ASA 8.X: Laat de gebruikerstoepassing lopen met het opnieuw instellen van de L2L VPN-tunnel

Inhoud

Inleiding

Dit document geeft informatie over de Persistente IPSec Tunneled Flows-functie en hoe de TCP-stroom te behouden bij de verstoring van een VPN-tunnel.

Voorwaarden

Vereisten

Lezers van dit document zouden basiskennis moeten hebben over hoe VPN werkt. Raadpleeg deze documenten voor meer informatie:

- Configuratie van L2L VPN-voorbeeld
- L2L VPN-software

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco adaptieve security applicatie (ASA) met versie 8.2 en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

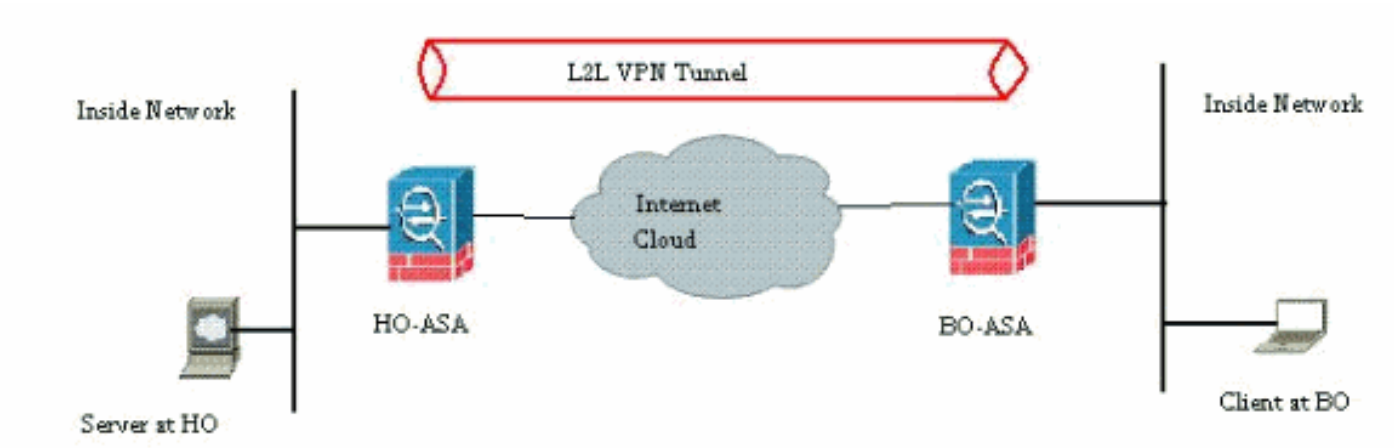
Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

Zoals in het netwerkdiagram wordt getoond, wordt het bijkantoor (BO) aangesloten op het hoofdkantoor (HO) door het site-to-site VPN. Neem een eindgebruiker bij het bijkantoor in overweging om een groot bestand van de server in het hoofdkantoor te downloaden. De download duurt uren. De bestandsoverdracht werkt prima totdat VPN werkt. Wanneer VPN echter wordt verstoord, wordt de bestandsoverdracht opgeslagen en moet de gebruiker het bestand-overdrachtverzoek opnieuw openen vanaf het begin nadat de tunnel is ingesteld.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Dit probleem ontstaat door de ingebouwde functionaliteit op de manier waarop de ASA werkt. De ASA controleert elke verbinding die erdoor gaat en handhaaft een ingang in zijn staatslijst volgens de functie van de toepassingsinspectie. De gecodeerde verkeersdetails die door VPN gaan worden onderhouden in de vorm van een SA-database (Security Association). Voor het scenario van dit document handhaaft het twee verschillende verkeersstromen. Het ene is het gecodeerde verkeer tussen de VPN gateways en het andere is de verkeersstroom tussen de Server aan het hoofd en de eindgebruiker aan het bijkantoor. Wanneer VPN wordt beëindigd, worden de stroomdetails voor deze specifieke SA geschrapt. Maar de site table entry, die door de ASA onderhouden wordt voor deze TCP verbinding wordt gestaal vanwege het gebrek aan activiteit, wat de download belemmert. Dit betekent dat de ASA de TCP verbinding voor die bepaalde stroom zal behouden terwijl de gebruikerstoepassing eindigt. Maar de TCP verbindingen zullen afstammen en uiteindelijk pauzeren na verloop van de TCP idle-timer.

Dit probleem is opgelost door de introductie van een functie die Persistente IPSec Tunneled Flows wordt genoemd. Een nieuwe opdracht is in Cisco ASA geïntegreerd om de informatie van de staatstabel te behouden bij het opnieuw onderhandelen van de VPN-tunnel. Deze opdracht wordt hier weergegeven:

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

Deze opdracht is standaard uitgeschakeld. Door dit toe te laten, zal Cisco ASA de informatie van de TCP-statetabel bewaren wanneer L2L VPN van de ontwrichting herstelt en de tunnel herstelt.

In dit scenario moet deze opdracht aan beide uiteinden van de tunnel worden ingeschakeld. Als het een niet-Cisco apparaat aan het andere eind is, zou het toelaten van deze opdracht op Cisco ASA moeten volstaan. Als de opdracht is ingeschakeld toen de tunnels al actief waren, moeten de tunnels worden gewist en opnieuw worden geïnstalleerd zodat deze opdracht effect heeft. Raadpleeg voor meer informatie over het opruimen en herstellen van de tunnels de Security Associations.

