centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1448

Procedimiento de Empleo Seguro
Cisco Secure Client - AnyConnect



Noviembre 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:00 +01:00

Fecha de Edición: Noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 4
2 OBJETO Y ALCANCE 5
3 ORGANIZACIÓN DEL DOCUMENTO 6
4 FASE PREVIA A LA INSTALACIÓN 7
4.1 ENTREGA SEGURA DEL PRODUCTO 7
4.1.1 ENTREGA SEGURA PARA WINDOWS 7
4.1.2 ENTREGA SEGURA PARA ANDROID 7
4.1.3 ENTREGA SEGURA PARA IOS 7
4.1.4 ENTREGA SEGURA PARA LINUX 7
4.2 ENTORNO DE INSTALACIÓN SEGURO 8
4.3 REGISTRO Y LICENCIAS 8
4.4 CONSIDERACIONES PREVIAS 8
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 8
5 FASE DE INSTALACIÓN 10
5.1 INSTALACIÓN EN WINDOWS 10
5.2 INSTALACIÓN EN ANDROID 10
5.3 INSTALACIÓN EN IOS 11
5.4 INSTALACIÓN EN LINUX 11
6 FASE DE CONFIGURACIÓN 12
6.1 MODO DE OPERACIÓN SEGURO 12
6.1.1 CONFIGURACIÓN CRIPTOGRÁFICA PARA WINDOWS 12
6.1.2 CONFIGURACIÓN CRIPTOGRÁFICA PARA ANDROID 12
6.1.3 CONFIGURACIÓN CRIPTOGRÁFICA PARA IOS 12
6.1.4 CONFIGURACIÓN CRIPTOGRÁFICA PARA LINUX 12
6.2 AUTENTICACIÓN 13
6.3 ADMINISTRACIÓN DEL PRODUCTO 13
6.3.1 INSTALACIÓN Y CONFIGURACIÓN DE UNA PUERTA DE ENLACE VPN 13
6.3.2 CONFIGURACIÓN PARA WINDOWS 16
6.3.3 CONFIGURACIÓN PARA ANDROID 17
6.3.4 CONFIGURACIÓN PARA IOS 18
6.3.5 CONFIGURACIÓN PARA LINUX 20
6.4 GESTIÓN DE CERTIFICADOS 21
6.5 SINCRONIZACIÓN 22
6.6 ACTUALIZACIONES 22
6.7 AUTO-CHEQUEOS 22
6.8 AUDITORÍA 22
6.8.1 REGISTRO DE EVENTOS 22
6.8.2 ALMACENAMIENTO LOCAL 23
6.9 FUNCIONES DE SEGURIDAD 24
6.9.1 CONEXIÓN VPN EN WINDOWS 24
6.9.2 CONEXIÓN VPN EN ANDROID 24
6.9.3 CONEXIÓN VPN EN IOS 25
6.9.4 CONEXIÓN VPN EN LINUX 25
6.9.5 MODOS DE TRATAMIENTO DEL TRÁFICO VPN 25
7 REFERENCIAS 26

8 ABREVIATURAS 27

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Esquema de entorno operacional 9
Ilustración 2. Icono editor perfiles 12

1 INTRODUCCIÓN

El producto **Cisco Secure Client - AnyConnect** se trata de un software VPN con capacidad IPsec y TLS, de forma que se puedan establecer conexiones IP seguras entre dispositivos y redes corporativas para un control de acceso a la red y la transmisión cifrada de datos.

Este protege la información contra la divulgación y modificación no autorizada al establecer un túnel VPN seguro, lo que garantiza que los usuarios remotos puedan conectarse de manera segura a los recursos y servicios desplegados en la red interna de una organización.

2 OBJETO Y ALCANCE

El objeto del presente documento es servir como guía para una instalación, configuración y operación segura de **Cisco Secure Client - AnyConnect** en su versión 5.0 para las plataformas Windows, Android e iOS y su versión 5.1 para la plataforma Linux. No obstante, **se debe consultar el Catálogo para determinar la versión junto a la plataforma cualificada en cada momento**.

Para el despliegue en la plataforma Windows, se debe usar Windows 11.

Para el despliegue en la plataforma Android, se debe usar Android 16.

Para el despliegue en la plataforma iOS, se debe usar iOS 26.5.2.

Para el despliegue en la plataforma Linux, se debe usar Red Hat Enterprise Linux 10.2.

Adicionalmente, se deberá emplear el dispositivo Cisco ASA 5500-X Series VPN Gateway con la versión de software 9.2.2 o superior, como puerta de enlace de VPN.

El producto **Cisco Secure Client - AnyConnect** ha sido incluido en el CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF10]

3 ORGANIZACIÓN DEL DOCUMENTO

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

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

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

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

A continuación, se describe la entrega segura del producto dependiendo del sistema donde vaya a ser instalado.

4.1.1 ENTREGA SEGURA PARA WINDOWS

Para instalar el producto en Windows, se debe descargar el instalador correspondiente a la versión cualificada desde la página Central de Cisco [REF1]. El instalador tiene formato "MSI" y está denotado por el nombre Setup.exe.

Una vez descargado, para comprobar la integridad de los archivos de instalación, se proporciona un hash MD5 y un hash SHA-512. Para una verificación segura, únicamente utilizar el SHA-512. La comprobación se debe llevar a cabo siguiendo estos pasos:

a) Descargar el archivo de instalación de Cisco Secure Client - AnyConnect.

b) Generar el hash SHA-512 del fichero instalador facilitado por Cisco.

c) Compararlo con el hash facilitado por Cisco y verificar que coinciden.

4.1.2 ENTREGA SEGURA PARA ANDROID

La única fuente autorizada para descargar la aplicación Cisco Secure Client - AnyConnect es la tienda de aplicaciones de Google, conocida como **Google Play**. Es importante destacar que el desarrollador de esta aplicación es exclusivamente Cisco Systems, Inc. Por lo tanto, para obtener la aplicación de forma segura y legítima, buscarla en Google Play y verificar que el desarrollador sea Cisco Systems, Inc.

La plataforma del dispositivo móvil se encarga de verificar la firma digital del software, lo cual garantiza que proviene legítimamente de Cisco Systems, Inc. Esta verificación asegura la autenticidad y originalidad del software, evitando así cualquier modificación no autorizada.

4.1.3 ENTREGA SEGURA PARA IOS

La única fuente autorizada para descargar la aplicación Cisco Secure Client - AnyConnect es la tienda de aplicaciones de Apple, conocida como **App Store**. Es importante destacar que el desarrollador de esta aplicación es exclusivamente Cisco Systems, Inc. Por lo tanto, para obtener la aplicación de forma segura y legítima, buscarla en App Store y verificar que el desarrollador sea Cisco Systems, Inc.

La plataforma del dispositivo móvil se encarga de verificar la firma digital del software, lo cual garantiza que proviene legítimamente de Cisco Systems, Inc. Esta verificación asegura la autenticidad y originalidad del software, evitando así cualquier modificación no autorizada.

