centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1448

Procedimiento de Empleo Seguro
AnyConnect Secure Mobility Android y Windows

Febrero 2024

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 CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.03.01 11:20:21 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-101-5.
Fecha de Edición: febrero de 2024.

ÍNDICE

1. INTRODUCCIÓN

1. La aplicación AnyConnect es un cliente VPN diseñado para permitir a los usuarios remotos establecer un túnel seguro para la transferencia de información, tanto en redes IPv4 como IPv6.
2. Protege la información contra la divulgación y modificación no autorizada al establecer un túnel VPN seguro. Esto garantiza que los usuarios remotos puedan conectarse de manera segura a los recursos y servicios desplegados en la red interna de una organización.
3. El túnel VPN utiliza protocolos criptográficos de IPsec para garantizar la autenticación mutua de los extremos y el cifrado del tráfico en redes públicas inseguras.
4. El Gateway VPN actúa como extremo de la comunicación en la sede de la organización.

2. OBJETO Y ALCANCE

5. El objeto del presente documento es facilitar la instalación y configuración segura de la aplicación **Cisco AnyConnect Secure Mobility con la versión 4.10 para las plataformas Windows y Android 11 y la versión 5 para la plataforma Android 12**, junto con el aseguramiento del entorno en el que se despliega.
6. En los despliegues en la plataforma Windows, deberá tratarse de Microsoft Windows 10 Enterprise Edition.
7. En los despliegues en la plataforma Android, deberá emplearse el dispositivo Samsung Galaxy A71 con Android 11.
8. 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.

3. ORGANIZACIÓN DEL DOCUMENTO

9. Este documento se compone de los siguientes apartados:

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

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

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

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

   e) Apartado **8**: *Checklist* de las tareas a realizar y el estado de cada una de ellas.

   f) Apartado **9**: Referencias usadas en este documento.

   g) Apartado **10**: Abreviaturas usadas en este documento.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

4.1.1 ENTREGA SEGURA PARA ANDROID

10. La única fuente autorizada para descargar la aplicación 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*.
11. 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.

4.1.2 ENTREGA SEGURA PARA WINDOWS

12. Para instalar AnyConnect en Windows, se debe descargar el instalador *anyconnect-win-4.10.07062-predeploy-k9.zip* desde la página Central de Cisco [REF2]. El instalador tiene formato "MSI" y está denotado por el nombre *Setup.exe.*
13. 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:
    - Descargar el archivo de instalación de AnyConnect.
    - Generar el hash SHA-512 del fichero instalador facilitado por Cisco.
    - Compararlo con el hash facilitado por Cisco y verificar que coinciden.

4.2 ENTORNO DE INSTALACIÓN SEGURO

14. El entorno operacional de AnyConnect debe contar con al menos una Autoridad de Certificación (CA), un terminador VPN ASA-5500VPN y una plataforma que ejecute el sistema operativo Android 11 o Windows 10, dependiendo de la plataforma utilizada.
15. A continuación, se mencionarán los componentes mínimos necesarios para el funcionamiento de AnyConnect en el entorno, según el sistema operativo utilizado.

4.2.1 ENTORNO DE OPERACIÓN PARA WINDOWS

16. Una Autoridad de Certificación que proporcione certificados válidos y el método para comprobar el estado de revocación del certificado de la puerta de enlace de la VPN.

17. El producto se integra exclusivamente con las puertas de enlace Cisco ASA 5500-X, las cuales deben utilizar una versión del software 9.2.2 o posterior.
18. Para la administración remota, se empleará ASDM, con versión del software 7.1(x) o posterior, operando en cualquiera de los siguientes sistemas operativos:
    - Windows 7, 8, 10
    - Windows Server 2008, 2012, 2012 R2
    - Apple OS X 10.4 o posterior.
    - Ubuntu Linux 14.04
    - Debian Linux 7

4.2.2 ENTORNO DE OPERACIÓN PARA ANDROID

19. Se debe usar una Autoridad de Certificación para proveer certificados digitales válidos.
20. El producto se integra exclusivamente con las puertas de enlace Cisco ASA 5500-X, las cuales deben utilizar una versión del software 9.2.2 o posterior.
21. Para la administración remota, se empleará ASDM, con versión del software 7.1(x) o posterior, operando en cualquiera de los siguientes sistemas operativos:
    - Windows 7, 8
    - Apple OS X 10.4 o posterior.
    - Red Hat Enterprise Linux 5 (GNOME o KDE).

4.3 REGISTRO Y LICENCIAS

22. El producto no requiere de la instalación de licencias. Para la descarga de AnyConnect en la plataforma Windows, se debe estar registrado en el portal de Cisco.

4.4 CONSIDERACIONES PREVIAS

23. Es necesario importar los certificados de la Autoridad de Certificación (CA) en la plataforma en la que se está ejecutando el producto (Android o Windows). Ver apartado 6.4 GESTIÓN DE CERTIFICADOS.
24. Se debe emplear el modo de operación seguro para asegurar el uso de mecanismos criptográficos seguros. Ver apartado 6.1 MODO DE OPERACIÓN SEGURO.
25. La puerta de enlace de la VPN es referenciada en este documento como “ASA”.

5. FASE DE INSTALACIÓN

26. Para instalar 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 referencia [REF13].

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

    - Ejecutar el archivo descargado llamado *anyconnect-win-4.10.06090-predeploy-k9*.
    - Aparecerá el instalador del cliente de Cisco AnyConnect para movilidad segura. Hacer clic en el botón "Siguiente" para continuar.
    - Después de leer el acuerdo de licencia para el usuario final, seleccionar la opción que indica la aceptación de los términos del acuerdo y hacer clic en "Siguiente" para continuar.
    - Aparecerá el mensaje "Listo para instalar". Seleccionar la opción "Instalar" para iniciar el proceso de instalación.
    - El software se instalará en el sistema. Seleccionar la opción "Terminar" cuando el proceso haya finalizado.

