Guía de Seguridad de las TIC
CCN-STIC 1434

Procedimiento de empleo seguro
Sonicwall SMA

Mayo de 2022

MINISTERIO DE DEFENSA

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

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2022
NIPO: Pendiente de asignación

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

1. Los dispositivos SonicWall *Secure Mobile Access* (SMA) brindan acceso seguro, incluido el acceso sin cliente a aplicaciones web, acceso a aplicaciones cliente/servidor y uso compartido de archivos, a empleados, socios comerciales y clientes. Todo el tráfico es cifrado usando Transport Layer Security o TLS (anteriormente denominado Secure Sockets Layer (SSL)) para protegerlo de usuarios no autorizados.
2. El dispositivo hace que las aplicaciones estén disponibles desde una variedad de métodos de acceso, incluido un sitio web estándar, navegador, una aplicación de cliente (por ejemplo, *Connect Tunnel*) o una aplicación de dispositivo móvil, en una amplia gama de plataformas incluidos Windows, Mac, Linux y dispositivos móviles.
3. Puede utilizar el dispositivo para crear un:
    - VPN de acceso remoto que permite a los empleados remotos acceder de forma segura a aplicaciones como el correo electrónico a través de Internet.
    - VPN para *partners* comerciales que proporciona a los proveedores designados acceso a una aplicación de negocio a través de Internet.
4. El control de acceso granular del dispositivo le permite definir políticas y controlar el acceso hasta el usuario y nivel de recursos. La administración de políticas y la configuración del dispositivo son rápidas y sencillas con el sistema basado en la consola de administración basada en Web.

2 OBJETO Y ALCANCE

5. El objeto del presente documento es facilitar la instalación y configuración segura de los dispositivos de **Sonicwall Secure Mobile Access (SMA) con la versión de software 12.1**, junto con el aseguramiento del entorno en el que se despliega.
6. Los *appliances* físicos correspondientes a la versión 12.1 de SMA son:
    - SMA 6210.
    - SMA 7210.
7. El *appliance* virtual correspondiente a la versión 12.1 es SMA 8200v.

3 ORGANIZACIÓN DEL DOCUMENTO

8. El documento está estructurado en los siguientes apartados:

   a) Apartado **1**: Descripción de la familia de productos SMA.

   b) Apartado **2**: Alcance del documento.

   c) Apartado **3**: Organización del documento.

   d) Apartado **4**: Fase de despliegue en instalación.

   e) Apartado **5**: Recomendaciones en la fase de configuración y administración.

   f) Apartado **6**: Recomendaciones en la fase de operación.

   g) Apartado **7**: Checklist de las tareas a realizar y el estado de cada una de ellas.

   h) Apartado **8**: Referencias (links de consulta) usadas en este documento, así como el link general de acceso a información de producto de Sonicwall.

   i) Apartado **9**: Abreviaturas usadas en este documento.

4 FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. El dispositivo se entrega en un embalaje con el número de serie en un lateral, con un sello de Sonicwall precintando la caja. Los servicios contratados se entregan de forma electrónica, con las claves de activación y números de serie correspondientes, para ser registrados y activados a través del portal de gestión "*Mysonicwall*" (https://www.mysonicwall.com/).
10. **Se deberá verificar que el sello de precintado está intacto**, en caso contrario, contactar con el servicio de soporte de SonicWall.
11. Toda la documentación y manuales relativos a los productos, pueden encontrarse en el siguiente enlace:

    https://www.sonicwall.com/support/technical-documentation/?language=English
12. El embalaje de cada dispositivo incluye:
    - El *appliance* o dispositivo *hardware*.
    - Un adaptador de corriente (fuente de alimentación).
    - Un cable de corriente.
    - Un cable *ethernet*.
    - Un cable de consola.
    - La guía *Quick Start Guide*.
13. En caso de faltar algún componente, se recomienda contactar con el servicio de soporte de SonicWall desde:

    https://www.sonicwall.com/en-us/support/contact-support
14. Los dispositivos "*Zero-Touch*" son más fáciles de configurar y de poner en marcha, el siguiente logo certifica esta característica:

Ilustración 1. Logo "Zero-Touch".

15. El detalle de los pasos necesarios para la puesta en marcha de dispositivos con esta característica se puede consultar en el siguiente enlace:

    https://www.sonicwall.com/techdocs/pdf/zero-touch-deployment-guide.pdf
16. A modo de resumen, los pasos necesarios para la puesta en marcha de cualquier dispositivo se recogen en el siguiente diagrama de flujo:

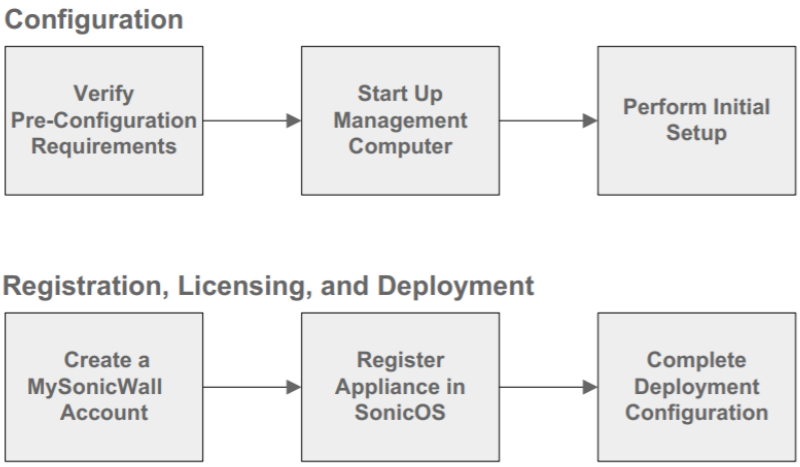

Ilustración 2. Pasos puesta en marcha dispositivos.