4.1.4 ENTREGA SEGURA PARA LINUX

Para instalar el producto en Linux, se debe descargar el instalador correspondiente a la versión cualificada desde la página Central de Cisco [REF1]. El instalador tiene formato

"gzip", que al ser descomprimido contendrá un archivo "tar" que también deberá de ser descomprimido. Para el caso concreto de RHEL como SO cualificado, deberá de usarse la herramienta *rpm* para la instalación del paquete

Una vez descomprimidos todos los archivos, estos contienen el propio paquete software y la firma digital del archivo, la cual deberá de ser verificada, a través del propio sistema Linux.

4.2 ENTORNO DE INSTALACIÓN SEGURO

El entorno operacional de Cisco Secure Client - AnyConnect debe contar con al menos una Autoridad de Certificación (CA), un terminador VPN ASA-5500VPN y la propia plataforma que ejecute el sistema operativo donde el producto se instalará. Este dependerá de si el despliegue es en Windows, Android, iOS o Linux.

Todos los dispositivos estarán gestionados por los administradores, donde el acceso estará limitado a un conjunto de personas que posean una autorización expresa, y se encargarán de que estos estén correctamente asegurados.

4.3 REGISTRO Y LICENCIAS

El producto no requiere de la instalación de licencias para poder hacer uso del mismo. Este requiere únicamente que el administrador deba estar registrado en la página Central de Cisco [REF1] desde donde podrá descargar todos los paquetes de instalación para los diferentes sistemas.

4.4 CONSIDERACIONES PREVIAS

Para poder hacer un uso correcto del producto, este requiere que se importen los certificados de la Autoridad de Certificación (CA) sobre la plataforma donde va a ser instalado el producto y sobre el que se ejecutará. Atender a la sección *6.4 GESTIÓN DE CERTIFICADOS* para poder configurar el certificado dependiendo del sistema donde va a ser instalado Cisco Secure Client - AnyConnect.

Por otro lado, el producto requiere de una puerta de enlace de la VPN para poder ofrecer todas sus funcionalidades. El fabricante de Cisco Secure Client - AnyConnect recomienda el uso de Cisco ASA 5500-X Series con una versión de software 9.2.2 o superior. A lo largo del documento se referenciará a esta puerta de enlace como "ASA".

Por último, se debe de atender a la sección *6.1 MODO DE OPERACIÓN SEGURO* para configurar el producto de forma que este opere de una forma segura.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

Para que el producto pueda funcionar correctamente, requiere de los siguientes componentes en el entorno:

a) Se requiere de una Autoridad de Certificación capaz de proveer certificados digitales válidos.

b) El producto deberá de instalarse sobre alguna de las plataformas permitidas.

c) El producto se integra exclusivamente con las puertas de enlace Cisco ASA, tal y como se ha mencionado en la sección anterior.

A continuación, se muestra un esquema de la integración del producto dentro de su entorno de operación:

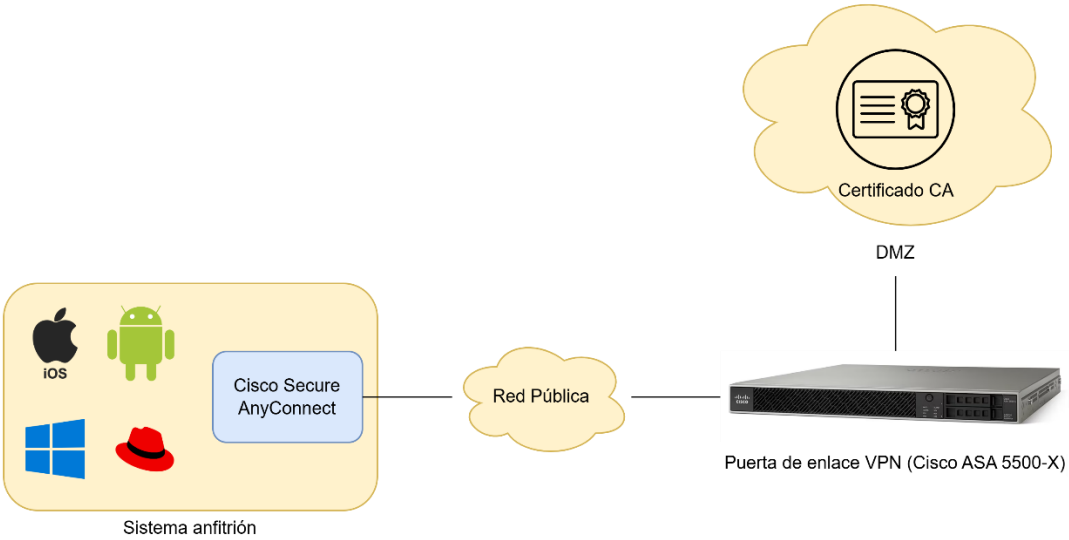

Ilustración 1. Esquema de entorno operacional

5 FASE DE INSTALACIÓN

Dependiendo del sistema donde vaya a instalarse el producto Cisco Secure Client - AnyConnect, a continuación, se detallan los pasos de instalación.

5.1 INSTALACIÓN EN WINDOWS

Para llevar a cabo la instalación en Windows, se deben seguir los siguientes pasos:

a) Ejecutar el archivo descargado de acuerdo con la sección *4.1.1 ENTREGA SEGURA PARA WINDOWS*.

b) Aparecerá el instalador del cliente de Cisco Secure Client - AnyConnect. Pulsar en el botón "Siguiente" para continuar.

c) Después de leer el acuerdo de licencia para el usuario final, seleccionar la opción que indica la aceptación de los términos del acuerdo y pulsar en "Siguiente" para continuar.

d) Aparecerá el mensaje "Listo para instalar". Seleccionar la opción "Instalar" para iniciar el proceso de instalación.

e) El software se instalará en el sistema. Seleccionar la opción "Terminar" cuando el proceso haya finalizado.

Habiendo finalizado los pasos anteriores, el producto quedará completamente instalado. Aun así, hay un paso opcional a realizar durante la instalación y es que el producto permite instalar un editor de perfiles VPN. Para ello, se deben de seguir los siguientes pasos:

a) Descargar el instalador del editor de perfiles desde la página Central de Cisco [REF1]. Este tiene el siguiente formato: *tools-anyconnect-win-{versión de AnyConnect}-profileeditor-k9*.

b) Ejecutar el archivo descargado donde aparecerá el propio instalador del editor de perfiles de Cisco Secure Client - AnyConnect. Pulsar en el botón "Siguiente" para continuar.

c) Aparecerá una ventana donde se deberá escoger el tipo de instalación personalizada.

d) Pulsar en el desplegable correspondiente al apartado Editor de perfiles VPN y Editor de políticas locales para VPN. Las otras opciones no son requeridas para llevar a cabo la instalación. Comprobar que ambas opciones están seleccionadas para ser instaladas en el disco local.

