Autenticación ASA 8.x Anyconnect con el indicador luminoso LED amarillo de la placa muestra gravedad menor belga del eID

Contenido

Introducción

Este documento describe cómo configurar la autenticación ASA 8.x Anyconnect para utilizar el indicador luminoso LED amarillo de la placa muestra gravedad menor belga del eID.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA 5505 con el software apropiado ASA 8.0
- Cliente de AnyConnect
- ASDM 6.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

El eID es un indicador luminoso LED amarillo de la placa muestra gravedad menor PKI (Public Key Infrastructure) publicado por el gobierno belga que los usuarios deben utilizar para autenticar en las ventanas remotas PC. El software cliente de AnyConnect está instalado en PC local y toma los credenciales de autenticación de la PC remota. Una vez que la autenticación es completa, el usuario remoto accede a los recursos centrales a través de un túnel lleno SSL. El usuario remoto es aprovisionado con una dirección IP obtenida de un pool manejado por el ASA.

PC local configuración

Sistema operativo

El sistema operativo (Windows, MacOS, Unix, o Linux) en su PC local deben ser actuales con todas las parches requerido instaladas.

Lector de tarjetas

Un lector de tarjetas electrónicas debe ser instalado en su computadora local para utilizar el indicador luminoso LED amarillo de la placa muestra gravedad menor del eID. El lector de tarjetas electrónicas es un dispositivo de hardware que los establishs un canal de comunicación entre los programas sobre el ordenador y el chip en el ID cardan.

Para una lista de lectores de tarjetas aprobados, refiera a este URL:
http://www.cardreaders.be/en/default.htm

Note: Para utilizar al lector de tarjetas, usted debe instalar los drivers recomendados por el proveedor de hardware.

software del Runtime del eID

Usted debe instalar el software del tiempo de ejecución del eID proporcionado por el gobierno belga. Este software permite que el usuario remoto lea, valide, e imprima el contenido del indicador luminoso LED amarillo de la placa muestra gravedad menor del eID. El software está disponible en francés y holandés para Windows, MAC OS X, y Linux.

Para más información, refiera a este URL:

- http://www.belgium.be/zip/eid_datacapture_nl.html

Certificado de la autenticación

Usted debe importar el certificado de la autenticación en el almacén de Microsoft Windows en PC local. Si usted no puede importar el certificado en el almacén, el cliente de AnyConnect no podrá establecer una conexión SSL al ASA.

Procedimiento

Para importar el certificado de la autenticación en el almacén de Windows, complete estos pasos:

1. Inserte su eID en el lector de tarjetas, y ponga en marcha el software intermediario para acceder el contenido del indicador luminoso LED amarillo de la placa muestra gravedad menor del eID.El contenido del indicador luminoso LED amarillo de la placa muestra gravedad menor del eID aparece.
2. Haga clic la lengueta de **Certificats** (FR).Se visualiza la jerarquía de los Certificados.
3. Amplíe **Bélgica raíz CA**, y después amplíe al **ciudadano CA.**
4. Elija la versión de la **autenticación de** su certificado Nombrado.
5. Haga clic el botón de **Enregistrer** (FR).El certificado se copia en el almacén de Windows.

Note: Cuando usted hace clic el **botón Details Button**, una ventana aparece que los detalles de las visualizaciones sobre el certificado. En los detalles tabule, seleccione el **campo Subject** para ver el campo del número de serie. El campo del número de serie contiene un valor único que se utilice para la autorización de usuario. Por ejemplo, el número de serie “56100307215" representa a un usuario cuya fecha de nacimiento sea de octubre el 3 de 1956 con un número de secuencia de 072 y un dígito de control de 15. *Usted debe someter una petición para la aprobación de las autoridades federales para salvar estos números. Es su responsabilidad hacer las declaraciones oficiales apropiadas relacionadas con el mantenimiento de una base de datos de los ciudadanos belgas en su país*.