17. Las guías de puesta en marcha de los distintos dispositivos se pueden consultar en el siguiente enlace.

4.2 ENTORNO DE INSTALACIÓN SEGURO

18. Es recomendable que el acceso físico a los dispositivos esté restringido y limitado a un conjunto de personas que posean una autorización expresa.
19. En caso de que el dispositivo se desee instalar en un armario rack, se encuentran disponibles kits de enracado. Para obtenerlos, contactar con el servicio de soporte de SonicWall desde:

    https://www.sonicwall.com/en-us/support/contact-support

20. **Se debe instalar el dispositivo en una ubicación donde pueda conectarse a los recursos de su red**, incluidos:
    - Servidores de aplicaciones y servidores de archivos, incluidos servidores Web o Windows, y aplicaciones cliente/servidor.
    - Repositorios de autenticación externos (como un servidor LDAP, *Microsoft Active Directory* o RADIUS).
    - Uno o más servidores del Sistema de nombres de dominio (DNS).
    - Opcionalmente, un servidor WINS (servicio de nombres de Internet de Windows). Esto es necesario para explorar redes de Windows usando *WorkPlace*.
21. El dispositivo SonicWall SMA no proporciona capacidades completas de firewall, por lo que se recomienda su protección detrás de un firewall.

4.3 CONSIDERACIONES PREVIAS

22. Todos los dispositivos SonicWall SMA se pueden configurar en una configuración de interfaz doble o de interfaz única. Adicionalmente incluyen interfaces de red que se pueden configurar para usar un balanceador de carga externo.

- Configuración *Dual-Home* (interfaces internas y externas): una interfaz de red se usa para el tráfico externo (es decir, hacia y desde Internet), y la otra interfaz se usa para el tráfico interno (hacia y de su red corporativa).

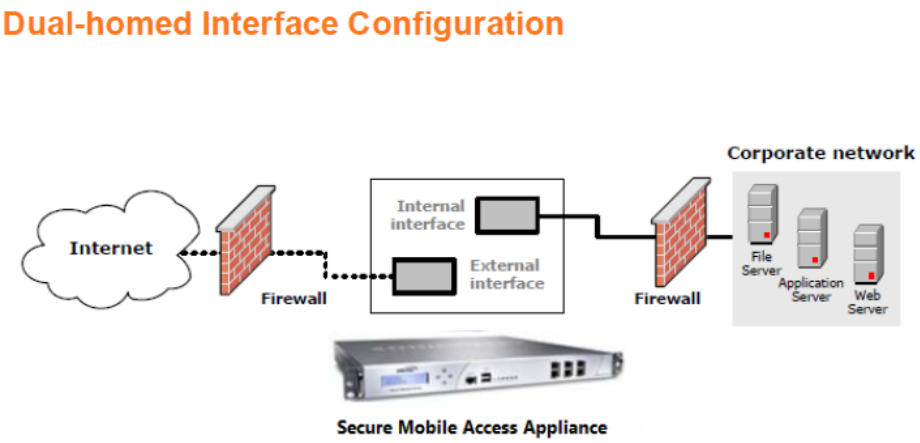

Ilustración 3. Configuración interfaz Dual-Homed

- Configuración de interfaz *Single-Home*: se utiliza una interfaz de red única para el tráfico interno y externo. El dispositivo generalmente se instala en la zona desmilitarizada (o DMZ, también conocida como red perimetral).

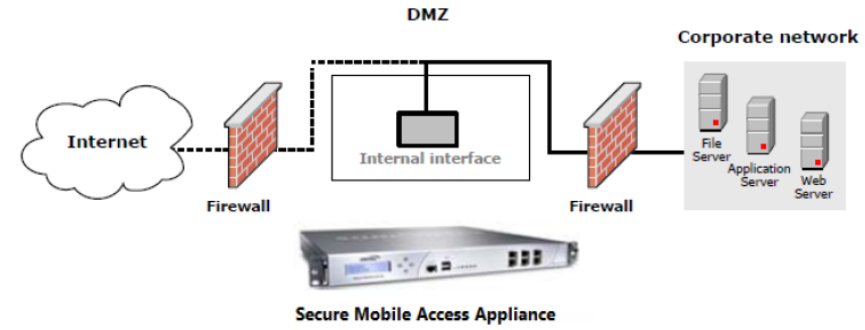

Ilustración 4. Configuración interfaz Single-Homed.

23. En ambas configuraciones, las solicitudes entrantes a los servicios de *Secure Mobile Access*, incluido el tráfico HTTP/S para el servicio de proxy web, se envían a través del puerto 80 (HTTP) y el puerto 443 (HTTPS). El tráfico del agente *OnDemand* siempre se envía a través del puerto 443. Debido a que la mayoría de las redes están configuradas para habilitar el tráfico a través de estos puertos, no se debería necesitar reconfigurar los cortafuegos en la red.
24. **Se recomienda también permitir ciertas comunicaciones desde los firewalls del entorno**:

    - **Firewall externo**. Para un acceso seguro al dispositivo desde un navegador web u *OnDemand*, debe asegurarse de que los puertos 80 y 443 estén abiertos en los firewalls de su sitio; consultar la siguiente tabla. Abrir el

firewall para permitir el acceso SSH es opcional, pero puede ser útil para realizar tareas administrativas desde un sistema remoto.