5.2 INSTALACIÓN EN ANDROID

Para instalar Cisco Secure Client - AnyConnect en un dispositivo Android, el usuario debe seguir los distintos menús de instalación que la aplicación muestra después de seleccionar la opción "Instalar" en Google Play. Para más detalles ver la guía de instalación de Cisco Secure Client - AnyConnect para Android [REF2].

5.3 INSTALACIÓN EN IOS

Para instalar Cisco Secure Client - AnyConnect en un dispositivo iOS, el usuario debe seguir los distintos menús de instalación que la aplicación muestra después de seleccionar la opción "Instalar" en App Store.

5.4 INSTALACIÓN EN LINUX

Para llevar a cabo la instalación en Linux (RHEL), se deben seguir los siguientes pasos:

a) Descargar el paquete de instalación de acuerdo a la sección *4.1.4 ENTREGA SEGURA PARA LINUX*.

b) Verifica la firma del paquete descargado mediante los siguientes comandos:

```
rpm --import CiscoSystemsInc.pgp
rpm -K cisco-secure-client-vpn-{version}.x86_64.rpm
```

c) En el caso de que los comandos anteriores devuelvan el mensaje “digests signatures OK” las firmas se habrán verificado y se habrán comprobado que son correctas.

d) Después de verificar la firma, se deberá de instalar mediante el siguiente comando:

```
rpm -i cisco-secure-client-vpn-{version}.x86_64.rpm
```

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Para que el producto opere de forma segura, este requiere que sea configurado para solo utilizar mecanismos criptográficos seguros y recomendados por CCN. A continuación, se detalla el proceso de configuración segura para cada despliegue.

6.1.1 CONFIGURACIÓN CRIPTOGRÁFICA PARA WINDOWS

Para configurar los clientes instalados sobre Windows se deberá de acceder a la sección *Todos los programas > Cisco > Cliente para la movilidad segura de Cisco AnyConnect*. Se deberá de hacer doble pulsación sobre el icono del editor de perfiles de Cisco Secure Client - AnyConnect.



Ilustración 2. Icono editor perfiles

Desde el Menú Archivo, seleccionar la opción Abrir. Se debe marcar la opción “FIPS Mode”. Seleccionar la opción de guardar y cerrar la aplicación

6.1.2 CONFIGURACIÓN CRIPTOGRÁFICA PARA ANDROID

En caso de tratarse de clientes instalados en Android, desde la ventana principal de Cisco Secure Client - AnyConnect, seleccionar Menú > Ajustes. Seleccionar “Modo FIPS” para activar el modo de operación segura.

Después de la confirmación de cambio de modo seguro, Cisco Secure Client - AnyConnect cerrará la aplicación y deberá ser arrancada manualmente.

6.1.3 CONFIGURACIÓN CRIPTOGRÁFICA PARA IOS

Para configurar el cliente iOS en modo de operación segura, desde la ventana principal de Cisco Secure Client - AnyConnect, se deberá de seleccionar Menú > Ajustes. Seleccionar “Modo FIPS” para activar el modo de operación segura con mecanismos criptográficos seguros.

Después de la confirmación de cambio de modo seguro, Cisco Secure Client - AnyConnect cerrará la aplicación y deberá ser arrancada manualmente.

6.1.4 CONFIGURACIÓN CRIPTOGRÁFICA PARA LINUX

En el caso del cliente Linux se deberá de editar el fichero “*AnyConnectLocalPolicy.xml*” el cual se encuentra en el directorio “*/opt/cisco/secureclient*”.

Concretamente, los siguientes valores deberán de tener el valor “true” tal y como se indica a continuación.

```
<ExcludeFirefoxNSSCertStore>true</ExcludeFirefoxNSSCertStore>
```

```
<FipsMode>true</FipsMode>
<StrictCertificateTrust>true</StrictCertificateTrust>
<OCSPRevocation>true</OCSPRevocation>
```

Después de realizar la configuración, el servicio deberá de reiniciarse mediante el siguiente comando.

```
systemctl restart vpnagentd
```

6.2 AUTENTICACIÓN

La autenticación de usuarios para acceder a la funcionalidad del producto la realiza el dispositivo sobre el cual se instala. Es decir, tendrán acceso al producto aquellos usuarios con acceso al sistema Windows, Android, iOS o Linux en el cual se encuentre instalado.

6.3 ADMINISTRACIÓN DEL PRODUCTO

Dada la naturaleza del producto, este consiste únicamente en una interfaz para poder elegir la dirección de destino hacia la que establecer la conexión VPN. Esto hace que no ofrezca la posibilidad de administración a través de sí mismo.

Para poder realizar la administración del producto se deberá de instalar Cisco ASA en su versión 9.2.2 o superior, y opcionalmente se utilizará con ASDM en su versión 7.7 o superior. Este es un software propietario de Cisco el cual permite manejar el ASA mediante una interfaz gráfica. De forma alternativa, la configuración puede llevarse a cabo a través de la línea de comandos (CLI).

6.3.1 INSTALACIÓN Y CONFIGURACIÓN DE UNA PUERTA DE ENLACE VPN

Para consultar los detalles de la instalación de las distintas versiones de Cisco ASA, consultar la guía de configuración de Cisco [REF3]

Activar *Secure Client* y el protocolo IKEv2 en ASA. Para ello, en ASDM, ir a *Configuración > VPN de Acceso Remoto > Acceso de Red (Cliente) > Perfiles de Conexión de Secure Client* y seleccionar “Activar Cisco Secure Client” y “Permitir Acceso bajo IKEv2”. Seleccionar también la casilla de *Enable Client Services*.

En la página de *Perfiles de Conexión de Secure Client* mencionada anteriormente, seleccionar *Certificado del Dispositivo*. Comprobar que la opción *Usar el mismo certificado de dispositivo* se encuentra desactivada y seleccionar el certificado RSA deseado en el parámetro *certificado RSA del dispositivo*. Después, pulsar en el botón “Ok”. El certificado deberá cumplir con los requisitos indicados en el apartado *6.4 GESTIÓN DE CERTIFICADOS*.

Crear una política de cifrado para IKEv2 utilizando únicamente algoritmos seguros. En ASDM ir a *Configuración > Acceso Remoto VPN > Acceso a la Red (Cliente) > Avanzado > IPsec > Políticas de IKE* y pulsar en el valor “Añadir” seleccionando los siguientes parámetros:

a) Prioridad: introducir el valor 1 para configurar la máxima prioridad posible. El rango de valores permitidos es de 1 a 65535, tomando como 1 el valor de mayor prioridad.

b) Cifrado: se recomienda emplear la opción AES-GCM-256. Las opciones disponibles son las siguientes.

   i. AES: Algoritmo AES en modo CBC con longitud de clave de 128b.

ii. AES-256: Algoritmo AES en modo CBC con longitud de clave de 256b.

iii. AES-GCM-128: Algoritmo AES en modo GCM con longitud de clave de 128b.

iv. AES-GCM-256: Algoritmo AES en modo GCM con longitud de clave de 256b.

c) D-H Group: se deberán seleccionar únicamente los valores 19 o 20.

d) Hash de integridad: null, MD5, SHA, SHA256, SHA384, SHA512. Se deberá elegir SHA256 o superior.

e) PRF Hash: se deberá seleccionar únicamente los valores SHA256 o SHA384.

f) Tiempo de vida: configurar un valor igual o inferior a 86400 segundos.

