centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1420

Procedimiento de empleo seguro
Sonicwall SonicOS

Octubre 2021

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA 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
2022.01.27 13:07:32 +01'00'

NIPO: 083-21-190-2.

Fecha de Edición: octubre de 2021

ÍNDICE

1. INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL DEL PRODUCTO

1. Los cortafuegos de las **series SonicWall TZ, NSa, SOHO y SM** se basan en **SonicOS**, el sistema operativo de SonicWall.
2. SonicOS incluye un conjunto de prestaciones que proporcionan a las organizaciones la flexibilidad necesaria para ajustar estos cortafuegos de gestión unificada de amenazas (UTM) a sus requisitos de red específicos. Por ejemplo, el controlador inalámbrico integrado, compatible con las normas IEEE 802.11, así como la posibilidad de añadir los *access points* SonicWave 802.11ac Wave 2, simplifican la creación de una red inalámbrica de alta velocidad. Con el fin de reducir el coste y la complejidad de la conexión de *access points* inalámbricos de alta velocidad y otros dispositivos con tecnología de Alimentación por Ethernet (PoE), como cámaras IP, teléfonos e impresoras, los firewalls TZ300P, TZ600P y TZ570P ofrecen alimentación PoE/PoE+.
3. Las organizaciones pequeñas pueden utilizar las herramientas de SonicOS para obtener mayores ventajas. Por ejemplo, las sucursales pueden intercambiar información con la oficina central de forma segura utilizando redes privadas virtuales (VPN). La creación de redes LAN virtuales (VLANs) permite segmentar la red en grupos corporativos y de clientes con normas que determinan el nivel de comunicación con dispositivos de otras VLANs.
4. SD-WAN ofrece una alternativa segura a los costosos circuitos MPLS al tiempo que proporciona un rendimiento y una disponibilidad constante de las aplicaciones. La implementación *Zero-Touch*, que permite aprovisionar el *firewall* de forma remota a través de la nube, simplifica la instalación de los firewalls TZ/NSa en ubicaciones remotas.
5. **Estos cortafuegos han sido cualificados para categoría ALTA del Esquema Nacional de Seguridad e incluidos en el CPSTIC (Catálogo de Productos y Servicios de Seguridad TIC) en las siguientes tres (3) familias: Cortafuegos, VPN IPsec y Dispositivos de Prevención y Detección de Intrusiones.**
6. Los dispositivos compatibles cualificados con el sistema operativo **SonicOS 6.5.2 y 6.5.4** son los siguientes:
    a) Serie SOHO (SOHOW).
    b) Serie NSA. Modelos: 2650, 3600, 4600, 4650, 5600, 5650, 6600, 6650, 9250, 9450 y 9650.
    c) Serie SM. Modelos: 9200, 9400, 9600 y 9800.
    d) Serie TZ. Modelos: 300/W, 400/W, 500/W y 600.

2. OBJETO Y ALCANCE

7. El objeto del presente documento es facilitar la instalación y configuración segura de los dispositivos de SonicWall compatibles con **SonicOS 6.5.2** y **SonicOS 6.5.4**, junto con el aseguramiento del entorno en el que se despliega.

3. ORGANIZACIÓN DEL DOCUMENTO

8. El documento está estructurado en los siguientes apartados:

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

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

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

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

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

   f) **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. Toda la documentación y manuales relativos a los productos, pueden encontrarse en el siguiente enlace:

    https://www.sonicwall.com/support/technical-documentation/?language=English
11. A modo de ejemplo, la guía de puesta en marcha de un dispositivo TZ600 es la siguiente:

    https://www.sonicwall.com/techdocs/pdf/tz600-quick-start-guide.pdf
12. El embalaje, tal como indica la guía *Quick-start-guide* de cada dispositivo, incluye:
    a) El *appliance* o dispositivo *hardware*.
    b) Un adaptador de corriente (fuente de alimentación).
    c) Un cable de corriente.
    d) Un cable *ethernet*.
    e) Un cable de consola.
    f) La propia guía *Quick Start Guide*.
13. En caso de faltar algún componente, o de haber indicios de manipulación en el embalaje de entrega, 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:

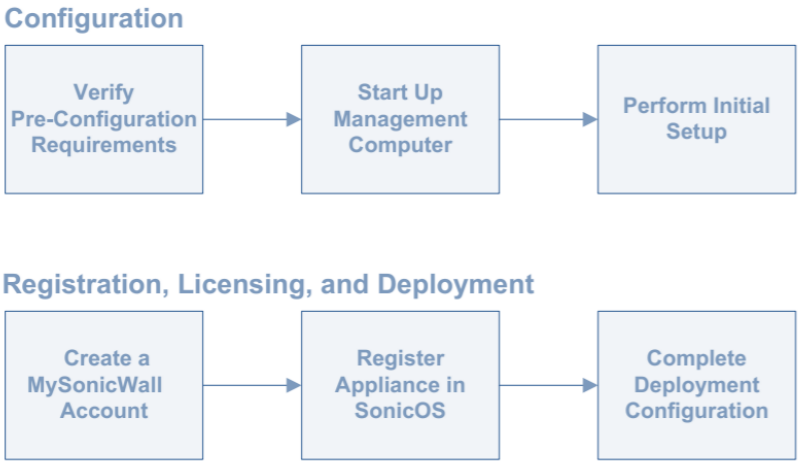


Ilustración 2. Pasos puesta en marcha dispositivos

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. El acceso físico a los dispositivos debe estar 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. Más información en la *Guía de instalación en rack de SonicWall TZ600 – REF1.*

4.3 REGISTRO Y LICENCIAS

20. Para poder activar licencias y hacer uso de los servicios de seguridad que ofrecen los dispositivos, primero es necesario registrarlos una cuenta de *www.mysonicwall.com*.
21. El registro se puede hacer desde *Mysonicwall*, o directamente desde la interfaz de gestión del propio dispositivo una vez que ya tiene conectividad a Internet. Para ello:
    a) Hacer clic en *Register* en la barra superior o desde *MONITOR > Current Status > System Status* en el área *Security Services*.
    b) Se pedirá acceso a *Mysonicwall*. Introducir los datos necesarios.
    c) Se obtendrá la información necesaria automáticamente.
22. En caso de no obtenerse automáticamente, los datos necesarios para poder hacer correctamente el registro son el Número de Serie (SN) del dispositivo y el Código

de Autenticación (*Auth Code*), que se pueden encontrar en las pegatinas que hay en la caja y en el chasis del propio dispositivo.

23. En caso de tener problemas durante el registro del dispositivo debido a problemas de conexión, consultar la siguiente nota técnica.

4.4 INSTALACIÓN

24. Se pueden hacer dos (2) tipos de despliegues: Manual y Automático, mediante el procedimiento *Zero-Touch*.

    a) **Automático *Zero-Touch*.** Este procedimiento permite automatizar el despliegue y configuración del dispositivo mediante (3) tres pasos. Una vez que el dispositivo esté encendido y tenga conectividad con Internet, si está habilitada la opción de *Zero-Touch* para ese dispositivo en *Mysonicwall*, se añadirá automáticamente a una consola de gestión centralizada (*On-Premise* o en la nube) vinculada a esa cuenta de *Mysonicwall*. Desde dicha consola se podrán configurar remotamente múltiples dispositivos haciendo uso de plantillas de configuración personalizables. En este proceso se requiere descargar la última versión del *firmware* del producto, para ello, una vez descargado, deberá verificarse la firma digital del fichero. Esta verificación se realiza automáticamente al cargar el fichero. No se deberá continuar el proceso de actualización si la firma no es válida. El detalle sobre el procedimiento *Zero-Touch* se puede consultar en la *Deployment Guide de Zero-Touch – REF5*.

    b) **Manual.** Para una instalación manual básica, se pueden seguir dos (2) procedimientos. Se recomienda utilizar el Asistente de Configuración y se debe cambiar la contraseña por defecto del usuario *Admin*, en el paso correspondiente del Asistente.

        a. El procedimiento descrito en la siguiente guía, haciendo uso del Asistente de Configuración Inicial (*Basic Setup Wizard*): *Guía de configuración inicial – REF6.*

        b. El procedimiento descrito en la siguiente guía, sin hacer uso del asistente: *Guía de configuración inicial con asistente – REF7.*

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

25. El producto soporta el modo de operación seguro o *FIPS Mode*, pero no está configurado por defecto para operar en este modo. **El producto debe ser configurado para que utilice el modo FIPS**. Cuando se habilita, el producto refuerza una serie de políticas de seguridad entre las que se encuentran las siguientes:

    a) Establece contraseñas de al menos ocho (8) caracteres, tanto para el administrador como para los usuarios.

    b) No permite habilitar LDAP en el menú de *User > Settings*.

    c) Utiliza IKE con certificados de terceros para el modo de codificación IPsec al crear túneles VPN.

    d) Al crear túneles VPN, asegura que ESP esté habilitado para IPSec.

    e) Utiliza algoritmos de autenticación y cifrado aprobados por FIPS al crear túneles VPN. Los dispositivos admiten los siguientes algoritmos criptográficos aprobados por FIPS:

        i. AES (128, 192 y 256 bits) en modo CBC (Cert. # 1200).

        ii. Triple-DES en modo CBC (Cert. # 868).

        iii. SHA-1 (Certificado # 1105).

        iv. DSA (Cert. # 398).

        v. RNG (Cert. # 664).

        vi. RSA (Cert. # 577).

        vii. HMAC-SHA-1 (Cert. # 697).

    f) La administración por HTTP, SSH o SNMP no está permitida en el modo FIPS.

    g) No habilita los servicios de enrutamiento avanzados (ARS – *Advanced Routing Services*).

26. La configuración para la activación del modo seguro se puede determinar a través del parámetro *Enable FIPS Mode:*

    a) Ir al menú *Manage > Firmware & Backup > Settings*.

    b) Si la casilla de verificación *Enable FIPS Mode* está habilitada, el módulo se está ejecutando en el modo de operación seguro.

    c) En caso contrario, se recomienda habilitar la opción de *Enable FIPS Mode*.

    d) Cuando se habilita esta opción, el producto muestra un cuadro de diálogo con el siguiente mensaje:

Warning! Modifying the FIPS mode will disconnect all users and restart the device. Click OK to proceed.

¡Advertencia! La modificación del modo FIPS desconectará a todos los usuarios y reiniciará el dispositivo. Haga clic en Aceptar para continuar.

e) Al hacer clic en *Aceptar* el dispositivo se reiniciará en modo FIPS. Aparecerá una segunda advertencia. Al hacer clic en *Sí* el dispositivo continuará reiniciando.

f) Para volver al funcionamiento normal, habría que desmarcar la opción de *Enable FIPS Mode* y reiniciar el dispositivo en modo no-FIPS. En cualquier caso, no se recomienda tener el modo FIPS deshabilitado.

27. Cuando se utiliza el dispositivo en modo FIPS, la etiqueta de seguridad adherida al dispositivo debe permanecer en su lugar y sin tocar. Esta etiqueta suele estar en la parte inferior o en la parte trasera (dependiendo del modelo) y sirve como garantía de que el equipo no ha sido manipulado.

28. El detalle de la configuración del uso del modo seguro se puede consultar la guía *Cómo configurar el modo FIPS – REF8*.

5.2 AUTENTICACIÓN

29. Los dispositivos de seguridad de SonicWall proporcionan un mecanismo para la autenticación a nivel de usuario que les da acceso a la LAN desde ubicaciones remotas en Internet, así como un medio para hacer cumplir o evitar las políticas de filtrado de contenido para los usuarios de LAN que intentan acceder a Internet. También se puede permitir que solo los usuarios autenticados accedan a los túneles VPN y envíen datos a través de la conexión cifrada.

30. El dispositivo autentica a todos los usuarios tan pronto como intentan acceder a los recursos de la red en una zona diferente (como WAN, VPN, WLAN), lo que hace que el tráfico de la red pase a través del dispositivo. Los usuarios que inician sesión en un equipo de la LAN, pero realizan solo tareas locales, no son autenticados por el dispositivo. La autenticación a nivel de usuario se puede realizar utilizando una base de datos de usuario local, LDAP, RADIUS, TACACS+ o una combinación de una base de datos local con LDAP, con RADIUS o con TACACS+.

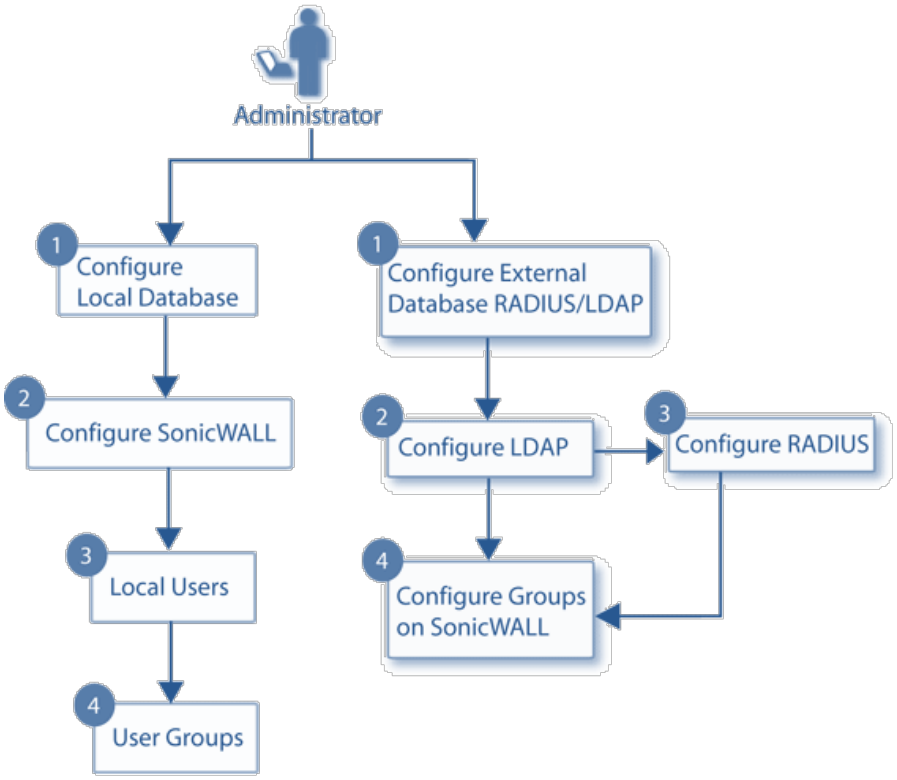


Ilustración 3. Esquema de autenticación.

31. El dispositivo también ofrece la opción de autenticación transparente de usuarios mediante ***Single Sign-On*** (SSO). SSO se puede utilizar junto con LDAP.

32. La base de datos local del dispositivo puede admitir hasta 1000 usuarios (dependiendo del modelo). Si hay más de 1000 usuarios, se debe utilizar LDAP, RADIUS o TACACS+ para la autenticación.

33. El detalle sobre los mecanismos de autenticación se puede consultar en la guía *Diferentes modos de autenticación de usuarios – REF9*.

5.2.1 AUTENTICACIÓN LOCAL

34. El dispositivo proporciona una base de datos local para almacenar información de usuarios y grupos. Se puede usar esta base de datos local para autenticar a los usuarios y controlar su acceso a la red. La base de datos local es una buena opción frente a LDAP o RADIUS cuando el número de usuarios que acceden a la red es relativamente pequeño. La creación de entradas para decenas de usuarios y grupos lleva tiempo, aunque una vez que las entradas configuradas, no son difíciles de mantener.

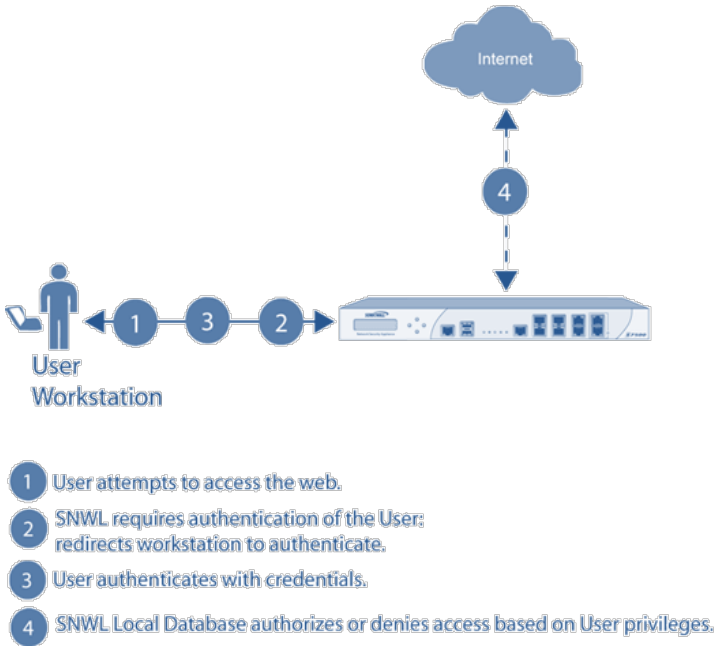


Ilustración 4. Proceso de autenticación local de usuarios.

35. La interfaz de usuario de SonicOS proporciona una forma de crear cuentas de grupos y usuarios locales (ver apartado 5.3.2 GESTIÓN DE USUARIOS LOCALES). Permite agregar usuarios y editar la configuración para cualquier usuario, incluidos los siguientes parámetros:

    a) *Group membership* - Los usuarios pueden pertenecer a uno o más grupos locales. De forma predeterminada, todos los usuarios pertenecen a los grupos *Everyone* y *Trusted Users*. Desde este menú se puede agregar/eliminar al usuario a/de uno o más grupos. Los grupos se corresponden con la **asignación de roles**, determinando los permisos del usuario.

    b) *VPN access* - Puede configurar las redes a las que puede acceder el usuario desde un cliente VPN. Al configurar los ajustes de acceso a VPN, puede seleccionar de una lista de redes. Las redes se designan por su nombre de *Address Object* o *Address Group* (ver apartado 5.4.4 ADDRESS OBJECTS Y ADDRESS GROUPS).

36. La configuración de *VPN Access* para usuarios y grupos se aplica tanto a los clientes IPSec (*Sonicwall Global VPN Client (GVC))* como a los clientes *SSL-VPN* (*Sonicwall NetExtender*), o a los *bookmarks* definidos en el portal SSL-VPN *(Virtual Office*) para ese usuario. Para permitir que los usuarios de *Global VPN Client, NetExtender* o *Virtual* Office accedan a un recurso de red, los *Address Objects* o *Address Groups* (ver apartado 5.4.4 ADDRESS OBJECTS Y ADDRESS GROUPS) correspondientes deben agregarse a la lista “Allow” en la pestaña VPN Access.

5.2.2 AUTENTICACIÓN CON RADIUS

37. Para configurar la autenticación con RADIUS, se debe seleccionar *RADIUS* o *RADIUS + Local Users,* en la lista desplegable de *User Authentication Method* del menú *Manage > Users > Settings*.

    a) Hacer clic en el botón de *Configure RADIUS* para configurar los parámetros del servidor RADIUS. Se mostrará una ventana con los parámetros de configuración:

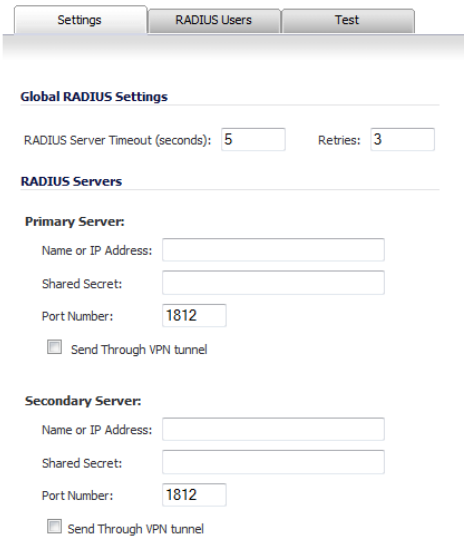


Ilustración 5. Configuración de RADIUS

    b) En la pestaña de *Settings* introducir la dirección IP y el puerto de los servidores RADIUS primario y secundario.

    c) En caso necesario, especificar una clave pre-compartida (*Shared Secret*) y la posibilidad de enviar el tráfico a través de un túnel VPN. La clave pre-compartida tiene que tener una longitud entre 1 y 31 caracteres y es sensible a mayúsculas. Se debe escoger una clave que se ajuste a las buenas prácticas sobre contraseñas seguras (sección 5.3.3.3 PARÁMETROS DE SEGURIDAD).

    d) Para guardar la configuración, hacer clic en *OK*.

38. El detalle de la configuración de la autenticación mediante RADIUS se puede consultar en el apartado *Configuring RADIUS Authentication* de la *Guía de Configuración – REF 37*.

5.2.3 AUTENTICACIÓN CON LDAP

39. Además de RADIUS y la base de datos de usuarios local, el producto también soporta LDAP para la autenticación de usuarios, con soporte para numerosos esquemas, incluidos *Microsoft Active Directory*, servicios de *directorio Novell eDirectory* y una opción completamente configurable definida por el usuario que

debería permitirle interactuar con cualquier esquema. *Microsoft Active Directory* también se integra con *Sonicwall Single Sign-On*.

40. Para integrarse con los servicios de directorio más comunes utilizados en las redes de la empresa, SonicOS admite la integración con los siguientes esquemas LDAP:
    a) *Microsoft Active Directory*.
    b) RFC2798 *InetOrgPerson*.
    c) RFC2307 *Network Information Service*.
    d) *Samba SMB*.
    e) *Novell eDirectory*.
    f) User-defined schemas.
41. SonicOS proporciona soporte para servidores de directorio que ejecutan los siguientes protocolos:
    a) *LDAPv2* (RFC3494).
    b) *LDAPv3* (RFC2251-2256, RFC3377).
    c) *LDAPv3 over TLS* (RFC2830).
    d) *LDAPv3 with STARTTLS* (RFC2830).
    e) *LDAP Referrals* (RFC2251).
42. Para la configuración de LDAP ir a *Users > Settings > Authentication* y seleccionar *LDAP + Local Users* y hacer clic en *Configure LDAP.* En la página que se abrirá, ir a *LDAP Servers* y hacer clic en *Add.* Introducir la información del servidor. Se recomienda activar la casilla *Use TLS (SSL)*, para incrementar la seguridad de las comunicaciones.

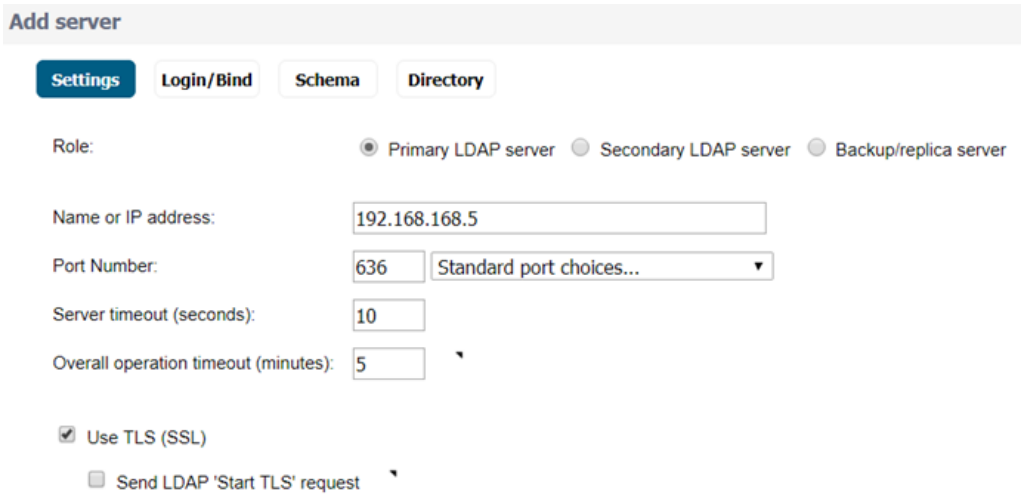


Ilustración 6. Configuración del servidor LDAP (I)

43. En la pestaña *General Settings* de la ventana Configuración LDAP, seleccionar:
    a) Versión del protocolo: se recomienda el uso de LDAP versión 3.

b) Seleccionar *Require valid certificate from the server when using TLS*. Con esta opción se valida el certificado presentado por el servidor.

c) *Local certificate for TLS*: opcional, usar solo si el servidor LDAP requiere un certificado de cliente para las conexiones.

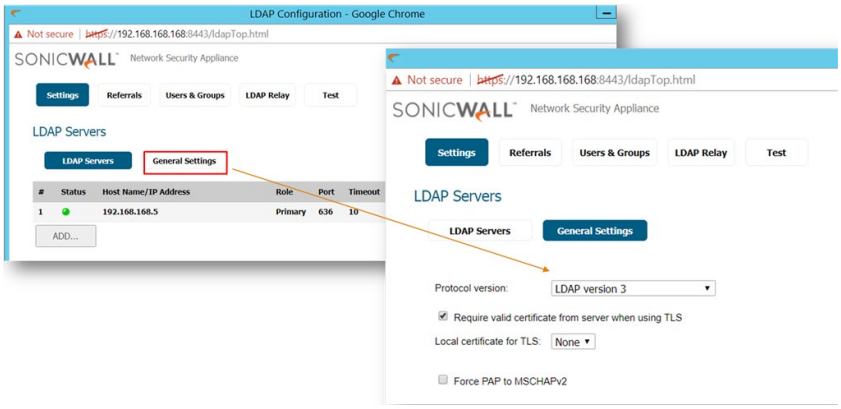


Ilustración 7. Configuración del servidor LDAP (II)

44. El detalle de la integración con LDAP se puede consultar en la guía *Cómo configurar la integración con LDAP – REF10*.

5.2.4 AUTENTICACIÓN CON SSO

45. Los dispositivos de seguridad de SonicWall brindan funcionalidad SSO utilizando el agente *Single Sign-On* (*Sonicwall SSO Agent*) y el agente *Terminal Services Agent* (*Sonicwall TSA*) para identificar la actividad del usuario. El agente SSO identifica a los usuarios según la dirección IP de la estación de trabajo. El agente TSA identifica a los usuarios mediante una combinación de dirección IP del servidor, nombre de usuario y dominio.

46. La autenticación mediante SSO también está disponible para usuarios de Mac y Linux cuando se usa con Samba. Además, la autenticación NTLM del navegador permite a *SonicWall SSO* autenticar a los usuarios que envían tráfico HTTP, sin involucrar al *SonicWall SSO Agent* o *Samba*.

47. SSO es independiente del método de autenticación para la configuración de inicio de sesión, que se puede utilizar al mismo tiempo para la autenticación de usuarios de clientes VPN/L2TP o usuarios administrativos. Los agentes SSO y TSA usan varios protocolos y mecanismos para determinar automáticamente cuando un usuario se ha conectado o desconectado de la red para prevenir accesos no autorizados. Según los datos del agente SSO o del agente TSA, el dispositivo consulta LDAP o la base de datos local para determinar la pertenencia al grupo. Las pertenencias a grupos se verifican opcionalmente mediante políticas de firewall para controlar quién tiene acceso, y se pueden usar para seleccionar políticas para el filtrado de contenido y el control de aplicaciones para controlar a qué se les permite acceder. Los nombres de usuario aprendidos mediante SSO se informan en registros de tráfico y eventos de los usuarios y en *App Flow Monitoring.*

48. El temporizador de inactividad configurado se aplica con SSO, pero el límite de sesión no, aunque los usuarios que estén desconectados vuelven a conectarse de forma automática y transparente cuando envían más tráfico. Este temporizador de inactividad (*inactivity timeout*) se configura desde el menú *Users > Settings > pestaña User Sessions*.

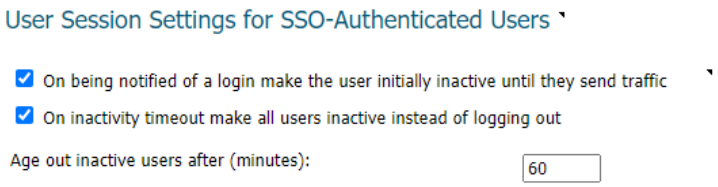


Ilustración 8. Configuración de *Single Sign On*

49. Los usuarios que inician sesión en una estación de trabajo o en el servidor de *Terminal Services / Citrix* directamente, pero que no inician sesión en el dominio, no se autentican a menos que envíen tráfico HTTP y la autenticación NTML del navegador esté habilitada (aunque opcionalmente pueden autenticarse para acceso limitado). Para los usuarios que no están autenticados por SSO, aparece una pantalla en el navegador que indica que se requiere un inicio de sesión manual en el dispositivo para una autenticación adicional.

50. Los usuarios que están identificados y carecen de la pertenencia a los grupos requeridos por las reglas de política configuradas son redirigidos a una página de Acceso Restringido.

