ASA 8.X: Exemplo de Configuração de Roteamento de Tráfego VPN SSL através de Gateway Padrão em Túneis

Contents

Introduction Prerequisites Requirements Componentes Utilizados Conventions Informações de Apoio Configurar Diagrama de Rede Configuração do ASA com o ASDM 6.1(5) Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento descreve como configurar o Adaptive Security Appliance (ASA) para rotear o tráfego de SSL VPN através de um gateway padrão em túnel (TDG). Quando você cria uma rota padrão com a opção de túnel, todo o tráfego de um túnel terminando no ASA que não pode ser roteado usando rotas aprendidas ou estáticas é enviado para essa rota. Para o tráfego que sai de um túnel, essa rota substitui qualquer outra rota padrão configurada ou aprendida.

Prerequisites

Requirements

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

- ASA executado na versão 8.x
- Cisco SSL VPN Client (SVC) 1.xObservação: faça o download do pacote SSL VPN Client (sslclient-win*.pkg) do <u>Cisco Software Download</u> (<u>somente</u> clientes<u>registrados</u>). Copie o SVC para a memória flash no ASA. O SVC precisa ser baixado para os computadores do usuário remoto para estabelecer a conexão VPN SSL com o ASA.

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

- Cisco 5500 Series ASA que executa a versão de software 8.x
- Versão do Cisco SSL VPN Client para Windows 1.1.4.179
- PC com Windows 2000 Professional ou Windows XP
- Cisco Adaptive Security Device Manager (ASDM) versão 6.1(5)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Informações de Apoio

O SSL VPN Client (SVC) é uma tecnologia de tunelamento VPN que oferece aos usuários remotos os benefícios de um cliente VPN IPSec sem a necessidade de administradores de rede instalarem e configurarem clientes VPN IPSec em computadores remotos. O SVC usa a criptografia SSL que já está presente no computador remoto, bem como o login e a autenticação do WebVPN do Security Appliance.

No cenário atual, há um cliente VPN SSL conectando-se aos recursos internos por trás do ASA através do túnel VPN SSL. O split-tunnel não está ativado. Quando o cliente VPN SSL estiver conectado ao ASA, todos os dados serão encapsulados. Além de acessar os recursos internos, o critério principal é rotear esse tráfego encapsulado por meio do Gateway túnel padrão (DTG).

Você pode definir uma rota padrão separada para o tráfego em túnel junto com a rota padrão. O tráfego não criptografado recebido pelo ASA, para o qual não há rota estática ou aprendida, é roteado através da rota padrão. O tráfego criptografado recebido pelo ASA, para o qual não há rota estática ou aprendida, será passado ao DTG definido através da rota padrão encapsulada.

Para definir uma rota padrão encapsulada, use este comando:

route <if_name> 0.0.0.0 0.0.0.0 <gateway_ip> tunneled

<u>Configurar</u>

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:



Neste exemplo, o SSL VPN Client acessa a rede interna do ASA através do túnel. O tráfego destinado a destinos diferentes da rede interna também é encapsulado, pois não há nenhum túnel dividido configurado, e é roteado através do TDG (192.168.100.20).

Depois que os pacotes são roteados para o TDG, que é o Roteador 2 nesse caso, ele executa a conversão de endereço para rotear esses pacotes antes da Internet. Para obter mais informações sobre como configurar um roteador como um gateway de Internet, consulte <u>Como configurar um roteador Cisco por trás de um modem a cabo não Cisco</u>.

Configuração do ASA com o ASDM 6.1(5)

Este documento pressupõe que as configurações básicas, como a configuração da interface, estão completas e funcionam corretamente.

Observação: consulte <u>Permitindo Acesso HTTPS para ASDM</u> para obter informações sobre como permitir que o ASA seja configurado pelo ASDM.

Observação: WebVPN e ASDM não podem ser habilitados na mesma interface do ASA a menos que você altere os números de porta. Consulte <u>ASDM e WebVPN Habilitados na Mesma Interface</u> <u>do ASA para obter mais informações.</u>

Conclua estes passos para configurar a VPN SSL usando o Assistente de VPN SSL.

1. No menu Assistentes, escolha Assistente de VPN

le	View	Tools	Wizards	Window Help	
MICE FISC	Home Cor Home	Sta IPs(SSL Higt	rtup Wizard ec VPN Wizard VPN Wizard n Availability and Scalability Wizard	n 💽 Back 🕥 Forward 🦓 Help	
	Devi	ce Into	Pac	ket Capture Wizard	

2. Clique na caixa de seleção **Cisco SSL VPN Client** e clique em **Next**.



 Insira um nome para a conexão no campo Nome da conexão e escolha a interface que está sendo usada pelo usuário para acessar a VPN SSL na lista suspensa Interface VPN SSL.

