ASA 7.2(2): Cliente VPN SSL (SVC) para os Internet públicas VPN em um exemplo de configuração da vara

Índice

Introdução

Este documento descreve como estabelecer uma ferramenta de segurança adaptável (ASA) 7.2.2 para executar SSL VPN em uma vara. Esta instalação aplica-se a um caso específico em que o ASA não permite o Split Tunneling e os usuários conectam diretamente ao ASA antes que estejam permitidos para ir ao Internet.

Note: Na versão ASA 7.2.2, a palavra-chave da intra-*relação do* comando configuration mode da **licença do same-security-traffic** permite que todo o tráfego incorpore e retire a mesma relação (não apenas tráfego de IPSec).

Pré-requisitos

Requisitos

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

- A ferramenta de segurança do hub ASA precisa de executar a versão 7.2.2
- Cisco SSL VPN Client (SVC) 1.x**Note**: Transfira o pacote do cliente VPN SSL (sslclient-win*.package) da transferência de software Cisco (clientes registrados somente). Copie o

SVC à memória Flash no ASA. O SVC deve ser transferida aos computadores do usuário remoto a fim estabelecer a conexão de VPN SSL com o ASA. Refira a instalação da seção de software SVC do *guia do comando line configuration do dispositivo do Cisco Security, versão 7.2* para mais informação.

Componentes Utilizados

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

- A ferramenta de segurança adaptável do Cisco 5500 Series (o ASA) essa executa a versão de software 7.2(2)
- Versão do Cisco SSL VPN Client para Windows 1.1.4.179
- PC que executa Windows 2000 Professional ou Windows XP
- Versão 5.2(2) do Cisco Adaptive Security Device Manager (ASDM)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Informações de Apoio

O cliente VPN SSL (SVC) é uma tecnologia de tunelamento VPN que dê a usuários remotos os benefícios de um cliente do IPSec VPN sem a necessidade para que os administradores de rede instalem e configurem clientes do IPSec VPN em computadores remotos. O SVC usa a criptografia SSL que está já atual no computador remoto assim como o início de uma sessão WebVPN e a autenticação da ferramenta de segurança.

Para estabelecer uma sessão SVC, o usuário remoto incorpora o endereço IP de Um ou Mais Servidores Cisco ICM NT de uma relação WebVPN da ferramenta de segurança ao navegador, e o navegador conecta a essa relação e indica a tela de login WebVPN. Se o usuário satisfaz o início de uma sessão e a autenticação, e a ferramenta de segurança identifica o usuário como a exigência do SVC, a ferramenta de segurança transfere o SVC ao computador remoto. Se a ferramenta de segurança identifica o usuário como tendo a opção para usar o SVC, a ferramenta de segurança transfere o SVC ao computador remoto ao apresentar um link na tela do usuário para saltar a instalação SVC.

Após a transferência, o SVC instala e configura-se, e então as sobras SVC ou desinstala-se (segundo a configuração) do computador remoto quando a conexão termina.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Note: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Note: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

Configurações ASA 7.2(2) usando o ASDM 5.2(2)

Este documento supõe as configurações básicas, tais como a configuração da interface, é já feito e de trabalho corretamente.

Note: Consulte Habilitação de Acesso HTTPS para o ASDM para permitir que o ASA seja configurado pelo ASDM.

Note: O WebVPN e o ASDM não podem ser ativados na mesma interface do ASA, a menos que você altere os números de porta. Consulte ASDM e WebVPN Habilitados na Mesma Interface do ASA para obter mais informações.

Termine estas etapas a fim configurar o SSL VPN em uma vara no ASA:

1. Escolha o **configuração > interfaces**, e verificam o **tráfego da possibilidade entre dois ou mais anfitriões conectados à mesma** caixa de **verificação de interface** a fim permitir que o tráfego SSL VPN incorpore e retire a mesma relação.
2. Clique em Apply.**Note**: Está aqui o comando de configuração de CLI equivalente:
3. Escolha a **configuração > o VPN > o gerenciamento de endereços IP > das associações IP > Add** a fim criar um pool do endereço IP de Um ou Mais Servidores Cisco ICM NT nomeado *vpnpool*.
4. Clique em Apply.**Note**: Está aqui o comando de configuração de CLI equivalente:
5. Permita o WebVPN:Escolha a **configuração > o VPN > o WebVPN > o acesso WebVPN**, e selecione a interface externa.O clique **permite**.Verifique a **lista de drop-down do grupo de túneis da possibilidade na** caixa de verificação da **página de login WebVPN** a fim permitir que os usuários escolham seus grupos respectivos da página de login.Clique em Apply.Escolha a **configuração > o VPN > o WebVPN > do cliente VPN SSL > Add** a fim adicionar a imagem do cliente VPN SSL da memória Flash do ASA.Click **OK**.Click **OK**.Clique a caixa de verificação do **cliente VPN SSL**.**Note**: Estão aqui os comandos de configuração de CLI equivalentes:
6. Configurar a política do grupo:Escolha o **> Add da configuração > da política VPN > de general > de grupo (Política interna de grupo)** a fim criar uma política interna do grupo nomeada *clientgroup*.Clique o **tab geral**, e selecione a caixa de verificação **WebVPN** a fim permitir o WebVPN como o protocolo de tunelamento.Clique a aba da **configuração de cliente**, e clique então a aba do **general Cliente Parâmetro**.Escolha o **túnel todas as redes da** lista de drop-down da política do túnel em divisão a fim fazer todos os pacotes viajar do PC remoto através de um túnel seguro.Clique **WebVPN > de cliente SSLVPN** aba, e escolha estas opções:Para a opção de VPN client do uso SSL, desmarcar a caixa de verificação

herdar, e clique o botão de rádio **opcional**.Esta opção permite que o cliente remoto escolha mesmo se transferir o SVC. O sempre bem escolhido assegura-se de que o SVC esteja transferido à estação de trabalho remota durante cada conexão de VPN SSL.Para o instalador do mantimento na opção do sistema de cliente, desmarcar a caixa de verificação **herdar**, e clique o **botão Yes Radio Button**Esta opção permite que o software SVC permaneça na máquina cliente. Consequentemente, o ASA não precisa fazer o download do software SVC para o cliente toda vez que uma conexão é feita. Esta opção é uma boa escolha para os usuários remotos que acessam frequentemente a rede corporativa.Para a opção Renegotiation Interval, desmarque a caixa **Inherit**, desmarque a caixa de seleção **Unlimited** e insira o número de minutos até a geração de uma nova chave.**Note**: A segurança é aumentada com a definição de limites no intervalo de tempo durante o qual uma chave é válida.Para a opção Renegotiation Method, desmarque a caixa de seleção **Inherit** e clique no botão de opção **SSL**.**Note**: A negociação nova pode usar o túnel atual SSL ou um túnel novo criado especificamente para a negociação nova.Seus atributos do cliente VPN SSL devem ser configurados segundo as indicações desta imagem:**A APROVAÇÃO do** clique, e clica então **aplica-se**.**Note**: Estão aqui os comandos de configuração de CLI equivalentes:

7. Escolha a **configuração > o > Add VPN > de general > de usuários** a fim criar uma conta de novo usuário *ssluser1*.
8. Clique a **APROVAÇÃO**, e clique-a então **aplicam-se**.**Note**: Está aqui o comando CLI equivalente:
9. Escolha a **configuração > as propriedades > o AAA Setup > grupos de servidores AAA > editam**.
10. Selecione o o *LOCAL do* grupo de servidor do padrão, e o clique **edita**.
11. Na caixa de diálogo do grupo de servidor local da edição, clique a caixa de verificação do **fechamento do usuário local da possibilidade**, e incorpore 16 à caixa de texto máxima das tentativas.
12. Click **OK**.**Note**: Está aqui o comando CLI equivalente:
13. Configurar o grupo de túneis:Escolha a **configuração > o > Add VPN > de general > de grupo de túneis (acesso WebVPN)** a fim criar um grupo de túneis novo nomeado *sslgroup*.Clique o **tab geral**, e clique então a aba **básica**.Escolha o **clientgroup da** lista de drop-down da política do grupo.Clique a aba da **atribuição de endereço de cliente**, e clique-a então **adicionam** a fim atribuir o *vpnpool do* pool do endereço disponível.Clique a aba **WebVPN**, e clique então a aba dos **pseudônimos e URL do grupo**.Datilografe o nome de pseudônimo na caixa do parâmetro, e o clique **adiciona** a fim adicionar-la à lista de nomes do grupo na página de login.**A APROVAÇÃO do** clique, e clica então **aplica-se**.**Note**: Estão aqui os comandos de configuração de CLI equivalentes:
14. Configurar o NAT:Escolha a **configuração > a regra dinâmica do > Add NAT do > Add NAT** para permitir o tráfego que vem da rede interna a ser traduzida com o uso do endereço IP externo 172.16.1.5.Click **OK**.Escolha a **configuração > a regra dinâmica do > Add NAT do > Add NAT** para permitir o tráfego que vem da rede externa 192.168.10.0 a ser traduzido com o uso do endereço IP externo 172.16.1.5.Click **OK**.Clique em Apply.**Note**: Estão aqui os comandos de configuração de CLI equivalentes:

Configuração de CLI ASA 7.2(2)

Cisco ASA 7.2(2)

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter
!--- and exit the same interface. access-list 100
extended permit icmp any any pager lines 24 mtu inside
1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254

!--- The address pool for the SSL VPN Clients. no
failover icmp unreachable rate-limit 1 burst-size 1 asdm
image disk0:/asdm-522.bin no asdm history enable arp
timeout 14400 global (outside) 1 172.16.1.5

!--- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP. nat (inside) 1 0.0.0.0 0.0.0.0

!--- The NAT statement to define what to encrypt !---
(the addresses from vpn-pool). nat (outside) 1
192.168.10.0 255.255.255.0

access-group 100 in interface outside
```

```
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal

!--- Create an internal group policy "clientgroup."
group-policy clientgroup attributes
 vpn-tunnel-protocol webvpn

!--- Enable webvpn as tunneling protocol. split-tunnel-
policy tunnelall

!--- Encrypt all the traffic coming from the SSL VPN
Clients. webvpn
  svc required

!--- Activate the SVC under webvpn mode svc keep-
installer installed

!--- When the security appliance and the SVC perform a
rekey, they renegotiate !--- the crypto keys and
initialization vectors, increasing the security of !---
the connection. svc rekey time 30

--- Command that specifies the number of minutes from
the start of the !--- session until the rekey takes
place, from 1 to 10080 (1 week).  svc rekey method ssl

!--- Command that specifies that SSL renegotiation takes
place during SVC rekey. username ssluser1 password
ZRhW85jZqEaVd5P. encrypted

!--- Create an user account "ssluser1." aaa local
authentication attempts max-fail 16

!--- Enable the AAA local authentication. http server
enable http 0.0.0.0 0.0.0.0 inside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart tunnel-
group sslgroup type webvpn

!--- Create a tunnel group "sslgroup" with type as
WebVPN. tunnel-group sslgroup general-attributes
 address-pool vpnpool

!--- Associate the address pool vpnpool created.
default-group-policy clientgroup

!--- Associate the group policy "clientgroup" created.
tunnel-group sslgroup webvpn-attributes

 group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users. telnet
timeout 5 ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
```

```
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
webvpn
 enable outside

!--- Enable WebVPN on the outside interface. svc image
disk0:/sslclient-win-1.1.4.179.pkg 1

!--- Assign an order to the SVC image. svc enable

!--- Enable the security appliance to download SVC
images to remote computers. tunnel-group-list enable

!--- Enable the display of the tunnel-group list on the
WebVPN Login page. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa#
```

Estabeleça a conexão VPN SSL com o SVC

Termine estas etapas a fim estabelecer uma conexão de VPN SSL com ASA.

1. Datilografe dentro ao campo de endereço de seu navegador da Web a URL ou o endereço IP de Um ou Mais Servidores Cisco ICM NT para a relação WebVPN do ASA.Por exemplo:

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
```

```
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter !--- and exit the same interface.
access-list 100 extended permit icmp any any pager lines 24 mtu inside 1500 mtu outside
1500 ip local pool vpnpool 192.168.10.1-192.168.10.254

!--- The address pool for the SSL VPN Clients. no failover icmp unreachable rate-limit 1
burst-size 1 asdm image disk0:/asdm-522.bin no asdm history enable arp timeout 14400 global
(outside) 1 172.16.1.5

!--- The global address for Internet access used by VPN Clients. !--- Note: Uses an RFC
1918 range for lab setup. !--- Apply an address from your public range provided by your
ISP. nat (inside) 1 0.0.0.0 0.0.0.0

!--- The NAT statement to define what to encrypt !--- (the addresses from vpn-pool). nat
(outside) 1 192.168.10.0 255.255.255.0

access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal

!--- Create an internal group policy "clientgroup." group-policy clientgroup attributes
 vpn-tunnel-protocol webvpn

!--- Enable webvpn as tunneling protocol. split-tunnel-policy tunnelall

!--- Encrypt all the traffic coming from the SSL VPN Clients. webvpn
  svc required

!--- Activate the SVC under webvpn mode svc keep-installer installed

!--- When the security appliance and the SVC perform a rekey, they renegotiate !--- the
crypto keys and initialization vectors, increasing the security of !--- the connection. svc
rekey time 30

--- Command that specifies the number of minutes from the start of the !--- session until
the rekey takes place, from 1 to 10080 (1 week).  svc rekey method ssl

!--- Command that specifies that SSL renegotiation takes place during SVC rekey. username
ssluser1 password ZRhW85jZqEaVd5P. encrypted

!--- Create an user account "ssluser1." aaa local authentication attempts max-fail 16

!--- Enable the AAA local authentication. http server enable http 0.0.0.0 0.0.0.0 inside no
snmp-server location no snmp-server contact snmp-server enable traps snmp authentication
linkup linkdown coldstart tunnel-group sslgroup type webvpn

!--- Create a tunnel group "sslgroup" with type as WebVPN. tunnel-group sslgroup general-
attributes
 address-pool vpnpool

!--- Associate the address pool vpnpool created. default-group-policy clientgroup

!--- Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-
```

```
attributes

 group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console
timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map
type inspect dns preset_dns_map parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323
h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp
inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy
global_policy global webvpn
 enable outside

!--- Enable WebVPN on the outside interface. svc image disk0:/sslclient-win-1.1.4.179.pkg 1

!--- Assign an order to the SVC image. svc enable

!--- Enable the security appliance to download SVC images to remote computers. tunnel-
group-list enable

!--- Enable the display of the tunnel-group list on the WebVPN Login page. prompt hostname
context Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end ciscoasa#
```

2. Incorpore o seu nome de usuário e a senha, e escolha então seu grupo respectivo da lista de drop-down do grupo.**Note**: O software de ActiveX deve ser instalado em seu computador antes que você transfira o cliente VPN SSL.Esta caixa de diálogo aparece enquanto a conexão é estabelecida:Esta mensagem aparece uma vez que a conexão é estabelecida:
3. Uma vez que a conexão é estabelecida, fazer duplo clique o ícone chave amarelo que aparece na barra de tarefas de seu computador.A caixa de diálogo do cliente VPN do Cisco Systems SSL indica a informação sobre a conexão SSL.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

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.