51. SonicWall SSO requiere una configuración mínima y es transparente a los usuarios. Hay seis (6) pasos involucrados en la autenticación SSO de SonicWall, como se ilustra en la figura siguiente.

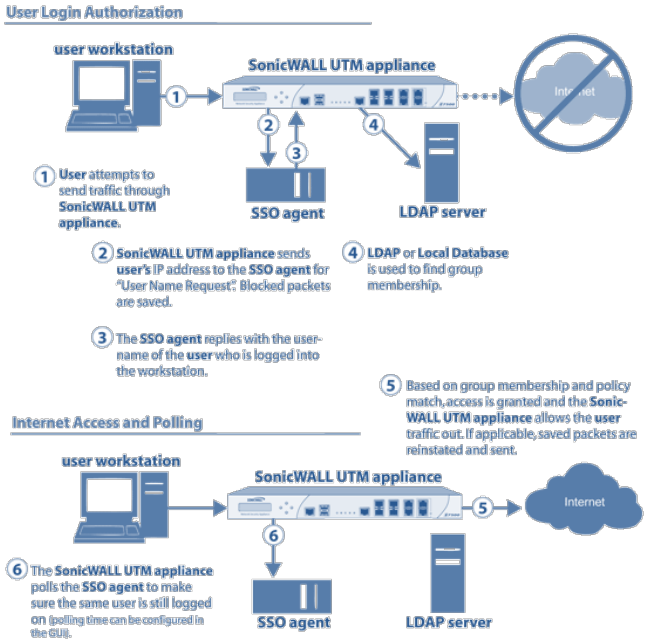


Ilustración 9. Autenticación SSO

52. Para la configuración de SSO, primero debe instalarse el agente en el dispositivo deseado. Tras ello:
    a) Ir a *Manage > Users > Settings.*
    b) En el apartado *Single-sign-on method(s)*, seleccionar *SSO Agent* y hacer clic en *Configure SSO* y después en *Add*.
    c) Se deberá introducir la información relativa al agente: dirección IP, clave compartida, número de intentos de acceso permitidos y tiempo de inactividad.
    d) Finalmente hacer clic en *Save*.
53. El detalle sobre la instalación y configuración del agente SSO se puede consultar en la guía *Cómo instalar y configurar la autenticación mediante Single Sign-On (SSO) – REF12*.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

54. Los dispositivos soportan varios tipos de accesos diferentes para la gestión, tanto local como remota. Entre los diferentes mecanismos soportados, se encuentran los siguientes:
    a) **Consola**: Todos los dispositivos incluyen un puerto dedicado de consola por el que es posible acceder a la configuración del equipo por CLI. Para ello, es necesario usar un cable de consola especial que viene en la caja del equipo (modelo NSa o superior). En la guía *Cómo habilitar la gestión por CLI a través del puerto de consola – REF14* se detalla el procedimiento y los parámetros necesarios para configurar interfaces desde el acceso CLI.
    b) **SSH:** El acceso que se tiene al dispositivo por SSH es de tipo CLI, muy similar al acceso por consola, pero en este caso no hay que acceder por ninguna interfaz dedicada, sino que se podría acceder a través de cualquier interfaz del dispositivo que tuviese este protocolo de administración habilitado.
    c) **HTTP/HTTPS**: También es posible gestionar el dispositivo a través de una interfaz gráfica (GUI) mediante los protocolos HTTP/HTTPS. Por seguridad, **no se debe usar el protocolo HTTP.**
55. El acceso por consola está siempre habilitado y no es posible deshabilitarlo, pero sólo se puede acceder a este servicio a través de un puerto dedicado y un cable especial. Los accesos por SSH, HTTP y HTTPS se pueden habilitar o deshabilitar en cualquier de las interfaces del dispositivo, pero por defecto, sólo tiene habilitada la gestión por HTTP/HTTPS en la interfaz X0 (*http(s)://192.168.168.168*) y en los puertos por defecto (*80/tcp y 443/tcp respectivamente*).
56. Para habilitar o deshabilitar los distintos accesos:
    a) Acceder a *Manage > System Setup > Network > Interfaces*.

b) Hacer clic en *Configure* en la interfaz WAN.

c) En la pestaña *General*, activar o desactivar las casillas correspondientes a HTTP, HTTPS y SSH, para habilitar o deshabilitar su uso respectivamente. **Se debe deshabilitar HTTP.**

57. Adicionalmente, pueden modificarse los puertos por defecto para los distintos tipos de acceso. Para ello ir a *Manage >System Setup > Appliance > Base Settings* y modificar el valor y *HTTPS Port* según se desee.

58. También puede habilitarse la comprobación de certificados de cliente para mayor seguridad:

    a) Ir a *Manage > Appliance > Base Settings*

    b) En el área de *Web Management* activar la casilla *Enable Client Certificate*.

    c) Ver el apartado 5.6.3 IMPORTACIÓN DE CERTIFICADOS RAIZ (*ROOT CERTIFICATES*), para consultar los pasos para configurar las CA raíz necesarias para la validación de los certificados del cliente.

5.3.2 GESTIÓN DE USUARIOS LOCALES

59. La creación de usuarios se lleva a cabo siguiendo los siguientes pasos:

    a) Desde el menú *Users > Local Users & Groups > pestaña Local Users*, hacer clic sobre el botón *Add…*

    e) Introducir el nombre de usuario deseado y su contraseña. . Se debe escoger una clave que se ajuste a las buenas prácticas sobre contraseñas seguras (sección 5.3.3.3 PARÁMETROS DE SEGURIDAD).

    b) Se debe seleccionar la casilla *User must change password*, para que el usuario deba modificar la contraseña la primera vez que acceda.

    c) En el parámetro *Account Lifetime*, seleccionar el tiempo durante el cual será válido dicho usuario. Se puede utilizar también el valor *Never expires*, de tal forma que se puede eliminar el usuario manualmente cuando se requiera.

    d) Adicionalmente es posible incluir una dirección de correo electrónico asociada al usuario (*E-mail address)* y un comentario (*Comment*).

    e) En la pestaña *Groups*, seleccionar el grupo o grupos a los que deba pertenecer el usuario. Esto determinará el rol de dicho usuario.

    f) En la pestaña *VPN Access,* seleccionar a qué recursos tendrá acceso.

    g) Hacer clic en *OK* para finalizar el proceso.

60. También se pueden agregar o editar grupos locales (roles) desde el menú *Users > Local Users & Groups > pestaña Local Groups* (ver apartado 5.3.3.2 CONFIGURACIÓN DE ROLES DE ADMINISTRADOR). Los parámetros configurables para grupos incluyen los siguientes:

a) ***Group settings***. Permite configurar los ajustes básicos del grupo, como el nombre, el dominio al que aplica o si será necesario el uso de OTPs (contraseñas de un solo uso) para el acceso.

b) ***Group members***. Permite configurar los usuarios que pertenecerán a dicho grupo. Estos pueden ser usuarios locales u otros grupos locales.

c) ***VPN Access***. El acceso VPN para grupos se configura de la misma manera que el acceso VPN para usuarios. Se pueden configurar las redes a las que puede acceder un cliente VPN iniciado por un miembro de este grupo.

61. El detalle sobre la administración de usuarios y grupos locales se puede consultar en la siguiente nota técnica.

5.3.3 CONFIGURACIÓN DE ADMINISTRADORES

5.3.3.1 ROLES DE ADMINISTRADOR

62. Los dispositivos proporcionan una cuenta de administrador predeterminada (Nombre de usuario: *admin*; Contraseña: *password*). Por motivos de seguridad, se recomienda cambiar las credenciales por defecto lo antes posible:

a) Ir al menú *Manage > Appliance > Base Settings*.

b) Ir al apartado *Administrator Name & Password*.

c) Introducir la contraseña anterior y la que se desea configurar.

d) Hacer clic en *Accept*.

63. Esta cuenta predefinida pertenece al grupo *Sonicwall Administrators*, que tiene permisos totales de administración. Además de este grupo, hay algunos otros perfiles adicionales.

64. Estos grupos se corresponden con los roles del producto, siendo la pertenencia a un grupo la que define los distintos permisos que tendrá un usuario.

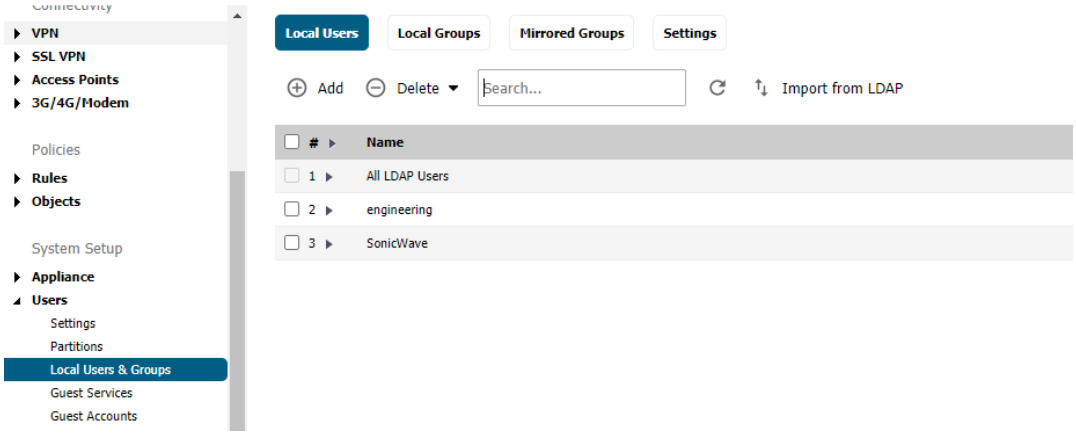


Ilustración 10. Usuarios y grupos

65. Principalmente existen (4) cuatro grupos predefinidos de administrador:

a) ***SonicWall Administrator***: tienen acceso completo a la administración.

b) ***Limited Administrator***: tienen acceso limitado a la administración.

c) ***SonicWall Read-Only Admin***: disponen de acceso de lectura solo.

d) ***Guest Administrators***: administradores "invitados", con acceso limitado a la administración.

Which zone(s) can these administrators access from?

Zone	Full admin	Limited Admin	Read-Only Admin	Guest Admin
WAN	X		X	X
LAN	X	X	X	X
DMZ	X	X	X	X
WLAN	X	X	X	X
VPN	X	X	X	X
SSLVPN	X	X	X	X

What are the access rights available for the different administrator?

Function	Full Admin in config mode	Full Admin in non-config mode	Read-only Admin	Limited Admin	Guest Admin
Import certificates	X				
Generate certificate sign-ing requests	X				
Export certificates	X				
Export appliance settings	X	X	X		
Download TSR	X	X	X		
Use other diagnostics	X	X		X	
Configure network	X			X	
Flush ARP cache	X	X		X	
Setup DHCP Server	X				
Renegotiate VPN tunnels	X	X			
Log users off	X	X		X guest users only	X guest users only
Unlock locked-out users	X	X			
Clear log	X	X		X	
Filter logs	X	X	X	X	
Export log	X	X	X	X	
Email log	X	X		X	
Configure log categories	X	X		X	
Configure log settings	X			X	
Generate log reports	X	X		X	
Browse the full UI	X	X	X		
Generate log reports	X	X		X	
Using CLI	X	X			

Ilustración 11. Acceso a zonas por perfiles de administración

66. Debido al potencial conflicto causado por varios administradores que realicen cambios de configuración al mismo tiempo, solo un administrador puede realizar cambios de configuración. Los administradores adicionales tienen acceso completo a la GUI, pero no pueden realizar cambios de configuración, es decir, accederían con permisos de sólo lectura.

67. Las reglas de prioridad en accesos concurrentes de administradores son las siguientes:

    a) El administrador predefinido (*admin*) y el sistema de administración global (GMS) de SonicWall tienen la máxima prioridad y pueden apropiarse de los permisos de escritura de cualquier otro usuario administrador que estuviese logueado al equipo.

    b) Un usuario que sea miembro de los administradores de SonicWall (administrador completo) puede apropiarse de los permisos de escritura de cualquier usuario excepto el administrador integrado y SonicWall GMS.

    c) Un usuario que es miembro de los administradores limitados solo puede apropiarse de los permisos de escritura de otros miembros del grupo de administradores limitados

68. El producto incluye grupos de administrador adicionales preconfigurados. Estos grupos adicionales se pueden habilitar configurando "M*ultiple Administrative Roles*" en el menú *Manage > Appliance > Base Settings*. Dichos grupos son los siguientes:

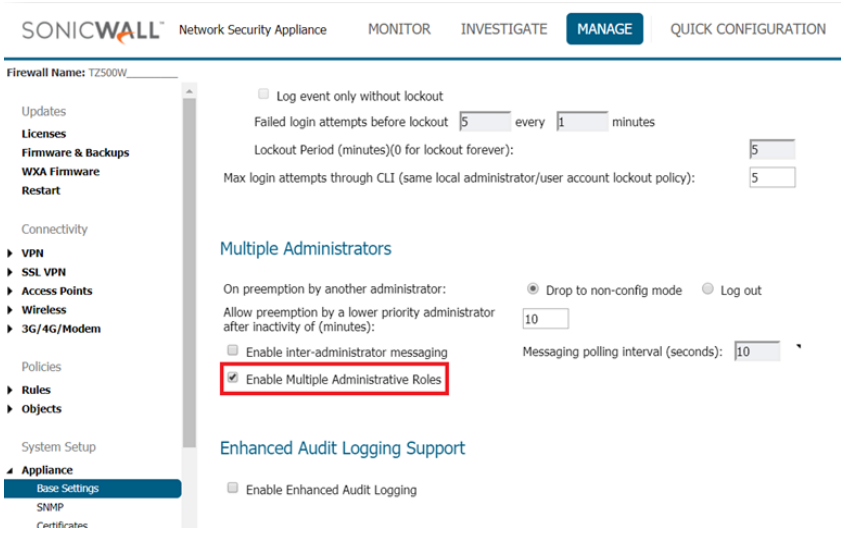


Ilustración 12. Configuración de roles de administración

a) *System Administrator (System):* Este rol da acceso a ciertas secciones del cortafuegos que pueden ayudar a verificar su estado.

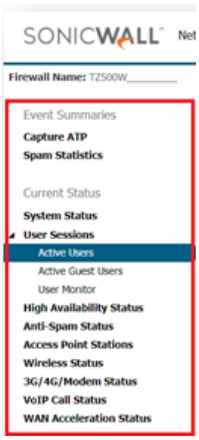


Ilustración 13. Permisos System Administrator.

b) *Cryptographic Administrator (Crypto):* Este rol solo da acceso a los menús de configuración VPN del dispositivo.

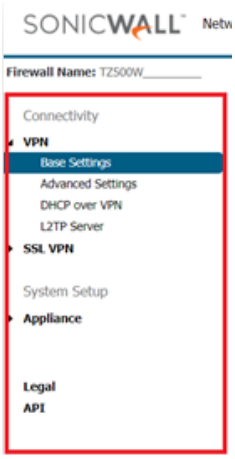


Ilustración 14. Permisos *Cryptographic Administrator*

c) *Audit Administrator (Audit):* Este rol da acceso a los menús y funcionalidades que podrían ser necesarias para fines de auditoría.

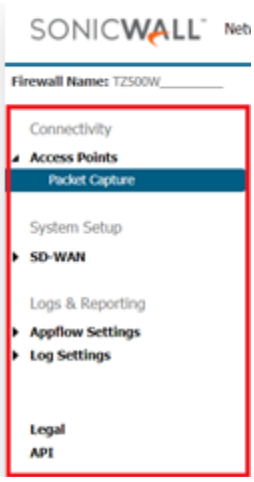


Ilustración 15. Permisos *Audit Administrator*

69. No es posible hacer a un usuario miembro de algún grupo básico de administradores y a la vez de cualquiera de los grupos de administración adicionales, como administradores del sistema, administradores criptográficos o administradores de auditoría, ya que dará el siguiente error:

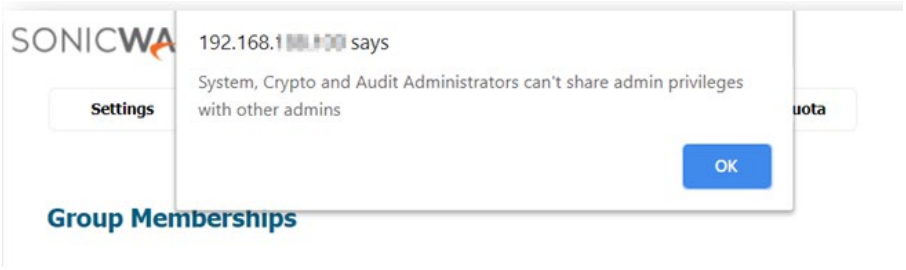


Ilustración 16. Excepción configuración de roles de administrador

70. Los grupos predefinidos indicados en este apartado definen todos los permisos del producto. Estos permisos no son modificables, de tal forma que cada usuario deberá pertenecer, al menos, a uno de los grupos predefinidos para determinar sus permisos de administración.

71. Adicionalmente, existen los grupos predefinidos *Everyone* y *Trusted Users*. Todos los usuarios pertenecen a estos grupos inicialmente, sin embargo, estos no aportan ningún permiso de administración ni permiten realizar cambios en la configuración del dispositivo.

72. A continuación, se indica cómo crear nuevos grupos en el producto. En dichos grupos no es posible definir permisos. Por lo tanto, su utilidad será la de organizar a nivel lógico los usuarios, siendo necesaria la pertenencia a alguno de los grupos predefinidos para disponer de permisos en el producto.

5.3.3.2 CONFIGURACIÓN DE ROLES DE ADMINISTRADOR

73. Para crear un nuevo grupo, seguir los siguientes pasos:

a) Ir a *Users > Local Users & Groups*.

b) Hacer clic en *Add*. Se abrirá una nueva ventana.

c) En las distintas pestañas, configurar los parámetros deseados para dicho grupo de usuarios.

d) En la pestaña *Settings*, activando la casilla *Require one-time passwords*, se puede exigir el uso de autenticación multi-factor (ver apartado 5.7 AUTENTICACIÓN CON 2FA). **Siempre que sea posible, se deberán configurar mecanismos de autenticación multi-factor.**

74. Para configurar la función de administrador múltiple, de modo que a los administradores que hayan iniciado sesión en el cortafuegos se les cierre la sesión cuando otro Administrador con más permisos inicie sesión:

a) Navegar hasta el menú *Appliance > Basic Setup*.

b) Seleccionar la opción *Log Out* en el parámetro *On preemption by another administrator* y hacer clic en *Aceptar*.

75. Cuando un administrador intente iniciar sesión mientras otro administrador está conectado, se mostrará el siguiente mensaje. El mensaje muestra el nombre de usuario del administrador actual, la dirección IP, el número de teléfono (si se puede recuperar de LDAP) y si el administrador inició sesión usando la GUI o CLI.

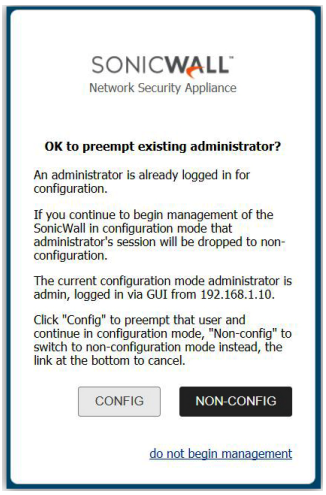


Ilustración 17. Mensaje de inicio de sesión de varios administradores.

76. Esta ventana le ofrece tres (3) opciones:

a) *Config*: da prioridad al nuevo administrador. El administrador actual pasa al modo sin configuración y se le otorga acceso de administrador completo al nuevo administrador.

b) *Non Config*: ha iniciado sesión en el dispositivo en modo *Non-Config*. La sesión del administrador actual no se ve afectada y el nuevo administrador inicia sesión como administrador de sólo lectura.

c) *Do not begin management*: vuelve a la pantalla de autenticación.

5.3.3.3 PARÁMETROS DE SEGURIDAD

77. El producto permite la definición de una política de contraseñas, así como distintos parámetros de seguridad. Esta garantiza que, tanto administradores como usuarios, hagan uso de contraseñas seguras y protege las cuentas de usuario. La política de contraseñas seguras y los parámetros de seguridad se puede configurar desde el menú *Manage > Appliance > Base Settings*, en el apartado *Login Security*:

    a) ***Password must be changed every x (days)**:* requiere que los usuarios cambien sus contraseñas una vez transcurrido el número designado de días. Cuando un usuario intenta iniciar sesión con una contraseña vencida, una ventana emergente le pedirá que ingrese una nueva contraseña. La ventana *Estado de inicio de sesión* del usuario, que aparece automáticamente en forma de ventana emergente cuando el usuario hace inicio de sesión vía web, incluye un botón *Cambiar contraseña* para que los usuarios puedan cambiar sus contraseñas en cualquier momento. El número predeterminado de días es de 90 días. **Se recomienda que las contraseñas se cambien cada 30 días, especialmente en el caso de usuarios administradores.**

    b) ***Bar repeated passwords for this many changes***: requiere que los usuarios utilicen no repitan contraseña en un número especificado de cambios. El número predeterminado es 4.

    c) ***New password must contain 4 characters different from the old password***: requiere que los usuarios cambien al menos 4 caracteres alfanuméricos en su contraseña anterior al crear una nueva.

    d) ***Enforce a minimum password length of***: establece el número mínimo de caracteres permitidos. **Se recomienda un valor de, al menos, 12 caracteres.**

    e) ***Enforce password complexity***: especifica los requisitos de complejidad que deben cumplir las contraseñas de usuario para ser aceptadas. El menú desplegable ofrece estas opciones:

        i. Ninguno (predeterminado).

        ii. Requiere caracteres alfabéticos y numéricos.

        iii. Requiere caracteres alfabéticos, numéricos y simbólicos; solo éstos caracteres simbólicos están permitidos: @, #, $,%, ^, &, *, (y); todos los demás están prohibidos.

        Se debe seleccionar la tercera opción, para mayor seguridad.

    f) ***Complexity Requirement***: cuando se selecciona la opción de complejidad de la contraseña, se establece el número mínimo de caracteres alfanuméricos y simbólicos en la contraseña de un usuario. El número predeterminado para cada uno es 0.

        i. Caracteres en mayúsculas.

        ii. Caracteres en minúscula.

iii. Caracteres numéricos.

iv. Caracteres simbólicos.

Se debe configurar un valor de, al menos, uno (1) en cada parámetro.

g) ***Apply these password constraints for***: las casillas de verificación especifican a qué clases de usuarios se aplican las restricciones de contraseña. De forma predeterminada, todas las casillas de verificación están seleccionadas.

i. Administrador: se refiere al administrador predeterminado con el nombre de usuario *admin*.

ii. Otros administradores completos.

iii. Administradores limitados.

iv. Administradores invitados.

v. Otros usuarios locales.

h) ***Log out the Administrator after inactivity of (minutes)****:* establece el tiempo de inactividad que transcurre antes de que se desconecte automáticamente de la interfaz de administración. De forma predeterminada, el dispositivo cierra la sesión del administrador después de 5 minutos de inactividad. El tiempo de espera de inactividad puede oscilar entre 1 y 9999 minutos. A pesar de la **configuración de un valor bajo de inactividad de sesiones**, se recomienda cerrar las sesiones una vez se terminen las tareas administrativas haciendo uso del botón *Cerrar sesión* situado en la esquina superior derecha de la página.

i) ***Enable administrator/user lockout***: impide que los administradores y usuarios accedan al dispositivo después del número especificado de intentos de inicio de sesión incorrectos. Esta opción está deshabilitada por defecto. Sin embargo, **debe ser activada**.

i. *Failed login attempts per minute before lockout*: especifica la cantidad de intentos de inicio de sesión incorrectos dentro de un período de un minuto que desencadena un bloqueo. El número mínimo es 1, el número máximo es 9999 y el predeterminado es 5. **Se recomienda un valor de 3 intentos.**

ii. *Lockout Period (minutes):* especifica el número de minutos que el administrador o usuario está bloqueado. El tiempo mínimo es 1 minuto, el tiempo máximo es 60 minutos y el predeterminado es 5 minutos. **Se configurar el mayor tiempo posible de desbloqueo de sesión.**

j) ***Max login attempts through CLI***. Utiliza los parámetros definidos para el bloqueo de usuarios (*Enable administrator/user lockout*), para la línea de comandos CLI, tras el número de intentos de acceso definido.

78. El periodo de inactividad, tras el cual se exigirá una reautenticación al usuario, se puede definir en el parámetro *Inactivity timeout (minutos)*, desde *Users > Settings > User Sessions*, introduciendo el valor en minutos deseado.

79. **Se debe definir un *banner* de acceso al sistema, que se muestre a todos los usuarios antes de iniciar sesión**. Para ello:
    a) Ir a *Manage > System Setyp > Users > Settings.* Hacer clic en *Customization.*
    b) En el apartado *Pre-Login Policy Banner*, marcar la casilla *Start with policy banner before login page*.
    c) En la casilla *Policy banner content*, introducir el mensaje deseado.
    d) Por último, hacer clic en *Accept.*
80. Es posible definir también un *banner* tras el acceso al sistema, que se mostrará a todos los usuarios después de iniciar sesión. **Se recomienda también la configuración de este banner.** Para ello:
    a) Ir a *Manage > System Setyp > Users > Settings.* Hacer clic en *Customization.*
    b) Ir al apartado *Post-Login Acceptable Use Policy*.
    c) Especificar en el parámetro *Disply on login from,* en qué tipos de red se presentará el mensaje (WAN, Trusted, etc).
    d) En la casilla *Acceptable use policy page content*, introducir el mensaje deseado.
    e) Por último, hacer clic en *Accept*.

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

5.4.1 ZONAS DE SEGURIDAD

81. Una zona de seguridad es una agrupación lógica de una o más interfaces diseñadas para hacer de la gestión, la definición y la aplicación de las Reglas de Acceso (ver apartado 5.4.3 REGLAS DE ACCESO POR DEFECTO) un proceso más simple e intuitivo que seguir un estricto esquema de interfaz física. La seguridad basada en zonas es un método flexible de administrar segmentos de red tanto internos como externos, lo que permite al administrador separar y proteger los recursos críticos de la red interna de accesos o ataques no aprobados.
82. Una zona de seguridad de red es simplemente un método lógico de agrupar una o más interfaces con nombres configurables por el usuario, y aplicar reglas de seguridad a medida que el tráfico pasa de una zona a otra. Las zonas de seguridad proporcionan una capa de seguridad adicional y más flexible para el producto. Con la seguridad basada en zonas, el administrador puede agrupar interfaces similares y aplicarles las mismas políticas, en lugar de tener que escribir la misma política para cada interfaz.

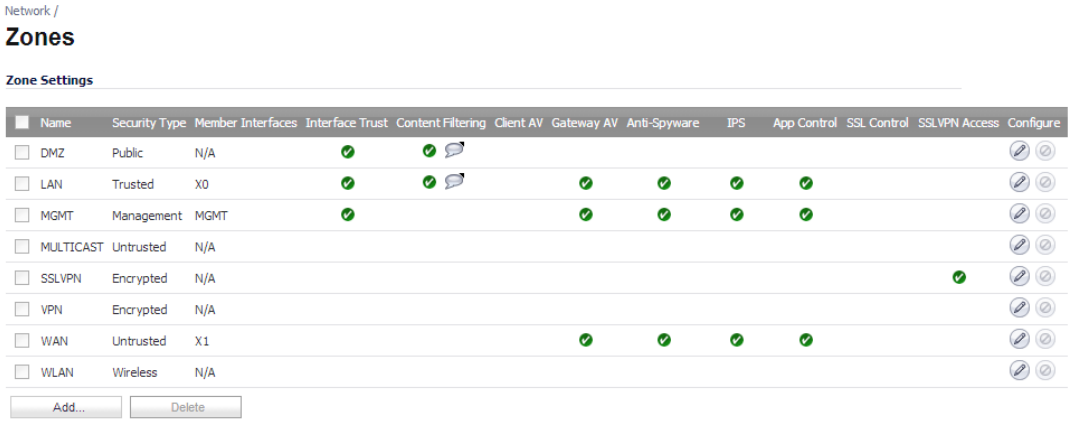


Ilustración 18. Configuración Zonas de Seguridad

83. Las zonas también permiten la exposición completa de la tabla NAT para permitir que el administrador controle el tráfico a través de las interfaces controlando las direcciones de origen y destino cuando el tráfico cruza de una zona a otra. Esto significa que NAT se puede aplicar internamente o a través de túneles VPN. Los cortafuegos SonicWALL también pueden impulsar el tráfico VPN a través de las políticas de NAT y las políticas de zona, ya que las VPN ahora están agrupadas lógicamente en su propia zona VPN.