28. Para instalar el editor de perfiles se deben seguir los siguientes pasos:

    - Ejecutar el archivo descargado llamado *tools-anyconnect-win-4.10.06090-profileeditor-k9*.
    - Aparecerá el instalador para el editor de perfiles de Cisco AnyConnect. Hacer clic en el botón "Siguiente" para continuar.
    - Aparecerá una ventana donde se deberá escoger el tipo de instalación **Customizada**.
    - Hacer clic 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.

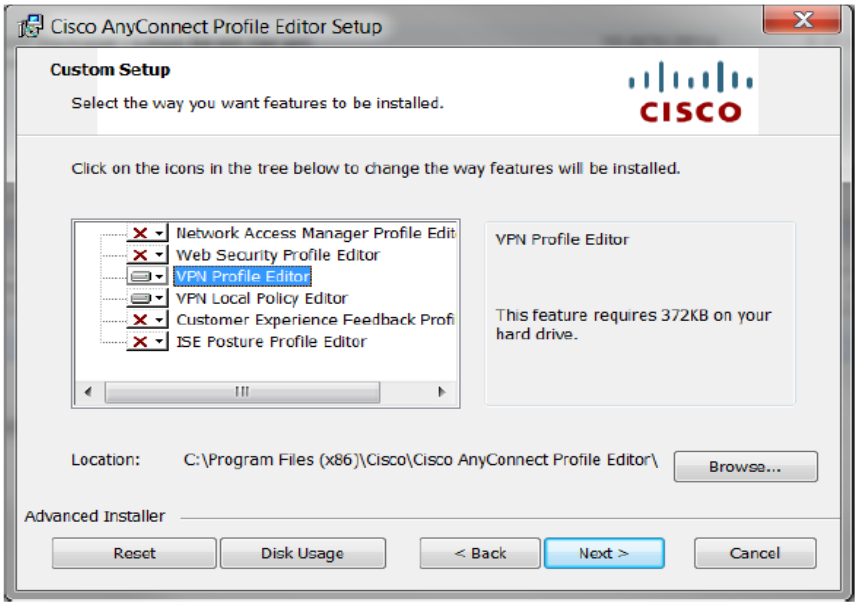

Ilustración 1. Instalador del Editor de Perfiles.

- Hacer clic en el botón “Siguiente” para continuar.
- Aparecerá un diálogo indicando que todo está listo para instalarse.
- El software se instalará en el sistema. Seleccionar la opción "Finalizar" cuando el proceso se haya completado.

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

29. Se debe configurar el cliente para funcionar en modo seguro para asegurar que solo se emplean mecanismos criptográficos seguros.
30. Para ello, en los clientes instalados en Windows, ir a *Todos los programas* > *Cisco* > *Cliente para la movilidad segura de Cisco AnyConnect* y hacer clic en el icono del editor de perfiles independiente de AnyConnect.

31. Desde el *Menu de Archivo*, selecionar la opción de *Abrir*. **Se debe marcar la opción FIPS Mode**. Seleccionar la opción de guardar y cerrar la aplicación.
32. En caso de tratarse de clientes instalados en Android, desde la ventana principal de AnyConnect, seleccionar *Menú* > *Ajustes***. Seleccionar *Modo FIPS* para activar el modo de operación segura**.
33. Después de la confirmación de cambio de modo seguro, AnyConnect cerrará la aplicación y deberá ser arrancada manualmente.

6.2 CONFIGURACIÓN DE LA PUERTA DE ENLACE VPN

6.2.1 INSTALAR Y CONFIGURAR UNA PUERTA DE ENLACE VPN

34. Se debe instalar **Cisco ASA en su versión 9.2.2** o posterior, opcionalmente con ASDM (permite que el usuario maneje el ASA desde una interfaz gráfica). De forma alternativa, la configuración puede llevarse a cabo a través de la línea de comandos (CLI).
35. Se puede consultar el detalle de instalación de las distintas versiones de Cisco ASA en el siguiente enlace.
36. Activar AnyConnect 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 AnyConnect* y seleccionar *Activar Cisco AnyConnect y Permitir Acceso bajo IKEv2*.

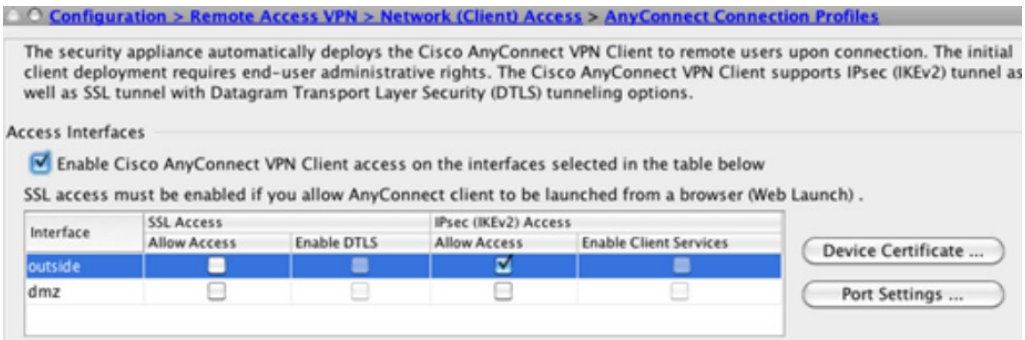

Ilustración 2. Perfiles de conexión de AnyConnect.

