Guía de Seguridad de las TIC
CCN-STIC 1613

Procedimiento de Empleo Seguro
F5 BIG-IP para LTM+AFM



Noviembre 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN, ou=SELLO ELECTRONICO, 2.5.4.97=VATES-S2800155J, serialNumber=S2800155J, cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

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.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 3
2 OBJETO Y ALCANCE 3
3 ORGANIZACIÓN DEL DOCUMENTO 4
4 FASE PREVIA A LA INSTALACIÓN 5
4.1 ENTREGA SEGURA DEL PRODUCTO 5
4.2 ENTORNO DE INSTALACIÓN SEGURO 5
4.3 REGISTRO Y LICENCIAS 5
4.4 CONSIDERACIONES PREVIAS 6
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 10
5 FASE DE INSTALACIÓN 11
6 FASE DE CONFIGURACIÓN 12
6.1 MODO DE OPERACIÓN SEGURO 12
6.2 AUTENTICACIÓN 12
6.3 ADMINISTRACIÓN DEL PRODUCTO 13
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 13
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 13
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 15
6.5 GESTIÓN DE CERTIFICADOS 16
6.6 SINCRONIZACIÓN 16
6.7 ACTUALIZACIONES 16
6.8 AUTO-CHEQUEOS 17
6.9 ALTA DISPONIBILIDAD 18
6.10 AUDITORÍA 19
6.10.1 REGISTRO DE EVENTOS 19
6.10.2 ALMACENAMIENTO LOCAL 21
6.10.3 ALMACENAMIENTO REMOTO 21
6.11 BACKUP 24
6.12 FIREWALL 25
6.13 BALANCEADOR DE CARGA 25
6.14 MITIGACIÓN DE VULNERABILIDADES 25
7 REFERENCIAS 27
8 ABREVIATURAS 29

ÍNDICE DE TABLAS

Tabla 1. Modelos cualificados 4
Tabla 2. Comandos TMSH no permitidos 8
Tabla 3. Módulos iControl no permitidos 8
Tabla 4. Interfaces iControl no permitidos 9
Figura 1. Entorno operacional del producto. 10
Figura 2. Comprobación de la versión. 11
Tabla 5. Artículos de referencia 15

1 INTRODUCCIÓN

El producto BIG-IP de F5 es un dispositivo de red orientado al mercado del ADC, "Application Delivery Controller". Esta herramienta ofrece múltiples funcionalidades que permiten adaptar, securizar y optimizar la entrega de las aplicaciones en los entornos más demandantes. Además, dispone de diversos licenciamientos de software que permiten desplegar funcionalidades específicas de control de acceso, seguridad, disponibilidad y optimización.

Para llevar a cabo estas funcionalidades en cualquier entorno, F5 dispone de un amplio catálogo de equipos que ofrecen soluciones para cualquier tipo de cliente. F5 ofrece tanto sistemas de bajo coste con un rendimiento más limitado como sistemas con un mayor rendimiento, escalabilidad y funcionalidad. Además, F5 ofrece la solución en modalidad virtual, adaptable a los hipervisores más distribuidos en el mercado.

Entre todas sus funcionalidades posibles, destacan sus módulos AFM (Advanced Firewall Manager) y LTM (Local Traffic Management), que permiten implementar funcionalidades de cortafuegos y de balanceo de carga respectivamente.

2 OBJETO Y ALCANCE

El objeto del presente documento es servir como guía para realizar una instalación, configuración y operación seguras de BIG-IP en su versión 17.1.0.1, centrándose en sus módulos AFM y LTM, siendo aplicable tanto a su modalidad virtual (BIG-IP Virtual Edition) como a los siguientes modelos de hardware:

ISERIES	i4000 series	F5-BIG-LTM-I4600 model
		F5-BIG-LTM-I4800 model
		F5-BIG-LTM-I4800B model
	i5000 series	F5-BIG-LTM-I5600 model
		F5-BIG-LTM-I5800 model
		F5-BIG-LTM-I5820-DF model
	i7000 series	F5-BIG-LTM-I7600 model F5-BIG-LTM-I7800 model
		F5-BIG-LTM-I7820-DF model
	i10000 series	F5-BIG-LTM-I10600 model
		F5-BIG-LTM-I10800 model
	i11000-DS series	F5-BIG-LTM-I11600-DS model
		F5-BIG-LTM-I11800-DS model
	i15000 series	F5-BIG-LTM-I15600 model
		F5-BIG-LTM-I15800 model
	I15000-DF series	F5-BIG-LTM-I15820-DF model
VIPRION	C2400 with B2250 series	F5-VPR-LTM-C2400-AC with F5-VPR-LTM-B2250 model

	C4480 with B4450 series	F5-VPR-LTM-C4480-AC with F5-VPR-LTM-B4450 model
RSERIES	r4000 series	F5-BIG-LTM-R4600 model
		F5-BIG-LTM-R4800 model
	R5000 series	F5-BIG-LTM-R5600 model
		F5-BIG-LTM-R5800 model
		F5-BIG-LTM-R5900 model
		F5-BIG-LTM-R5920-DF model
	R10000 series	F5-BIG-LTM-R10600 model
		F5-BIG-LTM-R10800 model
		F5-BIG-LTM-R10900 model
		F5-BIG-LTM-R10900-DF model
		F5-BIG-LTM-R10920-DF model
VELOS	BX110 with CX410 series	F5-VEL-CX410-AC with F5-VEL-LTM-BX110 model

Tabla 1. Modelos cualificados

Este producto ha sido cualificado e incluido en el Catálogo de Productos y Servicios STIC (CPSTIC) del Centro Criptológico Nacional en la categoría ENS ALTA en las familias “Cortafuegos” y “Balanceadores de carga”. Se recomienda consultar la versión cualificada en cada momento.

3 ORGANIZACIÓN DEL DOCUMENTO

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

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

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

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

El método de entrega segura del producto variará en función de si se adquiere el producto como hardware o en su modalidad virtual.

Para la modalidad hardware, los dispositivos son enviados directamente a través de un transportista de confianza (normalmente FedEx). El seguimiento también se realiza a través del mismo proveedor.

F5 enviará una caja sellada que incluye en su interior un albarán con una lista de componentes, con etiquetas impresas con la nomenclatura del producto, el número de venta correspondiente y el número de serie del producto.

Cuando el dispositivo es recibido, el paquete debe ser inspeccionado para detectar alteraciones u otros problemas. Además, se deberá revisar que las etiquetas externas coincidan con la entrega esperada, así como que los componentes coincidan con los de la documentación enviada del producto. En caso contrario, se deberá contactar al fabricante lo antes posible.

Finalmente, el producto es entregado a los clientes con una versión previamente instalada de BIG-IP. Se deberá revisar que esta versión se corresponde con la solicitada durante el proceso de compra del producto.

Para la modalidad virtual, el cliente deberá descargar el producto de la página de descargas oficial de F5 (https://downloads.f5.com). Deberá prestarse atención a la versión del producto a descargar, y verificarse tras comprobar el proceso de instalación descrito en la sección *5 FASE DE INSTALACIÓN* del presente documento.

4.2 ENTORNO DE INSTALACIÓN SEGURO

Se deberán cumplir las medidas de seguridad físicas y lógicas de aplicación a los sistemas en los que se desea desplegar BIG-IP.

Estas medidas de seguridad deberán garantizar que el producto se instale en una localización segura que disponga de protección física y no sea objeto de ataques físicos que comprometan la propia seguridad y/o interfieran en las interconexiones físicas y su correcta operación.

El nivel de seguridad de acceso hacia el recinto donde el producto se ha instalado debe estar acorde con la política del cliente para los activos a proteger en el entorno IT.