84. Para crear nuevas zonas seguir los siguientes pasos:

    a) Ir a *Manage > Network > Zones.*

    b) Hacer clic en *Add*.

    c) A continuación, se deberá seleccionar el *Security Type* y los distintos parámetros (detallado en los siguientes apartados).

    d) Finalmente, hacer clic en *OK.*

85. El detalle de configuración sobre las zonas de seguridad se puede consultar en la guía *Cómo crear una zona de seguridad personalizada – REF23*.

5.4.1.1 ZONAS PREDEFINIDAS

86. Las zonas predefinidas varían ligeramente en función del modelo de dispositivo y no se pueden modificar. Se definen de la siguiente manera:

    a) **WAN**: esta zona puede constar de una o más interfaces o subinterfaces. Si se va a usar *WAN Failover/Load Balancing* o SD-WAN, habría que añadir las interfaces WAN adicionales a los grupos de *Load Balancing* o SD-WAN correspondientes.

    b) **LAN**: esta zona puede constar de una o más interfaces. Aunque cada interfaz estará configurada en una subred diferente, cuando se agrupan en zonas se pueden administrar como una sola entidad.

    c) **DMZ**: esta zona se utiliza normalmente para servidores de acceso público. Esta zona puede constar de ninguna o más interfaces.

d) **VPN**: esta zona virtual se utiliza para simplificar la conectividad remota segura. Es la única zona que no tiene una interfaz física asignada.

e) **MULTICAST**: Esta zona brinda soporte para multicast IP.

f) **WLAN**: esta zona se aplica tanto a las antenas integradas que incluyen algunos modelos de cortafuegos, como a las interfaces en las que se vayan a conectar puntos de acceso inalámbricos.

87. A pesar de agrupar las interfaces en zonas de seguridad, se pueden aplicar políticas a una única interfaz dentro de la zona.

5.4.1.2 TIPOS DE ZONAS

88. Cada zona tiene un tipo de seguridad, que define el nivel de confianza otorgado a esa zona. La configuración del tipo de seguridad se lleva a cabo durante la creación de la zona, desde *Manage > Network > Zones*. Hay cinco (5) tipos de seguridad:

a) ***Trusted***: es un tipo de seguridad que proporciona el nivel más alto de confianza, lo que significa que se aplica la menor cantidad de escrutinio al tráfico que proviene de zonas de confianza. Se puede pensar que la seguridad confiable está en el lado LAN (protegido) del dispositivo de seguridad. La zona LAN siempre es de confianza.

b) ***Encrypted***: es un tipo de seguridad utilizado exclusivamente por la zona VPN. Todo el tráfico hacia y desde una zona cifrada está cifrado.

c) ***Wireless***: es un tipo de seguridad aplicado a la zona WLAN o cualquier zona donde se vayan a conectar dispositivos a través de puntos de acceso inalámbricos. El tipo de seguridad inalámbrica tiene algunas funcionalidades diseñadas específicamente para su uso con dispositivos *SonicWave*. Al configurar una interfaz en una zona de tipo Wireless, se habilitan los protocolos SDP (*SonicWALL Discovery Protocol*) y SSPP (*SonicWALL Simple Provisioning Protocol*) en esa interfaz para el descubrimiento automático y el aprovisionamiento de dispositivos SonicWave. Con la opción de *SonicWave Enforcement*, el cortafuegos puede descartar automáticamente todos los paquetes recibidos desde puntos de acceso que no sean SonicWave

d) ***Public***: una zona de seguridad de tipo *Public* ofrece un nivel de confianza más alto que una zona *Untrusted*, pero un nivel de confianza más bajo que una zona *Trusted*. Las zonas de tipo *Public* se pueden considerar como un área segura entre el lado LAN (protegido) del cortafuegos y el lado WAN (desprotegido). La DMZ, por ejemplo, es una zona pública porque el tráfico fluye desde ella hacia la LAN y la WAN. De forma predeterminada, se deniega el tráfico de DMZ a LAN. Pero se permite el tráfico de LAN a cualquier destino. La DMZ solo tendrá acceso predeterminado a la WAN, no a la LAN.

e) ***Untrusted***: el tipo de seguridad *Untrusted* representa el nivel más bajo de confianza. Lo utilizan tanto la WAN como la zona virtual *Multicast*. Se puede

considerar que la zona *Untrusted* abarca el lado WAN (desprotegido) del cortafuegos. De forma predeterminada, el tráfico de las zonas *Untrusted* no puede ingresar a ningún otro tipo de zona sin reglas explícitas, pero el tráfico de cualquier otro tipo de zona está permitido a zonas *Untrusted*.

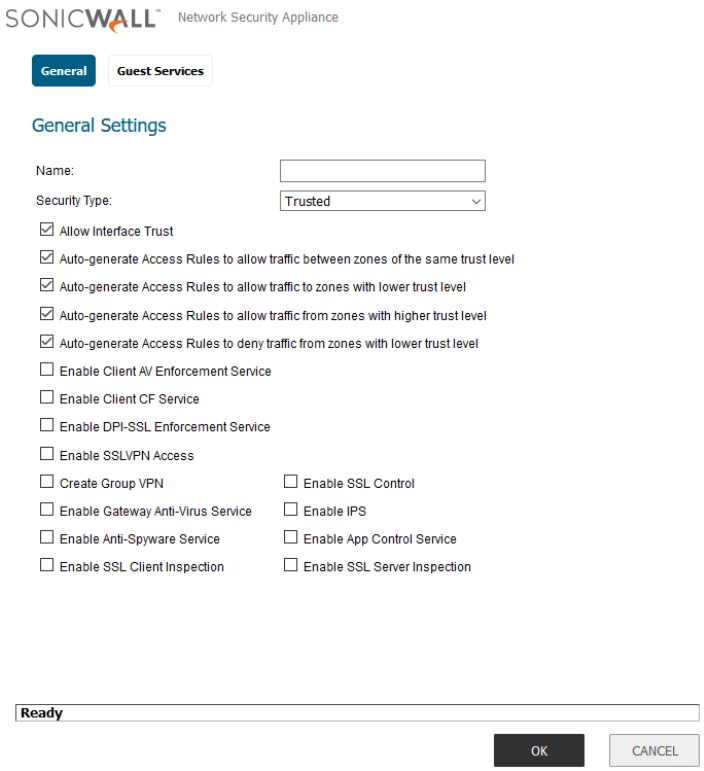


Ilustración 19. Parámetros de las zonas de seguridad

89. El parámetro *Security Type* permite seleccionar el nivel de confianza de la zona, entre uno de los vistos anteriormente.

90. Las casillas del tipo *Auto-generate Acces Rules,* permiten generar reglas por defecto automáticamente en función del nivel de confianza de cada zona. Se pueden deshabilitar al crear la zona si el comportamiento por defecto no es el deseado.

5.4.1.3 INTERFACE *TRUST*

91. El parámetro *Allow Interface Trust* disponible al agregar o editar una zona automatiza la creación de reglas de acceso para permitir que el tráfico fluya entre las interfaces de una misma zona. Por ejemplo, si la zona LAN tiene las interfaces X0 y X3 asignadas, al seleccionar la opción "*Allow Interface Trust*" en la zona LAN se crean las reglas de acceso necesarias para permitir que los *hosts* de estas interfaces se comuniquen entre sí.

5.4.1.4 HABILITAR SERVICIOS DE SEGURIDAD EN LAS ZONAS

92. Es posible activar o desactivar Servicios de Seguridad a nivel de zona durante su creación. Estos son los servicios que se pueden configurar:

    a) ***Enable Client AV Enforcement Service**:* refuerza el cumplimiento o la política de tener instalado el cliente AV de *Sonicwall Capture Client* en los dispositivos conectados a esa zona. Más información en la guía *Cómo habilitar la funcionalidad de Capture Client Enforcement en el cortafuegos – REF22*.

    b) ***Enable SSL-VPN Access***: permite el acceso mediante portales o clientes SSL-VPN a través de esa zona.

    c) ***Create Group VPN***: crea una nueva política de *GroupVPN* para permitir que se conecten clientes *IPSec (Global VPN Client)* a través de esa zona.

    d) ***Enable Gateway Anti-Virus***: aplica la protección Gateway AV basada en firmas en todas las interfaces que pertenecen a esa zona.

    e) ***Enable IPS***: habilita el servicio de detección y prevención de intrusiones en todas las interfaces que pertenecen a esa zona.

    f) **Enable Anti-Spyware Service**: habilita la detección y prevención de *spyware* en todas las interfaces que pertenecen a esa zona.

    g) ***Enable App Control Service***: habilita el servicio de control de aplicaciones en todas las interfaces que pertenecen a esa zona.

    h) ***Enable SSL Control***: habilita el servicio de SSL Control, para detectar comunicaciones que usen certificados que no cumplan ciertas medidas de seguridad, en todas las interfaces que pertenecen a esa zona.

    i) ***Enable SSL Client Inspection***: habilita el servicio *DPI-SSL Client*, para poder descifrar e inspeccionar en profundidad el tráfico cifrado con SSL generado por los usuarios internos en todas las interfaces que pertenecen a esa zona.

    j) ***Enable SSL Server Inspection***: habilita el servicio *DPI-SSL Server*, para poder descifrar e inspeccionar en profundidad el tráfico SSL destinado a servidores internos en todas las interfaces que pertenecen a esa zona.

5.4.2 CONFIGURACIÓN DE INTERFACES Y SUBINTERFACES

93. La configuración de interfaces se puede llevar a cabo desde *Manage > Network > Interface.* Haciendo clic en *Edit Icon* en la interfaz deseada.

94. Desde la misma página, haciendo clic sobre *Add Interface*, se ofrece la opción de crear nuevas interfaces.

95. Durante la configuración de una interfaz, uno de los primeros parámetros que se deben introducir es el tipo de zona (*Zone*), y en función del tipo de zona será posible escoger entre diferentes tipos de direccionamiento:

a) Si la zona es de tipo *Trusted* o *Public*, entonces se podrá escoger entre los siguientes tipos de direccionamiento:
   i. *Static IP Mode*
   ii. *Transparent IP Mode (Splice L3 Subnet)*
   iii. *Layer 2 Bridged Mode (IP Route Option)*
   iv. *Tap Mode (1-Port Tap)*
   v. *IP Unnumbered*
   vi. *PortShield Switch Mode*
   vii. *NativeBridge Mode*

b) Si la zona es de tipo *Wireless*, entonces se podrá escoger entre:
   i. *Static IP Mode*
   ii. *Layer 2 Bridged Mode (IP Route Option)*
   iii. *PortShield Switch Mode*
   iv. *NativeBridge Mode*

c) Si la zona es de tipo *Untrusted* (WAN), entonces se podrá escoger entre:
   i. *Static*
   ii. *DHCP*
   iii. *PPPoE*
   iv. *PPTP*
   v. *L2TP*
   vi. *Tap Mode (1-Port Tap)*

96. Los distintos modos disponibles aportan las siguientes funcionalidades:

a) ***Static IP***: utiliza una dirección IP estática y actúa como puerta de enlace para los dispositivos internos.

b) ***Transparent Mode***: permite asignar una única dirección IP a dos (2) interfaces físicas, donde cada interfaz accede a un rango exclusivo de direcciones IP en la subred compartida. Se comporta como un proxy en la Capa 3, interceptando ARP y cambiando las direcciones MAC de origen de los paquetes que atraviesan el par de interfaces (Proxy ARP).

c) ***Layer 2 Bridged Mode***: similar al modo transparente, pero aprende de forma dinámica las direcciones IP en ambas interfaces para que no sea necesario subdividir la subred que se está puenteando. Proporciona inspección profunda de paquetes y aplicación de políticas antes de reenviar paquetes. Coloca las interfaces puenteadas en modo promiscuo y pasa el tráfico entre ellas con las direcciones MAC de origen y destino intactas (sin hacer *Proxy ARP*).

d) ***Wire Mode***: es un modo de implementación que proporciona una forma menos intrusiva de implementar el dispositivo en una red existente.

Es muy adecuado para la implementación detrás de un cortafuegos de inspección de paquetes de estado (*Stateful Packet Inspection*) preexistente. Es una forma simplificada del modo *L2 Bridge Mode*. Una interfaz *Wire Mode* no tiene ninguna dirección IP y normalmente se configura como un puente (*bridge*) entre un par de interfaces. Ninguno de los paquetes recibidos en una interfaz en modo *Wire Mode* está destinado al cortafuegos, sino que solo se reenvía a la otra interfaz del *bridge*. *Wire Mode* tiene (3) tres modos diferentes de operación: *Bypass*, *Inspect* y *Secure*. La definición detallada del modo *Wire Mode* y sus modos de operación se puede consultar en el siguiente enlace.

e) ***Tap Mode***: brinda la misma visibilidad que el modo *Inspect* de *Wire Mode*, pero se diferencia del último en que ingiere un flujo de paquetes duplicado mediante uno o más puertos en el cortafuegos, lo que elimina la necesidad de una instalación en línea (*in-Line*). *Tap Mode* está diseñado para su uso en entornos que emplean *taps* de red, *taps* inteligentes, *port mirrors* o puertos SPAN en los switches para entregar copias de paquetes a dispositivos externos para inspección o recolección. Al igual que todas las demás formas de *Wire Mode*, el modo *Tap* puede operar en múltiples instancias de puerto concurrentes, admitiendo flujos discretos de múltiples tomas.

97. De todas formas, no todos los modos soportan las mismas funcionalidades. Como se puede ver en la tabla a continuación, algunos modos no soportan algunas de las funcionalidades ofrecidas por el dispositivo, por lo tanto, se debe tener en cuenta a la hora de escoger el modo de configuración.

Wire Modes: Functional Differences

	Bypass Mode	Inspect Mode	Secure Mode	Tap Mode	L2 Bridge, Transparent, NAT, Route Modes
Active/Active Clustering [1]	No	No	No	No	Yes
Application Control	No	No	Yes	No	Yes
Application Visibility	No	Yes	Yes	Yes	Yes
ARP/Routing/NAT [a.]	No	No	No	No	Yes
Comprehensive Anti-Spam Service [a.]	No	No	No	No	Yes
Content Filtering	No	No	Yes	No	Yes
DHCP Server [a.]	No	No	No	No	Yes [2]
DPI Detection	No	Yes	Yes	Yes	Yes
DPI Prevention	No	No	Yes	No	Yes
DPI-SSL [a.]	No	No	Yes	No	Yes
High-Availability [a.]	Yes	Yes	Yes	Yes	Yes
Link-State Propagation [3]	Yes	Yes	Yes	No	No
SPI	No	Yes	Yes	Yes	Yes
TCP Handshake Enforcement [4]	No	No	No	No	Yes
Virtual Groups [a.]	No	No	No	No	Yes

Ilustración 20. Funcionalidades de los modos de las Interfaces

98. El detalle sobre los diferentes modos de configuración soportados se puede consultar en la siguiente guía *Diferentes modos de configuración de interfaces de red – REF24*.

99. Para la creación de subinterfaces o VLANs, seguir los siguientes pasos:

    a) Ir a *Manage > Network > Interface*.

    b) Para la creación de una VLAN, seleccionar la opción *Virtual Interface* en el desplegable *Add Interface.*

    c) Introducir la zona a la cual pertenecerá y seleccionar en *Parent Interface* a qué interfaz pertenecerá.

    d) Seleccionar el modo en el que trabajará y completar la información.

    e) Por último, hacer clic en *OK*.

100. Para mayor detalle sobre la configuración de subinterfaces, consular la siguiente guía *Cómo configurar subinterfaces o VLANs – REF25*.

101. Los únicos servicios que se encuentran configurados por defecto en el dispositivo son:

    a) *Interfaz X0 (LAN): Ping, HTTP, HTTPS, SSH* y *DHCP Server*.

    b) *Interfaz X1 (WAN): DHCP Client.*

102. Si no se van a usar algunos de estos servicios, **se deben deshabilitar en la interfaz correspondiente** por seguridad. Para ello, editar la interfaz correspondiente desde el menú *Manage > Network > Interfaces* y en la sección de *Management* habilitar o deshabilitar los servicios en cuestión.

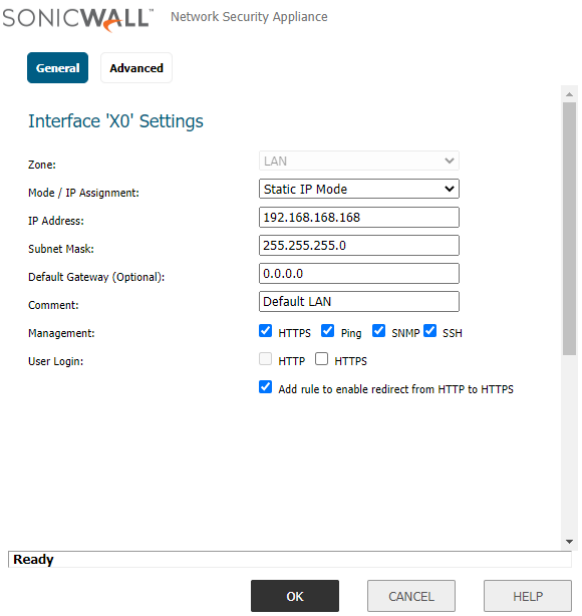


Ilustración 21. Configuración de los servicios de las interfaces

103. Para deshabilitar el cliente DHCP de la interfaz WAN, simplemente habría que cambiar la configuración a otro modo (*Static, PPPoE*, etc.).

5.4.3 REGLAS DE ACCESO POR DEFECTO

104. En la configuración por defecto del dispositivo sólo hay configuradas dos (2) interfaces:

    a) Interfaz X0 (LAN). Con un direccionamiento por defecto de 192.168.168.168/24.

    b) Interfaz X1 (WAN). Configurada como DHCP.

105. Con esta configuración básica, las únicas reglas de acceso que se aplican son las de LAN → WAN, con una única regla que permite todo el tráfico saliente por cualquier puerto; y las de WAN → LAN, también con una única regla por defecto que bloquea todo el tráfico entrante por cualquier puerto.

106. Para la creación de reglas de acceso personalizadas, seguir los siguientes pasos:

    a) Desde el menú *Manage > Rules > Access Rules*.

    b) Definir las reglas de acceso deseadas entre dos zonas de seguridad.

107. El detalle sobre la creación de reglas de acceso personalizadas se puede consultar en el apartado 5.14.2 REGLAS DE ACCESO.

5.4.4 ADDRESS OBJECTS Y ADDRESS GROUPS

108. Los *Address Objects* permiten que las entidades se definan una vez y se reutilicen en múltiples instancias referenciales en toda la interfaz de SonicOS.

109. Los *Address Objects* pueden ser de cinco (5) tipos:

    a) *Host*. Se definen mediante una única dirección IP.

    b) Range. Define un rango de direcciones IP.

    c) *Network*. Similar a los objetos de tipo *Range*, pero se definen mediante una máscara de red.

    d) *MAC address*. Identifican dispositivos mediante la dirección MAC.

    e) *FQDN*. Identifican dispositivos mediante su FQDN (*Full Qualified Domain Name*)

110. Una vez que los objetos están creados, se pueden utilizar en reglas de acceso, políticas de NAT o de *routing*, exclusiones o inclusiones en servicios de seguridad, etc.

111. Además de simplificar la configuración permitiendo agrupar objetos y reducir el número de reglas consiguiendo el mismo resultado final, si se usan nombres descriptivos, la configuración se hace más legible y por lo tanto se reducen las posibilidades de cometer errores humanos. Por este motivo se recomienda que los

nombres escogidos para cada uno de los objetos y grupos sigan una nomenclatura unificada que sea respetada por todos los administradores del dispositivo.

112. Para la creación de los *Address Objects*:

    a) Ir a *Manage > Policies > Objects > Address Objects.*

    b) Hacer clic sobre *Add*.

    c) Seleccionar el tipo de objeto que se desea crear e introducir su dirección IP y la zona a la cual está asignado.

    d) Por último, hacer clic en *Add.*

113. Para la creación de los Address Groups:

    a) Ir a *Manage > Policies > Objects > Address Objects > Address Groups*.

    b) Hacer clic sobre *Add*.

    c) Introducir el nombre del grupo e incluir los objetos que formarán parte del mismo.

    d) Hacer clic sobre *OK*.

114. El detalle de la creación y configuración de Address Objects y Address Groups se puede consultar en la siguiente guía *Cómo crear Address Objects y Address Groups – REF26*.

5.4.5 DHCP

115. El servidor DHCP está habilitado por defecto en la interfaz X0, con un rango dinámico preconfigurado que comprende las IPs 192.168.168.1 - 192.168.168.167. Este servicio puede ser muy útil para la configuración inicial, ya que evita tener que conocer la IP por defecto del dispositivo y configurar a mano la interfaz del equipo que se vaya a usar para gestionar el mismo. Una vez que se ha hecho la configuración inicial, si ya no se va a hacer uso de este servicio se recomienda deshabilitarlo para evitar posibles conflictos.

116. Para deshabilitar el servicio DHCP:

    a) Ir a *Network > System > DHCP Server.*

    b) Ir a la página *DHCP Server Settings*.

    c) Deshabilitar la casilla *Enable DHCPv4 Server*.

117. El detalle sobre la configuración del servidor DHCP se puede consultar en la siguiente guía *Cómo configurar el servidor DHCP – REF27*.

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

5.5.1 CONFIGURACIÓN SEGURA DE TLS (*TRANSPORT SECURITY LAYER*)

118. El producto es compatible con TLS 1.1 y TLS 1.2, y también permite deshabilitar la compatibilidad con versiones SSL/TLS antiguas e inseguras.

119. Por defecto, se puede acceder a la interfaz de administración del cortafuegos desde un navegador usando SSLv3, TLS 1.0, TLS 1.1 o TLS 1.2. **Se debe usar TLS 1.2 o superior y deshabilitar compatibilidades con versiones anteriores**. También se puede acceder a la funcionalidad de SSL-VPN utilizando estos protocolos. La funcionalidad DPI-SSL también soporta todos los protocolos anteriores.

120. Para configurar el producto para hacer uso solo de TLS1.2 o superiores, seguir los siguientes pasos:

    a) Iniciar sesión en la administración del dispositivo y luego reemplazar la palabra *main* por la palabra *diag* en la URL (es decir, https://192.168.168.168/main.html se convertirá en https://192.168.168.168/diag.html).

    b) Hacer clic en *Internal Settings.*

    c) Buscar la opción *Enable TLS compatible mode* y desactivarla si está activada.

    d) También puede deshabilitar TLS 1.1 desde dicha página, ya que se recomienda TLS 1.2 o superior para mayor seguridad. Para ello, seleccionar la casilla *Disable TLSv1_1*.

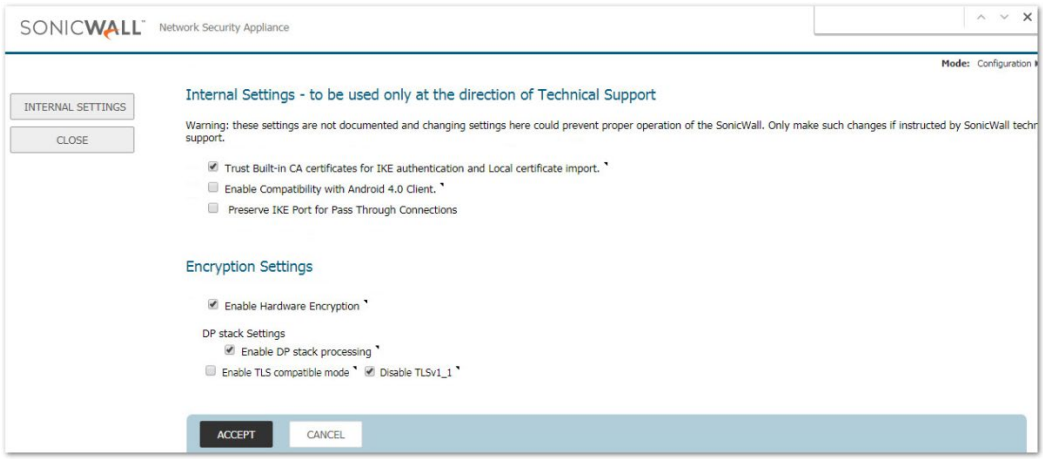


Ilustración 22. Configuración de TLS 1.2

5.5.2 CONFIGURACIÓN SEGURA DE SSH

121. La función de *Cipher Control* se puede utilizar para permitir o bloquear cualquiera de los *cipher suites* de TLS y SSH.

122. La pestaña *SSH Ciphers* del menú *Manage > Security Configuration > Firewall Settings > Cipher Control* permite especificar qué cifrados SSH criptográficos utiliza

SonicOS. La configuración segura de SSH se consigue activando o desactivando las casillas de verificación de cada uno de sus parámetros: el algoritmo de intercambio de claves, el algoritmo de clave pública, el algoritmo de cifrado o el algoritmo MAC.

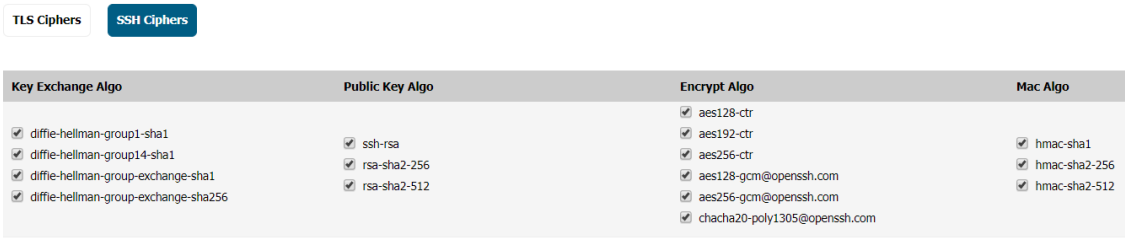


Ilustración 23. Configuración de SSH.

123. **No se recomienda el uso de SSH porque no ha formado parte del alcance de la certificación Common Criteria que se ha tomado de base para la cualificación del producto. Se debe configurar el producto a través de la consola web UI, canal protegido con HTTPS.**

5.5.3 CONFIGURACIÓN SEGURA DE IKE/IPSEC

124. El producto soporta tanto IKEv1, como IKEv2. **Se debe hacer uso de IKEv2 ya que proporciona mayor seguridad que IKEv1.**

125. Para hacer uso de IKEv2, seguir los siguientes pasos:

    a) Ir a *Manage > Connectivity > VPN > Base Settings*.

    b) Ir a la pestaña *Proposals*.

    c) En el parámetro *Exchange* seleccionar *IKEv2 Mode.*

    d) Hacer clic en *OK*, para guardar los cambios.

126. El detalle de la configuración de túneles *Site to Site VPN* usando IKEv2 se puede consultar en la siguiente guía *Cómo configurar túneles VPN Site to Site con IKEv2 – REF28.*

5.5.4 GESTIÓN DE ALGORITMOS Y FUNCIONES CRIPTOGRÁFICAS

127. La funcionalidad de *Cipher Control* se puede utilizar para permitir o bloquear cualquiera de los cifrados TLS y SSH. SonicOS tiene alrededor de 333 cifrados TLS en la lista que se pueden permitir o bloquear según la fortaleza, el soporte del modo CBC o la versión del protocolo TLS.

128. Se puede configurar desde el menú *Manage > Security Configuration > Firewall Settings > Cipher Control*. Se pueden filtrar fácilmente y tomar la decisión de bloquear o permitir ciertos cifrados.

129. Esta funcionalidad se aplica a DPI-SSL, gestión del dispositivo por HTTPS y SSL Control.

130. Los criterios para filtrar los cifrados son los siguientes:

a) Fortaleza (*Strength*): Recomendado, Seguro, Débil, Inseguro.

b) CBC: Indica si el cifrado utiliza el modo CBC (*Cipher-Block Chaining*).

c) Versión TLS: Hay filtros para todas las versiones desde TLS 1.0 a TLS 1.3. Se recomienda usar esta utilidad para habilitar solo los *cipher suite* de las versiones TLS1.2 y TLS1.3.

d) Acción: También se pueden ver todos los cifrados permitidos o bloqueados usando este menú desplegable.