Verificación

Para verificar que el certificado importado con éxito, complete estos pasos:

1. En una máquina de Windows XP, abra una ventana de DOS, y teclee el comando **mmc**.La aplicación de consola aparece.
2. Elija el **archivo > Add/quítelo Broche-en** (o prensa Ctrl+M).El agregar/quita Broche-en el cuadro de diálogo aparece.

3. ‘Haga clic en el botón Add (Agregar).’El agregar independiente Broche-en el cuadro de diálogo aparece.
4. En la lista independiente disponible Broche-INS, elija los **Certificados**, y el haga click en Add
5. Haga clic el **mi** botón de radio de la **cuenta de usuario**, y el clic en Finalizar.El certificado broche-en aparece en el agregar/quita Broche-en el cuadro de diálogo.
6. El tecleo **cercano** para cerrar el agregar independiente Broche-en el cuadro de diálogo, y después hacer clic la **AUTORIZACIÓN** en el agregar/quita Broche-en el cuadro de diálogo para salvar sus cambios y volver a la aplicación de consola.
7. Conforme a la carpeta de la raíz de la consola, amplíe los **Certificados - Usuario usuario actual**.
8. Amplíe **personal**, y después amplíe los **Certificados**.El certificado importado debe aparecer en el almacén de Windows tal y como se muestra en de esta imagen:

Instalación de AnyConnect

Usted debe instalar al cliente de AnyConnect en la PC remota. El software de AnyConnect utiliza un archivo de configuración XML que se pueda editar para preestablecer una lista de gatewayes disponibles. El archivo XML se salva en esta trayectoria en la PC remota:

C:\Documents and Settings\ el *%USERNAME%* \ datos de aplicación \ Cisco \ Cliente Cisco AnyConnect VPN

donde está el nombre el *%USERNAME% del* usuario en la PC remota.

El nombre del archivo XML es *preferences.xml. Aquí* está un ejemplo del contenido del archivo:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectPreferences>
<DefaultHost>192.168.0.1</DefaultHost> </AnyConnectPreferences>
```

donde está la dirección IP *192.168.0.1 del* gateway ASA.

Requisitos ASA

Asegúrese de que el ASA cumpla estos requisitos:

- AnyConnect y el ASDM deben ejecutarse en el flash.Para completar los procedimientos en este documento, utilice un ASA 5505 con el software apropiado ASA 8.0 instalado. El AnyConnect y las aplicaciones ASDM se deben cargar en el flash. Utilice el **comando show flash** para ver el contenido del flash:

```
ciscoasa#show flash:
--#--  --length--  -----date/time------  path
   66  14524416    Jun 26 2007 10:24:02  asa802-k8.bin
   67  6889764     Jun 26 2007 10:25:28  asdm-602.bin
   68  2635734     Jul 09 2007 07:37:06  anyconnect-win-2.0.0343-k9.pkg
```

- El ASA debe ejecutarse con los valores predeterminados de fábrica.Usted puede saltar este requisito si usted utiliza un nuevo chasis ASA para completar los procedimientos en este documento. Si no, complete estos pasos para reajustar el ASA a los valores predeterminados de fábrica:En la aplicación ASDM, conecte con el chasis ASA, y elija el **archivo > dispositivo reajustado a la configuración predeterminada de fábrica**.Deje los valores predeterminados en

la plantilla.Conecte su PC en los Ethernetes 0/1 interfaz interior, y renueve su dirección IP que sea aprovisionado del servidor DHCP del ASA.**Note**: Para reajustar el ASA a los valores predeterminados de fábrica de la línea de comando, utilice estos comandos:

```
ciscoasa#conf t
ciscoasa#config factory-default 192.168.0.1 255.255.255.0
```

Configuración ASA

Una vez que usted reajusta los valores predeterminados de fábrica ASA, usted puede comenzar el ASDM a 192.168.0.1 para conectar con el ASA en los Ethernetes 0/1 interfaz interior.

Note: Se preserva su contraseña anterior (o puede ser en blanco por abandono).

Por abandono, el ASA valida a una Sesión de administración entrante con una dirección IP de origen en la subred 192.168.0.0/24. El servidor DHCP predeterminado que se habilita en la interfaz interior del ASA proporciona los IP Addresses en el rango 192.168.0.2-129/24, válido para conectar con la interfaz interior con el ASDM.

Complete estos pasos para configurar el ASA:

1. Habilite la interfaz exterior
2. Configure el Domain Name, la contraseña, y el Tiempo del sistema
3. Habilite a un servidor DHCP en la interfaz exterior
4. Configure a la agrupación de direcciones del eID VPN
5. Importe la Bélgica certificado raíz CA
6. Configure Secure Sockets Layer
7. Defina la directiva del grupo predeterminado
8. Defina la asignación del certificado
9. Agregue a un usuario local
10. Reinicie el ASA

Paso 1. Habilite la interfaz exterior

Este paso describe cómo habilitar la interfaz exterior.

1. En la aplicación ASDM, la **configuración del** tecleo, y entonces hace clic la **configuración de dispositivo**.
2. En el área de configuración de dispositivo, elija las **interfaces**, y después haga clic la lengueta de las **interfaces**.
3. Seleccione la interfaz exterior, y el tecleo **edita**.
4. En la sección de la dirección IP de la ficha general, elija la opción del **uso IP estático**.
5. Ingrese **197.0.100.1** para el IP Address y **255.255.255.0** por la máscara de subred.
6. Haga clic en Apply (Aplicar).

Paso 2. Configure el Domain Name, la contraseña, y el Tiempo del sistema

Este paso describe cómo configurar el Domain Name, la contraseña, y el Tiempo del sistema.

1. En el área de configuración de dispositivo, elija el **Nombre del dispositivo/la contraseña**.

2. Ingrese **cisco.be para el** Domain Name, y ingrese cisco123for el valor de contraseña habilitada.**Note**: Por abandono, la contraseña es en blanco.
3. Haga clic en Apply (Aplicar).
4. En el área de configuración de dispositivo, elija el **Tiempo del sistema**, y cambie el valor del reloj (en caso necesario).
5. Haga clic en Apply (Aplicar).

Paso 3. Habilite a un servidor DHCP en la interfaz exterior.

Este paso describe cómo permitir a un servidor DHCP en la interfaz exterior para facilitar el probar.

1. **La configuración del** tecleo, y entonces hace clic la **Administración de dispositivos**.
2. En el área de la Administración de dispositivos, amplíe el **DHCP**, y elija al **servidor DHCP**.
3. Seleccione la interfaz exterior de la lista de interfaz, y el tecleo **edita**.El cuadro de diálogo del servidor DHCP del editar aparece.
4. Marque la casilla de verificación del **servidor DHCP del permiso**.
5. En conjunto de direcciones DHCP, ingrese un IP Address de 197.0.100.20 a 197.0.100.30.
6. En el área global de las opciones DHCP, desmarque la **autoconfiguración del permiso del** cuadro de **comprobaciones de interfaz**.
7. Haga clic en Apply (Aplicar).

Paso 4. Configure a la agrupación de direcciones del eID VPN

Este paso describe cómo definir un pool de los IP Addresses que se utiliza para provision a los clientes remotos de AnyConnect.

1. **La configuración del** tecleo, y entonces hace clic el **VPN de acceso remoto**.
2. En el área del VPN de acceso de la eliminación, amplíe el **acceso de la red (cliente)**, y después amplíe la **asignación de dirección**.
3. Elija a las **agrupaciones de direcciones**, y después haga clic el **botón Add** situado en la configuración nombrada área de pools de la dirección IP.Aparece el cuadro de diálogo Agregar Pool IP.
4. En el campo de nombre, ingrese el **EID-VPNPOOL**.
5. En el IP Address que comienza y la terminación de los campos del IP Address, ingrese un rango del IP Address de 192.168.10.100 a 192.168.10.110.
6. Elija **255.255.255.0 de la** lista desplegable de la máscara de subred, haga clic la **AUTORIZACIÓN**, y después haga clic **se aplican**.

Paso 5. Importe la Bélgica certificado raíz CA

Este paso describe cómo importar en el ASA la Bélgica certificado raíz CA.

1. Descargue y instale los Certificados de Bélgica raíz CA (belgiumrca.crt y belgiumrca2.crt) del sitio web del gobierno y sálvelos en su PC local.El sitio web del gobierno de Bélgica está situado en este URL: http://certs.eid.belgium.be/
2. En el área del VPN de acceso remoto, amplíe la **administración de certificados**, y elija los **Certificados de CA**.

3. El tecleo **agrega**, y después hace clic **instala del archivo**.
4. Hojee a la ubicación en la cual usted guardó el archivo de Bélgica certificado raíz CA (belgiumrca.crt), y haga clic InstallCertificate**.**
5. Haga clic en **Aplicar** para guardar los cambios.

Esta imagen muestra el certificado instalado en el ASA:

Paso 6. Configuración Secure Sockets Layer

Este paso describe cómo dar prioridad a las opciones de encripción seguras, definir la imagen del cliente VPN SSL, y definir el perfil de la conexión.

