ASA 8.x: O VPN alcança com o cliente VPN de AnyConnect que usa o exemplo de configuração do certificado auto-assinado

---

Índice

Introdução

Este documento descreve como usar certificados auto-assinados para permitir conexões de VPN do Acesso remoto SSL ao ASA do cliente de Cisco AnyConnect 2,0.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Configuração básica ASA que executa a versão de software 8,0
- ASDM 6.0(2)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ASA 8.0(2), ASDM 6,0 (2)
- Cisco AnyConnect 2,0

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O cliente de Cisco AnyConnect 2,0 é um cliente VPN SSL-baseado. O cliente de AnyConnect pode ser utilizado e instalado em uma variedade de sistemas operacionais, tais como o Windows 2000, o XP, a vista, o Linux (Distros múltiplo) e o MAC OS X. O cliente de AnyConnect pode ser instalado manualmente no PC remoto pelo administrador de sistema. Pode igualmente ser carregado na ferramenta de segurança e ser feito pronto para a transferência aos usuários remotos. Depois que a aplicação é transferida, pode automaticamente desinstalar-se depois que a conexão termina, ou pode permanecer no PC remoto para as conexões de VPN futuras SSL. Este exemplo faz o cliente de AnyConnect pronto para transferir em cima da autenticação com base em navegador bem sucedida SSL.

Para obter mais informações sobre do cliente de AnyConnect 2,0, refira AnyConnect a 2,0 Release Note.

Nota: Os serviços terminal MS não são apoiados conjuntamente com o cliente de AnyConnect. Você não pode RDP a um computador e para iniciar então uma sessão de AnyConnect. Você não pode RDP a um cliente que seja conectado através de AnyConnect.

Nota: A primeira instalação de AnyConnect exige o usuário ter direitos admin (se você usa o pacote autônomo do msi de AnyConnect ou empurra o arquivo de pacote do ASA). Se o usuário não tem direitos admin, uma caixa de diálogo parece que indica esta exigência. As elevações subseqüentes não exigirão o usuário que instalou AnyConnect previamente para ter direitos admin.

Configurar

A fim configurar o ASA para o VPN alcance usando o cliente de AnyConnect, terminam estas etapas:

1. Configurar um certificado Auto-emitido.
2. Transfira arquivos pela rede e identifique a imagem do cliente VPN SSL.
3. Permita o acesso de Anyconnect.
4. Crie uma política nova do grupo.
5. Configurar o desvio da lista de acessos para conexões de VPN.
6. Crie um perfil de conexão e um grupo de túneis para as conexões de cliente de AnyConnect.
7. Configurar a isenção de NAT para clientes de AnyConnect.
8. Adicionar usuários ao banco de dados local.

Etapa 1. Configurar um certificado Auto-emitido

À revelia, a ferramenta de segurança tem um certificado auto-assinado que seja regenerado todas as vezes o dispositivo seja recarregado. Você pode comprar seu próprio certificado dos vendedores, tais como Verisign ou EnTrust, ou você pode configurar o ASA separa emitir- um certificado de identidade. Este certificado permanece o mesmo mesmo quando o dispositivo é recarregado. Termine esta etapa a fim gerar um certificado auto-emitido que persista quando o dispositivo é recarregado.

Procedimento ASDM

1. **A configuração do** clique, e clica então o **acesso remoto VPN**.
2. Expanda o **gerenciamento certificado**, e escolha então **certificados de identidade**.
3. O clique **adiciona**, e clica então **adicionar um** botão de rádio **novo do certificado de identidade**.
4. Clique em **New**.
5. Na caixa de diálogo do par de chaves adicionar, clique o botão de rádio **novo do nome do par de chaves da entrada**.
6. Dê entrada com um nome para identificar o keypair.

   Este exemplo usa o *sslvpnkeypair*.
7. O clique **gera agora**.
8. Na caixa de diálogo do certificado de identidade adicionar, assegure-se de que o par de chaves recém-criado esteja selecionado.
9. Para o assunto DN do certificado, incorpore o nome de domínio totalmente qualificado (FQDN) que será usado para conectar ao VPN que termina a relação.

   CN=sslvpn.cisco.com
10. Clique **avançado**, e incorpore o FQDN usado para o campo do assunto DN do certificado.

    Por exemplo, **FQDN**: sslvpn.cisco.com
11. Clique em **OK**.
12. Verifique a caixa de verificação do **certificado assinado do auto da geração**, e o clique **adiciona o certificado**.
13. Clique em **OK**.
14. **A configuração do** clique, e clica então o **acesso remoto VPN**.
15. Expanda **avançado**, e escolha **ajustes SSL**.
16. Na área dos Certificados, escolha a relação que será usada para terminar o SSL VPN (fora), e o clique **edita**.
17. Na lista de drop-down do certificado, escolha o certificado auto-assinado que você gerou mais cedo.
18. Clique a **APROVAÇÃO**, e clique-a então **aplicam-se**.

Exemplo da linha de comando

ciscoasa

```
ciscoasa(config)#crypto key generate rsa label sslvpnkeypair
INFO: The name for the keys will be: sslvpnkeypair
Keypair generation process begin. Please wait...

!--- Generate an RSA key for the certificate. (The name should be unique.
!--- For example, sslvpnkeypair.)

ciscoasa(config)#crypto ca trustpoint localtrust

!--- Create a trustpoint for the self-issued certificate.

ciscoasa(config-ca-trustpoint)#enrollment self
ciscoasa(config-ca-trustpoint)#fqdn sslvpn.cisco.com
ciscoasa(config-ca-trustpoint)#subject-name CN=sslvpn.cisco.com

!--- The fully qualified domain name is used for both fqdn and CN.
!--- The name should resolve to the ASA outside interface IP address.

ciscoasa(config-ca-trustpoint)#keypair sslvpnkeypair

!--- The RSA key is assigned to the trustpoint for certificate creation.

ciscoasa(config-ca-trustpoint)#crypto ca enroll localtrust noconfirm
% The fully-qualified domain name in the certificate will be: sslvpn.cisco.com
ciscoasa(config)# ssl trust-point localtrust outside

!--- Assign the trustpoint to be used for SSL connections on the outside interface.
```

Etapa 2. Transfira arquivos pela rede e identifique a imagem do cliente VPN SSL

Este documento usa o cliente de AnyConnect SSL 2,0. Você pode obter este cliente no Web site da transferência de software Cisco. Uma imagem separada de Anyconnect é exigida para cada sistema operacional que os usuários remotos planeiam se usar. Para mais informação, refira Cisco AnyConnect a 2,0 Release Note.

Uma vez que você obtem o cliente de AnyConnect, termine estas etapas:

Procedimento ASDM

1. **A configuração do** clique, e clica então o **acesso remoto VPN**.
2. Expanda o **acesso da rede (cliente)**, e expanda então **avançado**.
3. Expanda **SSL VPN**, e escolha **ajustes do cliente**.
4. Na área das imagens do cliente VPN SSL, o clique **adiciona**, e clica então a **transferência de arquivo pela rede**.
5. Consulte ao lugar onde você transferiu o cliente de AnyConnect.
6. Selecione o arquivo, e clique o **arquivo da transferência de arquivo pela rede**.

   Uma vez que o cliente transfere arquivos pela rede, você recebe uma mensagem que indique que o arquivo estêve transferido arquivos pela rede para piscar successully.
7. Clique em **OK**.

   Uma caixa de diálogo parece confirmar que você quer usar a imagem recentemente transferida arquivos pela rede como a imagem atual do cliente VPN SSL.
8. Clique em **OK**.
9. **A APROVAÇÃO do** clique, e clica então **aplica-se**.
10. Repita as etapas nesta seção para cada pacote específico do sistema de Anyconnect do funcionamento que você quer usar.