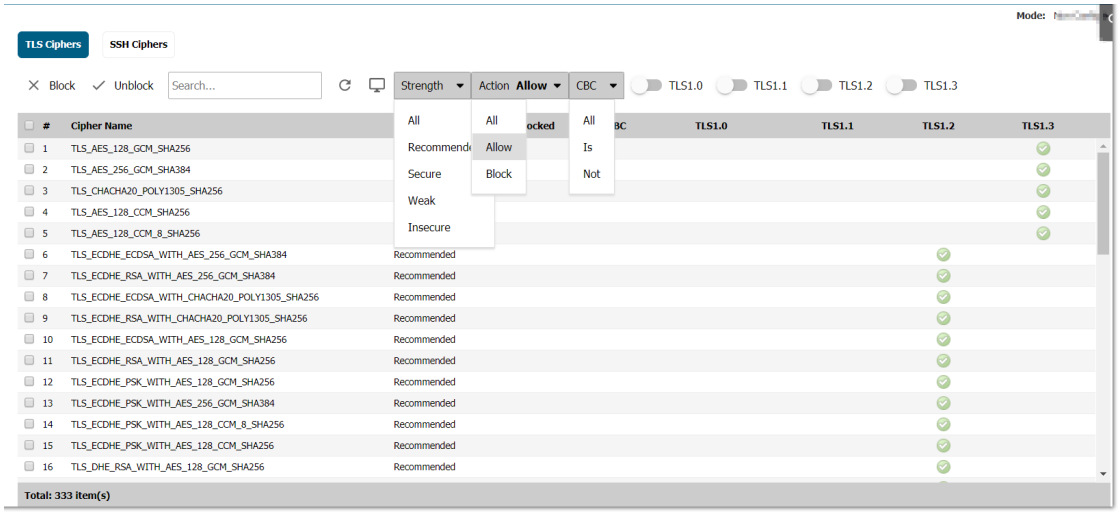


Ilustración 24. Configuración de la criptografía (I)

131. Los cifrados se ordenan en función de las fortalezas de seguridad, con los cifrados en la parte superior más seguros que los de abajo.

132. El icono rojo indica que está bloqueado y el icono verde indica si se encuentra disponible. Se puede usar la lista desplegable *Action* para filtrar todos los algoritmos bloqueados o permitidos.

133. Por ejemplo: El algoritmo *TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384* es un algoritmo de cifrado CBC y *TLS_ECDH_ECDSA_WITH_RC4_128_SHA* está bloqueado como se puede observar en la imagen de más abajo.

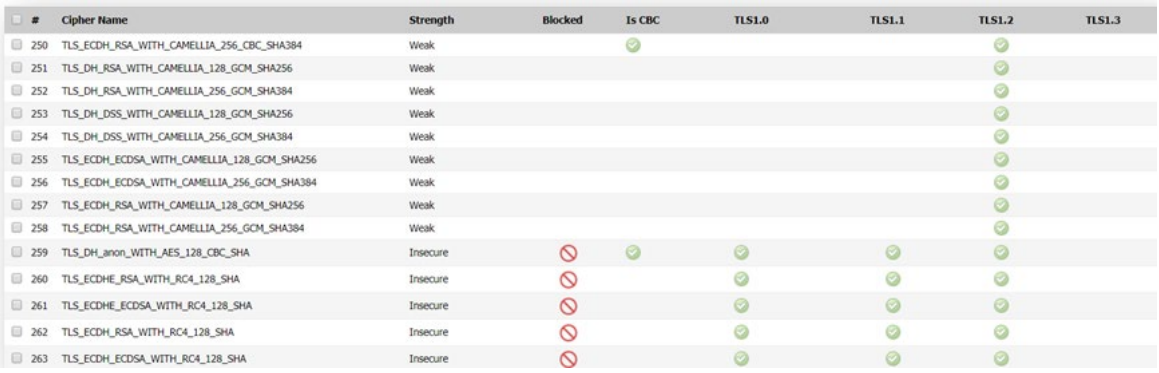


Ilustración 25. Configuración de la criptografía (II)

134. El comportamiento esperado, cuando se bloquea un cifrado es el siguiente. Por ejemplo, si el cifrado X está bloqueado, el comportamiento esperado es:

    a) DPI-SSL: el algoritmo de cifrado X ya no es parte del contexto TLS y no es parte de los cifrados anunciados por el cliente enviados por el protocolo de enlace del cortafuegos con el servidor de origen.

    b) Gestión mediante HTTPS: el algoritmo de cifrado X no forma parte de la aplicación del servidor HTTPS que se ejecuta en el dispositivo. Por lo tanto, si un cliente TLS negocia solo el cifrado X, el protocolo de enlace TLS entre el cliente y el firewall fallará.

    c) SSL Control: como esto se refiere al tráfico que pasa a través del dispositivo (que no sean sesiones descifradas DPI-SSL), el firewall bloquea cualquier conexión TLS entre el cliente de origen y el servidor de origen que use o intente negociar el algoritmo de cifrado X.

135. También se puede usar el icono de la pantalla para verificar si el algoritmo de cifrado es aplicable a DPI-SSL, gestión por HTTPS, o SSL Control.

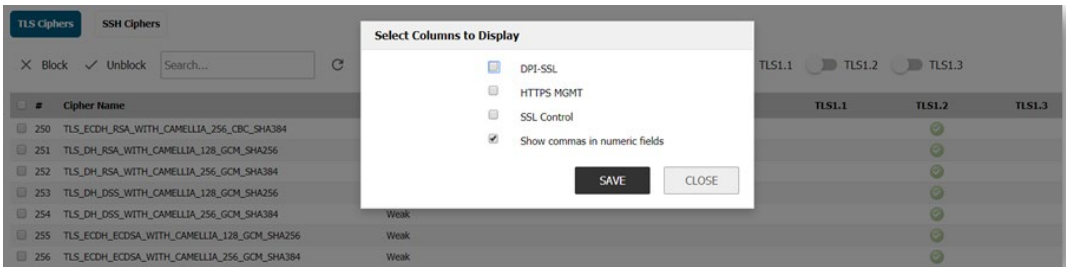


Ilustración 26. Configuración de la criptografía (III)

136. Se pueden seleccionar varios conjuntos de cifrado después de filtrar y usar los botones *Block* y *Unblock* para bloquear o permitir el cifrado respectivamente.

137. Para una configuración segura, se recomienda que **los algoritmos y funciones criptográficas que se utilicen, estén admitidos en la guía CCN-STIC-807**. Esto significa que deben utilizarse únicamente los siguientes algoritmos y funciones:

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

    b) ECDSA con curvas P-256 o superior.

    c) Funciones Hash SHA-256 o superior.

    d) Cifrado AES-128 o superior.

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

    f) *Elliptic Curve Diffie-Hellman* P-256 o superior.

5.5.5 SSL CONTROL

138. El producto soporta la funcionalidad de *SSL Control*, un sistema para proporcionar visibilidad del protocolo de enlace de las sesiones SSL y un método para construir políticas para controlar el establecimiento de conexiones SSL.

139. *SSL Control* proporciona una serie de métodos para abordar este desafío al dotar al administrador de seguridad de la capacidad de analizar y aplicar controles basados en políticas para el establecimiento de sesiones SSL. Si bien la implementación actual no decodifica los datos de la aplicación SSL, sí permite la identificación basada en la puerta de enlace y la desautorización del tráfico SSL sospechoso.

140. Para configurar el control SSL, seguir los siguientes pasos:

a) Ir al menú *Firewall Settings > SSL Control*.

b) En *General Settings*, seleccionar *Enable SSL Control* para habilitar el control SSL en el dispositivo.

c) En *Action*, seleccionar una de las siguientes opciones:

i. *Log the event*: si se detecta una violación de la política SSL, el evento se registra, pero la conexión SSL puede continuar.

ii. *Block the connection and log the event*: en el caso de una infracción de política, la conexión se bloquea y el evento se registra.

d) En *Configuration,* seleccionar una o más de las siguientes opciones:

i. *Enable Blacklist*: controla la detección de las entradas en la lista negra, como se configura en la sección *Custom Lists* a continuación.

ii. *Enable Whitelist*: controla la detección de las entradas en la lista blanca, como se configura en la sección *Custom Lists* a continuación. Las entradas de la lista blanca tienen prioridad sobre todas las demás configuraciones de control de SSL.

iii. *Detect Expired Certificates*: controla la detección de certificados cuya fecha de inicio es anterior a la hora actual del sistema o cuya fecha de finalización es posterior a la hora actual del sistema. La validación de la fecha depende de la hora del sistema del producto. Verificar de que la hora del sistema esté configurada correctamente, preferiblemente sincronizada con NTP, en el menú *Appliance > System Time*, ver apartado 5.8 SINCRONIZACIÓN HORARIA.

iv. *Detect SSLv2*: controla la detección de intercambios SSLv2. Se sabe que SSLv2 es susceptible a los ataques de degradación de cifrado porque no realiza una verificación de integridad en el protocolo de enlace. Se debe usar TLS 1.2 o superior.

v. *Detect Self-Signed Certificates*: controla la detección de certificados en los que tanto el emisor como el sujeto tienen el mismo nombre común.

vi. *Detect certificates signed by an Untrusted CA*: controla la detección de certificados donde el certificado del emisor no está en el repositorio de certificados de confianza (Trusted CA's) del cortafuegos.

vii. *Detect weak ciphers (<64 bits):* controla la detección de sesiones SSL negociadas con cifrados simétricos de menos de 64 bits, lo que generalmente indica el uso de cifrado de exportación.

141. En *Custom Lists*, configurar la lista negra y la lista blanca definiendo cadenas para que coincidan los nombres comunes en los certificados SSL. Las entradas distinguen entre mayúsculas y minúsculas y se utilizan con coincidencia de patrones. Por ejemplo, "*sonicwall.com*" coincide con "*https://www.sonicwall.com*" y "*https://mysonicwall.com*", pero no con "*https://www.sonicwall.de*".

    a) Para agregar una entrada a la lista negra, escribir la dirección deseada en el campo Lista negra y luego haga clic en *Agregar*.

    b) Para agregar una entrada a la lista blanca, escribir la dirección deseada en el campo Lista blanca y luego haga clic en *Agregar*.

142. Por último, hacer clic en *Actualizar*. Para volver a los valores predeterminados y comenzar de nuevo, hacer clic en *Restablecer*.

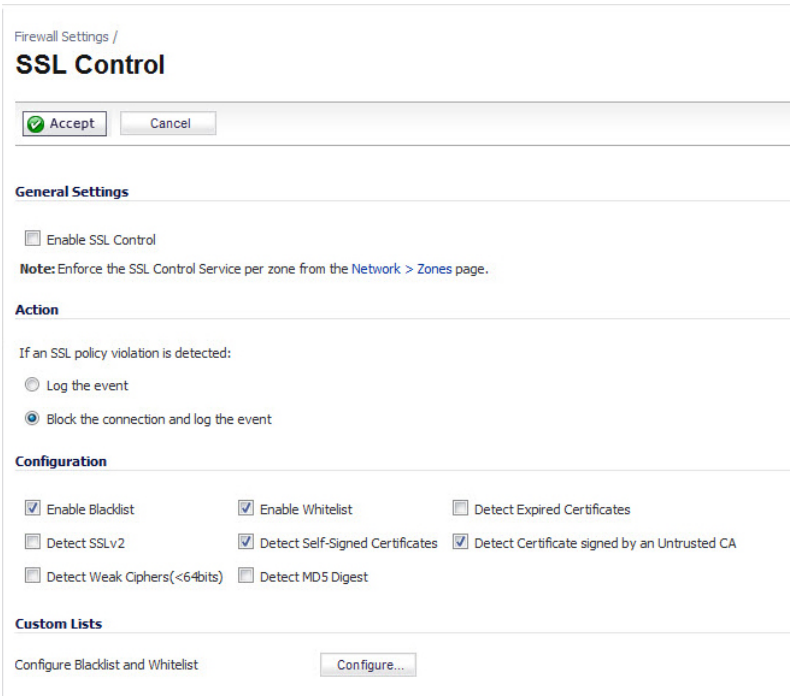


Ilustración 27. Configuración de SSL Control

5.6 GESTIÓN DE CERTIFICADOS

5.6.1 GENERACIÓN DE CERTIFICADOS

5.6.1.1 CREACIÓN DE UN CSR

143. El producto puede hacer uso de certificados para varios propósitos, entre los que se encuentran la gestión del equipo mediante HTTPS, la negociación de túneles VPN IPSec usando certificados, etc.

144. Para solicitar e importar un certificado de una autoridad de certificación reconocida o de confianza (CA) para el dispositivo, se debe crear una solicitud de firma de certificado (*Certificate Signing Request* - CSR) desde el dispositivo.

a) Para ello, ir al menú *Manage* > *Appliance* > *Certificates* y hacer clic en el botón *New Signing Request*.

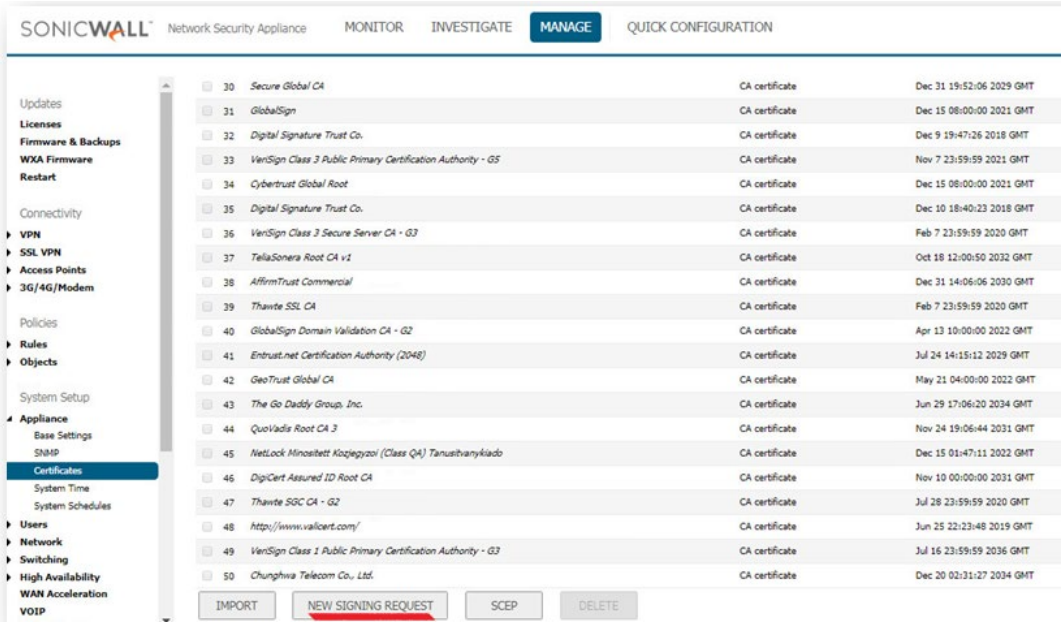


Ilustración 28. Creación de un CSR (I)

b) Completar la solicitud de firma de certificado con información sobre el nombre de dominio completo (FQDN) que utilizará para SSL. **Se deben usar longitudes de clave de 3072 o superiores (parámetro *Subject Key Size/Curve*) en el caso de certificados que utilicen RSA.**

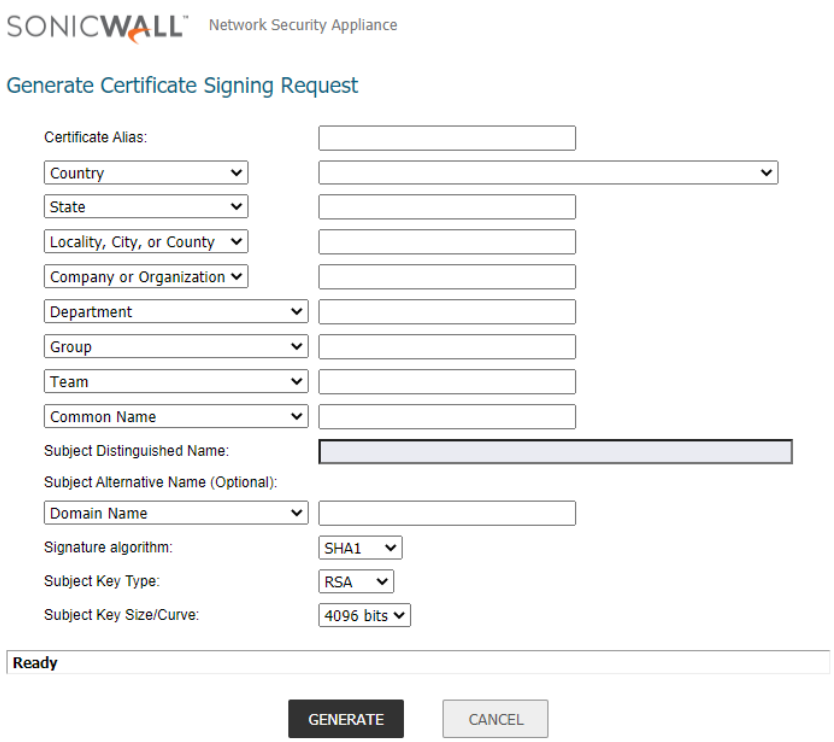


Ilustración 29. Creación de un CSR (II)

c) Descargar el CSR y enviar a una CA (Autoridad de Certificación). Para ello hacer clic sobre el icono de descarga, tal como puede verse en la siguiente imagen y posteriormente sobre *Export*, en la ventana emergente.

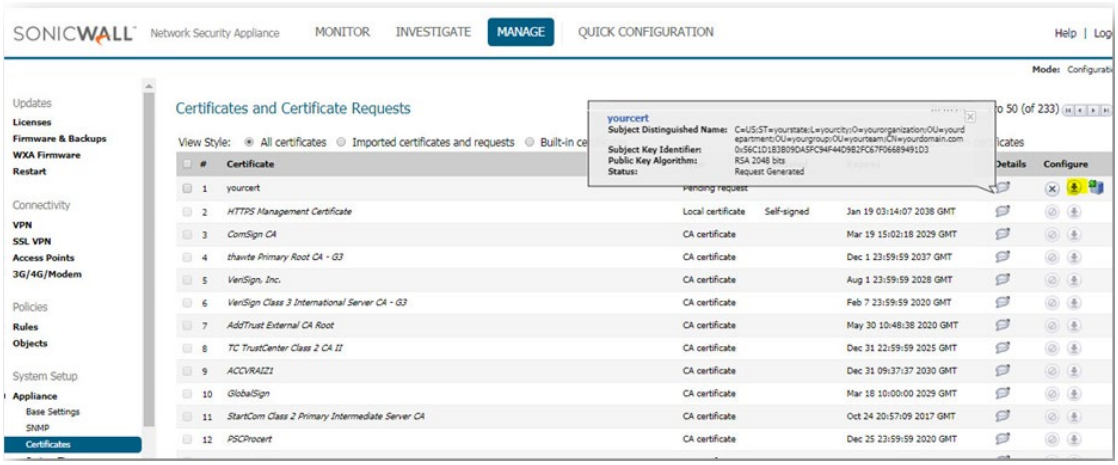


Ilustración 30. Creación de un CSR (III)

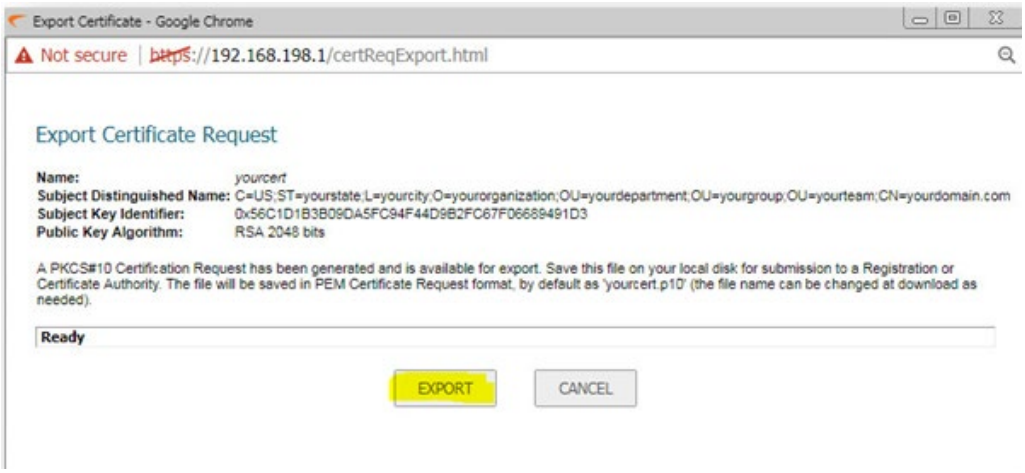


Ilustración 31. Creación de un CSR (IV)

d) Solicitar el certificado a la autoridad de certificación deseada, proporcionando el fichero descargado cuando lo soliciten.

e) Una vez que se obtenga el certificado de la autoridad de certificación, cargar el certificado en la solicitud pendiente. Para ello hacer clic sobre el icono que se muestra en la imagen a continuación. Después seleccionar el fichero y hacer clic en *Upload*.

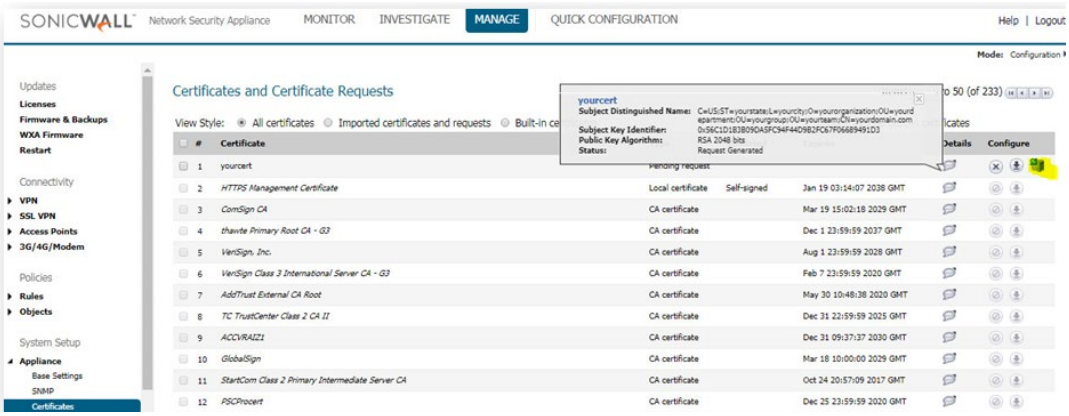


Ilustración 32. Creación de un CSR (V)

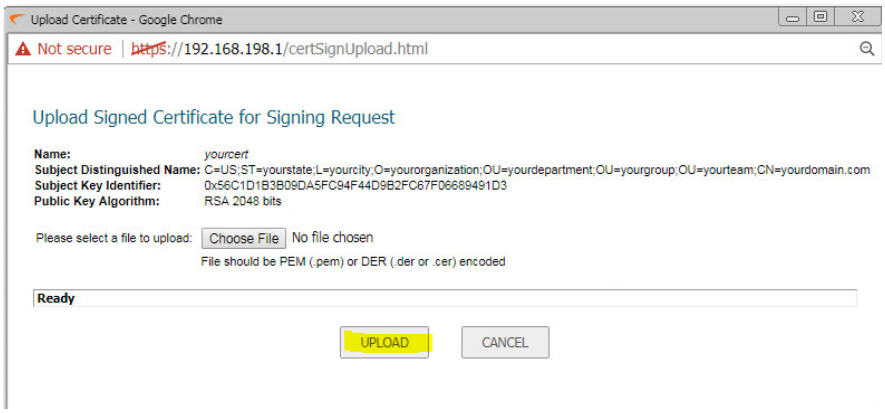


Ilustración 33. Creación de un CSR (VI)

f) Reiniciar el dispositivo para verificar que el certificado esté instalado y validado.

g) En caso que el certificado se muestre como "*Not Validated*", puede ser necesario importar los certificados raíz de la CA, o de CA intermedias. Para importar estos certificados en el dispositivo, consultar el apartado 5.6.3 IMPORTACIÓN DE CERTIFICADOS RAIZ (*ROOT CERTIFICATES*) y seguir el proceso indicado en dicho apartado para importar los certificados necesarios.

5.6.2 CONFIGURACIÓN DE *SIMPLE CERTIFICATE ENROLLMENT PROTOCOL* (SCEP)

145. El Protocolo Simple de Inscripción de Certificados (SCEP o *Simple Certificate Enrollment Request*) está diseñado para admitir la emisión segura de certificados a dispositivos de red de manera escalable. Hay dos (2) escenarios de inscripción para SCEP:

a) La CA del servidor SCEP emite certificados automáticamente.

b) La solicitud SCEP está configurada como PENDIENTE y el administrador de CA emite manualmente el certificado.

146. Para utilizar SCEP para emitir certificados, seguir los siguientes pasos:

a) Generar una solicitud de firma como se describe anteriormente en el apartado 5.6.1.1 CREACIÓN DE UN CSR.

b) Ir hasta la parte inferior del menú *System > Certificates* y hacer clic en el botón *SCEP*. Aparecerá la ventana de configuración de SCEP.

c) En el menú desplegable *CSR List*, la interfaz de usuario seleccionará automáticamente una lista de CSR predeterminada. Si tiene varias listas de CSR configuradas, puede modificar esto.

d) En el campo *CA URL*, introducir la URL de la autoridad de certificación.

e) En el campo *Challenge Password*, introduzcir la contraseña de la CA si es necesaria.

f) En el campo *Polling Interval (S)*, se puede modificar el valor predeterminado para la duración del tiempo en segundos entre el momento en que se envían los mensajes de sondeo.

g) En el campo *Max Polling Time (S)*, se puede modificar el valor predeterminado durante el tiempo que el firewall esperará una respuesta a un mensaje de sondeo antes de que se agote el tiempo.

h) Hacer clic en el botón *SCEP* para enviar la inscripción SCEP.

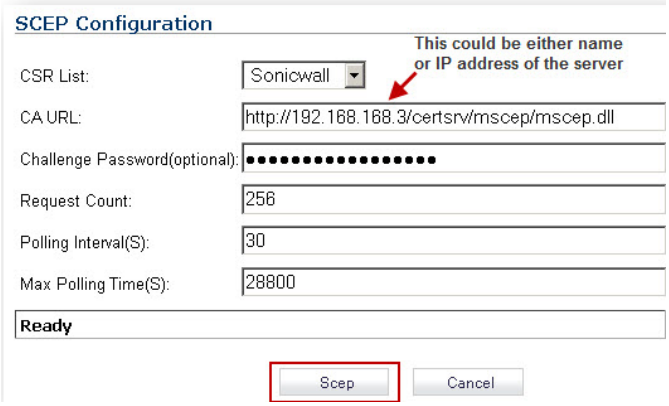


Ilustración 34. Configuración de SCEP (I)

147. El dispositivo se pondrá en contacto con la CA para solicitar el certificado. El tiempo que llevará esto dependerá de si la CA emite certificados de forma automática o manual. Desde el menú *Log* > *View*, se mostrarán mensajes sobre el estado de la inscripción al SCEP y la emisión del certificado. Una vez emitido el certificado, se mostrará en la lista de certificados disponibles en el menú *Appliance* > *Certificates*, en la sección *Certificates and Certificate Requests*.

Ilustración 35. Configuración de SCEP (II)

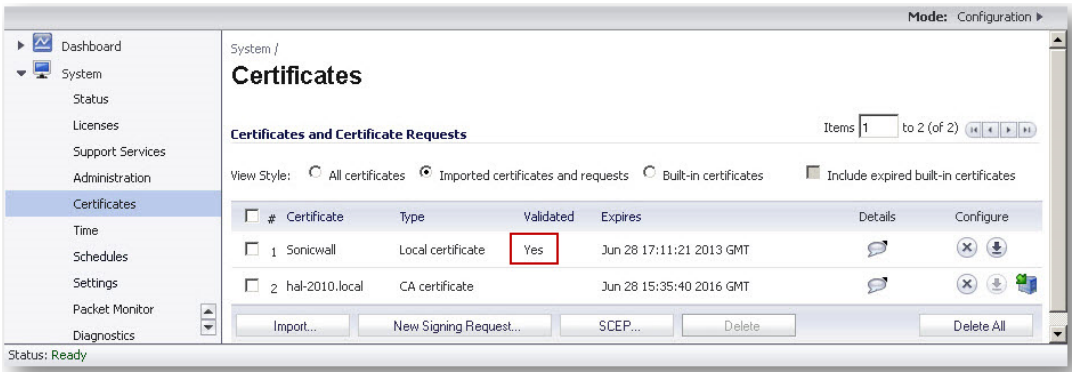


Ilustración 36. Configuración de SCEP (III)

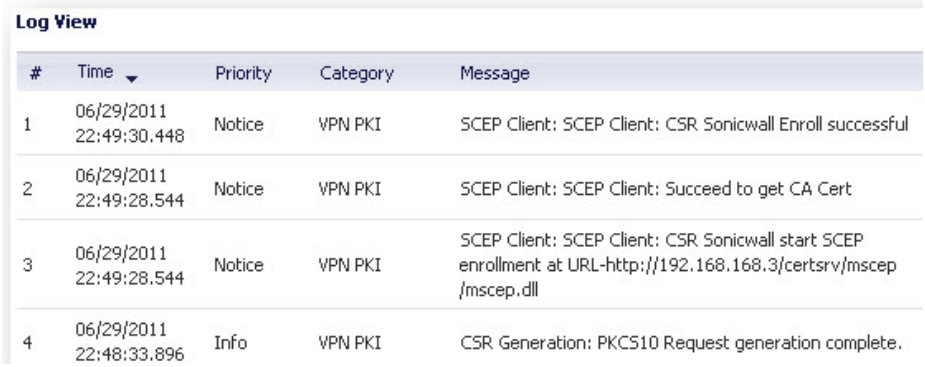


Ilustración 37. Configuración de SCEP (IV)

5.6.3 IMPORTACIÓN DE CERTIFICADOS RAIZ (*ROOT CERTIFICATES*)

148. Si el certificado intermedio o raíz de la cadena de certificados es diferente a los del dispositivo, o faltan en el mismo, entonces el certificado se mostrará como *Not Validated* y será necesario importar certificados adicionales para que el dispositivo pueda confiar en este certificado.