Traffic Types And Ports Used By SMA On External Network

Traffic type	Port/protocol	Usage	Required?
HTTP	80/tcp	Unencrypted network access	Y
HTTPS	443/tcp	Encrypted network access	Y
SSH	22/tcp	Administrative access to the appliance	
ESP	4500/UDP	Enable ESP encapsulation of tunnel network traffic	

Ilustración 5. Tráfico firewall externo.

- **Firewall Interno**. Si se dispone de un firewall en la red interna, es posible que se deba ajustar la política para abrir puertos para aplicaciones de *back-end* con las que debe comunicarse el dispositivo. Además de abrir puertos para servicios de red estándar, como DNS y correo electrónico, es posible que se deba modificar la política de firewall antes de que el dispositivo pueda acceder a los servicios que se muestran en la siguiente tabla:

Traffic Types And Ports Used By SMA On Internal Network

Traffic type	Port/protocol	Usage
Microsoft networking	• 138/tcp and 138/udp • 137/tcp and 137/udp • 139/udp • 162/snmp • 445/smb	Used by WorkPlace to perform WINS name resolution, browse requests, and access file shares
LDAP (unencrypted)	389/tcp	Communicate with an LDAP directory or Microsoft Active Directory
LDAP over SSL (encrypted)	636/tcp	Communicate with an LDAP directory or Microsoft Active Directory over SSL
RADIUS	1645/udp or 1812/udp	Communicate with a RADIUS authentication server
NTP	123/udp	Synchronize the appliance clock with an NTP server
Syslog	514/tcp	Send system log information to a syslog server
SNMP	161/udp	Monitor the appliance from an SNMP management tool

Ilustración 6. Tráfico firewall interno.

4.4 INSTALACIÓN

25. Una vez recibido el producto, conectar el cable al puerto marcado como *Puerto Consola*. Utilizar una aplicación de emulación de terminal (como *PuTTY*), con los siguientes parámetros de interfaz *serial line*:

- *115,200 baud.*
- *8 data bits.*
- *1 stop bit.*
- *no parity.*
- *no flow control.*

26. En el *login*, acceder con el nombre de usuario *root*. Esta cuenta deberá deshabilitarse posteriormente, tal como se ve en el apartado 5.4.3 PARÁMETROS DE SEGURIDAD PARA ADMINISTRADORES.
27. Introducir la información de las interfaces de red y utilizar el comando *logout* para salir.
28. Una vez llevados a cabo los pasos iniciales a través de CLI, acceder a la interfaz gráfica AMC (*Appliance Management Console*) en la *url https://<IP address>:8443*, donde la dirección IP corresponde con la configurada en el paso anterior. Se iniciará el *Wizard* de configuración.
29. En la página *Basic Settings*, indicar la zona horaria e introducir la contraseña para la cuenta *Admin*. Continuar rellenando la información solicitada por el *Wizard*. Hacer clic en *Finish* una vez terminado.

4.5 REGISTRO Y LICENCIAS

30. El producto requiere la instalación de licencias de uso para su correcto funcionamiento.
31. El detalle de las distintas licencias disponibles, así como la forma de configurarlas en los dispositivos, se puede consultar en el apartado *Sowtware Licenses* de la guía *SonicWall Secure Mobile Access 12.1 Administration Guide – REF16*.

5 FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

32. El producto permite la configuración de un modo de operación seguro, pero este no se encuentra configurado por defecto. Por lo tanto, **se deberá configurar el producto para funcionar en este modo**. Cuando se habilita, se eliminarán las claves y certificados del dispositivo (ver apartado 5.7 GESTIÓN DE CERTIFICADOS), también se permitirán solo cifrados seguros.
33. Para llevar a cabo la activación del modo seguro, seguir los siguientes pasos:
    - Ir a *System Configuration* > *General Settings*.
    - Hacer clic en *Edit* bajo *FIPS Security*.
    - Activar la casilla *Enable FIPS mode* y hacer clic en *Save*.

5.2 AUTENTICACIÓN

34. El producto requiere la autenticación de usuarios para el acceso a las funcionalidades, como las conexiones VPN. También requiere la autenticación de los usuarios administradores para el acceso a la gestión.
35. Los mecanismos de autenticación utilizados por el producto son los siguientes:
    - Credenciales locales, mediante usuario y contraseña. Dichas credenciales se almacenan en el producto. Para la creación y gestión de usuarios locales, ver apartado 5.4.2 GESTIÓN DE USUARIOS LOCALES.
    - Servidor de autenticación externo. Mediante la integración con distintos servidores de autenticación. Para la configuración y gestión de dichos servidores, ver apartado 5.3 SERVIDORES DE AUTENTICACIÓN EXTERNOS.
36. Se recomienda **hacer uso únicamente de la autenticación local** como método de autenticación de usuarios.

5.3 SERVIDORES DE AUTENTICACIÓN EXTERNOS

37. Para configurar un servidor externo de autenticación, se deben seguir los siguientes pasos:
    - Desde la consola AMC, ir a *Authentication Servers* y hacer clic en *New*.
    - En la página que se abrirá, seleccionar el tipo de servidor deseado (por ejemplo, LDAP o RADIUS).
    - Seleccionar el tipo de credenciales que se desea utilizar: usuario/contraseña, certificados o *token*.
    - Hacer clic en *Continue*.
    - En función del tipo de servidor, en las siguientes pantallas se deben rellenar los datos específicos.
    - Por último, guardar los cambios.

