centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1102

Procedimiento de Empleo Seguro
Citrix Netscaler ADC

Enero 2021

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.02.03 16:52:07 +01'00'

NIPO: 083-20-091-5

Fecha de Edición: enero de 2021

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

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Enero de 2021

Paz Esteban
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. Citrix ADC (antes NetScaler) es un *Application Delivery Controller* con funciones que abarcan un rango amplio, y que podríamos resumir como:
    a) Balanceo/proxy inverso -incluido terminación SSL, optimizaciones para tráfico HTTP, etc.
    b) Seguridad de Acceso y centralización de la autenticación y *Single Sign-On*.
    c) SSL VPN.
    d) *Web Application Firewall* -y otras capacidades de seguridad adicionales.
    e) Proxy directo -forward proxy o proxy de navegación.
2. No obstante, únicamente la de Seguridad de Acceso y centralización de la autenticación ha sido objeto del proceso de cualificación.
3. La solución se presenta en varios formatos: *appliance* hardware de Citrix, máquina virtual (sobre hipervisores VMWare vSphere, Microsoft Hyper-V, Citrix XenServer), o en nubes públicas (Microsoft, Amazon, Google, Oracle), *appliance* hardware virtualizado (*appliance* Citrix sobre el que corren instancias virtuales de Citrix ADC), imagen para contenedor *Docker*, y formato *bare-metal* (corre sobre Linux, como aplicación).

2. OBJETO Y ALCANCE

4. Las configuraciones indicadas en esta guía aplican, en gran medida, a cualquier formato de los mencionados en el punto anterior, ya que son configuraciones de administración de la solución que afectan principalmente al *firmware* principalmente. En los apartados en los que haya una configuración diferente en un modelo hardware o software se indicará convenientemente, de forma que la guía siga siendo válida en ambos casos.
5. Por último, los procedimientos descritos aplican a las versiones comprendidas entre la v11.1 y v13.0 (vigente durante la generación de este documento). En caso de existir, se harán constar las diferencias de configuración entre versiones.

3. ORGANIZACIÓN DEL DOCUMENTO

6. Este documento recoge el uso de los *appliance* Citrix ADC en distintas fases de su ciclo de vida, en los siguientes apartados:

   - **Apartado 4.** Recomendaciones que tener en cuenta durante la fase de despliegue e instalación del producto.
   - **Apartado 5**. Recomendaciones que tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
   - **Apartado 6.** Tareas recomendadas para la fase de operación o mantenimiento del producto.
   - **Apartado 7.** Listado resumen con las distintas recomendaciones mencionadas a lo largo del documento.

4. FASE DE INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. En el caso de que el producto sea un dispositivo hardware (*appliance*) se verificará que no haya signos evidentes de manipulación, como cinta de embalar sobre otra anterior, pegatinas de envío rasgadas o superpuestas, etc. Aunque este procedimiento pudiera cambiar, hoy en día las cajas llevan impreso CITRIX en el propio cartón.
8. En caso de que sea un producto software, se verificará que se ha obtenido directamente de la web de Citrix (www.citrix.com), asegurando que el certificado de seguridad es válido. Las descargas vía web proporcionan un hash, que deberá comprobarse para verificar la autenticidad del software descargado.

4.2 ENTORNO DE INSTALACIÓN SEGURO

9. Los *appliance* hardware deberán instalarse en un Centro de Proceso de Datos (CPD), al que solo personal autorizado tenga acceso. Las versiones software (*virtual appliance*) se suelen instalar sobre un hardware virtualizado mediante un hipervisor, que deberá estar también en un CPD con acceso restringido.

4.3 REGISTRO Y LICENCIAS

10. El *hardware* será registrado automáticamente en la cuenta de la organización adquiriente. Asimismo, en el *email* de confirmación de la adquisición se dan las instrucciones válidas en ese momento para aplicar al *appliance* (físico o virtual) la licencia adquirida. Hay varias formas de licenciar el *appliance*. La más sencilla consiste en:
    - Acceder en el GUI, en la pestaña ***Configuration***, al menú ***System > Licenses*.**
    - Hacer clic en *Manage License* y después en *Add New License*.
    - Elegir la opción ***Use License Access Code*** e introducir el código de licencia, que estará en la cuenta de usuario de la organización en Citrix.com.
    - De esta forma, se generará una licencia que el *appliance* descargará automáticamente de la web de Citrix.

4.4 CONSIDERACIONES PREVIAS

11. Los *appliance hardware* se instalarán, como cualquier otro *appliance*, en un rack estándar, para lo cual vienen incluidas con el equipo las guías metálicas. No hay consideraciones de seguridad más allá de las típicas en cualquier instalación de hardware en CPD y no hay piezas de hardware especiales que instalar, a menos que se use un HSM externo, en cuyo caso se seguirán las instrucciones del fabricante de este.
12. Una vez cableado el *appliance*, si se ha hecho de la forma correcta, no se requerirá acceso físico a este para la configuración. Aun así, es conveniente mantener la

posibilidad de acceso físico hasta asegurar que se puede seguir administrando desde un puesto normal de red. Además, la configuración es más sencilla si se realizan unas mínimas tareas utilizando la conexión al puerto serie, como se verá en el apartado 5.3. Si bien esto se puede hacer con un administrador de consolas, se requerirá acceso físico cuando no se disponga de él.

