IPsec 트러블슈팅을 위해 Debug 명령 이해 및 사용

목차

소개

이 문서에서는 Cisco IOS® Software 및 PIX/ASA에서 IPsec 문제를 해결하는 데 사용되는 commondebugcommands에 대해 설명합니다.

배경 정보

IPsec VPN 문제에 대한 가장 일반적인 해결책에 대한 자세한 내용은 Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions(가장 일반적인 L2L 및 원격 액세스 IPsec VPN 문제 해결 솔루션)를 참조하십시오.

여기에는 연결 트러블슈팅을 시작하기 전에 시도하고 Cisco 기술 지원에 전화하기 전에 수행할 수 있는 일반적인 절차의 체크리스트가 포함되어 있습니다.

사전 요구 사항

요구 사항

이 문서에서는 IPsec을 구성했다고 가정합니다. 자세한 내용은 IPSec 협상/IKE 프로토콜을 참조하십시오.

사용되는 구성 요소

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.

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- **Cisco IOS® 소프트웨어**IPsec 기능 집합56i - 단일 **Data Encryption Standard (DES)** 기능(Cisco IOS® Software 릴리스 11.2 이상)k2 - 트리플 DES 기능(Cisco IOS® Software 릴리스 12.0 이상)을 나타냅니다. Triple DES는 Cisco 2600 Series 이상에서 사용할 수 있습니다.
- **PIX**—V5.0 이상. 활성화하려면 단일 또는 트리플 DES 라이센스 키가 필요합니다.

표기 규칙

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

Cisco IOS® 소프트웨어 디버깅

이 단원의 항목에서는 Cisco IOS® 소프트웨어 디버그 명령에 대해 설명합니다. 자세한 내용은 IPSec 협상/IKE 프로토콜을 참조하십시오.

show crypto isakmp sa

이 명령은 **Internet Security Association Management Protocol (ISAKMP) Security Associations (SAs)** 구축할 수 있습니다.

```
dst      src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

암호화 ipsec sa 표시

이 명령은 피어 간에 구축된 IPsec SA를 표시합니다. 암호화된 터널은 네트워크 10.1.0.0과 10.1.1.0 사이를 이동하는 트래픽에 대해 10.1.0.1과 10.1.0.2 사이에 구축됩니다.

이 두 가지를 **Encapsulating Security Payload (ESP)** SA는 인바운드 및 아웃바운드를 구축했습니다. AH(Authentication Header)는 AH SA가 없으므로 사용되지 않습니다.

이 출력은 **show crypto ipsec sa** 명령을 실행합니다.

```
  interface: FastEthernet0
    Crypto map tag: test, local addr. 10.1.0.1
   local  ident (addr/mask/prot/port): (10.1.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
   current_peer: 10.1.0.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 7767918, #pkts encrypt: 7767918, #pkts digest 7767918
    #pkts decaps: 7760382, #pkts decrypt: 7760382, #pkts verify 7760382
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 1, #recv errors 0
     local crypto endpt.: 10.1.0.1, remote crypto endpt.: 10.1.0.2
     path mtu 1500, media mtu 1500
     current outbound spi: 3D3
     inbound esp sas:
      spi: 0x136A010F(325714191)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 3442, flow_id: 1443, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4608000/52)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
inbound pcp sas:
outbound esp sas:
   spi: 0x3D3(979)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 3443, flow_id: 1444, crypto map: test
    sa timing: remaining key lifetime (k/sec): (4608000/52)
    IV size: 8 bytes
    replay detection support: Y
```

```
outbound ah sas:
outbound pcp sas:
```

show crypto engine connection active

이 명령은 각 단계 2 SA가 구축되고 전송된 트래픽의 양을 표시합니다.

2단계에서는 **Security Associations (SAs)** 는 단방향이며 각 SA는 한 방향으로만 트래픽을 표시합니다 (암호화는 아웃바운드, 해독은 인바운드).

암호화 isakmp 디버그

이 출력은 **debug crypto isakmp** 명령을 실행합니다.

```
processing SA payload. message ID = 0
Checking ISAKMP transform against priority 1 policy
encryption DES-CBC
      hash SHA
default group 2
auth pre-share
life type in seconds
life duration (basic) of 240
atts are acceptable. Next payload is 0
processing KE payload. message ID = 0
processing NONCE payload. message ID = 0
processing ID payload. message ID = 0
SKEYID state generated
processing HASH payload. message ID = 0
SA has been authenticated
processing SA payload. message ID = 800032287
```

암호화 ipsec 디버그

이 명령은 IPsec 터널 엔드포인트의 소스 및 대상을 표시합니다. **Src_proxy** 및 **dest_proxy** 클라이언트 서브넷입니다.

2 **sa created** 메시지는 각 방향으로 하나씩 나타납니다. (ESP 및 AH를 수행하면 4개의 메시지가 나타납니다.)

이 출력은 **debug crypto ipsec** 명령을 실행합니다.

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 10.1.0.2, src=10.1.0.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 10.1.0.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
```

```
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 10.1.0.2, src=10.1.0.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 10.1.0.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src=10.1.0.2, dest= 10.1.0.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 10.1.0.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

샘플 오류 메시지

이러한 샘플 오류 메시지는 다음 목록에 나열된 **debug** 명령에서 생성되었습니다.

- **debug crypto ipsec**
- **debug crypto isakmp**
- **debug crypt engine**

재생 확인 실패

이 출력은 **Replay Check Failed** 오류:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection id=#.
```

이 오류는 전송 미디어의 재배열(특히 병렬 경로가 있는 경우) 또는 Cisco IOS® 내에서 처리된 패킷의 동일하지 않은 경로(큰 패킷과 작은 패킷 및 로드 중)로 인해 발생합니다.