38. El detalle de configuración de los servidores de autenticación externos se puede consultar el apartado *Managing User Authentication* en la guía *SonicWall Secure Mobile Access 12.1 Administration Guide – REF16.*

5.4 ADMINISTRACIÓN DEL PRODUCTO

5.4.1 ADMINISTRACIÓN LOCAL Y REMOTA

39. El producto dispone de las siguientes interfaces para la administración:

    - Administración local por consola. Todos los dispositivos incluyen un puerto dedicado de consola por el que se puede acceder a la configuración por CLI.
    - Administración remota de tipo CLI mediante SSH. No se recomienda hacer uso de este método, por lo que **se deberá deshabilitar tal como se indica a continuación**.
    - Administración remota mediante AMC (*Appliance Management Console*). **Se recomienda configurar y gestionar el producto haciendo uso de esta interfaz web**. El acceso mediante AMC hace uso de TLSv1.2 por defecto y no requiere ninguna configuración adicional.

40. Para deshabilitar el acceso mediante SSH, seguir los siguientes pasos:

    - Desde AMC, ir a *System Configuration > Services*.
    - En el apartado *SSH*, seleccionar *Configure > Select > Disable SSH*.

5.4.2 GESTIÓN DE USUARIOS LOCALES

41. Para poder crear y autenticar usuarios locales, primero **debe configurarse el producto para hacer uso del servidor local de autenticación**:

    - Desde AMC, ir a *System Configuration > Authentication Servers*.
    - Hacer clic en *New*.
    - Seleccionar *Local Users* en el apartado *Local users storage*. Hacer clic en *Continue*.
    - En el campo *Name*, escribir *local-auth*.
    - **Configurar la política de contraseñas** para los usuarios locales en el apartado *Password Policy*.
        - En la casilla *Password are X to X characers in lengh*, indicar una longitud mínima de 12 caracteres y una longitud máxima elevada.
        - Activar todas las casillas bajo *Passwords must contain at least one of the following*. De tal forma que las contraseñas deberán estar formadas por, al menos, una letra mayúscula, una minúscula, un número y un símbolo.
    - En el campo *One-Time Passwords*, seleccionar *Use one-time passwords with this authentication server*. **Se recomienda hacer uso de esta opción para utilizar autenticación de dos factores mediante contraseñas de un solo uso**. El detalle de configuración de las contraseñas de un solo uso se puede

consultar en el apartado *Using One-Time Passwords for Added Security* de la guía *SonicWall Secure Mobile Access 12.1 Administration Guide – REF16*.

- Hacer clic en *Save*.
- Para hacer uso del servidor configurado, ir a *System Configuration > General Settings*. Hacer clic en el botón *Authentication.*
- En el desplegable *Authentication Server*, seleccionar *local-auth*.
- Hacer clic en *Save* y aplicar los cambios.

42. Adicionalmente el administrador del sistema **deberá exigir a los usuarios la siguiente política de contraseñas de manera procedural**:

    - No reutilizar las últimas 5 contraseñas.
    - Cambiar las contraseñas cada 60 días.
    - No permitir un nuevo cambio de contraseñas antes de pasados 10 días.

43. Un usuario es una persona que necesita acceso a los recursos de la red y un grupo es una colección de usuarios. Una vez creados los usuarios o grupos en el dispositivo, se puede hacer referencia a ellos en una regla de control de acceso para permitir o denegar el acceso a los recursos. Para ello, ver apartado 5.13.1 RECURSOS Y REGLAS DE CONTROL DE ACCESO.

44. El detalle de creación y configuración de los usuarios y grupos se puede consultar el apartado *Managing Users and Groups* en la guía *SonicWall Secure Mobile Access 12.1 Administration Guide – REF16.*

45. Los usuarios creados tan solo tendrán permiso de acceso a las funcionalidades del producto, pero no podrán llevar a cabo ni ver las configuraciones del mismo. Para permitir a un usuario ver y modificar la configuración, se debe promover a este a Administrador.

46. Para configurar un usuario como administrador:

    - Desde AMC, ir a *System Configuration > General Settings*.
    - Hacer clic en *Administrators* y en *New*. Seleccionar *Administrator…*
    - Introducir el nombre de usuario y rol deseado y hacer clic en *Save*.

47. El producto hace uso de roles para determinar los distintos permisos que tendrán los usuarios administradores. Los roles por defecto del producto son los siguientes:

    - *Super Admin*. Tiene acceso de lectura/escritura a todas las configuraciones de AMC.
    - *Security Admin*. Tiene acceso de lectura/escritura a la administración de seguridad y las páginas de monitorización en AMC. Tiene acceso de lectura a las páginas de acceso al sistema.
    - *System Admin*. Tiene acceso de lectura/escritura a las páginas de acceso al Sistema y monitorización. Tiene acceso de lectura a las páginas de seguridad.

48. A su vez, pueden crearse y modificarse los roles de usuario para restringir los permisos de los distintos Administradores. Para ello:

    - Desde AMC, ir a *System Configuration > General Settings*.
    - Hacer clic en *Administrators* y en *Edit.* Hacer clic en *Roles*.
    - Hacer clic en *New*. Asignar un nombre y una descripción.

