

ASA 8.x : Exemple de configuration de l'accès VPN avec le client VPN AnyConnect à l'aide d'un certificat auto-signé

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Configurez](#)

[Étape 1. Configurez un certificat Auto-émis](#)

[Étape 2. Téléchargez et identifiez l'image de client de VPN SSL](#)

[Étape 3. Enable Anyconnect Access](#)

[Étape 4. Créez une nouvelle stratégie de groupe](#)

[Configurer le contournement de la liste d'accès pour les connexions VPN](#)

[Étape 6. Créez un profil de connexion et un groupe de tunnel pour les connexions client d'AnyConnect](#)

[Étape 7. Configurez le nat exemption pour des clients d'AnyConnect](#)

[Étape 8. Ajoutez les utilisateurs à la base de données locale](#)

[Vérifiez](#)

[Dépannez](#)

[Commandes de dépannage \(facultatif\)](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit comment employer des certificats auto-signés pour permettre des connexions VPN SSL d'accès à distance à ASA à partir du client Cisco AnyConnect 2.0.

[Conditions préalables](#)

[Conditions requises](#)

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Configuration Asa de base qui exécute le logiciel version 8.0
- ASDM 6.0(2)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

Le client Cisco AnyConnect 2.0 est un client VPN basé sur SSL. Le client AnyConnect peut être utilisé et installé sur un grand choix de systèmes d'exploitation, tels que Windows 2000, XP, Vista, Linux (Multi-distribution) et MAC OS X. Le client AnyConnect peut être installé manuellement sur le PC distant par l'administrateur système. Il peut également être chargé sur l'appliance de sécurité et préparé en vue du téléchargement aux utilisateurs distants. Après que l'application est téléchargée, il peut automatiquement être désinstallé une fois la connexion terminée, ou il peut rester sur le PC distant en vue de futures connexions VPN SSL. Cet exemple montre comment préparer le client AnyConnect en vue du téléchargement selon l'authentification SSL réussie basée sur le navigateur.

Pour plus d'informations sur le client AnyConnect 2.0, référez-vous aux [Notes de publication AnyConnect 2.0](#).

Remarque: MS Terminal Services n'est pas pris en charge en même temps que le client AnyConnect. Vous ne pouvez pas vous connecter via RDP à un ordinateur et lancer ensuite une session AnyConnect. Vous ne pouvez pas vous connecter via RDP à un client qui est connecté via AnyConnect.

Remarque: La première installation d'AnyConnect exige que l'utilisateur ait des droits d'administrateur (que vous utilisiez le package msi AnyConnect autonome ou que vous diffusiez le fichier pkg à partir de l'ASA). Si l'utilisateur n'a pas de droits d'administrateur, une boîte de dialogue énonçant cette condition s'affiche. Les mises à niveau ultérieures n'exigeront pas que l'utilisateur ayant installé AnyConnect précédemment ait des droits d'administrateur.

Configurez

Afin de configurer l'ASA pour l'accès VPN à l'aide du client AnyConnect, effectuez ces étapes :

1. [Configurez les certificats auto-émis.](#)
2. [Téléchargez et identifiez l'image du client VPN SSL.](#)
3. [Activez l'accès AnyConnect.](#)
4. [Créez une nouvelle politique de groupe.](#)
5. [Configurer le contournement de la liste d'accès pour les connexions VPN.](#)
6. [Créer un profil de connexion et un groupe de tunnels pour les connexions du client](#)

[AnyConnect.](#)

7. [Configurez l'exemption NAT pour les clients AnyConnect.](#)
8. [Ajoutez les utilisateurs à la base de données locale.](#)

Étape 1. Configurez un certificat Auto-émis

Par défaut, l'appliance de sécurité a un certificat auto-signé qui est généré à nouveau chaque fois que le périphérique est redémarré. Vous pouvez acheter votre propre certificat de constructeurs, tels que Verisign ou EnTrust, ou vous pouvez configurer l'ASA afin qu'il émette un certificat d'identité pour lui-même. Ce certificat ne change pas même lorsque le périphérique est redémarré. Terminez cette étape afin de générer des certificats auto-signés qui persistent quand le périphérique est redémarré.

