Exemplo de Configuração de Acesso VPN do ASA 8.x com o AnyConnect SSL VPN Client

Índice

Introdução

Este documento demonstra como permitir conexões VPN de acesso remoto ao ASA do Cisco AnyConnect 2.0 Client.

Pré-requisitos

Requisitos

Verifique se você atende a estes requisitos antes de tentar esta configuração:

Configuração básica do ASA com software versão 8.0

ASDM 6.0(2)

Componentes Utilizados

As informações deste documento baseiam-se 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 as convenções de documentos.

Informações de Apoio

O Cisco AnyConnect 2.0 Client é um cliente VPN baseado em SSL. O AnyConnect Client pode ser utilizado e instalado em vários sistemas operacionais, como o Windows 2000, XP, Vista, Linux (várias distribuições) e MAC OS X. O AnyConnect Client pode ser instalado manualmente no PC remoto pelo administrador do sistema. Ele também pode carregado no security appliance e disponibilizado para os usuários remotos através de download. Quando o download do aplicativo for encerrado, ele poderá se desinstalar automaticamente após o término da conexão, ou poderá permanecer no PC remoto para futuras conexões VPN SSL. Este exemplo prepara o AnyConnect Client para download quando a autenticação SSL baseada no navegador for bem-sucedida.

Para obter mais informações sobre o AnyConnect 2.0 Client, consulte as Notas de Versão do AnyConnect 2.0.

Nota: Não há suporte aos Serviços de Terminal da MS em conjunto com o AnyConnect Client. Você não pode executar RDP para um computador e, em seguida, iniciar uma sessão do AnyConnect. Não é possível executar RDP para um cliente que esteja conectado através do AnyConnect.

Nota: A primeira instalação do AnyConnect requer que o usuário possua privilégios de administrador (se você usar o pacote msi autônomo do AnyConnect ou enviar por push o arquivo pkg do ASA). Se o usuário não possuir privilégios de administrador, uma caixa de diálogo será exibida indicando este requisito. As atualizações subseqüentes não exigirão que o usuário que instalou o AnyConnect anteriormente possua privilégios de administrador.

Configuração

Para configurar o ASA para acesso VPN usando o AnyConnect Client, execute estes passos:

1. Configure um Certificado Auto-Emitido.
2. Carregue e Identifique a Imagem do SSL VPN Client.
3. Ative o Acesso do AnyConnect.
4. Crie uma Nova Política de Grupo.
5. Configure o Bypass da Lista de Acessos para Conexões VPN.
6. Crie um Perfil de Conexão e um Grupo de Túnel para as Conexões do AnyConnect Client.

Configure a Isenção de NAT para AnyConnect Clients.

Adicione Usuários ao Banco de Dados Local.

Passo 1. Configurar um Certificado Auto-Emitido

Por padrão, o security appliance possui um certificado auto-assinado gerado novamente cada vez que o dispositivo é reinicializado. Você pode adquirir o seu próprio certificado de fornecedores, como Verisign ou EnTrust, ou pode configurar o ASA para emitir um certificado de identidade para si mesmo. Esse certificado permanecerá o mesmo quando o dispositivo for reinicializado. Execute este passo para gerar um certificado auto-assinado que persista quando o dispositivo for reinicializado.

Procedimento do ASDM

Clique em **Configuration** e em **Remote Access VPN**.

Expanda **Certificate Management** e escolha **Identity Certificates**.

Clique em **Add** e no botão de opção **Add a new identity certificate**.

Clique em **New**.

Na caixa de diálogo Add Key Pair, clique no botão de opção **Enter new key pair name**.

Insira um nome para identificar o par de chaves.

Este exemplo usa *sslvpnkeypair*.

Clique em **Generate Now**.

Na caixa de diálogo Add Identity Certificate, verifique se o par de chaves recém-criado está selecionado.

Para Certificate Subject DN, insira o nome de domínio completamente qualificado (FQDN) que será usado para conectar à interface de término da VPN.

CN=sslvpn.cisco.com

Clique em **Advanced** e insira o FQDN usado para o campo Certificate Subject DN.

Por exemplo, **FQDN**: sslvpn.cisco.com

Clique em **OK**.

Selecione a caixa **Generate Self Signed Certificate** e clique em **Add Certificate**.

Clique em **OK**.

Clique em **Configuration** e em **Remote Access VPN**.

Expanda **Advanced** e escolha **SSL Settings**.

Na área Certificates, escolha a interface que será usada para término da VPN SSL (externa) e clique em **Edit**.

Na lista suspensa Certificate, escolha o certificado auto-assinado gerado anteriormente.

Clique em **OK** e em **Apply**.

Exemplo de 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...
!--- Gera uma chave RSA para o certificado. (O nome deve
ser exclusivo. !--- Por exemplo, sslvpnkeypair.)
ciscoasa(config)#crypto ca trustpoint localtrust
!--- Cria um trustpoint para o certificado auto-emitido.
ciscoasa(config-ca-trustpoint)#enrollment self
ciscoasa(config-ca-trustpoint)#fqdn sslvpn.cisco.com
ciscoasa(config-ca-trustpoint)#subject-name
CN=sslvpn.cisco.com
!--- O nome de domínio completamente qualificado é usado
para o fqdn e o CN. !--- O nome deve ser resolvido no
endereço IP da interface externa do ASA.
ciscoasa(config-ca-trustpoint)#keypair sslvpnkeypair
!--- A chave RSA é atribuída ao trustpoint para a
criação do certificado. 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
!--- Atribui o trustpoint a ser usado para as conexões
SSL na interface externa.
```

Passo 2. Carregar e Identificar a Imagem do SSL VPN Client

Este documento usa o AnyConnect SSL 2.0 Client. Você pode obter este cliente no Site de Download de Software da Cisco. Uma imagem separada do AnyConnect é necessária para cada sistema operacional que os usuários remotos planejam usar. Para obter mais informações, consulte as Notas de Versão do Cisco AnyConnect 2.0.

Quando você obtiver o AnyConnect Client, execute estes passos:

Procedimento do ASDM

Clique em **Configuration** e em **Remote Access VPN**.

Expanda **Network (Client) Access** e **Advanced**.

Expanda **SSL VPN** e escolha **Client Settings**.

Na área SSL VPN Client Images, clique em **Add** e em **Upload**.

Navegue para o local do qual você baixou o AnyConnect Client.

Selecione o arquivo e clique em **Upload File**.

Quando o cliente for carregado, você receberá uma mensagem indicando que o arquivo foi carregado na flash com êxito.

Clique em **OK**.

Uma caixa de diálogo será exibida para confirmar se você deseja usar a nova imagem carregada como a imagem do SSL VPN Client atual.

Clique em **OK**.

Clique em **OK** e em **Apply**.

Repita os passos nesta seção para cada pacote AnyConnect destinado a um sistema operacional específico que deseje usar.

Exemplo de 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)
!--- A imagem do AnyConnect é baixada para o ASA via
```

```
TFTP. ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#svc image disk0:/anyconnect-win-
2.0.0343-k9.pkg 1
!--- Especifica a imagem do AnyConnect que será baixada
pelos usuários. A imagem que for mais !--- baixada
deverá ter o menor número. Esta imagem usa 1 para a
imagem !--- do AnyConnect para Windows.
```

Passo 3. Ativar o Acesso do AnyConnect

Para permitir que o AnyConnect Client conecte ao ASA, você deverá ativar o acesso na interface que termina as conexões VPN SSL. Este exemplo usa a interface externa para terminar as conexões do AnyConnect.

Procedimento do ASDM

Clique em **Configuration** e em **Remote Access VPN**.

Expanda **Network (Client) Access** e escolha **SSL VPN Connection Profiles**.

Marque a caixa de seleção **Enable Cisco AnyConnect VPN Client**.

Marque a caixa de seleção **Allow Access** para a interface externa e clique em **Apply**.

Exemplo de linha de comando

ciscoasa

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable outside
ciscoasa(config-webvpn)#svc enable
!--- Permite que o AnyConnect seja enviado para
computadores remotos.
```

Passo 4. Criar uma Nova Política de Grupo

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

Procedimento do ASDM

Clique em **Configuration** e em **Remote Access VPN**.

Expanda **Network (Client) Access** e escolha **Group Policies**.

Clique em **Add**.

Escolha **General** e insira **SSLClientPolicy** no campo Name.

Desmarque a caixa de seleção **Inherit** de Address Pools.

Clique em **Select** e em **Add**.

A caixa de diálogo Add IP Pool será exibida.

Configure o pool de endereços de um intervalo de IPs que não esteja em uso na sua rede.

Este exemplo usa estes valores:

Name: SSLClientPool

Starting IP Address: 192.168.25.1

Ending IP Address: 192.168.25.50

Subnet Mask: 255.255.255.0

Clique em **OK**.

Escolha o pool recém-criado e clique em **Assign**.

Clique em **OK** e em **More Options**.

Desmarque a caixa de seleção **Inherit** de Tunneling Protocols.

Selecione **SSL VPN Client**.

No painel esquerdo, escolha **Servers**.

Desmarque a caixa de seleção **Inherit** de DNS Servers e insira o endereço IP do servidor de DNS interno que os clientes AnyConnect utilizam.

Este exemplo usa *192.168.50.5*.

Clique em **More Options**.

Desmarque a caixa de seleção **Inherit** de Default Domain.

Insira o domínio usado pela sua rede interna. Por exemplo, *tsweb.local .*

Clique em **OK** e em **Apply**.

Exemplo de linha de comando

ciscoasa

```
ciscoasa(config)#ip local pool SSLClientPool
192.168.25.1-192.168.25.50 mask 255.255.255.0
!--- Define o pool de IP. O pool de IP deve ser um
intervalo de endereços IP !--- que ainda não estejam em
uso na rede interna. ciscoasa(config)#group-policy
SSLClientPolicy internal
ciscoasa(config)#group-policy SSLClientPolicy attributes
ciscoasa(config-group-policy)#dns-server value
192.168.50.5
!--- Especifica o servidor DNS interno que será usado.
ciscoasa(config-group-policy)#vpn-tunnel-protocol svc
!--- Especifica o protocolo do túnel VPN que será usado
pela política de grupo. ciscoasa(config-group-
policy)#default-domain value tsweb.local
!--- Define o domínio padrão atribuído aos usuários da
VPN. ciscoasa(config-group-policy)#address-pools value
SSLClientPool
!--- Atribui o pool de IP criado pela política de grupo
SSLClientPolicy.
```

Passo 5. Configurar o Bypass da Lista de Acessos para Conexões VPN

Ao ativar esta opção, você permite que os clientes SSL/IPsec ignorem a lista de acessos da interface.

Procedimento do ASDM

Clique em **Configuration** e em **Remote Access VPN**.

Expanda **Network (Client) Access** e **Advanced**.

Expanda **SSL VPN** e escolha **Bypass Interface Access List**.

Verifique se a caixa de seleção **Enable inbound SSL VPN and IPSEC Sessions to bypass interface access lists** está marcada e clique em **Apply**.

Exemplo de linha de comando

ciscoasa

```
ciscoasa(config)#sysopt connection permit-vpn
!--- Ativa o desvio da lista de controle de acesso da
interface para conexões VPN. !--- Este exemplo usa o
comando vpn-filter para estabelecer o controle de
acesso.

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

Passo 6. Criar um Perfil de Conexão e um Grupo de Túnel para as Conexões do

AnyConnect Client

Quando clientes VPN se conectam ao ASA, eles se conectam a um perfil de conexão ou grupo de túnel. O grupo de túnel é usado para definir parâmetros de conexão para tipos específicos de conexões VPN, como IPsec L2L, acesso remoto IPsec, SSL sem cliente e cliente SSL.

Procedimento do ASDM

Clique em **Configuration** e em **Remote Access VPN**.

Expanda **Network (Client) Access** e **SSL VPN**.

Escolha **Connection Profiles** e clique em **Add**.

Escolha **Basic** e insira estes valores:

Name: SSLClientProfile

Authentication: LOCAL

Default Group Policy: SSLClientPolicy

Verifique se a caixa de seleção **SSL VPN Client Protocol** está marcada.

No painel esquerdo, expanda **Advanced** e escolha **SSL VPN**.

Em Connection Aliases, clique em **Add** e insira um nome ao qual os usuários possam associar suas conexões VPN. Por exemplo, *SSLVPNClient*.

Clique em **OK** e em **OK** novamente.

Na parte inferior da janela do ASDM, marque a caixa de seleção **Allow user to select connection, identified by alias in the table above at login page** e clique em **Apply**.

