일반적인 L2L 및 원격 액세스 IPsec VPN 문제 해결

목차

소개

배경 정보

사전 요구 사항

IPsec VPN 컨피그레이션이 작동하지 않음

VPN 클라이언트가 ASA에 연결할 수 없음

VPN 클라이언트는 첫 번째 시도 시 또는 "Security VPN Connection terminated by peer(피어에 의해 종료된 보안 VPN 연결)"에서 자주 연결을 삭제합니다. 이유 433." 또는 "Secure VPN Connection terminated by Peer 이유 433:(Reason Not Specified by Peer)"

원격 액세스 및 EZVPN 사용자는 VPN에 연결하지만 외부 리소스에 액세스할 수 없음

3명 이상의 VPN 클라이언트 사용자를 연결할 수 없음

터널 설정 후 세션 또는 애플리케이션을 시작할 수 없으며 전송 속도가 느려짐

ASA에서 VPN 터널을 시작할 수 없음

VPN 터널을 통해 트래픽을 전달할 수 없음

동일한 암호화 맵에서 vpn 터널에 대한 백업 피어 구성

VPN 터널 비활성화/재시작

일부 터널이 암호화되지 않음

오류:- %ASA-5-713904: 그룹 = DefaultRAGroup, IP = x.x.x, ...지원되지 않는 트랜잭션 모드 v2 version.Tunnel이 종료되었습니다.

오류:- %ASA-6-722036: Group client-group User xxxx IP x.x.x Transmitting large packet 1220(임계값 1206)

VPN 터널의 한 쪽에서 QoS가 활성화된 경우 오류 메시지

경고: 암호화 맵 항목이 불완전합니다.

오류:- %ASA-4-400024: IDS:2151 인터페이스 외부의 큰 ICMP 패킷에서 (으)로

오류:- %ASA-4-402119: IPSEC: 재전송 방지 확인에 실패한 remote_IP(사용자 이름)에서 local_IP로의 프로토콜 패킷(SPI=spi, 시퀀스 번호= seq_num)을 받았습니다.

오류 메시지 - %ASA-4-407001: 로컬 호스트 interface_name:inside_address에 대한 거부 트래픽, 라이센스 제한 개수 초과

오류 메시지 - %VPN_HW-4-PACKET_ERROR:

오류 메시지: 명령이 거부되었습니다. VLAN XXXX와 XXXX 간의 암호화 연결을 먼저 삭제하십시오.

오류 메시지 - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: 삭제된 패킷 - 세션 x.x.x.x:27331에서 x.x.x.x:23에 대한 잘못된 창 크기 옵션 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]

%ASA-5-305013: 비대칭 NAT 규칙이 정방향 및 역방향에 대해 일치합니다. 이 문제 흐름을 업데이트하십시오.

%ASA-5-713068: 비루틴 알림 메시지를 받았습니다. notify_type

%ASA-5-720012: (VPN-Secondary) 대기 유닛에서 IPSec 장애 조치(failover) 런타임 데이터를 업데이트하지 못했습니다. 또는 %ASA-6-720012: (VPN-unit) 대기 유닛에서 IPsec 장애 조치(failover) 런타임 데이터를 업데이트하지 못했습니다.

오류:- %ASA-3-713063: IKE 피어 주소가 대상 0.0.0.0에 대해 구성되지 않았습니다.

오류: %ASA-3-752006: 터널 관리자가 KEY_ACQUIRE 메시지를 디스패치하지 못했습니다.

오류: %ASA-4-402116: IPSEC: XX.XX.XX.XX(user= XX.XX.XX.XX)에서 YY.YY.YY.YY으로 ESP 패킷(SPI= 0x99554D4E, 시퀀스 번호= 0x9E)을 받았습니다.

0xffffffff 오류로 인해 64비트 VA 설치 관리자를 시작하여 가상 어댑터를 사용하도록 설정하지 못했습니다.

Cisco VPN Client는 Windows 7에서 데이터 카드와 작동하지 않음

경고: "VPN 기능이 전혀 작동하지 않을 수 있습니다."

IPSec 패딩 오류

VPN 터널은 18시간마다 연결 끊김

LAN-to-LAN 터널이 재협상된 후에는 트래픽 흐름이 유지되지 않습니다

암호화 기능에 대한 대역폭에 도달했다는 오류 메시지 상태

문제: 인바운드 암호 해독 트래픽이 작동하더라도 IPsec 터널의 아웃바운드 암호화 트래픽은 실패합니다.

기타

관련 정보

소개

이 문서에는 IPsec VPN 문제에 대한 가장 일반적인 솔루션을 설명합니다.

배경 정보

여기에 설명된 솔루션은 Cisco 기술 지원부에서 해결한 서비스 요청에서 직접 제공됩니다.

이러한 솔루션 중 상당수는 IPsec VPN 연결에 대한 심층적인 트러블슈팅 전에 구현됩니다.

이 문서에서는 연결 트러블슈팅을 시작하기 전에 시도하는 일반적인 절차에 대한 요약을 제공합니다.

이 문서의 컨피그레이션 예는 라우터와 보안 어플라이언스에서 사용되지만, 이러한 개념의 거의 대부분은 VPN 3000에도 적용됩니다.

Cisco IOS® 소프트웨어 및 의 IPsec 문제를 해결하는 데 사용되는 일반적인 디버그 명령에 대한 설명은 IP 보안 트러블슈팅 - 디버그 명령 이해 및 사용을 참조하십시오.

참고: ASA는 IPsec VPN 터널을 통해 멀티캐스트 트래픽을 전달하지 않습니다.

경고: 이 문서에 제시된 대부분의 솔루션은 디바이스에서 모든 IPsec VPN 연결이 일시적으로 손실될 수 있습니다.

이러한 솔루션은 사용자의 변경 제어 정책에 따라 신중하게 구현하는 것이 좋습니다.

사전 요구 사항

요구 사항

Cisco는 다음 Cisco 장치의 IPsec VPN 구성에 대한 지식을 권장합니다.

- Cisco ASA 5500 Series 보안 어플라이언스
- Cisco IOS® 라우터

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 5500 Series 보안 어플라이언스
- Cisco IOS®

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

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

IPsec VPN 컨피그레이션이 작동하지 않음

문제

최근에 구성되거나 수정된 IPsec VPN 솔루션이 작동하지 않습니다.

현재 IPsec VPN 컨피그레이션이 더 이상 작동하지 않습니다.

솔루션

이 섹션에는 가장 일반적인 IPsec VPN 문제에 대한 솔루션이 포함되어 있습니다.

이러한 솔루션은 특정 순서로 나열되지 않지만 심층적인 교정을 수행하기 전에 확인하거나 시도할 항목의 체크리스트로 사용할 수 있습니다.

이러한 모든 솔루션은 TAC 서비스 요청에서 직접 제공되며 수많은 문제를 해결했습니다.

- NAT-Traversal 활성화(#1 RA VPN 문제 해결)
- 올바르게 연결 테스트
- ISAKMP 활성화
- PFS 활성화/비활성화
- 기존 또는 기존 보안 연결 지우기(터널)
- ISAKMP 수명 확인

- ISAKMP 킵얼라이브 활성화 또는 비활성화
- 사전 공유 키 다시 입력 또는 복구
- 일치하지 않는 사전 공유 키
- 암호화 맵 제거 및 다시 적용
- sysopt 명령이 있는지 확인합니다(/ASA에만 해당).
- ISAKMP ID 확인
- 유휴/세션 시간 초과 확인
- ACL이 올바르고 암호화 맵에 바인딩되어 있는지 확인
- ISAKMP 정책 확인
- 라우팅이 올바른지 확인합니다.
- Transform-Set이 올바른지 확인
- 암호화 맵 시퀀스 번호 및 이름 확인
- 피어 IP 주소가 올바른지 확인합니다.
- 터널 그룹 및 그룹 이름 확인
- L2L 피어에 대해 XAUTH 비활성화
- VPN 풀 소모
- VPN 클라이언트 트래픽에 대한 레이턴시 문제

참고: 공간 고려 사항으로 인해 이러한 섹션의 일부 명령이 두 번째 줄로 내려왔습니다.

NAT-Traversal 활성화(#1 RA VPN 문제 해결)

NAT-Traversal(또는 NAT-T)은 VPN 트래픽이 Linksys SOHO 라우터와 같은 NAT 또는 PAT 디바이스를 통과하도록 허용합니다.

NAT-T가 활성화되지 않은 경우 VPN 클라이언트 사용자는 종종 문제 없이 ASA에 연결하는 것처럼 보이지만 보안 어플라이언스 뒤의 내부 네트워크에 액세스할 수 없습니다.

NAT/PAT 디바이스에서 NAT-T를 활성화하지 않으면 ASA에서 **프로토콜 50 src inside:10.0.1.26 dst outside:10.9.69.4** 오류 메시지에 대해 실패한 일반 변환 생성을 수신할 수 있습니다.

마찬가지로, 동일한 IP 주소에서 동시 로그인을 수행할 수 없는 경우 클라이언트에 의해 보안 VPN 연결이 로컬로 종료되었습니다. 이유 412: 원격 피어가 더 이상 응답하지 않습니다.오류 메시지가 나타납니다.

이 오류를 해결하려면 헤드 엔드 VPN 디바이스에서 NAT-T를 활성화합니다.

참고: Cisco IOS® Software Release 12.2(13)T 이상에서는 Cisco IOS®에서 NAT-T가 기본적으로 활성화됩니다.

Cisco Security Appliance에서 NAT-T를 활성화하는 명령입니다. 이 예에서 20은 keepalive time(기본값)입니다.

ASA

<#root>

securityappliance(config)#

crypto isakmp nat-traversal 20

고객도 수정이 되어야 효과가 있습니다.

Cisco VPN Client(Cisco VPN 클라이언트)에서 Connection Entries(연결 항목)로 이동하고 Modify(수정)를 클릭합니다. 새 창이 열리고 여기서 Transporttab(전송 탭)을 선택해야 합니다.

이 탭에서 Enable Transparent Tunneling(투명 터널링 활성화)을 클릭하고 IPSec over UDP(NAT / PAT) 라디오 버튼을 클릭합니다. 그런 다음 저장을 클릭하고 연결을 테스트합니다.

ASA가 NAT 디바이스 역할을 하므로 ACL 컨피그레이션을 통해 NAT-T, UDP 500 및 ESP 포트에 UDP 4500을 허용하는 것이 중요합니다.

ASA의 ACL 컨피그레이션에 대한 자세한 내용은 NAT를 사용하여 방화벽을 통해 IPsec 터널 구성을 참조하십시오.

올바르게 연결 테스트

VPN 연결은 암호화를 수행하는 엔드포인트 디바이스 뒤의 디바이스에서 테스트하는 것이 이상적이지만, 많은 사용자가 암호화를 수행하는 디바이스에서 ping 명령을 사용하여 VPN 연결을 테스트합니다.

ping은 일반적으로 이 용도로 작동하지만 올바른 인터페이스에서 ping을 시작하는 것이 중요합니다.

ping이 잘못 제공되면 VPN 연결이 제대로 작동하지 않는 것처럼 보일 수 있습니다. 다음은 한 가지 예입니다.

라우터 A 암호화 ACL

```
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

라우터 B 암호화 ACL

```
access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
```

이러한 상황에서는 두 라우터 뒤의 내부 네트워크에서 페이징을 소싱해야 합니다. 이는 암호화 ACL이 해당 소스 주소로 트래픽을 암호화하도록 구성되어 있기 때문입니다.

두 라우터의 외부 인터페이스에서 제공된 매핑은 암호화되지 않습니다. 특권 EXEC 모드에서 ping 명령의 확장 옵션을 사용하여 라우터의 내부 인터페이스에서 ping을 시작합니다.

<#root>

```
routerA#

ping

Protocol [ip]:

Target IP address: 192.168.200.10

Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 192.168.100.1

Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.100.1

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = ½/4 ms
```

이 다이어그램의 라우터를 ASA 보안 어플라이언스로 교체했다고 가정해 보십시오. 연결성을 테스트하는 데 사용되는 ping은 inside 키워드를 사용하여 내부 인터페이스에서 가져올 수도 있습니다.

<#root>

```
securityappliance#

ping inside 192.168.200.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

보안 어플라이언스의 내부 인터페이스를 ping으로 대상으로 삼지 않는 것이 좋습니다.

ping으로 내부 인터페이스를 대상으로 해야 하는 경우 해당 인터페이스에서 management-access를 활성화해야 합니다. 그렇지 않으면 어플라이언스가 응답하지 않습니다.

```
<#root>

securityappliance(config)#

management-access inside
```

연결에 문제가 있을 경우 VPN의 1단계도 작동하지 않습니다.

ASA에서 연결이 실패할 경우 SA 출력은 이 예와 유사합니다. 이는 잘못된 암호화 피어 컨피그레이션 및/또는 잘못된 ISAKMP 제안 컨피그레이션이 발생할 수 있음을 나타냅니다.

```
<#root>

Router#

show crypto isakmp sa


1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG2
```

상태는 MM_WAIT_MSG2에서 MM_WAIT_MSG5까지이며, 이는 MM(Main Mode)에서 관련 상태 교환의 실패를 나타냅니다.

1단계가 작동 중일 때의 Crypto SA 출력은 다음 예와 유사합니다.

```
<#root>

Router#

show crypto isakmp sa


1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

ISAKMP 활성화

IPsec VPN 터널이 작동한다는 표시가 없는 경우 ISAKMP가 활성화되지 않았을 수 있습니다. 디바이스에서 ISAKMP를 활성화했는지 확인합니다.

다음 명령 중 하나를 사용하여 디바이스에서 ISAKMP를 활성화합니다.

Cisco IOS®

```
<#root>

router(config)#

crypto isakmp enable
```

Cisco ASA(교체아웃사이드를 원하는 인터페이스로)

```
<#root>

securityappliance(config)#

crypto isakmp enable outside
```

외부 인터페이스에서 ISAKMP를 활성화할 때 다음 오류가 발생할 수도 있습니다.