13. En el caso de versiones software (máquina virtual), y dependiendo del hipervisor usado en cada caso, se seguirán estas instrucciones: *https://docs.citrix.com/en-us/citrix-adc/13/deploying-vpx.html*. En ellas, se especifican las necesidades hardware del servidor y la máquina virtual *mínima* que es necesario provisionar. Durante el proceso de adquisición de la solución se darán especificaciones concretas según la licencia adquirida, aunque también se podrán encontrar en la documentación técnica vigente en ese momento: *https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-adc-vpx-data-sheet.pdf*.
14. Para el caso de *appliance hardware*, se seguirán estas instrucciones: *https://docs.citrix.com/en-us/citrix-adc/13/getting-started-with-citrix-adc/install-hardware.html.*
15. Los *appliance* hardware vienen con una versión relativamente reciente del firmware, con lo que no es preciso realizar una instalación inicial del firmware sino que bastará con actualizarlo a la versión deseada. Este proceso se detalla más adelante en el apartado de Actualizaciones (ver 5.9).

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

16. La configuración inicial para poder operar con el equipo remotamente consiste en asignarle una IP de gestión, un Gateway y, opcionalmente, algún parámetro adicional mediante una conexión de consola (o usando la IP por defecto 192.168.100.1/16). Para ello bastará con ejecutar el siguiente comando e introducir los datos, así como cambiar la contraseña por defecto del usuario *nsroot*:

    >config ns

    *>set system user nsroot -password ** pedirá contraseña nueva*

17. Para los *appliance* que cumplen la normativa FIPS (en cuyo caso el propio nombre del equipo incluye el término *FIPS*), el administrador deberá habilitar ese modo seguro FIPS, mediante los siguientes comandos:

    >reset fips

    >reboot

    >set fips -initHSM Level-2 so12345 so12345 user123 -hsmLabel NSFIPS

    >saveconfig

    >reboot

    *>show fips ** debe aparecer un error "Operation not permitted - FIPS card was initialized, please reboot the system"*

    >reboot

    *>show fips ** esta vez sí debe aparecer información sobre los componentes FIPS*

    >set system parameter –fipsUserMode ENABLED

    >reboot

    *root@ns#sysctl netscaler.fips_mode **responderá con netscaler.fips_mode: 1*

5.2 AUTENTICACIÓN

18. Para la gestión de Citrix ADC deberá utilizar un usuario con los permisos suficientes (administrador). Este usuario puede estar definido en el propio *appliance*, o existir en un servidor externo LDAP, RADIUS o TACACS+..

19. Para la autenticación en el propio *appliance* deberá crearse una política de contraseñas restrictiva y que siga las recomendaciones generales establecidas en el apartado 5.3.

20. No obstante, se recomienda que la autenticación de usuarios se realice contra servidores de autenticación externos (LDAP, RADIUS, TACACS+), en cuyo caso la

política de contraseñas[1] vendrá determinada por esos sistemas acorde al resto de la organización. .

21. El método más habitual de autenticación externa es vía LDAP, que mostramos a continuación en su configuración más sencilla, que consiste en:

    a) Definir la acción (el servidor LDAP):

    >add authentication ldapAction LDAP_mgmt -serverIP

    <lb_vserver_ip> -serverPort 636 -ldapBase "DC=citrix,DC=lab" - ldapBindDn readonly@citrix.lab - ldapBindDnPassword-ldapLoginName sAMAccountName-searchFilter "&(memberof=CN=NSG_Admin,OU=AdminGroups,DC=citrix,DC=lab)" - groupAttrName memberOf

    b) Definir la política:

    >add authentication ldapPolicy pol_LDAPmgmt ns_true LDAP_mgmt

    c) Enlazar la política a nivel global en el appliance:

    >bind system global pol_LDAPmgmt -priority 110

22. Asimismo, es posible configurar el acceso requiriendo doble factor de autenticación, donde el segundo factor está accesible vía integración RADIUS, tal como se detalla en el siguiente enlace: https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-config-external-user-authn-con.html (ver Caso 3).

23. La integración de Citrix ADC con terceros para gestión de usuarios se hace como requieren esos servidores externos. Así, para LDAP se puede habilitar una comunicación segura mediante certificados digitales, mientras que con RADIUS hay que utilizar una contraseña. En el apartado 5.13.3 se describe cómo se establecen comunicaciones seguras con entidades externas. En este apartado solo se detalla el método nativo de cada servicio.

24. La gestión del *appliance* vía HTTPS exige la autenticación de este, que presentará un certificado al navegador antes de pedir las credenciales. La conexión mediante SSH se puede hacer mediante usuario/contraseña y también con autenticación de clave pública, si se configura de ese modo (configuración recomendada), tal como se detalla en el siguiente enlace: https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ssh-key-based-authentication.html.

25. Para habilitar la autenticación en el lado del cliente del servicio HTTPS del GUI, se puede utilizar el siguiente comando:

    >set ssl service nshttps-127.0.0.1-443 -clientAuth ENABLED

[1] En cualquier caso, la política de contraseñas debería cumplir las recomendaciones establecidas en el apartado **¡Error! No se encuentra el origen de la referencia.**, salvo que se apliquen medidas compensatorias que justificasen su relajación.