Una vez configurados todos los parámetros, pulsar en el botón "Ok".

Crear una proposición IPSEC. En ASDM, ir a *Configuración > Acceso Remoto VPN > Acceso a la red (Cliente) > Avanzado > IPsec > Proposiciones IPsec (Sets de transformación)* y añadir una proposición IPsec para IKEv2.

Cifrado: se recomienda emplear la opción AES-GCM-256. Las opciones disponibles son las siguientes.

i. AES: Algoritmo AES en modo CBC con longitud de clave de 128b.

ii. AES-192: Algoritmo AES en modo CBC con longitud de clave de 192b.

iii. AES-256: Algoritmo AES en modo CBC con longitud de clave de 256b.

iv. AES-GCM-128: Algoritmo AES en modo GCM con longitud de clave de 128b.

v. AES-GCM-192: Algoritmo AES en modo GCM con longitud de clave de 192b.

vi. AES-GCM-256: Algoritmo AES en modo GCM con longitud de clave de 256b.

Hash de integridad: null, MD5, SHA, SHA256, SHA384, SHA512. Se deberá elegir SHA256 o superior.

Después, pulsar en el botón "Ok".

Crear un mapa criptográfico dinámico. Seleccionar la proposición IPsec y aplicar los cambios para la interfaz de tráfico externo. En ASDM, seleccionar *Configuración > Acceso Remoto VPN > Acceso a la red (Cliente) > Avanzado > IPsec > Mapas Criptográficos*. Pulsar en el botón "Añadir", seleccionar la interfaz saliente y la proposición IKEv2. Pulsar en la pestaña de "Avanzado":

a) Activar NAT-T. Activar NAT transversal para esta política.

b) Tiempo de vida para el ajuste de la Asociación de Seguridad (SA). Marcar 8 horas (28800 segundos).

Crear un conjunto de direcciones *VPNUSERS* que será asignado a los usuarios de VPN. Los conjuntos de direcciones contienen los siguientes campos:

a) Nombre. Especificar el nombre asignado al conjunto de direcciones IP.

b) Dirección IP de Comienzo. Especificar la primera dirección IP del conjunto.

c) Dirección IP de Final. Especificar la última dirección IP del conjunto.

d) Máscara de subred. Seleccionar la máscara de subred que será aplicada a las direcciones del conjunto.

Para ello, en ASDM, ir a *Configuración > Acceso Remoto VPN > Acceso a la red (Cliente) > Asignación de direcciones > Conjuntos de direcciones* y añadir un conjunto de direcciones IP especificando los campos descritos anteriormente. Después, pulsar en el botón "Ok".

Añadir una política de grupo que aplicará la configuración deseada a los usuarios VPN. Una política de grupo VPN es una colección de pares atributo/valores asociados a un usuario y almacenados internamente en el dispositivo ASA. Configurar políticas de grupo VPN permite a los usuarios heredar atributos que no se encuentren configurados a nivel de su nombre de usuario. Por defecto, los usuarios VPN no poseen ninguna asociación a políticas de grupo. La información de políticas de grupo es utilizada por grupos de túnel VPN y cuentas de usuario.

En ASDM, ir a *Configuración > Acceso Remoto VPN > Acceso a la red (Cliente) > Políticas de Grupo* y añadir una política de grupo interna.

El protocolo de túnel VPN deberá estar configurado como IKEv2 únicamente y el conjunto de direcciones IP creado anteriormente se deberá referenciar en la política deseleccionando herencia y seleccionando la configuración pertinente. Nombres para DNS, WINS y dominios pueden ser también añadidos a la política en la sección de *Servidores*. Para finalizar, pulsar en el botón "Ok".

Crear un nombre de grupo para el túnel. Un grupo de túnel contiene políticas de conexión para la conexión IPsec. Una política de conexión puede especificar autenticación, autorización, servidores de cuentas, una política de grupo por defecto y atributos para el protocolo IKE.

Para ello, en ASDM, ir a Configuración > Acceso Remoto VPN > Acceso a la red (Cliente) > Perfiles de conexión de AnyConnect. En el fondo de la página bajo Perfiles de Conexión, pulsar en el botón "Añadir".

Se recomienda emplear la Autenticación con Certificado (la configuración de los certificados de cliente se puede consultar en el apartado *6.4 GESTIÓN DE CERTIFICADOS*), la política de grupo asociada NGE-VPN-GP y habilitar el uso del protocolo IPsec (IKEv2).

Crear un mapa de certificados mapeando los usuarios de NGE VPN al grupo de túnel VPN que ha sido creado con anterioridad. El mapa de certificados se aplicará a los usuarios de la CA. Los usuarios VPN que no posean un certificado de la CA serán dirigidos al grupo de túnel por defecto, fallará la autenticación y el acceso será denegado.

Para ello, en ASDM, ir a *Configuración > Acceso Remoto VPN > Avanzado > Certificado para AnyConnect y mapas de perfil de conexión SSL VPN sin cliente*. Bajo *Certificado para Mapas de perfil de conexión* pulsar en el botón "Añadir". Seleccionar el existente DefaultCertificateMap con una prioridad de 10 y el grupo de túnel NGE-RAS-VPN.

En ASDM, ir a *Configuración > Acceso Remoto VPN > Avanzado > Certificado* para AnyConnect y mapas de perfil de conexión SSL VPN sin cliente. Bajo *Criterios de mapeo* pulsar en el botón "Añadir". Elegir *Proveedor para Campo, Common Name (CN)* para componente, *Contains* para Operador y pulsar en el botón "Ok".

Importante pulsar el botón "APLICAR" en la página principal y "GUARDAR" la configuración.

6.3.2 CONFIGURACIÓN PARA WINDOWS

6.3.2.1 PERFILES DE CLIENTE DE ANYCONNECT

El cliente para la movilidad segura de Cisco Secure Client - AnyConnect almacena su configuración y funcionalidades en perfiles de AnyConnect. Los perfiles son creados utilizando los editores de perfiles de AnyConnect.

Dentro de la herramienta de ASDM existe un editor de perfiles de AnyConnect. Este editor de perfiles de AnyConnect es usado cuando el ASA se usa para administrar de forma centralizada todos los perfiles de los usuarios de AnyConnect.

Para añadir un nuevo perfil de cliente al ASA desde el ASDM se debe abrir el ASDM y seleccionar *Configuración > VPN de Acceso Remoto > Acceso de Red (Cliente) > Perfiles de Conexión de AnyConnect > Perfil de Cliente de AnyConnect*.

Existe también una versión independiente del editor de perfiles para Windows, se puede usar como alternativa al editor de perfiles integrado en el ASDM. Los usuarios con privilegios de administrador pueden modificar y manejar sus propios perfiles.

