centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1613

Procedimiento de empleo seguro
F5 BIG-IP 14.0.1 para LTM+AFM

Mayo 2022

MINISTERIO DE DEFENSA

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

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.09.20 17:12:14 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-232-5

Fecha de Edición: mayo de 2022.

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

El producto BIG-IP es un dispositivo ADC (*Application Delivery Controller*) "*full-proxy*" programable que utiliza el TMOS (Traffic Management Operating System) de F5. Como "*full-proxy*", BIG-IP es el encargado de mantener, optimizar y establecer las conexiones entre servidor y cliente de forma independiente, pudiendo adaptarse y programarse de forma óptima para cada aplicación o cliente. BIG-IP cuenta con múltiples funcionalidades que permiten adaptar, bastionar y optimizar la entrega de las aplicaciones en entornos de red. Además, dispone de diversos licenciamientos software que permiten desplegar funcionalidades específicas de control de acceso, seguridad, disponibilidad y optimización de la red.

El producto ADC consta de la combinación de los módulos LTM (*Local Traffic Manager*) y AFM (*Advanced Firewall Manager*).

El módulo AFM implementa filtrado estático de tráfico en paquetes de red de niveles 2 y 4, empleando reglas de filtrado definidas por usuarios con rol de administración, basándose en los atributos de los paquetes de red.

El TMM (*Traffic Management Microkernel*) provee al al Sistema de funcionalidades básicas de red, aportando al sistema funcionalidades de switch.

El entorno soporta vCMP (*Virtual Clustered Multiprocessing*), el cual permite la ejecución de múltiples instancias del sistema bajo el mismo hardware.

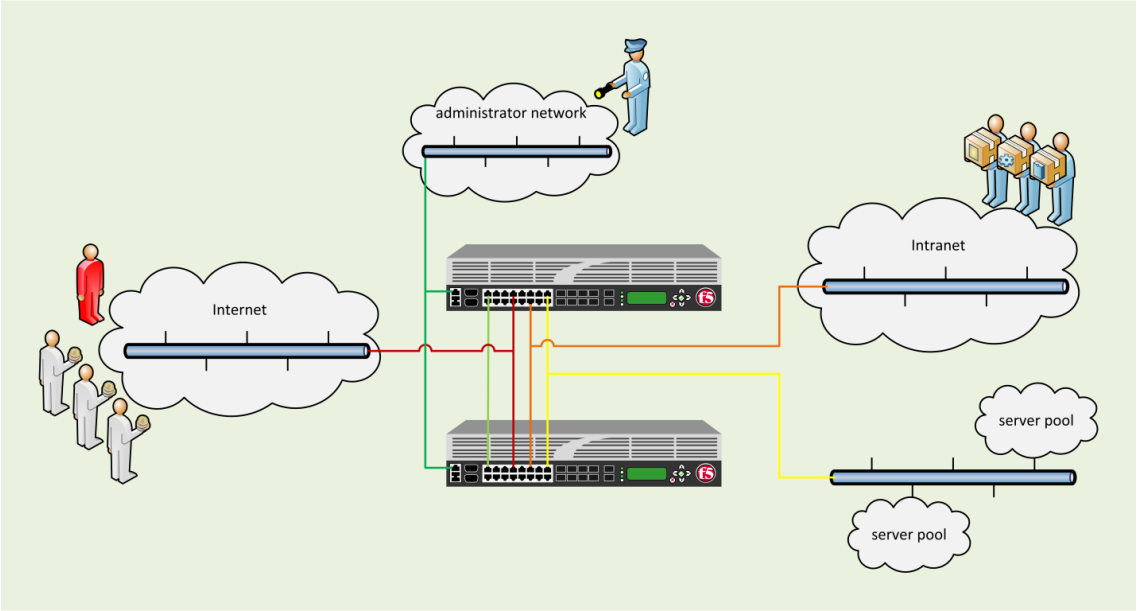


Figura 1 – Esquema de red de entorno BIG-IP LTM+AFM

2. OBJETO Y ALCANCE

En este documento se recoge el procedimiento de empleo seguro para el sistema **F5 BIG-IP LTM+AFM versión 14.1.0.3** con la revisión **HotfixBIGIP-14.1.0.3.0.75.6-ENG.**

En la tabla indicada a continuación se lista el hardware y el software del grupo de productos a los que aplica este procedimiento de empleo seguro:

SKU	vCMP	Part Number	Model Series
F5-BIG-LTM-I5600 F5-ADD-BIG-AFM-I5XXX F5-ADD-BIG-MODE	No	200-0396-02	i5000
F5-BIG-LTM-I7600 F5-ADD-BIG-AFM-I7XXX F5-ADD-BIG-MODE	No	500-0003-03	i7000
F5-BIG-LTM-I10600 F5-ADD-BIG-AFM-I10XXX F5-ADD-BIG-MODE	No	500-0002-03	i10000
F5-BIG-LTM-I11600-DS F5-ADD-BIG-AFMI11XXX F5-ADD-BIG-MODE	Sí	500-0015-03	i11000-DS
F5-BIG-LTM-I15600 F5-ADD-BIG-AFMI15XXX F5-ADD-BIG-MODE	No	500-0001-07	i15000
F5-BIG-LTM-I5800 F5-ADD-BIG-AFM-I5XXX F5-ADD-BIG-MODE	Sí	200-0396-02	i5000
F5-BIG-LTM-I5820-DF F5-ADD-BIG-AFM-I5XXX F5-ADD-BIG-MODE	Sí	500-0017-06	i5000
F5-BIG-LTM-I7800 F5-ADD-BIG-AFM-I7XXX F5-ADD-BIG-MODE	Sí	500-0003-03	i7000
F5-BIG-LTM-I7820-DF F5-ADD-BIG-AFM-I7XXX F5-ADD-BIG-MODE	Sí	500-0016-06	i7000
F5-BIG-LTM-I10800 F5-ADD-BIG-AFM-I10XXX F5-ADD-BIG-MODE	Sí	500-0002-03	i10000
F5-BIG-LTM-I11800-DS F5-ADD-BIG-AFMI11XXX F5-ADD-BIG-MODE	Sí	500-0015-03	i11000-DS
F5-BIG-LTM-I15800 F5-ADD-BIG-AFMI15XXX F5-ADD-BIG-MODE	Sí	500-0001-07	i15000

SKU	vCMP	Part Number	Model Series
F5-VPR-LTM-C2400-AC F5-VPR-LTM-B2250 F5-ADD-VPR-AFM-C2400 F5-ADD-BIG-MODE F5-ADD-VPR-VCMP-2400	Sí	400-0028-10 400-0039-03	C2400 B2250
F5-VPR-LTM-C4480-AC F5-VPR-LTM-B4450 F5-ADD-VPR-AFM-C4400 F5-ADD-BIG-MODE F5-ADD-VPR-VCMP-4480	Sí	400-0033-04 400-0053-10	C4480 B4450
F5-BIG-LTM-10350V-F F5-ADD-BIG-AFM-10000 F5-ADD-BIG-MODE	Sí	200-0398-00	10000 Series (FIPS)

Tabla 1. Productos contemplados para este procedimiento seguro.

Donde se puede identificar en cada columna las especificaciones:

- **SKU (*stock-keeping unit*):** identificador de hardware y software del producto.
- **vCMP:** soporte de la plataforma para utilizar vCMP.
- **Part Number:** número que especifica el chasis y el dispositivo hardware del producto.
- **Model Series:** familia de appliances del producto.

Los **modelos** anteriormente **listados** son los que han sido **cualificados** e incluidos en el Catálogo de Productos y Servicios STIC**, en las familias: *'Cortafuegos'* y *'Balanceadores de Carga'***.

3. ORGANIZACIÓN DEL DOCUMENTO

El presente documento se divide en los siguientes apartados que servirán de guía en la configuración segura del producto:

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

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

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.

Apartado 7. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

Apartado 8. En este apartado se incluye una *checklist* con las tareas necesarias.

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

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

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Tanto el envío como el seguimiento de los dispositivos hardware BIG-IP son realizados directamente desde un proveedor de confianza. El embalaje sellado debe incluir un comprobante con la lista de componentes en el interior:

- Etiquetas indicativas con la nomenclatura del producto.
- Información del número de venta y del envío.
- Número de serie del producto.

El embalaje del dispositivo BIG-IP debe de ser inspeccionado para detectar posibles alteraciones o irregularidades, las etiquetas externas deben coincidir con la entrega del producto esperado, así como los componentes deben coincidir con los de la documentación enviada con el producto.

En caso de identificarse algún problema durante la inspección, el cliente deberá ponerse en contacto inmediatamente con el proveedor.

4.1.1 OBTENCIÓN DEL SOFTWARE

El producto BIG-IP incluye un software ya instalado en el momento de su entrega. Sin embargo, se recomienda descargar una imagen software de la página oficial de F5 para una instalación de la versión segura del software. La instalación de este software asegurará que el sistema no ha sido manipulado.

Para instalar una versión limpia del sistema 14.1.0.3, debe de descargarse una nueva copia del software de la versión 14.1.x desde el sitio oficial de descarga de F5 [REF2], para posteriormente ser verificado. Una vez llevado a cabo este proceso, el software deberá ser instalado en una unidad de arranque inactiva. Para que la imagen del producto cumpla con la seguridad requerida, debe también descargar e instalar la revisión “Hotfix-BIGIP-14.1.0.3.0.75.6-ENG” desde la misma ubicación.

Dado que el aspecto exacto del sitio de descargas de F5 puede cambiar con el tiempo, las instrucciones a continuación sobre qué descargar son específicas para los archivos, pero no proporcionan instrucciones detalladas para navegar por el sitio. Sin embargo, las siguientes pautas siguen siendo válidas:

1. Se debe seleccionar el enlace o menú desplegable que permita acceder a la descarga del software, en el apartado de versiones v14.x.

F5 Product Family	Product Line
BIG-IP	BIG-IP v16.x / Virtual Edition with Traffic Management Operating System® (TMOS®)
	BIG-IP v15.x / Virtual Edition with Traffic Management Operating System® (TMOS®)
	BIG-IP v14.x / Virtual Edition with Traffic Management Operating System® (TMOS®)
	BIG-IP v13.x / Virtual Edition with Traffic Management Operating System® (TMOS®)
	BIG-IP v12.x / Virtual Edition with Traffic Management Operating System® (TMOS®)
	BIG-IP v11.x / Virtual Edition with Traffic Management Operating System® (TMOS®)
	APM Clients
	F5 Access Guard
	Guided Configuration
	iApp Templates
	iAppLX Templates

Figura 2. Sección de descargas de la web oficial de F5.

2. Una vez se haya accedido a dicho menú, se debe elegir la versión 14.1.x. En la página se proporcionan enlaces para todos los archivos ISO correspondientes a la versión 14.1.x

Select a Product Version and Container for

BIG-IP V14.X / VIRTUAL EDITION WITH TRAFFIC MANAGEMENT OPERATING SYSTEM® (TMOS®)

The latest product version is displayed by default. If you are looking for downloads related to a different version of this product, please select from the following options.

14.1.0 (LTS)

Select a product container.

Name	Version	Type	Date	Description
GeoLocationUpdates	14.1.0	Patches	11/05/2021	GeoLocationUpdates
epsec-1.0.0-852.0	14.1.0	Patches	07/09/2019	OPSWAT Endpoint Security Integration Update. See readme_minimum_version.txt before install
BotSignaturesUpdates	14.1.0	Release	11/07/2021	BotSignaturesUpdates
FPS-LatestSignatureFile	14.1.0	Release	11/07/2021	FPS-LatestSignatureFile
ASM-AttackSignaturesUpdates	14.1.0	Release	11/05/2021	ASM-AttackSignaturesUpdates
ThreatCampaignUpdates	14.1.0	Release	11/03/2021	ThreatCampaignUpdates
BrowserChallengesUpdates	14.1.0	Release	09/03/2021	BrowserChallengesUpdates

Figura 3. Panel de descarga de la versión del producto.