Y enlazar ese servicio a la CA que emite los certificados de cliente (esta CA se habrá importado previamente, como se indica en el apartado 5.6 “Gestión de Certificados”):

>bind ssl service nshttps-127.0.0.1-443 -certkeyName <CA_cert>FNMT_intemediate_USUARIOS -CA

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

26. El equipo se configurará de acuerdo a los principios de mínima funcionalidad y mínimo privilegio, es decir, se tratará que los usuarios administradores sean los mínimos posibles y que el conjunto de usuarios en general no disponga de más privilegios que los que necesita.
27. La administración del dispositivo podrá realizarse de manera local o remota, aunque la primera opción siempre será preferible a la segunda desde el punto de vista de la seguridad:
    a) Administración local. Podrá realizarse desde un terminal utilizando la interfaz de línea de comandos (CLI).
    b) Administración remota. Podrá realizarse a través de cualquier interfaz Ethernet utilizando un canal seguro. Como norma general, la administración se realizará desde la propia LAN en la que esté instalado en *appliance*.
    c) Alternativamente, se podrá conectar el PC del administrador directamente al puerto de gestión; en este caso se podrá usar SSH para acceder al CLI, y HTTPS para acceder al GUI, pero sin existir otros equipos compartiendo la red de acceso.
28. Para la administración remota del equipo deberán utilizarse únicamente protocolos seguros (HTTPS, SSH). Los protocolos HTTP, TELNET y FTP se consideran inseguros y no deberán utilizarse.
29. Para la administración remota del equipo deberán utilizarse únicamente protocolos seguros (HTTPS, SSH). Los protocolos TELNET y FTP se consideran inseguros y, por tanto, están deshabilitados de fábrica. En el caso de HTTP, se deshabilitará mediante el comando:

    >set ns ip <ip_gestion> -gui SECUREONLY

30. Aparte de las conexiones remotas para administración mencionadas, el producto ofrece, según el *appliance* del que se trate, distintas formas de conexión a través de consola:
    a) A través del puerto serie, en los *appliance* que lo incorporan.
    b) A través de la consola del *hipervisor*, en soluciones virtuales.
    c) A través del puerto LOM (*Lights Out Management*), en los *appliance* que lo incorporan.

31. En estas conexiones se gestionará mediante interfaz de comandos. En el caso del LOM existe un pequeño GUI *ad hoc* también para la gestión del hardware en casos de fallo de algún componente (independientemente de poder gestionar también la configuración como en los otros casos de consola).

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

32. La solución viene preconfigurada con unos pocos perfiles de administración: solo-lectura, operador de red, operador de configuración, *sysadmin*, *superuser*, etc. de modo que basta enlazar un perfil a un administrador concreto, por ejemplo:

    > bind system user <usuario> read-only <priority>

    <*priority*> es el orden que ocuparía el rol *read-only*, en caso de que ese usuario tuviera más roles asignados. Por ejemplo, un usuario puede tener un rol *read-only* con prioridad 100 que le permitirá ver toda la configuración, y después un rol *custom* con prioridad 110 para poder modificar ciertas partes de la configuración.

33. Sin embargo, se pueden crear perfiles con capacidades muy específicas, para segmentar mucho más el acceso y así ajustar más la seguridad. Esto se hace mediante las *Command Policies* (expresiones regulares que reflejan los comandos que se pueden aplicar o prohibir), como se explica en el siguiente enlace: https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-config-users-and-grps-tsk.html.

34. A modo de ejemplo, este comando añade una política expresa de acceso al *Shell* del sistema operativo, para luego poder limitarla a ciertos usuarios:

    *>add system cmdPolicy Shell_policy ALLOW (shell (mkdir|tar|.*installns|cat /tmp/aaad.debug|date|tail -f /var/log/notice.log|.logkeys_1.sh.|scp *|vi /nsconfig/ssh/sshd_banner|vi /nsconfig/issue|date *|sha256 *))*

    >bind system user <usuario> Shell_policy <priority>

35. Como ya se indicó anteriormente, se debe disponer del mínimo número de administradores posibles y cada uno de ellos tendrá los mínimos privilegios necesarios. Deberá evitarse trabajar con perfiles privilegiados salvo que se requiera realizar acciones sobre el sistema que así lo exijan.

36. Además, deberán configurarse otra serie de parámetros de sesión para ajustarlo a las políticas de seguridad que apliquen a la instalación/arquitectura en la que se instale la solución. Estas medidas son:

    a) *Timeout* por inactividad de la sesión de administración por usuario y/o grupo y/o por defecto:

       >set system user <user> -timeout 200

       >set system group <group> -timeout 350

       >set system parameter -timeout 400

b) Número máximo de intentos fallidos de autenticación antes de bloquear durante un tiempo de espera a ese usuario. En el ejemplo hemos puesto 3, este valor podría modificarse pero no debería ser superior a 5.

>set aaa parameter -maxloginAttempts 3 -failedLoginTimeout 10

c) Número de sesiones concurrentes máximas de un administrador:

>set system user <user> -maxsession 3

d) *Timeout* para la línea de comandos:

>set cli mode timeout 500

37. Se puede modificar el mensaje por consola y GUI que el usuario verá al loguearse (*login banner*). Para ello basta introducir el texto deseado en el fichero */nsconfig/motd* (mensaje enviado tras el *login*), en el fichero */etc/issue.net* (mensaje anterior al *login*) para ssh y */etc/issue* para acceso por consola serie. Se recomienda incluir un mensaje que advierta de que **solo los usuarios autorizados pueden acceder al Sistema y que toda la actividad será supervisada para verificar el cumplimiento de la política de seguridad.**

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

38. La configuración de interfaces no es más o menos segura *per se*, sino que depende de la arquitectura en que se despliega el *appliance* (una sola conexión física a la red o varias, VLAN única en cada puerto físico o uso de *trunks* de VLANs 802.1q, etc.) La configuración de interfaces e información relacionada como VLANs, etc., se encuentra en el siguiente enlace: *https://docs.citrix.com/en-us/citrix-adc/13/networking/interfaces.html.*

39. Deberán deshabilitarse las interfaces que no estén en uso, con el comando:

>disable interface 1/4

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

40. En el apartado 5.3.1 ya se describió cómo deshabilitar la administración mediante HTTP, TELNET o FTP para limitarla así a HTTPS. Para limitar, además, las versiones de SSL/TLS aceptables para la administración, la forma más sencilla es accediendo en el GUI a ***Traffic Management > Services >*** **pestaña *Internal Services***, editar el servicio ***nshttps-127.0.0.1-443***, y en el menú **SSL *Parameters*** desmarcar las versiones no deseadas.

