ASA 8.x: Acceso VPN con el cliente VPN de AnyConnect que usa el ejemplo de configuración del certificado autofirmado

Contenido

Introducción

Este documento describe cómo utilizar los certificados autofirmados para permitir las conexiones VPN del Acceso Remoto SSL al ASA del cliente de Cisco AnyConnect 2.0.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Configuración básica ASA que funciona con la versión de software 8.0
- ASDM 6.0(2)

Componentes Utilizados

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

- Cisco ASA 8.0(2), ASDM 6.0 (2)
- Cisco AnyConnect 2.0

Convenciones

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

Antecedentes

El cliente de Cisco AnyConnect 2.0 es un cliente VPN basado en SSL. El cliente de AnyConnect puede ser utilizado y ser instalado en una variedad de sistemas operativos, tales como Windows 2000, XP, Vista, Linux (Distros múltiple) y MAC OS X. El cliente de AnyConnect puede ser instalado manualmente en la PC remota por el administrador de sistema. Puede también ser cargado sobre el dispositivo de seguridad y ser hecho listo para la descarga a los usuarios remotos. Después de que se descargue la aplicación, puede desinstalarse automáticamente después de que la conexión termine, o puede permanecer en la PC remota para las conexiones VPN futuras SSL. Este ejemplo hace al cliente de AnyConnect listo para descargar sobre la autenticación basada en buscador acertada SSL.

Para más información sobre el cliente de AnyConnect 2.0, refiera a AnyConnect 2.0 Release Note.

Nota: No soportan a los servicios de terminal MS conjuntamente con el cliente de AnyConnect. Usted no puede RDP a un ordenador y entonces iniciar una sesión de AnyConnect. Usted no puede RDP a un cliente que esté conectado vía AnyConnect.

Nota: La primera instalación de AnyConnect requiere al usuario tener derechos admin (si usted utiliza el paquete independiente del msi de AnyConnect o avanza el archivo de paquete del ASA). Si el usuario no tiene derechos admin, un cuadro de diálogo aparece que estado este requisito. Las actualizaciones subsiguientes no requerirán al usuario que instaló AnyConnect previamente para tener derechos admin.

Configurar

Para configurar el ASA para el acceso VPN usando el cliente de AnyConnect, complete estos pasos:

1. Configure un certificado Uno mismo-publicado.
2. Cargue e identifique la imagen del cliente VPN SSL.
3. Habilite el acceso de Anyconnect.
4. Cree una nueva directiva del grupo.
5. Configure puente de la lista de acceso para las conexiones VPN.
6. Cree un perfil de la conexión y a un grupo de túnel para las conexiones cliente de

AnyConnect.
7. Configure la exención de NAT para los clientes de AnyConnect.
8. Agregue a los usuarios a la base de datos local.

Paso 1. Configure un certificado Uno mismo-publicado

Por abandono, el dispositivo de seguridad tiene un certificado autofirmado se reinicie que se regenere cada vez el dispositivo. Usted puede comprar su propio certificado de los vendedores, tales como Verisign o EnTrust, o usted puede configurar el ASA para publicar un certificado de identidad a sí mismo. Este certificado sigue siendo lo mismo incluso cuando se reinicia el dispositivo. Complete este paso para generar un certificado uno mismo-publicado que persista cuando se reinicia el dispositivo.

Procedimiento del ASDM

1. **La configuración del** tecleo, y entonces hace clic el **VPN de acceso remoto**.
2. Amplíe la **administración de certificados**, y después elija los **certificados de identidad**.
3. El tecleo **agrega**, y después hace clic el **agregar un nuevo** botón de radio del **certificado de identidad**.
4. Haga clic en **New**.
5. En el cuadro de diálogo de los pares de agregar clave, haga clic el **nuevo** botón de radio del **nombre del par clave del ingresar**.
6. Ingrese un nombre para identificar el keypair.Este ejemplo utiliza el *sslvpnkeypair*.
7. El tecleo **ahora genera**.
8. En el cuadro de diálogo del certificado de identidad del agregar, asegúrese que el par clave creado recientemente esté seleccionado.
9. Para el tema DN del certificado, ingrese el Nombre de dominio totalmente calificado (FQDN) (FQDN) que será utilizado para conectar con el VPN que termina la interfaz.**CN=sslvpn.cisco.com**
10. Haga clic **avanzado**, y ingrese el FQDN usado para el campo del tema DN del certificado.Por ejemplo, **FQDN**: sslvpn.cisco.com
11. Haga clic en OK.
12. Marque la casilla de verificación del **certificado firmado del uno mismo de la generación**, y el tecleo **agrega el certificado**.
13. Haga clic en OK.
14. **La configuración del** tecleo, y entonces hace clic el **VPN de acceso remoto**.
15. Amplíe **avanzado**, y elija las **configuraciones SSL**.
16. En el área de los Certificados, elija la interfaz que será utilizada para terminar el SSL VPN (afuera), y el tecleo **edita**.
17. En la lista desplegable del certificado, elija el certificado autofirmado que usted generó anterior.
18. El Haga Click en OK, y entonces hace clic **se aplica**.

