

ASA 7.1/7.2: Permita o Split Tunneling para o SVC no exemplo de configuração ASA

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações ASA usando o ASDM 5.2\(2\)](#)

[Configuração ASA 7.2\(2\) usando o CLI](#)

[Estabeleça a conexão VPN SSL com o SVC](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento fornece instruções passo a passo em como permitir aos clientes VPN do Secure Socket Layer (SSL) (SVC) o acesso ao Internet quando forem escavados um túnel em uma ferramenta de segurança adaptável de Cisco (ASA). Esta configuração permite o acesso seguro SVC aos recursos corporativos com o SSL e dá o acesso inseguro ao Internet com o uso do Split Tunneling.

A capacidade de transmitir tráfego protegido e não protegido na mesma interface é conhecida como tunelamento dividido. O Split Tunneling exige que você especifica exatamente que o tráfego é fixado e o que o destino desse tráfego é, de modo que somente o tráfego especificado incorpore o túnel, quando o resto for transmitido unencrypted através da rede pública (Internet).

[Pré-requisitos](#)

[Requisitos](#)

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

- Privilégios administrativos locais em todas as estações de trabalho remota
- Javas e controles activex na estação de trabalho remota
- A porta 443(SSL) não é obstruída em qualquer lugar ao longo do caminho de conexão

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**Nota:** Transfira o pacote do cliente VPN SSL (sslclient-win*.package) da [transferência de software Cisco \(clientes registrados somente\)](#). Copie o SVC à memória Flash do ASA, que deve ser transferida aos computadores do usuário remoto a fim estabelecer a conexão de VPN SSL com ASA. Refira a [instalação da seção de software SVC do](#) manual de configuração ASA para mais informação.
- PC que executa o Windows 2000 SP4 profissional ou Windows XP SP2
- 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.

A fim 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 você satisfaz o início de uma sessão e a autenticação, e a ferramenta de segurança o identifica como a exigência do SVC, a ferramenta de segurança transfere o SVC ao computador remoto. Se a ferramenta de segurança o identifica com a opção para usar o SVC, a ferramenta de segurança transfere o SVC ao computador remoto quando apresentar um link no indicador para saltar a instalação SVC.

Depois que você transferência, o SVC instala e se configura, e então as sobras SVC ou se desinstala, que depende da configuração, do computador remoto quando a conexão terminar.

Configurar

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

Nota: 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:

Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do [RFC 1918](#) que foram usados em um ambiente de laboratório.

Configurações ASA usando o ASDM 5.2(2)

Termine estas etapas a fim configurar como mostrado o SSL VPN no ASA com Split Tunneling:

1. O documento supõe que a configuração básica tal como a configuração da interface já está feita e assim por diante e trabalha corretamente. **Nota:** Consulte [Habilitação de Acesso HTTPS para o ASDM](#) para permitir que o ASA seja configurado pelo ASDM. **Nota:** 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.
2. Escolha a **configuração > o VPN > o gerenciamento de endereços IP > as associações IP** a fim criar um pool do endereço IP de Um ou Mais Servidores Cisco ICM NT: `vpnpool` para clientes VPN. Clique em **Apply**.
3. **Permita o WebVPN** Escolha a **configuração > o VPN > o WebVPN > o acesso WebVPN** e destaque a interface externa com o rato e o clique **permite**. A verificação **permite a lista de drop-down do grupo de túneis** na caixa de verificação da **página de login WebVPN** a fim permitir a gota parece para baixo na página de login para usuários, escolher seus grupos respectivos. 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 como mostrada. Clique em **OK**. Clique em **OK**. Clique a caixa de verificação do **cliente VPN SSL**. Clique em **Apply**. **Configuração via CLI Equivalente:**
4. **Configurar a política do grupo** Escolha o **> Add da configuração > da política VPN > de general > de grupo (Política interna de grupo)** a fim criar um **clientgroup** interno da política do grupo. Sob o **general**, escolha a caixa de verificação **WebVPN** a fim permitir o WebVPN como o protocolo de tunelamento. Na aba da **configuração de cliente > do general Cliente Parâmetro**, desmarcar a caixa **herdar** para a política do túnel em divisão e escolha a **lista da rede de túnel abaixo da** lista de drop-down. Desmarcar a caixa **herdar** para o **liste de redes do túnel em divisão** e clique-a então **controlam** a fim lançar o gerente ACL. No ACL Manager, selecione **Add > Add ACL...** para criar uma nova lista de acesso. Forneça um nome para a ACL e clique em **OK**. Uma vez que o nome da ACL é criado, escolha **Add > Add ACE** para adicionar uma entrada de controle de acesso (ACE). Defina a ACE que corresponde à LAN por trás do ASA. Neste caso, a rede é 10.77.241.128/26 e escolhe a **licença**. Clique em **OK** para sair do ACL Manager. Seja certo que o ACL que você apenas criou está selecionado para o **liste de redes do túnel em divisão**. Clique em **OK** para retornar à configuração da Política de Grupo. Na página principal, o clique **aplica-se** e **envia-se** então (se for necessário) a fim enviar os comandos ao ASA. Para a opção de VPN client do uso SSL, desmarcar a caixa de verificação **herdar** e clique o botão de rádio **opcional**. Esta escolha permite que o cliente remoto escolha se clicar **WebVPN > de cliente SSLVPN** aba, e escolher estas

