centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1449

Procedimiento de Empleo Seguro
Cisco AnyConnect Secure Mobility 4.9 para iOS 13

Enero 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

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.02.01 12:35:50 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-021-0.
Fecha de Edición: enero de 2024.

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

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. El objetivo de este documento es proporcionar una guía o procedimiento de configuración y empleo seguro de la aplicación Cisco AnyConnect Secure Mobility v4.9, en adelante AnyConnect.
2. La aplicación AnyConnect es un cliente VPN que permite a los usuarios remotos establecer un túnel VPN seguro para proteger la información en tránsito, tanto en redes IPv4 como IPv6.
3. Protege la información de la divulgación y/o modificación no autorizada mediante un túnel VPN, de forma que los usuarios remotos pueden conectarse de forma segura a los recursos y servicios desplegados en la red interna de una organización.
4. El túnel VPN se establece utilizando los protocolos criptográficos de IPsec, proporcionando la autenticación mutua de los extremos que se van a comunicar y el cifrado del tráfico de red a través de redes públicas inseguras.
5. Los dispositivos mencionados en esta guía han sido cualificados e incluidos en el **Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC)** para categoría ALTA en las familias de "*Redes Privadas Virtuales. SSL*". Se recomienda consultar el Catálogo para conocer la versión cualificada en cada momento.

2. OBJETO Y ALCANCE

6. El objeto del presente documento es facilitar la instalación y configuración segura de la aplicación **Cisco AnyConnect Secure Mobility con la versión 4.9 para la plataforma iOS v13.x**, junto con el aseguramiento del entorno en el que se despliega. El producto ha sido incluido en el Catálogo de Productos y Servicios de Seguridad TIC en la familia **Redes Privadas Viruales SSL.**

3. ORGANIZACIÓN DEL DOCUMENTO

7. 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 IOS

8. La única fuente autorizada para descargar la aplicación 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*.
9. 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.

4.2 ENTORNO DE INSTALACIÓN SEGURO

10. El producto requiere de al menos una Autoridad de Certificación (CA), un terminador VPN ASA-5500VPN y una plataforma con sistema operativo iOS 13 en el entorno operacional.
11. AnyConnect requiere, como mínimo, los siguientes componentes en el entorno dependiendo del sistema operativo:

4.2.1 ENTORNO DE OPERACIÓN PARA IOS

12. Se debe usar una Autoridad Certificadora para proveer certificados digitales válidos.
13. 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.
14. El software del ASDM 7.1(x) o posterior puede operar en cualquiera de los siguientes sistemas operativos:
    - Windows 7, 8
    - Apple OS X 10.4 or later
    - Red Hat Enterprise Linux 5 (GNOME or KDE) REGISTRO Y LICENCIAS

4.3 CONSIDERACIONES PREVIAS

15. Es necesario importar los certificados de la Autoridad de Certificación (CA) en la plataforma en la que se está ejecutando el producto. Ver apartado 6.4 GESTIÓN DE CERTIFICADOS.
16. Se debe emplear el modo de operación seguro para asegurar el uso de mecanismos criptográficos seguros. Ver apartado 6.1 MODO DE OPERACIÓN SEGURO.

17. La puerta de enlace de la VPN es referenciada en este documento como “ASA”

5. FASE DE INSTALACIÓN

18. Para instalar AnyConnect en iOS se deben seguir los diferentes menús de instalación que muestra la aplicación una vez se da a instalar desde la *App Store*.

    - Abrir la *App Store.*
    - Buscar Cisco AnyConnect.
    - Elegir *Gratis* e *Instalar Aplicación.*
    - Seleccionar *Instalar.*

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

19. Se debe configurar el cliente para funcionar en modo seguro para asegurar que solo se emplean mecanismos criptográficos seguros.
20. Desde la ventana principal de AnyConnect, seleccionar *Menú > Ajustes*. **Seleccionar *Modo FIPS* para activar el modo de operación segura**.
21. 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

6.2.1.1 INSTALAR Y CONFIGURAR UNA PUERTA DE ENLACE VPN

22. 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).
23. Se puede consultar el detalle de instalación de las distintas versiones de Cisco ASA en el siguiente enlace.
24. 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*. Seleccionar también la casilla de Enable Client Services.