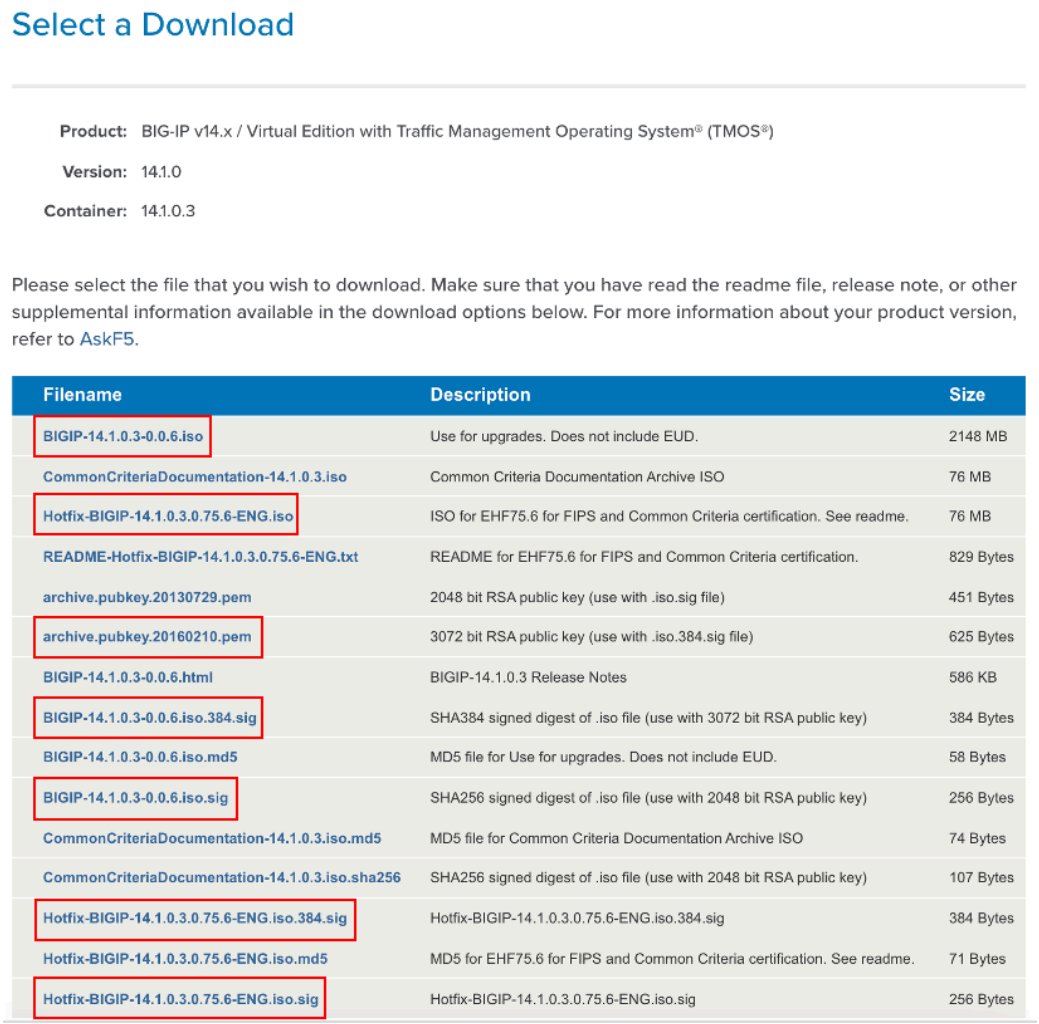
3. Cada página correspondiente a cada uno de los archivos ISO enumerados tiene la imagen software del producto, el archivo de firma digital y el archivo de clave pública correspondiente, tal y como se describe a continuación. Los archivos a descargar son los siguientes:

   a) El archivo imagen de software “BIGIP-14.1.0.3-0.0.6.iso”.

   b) Los archivos “BIGIP-14.1.0.3-0.0.6.iso.sig” o “BIGIP-14.1.0.3-0.0.6.iso.384.sig” para la verificación de la imagen.

c) La revision “Hotfix-BIG-IP-14.1.0.3.0.75.6-ENG.iso”.

d) Los archivos “archive.pubkey.20130729.pem” (correspondiente al archivo iso.sig) o “archive.pubkey.20160210.pem” (correspondiente al archivo iso.384.sig).



Select a Download

Product: BIG-IP v14.x / Virtual Edition with Traffic Management Operating System® (TMOS®)

Version: 14.1.0

Container: 14.1.0.3

Please select the file that you wish to download. Make sure that you have read the readme file, release note, or other supplemental information available in the download options below. For more information about your product version, refer to AskF5.

Filename	Description	Size
BIGIP-14.1.0.3-0.0.6.iso	Use for upgrades. Does not include EUD.	2148 MB
CommonCriteriaDocumentation-14.1.0.3.iso	Common Criteria Documentation Archive ISO	76 MB
Hotfix-BIGIP-14.1.0.3.0.75.6-ENG.iso	ISO for EHF75.6 for FIPS and Common Criteria certification. See readme.	76 MB
README-Hotfix-BIGIP-14.1.0.3.0.75.6-ENG.txt	README for EHF75.6 for FIPS and Common Criteria certification.	829 Bytes
archive.pubkey.20130729.pem	2048 bit RSA public key (use with .iso.sig file)	451 Bytes
archive.pubkey.20160210.pem	3072 bit RSA public key (use with .iso.384.sig file)	625 Bytes
BIGIP-14.1.0.3-0.0.6.html	BIGIP-14.1.0.3 Release Notes	586 KB
BIGIP-14.1.0.3-0.0.6.iso.384.sig	SHA384 signed digest of .iso file (use with 3072 bit RSA public key)	384 Bytes
BIGIP-14.1.0.3-0.0.6.iso.md5	MD5 file for Use for upgrades. Does not include EUD.	58 Bytes
BIGIP-14.1.0.3-0.0.6.iso.sig	SHA256 signed digest of .iso file (use with 2048 bit RSA public key)	256 Bytes
CommonCriteriaDocumentation-14.1.0.3.iso.md5	MD5 file for Common Criteria Documentation Archive ISO	74 Bytes
CommonCriteriaDocumentation-14.1.0.3.iso.sha256	SHA256 signed digest of .iso file (use with 2048 bit RSA public key)	107 Bytes
Hotfix-BIGIP-14.1.0.3.0.75.6-ENG.iso.384.sig	Hotfix-BIGIP-14.1.0.3.0.75.6-ENG.iso.384.sig	384 Bytes
Hotfix-BIGIP-14.1.0.3.0.75.6-ENG.iso.md5	MD5 for EHF75.6 for FIPS and Common Criteria certification. See readme.	71 Bytes
Hotfix-BIGIP-14.1.0.3.0.75.6-ENG.iso.sig	Hotfix-BIGIP-14.1.0.3.0.75.6-ENG.iso.sig	256 Bytes

Figura 4. Archivos requeridos para la instalación del producto.

4.1.2 VERIFICACIÓN DE LA ISO DEL PRODUCTO MEDIANTE LA FIRMA DIGITAL

Una vez descargado el software se debe realizar una verificación de integridad previa a la instalación. Junto con la descarga del software del producto se incluyen en la propia página de descarga varios archivos con el mismo nombre que el software, pero con los siguientes formatos: *.pem, *.sig y *.384.sig. Los archivos *.sig y *.384.sig contienen una firma digital para verificar que la imagen es un producto oficial de F5, cualquiera de los dos es válido para realizar dicha verificación. Se requiere la clave pública en formato *.pem para este paso de verificación, la cual será distinta para el archivo *.sig y el *.384.sig.

La verificación de la descarga se ha de hacer manualmente, ya que la verificación automática por firma solo estará habilitada cuando se ejecute el modo de operación seguro más adelante y la variable **Security.CommonCriteria DB** este activada. El modo de operación seguro activa dicha variable automáticamente, la cual desencadena varios procesos internos como la ejecución de syscheck en la inicialización, o las mencionadas pruebas de integridad de OpenSSL.

Si falla la verificación de la firma en BIG-IP, la instalación de la actualización del software fallará. En este caso, se deberá intentar descargar la ISO nuevamente. Si la verificación de la firma falla por segunda vez, será necesario ponerse en contacto con el soporte de F5.

Como se ha indicado previamente, se ha de verificar la ISO manualmente empleando la utilidad **OpenSSL** del sistema en el que se descargaron previamente los archivos ISO, *.sig o *.384.sig y *.pem.

A continuación, se presentan ejemplos de comandos de verificación a través de openSSL:

- **Linux:**

openssl sha256 –verify archive.pubkey.20130729.pem –signature BIGIP-14.1.0.3-0.0.6.iso.sig BIGIP-14.1.0.3-0.0.6.iso

- **Windows:**

C:\Users\name\Desktop> openssl dgst -sha256 -verify archive.pubkey.20130729.pem -signature BIGIP-14.1.0.3-0.0.6.iso.sig BIGIP-14.1.0.3-0.0.6.iso

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, se deberá intentar descargar la ISO nuevamente. Si la verificación de la firma falla por segunda vez, será necesario ponerse en contacto con el soporte de F5.

F5 cuenta con un *Knowledge Center* [REF1] para la consulta de artículos con documentación oficial para la administración y configuración del producto. Para más detalles sobre el proceso de verificación de software, acceder al artículo de F5: K24341140: Verifying BIG-IP software images using SIG and PEM files. [REF3]

4.2 ENTORNO DE INSTALACIÓN SEGURO

El dispositivo BIG-IP debe de instalarse en un Centro de Proceso de Datos (CPD), que disponga de protección física, de forma que no sea objeto de ataques que comprometan la propia seguridad y/o interfieran en las interconexiones físicas y su correcta operación. El nivel de seguridad debe ser acorde con la política del cliente para los activos a proteger en el entorno IT.

Los usuarios administradores del sistema BIG-IP deben ser únicamente los autorizados, adecuándose siempre a las políticas de seguridad estipuladas y las guías de documentación adecuadas.

Las credenciales del administrador (clave privada) utilizadas para acceder al dispositivo de red estarán protegidas en la plataforma en la que residen.

Los usuarios administrativos autorizados se encargarán de la actualización regular del firmware y el software de BIG-IP en respuesta a lanzamientos de actualizaciones debido a posibles vulnerabilidades conocidas.

Se debe asegurar que BIG-IP esté configurado para recibir, almacenar y proteger los registros de auditoría generados por la red.

Opcionalmente, en caso de contar con un equipo de redundancia, se recomienda configurar el sistema para conmutación por error (ver apartado 6.11 ALTA DISPONIBILIDAD). Los sistemas implicados en que los equipos del par sincronicen configuración y datos entre sí debe ser fiable. Lo que significa que el equipo redundante debe estar configurado de forma idéntica y bajo la misma administración que el resto del sistema.

4.3 REGISTRO Y LICENCIAS

Para poder utilizar el software de BIG-IP, debe de activarse la licencia recibida desde F5.

Se deben realizar dos actualizaciones de la configuración SSH antes de aplicar la licencia en el dispositivo: configuración de clave pública y algoritmos de cifrado SSH. Se recomienda revisar el apartado AUTENTICACIÓN A TRAVÉS DE SSH de este mismo documento antes de proceder a licenciar el producto.

Para activar la licencia se debe acceder a través de la web GUI al menú *System > License* usando una cuenta con rol de administrador, accediendo a través de la URL: “https://<Dirección IP>”. La dirección IP corresponde a la dirección asignada al puerto de administración del sistema.

Se deben seguir los pasos indicados por F5 para la activación de las licencias, accediendo a su documentación oficial: K7752: Licensing the BIG-IP system [REF4]

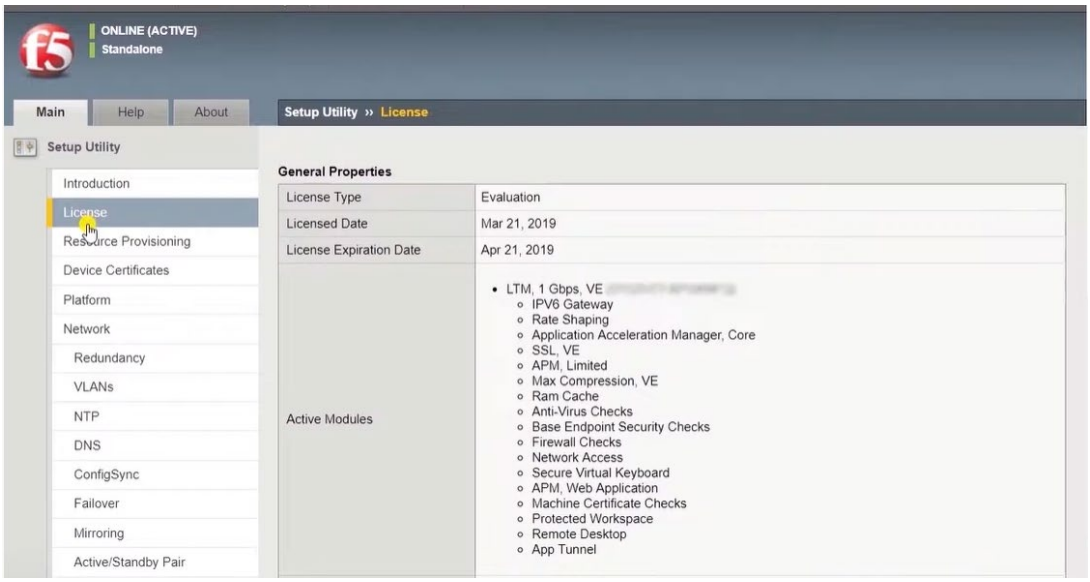


Figura 5. Licencia activa en el sistema BIG-IP.

4.4 CONSIDERACIONES PREVIAS

Antes de realizar las instalaciones de software correspondientes para una configuración segura del producto, se debe tener en cuenta que no se debe incluir software de propósito general en el sistema BIG-IP. Solo se incluirán los servicios para la operación, administración y soporte de la red.

Los siguientes elementos **están excluidos del sistema** para una configuración correcta de seguridad y **no deben configurarse** para mantener el cumplimiento de los requisitos de seguridad necesarios:

- **LBH (LOP + BUC: *Lights Out Processor + Backplane Microcontroller):*** de forma predeterminada no es accesible desde la red de administración y no debe configurarse. Los dispositivos BIG-IP incorporan un subsistema independiente de administración *Ligths Out* llamado AOM (*Lights Out Management*) que permite administrar funcionalidades de bajo nivel mediante SSH o la consola serie, incluso si el appliance está apagado. El appliance BIG-IP y el subsistema AOM funcionan de forma independiente.
- **Configuración de servidor remoto:** no configurar los siguientes servidores externos para el producto:
    a) SNMP.
    b) Delegación Kerberos.
    c) RADIUS.
    d) TACACS+.
- **Perfiles:** los perfiles son elementos de la configuración que determinan el comportamiento del sistema con determinados tipos de tráfico o contenidos (se puede encontrar una referencia completa en el siguiente enlace: BIG-IP Local Traffic Management: Profiles Reference [REF28]. Al igual que con los servidores remotos, no se deben configurar los siguientes perfiles:
    a) HTTP: Aceleración web: regula las técnicas de aceleración de entrega de contenidos web.
    b) Otros perfiles de capa de aplicación, los cuales regulan ciertos protocolos y comportamientos: RTSP (protocolo de *streaming*), ICAP *Request Adapt* y *Response Adapt* (protocolo de adaptación de contenido en peticiones HTTP), *Diameter* (protocolo de enrutamiento de mensajes), RADIUS (protocolo de autenticación remota), SIP (protocolo de señalización de comunicaciones multimedia), *Rewrite* (perfil de reescritura de URLs para proxy inverso).
    c) Perfiles de Persistencia (*Persistence*): solo se excluyen los de los siguientes tipos: *Microsoft Remote Desktop* (persistencia para conexiones que usan el protocolo RDP de conexión a escritorios remotos), SIP (Persistencia para conexiones mediante el protocolo SIP).

d) Protocolos: perfiles SCTP: regulan el comportamiento del protocolo de transporte SCTP.

e) Perfiles de Autenticación de servidor remoto: RADIUS, TACACS +, CRLDP y Kerberos.

f) Otros: NTLM (protocolos de autenticación de Microsoft para equipos Windows), *Stream* (perfil de modificación de contenido).