149. Para importar los certificados de CA, seguir los siguientes pasos:

a) Importar el fichero correspondiente al certificado de la CA. Para hacer esto ir a *Appliance* > *Certificates* y hacer clic en *Import*.

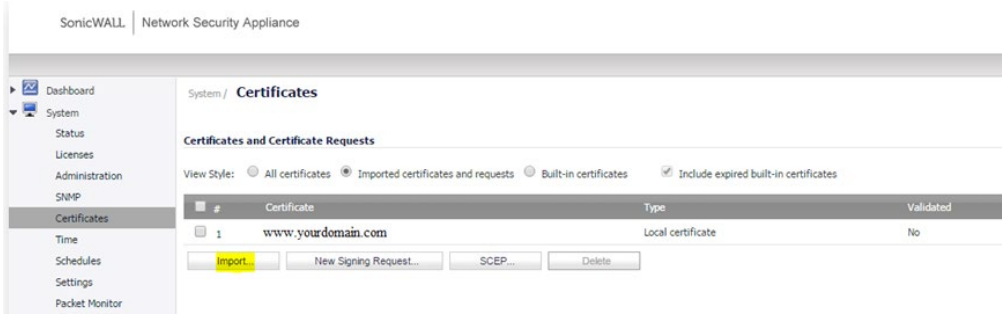


Ilustración 38. Importación de certificados (I)

b) En *Import Certificate,* seleccionar la opción necesaria, según el formato del fichero y hacer clic en el botón *Choose File*.

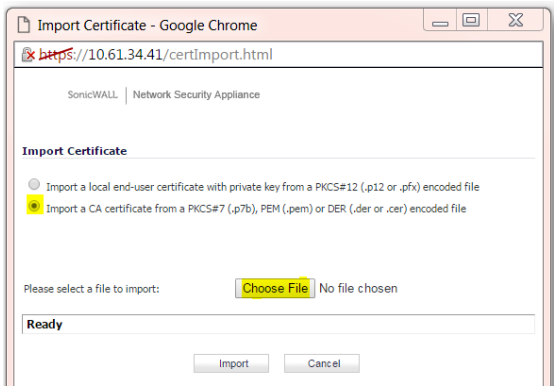


Ilustración 39. Importación de certificados (II)

c) Seleccionar el fichero y hacer clic en *Import*.

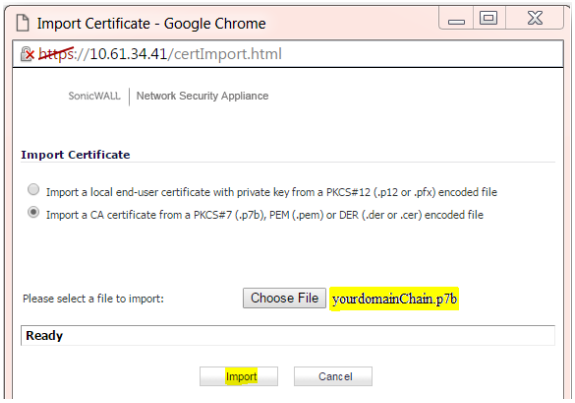


Ilustración 40. Importación de certificados (III)

d) El certificado ahora debería de aparecer como *Validated: Yes*.

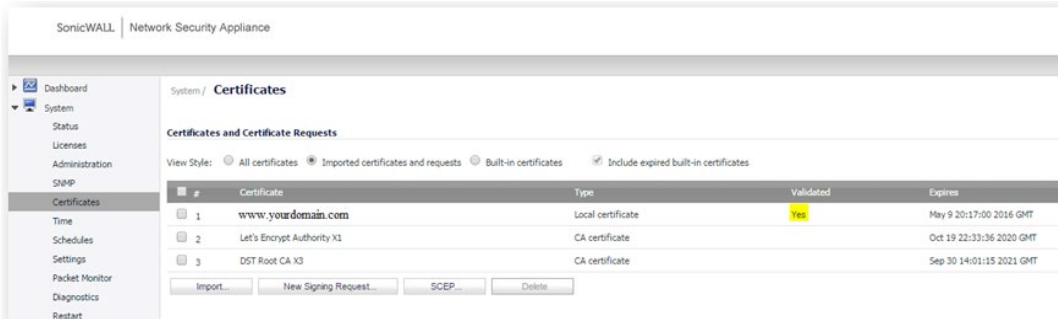


Ilustración 41. Importación de certificados (IV)

e) Reiniciar el dispositivo y verificar que el certificado sigue apareciendo como *Validated*.

5.6.4 VALIDACIÓN DE CERTIFICADOS

5.6.4.1 VALIDACIÓN DE CERTIFICADOS CON CRL (CERTIFICATE REVOCATION LIST)

150. El producto realiza la verificación de certificados mediante CRL de manera automática, siempre que el propio certificado incluya la URL para la descarga de la lista de revocación. En algunos casos puntuales, este proceso podría fallar y habría que hacer la importación del fichero CRL de manera manual, y se ha de seguir el siguiente orden:

a) En caso que el certificado final y el de su CA Intermediaria ya están importados (si el CSR se genera desde el dispositivo).

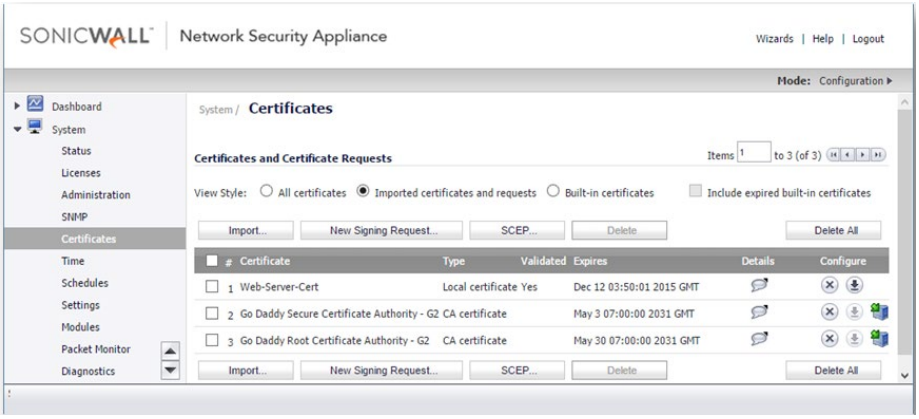


Ilustración 42. Configuración de CSR (I).

b) Obtener la URL de la lista CRL de la pestaña *Details* del propio certificado en el atributo *CRL Distribution Points*.

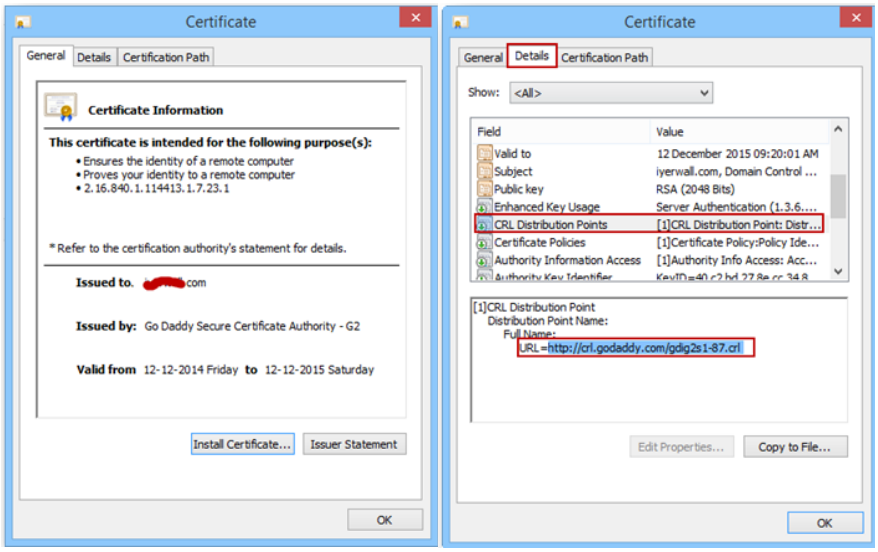


Ilustración 43. Configuración de CSR (II)

c) Descargar el fichero CRL desde dicha URL.

d) Hacer clic en el icono CRL del certificado de la CA Intermediaria.

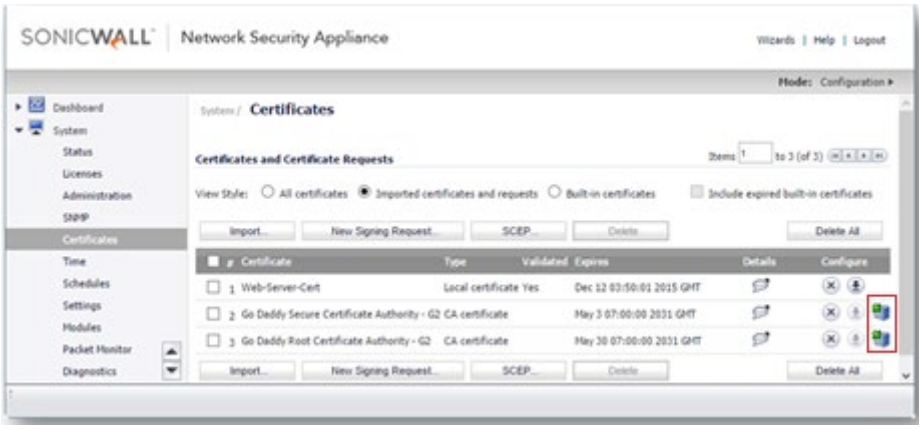


Ilustración 44. Configuración de CSR (III)

e) Especificar el fichero CRL descargado anteriormente (también se podría introducir directamente la URL de descarga).

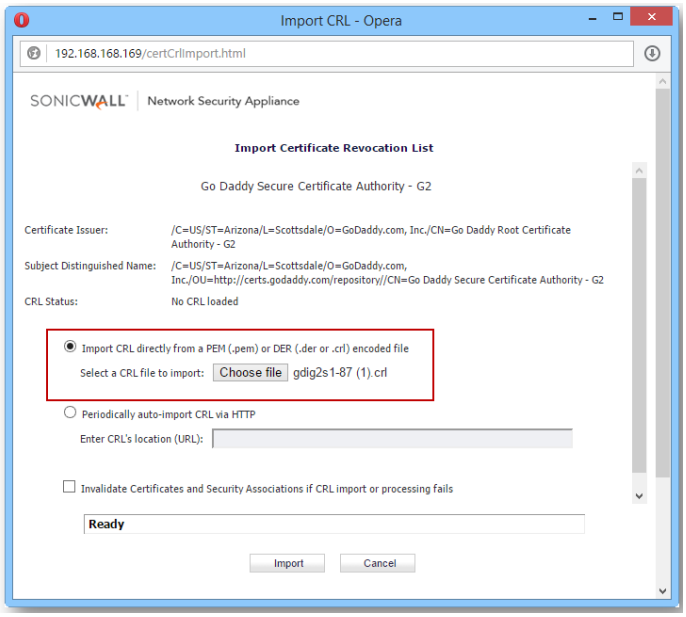


Ilustración 45. Configuración de CSR (IV)

f) Hacer clic en *Import* para importar el fichero CRL.

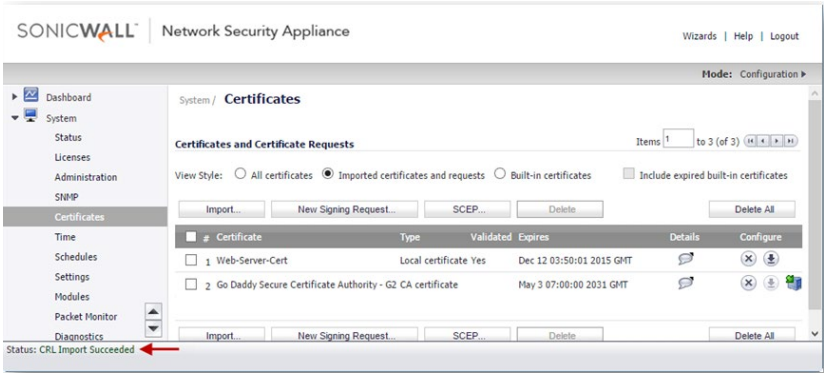


Ilustración 46. Configuración de CSR (VI)

5.6.4.2 VALIDACIÓN DE CERTIFICADOS CON OCSP (*ONLINE CERTIFICATE STATUS PROTOCOL*)

151. La principal desventaja de las listas de revocación de certificados (CRL) es la necesidad de actualizaciones frecuentes para mantener actualizada la CRL de cada cliente. Estas actualizaciones frecuentes aumentan en gran medida el tráfico de red cuando cada cliente descarga la CRL completa. Dependiendo de la frecuencia de las actualizaciones de CRL, puede existir un período de tiempo cuando un certificado es revocado por la CRL pero el cliente no ha recibido la actualización de CRL y permite que se utilice el certificado.

152. El Protocolo de Estado de los Certificado en Línea (OCSP - *Online Certificate Status Protocol*) determina el estado actual de un certificado digital sin utilizar una CRL.

OCSP permite al cliente o la aplicación determinar directamente el estado de un certificado digital identificado. Esto proporciona información más oportuna sobre el certificado de lo que es posible con las CRL. Además, cada cliente normalmente solo verifica unos pocos certificados y no incurre en la sobrecarga de descargar una CRL completa para solo unas pocas entradas. Esto reduce en gran medida el tráfico de red asociado con la validación de certificados.

153. Para que el producto actúe como un cliente OCSP para un OCSP Responder, el certificado de CA debe cargarse, según se ha visto en los apartados previos.

154. La configuración de OCSP del dispositivo se puede configurar a nivel de política o globalmente. Para configurar la verificación OCSP a nivel Global, es necesario habilitar la opción de "*Enable OCSP Checking*" desde el menú *Manage > VPN > Advanced Settings*. Para configurar la verificación OCSP para políticas de VPN individuales, es necesario hacerlo desde la pestaña *Advanced* de la página de configuración de la política VPN.

    a) Seleccionar la opción de *Enable OCSP Checking*.

    b) Especificar la URL del servidor OCSP Responder, por ejemplo http://192.168.168.220:2560 donde 192.168.168.220 es la dirección IP de su servidor OCSP y 2560 es el puerto de operación predeterminado para el servicio de respuesta OCSP de OpenCA.

5.7 AUTENTICACIÓN CON 2FA

155. Para incrementar la seguridad en el proceso de autenticación de usuarios, **se debe, siempre que sea posible, implementar autenticación de doble factor (2FA).** El producto soporta varias opciones de 2FA, entre las que se encuentran *One Time Passwords* (OTP), *Tokens Físicos* o *Time-Based OTP* (TOTP).

5.7.1.1 ONE TIME PASSWORD (OTP)

156. **One-Time Password (OTP)** es un esquema de autenticación de dos (2) factores que utiliza contraseñas aleatorias generadas por el sistema, además de las credenciales estándar de nombre de usuario y contraseña. Una vez que los usuarios envían las credenciales de inicio de sesión básicas correctas, el sistema genera una contraseña de un solo uso que se envía al usuario a una dirección de correo electrónico predefinida. El usuario debe recuperar la contraseña de un solo uso de su correo electrónico y luego introducirla en la pantalla de inicio de sesión.

157. Cada código OTP es de un solo uso. Siempre que un usuario ingresa exitosamente un nombre de usuario y contraseña válidos, se elimina cualquier código OTP existente para esa cuenta. Los códigos OTP no utilizados caducan según el valor de tiempo de espera (*Inactivity Timeout*) configurado en el menú *Users > Settings > User Sessions*. Los administradores pueden habilitar la autenticación OTP para usuarios y grupos locales.

158. OTP no se puede configurar para usuarios de *Global VPN Client* (GVC). En su lugar, los usuarios de GVC pueden usar *tokens* RSA para la autenticación con doble factor. Para más información, consultar la guía *Cómo configurar la autenticación 2FA con RSA para la autenticación con clientes VPN – REF31*.

159. Para utilizar la autenticación con OTP, el dispositivo debe tener acceso a un servidor SMTP configurado correctamente. Esta configuración se puede realizar desde el menú *Log Settings > Automation*:

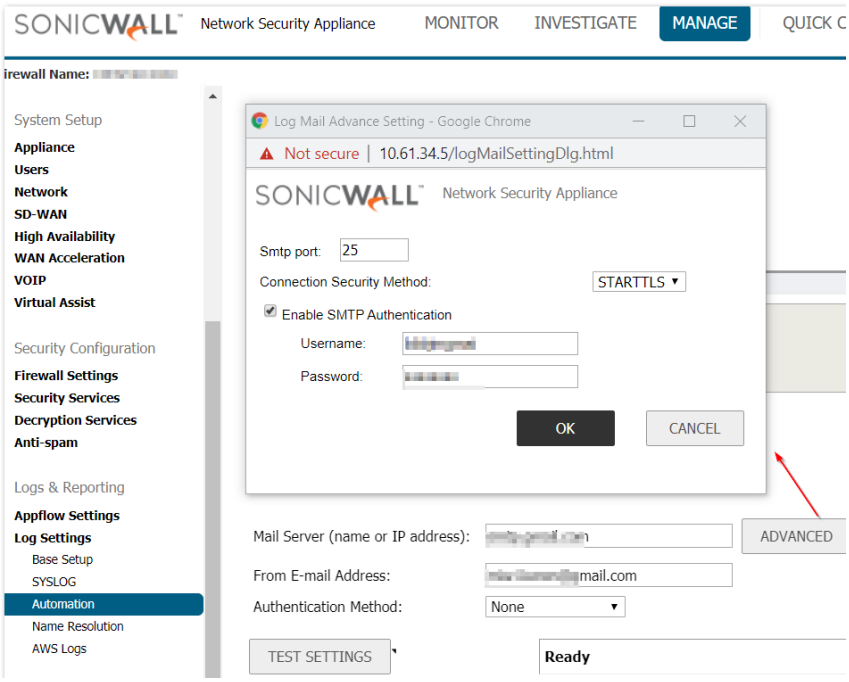


Ilustración 47. Configuración de OTP (I)

160. Para habilitar OTP a un solo usuario o grupo, es necesario editar el usuario o grupo correspondiente:

a) Ir a *Manage > Users > Local Users and Groups.*

b) Activar la casilla de *Require One-Time Password*.

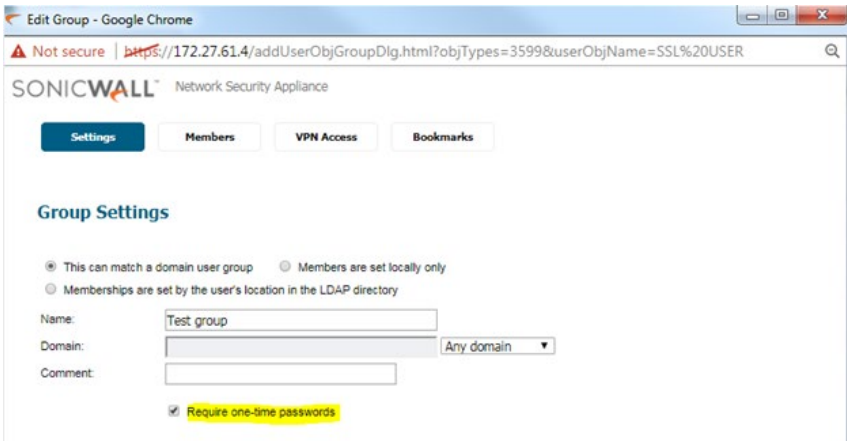


Ilustración 48. Configuración de OTP (II)

161. Si se trata de usuarios y grupos de LDAP, el dispositivo puede averiguar la dirección de correo asociada a cada usuario consultándoselo al servidor LDAP; pero en el caso de usuarios locales, es necesario introducir manualmente la dirección de correo asociada a cada usuario si se quiere hacer uso de la funcionalidad de OTP.

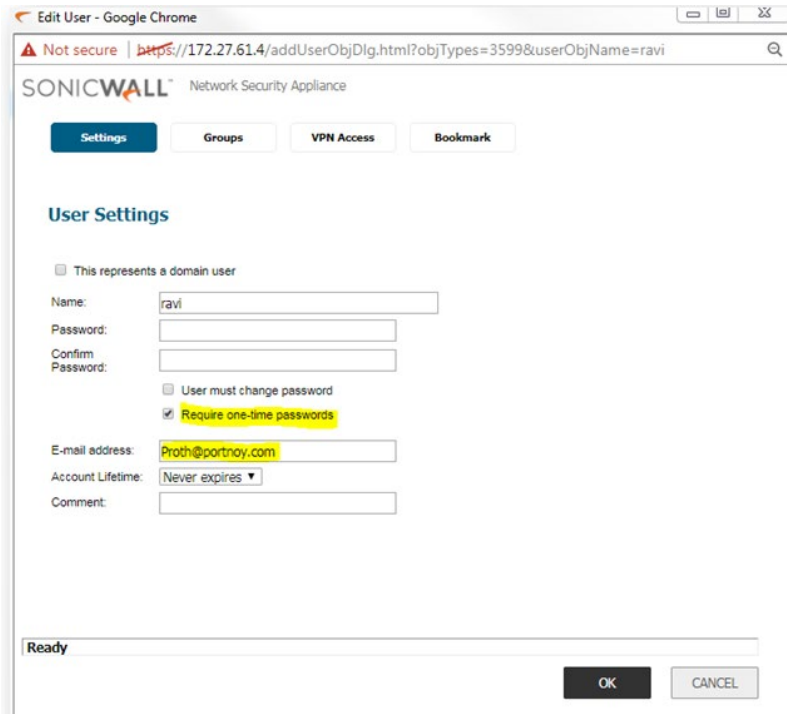


Ilustración 49. Configuración de OTP (III)

162. Cuando un usuario con OTP habilitado intenta iniciar sesión en SSL-VPN, aparecerá el siguiente mensaje después de que el usuario haya introducido sus credenciales.

Ilustración 50. Configuración de OTP (IV)

163. Simultáneamente, se enviará un código temporal a la dirección de correo electrónico de ese usuario. Utilizar el código OTP enviado por correo electrónico para finalizar el procedimiento de autenticación.

5.7.1.2 TOKENS FISICOS

164. Es posible integrar el producto con soluciones 2FA de terceros basadas en tokens físicos como RSA o *Quest Defender*.

165. Debido a que requiere configurar tanto el producto, como los tokens físicos, se recomienda seguir las siguientes guías de configuración:

    a) *Cómo configurar la autenticación 2FA con RSA para la autenticación con clientes VPN – REF31-*

    b) *Cómo configurar la autenticación 2FA con Quest Defender para la autenticación con clientes VPN – REF32*.

5.7.1.3 *TIME-BASED ONE TIME PASSWORD* (TOTP)

166. Otro de los mecanismos de 2FA más utilizados y más sencillo de configurar es *Time-Based One Time Password*, o TOTP, que se apoya en aplicaciones gratuitas como *Google Authenticator* o *Microsoft Authenticator*.

167. Para habilitar la autenticación 2FA mediante TOTP, simplemente habría que editar un usuario o grupo y seleccionar el método *TOTP* en el parámetro *One-time password method*:

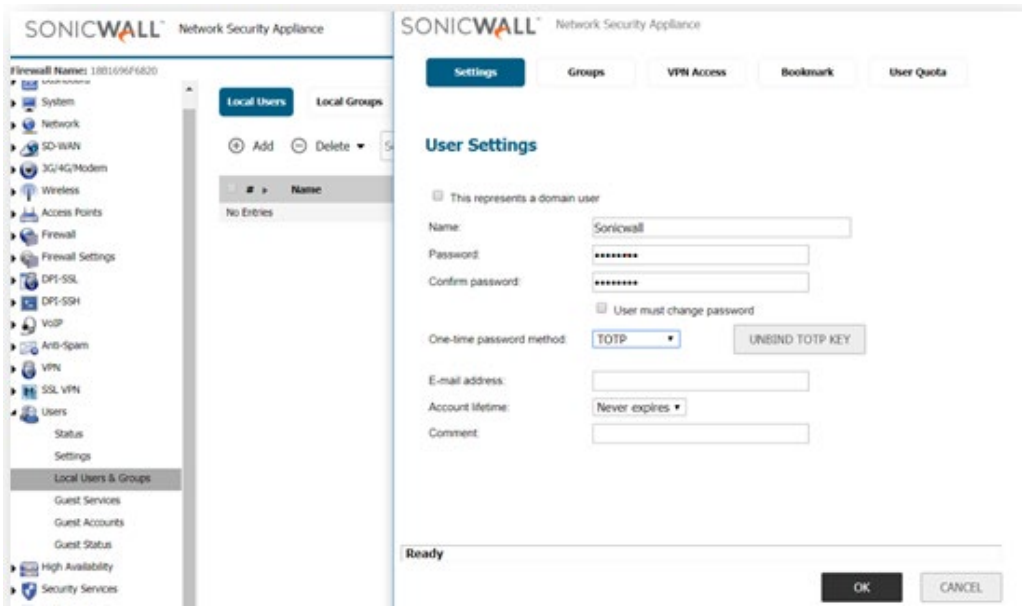


Ilustración 51. Configuración de TOTP (I)

168. Una vez que se instala en el móvil la aplicación correspondiente (*Google Authenticator* o Microsoft Authenticator), cuando el dispositivo pida credenciales de autenticación, se tendrán que introducir las credenciales:

Ilustración 52. Configuración de TOTP (II)

169. Y lo siguiente que aparecerá es una pantalla con un código QR y las instrucciones para finalizar el proceso de autenticación.

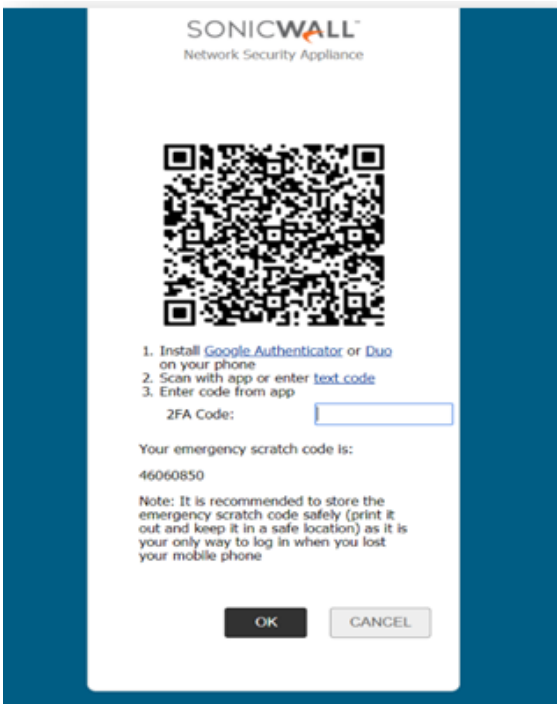


Ilustración 53. Configuración de TOTP (III).

170. El detalle sobre autenticación de usuarios mediante TOTP se puede consultar la nota técnica.

5.8 SINCRONIZACIÓN HORARIA

171. **Se debe hacer uso de NTP para la sincronización horaria del producto**. Se configura desde el menú *System > Time* y está habilitado de forma predeterminada.

172. El dispositivo utiliza automáticamente la configuración de la zona horaria para elegir los servidores apropiados de una lista interna de servidores NTP. Los nombres de los servidores no son visibles en la GUI de administración web.

173. También es posible usar servidores NTP personalizados. Para ello:

a) Ir a *System > Time.*

b) Hacer clic sobre *Add* e introducir la información del servidor: los nombres de host (FQDN) o las direcciones IP de sus servidores NTP a continuación.

c) Habilitar la opción "*Only use custom NTP servers*" si se quiere evitar el uso de cualquiera de los servidores NTP integrados en el dispositivo.