Ejemplo de la línea de comando

ciscoasa
ciscoasa(config)#**crypto key generate rsa label sslvpnkeypair** INFO: The name for the keys will be: sslvpnkeypair Keypair generation process begin. Please wait... *!--- Generate an RSA key for the certificate.*

```
(The name should be unique. !--- For example,
sslvpnkeypair.) ciscoasa(config)#crypto ca trustpoint
localtrust !--- Create a trustpoint for the self-issued
certificate. ciscoasa(config-ca-trustpoint)#enrollment
self ciscoasa(config-ca-trustpoint)#fqdn
sslvpn.cisco.com ciscoasa(config-ca-trustpoint)#subject-
name CN=sslvpn.cisco.com !--- The fully qualified domain
name is used for both fqdn and CN. !--- The name should
resolve to the ASA outside interface IP address.
ciscoasa(config-ca-trustpoint)#keypair sslvpnkeypair !--
- The RSA key is assigned to the trustpoint for
certificate creation. ciscoasa(config-ca-
trustpoint)#crypto ca enroll localtrust noconfirm % The
fully-qualified domain name in the certificate will be:
sslvpn.cisco.com ciscoasa(config)# ssl trust-point
localtrust outside !--- Assign the trustpoint to be used
for SSL connections on the outside interface.
```

Paso 2. Cargue e identifique la imagen del cliente VPN SSL

Este documento utiliza al cliente de AnyConnect SSL 2.0. Usted puede obtener a este cliente en el sitio web de la descarga de software de Cisco. Una imagen separada de Anyconnect se requiere para cada sistema operativo que los usuarios remotos planeen utilizar. Para más información, refiera a Cisco AnyConnect 2.0 Release Note.

Una vez que usted obtiene al cliente de AnyConnect, complete estos pasos:

Procedimiento del ASDM

1. **La configuración del** tecleo, y entonces hace clic el **VPN de acceso remoto**.
2. Amplíe el **acceso de la red (cliente)**, y después amplíe **avanzado**.
3. Amplíe **SSL VPN**, y elija las **configuraciones del cliente**.
4. En el área de las imágenes del cliente VPN SSL, el tecleo **agrega**, y después hace clic la **carga**.
5. Hojee a la ubicación en donde usted descargó al cliente de AnyConnect.
6. Seleccione el archivo, y haga clic el **archivo de la carga**.Una vez que las cargas del cliente, usted reciben un mensaje que estado el archivo fue cargado para contellear successully.
7. Haga clic en OK.Un cuadro de diálogo aparece confirmar que usted quiere utilizar la imagen nuevamente cargada como la imagen actual del cliente VPN SSL.
8. Haga clic en OK.
9. El Haga Click en OK, y entonces hace clic **se aplica**.
10. Relance los pasos en esta sección para cada paquete sistema-específico de Anyconnect del funcionamiento que usted quiera utilizar.