41. En el caso de SSH, por defecto el *appliance* solo permite conexiones SSH v2, ya que la versión 1 es sabida insegura.

42. En el caso de TLS, deberá permitirse únicamente le uso de versiones de TLS 1.2 o superior.

43. El *appliance* incorpora un número elevado de combinaciones de algoritmos y tamaños de clave para utilizar en conexiones seguras en cualquier entorno. Deberán limitarse mediante configuración, de forma que los administradores solo

puedan utilizar un conjunto restringido de ellos, en este caso los admitidos según la guía CCN-STIC-807. En concreto, los administradores podrán configurar y utilizar los algoritmos y funciones criptográficas admitidos según la guía CCN-STIC-807, como se detalla en los siguientes párrafos:

a) DSA o RSA con claves de, al menos, 3072 bits de longitud:

   >create ssl rsakey testcert.key 3072 -exponent F4 -keyform PEM –aes256 -password pwd

b) ECDSA con curvas P-256 o superior. Para ello, deberán seguirse los siguientes pasos:

c) Desenlazar del virtual server concreto la curva P-224 (por defecto viene enlazada también esa, que no cumple la restricción).

   >unbind ssl vserver <vserver_name> eccCurveName P_224

d) Enlazar al virtual server únicamente el cipher group ECDSA que ya existe por defecto en el appliance y contiene los cipher suites que usan ECDSA:

   >unbind ssl vserver <vserver_name> -cipherName DEFAULT

   >bind ssl vserver <vserver_name> -cipherName ECDSA

e) Funciones Hash SHA-256 o superior: basta con crear un cipher group e incluir en él los cipher suites que cumplan ese requerimiento y finalmente enlazar solo ese cipher group al virtual server como se indicó antes:

   >add cipher MiCiphergroup

   >bind ssl cipher MiCiphergroup -cipherName TLS1-ECDHE-ECDSA-AES256-SHA384

   >bind ssl cipher …

f) Cifrado AES-128 o superior: basta con incluir en los *cipher group* que se creen solo los cipher suites que contengan AES-128, como se mencionó antes para el requerimiento de SHA-256.

g) Grupos *Diffie-Hellman* 15, 16, 19, 20, 21, 28, 29 o 30:

h) Los distintos grupos Diffie-*Hellman* representan tamaños de clave a utilizar. En el *appliance* se encuentran en */nsconfig/ssl/certs/dh*, donde se pueden borrar, si se desea, los grupos que no se quieran usar. También es posible configurar el grupo deseado en el *SSL Profile* que se va a usar, tal como se muestra en el siguiente ejemplo:

   >set ssl profile <profile_name> -dh enabled –dhfile /nsconfig/ssl/certs/dh/dh4096.pem

i) *Elliptic Curve Diffie-Hellman* P-256 o superior: basta elegir únicamente *cipher* suites que contengan *Diffie-Hellman* (creando un *cipher group* como se indicó antes), y excluir la curva P-224 en el virtual server, como también se indicó.

5.6 GESTIÓN DE CERTIFICADOS

44. Una vez aplicadas las restricciones del apartado anterior en cuanto a claves y algoritmos válidos, el procedimiento para la instalación y uso de certificados se muestra en los siguientes párrafos, si bien la configuración completa con todas sus posibles variantes se puede consultar en el siguiente enlace: https://docs.citrix.com/en-us/citrix-adc/current-release/ssl/ssl-certificates.html.

45. Deberá importarse un certificado raíz de una CA, para lo cual simplemente es necesario copiar el fichero de certificado en el *appliance*; de esta forma está listo para ser utilizado en el lugar apropiado (típicamente un virtual server).

    >import ssl certfile <local_CAfilename> <http://www.test.com/CAcertname>

46. A continuación, se generará una solicitud de certificado digital mediante línea de comandos. Para ello, se deberán ejecutar los siguientes comandos:

    a) Crear la clave privada:

    > create ssl rsakey <keyFile> <bits> [-exponent (3 | F4)] [-keyform (DER | PEM)] [--aes256] {-password } [-pkcs8]

    b) Crear la solicitud (que quedará guardada en */nsconfig/ssl*):

    > create ssl certreq <reqFile> -keyFile <keyFile> | -fipsKeyName <string>) [-keyForm (DER | PEM) {-PEMPassPhrase }] -countryName <string> -stateName <string> -organizationName <string> -organizationUnitName <string> -localityName <string> -commonName <string> -emailAddress <string> {-challengePassword } -companyName <string> -digestMethod (SHA256)

47. Para importar el certificado generado por una CA a partir de la solicitud del paso anterior hay que *instalar* el certificado, que consiste en enlazar el certificado con la clave privada que se usó para generar la solicitud. Los siguientes comandos copian al *appliance* el certificado utilizando HTTP (también se puede hacer mediante SCP, o en la herramienta gráfica), y posteriormente lo enlazan a la clave privada utilizada (los ficheros deben estar en /nsconfig/ssl):

    >import ssl certfile <local_certfile> http://www.test.com/<certname>

    >add ssl certkey <certname> -cert <local_certfile> [-key <keyFile>] [-fipsKey <string>] [-inform (DER | PEM)] [-password]

48. Por defecto, el *appliance* chequea la vigencia de los certificados instalados para dar servicio (los invalida tras su caducidad), y de forma dinámica chequea la de los certificados cliente usados por un cliente en una conexión SSL autenticada (según el estándar SSL/TLS).