4.3 REGISTRO Y LICENCIAS

Durante la fase de instalación, se deberá activar la licencia del producto, la cual ha sido provista por F5. Para poder activar la licencia, se deberá obtener una clave de registro base.

Esta clave de registro consiste en una cadena de 27 caracteres que indica al servidor de licencias qué productos de F5 pueden licenciarse en el producto instalado. La clave de registro base está preinstalada en los nuevos sistemas BIG-IP.

Se debe seguir el manual de instalación de licencia de la guía oficial de F5 “K7752” [REF1] para comprobar la clave de registro y activar la licencia.

Una vez activada la licencia, debe verificarse que incluye lo siguiente:

- Para ADC-AFM, la licencia debe incluir solo AFM sobre la base de LTM.
- La licencia debe incluir "modo appliance".

Para comprobar el contenido de la licencia debe utilizarse la interfaz web (GUI) para acceder a la sección `System -> License`, y verificarse que los componentes requeridos están presentes en la sección de licencias activas.

4.4 CONSIDERACIONES PREVIAS

El producto BIG-IP admite diferentes configuraciones. La versión del producto cualificada requiere de una configuración concreta de este. Para alcanzar la configuración cualificada, se deberán de tener en cuenta aquellos parámetros que no han sido evaluados, y que deben de ser desactivados.

Por ello, los siguientes elementos quedan excluidos del alcance de la cualificación y deben de no estar configurados para mantener el cumplimiento con la configuración cualificada.

- LBH (LOP+BUC: Lights Out Processor + Backplane MicroController): Por defecto, este no es accesible desde la red de administración y no debe ser configurado.
- Para la configuración del servidor remoto, no se deberán configurar los siguientes campos, los cuales deben dejarse en blanco:
  - SNMP
  - Kerberos
  - RADIUS
  - TACACS+
- Los siguientes perfiles no se deberán configurar. Al igual que para las opciones de servidor remoto, la opción de configuración no deberá estar marcada, quedando en blanco las siguientes opciones:
  - HTTP: Aceleración web
  - Otros perfiles de la capa de aplicación: RTSP, ICAP, Request Adapt, Response Adapt, Diameter, RADIUS, SIP, Rewrite
  - Contenido: No se excluyen perfiles de este grupo.
  - Persistencia de la sesión: Protocolo de escritorio remoto de Microsoft, SIP
  - Protocolo: SCTP
  - SSL: No se excluyen perfiles de este grupo.
  - Autenticación de servidor remoto: RADIUS, TACACS+, CRLDP, Delegación Kerberos
  - Otro: NTLM, Stream
- Imi Shell: no se deberá configurar la shell.
- APM no se incluye en el sistema BIG-IP configurado como AFM. Por tanto, las siguientes opciones deberán estar desactivadas para el caso de uso AFM:
  - Base de datos de autenticación local, ya que la autenticación del tráfico se realiza únicamente mediante autenticación remota.

  - CRLDP, RADIUS, TACACS+ y RSA SecureID como sistemas de autenticación remota
  - Servidor de aplicaciones móviles
  - NTLM
  - Secure Web Gateway
  - Uso de DTLS para el tráfico de usuario (un cliente que intente establecer una conexión DTLS volverá a una conexión TLS sobre TCP cuando falle el intento de conexión DTLS).

- iRulesLX e iAppsLX: no deben usarse.
- BIG-IP no debe ejecutarse en modo de depuración.
- Al crear archivos de soporte como QKview o TCPDUMP, los archivos deben descargarse y eliminarse inmediatamente de BIG-IP.
- Algunos comandos tmsh no deberán utilizarse según la configuración cualificada. De igual forma, tampoco estarán permitidos ciertos módulos e interfaces de las API de iControl REST. A continuación, se detalla aquello que queda restringido:

COMANDOS TMSH NO PERMITIDOS	
`global publish`	`pem reporting commands`
`analytics application-security commands`	`sys geoip`
`analytics protocol-security report`	`sys smtp-server`
`analytics sip-dos report`	`sys snmp`
`auth radius`	`sys application commands`
`auth radius-server`	`sys crypto crl`
`auth tacacs`	`sys file ssl-crl`
`gtm commands`	`sys log-config dest arcsight`
`gtm global-settings commands`	`sys log-config dest local-database`
`gtm monitor commands`	`sys log-config splunk`
`ltm auth crldp-server`	`sys sflow commands`
`lmt auth kerberos-delegation`	`sys sflow data-source commands`
`ltm auth ocsp-responder`	`sys sflow global-settings commands`
`ltm-auth radius`	`util commands`
`ltm auth radius-server`	`wam commnds`
`ltm auth ssl-crldp`	`wam global-settings commands`
`ltm auth tacacs`	`wam resource commands`
`ltm classification commands`	`wom commands`
`ltm monitor diameter`	`wom profile commands`
`ltm monitor radius`	`apm aaa crldp`
`ltm monitor radius-accounting`	`apm aaa http`
`ltm monitor sip`	`apm aaa oam`

ltm persistence dest-addr	apm aaa radius
ltm persistence global-settings	apm aaa saml
ltm persistence hash	apm aaa saml-idp-connector
ltm persistence msrdp	apm aaa securid
ltm persistence persist-records	apm aaa tacacsplus
ltm persistence sip	apm ntlm commands
ltm persistence ssl	apm policy agent aaa-crldp
ltm persistence universal	apm policy agent aaa-radius
ltm profile analytics	apm policy agent aaa-securid
ltm profile diameter	apm policy agent acct-radius
ltm profile ntlm	apm policy agent acct-tacacsplus
ltm profile radius	apm policy agent decision-box
ltm profile rtsp	apm policy agent endpoint-windows-checkmachine-
ltm profile sctp	cert
ltm profile sip	apm policy agent endpoint-windows-grouppolicy
ltm profile stream	apm policy agent endpoint-windowsmachine-
ltm profile web-acceleration	info
ltm profile web-security	apm policy agent external-logon-page
net fdb commands	apm policy agent logging
net ipsec commands	apm policy agent message-box
pem commands	apm resource remote-desktop vmwareview
pem profile commands	apm sso Kerberos
apm policy agent oam	apm sso saml
apm policy agent tacacsplus	apm sso saml-resource
apm policy agent variable-assign	apm sso saml-sp-connector
apm profile exchange	asm commands
apm resource remote-desktop citrix	apm resource remote-desktop citrix-clientpackage-file
apm resource remote-desktop citrix-clientbundle	

Tabla 2. Comandos TMSH no permitidos

MÓDULOS ICONTROL NO PERMITIDOS	
ARX	ASM
WebAccelerator	PEM

Tabla 3. Módulos iControl no permitidos

INTERFACES ICONTROL NO PERMITIDOS

GlobalLB Application	Management SMTPConfiguration
GlobalLB PoolMember	Management SNMPConfiguration
GlobalLB VirtualServer	Management TACACSConfiguration
LocalLB NAT	Networking IPsecIkeDaemon
LocalLBNodeAddress	Networking IPsecIkePeer
LocalLB ProfileDiameter	Networking
LocalLB ProfileDiameterEndpoint	IPsecManualSecurityAssociation
LocalLB ProfileRADIUS	Networking IPsecPolicy
LocalLB ProfileRTSP	Networking IPsecTrafficSelector
LocalLB ProfileSCTP	Networking RouteDomain
LocalLB ProfileSIP	Networking RouteTable
LocalLB ProfileStream	Networking STPInstance
LocalLB VirtualAddress	Networking SelfIP
Log DestinationArcSight	Networking SelfIPPortLockdown
Log DestinationSplunk	Networking Tunnel
Management CRLDPConfiguration	Networking VLAN
Management CRLDPServer	Networking VLANGroup
Management OCSPConfiguration	Networking iSessionAdvertisedRoute
Management OCSPResponder	Networking iSessionRemoteInterface
Management RADIUSConfiguration	System GeoIP
Management RADIUSServer	System PerformanceSFlow