- Seleccionar los permisos de los que dispondrá dicho rol y hacer clic en *Save*.

49. El detalle de configuración de los administradores y roles se puede consultar el apartado *Managing Administrator Accounts and Roles* en la guía *SonicWall Secure Mobile Access 12.1 Administration Guide – REF16.*

5.4.3 PARÁMETROS DE SEGURIDAD PARA ADMINISTRADORES

50. Una vez creados los administradores, **se deben configurar los parámetros de sesión de los administradores del producto**, para ello se deben seguir los siguientes pasos:

- Desde AMC, ir a *System Configuration > Management*.
- Modificar la URL, añadiendo al final *?advanced=1* y pulsar en *Enter*.
- Ir a *Configure…,* en *Advanced > Configuration Extension*.
- Hacer clic en *New*.
- Añadir una nueva extensión *MGMT_ALLOW_MODIFY_ADMIN*, con valor *TRUE*. De esta forma se permite el acceso CLI a la cuenta por defecto *Admin* mediante SSH. De lo contrario, solo la cuenta *root* podría acceder al CLI.
- Añadir una nueva extensión *DISALLOW_ROOT_ACCESS* con valor *TRUE*. De esta forma se deshabilita el uso de la cuenta de usuario *root*.
- Añadir una nueva extensión *ADMINISTRATOR_ACCOUNT_LOCKOUT_ATTEMPTS* con valor 3. De esta forma tras tres intentos de acceso fallidos, se bloqueará la cuenta de administrador.
- Añadir una nueva extensión *ADMINISTRATOR_ACCOUNT_LOCKOUT_SECONDS* con valor de 300 segundos (5 minutos). De esta forma, tras los intentos fallidos configurados, se bloqueará la cuenta de administrador durante el tiempo configurado.
- Añadir una nueva extensión *AMC_SESSION_TIMEOUT_SECS* para configurar el tiempo de inactividad de las sesiones. Se recomienda un valor de 300 segundos (5 minutos).
- Hacer clic en *OK* y después en *Save*.

5.4.4 CONFIGURACIÓN DEL BANNER DE ACCESO

51. **Se debe configurar el mensaje de aviso antes de la autenticación en el producto**:

- Desde AMC, ir a *System Configuration > Management*.
- Modificar la URL, añadiendo al final *?advanced=1* y pulsar en *Enter*.
- Ir a *Configure…,* en *Advanced > Configuration Extension*.
- Hacer clic en *New*.
- Añadir una nueva extensión *ACCEPTABLE_USE_BANNER* e introducir el mensaje que desea mostrarse.
- Hacer clic en *OK* y en *Save*.

5.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

52. Para evitar el uso de interfaces y servicios inseguros en el producto, **se deben desactivar manualmente SNMP, SMTP y SSH**. Para ello, seguir los siguientes pasos:

    - Desde AMC, ir a *System Configurations > Services*.
    - Deshabilitar los servicios SNMP, SMTP y SSH, desde *Configure > Select > Disable Nombre_servicio*.

5.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

53. Para asegurar un uso seguro de TLS en todas las comunicaciones del producto, **se debe configurar el protocolo para utilizar únicamente la versión 1.2 y parámetros seguros**.

    - Desde AMC, ir a *System Configuration > Management*.
    - Modificar la URL, añadiendo al final *?advanced=1* y pulsar en *Enter*.
    - Ir a *Configure…,* en *Advanced > Configuration Extension*.
    - Hacer clic en *New*.
    - Añadir un nuevo parámetro *MGMT_STRICT_CERTIFICATE_VALIDATION* con valor *TRUE*. De esta forma, se fuerza la verificación de la CA del certificado, así como el estado de revocación del mismo.
    - Hacer clic en *Ok* y después en *Save*.
    - Ir a *System Configuration > SSL Settings*.
    - En *SSL Encryption* hacer clic en *Edit.*
    - Seleccionar ***TLS version 1.2 only*** en *SSL Protocols*.
    - En *SSL Ciphers*, seleccionar las siguientes *cipher suites*:
        - TLS_RSA_WITH_AES_128_CBC_SHA
        - TLS_RSA_WITH_AES_256_CBC_SHA
        - TLS_RSA_WITH_AES_128_CBC_SHA256
        - TLS_RSA_WITH_AES_256_CBC_ SHA256
    - Por último, hacer clic en *Save*.

5.7 GESTIÓN DE CERTIFICADOS

54. El detalle de configuración de los certificados se puede consultar en el apartado *Server Certificates* de la guía *SonicWall Secure Mobile Access 12.1 Administration Guide – REF16*.

55. **Deberán seguirse los siguientes pasos generales**:

    - Importar el certificado de la CA que se utilizará para generar el certificado de servidor. Especificar el uso de *Web server connection* y *OSCP response verification*.
    - Crear un CSR (*Certificate Signing Request*). **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 y algoritmo de firma SHA-384 o SHA-256.
  - Tipo d clave RSA, con una longitud de clave de 3072 bits o superior.

- Importar el certificado de servidor una vez recibido.
- Una vez importados los certificados, ir a *System Configuration > SSL Settings > SSL Certificates > Edit*. En la tabla *Certificate Usages*, seleccionar el uso de los certificados:
  - *AMC*: utilizado en las comunicaciones entre los administradores y a consola de gestión web.
  - *Default*: utilizado en el resto de conexiones del producto, por ejemplo, las conexiones VPN.

