ASA 8.X: Permitir que o aplicativo de usuário seja executado com o restabelecimento do túnel L2L VPN

Contents

Introduction

Este documento fornece informações sobre o recurso Fluxos encapsulados de IPSec persistentes e como manter o fluxo de TCP sobre a interrupção de um túnel VPN.

Prerequisites

Requirements

Os leitores deste documento devem ter uma compreensão básica de como a VPN funciona. Consulte estes documentos para obter outras informações:

- Exemplo de configuração de VPN L2L
- VPN L2L com ASA

Componentes Utilizados

As informações neste documento são baseadas no Cisco Adaptive Security Appliance (ASA) com a versão 8.2 e posterior.

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

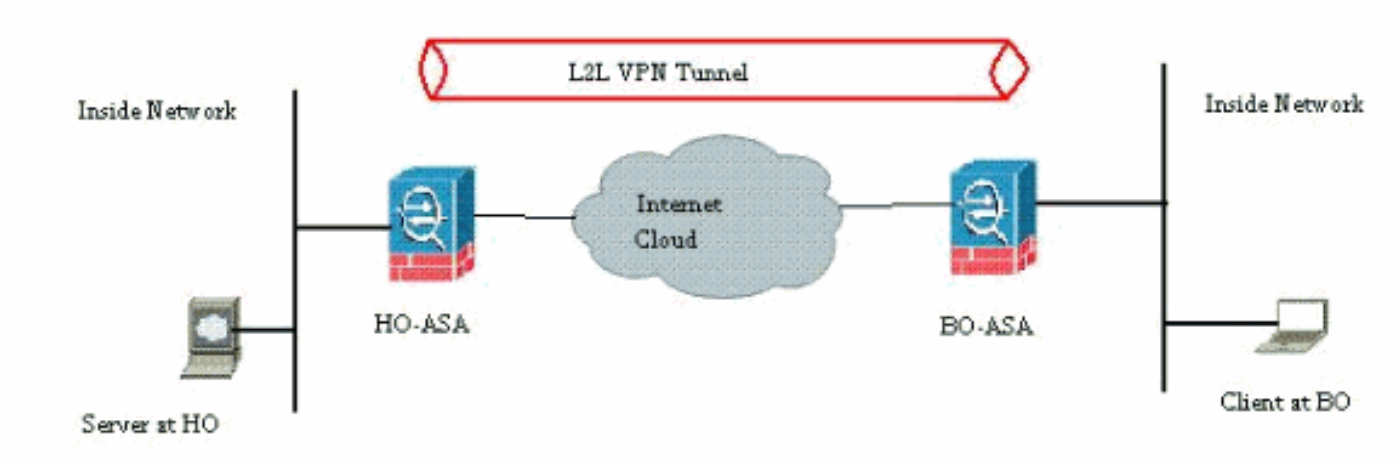
Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Como mostrado no diagrama de rede, a filial (BO) está conectada à matriz (HO) através da VPN site a site. Considere um usuário final na filial tentando fazer o download de um arquivo grande do servidor localizado na matriz. O download dura horas. A transferência de arquivos funciona bem até que a VPN funcione bem. No entanto, quando a VPN é interrompida, a transferência de arquivos é interrompida e o usuário precisa reiniciar a solicitação de transferência de arquivos novamente desde o início após o túnel ser estabelecido.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Esse problema ocorre devido à funcionalidade integrada de como o ASA funciona. O ASA monitora todas as conexões que passam por ele e mantém uma entrada em sua tabela de estados de acordo com o recurso de inspeção da aplicação. Os detalhes sobre o tráfego criptografado que passam pela VPN são mantidos como um banco de dados de associações de segurança (Security Association ou SA). No cenário deste documento, ele mantém dois fluxos de tráfego diferentes. Um é o tráfego criptografado entre os gateways VPN e o outro é o fluxo de tráfego entre o Servidor na matriz e o usuário final na filial. Quando a VPN é encerrada, os detalhes do fluxo dessa SA específica são excluídos. Contudo, a entrada na tabela de estados mantida pelo ASA para essa conexão TCP torna-se obsoleta por inatividade, o que dificulta o download. Isso significa que o ASA ainda retém a conexão TCP para esse fluxo específico mesmo que a aplicação do usuário tenha encerrado a comunicação. Contudo, as conexões TCP se tornarão erráticas e, por fim, chegarão ao tempo limite após a expiração do timer de inatividade do TCP.