37. En la página de *Perfiles de Conexión de AnyConnect* 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, hacer clic en el botón *Ok*. El certificado deberá cumplir con los requisitos indicados en el apartado 6.4 GESTIÓN DE CERTIFICADOS.

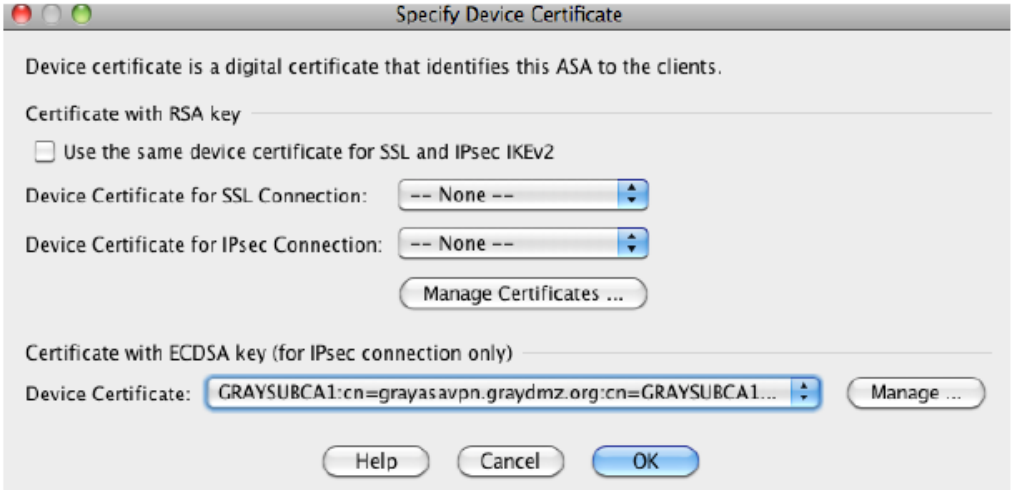

Ilustración 3. Certificado de dispositivo.

38. 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 hacer clic en el valor *Añadir* seleccionar los siguientes parámetros:

- 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.
- Cifrado: se recomienda **emplear la opción AES-GCM-256**. Las opciones disponibles son las siguientes.
  - AES: Algoritmo AES en modo CBC con longitud de clave de 128b.
  - AES-256: Algoritmo AES en modo CBC con longitud de clave de 256b.
  - AES-GCM-128: Algoritmo AES en modo GCM con longitud de clave de 128b.
  - AES-GCM-256: Algoritmo AES en modo GCM con longitud de clave de 256b.
- D-H Group: se deberán **seleccionar únicamente los valores 19 o 20**.
- Hash de integridad: null, MD5, SHA, SHA256, SHA384, SHA512. **Se deberá elegir SHA256 o superior**.
- PRF Hash: se deberá **seleccionar únicamente los valores SHA256 o SHA384**.
- Tiempo de vida: configurar un valor igual o inferior a 86400 segundos.

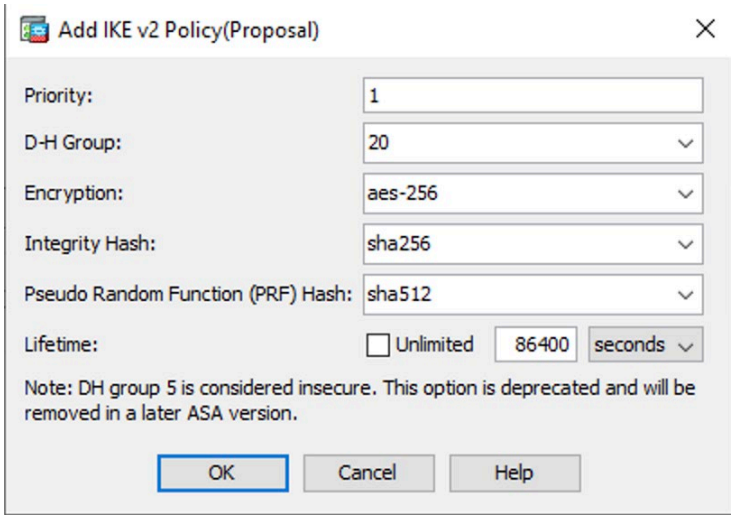

Ilustración 4. Política de IKE.

39. Una vez configurados todos los parámetros, hacer clic en el botón **Ok**.
40. 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.
        - AES: Algoritmo AES en modo CBC con longitud de clave de 128b.
        - AES-192: Algoritmo AES en modo CBC con longitud de clave de 192b.
        - AES-256: Algoritmo AES en modo CBC con longitud de clave de 256b.
        - AES-GCM-128: Algoritmo AES en modo GCM con longitud de clave de 128b.
        - AES-GCM-192: Algoritmo AES en modo GCM con longitud de clave de 192b.
        - 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**.
41. Después, hacer clic en el botón Ok.
42. 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***.** Hacer clic en el botón *Añadir*, seleccionar la interfaz saliente y la proposición **IKEv2**. Hacer clic en la pestaña de *Avanzado*:
    - **Activar NAT-T**. Activar NAT transversal para esta política.

