ASA 8.x: Ejemplo de Configuración de Acceso VPN con AnyConnect VPN Client Usando Certificado Autofirmado

Contenido

Introducción

Este documento describe cómo utilizar certificados autofirmados para permitir conexiones SSL VPN de acceso remoto al ASA desde el cliente Cisco AnyConnect 2.0.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Configuración básica de ASA que ejecuta 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 Cisco AnyConnect 2.0 es un cliente VPN basado en SSL. El cliente AnyConnect se puede utilizar e instalar en diversos sistemas operativos, como Windows 2000, XP, Vista, Linux (varias distribuciones) y MAC OS X. El administrador del sistema puede instalar el cliente AnyConnect manualmente en el equipo remoto. También puede cargarse en el dispositivo de seguridad y prepararse para su descarga a usuarios remotos. Después de descargar la aplicación, puede desinstalarse automáticamente después de que la conexión termine o puede permanecer en el equipo remoto para futuras conexiones SSL VPN. Este ejemplo hace que el cliente AnyConnect esté listo para descargar tras una autenticación SSL correcta basada en navegador.

Para obtener más información sobre el cliente AnyConnect 2.0, refiérase a Notas de la Versión de AnyConnect 2.0.

Nota: MS Terminal Services no se admite junto con el cliente AnyConnect. No puede RDP a un equipo y luego iniciar una sesión de AnyConnect. No puede RDP a un cliente que está conectado a través de AnyConnect.

Nota: La primera instalación de AnyConnect requiere que el usuario tenga derechos de administrador (ya sea que utilice el paquete msi AnyConnect independiente o presione el archivo pkg del ASA). Si el usuario no tiene derechos de administrador, aparece un cuadro de diálogo que indica este requisito. Las actualizaciones posteriores no requerirán que el usuario que instaló AnyConnect previamente tenga derechos de administrador.

Configurar

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

1. Configure un Certificado Autoemitido.
2. Cargue e Identifique la Imagen de SSL VPN Client.
3. Habilite Anyconnect Access.
4. Cree una nueva política de grupo.
5. Configure el Omitir de la Lista de Acceso para las Conexiones VPN.
6. Cree un perfil de conexión y un grupo de túnel para las conexiones del cliente AnyConnect.

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

Paso 1. Configurar un certificado autoemitido

De forma predeterminada, el dispositivo de seguridad tiene un certificado autofirmado que se regenera cada vez que se reinicia el dispositivo. Puede comprar su propio certificado a proveedores, como Verisign o EnTrust, o puede configurar el ASA para que se emita un certificado de identidad. Este certificado permanece igual incluso cuando se reinicia el dispositivo. Complete este paso para generar un certificado autoemitido que persiste cuando se reinicia el dispositivo.

Procedimiento ASDM

1. Haga clic en **Configuration** y luego en **Remote Access VPN**.
2. Expanda **Administración de certificados** y luego elija **Certificados de identidad**.
3. Haga clic en **Agregar** y, a continuación, haga clic en el botón de opción **Agregar un nuevo certificado de identidad**.
4. Haga clic en **New**.
5. En el cuadro de diálogo Agregar par de claves, haga clic en el botón de opción **Introducir nuevo nombre de par de claves**.
6. Introduzca un nombre para identificar el par de claves.Este ejemplo utiliza *sslvpnkeypair*.
7. Haga clic en **Generar ahora**.
8. En el cuadro de diálogo Agregar certificado de identidad, asegúrese de que esté seleccionado el par de claves recién creado.
9. Para el DN de asunto del certificado, introduzca el nombre de dominio completo (FQDN) que se utilizará para conectarse a la interfaz de terminación de VPN.**CN=sslvpn.cisco.com**
10. Haga clic en **Avanzado** e introduzca el FQDN utilizado para el campo DN del asunto del certificado.Por ejemplo, **FQDN**: sslvpn.cisco.com
11. Click OK.
12. Marque la casilla de verificación **Generar certificado firmado automáticamente** y haga clic en **Agregar certificado**.
13. Click OK.
14. Haga clic en **Configuration** y luego en **Remote Access VPN**.
15. Expanda **Advanced** y elija **SSL Settings**.
16. En el área Certificates, elija la interfaz que se utilizará para terminar SSL VPN (outside) y haga clic en **Edit**.
17. En la lista desplegable Certificado, elija el certificado autofirmado que generó anteriormente.
18. Haga clic en **Aceptar** y luego en **Aplicar**.