Ejemplo de la línea de comando

ciscoasa

```
ciscoasa(config)#copy tftp://192.168.50.5/anyconnect-
win-2.0.0343-k9.pkg flash Address or name of remote host
[192.168.50.5]? Source filename [anyconnect-win-
2.0.0343-k9.pkg]? Destination filename [anyconnect-win-
2.0.0343-k9.pkg]? Accessing
tftp://192.168.50.5/anyconnect-win-2.0.0343-
k9.pkg...!!!!!!!!!!!!! Writing file disk0:/anyconnect-
win-2.0.0343-k9.pkg...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!! 2635734 bytes copied in 4.480 secs
(658933 bytes/sec) !--- AnyConnect image is downloaded
to ASA via TFTP. ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#svc image disk0:/anyconnect-win-
2.0.0343-k9.pkg 1 !--- Specify the AnyConnect image to
be downloaded by users. The image that is !---
downloaded the most should have the lowest number. This
image uses 1 for the !--- AnyConnect Windows image.
```

Paso 3. Acceso de Anyconnect del permiso

Para permitir que el cliente de AnyConnect conecte con el ASA, usted debe habilitar el acceso en la interfaz que termina las conexiones VPN SSL. Este ejemplo utiliza la interfaz exterior para terminar las conexiones de Anyconnect.

Procedimiento del ASDM

1. **La configuración del** tecleo, y entonces hace clic el **VPN de acceso remoto**.
2. Amplíe el **acceso de la red (cliente)**, y después elija los **perfiles de la conexión VPN SSL**.
3. Marque la casilla de verificación del **Cliente Cisco AnyConnect VPN del permiso**.
4. Marque el cuadro de **verificación de acceso de la permit** para la interfaz exterior, y el tecleo **se aplica**.

Ejemplo de la línea de comando

ciscoasa

```
ciscoasa(config)#webvpn ciscoasa(config-webvpn)#enable
outside ciscoasa(config-webvpn)#svc enable !--- Enable
AnyConnect to be downloaded to remote computers.
```

Paso 4. Cree una nueva directiva del grupo

Una directiva del grupo especifica los parámetros de la configuración que se deben aplicar a los clientes cuando conectan. Este ejemplo crea una directiva del grupo nombrada *SSLClientPolicy*.

Procedimiento del ASDM

1. **La configuración del** tecleo, y entonces hace clic el **VPN de acceso remoto**.
2. Amplíe el **acceso de la red (cliente)**, y elija las **directivas del grupo**.
3. Haga clic en Add (Agregar).
4. Elija al **general**, y ingrese **SSLClientPolicy** en el campo de nombre.
5. Desmarque a las agrupaciones de direcciones **heredan la** casilla de verificación.
6. Haga clic **selecto**, y entonces el haga click en AddAparece el cuadro de diálogo Agregar Pool IP.
7. Configure a la agrupación de direcciones de un intervalo de direcciones IP que no sea actualmente funcionando en su red.Este ejemplo utiliza estos valores:Nombre: SSLClientPool**Comenzar la dirección IP**: 192.168.25.1**Terminación de la dirección IP**: 192.168.25.50**Máscara de subred**: 255.255.255.0
8. Haga clic en OK.
9. Elija el pool creado recientemente, y el tecleo **asigna**.
10. El Haga Click en OK, y entonces hace clic **más opciones**.
11. Desmarque los protocolos de túneles **heredan la** casilla de verificación.

12. Marque al **cliente VPN SSL**.
13. En el panel izquierdo, elija los **servidores**.
14. Desmarque a los servidores DNS **heredan la** casilla de verificación, y ingresan el IP Address del servidor DNS interno que los clientes de AnyConnect utilizarán.Este ejemplo utiliza *192.168.50.5*.
15. Haga clic **más opciones**.
16. Desmarque el Default Domain **heredan la** casilla de verificación.
17. Ingrese el dominio usado por su red interna. Por ejemplo, *tsweb.local.*
18. El Haga Click en OK, y entonces hace clic **se aplica**.

Ejemplo de la línea de comando

ciscoasa

```
ciscoasa(config)#ip local pool SSLClientPool
192.168.25.1-192.168.25.50 mask 255.255.255.0 !---
Define the IP pool. The IP pool should be a range of IP
addresses !--- not already in use on the internal
network. ciscoasa(config)#group-policy SSLCLientPolicy
internal ciscoasa(config)#group-policy SSLCLientPolicy
attributes ciscoasa(config-group-policy)#dns-server
value 192.168.50.5 !--- Specify the internal DNS server
to be used. ciscoasa(config-group-policy)#vpn-tunnel-
protocol svc !--- Specify VPN tunnel protocol to be used
by the Group Policy. ciscoasa(config-group-
policy)#default-domain value tsweb.local !--- Define the
default domain assigned to VPN users. ciscoasa(config-
group-policy)#address-pools value SSLClientPool !---
Assign the IP pool created to the SSLClientPolicy group
policy.
```

Puente de la lista de acceso de la configuración para las conexiones VPN

Cuando usted habilita esta opción, usted permite que los clientes SSL/IPsec desvíen la lista de acceso de la interfaz.