Procédure ASDM

1. Cliquez sur **Configuration**, puis sur **Remote Access VPN**.
2. Développez **Certificate Management**, et choisissez alors **Identity Certificates**.
3. Cliquez sur **Add**, puis cliquez sur la case d'option **Add a new identity certificate**.
4. Cliquez sur **New**.
5. Dans la boîte de dialogue Add Key Pair, cliquez sur la case d'option **Enter new key pair name**.
6. Entrez un nom pour identifier la paire de clés. Cet exemple utilise *sslvpnkeypair*.
7. Cliquez sur **Generate Now**.
8. Dans la boîte de dialogue Add Identity Certificate, assurez-vous que la paire de clés récemment créée est sélectionnée.
9. Pour le DN du sujet du certificat, écrivez le nom de domaine complet (FQDN) qui sera utilisé pour se connecter à l'interface de terminaison du VPN. **CN=sslvpn.cisco.com**
10. Cliquez sur **Advanced**, et écrivez le FQDN utilisé pour le champ Certificate Subject DN. Par exemple, **FQDN : sslvpn.cisco.com**
11. Cliquez sur **OK**.
12. Activez la case à cocher **Generate Self Signed Certificate** et cliquez sur **Add Certificate**.
13. Cliquez sur **OK**.
14. Cliquez sur **Configuration**, puis sur **Remote Access VPN**.
15. Développez **Advanced**, et choisissez **SSL Settings**.
16. Dans la zone Certificats, choisissez interface qui sera utilisée pour terminer le VPN SSL (dehors) et cliquez sur **Edit**.
17. Dans la liste déroulante Certificate, choisissez le certificat auto-signé que vous avez généré plus tôt.
18. Cliquez sur **OK**, puis sur **Apply**.

Exemple de ligne de commande

```
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.

```

Étape 2. Téléchargez et identifiez l'image de client de VPN SSL

Ce document utilise le client AnyConnect SSL 2.0. Vous pouvez obtenir ce client sur le [site Web de téléchargement de logiciel Cisco](#). Une image distincte Anyconnect est requise pour chaque système d'exploitation que les utilisateurs distants prévoient d'utiliser. Pour plus d'informations, reportez-vous aux [notes de publication relatives à Cisco AnyConnect 2.0](#).

Une fois que vous obtenez le client AnyConnect, effectuez ces étapes :

Procédure ASDM

1. Cliquez sur **Configuration**, puis sur **Remote Access VPN**.
2. Développez **Network (Client) Access**, puis développez **Advanced**.
3. Développez **SSL VPN**, et choisissez **client Settings**.
4. Dans la zone SSL VPN Client Images, cliquez sur **Add**, puis cliquez sur **Upload**.
5. Naviguez jusqu'à l'endroit où vous avez téléchargé le client AnyConnect.
6. Sélectionnez le fichier, puis cliquez sur **Upload File**. Une fois le client téléchargé, vous recevez un message énonçant que le fichier a été téléchargé dans la mémoire Flash avec succès.
7. Cliquez sur **OK**. Une boîte de dialogue pour confirmer que vous voulez utiliser l'image nouvellement téléchargée comme image actuelle de client VPN SSL s'affiche.
8. Cliquez sur **OK**.
9. Cliquez sur **OK**, puis sur **Apply**.
10. Répétez les étapes de cette section pour chaque package spécifique du système d'exploitation Anyconnect que vous voulez utiliser.

Exemple de ligne de commande

```

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.
```

Étape 3. Enable Anyconnect Access

Afin de permettre au client AnyConnect de se connecter à l'ASA, vous devez activer l'accès sur l'interface qui termine des connexions VPN SSL. Cet exemple utilise l'interface externe afin de terminer des connexions Anyconnect.

Procédure ASDM

1. Cliquez sur **Configuration**, puis sur **Remote Access VPN**.
2. Développez **Network (Client) Access**, puis choisissez **SSL VPN Connection Profiles**.
3. Activez la case à cocher **Enable Cisco AnyConnect VPN Client**.
4. Activez la case à cocher **Allow Access the outside interface**, puis cliquez sur **Apply**.