- **Imi Shell (Integrated Management Interface Shell):** no se requiere un shell de terceros de uso limitado para administrar el sistema de acuerdo con la configuración de seguridad requerida. El Modo Appliance evita el uso de esta Shell.
- **Comandos tmsh:** una serie de comandos no están incluidos o no están permitidos en la configuración segura. Ver ANEXO I: COMANDOS NO PERMITIDOS (TMSH) de este documento para consultar la lista de comandos excluidos. Esta lista también se aplica a las API de iControl Rest.
- **Módulos API iControl e interfaces:** no están incluidos o no están permitidos en la configuración segura del producto. Ver ANEXO II: APIS DE ICONTROL NO PERMITIDAS de este documento para consultar la lista de las APIs de iControl no permitidas.
- **iRulesLX e iAppsLX:** no deben usarse en la configuración segura del sistema. IRulesLX es una funcionalidad adicional de los dispositivos F5 BIG-IP que permite ampliar las funcionalidades del plano de datos de manera programática mediante el uso del lenguaje node.js. iAppsLX (junto con iControlLX) es una funcionalidad adicional que permite extender de manera programática la forma de aplicar configuraciones en un dispositivo BIG-IP.
- **Modo depuración:** BIG-IP no debe ejecutarse en modo de depuración.
- **Archivos de soporte:** todo archivo de soporte que se cree en el sistema, como pudiera ser a través de las funcionalidades de BIG-IP como qkview (utilidad de diagnóstico) o tcpdump (información de tráfico en la red), deben descargarse y eliminarse del sistema.

Finalmente, para evitar vulnerabilidades potenciales: no configurar actualización remota con autenticación TSIG ni *allow-transfer* con autenticación TSIG.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

El Sistema BIG-IP LTM+AFM utiliza la versión software 14.1.0.3. El appliance está compuesto de los siguientes componentes:

- Sistema BIG-IP LTM+AFM Traffic Management Operating System (TMOS): Sistema operativo basado en Linux que se ejecuta sobre el appliance (ya sea hardware o virtualizado). Dentro del TMOS se implementan el plano de datos y el plano de control.

- Traffic Management Microkernel (TMM): elemento dentro del sistema operativo TMOS que ejecuta un conjunto de procesos encargado de implementar el plano de datos y gestionar el tráfico de los clientes.
- Local Traffic Manager (LTM): balanceador de carga que permite recibir el tráfico externo y distribuirlo a los distintos servidores internos.
- Advanced Firewall Manager (AFM): módulo encargado de gestionar las reglas de control de acceso a las aplicaciones publicadas mediante BIG-IP.

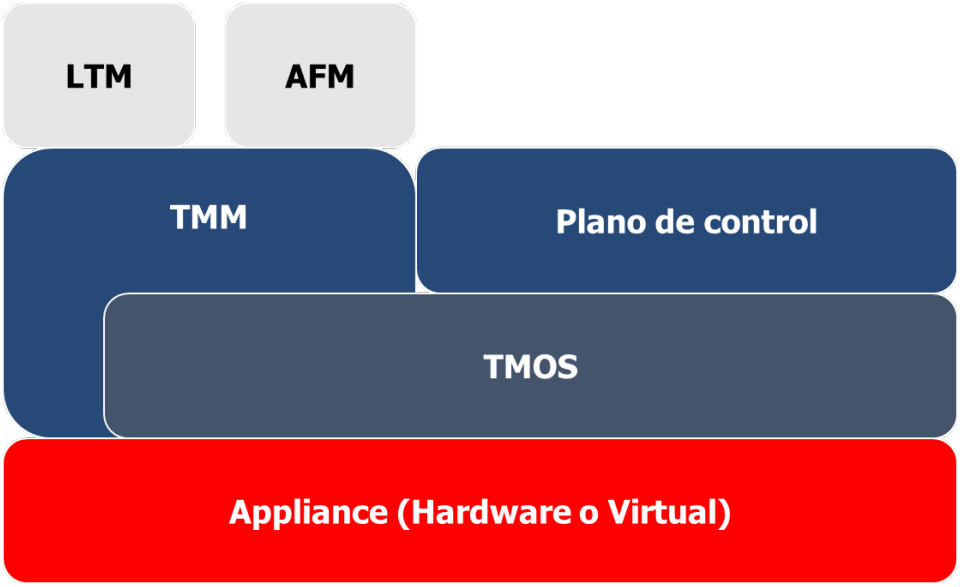


Figura 6. Componentes de la arquitectura BIGIP para un sistema LTM + AFM

Adicionalmente, también consta de los componentes externos:

- Servidor de auditoría Syslog.
- Servidor DNS.

5. FASE DE INSTALACIÓN

5.1 COMPROBACIÓN DEL SOFTWARE INSTALADO

Para verificar las versiones del software BIG-IP activas e instaladas en el equipo, puede emplearse tanto la interfaz gráfica (GUI) como la interfaz de comandos tmsh.

Para verificar la versión instalada en el sistema BIG-IP, se debe comparar la versión activa en la unidad de almacenamiento con la versión que se indica en este documento para una configuración segura (versión 14.1.0.3).

Verificación a través de línea de comandos (tmsh): Una vez se accede al sistema BIG-IP, se mostrará la interfaz de comandos tmsh, indicando cada línea con el siguiente texto: **(tmos)#.** En caso de que se quiera acceder a tmsh desde otra interfaz de línea de comandos, se debe introducir sencillamente el comando ***tmsh***. Introduciendo el comando ***tmsh show sys software status*** se muestra una tabla con las versiones del producto, mostrando la versión del software instalada en cada una de las dos ranuras (slots) de las que consta el producto. Se debe tener en cuenta que la ranura 1 en el siguiente ejemplo muestra la versión software para una configuración segura del producto, y dicha ranura será la única que utilizará BIG-IP; la ranura 2 muestra una versión inactiva instalada en dicha ranura. No se indicarán instrucciones para la instalación y configuración en la segunda ranura, dado que esta se encontrará inactiva.

Sys:: Software Status					
Volume	**Product**	**Version**	**Build**	**Active**	**Status**
HD1.1	BIG-IP	14.1.0.3	0.75.6	Yes	Complete
HD1.2	BIG-IP	13.1.0	0.0.1868	No	Complete

Tabla 2. Versiones instaladas en los slots del producto.

Empleando la interfaz gráfica (GUI) del producto, en la página *System > Software Management: Image List* se puede encontrar una tabla similar para consultar la versión software.

5.2 INSTALACIÓN DEL SOFTWARE

En el caso de que el equipo no tenga instalada la versión certificada (14.1.0.3), deberá de seguir los pasos de descarga y verificación de software oficial de F5 indicados en los apartados 4.1.1 OBTENCIÓN DEL SOFTWARE y 4.1.2 VERIFICACIÓN DE LA ISO DEL PRODUCTO MEDIANTE LA FIRMA DIGITAL.

Para proceder a la instalación del software 14.1.0.3 se debe acceder con permisos de administrador al menú *Configuration utility* y seguir los pasos indicados en la documentación de F5: K51113020: BIG-IP update and upgrade guide | Chapter 5: Update or upgrade a standalone BIG-IP system using the Configuration utility. [REF21]

A continuación, se deben seguir los pasos necesarios para instalar la revisión (*hotfix*) requerida (Hotfix-BIGIP-14.1.0.3.0.75.6-ENG) indicadas en la documentación oficial de F5: K13123: Managing BIG-IP product hotfixes (11.x - 16.x) [REF5].

6. FASE DE CONFIGURACIÓN

Las siguientes secciones proporcionan una guía preparativa para la configuración segura del producto BIG-IP LTM+AFM.

Las instrucciones de instalación y configuración se describen para un equipo, en caso de que se incluya una pareja de redundancia para la configuración en modo conmutación por error, estas instrucciones deben repetirse para el segundo equipo de la pareja.

Toda la configuración debe hacerse desde un usuario con rol Adminstrador. Para crearlo deben seguirse los pasos del apartado 6.3.2 CONFIGURACIÓN DE ADMINISTRADORES. Sus credenciales deben adaptarse a la política de contraseñas que se indica en el mismo apartado.

6.1 MODO DE OPERACIÓN SEGURO

Para que el sistema funcione de acuerdo a los requerimientos de seguridad necesarios, es necesario habilitar el modo de operación seguro. Este se activa introduciendo el comando ***ccmode*** en la interfaz de comandos tmsh. Este comando ejecuta un script de forma que este cumpla con ciertos requisitos de seguridad necesarios. En caso de que disponga de un equipo de redundancia y quiera establecer un sistema de alta disponibilidad, antes de ejecutar el comando *ccmode* debe consultar el apartado 6.11 ALTA DISPONIBILIDAD y realizar las configuración correspondiente.

La activación del comando *ccmode* ejecuta un chequeo de integridad del sistema que puede durar varios minutos.

Los comandos y la configuración establecida por *ccmode* se desglosan en la tabla que se muestra a continuación:

Comando	Descripcion
tmsh modify net self-allow defaults none	Configura los puertos de la IP propia a *"allow=none"*, bloqueando todos los puertos desde el punto de vista de administración.
tmsh modify /sys daemon-log-settings mcpd audit enabled **tmsh modify /sys daemon-log-settings tmm os-log-level error**	Habilita los procesos de registro de logs y auditoría. Esto asegura que cada comando de GUI y tmsh es auditado correctamente.
tmsh modify /sys db log.ssl.level value informational	Asegura que el acceso a través de TLS se audita de forma correcta.
tmsh modify / sys global-settings lcd-display disabled	Deshabilita el *display* LCD y panel frontal.
tmsh modify / sys service snmpd disable	Deshabilita el servicio SNMP.
Rutina interna para generar una nueva clave de dispositivo.	Asegura que se genera una clave para los certificados de dispositivo. Los certificados de dispositivo se usan para comunicación entre equipos BIG-IP usando solo cifrados restringidos. Para más información consultar: BIG-IP System: SSL Administration: Device Certificate Management [REF42]
tmsh modify /sys httpd (ssl-ciphersuite EECDH+AES:RSA+AES:@STRENGTH ssl-protocol all -SSLv2 -SSLv3 -TLSv1)	Asegura que el servicio HTTPS use cifrados y versiones de TLS seguras.
tmsh modify /ltm profile client-ssl clientssl ciphers COMMON_CRITERIA **tmsh modify /ltm profile server-ssl serverssl ciphers COMMON_CRITERIA**	Asegura que los perfiles SSL usen solo una serie de cifrados restringidos.
Script sed para actualizar el fichero de configuración de sshd.	El archivo de configuración del servicio SSH es actualizado para permitir únicamente aes128-cbc y aes256-cbc como cifrados válidos.
tmsh modify /auth password-policy policy-enforcement enabled minimum-length 15 required-uppercase 1 required-lowercase 1 required-numeric 1 required-special 1 max-	Configura la política por defecto de contraseñas:

Comando	Descripcion
duration 90 expiration-warning 7 max-login-failures 3 password-memory 3	• Mínima longitud de contraseña de 15 caracteres. • Al menos una mayúscula. • Al menos una minúscula. • Al menos un número. • Al menos un carácter especial. • Expiración de la contraseña en 90 días. • El usuario recibe un aviso de 7 días antes de la expiración de la contraseña. • El usuario tiene 3 intentos de acceso fallidos antes de ser bloqueado. • La contraseña no puede coincidir con ninguna de las 3 contraseñas previas.
tmsh modify cli global-settings idle-timeout 20	Configura el tiempo de sesión de tmsh en 20 minutos.
tmsh run util sys-icheck	Ejecuta la utilidad sys-icheck para validar los archivos RPM.
tmsh modify /sys db liveisntall.checksig value enable	Asegura que todos los archivos de instalación aplicados en la configuración inicial deben pasar la validación de firma.
tmsh modify /sys db provision.action value reboot	Actualización del *prompt* para recordar al administrador que debe reiniciar una vez el comando ccmode se ha completado.
tmsh modify /sys db security.commoncriteria value true	Modifica el valor de la variable security.commoncriteria indicando que el modo está activado.
tmsh modify /sys db statemirror.secure value enable **tmsh modify /sys db failover.secure value enable**	Asegura que las comunicaciones en *failover* son seguras y están cifradas.
tmsh modify /sys db systemauth.disablelocaladminlockout value true **tmsh modify /sys db systemauth.disablemanualunlock value true**	Asegura que el usuario administrativo principal puede acceder de forma local incluso si ha sido bloqueado del acceso remoto.

Comando	Descripcion
tmsh modify /sys db password.unlock_time value 600	Desactiva el desbloqueo manual y establece los desbloqueos por tiempo. Configuración del valor de desbloqueo a 600 segundos (10 minutos).
tmsh modify / sys aom enabled **tmsh modify /sys aom media-redirection enabled** **tmsh modify /sys aom vkvm enabled** **tmsh modify /sys aom webui enabled** **tmsh modify /sys aom ipmi enabled**	Se deshabilita el *Ligths Out Management* (Subsitema AOM)
tmsh save /sys config	Guarda la configuración establecida.