Por lo tanto, la configuración inicial del cliente debe de ser:

a) Creada usando el editor de perfiles integrado en ASDM y exportada a un ordenador Windows remoto o local, donde debe residir el cliente de Cisco Secure Client - AnyConnect.

b) Usar la versión independiente del editor de perfiles (Standalone), explicado en la siguiente sección.

6.3.2.2 EDITOR PERFILES DE INDEPENDIENTE DE ANYCONNECT

Es posible hacer uso del editor de perfiles independiente de Cisco Secure Client - AnyConnect para la configuración de los perfiles.

Para utilizar la versión de instalador único del editor de perfiles, ir a *Todos los programas > Cisco > Cliente para la movilidad segura de Cisco AnyConnect* y pulsar en el icono del editor de perfiles independiente de AnyConnect.

Por defecto, el perfil se encuentra en la siguiente localización: *%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\ RemoteAccessIKEv2_client_profile.xml.*

RemoteAccessIKEv2_client_profile.xml es un ejemplo de nombre. El nombre de la política de grupo en la puerta de enlace ASA debe coincidir con el nombre del fichero “xml” de la localización anterior. Si no coinciden ocurrirán errores de discordancia de perfiles.

Desde el menú de ficheros, seleccionar Abrir. Ir a la ruta anterior y pulsar en “Abrir”.

Si esta es la primera vez que se utiliza este tipo de editor de perfil, el fichero no existirá. Seguir con los pasos a continuación de esta sección y guardar el fichero como un nuevo fichero .xml en la localización especificada anteriormente.

Después, pulsar en *Lista de Servidores*. Comprobar que la lista de servidores está correctamente compuesta por las puertas de enlace VPN del entorno de la organización. Seleccionar una de las entradas. Para cada una de ellas, comprobar que IPsec está seleccionado como como el protocolo primario en la forma de lista desplegable.

Deshabilitar la casilla de *ASA Gateway* y seleccionar *IKE-RSA* en el *Auth Method during Ike Negotiation* en la lista desplegable.

La dirección y el nombre del host deben coincidir con los presentados en el certificado. Esto significa que el FQDN (o la dirección IP) debe coincidir con el nombre alternativo del sujeto (SAN) que figura en el certificado de ASA.

Desde el menú *Archivo*, seleccionar *Guardar* y después *Salir*. Reiniciar el ordenador.

Se puede encontrar información adicional acerca de estos términos en la sección *Edit a client Profile Using the Stand-Alone Profile Editor* de la guía *Cisco AnyConnect Secure Mobility Client Administrator Guide,* ver guía en [REF4]

Después de terminar la configuración inicial, los editores de perfil integrados en ASDM se deberán utilizar para almacenar y configurar de manera centralizada las opciones definidas en los perfiles para todos los usuarios de Cisco Secure Client - AnyConnect.

6.3.3 CONFIGURACIÓN PARA ANDROID

6.3.3.1 INICIAR LA APLICACIÓN

En el dispositivo Android, tocar el icono de Cisco Secure Client - AnyConnect para arrancar la aplicación.

Si es la primera vez que se inicia Cisco Secure Client - AnyConnect después de la instalación o la actualización de la aplicación, pulsar en OK para habilitar Cisco Secure Client - AnyConnect.

6.3.3.2 AÑADIR ENTRADAS DE CONEXIONES

Esta sección explica cómo añadir manualmente una entrada de conexión VPN, para de esta forma identificar la puerta de enlace segura de la ASA VPN a la que se desea conectar.

Desde la ventana principal de Cisco Secure Client - AnyConnect, pulsar en *Conexión > Añadir una nueva conexión VPN*, esto abrirá el editor de conexiones, se puede añadir una descripción opcional si se desea.

Seleccionar la *Dirección del Servidor* e introducir el FQDN (nombre de dominio) o dirección IP de la puerta de enlace segura de la ASA VPN.

A continuación, en *Advanced Settings* se puede seleccionar el certificado de cliente que se va a utilizar para la conexión en caso ya estar instalado en el teléfono (ver apartado *6.4 GESTIÓN DE CERTIFICADOS*). En caso contrario, basta con aceptar una vez definida la dirección de la puerta de enlace.

Si no se dispone de un certificado en el teléfono, una vez realizada la conexión se deberá guardar el certificado que se presente al establecer la primera conexión. Habrá que tener en cuenta que el certificado descargado podría ser suplantado por un atacante siempre que el certificado presentado sea confiable, ya sea porque está firmado por una autoridad certificadora de confianza o porque el usuario acepte el aviso de riesgo del certificado y lo aceptase.

Para finalizar la configuración específica de Android, se debe configurar la conexión Ipsec tal y como se indica a continuación.

a) Elegir *Conectar con IPsec*. El parámetro de *Autenticación* se activa en este momento, pulsar en él.

b) Elegir el método de Autenticación para la conexión IPsec. Si se desea emplear certificados RSA, seleccionar IKE-RSA. Si se desea emplear certificados ECDSA, seleccionar IKE-ECDSA.

c) Seleccionar "Hecho" en la ventana de Avanzado y también en la del Editor de Conexiones para guardar la configuración de la conexión. Secure Client añadirá la nueva conexión.

6.3.3.3 BLOQUEAR SERVIDORES NO CONFIABLES

El producto permite bloquear conexiones en caso de no identificar correctamente la puerta de enlace. Esta protección se encuentra activada por defecto y no debe ser desactivada.

Cisco Secure Client - AnyConnect utiliza el certificado recibido por el servidor para verificar su identidad. Si hay un error con el certificado por fecha expirada o inválida, mala utilización de las claves o confusión con el nombre, la conexión será bloqueada.

Desde la pantalla principal de Cisco Secure Client - AnyConnect, ir a *Menu > Ajustes*. Verificar que la opción de *Bloquear conexiones inseguras* está marcada.

6.3.3.4 CONFIGURAR LA REVOCACIÓN OCSP

Desde la ventana principal de Cisco Secure Client - AnyConnect, seleccionar *Menú > Ajustes*.

Seleccionar Revocación OCSP para activar esta configuración.

En el siguiente intento de conexión, se empleará OCSP para determinar el estado de revocación del certificado recibido por el extremo de la puerta de enlace VPN.

6.3.3.5 CERTIFICADO DE CONFIANZA

Se puede configurar el producto para descartar los certificados recibidos por la puerta de enlace VPN si no se pueden verificar automáticamente. Para ello, desde la ventana principal de Cisco Secure Client - AnyConnect, seleccionar *Menú > Ajustes*. Elegir *Certificado de Confia*nza para activar la protección.

En el siguiente intento de conexión, *Strict Certificate Trust* estará activado.

6.3.4 CONFIGURACIÓN PARA IOS

6.3.4.1 INICIAR LA APLICACIÓN

En el dispositivo iOS, tocar el icono de Cisco Secure Client - AnyConnect para arrancar la aplicación.