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

43. Crear un conjunto de direcciones *VPNUSERS* que será asignado a los usuarios de VPN. Los conjuntos de direcciones contienen los siguientes campos:
    - Nombre. Especificar el nombre asignado al conjunto de direcciones IP.
    - Dirección IP de Comienzo. Especificar la primera dirección IP del conjunto.
    - Dirección IP de Final. Especificar la última dirección IP del conjunto.
    - Máscara de subred. Seleccionar la máscara de subred que será aplicada a las direcciones del conjunto.
44. 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, hacer clic en el botón **Ok.**
45. 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.
46. En ASDM, ir a *Configuración > Acceso Remoto VPN > Acceso a la red (Cliente) > Políticas de Grupo* y añadir una política de grupo interna.
47. 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, hacer clic en el botón **Ok**.
48. 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.
49. 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***,** clic en el botón *Añadir*. A continuación, se muestra un ejemplo de configuración de un grupo de túnel.

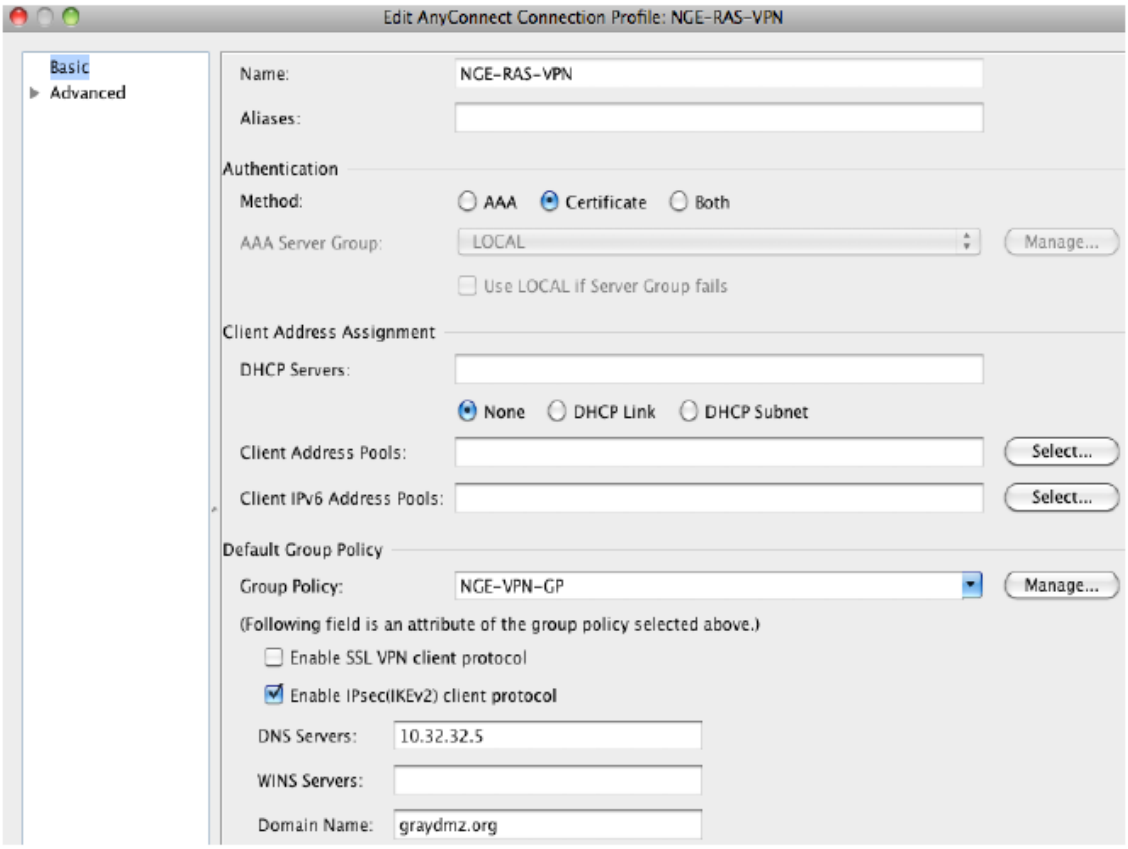

Ilustración 5. Creación del nombre de tunel.

50. **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 se habilita el uso del protocolo **IPsec (IKEv2).**

51. 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.

52. 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* clic en el botón *Añadir*. Seleccionar el existente *DefaultCertificateMap* con una prioridad de **10** y el grupo de túnel **NGE-RAS-VPN**.

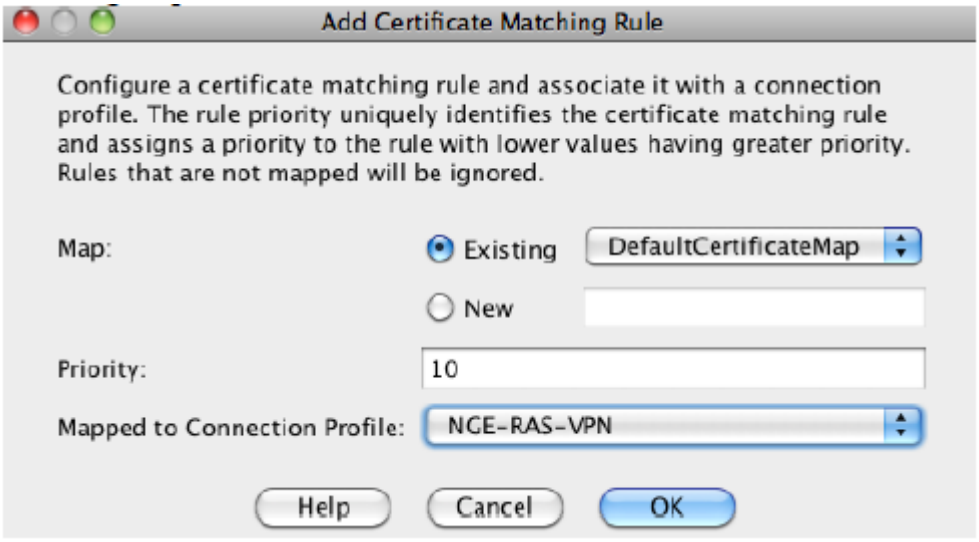

Ilustración 6. Añadir regla de certificados.