이를 반영하도록 변형 집합을 변경합니다. 이 **reply check** 이(가) **transform-set esp-md5-hmac** 이(가) 활성화됩니다. 이 오류 메시지를 표시하지 않으려면 disable(비활성화) **esp-md5-hmac** 암호화만 수행합니다.

Cisco 버그 IDCSCdp19680(등록된 고객만 해당)을 참조하십시오.

QM FSM 오류

PIX 방화벽 또는 ASA에 IPsec L2L VPN 터널이 표시되지 않으며 QM FSM 오류 메시지가 나타납니다.

한 가지 가능한 이유는 비정상적인 트래픽, **Access Control List (ACL),** 또는 암호화 ACL은 양쪽 끝에서 일치하지 않습니다.

두 디바이스 모두에서 컨피그레이션을 확인하고 암호화 ACL이 일치하는지 확인합니다.

또 다른 가능한 이유는 변형 집합 매개 변수가 일치하지 않기 때문입니다. 양쪽 끝에서 VPN 게이트웨이가 정확히 동일한 매개변수로 동일한 변형 집합을 사용하는지 확인합니다.

잘못된 로컬 주소

이 출력은 오류 메시지의 예를 보여줍니다.

```
IPSEC(validate_proposal): invalid local address 10.2.0.2
ISAKMP (0:3): atts not acceptable. Next payload is 0
ISAKMP (0:3): SA not acceptable!
```

이 오류 메시지는 다음 두 가지 일반적인 문제 중 하나에 기인합니다.

- 이 **crypto map map-name local-address interface-id** 이 명령은 라우터가 지정된 주소를 사용하도록 강제하므로 라우터가 잘못된 주소를 id로 사용하게 합니다.
- **Crypto map** 가 잘못된 인터페이스에 적용되었거나 전혀 적용되지 않습니다. 컨피그레이션을 확인하여 암호화 맵이 올바른 인터페이스에 적용되었는지 확인합니다.

X.X.X.X의 IKE 메시지가 온전성 검사에 실패했거나 형식이 잘못됨

이 **디버그** 오류는 피어의 사전 공유 키가 일치하지 않는 경우에 나타납니다. 이 문제를 해결하려면 양쪽의 사전 공유 키를 확인하십시오.

```
1d00H:%CRPTO-4-IKMP_BAD_MESSAGE: IKE message from 198.51.100.1 failed its
 sanity check or is malformed
```

주 모드 프로세스가 피어 때문에 실패했습니다.

다음은 **Main Mode** 오류 메시지가 표시됩니다. 주 모드가 실패하면 1단계 정책이 양쪽에서 일치하지 않음을 나타냅니다.

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0
1d00h: ISAKMP (0:1); no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with
peer at 198.51.100.1
```

show **crypto isakmp sa** 명령은 의 ISAKMP SA를 표시합니다 **MM_NO_STATE**. 이는 주 모드가 실패했음을 의미하기도 합니다.

```
dst      src        state     conn-id     slot
10.1.1.2  10.1.1.1   MM_NO_STATE    1           0
```

1단계 정책이 두 피어 모두에 있는지 확인하고 모든 특성이 일치하는지 확인합니다.

```
Encryption DES or 3DES
Hash MD5 or SHA
Diffie-Hellman Group 1 or 2
Authentication {rsa-sig | rsa-encr | pre-share
```

프록시 ID가 지원되지 않음

이 메시지는 IPsec 트래픽에 대한 액세스 목록이 일치하지 않는 경우 디버깅에 표시됩니다.

```
1d00h: IPSec(validate_transform_proposal): proxy identities not supported
1d00h: ISAKMP: IPSec policy invalidated proposal
1d00h: ISAKMP (0:2): SA not acceptable!
```

각 피어의 액세스 목록은 서로 미러링해야 합니다(모든 항목은 가역적이어야 함). 이 예에서는 이 점을 설명합니다.

```
Peer A
access-list 150 permit ip 172.21.113.0 0.0.0.255 172.21.114.0 0.0.0.255
access-list 150 permit ip host 10.2.0.8 host 172.21.114.123
Peer B
access-list 150 permit ip 172.21.114.0 0.0.0.255 172.21.113.0 0.0.0.255
access-list 150 permit ip host 172.21.114.123 host 10.2.0.8
```

변환 제안이 지원되지 않음

이 메시지는 Phase 2(IPsec)가 양쪽에서 일치하지 않는 경우에 나타납니다. 이는 변환 세트에 불일치 또는 비호환성이 있는 경우 가장 일반적으로 발생합니다.

