centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1625

Procedimiento de empleo seguro
Cisco Web Security Appliance

Octubre 2023

MINISTERIO DE DEFENSA

cpage.mpr.gob.es

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

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2023

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.01.30 10:06:18 +01'00'

NIPO: 083-24-028-9.

Fecha de Edición: octubre de 2023.

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

ÍNDICE

1. INTRODUCCIÓN

1. El objetivo de este documento es proporcionar las directrices de seguridad que deben ser tenidas en cuenta para la configuración de los equipos *de Cisco Web Security Appliance*, con sistema operativo AsyncOS versión 11.X.
2. Esta guía incluye el detalle asociado a la configuración de seguridad cuando es necesario y referencias a la documentación de Cisco.
3. **Los siguientes modelos han sido cualificados e incluidos en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) del Centro Criptológico Nacional en la familia "*Herramientas de filtrado de navegación*":**
    - S695
    - S695F
    - S395
    - S195
    - S690
    - S690X
    - S680
    - S390
    - S380
    - S190

    NOTA:

    Se debe consultar el CPSTIC para conocer la versión del *firmware* actualmente cualificado.

4. La estructura del documento y sus contenidos no exigen una lectura lineal del mismo. Se recomienda al lector utilizar el índice de contenidos para localizar el capítulo que trate el aspecto concreto sobre el que se desee obtener información.

2. OBJETO Y ALCANCE

5. El objeto de la presente guía es detallar la configuración del producto para utilizarlo de forma segura. De esta forma, es posible establecer un marco de referencia que contemple las recomendaciones STIC en el despliegue y utilización de estos productos.
6. Este documento, salvo menciones especiales, no aporta ajustes de configuración para la operación del producto, fuera de las directamente relacionadas con su operación en modo seguro. Aspectos como las políticas de flujo de información y el control de acceso, deben ser implementadas de acuerdo a las políticas vigentes en la organización.
7. Las autoridades responsables de la aplicación de la política de seguridad de las TIC (STIC) determinarán el análisis y aplicación de este documento a los equipos Cisco WLC bajo su responsabilidad.

3. ORGANIZACIÓN DEL DOCUMENTO

8. Este documento se compone de los siguientes apartados:

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

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

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

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

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. El equipo debe ser examinado para comprobar que no ha sido manipulado durante su entrega confirmando los siguientes pasos:

    a) Antes de abrir el paquete donde fue entregado el producto, se debe comprobar que el paquete contenga la serigrafía y logo de Cisco Systems. Si no es así, se recomienda contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado).

    b) Es necesario comprobar que el paquete no ha sido abierto y sellado de nuevo, mediante inspección de la cinta que lo cierra. Si el paquete parece haber sido abierto y después sellado de nuevo, es recomendable contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado).

    c) Se debe verificar que el paquete contiene la impresión resistente a manipulaciones de Cisco en la cara externa de la caja de cartón. Si no es así, se deberá contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado). Esta impresión contiene el número de producto de Cisco, su número de serie e información adicional sobre el contenido de la caja.

    d) Es importante chequear el número de serie del producto especificado en la documentación del pedido. El número de serie que figura en la etiqueta blanca de la caja se debe corresponder con el número de serie del dispositivo. Por tanto, es necesario verificar que este número concuerda con el número de serie en la factura enviada por correo. Si no es así, se debe contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado).

    e) En la recepción de la unidad, es necesario comprobar que el pedido fue enviado por el proveedor esperado (Cisco Systems o un distribuidor autorizado). Este proceso puede llevarse a cabo verificando el código de envío/paquete junto con la empresa de transporte. También es recomendable comprobar que los números de serie de los productos enviados concuerdan con los números de serie de los productos recibidos. Esta verificación debe ser llevada a cabo por algún mecanismo externo que no pertenezca al proceso de envío. Por ejemplo, teléfono, fax o un servicio online de rastreo de paquetes.

10. Una vez que el paquete ha sido abierto, es recomendable inspeccionar el dispositivo. Aquí es necesario comprobar que el número de serie mostrado en él concuerda con el número de serie que aparece en la documentación del envío y la factura. Si no es así, se debe contactar con el proveedor del equipo (*Cisco Systems* o un distribuidor autorizado).