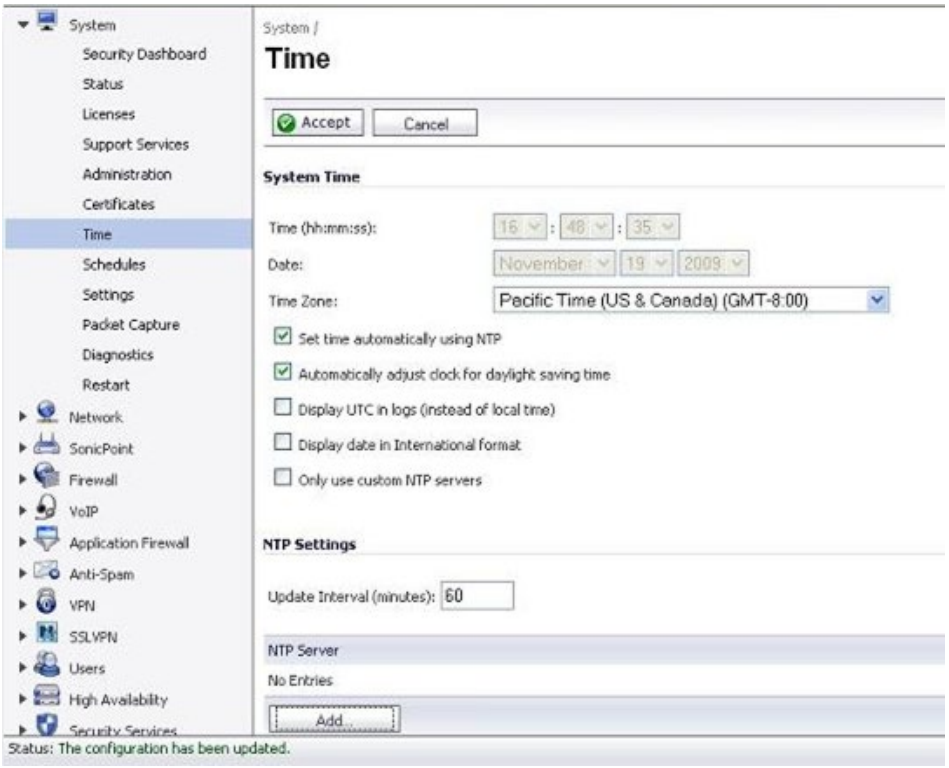


Ilustración 54. Configuración de NTP

174. El dispositivo debe poder enviar tráfico a Internet para la resolución DNS de los nombres de host del servidor NTP y para el protocolo NTP en sí (123/udp).

5.9 ACTUALIZACIONES

175. En el menú *Manage > Firmware & Backups* se puede encontrar la siguiente información:

Ilustración 55. Actualizaciones del dispositivo (I).

a) *Current Firmware Version. Firmware* actual del dispositivo.

b) *Firmware Load Date*. Fecha y hora de cuando fue instalado el firmware.

c) *Firmware Build Date*. Fecha y hora de cuando fue se creó el firmware.

d) *Configuration Date*. Fecha y hora del último cambio en la configuración.

e) *Username*. Usuario que instaló o actualizó el firmware.

f) *Boot*. Haciendo clic en el icono de *Boot* se reinicia el dispositivo con la versión de firmware correspondiente a esa misma fila.

g) *Firmware Actions*. Haciendo clic en el icono de *Download* se puede descargar el firmware a un equipo local.

h) Las actualizaciones de *firmware* se realizan de forma manual, y para verificar si hay actualizaciones disponibles, **es necesario buscar la versión de *firmware* más reciente en el centro de descargas** (*Download Center*) de la cuenta de *Mysonicwall* en la que esté registrado el cortafuegos.

176. Las actualizaciones de *firmware* debe realizarlas manualmente un usuario administrador. Para ello se deberá comprobar periódicamente en el centro de descargas (*Download Center*) la existencia de nuevas versiones del *firmware* y realizar la descarga desde dicha página para posteriormente actualizar el sistema.

177. Haciendo clic en el botón de *Upload Firmware* se puede actualizar el *firmware* del dispositivo.

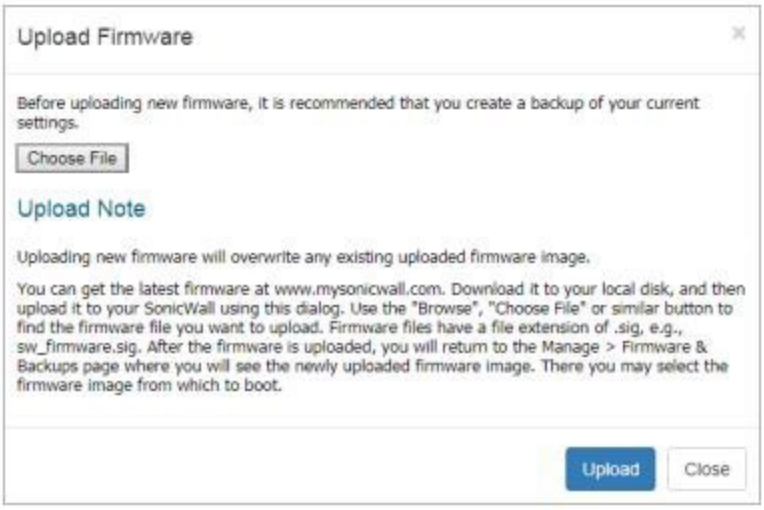


Ilustración 56. Actualizaciones del dispositivo (II)

178. Al subir una nueva imagen de *firmware* se sobrescribirá cualquier imagen de *firmware* que se haya subido previamente.

179. Si la imagen de *firmware* se ha subido con éxito y es un fichero válido, se verá el siguiente mensaje en la barra de estado del navegador:

180. En este punto se verifica la firma digital de la imagen de *firmware*. Si la verificación falla, se mostrará un mensaje de error.

181. Una vez subido el nuevo *firmware*, se puede instalar arrancando el equipo en valores de fábrica o reutilizando la configuración actual. Esto se puede decidir haciendo clic en el botón de *Boot*.

182. El dispositivo mostrará un par de mensajes informativos:

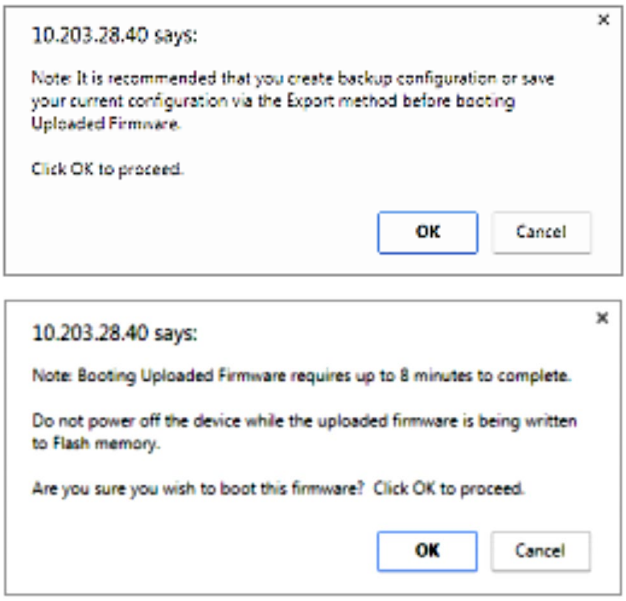


Ilustración 57. Actualizaciones del dispositivo (III)

183. Tras hacer clic en *OK*, el dispositivo se reiniciará. Una vez reiniciado el dispositivo, se debe verificar que el *firmware* se ha actualizado correctamente.

184. En cuanto a la actualización de las bases de datos de firmas de los servicios de seguridad, de forma predeterminada el dispositivo comprueba automáticamente los servidores de firmas cada 60 minutos.

185. Las actualizaciones de firmas se realizan de forma segura. Primero el dispositivo debe autenticarse con una *Pre-Shared Secret*, creada durante el registro del dispositivo en Mysonicwall. La conexión se realiza a través de HTTPS, junto con la verificación completa del certificado del servidor.

186. Si no desea el comportamiento predeterminado de verificar las actualizaciones de firmas cada hora, puede habilitar la opción *Reduce Anti-Virus traffic for ISDN connections* (menú *Manage > Security Services > Base Setup*) para verificarlas cada 24 horas. Sin embargo, se recomienda que esta actualización se realiza con la mayor periodicidad posible.

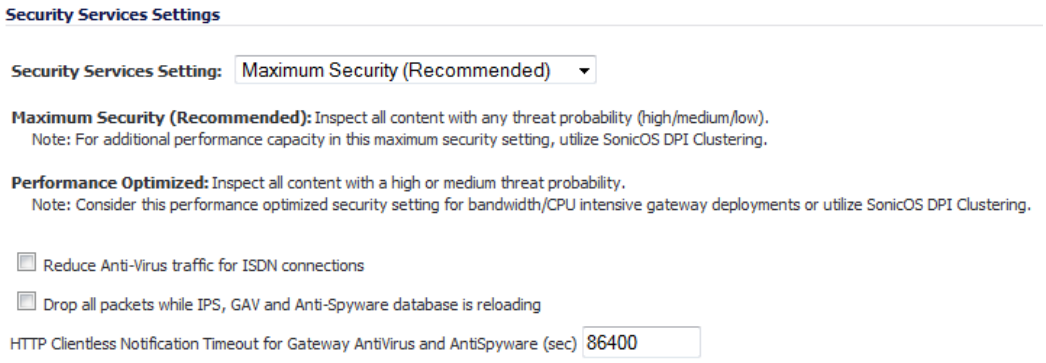


Ilustración 58. Actualizaciones del dispositivo (IV)

5.10 SNMP

187. El producto soporta SNMPv2 y SNMPv3. **Para una mayor seguridad, se debe usar SNMPv3.** Para forzar el uso obligatorio de SNMPv3:

a) Ir al menú *Manage > Appliance > SNMP.*

b) Hacer clic en el botón *Configure*.

c) Se abrirá una ventana emergente. Ir a la pestaña *Advanced*.

d) Seleccionar la casilla *Mandatory Require SNMPv3.*

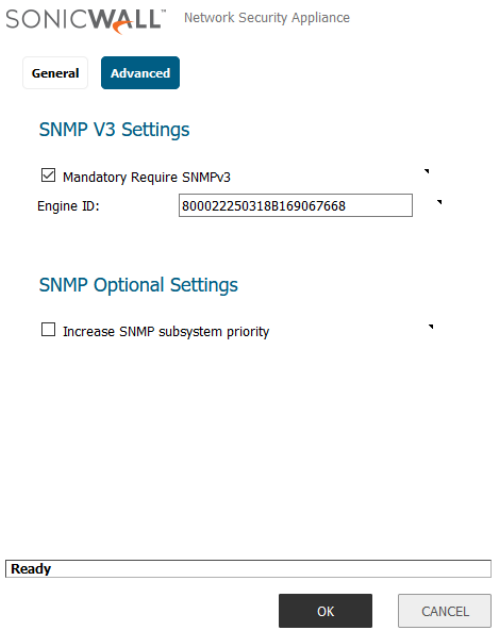


Ilustración 59. Configuración de SNMP

188. El detalle sobre la configuración de usuarios y grupos del servicio SNMP se puede consultar la guía *Cómo configurar SNMPv3 – REF33*.

5.11 ALTA DISPONIBILIDAD

189. Para configurar Alta Disponibilidad por *hardware* (*Hardware High Availability* - HA), se deben cumplir los siguientes requisitos:

a) Los dispositivos Principal (*Primary*) y de Respaldo (*Backup*) deben ser exactamente el mismo modelo de cortafuegos. Actualmente **no se admite la combinación de diferentes tipos de *hardware*.**

b) Es necesario que los dispositivos Principal y de Respaldo ejecuten la misma versión del *firmware*. Puede producirse inestabilidad del sistema si las versiones de *firmware* no están sincronizadas y es posible que algunas funciones de alta disponibilidad no funcionen correctamente.

c) Ambas unidades deben registrarse en la misma cuenta y *tenant* de *Mysonicwall*, y establecer una asociación de tipo HA entre ellas (en *Mysonicwall*) antes de conectarlas físicamente. Si ambos dispositivos no están correctamente vinculados en *Mysonicwall*, el dispositivo Primario no podrá compartir las licencias con el Secundario, por lo tanto, en un evento de *Failover*, el cortafuegos Secundario no podrá proporcionar el mismo nivel de seguridad que el primario, y dejarían de funcionar todos aquellos servicios que requieran la activación de alguna licencia para su funcionamiento. En el siguiente enlace se puede consultar cómo asociar dos equipos en HA durante el registro. En el siguiente enlace se puede consultar cómo asociar dos equipos en HA en caso de estar ya registrados.

d) La dirección IP virtual de la WAN (la que está vinculada al dispositivo activo en cada momento), así como las IPs asignadas a las interfaces WAN de cada cortafuegos (en caso de estar configuradas) deben de utilizar direccionamiento estático. La configuración de Alta Disponibilidad (HA) no permite la asignación dinámica de IPs por parte del ISP.

e) Se requieren tres direcciones IP para la LAN:

   i. Dirección IP Virtual (LAN). Es el direccionamiento configurado en la interfaz X0 de la unidad primaria. Esta es la puerta de enlace predeterminada para todos los dispositivos configurados en la red LAN. Al acceder a la interfaz de administración con esta dirección IP, iniciará sesión en el dispositivo que está activo, ya sea la unidad principal o la unidad de respaldo.

   ii. Dirección IP Gestión Primario (LAN). Configurable desde el menú *High Availability > Monitoring Settings*. Esta es la dirección IP utilizada para administrar la unidad principal a través de la interfaz LAN, independientemente del estado activo o inactivo de la unidad.

   iii. Dirección IP Gestion Secundario (LAN). Configurable desde el menú *High Availability > Monitoring Settings*. Ésta es la dirección IP utilizada para administrar la unidad de respaldo a través de la interfaz LAN, independientemente del estado activo o inactivo de la unidad.

f) Se requiere al menos una dirección IP para la WAN:

   i. Dirección IP Virtual (WAN). Es el direccionamiento configurado en la interfaz X1 de la unidad principal. Al acceder a la interfaz de administración con esta dirección IP, iniciará sesión en el dispositivo que está activo, ya sea la unidad principal o la unidad de respaldo.

   ii. Dirección IP Gestión Primario (WAN) – Opcional. Configurable desde el menu *High Availability > Monitoring Settings*. Esta es la dirección IP que se utiliza para administrar la unidad principal a través de la interfaz WAN, independientemente del estado activo o inactivo de la unidad. Esto requiere que tenga una dirección IP enrutable adicional disponible. Esto es opcional, ya que siempre puede administrar la unidad activa con una dirección IP WAN estática.

   iii. Dirección IP Gestión Secundario (WAN) – Opcional. Configurable desde el menú *High Availability > Monitoring Settings*. Esta es la dirección IP utilizada para administrar la unidad de respaldo a través de la interfaz WAN, independientemente del estado activo o inactivo de la unidad. Esto requiere que tenga una dirección IP enrutable adicional disponible. Esto es opcional, ya que siempre puede administrar la unidad activa con una dirección IP WAN estática.

190. En caso de hacer uso de una sola IP WAN, tener en cuenta que el dispositivo de respaldo, cuando está en modo inactivo, no podrá usar NTP para sincronizar su reloj interno.

191. La siguiente figura muestra un ejemplo de cómo conectar dos cortafuegos SonicWall en Alta Disponibilidad (*High Availability*) con sincronización de estados (*Stateful Synchronization*). Las unidades están conectadas directamente a través sus puertos HA dedicados.

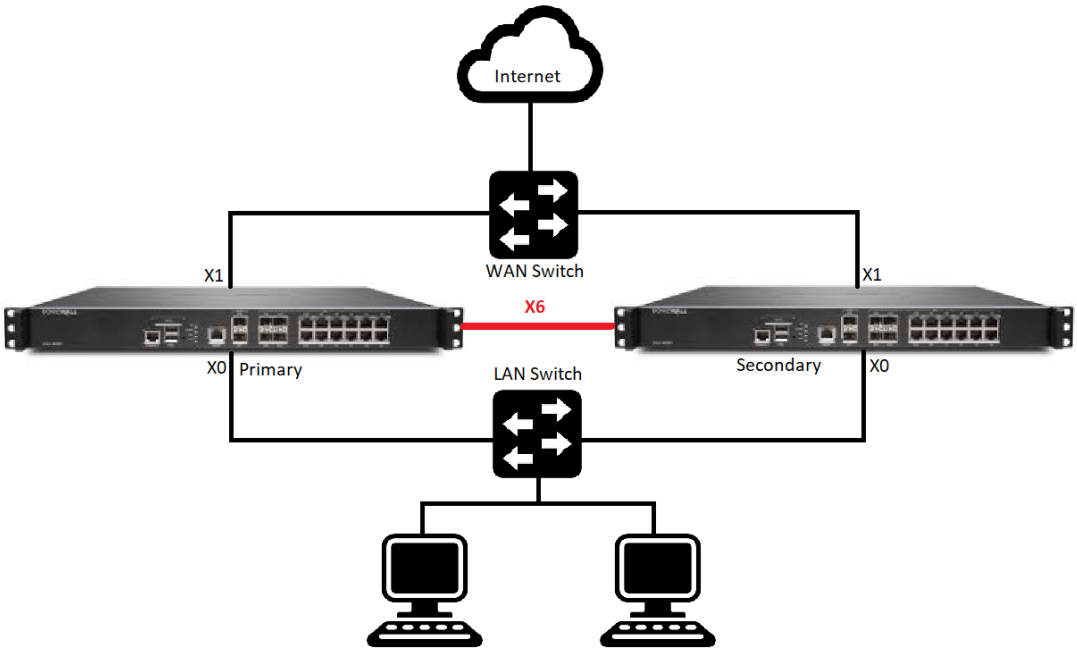


Ilustración 60. Esquema de despliegue de Alta Disponibilidad

192. Las interfaces LAN (X0) están conectadas a un *switch* en el segmento LAN. Las interfaces WAN (X1) están conectadas a otro *switch*, que se conecta a Internet (también se podría usar el mismo *switch* y segmentar las diferentes zonas con VLANs). Las interfaces de alta disponibilidad dedicadas se conectan directamente entre sí.

193. A continuación, se mencionan algunos consejos adicionales:

a) Se deben agregar direcciones IP de "Monitorización" (*Management IP's*) a X0. Estas IP de "*supervisión*" son necesarias al menos en la interfaz X0, para que la unidad inactiva tenga una IP y, por lo tanto, una ruta a Internet a través de la unidad activa para obtener actualizaciones de firmas, sincronizar licencias con *MySonicWall*, etc. También le permiten iniciar sesión en la unidad inactiva cuando sea necesario, pero cualquier interfaz puede tener IPs de monitorización para eso; asegúrese de habilitar "*Allow Management on Primary/Secondary IPv4 Address*" en cualquier interfaz desde la que desee administrar el cortafuegos. Sin embargo, solo una interfaz WAN participa en la tabla de enrutamiento del *firewall*, por lo que no puede acceder a la unidad inactiva a través de su IP de monitoreo X0 a menos que su IP de origen esté en la misma subred.

   i. Si no se utiliza X0 (es decir, todo lo que se utiliza son interfaces SFP + de 10 Gbps), asigne a X0 una dirección IP "virtual" o "flotante" (desde el menú *Network > Interfaces*), y direcciones IP de supervisión con un

direccionamiento IP que no se utilice en la red de producción, y conecte ambos cortafuegos directamente entre sí a través de X0 con un cable Ethernet. El *firewall* utilizará la interfaz X0 como enlace de respaldo para el intercambio de *heartbeats* entre ambos dispositivos en caso de que no puedan comunicarse a través de la interfaz de control HA dedicada.

ii. Se pueden configurar IP de "Monitorización" en todas las interfaces utilizadas, incluidas las subinterfaces o VLANs.

b) Utilice la opción de Virtual Mac (menú *High Availability > Base Setup > General*). Esto ayuda a reducir el tiempo de convergencia de ARP durante un evento de *Failover*.

c) Interfaces MGMT (Gestión HTTPS) y HA: La unidad Activa siempre escuchará lo que está configurado para la interfaz MGMT (menú *Network > Interfaces > "IP Address (Primary)"*). Asimismo, la unidad Inactiva o Pasiva solo responderá a la "*IP Address* (*Secondary*)". Si la unidad Secundaria o Pasiva se activa debido a un evento de *failover*, responderá a lo que está configurado como la "IP *Address* (*Primary*)".

i. Esto sigue una lógica diferente de las otras interfaces donde tiene las 3 direcciones IP: la IP "virtual", que es siempre la IP a la que responde la unidad Activa; y luego las 2 IPs de monitorización, donde la "*Primary* IPv4 *Address*" siempre permanece con el dispositivo Primario independientemente de si está activo o inactivo, y la "*Secondary* IPv4 *Address*" siempre permanece con el dispositivo Secundario independientemente de su estado.

ii. Además, como se mencionó anteriormente para todas las demás interfaces de zona no WAN, no se puede acceder a la unidad Inactiva a través de la "*IP Address (Secondary)"* de MGMT a menos que provenga de una máquina en la misma subred.

d) *Preemtp Mode*: Si no se está interesado en la sincronización de estados con Stateful HA, puede seleccionar la opción de *Enable Preempt Mode*. Esta función controla el comportamiento a la hora de volver al estado normal después de un evento de *Failover*. Si está habilitada, el dispositivo Primario asumirá el rol Activo en cuanto se recupere de la situación que provocó el evento de *Failover*; en caso contrario, el dispositivo secundario mantendrá el rol Activo incluso después de que el dispositivo Primario se haya recuperado, y continuará sumiendo este rol hasta que se vuelva a producir otro evento de *Failover*.

No se recomienda habilitar la opción de *Preempt Mode* cuando está habilitada la sincronización de estados (*Stateful Synchronization*) en la configuración de Alta Disponibilidad, ya que el modo *Preempt Mode* fuerza sincronizaciones adicionales del tráfico, lo que no se recomienda en redes de alta carga.

194. El detalle sobre la configuración de Alta Disponibilidad de Hardware se puede consultar en la guía *Cómo configurar Alta Disponibilidad – REF34*.

5.12 AUDITORÍA

5.12.1 REGISTRO DE EVENTOS

195. El producto puede registrar eventos a nivel local, así como también enviar eventos a uno o más servidores *Syslog* externos configurados por el administrador.

196. Desde el menú *Manage > Log Settings > Base Setup* se puede configurar el nivel de *logging*, así como los protocolos que se quieren usar para la recepción de alertas en cada uno de los eventos, marcando las casillas de selección correspondientes (*GUI, Alert, Syslog, Ipfix* y *Email*).

197. Se recomienda seleccionar la casilla *Syslog* para todos los tipos de log y configurar un servidor de auditoría externo tal como se indica en el apartado 5.12.3 ALMACENAMIENTO REMOTO.

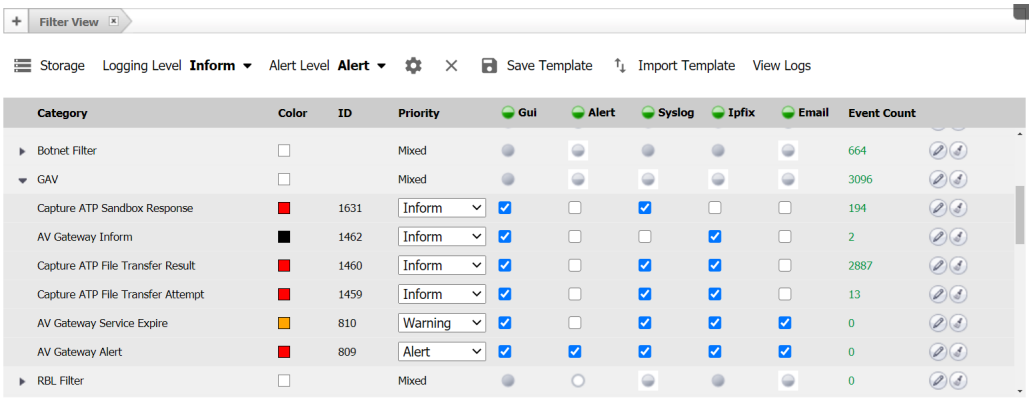


Ilustración 61. Configuración de logs de Auditoría (I)

198. Los eventos registrados localmente se pueden visualizar en tiempo real desde el menú *Investigate > Event Logs*.

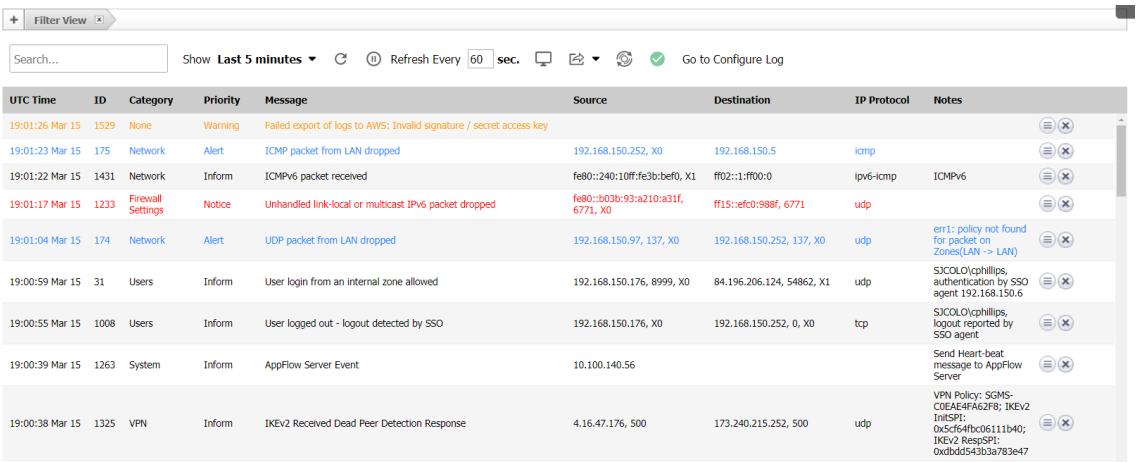


Ilustración 62. Configuración de Logs de Auditoría (II)

199. Los logs o el registro de eventos se pueden exportar presionando sobre el icono . Se mostrarán las opciones de exportación, que son; CSV, texto plano y correo electrónico. Al hacer *clic* sobre las dos (2) primeras se iniciará automáticamente la descarga en el navegador. En el caso de seleccionar a opción *Email* el *firewall* enviará los *logs* por correo electrónico a la cuenta configurada en la opción *Send Log to E-mail Address* que se encuentra en el menú *Manage > Logs & Reporting > Log Settings > Automation*.

200. Además de los eventos que se pueden incluir o excluir desde el menú *Manage > Log Settings > Base Setup*, **se debe habilitar el soporte para *Enhanced Audit Logging***, de forma que el cortafuegos también registrará eventos específicos del modo NDPP (*Network Devices Protection Profile*). El soporte para *Enhanced Audit Logging* se puede habilitar desde el menú *Manage > Appliance > Base Settings*:

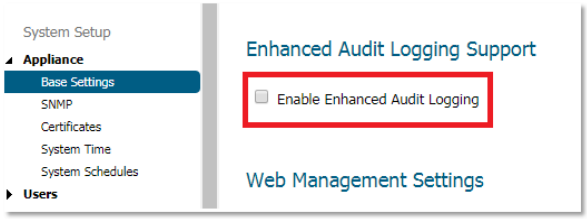


Ilustración 63. Configuración de Logs de Auditoría (III)

201. El detalle sobre la configuración de los requisitos del modo NDPP se puede consultar en la siguiente guía *Cómo habilitar el perfil de protección NDPP – REF35*.

5.12.2 ALMACENAMIENTO LOCAL

202. Los eventos se almacenan en un búfer local de registro continuo de 32 kilobytes. Cuando el búfer se llena, los registros más antiguos se sobrescriben, por lo que, si se quiere tener un registro histórico de eventos es recomendable integrar el dispositivo con un colector *Syslog* o *NetFlow/IPFix* externo. También se puede configurar el dispositivo para que envíe automáticamente los logs por correo electrónico cada vez que se llene el búfer. **Se recomienda hacer uso de un servidor de auditoría externo.**

5.12.3 ALMACENAMIENTO REMOTO

203. Además de mostrar mensajes de eventos en la interfaz gráfica de gestión (GUI), el producto también puede enviar los mismos mensajes a un servidor *Syslog* externo configurado por el administrador.