Tabla 4. Interfaces iControl no permitidos

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

Para el correcto funcionamiento del producto, este establece distintas comunicaciones con los siguientes componentes en su entorno de operación, tal y como se muestra en el siguiente diagrama:

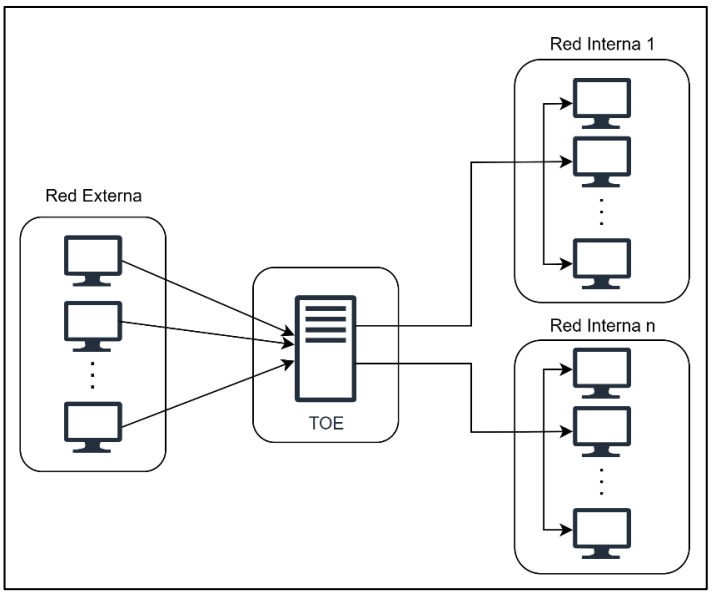


Figura 1. Entorno operacional del producto.

5 FASE DE INSTALACIÓN

En primer lugar, la fase de instalación deberá distinguirse en función de si se hace uso del producto mediante hardware o mediante la Virtual Edition.

En caso de hacer uso del producto mediante hardware, el software ya se proporcionará instalado. El administrador únicamente deberá comprobar la versión instalada como se describe en la presente sección.

En caso de hacer uso del producto mediante la Virtual Edition, el administrador deberá llevar a cabo el proceso de instalación como se describe en la sección 2 de [REF18]. Tras completar satisfactoriamente la instalación, el administrador deberá consultar la versión como se describe en la presente sección.

Para verificar las versiones del software BIG-IP instaladas en el equipo, use los comandos GUI o tmsh en el sistema y compare la versión en la ranura activa con la versión especificada. El comando *tmsh show sys software status* muestra el estado de las dos ranuras en el hardware y qué software está instalado en cada ranura.

```
---------------------------------------------------
Sys::Software Status
Volume  Product  Version   Build  Active   Status
---------------------------------------------------
HD1.1   BIG-IP   17.1.0.1  0.61.4   yes  complete
HD1.2   BIG-IP   17.1.0.1  0.0.4    no   complete
```

Figura 2. Comprobación de la versión.

Otra forma de llevar a cabo la comprobación de la versión es accediendo a la sección *System -> Software Management: Image List* de la GUI, donde se muestra una imagen similar al resultado obtenido a través de tmsh.

6 FASE DE CONFIGURACIÓN

Las siguientes secciones se consideran una guía para la configuración de BIG-IP. Los administradores deben revisar este documento y todos los documentos de referencia (según sea necesario) antes de comenzar con el proceso de configuración y administración de BIG-IP.

6.1 MODO DE OPERACIÓN SEGURO

Antes de realizar cualquier configuración en el producto, es necesario activar el modo de trabajo "ccmode", el cual hace que el producto cumpla con todos los requisitos de la certificación Common Criteria, que forma parte de la configuración cualificada. Para ello, los administradores deberán acceder a la línea de comandos de BIG-IP como usuario "root" y ejecutar el siguiente comando:

```
ccmode
```

Una vez ejecutado, se deberá escribir "yes" para aceptar la activación de este modo. Como paso final, en la propia terminal se mostrará un mensaje el cual indica que se deberá de reiniciar el sistema para que los cambios se hagan efectivos. Una vez finalice el proceso de reinicio, se deberá de comprobar si se ha aplicado la configuración segura. Para ello, se deberá de utilizar el siguiente comando:

```
tmsh list sys db security.commoncriteria
```

La salida esperada debe de ser del tipo "*sys db security.commoncriteria {value "true"}*", lo que indica que el modo seguro se ha activado correctamente. Una vez verificado esto, se podrá continuar con el resto de configuraciones descritas a continuación.

6.2 AUTENTICACIÓN

El producto BIG-IP ofrece distintas interfaces de gestión a las cuales se debe acceder mediante un usuario y contraseña. Las distintas interfaces de gestión ofrecidas por el producto son:

- Puerto serie (local).
- Shell de gestión de tráfico (tmsh) sobre SSHv2.
- GUI (interfaz web) sobre HTTPS.
- Interfaces programáticas iControl SOAP o iControl REST sobre HTTPS.

La ejecución del comando `ccmode` previamente mencionado incluye la configuración de la política de contraseñas. En concreto, se establece la siguiente configuración:

- Longitud mínima de 15 caracteres.
- Necesidad de, al menos, un carácter especial.
- Necesidad de, al menos, un número.
- Necesidad de, al menos, una letra mayúscula.
- Necesidad de, al menos, una letra minúscula.
- Período de expiración de 90 días.

Además, aplicando el comando `ccmode` previamente mencionado, se establece un límite de 3 intentos de inicio de sesión fallidos tras los cuales los usuarios quedarán bloqueados por 600

segundos (10 minutos) sin la posibilidad de ser desbloqueados manualmente. Estos parámetros son aplicados por defecto y no se deben cambiar. Para más información sobre la configuración de estos, atender al manual “Common Criteria Evaluation Configuration Guide“ [REF18].

El contador de intentos fallidos será común para las distintas interfaces de gestión. No obstante, el usuario administrador conocido como “admin” podrá acceder localmente a través del puerto serie, aunque se encuentre bloqueado.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

El producto puede ser administrado usando cualquiera de las interfaces previamente mencionadas a través de una conexión local (puerto serie) o remota (resto de interfaces). Para acceder a la interfaz local, el usuario deberá contar con acceso físico al producto.

A continuación, se indican unas guías de ayuda para la correcta utilización y administración de estos canales de comunicación.

- Guía completa de comandos tmsh: [REF5]
- Administración del módulo LTM a través de la interfaz web: [REF6]
- Configuración de políticas e implementaciones para el módulo AFM: [REF7]
- Administración de usuarios de iControl: [REF8]

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

Durante la fase de instalación se requerirá el acceso de los administradores al producto mediante SSH. Para una correcta autenticación de los administradores durante esta fase, primeramente, se deberá habilitar este canal SSH siguiendo la guía oficial de F5 [REF3]

Una vez habilitado el canal SSH, se deberán realizar cambios en la configuración de los mecanismos criptográficos del canal SSH. Para poder limitar los mecanismos criptográficos del canal, se deberá ejecutar el siguiente comando:

```
tmsh -c " $(echo -e "modify sys sshd include \"Ciphers aes128-ctr,aes128-gcm@openssh.com,aes192-ctr,aes256-ctr,aes256-gcm@openssh.com $(echo "\n\t")MACs hmac-sha2-256,hmac-sha2-512 $(echo "\n\t")HostKeyAlgorithms ecdsa-sha2-nistp256 $(echo "\n\t")HostKey /config/ssh/ssh_host_ecdsa_key\"")"
```

Esta configuración se aplicará de forma inmediata en el sistema sin necesidad de reiniciar y, de esta forma, los únicos algoritmos ofrecidos por el producto serán categorizados como recomendados por el CCN. Para más información sobre el filtrado de algoritmos en SSH, consulte la guía oficial [REF4].