Ejemplo de línea de comandos

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. Cargar e identificar la imagen de SSL VPN Client

Este documento utiliza el cliente AnyConnect SSL 2.0. Puede obtener este cliente en el sitio web de descarga de software de Cisco. Se requiere una imagen de Anyconnect independiente para cada sistema operativo que los usuarios remotos planean utilizar. Para obtener más información, consulte Notas de la versión de Cisco AnyConnect 2.0.

Una vez que obtenga el cliente AnyConnect, complete estos pasos:

Procedimiento ASDM

1. Haga clic en **Configuration** y luego en **Remote Access VPN**.
2. Amplíe **Acceso a la red (Cliente)** y luego **Avanzado**.
3. Expanda **SSL VPN** y elija **Client Settings**.
4. En el área SSL VPN Client Images, haga clic en **Add** y luego haga clic en **Upload**.
5. Busque la ubicación en la que descargó el cliente AnyConnect.
6. Seleccione el archivo y haga clic en **Cargar archivo**.Una vez que el cliente carga, recibe un mensaje que indica que el archivo se cargó en flash correctamente.
7. Click OK.Aparece un cuadro de diálogo para confirmar que desea utilizar la imagen recién cargada como la imagen de cliente SSL VPN actual.
8. Click OK.
9. Haga clic en **Aceptar** y luego en **Aplicar**.
10. Repita los pasos de esta sección para cada paquete Anyconnect específico del sistema operativo que desee utilizar.

Ejemplo de línea de comandos

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. Activar acceso a Anyconnect

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

Procedimiento ASDM

1. Haga clic en **Configuration** y luego en **Remote Access VPN**.
2. Expanda **Acceso a Red (Cliente)** y luego elija **Perfiles de Conexión VPN SSL**.
3. Marque la casilla de verificación **Enable Cisco AnyConnect VPN Client**.
4. Marque la casilla de verificación **Permitir acceso** para la interfaz exterior y haga clic en **Aplicar**.

Ejemplo de línea de comandos

ciscoasa

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

Paso 4. Crear una nueva política de grupo

Una política de grupo especifica los parámetros de configuración que se deben aplicar a los clientes cuando se conectan. Este ejemplo crea una política de grupo denominada *SSLClientPolicy*.

Procedimiento ASDM

1. Haga clic en **Configuration** y luego en **Remote Access VPN**.
2. Amplíe **Acceso de Red (Cliente)** y elija **Políticas de Grupo**.
3. Haga clic en Add (Agregar).
4. Elija **General** e ingrese **SSLClientPolicy** en el campo Nombre.
5. Desactive la casilla de verificación Conjuntos de direcciones **Heredar**.
6. Haga clic en **Seleccionar** y luego en **Agregar**.Aparece el cuadro de diálogo Agregar Pool IP.

7. Configure el conjunto de direcciones desde un rango de IP que no esté actualmente en uso en su red.Este ejemplo utiliza estos valores:**Nombre:** SSLClientPool**Dirección IP inicial**: 192.168.25.1**Dirección IP final**: 192.168.25.50**Máscara de subnet:** 255.255.255.0
8. Click OK.
9. Elija el grupo recién creado y haga clic en **Asignar**.
10. Haga clic en **Aceptar** y luego en **Más opciones**.
11. Desmarque la casilla de verificación Tunneling Protocols **Inherit**.
12. Verifique **SSL VPN Client**.
13. En el panel izquierdo, elija **Servidores**.
14. Desmarque la casilla de verificación **Heredar** servidores DNS e introduzca la dirección IP del servidor DNS interno que utilizarán los clientes de AnyConnect.Este ejemplo utiliza *192.168.50.5*.
15. Haga clic en **Más opciones**.
16. Desactive la casilla de verificación Default Domain **Inherit**.
17. Introduzca el dominio utilizado por la red interna. Por ejemplo, *tsweb.local* .
18. Haga clic en **Aceptar** y luego en **Aplicar**.