```
1d00h: IPSec (validate_proposal): transform proposal
   (port 3, trans 2, hmac_alg 2) not supported
1d00h: ISAKMP (0:2) : atts not acceptable. Next payload is 0
1d00h: ISAKMP (0:2) SA not acceptable
```

변환 세트가 양쪽에서 일치하는지 확인합니다.

```
crypto ipsec transform-set transform-set-name transform1
[transform2 [transform3]]
? ah-md5-hmac
? ah-sha-hmac
? esp-des
? esp-des and esp-md5-hmac
? esp-des and esp-sha-hmac
? esp-3des and esp-md5-hmac
? esp-3des and esp-sha-hmac
? comp-lzs
```

원격 피어가 있는 인증서 및 키 없음

이 메시지는 라우터에 구성된 피어 주소가 잘못되었거나 변경되었음을 나타냅니다. 피어 주소가 올바른지, 그리고 주소에 연결할 수 있는지 확인합니다.

```
1d00h: ISAKMP: No cert, and no keys (public or pre-shared) with
remote peer 198.51.100.2
```

피어 주소 X.X.X.X를 찾을 수 없음

이 오류 메시지는 **VPN 3000 Concentrator** 오류 메시지가 표시됩니다 **Message: No proposal chosen(14).** 이는 연결이 호스트 대 호스트이기 때문입니다.

라우터 컨피그레이션에는 IPsec 제안이 포함되어 있습니다. 이 순서대로 라우터에 대해 선택한 제안이 액세스 목록과 일치하지만 피어는 일치하지 않습니다.

액세스 목록에는 트래픽을 교차하는 호스트를 포함하는 더 큰 네트워크가 있습니다. 이 문제를 해결하려면 이 Concentrator-to-Router 연결에 대한 라우터 제안을 행에서 먼저 만듭니다.

이렇게 하면 먼저 특정 호스트를 매칭할 수 있습니다.

```
20:44:44: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.15, src=198.51.100.6,
    dest_proxy= 10.0.0.76/255.255.255.255/0/0 (type=1),
    src_proxy= 198.51.100.23/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:44:44: IPSEC(validate_transform_proposal):
   peer address 198.51.100.6 not found
```

IPsec 패킷에 잘못된 SPI가 있습니다.

이 출력은 오류 메시지의 예입니다.

```
%PIX|ASA-4-402101: decaps: recd IPSEC packet has
invalid spi for destaddr=dest_address, prot=protocol, spi=number
```

수신된 IPsec 패킷은 **Security Parameters Index (SPI)** 이(가) **Security Associations Database (SADB).** 다음과 같은 이유로 일시적인 상황이 될 수 있습니다.

- 의 에이징에 대한 약간의 차이 **Security Sssociations (SAs)** IPsec 피어 간
- 로컬 SA가 삭제되었습니다.
- IPsec 피어에서 보낸 잘못된 패킷

이것은 아마도 공격일 것입니다.

권장 조치: 피어가 로컬 SA가 지워졌음을 인정하지 않을 수 있습니다. 로컬 라우터에서 새 연결이 설정되면 두 피어가 성공적으로 다시 설정될 수 있습니다.

그렇지 않은 경우, 문제가 짧은 기간 이상 발생하면 새 연결을 시도하거나 해당 피어의 관리자에게 문의하십시오.

IPSEC(initialize_sas): 잘못된 프록시 ID

오류 **21:57:57: IPSEC(initialize_sas): invalid proxy IDs** 수신된 프록시 id가 액세스 목록에 따라 구성된 프록시 id와 일치하지 않음을 나타냅니다.

둘 다 일치하는지 확인하려면 debug 명령의 출력을 확인합니다.

제안 요청의 **debug** 명령 출력에서 access-list 103 permit ip 10.1.1.0 0 0.0.0.255 10.1.0.0 0.0.255가 일치하지 않습니다.

액세스 목록은 한 쪽 끝에는 네트워크별, 다른 쪽 끝에는 호스트별 입니다.

```
21:57:57: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.1, src=192.0.2.2,
    dest_proxy= 10.1.1.1/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.0.1/255.255.255.0/0/0 (type=4)
```

페이로드 5에서 예약되지 않음

즉, ISAKMP 키가 일치하지 않습니다. 정확성을 보장하기 위해 키를 다시 입력/재설정합니다.

제공된 해시 알고리즘이 정책과 일치하지 않습니다.

구성된 ISAKMP 정책이 원격 피어에서 제안한 정책과 일치하지 않으면 라우터는 기본 정책인 65535을 시도합니다.

둘 중 하나와 일치하지 않으면 ISAKMP 협상에 실패합니다.

사용자는 **Hash algorithm offered does not match policy!** 또는 **Encryption algorithm offered does not match policy!** 라우터에 오류 메시지가 표시됩니다.

```
=RouterA=
3d01h: ISAKMP (0:1): processing SA payload. message ID = 0
3d01h: ISAKMP (0:1): found peer pre-shared key matched 203.0.113.22
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1): Hash algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 0
=RouterB=
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 65535 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 0
ISAKMP (0:1): no offers accepted!
ISAKMP (0:1): phase 1 SA not acceptable!
```

HMAC 확인 실패

이 오류 메시지는 의 확인에 실패할 경우 보고됩니다. **Hash Message Authentication Code** IPsec 패킷에서 확인할 수 있습니다. 이 문제는 일반적으로 패킷이 어떤 방식으로든 손상되었을 때 발생합니다.