- **show webvpn svc** — Mostra as imagens do SVC armazenadas na memória flash do ASA.

```
ciscoasa#show webvpn svc
1. disk0:/sslclient-win-1.1.4.179.pkg 1
  CISCO STC win2k+ 1.0.0
  1,1,4,179
  Fri 01/18/2008 15:19:49.43

1 SSL VPN Client(s) installed
```

- **show vpn-sessiondb svc** — Mostra informações sobre as conexões SSL atuais.

```
ciscoasa#show vpn-sessiondb svc

Session Type: SVC

Username     : ssluser1
Index        : 1
Assigned IP  : 192.168.10.1           Public IP    : 192.168.1.1
Protocol     : SVC                    Encryption   : 3DES
Hashing      : SHA1
Bytes Tx     : 131813                 Bytes Rx     : 5082
```

```
Client Type  : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Client Ver   : Cisco Systems SSL VPN Client 1, 1, 4, 179
Group Policy : clientgroup
Tunnel Group : sslgroup
Login Time   : 12:38:47 UTC Mon Mar 17 2008
Duration     : 0h:00m:53s
Filter Name  :
```

- **show webvpn group-alias** — Exibe o alias configurado para vários grupos.

```
ciscoasa#show webvpn group-alias
Tunnel Group: sslgroup   Group Alias: sslgroup_users enabled
```

- No ASDM, escolha a **monitoração > o VPN > as estatísticas de VPN > as sessões** a fim ver a informação sobre as sessões de VPN da Web atuais no ASA.

Troubleshooting

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

- **<username> do nome do fazer logoff VPN-sessiondb** — Permite que você termine a sessão de VPN SSL para o nome de usuário especificado.

```
ciscoasa#vpn-sessiondb logoff name ssluser1
Called vpn_remove_uauIth: success!
webvpn_svc_np_tear_down: no ACL
NFO: Number of sessions with name "ssluser1" logged off : 1
```

  Similarmente, você pode usar o **fazer logoff svc do** comando **VPN-sessiondb** a fim terminar todas as sessões SVC.**Note**: Se o PC entrar no modo de espera ou hibernação, a conexão VPN SSL poderá ser encerrada.

```
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got message
SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, etc)
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
```

```
ciscoasa#show vpn-sessiondb svc
INFO: There are presently no active sessions
```

- **Debugar o webvpn svc <1-255>** — Fornece os eventos do tempo real WebVPN a fim estabelecer a sessão.

```
Ciscoasa#debug webvpn svc 7

ATTR_CISCO_AV_PAIR: got SVC ACL: -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: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4, 179'
Processing CSTP header line: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4,
179'
Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179'
```

```
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: tacweb'
Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb'
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: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486
D5BC554D2'
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1
CF236DB5E8BE70B1486D5BC554D2'
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1
486D5BC554D2'
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B
C554D2'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
CSTP state = HAVE_ADDRESS
No subnetmask... must calculate it
SVC: NP setup
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC: adding to sessmgmt
SVC: Sending response
CSTP state = CONNECTED
```

- No ASDM, escolha a **monitoração > registrando > Log Viewer > opinião do tempo real** a fim ver os eventos de tempo real. Estes exemplos mostram a informação de sessão entre o SVC 192.168.10.1 e web server 10.2.2.2 no Internet através de ASA 172.16.1.5.

Informações Relacionadas

- Página de Suporte do Cisco 5500 Series Adaptive Security Appliance
- Exemplo de Configuração de PIX/ASA 7.x e VPN Client para VPN de Internet Pública "on a Stick"
- Exemplo de Configuração de Cliente VPN SSL (SVC) no ASA com o ASDM
- Suporte Técnico e Documentação - Cisco Systems