Por otra parte, se deberá ejecutar el siguiente comando para que el producto tan solo ofrezca suites de cifrado para TLS que se consideren recomendadas por el CCN. No será necesario reiniciar el sistema para su aplicación.

```
tmsh modify sys http ssl-ciphersuite ECDHE-RSA-AES256-GCM-SHA384,ECDHE-RSA-AES128-GCM-SHA256
```

Respecto a la gestión de usuarios, se deberá consultar el manual "BIG-IP Systems: User Account Administration" [REF2] donde se encuentran recomendaciones y los pasos concretos acerca de la gestión de los usuarios y sus roles.

Además de ello, se deberán seguir los siguientes pasos de configuración para definir: la cantidad máxima de usuarios simultáneos permitidos, la duración máxima que la utilidad de configuración puede estar inactiva antes del cierre de sesión automático del usuario y un mensaje de seguridad que desea que el sistema muestre en la pantalla de inicio de sesión de BIG-IP.

En la pestaña Principal, haga clic en *System -> Preferences*.

En la lista *System Settings*, seleccione *Advanced*. Aparecerán configuraciones adicionales en la pantalla.

En el campo etiquetado *Maximum HTTP Connections To Configuration Utility*, conserve o revise el valor predeterminado.

En el campo etiquetado *Idle Time Before Automatic Logout*, revise el valor predeterminado. F5 recomienda un valor de 120 segundos.

Para la configuración etiquetada *Show The Security Banner On The Login Screen*, verifique que la casilla esté marcada. Esto garantiza que el mensaje de seguridad que especifique se muestre en la pantalla de inicio de sesión de la utilidad de configuración BIG-IP.

En el campo etiquetado *Security Banner Text To Show On The Login Screen*, revise el mensaje de seguridad predeterminado. Un buen mensaje de seguridad es aquel que brinda protección legal a la organización, como un mensaje que indica que el acceso no autorizado está prohibido. La pantalla de inicio de sesión de la utilidad de configuración BIG-IP muestra el texto que especifica en este campo.

Haga clic en Update para que todos los cambios surtan efecto.

> Nota: Para configurar estos mismos parámetros desde la línea de comandos, consulte la sección "*sys sshd*" en el manual de comandos de tmsh [REF5].

El mensaje de advertencia de la GUI está habilitado de forma predeterminada y el valor predeterminado es "Bienvenido a la utilidad de configuración BIG-IP". Para actualizar ese mensaje y asegurarse de que esté habilitado, use el siguiente comando desde dentro de tmsh, reemplazando <Text> con el texto que desee. Esta configuración se aplicará de forma inmediata en el sistema sin necesidad de reiniciar.

```
modify sys global-settings gui-security-banner enabled gui-security-banner-text "<Text>"
```

El banner de advertencia para tmsh está deshabilitado por defecto, por lo que se debe ejecutar el siguiente comando para habilitarlo y definir el mensaje, reemplazando <Text> con el texto deseado. De nuevo, esta configuración también se aplicará de forma inmediata en el sistema sin necesidad de reiniciar

```
modify sys sshd banner enabled banner-text "<Text>"
```

Además de todas las configuraciones explicadas previamente, a continuación, se describen algunos artículos de interés de la página web oficial de F5 para la correcta administración del producto.

ARTICULO	DESCRIPCIÓN
K15497: Configuring a secure password policy for the BIG-IP system	Cómo garantizar que los usuarios de BIG-IP que tienen cuentas de usuario locales creen y mantengan contraseñas lo más seguras posible.
K13121: Changing system maintenance account passwords	Cómo modificar las contraseñas de las cuentas de mantenimiento de BIG-IP desde sus valores predeterminados.
K4139: Configuring the BIG-IP system to enforce the use of strict passwords	Cómo utilizar la comprobación estricta de contraseñas para probar las contraseñas de los usuarios de varias formas diferentes.
K32203233: The root and admin accounts are now subject to the enforcement restrictions of the secure password policy	Cómo asegurarse de que todas las cuentas de usuario utilicen las opciones de configuración de la política de contraseña Longitud mínima, Longitud máxima y Caracteres requeridos.
K12173: Overview of BIG-IP administrative access controls	Descripción general de los mecanismos de control de acceso que mantienen la seguridad, garantizan la interoperabilidad en una variedad de entornos y ayudan a cumplir con los estándares de la industria.
K13426: Monitoring login attempts (11.x - 17.x)	Cómo ver los intentos de inicio de sesión exitosos y fallidos en el registro de auditoría del sistema BIG-IP.

Tabla 5. Artículos de referencia

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

BIG-IP permite la configuración de VLAN, las cuales segmentan la red que se esté gestionando. Estas VLANs están asociadas directamente con las interfaces físicas en el sistema BIG-IP, por lo que cada VLAN deberá estar asignada a una o más interfaces del sistema BIG-IP. Una vez que se asigna una interfaz a una VLAN, el producto será capaz de controlar el envío y la recepción de mensajes de los equipos a través de la interfaz asignada.

El sistema de creación de VLAN se basa en la asignación de etiquetas, que puede ser única si solo se asigna una VLAN en cada interfaz o doble si se asignan dos o más VLAN por interfaz. Esta etiqueta se asocia como número de identificación único para identificar así la red de origen/destino de los paquetes.

Si no se asigna explícitamente una etiqueta a una VLAN, el sistema BIG-IP asigna una etiqueta automáticamente. El valor de una etiqueta puede estar entre 1 y 4094. Una vez que se asigna una etiqueta a una VLAN, cualquier mensaje enviado desde o hacia un host en esa VLAN incluye esta etiqueta VLAN como encabezado del mensaje.

Cada VLAN debe tener una dirección IP estática asociada. La dirección IP propia de una VLAN representa un espacio de direcciones, es decir, el rango de direcciones IP pertenecientes a los

hosts en esa VLAN. Al enviar una solicitud a un servidor de destino, el sistema BIG-IP puede usar estas direcciones IP propias para determinar la VLAN específica que contiene el servidor de destino.

A la hora de configurar las VLAN, las opciones "Source Check" y "Fail-safe" deberán estar habilitadas. El valor de la opción "Fail-safe Timeout" deberá ser, como mínimo, el que el producto tiene por defecto.

Finalmente, habrá que atender a la sección "VLANs, VLAN Groups and VXLAN" en el manual de administración de enrutamiento [REF119] para poder configurar las VLANs en el producto.

6.5 GESTIÓN DE CERTIFICADOS

Para la administración de los certificados en el producto BIG-IP, se recomienda consultar los siguientes manuales:

- Descripción general del certificado de dispositivo según la guía oficial de F5 "K15664" [REF11].
- Gestión de certificados SSL según la sección SSL Certificate Management de la guía "SSL Administration" de F5 [REF12]. En este mismo documento se encuentran otras secciones sobre la creación y solicitud de certificados, la gestión del tráfico SSL y la configuración del tráfico del lado del cliente y del servidor, que pueden ser de interés para la gestión de los certificados.
- Gestión de certificados a través de la GUI, según la guía oficial de F5 "K14620" [REF13].

Se recomienda utilizar un esquema de certificados RSA con una longitud de 3072 bits o más, o un esquema ECDSA con las curvas P-256 o P-384.

6.6 SINCRONIZACIÓN

El producto está configurado por defecto para obtener la sincronización de tiempo del hardware o del sistema operativo subyacente. Esta opción por defecto es la recomendada de mantener.