```
Sep 22 11:02:39 203.0.113.16 2435:
Sep 22 11:02:39: %MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure
Sep 22 11:02:39 203.0.113.16 2436:
Sep 22 11:02:39: %MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                 PktEngReturn_MACMiscompare
```

이 오류 메시지가 가끔 나타나면 무시할 수 있습니다. 그러나 이 경우가 더 자주 발생하면 패킷 손상의 원인을 조사해야 합니다. 이는 암호화 가속기의 결함 때문일 수 있습니다.

원격 피어가 응답하지 않음

이 오류 메시지는 변형 집합이 일치하지 않을 때 발생합니다. 일치하는 변환 세트가 두 피어에 모두 구성되어 있는지 확인합니다.

허용되지 않는 모든 IPSec SA 제안 발견

이 오류 메시지는 2단계 IPSec 매개변수가 로컬 사이트와 원격 사이트 간에 일치하지 않을 때 발생합니다.

이 문제를 해결하려면 일치하는 VPN을 성공적으로 설정하도록 변형 집합에서 동일한 매개변수를 지정합니다.

패킷 암호화/암호 해독 오류

이 출력은 오류 메시지의 예입니다.

```
HW_VPN-1-HPRXERR: Virtual Private Network (VPN) Module0/2: Packet Encryption/Decryption
error, status=4615
```

이 오류 메시지는 다음 원인 중 하나 때문일 수 있습니다.

- 프래그먼트화 — 프래그먼트화된 암호화 패킷은 프로세스 스위칭됩니다. 즉, 프로세스 스위칭된 패킷보다 빠르게 스위칭된 패킷이 먼저 VPN 카드로 전송됩니다.

빠르게 전환된 패킷이 프로세스 전환 패킷보다 먼저 처리되면 프로세스 전환 패킷에 대한 ESP 또는 AH 시퀀스 번호가 부실해지고 패킷이 VPN 카드에 도착하면 해당 시퀀스 번호가 재생 윈도우 외부에 있습니다.

그러면 사용하는 캡슐화에 따라 AH 또는 ESP 시퀀스 번호 오류(각각 4615 및 4612)가 발생합니다.

- 오래된 캐시 엔트리 — 이 경우 가능한 또 다른 예는 fast-switch 캐시 엔트리가 부실해지고 캐시 누락이 있는 첫 번째 패킷이 프로세스를 전환하는 경우입니다.

해결 방법

1. 3DES 변형 집합에서 모든 유형의 인증을 끄고 ESP-DES/3DES를 사용합니다. 이렇게 하면 인증/재전송 방지 보호가 효과적으로 비활성화되어 순서가 지정되지 않은(혼합된) IPsec 트래픽과 관련된 패킷 삭제 오류가 방지됩니다 **%HW_VPN-1-HPRXERR: Hardware VPN0/2: Packet Encryption/Decryption error, status=4615.**
2. 여기서 언급한 사유에 적용되는 한 가지 해결 방법은 **Maximum Transmission Unit (MTU)** 인바운드 스트림의 크기를 1400바이트 미만으로 설정합니다. 인바운드 스트림의 MTU(최대 전송 단위) 크기를 1400바이트 미만으로 설정하려면 다음 명령을 입력합니다.
   ```
   ip tcp adjust-mss 1300
   ```
3. AIM 카드를 비활성화합니다.
4. 라우터 인터페이스에서 fast/CEF 스위칭을 끕니다. 빠른 스위칭을 제거하려면 인터페이스 컨피그레이션 모드에서 다음 명령을 사용합니다.
   ```
   no ip route-cache
   ```

ESP 시퀀스 실패로 인한 패킷 수신 오류

다음은 오류 메시지의 예입니다.

```
%C1700_EM-1-ERROR: packet-rx error: ESP sequence fail
```

이 오류 메시지는 일반적으로 다음 가능한 조건 중 하나를 나타냅니다.

- IPsec 암호화 패킷은 잘못 구성된 QoS 메커니즘 때문에 암호화 라우터에 의해 순서가 바뀌어 전달됩니다.
- 해독 라우터가 수신한 IPsec 패킷이 중간 디바이스에서 패킷 순서 변경으로 인해 순서가 잘못 되었습니다.
- 수신된 IPsec 패킷이 조각화되어 인증 확인 및 암호 해독 전에 다시 어셈블해야 합니다.

해결 방법

1. 암호화 또는 중간 라우터에서 IPsec 트래픽에 대해 QoS를 비활성화합니다.
2. 암호화 라우터에서 IPsec 사전 조각화를 활성화합니다.
   ```
   Router(config-if)#crypto ipsec fragmentation before-encryption
   ```
3. MTU 값을 조각화할 필요가 없는 크기로 설정합니다.
   ```
   Router(config)#interface type [slot_#/]port_#
   ```

   ```
   Router(config-if)#ip mtu MTU_size_in_bytes
   ```

4. 해당 열차에서 Cisco IOS® 이미지를 사용 가능한 최신 안정된 이미지로 업그레이드합니다.

라우터에서 MTU 크기가 변경되면 해당 인터페이스에서 종료되는 모든 터널이 해제됩니다.

예약된 다운타임 동안 이 해결 방법을 완료할 계획입니다.

7600 Series 라우터에서 VPN 터널을 설정하는 동안 오류가 발생했습니다.

이 오류는 7600 Series 라우터에서 VPN 터널을 설정하려고 할 때 발생합니다.