Procedimiento del ASDM

1. **La configuración del** tecleo, y entonces hace clic el **VPN de acceso remoto**.
2. Amplíe el **acceso de la red (cliente)**, y después amplíe **avanzado**.
3. Amplíe **SSL VPN**, y elija la **lista de acceso de la interfaz de puente**.
4. Asegúrese que el **permiso las sesiones entrantes SSL VPN y del IPSEC para desviar la** casilla de verificación de las **Listas de acceso de la interfaz** esté marcado, y el tecleo **se aplica**.

Ejemplo de la línea de comando

ciscoasa

```
ciscoasa(config)#sysopt connection permit-vpn !---
Enable interface access-list bypass for VPN connections.
!--- This example uses the vpn-filter command for access
control. ciscoasa(config-group-policy)#
```

Paso 6. Cree un perfil de la conexión y a un grupo de túnel para las conexiones cliente de AnyConnect

Cuando los clientes VPN conectan con el ASA, conectan con un perfil de la conexión o un grupo de túnel. Utilizan al grupo de túnel para definir los parámetros de la conexión para los tipos de conexiones VPN específicos, tales como Acceso Remoto del IPSec L2L, del IPSec, clientless SSL, y cliente SSL.

Procedimiento del ASDM

1. **La configuración del** tecleo, y entonces hace clic el **VPN de acceso remoto**.
2. Amplíe el **acceso de la red (cliente)**, y después amplíe **SSL VPN**.
3. Elija los **perfiles de la conexión**, y el haga click en Add
4. Elija **básico**, y ingrese estos valores:Nombre: SSLClientProfileAutenticación: LOCAL**Directiva del grupo predeterminado**: SSLClientPolicy
5. Asegúrese que la casilla de verificación del **protocolo del cliente VPN SSL** esté marcada.
6. En el panel izquierdo, amplíe **avanzado**, y elija **SSL VPN**.
7. Bajo alias de la conexión, el tecleo **agrega**, y ingresa un nombre al cual los usuarios puedan asociar sus conexiones VPN. Por ejemplo, *SSLVPNClient*.
8. El Haga Click en OK, y entonces hace clic la **AUTORIZACIÓN** otra vez.
9. En la parte inferior de la ventana del ASDM, marque al **usuario de la permit para seleccionar la conexión, identificada por el alias en la tabla arriba en la** casilla de verificación de la **página de registro**, y el tecleo **se aplica**.

Ejemplo de la línea de comando

ciscoasa

```
ciscoasa(config)#tunnel-group SSLClientProfile type
remote-access !--- Define tunnel group to be used for
VPN remote access connections. ciscoasa(config)#tunnel-
group SSLClientProfile general-attributes
ciscoasa(config-tunnel-general)#default-group-policy
SSLCLientPolicy ciscoasa(config-tunnel-general)#tunnel-
group SSLClientProfile webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias SSLVPNClient
enable !--- Assign alias for tunnel group.
ciscoasa(config-tunnel-webvpn)#webvpn ciscoasa(config-
webvpn)#tunnel-group-list enable !--- Enable
alias/tunnel group selection for SSL VPN connections.
```

Paso 7. Exención de NAT de la configuración para los clientes de AnyConnect

La exención de NAT se debe configurar para cualquier IP Addresses o se extiende usted quiere permitir que los clientes VPN SSL accedan. En este ejemplo, los clientes VPN SSL necesitan el acceso al IP interno 192.168.50.5 solamente.

Nota: Si el NAT control no se habilita, este paso no se requiere. Utilice el **comando nat-control del funcionamiento de la demostración** de verificar. Para verificar con el ASDM, haga clic la **configuración**, haga clic el **Firewall**, y elija las **reglas nacionales**. Si el **tráfico del permiso con el Firewall sin la** casilla de verificación de la **traducción de la dirección** se marca, usted puede saltar este paso.