```
UDP: ERROR - socket <unknown> 62465 in used
ERROR: IkeReceiverInit, unable to bind to port
```

ASA 뒤에 있는 클라이언트가 PAT를 udp 포트 500으로 가져와서 인터페이스에서 isakmp를 활성화할 수 있기 때문에 오류가 발생할 수 있습니다. PAT 변환이 제거되면(clear xlate) isakmp를 활성화할 수 있습니다.

UDP 500 및 4500 포트 번호가 피어와의 ISAKMP 연결 협상을 위해 예약되어 있는지 확인합니다.

인터페이스에서 ISAKMP가 활성화되지 않은 경우 VPN 클라이언트에는 다음과 같은 오류 메시지가 표시됩니다.

```
Secure VPN connection terminated locally by client.
Reason 412: The remote peer is no longer responding
```

이 오류를 해결하려면 VPN 게이트웨이의 암호화 인터페이스에서 ISAKMP를 활성화합니다.

PFS 활성화/비활성화

IPsec 협상에서 PFS(Perfect Forward Secrecy)는 각 새 암호화 키가 이전 키와 관련이 없도록 합니다.

두 터널 피어 모두에서 PFS를 활성화하거나 비활성화합니다. 그렇지 않으면 ASA/Cisco IOS® 라우터에서 LAN-to-LAN(L2L) IPsec 터널이 설정되지 않습니다.

PFS(Perfect Forward Secrecy)는 Cisco의 독점 기술이며 서드파티 디바이스에서 지원되지 않습니다.

ASA:

PFS는 기본적으로 비활성화되어 있습니다. PFS를 활성화하려면 group-policy 컨피그레이션 모드에서 enable 키워드와 함께 pfscommand를 사용합니다. PFS를 비활성화하려면 disable 키워드를 입력합니다.

```
<#root>

hostname(config-group-policy)#

pfs {enable | disable}
```

컨피그레이션에서 PFS 특성을 제거하려면 이 명령의 no 형식을 입력합니다.

그룹 정책은 다른 그룹 정책에서 PFS에 대한 값을 상속할 수 있습니다. 값 전송을 방지하려면 이 명령의 no 형식을 입력합니다.

```
<#root>

hostname(config-group-policy)#

no pfs
```

Cisco IOS® 라우터:

이 암호화 맵 엔트리에 대해 새 보안 연결이 요청될 때 IPsec에서 PFS를 요청하도록 지정하려면 암호화 맵 컨피그레이션 모드에서 set pfscommand를 사용합니다.

IPsec이 새 보안 연결에 대한 요청을 받을 때 PFS를 요구하도록 지정하려면 암호화 맵 컨피그레이션 모드에서 set pfscommand를 사용합니다.

IPsec에서 PFS를 요청하지 않도록 지정하려면 이 명령의 no 형식을 사용합니다. 기본적으로 PFS는 요청되지 않습니다. 이 명령으로 그룹을 지정하지 않으면 group1이 기본값으로 사용됩니다.

```
set pfs [group1 | group2]
no set pfs
```

set pfs 명령의 경우

- group1 - 새 Diffie-Hellman 교환을 수행할 때 IPsec에서 768비트 Diffie-Hellman 프라임 모듈러스 그룹을 사용하도록 지정합니다.
- group2 - 새 Diffie-Hellman 교환을 수행할 때 IPsec에서 1024비트 Diffie-Hellman 프라임 모듈러스 그룹을 사용하도록 지정합니다.

예:

<#root>

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#
```

set pfs group2

기존 또는 현재 보안 연결 지우기(터널)

Cisco IOS®® 라우터에서 이 오류 메시지가 발생하면 SA가 만료되었거나 지워진 것이 문제입니다.

원격 터널 엔드 디바이스는 만료된 SA를 사용하여 패킷(SA 설정 패킷이 아님)을 전송하는지 알지 못합니다.

새 SA가 설정되면 통신이 다시 시작됩니다. 따라서 새 SA를 생성하고 터널을 다시 설정하기 위해 터널을 통과하는 흥미로운 트래픽을 시작합니다.

<#root>

%CRYPTO-4-IKMP_NO_SA: IKE message from x.x.x.x has no SA

ISAKMP(Phase I) 및 IPsec(Phase II) SA(Security Association)를 지울 경우 IPsec VPN 문제를 해결하는 가장 간단하고 가장 적합한 솔루션입니다.

SA를 지우면 트러블슈팅할 필요 없이 다양한 오류 메시지 및 이상한 동작을 자주 해결할 수 있습니다.

이 기술은 어떤 상황에서도 쉽게 사용할 수 있지만, 현재 IPsec VPN 컨피그레이션을 변경하거나 추가한 후에는 SA를 지워야 하는 경우가 거의 항상 있습니다.

또한 특정 보안 연결만 지울 수 있지만, 가장 큰 이점은 디바이스에서 전체적으로 SA를 지울 때 얻을 수 있습니다.

보안 연결을 지운 후에는 터널을 통해 트래픽을 전송하여 다시 설정해야 할 수 있습니다.

경고: 삭제할 보안 연결을 지정하지 않는 한, 여기에 나열된 명령은 디바이스의 모든 보안 연결을 지울 수 있습니다. 다른 IPsec VPN 터널이 사용 중인 경우 주의해서 진행합니다.

1. 지우기 전에 보안 연결 보기

    a. Cisco IOS®

    <#root>

    router#

    show crypto isakmp sa

    router#

    show crypto ipsec sa

    b. Cisco ASA 보안 어플라이언스

    <#root>

    securityappliance#

    show crypto isakmp sa

    securityappliance#

    show crypto ipsec sa

2. 보안 연결을 지웁니다. 각 명령은 굵게 표시된 대로 입력하거나 옵션과 함께 입력할 수 있습니다.

    a. Cisco IOS®

        a. ISAKMP(1단계)

        <#root>

        router#

        clear crypto isakmp

        ?
          <0 - 32766> connection id of SA
          <cr>

        b. IPsec(단계 II)

        <#root>

        router#

        clear crypto sa

```
?
 counters  Reset the SA counters
 map       Clear all SAs for a given crypto map
 peer      Clear all SAs for a given crypto peer
 spi       Clear SA by SPI
 <cr>
```

b. Cisco ASA 보안 어플라이언스

a. ISAKMP(1단계)

```
<#root>

securityappliance#

clear crypto isakmp sa
```

b. IPsec(단계 II)

```
<#root>

security appliance#

clear crypto ipsec sa

 ?

  counters  Clear IPsec SA counters
  entry     Clear IPsec SAs by entry
  map       Clear IPsec SAs by map
  peer      Clear IPsec SA by peer
  <cr>
```

ISAKMP 수명 확인

L2L 터널을 통해 사용자 연결이 자주 끊기는 경우 ISAKMP SA에 구성된 수명이 더 짧을 수 있습니다.

ISAKMP 수명에 불일치가 발생하는 경우 %ASA-5-713092(그룹 = x.x.x.x, IP = x.x.x, 1단계 키 재설정 중 /ASA에서 충돌 오류 메시지로 인한 실패)를 받을 수 있습니다.

기본값은 86,400초 또는 24시간입니다. 일반적으로 수명이 짧으면 ISAKMP 협상을 더 안전하게 수행할 수 있지만(최대 한 시점까지), 수명이 짧을수록 보안 어플라이언스는 향후 IPsec SA를 더 빨리 설정합니다.

두 피어의 두 정책이 모두 동일한 암호화, 해시, 인증 및 Diffie-Hellman 매개변수 값을 포함하고, 원격 피어의 정책이 비교 정책의 수명보다 작거나 같은 수명을 지정하는 경우 일치가 이루어집니다.

수명이 동일하지 않으면 원격 피어의 정책에서 더 짧은 수명이 사용됩니다. 허용 가능한 일치 항목을 찾지 못하면 IKE가 협상을 거부하고 IKE SA가 설정되지 않습니다.

SA 수명을 지정합니다. 이 예에서는 수명을 4시간(14400초)으로 설정합니다. 기본값은 86400초(24시간)입니다.

ASA

<#root>

```
hostname(config)#
isakmp policy 2 lifetime  14400
```

Cisco IOS® 라우터

<#root>

```
R2(config)#
crypto isakmp policy 10
R2(config-isakmp)#
lifetime 86400
```

구성된 최대 수명을 초과할 경우 VPN 연결이 종료되면 다음과 같은 오류 메시지가 표시됩니다.

클라이언트에서 보안 VPN 연결을 로컬로 종료했습니다. 이유 426: 구성된 최대 수명이 초과되었습니다.

이 오류 메시지를 해결하려면 IKE 보안 연결의 수명을 무한대로 설정하려면 thlifetimevalue를 0(0)으로 설정합니다. VPN은 항상 연결되어 있으며 종료되지 않습니다.

```
hostname(config)#isakmp policy 2 lifetime 0
```

또한 문제를 해결하기 위해 그룹 정책에서 rexauth를 비활성화할 수 있습니다.

ISAKMP 킵얼라이브 활성화 또는 비활성화

ISAKMP 킵얼라이브를 구성하는 경우 VPN 클라이언트, 터널 및 일정 기간 동안 사용하지 않은 후 삭제된 터널이 포함된 LAN-to-LAN 또는 원격 액세스 VPN이 산발적으로 삭제되는 것을 방지할 수 있습니다.

이 기능을 사용하면 터널 엔드포인트가 원격 피어의 지속적인 프레즌스를 모니터링하고 해당 피어에 자신의 프레즌스를 보고할 수 있습니다.

피어가 응답하지 않으면 엔드포인트는 연결을 제거합니다.

ISAKMP 킵얼라이브가 작동하려면 두 VPN 엔드포인트 모두 이를 지원해야 합니다.

다음 명령을 사용하여 Cisco IOS®에서 ISAKMP 킵얼라이브를 구성합니다.

```
<#root>

router(config)#

crypto isakmp keepalive 15
```

ASA Security Appliance에서 ISAKMP 킵얼라이브를 구성하려면 다음 명령을 사용합니다.

터널 그룹 10.165.205.222용 Cisco ASA

```
<#root>

securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes


securityappliance(config-tunnel-ipsec)#

isakmp keepalive
   threshold 15 retry 10
```

예를 들어 VPN 클라이언트가 DPD 패킷을 방지하는 방화벽 뒤에 있는 경우 문제를 해결하려면 이 기능을 비활성화해야 합니다.

Cisco ASA, 터널 그룹 이름 10.165.205.222

기본적으로 활성화되어 있는 IKE 킵얼라이브 처리를 비활성화합니다.

```
<#root>

securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes


securityappliance(config-tunnel-ipsec)#

isakmp keepalive


disable
```

Cisco VPN Client 4.x에 대해 Keepalive 비활성화

문제가 발생한 클라이언트 PC에서 %System Root% > Program Files > Cisco Systems >VPN Client > Profiles로 이동하여 IKE 킵얼라이브를 비활성화하고 연결에 대해 PCF 파일을 편집합니다.

ForceKeepAlives=0(기본값)을 ForceKeepAlives=1로 변경합니다.

Keepalive는 Cisco 소유의 제품이며 타사 장치에서 지원되지 않습니다.

사전 공유 키 다시 입력 또는 복구

대부분의 경우 IPsec VPN 터널이 작동하지 않을 때 단순한 입력 오류가 원인일 수 있습니다. 예를 들어, 보안 어플라이언스에서 사전 공유 키를 입력하면 숨겨집니다.

이러한 난독화 때문에 키가 잘못되었는지 확인할 수 없습니다. 각 VPN 엔드포인트에서 사전 공유 키를 올바르게 입력했는지 확인합니다.

키를 다시 입력하여 키가 올바른지 확인합니다. 이 방법은 심층적인 트러블슈팅을 방지하는 데 도움이 되는 간단한 솔루션입니다.

원격 액세스 VPN에서 CiscoVPN 클라이언트에 유효한 그룹 이름과 사전 공유 키가 입력되었는지 확인합니다.

그룹 이름 또는 사전 공유 키가 VPN 클라이언트와 헤드 엔드 디바이스 간에 일치하지 않는 경우 이 오류가 발생할 수 있습니다.

```
 1 12:41:51.900 02/18/06 Sev=Warning/3 IKE/0xE3000056
 The received HASH payload cannot be verified
 2 12:41:51.900 02/18/06 Sev=Warning/2 IKE/0xE300007D
Hash verification failed
3      14:37:50.562  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
4      14:37:50.593  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
5      14:44:15.937  10/05/06  Sev=Warning/2 IKE/0xA3000067
Received Unexpected InitialContact Notify (PLMgrNotify:888)
6      14:44:36.578  10/05/06  Sev=Warning/3 IKE/0xE3000056
The received HASH payload cannot be verified
7      14:44:36.593  10/05/06  Sev=Warning/2 IKE/0xE300007D
Hash verification failed... possibly be configured with invalid group password.
8      14:44:36.609  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
9      14:44:36.640  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
```

경고: 암호화 관련 명령을 제거할 경우 VPN 터널 중 하나 또는 전체를 다운할 수 있습니다. 암호화 관련 명령을 제거하기 전에 이러한 명령을 신중하게 사용하고 조직의 변경 제어 정책을 참조하십시

오.

다음 명령을 사용하여 피어 10.0.0.1 또는 groupvpngrouppin Cisco IOS®에 대한 사전 공유 keysecretkey를 제거하고 다시 입력합니다.

Cisco LAN-to-LAN VPN

<#root>

```
router(config)#

no crypto isakmp key secretkey
   address 10.0.0.1

router(config)#

crypto isakmp key secretkey
   address 10.0.0.1
```

Cisco 원격 액세스 VPN

<#root>

```
router(config)#

crypto isakmp client configuration
   group vpngroup

router(config-isakmp-group)#

no key secretkey

router(config-isakmp-group)#

key secretkey
```

/ASA Security Appliance에서 피어 10.0.0.1에 대한 사전 공유 keysecretkeye를 제거하고 다시 입력하려면 다음 명령을 사용합니다.

Cisco 6.x

<#root>

```
(config)#

no isakmp key secretkey address 10.0.0.1

(config)#

isakmp key secretkey address 10.0.0.1
```

Cisco /ASA 7.x 이상

<#root>

securityappliance(config)#

tunnel-group 10.0.0.1
ipsec-attributes

securityappliance(config-tunnel-ipsec)#

no ikev1 pre-shared-key

securityappliance(config-tunnel-ipsec)#

ikev1

pre-shared-key
secretkey

일치하지 않는 사전 공유 키

VPN 터널의 시작이 분리됩니다. 이 문제는 I단계 협상 중에 일치하지 않는 사전 공유 키 때문에 발생합니다.

crypto isakmp 명령의 MM_WAIT_MSG_6 메시지는 다음 예에 표시된 대로 일치하지 않는 사전 공유 키를 나타냅니다.

<#root>

ASA#

show crypto isakmp sa

```
Active SA: 1
Rekey SA: 0 (A tunnel reports 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1         IKE Peer: 10.7.13.20
             Type : L2L                                Role : initiator
             Rekey : no                                State :
```

MM_WAIT_MSG_6

이 문제를 해결하려면 두 어플라이언스 모두에서 사전 공유 키를 다시 입력하십시오. 사전 공유 키는 고유해야 하며 일치해야 합니다. 자세한 내용은 사전 공유 키 다시 입력 또는 복구를 참조하십시오.

암호화 맵 제거 및 다시 적용

보안 연결을 지우더라도 IPsec VPN 문제가 해결되지 않을 경우, VPN 터널의 간헐적인 삭제 및 일부 VPN 사이트의 가동 실패와 같은 다양한 문제를 해결하려면 관련 암호화 맵을 제거하고 다시 적용하십시오.

경고: 인터페이스에서 암호화 맵을 제거하면 그 암호화 맵과 연결된 IPsec 터널이 자동으로 종료됩니다. 이러한 단계를 신중하게 진행하고 조직의 변경 제어 정책을 고려한 후 진행합니다.

Cisco IOS®에서 암호화 맵을 제거하고 교체하려면 다음 명령을 사용합니다.

인터페이스에서 암호화 맵을 제거하는 것부터 시작합니다. crypto mapcommand의 no 형식을 사용합니다.

```
<#root>

router(config-if)#

no crypto map mymap
```

계속해서 enoform을 사용하여 전체 암호화 맵을 제거합니다.

```
<#root>

router(config)#

no crypto map mymap 10
```

피어 10.0.0.1에 대한 인터페이스 Ethernet0/0의 암호화 맵을 교체합니다. 다음 예에서는 필요한 최소 암호화 맵 컨피그레이션을 보여줍니다.

```
<#root>

router(config)#

crypto map mymap 10 ipsec-isakmp

router(config-crypto-map)#

match address 101

router(config-crypto-map)#

set transform-set mySET

router(config-crypto-map)#

set peer 10.0.0.1

router(config-crypto-map)#

exit

router(config)#
```

```
interface ethernet0/0

router(config-if)#

crypto map mymap
```

ASA에서 암호화 맵을 제거하고 교체하려면 다음 명령을 사용합니다.

인터페이스에서 암호화 맵을 제거하는 것부터 시작합니다. crypto mapcommand의 no 형식을 사용합니다.

<#root>

```
securityappliance(config)#

no crypto map mymap interface outside
```

계속해서 thenoform을 사용하여 다른 암호화 맵 명령을 제거합니다.

<#root>

```
securityappliance(config)#

no crypto map mymap 10 match
   address 101

securityappliance(config)#

no crypto map mymap set
   transform-set mySET

securityappliance(config)#

no crypto map mymap set
   peer 10.0.0.1
```

피어 10.0.0.1의 암호화 맵을 대체합니다. 다음 예에서는 필요한 최소 암호화 맵 컨피그레이션을 보여줍니다.

<#root>

```
securityappliance(config)#

crypto map mymap 10 ipsec-isakmp

securityappliance(config)#

crypto map mymap 10
   match address 101

securityappliance(config)#

crypto map mymap 10 set
```

```
   transform-set mySET

securityappliance(config)#

crypto map mymap 10 set
   peer 10.0.0.1

securityappliance(config)#

crypto map mymap interface outside
```

암호화 맵을 제거하고 다시 적용하면 헤드엔드의 IP 주소가 변경된 경우에도 연결 문제가 해결됩니다.

sysopt 명령이 있는지 확인합니다(ASA에만 해당).

commandssysopt connection permit-ipsecandsysopt connection permit-vpnallow IPsec 터널의 패킷 및 페이로드를 보안 어플라이언스의 인터페이스 ACL을 우회하도록 허용합니다.

보안 어플라이언스에서 종료되는 IPsec 터널은 이러한 명령 중 하나가 활성화되지 않은 경우 실패할 가능성이 높습니다.

Security Appliance Software Version 7.0 이하에서 이 상황에 대한 관련 sysopt 명령은 sysopt connection permit-ipsec입니다.

Security Appliance Software Version 7.1(1) 이상에서 이 상황에 대한 관련 sysopt 명령은 sysopt connection permit-vpn입니다.

6.x에서는 이 기능이 기본적으로 비활성화되어 있습니다. /ASA 7.0(1) 이상에서는 이 기능이 기본적으로 활성화되어 있습니다. 다음 show 명령을 사용하여 디바이스에서 관련 sysoptcommand가 활성화되었는지 확인합니다.

Cisco ASA

<#root>

```
securityappliance#

show running-config all sysopt

no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret

sysopt connection permit-vpn


!--- sysopt connection permit-vpn is enabled !--- This device is running 7.2(2)
```

디바이스에 대해 correctsysoptcommand를 활성화하려면 다음 명령을 사용합니다.

Cisco ASA

<#root>

securityappliance(config)#

sysopt connection permit-vpn

thesysopt connectioncommand를 사용하지 않으려면 소스에서 목적지까지 필요한 흥미로운 트래픽을 명시적으로 허용합니다.

예를 들어, 외부 ACL에서는 원격 디바이스의 원격-로컬 LAN 및 원격 디바이스의 외부 인터페이스용 "UDP 포트 500"을 로컬 디바이스의 외부 인터페이스로 설정합니다.

ISAKMP ID 확인

IPsec VPN 터널이 IKE 협상 내에서 실패한 경우, 실패는 피어가 피어의 ID를 인식할 수 없거나 를 통해 발생할 수 있습니다.

두 피어가 IKE를 사용하여 IPsec 보안 연결을 설정하면 각 피어는 ISAKMP ID를 원격 피어로 전송합니다.

각 ISAKMP ID가 설정된 방식에 따라 IP 주소 또는 호스트 이름을 전송합니다.

기본적으로 방화벽 유닛의 ISAKMP ID는 IP 주소로 설정됩니다.

일반적으로 IKE 협상 실패를 방지하기 위해 보안 어플라이언스 및 피어의 ID를 동일한 방법으로 설정합니다.

피어로 전송할 2단계 ID를 설정하려면 글로벌 컨피그레이션 모드에서 isakmp identitycommand를 사용합니다.

```
crypto isakmp identity address

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with pre-shared key as authentication typ
```

또는

```
crypto isakmp identity auto

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by connection typ
```

또는

```
crypto isakmp identity hostname

!--- Uses the fully-qualified domain name of !--- the host exchange ISAKMP identity information (defaul
```

ASA 컨피그레이션 마이그레이션 툴을 사용하여 컨피그레이션을 ASA로 변경한 후 VPN 터널이 시작되지 않습니다. 다음 메시지가 로그에 나타납니다.

[IKEv1]: 그룹 = x.x.x.x, IP = x.x.x, 오래된 PeerTblEntry가 있습니다. 제거됨!

[IKEv1]: 그룹 = x.x.x.x, IP = x.x.x, 상관기 테이블에서 피어 제거 실패, 일치하지 않음!

[IKEv1]: 그룹 = x.x.x.x, IP = x.x.x, construct_ipsec_delete(): 2단계 SA를 식별하는 SPI 없음!

[IKEv1]: 그룹 = x.x.x.x, IP = x.x.x, 상관기 테이블에서 피어 제거 실패, 일치하지 않음!

유휴/세션 시간 초과 확인

유휴 시간 제한을 30분(기본값)으로 설정하면 30분 동안 트래픽이 통과하지 않으면 터널이 삭제됩니다.

VPN 클라이언트는 유휴 시간 제한 매개변수에 관계없이 30분 후에 연결이 끊어지고 PEER_**DELETE-IKE_DELETE_UNSPECIFIEDerror**가 발생합니다.

터널을 항상 활성화하려면 유휴 시간 초과 및 세션 시간 초과를 구성합니다. 이렇게 하면 서드파티 디바이스를 사용하더라도 터널이 삭제되지 않습니다.

ASA

사용자 시간 초과 기간을 구성하려면 group-policy 컨피그레이션 모드 또는 username 컨피그레이션 모드에서 vpn-idle-timeoutcommand를 입력합니다.

<#root>

```
hostname(config)#

group-policy DfltGrpPolicy attributes

hostname(config-group-policy)#

vpn-idle-timeout none
```

그룹 정책 컨피그레이션 모드 또는 사용자 이름 컨피그레이션 모드에서 vpn-session-timeoutcommand를 사용하여 VPN 연결에 대한 최대 시간을 구성합니다.

<#root>

hostname(config)#

group-policy DfltGrpPolicy attributes

hostname(config-group-policy)#

vpn-session-timeout none

tunnel-allconfigured가 있는 경우, VPN-idle timeout을 구성하더라도 모든 트래픽이 터널을 통과하기 때문에(tunnel-all이 구성되기 때문에) 작동하지 않기 때문에 idle-timeouts를 구성할 필요가 없습니다.

따라서 흥미로운 트래픽(또는 PC에서 생성된 트래픽)은 흥미롭고 유휴 시간 초과가 발생하지 않습니다.

Cisco IOS® 라우터

IPsec SA 유휴 타이머를 구성하려면 글로벌 컨피그레이션 모드 또는 암호화 맵 컨피그레이션 모드에서 crypto ipsec security-association idle-timecommand를 사용합니다.

기본적으로 IPsec SA 유휴 타이머는 비활성화되어 있습니다.

<#root>

crypto ipsec security-association idle-time

seconds

유휴 타이머로 인해 비활성 피어가 SA를 유지할 수 있는 시간이 초 단위로 측정됩니다. seconds 인수의 유효한 값은 60~86400입니다.

ACL이 올바르고 암호화 맵에 바인딩되어 있는지 확인

일반적인 IPsec VPN 컨피그레이션에는 2개의 액세스 목록이 사용됩니다. NAT 프로세스에서 VPN 터널로 향하는 트래픽을 제외하는 데 하나의 액세스 목록이 사용됩니다.

다른 액세스 목록은 암호화할 트래픽을 정의합니다. 여기에는 LAN-to-LAN 설정의 암호화 ACL 또는 원격 액세스 구성의 스플릿 터널 ACL이 포함됩니다.

이러한 ACL이 잘못 구성되거나 누락되면 트래픽이 VPN 터널을 통해 한 방향으로 흐르거나 터널을 통해 전혀 전송되지 않을 수 있습니다.

글로벌 컨피그레이션 모드에서 crypto map match address 명령을 사용하여 암호화 맵이 있는 암호화 ACL을 바인딩해야 합니다.

IPsec VPN 컨피그레이션을 완료하는 데 필요한 모든 액세스 목록을 구성했으며 이러한 액세스 목록이 올바른 트래픽을 정의하는지 확인하십시오.

이 목록에는 ACL이 IPsec VPN 문제의 원인이라고 의심되는 경우 확인할 수 있는 간단한 내용이 포함되어 있습니다.

NAT 예외 및 암호화 ACL이 올바른 트래픽을 지정하는지 확인합니다.

여러 VPN 터널과 여러 암호화 ACL이 있는 경우 해당 ACL이 중복되지 않는지 확인합니다.

디바이스가 NAT 예외 ACL을 사용하도록 구성되어 있는지 확인합니다. 라우터에서 theroute-mapcommand를 사용한다는 것을 의미합니다.

ASA에서 이는 thenat (0) 명령을 사용함을 의미합니다. NAT 예외 ACL은 LAN-to-LAN 및 원격 액세스 구성에 모두 필요합니다.

여기서 Cisco IOS® 라우터는 NAT에서 192.168.100.0 /24와 192.168.200.0 /24 또는 192.168.1.0 /24 사이에 전송되는 트래픽을 제외하도록 구성됩니다. 다른 곳으로 향하는 트래픽에는 NAT 오버로드가 적용됩니다.

```
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.1.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 any

route-map nonat permit 10
  match ip address 110

ip nat inside source route-map nonat interface FastEthernet0/0 overload
```

NAT 예외 ACL은 IP 주소 또는 IP 네트워크에서만 작동하며(예: 위에서 언급한 예(access-list noNAT), 암호화 맵 ACL과 동일해야 합니다.

