ASA 8.X: L2L VPN 터널 재설정과 함께 사용자 애플리케이션을 실행할 수 있도록 허용

목차

소개

이 문서에서는 지속적인 IPSec 터널링 흐름 기능에 대한 정보와 VPN 터널 중단을 통해 TCP 흐름을 유지하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서의 독자는 VPN의 작동 방식에 대한 기본적인 지식을 가져야 합니다. 자세한 내용은 다음 문서를 참조하십시오.

- 샘플 L2L VPN 컨피그레이션
- ASA를 사용하는 L2L VPN

사용되는 구성 요소

이 문서의 정보는 버전 8.2 이상의 Cisco ASA(Adaptive Security Appliance)를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

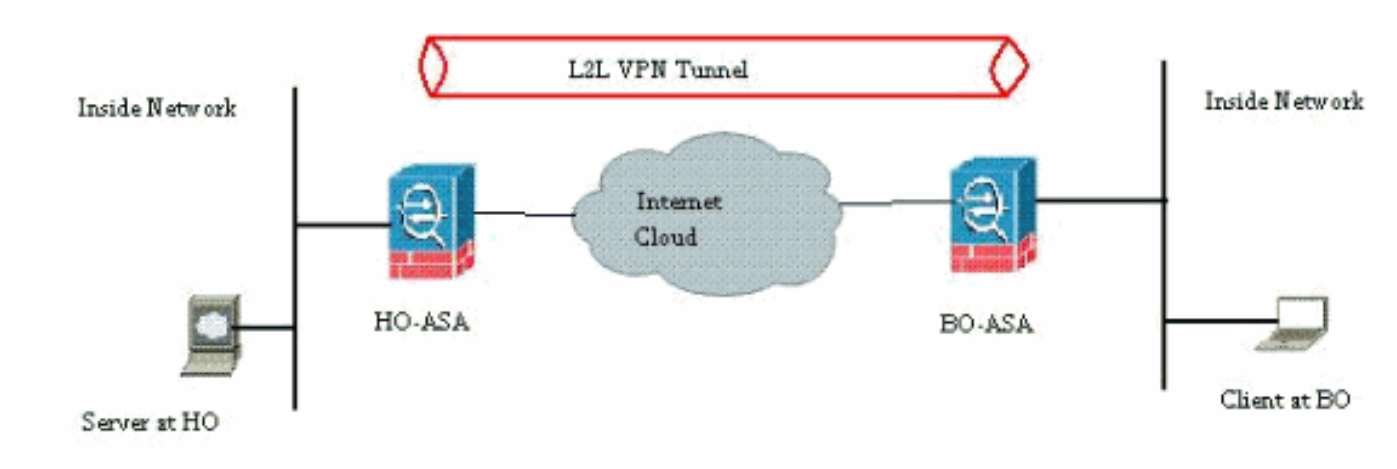
문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

네트워크 다이어그램에 표시된 것처럼 BO(Branch Office)는 Site-to-Site VPN을 통해 HO(Head Office)에 연결됩니다. 본사에 있는 서버에서 대용량 파일을 다운로드하려고 시도하는 지사의 최종 사용자를 고려해 보십시오. 다운로드가 몇 시간 동안 지속됩니다. VPN이 제대로 작동할 때까지 파일 전송이 정상적으로 작동합니다. 그러나 VPN이 중단되면 파일 전송이 정지되고 사용자는 터널이 설정된 후 처음부터 파일 전송 요청을 다시 시작해야 합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



이 문제는 ASA 작동 방식에 대한 내장 기능 때문에 발생합니다. ASA는 통과하는 모든 연결을 모니터링하고 애플리케이션 검사 기능에 따라 상태 테이블의 항목을 유지합니다. VPN을 통과하는 암호화된 트래픽 세부 정보는 SA(Security Association) 데이터베이스의 형태로 유지됩니다. 이 문서의 시나리오에서는 서로 다른 두 트래픽 흐름을 유지합니다. 하나는 VPN 게이트웨이 간의 암호화된 트래픽이고 다른 하나는 본사의 서버와 지사의 최종 사용자 간의 트래픽 흐름입니다. VPN이 종료되면 이 특정 SA에 대한 흐름 세부사항이 삭제됩니다. 그러나 ASA에서 이 TCP 연결에 대해 유지 관리하는 상태 테이블 항목은 활동이 없어 다운로드가 중단됩니다. 즉, ASA는 사용자 애플리케이션이 종료되는 동안 해당 특정 플로우에 대한 TCP 연결을 계속 유지합니다. 그러나 TCP 유휴 타이머가 만료되면 TCP 연결이 끊기고 결국 시간 초과됩니다.

이 문제는 Persistent IPSec Tunneled Flows라는 기능을 도입하여 해결되었습니다. VPN 터널의 재협상 시 상태 테이블 정보를 유지하기 위해 새 명령이 Cisco ASA에 통합되었습니다. 이 명령은 다음과 같습니다.

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

기본적으로 이 명령은 비활성화되어 있습니다. 이를 활성화하면 L2L VPN이 중단으로부터 복구되고 터널을 다시 설정할 때 Cisco ASA는 TCP 상태 테이블 정보를 유지합니다.

이 시나리오에서는 터널의 양쪽 끝에서 이 명령을 활성화해야 합니다. 다른 쪽 끝에 Cisco 이외의 디바이스인 경우 Cisco ASA에서 이 명령을 활성화하면 충분합니다. 터널이 이미 활성 상태일 때 명령이 활성화된 경우 이 명령을 적용하려면 터널을 지우고 다시 설정해야 합니다. 터널 지우기 및 재설정에 대한 자세한 내용은 보안 연결 지우기를 참조하십시오.