Tabla 3. Comandos del script ejecutado por ccmode.

A pesar de que este comando es necesario para el establecimiento del modo de operación seguro, sus configuraciones no son suficientes, por lo que se deberán seguir todas las modificaciones indicadas a lo largo del procedimiento en el apartado 6 FASE DE CONFIGURACIÓN

En caso de que se quiera deshacer alguna configuración establecida por *ccmode* o modificar su configuración, se deberá deshacer cada uno de sus comandos individualmente y modificar las variables de la base de datos a sus valores iniciales.

En caso de que ocurra una conmutación por error, los sistemas que están configurados en un grupo de dispositivos para sincronizar datos de configuración entre sí deben ser fiables. Todos ellos deben estar bajo la misma administración que el sistema principal, configurados de manera idéntica y deben poder hacerse sobre ellos las mismas suposiciones que para el sistema principal. Para más información sobre la configuración del modo de conmutación por error, ir al apartado 6.11 ALTA DISPONIBILIDAD

Los usuarios de administración deben asegurarse de que el equipo de red se descarte o se retire de la operación de una manera que garantice que no sea posible el acceso no autorizado a la información residual sensible previamente almacenada en el equipo. Esto incluye asegurarse de que las claves criptográficas, el material de claves, los PIN y las contraseñas de los dispositivos de red no sean accesibles después de que los dispositivos se descarten o se retiren del funcionamiento.

De forma predeterminada, BIG-IP implementa la destrucción de claves.

El generador de números aleatorios implementado en BIG-IP no requiere configuración, dado que las fuentes de entropía están configuradas de forma segura por defecto.

6.2 AUTENTICACIÓN

El sistema BIG-IP autentica principalmente a los administradores por nombre de usuario y contraseña, almacenados en la base de datos local de configuración. A continuación, se explican las formas de autenticación a través de SSH y TLS:

6.2.1 AUTENTICACIÓN A TRAVÉS DE SSH

Para la autenticación a través de SSH, el sistema soporta los siguientes métodos:

- Autenticación con clave pública.
- Autenticación basada en contraseñas.

Autenticación con clave pública: para utilizar la autenticación basada en clave pública para la administración a través de SSH, **esta deberá ser configurada antes de aplicar la licencia del dispositivo**, puesto que la aplicación de la licencia configura el dispositivo en Modo Appliance con una funcionalidad limitada sobre la línea de comandos.

La autenticación con clave pública mediante SSH requiere de la generación de una pareja de claves SSH pública y privada (el modo de generarlas dependerá del sistema operativo) en el dispositivo remoto, de manera que se intercambie la clave pública entre el dispositivo remoto y el BIG-IP. Para ello se deberán llevar a cabo los pasos que se enumeran a continuación:

```
mkdir /home/<username>
mkdir /home/<username>/.ssh
chgrp webusers <groupname>
vim /home/<username>/.ssh/authorized_keys
chmod 644 /home/<username>/.ssh/authorized_keys
restorecon -R -v /home/
```

Donde los nombres especificados son:

- ***<username>***: nombre del usuario al que le está otorgando acceso.
- ***<groupname>***: grupo para el archivo de claves.
- ***authorized_keys: es un*** contiene las claves que está autorizando.
- En el paso ***vim /home/<username>/.ssh/authorized_keys*** será necesario añadir mediante el editor de texto la clave (o claves) de acceso previamente generadas.

Se ha de tener en cuenta que este conjunto de comandos permite crear los usuarios a nivel de sistema operativo Linux, y copiar las claves públicas usadas en la autenticación SSH. Este procedimiento debe ejecutarse para cada usuario que se va a autenticar.

Se ha de tener en cuenta que es posible definir las claves para los usuarios del sistema operativo que aún no están definidos a nivel de BIG-IP (dado que los usuarios a nivel de

sistema operativo y BIG-IP son independientes). Estos usuarios se pueden definir más adelante usando la interfaz de comandos tmsh o la interfaz gráfica (GUI) del producto, tal y como se indica en el apartado 6.3.2 CONFIGURACIÓN DE ADMINISTRADORES.

Para obtener más detalles acerca de la configuración de autenticación SSH mediante el uso de clave pública, se debe consultar la sección sobre autenticación segura unidireccional basada en host desde un sistema remoto al sistema BIG-IP: K13454: Configuring SSH public key authentication on BIG-IP systems (11.x – 16.x) [REF8].

Autenticación basada en contraseñas: los administradores se autentican con usuario y contraseñas almacenadas en la base de datos local. Los servidores de autenticación remotos (como LDAP o AD) no están soportados para una configuración segura del producto. Para seguir la política de contraseñas seguras se debe consultar el apartado 6.3.2 CONFIGURACIÓN DE ADMINISTRADORES.

Para configurar y establecer un cifrado seguro de los canales de autenticación a través de SSH, consultar el apartado 6.3.1.1 CONFIGURACIÓN DE SSH.

6.2.2 AUTENTICACIÓN A TRAVÉS DE TLS

Los administradores se conectan al producto vía HTTPS implementando TLS sobre una interfaz de red dedicada usada exclusivamente para la administración del sistema. Se autentican utilizando la base de datos local con usuario y contraseña.

La autenticación remota a través de la interfaz web GUI, protocolo SOAP (iControl API) o la REST API (iControl REST API) está protegida por TLS, estando este limitado a la versión TLSv1.2. Para la configuración de TLSv1.2 y los cifrados seguros consultar el apartado 6.3.1.2 CONFIGURACIÓN DE TLS.

Para acceder al sistema a través de la interfaz gráfica, se debe acceder utilizando la dirección IP establecida durante el proceso de configuración inicial, empleando para ello un navegador web con la URL: “https://<Dirección IP>”. Posteriormente, se debe introducir el usuario y contraseña de administración para gestionar y configurar el producto.

Si no se ha configurado un certificado SSL para reemplazar el certificado autofirmado al acceder a la interfaz web GUI, se permitirá acceder a la pantalla de inicio de sesión añadiendo una única excepción de seguridad, pero el navegador mostrará un mensaje indicando que la conexión es insegura. Se debe sustituir el certificado autofirmado siguiendo el artículo de la web de F5: K42531434: Replacing the Configuration utility’s self-signed SSL certificate with a CA-signed SSL certificate [REF9] y configurar el nuevo certificado consultando el apartado 6.5 GESTIÓN DE CERTIFICADOS.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

El sistema BIG-IP se puede configurar a través de una conexión local directa (ethernet) o remota (a través de la red de administración).

La administración del producto de forma local se realiza a través del terminal del puerto serie.

Para la administración remota del producto, las interfaces de administración que pueden utilizarse son:

- **Shell de gestión de tráfico (tmsh):** funciona sobre el protocolo SSH. Se trata de la única interfaz de comandos que debe usarse para realizar una administración segura del producto. Como documentación adicional para la administración a través de tmsh, puede consultarse la documentación: Guía completa de comandos tmsh [REF7]
- **GUI web:** funciona sobre el protocolo HTTPS. Se establece como mínimo **TLSv1.2** para una gestión segura a través de la web GUI. Como información adicional sobre la administración del sistema BIG-IP puede consultarse la documentación: Administración del módulo de LTM: Aspectos básicos. [REF10]
- **iControl SOAP o iControl REST:** ambas interfaces programáticas que funcionan sobre el protocolo **TLSv1.2.** Como información adicional para la administración se recomienda consultar: Guía de usuarios de iControl. [REF11]

6.3.1.1 CONFIGURACIÓN DE SSH

El producto implementa un servidor y un cliente SSHv2. **No debe utilizarse el cliente SSH del producto**, ya que no se considera como canal seguro de comunicación.

Se deben **deshabilitar** los siguientes cifrados de la configuración del producto:

- diffie-hellman-group14-sha1
- ecdh-sha2-nistp521
- hmac-sha2-512
- aes128-ctr
- aes 256-ctr
- aes128-gmc
- aes256-gmc

Para ello, a través de la consola tmsh se debe modificar el apartado *include* en el archivo de configuración ***sys sshd*** con el siguiente comando:

```
tmsh modify /sys sshd include “Ciphers aes128-cbc, aes128-cbc
MACs hmac-sha1, hmac-sha2-256”
KexAlgorithms “ecdh-sha2-nistp256, ecdh-sha2-nistp384”
```

Para comprobar que la configuración de cifrado del producto ha quedado configurada con éxito, se debe introducir el comando *list /sys sshd all-properties.* En caso de que se quiera modificar la configuración con un editor de texto, introducir el comando *edit /sys*

sshd all-properties y modificar manualmente el apartado *include* con los cifrados previamente indicados. Se puede consultar información detallada en la documentación de F5: K80425458: Modifying the list of ciphers and MAC and key exchange algorithms used by the SSH service on the BIG-IP or BIG-IQ systems.[REF6]

En cuanto a la autenticación con clave pública RSA, se recomienda utilizar una **longitud mínima de 3072 bits**. Para cambiar la longitud de la clave pública, se deben seguir los siguientes pasos a través de la consola tmsh:

1. Deshabilitar el uso de claves DSA mediante el comando: *modify sys sshd include "DisableDSAAuth yes"*
2. Establecer la clave RSA usando el comando: *modify sys sshd include "HostKey /config/ssh/<key-name>"*
3. Establecer permisos de escritura y editar el archivo *keyswap.sh* tras hacer una copia de seguridad de dicho archivo tal y como se indica en el ejemplo:

```
mount -o remount,rw /usr
cp /usr/bin/keyswap.sh /usr/bin/keyswap.sh_K26031800
vim /usr/bin/keyswap.sh
```

4. Editar el archivo /usr/bin/keyswap.sh en los campos ssh-keygen estableciendo las siguientes longitudes:

```
ssh-keygen -q -f ${tmpdir}/${identity} -t rsa -b 3072 -N "" -C "$username"
ssh-keygen -q -f ${tmpdir}/ssh_host_key -t rsa1 -b 3072 -N "" -C "$hostname"
ssh-keygen -q -f ${tmpdir}/ssh_host_rsa_key -t rsa -b 3072 -N "" -C "$hostname"
```

5. Guardar el archivo. Asegurarse de que el archivo ha sido actualizado correctamente con el siguiente comando: *grep keygen /usr/bin/keyswap.sh*
6. Establecer de nuevo el modo lectura en el directorio */usr* montando el sistema de archivos con el comando: *mount -o remount,ro /usr*
7. Las claves nuevas deberán de generarse con la longitud actualizada con el siguiente comando: */usr/bin/keyswap.sh -genkeys*
8. El servicio sshd se reiniciará. Para comprobar que las nuevas longitudes son correctas, ejecute el siguiente comando *openssl rsa -noout -text -in /var/ssh/ssh_host_rsa_key | grep -i key*

Se puede consultar la documentación de F5 para más información en el artículo: K26031800: Increasing SSH keys from 1024-bit to 2048-bit keys [REF31] (se debe incrementar la longitud de clave a 3072 bits en el caso de una configuración segura).

Para restricciones adicionales en la conexión a través del SSH, se puede restringir el acceso al dispositivo desde un direccionamiento IP específico. Es posible hacerlo mediante el en menú principal, *System > Platform > SSH IP Allow > Specific Range,* donde se permite especificar el rango de IPs permitidas.

Para configurar la restricción de acceso de direcciones IP de administración al equipo mediante tmsh, se puede hacer mediante el siguiente comando:

```
Tmsh modify sys httpd allow add <rango de direccionamiento IP>
```

Adicionalmente, el programa *ssh-agent* no debe ser utilizado en el sistema BIG-IP para una configuración segura del producto.

6.3.1.2 CONFIGURACIÓN DE TLS

Para una conexión segura a través de TLS, debe configurarse para el acceso GUI exclusivamente el uso de **TLSv1.2**. Para ello, a través de la línea de comandos **tmsh** introducir los siguientes comandos:

```
(tmos)# list /sys httpd ssl-ciphersuite
(tmos)# modify /sys httpd ssl-ciphersuite
'ALL:!ADH:!EXPORT:!eNULL:!MD5:!DES:!SSLv2:!SSLv3:!TLSv1:!TLSv1.1'
(tmos)# save /sys config
```

Para más información al respecto, se recomienda consultar el enlace de la documentación: K40232071: Use TLS 1.2 only on BIG-IP GUI. [REF34]

Cuando BIG-IP actúa como servidor TLS, este genera parámetros de establecimiento de claves RSA. Se recomienda que la longitud de dichas claves sea de **3072 bits**, de la forma ya mencionada previamente en el apartado anterior de configuración de SSH.

El producto implementa un cliente TLS capaz de presentar certificados a un servidor TLS para una autenticación mutua. **El cliente TLS implementado en BIG-IP se utiliza para la comunicación con el servidor de auditoría externo Syslog**. Consultar los apartados de certificados (6.5 GESTIÓN DE CERTIFICADOS) y servidor de auditoría (6.12 AUDITORÍA) para más información al respecto.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

Por defecto, en el sistema BIG-IP vienen establecidos usuarios y contraseñas predeterminadas para las cuentas de administración *root* y *admin*:

Usuario	Contraseña
root	default
admin	admin

El sistema fuerza al usuario a modificar estas credenciales tras haber accedido por primera vez al sistema, debiendo el administrador ajustarse a la política de contraseñas seguras indicada en el apartado 6.3.2.1 POLÍTICAS DE SESIÓN Y CONTRASEÑAS en el momento de establecer dichas credenciales. Debe seguirse el procedimiento de la

documentación de F5: K13121: Changing system maintenance account passwords (11.x - 16.x) [REF35]

6.3.2.1 POLÍTICAS DE SESIÓN Y CONTRASEÑAS

La política de contraseñas establecidas por el modo de operación seguro establece los siguientes requisitos mínimos:

- Longitud mínima de 15 caracteres.
- Al menos un carácter especial.
- Al menos un carácter numérico.
- Al menos un carácter en mayúscula.
- Al menos un carácter en minúscula.

