ASA 8.x: VPN-toegang met de AnyConnect VPN-client met zelfgetekende configuratievoorbeeld van certificaat

Inhoud

Inleiding

Dit document beschrijft hoe u zelfgetekende certificaten kunt gebruiken om externe toegang tot SSL VPN-verbindingen naar de ASA te maken via de Cisco AnyConnect 2.0-client.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Basic ASA-configuratie die softwareversie 8.0 uitvoert
- ASDM 6.0(2)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

De Cisco AnyConnect 2.0-client is een SSL-gebaseerde VPN-client. De AnyConnect-client kan worden gebruikt en geïnstalleerd op verschillende besturingssystemen, zoals Windows 2000, XP, Vista, Linux (Multiple Distros) en MAC OS X. De AnyConnect-client kan door de systeembeheerder handmatig op de externe pc worden geïnstalleerd. Het kan ook op het security apparaat worden geladen en makkelijk te downloaden zijn, op externe gebruikers. Nadat de toepassing is gedownload, kan deze zichzelf automatisch verwijderen nadat de verbinding is beëindigd, of kan deze op de externe PC blijven voor toekomstige SSL VPN-verbindingen. Dit voorbeeld maakt de AnyConnect-client klaar om te downloaden bij succesvolle op browser gebaseerde SSL-verificatie.

Raadpleeg de AnyConnect 2.0-opmerkingen voor meer informatie over de AnyConnect 2.0-client.

Opmerking: MS Terminal Services wordt niet ondersteund in combinatie met de AnyConnect-client. U kunt geen RDP op een computer uitvoeren en vervolgens een AnyConnect-sessie starten. U kunt geen RDP uitvoeren op een client die is aangesloten via AnyConnect.

Opmerking: Voor de eerste installatie van AnyConnect moet de gebruiker beheerrechten hebben (of u het standalone AnyConnect-msi-pakket gebruikt of het kg-bestand van de ASA indrukt). Als de gebruiker geen beheerrechten heeft, verschijnt er een dialoogvenster waarin dit vereiste staat. Voor volgende upgrades hoeft de gebruiker die AnyConnect heeft geïnstalleerd geen beheerrechten te hebben.

Configureren

Voltooi de volgende stappen om de ASA for VPN-toegang te configureren met behulp van de AnyConnect-client:

1. Configureer een certificaat dat zelf is afgegeven.
2. Upload en identificeer de SSL VPN-clientafbeelding.
3. Toegang voor iedereen inschakelen.
4. Een nieuw groepsbeleid maken.
5. Configuratie van de Bypass van de Toegangslijst voor VPN-verbindingen.
6. Maak een verbindingsprofiel en een tunnelgroep voor de AnyConnect-clientverbindingen.
7. Configureer de NAT-vrijstelling voor AnyConnect-clients.
8. Voeg gebruikers aan de lokale databank toe.

Stap 1. Een door henzelf afgegeven certificaat configureren

Het beveiligingsapparaat heeft standaard een zichzelf ondertekend certificaat dat opnieuw wordt gegenereerd elke keer dat het apparaat wordt herstart. U kunt uw eigen certificaat van verkopers kopen, zoals Versiering of EnTrust, of u kunt de ASA configureren om een identiteitsbewijs aan zichzelf te verstrekken. Dit certificaat blijft hetzelfde, ook wanneer het apparaat wordt herstart. Voltooi deze stap om een zelf-afgegeven certificaat te genereren dat blijft bestaan wanneer het apparaat wordt herstart.