Sin embargo, por otro lado, el producto permite configurar la sincronización horaria automática. En caso de querer habilitar esta configuración, sería necesario establecer comunicación con un servidor externo a través del servicio NTP. El administrador podrá seleccionar tanto una dirección IP como el nombre del servidor para el servicio de sincronización horaria.

Para ello, se deberá acceder a la sección System -> Configuration -> Device -> NTP de BIG-IP. En esta sección se mostrarán las diferentes opciones de configuración del servicio NTP. Se deberá rellenar el campo de dirección IP del servidor dentro de la configuración de Time Server List y el servicio de sincronización quedará configurado.

6.7 ACTUALIZACIONES

Periódicamente, el software de BIG-IP contará con nuevas actualizaciones. Estas nuevas versiones se publicarán y podrán ser revisadas a través del repositorio oficial de F5, en la página web https://downloads.f5.com/. El software está dividido por familia de productos y línea de productos. Dentro de la línea de productos se encuentran las diferentes versiones y notas de versión para cada uno de los productos.

En la página oficial de F5 se podrá comprobar que estarán disponibles los diferentes archivos de instalación para todas las versiones del producto. Cada página contiene la imagen del producto con distintos formatos (ISO, OVA, qcow2, VHD…), el archivo de firma digital y el archivo de clave pública. Para cada versión, se podrán encontrar los siguientes archivos:

- BIGIP-{version}.{format}
- BIGIP-{version}.{format}.sig o BIGIP-{version}.{format}.384.sig
- Hotfix-BIG-IP-{version}-ENG.{format}
- Hotfix-BIG-IP-{version}-ENG.{format}.sig o Hotfix-BIG-IP-{version}-ENG.{format}.384.sig
- archive.pubkey.{fecha_clave}.pem (uno para cada archivo {format}.sig o {format}.384.sig)

Una vez se hayan descargado todos los archivos para la versión deseada, se deberán verificar las imágenes ISO mediante sus archivos de firma y clave pública. A continuación, se muestra un ejemplo de verificación en Linux y Windows:

```
(Linux) openssl dgst -sha384 -verify archive.pubkey.{fecha_clave}.pem
-signature BIGIP-{version}.{format}.sig BIGIP-{version}.{format}
(Windows) C:\Users\user\Desktop> openssl dgst -sha256 -verify
archive.pubkey.{fecha_clave}.pem -signature BIGIP-
{version}.{format}.sig BIGIP-{version}.{format}
```

Si la verificación de la firma falla (el comando openssl muestra un mensaje de error "Verificación fallida"), la instalación de la actualización del software fallará. En este caso, intente descargar la ISO nuevamente. Si la verificación de la firma falla por segunda vez, comuníquese con el soporte de F5.

En el caso de que la verificación haya sido satisfactoria, se podrá comenzar a instalar la imagen en el sistema. Una vez instalado BIG-IP, se debe verificar la versión del producto instalado y, por tanto, que el proceso de instalación se ha realizado correctamente. Para ello, se deberán de seguir los pasos descritos en la sección 5 FASE DE INSTALACIÓN de este documento para la verificación de versión de producto.

El proceso de actualización puede revisarse en la guía oficial de F5 “K51113020” sobre el proceso de actualización de BIG-IP [REF9].

6.8 AUTO-CHEQUEOS

El producto BIG-IP monitoriza todos los elementos internos del equipo de forma automática y, una vez que detecta un problema, es capaz de almacenar el evento, así como enviarlo a un servidor de terceros para la gestión de la incidencia. Estos chequeos son automáticos y constantes.

En paralelo a esta monitorización automática, BIG-IP permite analizar en cualquier momento el estado del hardware mediante el siguiente comando de tmsh, utilizando permisos de root:

```
tmsh platform_check
```

Además de ello, mediante la herramienta qkview, BIG-IP también es capaz de incorporar toda la información relativa al dispositivo y su diagnóstico, así como este chequeo de hardware.

6.9 ALTA DISPONIBILIDAD

BIG-IP ofrece la posibilidad de ser desplegado en un modo de alta disponibilidad, desplegando dos equipos que actúan virtualmente como uno solo. El tipo de redundancia que ofrece el producto es conmutación por error, lo que significa que todas las funcionalidades serán llevadas a cabo por un solo equipo y que, en caso de fallo, todas pasarán automáticamente y en tiempo real al otro.

La funcionalidad de alta disponibilidad está basada en DSC, Device Service Cluster, que administra la sincronización del tráfico y la configuración de todos los elementos necesarios.

La agrupación en clústeres de servicios de dispositivos, o DSC, es una arquitectura subyacente dentro de BIG-IP TMOS. DSC proporciona sincronización y conmutación por fallo de datos de configuración de BIG-IP en los niveles de granularidad definidos por el usuario, entre múltiples dispositivos BIG-IP de una red. Más específicamente, puede configurar un dispositivo BIG-IP en una red para:

- Sincronizar algunos o todos sus datos de configuración entre varios dispositivos BIG-IP.
- Conmutar a uno de los muchos dispositivos disponibles.
- Reflejar las conexiones a un dispositivo del mismo nivel para evitar la interrupción del servicio durante la conmutación por fallo.

Si solo tiene dos dispositivos BIG-IP, puede crear una configuración activo-standby o activo-activo. Con más de dos dispositivos, puede crear una configuración en la que estén activos varios dispositivos y, si es necesario, puede conmutar por fallo a uno de los restantes.

Al configurar DSC, se asegura de que los objetos de configuración BIG-IP estén sincronizados y que otros dispositivos BIG-IP disponibles en la red puedan asumir el tráfico. También se asegura de que la conmutación por fallo de un dispositivo a otro, cuando esté habilitada, se produzca sin problemas, con una interrupción mínima o nula en la entrega de aplicaciones.

Si usa la utilidad de configuración para crear una configuración DSC, puede volver a ingresar a la utilidad en cualquier momento para ajustar la configuración. Simplemente haga clic en el logotipo de F5 en la esquina superior izquierda de la utilidad de configuración BIG-IP y, en la pantalla de bienvenida, haga clic en Ejecutar la utilidad *Config Sync -> HA*.

La agrupación de servicios de dispositivos (DSC) se basa en algunos componentes clave. Un dispositivo es un sistema BIG-IP físico o un sistema BIG-IP virtual (BIG-IP Virtual Edition o vCMP). Cada miembro del grupo de dispositivos tiene un conjunto de propiedades de identificación únicas que genera el sistema BIG-IP. Para los grupos de dispositivos configurados para la conmutación por fallo, es importante que el dispositivo con la menor capacidad tenga la capacidad de procesar todos los grupos de tráfico. Esto garantiza la disponibilidad de la aplicación en caso de que todos los dispositivos del grupo de dispositivos, excepto uno, no estén disponibles por algún motivo.

Un grupo de dispositivos es una colección de dispositivos BIG-IP que confían entre sí y pueden sincronizar, y a veces conmutar por fallo, sus datos de configuración BIG-IP. Un grupo de dispositivos Sync-Failover contiene dispositivos que sincronizan datos de configuración y admiten grupos de tráfico con fines de conmutación por error cuando un dispositivo deja de estar disponible. El sistema BIG-IP admite plataformas de hardware homogéneas o heterogéneas dentro de un grupo de dispositivos.

Un grupo de tráfico es una colección de objetos de configuración relacionados (como una dirección IP virtual y una dirección IP propia) que se ejecutan en un dispositivo BIG-IP y procesan un tipo particular de tráfico de aplicaciones. Cuando un dispositivo BIG-IP deja de estar disponible, un grupo de tráfico puede flotar a otro dispositivo en un grupo de dispositivos para garantizar que el tráfico de la aplicación continúe procesándose con poca o ninguna interrupción en el servicio.