Además, se recomienda que se ajusten los siguientes parámetros de contraseña:

- Número de contraseñas anteriores ya utilizadas que no podrán repetirse se limitará, al menos, a las **últimas 5**. Para ello se debe ejecutar el comando en la consola tmsh: *modify /auth password-policy password-memory 5.*
- Tiempo de validez de las contraseñas, que deberá ser de una duración de **60 días**. Para ello debe ejecutarse el comando: *modify /auth password-policy max-duration 60.*
- Tiempo tras el cambio de contraseña tras el que se puede volver a modificar dicha contraseña, para el cual se recomiendan **10 días**. El comando tmsh que establece dicho tiempo es: *modify /auth password-policy min-duration 10.*

Entre el resto de configuraciones de contraseñas, en caso de que un usuario administrador se autentique de forma errónea un número determinado de **3 veces**, se establecerá un tiempo de bloqueo, de forma que el acceso del usuario al sistema quedará restringido durante **10 minutos** (configurado automáticamente activando el modo de operación seguro). No es posible que todos los usuarios administradores queden bloqueados del sistema, ya que el administrador principal puede autenticarse a través de la consola local incluso si está bloqueado para interfaces remotas.

Adicionalmente, se recomienda establecer un tiempo de expiración para sesiones que se han mantenido inactivas durante al menos **5 minutos** (300 segundos). Los comandos tmsh necesarios para sesiones web GUI (HTTPS/TLS) y tmsh (SSH) respectivamente, son:

- *modify /sys httpd auth-pam-idle-timeout 300*
- *modify /sys sshd inactivity-timeout 300*

Las configuraciones de política de contraseña restantes cuya configuración no ha sido especificada en este apartado, ya han sido previamente establecidas automáticamente al activar el modo de operación seguro. Dichas configuraciones se pueden consultar en la Tabla 3 del apartado 6.1 MODO DE OPERACIÓN SEGURO.

6.3.2.2 CREACIÓN DE USUARIOS Y ROLES

Para configurar nuevas cuentas de usuario, es imprescindible indicar sus roles asociados y contraseñas que cumplan con la política de contraseñas definida para el sistema. Los usuarios administrativos solo se configuran localmente (no se utilizarán servidores remotos).

Para configurar un usuario administrador es necesario crearlos o configurarlos en el menú *System > Users*, completando sus parámetros según se muestra a continuación:

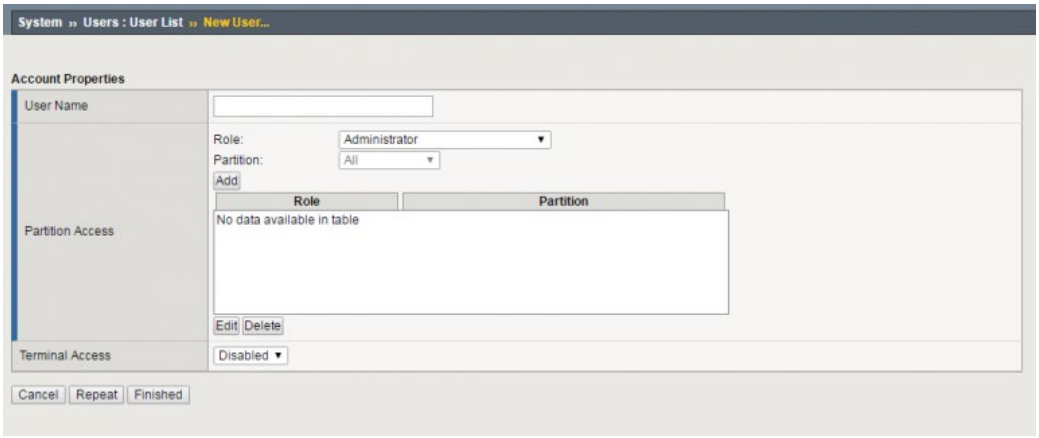


Figura 7. Menú de creación de usuarios y asignación de roles.

Los distintos roles de usuario asignables se encuentran predefinidos, e indican a que tareas o recursos tienen acceso dichos usuarios. BIG-IP establece el concepto de particiones (*partitions*) para acotar dominios del sistema a las que el usuario puede acceder. De esta forma, se puede limitar el acceso a determinadas funciones y recursos a roles específicos, permitiendo así variar los roles de un determinado usuario en las distintas particiones. Para más información sobre la configuración de particiones consultar el capítulo *Administrative Partitions* de la guía de F5: BIG-IP System: User Account Administration. [REF12]

Para información en detalle para la asignación de roles y configuración de los mismos, puede consultar el apartado *User roles* del mismo artículo: BIG-IP Systems: User Account Administration. [REF12]

Se debe asegurar que, al menos, una cuenta (además del administrador principal) de usuario administrativo tenga acceso tmsh (generalmente, la cuenta con la que se está realizando todo el proceso de configuración); esto es seleccionable eligiendo la opción *Enabled* en el atributo *Terminal Access*.

Se recomienda que el usuario administrativo principal (denominado inicialmente como *admin*) tenga acceso a la consola tmsh, debido a que este usuario es el único usuario administrativo que puede iniciar sesión localmente en caso de que todas las cuentas queden bloqueadas.

Los usuarios deben proteger su contraseña de la divulgación no autorizada. La contraseña debe almacenarse de forma segura para que otros usuarios no puedan

acceder a ella. Un usuario nunca deberá proporcionar su contraseña a ninguna otra persona.

6.3.2.3 CONFIGURACIÓN DEL BANNER DE INICIO DE SESIÓN

El cumplimiento de la configuración segura requiere que se muestre una nota de aviso y una advertencia de consentimiento (banner) antes del establecimiento de cualquier sesión de usuario administrativo para la gestión del producto. La advertencia únicamente puede ser definida por un administrador autorizado; A continuación, se muestra un ejemplo de mensaje de aviso:

> "Bienvenido a BIG-IP. Está prohibido el uso no autorizado de este sistema"

Este aviso debe mostrarse para las sesiones **GUI** y **tmsh**. Se debe seguir el proceso de configuración del banner consultando el artículo de la documentación oficial: K6068: Configuring a pre-login or post-login message banner for the BIG-IP or Enterprise Manager system. [REF13]

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

6.4.1 CONFIGURACIÓN DE INTERFACES

Para mantener una configuración segura, los siguientes interfaces y servicios **no están recomendados** o deben estar deshabilitados:

- Todas las interfaces de comandos (*shell*) aparte de tmsh deben quedar deshabilitadas. Esto se consigue mediante la aplicación de la licencia y quedando el sistema en *appliance mode*.
- La administración del producto vía protocolo SNMP debe quedar deshabilitada. Se consigue mediante la aplicación del modo de operación seguro.
- La administración del producto a través de la pantalla LCD debe quedar deshabilitada. Se consigue mediante la aplicación del modo de operación seguro.
- La administración remota mediante el subsistema *Lights Out / Always On* debe quedar deshabilitada. Se consigue mediante la aplicación del modo de operación seguro.
- El cliente SSH del producto BIG-IP **no debe ser utilizado** para establecer conexiones, ya que no se considera para una configuración segura.

Se debe asegurar que BIG-IP pueda configurarse de forma que se pueda conectar a, al menos, tres redes independientes:

- **Gestión:** para funciones administrativas, registro remoto y comunicaciones con syslog. Debe de tratarse de una red física, privada e independiente protegida contra ataques y accesos físicos no autorizados.

- **Interna:** para acceder a los servidores *backend* de soporte.
- **Externa**: para acceso a Internet o acceso de usuarios.

Opcionalmente, en caso de que se configure alta disponibilidad, también se debe establecer:

- **Red privada de conmutación por error:** utilizada para separar las conexiones de conmutación por error.

6.4.2 CONFIGURACIÓN DE VLANS

La configuración por defecto de BIG-IP incluye dos (2) VLANs: *internal* y *external,* en la partición *common.* Inicialmente, se deben asignar a cada VLAN:

- Una IP estática y una IP flotante propia.
- Una etiqueta VLAN.
- Uno o más interfaces del sistema BIG-IP.

Para crear una VLAN, se deben seguir los siguientes pasos:

1. Acceder desde la GUI web a Network > VLANs. Se abrirá una ventana de para configurar la VLAN.
2. Seleccionar *Create* para proceder a rellenar los valores de la VLAN.

Cuando se configura la VLAN, es necesario asegurarse de que las siguientes opciones están activadas:

- ***Source Check:*** permite que el sistema BIG-IP siempre devuelva el tráfico por la VLAN en la que lo recibió.
- ***Advanced > Fail-Safe****:* opción para alta disponibilidad que determina la acción a realizar en un cluster activo-pasivo cuando se deja de recibir tráfico en una VLAN. Además, el valor de *Fail-safe Timeout* debe ser como mínimo el valor por defecto y la acción seleccionada *Failover*. Para más información sobre alta disponibilidad, se debe consultar el apartado 6.11 ALTA DISPONIBILIDAD

Para más información y detalle en la gestión de VLANs, se debe acceder a la documentación detallada de F5**:** BIG-IP TMOS Routing Administration: VLANs VLAN Groups and VXLAN.[REF36]

6.5 GESTIÓN DE CERTIFICADOS

El producto requiere la instalación y configuración de certificados para TLS. Deberán utilizarse certificados de una Autoridad de Certificación de confianza, **evitando el uso de certificados autofirmados**.

El producto soporta la validación de certificados digitales X.509, usando listas de revocación de certificados (CRL). Los administradores crean perfiles SSL que son utilizados para definir los parámetros usados para comunicarse con entidades externas.

Entre estos parámetros se encuentran las posibilidades de requerir el uso de TLS, autenticación mutua y una definición del certificado a usar para la autenticación.

El detalle de configuración de los certificados del producto se debe consultar en la documentación oficial:

- Descripción general de certificado del dispositivo: K15664: Overview of BIG-IP Device Certificates. [REF15]
- Gestión de certificados SSL: sección *SSL Certificate Management* en BIG-IP System: SSL Administration [REF16]. El mismo documento contiene 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.
- Gestión de certificados a través de la GUI: K14620: Managing SSL certificates for BIG-IP systems using the Configuration utility. [REF17].

Los perfiles *Client SSL* o *Server SSL* determinan el tipo de comunicación TLS del BIG-IP con los clientes y los servidores respectivamente. Los artículos K14806: Overview of the Server SSL profile (11.x – 17.x) [REF18], K14783: Overview of the Client SSL profile (11.x – 17.x) [REF19] detallan las opciones de configuración de estos perfiles.

TLS se usa para crear una conexión con autenticación mutua con el servidor externo syslog de auditoría. El servidor externo de auditoría proporciona su certificado al producto durante el establecimiento de la conexión TLS para autenticarse.

Deberán seguirse los siguientes pasos generales:

1. Instalar el certificado de la CA raíz que firmará el certificado del producto, así como el certificado de la CA del servidor syslog externo.
2. Generar una CSR (Certificate Signing Request), para crear el certificado que usará el producto. Se deberá utilizar uno de los siguientes parámetros para la creación del certificado:
    - Tipo de clave **ECDSA**, con un tamaño de **256 o 384 bits.**
    - Tipo de clave **RSA**, con un tamaño de clave de **3072 bits o superior.**
    - Se puede consultar el detalle de configuración de estos cifrados en la documentación de F5: K01770517: Configuring the cipher strength for SSL profiles (14.x - 15.x) [REF43]
3. Importar el certificado una vez obtenido. Para más información, consultar la documentación: K14620: Managing SSL certificates for BIG-IP systems using the Configuration utility [REF17]

Para asegurarse de que la revocación de certificados intermedios cause un fallo en la conexión, **las CAs intermedias NO deben estar incluidas entre las Autoridades de Certificación de confianza** (*Trusted Certificate Authorities*). BIG-IP considera todos los certificados intermedios establecidos en las Autoridades de Certificación de confianza como fiables, y no están validados (son explícitamente considerados como fiables), por lo que no pueden ser revocados. Por lo tanto, al configurar un perfil SSL, siga las

instrucciones indicadas en K13302: Configuring the BIG-IP system to use an SSL chain certificate (11.x – 16.x) [REF25] para **definir solo la CA raíz como fiable**.

6.6 SERVIDORES DE AUTENTICACIÓN

Para una configuración segura del producto, los servidores externos de autenticación, como Kerberos, RADIUS y TACACS+ no deben ser configurados para la administración del sistema BIG-IP LTM. Por tanto, la autenticación remota debe estar deshabilitada, únicamente recurriendo a la autenticación local del producto.

6.7 SINCRONIZACIÓN HORARIA

Para el establecimiento de fechas y registros de tiempo, especialmente necesarios para los logs de auditoría, el producto incluye un reloj en su hardware y un reloj en tiempo real disponible en el sistema BIG-IP.

Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados para permitir una alta fiabilidad en los sistemas de auditoría y logging.

Se puede comprobar la hora configurada en el sistema a través de tmsh con el comando *date ; hwclock.*

Para establecer la fecha y hora del sistema BIG-IP, a través de tmsh puede introducirse el comando: *date MMDDHHmmYYYY.SS* (<month><day><hour><minute><year>.<second>).

También es posible modificarla posteriormente con el comando: *sys modify clock time YYYY-MM-DD:HH:MM:SS (year-month-day:hour:minute:second).*

No está soportado el uso de un servidor NTP para una configuración segura del producto.

Para más información, puede consultarse el artículo: K3381: Setting the time and date on the BIG-IP system [REF37].

6.8 ACTUALIZACIONES

El software de BIG-IP es actualizado periódicamente, y debe ser obtenido siempre desde la página oficial de F5 [REF4].