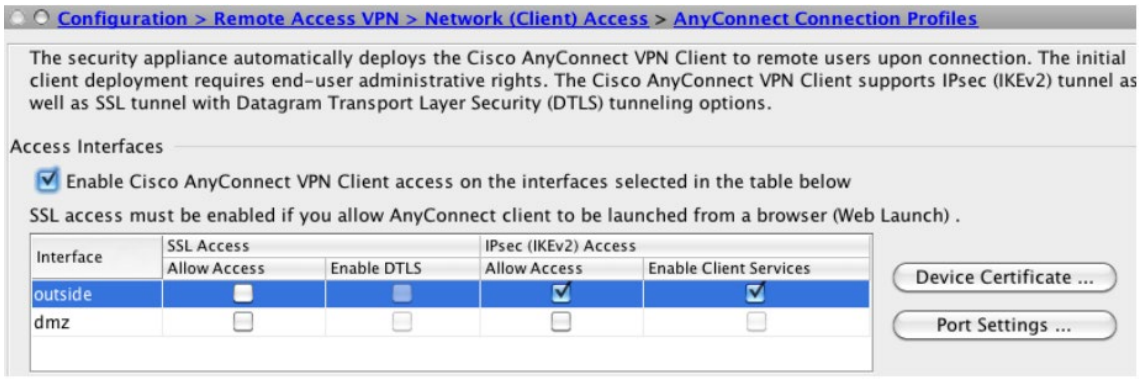

Ilustración 1. Perfiles de conexión de AnyConnect.

25. 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.

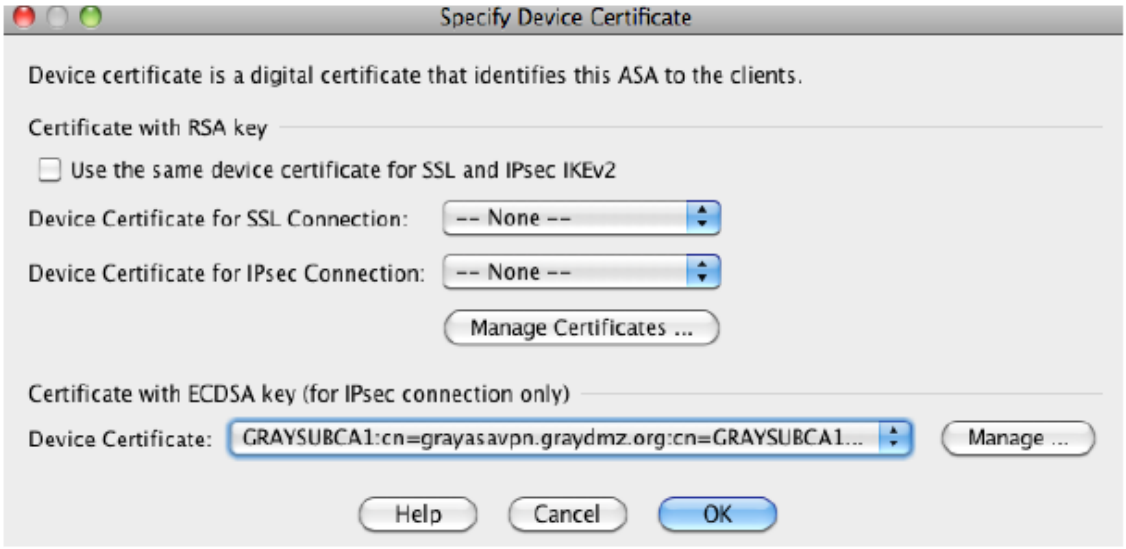

Ilustración 2. Certificado de dispositivo.

26. 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.

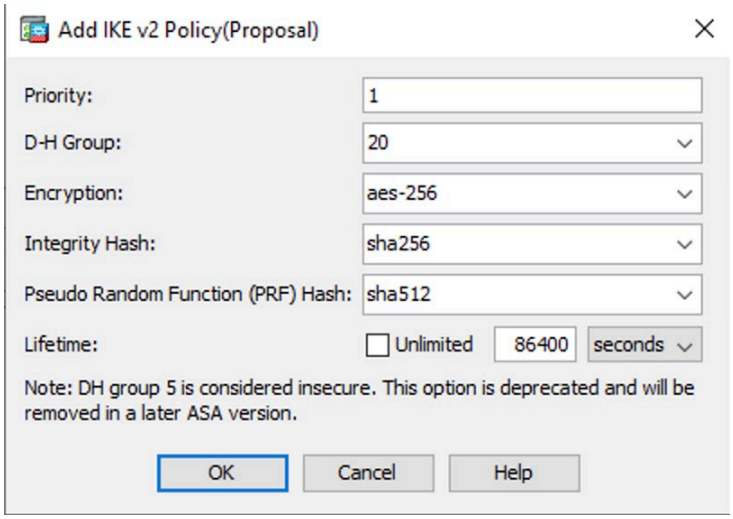

Ilustración 3. Política de IKE.