ASDM-procedure

1. Klik op **Configuration** en klik vervolgens op **Remote Access VPN**.
2. vouwt **certificaatbeheer uit** en kies vervolgens **identiteitsbewijzen**.
3. Klik op **Add** en vervolgens op de knop **Add a new Identity Certificate** radioknop.
4. Klik op **Nieuw**.
5. Klik in het dialoogvenster Toetsenpaneel toevoegen op de radioknop **Voer** de **naam van het nieuwe sleutelpaar in**.
6. Voer een naam in om het sleutelpaar te identificeren.Dit voorbeeld gebruikt *sslvpkeypair*.
7. Klik op **Generate Now**.
8. Zorg ervoor dat in het dialoogvenster Identiteitscertificaat toevoegen de nieuw gemaakte sleutel is geselecteerd.
9. Voor certificaatonderwerp DN voert u de volledig gekwalificeerde domeinnaam (FQDN) in die wordt gebruikt om met de VPN-terminatie-interface te verbinden.**CN=sslvpn.cisco.com**
10. Klik op **Geavanceerd** en voer de FQDN in die voor het veld certificaatonderwerp van het certificaat wordt gebruikt.Bijvoorbeeld, **FQDN**: sslvpn.cisco.com
11. Klik op **OK**.
12. Controleer het dialoogvenster **Zelfgetekend certificaat genereren** en klik op **Certificaat toevoegen**.
13. Klik op **OK**.
14. Klik op **Configuration** en klik vervolgens op **Remote Access VPN**.
15. Vouw **Geavanceerd uit** en kies **SSL Instellingen**.
16. Kies in het gebied Certificaten de interface die wordt gebruikt om SSL VPN (buiten) te beëindigen en klik op **Bewerken**.
17. Selecteer in de vervolgkeuzelijst Certificaat het zelfgetekende certificaat dat u eerder hebt gegenereerd.
18. Klik op **OK** en vervolgens op **Toepassen**.

Opdrachtlijnvoorbeeld

ciscoa

```
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.
```

Stap 2. Upload en identificeer de SSL VPN-clientafbeelding.

Dit document gebruikt de AnyConnect SSL 2.0-client. U kunt deze client verkrijgen op de Cisco Software Download website. Er is een afzonderlijk AnyConnect-beeld vereist voor elk besturingssysteem dat externe gebruikers willen gebruiken. Raadpleeg voor meer informatie de opmerkingen van Cisco AnyConnect 2.0 release.

Voltooi de volgende stappen zodra u de AnyConnect-client hebt aangeschaft:

ASDM-procedure

1. Klik op **Configuration** en klik vervolgens op **Remote Access VPN**.
2. **Network (Client) Access** uitbreiden en vervolgens **Advanced** uitbreiden.
3. Vergroot **SSL VPN** en kies **Clientinstellingen**.
4. Klik in het gebied SSL VPN-clientafbeeldingen op **Add** en klik vervolgens op **Upload**.
5. Bladeren naar de locatie waar u de AnyConnect-client hebt gedownload.
6. Selecteer het bestand en klik op **Upload File**.Zodra de client is geüpload ontvangt u een bericht waarin staat dat het bestand met succes is geüpload naar flitser.
7. Klik op **OK**.Een dialoogvenster verschijnt om te bevestigen dat u de nieuwe geüploade afbeelding wilt gebruiken als de huidige SSL VPN-clientafbeelding.
8. Klik op **OK**.
9. Klik op **OK** en vervolgens op **Toepassen**.
10. Herhaal de stappen in deze sectie voor elk besturingssysteem-specifiek AnyConnect-pakket dat u wilt gebruiken.

Opdrachtlijnvoorbeeld

ciscoa

```
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.
```

Stap 3. Schakel toegang voor iedereen in

Om de AnyConnect-client in staat te stellen verbinding te maken met de ASA, moet u toegang mogelijk maken op de interface die SSL VPN-verbindingen beëindigt. Dit voorbeeld gebruikt de externe interface om AnyConnect-verbindingen te beëindigen.

ASDM-procedure

1. Klik op **Configuration** en klik vervolgens op **Remote Access VPN**.
2. Uitbreidt **Network (Client) Access** en kies vervolgens **SSL VPN-verbindingsprofielen**.
3. Controleer het vakje **Cisco AnyConnect VPN-client** inschakelen.
4. Controleer het aanvinkvakje **Toegang toestaan** voor de externe interface en klik op **Toepassen**.

Opdrachtlijnvoorbeeld

ciscoa

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

Stap 4. Maak een nieuw groepsbeleid

Een groepsbeleid specificeert de configuratieparameters die op klanten moeten worden toegepast wanneer ze verbinding maken. Dit voorbeeld creëert een groepsbeleid genaamd *SSLClientPolicy*.