El proceso de actualización del sistema es similar al descrito en el apartado 5.2 INSTALACIÓN DEL SOFTWARE , con la salvedad de que el administrador no tiene la necesidad de verificar manualmente la imagen, ya que la activación del modo de operación seguro configura la verificación automática de la nueva ISO a la que se desea actualizar comprobando su firma digital. Si la verificación de firma falla, la actualización del software no se realizará.

Para más información detallada de las actualizaciones, procedimientos y tipos de actualización, se recomienda la lectura del siguiente artículo: K51113020: BIG-IP update and upgrade guide | Chapter 5: Update or upgrade a standalone BIG-IP system using the Configuration utility [REF21]

6.9 AUTO-CHEQUEOS

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

En paralelo a esta monitorización, BIG-IP puede analizar en un momento determinado el estado del hardware mediante el comando de tmsh *platform_check* utilizando permisos de *root*. Este chequeo deberá de ser solicitado por soporte de F5 en caso de sospecha de fallo en el hardware.

Además, mediante la herramienta qkview, BIG-IP también es capaz de incorporar toda la información relativa al dispositivo y su diagnóstico, así como este chequeo hardware. Para generar datos de diagnóstico con qkview seguir las instrucciones presentes en el artículo K12878: Generating diagnostic data using the qkview utility [REF32]

De forma automática, BIG-IP lleva a cabo una serie de auto-chequeos durante el arranque del sistema:

- El **mecanismo de auto-chequeos** en el inicio es un programa de diagnóstico que lleva a cabo chequeos sobre los componentes esenciales que garantizan que el hardware funcione. Este chequeo solo se lleva a cabo durante la fase de encendido del producto. En caso de producirse un fallo, este quedará reflejado en la consola. En caso de que los fallos persistan, se recomienda ponerse en contacto con el equipo de soporte de F5.
- La **utilidad sys-icheck** proporciona mecanismos de comprobación de integridad del software, comparando el estado actual de los ficheros del sistema con una base de datos creada en tiempo de instalación, y reportando cualquier discrepancia detectada. Este chequeo se ejecuta de forma automática cada vez que se arranca el sistema, cuando el modo de operación seguro está habilitado. Asimismo, este chequeo puede ejecutarse en cualquier momento bajo demanda desde el Shell tmsh. En caso de detectar modificaciones no esperadas en el sistema, se recomienda que el administrador reinstale el mismo. En caso de que la utilidad sys-icheck detecte un error durante el arranque, este se detendrá, recomendando en este caso que el administrador reinstale el sistema.
- Asimismo, durante la fase de arranque del sistema se llevan a cabo **tests sobre OpenSSL**, **algoritmos criptográficos** y **generación de números aleatorios**. En caso de que se produzca un fallo, estos tests se detendrán, y en este caso se recomendará que el administrado reinstale el sistema.

6.10 SNMP

La administración del producto mediante SNMP no está soportada, quedando esta deshabilitada en el momento de activación del modo de operación seguro. A la hora de configurar los servidores, los campos relativos a SNMP deben quedar en blanco.

6.11 ALTA DISPONIBILIDAD

Se puede utilizar un segundo equipo de redundancia para establecer una configuración **de alta disponibilidad Activo-Pasivo** (*High Availability > Active / Standby*). Este despliegue consiste en dos sistemas BIG-IP sincronizados con la misma configuración: el sistema principal está activo y se encarga de todo el procesamiento del tráfico, mientras que el otro se encuentra inactivo en estado de espera, en caso de que el sistema principal quede inoperativo.

Toda la configuración de alta disponibilidad deberá realizarse **antes de activar el modo de operación seguro** para que la conexión de alta disponibilidad funcione correctamente.

Es necesario habilitar *Connection Mirroring* en el dispositivo, será necesario realizar los siguientes pasos:

ANEXO A. Acceder a través de la GUI Configuration Utility al apartado Device Management > Devices

ANEXO B. Seleccionar la opción correspondiente al dispositivo local. El dispositivo local se identificará porque al final del nombre de dispositivo aparece (Self).

ANEXO C. Seleccionar la pestaña Mirroring.

ANEXO D. En el apartado Primary Local Mirror Address, seleccionar la dirección IP y VLAN que será usada como primera opción en la comunicación de mirroring entre los equipos.

ANEXO E. En el apartado Secondary Local Mirror Address, seleccionar la dirección IP y VLAN que será usada como opción secundaria en la comunicación de mirroring entre los equipos.

La configuración por defecto incluye la seguridad en la comunicación de la sincronización entre dispositivos. Durante el proceso de configuración descrito en este documento se sincronizarán los sistemas de forma automática.

Para asegurar que la sincronización sigue activa tras ejecutar el modo de operación seguro, debe ejecutarse el siguiente comando en tmsh:

```
tmsh modify net self-allow defaults add {tcp:443 tcp:4353}
```

Para las IPs configuradas para la VLAN donde se produce el *mirroring*, debe ejecutarse:

```
tmsh modify net self <name> allow-service default
```

Una vez que la sincronización se realice con éxito, será necesario reiniciar ambos sistemas.

Para mayor detalle en las configuraciones de alta disponibilidad, ir a *Creating an Active-Standby Configuration Using the Setup Utility* en BIG-IP Device Service Clustering: Administration [REF22].

6.12 AUDITORÍA

6.12.1 REGISTRO DE EVENTOS

Para un entorno seguro del sistema BIG-IP es necesario auditar los eventos y almacenarlos en un archivo de auditoría local. Los eventos registrados se pueden enviar de manera simultánea a un servidor de syslog externo.

Un conjunto de opciones de registro de logs deben estar habilitadas para asegurar que el producto genere los eventos requeridos. Desde *System > Logs > Configuration > Options* se recomienda seleccionar la habilitación de, al menos, los siguientes eventos para *Local Traffic Logging* y *Audit Logging*:

- **Local Traffic Logging: MCP > Notice:** nivel de logs relacionados con el MCP (Master Control Program).
- **Local Traffic Logging: Traffic Management OS > Notice:** nivel de logs relacionados con el TMOS.
- **Audit Logging: MCP > Enable:** establece el registro de logs para cambios en la configuración del MCP por parte del usuario.
- **Audit Logging: tmsh > Enable:** establece el registro de logs para cambios en la configuración del sistema por parte del usuario utilizando tmsh.

Para más información y detalle sobre configuración de logs, se puede consultar la documentación oficial de F5: K5532: Configuring the level of information logged for Traffic Management-related events [REF38]

Si la funcionalidad de filtrado de paquetes está habilitada, la función de registro (logging) debe ser habilitada para cada regla, tal y como se indica en el apartado 6.14.1 FUNCIONES BIG-IP LTM sobre la funcionalidad de filtrado de paquetes. Para más detalles sobre el proceso de configuración de la funcionalidad, ir a tmsh Reference Guide [REF7] y BIG-IP TMOS: Routing Administration [REF14].

Si está habilitada la funcionalidad de cortafuegos, se deben configurar perfiles de logging (*logging profiles*) para registrar los eventos del cortafuegos. Consultar el apartado 6.14.2 FUNCIONES MÓDULO AFM para la creación de perfiles de logging.

A continuación, se muestra un ejemplo del formato y aspecto que se puede mostrar en los registros:

Jul 29 15:56:22 BIGIP138 notice mcpd[6112]: 01070417:5: AUDIT - user admin - transaction #2372153-3 - object 0 - create_if { ltcfg_instance_field { ltcfg_instance_field_instance_name "/Common/cli" ltcfg_instance_field_field_name "audit" ltcfg_instance_field_class_name "cli" ltcfg_instance_field_container ""

Se puede consultar más información sobre el formato de los registros en el artículo oficial de F5: K16197: Reviewing BIG-IP log files [REF44]

Se requiere asegurar el almacenamiento remoto seguro de los eventos de auditoría, así como el almacenamiento local de los mismos a modo de copia de seguridad. El *framework* de registro de eventos envía de forma simultánea los eventos a su localización tanto local como remota. Para más información al respecto ir a *Configuring Remote High-Speed Logging* en External Monitoring of BIG-IP Systems: Implementations [REF23].

En caso de que la conexión entre el Sistema BIG-IP y el servidor syslog falle, el sistema intentará llevar a cabo la reconexión un número ilimitado de intentos hasta que la conexión sea reestablecida. Durante ese periodo de tiempo, los logs serán almacenados localmente.

6.12.2 ALMACENAMIENTO LOCAL

BIG-IP almacena localmente los mensajes producidos por eventos de tráfico generados por la monitorización. Estos mensajes son guardados en el directorio ***/var/log***, almacenados de forma independiente y por tipo de evento.

El almacenamiento local de logs en BIG-IP utiliza el script de rotación de logs "logrotate" para eliminar los mensajes más antiguos. Un mensaje de aviso es enviado cuando se supera el 90% del almacenamiento local de logs. Este mensaje de advertencia queda registrado en los archivos de log. En caso de ocuparse completamente la partición de logs, el sistema será incapaz de registrar localmente nuevos mensajes. Para más detalle acerca de cómo gestionar los ficheros de log en el sistema BIGIP consultar el artículo K13367: Managing log files on the BIG-IP system (11.x - 16.x) [REF33]

Por defecto, BIG-IP protege el almacenamiento local de logs de modificaciones y eliminaciones no autorizadas sin necesidad de configuraciones adicionales.

6.12.3 ALMACENAMIENTO REMOTO

De forma complementaria al almacenamiento local, se debe configurar un servidor syslog remoto que almacene una copia de los logs.

Para implementar una configuración segura de almacenamiento remoto syslog de eventos, es necesario configurar en servidor remoto una comunicación TLS. En el siguiente gráfico se muestra a nivel esquemático la configuración de referencia:

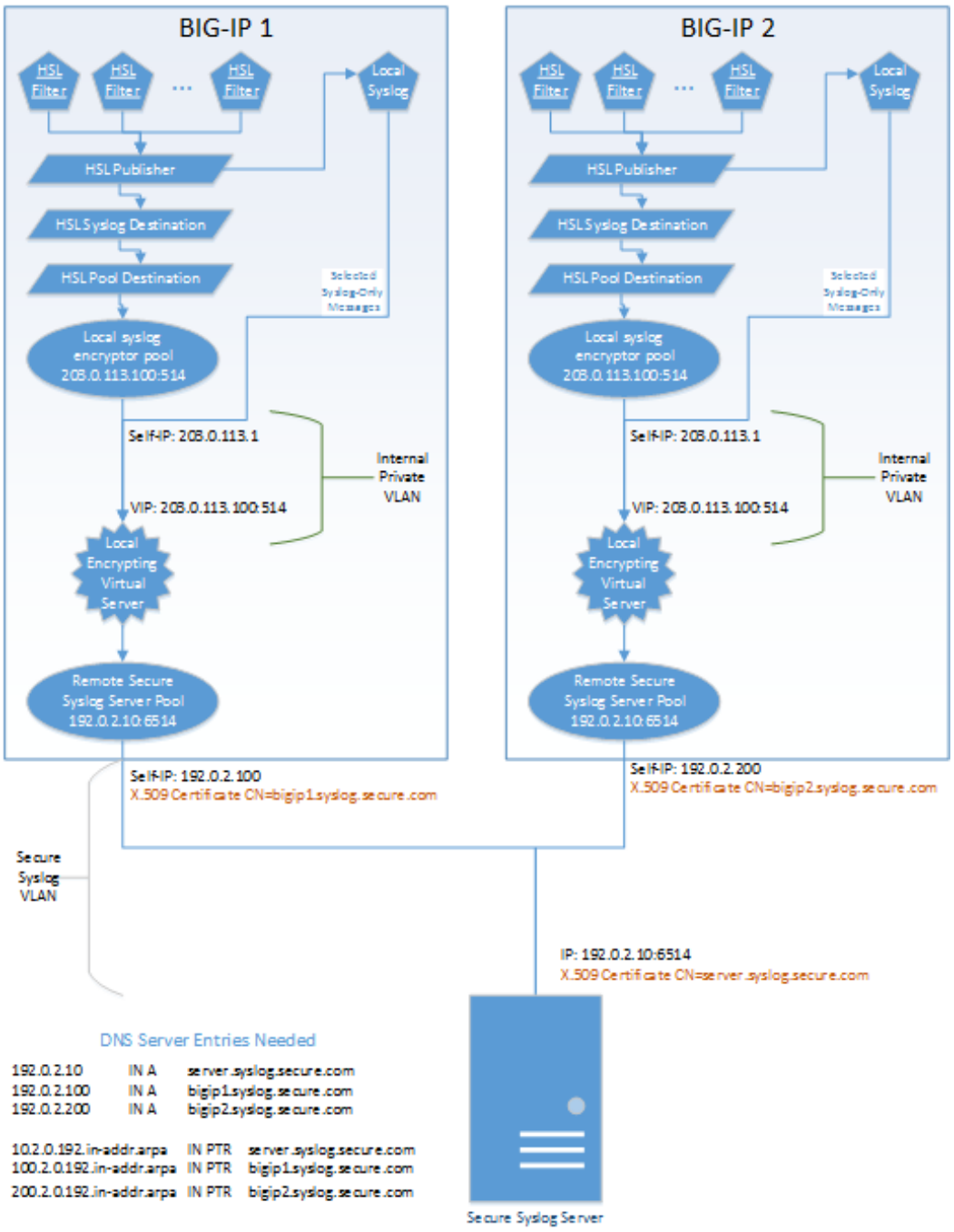


Figura 8. Arquitectura de sistema BIG-IP con servidor Syslog.

A continuación, se ilustra, como referencia, un ejemplo de entorno de alta disponibilidad con un sistema BIG-IP de redundancia y un servidor syslog.

En la configuración de ejemplo se asume la siguiente configuración previa:

a) Un grupo de dispositivos en un sistema de alta disponibilidad con sincronización automática. Consultar el apartado 6.11 ALTA DISPONIBILIDAD para dicha configuración. Es posible replicar el ejemplo también en caso de no utilizar alta disponibilidad.

b) Cada dispositivo tiene un FQDN independiente.

c) Configuración de un servidor DNS.