Exemplo da linha de comando

ciscoasa

```
ciscoasa(config)#copy tftp://192.168.50.5/anyconnect-win-2.0.0343-k9.pkg flash

Address or name of remote host [192.168.50.5]?

Source filename [anyconnect-win-2.0.0343-k9.pkg]?

Destination filename [anyconnect-win-2.0.0343-k9.pkg]?

Accessing tftp://192.168.50.5/anyconnect-win-2.0.0343-k9.pkg...!!!!!!!!!!!!!
Writing file disk0:/anyconnect-win-2.0.0343-k9.pkg...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
2635734 bytes copied in 4.480 secs (658933 bytes/sec)

!--- AnyConnect image is downloaded to ASA via TFTP.

ciscoasa(config)#webvpn
```

```
ciscoasa(config-webvpn)#svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1

!--- Specify the AnyConnect image to be downloaded by users. The image that is
!--- downloaded the most should have the lowest number. This image uses 1 for the
!--- AnyConnect Windows image.
```

Etapa 3. Permita o acesso de Anyconnect

A fim permitir que o cliente de AnyConnect conecte ao ASA, você deve permitir o acesso na relação que termina conexões de VPN SSL. Este exemplo usa a interface externa a fim terminar conexões de Anyconnect.

Procedimento ASDM

1. **A configuração do** clique, e clica então o **acesso remoto VPN**.
2. Expanda o **acesso da rede (cliente)**, e escolha então **perfis da conexão de VPN SSL**.
3. Verifique a caixa de verificação do **Cisco AnyConnect VPN Client da possibilidade**.
4. Verifique a caixa de **verificação de acesso reservar** para ver se há a interface externa, e o clique **aplica-se**.

Exemplo da linha de comando

ciscoasa

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

Etapa 4. Crie uma política nova do grupo

Uma política do grupo especifica os parâmetros de configuração que devem ser aplicados aos clientes quando conectam. Este exemplo cria uma política do grupo nomeada *SSLClientPolicy*.

Procedimento ASDM

1. **A configuração do** clique, e clica então o **acesso remoto VPN**.
2. Expanda o **acesso da rede (cliente)**, e escolha **políticas do grupo**.
3. Clique em Add.
4. Escolha o **general**, e inscreva **SSLClientPolicy no** campo de nome.
5. Desmarcar os conjuntos de endereços **herdam a** caixa de verificação.
6. Clique **seleto**, e clique-o então **adicionam**.

   A caixa de diálogo do IP pool adicionar aparece.
7. Configurar o conjunto de endereços de uma escala IP que não seja atualmente em uso em sua rede.

   Este exemplo usa estes valores:

   - Nome: SSLClientPool
   - **Começando o endereço IP de Um ou Mais Servidores Cisco ICM NT**: 192.168.25.1
   - **Terminando o endereço IP de Um ou Mais Servidores Cisco ICM NT**: 192.168.25.50
   - **Máscara de sub-rede**: 255.255.255.0
8. Clique em **OK**.
9. Escolha o pool recém-criado, e o clique **atribui**.
10. Clique a **APROVAÇÃO**, e clique então **mais opções**.
11. Desmarcar os protocolos de tunelamento **herdam a** caixa de verificação.
12. Verifique o **cliente VPN SSL**.
13. No painel esquerdo, escolha **server**.
14. Desmarcar os servidores DNS **herdam a** caixa de verificação, e incorporam o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor interno de DNS que os clientes de AnyConnect usarão.

    Este exemplo usa *192.168.50.5*.
15. Clique **mais opções**.

16. Desmarcar o domínio padrão **herdam a** caixa de verificação.

17. Incorpore o domínio usado por sua rede interna. Por exemplo, *tsweb.local.*
18. **A APROVAÇÃO do** clique, e clica então **aplica-se**.

Exemplo da linha de comando

ciscoasa

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

Configurar o desvio da lista de acessos para conexões de VPN

Quando você permite esta opção, você permite que os clientes SSL/IPsec contorneiem a lista de acessos da relação.

Procedimento ASDM

1. **A configuração do** clique, e clica então o **acesso remoto VPN**.
2. Expanda o **acesso da rede (cliente)**, e expanda então **avançado**.
3. Expanda **SSL VPN**, e escolha a **lista de acessos da relação do desvio**.
4. Assegure-se de que a **possibilidade SSL de entrada VPN e as sessões IPSec contornear a** caixa de verificação das **Listas de acesso da relação** estejam verificadas, e o clique **se aplique**.