1. Dé prioridad a las opciones de encripción más seguras.En el área del VPN de acceso remoto, amplíe **avanzado**, y elija las **configuraciones SSL**. En la sección del cifrado, los algoritmos activos se empilan, top abajo, como sigue:AES256-SHA1AES128-SHA13DES-SHA1RC4-SHA1
2. Defina la imagen del cliente VPN SSL para el cliente de AnyConnect.En el área del VPN de acceso remoto, amplíe **avanzado**, amplíe **SSL VPN**, y elija las **configuraciones del cliente**.En el área de las imágenes del cliente VPN SSL, haga click en AddElija el paquete de AnyConnect que se salva en el flash.El paquete de AnyConnect aparece en el cliente VPN SSL que las imágenes enumeran tal y como se muestra en de esta imagen:
3. Defina el perfil de la conexión de DefaultWEBVPNGroup.En el área del VPN de acceso remoto, amplíe el **acceso de la red (cliente)**, y elija los **perfiles de la conexión VPN SSL**.En el área de las interfaces de acceso, marque la **casilla de verificación del Cliente Cisco AnyConnect VPN del permiso**.Para la interfaz exterior, marque el **acceso de la permit**, **requiera el certificado del cliente**, y **habilite las** casillas de verificación **DTL** tal y como se muestra en de esta imagen:En el área de los perfiles de la conexión, elija **DefaultWEBVPNGroup**, y el tecleo **edita**.El cuadro de diálogo del perfil de la conexión VPN del editar SSL aparece.En el área de la navegación, elija **básico**.En el área de la autenticación, haga clic el botón de radio del **certificado**.En el área de directiva del grupo predeterminado, marque la casilla de verificación del **protocolo del cliente VPN SSL**.Amplíe **avanzado**, y elija la **autenticación**.El tecleo **agrega**, y agrega la interfaz exterior con un grupo de servidor local tal y como se muestra en de esta imagen:En el área de la navegación, elija la **autorización**.En el área predeterminada del grupo de servidor de autorización, elija el **LOCAL de la** lista desplegable del grupo de servidores, y marque a los **usuarios debe existir en la base de datos de la autorización para conectar la** casilla de verificación.En el Nombre de usuario que asocia el área, elija **SER (número de serie) de la** lista desplegable del campo del DN primario, no elija **ninguno del** campo del DN secundario, y haga clic la **AUTORIZACIÓN**.

Paso 7. Defina la directiva del grupo predeterminado

Este paso describe cómo definir la directiva del grupo predeterminado.

1. En el área del VPN de acceso remoto, amplíe el **acceso de la red (cliente)**, y elija las **directivas del grupo**.
2. Elija el **DfltGrpPolicy de la** lista de directivas del grupo, y el tecleo **edita**.
3. El cuadro de diálogo del Internal group policy (política grupal interna) del editar aparece.
4. Del área de la navegación, elija al **general**.

5. Para las agrupaciones de direcciones, haga clic **selecto** para elegir a una agrupación de direcciones, y elija el **EID-VPNPOOL**.
6. En la más área de las opciones, desmarque las casillas de verificación del **IPSec** y **L2TP/IPsec**, y haga clic la **AUTORIZACIÓN**.

Paso 8. Defina la asignación del certificado

Este paso describe cómo definir los criterios de la asignación del certificado.

1. En el área del VPN de acceso remoto, haga clic **avanzado**, y elija el **certificado a las correspondencias del perfil de la conexión VPN SSL**.
2. En el certificado al área de las correspondencias del perfil de la conexión, el tecleo **agrega**, y elige **DefaultCertificateMap de la** lista de la correspondencia.Esta correspondencia debe hacer juego *DefaultWEBVPNProfile* en asociado al campo del perfil de la conexión.
3. En la Criteria area (Zona de criterios) que asocia, el tecleo **agrega**, y agrega estos valores:Campo: El emisor, el país (c), los iguales, “sea”Campo: Emisor, Common Name (CN), iguales, “ciudadano Ca”Los criterios de la asignación deben aparecer tal y como se muestra en de esta imagen:
4. Haga clic en Apply (Aplicar).

Paso 9. Agregue a un usuario local

Este paso describe cómo agregar a un usuario local.

1. En el área del VPN de acceso remoto, amplíe la **configuración AAA**, y elija a los **usuarios locales**.
2. En el área de usuarios locales, haga click en Add
3. En el campo de nombre de usuario, ingrese el número de serie del Certificado de usuario. Por ejemplo, 56100307215 (según lo descrito en la sección del certificado de la autenticación de este documento).
4. Haga clic en Apply (Aplicar).

Paso 10. Reinicie el ASA

Reinicie el ASA para asegurarse de que todos los cambios están aplicados a los servicios del sistema.

Ajuste

Mientras que probaban, algunos túneles SSL no pudieron cerrarse correctamente. Puesto que el ASA asume que el cliente de AnyConnect puede desconectar y volver a conectar, el túnel no se cae, que le da una oportunidad de volverse. Sin embargo, durante los pruebas de laboratorio con una licencia baja (2 túneles SSL por abandono), usted puede ser que agote su licencia cuando los túneles SSL no se cierran correctamente. Si ocurre este problema, utilice el **<option > el** comando del **cierre de sesión de VPN-sessiondb** para terminar una sesión a todas las sesiones SSL activas.

Configuración del minuto

Para crear rápidamente una configuración en funcionamiento, reajuste su ASA al valor predeterminado de fábrica, y pegue esta configuración en el modo de configuración:

ciscoasa