53. 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* clic en el botón *Añadir*. Elegir *Proveedor* para *Campo*, *Common Name* (CN) para componente, *Contains* para Operador y hacer clic en el botón Ok.

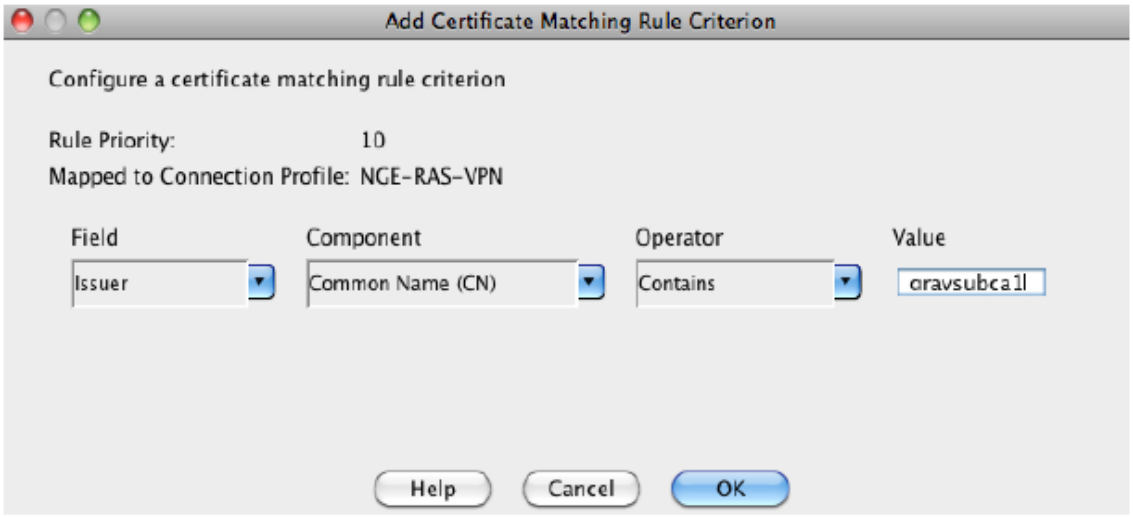

Ilustración 7. Añadir regla de certificados (II).

54. Importante darle al botón *APLICAR* en la página principal y *GUARDAR* la configuración.

6.2.2 CONFIGURACIÓN PARA WINDOWS

6.2.2.1 PERFILES DE CLIENTE DE ANYCONNECT

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

56. 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.

57. 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.*

58. Existe también una versión independiente del editor de perfiles para Windows, 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.

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

    - Creada usando el editor de perfiles integrado en ASDM y exportada a un ordenador Windows remoto o local, donde debe residir el cliente de AnyConnect.
    - Usar la versión independiente del editor de perfiles (Standalone), explicado en la siguiente sección.

6.2.2.2 EDITOR DE PERFILES INDEPENDIENTE DE ANYCONNECT

60. Es posible hacer uso del editor de perfiles independiente de AnyConnect para la configuración de los perfiles.

61. 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 hacer clic en el icono del editor de perfiles independiente de AnyConnect.

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

63. *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.

64. Desde el menú de ficheros, seleccionar *Abrir*. Ir a la ruta anterior y hacer clic en *Abrir*.

Nota de configuración: 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.

65. Después, hacer clic 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.

Ilustración 8. Lista de servidores.

66. 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.
67. Desde el menú *Archivo*, seleccionar *Guardar* y después *Salir*. Reiniciar el ordenador.
68. 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]**
69. 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 AnyConnect.

6.2.2.3 POLÍTICA LOCAL DE ANYCONNECT

70. Ir a *Todos los programas > Cisco > Cliente para la movilidad segura de Cisco AnyConnect* y hacer clic en el icono del editor de perfiles independiente de AnyConnect.

71. El archivo AnyConnectLocalPolicy.xml es un archivo XML del cliente que contiene configuraciones de seguridad. Este archivo no forma parte de la puerta de enlace ASA VPN. Por defecto se encuentra localizado en la siguiente dirección: *"%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\AnyConnectLocalPolicy.xml"*
72. Desde el *Menu de Archivo*, selecionar la opción de *Abrir*. Las siguientes configuraciones deben de estar marcadas:
    - *FIPS Mode.*
    - *Strict Certificate Trust.*
    - *Enable CRL check*.
73. La casilla de *Bypass Downloader* debe dejarse sin marcar.

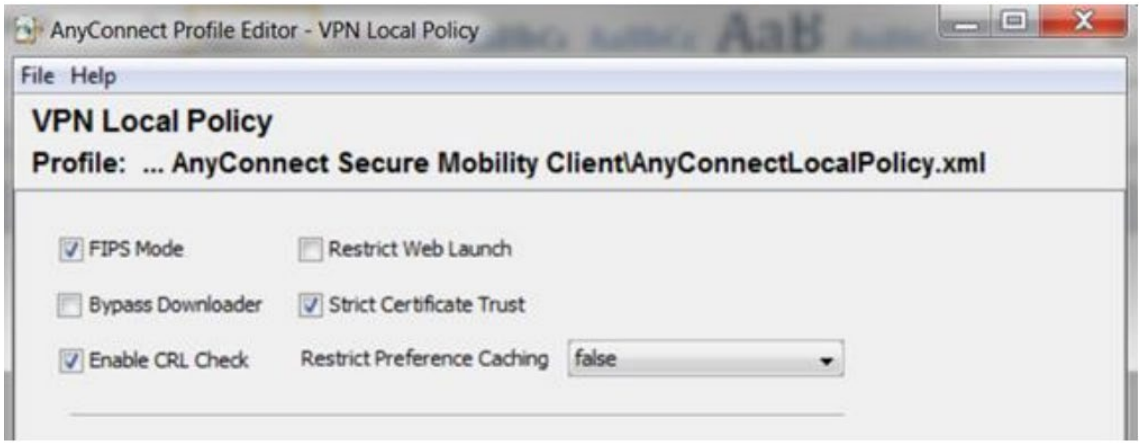

Ilustración 9. Política local de VPN.