Uno de los requisitos para la configuración es la validación mutua del certificado X.509 para cada dispositivo, tanto ambos BIG-IP, como el servidor de logging. Cada dispositivo debe tener un certificado asignado con el nombre de certificado a su FQDN. Si hubiese una autoridad certificadora (CA) deberá ser incluida, así como su cadena de certificados al que se hace referencia en el perfil SSL.

Para esta configuración es necesario realizar los siguientes pasos en BIG-IP:

1. En la ventana principal, ir a *System > Device Certificates.*
2. Acceder a *Import.*
3. Desde la lista *Import Type,* seleccionar *Certificate and Key.*
4. Para la configuración de *Certificate Source*, seleccione *Upload File* y seleccione dentro del dispositivo cliente el archivo firmado por el servidor de autoridad certificadora (CA).
5. Para la configuración de Key Source, seleccionar *Upload File* y seleccionar del dispositivo cliente el archivo de clave.
6. Hacer click en *Import*.

Para crear a un grupo de servidores de logging, es necesario crear un pool donde se contenga el o los servidores de logging. El ejemplo siguiente es configurado mediante tmsh:

```
create ltm pool <pool_remote_secure_syslog_name> {
  members replace-all-with {192.0.2.10:6514 {address 192.0.2.10} }
  monitor tcp_half_open
}
```

- Donde 192.0.2.10 representa la dirección del servidor Syslog remoto.
- Guardar la configuracion mediante *save /sys config*

En este punto es necesario crear un perfil SSL el cual se encargará de cifrar el tráfico con destino al servidor de logging. Para este caso, deberán indicarse los siguientes comandos de tmsh:

```
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
}
```

- Donde en este ejemplo: *profile_serverssl_syslog-1* es el nombre del perfil personalizado de SSL para este servicio, *F5secureLoggingCA_bundle.crt* es el certificado de la CA utilizada, *b3-1.logging.f5cc.com.crt* es el certificado del servidor de logging y *key b3-1.logging.f5cc.com.key*, que es la clave.

Para una configuración segura de almacenamiento remoto de logs se recomienda **crear una VLAN dedicada y red específica** para la comunicación entre el servidor de logging y BIG-IP. Acudir al apartado 6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS para más información sobre este procedimiento.

El siguiente paso debería ser crear un virtual server en la red creada previamente. Un virtual server es un objeto de gestión de tráfico representado por una dirección IP y un servicio. Los clientes se conectan a este servicio el cual el BIG-IP dirigirá al destino, típicamente servidores.

```
create ltm virtual-address 203.0.113.100
  traffic-group traffic-group-local-only
  auto-delete false
```

- En el ejemplo 203.0.113.100 representa la dirección IP del servicio.
- Donde en el ejemplo *vs_secure_syslog_target-1* representa el nombre del servicio. La dirección IP creada previamente es asociada al servicio virtual, asi como el *pool* y el perfil SSL. Se utiliza en este ejemplo la vlan *vlan_securelog* como red de comunicación entre BIG-IP y servidor de logging.

```
create ltm virtual vs_secure_syslog_target-1 {
  destination 203.0.113.100:514
  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
```

Estos pasos deberían de repetirse en el otro BIG-IP que conforma la configuración de alta disponibilidad con este.

Para más información sobre todos los detalles de esta configuración, se aconseja seguir la guía de la documentación de la siguiente referencia: Setting Up Secure Remote Logging [REF24]

6.13 BACKUP

BIG-IP es capaz de hacer una copia de seguridad y restauración basado un archivo llamado UCS (*User Configuration Set*). Este archivo por defecto incluye todos los elementos necesarios para restaurar la configuración a un dispositivo nuevo, incluyendo:

- Archivos de configuración del sistema BIG-IP.
- Licencias del producto.
- Información de usuarios y credenciales.
- Información de DNS.
- Certificados y claves SSL.

Los archivos de configuración son guardados por defecto en el directorio */var/local/ucs* y por defecto la extensión es *.ucs.

Para evitar errores de compatibilidad se recomienda emplear la misma versión de software en el sistema BIG-IP de destino que la empleada en el sistema BIG-IP del que se hizo la copia de seguridad.

Se debe mantener un almacenamiento seguro del archivo UCS, el cual contiene información asociada a cuentas de usuario, contraseñas, ficheros críticos del sistema, y claves privadas SSL. Para más información respecto a las copias de seguridad, se recomienda consultar los artículos:

- K175: Transferring files to or from an f5 system [REF25]
- K13132: Backing up and restoring BIG-IP configuration files with a UCS archive [REF42]
- K4423: Overview of UCS archives [REF43]

6.14 FUNCIONES DE SEGURIDAD

6.14.1 FUNCIONES BIG-IP LTM

El producto dispone de funciones básicas de filtrado de paquetes, configurando sus interfaces indicando la aceptación o rechazo de paquetes entrantes en base a una serie de criterios definibles.

Para habilitar el filtrado de paquetes, se ha de activar con la opción *Enable* en *Packet Filtering* en la configuración *Networks > Packet Filters.*

Para crear reglas de filtrado, es posible configurarlas siguiendo los siguientes pasos:

1. Desde *Network > Packet Filters*, acceder a *Rules > Create*
2. Se mostrarán distintas opciones de configuración como el *Rate Class*, el cual permite establecer clases con distintas políticas para limitar la cadencia de paquetes o su flujo de entrada. También se puede controlar el ancho de banda con la opción *Bandwidth Controller* o indicar una VLAN con la opción *VLAN/Tunnel.*

3. La opción Logging debe activarse estableciendo la configuración Enabled.
4. Seleccionar en *Filter Expression Method* la opción *Enter Expression.*
5. En el campo *Filter Expression* se debe introducir una expresión utilizando la sintaxis de tcpdump para establecer una regla. Por ejemplo, para excluir paquetes con destino a puertos sensibles:

   not dst port 80 and not dst port 443 and not dst port 53 and not dst port 22 and not dst port 20 and not dst port 21 and not dst host <internal_self_IP_address>

6. Una vez están habilitadas las reglas, se puede establecer qué hacer con los paquetes que no las cumplen con las reglas seleccionando las opciones *Accept, Discard o Reject* en la opción *Unhandled Packet Action.* Se recomienda *a*segurar que las reglas establecidas cumplen con los criterios deseados de forma que no provoquen descartes erróneos en el tráfico de entrada.

Para más información sobre las reglas de filtrado de paquetes y detalles de su configuración, consultar el apartado *Packet Filters* del manual BIG-IP TMOS: Routing Administration [REF14] y el apartado *Configuring Packet Filtering* del manual BIG-IP LTM BIG-IP TMOS: Implementations [REF40]

6.14.2 FUNCIONES MÓDULO AFM

La función de seguridad principal del módulo AFM consiste en un cortafuegos para tráfico de capas 3 y 4:

Los administradores pueden definir reglas de filtrado basadas en los atributos de los paquetes de red, como direcciones IP de origen y destino, puertos, números de secuencia, códigos, etc. BIG-IP solo permitirá a los diferentes paquetes de red llegar a su destino si hay reglas de cortafuegos que así lo permitan y no cuenten con ciertas características propias de tráfico considerado comúnmente como malicioso.

BIG-IP tiene en cuenta el estado de diferentes protocolos basados en estado a la hora de aplicar las diferentes reglas del cortafuegos. Por ejemplo, el tráfico TCP solo será permitido si la sesión TCP correspondiente ha sido debidamente establecida con anterioridad, y los paquetes iniciales cumplen con las reglas del cortafuegos establecidas.

Se pueden crear reglas de firewall para los siguientes protocolos:

- ICMPv4
- ICMPv6
- IPv4
- IPv6
- TCP

- UDP

El cortafuegos de BIG-IP está configurado de forma predeterminada en modo ADC, lo que significa que acepta el tráfico por defecto y cualquier tráfico a bloquear debe de ser especificado. Para establecer una configuración segura del producto, se debe configurar el módulo AFM del BIG-IP en modo cortafuegos, también llamado *default deny policy*, en lugar de este modo ADC. Para establecer dicho modo se debe acceder desde la GUI web a la siguiente configuración:

1. Ir a *Security > Options > Network Firewall*. Se abrirá una ventana con las opciones del firewall.
2. En *Virtual Server & Self IP Contexts list*, seleccionar la acción por defecto para la *self IP* y *virtual server*.
3. Seleccionar *Drop y Reject* según sea requerido para descartar o rechazar el tráfico que no ha sido especificado como permitido (tráfico por defecto).

Este modo cortafuegos establece una política de denegación del tráfico por defecto. Para más información, consulte Implementación de AFM en modo de cortafuegos (*Firewall Mode*) en el apartado *Deploying AFM in Firewall Mode* de la documentación: BIG-IP AFM: Network Firewall Policies and Implementations [REF27] para el detalle de configuración del modo de cortafuegos.

A continuación, se indica una serie de funcionalidades de seguridad destacadas del módulo AFM. Todos los apartados mencionados a continuación corresponden a [REF27]. Las funcionalidades son:

a) **Reglas de filtrado de tráfico:** como ya se ha mencionado en este apartado, se pueden configurar reglas y listas de reglas de filtrado de tráfico. Estas controlan el acceso a la red y el centro de datos en base a los criterios determinados. Se pueden consultar los procedimientos de creación de reglas en los apartados *Policies and Rules* y *Applying AFM Network Firewall Policies*.

b) ***IP Address Intelligence:*** el módulo AFM permite configurar políticas de validación de tráfico en función de una base de datos de direcciones IP. El tráfico acorde a estas políticas se gestionará automáticamente en base a las direcciones IP consideradas como maliciosas o de dudosa procedencia incluidas en la base de datos. Se puede consultar como descargar y configurar la base de datos en el apartado *Configuring AFM IP Address Intelligence.*

c) ***Firewall NAT:*** soporta funcionalidades avanzadas de NAT, permitiendo el encaminamiento de direcciones de tráfico de redes externas a internas. Las políticas NAT permiten configurar una serie de reglas para conexiones internas privadas, regulando el paso de tráfico de una red a otra. Para más información sobre cómo configurar dichas funcionalidades se debe consultar el apartado *Using Firewall NAT for IP and Port Translation.*

d) **Inspección de protocolos:** se pueden configurar perfiles para inspeccionar los protocolos del tráfico. Estos perfiles se configuran para recopilar reglas para la inspección de protocolos, basadas en *Snort.* Para configurar la inspección de

anomalías en protocolos y los perfiles de inspección, consultar el apartado *Inspecting Protocol Anomalies.*

e) ***SSH Proxy:*** permite a los administradores gestionar los distintos usos de SSH, determinando quién puede hacer qué según el servidor. El Proxy SSH proporciona políticas de control del canal SSH y previene ataques avanzados.

   El proxy SSH soporta autenticación mediante clave pública y contraseña. A la hora de generar las claves, es necesario seguir los pasos del punto *Defining SSH proxy password or keyboard interactive authentication* y *Defining SSH proxy public key authentication* dentro del apartado *SSH Proxy Security* y asegurarse de que se establece un **tamaño de clave RSA de 3072 bits.** Consultar el apartado completo para más información de cómo configurar la funcionalidad y sus perfiles.

f) **Bastionado HTTP:** se pueden establecer y ajustar políticas especiales para la gestión y filtrado del tráfico HTTP, permitiendo comprobar la validez del protocolo, detectar técnicas de evasión, comprobación de longitud y cabeceras HTTP, etc. También se puede especificar como el sistema responde a los distintos incumplimientos de dichas reglas. Para su configuración, se debe consultar el apartado *HTTP Protocol Security.*

g) **Prevención de ataques (Políticas de desalojo y límites de conexión):** se pueden establecer políticas de desalojo (*eviction policies*) que previenen de los ataques de tablas de flujo (uso de flujos de tráfico lentos para consumir recursos del sistema), determinando también como responde el sistema a dichos ataques.

   Se pueden establecer también límites de conexión a un servidor, ruta o dominio, de forma que superado dicho límite no se acepten más conexiones, previniendo de esta forma ataques al sistema. Consultar el apartado *Preventing Attacks with Eviction Policies and Connection Limits* para más información y cómo configurar las políticas.

h) **Políticas de servicio (temporizadores y políticas de uso de puertos):** el sistema permite establecer políticas de servicio, las cuales incluyen temporizadores y políticas de uso de puertos para que BIG-IP pueda gestionar conexiones inactivas o indebidas (por ejemplo, protocolo usando un puerto incorrecto) en función de unas determinadas reglas asignadas a puertos. Por ejemplo, establecer un timeout de una conexión TCP al puerto 443 inactiva o rechazar conexiones TCP al puerto 80. Consultar el apartado *Setting Timers and Preventing Port Misuse with Service Policies* para más información y la configuración detallada.

i) **Probador de paquetes (*Packet Tester*)**: el módulo AFM incluye una herramienta de pruebas (*troubleshooting)* que permite al usuario introducir determinados paquetes en el tráfico del sistema y comprobar cómo se comporta el cortafuegos y sus distintas reglas de control y prevención de ataques. De esta forma se puede comprobar la correcta configuración del AFM. Para más información sobre esta funcionalidad, consultar el apartado *Testing Packets with Firewall, IP Intelligence, and DoS Rules.*

Para asegurar que todos los paquetes denegados también queden registrados en el registro de auditoría, debe hacerse a través de un **perfil de logging** *(logging profile*) accediendo a *Security > Event Logs > Logging Profiles* y crear un perfil marcando las *Log Rule Matches* necesarias para el registro de eventos, siguiendo las instrucciones de la sección *Creating a local Logging profile* del capítulo *Local Logging with the AFM Network Firewall* del manual BIG-IP AFM: Network Firewall Policies and Implementations [REF27], así como la sección *Creating a custom Network Firewall Logging profile* del capítulo *Remote High-Speed Logging with the Network Firewall* en el mismo manual [REF27]. En ambos casos, cuando configure la opción *Log Rule Matches*, usar la opción **DROP**.