```
crypto_engine_select_crypto_engine: can't handle any more
```

이 오류는 소프트웨어 암호화가 7600 Series 라우터에서 지원되지 않기 때문에 발생합니다. 7600 Series 라우터는 IPsec SPA 하드웨어 없이 IPsec 터널 종료를 지원하지 않습니다. VPN은 7600 라우터의 IPSEC-SPA 카드에서만 지원됩니다.

PIX 디버그

show crypto isakmp sa

이 명령은 피어 간에 구축된 ISAKMP SA를 표시합니다.

```
dst      src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

이 **방법 암호화 isakmp saoutput**에서 상태는 항상 **QM_**IDLE이어야 합니다. 상태가 **MM_KEY_EXCH이면**

구성된 사전 공유 키가 올바르지 않거나 피어 IP 주소가 다름을 의미합니다.

```
PIX(config)#show crypto isakmp sa
Total     : 2
Embryonic : 1
        dst               src        state     pending     created
 192.168.254.250   10.177.243.187    MM_KEY_EXCH   0           0
```

올바른 IP 주소 또는 사전 공유 키를 구성할 때 이를 수정할 수 있습니다.

암호화 ipsec sa 표시

이 명령은 피어 간에 구축된 IPsec SA를 표시합니다. 네트워크 10.1.0.0과 10.1.1.0 사이를 이동하는 트래픽에 대해 10.1.0.1과 10.1.0.2 사이에 암호화된 터널이 구축됩니다.

인바운드 및 아웃바운드에 구축된 2개의 ESP SA를 확인할 수 있습니다. AH는 AH SA가 없으므로 사용되지 않습니다.

의 예 **show crypto ipsec sa** 명령이 이 출력에 표시됩니다.

```
interface: outside
    Crypto map tag: vpn, local addr. 10.1.0.1
   local  ident (addr/mask/prot/port): (10.1.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.0.2/255.255.255.255/0/0)
   current_peer: 10.2.1.1
   dynamic allocated peer ip: 10.1.0.2
     PERMIT, flags={}
    #pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0
    #pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0
     local crypto endpt.: 10.1.0.1, remote crypto endpt.: 10.1.0.2
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 9a46ecae
     inbound esp sas:
      spi: 0x50b98b5(84646069)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x9a46ecae(2588339374)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
    outbound ah sas:
```

암호화 isakmp 디버그

이 명령은 IPsec 연결에 대한 디버그 정보를 표시하고 양쪽 끝의 비호환성 때문에 거부된 첫 번째 특성 집합을 표시합니다.

두 번째 일치 시도(DES 대신 3DES를 시도하고 **Secure Hash Algorithm (SHA)** ISAKMP SA가 구축됩니다.

이 디버그는 또한 로컬 풀에서 IP 주소(10.32.8.1)를 받는 전화 접속 클라이언트에서 가져옵니다. ISAKMP SA가 구축되면 IPsec 특성이 협상되고 허용 가능한 것으로 확인됩니다.

그런 다음 PIX는 여기에 표시된 대로 IPsec SA를 설정합니다. 이 출력은 **debug crypto isakmp** 명령을 실행합니다.

```
crypto_isakmp_process_block: src 10.1.0.1, dest 10.1.0.2
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP: Created a peer node for 10.1.0.2
OAK_QM exchange
ISAKMP (0:0): Need config/address
ISAKMP (0:0): initiating peer config to 10.1.0.2. ID = 2607270170 (0x9b67c91a)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.1.0.2.
   message ID = 2156506360
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): peer accepted the address!
ISAKMP (0:0): processing saved QM.
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 818324052
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
IPSEC(validate_proposal): transform proposal
   (prot 3, trans 2, hmac_alg 1) not supported
ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 2
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP (0): atts are acceptable.
ISAKMP (0): processing NONCE payload. message ID = 818324052
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR src 10.32.8.1 prot 0 port 0
```

```
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR dst 10.1.0.1 prot 0 port 0
INITIAL_CONTACTIPSEC(key_engine): got a queue event...
```

암호화 ipsec 디버그

이 명령은 IPsec 연결에 대한 디버그 정보를 표시합니다.

```
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xd532efbd(3576885181) for SA
        from  10.1.0.2  to  10.1.0.1  for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from  10.1.0.2  to  10.1.0.1
           (proxy 10.32.8.1 to  10.1.0.1.)
        has spi 3576885181 and conn_id 2 and flags 4
        outbound SA from  10.1.0.1  to  10.1.0.2
           (proxy 10.1.0.1 to 10.32.8.1)
        has spi 2749108168 and conn_id 1 and flags 4IPSEC(key_engine):
           got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 10.1.0.1, src=10.1.0.2,
    dest_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    src_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xd532efbd(3576885181), conn_id= 2, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src=10.1.0.1, dest= 10.1.0.2,
    src_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    dest_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xa3dc0fc8(2749108168), conn_id= 1, keysize= 0, flags= 0x4
return status is IKMP_NO_ERROR
```

일반적인 라우터-VPN 클라이언트 문제

VPN 터널 외부의 서브넷에 액세스할 수 없음: 스플릿 터널

이 샘플 라우터 컨피그레이션 출력은 VPN 연결에 대해 스플릿 터널을 활성화하는 방법을 보여줍니다.