Si es la primera vez que se inicia Cisco Secure Client - AnyConnect después de la instalación o la actualización de la aplicación, pulsar en OK para habilitar Cisco Secure Client - AnyConnect.

6.3.4.2 AÑADIR ENTRADAS DE CONEXIONES

Esta sección explica cómo añadir manualmente una entrada de conexión VPN, para de esta forma identificar la puerta de enlace segura de la ASA VPN a la que se desea conectar.

Desde la ventana principal de Cisco Secure Client - AnyConnect, pulsar en *Conexión > Añadir una nueva conexión VPN*, esto abrirá el editor de conexiones, se puede añadir una descripción opcional si se desea.

Seleccionar la *Dirección del Servidor* e introducir el FQDN (nombre de dominio) o dirección IP de la puerta de enlace segura de la ASA VPN.

A continuación, en *Advanced Settings* se puede seleccionar el certificado de cliente que se va a utilizar para la conexión en caso ya estar instalado en el teléfono (ver apartado *6.4 GESTIÓN DE CERTIFICADOS*). En caso contrario, basta con aceptar una vez definida la dirección de la puerta de enlace.

Si no se dispone de un certificado en el teléfono, una vez realizada la conexión se deberá guardar el certificado que se presente al establecer la primera conexión. Habrá que tener en cuenta que el certificado descargado podría ser suplantado por un atacante siempre que el certificado presentado sea confiable, ya sea porque está firmado por una autoridad certificadora de confianza o porque el usuario acepte el aviso de riesgo del certificado y lo aceptase.

6.3.4.3 BLOQUEAR SERVIDORES NO CONFIABLES

El producto permite bloquear conexiones en caso de no identificar correctamente la puerta de enlace. Esta protección se encuentra activada por defecto y no debe ser desactivada.

Cisco Secure Client - AnyConnect utiliza el certificado recibido por el servidor para verificar su identidad. Si hay un error con el certificado por fecha expirada o inválida, mala utilización de las claves o confusión con el nombre, la conexión será bloqueada.

Desde la pantalla principal de Cisco Secure Client - AnyConnect, ir a *Menu > Ajustes*. Verificar que la opción de *Bloquear conexiones inseguras* está marcada.

6.3.4.4 CONFIGURAR LA REVOCACIÓN OCSP

Desde la ventana principal de Cisco Secure Client - AnyConnect, seleccionar *Menú > Ajustes*.

Seleccionar Revocación OCSP para activar esta configuración.

En el siguiente intento de conexión, se empleará OCSP para determinar el estado de revocación del certificado recibido por el extremo de la puerta de enlace VPN.

6.3.4.5 CERTIFICADO DE CONFIANZA

Se puede configurar el producto para descartar los certificados recibidos por la puerta de enlace VPN si no se pueden verificar automáticamente. Para ello, desde la ventana principal de Cisco Secure Client - AnyConnect, seleccionar *Menú > Ajustes*. Elegir *Certificado de Confia*nza para activar la protección.

En el siguiente intento de conexión, *Strict Certificate Trust* estará activado.

6.3.5 CONFIGURACIÓN PARA LINUX

6.3.5.1 PERFILES DE CLIENTE DE ANYCONNECT

Al igual que en el despliegue en Windows, el cliente Linux para la movilidad segura de Cisco Secure Client - AnyConnect almacena su configuración y funcionalidades en perfiles de Cisco Secure Client - AnyConnect. Los perfiles son creados utilizando los editores de perfiles de Cisco Secure Client - AnyConnect.

Dentro de la herramienta de ASDM existe un editor de perfiles de Cisco Secure Client - AnyConnect. Este editor de perfiles de Cisco Secure Client - AnyConnect es usado cuando el ASA se usa para administrar de forma centralizada todos los perfiles de los usuarios de Cisco Secure Client - AnyConnect.

Para añadir un nuevo perfil de cliente al ASA desde el ASDM se debe abrir el ASDM y seleccionar *Configuración > VPN de Acceso Remoto > Acceso de Red (Cliente) > Perfil de Secure Client*.

Existe también una versión independiente del editor de perfiles para Linux, se puede usar cómo alternativa al editor de perfiles integrado en el ASDM. Los usuarios con privilegios de administrador pueden modificar y manejar sus propios perfiles.

Por lo tanto, la configuración inicial del cliente debe de ser:

a) Creada usando el editor de perfiles integrado en ASDM y exportada a un ordenador Linux remoto o local, donde debe residir el cliente de Cisco Secure Client - AnyConnect.

b) Usar la versión independiente del editor de perfiles (Standalone), explicado en la siguiente sección.

6.3.5.2 EDITOR PERFILES DE INDEPENDIENTE DE ANYCONNECT

Es posible hacer uso del editor de perfiles independiente de Cisco Secure Client - AnyConnect para la configuración de los perfiles.

Para utilizar la versión del editor de perfiles independiente, se deberá de editar manualmente el fichero /opt/cisco/secureclient/vpn/profile/myvpn.xml.

Hay que tener en cuenta que el nombre de la política de grupo en ASA debe coincidir con el nombre específico y la ruta indicados anteriormente. De lo contrario, se producirán errores por discrepancia de perfiles.

Dentro de este fichero, se deberá de indicar en el campo *Primary Protocol* el protocolo IPsec y en el campo Standard Athentication, “false”. Esta configuración quedará tal y como se muestra a continuación.

```
<ServerList>
     <HostEntry>
           <HostName>Example Org</HostName>
           <HostAddress>vpn.example.com</HostAddress>
           <PrimaryProtocol>IPsec
                 <StandardAuthenticationOnly>false
                 </StandardAuthenticationOnly>
           </PrimaryProtocol>
     </HostEntry>
```

```
</ServerList>
```

Los valores de “Hostname” y “HostAddress” deberán de editarse de acuerdo a los valores correspondientes en la organización. La sección “HostAddress” especifica la configuración del identificador de referencia de la pasarela VPN. Durante la fase 1 de la autenticación IKE, la aplicación Secure Client compara el identificador de referencia con el identificador presentado por la pasarela VPN. Si la aplicación Secure Client determina que no coinciden, la autenticación no se completará con éxito.

6.4 GESTIÓN DE CERTIFICADOS

6.4.1.1 PROPIEDADES DEL CERTIFICADO

Independientemente de la CA empleada, el certificado RSA utilizado en el gateway ASA debe poseer las siguientes propiedades para el uso de clave y uso de clave extendido:

a) Uso de clave (Key Usage): Firma digital, Acuerdo de Clave.

b) Uso de clave extendido (Extended Key Usage): IP security IKE intermediate, IP end security system.

Los certificados RSA deberán emplear siempre una longitud de clave de 3072 bits o superior.

6.4.1.2 CREACIÓN DEL CERTIFICADO CLIENTE

Se deberá generar un certificado para ser empleado por el dispositivo del usuario para autenticación. Esto se tendrá que hacer de forma externa al producto y al propio sistema donde este se va a instalar.