Detrás del éxito de los grupos de dispositivos y los grupos de tráfico se encuentra una característica conocida como confianza en los dispositivos. La confianza del dispositivo establece relaciones de confianza entre los dispositivos BIG-IP en la red, a través de la autenticación basada en certificados mutuos. Un dominio de confianza es una colección de dispositivos BIG-IP que confían entre sí y es un requisito previo para crear un grupo de dispositivos para las operaciones de sincronización de configuración y conmutación por error. El dominio de confianza está representado por un grupo de dispositivos especial generado y administrado por el sistema llamado device_trust_group, que se utiliza para sincronizar la información del dominio de confianza en todos los dispositivos.

Las carpetas son contenedores para los objetos de configuración en un dispositivo BIG-IP. Para cada partición administrativa del sistema BIG-IP, existe una carpeta de alto nivel. En el nivel más alto de la jerarquía de carpetas hay una carpeta llamada raíz. El sistema BIG-IP utiliza carpetas para afectar el nivel de granularidad con el que sincroniza los datos de configuración con otros dispositivos del grupo de dispositivos.

Para los detalles de la configuración y las diferentes opciones de la administración de DSC, se recomienda consultar la guía oficial de F5 sobre la agrupación de servicios de dispositivos BIG-IP [REF14].

Dentro de todas las opciones de DSC, la opción recomendada y típicamente más utilizada es la configuración de activo-standby que puede realizarse siguiendo la guía oficial de F5 para este caso concreto [REF15]

6.10 AUDITORÍA

6.10.1 REGISTRO DE EVENTOS

BIG-IP es capaz de registrar múltiples eventos relativos a acciones de los usuarios o a cambios en la configuración del producto.

Se recomienda revisar la sección “Auditing user access” del manual de gestión de cuentas de usuario [REF2] para comprobar la lista de todos los eventos relacionados con las cuentas de usuario que se generan, así como una descripción de su formato.

Finalmente, para configurar el nivel de registro se recomienda revisar la guía oficial de F5 “K5532” [REF17], donde se detalla cómo realizar dicha configuración para la gestión de los eventos recogidos por el producto.

Todos los eventos auditados por el producto se listan a continuación y pueden ser consultados por los usuarios según indica la sección *Appendix: Audit and event records* de [REF18]:

a. **Nivel de logs del mcpd**
b. **Tmsh**
c. **Modificación de la GUI**

d. **iControl**
e. **iControl REST**
f. **Generación de una clave criptográfica**
g. **Importación de una clave criptográfica**
h. **Cambio de una clave criptográfica**
i. **Eliminación de una clave criptográfica**
j. **Restauración de contraseñas**
k. **Arrancado de servicios**
l. **Parada de servicios**
m. **Aviso de poco espacio de almacenamiento**
n. **Fallos al establecer sesiones HTTPS**
o. **Fallos al establecer sesiones SSH:**
p. **Fallos al establecer sesiones TLS (BIG-IP como cliente)**
q. **Fallos al establecer sesiones TLS (BIG-IP como servidor)**
r. **Autenticación basada en contraseñas**
s. **Login (correcto y fallido) via GUI**
t. **Login (correcto y fallido) via SSH**
u. **Login (correcto y fallido) via iControl**
v. **Login (correcto y fallido) via iControl REST**
w. **Validación de certificados**
x. **Restricción de la gestión de funciones de seguridad**
y. **Restricción de la gestión de servicios**
z. **Restricción de la gestión de actualizaciones**
aa. **Restricción de la gestión de los datos TSF**
bb. **Ejecución del comando "run util unix-rm -f /var/log/wccpd.log" por el usuario invitado.**
cc. **Restablecimiento de la contraseña administrativa desde la línea de comando usando tmsh por el usuario invitado.**
dd. **Restricción de la gestión de claves criptográficas**
ee. **Cambios de hora**
ff. **Timeout por inactividad en sesiones locales y remota interactivas**
gg. **Fin de sesión de usuario**
hh. **Canal confiable**
ii. **Path confiable**
jj. **Logout**

kk. Inicio de la sesión SSH

ll. Fallos de las conexiones SSH

mm. Terminación de las sesiones SSH

nn. Configuración de las reglas de tráfico de red del cortafuegos

oo. Aplicación de reglas configuradas con la opción "log"

pp. Avisos de descarte de paquetes por exceso de tráfico de red.

6.10.2 ALMACENAMIENTO LOCAL

BIG-IP almacena localmente los mensajes generados por eventos de tráfico en la red que gestiona. Estos estarán generados por la monitorización del propio dispositivo o seguridad, entre otros. Por un lado, la finalidad de los mensajes generados es que sean almacenados remotamente tal y como se muestra en la siguiente sección de almacenamiento remoto. Sin embargo, los registros de auditoría generados por el propio envío de los datos son guardados en el directorio /var/log de forma independiente y por tipo de evento.

6.10.3 ALMACENAMIENTO REMOTO

Como se ha mencionado en la sección anterior, los mensajes generados por eventos de tráfico en la red gestionada se enviarán a una entidad externa. Para ello, se recomienda que se configure un servidor Syslog externo.

A continuación, se describe mediante un ejemplo cómo configurar este servicio paso a paso.

Para configurar el registro seguro en un servidor syslog externo, se debe configurar un servidor virtual de SSL a servidor local para cifrar el tráfico TCP Syslog generado por los sistemas de registro de BIG-IP. Este servidor virtual dirigirá el tráfico a un grupo que contenga la dirección IP y el puerto del servidor syslog seguro remoto.

El sistema de registro de alta velocidad requiere un grupo al que apuntar, por lo que crearemos un grupo que contenga la dirección IP y el puerto del servidor virtual de cifrado local. Todos estos son elementos de configuración de nivel básico, por lo que deberán configurarse en cada BIG-IP en el clúster, utilizando las direcciones IP, claves y certificados adecuados para cada BIG-IP, aunque todos enviarán tráfico a un servidor syslog seguro remoto. Crearemos los objetos de configuración en orden, desde el servidor seguro de syslog hasta el syslog y el sistema de registro de alta velocidad, de modo que cada objeto de la cadena esté disponible cuando configuremos el objeto al que invocaremos.

Asegúrese de haber importado un paquete de CA (en adelante, el archivo: "F5secureLoggingCA_bundle.crt") y el certificado de cliente y la clave adecuados (que coincidan con el nombre de host de su DUT) a cada una de sus BIG-IP en la ruta */config/ssl/ssl.crt/* del sistema. Luego, cree un grupo que contenga la dirección IP y el puerto TCP de la interfaz de red de registro en el servidor syslog seguro remoto (tenga en cuenta que cada uno de estos comandos se ingresa como una sola línea de comando, hemos agregado nuevas líneas para facilitar la lectura):

```
create ltm pool pool_remote_secure_syslog {
 members replace-all-with { 10.89.179.1:6514 { address 10.89.179.1 } }
 monitor tcp_half_open
}
```

A continuación, se crea un servidor virtual de SSL no flotante y cifrado, utilizando la clave y el certificado de BIG-IP, en una VLAN privada, apuntando a ese grupo en cada BIG-IP. Tenga en cuenta que las direcciones IP utilizadas en la VLAN privada son arbitrarias, no enrutables y que todas las BIG-IP del clúster utilizan las mismas direcciones IP, por lo que cada una tiene un servidor virtual de cifrado idéntico. Esto se debe a que la configuración de syslog está sincronizada en todos los BIG-IP del clúster y solo contiene una IP/puerto para enviar mensajes de syslog.