이 **split tunnel** 명령은에 구성된 그룹과 연결됩니다. **crypto isakmp client configuration group hw-client-groupname** 명령을 실행합니다.

이렇게 하면 **Cisco VPN Client** VPN 터널의 일부가 아닌 추가 서브넷에 액세스하기 위해 라우터를 사용합니다.

이 작업은 IPsec 연결 보안에서 성능 저하 없이 수행됩니다. 터널은 192.0.2.18 네트워크에 형성됩니다.

트래픽은 암호화되지 않은 상태로 **access list 150** 명령입니다.

```
!
crypto isakmp client configuration group hw-client-groupname
 key hw-client-password
 dns 192.0.2.20 198.51.100.21
 wins 192.0.2.22 192.0.2.23
 domain cisco.com
 pool dynpool
 acl 150
!
!
access-list 150 permit ip 192.0.2.18 0.0.0.127 any
!
```

일반적인 PIX-to-VPN 클라이언트 문제

이 단원의 항목에서는 VPN Client 3.x의 도움을 받아 PIX를 IPsec으로 구성할 때 흔히 발생하는 문제를 다룹니다. PIX의 샘플 컨피그레이션은 버전 6.x를 기반으로 합니다.

터널이 설정된 후에는 트래픽이 흐르지 않습니다. PIX를 통해 네트워크 내부에서 Ping할 수 없음

이는 라우팅과 관련된 일반적인 문제입니다. PIX에 동일한 서브넷에 직접 연결되지 않고 내부에 있는 네트워크에 대한 경로가 있는지 확인합니다.

또한 내부 네트워크에는 클라이언트 주소 풀의 주소에 대해 PIX로 돌아가는 경로가 있어야 합니다.

이 출력은 예를 보여줍니다.

```
!--- Address of PIX inside interface.

ip address inside 10.1.1.1 255.255.255.240

!--- Route to the networks that are on the inside segment. !--- The next hop is the router on
the inside.

route inside 172.16.0.0 255.255.0.0 10.1.1.2 1

 !--- Pool of addresses defined on PIX from which it assigns !--- addresses to the VPN Client
for the IPsec session.

ip local pool mypool 10.1.2.1-10.1.2.254

!--- On the internal router, if the default gateway is not !--- the PIX inside interface, then
the router needs to have route !--- for 10.1.2.0/24 network with next hop as the PIX inside
interface !.

ip route 10.1.2.0 255.255.255.0 10.1.1.1
```

터널이 가동되면 사용자가 인터넷을 탐색할 수 없습니다. 스플릿 터널

이 문제의 가장 일반적인 원인은 VPN 클라이언트에서 PIX로 이동하는 IPsec 터널의 경우 모든 트래픽이 터널을 통해 PIX 방화벽으로 전송되기 때문입니다.

PIX 기능에서는 트래픽이 수신된 인터페이스로 다시 전송되도록 허용하지 않습니다. 따라서 인터넷으로 향하는 트래픽은 작동하지 않습니다.

이 문제를 해결하려면 **split tunnel** 명령을 실행합니다. 이러한 수정 이면에 있는 아이디어는 터널을 통해 특정 트래픽을 보내는 트래픽만 있고 나머지 트래픽은 터널이 아닌 인터넷으로 직접 이동한다는 것입니다.

```
vpngroup vpn3000 split-tunnel 90
access-list 90 permit ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0
access-list 90 permit ip 172.16.0.0 255.255.0.0 10.1.2.0 255.255.255.0
```

이 **vpngroup vpn3000 split-tunnel 90** 명령을 사용하여 스플릿 터널을 **access-list number 90.**

이 **access-list number 90** 명령은 터널을 통과하는 트래픽 흐름을 정의하며, 나머지 트래픽은 액세스 목록의 끝에서 거부됩니다.

거부하려면 액세스 목록이 동일해야 합니다. **Network Address Translation (NAT)** 제공합니다.

터널이 가동되면 특정 애플리케이션이 작동하지 않습니다. 클라이언트에서 MTU 조정

터널이 설정되면 PIX 방화벽 뒤의 네트워크에 있는 시스템에 ping할 수 있지만 Microsoft와 같은 특정 애플리케이션을 사용할 수 없습니다 **Outlook.**

일반적인 문제는 패킷의 MTU(Maximum Transfer Unit) 크기입니다. IPsec 헤더는 최대 50~60바이트까지 가능하며, 이는 원래 패킷에 추가됩니다.