4.2 ENTREGA SEGURA DEL *SOFTWARE*

11. El equipo se entrega con *software* instalado, pero puede ocurrir que no sea la versión recomendada. En este caso, el software deberá actualizarse.
12. El procedimiento de *upgrade* se encuentra en el apartado *"Downloading and Installing an Upgrade"* de la guía Ref1.
13. El WSA descarga a la vez el valor de *hashing* (SHA-384) y el *software* desde *cisco.com*. Una vez que el *software* es conseguido, el WSA calcula el *hash* y lo verifica de manera automática. Si falla la integridad, el WSA lo indica. Por tanto, no es necesario realizar ninguna verificación manual de la integridad del *software* a instalar.

4.3 ENTORNO DE INSTALACIÓN SEGURO

14. El equipo debe instalarse en una ubicación físicamente segura donde **solo se permita acceso físico al personal autorizado.**

4.4 REGISTRO Y LICENCIAS

15. El sistema de licencias se denomina *Smart Software Licensing*. Cada cliente tiene una cuenta propia en *Smart Licensing* en el portal Cisco Smart Software Manager (CSSM) : *https://software.cisco.com/*. CSSM refleja las las licencias adquiridas y usadas.
16. El procedimiento de gestión de licencias en CSSM se encuentra en el apartado "*Smart Accounts*" de la guía Ref2.
17. El procedimiento de activación de licencia en el equipo se encuentra en el apartado "*Smart Software Licensing*" de la guía Ref1.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

18. El equipo requiere los siguientes componentes en el entorno operacional:
    a) Servidor de monitorización
    b) Este punto hace referencia a un servidor que permita una conexión SCP en un servidor de syslog remoto.
    c) Puesto de gestión
    d) Este puesto hace referencia a cualquier estación de trabajo que permita una conexión por Ethernet al equipo.
    e) Puesto de gestión con cliente SSH
    f) Este puesto hace referencia a cualquier estación de trabajo con un cliente SSHv2 instalado, que se emplea para la configuración y administración del equipo.

5. FASE DE INSTALACIÓN

19. Para la instalación del equipo siga los diferentes apartados de la guía "*Hardware Installation Guide*" Ref3.
20. Se deberán seguir también, en la medida de lo posible, las buenas prácticas publicadas por el fabricante, en lo que respecta al diseño de red, despliegue y configuración de políticas. Se pueden encontrar en el siguiente enlace:

    https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/guide-c07-742373.html

6. FASE DE CONFIGURACIÓN

21. El equipo necesita de una configuración básica mediante un cable Ethernet conectado directamente al puerto M1 del equipo.
22. El administrador autorizado se conecta a https://192.168.42.42:8443 y se autentifica con el usuario *admin* y el *default password ironport*. *El System Wizard Setup* arrancará automáticamente para asegurar una configuración inicial completa. El primer paso de la configuración inicial consiste en cambiar el password.
23. El procedimiento se encuentra en los diferentes apartados de la guía *"Getting Starting Guide"* Ref4.
24. Además, la contraseña seleccionada debe cumplir los requerimientos de complejidad para ser catalogada como segura. Esta contraseña debe ser una contraseña con seis o más caracteres y debe almacenarse en una localización segura.

6.1 MODO DE OPERACIÓN SEGURO

2. **El producto debe utilizarse en el denominado modo de operación seguro. Para ello, el equipo debe ejecutarse en modo de operación FIPS.**
25. Con la configuración FIPS se utilizan automáticamente los algoritmos y los tamaños de llave necesarios para poder realizar una ejecución de WSA de forma segura. Además, todas las contraseñas almacenadas y las llaves se cifrarán.
26. El procedimiento de activación de FIPS se encuentra en el apartado *"Enabling or Disabling FIPS Mode"* de la guía Ref1.

6.2 ADMINISTRACIÓN DEL PRODUCTO

6.2.1 DESHABILITACIÓN TELNET

27. Por defecto *Telnet viene deshabilitado*. En cualquier caso, **se debe comprobar** siguiendo el apartado *"The Commands: Reference Examples > interfaceconfig"* de la guía Ref6.