Exemple de ligne de commande

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

Étape 4. Créez une nouvelle stratégie de groupe

Une politique de groupe spécifie les paramètres de configuration qui devraient être appliqués aux clients quand ils se connectent. Cet exemple crée une politique de groupe nommée *SSLClientPolicy*.

Procédure ASDM

1. Cliquez sur **Configuration**, puis sur **Remote Access VPN**.
2. Développez **Network (Client) Access**, puis choisissez **Group Policies**.
3. Cliquez sur **Add**.
4. Choisissez **General**, puis entrez **SSLClientPolicy** dans le champ Name.
5. Désactivez la case à cocher **Address Pools Inherit**.
6. Cliquez sur **Select**, puis cliquez sur **Add**. La boîte de dialogue Add IP Pool apparaît.
7. Configurez le pool d'adresses d'une plage d'adresses IP qui n'est pas actuellement en service sur votre réseau. Cet exemple utilise ces valeurs : **Nom** : **SSLClientPoolStarting IP Address: 192.168.25.1Ending IP Address: 192.168.25.50Subnet Mask: 255.255.255.0**
8. Cliquez sur **OK**.
9. Choisissez le pool nouvellement créé, puis cliquez sur **Assign**.
10. Cliquez **OK**, puis cliquez sur **More Options**.
11. Désactivez la case à cocher **Inherit** des protocoles de transmission tunnel.
12. Activez **SSL VPN Client**.
13. Dans le volet gauche, choisissez **Servers**.
14. Désactivez la case à cocher des serveurs DNS **Inherit**, puis entrez l'adresse IP du serveur DNS interne que les clients AnyConnect utiliseront. Cet exemple utilise *192.168.50.5*.
15. Cliquez sur **More Options**.

16. Désactivez la case à cocher **Default Domain Inherit**.
17. Entrez dans le domaine utilisé par votre réseau interne. Par exemple, *tsweb.local*.
18. Cliquez sur **OK**, puis sur **Apply**.

Exemple de ligne de commande

```
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.
```

Configurer le contournement de la liste d'accès pour les connexions VPN

Quand vous activez cette option, vous permettez aux clients SSL/IPsec de contourner la liste d'accès de l'interface.

Procédure ASDM

1. Cliquez sur **Configuration**, puis sur **Remote Access VPN**.
2. Développez **Network (Client) Access**, puis développez **Advanced**.
3. Développez **SSL VPN**, puis choisissez **Bypass Interface Access List**.
4. Assurez-vous que la case à cocher **Enable inbound SSL VPN and IPSEC Sessions to bypass interface access lists** est activée, puis cliquez sur **Apply**.

Exemple de ligne de commande

```
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)#
```

Étape 6. Créez un profil de connexion et un groupe de tunnel pour les connexions client d'AnyConnect

Quand les clients VPN se connectent à l'ASA, ils se connectent à un profil de connexion ou à un groupe de tunnels. Le groupe de tunnels est utilisé pour définir des paramètres de connexion pour les types spécifiques de connexions VPN, tels que L2L IPsec, l'accès à distance IPsec L2L, le SSL sans client et le SSL client.

Procédure ASDM

1. Cliquez sur **Configuration**, puis sur **Remote Access VPN**.
2. Développez **Network (Client) Access**, puis développez **SSL VPN**.
3. Choisissez **Connection Profiles**, puis cliquez sur **Add**.
4. Choisissez **Basic**, et entrez ces valeurs : **Nom** : SSLClientProfileAuthentification : GENS DU PAYSD **Default Group Policy**: SSLClientPolicy
5. Assurez que la case à cocher **SSL VPN Client Protocol** est activée.
6. Dans le volet gauche, développez **Advanced**, puis choisissez **SSL VPN**.
7. Sous **Connection Aliases**, cliquez sur **Add**, et entrez un nom auquel les utilisateurs peuvent associer leurs connexions VPN. Par exemple, *SSLVPNClient*.
8. Cliquer sur **OK**, puis à nouveau sur **OK**.
9. Au bas de la fenêtre ASDM, activez la case à cocher **Allow user to select connection, identified by alias in the table above at login page**, puis cliquez sur **Apply**.