49. Además de la caducidad, deberá validarse el estado de revocación de los certificados, para lo que se deberá configurar en cada punto en el cual se instala un certificado (típicamente los virtual servers). Para validar los certificados podrá utilizarse CRL u OCSP.

50. Para realizar la comprobación utilizando CRL deberán seguirse los siguientes pasos:

    a) Definir la CRL a descargar (y actualizar periódicamente, que puede ser por HTTP o LDAP):

    >add ssl crl <DesiredCRLName> <Desired_CRL_Filename.crl> -inform DER -refresh ENABLED -CAcert <MyCAsRootCertificatehere> -method HTTP -url "<http://myCRLurlhere/mycrl.crl>" [-interval <interval>] [-day <positive_integer>] [-time <HH:MM>]

    b) Configurar el virtual server deseado (y que tendrá una CA asociada previamente) para comprobar los certificados contra la CRL asociada a esa CA en el paso anterior:

    >bind ssl vserver <vServerName> -certkeyName <string> [(-CA -crlCheck (Mandatory |))]

51. Para realizar la comprobación utilizando OCSP deberán seguirse los siguientes pasos:

    a) Definir el servidor OCSP y los parámetros de la comprobación:

    >add ssl ocspResponder <name> -url <URL> [-cache (ENABLED | DISABLED)[-cacheTimeout <positive_integer>]] [-batchingDepth <positive_integer>][-batchingDelay <positive_integer>] [-resptimeout <positive_integer>] [-responderCert <string> | -trustResponder] [-producedAtTimeSkew <positive_integer>][-signingCert <string>][-useNonce (YES | NO)][-insertClientCert(YES | NO)]

    b) Enlazar ese responder al certificado que ha de usarlo para sus comprobaciones:

    >bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <positive_integer>]

    c) Configurar el virtual server donde se instaló ese certificado, para que lo verifique mediante ese responder:

    >bind ssl vserver <vServerName>@ (-certkeyName <string> (CA [-ocspCheck (Mandatory | Optional)]))

52. Además de las comprobaciones del estado de expiración y revocación del certificado, es posible configurar políticas para comprobar el contenido de cualquier campo con objeto de permitir, bloquear o simplemente hacer uso de esa información en pasos posteriores. Como ejemplo, esta política (una vez enlazada al virtual server deseado) impediría las conexiones si el certificado usado tiene un *keyUsage* que lo permite usar para firma digital y además el emisor del certificado contiene "*digicert*" en su nombre:

    >add responder policy del_esto3
    (CLIENT.SSL.CLIENT_CERT.KEY_USAGE(DIGITAL_SIGNATURE) ||
    CLIENT.SSL.CLIENT_CERT.ISSUER.CONTAINS("digicert")) DROP

53. La verificación de la cadena de certificados es realizada por el producto de forma automática.

5.7 SERVIDORES DE AUTENTICACIÓN

54. No son imprescindibles, y depende de los métodos de administración de cada organización el utilizar o no servidores de autenticación para los usuarios de administración. El *appliance* permite integrarse con RADIUS, LDAP, TACACS+, para los cuales es posible definir usuarios/grupos a los que asignar roles distintos de administración. La configuración básica se ha mencionado en el apartado 5.2 sobre Autenticación, pero aquí mencionaremos la forma de realizar estas conexiones de manera segura.

55. Para la conexión con LDAP es posible utilizar TLS de forma nativa, y basta configurar el *appliance* para conectar con LDAP en el puerto 636 (conexión directa por TLS) o en el puerto por defecto 389 pero indicando que la conexión es segura (en este modo se inicia la conexión sin cifrar, pero se pasa inmediatamente a TLS). Para ello, en un hipotético servidor *ext_ldap* ya creado con anterioridad, bastaría:

    >set authentication ldapaction ext_ldap -secType SSL -serverport 389

    Ó

    >set authentication ldapaction ext_ldap -secType TLS -serverport 636

56. La configuración de otros servicios de autenticación de forma que utilicen canales seguros TLS se hace definiendo un *virtual server* en el propio *appliance*, que hablará mediante TLS con el servidor de autenticación deseado; el *appliance* se configura entonces para usar ese virtual server en lugar del servidor directamente. (La configuración es equivalente a la que se presenta en el apartado 5.13.3 para el caso de SYSLOG, pero definiendo los servicios para que apunten a los servidores de autenticación deseados, RADIUS, TACACS+ y por su puerto correspondiente, en lugar del 514.)

5.8 SINCRONIZACIÓN HORARIA

57. Es recomendable configurar la sincronización horaria mediante NTP. Para ello, bastará con ejecutar los comandos siguientes (eligiendo el servidor NTP deseado):

    >add ntp server 0.es.pool.ntp.org

    >enable ntp sync

5.9 ACTUALIZACIONES

58. Las actualizaciones de firmware del *appliance* solo podrán ser realizadas por un número reducido de administradores/administradores de seguridad.

59. Las actualizaciones del *appliance* (físico o virtual) se realizan mediante un único paquete de *firmware* que se descarga de forma segura de la web de Citrix. El paquete descargado se guardará en una carpeta a crear bajo /var/nsinstall.

