transportados a un servidor de terceros mediante.

372. El nivel de auditoría por defecto ("NOTICE") proporciona el registro de todos los comandos introducidos por los usuarios, proporcionando así información de auditoría para cualquier cambio de configuración.

373. Existen los siguientes niveles de auditoría:

Nivel de Auditoría	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	Condición normal pero significativa.

info	Mensajes informativos.
debug	Mensajes de nivel de depuración. Autorizado para uso exclusivo en fábrica.

Tabla 3. Nivel de Auditoría

374. 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.
375. 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.
376. 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
```

Ilustración 88. Habilitar logging en un equipo GigaVUE

377. El ejemplo anterior, se enviarán al servidor configurado todos los comandos introducidos por los usuarios que utilizan el dispositivo GigaVUE (con nivel de "NOTICE").
378. 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.

6.12 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

379. SNMP es un protocolo útil para supervisar la actividad de los dispositivos de red. Sin embargo, **no se deben usar SNMPv1 y SNMPv2** porque se autentican mediante contraseñas en texto plano.
380. **Se debe utilizar, por tanto, SNMPv3** que aporta mejoras de seguridad. La autenticación ya no se realiza mediante contraseñas en texto plano. 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

381. 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 en 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, eliminando (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

NPB	Network Packet Broker
CLI	Command Line Interface
GUI	Graphical User Interface
RMA	Return Material Authorization
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ACL	Access Control List
SSH	Secure Shell
SCP	Secure Copy Protocol
SFTP	Secure File Transfer Protocol
TLS	Transport Layer Security
HTTPS	HyperText Transfer Protocol Secure
SNMP	Simple Network Management Protocol
LDAP	Lightweight Directory Access Protocol
CSR	Certificate Signing Request
RBAC	Role-Based Access Control
UTC	Coordinated Universal Time
NTP	Network Time Protocol
SNMPv3	Simple Network Management Protocol version 3
Syslog	System Logging Protocol

9 REFERENCIAS

- [REF1] *GigaVUE-OS 6.5.00 – Guía de usuario*
<https://docs.gigamon.com/doclib65/Content/gigaDoc-Lib-Welcome-intro.html>
- [REF2] *Certificación Common Criteria de la tecnología Giga-VUE OS de Gigamon*
<https://www.niap-ccevs.org/products/11487>
- [REF3] *Certificación FIPS 140-2 de la tecnología Giga-VUE OS de Gigamon*
https://docs.gigamon.com/doclib65/Content/GV-Admin/FM-FIPS_140_2_Compliance.html?Highlight=fips
- [REF4] *Certificación UC APL de la tecnología Giga-VUE OS de Gigamon*
https://docs.gigamon.com/doclib65/Content/GV-Admin/UC_APL_Compliance.html?Highlight=uc%20apl

10 ABREVIATURAS

ACL	Lista de control de acceso.
CLI	Interfaz de Línea de Comando
CSR	Petición de firma de certificado
FTP	Protocolo de transferencia de ficheros
HTTP	Protocolo de transferencia de hipertexto
NTP	Protocolo de tiempo de red
RBAC	Control de Acceso Basado en Roles
SCP	Protocolo de copia segura
SNMP	Protocolo de gestión de red simple
RMA	Autorización de retorno de material
SSH	Secure Shell
UTC	Tiempo Universal Coordinado
TLS	Seguridad en capa de transporte
SSL	Capa de Sockets Seguros
GUI	Interfaz gráfico de usuario
SFTP	Protocolo de transferencia segura de ficheros
TACACS	Sistema de Control de Acceso Mediante Control del Acceso desde Terminales
RADIUS	Servicio de autenticación remota de usuario Dial-In
IP	Protocolo Internet
Syslog	Protocolo de registro de sistema
HTTPS	Protocolo de transferencia de hipertexto Seguro
ENS	Esquema Nacional de Seguridad.