5.8 SINCRONIZACIÓN HORARIA

56. **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*.

57. El producto permite indicar de forma local la hora del dispositivo, así como la zona horaria. Para ello:

    - Desde AMC, ir a *System Configuration > General Settings*.
    - En el área *Appliance Options*, hacer clic en *Edit*.
    - En el área *Date/Time*, con el botón *Change* bajo *Time Zone* se puede modificar la zona horaria.
    - En el área *Date/Time*, con el botón *Change* bajo *Current Time* se puede modificar la fecha y hora del producto.

58. Adicionalmente se permite configurar la sincronización con un servidor de tiempo mediante NTP. Para ello seguir los siguientes pasos:

    - Desde AMC, ir a *System Configuration > Services*.
    - En el área *Network services*, hacer clic en *Configure* sobre NTP. Se abrirá la página de configuración.
    - Activar la casilla *Enable NTP*. Introducir los datos del servidor de tiempo.

59. No se permite el uso de claves de autenticación para el servicio NTP. Debido a esto, **se recomienda utilizar sólo servidores de tiempo ubicados en la red interna de la organización para evitar posibles ataques**.

60. El detalle de configuración de los servidores de autenticación externos se puede consultar el apartado *Configuring Time Settings* en la guía *SonicWall Secure Mobile Access 12.1 Administration Guide – REF16.*

5.9 ACTUALIZACIONES

61. El detalle sobre el proceso de actualización de los dispositivos se puede consultar en la guía *SonicWall Secure Mobile Access 12.1 Upgrade Guide – REF14*. Este

proceso deberá realizarse siempre de forma manual por parte de un usuario administrador.

5.10 ALTA DISPONIBILIDAD

62. El producto permite realizar un despliegue en alta disponibilidad haciendo uso de CMS (*Central Management Server*). El despliegue consta de varios *appliance* SMA bajo un mismo nombre para asegurar la disponibilidad para los usuarios finales.
63. El detalle de configuración en alta disponibilidad se puede consultar en la guía *SonicWall Secure Mobile Access 12.1 Central Management Server with Global High Availability – REF9*.

5.11 AUDITORÍA

64. El producto permite generar registros de auditoría para todos los servicios disponibles. Estos registros se almacenarán, por defecto, localmente. En caso de llenarse el almacenamiento, de forma automática se realiza la rotación de los registros, eliminando los más antiguos para permitir la creación de los más recientes.
65. El detalle de configuración de los registros de auditoría se puede consultar el apartado *System Logging and Monitoring* en la guía *SonicWall Secure Mobile Access 12.1 Administration Guide – REF16.*
66. Debido al espacio limitado de almacenamiento local, **se recomienda realizar el envío de los registros a un servidor de auditoría externo mediante *Syslog***. Para ello:
    - Desde AMC, ir a *System Configuration > Maintenance*.
    - Modificar la URL, añadiendo al final *?advanced=1* y pulsar en *Enter*.
    - Ir a *Configure…,* en *Advanced > Configuration Extension*.
    - Añadir un nuevo parámetro *LOGGING_SECURE_SYSLOG* y asignarle un valor *TRUE*. De esta forma se fuerza el uso de TLSv1.2 en las comunicaciones con el servidor *Syslog*.
    - Hacer clic en *OK* y después en *Save*.
    - Ir a *Monitoring > Logging.*
    - Bajo *Syslog Configuration*, añadir la dirección IP y el puerto del servidor externo al que se desean enviar los registros.
    - Seleccionar como protocolo TCP.
    - Hacer clic en *Save*.

5.12 COPIAS DE SEGURIDAD

67. **Se recomienda realizar copias de seguridad periódicas de la configuración del producto** para, en caso de ser necesario, poder recuperar el estado de la máquina. Para ello es posible crear copias de seguridad locales o exportarlas a una ubicación externa.

68. Para crear una copia local:

    - Desde AMC, ir a *Maintenance*.
    - En el área *System Configuration*, hacer clic en *Import/export*.
    - Hacer clic en *New* en la lista *Saved configurations*.
    - Incluir una descripción de la copia que se va a realizar.
    - Hacer clic en *Save*.
    - Desde el mismo menú, seleccionar una copia y hacer clic en *Restore* para restaurarla.

69. **Se recomienda realizar la exportación, para una mayor seguridad, a una ubicación externa**. Para exportar las configuraciones a una ubicación segura:

    - Desde AMC, ir a *Maintenance*.
    - En el área *System Configuration*, hacer clic en *Import/export*.
    - Hacer clic en *Export*, se abrirá una nueva ventana. Seleccionar la ubicación en la que se quiere almacenar y hacer clic en *OK*.
    - Esto guarda el fichero de copia de seguridad en el disco duro del appliance físico del producto. Deberá transportarse de forma segura a una ubicación externa, por ejemplo, mediante SCP o SFTP.
    - Para importar y restaurar una copia de seguridad, hacer clic en *Browe*, seleccionar el fichero y hacer clic en *Import*.