```
ciscoasa#conf t
ciscoasa#clear configure all
ciscoasa#domain-name cisco.be
ciscoasa#enable password 9jNfZuG3TC5tCVH0 encrypted
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.0
interface Vlan2
 nameif outside
 security-level 0
 ip address 197.0.100.1 255.255.255.0
interface Ethernet0/0
 switchport access vlan 2
 no shutdown
interface Ethernet0/1
 no shutdown
!
passwd 2KFQnbNIdI.2KYOU encrypted
dns server-group DefaultDNS
 domain-name cisco.be
ip local pool eID-VPNPOOL 192.168.10.100-192.168.10.110
mask 255.255.255.0
asdm image disk0:/asdm-602.bin
no asdm history enable
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.255.0 inside
crypto ca trustpoint ASDM_TrustPoint0
 enrollment terminal
 crl configure
crypto ca certificate map DefaultCertificateMap 10
 issuer-name attr c eq be
 issuer-name attr cn eq citizen ca
crypto ca certificate chain ASDM_TrustPoint0
 certificate ca 580b056c5324dbb25057185ff9e5a650
    30820394 3082027c a0030201 02021058 0b056c53
24dbb250 57185ff9 e5a65030
    0d06092a 864886f7 0d010105 05003027 310b3009
06035504 06130242 45311830
    16060355 0403130f 42656c67 69756d20 526f6f74
20434130 1e170d30 33303132
    36323330 3030305a 170d3134 30313236 32333030
30305a30 27310b30 09060355
    04061302 42453118 30160603 55040313 0f42656c
6769756d 20526f6f 74204341
    30820122 300d0609 2a864886 f70d0101 01050003
82010f00 3082010a 02820101
    00c8a171 e91c4642 7978716f 9daea9a8 ab28b74d
c720eb30 915a75f5 e2d2cfc8
    4c149842 58adc711 c540406a 5af97412 2787e99c
```