Exemplo da linha de comando

ciscoasa

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

Etapa 6. Crie um perfil de conexão e um grupo de túneis para as conexões de cliente de AnyConnect

Quando os clientes VPN conectam ao ASA, conectam a um perfil de conexão ou a um grupo de túneis. O grupo de túneis é usado para definir parâmetros de conexão para tipos de conexões de VPN específicos, tais como o Acesso remoto do IPsec L2L, do IPsec, os sem clientes SSL, e o cliente SSL.

Procedimento ASDM

1. **A configuração do** clique, e clica então o **acesso remoto VPN**.
2. Expanda o **acesso da rede (cliente)**, e expanda então **SSL VPN**.
3. Escolha **perfis de conexão**, e o clique **adiciona**.

4. Escolha **básico**, e incorpore estes valores:

    - Nome: SSLClientProfile
    - **Autenticação:** LOCAL

- **Política do grupo padrão**: SSLClientPolicy

5. Assegure-se de que a caixa de verificação do **protocolo do cliente VPN SSL** esteja verificada.

6. No painel esquerdo, expanda **avançado**, e escolha **SSL VPN**.
7. Sob pseudônimos da conexão, o clique **adiciona**, e dá entrada com um nome a que os usuários podem associar suas conexões de VPN. Por exemplo, *SSLVPNClient*.
8. Clique a **APROVAÇÃO**, e clique então a **APROVAÇÃO** outra vez.

9. Na parte inferior do indicador ASDM, verifique o **usuário reservar para selecionar a conexão, identificada pelo pseudônimo na tabela acima na** caixa de verificação da **página de login**, e o clique **aplica-se**.

Exemplo da linha de comando

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

Etapa 7. Configurar a isenção de NAT para clientes de AnyConnect

A isenção de NAT deve ser configurada para todos os endereços IP de Um ou Mais Servidores Cisco ICM NT ou varia você quer permitir que os clientes VPN SSL alcancem. Neste exemplo, os clientes VPN SSL precisam o acesso ao IP interno 192.168.50.5 somente.

Nota: Se o controle nat não é permitido, esta etapa não está exigida. Use o **comando nat-control da corrida da mostra** verificar. A fim verificar com o ASDM, clique a **configuração**, clique o **Firewall**, e escolha **regras Nat**. Se o **tráfego da possibilidade com o Firewall sem** caixa de verificação da **tradução de endereços** é verificado, você pode saltar esta etapa.

Procedimento ASDM

1. **A configuração do** clique, e clica então o **Firewall**.
2. Escolha **regras Nat**, e o clique **adiciona**.
3. Escolha **adicionam a regra isenta NAT**, e incorporam estes valores:

    - Ação: Isento
    - Interface: interna
    - Fonte: 192.168.50.5
    - Destino: 192.168.25.0/24
    - **Sentido isento NAT**: Tráfego de saída isento NAT da relação “interior” às interfaces de segurança mais baixa (opção)

4. **A APROVAÇÃO do** clique, e clica então **aplica-se**.

Exemplo da linha de comando

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

Etapa 8. Adicionar usuários ao banco de dados local

Se você usa a autenticação local (a opção), você deve definir nomes de usuário e senhas no banco de dados local para a autenticação de usuário.

Procedimento ASDM

1. **A configuração do** clique, e clica então o **acesso remoto VPN**.
2. Expanda a **instalação AAA**, e escolha **usuários locais**.
3. O clique **adiciona**, e incorpora estes valores:
    - Nome de usuário: matthewp
    - Senha: p@ssw0rd
    - **Confirme a senha**: p@ssw0rd
4. Não selecione **nenhum** botão de rádio **ASDM, SSH, telnet ou de acesso de console**.
5. Clique a **APROVAÇÃO**, e clique-a então **aplicam-se**.
6. Repita esta etapa para usuários adicionais, e clique então a **salvaguarda**.