5.13 FUNCIONES DE SEGURIDAD

5.13.1 RECURSOS Y REGLAS DE CONTROL DE ACCESO

70. Los recursos hacen referencia a elementos existentes en la red, de tal forma que el producto puede permitir/denegar el acceso a los usuarios a estos elementos. Están divididos en cuatro tipos:

    - Recursos integrados. Se dispone de varios recursos integrados en el dispositivo. Estos recursos no pueden eliminarse.
    - Recursos web. Estos incluyen aplicaciones o servicios basados en la web a los que se accede mediante HTTP o HTTPS. Algunos ejemplos son *Microsoft Outlook Web Access* y otros programas de correo electrónico basados en la web, portales web y servidores web estándar.
    - Recursos cliente/servidor. Son aplicaciones que se ejecutan sobre TCP/IP (incluidas las aplicaciones que utilizan UDP). Algunos ejemplos son las aplicaciones *thin-client*, como Citrix; las aplicaciones cliente/servidor completas, como Microsoft Outlook; Lotus Notes; SAP; y servidores de terminales.
    - Recursos de compartición de ficheros. Cuando los usuarios se conectan a *WorkPlace*, tienen acceso a los recursos del sistema de archivos que se configuren. Estos pueden incluir ordenadores que contienen carpetas y archivos compartidos y servidores de red de Windows. Se puede definir un recurso compartido del sistema de archivos específico escribiendo una ruta UNC, o puede definir un dominio de Windows completo:

71. Para añadir nuevos recursos al producto, seguir los siguientes pasos:
    - Desde AMC, ir a *Security Administration > Resources*.
    - Hacer clic en *New* y seleccionar el tipo de recurso que se quiere añadir. Se abrirá una nueva página.
    - Introducir los datos correspondientes. Finalmente, hacer clic en *Save*.
72. El detalle de configuración de los recursos se puede consultar el apartado *Creating and Managing Resources* en la guía *SonicWall Secure Mobile Access 12.1 Administration Guide – REF16.*
73. Una vez creados los recursos, las reglas de control de acceso permiten controlar los recursos que se encuentran disponibles para los distintos usuarios y grupos. Las reglas existentes se pueden consultar en AMC, desde *Security Administration > Access Control*.
74. Para configurar estas reglas, se deben seguir los siguientes pasos:
    - Desde AMC, ir a *Security Administration > Access Control.*
    - Hacer clic en *New*, se abrirá una nueva página.
    - En el parámetro *Position*, se define el orden de las reglas, de tal forma que aquellas con un número menor, se verificarán primero. Configurar el resto de parámetros acorde a lo que se necesite.
    - La pestaña *Advanced*, permite configurar parámetros adicionales, como el tipo de agente al que aplican las restricciones.
75. El detalle de configuración de las reglas de control de acceso se puede consultar el apartado *Access Control Rules* en la guía *SonicWall Secure Mobile Access 12.1 Administration Guide – REF16.*

5.13.2 COMUNIDADES Y DOMINIOS

76. Para permitir una mayor granularidad en el acceso de los usuarios, además de los usuario y grupos, el producto dispone de comunidades y dominios. Estos permiten organizar con mayor detalle los usuarios, asignando accesos específicos en función del dominio o comunidad al que pertenecen.
77. Las comunidades son conjuntos de usuarios que permiten determinar el método de acceso y los agentes desplegados a los distintos miembros al acceder a un dominio. Los dominios (*Realms*) hacen referencia a un servidor de autenticación determinado y permite determinar los agentes que se provisionan a los usuarios y si se imponen restricciones adicionales.
78. Haciendo uso de estas características, se puede denegar el acceso en función de la seguridad del dispositivo final utilizado para la conexión.
79. El detalle de configuración de comunidades y dominios se puede consultar el apartado *Configuring Realms and Communities* en la guía *SonicWall Secure Mobile Access 12.1 Administration Guide – REF16.*

5.13.3 PARÁMETROS DE SEGURIDAD DE LAS VPN

80. Se pueden configurar los parámetros específicos de las conexiones VPN. Estos se configuran desde AMC:

    - Ir a la *Comunidad* por defecto o, en caso de haber configurado comunidades adicionales, a la comunidad deseada.
    - Ir a *Access Methods > Network Tunnel Client Settings*.
    - Configurar los parámetros deseados.
    - En el área *Session Termination*, **se recomienda activar la casilla *Limit session lenth to credential lifetime***. De esta forma, tras el tiempo configurado en el parámetro *Credential lifetime*, la sesión terminará y el usuario se deberá reautenticar.
    - En el área *Advanced*, **se recomienda activar la casilla *Enable ESP encapsulation of tunnel network traffic*, con la opción *Use for all network traffic***.
    - Finalmente hacer clic en *Ok*.

81. **Se recomienda también configurar la VPN para obligar a que todo el tráfico de los clientes remotos pase a través del túnel VPN (*full tunneling*)**. Para ello:

    - Ir a *Realms > Configure Community > Tunnel Access*. Seleccionar el dominio (*Realm*) y comunidad (*Community*) deseados.
    - En el apartado *Redirection mode*, seleccionar la casilla *Redirect All*.
    - Hacer clic en *Ok*.

82. El detalle de configuración de las VPN se puede consultar en el apartado *Configuring Tunnel Client Settings* de la guía *SonicWall Secure Mobile Access 12.1 Administration Guide – REF16.*

5.13.4 ENDPOINT CONTROL

83. El producto dispone de compatibilidad con *Endpoint Control*. Este se puede utilizar para proteger los datos de la organización cuando se acceda desde entornos remotos. Esta funcionalidad permite:

    - Verificar el entorno del usuario.
    - Eliminar los datos del usuario de un dispositivo final después de finalizar la sesión.
    - Controlar el acceso a los recursos sensibles.