74. Desde el *Menu de Archivo* seleccionar la opción de guardar y cerrar la aplicación.
75. La opción *Strict Certificate Trust* sirve para prevenir que los usuarios acepten certificados que no han sido verificados.
76. Para información más detallada sobre la configuración véase la **[REF4].**
77. Desde el menú de archivo hacer clic primero en guardar y luego en salir.

6.2.3 CONFIGURACIÓN PARA ANDORID

6.2.3.1 INICIAR LA APLICACIÓN

78. En el dispositivo Android, tocar el icono de AnyConnect para arrancar la aplicación.
79. Si es la primera vez que se inicia AnyConnect después de la instalación o la actualización de la aplicación, hacer clic en *OK* para habilitar AnyConnect.

6.2.3.2 AÑADIR ENTRADAS DE CONEXIONES

80. 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.

81. Desde la venta principal de AnyConnect, hacer clic en *Conexión > Añadir una nueva conexión VPN*, esto abrirá el editor de conexiones, se puede añadir una descripción opcional si se desea.

82. 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.

83. 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.

84. 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 como se muestra a continuación en el ejemplo:

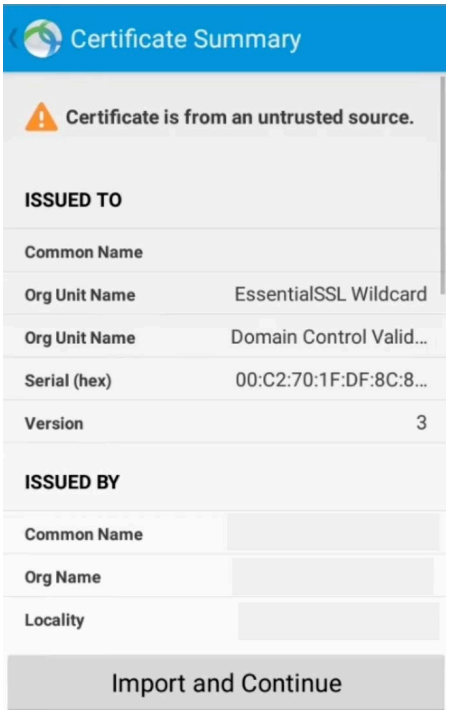

Ilustración 10. Conexión inicial en Android.

6.2.3.3 BLOQUEAR SERVIDORES NO CONFIABLES

85. 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.

86. 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.

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

6.2.3.4 CONFIGURAR LA REVOCACIÓN OCSP

88. Desde la ventana principal de AnyConnect, seleccionar *Menú > Ajustes*.

89. Seleccionar *Revocación OCSP* para activar esta configuración.

90. 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.

6.2.3.5 CERTIFICADO DE CONFIANZA

91. 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 AnyConnect, seleccionar *Menú > Ajustes*. Elegir *Certificado de Confianza* para activar la protección.

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

6.3 AUTENTICACIÓN

93. 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 dispositivo Windows o Android en el cual se encuentre instalado.

6.4 GESTIÓN DE CERTIFICADOS

6.4.1 REQUISITOS SOBRE EL CERTIFICADO DE LA PUERTA DE ENLACE

94. 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:

    - Uso de clave (Key Usage): Firma digital, Acuerdo de Clave.
    - Uso de clave extendido (Extended Key Usage): IP security IKE intermediate, IP end security system.

95. **Los certificados RSA deberán emplear siempre una longitud de clave de 3072 bits o 4096 bits.**

6.4.2 CONFIGURAR EL USO DE UN CERTIFICADO EN WINDOWS

96. Se debe 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 el siguiente enlace: http://technet.microsoft.com/en-us/library/dd632619.aspx

97. Se deberán generar los CSR siguiendo los pasos indicados en el siguiente enlace: http://technet.microsoft.com/en-us/library/cc730929.aspx

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

    - Plantilla: (Sin plantilla) Clave CNG
    - Formato de fichero: *PKCS#10*.
    - 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.
    - Uso de clave: seleccionar Firma Digital.
    - Uso de clave extendido: seleccionar Autenticación de servidor.

99. 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 Windows donde se emplee el Cliente. Para hacer esto, consultar **[REF8]**.

100. Por último, importar el certificado en el almacén de certificados dispositivo Windows una vez obtenido. Este certificado se empleará para la autenticación del cliente.

6.4.3 CONFIGURAR EL USO DE UN CERTIFICADO EN ANDROID

101. En el caso de los clientes instalados en Android, no se puede generar la CSR para obtener el certificado en el mismo dispositivo, por lo que este se deberá crear de forma externa. **Se deberán seguir las mismas recomendaciones sobre las opciones del certificado especificadas en el apartado anterior**.

102. Una vez obtenido el certificado, instalarlo en el dispositivo Android y almacenar la correspondiente clave privada en el almacén de certificados del dispositivo.