```
e5714e22 2cd11218 aa305ea2
    21b9d9bb fff674eb 3101e73b 7e580f91 164d7689
a8014fad 226670fa 4b1d95c1
    3058eabc d965d89a b488eb49 4652dfd2 531576cb
145d1949 b16f6ad3 d3fdbcc2
    2dec453f 093f58be fcd4ef00 8c813572 bff718ea
96627d2b 287f156c 63d2caca
    7d05acc8 6d076d32 be68b805 40ae5498 563e66f1
30e8efc4 ab935e07 de328f12
    74aa5b34 2354c0ea 6ccefe36 92a80917 eaa12dcf
6ce3841d de872e33 0b3c74e2
    21503895 2e5ce0e5 c631f9db 40fa6aa1 a48a939b
a7210687 1d27d3c4 a1c94cb0
    6f020301 0001a381 bb3081b8 300e0603 551d0f01
01ff0404 03020106 300f0603
    551d1301 01ff0405 30030101 ff304206 03551d20
043b3039 30370605 60380101
    01302e30 2c06082b 06010505 07020116 20687474
703a2f2f 7265706f 7369746f
    72792e65 69642e62 656c6769 756d2e62 65301d06
03551d0e 04160414 10f00c56
    9b61ea57 3ab63597 6d9fddb9 148edbe6 30110609
60864801 86f84201 01040403
    02000730 1f060355 1d230418 30168014 10f00c56
9b61ea57 3ab63597 6d9fddb9
    148edbe6 300d0609 2a864886 f70d0101 05050003
82010100 c86d2251 8a61f80f
    966ed520 b281f8c6 dca31600 dacd6ae7 6b2afa59
48a74c49 37d773a1 6a01655e
    32bde797 d3d02e3c 73d38c7b 83efd642 c13fa8a9
5d0f37ba 76d240bd cc2d3fd3
    4441499c fd5b29f4 0223225b 711bbf58 d9284e2d
45f4dae7 b5634544 110d2a7f
    337f3649 b4ce6ea9 0231ae5c fdc889bf 427bd7f1
60f2d787 f6572e7a 7e6a1380
    1ddce3d0 631e3d71 31b160d4 9e08caab f094c748
755481f3 1bad779c e8b28fdb
    83ac8f34 6be8bfc3 d9f543c3 6455eb1a bd368636
ba218c97 1a21d4ea 2d3bacba
    eca71dab beb94a9b 352f1c5c 1d51a71f 54ed1297
fff26e87 7d46c974 d6efeb3d
    7de6596e 069404e4 a2558738 286a225e e2be7412
b004432a
  quit
no crypto isakmp nat-traversal
!
dhcpd address 192.168.0.2-192.168.0.129 inside
dhcpd enable inside
dhcpd address 197.0.100.20-197.0.100.30 outside
dhcpd enable outside
!
service-policy global_policy global
ssl encryption aes256-sha1 aes128-sha1 3des-sha1 rc4-
sha1
ssl certificate-authentication interface outside port
443
webvpn
 enable outside
 svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
 svc enable
certificate-group-map DefaultCertificateMap 10
DefaultWEBVPNGroup
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol svc webvpn
```

```
 address-pools value eID-VPNPOOL
username 63041403325 nopassword
tunnel-group DefaultWEBVPNGroup general-attributes
 authentication-server-group (outside) LOCAL
 authorization-server-group LOCAL
 authorization-required
 authorization-dn-attributes SER
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
exit
copy run start
```

Información Relacionada

- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems