ASA 8.x: Accesso VPN con il client VPN AnyConnect utilizzando un esempio di configurazione di un certificato autofirmato

Sommario

Introduzione

In questo documento viene descritto come usare certificati autofirmati per consentire le connessioni VPN SSL per l'accesso remoto all'appliance ASA dal client Cisco AnyConnect 2.0.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Configurazione ASA base con software versione 8.0
- ASDM 6.0(2)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Il client Cisco AnyConnect 2.0 è un client VPN basato su SSL. Il client AnyConnect può essere utilizzato e installato su diversi sistemi operativi, ad esempio Windows 2000, XP, Vista, Linux (Multiple Distors) e MAC OS X. Il client AnyConnect può essere installato manualmente sul PC remoto dall'amministratore di sistema. Può anche essere caricato sull'appliance di sicurezza e pronto per essere scaricato dagli utenti remoti. Dopo il download, l'applicazione può essere disinstallata automaticamente al termine della connessione oppure può rimanere sul PC remoto per le connessioni VPN SSL future. In questo esempio, dopo aver completato con successo l'autenticazione SSL basata su browser, il client AnyConnect è pronto per il download.

Per ulteriori informazioni sul client AnyConnect 2.0, consultare le note sulla versione di AnyConnect 2.0.

Nota: MS Terminal Services non è supportato insieme al client AnyConnect. Non è possibile eseguire il RDP su un computer e quindi avviare una sessione AnyConnect. Non è possibile eseguire RDP su un client connesso tramite AnyConnect.

Nota: la prima installazione di AnyConnect richiede che l'utente disponga di diritti di amministratore (sia che si utilizzi il pacchetto AnyConnect msi standalone o che si estenda il file pkg dall'appliance ASA). Se l'utente non dispone dei diritti di amministratore, viene visualizzata una finestra di dialogo che indica questo requisito. Per gli aggiornamenti successivi, l'utente che ha installato AnyConnect in precedenza non deve avere i diritti di amministratore.

Configurazione

Per configurare l'ASA per l'accesso VPN con il client AnyConnect, attenersi alla seguente procedura:

1. Configurare un certificato autocertificato.
2. Caricare e identificare l'immagine client VPN SSL.
3. Abilitare Anyconnect Access.
4. Creare un nuovo criterio di gruppo.
5. Configurare il bypass dell'elenco accessi per le connessioni VPN.
6. Creare un profilo di connessione e un gruppo di tunnel per le connessioni del client AnyConnect.

7. Configurare l'esenzione NAT per i client AnyConnect.
8. aggiungere utenti al database locale.

Passaggio 1. Configurare un certificato autocertificato

Per impostazione predefinita, l'accessorio di protezione dispone di un certificato autofirmato che viene rigenerato a ogni riavvio del dispositivo. È possibile acquistare un certificato personalizzato da altri fornitori, ad esempio Verisign o EnTrust, oppure configurare l'appliance ASA in modo che emetta un certificato di identità per se stessa. Il certificato rimane invariato anche quando il dispositivo viene riavviato. Completare questo passaggio per generare un certificato autoemesso che persiste quando il dispositivo viene riavviato.

Procedura ASDM

1. Fare clic su **Configurazione** e quindi su **VPN ad accesso remoto**.
2. Espandere **Gestione certificati**, quindi scegliere **Certificati di identità**.
3. Fare clic su **Aggiungi** e quindi sul pulsante di opzione **Aggiungi nuovo certificato di identità**.
4. Fare clic su **New**.
5. Nella finestra di dialogo Aggiungi coppia di chiavi fare clic sul pulsante di opzione **Immetti nuovo nome coppia di chiavi**.
6. Immettere un nome per identificare la coppia di chiavi.In questo esempio viene utilizzato *sslvpnkeypair*.
7. Fare clic su **Genera**.
8. Nella finestra di dialogo Aggiungi certificato di identità verificare che la coppia di chiavi appena creata sia selezionata.
9. In Nome distinto soggetto certificato immettere il nome di dominio completo (FQDN) che verrà utilizzato per connettersi all'interfaccia di terminazione VPN.**CN=sslvpn.cisco.com**
10. Fare clic su **Avanzate** e immettere il nome di dominio completo utilizzato per il campo DN soggetto certificato.Ad esempio, **FQDN**: sslvpn.cisco.com
11. Fare clic su **OK**.
12. Selezionare la casella di controllo **Genera certificato autofirmato** e fare clic su **Aggiungi certificato**.
13. Fare clic su **OK**.
14. Fare clic su **Configurazione** e quindi su **VPN ad accesso remoto**.
15. Espandere **Avanzate** e scegliere **Impostazioni SSL**.
16. Nell'area Certificati scegliere l'interfaccia che verrà utilizzata per terminare la VPN SSL (esterna) e fare clic su **Modifica**.
17. Nell'elenco a discesa Certificato scegliere il certificato autofirmato generato in precedenza.
18. Fare clic su **OK**, quindi su **Applica**.

Esempio della riga di 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.
```

Passaggio 2. Caricare e identificare l'immagine client VPN SSL

Nel documento viene usato il client AnyConnect SSL 2.0. È possibile ottenere questo client sul sito Web di download del software Cisco. Per ciascun sistema operativo che gli utenti remoti intendono usare, è richiesta un'immagine Anyconnect distinta. Per ulteriori informazioni, consultare le note sulla versione di Cisco AnyConnect 2.0.

Dopo aver ottenuto il client AnyConnect, procedere come segue:

Procedura ASDM

1. Fare clic su **Configurazione** e quindi su **VPN ad accesso remoto**.
2. Espandere **Accesso di rete (client)**, quindi **Avanzate**.
3. Espandere **SSL VPN** e scegliere **Impostazioni client**.
4. Nell'area Immagini client VPN SSL fare clic su **Aggiungi**, quindi su **Carica**.
5. Selezionare il percorso in cui è stato scaricato il client AnyConnect.
6. Selezionare il file e fare clic su **Upload File** (Carica file).Una volta caricato il client, viene visualizzato un messaggio che indica che il file è stato caricato correttamente nella memoria flash.
7. Fare clic su **OK**.Verrà visualizzata una finestra di dialogo per confermare che si desidera utilizzare l'immagine appena caricata come immagine client VPN SSL corrente.
8. Fare clic su **OK**.
9. Fare clic su **OK**, quindi su **Applica**.
10. Ripetere i passaggi di questa sezione per ciascun pacchetto Anyconnect specifico del sistema operativo che si desidera utilizzare.

Esempio della riga di 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.
```

Passaggio 3. Abilitazione Dell'Accesso Anyconnect

Per consentire al client AnyConnect di connettersi all'ASA, è necessario abilitare l'accesso sull'interfaccia che termina le connessioni VPN SSL. In questo esempio viene usata l'interfaccia esterna per terminare le connessioni Anyconnect.

Procedura ASDM

1. Fare clic su **Configurazione** e quindi su **VPN ad accesso remoto**.
2. Espandere **Accesso di rete (client)**, quindi scegliere **Profili connessione VPN SSL**.
3. Selezionare la casella di controllo **Abilita client VPN Cisco AnyConnect**.
4. Selezionare la casella di controllo **Consenti accesso** per l'interfaccia esterna e fare clic su **Applica**.

Esempio della riga di comando

ciscoasa

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

Passaggio 4. Creare un nuovo criterio di gruppo

Un criterio di gruppo specifica i parametri di configurazione da applicare ai client quando si connettono. In questo esempio viene creato un criterio di gruppo denominato *SSLClientPolicy*.

Procedura ASDM

1. Fare clic su **Configurazione** e quindi su **VPN ad accesso remoto**.
2. Espandere **Accesso di rete (client)** e scegliere **Criteri di gruppo**.
3. Fare clic su **Add**.
4. Scegliere **Generale** e immettere **SSLClientPolicy** nel campo Nome.
5. Deselezionare la casella di controllo **Eredita** pool di indirizzi.
6. Fare clic su **Seleziona**, quindi su **Aggiungi**.Verrà visualizzata la finestra di dialogo Aggiungi

pool IP.

7. Configurare il pool di indirizzi da un intervallo IP attualmente non in uso nella rete.In questo esempio vengono utilizzati i valori seguenti:**Nome:** SSLClientPool**Indirizzo IP iniziale**: 192.168.25.1**Indirizzo IP finale**: 192.168.25.50**Subnet mask:** 255.255.255.0
8. Fare clic su **OK**.
9. Scegliere il pool appena creato e fare clic su **Assegna**.
10. Fare clic su **OK**, quindi su **Altre opzioni**.
11. Deselezionare la casella di controllo **Eredita** protocolli di tunneling.
12. Selezionare **SSL VPN Client**.
13. Nel riquadro di sinistra, scegliere **Server**.
14. Deselezionare la casella di controllo **Eredita** server DNS e immettere l'indirizzo IP del server DNS interno che verrà utilizzato dai client AnyConnect.In questo esempio viene utilizzato *192.168.50.5*.
15. Fare clic su **Altre opzioni**.
16. Deselezionare la casella di controllo **Eredità** dominio predefinito.
17. Immettere il dominio utilizzato dalla rete interna. Ad esempio, *tsweb.local*.
18. Fare clic su **OK**, quindi su **Applica**.