Exemple de ligne de commande

```

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.

```

Étape 7. Configurez le nat exemption pour des clients d'AnyConnect

L'exemption NAT devrait être configurée pour toutes les adresses IP ou plages que vous voulez permettre aux clients VPN SSL d'accéder. Dans cet exemple, les clients VPN SSL ont besoin de l'accès à l'IP interne 192.168.50.5 seulement.

Remarque: Si Nat-control n'est pas activé, cette étape n'est pas requise. Employez la commande **show run nat-control** pour vérifier. Afin de vérifier via ASDM, cliquez sur **Configuration**, cliquez sur **Firewall**, puis choisissez **Nat Rules**. Si la case à cocher **Enable traffic through the firewall without address translation** est activée, vous pouvez ignorer cette étape.

Procédure ASDM

1. Cliquez sur **Configuration**, puis cliquez sur **Firewall**.
2. Choisissez **Nat Rules**, puis cliquez sur **Add**.
3. Choisissez **Add NAT Exempt Rule**, et entrez ces valeurs : **Action** : ExemptInterface : à l'intérieur **Source** : 192.168.50.5 **Destination** : 192.168.25.0/24 **NAT Exempt Direction**: NAT Exempt outbound traffic from interface 'inside' to lower security interfaces (Default)
4. Cliquez sur **OK**, puis sur **Apply**.

Exemple de ligne de commande

```

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)#
```

Étape 8. Ajoutez les utilisateurs à la base de données locale

Si vous utilisez l'authentification locale (par défaut), vous devez définir des noms d'utilisateur et des mots de passe dans la base de données locale pour l'authentification des utilisateurs.

Procédure ASDM

1. Cliquez sur **Configuration**, puis sur **Remote Access VPN**.
2. Développez **AAA Setup**, puis choisissez **Local Users**.
3. Cliquez sur **Add**, puis entrez ces valeurs :
Nom d'utilisateur : matthewp
Mot de passe : p@ssw0rd
Confirm Password: p@ssw0rd
4. Sélectionnez la case d'option **No ASDM, SSH, Telnet or Console Access**.
5. Cliquez sur **OK**, puis sur **Apply**.
6. Répétez cette étape pour les utilisateurs supplémentaires, puis cliquez sur **Save**.

Exemple de ligne de commande

```
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.
```

Vérifiez

Employez cette section afin de vérifier que la configuration du VPN SSL est réussie

Connectez-vous à l'ASA avec le client AnyConnect

Installez le client directement sur un PC, et connectez-vous à l'interface externe ASA, ou entrez https et l'adresse FQDN/IP de l'ASA dans un navigateur Web. Si vous utilisez un navigateur Web, le client s'installe lui-même si l'ouverture de session est réussie.

Vérifiez les connexions client VPN SSL

Employez la commande **show vpn-sessiondb svc** afin de vérifier les clients VPN SSL connectés.

```
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)#
```

La commande **vpn-sessiondb logoff name username** ferme la session des utilisateurs par nom d'utilisateur. Un message *Administrator Reset* est envoyé à l'utilisateur une fois ce dernier déconnecté.


```
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)#
```

Pour plus d'informations sur le client AnyConnect 2.0, référez-vous au [Guide de l'administrateur Cisco AnyConnect VPN](#).

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

[Commandes de dépannage \(facultatif\)](#)

L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

Remarque: Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

- **debug webvpn svc 255** - Affiche des messages de débogage sur les connexions aux clients

```
VPN SSL sur WebVPN.Successful AnyConnect Loginciscoasa(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 Unsuccessful AnyConnect Login (Bad
Password)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]
```

[Informations connexes](#)

- [Guide de l'administrateur Cisco AnyConnect VPN Client, Version 2.0](#)
- [Notes de publication relatives au client VPN d'AnyConnect, Version 2.0](#)
- [Support et documentation techniques - Cisco Systems](#)