6.2.2 CONFIGURACIÓN SSHV2

28. **No debe utilizarse SSH como protocolo de administración** dado que el mecanismo de intercambio de claves (*Diffie-Hellman Grupo 14*) con parámetros (*modulus*) de 2048 bits, representa una fortaleza máxima de 112 bits y, según la guía CCN-STIC-807, la fortaleza deberá ser equivalente, al menos, a 128 bits.

6.2.3 CONFIGURACIÓN TLS

29. Como el equipo está configurado en modo FIPS, se limita el conjunto de ciphersuites disponibles. Sin embargo, de entre aquellas disponibles, se deben utilizar aquellas que estén recomendadas por la guía *CCN-STIC-807 Criptología de empleo en el ENS*:
    - *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
    - *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
30. Para la configuración de TLS se debe seguir el apartado "*The Commands: Reference Examples > sslconfig"* de la guía Ref6.
31. Durante el proceso de configuración, aparecerá la pregunta "*Would you like to Enable/Disable TLS Renegotiation for GUI HTTPS?"* a lo que se debe responder con "*n"* para deshabilitar la renegociación de TLS para la GUI en HTTPS.
32. Para limitar el cifrado por defecto, se debe editar la lista con "!" delante de aquellos que no están permitidos haciendo uso del comando "*sslconfig*".
33. **TLSv1.0 y TLSv1.1 no está permitida y no debería ser seleccionada durante el proceso de configuración.**

6.2.4 OBTENCIÓN E INSTALACIÓN DE CERTIFICADO X.509

34. Para usar TLS, el equipo debe tener un certificado X.509v3 y tiene que coincidir con la clave privada para securizar el tráfico. El equipo puede generar un CSR para subirlo a una autoridad certificadora y obtener así un certificado público. Así, será devuelto por la entidad certificadora un certificado público de confianza firmado por una clave privada.
35. Para hacer uso del certificado se debe seguir el apartado "*The Commands: Reference Examples > certconfig"* de la guía Ref6.
36. Para la generación de llave se debe asegurar la longitud de 3072 bits.

6.2.5 AUTOCHEQUEOS

37. El propio equipo contiene test criptográficos propios para chequear que las siguientes funcionalidades están correctas:
    - Prueba de respuesta conocida AES
    - Prueba de respuesta conocida de firma RSA
    - Prueba de respuesta conocida HMAC
    - Prueba de respuesta conocida SHA-1/256/512
    - Prueba de integridad del software
38. Durante el proceso de arranque del sistema (encendido o reinicio), todos los test POST comprobarán que los algoritmos criptográficos funcionan correctamente.

39. En caso de que algún error ocurra durante este proceso se podrá ver en los logs del sistema el siguiente mensaje:

    _FIPS-2-SELF_TEST_WAS_FAILURE: "WAS crypto FIPS self test failed at %s."

40. En caso de que esto ocurra, contactad con el soporte de Cisco vía http://www.cisco.com/techsupport or 1 800 553-2447

41. Estas comprobaciones son suficientes para verificar que las operaciones criptográficas se están realizando de una manera correcta.

6.2.5.1 PUESTA A CERO DE LAS LLAVES

42. Aunque la puesta a cero de las llaves se gestiona desde el módulo criptográfico, existe un comando *wipe* para confirmar que esto ocurre.

43. Para lanzar el comando, se debe seguir el apartado "*The Commands: Reference Examples > wipedata"* de la guía Ref6.

6.2.6 SINCRONIZACIÓN

44. **El producto debe estar configurado de acuerdo a una fuente de tiempo fiable**. Para realizar la configuración NTP el procedimiento viene descrito en el apartado "*System Date and Time Management*" de la guía Ref1.

6.2.7 CONFIGURACIÓN DE PUERTOS Y SERVICIOS

45. En la siguiente tabla se puede encontrar la lista de servicios y protocolos permitidos en WSA como cliente (siendo el iniciante) o cómo servidor (como terminador) ejecutándose a nivel de procesos *system-level*.