204. A continuación, se indica cómo configurar el servicio *Syslog* y cómo añadir servidores de auditoría externos.

5.12.3.1 CONFIGURACIÓN DEL SERVICIO SYSLOG

205. Para configurar los ajustes de Syslog en el dispositivo:

a) Ir al menú *Manage > Log Settings > Syslog.*

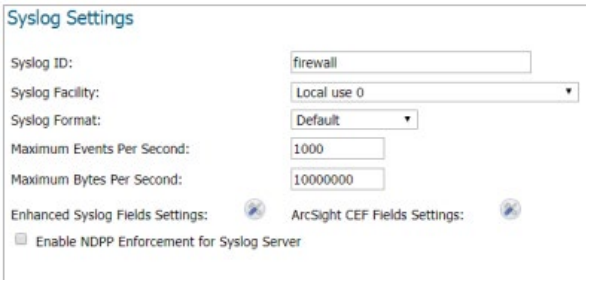


Ilustración 64. Configuración de *Syslog*

b) En el campo *Syslog ID*, introducir el nombre de *Syslog* deseado.

c) El parámetro *Syslog Facility* se puede dejar en su valor por defecto. Sin embargo, opcionalmente, en el menú desplegable *Syslog Facility*, podría seleccionar la función *Syslog* adecuada para la red:

Syslog Facility

Kernel	UUCP Subsystem	Local Use 0
User-Level Messages	Clock Daemon (BSP Linux)	Local Use 1
Mail System	AUTHPRV Security/Authorization Messages	Local Use 2
System Daemons	FTP Daemon	Local Use 3
Security/Authorization Messages	NTP Subsystem	Local Use 4
Messages Generated Internally by syslogd	Log Audit	Local Use 5
Line Printer Subsystem	Log Alert	Local Use 6
Network News Subsystem	Clock Daemon (Solaris)	Local Use 7

Ilustración 65. Niveles de *Syslog*

d) En la opción de *Syslog Format*, seleccionar el formato de log adecuado a su caso:

Syslog formats

Default	Default SonicWall Syslog format. **NOTE:** This format is required for GMS or Reporting software.
WebTrends	WebTrends Syslog format. You must have WebTrends software installed on your system.
Enhanced Syslog	Enhanced SonicWall Syslog format.
ArcSight	ArcSight Syslog format. The Syslog server must be configured with the ArcSight Logger application to decode the ArcSight messages.

Ilustración 66. Formatos *Syslog* disponibles

e) Opcionalmente, especificar el número máximo de eventos en el campo *Maximum Events Per Second*; el número mínimo es 0 por segundo, el máximo es 1000 por segundo y el valor predeterminado es 1000. Esta opción limita los eventos registrados para evitar que el mecanismo de registro interno o externo se sature.

f) Opcionalmente, especificar el número máximo de bytes en el campo *Maximum Bytes Per Second;* el número mínimo es 0 bytes por segundo, el máximo es 1000000000 bytes por segundo y el valor predeterminado es

10000000. Este control limita los datos registrados para evitar que el mecanismo de registro interno o externo se vea abrumado por eventos de registro.

g) Seleccionar *Enable NDPP Enforcement for Syslog Server*.

h) Hacer clic en *Aceptar.*

5.12.3.2 COMO AÑADIR UN SERVIDOR *SYSLOG*

206. Para añadir un servidor *Syslog* en el dispositivo, ir al menu *Manage > Log Settings > Syslog* y hacer clic en el botón *Add*.

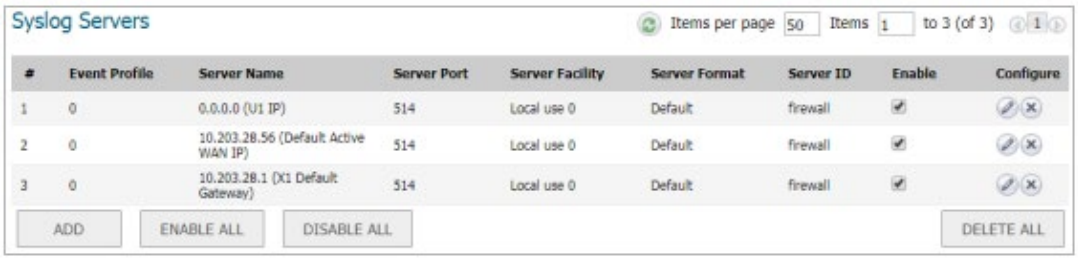


Ilustración 67. Configuración del servidor *Syslog* (I)

207. Rellenar todos los campos que aparecerán en la ventana que se abrirá:

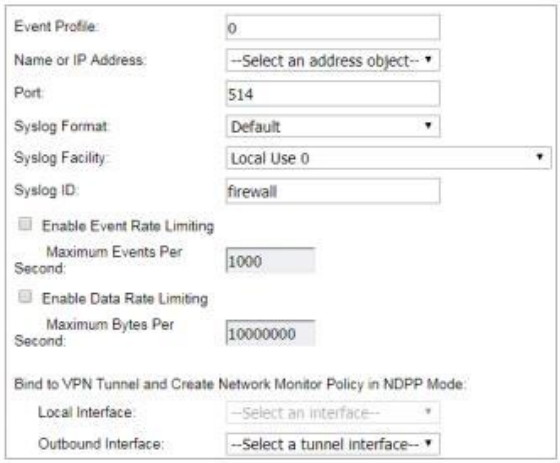


Ilustración 68. Configuración del servidor Syslog (II)

208. El parámetro titulado *Bind to VPN Tunnel and Create Network Monitor Policy in NDPP Mode* configura el dispositivo para enviar el tráfico de *syslog* a través de un túnel IPsec. **Se recomienda la utilización de esta opción**.

5.13 COPIAS DE SEGURIDAD O *BACKUPS*

209. El producto permite realizar copias de seguridad de la configuración tanto a nivel local como en la nube. Estos *backups* se pueden realizar de forma manual, o de forma programada.

210. Las copias de seguridad se pueden realizar desde el menú *Manage > Firmware & Backups*. El detalle sobre cómo realizar copias de seguridad en SonicOS se puede consultar en la guía *Cómo exportar un backup de la configuración REF – 36*. A continuación se indican los principales pasos a seguir.

5.13.1 COPIAS DE SEGURIDAD LOCALES

211. El producto solo soporta una única copia de seguridad local, por lo tanto, si se crea una nueva copia de seguridad, se sobrescribirá la copia anterior. Para realizar una copia de seguridad local, ir a *Manage > Firmware & Backups* y hacer clic en *Create Backup > Local Backup*.

5.13.2 COPIAS DE SEGURIDAD EXTERNAS

212. También se puede realizar una exportación manual haciendo clic en el botón *Import/Export* desde *Configuration > Export Configuration*. Esto servirá para crear una copia de seguridad de la configuración del producto en un fichero.

213. Además de la exportación manual, también se puede programar la exportación de la configuración y enviarla a un servidor FTP externo haciendo clic en el botón *Settings* y configurando los parámetros del servidor FTP. Haciendo clic en el botón *Set Schedule* se podrá programar el envío periódico de la configuración al servidor FTP:

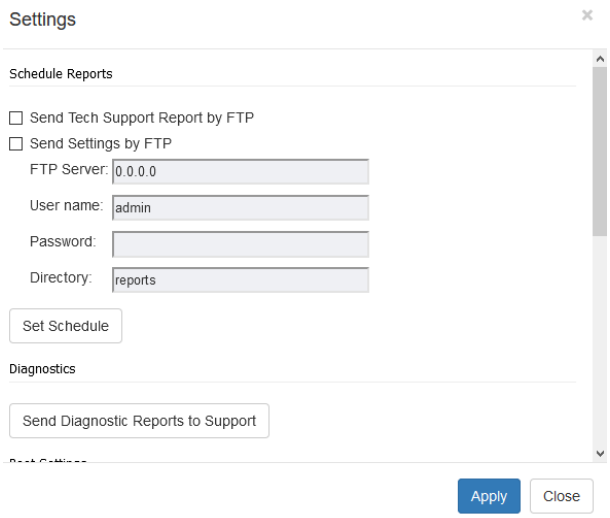


Ilustración 69. Programación de copias de seguridad

5.13.3 COPIAS DE SEGURIDAD EN LA NUBE (*CLOUD BACKUP*)

214. También es posible realizar copias de seguridad periódicas en la nube a través del servicio *Cloud Backup*. Para habilitarlas, simplemente hay que hacer clic en la casilla de verificación *Cloud Backup Enabled*, desde *Manage > Firmware & Backups.*

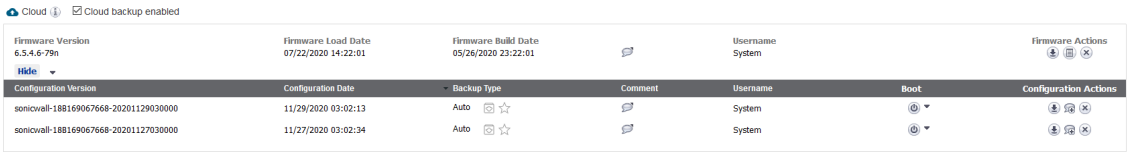


Ilustración 70. Copias de seguridad en la Nube (I)

215. A partir de ese momento, el dispositivo gestionará automáticamente la frecuencia y periodicidad de las copias.

216. Si se desea tener un control más estricto, se pueden programar las copias de seguridad en la nube haciendo clic en el botón *Create Backup > Schedule Backup*. En dicha página se pueden especificar los parámetros de periodicidad de las copias de seguridad.

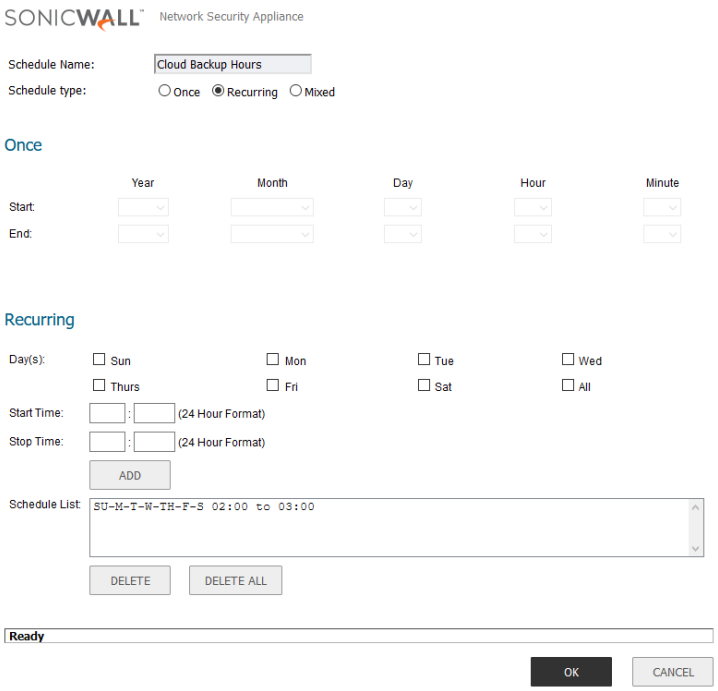


Ilustración 71. Copias de seguridad en la Nube (II)

217. Se destaca que el almacenamiento de copias de seguridad en la nube debe ser aprobado por las políticas de seguridad de la organización. **Se recomienda que el canal entre el dispositivo y el almacenamiento *cloud* esté protegido y la información esté cifrada antes de su envío a la nube.**

5.14 SERVICIOS DE SEGURIDAD

5.14.1 *FIREWALL*

218. Esta sección proporciona una descripción general de las reglas de acceso predeterminadas y las reglas de acceso personalizadas del cortafuegos SonicWall.

Se pueden aplicar reglas a varios tipos de tráfico, como: ICMPv4, ICMPv6, IPv4, IPv6, TCP, UDP.

5.14.2 REGLAS DE ACCESO

219. El menú *Manage* > *Rules* > *Access Rules* proporciona una interfaz de administración de reglas de acceso ordenable.

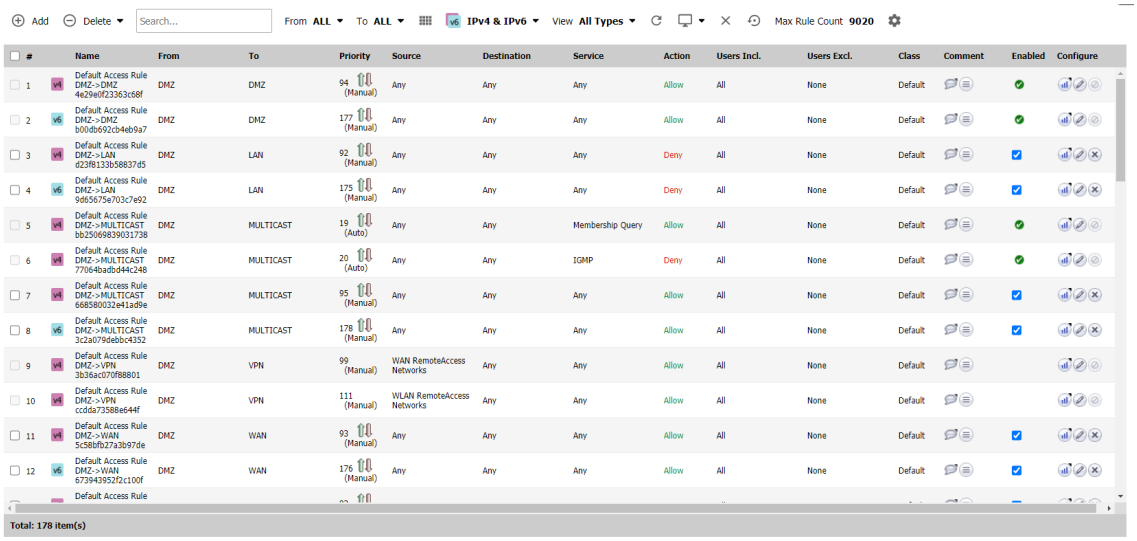


Ilustración 72. Configuración de reglas de acceso

220. Las reglas se clasifican en tablas independientes para cada zona de origen a zona de destino y para IPv4/IPv6. Por lo tanto, todos los tipos de prioridad solo se aplican dentro de la tabla de reglas a la que pertenece la regla.

221. Las reglas de acceso están ordenadas desde las más específicas en la parte superior hasta las menos específicas en la parte inferior de la tabla. En la parte inferior de la tabla está la regla por defecto *Any* que se aplica al tráfico de cualquier origen, cualquier destino y cualquier puerto o servicio.

222. La prioridad de las reglas se puede determinar en el momento de su creación, o posteriormente. Al crear la regla de acceso, se puede escoger entre tres (3) opciones en cuanto a la prioridad (campo *Priority*):

a) *Auto Prioritize*: Sigue la lógica de ordenación por defecto (mayor prioridad a las reglas específicas que a las genéricas).

b) *Insert at the end*: Añade la regla al final de la tabla.

c) *Manual*: Permite introducir un valor numérico que indicaría la posición de la regla dentro de la tabla.

223. Para modificar la prioridad de la regla una vez que ya está creada, simplemente hay que hacer clic en alguna de las flechas de la columna *Priority* de esa regla, e introducir un valor numérico que representa la posición que se desea para esa regla dentro de la tabla:

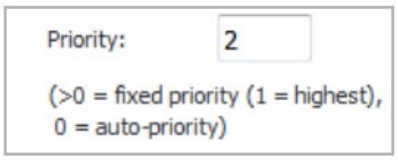


Ilustración 73. Configuración de la prioridad de reglas de acceso

224. Como regla general de seguridad, **se debe crear una regla de denegación aplicada a cualquier interfaz, cualquier zona y para cualquier tráfico con la prioridad más baja**. Esto garantiza que se denegará cualquier tráfico que no coincida con una regla configurada.

5.14.2.1 CONFIGURACIÓN TCP (TCP SETTINGS)

225. La gestión de las conexiones TCP y algunos parámetros relacionados se pueden configurar desde el menú *Manage > Firewall Settings > Flood Protection > TCP Settings*:

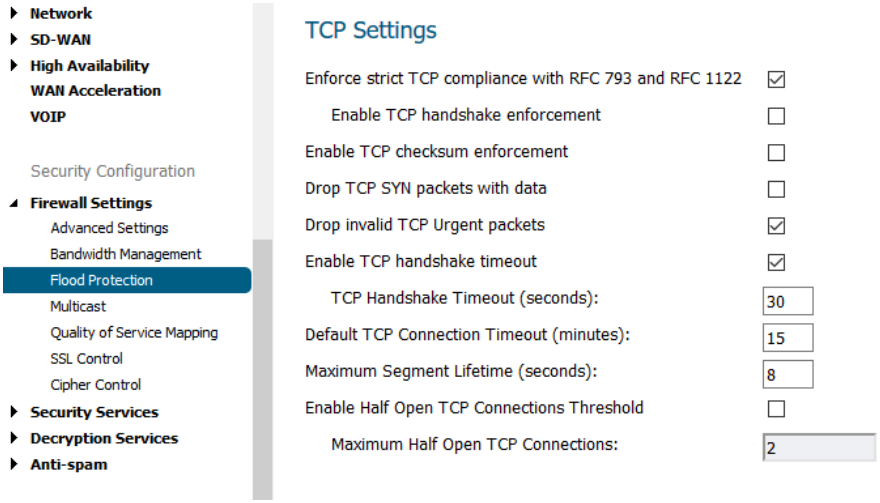


Ilustración 74. Configuración de TCP

226. Cuando se habilita la opción de *Enable Half Open TCP Connections Threshold*, el cortafuegos rastrea y mantiene la información relacionada con el número de conexiones TCP medio abiertas de la siguiente manera:

227. Existe un límite definido administrativamente para conexiones TCP semiabiertas basado en:

a) *TCP Handshake Timeout (seconds)*: Cada conexión TCP semiabierta se elimina si el protocolo de enlace no se completa para cuando se alcanza este tiempo de espera

b) *Maximum Half Open TCP Connections*: Hay un número máximo de conexiones TCP medio abiertas permitidas

228. El cortafuegos utiliza un contador global para rastrear el número de todas las conexiones TCP medio abiertas. Cuando este número alcanza el valor máximo de conexiones TCP medio abiertas, se descartan las nuevas conexiones TCP entrantes.

229. Cuando se habilita la opción de *Enforce strict TCP compliance with RFC 793 and RFC 1122*, el cortafuegos descarta los paquetes TCP que no forman parte de una conexión establecida.

5.14.3 *INTRUSION PROTECTION SERVICE* (IPS)

230. El servicio *Intrusion Prevention Service* (IPS) es un servicio basado en firmas que se configura desde el menú *Manage > Security Services > Intrusion Prevention*, donde se pueden encontrar tres (3) secciones diferentes:

a) *IPS Status*

b) *IPS Global Settings*

c) *IPS Policies*

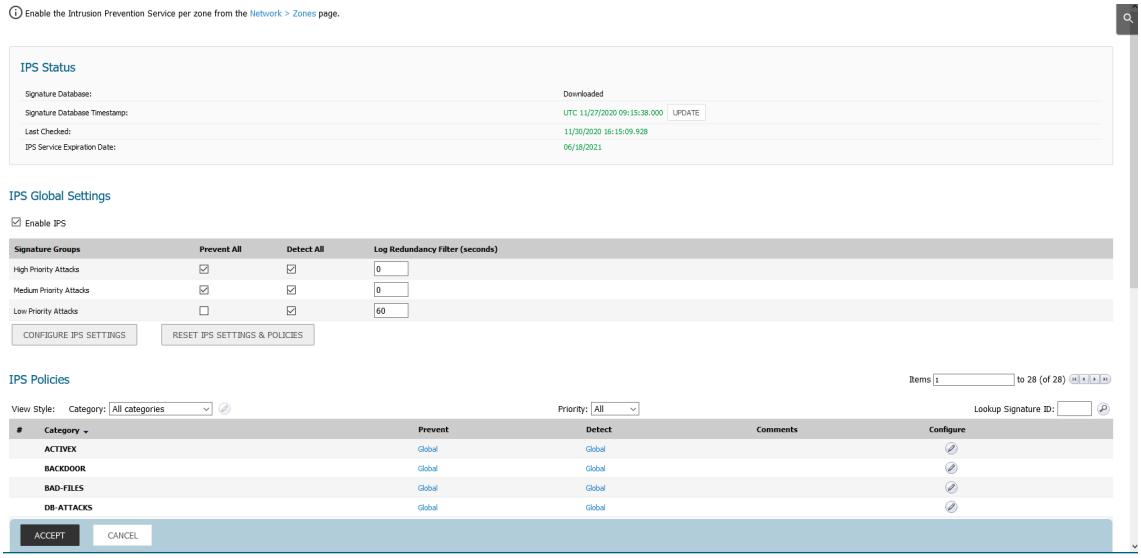


Ilustración 75. Configuración de IPS

5.14.3.1 IPS STATUS

231. La sección *IPS Status* muestra información de estado del servicio IPS y de la base de datos de firmas.

232. El panel de estado de IPS muestra la siguiente información:

a) *Signature database*: indica si la base de datos de firmas se está descargando, se ha descargado o debe descargarse. La base de datos de firmas se actualiza automáticamente aproximadamente una vez por hora. También puede actualizar manualmente la base de datos IPS en cualquier momento haciendo clic en el botón *Update* ubicado en la sección *IPS Status*.

b) *Signature database timestamp:* muestra la última actualización de la base de datos de firmas IPS.

c) *Last checked*: indica la última vez que el cortafuegos comprobó la base de datos de firmas en busca de actualizaciones.

d) *IPS Service expiration date*: indica la fecha en la que vence el servicio IPS. Si su suscripción al servicio de IPS caduca, la inspección IPS se detendrá y la configuración del servicio IPS se elimina del cortafuegos. Después de renovar el servicio IPS, esta configuración se restaura automáticamente al estado configurado previamente.

5.14.3.2 IPS GLOBAL SETTINGS

233. Todas las firmas del servicio IPS están categorizadas según su nivel de riesgo, que puede ser *High, Medium* o *Low*. A la hora de configurar el servicio IPS a nivel global, se pueden especificar acciones diferentes en función del nivel de riesgo de las firmas. Las acciones que se pueden configurar son Detectar y/o Prevenir.

234. **La recomendación general es habilitar la detección (*Detect All*) para todas las categorías (*High, Medium* y *Low*), y habilitar la prevención (*Prevent All*) sólo para las categorías *High* y *Medium*.**

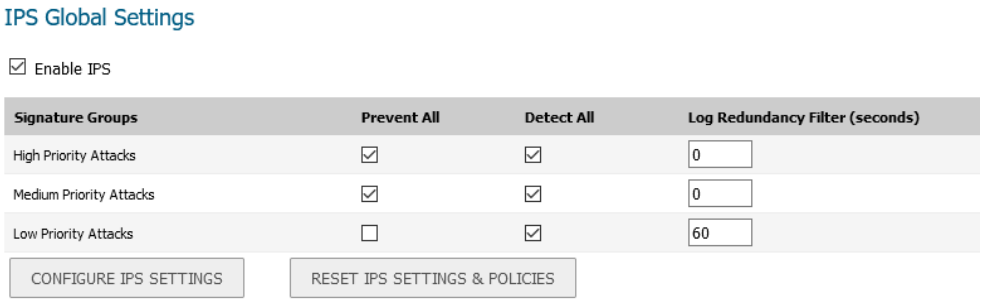
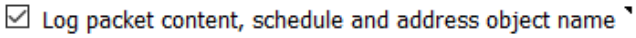


Ilustración 76. Configuración general de IPS

235. Para habilitar logs detallados del servicio IPS, navegar al menú *https://<ip_cortafuegos>/diag.html* y habilitar la opción de *Log packet contents, schedule and address object name.*



5.14.3.3 PACKET DISSECTION

236. El menú *Packet Dissection* permite aplicar filtros en base a diferentes características de los paquetes, como las siguientes:

a) ***Name***: nombre de la regla.

b) ***Enable Negative Matching***: le permite examinar solo el tipo de tráfico especificado en la regla.

c) ***Family***: tipo de análisis a realizar.

d) ***Header Field***: el encabezado que se examinará.

e) ***Data Type***: tipo de datos que se examinarán.

f) ***Numeric***: valor de examen.

Ilustración 77. Configuración de filtros en los paquetes en IPS.

237. Es posible examinar los siguientes campos:

a) ***IPv4***: *Version; Header Length; Packet Length; ID; IP Flags; Fragment Offset; Time to Live (TTL); Protocol; Header Checksum; Source Address; Destination Address; y IP Options.*

b) ***IPv6***: *Version; traffic class; flow label; payload length; next header; hop limit; source address; destination address; routing header; home address options.*

c) ***ICMP***: *Type; Code; Header Checksum; y el resto de la cabecera (varía en función del tipo y el código del mensaje ICMP).*

d) ***ICMPv6***: *Type; Code; y Header Checksum.*

e) ***TCP***: *Source port; destination port; sequence number; acknowledgement number; offset; reserved; TCP flags; window; checksum; urgent pointer; y TCP options.*

f) ***UDP***: *Source port; destination port; length; y UDP checksum.*

5.14.3.4 FIRMAS PERSONALIZADAS

238. Es posible crear firmas personalizadas a través de *Custom Objects* y *Custom App Rules*. Para crear un objeto personalizado (*Custom Object*), ir al menú *Manage > Objects > Match Objects > botón Add > Match Object*, y en el campo *Match Object Type* de la lista desplegable, seleccionar la opción de *Custom Object*.

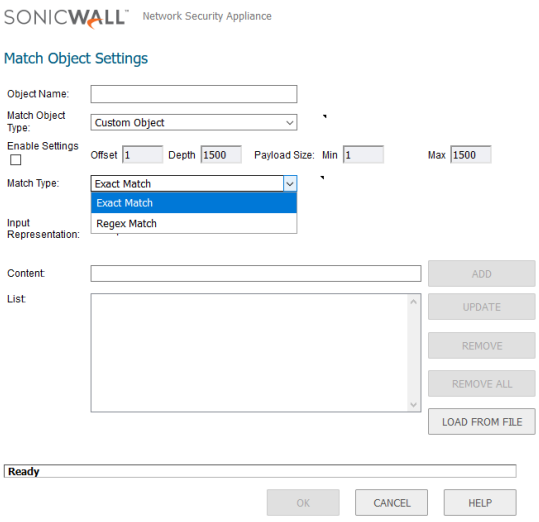


Ilustración 78. Creación de firmas personalizadas (I)

239. Una vez creado el objeto, habrá que crear una regla de App Firewall (menú *Rules* > *App Rules*) haciendo uso de ese objeto e indicándole algunos parámetros adicionales como: zonas origen/destino, IPs origen/destino, puertos, usuarios incluidos/excluidos, horas del día, etc.

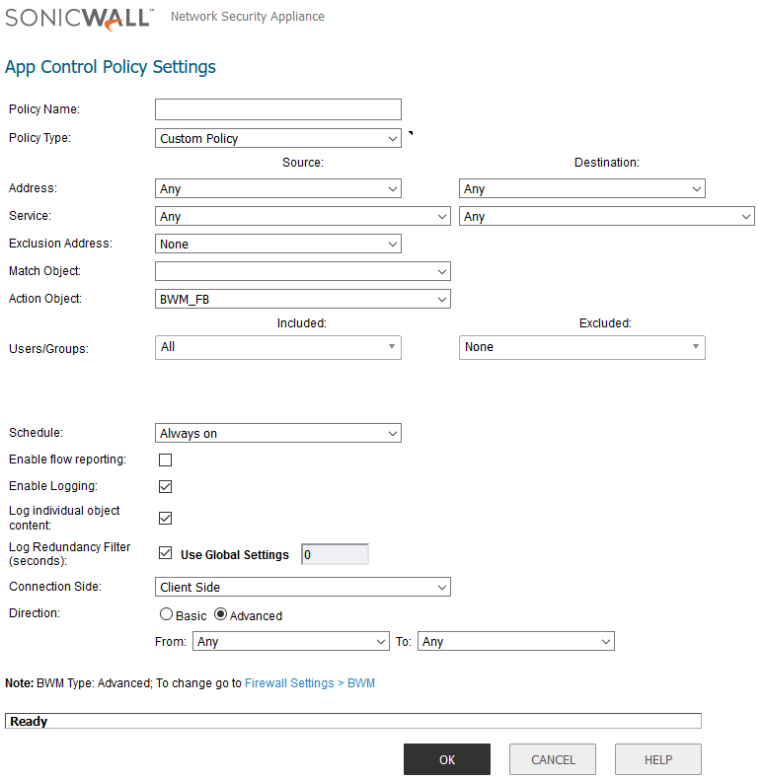


Ilustración 79. Creación de firmas personalizadas (II)

5.14.3.5 DETECCIÓN DE ESCANEOS

240. Seguir estos pasos para configurar la detección de escaneos a nivel de IP, de puertos TCP, de puertos UDP y de tipos ICMP:

a) Ir a *https://<ip_cortafuegos>/diag.html*.

b) Desplazarse hasta la sección de *NDPP Port Scan Settings*.

c) Seleccionar la opción *Enable NDPP Port Scan Detection*.