Se puede emplear la herramienta de complemento de certificado “MMC” de Microsoft para generar CSR (Certificate Signing Request) e importar certificados. Se puede consultar más información acerca del uso de MMC en la siguiente referencia [REF5]. Se deberán generar los CSR siguiendo los pasos indicados en la siguiente referencia [REF6].

Para la generación del CSR, se deberán seleccionar las siguientes opciones:

a) Plantilla: (Sin plantilla) Clave CNG

b) Formato de fichero: PKCS#10.

c) Propiedades del certificado: seleccionar el proveedor de almacenamiento de claves de Microsoft y elegir ECDSA_P384 como tipo de clave. En caso de desear usar RSA, se deberá elegir RSA como tipo de clave y 3072 bits o superior como longitud de clave. Elegir SHA-384 como algoritmo de hash.

d) Uso de clave: seleccionar Firma Digital.

e) Uso de clave extendido: seleccionar Autenticación de servidor.

Una vez creado el CSR, se deberá mandar a la CA para obtener el certificado. Para asegurar el correcto funcionamiento, se deben importar los certificados de la CA y cualquier certificado intermedio en el almacén de certificados del dispositivo iOS donde se emplee el Cliente. Para hacer esto, consultar [REF7]. Por último, importar el certificado en el almacén de certificados dispositivo iOS una vez obtenido. Este certificado se empleará para la autenticación del cliente.

Tras instalar el certificado en el dispositivo, ir a la ventana principal de Secure Client y seleccionar *Menu > Diagnósticos > Gestión de Certificados*. Seleccionar la pestaña de *Usuario > Importar > Almacenamiento de Credenciales del Dispositivo* para enlazar un certificado que se encuentre actualmente en dicho almacenamiento.

6.5 SINCRONIZACIÓN

Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados para permitir una alta fiabilidad en los sistemas de auditoría y logging. El producto emplea el reloj del sistema operativo en el cual se encuentre instalado para todos los casos de despliegue.

6.6 ACTUALIZACIONES

Para poder estar al tanto de las nuevas versiones del producto disponibles, es posible suscribirse al servicio de notificaciones de Cisco para recibir información importante sobre las actualizaciones de productos. A través de esta plataforma se notificarán todas las nuevas versiones para los diferentes sistemas donde se puede instalar el producto. Para obtener más detalles, consultar la documentación de referencia [REF8].

Para todos los sistemas en los que el producto se puede instalar, el proceso de actualización consiste en la instalación del producto en la nueva versión. Por ello, se recomienda atender a las diferentes subsecciones del apartado *5 FASE DE INSTALACIÓN* para instalar la nueva versión del cliente dependiendo del proceso de cada sistema.

6.7 AUTO-CHEQUEOS

La aplicación Cisco Secure Client - AnyConnect realiza una verificación de integridad cada vez que se carga. Durante este proceso, se emplean los servicios criptográficos para verificar la firma digital de los archivos ejecutables del producto.

Si la verificación de integridad falla, la interfaz de usuario no se cargará y la aplicación no podrá ser utilizada.

6.8 AUDITORÍA

6.8.1 REGISTRO DE EVENTOS.

Dado que para cualquier sistema es necesaria la integración del producto con un dispositivo ASA, este genera y almacena sus propios registros. Dentro de los cuales se incluyen los relativos a los clientes VPN. El detalle de configuración de Logging de los Gateway ASA se puede consultar en el apartado Logging de las guías CLI Book 1 de configuración de las distintas versiones de ASA, disponibles en el manual de configuración de ASA [REF4].

Además de ello, el propio producto genera registros de eventos tal y como se indica a continuación.

6.8.1.1 REGISTRO DE EVENTOS EN WINDOWS

El registro de eventos y logs de la aplicación y de los procesos que se ejecutan dentro del sistema operativo de Windows, se lleva a cabo con el uso de la utilidad DART de Cisco Secure Client - AnyConnect. El detalle sobre el uso de DART se puede consultar en [REF4].

El almacenamiento de los registros dentro del sistema operativo de Windows se realiza de forma local y se encuentra situado en la siguiente dirección: *\Windows\Inf\setupapi.app.log o en \Windows\Inf\setupapi.dev.log*.

6.8.1.2 REGISTRO DE EVENTOS EN ANDROID

Los dispositivos Android incluyen dentro de la propia aplicación una herramienta de diagnóstico integrada, esta herramienta permite acceder y gestionar los registros desde dentro de la propia aplicación de Cisco Secure Client - AnyConnect.

Para acceder y gestionar los registros, acceder a la siguiente dirección desde la pantalla de inicio de AnyConnect, *Menu > Diagnostics > Logging and System Information*. Los registros se dividen en: Mensajes, Sistema o Debug. Para más información sobre cómo acceder a los registros y las acciones que se pueden realizar con ellos consultar [REF9].

El almacenamiento de registros dentro del sistema operativo Android se realiza de forma local y se encuentra situado dentro de la carpeta de registros de la propia aplicación de Cisco Secure Client - AnyConnect.

6.8.1.3 REGISTRO DE EVENTOS EN IOS

En el caso de los dispositivos iOS se deberá acceder a *Menu > Diagnostics* y activar "Registros de depuración de VPN" para que el producto genere y almacene los registros. Estos se pueden consultar desde *Menu > Diagnostics > Logging and System Information*.

El producto no permite configurar límites de retención de los registros, por lo que los usuarios deberán revisar periódicamente el almacenamiento de registros para verificar que no se llena el espacio.

Para más información sobre cómo acceder a los registros y las acciones que se pueden realizar con ellos consultar [REF11].

6.8.1.4 REGISTRO DE EVENTOS EN LINUX

En el despliegue del producto en Linux, este siempre lo almacenará en el directorio "*/var/log*". Dependiendo de la distribución Linux, el propio archivo donde se almacena el registro de eventos variará.

En el caso concreto de los sistemas RHEL, los registros se almacenarán en "*/var/log/messages*".

6.8.2 ALMACENAMIENTO LOCAL

Tal y como se puede comprobar en las secciones anteriores, todo el almacenamiento del sistema se realiza de forma local sobre los sistemas donde el producto se instala. Esto es así ya que el producto no dispone de la capacidad de reenviar dichos registros a un servidor externo y por tanto no permite el almacenamiento remoto de los registros de auditoría.

Por otro lado, el producto no permite configurar límites de retención de los registros, por lo que el administrador deberá revisar periódicamente el almacenamiento de registros, verificando que no se llene el espacio disponible.

6.9 FUNCIONES DE SEGURIDAD

6.9.1 CONEXIÓN VPN EN WINDOWS

Para establecer una conexión VPN, ejecutar el Cliente de Cisco Secure Client - AnyConnect Secure Mobility. Elegir la conexión VPN a establecer y pulsar en el botón de "Conectar" para conectarse a una de las puertas de enlace VPN predefinidas.

Para bloquear certificados, seleccionar el icono del engranaje para acceder a la configuración del cliente de Cisco Secure Client - AnyConnect y seleccionar la casilla de "Block Connections to Untrusted Servers".