ASDM-procedure

1. Klik op **Configuration** en klik vervolgens op **Remote Access VPN**.
2. Uitbreidt **de Toegang tot netwerk (client)** en kiest **groepsbeleid**.
3. Klik op **Toevoegen**.
4. Kies **Algemeen** en voer **SLClientPolicy** in het veld Naam in.
5. Schakel het vakje Adres Pools **in**.
6. Klik op **Selecteren** en vervolgens op **Toevoegen**.Het dialoogvenster Wol toevoegen verschijnt.
7. Configuratie van de adrepool van een IP bereik dat momenteel niet op uw netwerk in gebruik is.Dit voorbeeld gebruikt deze waarden:Name: SLB: clientpool**IP-adres starten**: 192.168.25.1**IP-adres beëindigen**: 192.168.25.50**Subnetmasker**: 255.255.255.0

8. Klik op **OK**.
9. Kies de nieuwe pool en klik op **Toewijzen**.
10. Klik op **OK** en vervolgens op **Meer opties**.
11. Schakel het vakje voor de **innerlijke** tunneling-protocollen uit.
12. Controleer **SSL VPN-client**.
13. Kies in het linker deelvenster **servers**.
14. Schakel het aankruisvakje voor DNS-servers **uit** en voer het IP-adres van de interne DNS-server in dat de AnyConnect-clients gebruiken.Dit voorbeeld gebruikt *192.168.50.5*.
15. Klik op **Meer opties**.
16. Schakel het aanvinkvakje Default Domain **Inherit uit**.
17. Voer het domein in dat door uw interne netwerk wordt gebruikt. Bijvoorbeeld *tsweb.local.*
18. Klik op **OK** en vervolgens op **Toepassen**.

Opdrachtlijnvoorbeeld

ciscoa
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.*

Bypass voor toegangslijst voor VPN-verbindingen configureren

Wanneer u deze optie activeert, kunt u de SSL/IPsec-clients gebruiken om de lijst met interfacetoegang te omzeilen.

ASDM-procedure

1. Klik op **Configuration** en klik vervolgens op **Remote Access VPN**.
2. **Network (Client) Access** uitbreiden en vervolgens **Advanced** uitbreiden.
3. Vul **SSL VPN** uit en kies **de toegangslijst voor interface-omzeilen**.
4. Zorg ervoor dat de **inbound SSL VPN en IPSEC sessies om de lijsten van de interfacetoegang te omzeilen** zijn ingeschakeld en klik op **Toepassen**.

Opdrachtlijnvoorbeeld

ciscoa
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)#
```

Stap 6. Maak een verbindingsprofiel en een tunnelgroep voor de AnyConnect-clientverbindingen

Wanneer VPN-klanten verbinding maken met de ASA, verbinden ze zich met een verbindingsprofiel of tunnelgroep. De tunnelgroep wordt gebruikt om verbindingsparameters te definiëren voor specifieke typen VPN-verbindingen, zoals IPsec L2L, IPsec externe toegang, clientloze SSL en client-SSL.

ASDM-procedure

1. Klik op **Configuration** en klik vervolgens op **Remote Access VPN**.
2. **Network (Client) Access** uitbreiden en **SSL VPN** vervolgens uitbreiden.
3. Kies **verbindingsprofielen** en klik op **Toevoegen**.
4. Kies **Basic** en voer deze waarden in:Name: SLB: contentprofiel**Verificatie**: LOKAAL**Standaardgroepsbeleid**: SLBbeleid voor contanten
5. Zorg ervoor dat het aanvinkvakje **SSL VPN Client Protocol** is ingeschakeld.
6. In het linker deelvenster, vouwt u **Geavanceerd uit** en kiest u **SSL VPN**.
7. Onder Connection Aliases, klik op **Add** en voer een naam in waaraan de gebruikers hun VPN-verbindingen kunnen associëren. Bijvoorbeeld *SSLVPN-client*.
8. Klik op **OK** en vervolgens **op OK** opnieuw.
9. Controleer onder in het ASDM-venster de **gebruiker toestaan om een verbinding te selecteren, geïdentificeerd door alias in de tabel hierboven bij de** controle **van de logpagina** en klik op **Toepassen**.

Opdrachtlijnvoorbeeld

ciscoa