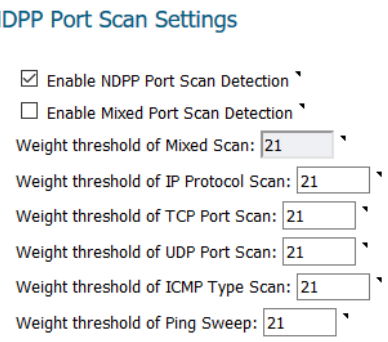


Ilustración 80. Configuración de la detección de escaneos

5.14.4 SERVICIO ANTIVIRUS

241. El servicio de *antimalware* de *Sonicwall* está basado en tres (3) servicios que se combinan entre sí. El servicio de *Gateway* AV (GAV), es un servicio basado en firmas que se apoya en una base de datos local de más de 20.000 firmas; el servicio de Cloud AV, también es un servicio basado en firmas, pero ofrecido desde la nube y con una base de datos de más de 75 millones de firmas; y el servicio de *Capture ATP*, es una solución de *sandboxing* multimotor que se suministra desde la nube y también en formato *on-premise* a través de un dispositivo físico.

5.14.4.1 SERVICIO GATEWAY ANTIVIRUS (GAV)

242. El servicio *Gateway Antivirus* (GAV) de los cortafuegos *Sonicwall* soporta un gran número de protocolos TCP, y permite configurar este servicio de manera granular para los protocolos más comunes, como HTTP, FTP, NetBIOS/CIFS, SMTP, POP3 o IMAP.

243. Para una mayor protección, se recomienda activar este servicio para todos los protocolos (incluido *TCP Stream*) y en ambos sentidos (*Inbound* y *Outbound*).

244. Estos parámetros son configurables desde el menú *Manage* > *Security Services* > *Gateway Antivirus*:

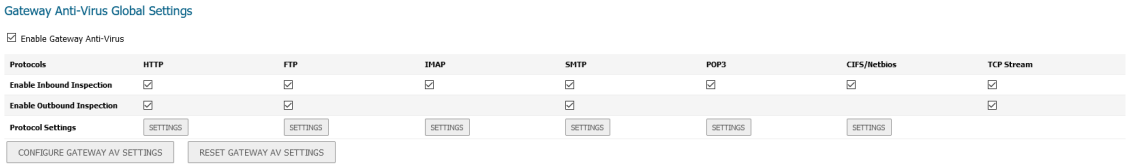


Ilustración 81. Configuración del antivirus (I)

245. Para cada uno de estos protocolos, se pueden configurar algunas opciones avanzadas como el bloqueo de fichero *MS Office* que contengan macros, ficheros ejecutables empaquetados o ficheros comprimidos. La configuración recomendada de estas opciones, dependerá del tipo de actividad de la red en cuestión.

246. Para acceder a este tipo de configuraciones avanzadas, hacer clic en el botón de *Settings*, en el protocolo que nos interese configurar:

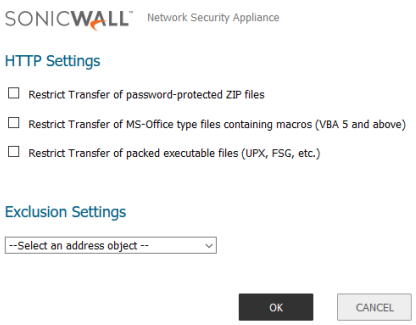


Ilustración 82. Configuración del antivirus (I)

247. También se pueden crear exclusiones a nivel de IP usando *Address Objects* y *Address Groups* desde la sección de *Gateway AV Exclusion List* (Menú *Manage > Security Services > Gateway AV > Botón Configure Gateway AV Settings*)

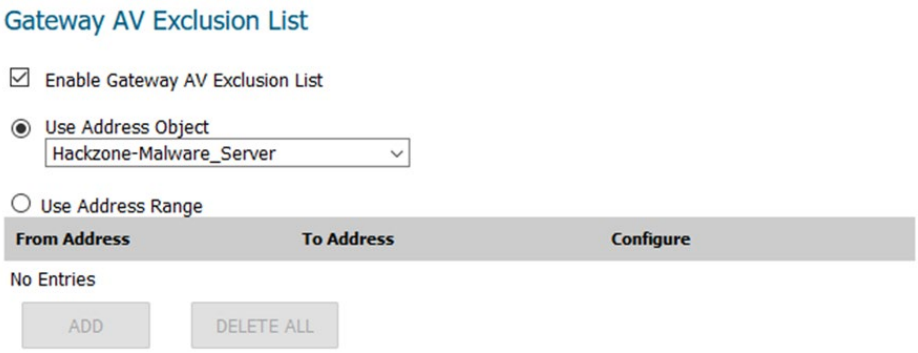


Ilustración 83. Configuración del antivirus (III)

5.14.4.2 SERVICIO CLOUD ANTIVIRUS (CLOUD AV)

248. Se puede activar también el servicio de Cloud AV desde el menú *Manage > Security Services > Gateway Antivirus:*

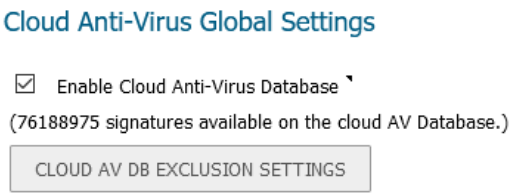


Ilustración 84. Activación de Cloud AntiVirus

249. Haciendo clic en el botón de *Cloud AV DB Exclusion Settings*, se pueden hacer exclusiones de firmas por ID:

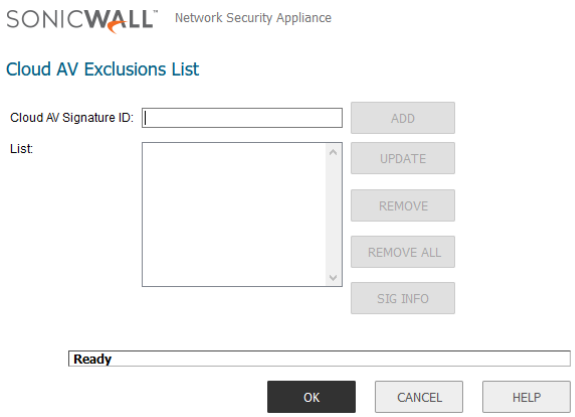


Ilustración 85. Configuración de Cloud AntiVirus

250. El ID de la firma se puede obtener de los logs del cortafuegos (menú *Investigate > Event* Logs).

5.14.5 SERVICIO *ANTISPYWARE* (AS)

251. Las opciones de configuración del servicio de *AntiSpyware (AS)* son una mezcla de las opciones que aporta el servicio GAV y el servicio IDS/IPS. Por un lado, todas las firmas del servicio AS están también categorizadas por nivel de riesgo: *High, Medium* y *Low*, y se puede habilitar o deshabilitar tanto la detección como la prevención (de manera similar al servicio IDS/IPS); y por otro lado, se puede activar este servicio en función del protocolo: HTTP, FTP, IMAP, SMTP y POP3 (de manera similar al servicio GAV). **Para una mayor protección, es recomendable activar tanto la detección como la prevención para las firmas High, Medium y Low y para todos los protocolos y también en sentido saliente (*Enable Inspection of Outbound Spyware Communication*).**

252. Este servicio se puede configurar desde el menú *Manage > Security Services > Antispyware*:

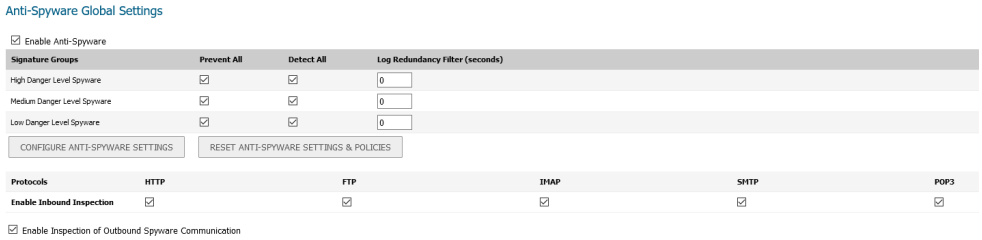


Ilustración 86. Configuración de *Anti-Spyware* (I)

253. Haciendo *clic* en el botón de *Configure AntiSpyware Settings*, se podrán definir exclusiones basadas en direcciones o rangos IP para que los dispositivos de ese rango queden excluidos de este servicio en su totalidad:

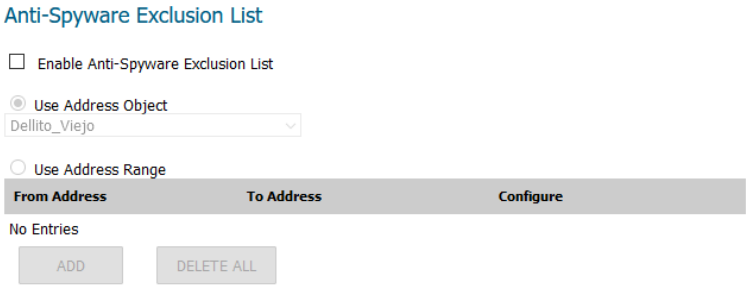


Ilustración 87. Configuración de *Anti-Spyware* (II)

254. Desde esta sección también se podrán realizar búsquedas de firmas en la base de datos local y editar su configuración para modificar los parámetros de detección y prevención (al igual que se hace con las firmas de IPS):

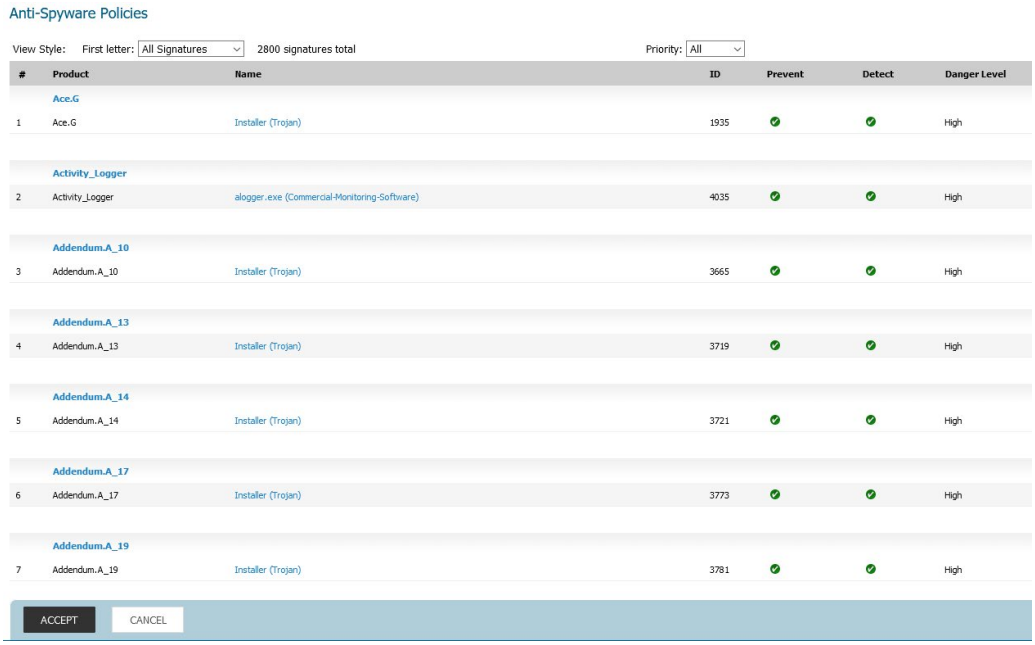


Ilustración 88. Configuración de Anti-Spyware (III)

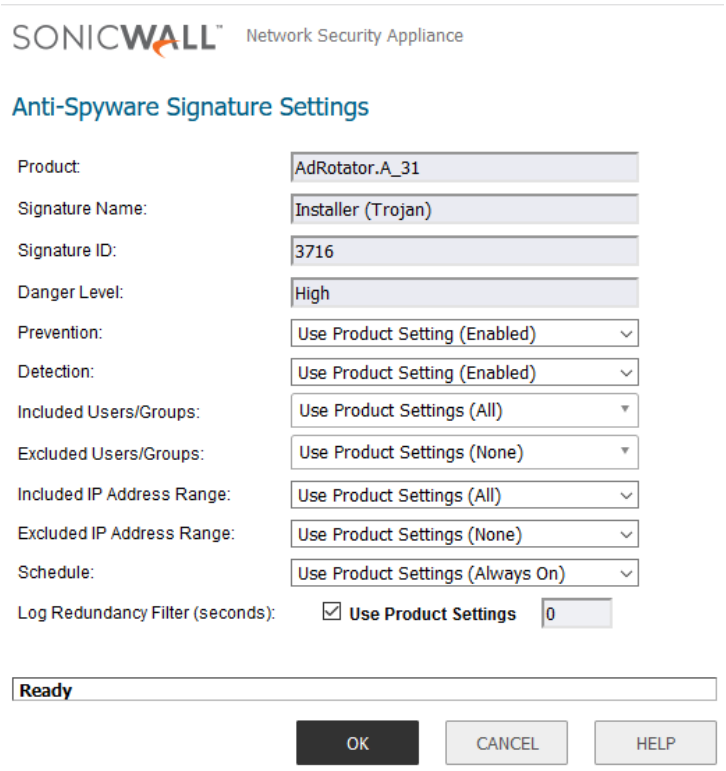


Ilustración 89. Configuración de Anti-Spyware (VI)

255. Desde el log del cortafuegos, se verá una alerta (en amarillo) cada vez que este servicio detecte y/o bloquee un componente considerado *spyware*, y desde allí se podrá acceder al menú de configuración de esa firma en concreto para modificar los parámetros de configuración (de la misma manera que con las firmas de IPS).

5.14.6 SERVICIO *GEOIP*

256. Es posible aplicar bloqueos por países a través del servicio de GeoIP. Este servicio se puede configurar a nivel global o a nivel de reglas de acceso. Esto se puede decidir desde el menú *Manage > Security Services > Geo-IP Filter > Pestaña Settings*:

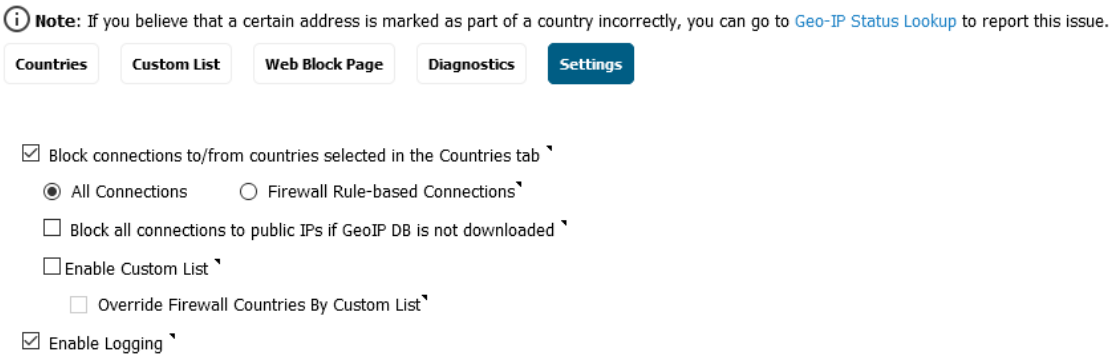


Ilustración 90. Configuración de *GeoIP* (I)

257. Si se escoge el modo de configuración global, se aplicará la configuración de países bloqueados definidos en la pestaña *Countries* del mismo menú. Si, por el contrario, se habilita la opción *Firewall Rule-based Connections*, entonces la configuración de GeoIP se aplicará a nivel de regla de acceso, pudiendo configurar en cada regla si se quiere heredar la configuración global definida en la pestaña *Countries*, o si se quiere una configuración de GeoIP específica para el tráfico que haga match con esa regla de acceso concreta.

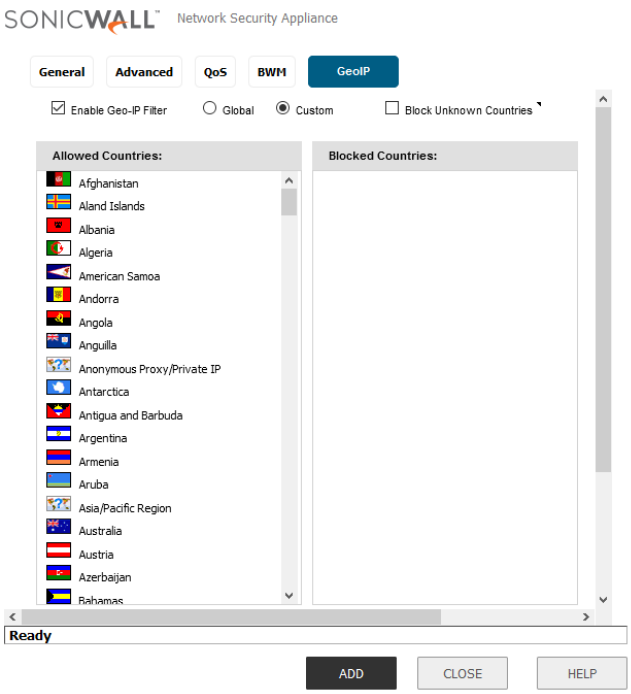


Ilustración 91. Configuración de *GeoIP* (II)

258. En cualquier caso, el procedimiento a la hora de añadir países a la lista de bloqueo es el mismo, simplemente hay que arrastrar y soltar los países que se quieran bloquear, de la lista de la izquierda a la lista de la derecha.

259. Si se quieren bloquear también IPs cuya procedencia sea de algún país desconocido (o no exista ninguna vinculación de esa IP a ningún país), habría que seleccionar la opción de *Block Unknown Countries*.

6. FASE DE OPERACIÓN

260. En este apartado se indican algunas de las operaciones más importantes a realizar para **mantener una protección segura** con un firewall de Sonicwall basado en SonicOS 6.5.2 y 6.5.4.

261. La operación correcta debe incluir los procedimientos necesarios para realizar las siguientes tareas:

a) Comprobaciones periódicas del *hardware* y *software* para asegurar que no se ha introducido *hardware* o *software* no autorizado. El *firmware* activo deberá verificarse periódicamente para comprobar que está libre de software malicioso, además de verificar su actualización.

b) Actualizaciones del *software* de los equipos, con el fin de garantizar sus capacidades, tanto en las capacidades de reconocimiento de aplicaciones, como en la prevención de amenazas.

c) Mantenimiento de los registros de auditoria, protegidos de borrados y modificaciones no autorizadas, y solamente el personal IT de seguridad autorizado podrá acceder a los mismos. La información de auditoria se guardará en las condiciones y por el periodo establecido según la normativa de seguridad vigente.

d) Auditar como mínimo los eventos especificados en la normativa de referencia y aquellos procedentes del análisis de riesgos.

e) Backups automáticos periódicos.

f) Es recomendable, en concreto, llevar a cabo revisiones de los cambios en la configuración del sistema y revisar los logs correspondientes a dichos cambios.

262. Para más información, puede consultar las guías de operación y administración en el portal de soporte:

https://www.sonicwall.com/support/technical-documentation/?language=English&resources=Administration%20Guide,Operations%20Guide

7. CHECKLIST

263. En esta sección se incluye una lista de verificación con cada una de las recomendaciones sobre configuraciones seguras que se han comentado a lo largo del documento:

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*	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Habilitar modo seguro FIPS	☐	☐	
Configuración de servidores de autenticación (Local, LDAP, RADIUS)	☐	☐	
Configuración de política de contraseñas	☐	☐	
Configuración de administradores	☐	☐	
Configuración de acceso seguro a la gestión	☐	☐	
Configuración de zonas e interfaces	☐	☐	
Configuración segura de servicios (*DHCP, SNMP*, etc.)	☐	☐	
Configuración de reglas de acceso	☐	☐	
Configuración de protocolos seguros (*TLS, IPSec*, etc.)	☐	☐	
Gestión de los certificados	☐	☐	
Configuración servicio *Antivirus*	☐	☐	
Configuración servicio *Antispyware*	☐	☐	
Configuración servicio IPS	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Configuración *Flood Protection*	☐	☐	
Configuración Control de Aplicaciones	☐	☐	
Configuración DPI-SSL/DPI-SSH	☐	☐	
Configuración servicio *GeoIP*	☐	☐	
Configuración servicio *antispam* (RBL)	☐	☐	
Configurar sistema de logs o registro de eventos	☐	☐	
Crear y exportar copias de seguridad de la configuración	☐	☐	

8. REFERENCIAS

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

265. Otros links interesantes, también citados en este documento son:

REF1 Guía de instalación en rack de SonicWall TZ600.

https://www.sonicwall.com/techdocs/pdf/tz600-rack-mount-tray-assembly-installation-guide.pdf

REF2 Página de acceso a MySonicWall.

http://www.mysonicwall.com/

REF3 Cómo diagnosticar problemas de conectividad con los servidores de licenciamiento.

https://www.sonicwall.com/support/knowledge-base/troubleshooting-license-manager-connectivity-issues/170503593981866/

REF4 Guía de configuración rápida TZ 600

https://www.sonicwall.com/techdocs/pdf/tz600-quick-start-guide.pdf

REF5 Guía de despliegue con Zero Touch

https://www.sonicwall.com/techdocs/pdf/zero-touch-deployment-guide.pdf

REF6 Guía de configuración inicial

https://www.sonicwall.com/support/knowledge-base/sonicwall-out-of-the-box-setup/170505828413340/

REF7 Guía de configuración inicial con asistente

https://www.sonicwall.com/support/knowledge-base/how-to-set-up-out-of-the-box-without-using-the-setup-wizard/170817105332862/

REF8 Cómo configurar el modo FIPS

https://www.sonicwall.com/support/knowledge-base/how-do-i-enable-fips-mode/170505541129412/

REF9 Diferentes modos de autenticación de usuarios

https://www.sonicwall.com/support/knowledge-base/help-with-user-level-authentication-settings-like-local-users-ldap-radius/170503274714653/

REF10 Cómo configurar la integración con LDAP

https://www.sonicwall.com/support/knowledge-base/ldap-integration-in-sonicos-6-5-and-above/170817095417807/

REF11 Cómo configurar la integración con LDAP usando TLS

https://www.sonicwall.com/support/knowledge-base/configuring-active-directory-ldap-over-tls-certificate/170505251062387/

REF12 Cómo instalar y configurar la autenticación mediante Single Sign-On (SSO)

https://www.sonicwall.com/support/knowledge-base/how-can-i-install-single-sign-on-sso-software-and-configure-the-sso-feature/170505740046553/

REF13 Cómo construir un cable de consola para cortafuegos Sonicwall

https://www.sonicwall.com/support/knowledge-base/how-do-i-make-a-console-cable-for-sonicwall-firewall-appliances/170505608988182/

REF14 Cómo habilitar la gestión por CLI a través del puerto de consola

https://www.sonicwall.com/support/knowledge-base/how-can-i-configure-interface-from-cli-once-connected-over-console-port/170505499805697/

REF15 Cómo habilitar/deshabilitar el acceso a la gestión del cortafuegos

https://www.sonicwall.com/es-mx/support/knowledge-base/how-can-i-enable-or-disable-sonicwall-firewall-management-access/170504751491991/

REF16 Cómo cambiar los puertos por defecto de gestión por HTTP/HTTPS

https://www.sonicwall.com/support/knowledge-base/how-can-i-change-the-http-and-https-management-ports-on-utm-appliances/170503585288297/

REF17 Cómo habilitar la autenticación con certificados de cliente para la gestión del cortafuegos por HTTPS

https://www.sonicwall.com/support/knowledge-base/how-can-i-enable-client-certificate-check-for-https-management-on-the-sonicwall/170503966127092/

REF18 Cómo habilitar la autenticación mediante TOTP para la gestión del cortafuegos por HTTPS
https://www.sonicwall.com/support/knowledge-base/how-to-configure-two-factor-authentication-using-totp-for-https-management/190201153847934/

REF19 Introducción a las APIs de Sonicwall

https://www.sonicwall.com/support/knowledge-base/introduction-to-sonicos-api/200818060121313/

REF20 Cómo abrir un puerto del cortafuegos usando SonicOS APIs

https://www.sonicwall.com/support/knowledge-base/port-forwarding-configured-using-sonicos-api/190224162643523/

REF21 Guía de referencia de SonicOS API

https://software.sonicwall.com/Documentation/SonicOS_API_6.5.1_Beta_Reference.pdf

REF22 Cómo habilitar la funcionalidad de Capture Client Enforcement en el cortafuegos

https://www.sonicwall.com/support/knowledge-base/capture-client-enforcement-through-firewall/180424061807489/

REF23 Cómo crear una zona de seguridad personalizada

https://www.sonicwall.com/support/knowledge-base/how-to-create-a-custom-zone/170503641320709/

REF24 Diferentes modos de configuración de interfaces de red

http://help.sonicwall.com/help/sw/eng/7634/8/0/0/content/Configuring_Device_Management_Network_Page.10.05.htm

REF25 Cómo configurar subinterfaces o VLANs

https://www.sonicwall.com/support/knowledge-base/how-can-i-configure-sub-interfaces/170503889544086/

REF26 Cómo crear Address Objects y Address Groups

https://www.sonicwall.com/support/knowledge-base/understanding-address-objects-in-sonicos/170504660027820/

REF27 Cómo configurar el servidor DHCP

https://www.sonicwall.com/support/knowledge-base/configuring-the-dhcp-server-on-the-sonicwall/170505423294713/

REF28 Cómo configurar túneles VPN Site to Site con IKEv2

https://www.sonicwall.com/support/knowledge-base/how-can-i-setup-site-to-site-vpn-with-ike2-dynamic-client-proposal-in-sonicos-6-2-and-above/170505514010727/

REF29 Qué hacer cuando los certificados importados aparecen como no validados

https://support.sonicwall.com/kb/187026

REF30 Cómo configurar la autenticación con RADIUS

http://help.sonicwall.com/help/sw/eng/6800/26/2/3/content/PANEL_radiusProps.htm

REF31 Cómo configurar la autenticación 2FA con RSA para la autenticación con clientes VPN

https://www.sonicwall.com/support/knowledge-base/two-factor-authentication-using-rsa-radius-and-securid-for-sonicwall-gvc-and-netextender-clients/170503789509355/

REF32 Cómo configurar la autenticación 2FA con Quest Defender para la autenticación con clientes VPN

https://www.sonicwall.com/support/knowledge-base/two-factor-authentication-with-quest-defender-for-sonicwall-global-vpn-clients/170505842377009/

REF33 Cómo configurar SNMPv3

https://www.sonicwall.com/support/knowledge-base/configuring-snmpv3-in-sonicos-5-9-6-1-above/170505490315087/

REF34 Cómo configurar Alta Disponibilidad

https://www.sonicwall.com/support/knowledge-base/how-to-configure-high-availability-ha/170503978252820/

REF35 Cómo habilitar el perfil de protección NDPP

https://www.sonicwall.com/support/knowledge-base/how-to-configure-network-devices-protection-profile-ndpp-compliance-checklist-sonicos-5-9-0/170503476740702/

REF36 Cómo exportar un backup de la configuración

https://www.sonicwall.com/support/knowledge-base/how-can-i-save-a-backup-settings-file-from-a-sonicwall-firewall/170504841802992/

REF37 Guía de configuración

https://www.sonicwall.com/techdocs/pdf/sonicos-6-5-system-setup.pdf

9. ABREVIATURAS

ARS	*Advanced Routing Services*
ATP	*Advanced Threat Protection*
CLI	*Command Line Interface*
CRL	*Certificate Revocation List*
CSR	*Certificate Signing Request*
DNS	*Domain Name Servers*
DNSBL	DNS *BlackList*
ENS	Esquema Nacional de Seguridad.
ESP	*Encapsulating Security Payload*
FQDN	*Full Qualified Domain Name*
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*
OCSP	*Online Certificate Status Protocol*
PKI	*Public Key Infrastructure*
POE	*Power Over Ethernet*
PSK	*Pre-Shared Key*
RTDMI	*Real Time Deep Memory Inspection*
SCEP	*Simple Certificate Enrollment Request*
SDP	*SonicWALL Discovery Protocol*
SONICOS	Sistema Operativo de *Sonicwall*
SSH	*Secure Shell*
SSO	*Single Sing-on*
SSPP	*SonicWALL Simple Provisioning Protocol*
TCP	*Transport Control Protocol*
TLS	*Transport Layer Security*
TSA	*Terminal Services Agent*

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