60. Se deberá verificar que el paquete es original de Citrix comparando el *checksum* que aparece en la página de descarga de Citrix para esa versión de firmware, con el del paquete que se acaba de guardar en el paso anterior y que se obtiene mediante el comando:

    >shell sha256 /var/nsinstall/build-xx.x.tgz

61. Posteriormente, se desempaquetará e instalará el firmware con:

    >shell tar -zxvf /var/nsinstall/build-xx.x.tgz

    >shell /var/nsinstall/installns

5.10 AUTO-CHEQUEOS

62. Además de los chequeos habituales del hardware base (placa base y otros componentes), el *appliance* realiza durante el arranque chequeos de integridad de la tarjeta FIPS, en caso de existir. Si fallase la comprobación, la consola mostraría el error *"NGFIPS: ERROR!!! Secure handshake failed."*, y el sistema bloquearía la operativa.

5.11 SNMP

63. Citrix ADC soporta SNMP v1, v2 y v3. Deberá usarse SNMP v3 siempre que lo permita en el entorno en que se integrará el equipo.

64. Para la configuración mínima, SNMP *community*, SNMP *manager* y SNMP *trap listener*. El resto de customización, como la elección de alarmas que se envían en los traps, podrá consultarse en el siguiente enlace: https://docs.citrix.com/en-us/citrix-adc/13/system/snmp/generating-snmp-traps-on-citrix-adc.html):

    >add snmp community <communityName> <permissions>

    >add snmp manager <IPAddress> ... [-netmask <netmask>]

    >add snmp trap [specific | generic] <IPAddress>

65. La configuración de SNMPv3 permite Views (acceso a una rama concreta el árbol de OIDs), grupos y usuarios (con autenticación y cifrado del tráfico si se requiere), y asignación (*bind*) de traps a usuarios:

    >add snmp view <name> <subtree> -type (included | excluded)

    >add snmp group <name> <securityLevel> -readViewName<string>

    >add snmp user <name> -group <string> [-authType SHA {-authPasswd } [-privType AES {-privPasswd }]]

    >add snmp trap <trapClass> <trapDestination> -version V3 -destPort <port> -communityName <string> -srcIP <ip_addr> -severity <severity>

    >bind snmp trap <trapClass> <trapDestination> [-version <version>] (-userName <string> [-securityLevel <securityLevel>])

5.12 ALTA DISPONIBILIDAD

66. Los *appliances* Citrix ADC permiten distintas configuraciones que pueden ofrecer disponibilidad mayor que la que se obtiene con un único *appliance*, ofreciendo redundancia a nivel local (HA, *High Availability*), geográfico (GSLB, *Global Server Load Balancing*), o configuraciones avanzadas de *cluster* multi-máquina (*Clustering mode*), y con múltiples variantes en cada uno de los casos. La configuración de alta disponibilidad recomendada, siempre que no existan otros requerimientos especiales, es la llamada habitualmente HA, activo-pasivo, cuya configuración completa se puede consultar en https://docs.citrix.com/en-us/citrix-adc/13/system/high-availability-introduction.html y que se puede configurar de forma mínima y segura cambiando la contraseña por defecto de comunicación entre los *appliances*, e indicando a un *appliance* cuál es su pareja, con:

    >set ns rpcNode <IPAddress> {-password} -secure YES

    >add ha node <id> <IPAddress>

5.13 AUDITORÍA

5.13.1 REGISTRO DE EVENTOS

67. El sistema registra todo tipo de eventos: de tipo informativo, relacionados con fallos, de interacción a nivel de administración y, por supuesto, aquellos relacionados con su funcionalidad principal. Los eventos quedan registrados en distintos ficheros en la carpeta /var/log. Los ficheros más relevantes a la hora de administrar el sistema son *ns.log*, *messages y httpaccess.log*. Como norma general, el resto de ficheros son usados únicamente por el personal de soporte de Citrix en incidencias concretas.

68. Los principales *logs* que suelen revisar los administradores son:

Fichero	Información que contiene
Ns.log	Contiene los mensajes registrados vía syslog; los comandos de configuración ejecutados (con hora, usuario y resto de información permitente)
Messages	Eventos de sistema; mensajes de autenticación; mensajes del arranque del sistema; mensajes de la consola
Httpaccess.log	Comandos de configuración ejecutados en el GUI de administración

5.13.2 ALMACENAMIENTO LOCAL

69. Por defecto, el *appliance* almacena de forma local los registros de eventos de sistema, sin necesidad de configuración adicional. Estos logs almacenados van rotando para no utilizar demasiado espacio en disco, por lo que se recomienda

exportarlos mediante *syslog* a un servidor SYSLOG externo, cuya configuración se describe en el siguiente apartado.

70. Los eventos se pueden consultar de varias formas, entre ellas desde la propia línea de comandos. La información de eventos de auditoría está, fundamentalmente, en */var/log/ns.log.*

    >shell more /var/log/ns.log

71. Los logs en Citrix ADC se gobiernan con una política de rotación para evitar saturar el disco. En el caso del log mencionado, la política por defecto indica que se empaquetará (comprimido) cuando llegue a 100 KB, y se mantendrán hasta los 25 últimos ficheros.

5.13.3 ALMACENAMIENTO REMOTO

72. Además de guardar los eventos en un *syslog* local, Citrix ADC permite exportarlos a servidores externos mediante una comunicación *syslog* estándar. No obstante, esta opción se desaconseja. En su lugar, deberá utilizarse una conexión segura.