Esse problema foi resolvido com a introdução de um recurso chamado Persistent IPSec Tunneled Flows (Fluxos em túnel IPSec persistente). Um novo comando foi integrado ao Cisco ASA para manter as informações da tabela de estado na renegociação do túnel VPN. O comando é mostrado aqui:

```
sysopt connection preserve-vpn-flows
```

Por padrão, esse comando está desativado. Ao habilitar isso, o Cisco ASA manterá as informações da tabela de estado do TCP quando a VPN L2L se recuperar da interrupção e restabelecer o túnel.

Neste cenário, esse comando deve ser ativado em ambas as extremidades do túnel. Se for um dispositivo que não é da Cisco na outra extremidade, habilitar esse comando no Cisco ASA deve ser suficiente. Se o comando estiver ativado quando os túneis já estiverem ativos, os túneis deverão ser limpos e restabelecidos para que esse comando tenha efeito. Para obter mais detalhes sobre como limpar e restabelecer os túneis, consulte Limpar as associações de segurança.

Detalhes de compatibilidade para este recurso

Esse recurso foi introduzido no software Cisco ASA versão 8.0.4 e posterior. Isso é suportado somente para estes tipos de VPN:

- Túneis de LAN para LAN
- Túneis de acesso remoto no modo de extensão de rede (NEM)

Este recurso não é suportado para estes tipos de VPN:

- Túneis de acesso remoto IPSec no modo cliente
- Túneis VPN AnyConnect ou SSL

Este recurso não existe nestas plataformas:

- Cisco PIX com software versão 6.0
- Cisco VPN Concentrators
- Plataformas Cisco IOS®

Habilitar esse recurso não cria nenhuma sobrecarga adicional no processamento interno da CPU do ASA porque ele manterá as mesmas conexões TCP que o dispositivo tem quando o túnel está ativo.

Observação: este comando é aplicável somente para conexões TCP. Ele não tem nenhum efeito no tráfego UDP. As conexões UDP expirarão conforme o período de tempo limite configurado.

Configurações

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

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

Este documento utiliza esta configuração:

- CiscoASA

Este é um exemplo de saída de configuração de execução do firewall Cisco ASA em uma extremidade do túnel VPN:

CiscoASA

```
ASA Version 8.2(1)
!
hostname CiscoASA
domain-name example.com
enable password <removed>
passwd <removed>
names
!
interface Ethernet0/0
 speed 100
 duplex full
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.248
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.224.9.5 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
!
interface Management0/0
 nameif management
 security-level 100
 ip address 10.224.14.10 255.255.255.0
!
boot system disk0:/asa822-k8.bin
ftp mode passive
 !---Output Suppressed ! access-list test extended
permit ip 10.224.228.0 255.255.255.128 any access-list
test extended permit ip 10.224.52.0 255.255.255.128 any
access-list 100 extended permit ip 10.224.228.0
255.255.255.128 any access-list 100 extended permit ip
10.224.52.0 255.255.255.128 any access-list
inside_access_out extended permit ip any 10.224.228.0
255.255.255.1 ! !---Output Suppressed global (outside) 1
interface nat (inside) 0 access-list test nat (inside) 1
10.224.10.0 255.255.255.0 ! !---Output Suppressed route
inside 10.0.0.0 255.0.0.0 10.224.9.1 1 route outside
0.0.0.0 255.255.255.255 209.165.201.1 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 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout sip-provisional-media 0:02:00
uauth 0:05:00 absolute timeout tcp-proxy-reassembly
0:01:00 dynamic-access-policy-record DfltAccessPolicy !
```

```
!---Output Suppressed http server idle-timeout 40 http
10.224.3.0 255.255.255.0 management http 0.0.0.0 0.0.0.0
inside ! snmp-server enable traps snmp authentication
linkup linkdown coldstart ! !--- To preserve and resume
stateful (TCP) tunneled IPsec LAN-to-LAN traffic within
the timeout period after the tunnel drops and recovers.
sysopt connection preserve-vpn-flows
service resetoutside
!
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256
esp-md5-hmac
crypto ipsec transform-set testSET esp-3des esp-md5-hmac
crypto map map1 5 match address 100
crypto map map1 5 set peer 209.165.200.10
crypto map map1 5 set transform-set testSET
crypto map map1 interface outside
crypto isakmp enable outside
crypto isakmp policy 5
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
!---Output Suppressed ! telnet timeout 5 ssh timeout 5
console timeout 0 threat-detection basic-threat threat-
detection statistics access-list ! !---Output Suppressed
! tunnel-group 209.165.200.10 type ipsec-l2l tunnel-
group 209.165.200.10 ipsec-attributes pre-shared-key *
!---Output Suppressed 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 rsh inspect rtsp inspect esmtp
inspect sqlnet inspect skinny inspect sunrpc inspect
xdmcp inspect sip inspect netbios inspect tftp !
service-policy global_policy global prompt hostname
state Cryptochecksum:5c228e7131c169f913ac8198ecf8427e :
end
```