Procedimiento del ASDM

1. **La configuración del** tecleo, y entonces hace clic el **Firewall**.
2. Elija las **reglas nacionales**, y el haga click en Add

3. Elija **agregan la regla exenta NAT**, y ingresan estos valores:Acción: ExentoInterfaz: dentroFuente: 192.168.50.5Destino: 192.168.25.0/24**Dirección exenta NAT**: Tráfico saliente exento NAT de la interfaz “interior” a las interfaces de menor seguridad (valor por defecto)
4. El Haga Click en OK, y entonces hace clic **se aplica**.

Ejemplo de la línea de comando

ciscoasa

```
ciscoasa(config)#access-list no_nat extended permit ip
host 192.168.50.5 192.168.25.0 255.255.255.0 !--- Define
access list to be used for NAT exemption.
ciscoasa(config)#nat (inside) 0 access-list no_nat !---
Allow external connections to untranslated internal !---
addresses defined by access lisy no_nat.
ciscoasa(config)#
```

Paso 8. Agregue a los usuarios a la base de datos local

Si usted utiliza la autenticación local (el valor por defecto), usted debe definir los Nombres de usuario y las contraseñas en la base de datos local para la autenticación de usuario.

Procedimiento del ASDM

1. **La configuración del** tecleo, y entonces hace clic el **VPN de acceso remoto**.
2. Amplíe la **configuración AAA**, y elija a los **usuarios locales**.
3. El tecleo **agrega**, y ingresa estos valores:Nombre de usuario: matthewpContraseña p@ssw0rd**Confirme la contraseña**: p@ssw0rd
4. No seleccione el **ningún** botón de radio del **ASDM, de SSH, de Telnet o del acceso a la consola**.
5. El Haga Click en OK, y entonces hace clic **se aplica**.
6. Relance este paso para los usuarios adicionales, y después haga clic la **salvaguardia**.

Ejemplo de la línea de comando

ciscoasa

```
ciscoasa(config)#username matthewp password p@ssw0rd
ciscoasa(config)#username matthewp attributes
ciscoasa(config-username)#service-type remote-access !--
- Assign user remote access only. No SSH, Telnet, ASDM
access allowed. ciscoasa(config-username)#write memory
!--- Save the configuration.
```

Verificación

Utilice esta sección para verificar que la configuración VPN SSL es acertada

Conecte con el ASA con el cliente de AnyConnect

Instale al cliente directamente en un PC, y conecte con la interfaz exterior ASA, o ingrese el https y el IP Address FQDN del ASA en un buscador Web. Si usted utiliza a un buscador Web, el cliente se instala sobre la registración satisfactoria.

Verifique las conexiones de cliente VPN SSL

Utilice el **comando svc de VPN-sessiondb de la demostración** para verificar a los clientes VPN conectados SSL.

```
ciscoasa(config-group-policy)#show vpn-sessiondb svc Session Type: SVC Username : matthewp Index
: 6 Assigned IP : 192.168.25.1 Public IP : 172.18.12.111 Protocol : Clientless SSL-Tunnel DTLS-
Tunnel Encryption : RC4 AES128 Hashing : SHA1 Bytes Tx : 35466 Bytes Rx : 27543 Group Policy :
SSLClientPolicy Tunnel Group : SSLClientProfile Login Time : 20:06:59 UTC Tue Oct 16 2007
Duration : 0h:00m:12s NAC Result : Unknown VLAN Mapping : N/A VLAN : none ciscoasa(config-group-
policy)#
```

El comando username del **nombre del cierre de sesión de VPN-sessiondb** termina una sesión a los usuarios por el Nombre de usuario. Un mensaje de la *restauración del administrador* se envía al usuario cuando está desconectado.

```
ciscoasa(config)#vpn-sessiondb logoff name matthewp Do you want to logoff the VPN session(s)?
[confirm] INFO: Number of sessions with name "matthewp" logged off : 1 ciscoasa(config)#
```

Para más información sobre el cliente de AnyConnect 2.0, refiera al guía del administrador de Cisco AnyConnect VPN.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas (opcional)