Servicio o protocolo	Cliente (iniciante)	Permitido	Servidor (terminador)	Permitido	Uso permitido con configuración certificada
DHCP	Sí	Sí	Sí	Sí	Sin restricción
DNS	Sí	Sí	No	n/a	Sin restricción
FTP	Sí	No	No	n/a	Usar SCP o HTTPS
HTTP	Sí	No	Sí	No	
HTTPS	Sí	Sí	Sí	Sí	Sin restricción
ICMP	Sí	Sí	Sí	Sí	Sin restricción
IMAP4S	Sí	Sobre TLS	No	n/a	Sin restricción
LDAP	Sí	No	No	n/a	Si se usa para autenticación, configurar TLS
LDAP-over-SSL	Sí	No	No	n/a	Si se usa para autenticación, configurar TLS

Servicio o protocolo	Cliente (iniciante)	Permitido	Servidor (terminador)	Permitido	Uso permitido con configuración certificada
NTP	Sí	Sí, no probado	No	n/a	Cualquier configuración. Se recomienda autenticación *key-based.*
RADIUS	Sí	No	No	n/a	Si se usa para autenticación, usar TLS para securizar.
SCP	Sí	Sí	Sí	Sí	
SMTP	Sí	Sí	No	n/a	Se recomienda el uso de SMTPS
SMTPS	Sí	Sobre TLS	No	n/a	Configurar TLS
SNMP	Sí (traps)	Sí	Sí	No	Sólo traps y recomendado sobre túnel en TLS
SSH	Sí	Sí (para syslog)	Sí	No	
SSL (no TLS)	Sí	No	Sí	No	Usar TLS
Telnet	Sí	No	Sí	No	Usar TLS
TLS	Sí	Sí	Sí	Sí	
TFTP	Sí	No	No	n/a	Se recomienda usar SCP o HTTPS.

Tabla 1 - Lista de servicios y protocolos permitidos

6.3 GESTIÓN SEGURA

6.3.1 ADMINISTRADORES AUTORIZADOS

46. La configuración de administradores autorizados se hace siguiendo el apartado "*Administering User Accounts*" de la guía Ref1.

47. En él se encuentran las descripciones de cada uno de los roles: *Administrator, Operator, Read-Only Operator, Guest.*

6.3.2 COMPLEJIDAD DE LA CONTRASEÑA

48. La contraseña que se genere para cada uno de los roles debe tener de **un mínimo de 15 caracteres**, haciendo uso de mayúsculas, minúsculas, números y al menos un carácter especial.

49. Se debe seguir el apartado "*Setting Passphrase Requirements*" de la guía Ref1.

6.3.3 GENERACIÓN DE UN *BANNER*

50. El administrador autorizado **debe crear un banner** para mostrar a los usuarios antes de acceder.
51. Se debe seguir el apartado *"Additional Security Settings for Accessing the Appliance"* de la guía Ref1.

6.3.4 CIERRE Y TERMINACIÓN DE SESIÓN

6.3.4.1 BLOQUEO DE USUARIO

52. Las cuentas de usuario deben bloquearse tras un número de autenticaciones fallidas concretas. El número por defecto es de 5 intentos, **pero deberá fijarse a 3.**
53. Para realizar el cambio, el procedimiento se encuentra en el apartado *"Configuring Restrictive User Account and Passphrase Settings"* de la guía Ref1.

6.3.5 CIERRE DE SESIÓN INACTIVA

54. Las sesiones deben tener una configuración de inactividad para que estas se cierren al cabo de un lapso de tiempo determinado. El tiempo por defecto es de 30 minutos, pero **deberá fijarse a 10 minutos.**
55. Para realizar el cambio, el procedimiento se encuentra en el apartado *" Additional Security Settings for Accessing the Appliance"* de la guía Ref1.

6.3.6 CIERRE DE SESIÓN

56. El usuario debe realizar el cierre de sesión mediante el "*logout*" si está en GUI y mediante un "*exit*" si se encuentra en CLI.

6.4 AUDITORÍA

6.4.1 CONFIGURACIÓN DE LOGGING

57. **Los ficheros de log generados se deben guardar realizando una copia de seguridad a un servidor SCP o a un servidor de *syslogs* remoto**. El procedimiento se encuentra en el apartado "*Monitor System Activity Through Logs* " de la guía Ref7.
58. SCP es securizado por SSHv2. Para la configuración SSHv2 se debe seguir el apartado "*The Commands: Reference Examples > sshconfig*" de la guía Ref6.
59. Las recomendaciones de CCN-STIC-807 soportadas son:
    - Algoritmos KEX: *ecdh-sha2-nistp256, ecdh-sha2-nistp384 y ecdh-sha2-nistp521.*
    - Algoritmos Cifrado: *aes128-ctr, aes192-ctr, aes256-ctr.*