Compatibiliteitsdetails voor deze functie

Deze optie is toegevoegd in Cisco ASA-softwareversie 8.0.4 en hoger. Dit wordt alleen ondersteund voor deze typen VPN:

- LAN-tunnels
- Remote Access-tunnels in Network Extension Mode (NEM)

Deze optie wordt niet ondersteund voor deze VPN-typen:

- IPSec Remote Access-tunnels in clientmodus
- AnyConnect of SSL VPN-tunnels

Deze optie bestaat niet op deze platforms:

- Cisco PIX met softwareversie 6.0
- Cisco VPN-concentraties
- Cisco IOS®-platforms

Het in werking stellen van deze functie creëert geen extra overload op de interne CPU-verwerking van de ASA omdat het dezelfde TCP-verbindingen zal behouden die het apparaat heeft wanneer de tunnel omhoog is.

Opmerking: deze opdracht is alleen van toepassing op TCP-verbindingen. Het heeft geen enkel effect op het UDP-verkeer. De UDP-verbindingen onderbreken de tijd per de geconfigureerde time-out-periode.

Configuraties

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Dit document gebruikt deze configuratie:

- Cisco ASA

Dit is een voorbeeld-actieve configuratie-uitvoer van de Cisco ASA-firewall aan één uiteinde van de VPN-tunnel:

Cisco ASA

```
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
```

Deze functie inschakelen

Deze optie is standaard uitgeschakeld. Dit kan mogelijk worden gemaakt door deze opdracht te gebruiken bij de CLI van de ASA:

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

U kunt deze opdracht als volgt bekijken:

```
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
```

Wanneer u ASDM gebruikt, kan deze functie worden ingeschakeld door het volgende pad te volgen:

Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > systeemopties.

Controleer vervolgens de *stateful VPN-stromen wanneer de tunnel zakt voor Network Extension Mode (NEM)* optie.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **vpn-context van de asp-tabel**-toont de VPN context inhoud van het versnelde security pad, dat u zou kunnen helpen bij het oplossen van een probleem. Het volgende is een steekproefuitvoer van de **show asp table vpn-context** opdracht wanneer de persistente IPSec tunneled flow is ingeschakeld. Merk op dat het een specifieke **PRESERVE**-vlag bevat.

```
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
```

Problemen oplossen

In dit deel worden bepaalde omwentelingen aangebracht om het fladderen van tunnels te voorkomen. Ook de voor- en nadelen van de omwonenden zijn gedetailleerd.

Stel de levensduur van IKE in op nul

U kunt een VPN-tunnel voor onbepaalde tijd in leven houden, maar niet opnieuw onderhandelen door de IKE-levenswaarde op nul te houden. De informatie over de SA wordt bewaard door de peers van VPN tot het leven verstrijkt. Door een waarde als nul toe te kennen, kunt u deze IKE-sessie voor altijd laten duren. Door dit te vermijden, kunt u de intermitterende stroom afkoppelingskwesties tijdens het hersluiten van de tunnel vermijden. Dit kan met deze opdracht worden gedaan:

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

Dit heeft echter een specifiek nadeel als het gaat om het in gevaar brengen van het veiligheidsniveau van de VPN-tunnel. Het opnieuw bijhouden van de IKE-sessie binnen de

opgegeven tijdintervallen biedt meer beveiliging tegen de VPN-tunnel in termen van aangepaste coderingstoetsen telkens en het wordt voor een indringer moeilijk om de informatie te decoderen.

Opmerking: het uitschakelen van het IKE-leven betekent niet dat de tunnel helemaal niet opnieuw wordt ingestuurd. Niettemin zal IPSec SA op het gespecificeerde tijd-interval opnieuw zeer belangrijk zijn omdat dat niet op nul kan worden ingesteld. De minimale levensduur van een IPSec SA is 120 seconden en het maximum is 214783647 seconden. Raadpleeg voor meer informatie hierover IPSec SA-leven.

Foutbericht wanneer tunnels vallen

Wanneer deze optie niet in de configuratie gebruikt wordt, retourneert Cisco ASA dit logbericht wanneer de VPN-tunnel verstoord is:

```
%ASA-6-302014: Schakel TCP-verbinding 57983 voor buitengebruik:XX.XX.XX.XX/80 naar
binnen:10.0.0.100/1135 durend 0:00:36 bytes 53947 Tunnel is afgebroken
```

Je ziet dat de reden is dat de **Tunnel is afgebroken**.

Opmerking: niveau 6 voor de vastlegging moet zijn ingeschakeld om dit bericht te zien.

Hoe deze optie verschilt met de optie herindeling-VPN

De optie voor het behoud van de VPN-flow wordt gebruikt wanneer een tunnel vlakt. Dit laat een vorige TCP-stroom open staan zodat wanneer de tunnel weer omhoog komt, dezelfde stroom gebruikt kan worden.

Wanneer de opdracht **voor** de **herindeling van de systeemverbinding door vpn** wordt gebruikt, wordt elke vorige stroom die op het tunnelverkeer betrekking heeft, gewist en wordt de stroom geclassificeerd om door de tunnel te gaan. De optie herindelen-VPN wordt gebruikt in een situatie wanneer een TCP-stroom al is gecreëerd die niet VPN-gerelateerd is. Dit creëert een situatie waar het verkeer niet door de tunnel stroomt nadat het VPN is gevestigd. Raadpleeg voor meer informatie hierover het systeem herindeling-vpn.

Gerelateerde informatie

- Site to Site VPN (L2L) met ASA
- Cisco ASA-documentatiepagina
- Technische ondersteuning en documentatie – Cisco Systems