Exemplo da linha de comando

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

Verificar

Use esta seção a fim verificar que a configuração de VPN SSL é bem sucedida

Conecte ao ASA com o cliente de AnyConnect

Instale o cliente diretamente em um PC, e conecte-o à interface externa ASA, ou incorpore-o https e o endereço IP de Um ou Mais Servidores Cisco ICM NT FQDN do ASA a um navegador da Web. Se você usa um navegador da Web, o cliente instala-se em cima do login bem-sucedido.

Verifique conexões de cliente de VPN SSL

Use o **comando svc da mostra VPN-sessiondb** a fim verificar clientes VPN conectados SSL.

```
ciscoasa(config-group-policy)#show vpn-sessiondb svc

Session Type: SVC

Username     : matthewp               Index        : 6
Assigned IP  : 192.168.25.1           Public IP    : 172.18.12.111
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 35466                  Bytes Rx     : 27543
Group Policy : SSLClientPolicy        Tunnel Group : SSLClientProfile
Login Time   : 20:06:59 UTC Tue Oct 16 2007
Duration     : 0h:00m:12s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

ciscoasa(config-group-policy)#
```

O comando username do **nome do término de uma sessão VPN-sessiondb** termina usuários pelo nome de usuário. Uma mensagem da *restauração do administrador* é enviada ao usuário quando desligada.

```
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 obter mais informações sobre do cliente de AnyConnect 2,0, refira o guia do administrador de Cisco AnyConnect VPN.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos de Troubleshooting (Opcional)

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **debugar o webvpn svc 255** — Os indicadores debugam mensagens sobre conexões aos clientes VPN SSL sobre o WebVPN.

  Início de uma sessão bem sucedido de AnyConnect

```
ciscoasa(config)#debug webvpn svc 255
INFO: debug webvpn svc enabled at level 255.
ciscoasa(config)#ATTR_FILTER_ID: Name:

SSLVPNClientAccess

, Id: 1, refcnt: 1
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 10.10.1.5' -
!--- Outside IP of ASA

Processing CSTP header line: 'Host: 10.10.1.5'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' -
!--- AnyConnect Version

Processing CSTP header line: 'User-Agent: Cisco AnyConnect
                                        VPN Client 2, 0, 0343'
Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=3338474156@28672@1192565782@EFB9042D72C
                  63CE02164F790435897AC72EE70AE'
Processing CSTP header line: 'Cookie: webvpn=3338474156@28672@119
                  2565782@EFB9042D72C63CE02164F790435897AC72EE70AE'
Found WebVPN cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C
                  63CE02164F790435897AC72EE70AE'
WebVPN Cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C63CE02
                  164F790435897AC72EE70AE'
IPADDR: '3338474156', INDEX: '28672', LOGIN: '1192565782'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: wkstation1' -
!--- Client desktop hostname

Processing CSTP header line: 'X-CSTP-Hostname: wkstation1'
Setting hostname to: 'wkstation1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1206'
Processing CSTP header line: 'X-CSTP-MTU: 1206'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451CB0948AFBE98296FD849
                        49EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51'
Processing CSTP header line: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451C
      B0948AFBE98296FD84949EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:
                            DES-CBC3-SHA:DES-CBC-SHA'
```

```
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.25.1/255.255.255.0 -
!--- IP assigned from IP Pool

CSTP state = HAVE_ADDRESS
SVC: NP setup
np_svc_create_session(0x7000, 0xD41612C8, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got internal message
Unable to initiate NAC, NAC might not be enabled or invalid policy
```

Início de uma sessão mal sucedido de AnyConnect (senha ruim)

```
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]
```

Informações Relacionadas

- **Guia do administrador do Cisco AnyConnect VPN Client, versão 2.0**
- **Release Notess do AnyConnect VPN Client, Release 2.0**
- **Exemplos de Configuração e Notas Técnicas**

Data da Geração do PDF: 29 Julho 2013

http://www.cisco.com/cisco/web/support/BR/104/1044/1044565_asa8.x_anyconnect_vpn.html