opções: Não transfira 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 a opção **Keep Installer on Client System**, desmarque a caixa de seleção **Inherit** e clique no botão de opção **Yes**. Esta ação permite que o software SVC permaneça na máquina cliente; conseqüentemente, o ASA não está exigido para transferir o software SVC ao cliente cada 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. A Segurança é aumentada quando você ajusta os limites no intervalo de tempo que uma chave é válida. Para a opção **Renegotiation Method**, desmarque a caixa de seleção **Inherit** e clique no botão de opção **SSL**. A renegociação pode utilizar o túnel SSL existente ou um túnel novo criado especificamente para a renegociação. Seus atributos do cliente VPN SSL devem ser configurados segundo as indicações desta imagem: Clique em **OK** e, em seguida, em **Apply**. **Configuração via CLI**

Equivalente:

5. Escolha a **configuração > o > Add VPN > de general > de usuários** a fim criar uma conta de novo usuário **ssluser1**. Clique em **OK** e, em seguida, em **Apply**. **Configuração via CLI**

Equivalente:

6. Escolha a **configuração > as propriedades > o AAA Setup > grupos de servidores AAA > editam** a fim alterar o grupo de servidor de padrão **LOCAL** e escolher a caixa de verificação do **fechamento do usuário local da possibilidade** com valor máximo das tentativas como **16**. **Configuração via CLI** **Equivalente:**

7. **Configurar o grupo de túneis** Escolha a **configuração > o > Add VPN > de general > de grupo de túneis (acesso WebVPN)** a fim criar um **sslgroup** novo do grupo de túneis. Na aba **geral > básica**, escolha a política do grupo como o **clientgroup** da lista de drop-down. Geralmente a aba da **atribuição de endereço de cliente**, sob conjuntos de endereços, clique **adiciona >>** a fim atribuir o **vpnpool** do pool do endereço disponível. No **o WebVPN > dos pseudônimos e URL do grupo** aba, datilografam o nome de pseudônimo na caixa do parâmetro e o clique **adiciona >>** a fim fazê-la aparecer na lista de nomes do grupo na página de login. Clique em **OK** e, em seguida, em **Apply**. **Configuração via CLI** **Equivalente:**

8. **Configurar o NAT** Escolha a **configuração > a regra dinâmica do > Add NAT do > Add NAT** para o tráfego que vem da rede interna que pode ser traduzida com o endereço IP externo **172.16.1.5**. Clique a **APROVAÇÃO** e o clique **aplica-se** na página principal. **Configuração via CLI** **Equivalente:**

9. **Configurar a NAT-isenção para o tráfego de retorno do interior da rede ao cliente**

```
ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0
```

```
ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0 ciscoasa(config)#nat (inside) 0 access-list nonat
```

[Configuração ASA 7.2\(2\) usando o CLI](#)