Ativar este recurso

Por padrão, este recurso está desabilitado. Isso pode ser ativado usando este comando na CLI do ASA:

```
CiscoASA(config)#sysopt connection preserve-vpn-flows
```

Isso pode ser visualizado usando este comando:

```
CiscoASA(config)#show run all sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
```

```
sysopt connection permit-vpn
sysopt connection reclassify-vpn
sysopt connection preserve-vpn-flows
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
no sysopt noproxyarp outside
```

Ao usar o ASDM, esse recurso pode ser ativado seguindo este caminho:

Configuração > VPN de acesso remoto > Acesso à rede (cliente) > Avançado > IPsec > Opções do sistema.

Em seguida, marque a *opção Preservar fluxos de VPN stateful quando o túnel cair para o Network Extension Mode (NEM)*.

Verificar

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

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.

- **show asp table vpn-context detail** — Mostra o conteúdo do contexto VPN do caminho de segurança acelerado, o que pode ajudá-lo a solucionar um problema. Veja a seguir um exemplo de saída do comando **show asp table vpn-context** quando o recurso de fluxos de túnel IPSec persistente está ativado. Observe que ele contém um sinalizador **PRESERVE** específico.

```
CiscoASA(config)#show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
```

Troubleshoot

Nesta seção, algumas soluções alternativas são apresentadas para evitar a oscilação de túneis. Os prós e contras das soluções alternativas também são detalhados.

Defina IKE Lifetime Value como Zero

Você pode fazer com que um túnel VPN permaneça ativo por um tempo infinito, mas não para renegociar, mantendo o valor de vida do IKE como zero. As informações sobre o SA são mantidas pelos peers da VPN até que o tempo de vida expire. Atribuindo um valor como zero, você pode fazer com que esta sessão IKE dure para sempre. Por meio disso, você pode evitar problemas intermitentes de desconexão de fluxo durante a rechaveamento do túnel. Isso pode ser feito com este comando:

```
CiscoASA(config)#crypto isakmp policy 50 lifetime 0
```

No entanto, isso tem uma desvantagem específica em termos de comprometer o nível de segurança do túnel VPN. A rechaveamento da sessão IKE em intervalos de tempo especificados

fornece mais segurança ao túnel VPN em termos de chaves de criptografia modificadas a cada vez e torna-se difícil para qualquer intruso decodificar as informações.

Observação: desativar o tempo de vida do IKE não significa que o túnel não seja rechaveado. Ainda assim, o SA do IPSec será remarcado no intervalo de tempo especificado porque não pode ser definido como zero. O valor de tempo de vida mínimo permitido para uma SA IPSec é de 120 segundos e o máximo é 214783647 segundos. Para obter mais informações sobre isso, consulte IPSec SA lifetime.

Mensagem de erro quando o túnel cai

Quando esse recurso não é usado na configuração, o Cisco ASA retorna esta mensagem de log quando o túnel VPN é interrompido:

```
%ASA-6-302014: Teardown da conexão TCP 57983 para fora:XX.XX.XX.XX/80 para
dentro:10.0.0.100/1135 duração 0:00:36 bytes 0 túnel 53947 foi destruído
```

Você pode ver que o motivo é que o **túnel foi destruído**.

Observação: o registro de nível 6 deve ser ativado para ver esta mensagem.

Como esse recurso difere com a opção reclassify-vpn

A opção preserve-vpn-flow é usada quando um túnel salta. Isso permite que um fluxo TCP anterior permaneça aberto para que quando o túnel voltar, o mesmo fluxo possa ser usado.

Quando o comando **sysopt connection reclassify-vpn** é usado, ele limpa qualquer fluxo anterior relativo ao tráfego em túnel e classifica o fluxo para passar pelo túnel. A opção reclassify-vpn é usada em uma situação em que um fluxo TCP já foi criado e não está relacionado à VPN. Isso cria uma situação em que o tráfego não flui pelo túnel depois que a VPN é estabelecida. Para obter mais informações sobre isso, consulte sysopt reclassify-vpn.

Informações Relacionadas

- VPN site a site (L2L) com ASA
- Página de documentação do Cisco ASA
- Suporte Técnico e Documentação - Cisco Systems