27. Una vez configurados todos los parámetros, hacer clic en el botón **Ok**.
28. 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**.
29. Después, hacer clic en el botón Ok.
30. 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).

31. 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.
32. 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.**
33. 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.
34. En ASDM, ir a *Configuración > Acceso Remoto VPN > Acceso a la red (Cliente) > Políticas de Grupo* y añadir una política de grupo interna.
35. 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**.
36. 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.
37. 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.

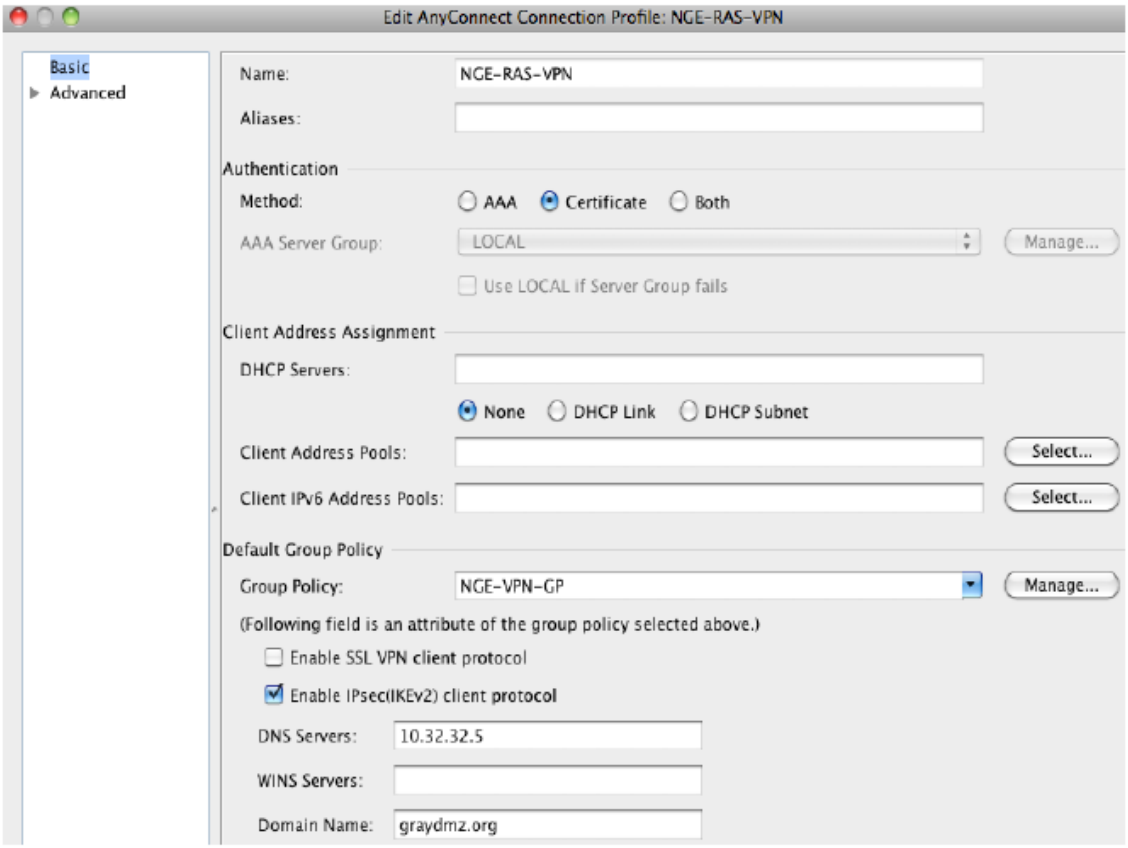

Ilustración 4. Editor de conexiones de perfil.

38. **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).**

39. 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.

40. 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**.