```
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.
```

Stap 7. Configureer de NAT-vrijstelling voor AnyConnect-clients

NAT-vrijstelling moet worden ingesteld voor elke IP-adressen of -bereiken die u de SSL VPN-

clients wilt toestaan. In dit voorbeeld hebben de SSL VPN-clients alleen toegang tot de interne IP 192.168.50.5 nodig.

N.B.: Als NAT-regeling niet is ingeschakeld, is deze stap niet vereist. Gebruik de opdracht **NAT-besturing tonen** om te controleren. Om via ASDM te controleren klikt u op **Configuration**, klikt u op **Firewall** en kiest u **NAT-regels**. Als het dialoogvenster **Toegang via de firewall zonder** adresomzetting is ingeschakeld, kunt u deze stap overslaan.

ASDM-procedure

1. Klik op **Configuration** en vervolgens op **Firewall**.
2. Kies **NAT-regels** en klik op **Toevoegen**.
3. Kies **NAT-vrijstellingsregel toevoegen** en voer deze waarden in:**Actie**: vrijstellen**Interface**: binnenkant**Bron**: 192.168.50.5**Bestemming**: 192.168.25.0/24**NAT-vrije richting**: NAT Vrijgesteld uitgaande verkeer van interface 'binnen' naar lagere veiligheidsinterfaces (standaard)
4. Klik op **OK** en vervolgens op **Toepassen**.

Opdrachtlijnvoorbeeld

ciscoa

```
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)#
```

Stap 8: Voeg gebruikers toe aan de lokale database

Als u lokale authenticatie gebruikt (de standaard), moet u gebruikersnamen en wachtwoorden definiëren in de lokale database voor gebruikersverificatie.

ASDM-procedure

1. Klik op **Configuration** en klik vervolgens op **Remote Access VPN**.
2. **AAA-instelling** uitvouwen en **lokale gebruikers** kiezen.
3. Klik op **Add** en voer deze waarden in:Username: matthewp**Wachtwoord**: p@ssw0rd**Wachtwoord bevestigen**: p@ssw0rd
4. Selecteer de radioknop **Geen ASDM, SSH, telnet of console Access**.
5. Klik op **OK** en vervolgens op **Toepassen**.
6. Herhaal deze stap voor extra gebruikers en klik vervolgens op **Opslaan**.

Opdrachtlijnvoorbeeld

ciscoa

```
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.
```

Verifiëren

Gebruik deze sectie om te controleren of de SSL VPN-configuratie geslaagd is

Aansluiten op de ASA met AnyConnect-client

Installeer de client direct op een pc en sluit aan op de ASA externe interface of voer https en het FQDN/IP-adres van de ASA in in een webbrowser in. Als u een webbrowser gebruikt, installeert de client zichzelf bij succesvolle aanmelding.

Controleer SSL VPN-clientverbindingen

Gebruik de opdracht **show vpn-sessiondb svc** om aangesloten SSL VPN-clients te controleren.

```
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)#
```

De **vpn-sessiondb naam** *gebruikersnaam* **voor de** gebruikersnaam **voor** de **gebruikersnaam** afwerkt. Een bericht met *Administrator Reset* wordt naar de gebruiker verzonden als de verbinding wordt verbroken.

```
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)#
```

Raadpleeg de Cisco AnyConnect VPN-beheerdershandleiding voor meer informatie over de AnyConnect 2.0-client.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor probleemoplossing (optioneel)

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **debug van webversie svc 255** - displays debug de berichten over verbindingen naar SSL VPN-clients via WebVPN.**Succesvolle AnyConnect-aanmelding**

```
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
```

Geen verbinding maken (slecht wachtwoord)

```
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]
```

Gerelateerde informatie

- Cisco AnyConnect VPN-clientbeheerdershandleiding, versie 2.0
- Releaseopmerkingen van AnyConnect VPN-client, release 2.0
- Technische ondersteuning en documentatie – Cisco Systems