🖆 SSL VPN Wizard	
SSL VPN Wizard	SSL VPN Interface (Step 2 of 6)
	Provide a connection name and the interface that SSL VPN users connect to. Connection Name: Test The interface users access for SSL VPN connections. SSL VPN Interface: Outside Digital Certificate
	When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA. Certificate: None
A AND	Connection Group Alias/URU Display Group Alias list at the login page
	Information URL to access SSL VPN Service: https://209.165.201.2 URL to access ASDM: https://209.165.201.2/admin
1	<u>≤Back</u> <u>Next</u> > Fish <u>Cancel</u> <u>H</u> elp

- 4. Clique em Next.
- 5. Escolha um modo de autenticação e clique em **Avançar**. (Este exemplo usa autenticação local.)

🖆 SSL VPN Wizard		X
SSL VPN Wizard	User Authentication (Step 3 of 6)	-
	The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login. AAA Server Group Name: AAA Server Group Name: AAA Server Group Name: Authenticate using the local user database User to be Added Beename: Cisco Password: Confirm Password: Confirm Password:	
	Seck Next > Cinish Cancel	qle

6. Crie uma nova política de grupo diferente da política de grupo padrão existente.

🐔 SSL VPN Wizard			
SSL VPN Wizard	Group Policy (Step 4 of 6)		
2 D	A group policy is a collection of user- policy, all users are members of the default group policy lets users inherit policy or username level.	oriented attribute/value pa default group policy (Dfl:Grj t attributes that you have r	irs. Unless assigned to a specific group Policy). Therefore, configuring the not configured at the individual group
6 6	Create new group policy	grppolicy	\triangleright
	O Modify existing group policy	DFRGrpPolicy	
B.			
		<u>≤</u> Back Ne	xt > nish Cancel Help

7. Crie um novo pool de endereços que serão atribuídos aos PCs clientes VPN SSL quando eles forem



Um pool do intervalo 192.168.10.40-192.168.10.50 foi criado pelo nome

Name:	newpool
Starting IP Address:	192.168.10.40
Ending IP Address:	192.168.10.50
Subnet Mask:	255.255.255.0

newpool.

8. Clique em **Procurar** para escolher e carregar a imagem do SSL VPN Client na memória flash

ASA.				
SSL VPN Wizard				
SSL VPN Wizard	IP Address Pools an	d Client Image - Any	Connect VPN Clier	t Connections Only (Step 5 of 6)
	The security appliand client self-instals, us to resources on a cou IP Address Pool Create a new add from the pool when	e downloads the AnyCo es SSL or DTLS encryptio porate network. The re ess pool or select an ex in they connect.	nnect VPN Client to on for the duration o mote PC becomes pa isting address pool. I	emote users when they connect. The f the connection, and allows full access rt of the corporate network. Remote PCs are assigned addresses
	IP Address Pool:	newpool	× [New
	Address Pool Rang	e: 192.168.10.40 - 1	92.168.10.50	
	AnyConnect VPN Clie	nt Image Location		
- ista	Identify a file in fla the file and loads i	sh memory as an AnyCo into cache memory for	onnect VPN Client inv downloading to rema	ige. The security appliance expands
-Itt	Location:		([8	rowse
	E Download latest A	nyConnect VPN Client fr	om Cisco.com	
			≤ Back Next	> Einish Gancel Help

9. Clique em **Carregar** para definir o caminho do arquivo do diretório local da máquina.

do

📬 Add SSL VPN Clie	ent Image			
AnyConnect Image:				Browse Flash
	ок	Cancel	Help	

10. Clique em **Procurar arquivos locais** para selecionar o diretório onde o arquivo sslclient.pkg existe.

📧 Upload Image	
Upload a file from local c few minutes. Please wai	omputer to flash file system on the device. The upload process might take a for the operation to finish.
Local File Path:	Browse Local Files
Flash File System Path:	Browse Flash
1	Upload File Close Help

11. Clique em **Carregar arquivo** para carregar o arquivo selecionado na flash do ASA.

🖆 Upload Image 🛛 🛛 🔀
Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish.
Local File Path: C:\Documents and Settings\jtammera\My Docum Browse Local Files
Flash File System Path: disk0:/sslclient-win-1.1.4.179.pkg Browse Flash
Upload File Close Help
💰 Status 🛛 🔀
Please wait while ASDM is uploading the file. The upload process may take a few minutes. 77% Completed transfer of 360,448 bytes out of 418,765 bytes
🖆 Information
File has been uploaded to flash successfully.
ОК

12. Quando o arquivo for carregado na flash do ASA, clique em **OK** para concluir essa tarefa.

Browse Flash
Upload

 Agora, ele mostra o mais recente arquivo pkg do anyconnect carregado na memória flash do ASA. Clique em



 O resumo da configuração do cliente VPN SSL é mostrado. Clique em Concluir para concluir o assistente.