Exemplo de linha de comando

ciscoasa
ciscoasa(config)#**tunnel-group SSLClientProfile type remote-access** *!--- Define o grupo de túneis a ser usado para as conexões de acesso remoto de VPN.* 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
!--- Atribui um alias a um grupo de túneis.
ciscoasa(config-tunnel-webvpn)#webvpn
ciscoasa(config-webvpn)#tunnel-group-list enable
!--- Ativa a seleção de alias/grupo de túneis para as
conexões VPN SSL.
```

Passo 7. Configurar a Isenção de NAT para AnyConnect Clients

A isenção de NAT deve ser configurada para quaisquer endereços IP ou intervalos desejados para permitir que os clientes VPN SSL obtenham acesso. Neste exemplo, os clientes VPN SSL precisam de acesso somente ao IP interno 192.168.50.

Nota: Se o controle de NAT não estiver ativado, este passo não será necessário. Use o comando **show run nat-control** para verificar. Para verificar através do ASDM, clique em **Configuration**, **Firewall** e escolha **Nat Rules**. Se a caixa de seleção **Enable traffic through the firewall without address translation** estiver marcada, você poderá ignorar este passo.

Procedimento do ASDM

Clique em **Configuration** e em **Firewall**.

Escolha **Nat Rules** e clique em **Add**.

Escolha **Add NAT Exempt Rule** e insira estes valores:

Action: Exempt

Interface: inside

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)

Clique em **OK** e em **Apply**.

Exemplo de 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 a lista de acesso que será usada para as
exceções do NAT. ciscoasa(config)#nat (inside) 0 access-
list no_nat
!--- Permite conexões externas para endereços internos
!--- não convertidos definidos pela lista de acesso
no_nat. ciscoasa(config)#
```

Passo 8. Adicionar Usuários ao Banco de Dados Local

Se você utilizar a autenticação local (o padrão), será necessário definir os nomes dos usuários e as senhas no banco de dados local para autenticação do usuário.

Procedimento do ASDM

Clique em **Configuration** e em **Remote Access VPN**.

Expanda **AAA Setup** e escolha **Local Users**.

Clique em **Add** e insira estes valores:

Username: matthewp

Password: p@ssw0rd

Confirm Password: p@ssw0rd

Selecione o botão de opção **No ASDM, SSH, Telnet or Console Access**.

Clique em **OK** e em **Apply**.

Repita este passo para usuários adicionais e clique em **Save**.

Exemplo de linha de comando

ciscoasa

```
ciscoasa(config)#username matthewp password p@ssw0rd
ciscoasa(config)#username matthewp attributes
ciscoasa(config-username)#service-type remote-access
!--- Atribui o acesso de usuário remoto somente. Acesso
de SSH, Telnet e ASDM não é permitido. ciscoasa(config-
username)#write memory
!--- Salva a configuração.
```

Verificação

Use esta seção para verificar se a configuração de VPN SSL foi bem-sucedida.

Conecte ao ASA com o AnyConnect Client

Instale o cliente diretamente em um PC e conecte à interface externa do ASA ou insira https e o endereço FQDN/IP do ASA em um navegador da Web. Se você usar um navegador da Web, o cliente se instalará quando houver êxito no login.

Verifique as Conexões do SSL VPN Client

Use o comando **show vpn-sessiondb svc** para verificar os SSL VPN Clients conectados.

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

Session Type: SVC

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

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

O comando **vpn-sessiondb logoff name** *username* faz logoff de usuários pelo nome do usuário. Uma mensagem *Administrator Reset* é enviada ao usuário quando desconectado.

```
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 o AnyConnect 2.0 Client, consulte o Guia do Administrador do Cisco AnyConnect VPN.

Troubleshooting

Esta seção fornece informações que você pode usar no troubleshooting de sua configuração.

Comandos de Troubleshooting (Opcional)

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a 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** .

debug webvpn svc 255 — Exibe mensagens de depuração sobre conexões a SSL VPN Clients através de WebVPN.

Êxito no Login do 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' - !--- IP externo do 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' - !--- Versão do
AnyConnect. 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' - !---
Nome de host do desktop cliente. 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 atribuído do
pool de IP. 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
```

Falha no Login do AnyConnect (Senha Incorreta)

```
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]
```