Ejemplo de línea de comandos

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.
```

Configuración del desvío de la lista de acceso para conexiones VPN

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

Procedimiento ASDM

1. Haga clic en **Configuration** y luego en **Remote Access VPN**.
2. Amplíe **Acceso a la red (Cliente)** y luego **Avanzado**.
3. Expanda **SSL VPN** y elija **Bypass Interface Access List**.
4. Asegúrese de que la casilla de verificación **Enable SSL VPN and IPSEC Sessions to bypass interface access lists** esté marcada y haga clic en **Apply**.

Ejemplo de línea de comandos

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 conexión y un grupo de túnel para las conexiones del cliente AnyConnect

Cuando los clientes VPN se conectan al ASA, se conectan a un perfil de conexión o grupo de túnel. El grupo de túnel se utiliza para definir parámetros de conexión para tipos específicos de conexiones VPN, como IPsec L2L, IPsec remote access, Cliless SSL y Client SSL.

Procedimiento ASDM

1. Haga clic en **Configuration** y luego en **Remote Access VPN**.
2. Expanda **Network (Client) Access** y luego **SSL VPN**.
3. Elija **Perfiles de Conexión** y haga clic en **Agregar**.
4. Elija **Basic**, e ingrese estos valores:**Nombre:** SSLClientProfile**Autenticación:** LOCAL**Política de grupo predeterminada**: SSLClientPolicy
5. Asegúrese de que la casilla de verificación **SSL VPN Client Protocol** esté marcada.
6. En el panel izquierdo, expanda **Advanced** y elija **SSL VPN**.
7. En Connection Aliases (Alias de conexión), haga clic en **Add** (Agregar) e introduzca un nombre al que los usuarios puedan asociar sus conexiones VPN. Por ejemplo, *SSLVPNClient*.
8. Haga clic en **Aceptar** y, a continuación, en **Aceptar** de nuevo.
9. En la parte inferior de la ventana de ASDM, marque la casilla de verificación **Permitir que el usuario seleccione la conexión, identificada por el alias en la tabla anterior en la página de inicio de sesión**, y haga clic en **Aplicar**.

Ejemplo de línea de comandos

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. Configuración de la exención de NAT para clientes AnyConnect

La exención de NAT debe configurarse para cualquier dirección IP o rango al que desee permitir el acceso de los clientes SSL VPN. En este ejemplo, los clientes VPN SSL necesitan acceso a la IP interna 192.168.50.5 solamente.

Nota: Si el control NAT no está habilitado, este paso no es necesario. Utilice el comando **show run nat-control** para verificar. Para verificar a través de ASDM, haga clic en **Configuration**, haga clic en **Firewall** y elija **Nat Rules**. Si la casilla de verificación **Habilitar tráfico a través del firewall sin traducción de dirección** está marcada, puede saltarse este paso.

Procedimiento ASDM

1. Haga clic en **Configuration** y luego en **Firewall**.
2. Elija **Nat Rules**, y haga clic en **Add**.
3. Elija **Add NAT Exempt Rule**, e ingrese estos valores:**Acción:** Exención**Interfaz:** dentro**Fuente:** 192.168.50.5**Destino:** 192.168.25.0/24**Dirección de exención de NAT**: NAT Exime el tráfico saliente de la interfaz 'interior' a interfaces de menor seguridad (Predeterminado)
4. Haga clic en **Aceptar** y luego en **Aplicar**.

Ejemplo de línea de comandos

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. Agregar usuarios a la base de datos local

Si utiliza la autenticación local (el valor predeterminado), debe definir nombres de usuario y contraseñas en la base de datos local para la autenticación de usuario.

Procedimiento ASDM

1. Haga clic en **Configuration** y luego en **Remote Access VPN**.
2. Expanda **AAA Setup** y elija **Local Users**.
3. Haga clic en **Agregar** e ingrese estos valores:**Nombre de usuario:** matthewp**Contraseña** p@ssw0rd**Confirmar contraseña**: p@ssw0rd
4. Seleccione el botón de opción **No ASDM, SSH, Telnet o Acceso a la consola**.
5. Haga clic en **Aceptar** y luego en **Aplicar**.
6. Repita este paso para usuarios adicionales y, a continuación, haga clic en **Guardar**.

Ejemplo de línea de comandos

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 de SSL VPN es correcta

Conéctese al ASA con AnyConnect Client

Instale el cliente directamente en un PC y conéctese a la interfaz exterior de ASA, o introduzca https y la dirección FQDN/IP del ASA en un navegador web. Si utiliza un navegador web, el cliente se instala cuando se inicia sesión correctamente.

Verificar las Conexiones de SSL VPN Client

Utilice el comando **show vpn-sessiondb svc** para verificar los clientes SSL VPN conectados.

```
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 **vpn-sessiondb logoff name *username*** desconecta a los usuarios por nombre de usuario. Se envía al usuario un mensaje *Administrator Reset* cuando se desconecta.

```
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 obtener más información sobre el cliente AnyConnect 2.0, refiérase a la Guía del Administrador de Cisco AnyConnect VPN.

Troubleshoot

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 Debug antes de utilizar los comandos **debug**.

- **debug webvpn svc 255** —Muestra mensajes de depuración sobre conexiones a clientes SSL VPN a través de WebVPN.**Inicio de sesión de AnyConnect correcto**

```
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
```

Inicio de sesión de AnyConnect incorrecto (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 de Cisco AnyConnect VPN Client, versión 2.0
- Notas de Versión para AnyConnect VPN Client, Release 2.0
- Soporte Técnico y Documentación - Cisco Systems