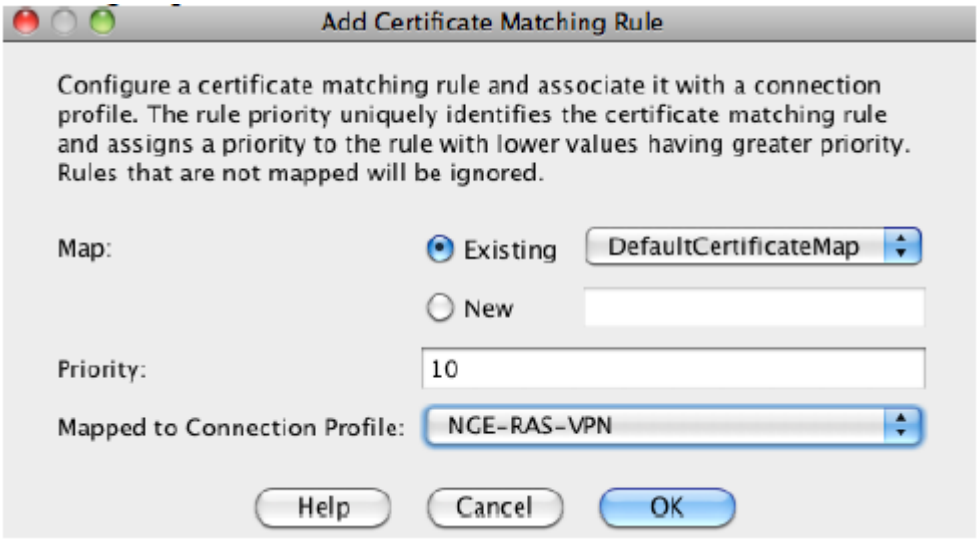

Ilustración 5. Añadir regla de certificado.

41. 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.

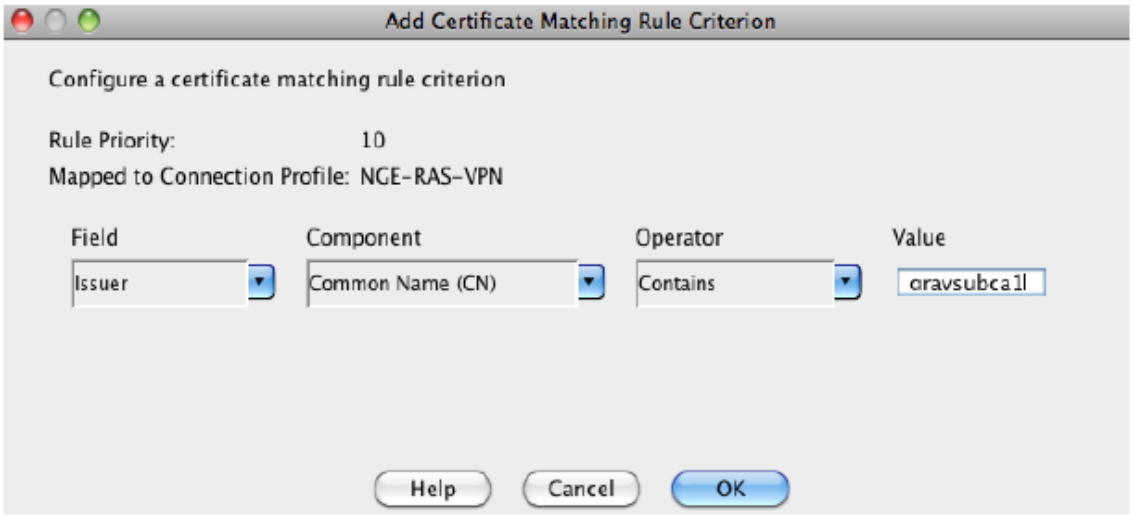

Ilustración 6. Añadir criterio de regla de certificado.

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

6.2.1.2 INICIAR LA APLICACIÓN

43. Tocar el icono de AnyConnect para arrancar la aplicación.
44. Si es la primera vez que se inicia AnyConnect después de la instalación o la actualización de la aplicación, haga click en *OK* para habilitar AnyConnect.

6.2.1.3 AÑADIR ENTRADAS DE CONEXIONES

45. 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.
46. Desde la ventana 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.
47. 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.
48. 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.
49. 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:
50. Para finalizar, se debe configurar la conexión IPsec.
    - Elegir *Conectar con IPsec*. El parámetro de *Autenticación* se activa en este momento, hacer click en él.
    - 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.
    - Seleccionar *Hecho* en la ventana de *Avanzado* y también en la del *Editor de Conexiones* para guardar la configuración de la conexión. AnyConnect añadirá la nueva conexión.