- *HMAC-SHA1.*
- Algoritmo de autenticación: *rsa-sha2-512 (key 3072).*

60. El administrador autorizado debe asegurarse de que al menos las siguientes alertas están incluidas:
    - *Audit Logs* (activado por defecto)
    - *CLI Audit Logs* (activado por defecto)
    - *Configuration Logs*
    - *GUI logs* (activado por defecto)
    - *Logging logs* (activado por defecto)
    - *Authentification Framework Logs* (activado por defecto)
    - *Status Logs* (activado por defecto)
    - *System Logs* (activado por defecto)
    - *Updater Logs* (activado por defecto)

6.5 BACKUP

61. **Se deben realizar copias de la configuración del producto**. El procedimiento se encuentra en el apartado "*Saving the Appliance Configuration File*" de la guía Ref1.

7. FASE DE OPERACIÓN

62. Durante la fase de operación del equipo, el administrador debe llevar a cabo las siguientes tareas:

    - Mantenimiento del **control de acceso** al equipo.
    - **Comprobaciones periódicas del *hardware* y *software*** para asegurar que no se ha introducido hardware o software no autorizado.
    - **Seguimiento de las alertas de seguridad de Cisco** (*Security Advisories*) y, si es necesario, aplicar un *patch*.
    - **Mantenimiento de los registros de auditoría**. Estos registros estarán protegidos contra borrados y modificaciones no autorizados, y solamente el personal de seguridad autorizado podrá acceder a ellos.

8. REFERENCIAS

Ref1 *User Guide for AsyncOS 11.8 for Cisco Web Security Appliances - GD (General Deployment) - Chapter: Perform System Administration Tasks*
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-8/user_guide/b_WSA_UserGuide_11_8/b_WSA_UserGuide_11_7_chapter_010110.html

Ref2 *Cisco Software Licensing Guide*
https://www.cisco.com/c/en/us/buy/licensing/licensing-guide.html#smart-licensing

Ref3 *Hardware Installation Guide*
https://www.cisco.com/c/en/us/td/docs/security/content_security/x95_series/hw/guide/wsa/install-wsa-x95/overview.html

Ref4 *Getting Starting Guide*
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa-sx95-gsg/cisco-wsa-sx95-gsg/m-plan-the-installation.html

Ref5 *Cisco Secure Email and Web Virtual Appliance Installation Guide*
https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_Security_Virtual_Appliance_Install_Guide.pdf

Ref6 *CLI Reference Guide for AsyncOS 13.0*
https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/cli_reference_guide/b_CLI_Reference_Guide_13_0.html

Ref7 *User Guide for AsyncOS 11.8 for Cisco Web Security Appliances - GD (General Deployment) - Chapter: Monitor System Activity Through Logs*
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-8/user_guide/b_WSA_UserGuide_11_8/b_WSA_UserGuide_11_7_chapter_010101.html

9. ABREVIATURAS

AES	*Advanced Encryption Standard*
CLI	*Command Line Interface*
CSR	*Certificate Signing Request*
CSSM	*Cisco Smart Software Manager*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name Service*
ESA	*Email Security Appliance*
FIPS	*Federal Information Processing Standard*
FTP	*File Transfer Protocol*
GUI	*Graphical User Interface*
HTTP	*Hypertext Trasfer Protocol*
HTTPS	*Hypertext Trasfer Protocol Secure*
ICMP	*Internet Control Message Protocol*
IMAP4S	*Internet Message Protocol Secure version 4*
LDAP	*Lightweight Directory Access Protocol*
NTP	*Network Time Protocol*
POST	*Power On Self Test*
RADIUS	*Remote Authenticatio Dial in User Service*
RSA	*Rivest, Shamir and Adleman*
SCP	*Secure Copy Protocol*
SMTP	*Simple Mail Transfer Protocol*
SMTPS	*Simple Mail Transfer Protocol over TLS*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
SSL	*Secure Socket Layer*
TCP	*Transport Control Protocol*
TCP/IP	*Transport Control Protocol/ Internet Protocol*
TLS	*Transport Layer Security*
TFTP	*Trivial File Transfer Protocol*
WSA	*Web Security Appliance*

PUBLICACIONES DE DEFENSA

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