Los registros de eventos de estas reglas son controlados por los perfiles de logging, que pueden ser personalizados por el cliente. Estos perfiles tienen la misión de seleccionar los elementos que tienen que ser agregados al registro de eventos, y donde tienen que ser enviados. Para más información acerca del proceso de configuración de perfiles, consultar *Creating a local logging profile* de [REF27].

7. FASE DE OPERACIÓN

En la operación habitual de BIG-IP incluye tareas de configuración ya descritas en los puntos anteriores, aunque también son necesarias una serie de tareas de mantenimiento:

- Comprobaciones periódicas del hardware y software para asegurar que no se ha introducido hardware o software no autorizado. El firmware activo y su integridad, deberán verificarse periódicamente para comprobar que está libre de software malicioso.
- Se recomienda el uso de la funcionalidad iHealth de BIG-IP para garantizar el correcto funcionamiento del hardware y software del producto. Para más información consultar: K44841551: BIG-IP TMOS operations guide | Chapter 3: F5 iHealth [REF39]
- Comprobaciones periódicas de la correcta operación de los algoritmos y funciones criptográficas, a través de la ejecución de los correspondientes auto-chequeos.
- Los administradores deben estar correctamente entrenados en el uso y la correcta operación del producto, así como en las características del entorno seguro en que está presente. Al mismo tiempo, los administradores seguirán las guías e indicaciones presentes.
- Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.
- Actualizaciones periódicas del software de los equipos, para garantizar que están al día, tanto en las capacidades de protección, como en funcionalidades avanzadas.
- Realización de *backups* automáticos de forma periódica y, a poder ser, de forma centralizada.
- Mantenimiento de los registros de auditoría. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el administrador principal podrá acceder a ellos. La información de auditoria se guardará en las condiciones y por el periodo establecido en la normativa de seguridad. La revisión de logs de auditoria debe realizarse periódicamente.
- La revisión de logs de auditoria debe de hacerse al menos una vez a la semana.
- Todas las interfaces administrativas están diseñadas para ser usadas con la finalidad de la configuración de BIG-IP, no para otros propósitos. En particular, no se debe de usar para acceder a páginas web externas más allá de las que específicamente estén permitidas por la documentación de F5.
- Se recomienda la inscripción en las lista de correos de seguridad de F5 para recibir notificaciones y actualizaciones sobre las últimas vulnerabilidades: https://interact.f5.com/Customer-Preference-Center.html [REF25]

Para más información acerca de algún proceso de operación, se recomienda consultar el artículo BIG-IP TMOS operations guide | Chapter 1: Guide introduction and contents [REF29]

8. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto hardware y actualización del firmware	☐	☐	Revisión de etiquetas y números de serie. Verificación de la versión software.
Instalación en un entorno seguro	☐	☐	
Registro de las licencias	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Activación de Modo de operación seguro	☐	☐	Configuración con ccmode
ADMINISTRACIÓN			
Configuración de protocolos y cifrados seguros	☐	☐	
Configuración de política de contraseñas	☐	☐	
Configuración de usuarios administradores	☐	☐	
Configuración de interfaces de red	☐	☐	
Configuración de certificados	☐	☐	
Sincronización horaria	☐	☐	
Configuración de alta disponibilidad	☐	☐	Configuración opcional
AUDITORÍA			
Configuración del registro de logs	☐	☐	
Configuración de envío a servidor remoto	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
COPIAS DE SEGURIDAD			
Creación de archivos de backup (UCS)	☐	☐	

9. REFERENCIAS

REF1 *Knowledge Center* del sitio web oficial de F5
https://support.f5.com/csp/home

REF2 Sitio web oficial de descarga de F5
https://downloads.f5.com

REF3 Verifying BIG-IP software images using SIG and PEM files
https://support.f5.com/csp/article/K24341140

REF4 K7752: Licensing the BIG-IP system
https://support.f5.com/csp/article/K7752

REF5 K13123: Managing BIG-IP product hotfixes (11.x - 17.x)
https://support.f5.com/csp/article/K13123

REF6 K80425458: Modifying the list of ciphers and MAC and key exchange algorithms used by the SSH service on the BIG-IP or BIG-IQ systems
https://support.f5.com/csp/article/K80425458

REF7 F5 TMSH Reference - 14.x
https://clouddocs.f5.com/cli/tmsh-reference/v14/_downloads/7c8d38e557b65b7b0f857f79cfb6441b/tmsh_14.0.0.pdf

REF8 K13454: Configuring SSH public key authentication on BIG-IP systems (11.x – 16.x)
https://support.f5.com/csp/article/K13454

REF9 K42531434: Replacing the Configuration utility's self-signed SSL certificate with a CA-signed SSL certificate
https://support.f5.com/csp/article/K42531434

REF10 BIG-IP Local Traffic Management: Basics
https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/big-ip-local-traffic-management-basics-14-0-0.html

REF11 Guía de usuarios de iControl
https://cdn.f5.com/websites/devcentral.f5.com/downloads/icontrol-rest-api-user-guide-14-1-0.pdf

REF12 BIG-IP System: User Account Administration
https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-user-account-administration-13-0-0.html

REF13 K6068: Configuring a pre-login or post-login message banner for the BIG-IP or Enterprise Manager system.
https://support.f5.com/csp/article/K6068

REF14 BIG-IP TMOS: Routing Administration
https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-routing-administration-11-6-0.html

REF15 K15664: Overview of BIG-IP Device Certificates.
https://support.f5.com/csp/article/K15664

REF16 BIG-IP System: SSL Administration
https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ssl-administration-13-0-0.html

REF17 K14620: Managing SSL certificates for BIG-IP systems using the Configuration utility
https://support.f5.com/csp/article/K14620

REF18 K14806: Overview of the Server SSL profile (11.x – 17.x)
https://support.f5.com/csp/article/K14806

REF19 K14783: Overview of the Client SSL profile (11.x – 17.x)
https://support.f5.com/csp/article/K14783

REF20 K13302: Configuring the BIG-IP system to use an SSL chain certificate (11.x – 17.x)
https://support.f5.com/csp/article/K13302

REF21 K51113020: BIG-IP update and upgrade guide | Chapter 5: Update or upgrade a standalone BIG-IP system using the Configuration utility
https://support.f5.com/csp/article/K51113020

REF22 BIG-IP Device Service Clustering: Administration
https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-system-device-service-clustering-administration-13-0-0.html

REF23 External Monitoring of BIG-IP Systems: Implementations
https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-12-0-0.html

REF24 Setting Up Secure Remote Logging
https://techdocs.f5.com/en-us/bigip-14-0-0/external-monitoring-of-big-ip-systems-implementations-14-0-0/setting-up-secure-remote-logging.html

REF25 F5 Customer Preference Center
https://interact.f5.com/Customer-Preference-Center.html

REF26 K175: Transferring files to or from an F5 system
https://support.f5.com/csp/article/K175

REF27 BIG-IP AFM: Network Firewall Policies and Implementations
https://techdocs.f5.com/kb/en-us/products/big-ip-afm/manuals/product/big-ip-network-firewall-policies-and-implementations-14-1-0.html

REF28 BIG-IP Local Traffic Management: Profiles Reference
https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/big-ip-local-traffic-management-profiles-reference-14-0-0.html

REF29 K05939436: BIG-IP TMOS operations guide | Chapter 1: Guide introduction and contents
https://support.f5.com/csp/article/K05939436

REF30 BIG-IP System: SSL Administration: Device Certificate Management
https://techdocs.f5.com/en-us/bigip-14-0-0/big-ip-system-ssl-administration-14-0-0/device-certificate-management.html

REF31 K26031800: Increasing SSH keys from 1024-bit to 2048-bit keys
https://support.f5.com/csp/article/K26031800

REF32 K12878: Generating diagnostic data using the qkview utility
https://support.f5.com/csp/article/K12878

REF33 K13367: Managing log files on the BIG-IP system (11.x - 17.x)
https://support.f5.com/csp/article/K13367

REF34 Use TLS 1.2 only on BIG-IP GUI
https://support.f5.com/csp/article/K40232071

REF35 K13121: Changing system maintenance account passwords
https://support.f5.com/csp/article/K13121

REF36 VLANs VLAN Groups and VXLAN
https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-routing-administration-11-6-0/4.html

REF37 Setting the time and date on the BIG-IP system
https://support.f5.com/csp/article/K3381

REF38 K5532: Configuring the level of information logged for Traffic Management-related events
https://support.f5.com/csp/article/K5532

REF39 K44841551: BIG-IP TMOS operations guide | Chapter 3: F5 iHealth
https://support.f5.com/csp/article/K44841551

REF40 BIG-IP TMOS: Implementations
https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-13-0-0.html

REF41 K01770517: Configuring the cipher strength for SSL profiles (14.x - 16.x)
https://support.f5.com/csp/article/K01770517

REF42 K13132: Backing up and restoring BIG-IP configuration files with a UCS archive
https://support.f5.com/csp/article/K13132

REF43 K4423: Overview of UCS archives
https://support.f5.com/csp/article/K4423
REF44 K16197: Reviewing BIG-IP log files
https://support.f5.com/csp/article/K16197

10.ABREVIATURAS

AAA	Authentication, Authorization and Accounting
ADC	Application Delivery Controller
AFM	Advanced Firewall Manager.
API	Application Programming Interface.
DNS	Domain Name System
GUI	Graphical User Interface.
HTTP	Hypertext Transfer Protocol.
IAM	Identity and Access Management
ICAP	Internet Content Adaptation Protocol.
Imi	Integrated Management Interface
LTM	Local Traffic Manager.
REST	Representational State Transfer.
SSL	Secure Sockets Layer.
SSO	Single-Sign-On
TLS	Transport Layer Security
TMM	Traffic Management Microkernel
TMOS	Traffic Management Operating System
TMSH	Traffic Management Shell.
TSIG	Transaction Signature
UCS	User Configuration Set.
vCMP	Virtual Clustered Multiprocessing

ANEXO A. COMANDOS NO PERMITIDOS (TMSH)

- *global publish*
- *analytics application-security commands*
- *analytics protocol-security report*
- *analytics sip-dos report*
- *auth radius*
- *auth radius-server*
- *auth tacacs*
- *gtm commands*
- *gtm global-settings commands*
- *gtm monitor commands*
- *ltm auth crldp-server*
- *lmt auth kerberos-delegation*
- *ltm auth ocsp-responder*
- *ltm-auth radius*
- *ltm auth radius-server*
- *ltm auth ssl-crldp*
- *ltm auth tacacs*
- *ltm classification commands*
- *ltm monitor diameter*
- *ltm monitor radius*
- *ltm monitor radius-accounting*
- *ltm monitor sip*
- *ltm persistence dest-addr*
- *ltm persistence global-settings*
- *ltm persistence hash*
- *ltm persistence msrdp*
- *ltm persistence persist-records*
- *ltm persistence sip*
- *ltm persistence ssl*
- *ltm persistence universal*
- *ltm profile analytics*
- *ltm profile diameter*
- *ltm profile ntlm*
- *ltm profile radius*
- *ltm profile rtsp*
- *ltm profile sctp*
- *ltm profile sip*
- *ltm profile stream*
- *ltm profile web-acceleration*
- *ltm profile web-security*
- *net fdb commands*

- *net ipsec commands*
- *pem commands*
- *pem profile commands*
- *pem reporting commands*
- *sys geoip*
- *sys smtp-server*
- *sys snmp*
- *sys application commands*
- *sys crypto crl*
- *sys file ssl-crl*
- *sys log-config dest arcsight*
- *sys log-config dest local-database*
- *sys log-config splunk*
- *sys sflow commands*
- *sys sflow data-source commands*
- *sys sflow global-settings commands*
- *util commands*
- *wam commnds*
- *wam global-settings commands*
- *wam resource commands*
- *wom commands*
- *wom profile commands*
- *asm commands*

ANEXO B. APIS DE ICONTROL NO PERMITIDAS

No se consideran los siguientes módulos iControl para la configuración segura del producto:

- ARX
- ASM
- PEM
- WebAccelerator

Las siguientes interfaces de módulos no están incluidas en la configuración segura:

- GlobalLB Application
- GlobalLB PoolMember
- GlobalLB VirtualServer
- LocalLB NAT
- LocalLBNodeAddress
- LocalLB ProfileDiameter
- LocalLB ProfileDiameterEndpoint
- LocalLB ProfileRADIUS
- LocalLB ProfileRTSP
- LocalLB ProfileSCTP
- LocalLB ProfileSIP
- LocalLB ProfileStream
- LocalLB VirtualAddress
- Log DestinationArcSight
- Log DestinationSplunk
- Management CRLDPConfiguration
- Management CRLDPServer
- Management OCSPConfiguration
- Management OCSPResponder
- Management RADIUSConfiguration
- Management RADIUSServer
- Management SMTPConfiguration
- Management SNMPConfiguration
- Management TACACSConfiguration
- Networking IPsecIkeDaemon
- Networking IPsecIkePeer
- Networking IPsecManualSecurityAssociation
- Networking IPsecPolicy
- Networking IPsecTrafficSelector
- Networking RouteDomain
- Networking RouteTable
- Networking STPInstance
- Networking SelfIP

- Networking SelfIPPortLockdown
- Networking Tunnel
- Networking VLAN
- Networking VLANGroup
- Networking iSessionAdvertisedRoute
- Networking iSessionRemoteInterface
- System GeoIP
- System PerformanceSFlow

PUBLICACIONES DE DEFENSA

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