SSL VPN Wizard	Summary (Step 6 of 6)	
	You have created a SSL VPN connection with following attributes: Selected Features: SSL VPN Client Connection Name: Test SSL VPN Interface: outside User Authentication: LOCAL Group Policy: grppolicy IP Address Pool: newpool SSL VPN Client Location: disk0;/sslclient-win-1.1.4.179.pkg	

A configuração mostrada no ASDM se refere principalmente à configuração do SSL VPN Client Wizard.

Na CLI, você pode observar algumas configurações adicionais. A configuração completa da CLI é mostrada abaixo e comandos importantes foram destacados.

ciscoasa ciscoasa#show running-config : Saved : ASA Version 8.0(4) ! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif outside security-level 0 ip address 209.165.201.2 255.255.254 ! interface Ethernet0/1 nameif inside security-level 100 ip address 192.168.100.2 255.255.255.0 ! interface Ethernet0/2 nameif manage security-level 0 ip address 10.1.1.1 255.255.255.0

```
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
interface Ethernet0/4
shutdown
no nameif
no security-level
no ip address
1
interface Ethernet0/5
shutdown
no nameif
no security-level
no ip address
1
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list nonat extended permit ip 192.168.100.0
255.255.255.0 192.168.10.0 255.255.255.0
access-list nonat extended permit ip 192.168.10.0
255.255.255.0 192.168.100.0 255.255.255.0
!--- ACL to define the traffic to be exempted from NAT.
no pager logging enable logging asdm informational mtu
outside 1500 mtu inside 1500 mtu manage 1500 !---
Creating IP address block to be assigned for the VPN
clients ip local pool newpool 192.168.10.40-
192.168.10.50 mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-615.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
!--- The traffic permitted in "nonat" ACL is exempted
from NAT. nat (inside) 1 192.168.100.0 255.255.255.0
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
!--- Default route is configured through "inside"
interface for normal traffic. route inside 0.0.0.0
0.0.0.0 192.168.100.20 tunneled
!--- Tunneled Default route is configured through
"inside" interface for encrypted traffic ! 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 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy http
server enable
!--- Configuring the ASA as HTTP server. http 10.1.1.0
255.255.255.0 manage
!--- Configuring the network to be allowed for ASDM
access. ! !--- Output is suppressed ! telnet timeout 5
ssh timeout 5 console timeout 0 threat-detection basic-
threat threat-detection statistics access-list ! 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 ! !--- Output suppressed !
webvpn
enable outside
!--- Enable WebVPN on the outside interface svc image
disk0:/sslclient-win-1.1.4.179.pkg 1
!--- Assign the AnyConnect SSL VPN Client image to be
used svc enable
!--- Enable the ASA to download SVC images to remote
computers group-policy grppolicy internal
!--- Create an internal group policy "grppolicy" group-
policy grppolicy attributes
VPN-tunnel-protocol svc
!--- Specify SSL as a permitted VPN tunneling protocol !
username cisco password ffIRPGpDS0Jh9YLq encrypted
privilege 15
!--- Create a user account "cisco" tunnel-group Test
type remote-access
!--- Create a tunnel group "Test" with type as remote
access tunnel-group Test general-attributes
address-pool newpool
!--- Associate the address pool vpnpool created default-
group-policy grppolicy
!--- Associate the group policy "clientgroup" created
prompt hostname context
Cryptochecksum:1b247197c8ff70ee4432c13fb037854e : end
ciscoasa#
```

Verificar

Os comandos fornecidos nesta seção podem ser usados para verificar essa configuração.

A <u>Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados</u> <u>comandos show.</u> Use a OIT para exibir uma análise da saída do comando show.

- show webvpn svc Exibe as imagens SVC armazenadas na memória flash do ASA.
- show vpn-sessiondb svc Mostra informações sobre as conexões SSL atuais.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Suporte do Cisco 5500 Series Adaptive Security Appliance
- Exemplo de configuração PIX/ASA e VPN Client para VPN de Internet Pública em um Stick
- Exemplo de Configuração de Cliente VPN SSL (SVC) no ASA com o ASDM
- Suporte Técnico e Documentação Cisco Systems