Seguidamente, en BIG-IP-1 (uno de los dos BIG-IP desplegados) ejecute los siguientes comandos:

```
create ltm profile server-ssl profile_serverssl_syslog-1 {
  ca-file F5secureLoggingCA_bundle.crt
  cert b3-1.logging.f5cc.com.crt
  defaults-from serverssl
  key b3-1.logging.f5cc.com.key
  peer-cert-mode require
  authenticate-name vm179.logging.f5cc.com
}
create net vlan vlan_securelog
create net self 10.254.216.1/24 vlan vlan_securelog
create ltm virtual-address 10.254.216.100
  traffic-group traffic-group-local-only
  auto-delete false
create ltm virtual vs_secure_syslog_target-1 {
  destination 10.254.216.100:514
  ip-protocol tcp
  pool pool_remote_secure_syslog
  profiles replace-all-with { profile_serverssl_syslog-1 tcp }
  vlans replace-all-with { vlan_securelog }
  vlans-enabled
}
```

En BIG-IP-2 (el segundo BIG-IP desplegado) ejecute los siguientes comandos:

```
create ltm profile server-ssl profile_serverssl_syslog-2 {
  ca-file F5secureLoggingCA_bundle.crt
  cert b3-2.logging.f5cc.com.crt
  defaults-from serverssl
  key b3-2.logging.f5cc.com.key
  peer-cert-mode require
  authenticate-name vm179.logging.f5cc.com
}
create net vlan vlan_securelog
create net self 10.254.216.1/24 vlan vlan_securelog
create ltm virtual-address 10.254.216.100
  traffic-group traffic-group-local-only
  auto-delete false
create ltm virtual vs_secure_syslog_target-2 {
  destination 10.254.216.100:514
  ip-protocol tcp
  pool pool_remote_secure_syslog
  profiles replace-all-with { profile_serverssl_syslog-2 tcp }
  vlans replace-all-with { vlan_securelog }
  vlans-enabled
}
```

Luego, debido a que algunos de los mensajes de registro de auditoría más antiguos no utilizan el sistema de registro de alta velocidad, modificamos el servidor syslog local de BIG-IP para

enviar datos de auditoría al servidor virtual de cifrado. Este elemento de configuración está sincronizado entre las BIG-IP, por lo que no es necesario ingresarlo dos veces:

```
modify sys syslog {
  include `
    destination   d_to_secure_syslog   {   network(\"10.254.216.100"\"
port(514) transport(tcp)); };
    log        {        source(s_syslog_pipe);        filter(f_audit);
destination(d_to_secure_syslog); };
    log       {       source(s_syslog_pipe);       filter(f_authpriv);
destination(d_to_secure_syslog); };
    log        {        source(s_syslog_pipe);        filter(f_apm);
destination(d_to_secure_syslog); };
    log        {        source(s_syslog_pipe);        filter(f_sso);
destination(d_to_secure_syslog); };
  `
}
```

Ahora, para activar High-Speed-Logging (HSL), se crea un grupo que contiene la dirección IP y el puerto TCP de los servidores virtuales de cifrado SSL-a-servidor (un grupo para ambos servidores virtuales de destino de syslog seguro BIG-IP, el grupo selecciona automáticamente el virtual local adecuado para usar):

```
create ltm pool pool_syslog_encryptor {
  members replace-all-with {
     10.254.216.100:514 { address 10.254.216.100 }
  }
  monitor tcp_half_open
}
```

A continuación, cree de registro de alta velocidad remoto HSL dirigido al grupo:

```
create     sys     log-config     destination     remote-high-speed-log
hsldest_to_encryptor {
  pool-name pool_syslog_encryptor
}
```

Luego, para obtener la marca de tiempo del registro del sistema y otra información de identificación incluida con cada mensaje de registro, cree un destino de registro del sistema remoto HSL dirigido al registro remoto de alta velocidad:

```
create sys log-config destination remote-syslog hsldest_syslog {
  format rfc5424
  remote-high-speed-log hsldest_to_encryptor
}
```

Ahora, cree un editor HSL, que enviará los mensajes de registro de auditoría seleccionados tanto al servidor syslog interno (para el registro local) como al destino HSL que acabamos de crear:

```
create sys log-config publisher hslpub_secure_remote_syslog {
  destinations replace-all-with {
    hsldest_syslog
    local-syslog
  }
}
```

A continuación, se crean filtros HSL para seleccionar mensajes de registro y enviarlos a través de la cadena al servidor syslog remoto seguro:

```
create sys log-config filter hslfilter_packet_filter {
```

```
  publisher hslpub_secure_remote_syslog
  source packet_filter
}
create sys log-config filter hslfilter_ssl {
  publisher hslpub_secure_remote_syslog
  source ssl
}
create sys log-config filter hslfilter_tamd {
  publisher hslpub_secure_remote_syslog
  source tamd
}
create sys log-config filter hslfilter_tmsh {
  publisher hslpub_secure_remote_syslog
  source tmsh
}
```

Finalmente, si estamos probando un sistema con APM aprovisionado (ADC-AP), habilitaremos el registro de syslog de APM y agregaremos varios filtros HSL adicionales:

```
modify sys db log.access.syslog value enable
create sys log-config filter remote_apm_filter {
  level info
  publisher hslpub_secure_remote_syslog
  source accesscontrol
}
create sys log-config filter remote_acl_filter {
  level info
  publisher hslpub_secure_remote_syslog
  source apmacl
}
create sys log-config filter remote_sso_filter {
  level info
  publisher hslpub_secure_remote_syslog
  source sso
}
```

6.11 BACKUP

BIG-IP es capaz de hacer una copia de seguridad y la restauración de esta basado en un archivo de configuración llamado *User Configuration Set* (UCS). Este archivo por defecto incluye todos los archivos necesarios para restaurar la configuración sobre un dispositivo nuevo, incluyendo archivos de configuración, licencias, cuentas de usuarios locales y certificados y claves SSL.

Este archivo de configuración se almacena por defecto en el directorio /var/local/ucs y su extensión por defecto es .ucs. Estos archivos pueden ser generados mediante la GUI en la sección System -> Archives -> Create, en la que se muestran todos los archivos creados que se encuentren en el directorio por defecto. En esta misma pantalla también es posible borrar, descargar o subir un archivo .ucs.

Por otro lado, también es posible crear un archivo UCS mediante tmsh con el siguiente comando:

```
save /sys ucs {nombre del archivo}
```

Para la gestión de los archivos UCS es necesario tener permisos de administración del dispositivo.

Finalmente, se recomienda consultar la guía oficial de F5 “K13132” [REF10] sobre la generación y restauración de copias de seguridad mediante archivos UCS en BIG-IP.

6.12 FIREWALL

El producto BIG-IP permite su configuración y utilización como cortafuegos (firewall) mediante su módulo AFM.

Para más información acerca de la funcionalidad de firewall de BIG-IP, atender a la guía oficial de F5 “BIG-IP AFM: Network Firewall Policies and Implementations” [REF7]

6.13 BALANCEADOR DE CARGA

El producto BIG-IP permite su configuración y utilización como balanceador de carga mediante su módulo LTM.

Para más información sobre la configuración de BIG-IP como balanceador de carga, consulte la guía oficial de F5 “Configuring ISP Load Balancing” [REF6]

6.14 MITIGACIÓN DE VULNERABILIDADES

Esta sección sirve para configurar BIG-IP de forma que se mitiguen las vulnerabilidades encontradas en el producto durante su evaluación. A fecha de publicación de este documento las vulnerabilidades aplicables a la versión cualificada del producto son las siguientes, aunque esto no evita que se encuentren nuevas vulnerabilidades en el futuro para la versión concreta evaluada.