84. El detalle de configuración de *Endpoint Control* se puede consultar en el apartado *End Point Control* de la guía *SonicWall Secure Mobile Access 12.1 Administration Guide – REF16.*

6 FASE DE OPERACIÓN

85. El correcto funcionamiento del producto requiere de unas características que deben estar presentes en el entorno operacional:

- El producto debe contar con las últimas actualizaciones de seguridad para preservar al mismo de amenazas y vulnerabilidades conocidas.
- Se deben mantener y analizar los registros de auditoría. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
- Se deben gestionar correctamente los certificados utilizados, actualizándolos cuando sea necesario, por ejemplo, al expirar.
- Se deben realizar copias de seguridad de manera periódica.

7 CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la integridad del paquete	☐	☐	
Registro de licencias	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Activación del modo seguro	☐	☐	
ADMINISTRACIÓN DEL PRODUCTO			
Configuración del servidor de autenticación local	☐	☐	
Configuración de la política de contraseñas	☐	☐	
Configuración de los parámetros de sesión	☐	☐	
Creación de usuarios y configuración de los administradores	☐	☐	
CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS			
Deshabilitación de SSH, SNMP y SMTP	☐	☐	
CONFIGURACIÓN DE PROTOCOLOS SEGUROS			
Configuración de TLSv1.2	☐	☐	
GESTIÓN DE CERTIFICADOS			
Importar CA, crear CSR e importar el certificado de servidor	☐	☐	
SINCRONIZACIÓN HORARIA			
Configuración de la sincronización de la hora de los sistemas	☐	☐	
SINCORNIZACIÓN			
Configuración de un servidor de hora NTP	☐	☐	
COPIAS DE SEGURIDAD			

ACCIONES	SÍ	NO	OBSERVACIONES
Creación de los backups	☐	☐	
AUDITORÍA			
Configuración del envío de los logs a un servidor *Syslog*	☐	☐	

8 REFERENCIAS

86. El link principal de soporte de Sonicwall contiene acceso a toda la documentación técnica, tablas de ciclo de vida de producto, a la comunidad de Sonicwall y a tutoriales: https://www.sonicwall.com/support/

REF1 Página de acceso a Capture Security Center
https://cloud.sonicwall.com/

REF2 Página de acceso a MySonicWall.
http://www.mysonicwall.com/

REF3 Guía de configuración rápida SMA en ESXi.
https://www.sonicwall.com/techdocs/pdf/sma_1000-12-4-esxi_gsg.pdf

REF4 Guía de configuración rápida SMA en Hyer-V.
https://www.sonicwall.com/techdocs/pdf/sma_1000-12-4-hyperv_gsg.pdf

REF5 Guía de instalación en Red Hat / Ubuntu-KVM/QEMU
https://www.sonicwall.com/support/technical-documentation/docs/sma_1000-12-4-kvm_gsg//Content/Installing_KVM/installing-kvm-redhat.htm

REF6 Guía de administración
https://www.sonicwall.com/support/knowledge-base/initial-setup-guide-of-sma1000-for-high-security-environments/210825134517523/

REF7 Guía de usuario Connect Tunnel
https://www.sonicwall.com/techdocs/pdf/sma_1000-12-4-connect_tunnel_guide.pdf

REF8 Guía configuración WorkPlace
https://www.sonicwall.com/techdocs/pdf/sma_1000-12-4-workplace_user_guide.pdf

REF9 Guía de administración de CMS, Global High Availability
https://www.sonicwall.com/techdocs/pdf/sma-12-1-cms-with-gto-administration-guide.pdf

REF10 Guía de planificación de instalación
https://www.sonicwall.com/techdocs/pdf/secure-mobile-access-12-1-deployment-planning-guid.pdf

REF11 Configuración de cliente VPN para Windows Remote Access Service
https://www.sonicwall.com/techdocs/pdf/sma-12-3-client-extensibility-toolkit-reference-guide.pdf

REF12 Instalación Disco duro
https://www.sonicwall.com/techdocs/pdf/secure-mobile-access-6210-7210-hard-drive-installation-guide.pdf

REF13 Instalación ventilador
https://www.sonicwall.com/techdocs/pdf/secure-mobile-access-6200-7200-system-fan-installation-guide.pdf

REF14 Guía de Upgrade
https://www.sonicwall.com/techdocs/pdf/secure-mobile-access-12-1-upgrade-guide.pdf

REF15 Guía instalación SMA en Azure
https://www.sonicwall.com/techdocs/pdf/sma_1000-12-4-azure_gsg.pdf

REF16 *SonicWall Secure Mobile Access 12.1 Administration Guide*
https://www.niap-ccevs.org/MMO/Product/st_VID11023-agd2.pdf

9 ABREVIATURAS

AMC	Appliance Management Console
ATP	Advanced Threat Protection
CLI	Command Line Interface
CMC	Central Management Control
CRL	Certificate Revocation List
DNS	Domain Name Servers
DNSBL	DNS BlackList
ENS	Esquema Nacional de Seguridad
ESP	Encapsulating Security Payload
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IT	Information Technology
NAT	Network Address Translation
NGFW	Next Generation Firewall
PKI	Public Key Infrastructure
POE	Power Over Ethernet
PSK	Pre-Shared Key
RTDMI	Real Time Deep Memory Inspection
SONICOS	Sistema Operativo de Sonicwall
SSH	Secure Shell
TCP	Transport Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network

PUBLICACIONES DE DEFENSA

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