6.2.1.4 BLOQUEAR SERVIDORES NO CONFIABLES

51. Esta sección de configuración de la aplicación determina si AnyConnect bloqueará conexiones cuando no pueda identificar correctamente a la puerta de enlace segura. Esta protección se encuentra activada por defecto y no debe ser desactivada.
52. 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.
53. Desde la pantalla principal de AnyConnect, ir a *Menu > Ajustes.* Verificar que la opción de *Bloquear conexiones inseguras* está marcada.

6.2.1.5 CONFIGURAR LA REVOCACIÓN OSCP

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

55. Seleccionar *Revocación OCSP* para activar esta configuración.
56. 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.

6.2.1.6 CERTIFICADO DE CONFIANZA

57. 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.
58. En el siguiente intento de conexión, *Strict Certificate Trust* estará activado.

6.3 AUTENTICACIÓN

59. 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 en el cual se encuentre instalado.

6.4 GESTIÓN DE CERTIFICADOS

6.4.1 INSTALAR Y CONFIGURAR UNA AUTORIDAD CERTIFICADORA

60. 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.
61. **Los certificados RSA deberán emplear siempre una longitud de clave de 3072 bits o 4096 bits.**

6.4.2 CREACIÓN DEL CERTIFICADO DE CLIENTE

62. Se debe generar un certificado para ser empleado por el dispositivo móvil para autenticación. Esto se tendrá que hacer de forma externa al dispositivo móvil.
63. 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 el siguiente enlace: http://technet.microsoft.com/en-us/library/dd632619.aspx
64. Se deberán generar los CSR siguiendo los pasos indicados en el siguiente enlace: http://technet.microsoft.com/en-us/library/cc730929.aspx
65. 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.

66. 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 **[REF8]**.
67. Por último, importar el certificado en el almacén de certificados dispositivo iOS una vez obtenido. Este certificado se empleará para la autenticación del cliente.
68. 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.

6.5 SINCRONIZACIÓN HORARIA

69. **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

70. Para verificar si existen nuevas actualizaciones, se debe ir a *App Store* y buscar Cisco AnyConnect. La aplicación mostrará si es necesaria una actualización o existen versiones nuevas.
71. Si alguna actualización está disponible, el proceso de actualización será el mismo que el proceso de instalación descrito en el apartado 5 FASE DE INSTALACIÓN.

6.7 AUTO-CHEQUEOS

72. El producto realiza verificaciones de integridad al cargar la aplicación. Se verifican los servicios criptográficos y si alguna prueba falla, no carga la interfaz de usuario, impidiendo así su uso.

6.8 AUDITORÍA

6.8.1 REGISTRO DE EVENTOS

73. **Se debe acceder a *Menu* > *Diagnostics* y activar "Registros de depuración de VPN"** para que el producto genere y almacene los registros.
74. Estos se pueden consultar desde *Menu* > *Diagnostics* > *Logging and System Information*.
75. 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.
76. 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.

6.9 FUNCIONES DE SEGURIDAD

6.9.1 ESTABLECER UNA CONEXIÓN VPN EN IOS

77. 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.
78. Se debe disponer de una conexión Wi-Fi activa, o de una conexión con un proveedor de servicios para conectarse a una VPN.
79. 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.
80. 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.
81. AnyConnect se desconecta de cualquier conexión VPN activa y realiza la nueva conexión.
82. Si el proceso de autenticación se completa satisfactoriamente, se mostrará un mensaje indicando que la conexión VPN se ha completado satisfactoriamente.

6.9.2 VISUALIZAR LAS ESTADÍSITCAS DE ANYCONNECT

83. AnyConnect recopila estadísticas cuando hay presente una conexión VPN. Desde la pantalla principal de AnyConnect, seleccionar *Detalles*. Las estadísticas detalladas incluyen los siguientes valores:

    - Rutas seguras: Una entrada que contiene el destino 0.0.0.0 y la máscara de subred 0.0.0.0 indica que el tráfico VPN está cifrado y enviado o recibido a través de la conexión VPN. Esto se corresponde con tráfico en el SPD que requiere IPsec.
    - Rutas no seguras: Mostradas únicamente si 0.0.0.0/0.0.0.0 está presente bajo los destinos de rutado de tráfico seguro si el túnel dividido se encuentra activado por el administrador de la puerta de enlace VPN. Esto se corresponde con tráfico que evadirá la protección IPsec.

7. FASE DE OPERACIÓN

84. 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 iOS 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/anyconnect49/administration/guide/b_AnyConnect_Administrator_Guide_4-9/b_AnyConnect_Administrator_Guide_4-4_chapter_01101.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 DE DEFENSA

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