ASA 8.X: Permita o aplicativo de usuário ser executado com o restabelecimento do túnel L2L VPN

Índice

Introdução

Este documento fornece a informação sobre IPsec persistente a característica escavada um túnel dos fluxos e como reter o fluxo de TCP sobre o rompimento de um túnel VPN.

Pré-requisitos

Requisitos

Os leitores deste documento devem ter a compreensão básica em como o VPN trabalha. Consulte estes documentos para obter outras informações:

- Prove a configuração de VPN L2L
- L2L VPN com ASA

Componentes Utilizados

A informação neste documento é baseada na ferramenta de segurança adaptável de Cisco (ASA) com versão 8.2 e mais recente.

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

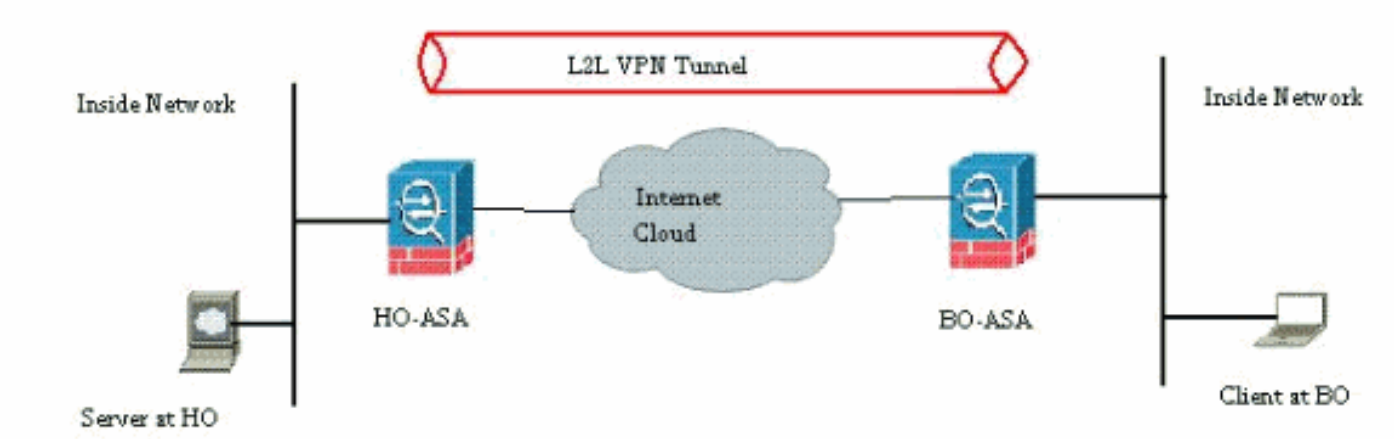
Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Segundo as indicações do diagrama da rede, o escritório filial (BO) é conectado à sede (HO) com o VPN de Site-para-Site. Considere um utilizador final no escritório filial que tenta transferir um arquivo grande do server situado na sede. A transferência dura horas. Transferência de arquivo trabalha muito bem até que o VPN trabalhe muito bem. Contudo, quando o VPN é interrompido, transferência de arquivo está pendurada e o usuário tem que re-novato o pedido de transferência de arquivo outra vez desde o início depois que o túnel é estabelecido.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Este problema elevara devido à funcionalidade incorporado em como o ASA trabalha. O ASA monitora cada conexão que as passagens com ele e mantêm uma entrada em sua tabela de estado de acordo com a característica da inspeção de aplicativo. Os detalhes do tráfego criptografado que passam com o VPN são mantidos sob a forma de um base de dados da associação de segurança (SA). Para a encenação deste documento, mantém dois fluxos de tráfego diferentes. Um é o tráfego criptografado entre os gateways de VPN e os outro é o fluxo de tráfego entre o server na sede e o utilizador final no escritório filial. Quando o VPN é terminado, os detalhes do fluxo para este SA particular estão suprimidos. Contudo, a entrada de tabela do estado mantida pelo ASA para esta conexão de TCP torna-se velha devido a nenhuma atividade, que impede da transferência. Isto significa que o ASA ainda reterá a conexão de TCP para esse fluxo particular quando o aplicativo de usuário terminar. Contudo, as conexões de TCP transformar-se-ão estática e eventualmente intervalo depois que o temporizador de ociosidade

TCP expira.

Este problema foi resolvido introduzindo uma característica chamada fluxos escavados um túnel IPsec de Persistente. Um comando new foi integrado em Cisco ASA reter a informação da tabela de estado na negociação nova do túnel VPN. O comando é mostrado aqui:

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

Àrevelia, este comando é desabilitado. Permitindo isto, Cisco ASA manterá a informação da tabela de estado TCP quando o L2L VPN recupera do rompimento e restabelece o túnel.