103. Tras instalar el certificado en el dispositivo, ir a la ventana principal de AnyConnect 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.

104. Este certificado se empleará para la autenticación del cliente.

6.5 SINCRONIZACIÓN HORARIA

105. **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.

6.6 ACTUALIZACIONES

106. Para actualizar el producto a una nueva versión deben seguirse los siguientes pasos:

- Verificar la versión actual: antes de realizar la actualización, verificar la versión actual de Cisco AnyConnect en el dispositivo Windows. Puede hacerse haciendo clic en el botón "Acerca de", que mostrará la información de la versión actual.
- Comprobar actualizaciones: en dispositivos Windows, verificar las actualizaciones disponibles para el software en la central de software de Cisco. En dispositivos Android, desde *Google Play Store*, buscar Cisco AnyConnect y verificar si hay una nueva versión disponible para descargar e instalar
- Suscribirse a notificaciones: es posible suscribirse al servicio de notificaciones de Cisco para recibir información importante sobre las actualizaciones de productos. Para obtener más detalles, consultar la documentación de referencia **[REF9].**
- Descargar la nueva versión: cuando haya una actualización disponible para Cisco AnyConnect, el proceso de actualización es igual a una nueva instalación, descrito en el apartado 5 FASE DE INSTALACIÓN. En el caso de dispositivos Android, descargar desde *Google Play Store* y seguir las instrucciones por pantalla de Anyconnect.

107. Para dispostivos Windows, una vez descargado el fichero se deberá comprobar la integridad de los archivos de instalación, empleando el hash SHA-512 disponible en la página de descarga. La comprobación se debe llevar a cabo siguiendo estos pasos:

- Descargar el archivo de instalación de AnyConnect.
- Generar el hash SHA-512 del fichero instalador facilitado por Cisco.
- Compararlo con el hash facilitado por Cisco y verificar que coinciden.

6.7 AUTO-CHEQUEOS

108. La aplicación 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.

109. 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

110. 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 AnyConnect. El detalle sobre el uso de DART se puede consultar en **[REF10].**

111. 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 AnyConnect.

112. 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 **[REF11].**

113. Por último, el *Gateway* también 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 siguiente enlace.

6.8.2 ALMACENAMIENTO LOCAL

114. 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.*

115. 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 AnyConnect.

116. 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.

6.8.3 ALMACENAMIENTO REMOTO

117. Debido a que los registros generados por los clientes son almacenados en el dispositivo en el cual se encuentran instalados, el producto no dispone de la capacidad de reenviar dichos registros a un servidor externo.

6.9 FUNCIONES DE SEGURIDAD

6.9.1 ESTABLECER UNA CONEXIÓN VPN EN WINDOWS

118. Para establecer una conexión VPN, ejecutar el Cliente de Cisco AnyConnect Secure Mobility. Hacer click en el botón de conectar para conectarse a una de las puertas de enlace VPN predefinidas.

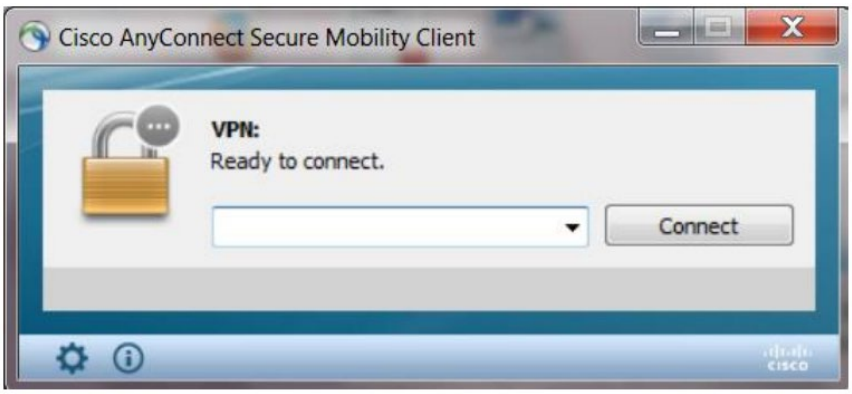

Ilustración 11. Conexión VPN.

6.9.2 BLOQUEAR CERTIFICADOS NO CONFIABLES EN WINDOWS

119. Seleccionar el icono del engranaje para acceder a la configuración del cliente de AnyConnect y seleccionar la casilla de “Block Connections to Untrusted Servers”.

6.9.3 ACEPTACIÓN DEL CERTIFICADO PARA LA PUERTA DE ENLACE DE LA VPN EN WINDOWS

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

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

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

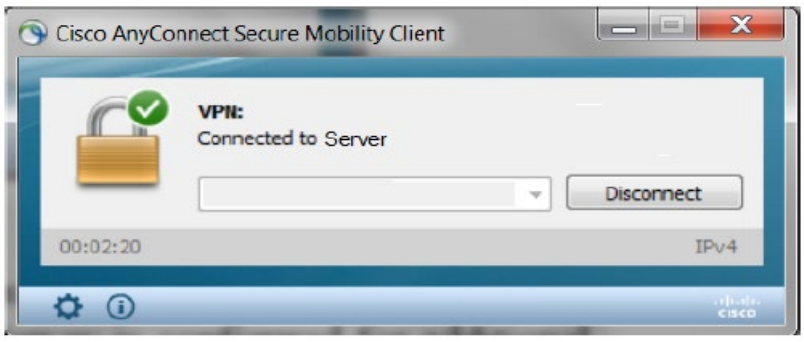

Ilustración 12. Cliente conectado al servidor.