NAT 예외 ACL은 포트 번호(예: 23, 25,...)와 작동하지 않습니다.

VPN을 통해 네트워크 간 음성 통화가 전달되는 VOIP 환경에서는 NAT 0 ACL이 제대로 구성되지 않으면 음성 통화가 작동하지 않습니다.

트러블슈팅을 수행하기 전에 NAT 제외 ACL의 컨피그레이션이 잘못되었을 수 있으므로 VPN 연결 상태를 확인하는 것이 좋습니다.

NAT 예외(nat 0) ACL에 잘못된 컨피그레이션이 있는 경우 표시된 대로 오류 메시지를 받을 수 있습니다.

```
%ASA-3-305005: No translation group found for
udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p
```

잘못된 예:

<#root>

```
access-list noNAT extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
```

eq 25

NAT 예외(nat 0)가 작동하지 않으면 이를 제거하고 NAT 0 명령을 실행하여 동작합니다.

ACL이 역방향이 아닌지, 올바른 유형인지 확인하십시오.

LAN-to-LAN 컨피그레이션을 위한 암호화 및 NAT 예외 ACL은 ACL이 구성된 디바이스의 관점에서 작성해야 합니다.

즉, ACL은 다른 ACL에 도달해야 합니다. 이 예에서는 LAN-to-LAN 터널이 192.168.100.0 /24와 192.168.200.0 /24 사이에 설정됩니다.

라우터 A 암호화 ACL

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
```

라우터 B 암호화 ACL

```
access-list 110 permit ip 192.168.200.0 0.0.0.255
   192.168.100.0 0.0.0.255
```

여기서는 설명하지 않지만 ASA Security Appliance에도 동일한 개념이 적용됩니다.

ASA에서 원격 액세스 컨피그레이션을 위한 스플릿 터널 ACL은 VPN 클라이언트가 액세스해야 하는 네트워크에 대한 트래픽을 허용하는 액세스 목록을 준수해야 합니다.

Cisco IOS® 라우터는 스플릿 터널에 확장 ACL을 사용할 수 있습니다. 확장 액세스 목록에서 스플릿 터널 ACL의 소스에서 'any'를 사용하는 것은 스플릿 터널을 비활성화하는 것과 유사합니다.

스플릿 터널에 확장 ACL의 소스 네트워크만 사용합니다.

올바른 예:

<#root>

```
access-list 140 permit ip
```

10.1.0.0 0.0.255.255

```
 10.18.0.0 0.0.255.255
```

잘못된 예:

<#root>

```
access-list 140 permit ip
any
 10.18.0.0 0.0.255.255
```

Cisco IOS®

<#root>

```
router(config)#
access-list 10 permit ip 192.168.100.0
router(config)#
crypto isakmp client configuration group MYGROUP
router(config-isakmp-group)#
acl 10
```

Cisco ASA

<#root>

```
securityappliance(config)#
access-list 10 standard
   permit 192.168.100.0 255.255.255.0
securityappliance(config)#
group-policy MYPOLICY internal
securityappliance(config)#
group-policy MYPOLICY attributes
securityappliance(config-group-policy)#
split-tunnel-policy
   tunnelspecified
securityappliance(config-group-policy)#
split-tunnel-network-list
   value 10
```

ASA 버전 8.3의 Site-to-Site VPN 터널용 NAT 예외 컨피그레이션:

두 ASA 모두 버전 8.3을 사용하는 경우 HOASA와 BOASA 간에 사이트 대 사이트 VPN을 설정해야 합니다. HOASA의 NAT 예외 컨피그레이션은 다음과 비슷합니다.

```
object network obj-local
subnet 192.168.100.0 255.255.255.0
object network obj-remote
subnet 192.168.200.0 255.255.255.0
nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote objremote
```

ISAKMP 정책 확인

IPsec 터널이 UP가 아닌 경우 ISAKMP 정책이 원격 피어와 일치하는지 확인합니다. 이 ISAKMP 정책은 L2L(Site-to-Site) 및 원격 액세스 IPsec VPN에 모두 적용됩니다.

Cisco VPN 클라이언트 또는 Site-to-Site VPN이 원격 엔드 디바이스로 터널을 설정할 수 없는 경우 두 피어에 동일한 암호화, 해시, 인증 및 Diffie-Hellman 매개변수 값이 포함되어 있는지 확인합니다.

원격 피어 정책이 개시자가 전송한 정책의 수명보다 작거나 같은 수명을 지정하는 경우를 확인합니다.

수명이 동일하지 않으면 보안 어플라이언스에서 더 짧은 수명을 사용합니다. 허용 가능한 일치 항목이 없으면 ISAKMP가 협상을 거부하고 SA가 설정되지 않습니다.

```
"Error: Unable to remove Peer TblEntry, Removing peer from peer table
failed, no match!"
```

자세한 로그 메시지는 다음과 같습니다.

```
4|Mar 24 2010 10:21:50|713903: IP = X.X.X.X, Error: Unable to remove PeerTblEntry
3|Mar 24 2010 10:21:50|713902: IP = X.X.X.X, Removing peer from peer table failed,
no match!
3|Mar 24 2010 10:21:50|713048: IP = X.X.X.X, Error processing payload: Payload ID: 1
4|Mar 24 2010 10:21:49|713903: IP = X.X.X.X, Information Exchange processing failed
5|Mar 24 2010 10:21:49|713904: IP = X.X.X.X, Received an un-encrypted
NO_PROPOSAL_CHOSEN notify message, drop
```

이 메시지는 일반적으로 일치하지 않는 ISAKMP 정책 또는 누락된 NAT 0 문 때문에 나타납니다.

또한 다음 메시지가 나타납니다.

```
Error Message    %ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when
P1 SA is complete.
```

이 메시지는 1단계가 완료된 후 2단계 메시지가 대기열에 있음을 나타냅니다. 이 오류 메시지는 다음 이유 중 하나로 인해 발생합니다.

- 모든 피어에서 위상 불일치
- ACL은 피어의 1단계 완료를 차단합니다

이 메시지는 일반적으로 피어 테이블에서 피어 제거 실패 후 발생합니다. `match!` 오류 메시지입니다.

Cisco VPN Client가 헤드엔드 디바이스에 연결할 수 없는 경우, ISAKMP 정책의 불일치가 문제가 될 수 있습니다. 헤드엔드 디바이스는 Cisco VPN Client의 IKE 제안서 중 하나와 일치해야 합니다.

ASA에서 사용되는 ISAKMP 정책 및 IPsec Transform-set의 경우 Cisco VPN 클라이언트는 DES와 SHA가 조합된 정책을 사용할 수 없습니다.

DES를 사용하는 경우 해시 알고리즘에 MD5를 사용해야 합니다. 또는 SHA가 포함된 3DES와 MD5가 포함된 3DES의 다른 조합을 사용할 수 있습니다.

라우팅이 올바른지 확인합니다.

라우터 및 ASA 보안 어플라이언스와 같은 암호화 디바이스에 VPN 터널을 통해 트래픽을 전송할 수 있는 적절한 라우팅 정보가 있는지 확인합니다.

게이트웨이 디바이스 뒤에 다른 라우터가 있는 경우 해당 라우터가 터널에 도달하는 방법과 반대쪽에 있는 네트워크를 알고 있는지 확인하십시오.

VPN 구축에서 라우팅의 한 가지 주요 구성 요소는 RRI(Reverse Route Injection)입니다.

RRI는 원격 네트워크 또는 VPN 클라이언트에 대한 동적 항목을 VPN 게이트웨이의 라우팅 테이블에 배치합니다.

이러한 경로는 RRI에 의해 설치된 경로가 EIGRP 또는 OSPF와 같은 라우팅 프로토콜을 통해 재배포될 수 있기 때문에 네트워크가 설치된 장치는 물론 네트워크의 다른 장치에도 유용합니다.

LAN-to-LAN 컨피그레이션에서는 각 엔드포인트가 트래픽을 암호화할 네트워크에 대한 경로 또는 경로를 갖는 것이 중요합니다.

이 예에서 라우터 A는 라우터 B에서 10.89.129.2를 통과하는 네트워크에 대한 경로를 가지고 있어야 합니다. 라우터 B는 192.168.100.0 /24와 유사한 경로를 가져야 합니다.

각 라우터가 적절한 경로를 인식하도록 하는 첫 번째 방법은 각 대상 네트워크에 대한 고정 경로를 구성하는 것입니다. 예를 들어 라우터 A는 다음과 같은 경로 명령문을 구성할 수 있습니다.

```
ip route 0.0.0.0 0.0.0.0 172.22.1.1
ip route 192.168.200.0 255.255.255.0 10.89.129.2
```

```
ip route 192.168.210.0 255.255.255.0 10.89.129.2
ip route 192.168.220.0 255.255.255.0 10.89.129.2
ip route 192.168.230.0 255.255.255.0 10.89.129.2
```

라우터 A를 ASA로 교체한 경우 컨피그레이션은 다음과 같을 수 있습니다.

```
route outside 0.0.0.0 0.0.0.0 172.22.1.1
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
```

각 엔드포인트 뒤에 많은 수의 네트워크가 존재하는 경우 고정 경로의 컨피그레이션을 유지 관리하기가 어려워집니다.

대신 설명된 대로 Reverse Route Injection을 사용하는 것이 좋습니다. RRI는 암호화 ACL에 나열된 모든 원격 네트워크의 라우팅 테이블 경로에 배치됩니다.

예를 들어, 라우터 A의 암호화 ACL 및 암호화 맵은 다음과 같을 수 있습니다.

<#root>

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.210.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.220.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.230.0 0.0.0.255

crypto map myMAP 10 ipsec-isakmp
 set peer 10.89.129.2
```

reverse-route

```
 set transform-set mySET
 match address 110
```

라우터 A가 ASA로 대체된 경우 컨피그레이션은 다음과 같을 수 있습니다.

<#root>

```
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.210.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
```

```
   255.255.255.0 192.168.220.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.230.0 255.255.255.0

crypto map myMAP 10 match address cryptoACL
crypto map myMAP 10 set peer 10.89.129.2
crypto map myMAP 10 set transform-set mySET
```

crypto map mymap 10 set reverse-route

원격 액세스 컨피그레이션에서는 라우팅 변경이 항상 필요한 것은 아닙니다.

그러나 VPN 게이트웨이 라우터 또는 보안 어플라이언스 뒤에 다른 라우터가 있는 경우 그 라우터는 어떻게든 VPN 클라이언트에 대한 경로를 파악해야 합니다.

이 예에서는 VPN 클라이언트에 연결할 때 10.0.0.0 /24 범위의 주소가 제공된다고 가정합니다.

게이트웨이와 다른 라우터 간에 라우팅 프로토콜이 사용되지 않는 경우 라우터 2와 같은 라우터에서 고정 경로를 사용할 수 있습니다.

```
ip route 10.0.0.0 255.255.255.0 192.168.100.1
```

EIGRP 또는 OSPF와 같은 라우팅 프로토콜이 게이트웨이와 다른 라우터 간에 사용 중인 경우, 설명된 대로 Reverse Route Injection을 사용하는 것이 좋습니다.

RRI는 VPN 클라이언트의 경로를 게이트웨이의 라우팅 테이블에 자동으로 추가합니다. 그런 다음 이러한 경로를 네트워크의 다른 라우터로 배포할 수 있습니다.

Cisco IOS® 라우터:

<#root>

```
crypto dynamic-map dynMAP 10
 set transform-set mySET
```

reverse-route

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Cisco ASA 보안 어플라이언스:

<#root>

```
crypto dynamic-map dynMAP 10 set transform-set mySET
```

crypto dynamic-map dynMAP 10 set reverse-route

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

라우팅 문제는 VPN 클라이언트에 할당된 IP 주소 풀이 헤드엔드 디바이스의 내부 네트워크와 겹치는 경우 발생합니다. 자세한 내용은 Overlapping Private Networks 섹션을 참조하십시오.

Transform-Set이 올바른지 확인

양쪽 끝에 있는 변환 세트에서 사용할 IPsec 암호화 및 해시 알고리즘이 동일한지 확인합니다.

자세한 내용은 Cisco Security Appliance 컨피그레이션 가이드의 명령 참조 섹션을 참조하십시오.

ASA에서 사용되는 ISAKMP 정책 및 IPsec Transform-set의 경우 Cisco VPN 클라이언트는 DES와 SHA가 조합된 정책을 사용할 수 없습니다.

DES를 사용하는 경우 해시 알고리즘에 MD5를 사용해야 합니다. 또는 SHA가 포함된 3DES와 MD5가 포함된 3DES의 다른 조합을 사용할 수 있습니다.

암호화 맵 시퀀스 번호 및 이름을 확인하고 암호화 맵이 IPsec 터널이 시작/종료되는 올바른 인터페이스에 적용되었는지 확인합니다

고정 및 동적 피어가 동일한 암호화 맵에 구성된 경우 암호화 맵 엔트리의 순서가 매우 중요합니다.

동적 암호화 맵 엔트리의 시퀀스 번호는 다른 모든 정적 암호화 맵 엔트리보다 높아야 합니다.

고정 엔트리가 동적 엔트리보다 높은 번호가 지정되면 해당 피어와의 연결이 실패하고 그림과 같은 디버그가 나타납니다.

```
IKEv1]: Group = x.x.x.x, IP = x.x.x.x, QM FSM error (P2 struct &0x49ba5a0, mess id 0xcd600011)!
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

Security Appliance의 각 인터페이스에는 동적 암호화 맵을 하나만 사용할 수 있습니다.

다음은 고정 엔트리와 동적 엔트리를 포함하는 적절하게 번호가 매겨진 암호화 맵의 예입니다. 동적 항목의 시퀀스 번호가 가장 높고 고정 항목을 추가할 수 있는 공간이 남아 있습니다.

<#root>

```
crypto dynamic-map cisco 20 set transform-set myset
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.16.77.10
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside
```

crypto map mymap 60000 ipsec-isakmp dynamic ciscothe

암호화 맵 이름은 대/소문자를 구분합니다.

이 오류 메시지는 동적 암호화 남자 시퀀스가 올바르지 않아 피어가 잘못된 암호화 맵을 적중하는 경우에도 표시됩니다.

또한 이 문제는 흥미로운 트래픽을 정의하는 암호화 액세스 목록이 일치하지 않아 발생합니다.

%ASA-3-713042: IKE 개시자가 정책을 찾을 수 없습니다.

동일한 인터페이스에서 종료되는 여러 VPN 터널의 경우, 이름이 같지만(인터페이스당 하나의 암호화 맵만 허용됨) 시퀀스 번호가 다른 암호화 맵을 생성합니다.

이는 라우터 및 ASA에 적용됩니다.

마찬가지로, L2L 및 원격 액세스 VPN 시나리오 모두에 대한 암호화 맵 컨피그레이션에 대한 자세한 내용은 ASA: Add a New Tunnel or Remote Access to an Existing L2L VPN - Cisco를 참조하십시오.

피어 IP 주소가 올바른지 확인합니다.

IPsec에 대한 연결별 레코드의 데이터베이스를 만들고 관리합니다.

ASA Security Appliance LAN-to-LAN(L2L) IPsec VPN 컨피그레이션의 경우 tunnel-group <name> type ipsec-l2lcommand에서 터널 그룹의<name>을 Remote peer IP Address(remote tunnel end)로 지정합니다.

피어 IP 주소는 intunnel group name 및 Crypto map set addresssses 명령과 일치해야 합니다.

ASDM을 사용하여 VPN을 구성하는 동안 올바른 피어 IP 주소로 터널 그룹 이름을 자동으로 생성했습니다.

피어 IP 주소가 올바르게 구성되지 않은 경우 로그는 이 메시지를 포함할 수 있으며, 이는 피어 IP 주소의 적절한 컨피그레이션으로 확인할 수 있습니다.

```
[IKEv1]: Group = DefaultL2LGroup, IP = x.x.x.x,
ERROR, had problems decrypting packet, probably due to mismatched pre-shared key. Aborting
```

피어 IP 주소가 ASA 암호화 컨피그레이션에서 제대로 구성되지 않은 경우 ASA는 VPN 터널을 설정할 수 없으며 MM_WAIT_MSG4단계에서만 정지됩니다.

이 문제를 해결하려면 컨피그레이션에서 피어 IP 주소를 수정하십시오.

VPN 터널이 MM_WAIT_MSG4 상태에서 정지할 때 표시되는 how crypto isakmp 명령의 출력입니다.

<#root>

```
hostname#
```

show crypto isakmp sa

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG4
```

터널 그룹 및 그룹 이름 확인

```
%ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by
tunnel-group and group-policy
```

그룹 정책에 지정된 허용 터널이 터널 그룹 컨피그레이션의 허용 터널과 다르기 때문에 터널이 삭제될 경우 이 메시지가 나타납니다.

<#root>

```
group-policy hf_group_policy attributes
  vpn-tunnel-protocol l2tp-ipsec

username hfremote attributes
  vpn-tunnel-protocol l2tp-ipsec
```

Both lines read:

```
  vpn-tunnel-protocol ipsec l2tp-ipsec
```

기본 그룹 정책의 기존 프로토콜에 대한 기본 그룹 정책의 IPSec을 활성화합니다.

```
group-policy DfltGrpPolicy attributes
   vpn-tunnel-protocol L2TP-IPSec IPSec webvpn
```

L2L 피어에 대해 XAUTH 비활성화

LAN-to-LAN 터널과 원격 액세스 VPN 터널이 동일한 암호화 맵에 구성된 경우, LAN-to-LAN 피어에 XAUTH 정보를 입력하라는 메시지가 표시되고 LAN-to-LAN 터널이 show crypto isakmp saccommand의 출력에 "CONF_XAUTH"로 실패합니다.

다음은 SA 출력의 예입니다.

<#root>

```
Router#
```

```
show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst             src             state          conn-id  slot  status
X.X.X.X         Y.Y.Y.Y         CONF_XAUTH       10223    0   ACTIVE
X.X.X.X         Z.Z.Z.Z         CONF_XAUTH       10197    0   ACTIVE
```

이 문제는 Cisco IOS®에만 적용되지만 ASA는 터널 그룹을 사용하므로 이 문제의 영향을 받지 않습니다.

디바이스가 피어에게 XAUTH 정보(사용자 이름 및 비밀번호)를 묻는 메시지를 표시하지 않도록 isakmp 키를 입력할 때 no-xauthkeyword를 사용합니다.

이 키워드는 고정 IPsec 피어에 대해 XAUTH를 비활성화합니다. 동일한 암호화 맵에 L2L 및 RA VPN이 모두 구성된 디바이스에서 다음과 유사한 명령을 입력합니다.

```
<#root>

router(config)#

crypto isakmp key cisco123 address
   172.22.1.164 no-xauth
```

ASA가 Easy VPN Server 역할을 하는 시나리오에서 Easy VPN 클라이언트는 Xauth 문제로 인해 헤드엔드에 연결할 수 없습니다.

다음과 같이 문제를 해결하기 위해 ASA에서 사용자 인증을 비활성화합니다.

```
<#root>

ASA(config)#

tunnel-group example-group type ipsec-ra

ASA(config)#

tunnel-group example-group ipsec-attributes

ASA(config-tunnel-ipsec)#

isakmp ikev1-user-authentication none
```

isakmp ikev1-user-authenticationcommand에 대한 자세한 내용은 이 문서의 Miscellaneoussection을 참조하십시오.

VPN 풀 소모

VPN 풀에 할당된 IP 주소의 범위가 충분하지 않으면 다음 두 가지 방법으로 IP 주소의 가용성을 확장할 수 있습니다.

1. 기존 범위를 제거하고 새 범위를 정의합니다. 예를 들면 다음과 같습니다.

```
<#root>
CiscoASA(config)#
no ip local pool testvpnpool 10.76.41.1-10.76.41.254
CiscoASA(config)#
ip local pool testvpnpool 10.76.41.1-10.76.42.254
```

2. 인접하지 않은 서브넷을 VPN 풀에 추가하려는 경우 두 개의 개별 VPN 풀을 정의한 다음 "tunnel-group attributes" 아래에서 순서대로 지정할 수 있습니다. 예를 들면 다음과 같습니다.

```
<#root>
CiscoASA(config)#
ip local pool testvpnpoolAB 10.76.41.1-10.76.42.254
CiscoASA(config)#
ip local pool testvpnpoolCD 10.76.45.1-10.76.45.254
CiscoASA(config)#
tunnel-group test type remote-access
CiscoASA(config)#
tunnel-group test general-attributes
CiscoASA(config-tunnel-general)#
address-pool (inside) testvpnpoolAB testvpnpoolCD
CiscoASA(config-tunnel-general)#
exit
```

ASA는 이 명령에 풀이 표시되는 순서대로 이러한 풀에서 주소를 할당하므로 풀을 지정하는 순서는 매우 중요합니다.

group-policy address-pools 명령의 주소 풀 설정은 항상 tunnel-group address-pool 명령의 로컬 풀 설정을 재정의합니다.

VPN 클라이언트 트래픽에 대한 레이턴시 문제

VPN 연결을 통해 대기 시간 문제가 발생하는 경우, 이를 해결하려면 다음 조건을 확인하십시오.

1. 패킷의 MSS를 더 줄일 수 있는지 확인합니다.
2. IPsec/udp 대신 IPsec/tcp를 사용하는 경우 configure-preserve-vpn-flow를 구성합니다.

3. Cisco ASA를 다시 로드합니다.

VPN 클라이언트가 ASA에 연결할 수 없음

문제

Cisco VPN 클라이언트는 X-auth가 Radius 서버와 함께 사용될 때 인증할 수 없습니다.

솔루션

xauth가 시간 초과될 수 있습니다. 이 문제를 해결하려면 AAA 서버의 시간 제한 값을 늘리십시오.

예를 들면 다음과 같습니다.

```
<#root>

Hostname(config)#

aaa-server test protocol radius

hostname(config-aaa-server-group)#

aaa-server test host 10.2.3.4

hostname(config-aaa-server-host)#

timeout 10
```

문제

Cisco VPN 클라이언트는 X-auth가 Radius 서버와 함께 사용될 때 인증할 수 없습니다.

솔루션

처음에는 인증이 제대로 작동하는지 확인합니다. 문제를 좁히려면 먼저 ASA에서 로컬 데이터베이스를 사용하여 인증을 확인합니다.

```
tunnel-group tggroup general-attributes
              authentication-server-group none
              authentication-server-group LOCAL
        exit
```

이 문제가 잘 작동하면 Radius 서버 컨피그레이션과 관련된 문제입니다.

ASA에서 Radius 서버의 연결을 확인합니다. Ping이 문제 없이 작동하면 ASA의 Radius 관련 컨피

그레이션과 Radius 서버의 데이터베이스 컨피그레이션을 확인합니다.

debug radiuscommand를 사용하여 RADIUS 관련 문제를 해결할 수 있습니다. sampledebug radiusoutput에 대해서는 이 샘플 출력을 참조하십시오.

ASA에서 debugcommand를 사용하기 전에 다음 설명서를 참조하십시오. 경고 메시지.

VPN 클라이언트는 첫 번째 시도 시 또는 "Security VPN Connection terminated by peer(피어에 의해 종료된 보안 VPN 연결)"에서 자주 연결을 삭제합니다. 이유 433." 또는 "Secure VPN Connection terminated by Peer 이유 433:(Reason Not Specified by Peer)"

문제

Cisco VPN 클라이언트 사용자가 헤드 엔드 VPN 장치에 연결을 시도할 때 이 오류가 발생합니다.

VPN 클라이언트가 첫 번째 시도에서 자주 연결 끊기

피어에 의해 보안 VPN 연결이 종료되었습니다. 이유 433.

보안 VPN 연결이 피어 이유 433에 의해 종료됨:(피어에서 지정하지 않은 이유)

네트워크 또는 브로드캐스트 IP 주소를 할당하려고 했습니다. 풀에서 (x.x.x.x)를 제거합니다.

해결 방법 1

ASA, Radius 서버, DHCP 서버를 통해 또는 DHCP 서버로 작동하는 Radius 서버를 통해 IP 풀을 할당하면 문제가 발생할 수 있습니다.

netmask와 IP 주소가 올바른지 확인하려면 debug cryptocommand를 사용합니다. 또한 풀에 네트워크 주소 및 브로드캐스트 주소가 포함되어 있지 않은지 확인합니다.

Radius 서버는 클라이언트에 적절한 IP 주소를 할당할 수 있어야 합니다.

해결 방법 2

이 문제는 확장 인증 실패로 인해 발생합니다. 이 오류를 해결하려면 AAA 서버를 확인해야 합니다.

서버 및 클라이언트에서 서버 인증 비밀번호를 확인합니다. AAA 서버를 다시 로드하면 이 문제를 해결할 수 있습니다.

해결 방법 3

이 문제의 또 다른 해결 방법은 위협 감지 기능을 비활성화하는 것입니다.

서로 다른 불완전한 SA(Security Association)에 대한 재전송이 여러 개 있는 경우, 위협 탐지 기능이 활성화된 ASA는 스캐닝 공격이 발생한 것으로 간주하고 VPN 포트가 주 공격자로 표시됩니다.

ASA 처리에 많은 오버헤드가 발생할 수 있으므로 위협 감지 기능을 비활성화해 보십시오. 위협 탐지를 비활성화하려면 다음 명령을 사용합니다.

```
no threat-detection basic-threat
no threat-detection scanning-threat shun
no threat-detection statistics
no threat-detection rate
```

이를 통해 실제 문제가 해결되는지 확인할 수 있습니다.

Cisco ASA에서 위협 탐지를 비활성화하려면 스캐닝 시도 완화, 잘못된 SPI를 사용하는 DoS, 애플리케이션 검사에 실패한 패킷, 불완전한 세션 등 여러 보안 기능이 실제로 손상되었는지 확인합니다.

해결 방법 4

이 문제는 변형 집합이 제대로 구성되지 않은 경우에도 발생합니다. 변형 집합을 적절하게 구성하면 문제가 해결됩니다.

원격 액세스 및 EZVPN 사용자는 VPN에 연결하지만 외부 리소스에 액세스할 수 없음

문제

원격 액세스 사용자는 VPN에 연결되면 인터넷에 연결되지 않습니다.

원격 액세스 사용자는 동일한 디바이스의 다른 VPN 뒤에 있는 리소스에 액세스할 수 없습니다.

원격 액세스 사용자는 로컬 네트워크에만 액세스할 수 있습니다.

솔루션

이 문제를 해결하려면 다음 솔루션을 사용해 보십시오.

- DMZ의 서버에 액세스할 수 없음
- VPN 클라이언트가 DNS를 확인할 수 없음
- Split-Tunnel(스플릿 터널) - 인터넷 또는 제외된 네트워크에 액세스할 수 없습니다.
- 로컬 LAN 액세스
- 겹치는 프라이빗 네트워크

DMZ의 서버에 액세스할 수 없음

VPN 클라이언트가 VPN 헤드 엔드 디바이스(ASA/Cisco IOS® Router)를 사용하여 IPsec 터널을 설정하면 VPN 클라이언트 사용자는 내부 네트워크(10.10.10.0/24) 리소스에 액세스할 수 있지만 DMZ 네트워크(10.1.1.0/24)에는 액세스할 수 없습니다.