Nesta encenação, este comando tem que ser permitido no ambas as extremidades do túnel. Se é um dispositivo que não é da Cisco no extremo oposto, permitir este comando em Cisco ASA deve bastar. Se o comando é permitido quando os túneis eram já ativos, os túneis devem ser cancelados e restabelecido para que este comando tome o efeito. Para mais detalhes ao o esclarecimento e restabelecer os túneis, consulte para cancelar as associações de segurança.

Detalhes da compatibilidade para esta característica

Esta característica foi introduzida na versão de software 8.0.4 de Cisco ASA e mais atrasado. Isto é apoiado somente para estes tipos de VPN:

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

Esta característica não é apoiada para estes tipos de VPN:

- Túneis de acesso remoto do IPsec no modo de cliente
- AnyConnect ou túneis SSL VPN

Esta característica não existe nestas Plataformas:

- Cisco PIX com versão de software 6.0
- Cisco VPN concentratores
- Plataformas de Cisco IOS®

Permitir esta característica não cria nenhuma sobrecarga adicional no processamento de CPU interno do ASA porque está indo manter as mesmas conexões de TCP que o dispositivo tem quando o túnel está acima.

Nota: Este comando é aplicável para conexões de TCP somente. Não tem nenhum efeito no tráfego UDP. As conexões de UDP querem o intervalo conforme o período de timeout 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

Esta é umas saídas de configuração running da amostra do Firewall de 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
```

Permita esta característica

Àrevelia, esta característica é desabilitada. Isto pode ser permitido usando este comando no CLI do ASA:

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

Isto pode ser visto 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, esta característica pode ser permitida seguindo este trajeto:

A configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançaram > IPsec > opções de sistema.

Então, verifique os *fluxos do stateful VPN da conserva quando o túnel deixa cair para a* opção do *modo de extensão de rede (NEM)*.

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.

- **mostre o detalhe do VPN-contexto da tabela asp** — Mostra os índices do contexto VPN do trajeto acelerado da Segurança, que pôde o ajudar a pesquisar defeitos um problema. O seguinte é um exemplo de saída do comando do VPN-**contexto da tabela asp da mostra** quando o IPsec persistente escavou um túnel fluxos que a característica é permitida. Note que contém uma bandeira específica da **CONSERVA**.`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`

Troubleshooting

Nesta seção, determinadas ações alternativas são apresentadas para evitar o flapping dos túneis. Os profissionais - e - contra das ações alternativas são detalhados igualmente.

Ajuste o valor da duração de IKE a zero

Você pode fazer um túnel VPN para ficar vivo por um tempo infinito, mas para não renegociar, mantendo o valor da duração de IKE como zero. A informação sobre o SA está retida pelos pares VPN até que a vida expire. Atribuindo um valor como zero, você pode fazer este último da sessão de IKE para sempre. Com isto, você pode evitar as edições intermitentes da desconexão do fluxo durante re-fechar do túnel. Isto pode ser feito com este comando:

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

Contudo, isto tem uma desvantagem específica em termos de comprometer o nível de segurança do túnel VPN. Re-fechar a sessão de IKE dentro dos intervalos de tempo especificado fornece mais Segurança ao túnel VPN em termos das chaves de criptografia alteradas cada vez e torna-se difícil para todo o intruso descodificar a informação.

Nota: Desabilitar a duração de IKE não significa que o túnel não faz re-chave de todo. Ainda, IPsec SA re-chave no intervalo de tempo especificado porque aquele não pode ser ajustado a zero. O valor mínimo da vida permitido IPsec SA é 120 segundos e o máximo é 214783647 segundos. Para obter mais informações sobre disto, refira a vida IPsec SA.

Mensagem de Erro quando o túnel deixar cair

Quando esta característica não é usada na configuração, Cisco ASA retorna este mensagem de registro quando o túnel VPN é interrompido:

```
%ASA-6-302014: A conexão de TCP 57983 do Teardown para outside:XX.XX.XX.XX/80
inside:10.0.0.100/1135 ao túnel dos bytes 53947 da duração 0:00:36 foi rasgada para baixo
```

Você pode ver que a razão é que o **túnel esteve rasgado para baixo**.

Nota: O registro do nível 6 deve ser permitido de considerar esta mensagem.

Como esta característica difere com a opção reclassificar-VPN

A opção do conserva-VPN-fluxo é usada quando um túnel salta. Isto permite que um fluxo de TCP precedente fique aberto assim quando o túnel vem apoio, o mesmo fluxo pode ser usado.

Quando o comando da **conexão reclassificar-VPN do sysopt** é usado, cancela todo o fluxo

precedente que se referir o tráfego em túnel e se classificar o fluxo para atravessar o túnel. A opção reclassificar-VPN é usada em uma situação quando um fluxo de TCP foi criado já que não seja VPN relativo. Isto cria uma situação aonde o tráfego não flua através do túnel depois que o VPN é estabelecido. Para obter mais informações sobre disto, refira o sysopt reclassificar-VPN.

Informações Relacionadas

- Local para situar VPN (L2L) com ASA
- Página de documentação de Cisco ASA
- Suporte Técnico e Documentação - Cisco Systems