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 access-list split-tunnel standard
permit 10.77.241.128 255.255.255.192 !--- ACL for Split
Tunnel network list for encryption. access-list nonat
permit ip 10.77.241.0 192.168.10.0 access-list nonat
permit ip 192.168.10.0 10.77.241.0 !--- ACL to define
the traffic to be exempted from NAT. 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) 0 access-list
nonat !--- The traffic permitted in "nonat" ACL is
exempted from NAT. nat (inside) 1 0.0.0.0 0.0.0.0
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
tunnelspecified split-tunnel-network-list value split-
tunnel !--- Encrypt the traffic specified in the split
tunnel ACL only. 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, !--- and increase 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
esmtplib 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 a URL ou o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação WebVPN do ASA em seu navegador da Web no formato como mostrado. `https://url` OU `https://<IP address of the ASA WebVPN interface>`
2. Incorpore seu nome de usuário e senha e escolha então seu grupo respectivo da lista de gota para baixo como mostrado.
3. O software de ActiveX deve ser instalado em seu computador antes da transferência o SVC.
4. Estes indicadores aparecem antes que a conexão de VPN SSL esteja estabelecida.
5. Você pode obter estes indicadores uma vez que a conexão é estabelecida.
6. Clique a chave amarela que aparece na barra de tarefas de seu computador. Estes indicadores aparecem que dá a informação sobre a conexão SSL. Por exemplo, **192.168.10.1** é o IP atribuído para o cliente e servidor que o endereço IP de Um ou Mais Servidores Cisco ICM NT é 172.16.1.1, **Split Tunneling é permitido**, e assim por diante. Você pode igualmente verificar a rede assegurada que deve ser cifrada pelo SSL, o liste de redes é transferido da lista de acessos do túnel em divisão configurada no ASA. Neste exemplo, o cliente VPN SSL fixa o acesso a 10.77.241.128/24 quando todo tráfego restante não for cifrado e não é enviado através do túnel.

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 saber 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.

1. **vpn-sessiondb logoff name <username>** — Comando para desconectar a sessão VPN SSL

para o nome de usuário específico. `ciscoasa#vpn-sessiondb logoff name ssluser1` Called `vpn_remove_uauth: success!` `webvpn_svc_np_tear_down: no ACL NFO: Number of sessions with name "ssluser1" logged off : 1` De forma semelhante, você pode utilizar o comando **vpn-sessiondb logoff svc** para encerrar todas as sessões do SVC.

2. **Nota:** 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

3. **depurar o webvpn svc <1-255>** — Fornece os eventos tempo real do WebVPN a fim de

estabelecer a sessão. `Ciscoasa#debug webvpn svc 7` ATTR_CISCO_AV_PAIR: got SVC ACL: -1 `webvpn_rx_data_tunnel_connect CSTEP 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 CSTEP 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 CSTEP 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-CSTEP-Version: 1' Processing CSTEP header line: 'X-CSTEP-Version: 1' Setting version to '1' webvpn_cstp_parse_request_field() ...input: 'X-CSTEP-Hostname: tacweb' Processing CSTEP header line: 'X-CSTEP-Hostname: tacweb' Setting hostname to: 'tacweb' webvpn_cstp_parse_request_field() ...input: 'X-CSTEP-Accept-Encoding: deflate;q=1.0' Processing CSTEP header line: 'X-CSTEP-Accept-Encoding: deflate;q=1.0' webvpn_cstp_parse_request_field() ...input: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486 D5BC554D2' Processing CSTEP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5BC554D2' Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1 486D5BC554D2' WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B C554D2' Validating address: 0.0.0.0 CSTEP state = WAIT_FOR_ADDRESS webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0 CSTEP 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 CSTEP state = CONNECTED`

4. No ASDM, selecione **Monitoring > Logging > Real-time Log Viewer > View** para ver os eventos em tempo real. Estas mostras do exemplo sobre a informação de sessão entre o SVC 192.168.10.1 e web server 10.2.2.2 no Internet com ASA 172.16.1.5.

Informações Relacionadas

- [Sustentação do produto adaptável da ferramenta de segurança do Cisco 5500 Series](#)
- [ASA/PIX: Exemplo de Configuração de Habilitação do Tunelamento Dividido for VPN Clients no ASA](#)
- [Exemplo de Configuração de Roteador que Permite Clientes VPN se Conectarem via IPsec e à Internet Usando a Separação de Túneis](#)

- [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](#)