Esempio della riga di 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.
```

Configura esclusione elenco accessi per connessioni VPN

Se si attiva questa opzione, i client SSL/IPsec potranno ignorare l'elenco degli accessi all'interfaccia.

Procedura ASDM

1. Fare clic su **Configurazione** e quindi su **VPN ad accesso remoto**.
2. Espandere **Accesso di rete (client)**, quindi **Avanzate**.
3. Espandere **SSL VPN** e scegliere **Ignora elenco accessi interfaccia**.
4. Verificare che la casella di controllo **Abilita sessioni VPN e IPSEC SSL in ingresso per ignorare gli elenchi degli accessi all'interfaccia** sia selezionata e fare clic su **Applica**.

Esempio della riga di 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)#

Passaggio 6. Creazione di un profilo di connessione e di un gruppo di tunnel per le connessioni client AnyConnect

Quando i client VPN si connettono all'ASA, si connettono a un profilo di connessione o a un gruppo di tunnel. Il gruppo di tunnel viene utilizzato per definire i parametri di connessione per tipi specifici di connessioni VPN, ad esempio IPsec L2L, accesso remoto IPsec, SSL senza client e SSL client.

Procedura ASDM

1. Fare clic su **Configurazione** e quindi su **VPN ad accesso remoto**.
2. Espandere **Accesso di rete (client)**, quindi **VPN SSL**.
3. Scegliere **Profili di connessione**, quindi fare clic su **Aggiungi**.
4. Scegliere **Base** e immettere i seguenti valori:**Nome:** ProfiloClientLC**Autenticazione:** LOCALE**Criteri di gruppo predefiniti**: CriterioClientLC
5. Verificare che la casella di controllo **SSL VPN Client Protocol** sia selezionata.
6. Nel riquadro di sinistra, espandere **Avanzate** e scegliere **SSL VPN**.
7. In Alias di connessione fare clic su **Aggiungi** e immettere un nome a cui gli utenti possono associare le connessioni VPN. Ad esempio, *SSLVPNClient*.
8. Fare clic su **OK**, quindi fare di nuovo clic su **OK**.
9. Nella parte inferiore della finestra ASDM, selezionare la casella di controllo **Consenti all'utente di selezionare la connessione, identificata dall'alias nella tabella riportata sopra nella pagina di accesso**, quindi fare clic su **Applica**.

Esempio della riga di 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.
```

Passaggio 7. Configurare l'esenzione NAT per i client AnyConnect

Ènecessario configurare l'esenzione NAT per tutti gli indirizzi IP o gli intervalli a cui si desidera consentire l'accesso ai client VPN SSL. Nell'esempio, i client VPN SSL devono accedere solo all'indirizzo IP 192.168.50.5 interno.

Nota: se il controllo NAT non è abilitato, questo passaggio non è necessario. Per la verifica, usare il comando **show run nat-control**. Per eseguire la verifica tramite ASDM, fare clic su **Configuration**, quindi su **Firewall** e selezionare **Nat Rules**. Se la casella di controllo **Abilita traffico attraverso il firewall senza conversione degli indirizzi** è selezionata, è possibile ignorare questo passaggio.

Procedura ASDM

1. Fare clic su **Configurazione** e quindi su **Firewall**.
2. Scegliere **Regole Nat**, quindi fare clic su **Aggiungi**.
3. Scegliere **Aggiungi regola esenzione NAT** e immettere i seguenti valori:**Azione:** Esente**Interfaccia:** interno**Fonte**: 192.168.50.5**Destinazione:** 192.168.25.0/24**Direzione esenzione NAT**: NAT - Esenzione traffico in uscita dall'interfaccia 'inside' per interfacce di sicurezza inferiori (impostazione predefinita)
4. Fare clic su **OK**, quindi su **Applica**.

Esempio della riga di 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)#
```

Passaggio 8. Aggiunta di utenti al database locale

Se si utilizza l'autenticazione locale (predefinita), è necessario definire i nomi utente e le password nel database locale per l'autenticazione utente.

Procedura ASDM

1. Fare clic su **Configurazione** e quindi su **VPN ad accesso remoto**.
2. Espandere **Impostazione AAA** e scegliere **Utenti locali**.
3. Fare clic su **Add** e immettere i seguenti valori:**Username:** matthewp**Password**: p@ssw0rd**Conferma password**: p@ssw0rd
4. Selezionare il pulsante di opzione **No ASDM, SSH, Telnet o Accesso console**.
5. Fare clic su **OK**, quindi su **Applica**.
6. Ripetere questo passaggio per altri utenti e quindi fare clic su **Salva**.

Esempio della riga di 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.*

Verifica

Per verificare che la configurazione della VPN SSL abbia esito positivo, utilizzare questa sezione

Connessione all'ASA con il client AnyConnect

Installare il client direttamente su un PC e collegarsi all'interfaccia esterna dell'ASA oppure immettere https e l'indirizzo FQDN/IP dell'ASA in un browser Web. Se si utilizza un browser Web, il client si installa al completamento dell'accesso.

Verifica connessioni client VPN SSL

Usare il comando **show vpn-sessiondb svc** per verificare i client VPN SSL connessi.

```
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)#
```

Il comando **vpn-sessiondb logoff name** *username* disconnette gli utenti in base al nome utente. Quando si è disconnessi, viene inviato all'utente un messaggio di *ripristino dell'amministratore*.

```
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)#
```

Per ulteriori informazioni sul client AnyConnect 2.0, consultare la Guida dell'amministratore VPN di Cisco AnyConnect.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi (opzionali)

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug webvpn svc 255**: visualizza i messaggi di debug sulle connessioni ai client VPN SSL su WebVPN.**Accesso AnyConnect riuscito**

```
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
```

Accesso ad AnyConnect non riuscito (password errata)

```
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]
```

Informazioni correlate

- Cisco AnyConnect VPN Client Administrator Guide, versione 2.0
- Note sulla versione per AnyConnect VPN Client, versione 2.0
- Documentazione e supporto tecnico – Cisco Systems