다이어그램

DMZ 네트워크의 리소스에 액세스하기 위해 헤드 엔드 디바이스에 스플릿 터널, NAT 없음 컨피그레이션이 추가되었는지 확인합니다.

예:

ASA 구성:

이 컨피그레이션에서는 VPN 사용자가 DMZ 네트워크에 액세스할 수 있도록 DMZ 네트워크에 대한 NAT 제외를 구성하는 방법을 보여 줍니다.

```
object network obj-dmz
subnet 10.1.1.0 255.255.255.0
object network obj-vpnpool
subnet 192.168.1.0 255.255.255.0
nat (inside,dmz) 1 source static obj-dmz obj-dmz destination static obj-vpnpool obj-vpnpool
```

NAT 컨피그레이션에 대한 새 엔트리를 추가한 후 NAT 변환을 지웁니다.

```
Clear xlate
Clear local
```

확인:

터널이 설정된 경우 Cisco VPN 클라이언트로 이동하여 Status(상태) > Route Details(경로 세부사항)를 선택하여 DMZ 및 INSIDE 네트워크 모두에 대해 보안 경로가 표시되는지 확인합니다.

기존의 L2L VPN에 새 VPN 터널 또는 원격 액세스 VPN을 추가하는 데 필요한 단계는 ASA: Add a New Tunnel or Remote Access to an Existing L2L VPN - Cisco를 참조하십시오.

Cisco 5500 Series ASA(Adaptive Security Appliance)로 터널링된 동안 VPN 클라이언트가 인터넷에 액세스하도록 허용하는 방법에 대한 단계별 지침은 ASA: ASA 컨피그레이션 예에서 VPN 클라이언트에 대해 스플릿 터널링 허용을 참조하십시오.

VPN 클라이언트가 DNS를 확인할 수 없음

터널이 설정된 후 VPN 클라이언트가 DNS를 확인할 수 없는 경우, 문제는 ASA(Head-end Device)의 DNS 서버 컨피그레이션일 수 있습니다.

VPN 클라이언트와 DNS 서버 간의 연결도 확인합니다. DNS 서버 컨피그레이션은 그룹 정책에서 구성하고 터널 그룹 일반 특성의 그룹 정책에서 적용해야 합니다. 예를 들면 다음과 같습니다.

<#root>

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP address(172.16.1.1) !---
```

```
group-policy vpn3000 internal
group-policy vpn3000 attributes
 dns-server value 172.16.1.1
 default-domain value cisco.com
```

```
!--- Associate the group policy(vpn3000) to the tunnel group !--- with the default-group-policy.
```

```
tunnel-group vpn3000 general-attributes
 default-group-policy vpn3000
```

VPN 클라이언트가 내부 서버를 이름으로 연결할 수 없음

VPN 클라이언트가 원격 또는 헤드 엔드 내부 네트워크의 호스트 또는 서버에 대해 이름으로 ping할 수 없습니다. 이 문제를 해결하려면 ASA에서 스플릿 dns 구성을 활성화해야 합니다.

Split-Tunnel(스플릿 터널) - 인터넷 또는 제외된 네트워크에 액세스할 수 없습니다.

스플릿 터널은 원격 액세스 IPsec 클라이언트가 조건에 따라 암호화된 형식으로 IPsec 터널을 통해 또는 해독된 일반 텍스트 형식의 네트워크 인터페이스로 패킷을 전달할 수 있게 합니다. 이 경우 패킷이 최종 대상으로 라우팅됩니다.

Split-tunnel은 기본적으로 비활성화되어 있으며, 이 경우 모든 트래픽이 비활성화됩니다.

```
split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}
```

excludespecified 옵션은 EZVPN 클라이언트가 아닌 Cisco VPN 클라이언트에 대해서만 지원됩니다.

```
ciscoasa(config-group-policy)#split-tunnel-policy excludespecified
```

스플릿 터널의 자세한 컨피그레이션 예는 다음 문서를 참조하십시오.

- ASA: ASA 컨피그레이션의 VPN 클라이언트에 대해 스플릿 터널링 허용 예

- 라우터는 VPN 클라이언트가 스플릿 터널링 구성을 사용하여 IPsec 및 인터넷에 연결할 수 있도록 허용합니다. 예

헤어핀 솔루션

이 기능은 인터페이스에 진입하지만 동일한 인터페이스에서 라우팅되는 VPN 트래픽에 유용합니다 .

예를 들어, 보안 어플라이언스가 허브이고 원격 VPN 네트워크가 스포크인 허브 및 스포크 VPN 네트워크에서 스포크 투 스포크 통신 트래픽은 보안 어플라이언스로 이동한 다음 다시 다른 스포크로 전달되어야 합니다.

트래픽이 동일한 인터페이스로 들어오고 나가도록 허용하려면 동일한-security-traffic 컨피그레이션을 사용합니다.

<#root>

securityappliance(config)#

same-security-traffic permit intra-interface

로컬 LAN 액세스

원격 액세스 사용자는 VPN에 연결하며 로컬 네트워크에만 연결할 수 있습니다.

자세한 컨피그레이션 예는 ASA: Allow local LAN access for VPN clients를 참조하십시오.

겹치는 프라이빗 네트워크

문제

터널 설정 후 내부 네트워크에 액세스할 수 없는 경우 VPN 클라이언트에 할당된 IP 주소가 헤드 엔드 디바이스 뒤의 내부 네트워크와 겹치는지 확인합니다.

솔루션

VPN 클라이언트, 헤드 엔드 디바이스의 내부 네트워크 및 VPN 클라이언트 내부 네트워크에 할당할 풀의 IP 주소가 서로 다른 네트워크에 있는지 확인합니다.

서로 다른 서브넷으로 동일한 주요 네트워크를 할당할 수 있지만 라우팅 문제가 발생하는 경우도 있습니다.

자세한 예제는 DMZ의 서버에 액세스할 수 없음의 DiagramandExample을 참조하십시오.

3명 이상의 VPN 클라이언트 사용자를 연결할 수 없음

문제

ASA/에 연결할 수 있는 VPN 클라이언트는 3개뿐입니다. 네 번째 클라이언트에 대한 연결은 실패합니다. 실패 시 다음 오류 메시지가 표시됩니다.

```
Secure VPN Connection terminated locally by the client.
     Reason 413: User Authentication failed.
```

```
tunnel rejected; the maximum tunnel count has been reached
```

솔루션

대부분의 경우 이 문제는 그룹 정책 내의 동시 로그인 설정 및 최대 세션 제한과 관련이 있습니다.

이 문제를 해결하려면 다음 솔루션을 사용해 보십시오.

- 동시 로그인 구성
- CLI로 ASA 구성
- 구성

동시 로그인 구성

ASDM에서 Inheritcheck(상속) 확인란을 선택하면 사용자에게 기본 동시 로그인 수만 허용됩니다. 동시 로그인의 기본값은 3입니다.

이 문제를 해결하려면 동시 로그인 값을 늘리십시오.

1. ASDM을 시작한 다음 Configuration(컨피그레이션) > VPN > Group Policy(그룹 정책)로 이동합니다.
2. 적절한 그룹을 선택하고 편집 단추를 누릅니다.
3. Generaltab에서 Simultaneous LoginsenderConnection Settings의 Inheritcheck 상자를 실행 취소합니다. 필드에서 적절한 값을 선택합니다.

   이 필드의 최소값은 0(영)입니다. 그러면 로그인이 비활성화되고 사용자 액세스가 차단됩니다.

   다른 PC에서 같은 사용자 계정으로 로그인하면 현재 세션(같은 사용자 계정으로 다른 PC에서 설정한 연결)이 종료되고 새 세션이 설정됩니다.

이는 기본 동작이며 VPN 동시 로그인에 독립적입니다.

CLI로 ASA 구성

원하는 동시 로그인 수를 구성하려면 다음 단계를 완료합니다. 이 예에서는 20개(20)를 원하는 값으로 선택하였다.

<#root>

```
ciscoasa(config)#
group-policy Bryan attributes
ciscoasa(config-group-policy)#
vpn-simultaneous-logins 20
```

이 명령에 대한 자세한 내용은 Cisco Security Appliance 명령 참조를 참조하십시오.

보안 어플라이언스에서 허용하는 값보다 낮은 값으로 VPN 세션을 제한하려면 글로벌 컨피그레이션 모드에서 vpn-sessiondb max-session-limitcommand를 사용합니다.

세션 제한을 제거하려면 이 명령의 overvision을 사용합니다. 현재 설정을 덮어쓰려면 명령을 다시 사용하십시오.

```
vpn-sessiondb max-session-limit {session-limit}
```

다음 예에서는 최대 VPN 세션 제한을 450으로 설정하는 방법을 보여 줍니다.

<#root>

```
hostname#
vpn-sessiondb max-session-limit 450
```

구성

오류 메시지

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

솔루션

원하는 동시 로그인 수를 구성하려면 다음 단계를 완료합니다. 이 SA에 대해 동시 로그인을 5로 설

정할 수도 있습니다.

Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneous Logins를 선택하고 로그인 수를 5로 변경합니다.

터널 설정 후 세션 또는 애플리케이션을 시작할 수 없으며 전송 속도가 느려짐

문제

IPsec 터널 설정 후에는 애플리케이션 또는 세션이 터널 전체에서 시작되지 않습니다.

솔루션

네트워크를 확인하거나 네트워크에서 애플리케이션 서버에 연결할 수 있는지 확인하려면 theping 명령을 사용합니다.

라우터 또는 /ASA 디바이스를 통과하는 임시 패킷의 MSS(Maximum Segment Size), 특히 SYN 비트가 설정된 TCP 세그먼트의 문제가 될 수 있습니다.

Cisco IOS® Router - 라우터의 외부 인터페이스(터널 끝 인터페이스)에서 MSS 값을 변경합니다

라우터의 외부 인터페이스(터널 끝 인터페이스)에서 MSS 값을 변경하려면 다음 명령을 실행합니다.

```
<#root>

Router>

enable

Router#

configure terminal

Router(config)#

interface ethernet0/1

Router(config-if)#ip tcp adjust-mss 1300

Router(config-if)#

end
```

다음 메시지는 TCP MSS에 대한 디버그 출력을 표시합니다.

<#root>

```
Router#debug ip tcp transactions

Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 -> 10.0.1.1(38437)]
Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS 1300, MSS is
1300
Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751
Sep 5 18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 1300
Sep 5 18:42:46.251: TCP0: state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

구성된 대로 라우터에서 MSS가 1300으로 조정됩니다.

자세한 내용은 ASA 및 Cisco IOS®: VPN Fragmentation을 참조하십시오.

ASA —/ASA 설명서 참조

MTU 크기 오류 메시지 및 MSS 문제를 제공하기 때문에 인터넷에 제대로 액세스하지 못하거나 터널을 통한 전송 속도가 느려질 수 없습니다.

이 문제를 해결하려면 다음 문서를 참조하십시오.

- ASA 및 Cisco IOS®: VPN 단편화

ASA에서 VPN 터널을 시작할 수 없음

문제

ASA 인터페이스에서 VPN 터널을 시작할 수 없으며, 터널 설정 후 원격 엔드/VPN 클라이언트가 VPN 터널에서 ASA의 내부 인터페이스에 ping할 수 없습니다.

예를 들어, vpn 클라이언트는 VPN 터널을 통해 인터페이스 내부의 ASA에 대한 SSH 또는 HTTP 연결을 시작할 수 없습니다.

솔루션

전역 컨피그레이션 모드에서 management-accesscommand를 구성하지 않으면 의 내부 인터페이스를 터널의 다른 끝에서 ping할 수 없습니다.

<#root>

```
ASA-02(config)#

management-access inside


ASA-02(config)#

show management-access

management-access inside
```

이 명령은 VPN 터널을 통해 ASA의 내부 인터페이스에 대한 ssh 시작 또는 http 연결도 지원합니다.

이 정보는 DMZ 인터페이스에서도 마찬가지입니다. 예를 들어 /ASA의 DMZ 인터페이스를 ping하거나 DMZ 인터페이스에서 터널을 시작하려는 경우 management-access DMZ 명령이 필요합니다.

<#root>

```
ASA-02(config)#
management-access DMZ
```

VPN 클라이언트가 연결할 수 없는 경우 ESP 및 UDP 포트가 열려 있는지 확인합니다.

그러나 이러한 포트가 열려 있지 않으면 VPN 클라이언트 연결 항목 아래에서 이 포트를 선택하여 TCP 10000에서 연결을 시도합니다.

마우스 오른쪽 버튼으로 modify(수정) > transport(전송) 탭 > IPsec over TCP를 클릭합니다.

VPN 터널을 통해 트래픽을 전달할 수 없음

문제

VPN 터널을 통해 트래픽을 전달할 수 없습니다.

솔루션

이 문제는 ESP 패킷이 차단된 경우에도 발생할 수 있습니다. 이 문제를 해결하려면 VPN 터널을 다시 구성하십시오.

이 문제는 데이터가 암호화되지 않고 이 출력에 표시된 대로 VPN 터널을 통해서만 해독될 경우 발생할 수 있습니다.