La vulnerabilidad CVE-2023-46747 afecta directamente a BIG-IP permitiendo la ejecución remota de código por un usuario que no esté autenticado en la red. Para mitigar esta vulnerabilidad se deberán seguir los siguientes pasos:

Descargar el script de mitigación (mitigation-1.0.txt) desde la siguiente página oficial de F5: https://my.f5.com/manage/s/article/K000137353 (Sección “*Mitigation*”)

Acceder a la línea de comandos de BIG-IP y situar el archivo de mitigación anteriormente descargado en la ruta */config*

Iniciar sesión con el usuario root

Con un editor de textos, crear el archivo “mitigation-1.0.txt.md5” en el directorio */config* con el siguiente contenido:

```
3be77752826lff9cb58f66c5d9af494b  mitigation-1.0.txt
```

Se debe verificar la integridad del archivo mitigation-1.0.txt descargado, mediante el siguiente comando:

```
md5sum --check /config/mitigation-1.0.txt.md5
```

Debería aparecer el siguiente mensaje indicando que la verificación de integridad es correcta.

```
mitigation-1.0.txt: OK
```

Una vez se ha verificado la integridad del archivo, se deberán conceder permisos de ejecución al archivo mediante el siguiente comando:

```
chmod +x /config/mitigation-1.0.txt
```

Una vez concedidos los permisos, se deberá ejecutar el archivo mediante el siguiente comando:

```
/config/mitigation-1.0.txt
```

Por pantalla se mostrarán los siguientes mensajes:

```
Applying ID1378329 mitigation...
Restarting httpd...
Stopping httpd:                                    [  OK  ]
Starting httpd:                                    [  OK  ]
Restarting tomcat...
Done!
```

Finalmente, se deberá comprobar que la mitigación se ha aplicado correctamente. Para ello, se deberá comprobar que el valor 'secret=' en el archivo proxy_ajp.conf y el valor de 'requiredSecret=' en el archivo server.xml coinciden. Para ello, se deberá ejecutar el siguiente comando:

```
grep -m1 -ioE '(required)?secret.*'
/config/httpd/conf.d/proxy_ajp.conf /etc/tomcat/server.xml
```

La salida esperada de este comando será del siguiente tipo:

```
/config/httpd/conf.d/proxy_ajp.conf:secret=9b81...
/etc/tomcat/server.xml:requiredSecret="9b81..."
```

Se puede encontrar más información sobre la mitigación de esta vulnerabilidad en la guía oficial de F5 "K000137353" [REF16].

Por último, es importante que el administrador encargado de gestionar y mantener el producto revise periódicamente si se ha encontrado alguna otra vulnerabilidad aplicable a la versión del producto cualificada.

7 REFERENCIAS

[REF1] Guía de activación de la licencia: https://my.f5.com/manage/s/article/K7752

[REF2] Guía de administración de cuentas de usuario https://techdocs.f5.com/en-us/bigip-17-0-0/big-ip-systems-user-account-administration.html

[REF3] Guía de gestión de canal SSH https://my.f5.com/manage/s/article/K13454

[REF4] Guía de filtrado de criptografía para el canal SSH https://my.f5.com/manage/s/article/K80425458

[REF5] Guía de comandos tmsh: https://clouddocs.f5.com/cli/tmsh-reference/latest/_downloads/dff789d01119c67e4c9d00d212399967/tmsh_17.0.0.pdf

[REF6] Guía de administración de LTM: https://techdocs.f5.com/en-us/bigip-17-0-0/big-ip-local-traffic-manager-implementations.html

[REF7] Guía de configuración de AFM: https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-network-firewall-policies-and-implementations.html

[REF8] Guía de gestión de usuarios de iControl: https://cdn.f5.com/websites/devcentral.f5.com/downloads/icontrol-rest-api-user-guide-14-1-0.pdf

[REF9] Guía de actualización de BIG-IP: https://my.f5.com/manage/s/article/K51113020

[REF10] Guía de generación y restauración de copias de seguridad mediante archivos UCS en BIG-IP: https://support.f5.com/csp/article/K13132

[REF11] Descripción general de los certificados de BIG-IP: https://my.f5.com/manage/s/article/K15664

[REF12] Guía de administración de SSL: https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-system-ssl-administration.html

[REF13] Guía de gestión de certificados a través de la GUI: https://my.f5.com/manage/s/article/K14620

[REF14] Guía de agrupación de servicios de dispositivos BIG-IP: https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-device-service-clustering-administration-14-1-0.html

[REF15] Guía de creación de sistema de HA en modo Activo-Standby: https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-device-service-clustering-administration-14-1-0/creating-an-active-standby-configuration-using-the-configuration-utility.html

[REF16] Guía de mitigación de vulnerabilidad CVE-2023-46747: https://my.f5.com/manage/s/article/K000137353

[REF17] Guía de configuración del nivel de log registrado: https://my.f5.com/manage/s/article/K5532

[REF18] BIG-IP® Common Criteria Evaluation Configuration Guide, BIG-IP® Release 17.1.0.1, Document Number: CC2023-AGD-001, Document Version: 7.7, Date: 03/08/2024. https://my.f5.com/manage/s/article/K000132573

[REF19] Guía de enrutamiento de BIG-IP: https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-tmos-routing-administration-14-1-0.html

8 ABREVIATURAS

ACL	Access Control List
ADC	Application Delivery Controller
AES	Advanced Encryption Standard
AFM	Advanced Firewall Manager
AJP	Apache JServ Protocol
API	Application Programming Interface
APM	Access Policy Manager
BIG-IP	Big Internet Gateway Internet Protocol
BUC	Backplane MicroController
CA	Certificate Authority
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Producto STIC
CRLDP	Certificate Revocation List Distribution Point
CRT	Certificate
CVE	Common Vulnerabilities and Exposures
DB	Database
DOS	Denial of Service
DSC	Device Service Cluster
DTLS	Datagram TLS
DUT	Device Under Test
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad.
F5	F Five
GUI	Graphics User Interface
HMAC	Hashbased Message Authentication Code
HSL	High Speed Logging
HTTP	Hypertext Transfer Protocol
HTTPD	Hypertext Transfer Protocol Daemon
HTTPS	HTTP over TLS
ICAP	Internet Content Adaptation Protocol
ICMP	Internet Control Message Protocol
iControl	iControl
IP	Internet Protocol

ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
LBH	LOP BUC Hybrid
LOP	Lights Out Processor
LTM	Local Traffic Management
MCP	Master Control Program
MD5	Message Digest 5
NTLM	New Techonlogy LAN Manager
NTP	Network Time Protocol
OVA	Open Virtual Appliance
PAM	Pluggable Authentication Module
pem	Privacy Enhanced Mail
REST	Representational State Transfer
RFC	Request for Comments
RSA	Rivest–Shamir–Adleman
RST	Reset
RTSP	RealTime Streaming Protocol
SCF	Single Configuration File
SCTP	Stream Control Transmission Protocol
SHA	Secure Hash Algorithm
SHA1	Secure Hash Algorithm 1
sig	Signature
SIP	Session Initiation Protoco
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSHD	Secure Shell Daemon
SSHv2	Secure Shell version 2
SSL	Secure Sockets Layer
STIC	Seguridad de las Tecnologías de la Información y Comunicación
TACACS	Terminal Access Controller AccessControl System
TCP	Transmission Control Protocol
TCPDUMP	Transmission Control Protocol Dump
TLS	Transport Layer Security

TMOS	Traffic Management Operating System
tmsh	Traffic Management Shell
TMSH	Traffic Management Shell
TMUI	Traffic Management User Interface
TOE	Target Of Evaluation
UCS	User Configuration Set
US	United States
vCMP	Virtual Clustered Multiprocessing
VHD	Virtual Hard Disk
VLAN	Virtual Local Area Network
VXLAN	Virtual Extensible Local Area Network
WA	Washington
XML	Extensible Markup Language