En el caso de que el certificado sea válido y es la primera vez que nos conectamos, se requiere que el certificado sea aceptado en el almacén de certificados de Windows.

El producto elige de manera autónoma qué certificado de cliente usar del almacén de certificados de Windows.

Para verificar el establecimiento de la conexión, pulsar en el icono de Cisco Secure Client - AnyConnect de la barra de tareas. Debería obtener un mensaje afirmativo indicando que está conectado correctamente a la puerta de enlace VPN (Servidor).

Para finalizar la sesión VPN, pulsar en el botón "Desconectar". Si el certificado de la puerta VPN no es válido o falla la comprobación del CLR, Cisco Secure Client - AnyConnect no permitirá la conexión. Si esta situación ocurriese, se mostrará un mensaje indicando el error.

6.9.2 CONEXIÓN VPN EN ANDROID

Para conectarse a una VPN hay que pulsar en el *checkbox* o desplegable asociado con la conexión activa mostrada en panel VPN de Cisco Secure Client - AnyConnect. También se puede seleccionar una u otra conexión en las entradas mostradas por la pantalla principal de Cisco Secure Client - AnyConnect.

Se debe disponer de una conexión Wi-Fi activa, o de una conexión con un proveedor de servicios para conectarse a una VPN.

Para iniciar una conexión VPN, se debe disponer de al menos una entrada mostrada bajo el apartado "Elegir una conexión" en la pantalla principal de Cisco Secure Client - AnyConnect.

Para completar una conexión VPN, se debe tener la información de autenticación requerida por su puerta de enlace segura.

a) Ir a la pantalla principal de Cisco Secure Client - AnyConnect.

b) Tocar en "Conexión" y después otra vez en el objetivo de su conexión. En el caso de que el sistema ya estuviera conectado a otro objetivo, Cisco Secure Client - AnyConnect se desconecta de cualquier conexión VPN activa y realiza la nueva conexión.

Si el proceso de autenticación se completa satisfactoriamente, se mostrará un mensaje indicando que la conexión VPN se ha completado satisfactoriamente.

6.9.3 CONEXIÓN VPN EN IOS

Para conectarse a una VPN hay que pulsar en el *checkbox* o desplegable asociado con la conexión activa mostrada en panel VPN de Cisco Secure Client - AnyConnect. También se puede seleccionar una u otra conexión en las entradas mostradas por la pantalla principal de Cisco Secure Client - AnyConnect.

Se debe disponer de una conexión Wi-Fi activa, o de una conexión con un proveedor de servicios para conectarse a una VPN.

Para iniciar una conexión VPN, se debe disponer de al menos una entrada mostrada bajo el apartado “Elegir una conexión” en la pantalla principal de Cisco Secure Client - AnyConnect.

Para completar una conexión VPN, se debe tener la información de autenticación requerida por su puerta de enlace segura.

a) Ir a la pantalla principal de Cisco Secure Client - AnyConnect.

b) Tocar en “Conexión” y después otra vez en el objetivo de su conexión. En el caso de que el sistema ya estuviera conectado a otro objetivo, Cisco Secure Client - AnyConnect se desconecta de cualquier conexión VPN activa y realiza la nueva conexión.

Si el proceso de autenticación se completa satisfactoriamente, se mostrará un mensaje indicando que la conexión VPN se ha completado satisfactoriamente.

6.9.4 CONEXIÓN VPN EN LINUX

Primeramente, se deberá de comprobar que el producto está corriendo sobre el sistema. En caso afirmativo, se deberá de abrir la sección de VPN del sistema, donde aparecerá el mensaje “Listo para Conectar”.

Se deberá de indicar o seleccionar la dirección a la que se conectará la VPN y se deberá de pulsar sobre el botón “Conectar”.

6.9.5 MODOS DE TRATAMIENTO DEL TRÁFICO VPN

Hay que tener en cuenta que, a la hora de la conexión, se tendrán en cuenta 3 reglas diferentes:

a) PROTECT: Regla aplicada por defecto, donde todo el tráfico entre el producto y ASA viajará protegido por el túnel VPN.

b) BYPASS: En este caso el túnel VPN se divide, eligiendo qué tráfico se desea enviar a través de la VPN y cual viajará sin estar tunelizado, aunque a través de la comunicación punto a punto. Este caso se utiliza para aumentar el rendimiento de la comunicación enviando a través del túnel aquella información especialmente sensible.

c) DISCARD: Reglas para bloquear tráfico específico a través de la VPN.

7 REFERENCIAS

REF1 Página Central de Cisco, https://software.cisco.com/

REF2 Guía de instalación de Cisco Secure Client - AnyConnect para Android, https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/user/guide/b_Android_AnyConnect_User_Guide_4-0-x.html

REF3 Guía de Configuración de Cisco ASA, https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html

REF4 Guía de Administración de Cisco Secure Client (Incluyendo AnyConnect), https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-1.html

REF5 Guía de Windows para el uso de MMC, http://technet.microsoft.com/en-us/library/dd632619.aspx

REF6 Guía de Windows para la generación de CSR, http://technet.microsoft.com/en-us/library/cc730929.aspx

REF7 Guía de Windows para la Importación de certificados, https://learn.microsoft.com/en-us/windows-hardware/drivers/install/certificate-stores

REF8 Página de notificaciones sobre nuevos lanzamientos de versiones, https://www.cisco.com/c/en/us/support/security/category.html

REF9 Guía de registro de eventos de AnyConnect para Android, https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/user/guide/b_Android_AnyConnect_User_Guide_4-0-x.html

REF10 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del CCN. https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

REF11 Guía de registro de eventos de AnyConnect para iOS, https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/user/guide/b_Apple_iOS_AnyConnect_User_Guide_4-0-x.html

8 ABREVIATURAS

AES	Advanced Encryption Standard
ASA	Adaptive Security Appliance
ASDM	Adaptive Security Device Manager
CA	Certification Authority
CBC	Cipher Block Chaining (Modo de Operación de AES)
CCN	Centro Criptológico Nacional
CLI	Command Line Interface
CLR	Common Language Runtime
CN	Common Name
CPSTIC	Catálogos de Productos y Servicios de Tecnologías de la Información y Comunicación
CSR	Certificate Signing Request
DART	Diagnostics and Reporting Tool
DNS	Domain Name Service
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad.
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
GCM	Galois Counter Mode (Modo de Operación de AES)
GP	Group Policy
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
MMC	Microsoft Management Console
MSI	Microsoft Software Installer
NGE	Next-Generation Encryption
OCSP	Online Certificate Status Protocol
PKCS	Public-Key Cryptography Standards
RHEL	Red Hat Enterprise Linux
RSA	Rivest-Shamir-Adleman
SA	Secure Association
SHA	Secure Hash Algorithm
SO	Sistema Operativo
SSL	Secure Socket Layer
TLS	Transport Layer Security
VPN	Virtual Private Network
WINS	Windows Internet Name Service