패킷의 크기가 1500(인터넷의 기본값)보다 커지면 디바이스에서 프래그먼트화해야 합니다. IPsec 헤더를 추가한 후에도 크기는 여전히 IPsec의 최대값인 1496보다 작습니다.

이 **show interface** 이 명령은 액세스 가능한 라우터 또는 자체 프레미스의 라우터에서 특정 인터페이스의 MTU를 표시합니다.

소스에서 대상까지 전체 경로의 MTU를 결정하기 위해 다양한 크기의 데이터그램이 **Do Not Fragment (DF)** 전송된 데이터그램이 MTU보다 큰 경우 이 오류 메시지가 소스로 다시 전송되도록 비트를 설정합니다.

```
frag. needed and DF set
```

이 출력은 IP 주소가 10.1.1.2 및 172.16.1.56인 호스트 간 경로의 MTU를 찾는 방법의 예를 보여줍니다.

```
Router#debug ip icmp
ICMP packet debugging is on


!--- Perform an extended ping.

Router#ping
Protocol [ip]:
Target IP address: 172.16.1.56
Repeat count [5]:
Datagram size [100]: 1550
Timeout in seconds [2]:


!--- Make sure you enter y for extended commands.
```

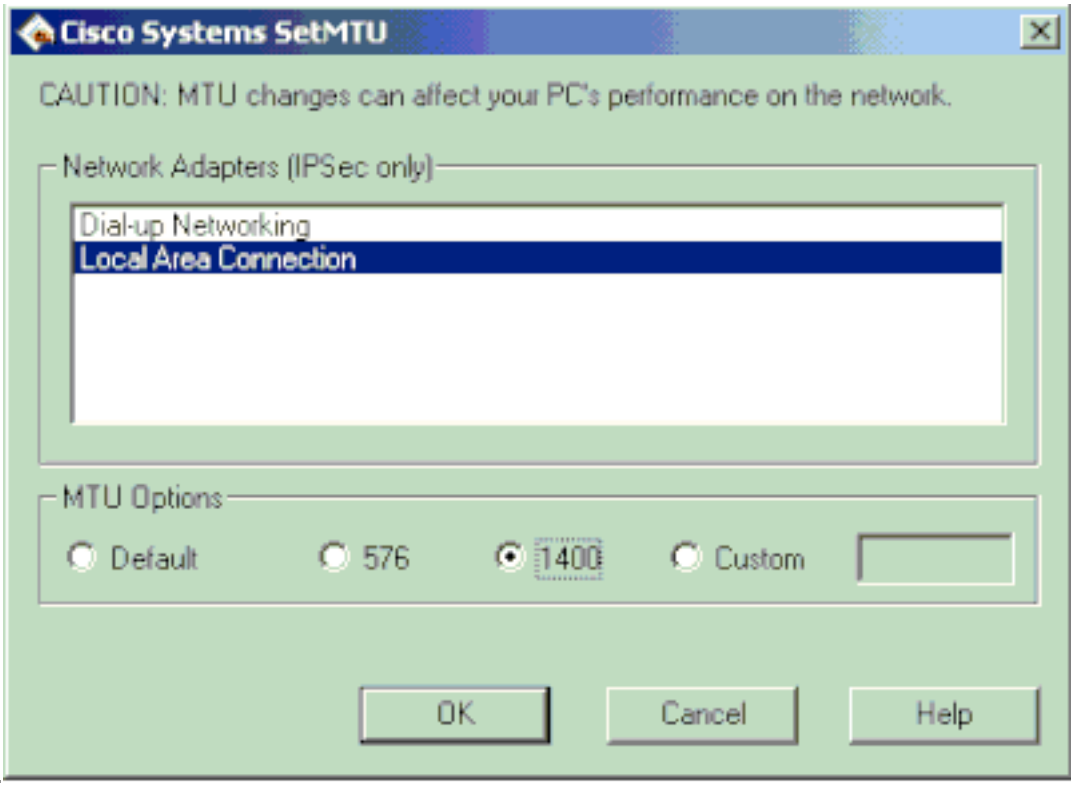
```
Extended commands [n]: y
Source address or interface: 10.1.1.2
Type of service [0]:


!--- Set the DF bit as shown.


Set DF bit in IP header? [no]: y
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, 1550-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:

2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
Success rate is 0 percent (0/5)


!--- Reduce the datagram size further and perform extended ping again.

Router#ping
Protocol [ip]:
Target IP address: 172.16.1.56
Repeat count [5]:
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.2
Type of service [0]:
Set DF bit in IP header? [no]: y
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, 1500-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:
!!!!!
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2

Success rate is 100 percent (5/5), round-trip min/avg/max = 380/383/384 ms
```

VPN 클라이언트에는 사용자가 Cisco VPN 클라이언트에 대한 MTU를 조정할 수 있는 MTU 조정 유틸리티가 제공됩니다.