이 기능에 대한 호환성 세부 정보

이 기능은 Cisco ASA 소프트웨어 버전 8.0.4 이상에서 도입되었습니다. 이는 다음 유형의 VPN에서만 지원됩니다.

- LAN-to-LAN 터널
- NEM(Network Extension Mode)의 원격 액세스 터널

이 기능은 다음 유형의 VPN에서 지원되지 않습니다.

- 클라이언트 모드의 IPSec 원격 액세스 터널
- AnyConnect 또는 SSL VPN 터널

이 기능은 다음 플랫폼에 존재하지 않습니다.

- 소프트웨어 버전 6.0이 포함된 Cisco PIX
- Cisco VPN Concentrator
- Cisco IOS® 플랫폼

이 기능을 활성화해도 ASA의 내부 CPU 처리에서는 추가 오버로드가 발생하지 않습니다. 터널이 가동될 때 디바이스가 가진 것과 동일한 TCP 연결을 유지할 것이기 때문입니다.

참고: 이 명령은 TCP 연결에만 적용됩니다. UDP 트래픽에는 아무런 영향을 미치지 않습니다. UDP 연결은 구성된 시간 제한 기간에 따라 시간 초과됩니다.

구성

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

이 문서에서는 다음 구성을 사용합니다.

- CiscoASA

다음은 VPN 터널의 한쪽 끝에서 Cisco ASA 방화벽의 실행 중인 컨피그레이션 출력의 샘플입니다.

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
```

이 기능 사용

기본적으로 이 기능은 비활성화되어 있습니다. ASA의 CLI에서 다음 명령을 사용하여 이 명령을 활성화할 수 있습니다.

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

이 명령은 다음 명령을 사용하여 볼 수 있습니다.

```
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
```

ASDM을 사용하는 경우 이 경로를 따라 이 기능을 활성화할 수 있습니다.

Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > IPsec > System Options(시스템 옵션).

그런 다음 Preserve stateful *VPN flows when the tunnel drops for Network Extension Mode (NEM)* 옵션을 선택합니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show asp table vpn-context detail** - 문제를 해결하는 데 도움이 될 수 있는 가속화된 보안 경로의 VPN 컨텍스트 내용을 표시합니다. 다음은 지속적인 IPSec 터널링 흐름 기능이 활성화된 경우 **show asp table vpn-context** 명령의 샘플 출력입니다. 여기에는 특정 PRESERVE 플래그가 포함되어 **있습니다**.

```
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
```

문제 해결

이 섹션에서는 터널의 플랩을 방지하기 위해 특정 해결 방법을 제시합니다. 해결 방법의 장점과 단점들도 또한 상세하다.

IKE 수명 값을 0으로 설정

IKE 수명 값을 0으로 유지하여 VPN 터널을 무한 시간 동안 활성 상태로 유지할 수 있지만 재협상하지 않도록 할 수 있습니다. SA에 대한 정보는 수명이 만료될 때까지 VPN 피어가 보존합니다. 값을 0으로 할당하면 이 IKE 세션을 영구적으로 유지할 수 있습니다. 이를 통해 터널을 재키하는 동안 간헐적인 플로우 연결 해제 문제를 방지할 수 있습니다. 이 명령은 다음 명령으로 수행할 수 있습니다.

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

그러나 이는 VPN 터널의 보안 수준을 손상시킨다는 점에서 구체적인 단점을 가지고 있습니다. 지정된 시간 간격 내에 IKE 세션을 재키하면 매번 수정된 암호화 키의 관점에서 VPN 터널에 더 많은 보안을 제공하며 침입자가 정보를 디코딩하기가 어려워집니다.

참고: IKE 수명을 비활성화한다고 해서 터널이 다시 키가 지정되지 않습니다. 그러나 IPSec SA는 0으로 설정할 수 없으므로 지정된 시간 간격으로 키를 다시 설정합니다. IPSec SA에 허용되는 최소 수명 값은 120초이며 최대값은 214783647초입니다. 이에 대한 자세한 내용은 IPSec SA 수명을 참조하십시오.

터널 삭제 시 오류 메시지

이 기능을 컨피그레이션에서 사용하지 않으면 VPN 터널이 중단되면 Cisco ASA에서 이 로그 메시지를 반환합니다.

```
%ASA-6-302014: :XX.XX.XX.XX/80  TCP  57983 .:10.0.0.100/1135  0:00:36 53947  .
```

그 이유는 **터널**이 **헐렸기 때문입니다**.

참고: 이 메시지를 보려면 레벨 6 로깅을 활성화해야 합니다.

이 기능이 reclassify-vpn 옵션과 어떻게 다른지

preserve-vpn-flow 옵션은 터널이 바운스될 때 사용됩니다. 이를 통해 이전 TCP 플로우가 열린 상태로 유지되므로 터널이 다시 작동하면 동일한 플로우를 사용할 수 있습니다.

sysopt **connection reclassify-vpn** 명령을 사용하면 터널링된 트래픽과 관련된 이전 흐름을 모두 지우고 터널을 통과하도록 흐름을 분류합니다. reclassify-vpn 옵션은 VPN과 관련되지 않은 TCP 흐름이 이미 생성된 경우에 사용됩니다. 이렇게 하면 VPN이 설정된 후 터널에서 트래픽이 전달되지 않는 상황이 발생합니다. 이에 대한 자세한 내용은 sysopt reclassify-vpn을 참조하십시오.

관련 정보

- ASA를 사용하는 사이트 대 사이트 VPN(L2L)
- Cisco ASA 설명서 페이지
- 기술 지원 및 문서 – Cisco Systems