73. Para enviar eventos *syslog* mediante una conexión segura, deberá definirse un *virtual server* como servidor *syslog* en el propio *appliance*, que se comunicará con los servidores *syslog* remotos mediante TLS. Para ello, deberán seguirse los siguientes pasos:

    a) Copiamos en /nsconfig/ssl el certificado de la CA que emitió el certificado del servidor *syslog*, y lo instalamos con el comando:

       >add ssl certkey server_cacert -cert <path_to_ca_cert>

    b) Creamos un servicio syslog que apunta al servidor syslog real, y un virtual server al cual lo enlazamos, y enlazamos el certificado introducido en el paso anterior:

       >add service syslog_service <syslog_server_ip> SSL_TCP <syslog_server_port>

       >add lb vserver lb_vserver TCP <lb_vserver_ip> 514

       >bind lb vserver lb_vserver syslog_service

       >bind ssl service syslog_service -certkeyName server_cacert –CA

       >set ssl service syslog_service -serverAuth ENABLED

    c) Por último, configuramos que se envíen los eventos syslog a ese virtual server:

       >add syslogaction sys_act <lb_vserver_ip> -loglevel all -transport TCP -serverPort 514

       >add syslogpolicy sys_pol true sys_act

       >bind syslogglobal -policyname sys_pol -priority 1

5.14 BACKUP

74. La utilidad de *backup* se encarga de realizar automáticamente el salvado de todos los directorios en los que se guardan ficheros modificados (por ejemplo: certificados, customizaciones, etc.), además de los de configuración propiamente dicha. La forma más sencilla de realizar un *backup* consiste en ejecutar el siguiente comando, tras salvar la configuración activa:

    >save ns config

    >create system backup [<fileName>] -level full -comment <string>

5.15 SERVICIOS DE SEGURIDAD

75. Citrix ADC proporciona multitud de funciones de seguridad, según la licencia empleada y el uso que se desee hacer de él. En el presente documento, Citrix ADC se presenta como solución de acceso seguro a red, con lo que algunas de las funcionalidades que aplican, según la configuración deseada, serían las presentadas a en los siguientes párrafos.

76. La funcionalidad SSL VPN (y a pesar de tener una categoría propia en el CCN), entraría también dentro de esta definición de acceso seguro. La configuración completa, y que depende de la arquitectura y funcionalidad deseada, se encuentra en https://docs.citrix.com/en-us/citrix-gateway/current-release.

77. Un caso particular de acceso seguro es *Unified Gateway*: es un portal único, en el cual se presentarán a un usuario todas sus aplicaciones web internas, virtualizadas con Citrix Virtual Apps and Desktops o VMWare Horizon View, aplicaciones web externas (por ejemplo SaaS), sitios accesibles por RDP, almacenamiento online, e incluso posibilidad de acceso SSL VPN si el usuario debe tener esa opción. Esto permite que un usuario tenga en portal único, personalizado, todo lo que pueda necesitar acceder para trabajar a diario. https://docs.citrix.com/en-us/citrix-gateway/current-release/unified-gateway.html.

78. En ambos casos anteriores, todas las capacidades de autenticación y autorización de la solución se encuentran en https://docs.citrix.com/en-us/citrix-adc/current-release/aaa-tm.html.

79. También en ambos casos, una parte fundamental de la solución para acceso seguro es la comprobación de la seguridad en el puesto cliente. La configuración de este motor puede encontrarse en https://docs.citrix.com/en-us/citrix-gateway/current-release/vpn-user-config/endpoint-policies.html y en https://docs.citrix.com/en-us/citrix-gateway/current-release/vpn-user-config/advanced-epa-policies.html.

80. Una función adicional de seguridad a utilizar en ocasiones es la capacidad de crear reglas de filtrado (ACL). Son reglas *stateful* similares a las de un firewall perimetral. https://docs.citrix.com/en-us/citrix-adc/current-release/networking/access-control-lists-acls.html.

6. FASE DE OPERACIÓN

81. En la pestaña Security de los secretos, se pueden configurar los siguientes ajustes La fase de operación de Citrix ADC no varía mucho frente a la de cualquier *appliance* o virtual *appliance* similar y los procedimientos mínimos son igualmente parecidos, y muy dependientes del entorno operativo y funcional en cada instalación, y entre los cuales podemos citar, a modo de ejemplo:

    - Comprobaciones de las alertas que el equipo envíe a sistemas de gestión (vía SNMP, o la propia consola de gestión y supervisión de Citrix ADC, llamada ADM -*Analytics and Management System*-, que se recomienda utilizar dada su extensa funcionalidad).
    - Auditoría de al menos los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.
    - Exportación de registros de auditoría a un servidor externo. Estos registros estarán protegidos de borrado y modificación no autorizada y solamente el personal de seguridad autorizado podrá acceder a ellos. Para ello deberá garantizarse un almacenamiento seguro con restricciones de acceso, cifrado y *backups* de duración al menos la estipulada por la regulación aplicable.
    - Actualización periódica del firmware, si no a la última versión disponible, al menos sí a una relativamente reciente y que incluya parches para vulnerabilidades consideradas de riesgo, en especial si pueden afectar a esa instalación concreta y las aplicaciones del entorno.
    - Comprobaciones periódicas del hardware y software para asegurar que no se ha introducido hardware o software no autorizado. El código fuente del código activo y su integridad deberá verificarse periódicamente y estará libre de software malicioso.
    - Es recomendable la revisión periódica (no necesariamente frecuente) de los informes de uso, para poder detectar a tiempo la posible necesidad de un *upgrade* de licencia para aumentar la capacidad de la solución, así como para detectar posibles anomalías que permitan deducir que hay algún problema a resolver.