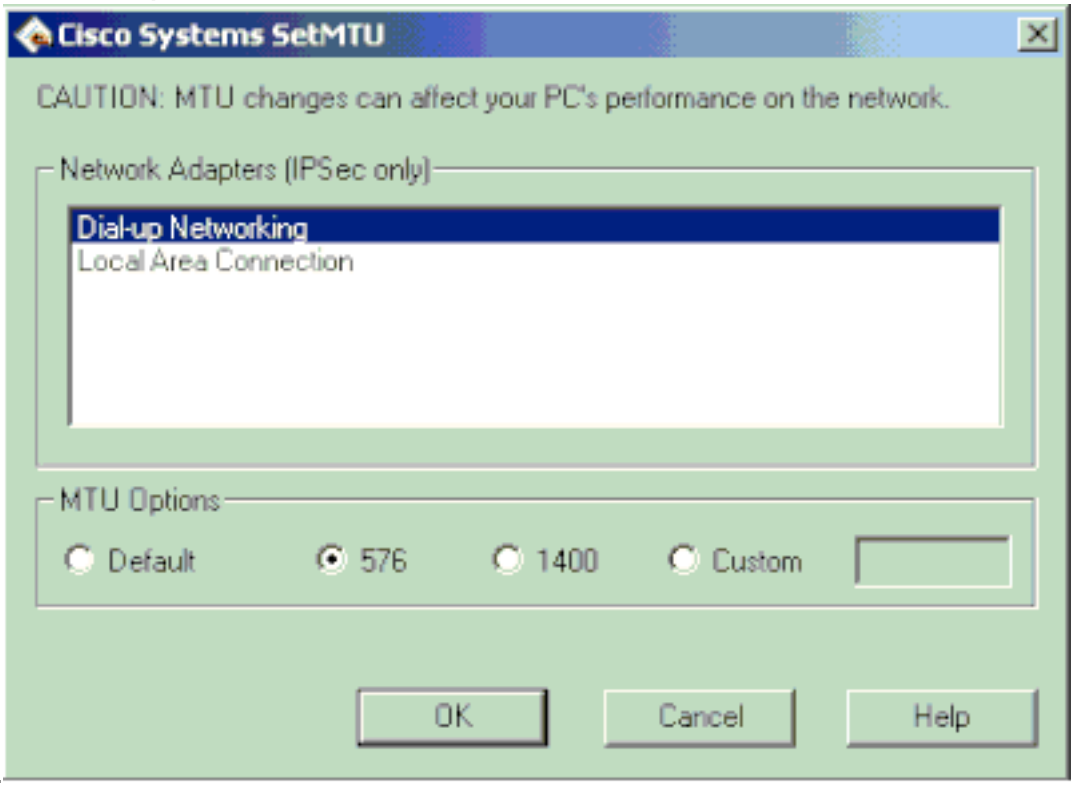
PPPoE(PPP over Ethernet) 클라이언트 사용자의 경우 PPPoE 어댑터의 MTU를 조정합니다.

VPN 클라이언트에 대한 MTU 유틸리티를 조정하려면 다음 단계를 완료합니다.

1. 선택 **Start > Programs > Cisco System VPN Client > Set MTU**.
2. 선택 **Local Area Connection**을 클릭한 다음 1400 라디오 버튼을 클릭합니다.



3. 클릭 **OK.**
4. 1단계를 반복하고 **Dial-up Networking.**
5. 576 라디오 **버튼**을 클릭한 다음



OK.

sysopt 명령 누락

이 **sysopt connection permit-ipsec** IPsec 트래픽이 확인 없이 PIX 방화벽을 통과하도록 허용하기 위해 PIX의 IPsec 컨피그레이션에서 명령 **conduit** 또는 **access-list** 명령문입니다.

기본적으로 모든 인바운드 세션은 **conduit** 또는 **access-list** 명령문입니다. IPsec 보호 트래픽에서는 보조 액세스 목록 검사를 중복할 수 있습니다.

IPsec 인증/암호화 인바운드 세션이 항상 허용되도록 하려면 **sysopt connection permit-ipsec** 명령을 실

행합니다.

ACL(Access Control List) 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 누락될 경우, 트래픽은 VPN 터널 전체에서 한 방향으로만 흐르거나 터널 전체에서 전송되지 않았을 수 있습니다.

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 항목이 포함되어 있습니다.

- NAT 예외 및 암호화 ACL이 올바른 트래픽을 지정하는지 확인합니다.
- 여러 VPN 터널과 여러 암호화 ACL이 있는 경우 해당 ACL이 중복되지 않는지 확인하십시오.
- ACL을 두 번 사용하지 마십시오. NAT 예외 ACL과 암호화 ACL이 동일한 트래픽을 지정하는 경우에도 두 개의 다른 액세스 목록을 사용합니다.
- 디바이스가 NAT 예외 ACL을 사용하도록 구성되어 있는지 확인합니다. 즉, **route-map** 라우터에 대한 명령, 이 **nat (0)** 명령을 실행합니다. NAT 예외 ACL은 LAN-to-LAN 및 원격 액세스 컨피그레이션에 모두 필요합니다.

ACL 문을 확인하는 방법에 대한 자세한 내용은 Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions(가장 일반적인 L2L 및 원격 액세스 IPsec VPN 트러블슈팅 솔루션)에서 ACL이 Correct인지 확인 섹션을 참조하십시오.

관련 정보

- **IPsec 협상/IKE 프로토콜 지원 페이지**
- **PIX 지원 페이지**
- **기술 노트**
- **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.