<#root>

```
ASA# sh crypto ipsec sa peer x.x.x.x
peer address: y.y.y.y
    Crypto map tag: IPSec_map, seq num: 37, local addr: x.x.x.x
      access-list test permit ip host xx.xx.xx.xx host yy.yy.yy.yy
      local ident (addr/mask/prot/port): (xx.xx.xx.xx/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (yy.yy.yy.yy/255.255.255.255/0/0)
      current_peer: y.y.y.y


 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 393, #pkts decrypt: 393, #pkts verify: 393

      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
```

```
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0
```

이 문제를 해결하려면 다음 조건을 확인하십시오.

1. 암호화 액세스 목록이 원격 사이트와 일치하며 NAT 0 액세스 목록이 올바른 경우
2. 라우팅이 올바르고 트래픽이 내부를 통과하는 외부 인터페이스에 도달하는 경우 샘플 출력에서는 암호 해독이 완료되었지만 암호화가 발생하지 않음을 보여 줍니다.
3. ASA에서 syssopt permit connection-vpn 명령이 구성된 경우 구성되지 않은 경우, ASA에서 인터페이스 ACL 검사에서 암호화된/VPN 트래픽을 제외할 수 있으므로 이 명령을 구성합니다 .

동일한 암호화 맵에서 vpn 터널에 대한 백업 피어 구성

문제

단일 vpn 터널에 여러 백업 피어를 사용할 수 있습니다.

솔루션

여러 피어의 컨피그레이션은 폴백 목록의 프로비저닝과 동일합니다. 각 터널에 대해 보안 어플라이언스는 목록의 첫 번째 피어와 협상을 시도합니다.

해당 피어가 응답하지 않을 경우 보안 어플라이언스는 피어가 응답하거나 목록에 더 이상 피어가 없을 때까지 목록의 맨 아래로 작동합니다.

ASA에 기본 피어로 이미 구성된 암호화 맵이 있습니다. 기본 피어 다음에 보조 피어를 추가할 수 있습니다.

다음 예제 컨피그레이션에서는 기본 피어를 X.X.X.X로 표시하고 백업 피어를 Y.Y.Y.Y로 표시합니다.

<#root>

ASA(config)#

crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y

VPN 터널 비활성화/재시작

문제

VPN 터널을 일시적으로 비활성화하고 서비스를 다시 시작하려면 이 섹션에 설명된 절차를 완료합니다.

솔루션

인터페이스에 대해 이전에 정의된 암호화 맵 집합을 제거하려면 글로벌 컨피그레이션 모드에서 crypto map interfaceccommand를 사용합니다.

인터페이스에서 암호화 맵 집합을 제거하려면 이 명령의 enoform을 사용합니다.

<#root>

hostname(config)#

no crypto map

map-name

interface

interface-name

이 명령은 활성 보안 어플라이언스 인터페이스에 설정된 암호화 맵을 제거하고 해당 인터페이스에서 IPsec VPN 터널을 비활성화합니다.

인터페이스에서 IPsec 터널을 다시 시작하려면 해당 인터페이스에서 IPsec 서비스를 제공하려면 먼저 인터페이스에 암호화 맵 집합을 할당해야 합니다.

<#root>

hostname(config)#

crypto map

map-name

interface

interface-name

일부 터널이 암호화되지 않음

문제

VPN 게이트웨이에 대량의 터널이 구성된 경우 일부 터널은 트래픽을 전달하지 않습니다. ASA는 이러한 터널에 대해 암호화된 패킷을 수신하지 않습니다.

솔루션

이 문제는 ASA가 터널을 통해 암호화된 패킷을 전달하지 못하기 때문에 발생합니다. 중복 암호화 규칙이 ASP 테이블에 생성됩니다.

오류:- %ASA-5-713904: 그룹 = DefaultRAGroup, IP = x.x.x, ... 지원되지 않는 트랜잭션 모드 v2 version.Tunnel이 종료되었습니다.

문제

%ASA-5-713904: Group = DefaultRAGroup, IP = 192.0.2.0,... 지원되지 않는 Transaction Mode v2 version.Tunnel terminatederror 메시지가 나타납니다.

솔루션

Transaction Mode v2 오류 메시지가 표시되는 이유는 ASA가 이전 V2 모드 버전이 아닌 IKE 모드 컨피그레이션 V6만 지원하기 때문입니다.

이 오류를 해결하려면 IKE 모드 컨피그레이션 V6 버전을 사용합니다.

오류:- %ASA-6-722036: Group client-group User xxxx IP x.x.x Transmitting large packet 1220(임계값 1206)

문제

%ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206) 오류 메시지가 ASA 로그에 나타납니다.

이 로그는 무엇을 의미하며 어떻게 해결할 수 있습니까?

솔루션

이 로그 메시지는 대용량 패킷이 클라이언트로 전송되었음을 나타냅니다. 패킷의 소스가 클라이언트의 MTU를 인식하지 못합니다.

이는 비압축 데이터의 압축 때문일 수도 있습니다. 해결 방법은 svc compression nonecommand를 사용하여 SVC 압축을 끄는 것입니다. 그러면 문제가 해결됩니다.

VPN 터널의 한 쪽에서 QoS가 활성화된 경우 오류 메시지

문제

VPN 터널의 한 쪽에서 QoS를 활성화한 경우 다음 오류 메시지가 표시될 수 있습니다.

```
IPSEC: Received an ESP packet (SPI= 0xDB6E5A60, sequence number= 0x7F9F) from
10.18.7.11 (user= ghufhi) to 172.16.29.23 that failed anti-replay check
```

솔루션

이 메시지는 일반적으로 터널의 한 쪽에서 QoS를 수행할 때 발생합니다. 이는 패킷이 잘못된 것으로 탐지될 때 발생합니다.

QoS를 비활성화하여 중지할 수 있지만 트래픽이 터널을 통과할 수 있는 한 무시할 수 있습니다.

경고: 암호화 맵 항목이 불완전합니다.

문제

암호화 맵 mymap 20 ipsec-isakmpcommand를 실행할 때 다음 오류가 발생할 수 있습니다.

경고: 암호화 맵 항목이 불완전합니다.

예를 들면 다음과 같습니다.

```
<#root>

ciscoasa(config)#

crypto map mymap 20 ipsec-isakmp

WARNING: crypto map entry incomplete
```

솔루션

이는 새 암호화 맵을 정의할 때의 일반적인 알림입니다. access-list(match address), 변형 집합 및 피어 주소와 같은 매개변수를 구성해야 작동합니다.

암호화 맵을 정의하기 위해 입력하는 첫 번째 줄은 컨피그레이션에 표시되지 않는 것이 일반적입니다.

오류:- %ASA-4-400024: IDS:2151 인터페이스 외부의 큰 ICMP 패킷에서 (으)로

문제

VPN 터널을 통해 큰 ping 패킷을 전달할 수 없습니다. 대규모 ping 패킷을 전달하려고 하면 **%ASA-4-400024: IDS:2151 Large ICMP packet from to interface outside 오류가 발생합니다.**

솔루션

이 문제를 해결하려면 서명 2150 및 2151을 사용하지 않도록 설정하십시오.서명이 사용하지 않도

록 설정되면 ping이 정상적으로 작동합니다.

서명을 비활성화하려면 다음 명령을 사용합니다.

ASA(config)#ip 감사 서명 2151 비활성화

ASA(config)#ip 감사 서명 2150 비활성화

오류:- %ASA-4-402119: IPSEC: 재전송 방지 확인에 실패한 remote_IP(사용자 이름)에서 local_IP로의 프로토콜 패킷(SPI=spi, 시퀀스 번호= seq_num)을 받았습니다.

문제

ASA의 로그 메시지에서 이 오류를 받았습니다.

오류:- %|ASA-4-402119: IPSEC: 재전송 방지 확인에 실패한 remote_IP(사용자 이름)에서 local_IP로의 프로토콜 패킷(SPI=spi, 시퀀스 번호= seq_num)을 받았습니다.

솔루션

이 오류를 해결하려면 crypto ipsec security-association replay window-size 명령을 사용하여 창 크기를 변경합니다.

<#root>

hostname(config)#

crypto ipsec security-association replay window-size 1024

재전송 방지 문제를 해결하려면 전체 1024 윈도우 크기를 사용하는 것이 좋습니다.

오류 메시지 - %ASA-4-407001: 로컬 호스트 interface_name:inside_address에 대한 거부 트래픽, 라이센스 제한 개수 초과

문제

일부 호스트가 인터넷에 연결할 수 없으며 이 오류 메시지가 syslog에 나타납니다.

오류 메시지 - %ASA-4-407001: 로컬 호스트 interface_name:inside_address에 대한 거부 트래픽, 라이센스 제한 개수 초과

솔루션

이 오류 메시지는 사용자 수가 사용된 라이센스의 사용자 제한을 초과할 때 수신됩니다. 이 오류는 라이센스를 더 많은 수의 사용자로 업그레이드하여 해결할 수 있습니다.

사용자 라이센스에는 필요에 따라 50명, 100명 또는 무제한 사용자가 포함될 수 있습니다.

오류 메시지 - %VPN_HW-4-PACKET_ERROR:

문제

오류 메시지 - %VPN_HW-4-PACKET_ERROR:오류 메시지는 라우터에서 수신한 HMAC의 ESP 패킷이 일치하지 않음을 나타냅니다. 이 오류는 다음 문제로 인해 발생할 수 있습니다.

- 결함 있는 VPN 하드웨어 모듈
- 손상된 ESP 패킷

솔루션

이 오류 메시지를 해결하려면 다음을 수행합니다.

- 트래픽 중단이 없는 한 오류 메시지를 무시합니다.
- 트래픽 중단이 발생하면 모듈을 교체합니다.

오류 메시지: 명령이 거부되었습니다. VLAN XXXX와 XXXX 간의 암호화 연결을 먼저 삭제하십시오.

문제

이 오류 메시지는 스위치의 트렁크 포트에 허용된 VLAN을 추가하려고 할 때 나타납니다. `Command rejected: delete crypto connection between VLAN XXXX and VLAN XXXX, first..`

추가 VLAN을 허용하도록 WAN 에지 트렁크를 수정할 수 없습니다. 즉, IPSEC VPN SPAtrunk에서 VLAN을 추가할 수 없습니다.

이 명령은 허용되는 VLAN 목록에 속하는 암호화 연결 인터페이스 VLAN을 초래하여 잠재적인 IPSec 보안 침해를 유발하므로 거부됩니다.

이 동작은 모든 트렁크 포트에 적용됩니다.

솔루션

`no switchport trunk allowed vlan(vlanlist)` 명령 대신 `witchport trunk allowed vlan noneccommand` 또는 `"switchport trunk allowed vlan remove(vlanlist)" 명령을` 사용합니다.

오류 메시지 - % FW-3-

RESPONDER_WND_SCALE_INI_NO_SCALE: 삭제된 패킷 - 세션 x.x.x.x:27331에서 x.x.x.x:23에 대한 잘못된 창 크기 옵션 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]

문제

이 오류는 VPN 터널의 맨 끝에 있는 디바이스에서 텔넷을 시도하거나 라우터 자체에서 텔넷을 시도할 때 발생합니다.

오류 메시지 - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: 삭제된 패킷 - 세션 x.x.x.x:27331에서 x.x.x.x:23에 대한 잘못된 창 크기 옵션 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]

솔루션

사용자 라이센스에는 필요에 따라 50명, 100명 또는 무제한 사용자가 포함될 수 있습니다.
LFN(Long Fat Network)에서 데이터를 빠르게 전송할 수 있도록 윈도우 스케일 기능을 추가했다.

일반적으로 대역폭이 매우 높지만 레이턴시도 높은 연결입니다.

위성 링크는 항상 전파 지연이 높지만 일반적으로 대역폭이 높기 때문에 위성 연결이 있는 네트워크는 LFN의 한 예입니다.

LFN을 지원하도록 윈도우 확장 기능을 활성화하려면 TCP 윈도우 크기가 65,535보다 커야 합니다. 이 오류 메시지는 TCP 창 크기를 65,535보다 크게 늘릴 경우 해결될 수 있습니다.

%ASA-5-305013: 비대칭 NAT 규칙이 정방향 및 역방향에 대해 일치합니다. 이 문제 흐름을 업데이트하십시오.

문제

이 오류 메시지는 VPN 터널이 가동되면 나타납니다.

%ASA-5-305013: 비대칭 NAT 규칙이 정방향 및 역방향에 대해 일치합니다. 이 문제 흐름을 업데이트하십시오.

솔루션

NAT를 사용하는 호스트와 동일한 인터페이스에 있지 않은 경우 이 문제를 해결하려면 실제 주소 대신 매핑된 주소를 사용하여 호스트에 연결합니다.

또한 애플리케이션이 IP 주소를 포함하면 inspectcommand를 활성화합니다.

%ASA-5-713068: 비루틴 알림 메시지를 받았습니다. notify_type

문제

이 오류 메시지는 VPN 터널이 가동되지 않을 경우 나타납니다.

%ASA-5-713068: 비루틴 알림 메시지를 받았습니다. notify_type

솔루션

이 메시지는 컨피그레이션 오류(정책 또는 ACL이 피어에서 동일하게 구성되지 않은 경우)로 인해 발생합니다.

정책과 ACL이 일치하면 터널이 문제 없이 나타납니다.

%ASA-5-720012: (VPN-Secondary) 대기 유닛에서 IPSec 장애 조치(failover) 런타임 데이터를 업데이트하지 못했습니다. 또는 %ASA-6-720012: (VPN-unit) 대기 유닛에서 IPsec 장애 조치(failover) 런타임 데이터를 업데이트하지 못했습니다.

문제

Cisco ASA(Adaptive Security Appliance)를 업그레이드하려고 할 때 다음 오류 메시지 중 하나가 나타납니다.

%ASA-5-720012: (VPN-Secondary) 스탠바이 유닛에서 IPSec 장애 조치(failover) 런타임 데이터를 업데이트하지 못했습니다.

%ASA-6-720012: (VPN-unit) 스탠바이 유닛에서 IPsec 장애 조치(failover) 런타임 데이터를 업데이트하지 못했습니다.

솔루션

이러한 오류 메시지는 유용한 오류입니다. 이 메시지는 ASA 또는 VPN의 기능에 영향을 주지 않습니다.

이러한 메시지는 관련 IPsec 터널이 스탠바이 유닛에서 삭제되었기 때문에 VPN 장애 조치 하위 시스템이 IPsec 관련 런타임 데이터를 업데이트할 수 없을 때 나타납니다.

이러한 문제를 해결하려면 액티브 유닛에서 wr standbycommand 명령을 실행합니다.

오류:- %ASA-3-713063: IKE 피어 주소가 대상 0.0.0.0에 대해 구성되지 않았습니다.

문제

%ASA-3-713063: IKE Peer address not configured for destination 0.0.0 오류 메시지가 나타나고 터널이 가동되지 않습니다.

솔루션

이 메시지는 IKE 피어 주소가 L2L 터널에 대해 구성되지 않은 경우 표시됩니다.

암호화 맵의 시퀀스 번호를 변경한 다음 암호화 맵을 제거하고 다시 적용하면 이 오류를 해결할 수 있습니다.

오류: %ASA-3-752006: 터널 관리자가 KEY_ACQUIRE 메시지를 디스패치하지 못했습니다.

문제

%ASA-3-752006: 터널 관리자가 KEY_ACQUIRE 메시지를 디스패치하지 못했습니다. 암호화 맵 또는 터널 그룹의 잘못된 구성일 수 있습니다." 오류 메시지가 Cisco ASA에 기록됩니다.

솔루션

이 오류 메시지는 암호화 맵 또는 터널 그룹의 잘못된 컨피그레이션으로 인해 발생할 수 있습니다. 둘 다 올바르게 구성되었는지 확인합니다. 이 오류 메시지에 대한 자세한 내용은 Error 752006 를 참조하십시오.

다음은 몇 가지 시정 조치입니다.

- 암호화 ACL(예: 동적 맵과 연결됨)을 제거합니다.
- 사용하지 않는 IKEv2 관련 컨피그레이션이 있는 경우 이를 제거합니다.
- 암호화 ACL이 올바르게 일치하는지 확인합니다.
- 중복 access-list 항목을 제거합니다(있는 경우).

오류: %ASA-4-402116: IPSEC: XX.XX.XX.XX(user= XX.XX.XX.XX)에서 YY.YY.YY.YY으로 ESP 패킷(SPI= 0x99554D4E, 시퀀스 번호= 0x9E)을 받았습니다.

LAN-to-LAN VPN 터널 설정에서 이 오류는 엔드 ASA에서 수신됩니다.

캡슐화되지 않은 내부 패킷이 SA에서 협상된 정책과 일치하지 않습니다.

패킷은 대상을 10.32.77.67, 소스를 10.105.30.1, 프로토콜을 icmp로 지정합니다.

SA는 로컬 프록시를 10.32.77.67/255.255.255.255/ip/0으로 지정하고 remote_proxy를 10.105.42.192/255.255.255.224/ip/0으로 지정합니다.

솔루션

VPN 터널의 양쪽 끝에 정의된 흥미로운 트래픽 액세스 목록을 확인해야 합니다. 두 이미지 모두 정확한 미러 이미지로 일치해야 합니다.

0xffffffff 오류로 인해 64비트 VA 설치 관리자를 시작하여 가상 어댑터를 사용하도록 설정하지 못했습니다.

문제

AnyConnect가 연결 실패 시 오류 0 xffffffffffffflog 메시지가 수신되어 64비트 VA 설치 프로그램을 실행하여 가상 어댑터를 활성화하지 못했습니다.

솔루션

이 문제를 해결하려면 다음 단계를 완료하십시오.

1. System(시스템) > Internet Communication Management(인터넷 통신 관리) > Internet Communication settings(인터넷 통신 설정)로 이동하여 Turn Off Automatic Root Certificates Updates(자동 루트 인증서 업데이트 끄기)가 비활성화되었는지 확인합니다.
2. 비활성화되어 있으면 영향을 받는 컴퓨터에 할당된 GPO의 전체 관리 템플릿 부분을 비활성화하고 다시 테스트합니다.

자세한 내용은 자동 루트 인증서 업데이트 해제를 참조하십시오.

Cisco VPN Client는 Windows 7에서 데이터 카드와 작동하지 않음

문제

Cisco VPN Client는 Windows 7의 데이터 카드에서 작동하지 않습니다.

솔루션

Windows 7에 설치된 Cisco VPN Client는 Windows 7 시스템에 설치된 VPN 클라이언트에서 데이터 카드가 지원되지 않으므로 3G 연결에서 작동하지 않습니다.

경고: "VPN 기능이 전혀 작동하지 않을 수 있습니다."

문제

ASA의 외부 인터페이스에서 isakmp를 활성화하려고 시도하는 동안 다음 경고 메시지가 수신됩니다.

```
ASA(config)# crypto isakmp enable outside
WARNING, system is running low on memory.  Performance may start to degrade.
VPN functionality may not work at all.
```

이때 ssh를 통해 ASA에 액세스합니다. HTTPS가 중지되고 다른 SSL 클라이언트도 영향을 받습니다.

솔루션

이 문제는 로거 및 암호화 등의 서로 다른 모듈에 의한 메모리 요구 사항 때문입니다.

로깅 대기열 0 명령이 없는지 확인합니다. 대기열 크기를 8192로 설정하고 메모리 할당을 늘립니다.

ASA5505 및 ASA5510과 같은 플랫폼에서 이 메모리 할당은 다른 모듈에 메모리가 부족한 경향이 있습니다.

IPSec 패딩 오류

문제

이 오류 메시지가 수신되었습니다.

```
%ASA-3-402130: CRYPTO: Received an ESP packet (SPI =
     0xXXXXXXX, sequence number= 0xXXXX) from x.x.x.x (user= user) to y.y.y.y with
     incorrect IPsec padding
```

솔루션

이 문제는 IPSec VPN이 해시 알고리즘 없이 협상하기 때문에 발생합니다. 패킷 해시는 ESP 채널에 대한 무결성 검사를 보장합니다.

따라서 해시가 없으면 형식이 잘못된 패킷이 Cisco ASA에서 탐지되지 않은 채 수락되고 이러한 패킷의 해독을 시도합니다.

그러나 이러한 패킷의 형식이 잘못되었으므로 ASA는 패킷 암호 해독 중에 결함을 찾습니다. 이로 인해 패딩 오류 메시지가 표시됩니다.

VPN에 대한 변형 집합에 해시 알고리즘을 포함하고 피어 간의 링크에 최소 패킷 형식이 있는지 확인하는 것이 좋습니다.

VPN 터널은 18시간마다 연결 끊김

문제

수명이 24시간으로 설정되어 있더라도 18시간마다 VPN 터널의 연결이 끊어집니다.

솔루션

수명은 SA를 rekey에 사용할 수 있는 최대 시간입니다. 수명으로 컨피그레이션에 입력하는 값은 SA의 rekey 시간과 다릅니다.

따라서 현재 SA가 만료되기 전에 새 SA(또는 IPsec의 경우 SA 쌍)를 협상해야 합니다.

첫 번째 키 재설정 시도가 실패할 경우 여러 시도를 허용하려면 항상 키 재설정 시간이 수명보다 작아야 합니다.

RFC는 키 재설정 시간을 계산하는 방법을 지정하지 않습니다. 이는 구현자의 재량에 맡겨져 있다.

따라서 플랫폼에 따라 시간이 달라집니다. 일부 구현들은 리키 타이머를 계산하기 위해 랜덤 인자를 사용할 수 있다.

예를 들어, ASA가 터널을 시작할 경우 64800초 = 75%의 속도로 다시 키가 설정되는 것이 86400.

라우터가 시작되면 ASA는 더 오래 기다렸다가 피어가 키 재설정을 시작할 시간을 줄 수 있습니다.

따라서 VPN 협상에 다른 키를 사용하려면 18시간마다 VPN 세션의 연결이 끊어지는 것이 일반적입니다. 이로 인해 VPN 삭제 또는 문제가 발생해서는 안 됩니다.

LAN-to-LAN 터널이 재협상된 후에는 트래픽 흐름이 유지되지 않습니다

문제

LAN-to-LAN 터널이 재협상된 후에는 트래픽 흐름이 유지되지 않습니다.

솔루션

ASA는 이를 통과하는 모든 연결을 모니터링하고 애플리케이션 검사 기능에 따라 상태 테이블의 항목을 유지 관리합니다.

VPN을 통과하는 암호화된 트래픽 세부사항은 SA(Security Association) 데이터베이스의 형태로 유지됩니다. LAN-to-LAN VPN 연결의 경우 두 가지 다른 트래픽 흐름을 유지합니다.

하나는 VPN 게이트웨이 간의 암호화된 트래픽입니다. 다른 하나는 VPN 게이트웨이 뒤의 네트워크 리소스와 다른 쪽 뒤의 최종 사용자 간의 트래픽 흐름입니다.

VPN이 종료되면 이 특정 SA에 대한 플로우 세부사항이 삭제됩니다.

그러나 활동이 없으므로 이 TCP 연결에 대해 ASA에서 유지 관리하는 상태 테이블 항목이 부실해져 다운로드가 방해됩니다.

즉, 사용자 애플리케이션이 종료되는 동안 ASA는 여전히 해당 특정 플로우에 대한 TCP 연결을 유지합니다.

그러나 TCP 연결이 끊어지고 TCP 유휴 타이머가 만료된 후 시간이 초과됩니다.

이 문제는 지속적인 IPSec 터널링 흐름이라는 기능을 도입하면서 해결되었습니다.

VPN 터널 재협상 시 상태 테이블 정보를 유지하기 위해 새로운 명령인 sysopt connection preserve-vpn-flows가 Cisco ASA에 통합되었습니다.

기본적으로 이 명령은 비활성화되어 있습니다. 이를 활성화하기 위해 L2L VPN이 중단으로부터 복구하고 터널을 재설정할 때 Cisco ASA는 TCP 상태 테이블 정보를 유지 관리합니다.

암호화 기능에 대한 대역폭에 도달했다는 오류 메시지 상태

문제

이 오류 메시지는 2900 Series 라우터에서 수신됩니다.

오류: 3월 20일 10:51:29: %CERM-4-TX_BW_LIMIT: securityk9 기술 패키지 라이선스의 암호화 기능에 대한 최대 Tx 대역폭 제한(85000Kbps)에 도달했습니다.

솔루션

이는 미국 정부가 발표한 엄격한 지침 때문에 발생하는 알려진 문제이다.

이에 따라 securityk9 라이센스는 90Mbps에 가까운 속도까지의 페이로드 암호화만 허용하고 디바이스에 대한 암호화된 터널/TLS 세션의 수를 제한할 수 있습니다.

암호화 내보내기 제한에 대한 자세한 내용은 Cisco ISR G2 SEC 및 HSEC 라이센싱을 참조하십시오.

Cisco 디바이스의 경우 ISR G2 라우터를 드나드는 단방향 트래픽이 85Mbps 미만이며 양방향의 총 전송 속도는 170Mbps입니다.

이 요구 사항은 Cisco 1900, 2900 및 3900 ISR G2 플랫폼에 적용됩니다. 이 명령은 다음과 같은 제한 사항을 확인하는 데 도움이 됩니다.

<#root>

```
Router#
show platform cerm-information

Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED
 ---------------------------------------------------------------
 Resource                      Maximum Limit          Available
 ---------------------------------------------------------------
 Tx Bandwidth(in kbps)          85000                  85000
 Rx Bandwidth(in kbps)          85000                  85000
 Number of tunnels                225                    225
 Number of TLS sessions          1000                   1000
---Output truncated----
```

이 문제를 방지하려면 HSECK9 라이센스를 구매하십시오. "hseck9" 기능 라이센스는 VPN 터널 수

및 보안 음성 세션 수를 늘려 향상된 페이로드 암호화 기능을 제공합니다.

Cisco ISR 라우터 라이센싱에 대한 자세한 내용은 소프트웨어 활성화를 참조하십시오.

문제: 인바운드 암호 해독 트래픽이 작동하더라도 IPsec 터널의 아웃바운드 암호화 트래픽은 실패합니다.

솔루션

이 문제는 여러 개의 키 재설정 후 IPsec 연결에서 관찰되었지만 트리거 조건이 명확하지 않습니다.

이 문제는 show asp dropcommand의 출력을 확인하고 전송된 각 아웃바운드 패킷에 대해 Expired VPN 컨텍스트 카운터가 증가하는지 확인하는 경우 설정할 수 있습니다.

기타

AG_INIT_EXCH 메시지가 "show crypto isakmp sa" 및 "debug" 명령 출력에 나타남

터널이 시작되지 않으면 crypto isakmp sacomand 및 indebugoutput의 출력에도 AG_INIT_EXCHmessage가 나타납니다.

isakmp 정책의 불일치 또는 도중에 포트 udp 500이 차단되는 경우 이러한 문제가 발생할 수 있습니다.

"잘못된 상태 중에 IPC 메시지를 받았습니다."라는 디버그 메시지가 나타납니다

이 메시지는 정보 메시지이며 VPN 터널의 연결 해제와 관련이 없습니다.

관련 정보

- ASA 및 Cisco IOS®: VPN 단편화
- Cisco ASA 5500 Series 보안 어플라이언스
- IPSec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.