7. CHECKLIST

82. Aquí mostramos las recomendaciones sobre la configuración de cada apartado:

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro de los equipos	☐	☐	
Registro de las licencias	☐	☐	
Actualización de firmware	☐	☐	Se detalla el proceso en un apartado posterior de Actualizaciones
Instalación inicial	☐	☐	
CONFIGURACIÓN			
Configuración mínima para administrar la solución	☐	☐	
Configuración FIPS (si aplica al *appliance* en concreto)	☐	☐	
Creación de usuarios de administración	☐	☐	
ADMINISTRACIÓN			
Uso de métodos seguros de administración	☐	☐	Configuración adicional se muestra en un apartado “Configuración de protocolos seguros”
Creación de roles de administración diferenciados	☐	☐	
Parámetros de securización de la administración (contraseñas, *timeouts*, etc.)	☐	☐	
Configuración de interfaces	☐	☐	
Configuración de algoritmos y claves de cifrado según la guía CCN-STIC-807 y las recomendaciones del CCN	☐	☐	
Gestión de certificados	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Acceso seguro a servidores de autenticación	☐	☐	
Sincronización horaria	☐	☐	
Actualizaciones de *firmware*	☐	☐	
Configuración SNMP	☐	☐	
Securización de la comunicación en configuración de alta disponibilidad	☐	☐	
Registro de eventos local y remoto de forma segura	☐	☐	
Backups	☐	☐	
Configuración de la funcionalidad	☐	☐	Se indican los apartados del manual de las funciones relacionadas con el acceso seguro

8. REFERENCIAS

[1] Despliegue de Citrix ADC como máquina virtual *https://docs.citrix.com/en-us/citrix-adc/13/deploying-vpx.html*

[2] Hoja de especificaciones de Citrix ADC en su versión virtual *https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-adc-vpx-data-sheet.pdf*

[3] Despliegue inicial de appliance físicos Citrix ADC *https://docs.citrix.com/en-us/citrix-adc/13/getting-started-with-citrix-adc/install-hardware.html*

[4] Autenticación externa de usuarios administradores *https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-config-external-user-authn-con.html*

[5] Autenticación con clave pública/privada para conexiones SSH *https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ssh-key-based-authentication.html*

[6] Configuración de políticas de administración granulares basadas en roles *https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-config-users-and-grps-tsk.html*

[7] Configuración de interfaces y VLANs *https://docs.citrix.com/en-us/citrix-adc/13/networking/interfaces.html*

[8] Distintos apartados para la configuración y gestión de certificados *https://docs.citrix.com/en-us/citrix-adc/current-release/ssl/ssl-certificates.html*

[9] Configuración de traps SNMP *https://docs.citrix.com/en-us/citrix-adc/13/system/snmp/generating-snmp-traps-on-citrix-adc.html*

[10] Configuración de Alta Disponibilidad *https://docs.citrix.com/en-us/citrix-adc/13/system/high-availability-introduction.html*

[11] Configuración completa de la funcionalidad de SSL VPN *https://docs.citrix.com/en-us/citrix-gateway/current-release*

[12] Configuración de la funcionalidad *Unified Gateway* *https://docs.citrix.com/en-us/citrix-gateway/current-release/unified-gateway.html*

[13] Configuración de las funciones de autenticación y autorización *https://docs.citrix.com/en-us/citrix-adc/current-release/aaa-tm.html*

[14] Configuración de la funcionalidad de escaneo de seguridad en el puesto cliente *https://docs.citrix.com/en-us/citrix-gateway/current-release/vpn-user-config/endpoint-policies.html*

[15] Más sobre la configuración de la funcionalidad de escaneo de seguridad en el puesto cliente *https://docs.citrix.com/en-us/citrix-gateway/current-release/vpn-user-config/advanced-epa-policies.html*

[16] Configuración de ACLs *https://docs.citrix.com/en-us/citrix-adc/current-release/networking/access-control-lists-acls.html*

9. ABREVIATURAS

ADC	*Application Delivery Controller*
ADM	*Application Delivery Management*
CA	*Certification Authority*
CCN	Centro Criptológico Nacional
CPD	Centro de Proceso de Datos
CRL	*Certificate Revocation List*
DSA	*Digital signature Algorithm*
EDCHE	*Elliptic curve Diffie Hellman Ephemeral*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
ENS	Esquema Nacional de Seguridad
GSLB	*Global Server Load Balancing*
HA	*High Availability*
IDS	*Intrusion Detection System*
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
FIPS	*Federal Information Processing Standard*
GUI	*Graphical User Interface*
HSM	*Hardware Security Module*
HTTP	*Hyper-Text Transfer Protocol*
HTTPS	*Hyper-Text Transfer Protocol Secure*
LDAP	*Lightweight Directory Access Protocol*
LOM	*Lights-Out Management*
NTP	*Network Time Protocol*
OCSP	*Online Certificate Status Protocol*
OID	*Object IDentifier*
RADIUS	*Remote Authentication Dial-In User Service*
RSA	*Rivest, Shamir, & Adleman*
SaaS	*Software as a Service*
SCP	*Secure CoPy*
SHA	*Secure Hash Algorithm*
SSH	*Secure SHell*
SSL	*Secure Sockets Layer*
SYSLOG	*SYStem LOGging Protocol*
TACACS	*Terminal Access Controller Access Control System*
TLS	*Transport Layer Security*
VLAN	*Virtual Local Access Network*
VPN	*Virtual Private Network*
WAF	*Web Application Firewall*