123. Para finalizar la sesión VPN, hacer click en el botón Desconectar, tal y como se muestra en la siguiente figura.

124. Si el certificado de la puerta VPN no es válido o falla la comprobación del CLR, AnyConnect no permitirá la conexión. Si esta situación ocurriese, el administrador recibirá el siguiente mensaje:

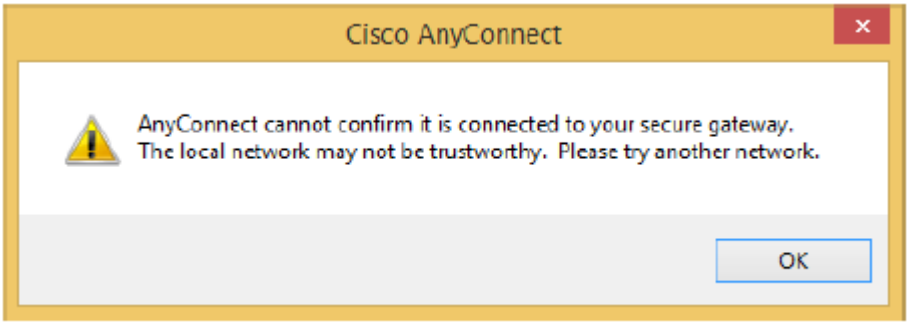

Ilustración 13. Advertencia de conexión no segura.

125. Después de seleccionar OK, el intento de conexión mostrará que ha fallado, tal y como muestra la siguiente figura:

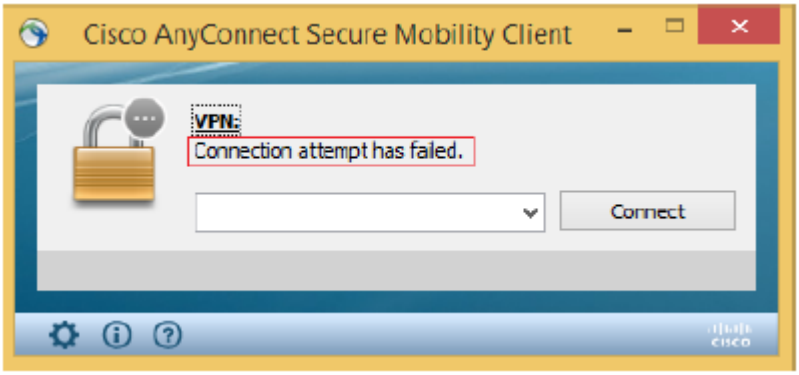

Ilustración 14. Fallo de conexión.

6.9.4 ESTABLECER UNA CONEXIÓN VPN EN ANDROID

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

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

128. 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 AnyConnect.

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

- Ir a la pantalla principal de AnyConnect.
- Tocar en “Conexión” y después otra vez en el objetivo de su conexión.

130. AnyConnect se desconecta de cualquier conexión VPN activa y realiza la nueva conexión.

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

7. FASE DE OPERACIÓN

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

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

8. *CHECKLIST*

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la integridad	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Activación del modo seguro	☐	☐	
CONFIGURACIÓN DE LA PUERTA DE ENLACE			
Configuración de los perfiles de cliente	☐	☐	
Configuración de la política local	☐	☐	
GESTIÓN DE CERTIFICADOS			
Importar CA, crear CSR e importar el certificado de cliente.	☐	☐	
Importar el certificado de la puerta de enlace	☐	☐	

9. REFERENCIAS

REF1 CCN-STIC-496

https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2913-ccn-stic-496-sistemas-de-comunicaciones-moviles/file.html

REF2 Cisco Software central

https://software.cisco.com/

REF3 AnyConnect VPN Wizard

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/vpn/asdm_71_vpn_config/vpn_asdm_wizard.html#pgfId-1052383

REF4 The AnyConnect VPN Profile

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect410/administration/guide/b-anyconnect-admin-guide-4-10/anyconnect-profile-editor.html#ID-1430-00000061

REF5 Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.6.x

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect46/user/guide/Android_AnyConnect_User_Guide_4-6-x.html

REF6 CCN-STIC-807

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html

REF7 Active Directory Certificate Services Step-by-Step Guide

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772393(v=ws.10)?redirectedfrom=MSDN

REF8 Import a Certificate Microsost

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754489(v=ws.11)?redirectedfrom=MSDN

REF9 Security Vulnerability Policy

https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html

REF10 DART guide

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect410/administration/guide/b-anyconnect-admin-guide-4-10/troubleshoot-anyconnect.html

REF11 How to get Anyconnect Diagnostic file from Android

https://community.cisco.com/t5/security-knowledge-base/how-to-get-anyconnect-diagnostic-file-from-android-and-ios/ta-p/3156497

REF12 VPN ASDM configuration Guide

https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/vpn/asdm-78-vpn-config/vpn-asdm-setup.html?bookSearch=true#ID-2188-00000218

REF13 Install and Configure Cisco AnyConnect for Android

https://dcloud-cms.cisco.com/help/android_anyconnect

10.ABREVIATURAS

ASDM	Herramienta de control de ASA
ASA	Puerta de enlace de la VPN
CA	Autoridad de certificación
CSR	*Certificate Signing Request*
CRL	*Certificate Revocation List*
ENS	Esquema Nacional de Seguridad.
FQDN	*Fully Qualified Domain Name*
IKE	*Internet Keey Exchange*
OS	*Operative System*
OCSP	*Online Certificate Status Protocol*
SSL	*Secure Sockets L*
VPN	Red privada virtual

PUBLICACIONES Pd DE DEFENSA

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