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **haga el debug del webvpn svc 255** — Mensajes del debug de las visualizaciones sobre las conexiones a los clientes VPN SSL sobre el WebVPN.**Login acertado de AnyConnect**

```
ciscoasa(config)#debug webvpn svc 255 INFO: debug webvpn svc enabled at level
255. ciscoasa(config)#ATTR_FILTER_ID: Name: SSLVPNClientAccess , Id: 1, refcnt: 1
webvpn_rx_data_tunnel_connect CSTP state = HEADER_PROCESSING http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1' webvpn_cstp_parse_request_field() ...input:
'Host: 10.10.1.5' - !--- Outside IP of ASA Processing CSTP header line: 'Host: 10.10.1.5'
webvpn_cstp_parse_request_field() ...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0,
0343' - !--- AnyConnect Version Processing CSTP header line: 'User-Agent: Cisco AnyConnect
VPN Client 2, 0, 0343' Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343'
webvpn_cstp_parse_request_field() ...input: 'Cookie:
webvpn=3338474156@28672@1192565782@EFB9042D72C 63CE02164F790435897AC72EE70AE' Processing
CSTP header line: 'Cookie: webvpn=3338474156@28672@119
2565782@EFB9042D72C63CE02164F790435897AC72EE70AE' Found WebVPN cookie:
'webvpn=3338474156@28672@1192565782@EFB9042D72C 63CE02164F790435897AC72EE70AE' WebVPN
Cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C63CE02 164F790435897AC72EE70AE'
IPADDR: '3338474156', INDEX: '28672', LOGIN: '1192565782' webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1' Processing CSTP header line: 'X-CSTP-Version: 1' Setting
version to '1' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Hostname: wkstation1' -
!--- Client desktop hostname Processing CSTP header line: 'X-CSTP-Hostname: wkstation1'
Setting hostname to: 'wkstation1' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-
Accept-Encoding: deflate;q=1.0' Processing CSTP header line: 'X-CSTP-Accept-Encoding:
deflate;q=1.0' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-MTU: 1206' Processing
CSTP header line: 'X-CSTP-MTU: 1206' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-
Address-Type: IPv4' Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
```

```
webvpn_cstp_parse_request_field() ...input: 'X-DTLS-Master-Secret:
72B8AD72F327059AE22CBB451CB0948AFBE98296FD849
49EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51' Processing CSTP header line: 'X-DTLS-
Master-Secret: 72B8AD72F327059AE22CBB451C
B0948AFBE98296FD84949EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51'
webvpn_cstp_parse_request_field() ...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-
CBC3-SHA:DES-CBC-SHA' Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-
SHA: DES-CBC3-SHA:DES-CBC-SHA' Validating address: 0.0.0.0 CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.25.1/255.255.255.0 - !--- IP assigned from IP Pool CSTP
state = HAVE_ADDRESS SVC: NP setup np_svc_create_session(0x7000, 0xD41612C8, TRUE)
webvpn_svc_np_setup SVC ACL Name: NULL SVC ACL ID: -1 SVC ACL ID: -1 vpn_put_uauth success!
SVC IPv6 ACL Name: NULL SVC IPv6 ACL ID: -1 SVC: adding to sessmgmt SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy CSTP state = CONNECTED
webvpn_rx_data_cstp webvpn_rx_data_cstp: got internal message Unable to initiate NAC, NAC
might not be enabled or invalid policy
```

Login fracasado de AnyConnect (contraseña incorrecta)

```
webvpn_portal.c:ewaFormSubmit_webvpn_login[1808]
ewaFormSubmit_webvpn_login: tgCookie = 0
ewaFormSubmit_webvpn_login: cookie = d53d2990
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
webvpn_portal.c:http_webvpn_kill_cookie[627]
webvpn_auth.c:http_webvpn_pre_authentication[1905]
WebVPN: calling AAA with ewsContext (-717386088) and nh (-717388536)!
WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[4380]
WebVPN: AAA status = (REJECT) webvpn_portal.c:ewaFormSubmit_webvpn_login[1808]
ewaFormSubmit_webvpn_login: tgCookie = 0 ewaFormSubmit_webvpn_login: cookie = d53d2990
ewaFormSubmit_webvpn_login: tgCookieSet = 0 ewaFormSubmit_webvpn_login: tgroup = NULL
webvpn_auth.c:http_webvpn_post_authentication[1180] WebVPN: user: (matthewp) rejected.
http_remove_auth_handle(): handle 9 not found!
webvpn_portal.c:ewaFormServe_webvpn_login[1749] webvpn_portal.c:http_webvpn_kill_cookie[627]
```

Información Relacionada

- Guía del administrador del Cliente Cisco AnyConnect VPN, versión 2.0
- Notas de Versión para AnyConnect VPN Client, Release 2.0
- Soporte Técnico y Documentación - Cisco Systems