ASA와 라우터 간의 Site-to-Site IKEv2 터널 구성

목차

소개

이 문서에서는 Cisco ASA와 Cisco IOS® 소프트웨어를 실행하는 라우터 간에 사이트 대 사이트 IKEv2 터널을 설정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- IKEv2(Internet Key Exchange 버전 2)
- 인증서 및 PKI(Public Key Infrastructure)
- NTP(Network Time Protocol)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 9.8.4를 실행하는 Cisco ASA 5506 Adaptive Security Appliance
- Cisco IOS 소프트웨어 버전 15.3(3)M1을 실행하는 Cisco 2900 Series ISR(Integrated Services Router)

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.

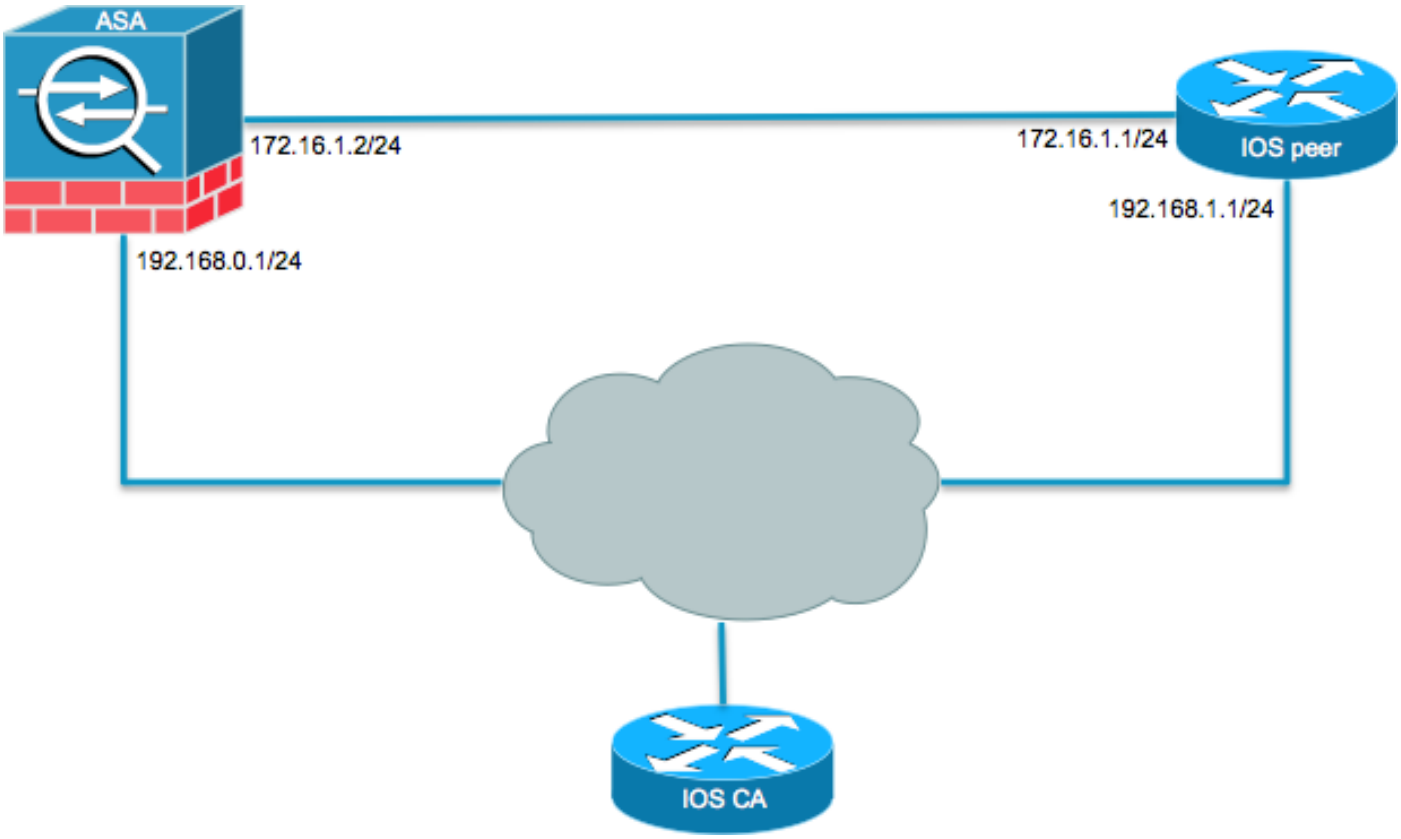
관련 제품

이 문서는 다음과 같은 하드웨어 및 소프트웨어 버전에서도 사용할 수 있습니다.

- 소프트웨어 버전 8.4(1) 이상을 실행하는 Cisco ASA
- Cisco IOS 소프트웨어 버전 15.2(4)M 이상을 실행하는 Cisco ISR Generation 2(G2)
- Cisco IOS-XE 소프트웨어 버전 15.2(4)S 이상을 실행하는 Cisco ASR 1000 Series Aggregation Services Router
- 소프트웨어 버전 15.2(4)M 이상을 실행하는 Cisco Connected Grid 라우터

구성

네트워크 다이어그램



배경 정보

사전 공유 키를 사용하여 ASA와 라우터 간의 IKEv2 터널을 간단하게 구성할 수 있습니다. 그러나 인증서 인증을 사용할 때는 주의해야 할 몇 가지 주의 사항이 있습니다.

NTP

인증서 인증에서는 사용되는 모든 디바이스의 시계를 공통 소스에 동기화해야 합니다. 각 장치에서 수동으로 시계를 설정할 수 있지만, 이는 매우 정확하지 않고 번거로울 수 있습니다. 모든 디바이스에서 시계를 동기화하는 가장 쉬운 방법은 NTP를 사용하는 것입니다. NTP는 분산 시간 서버 및 클라이언트 집합 간의 시간을 동기화합니다. 이 동기화를 통해 시스템 로그가 생성될 때와 다른 시간별 이벤트가 발생할 때 이벤트의 상관관계를 분석할 수 있습니다. NTP 구성 방법에 대한 자세한 내용은 Network Time Protocol: Best Practices 백서를 참조하십시오.

팁: Cisco IOS CA(Software Certificate Authority) 서버를 사용하는 경우 일반적으로 NTP 서버와 동일한 디바이스를 구성합니다. 이 예에서는 CA 서버가 NTP 서버로도 사용됩니다.

HTTP-URL 기반 인증서 조회

HTTP URL에 기반한 인증서 조회는 대용량 인증서가 전송될 때 발생하는 단편화를 방지합니다. 이 기능은 기본적으로 Cisco IOS 소프트웨어 디바이스에서 활성화되므로 Cisco IOS 소프트웨어에서는 인증서 요청 유형 12를 사용합니다.

Cisco 버그 ID CSCul48246에 대한 수정 사항이 없는 소프트웨어 버전이 ASA에서 사용되는 경우 HTTP-URL 기반 조회가 ASA에서 협상되지 않으며 Cisco IOS 소프트웨어로 인해 권한 부여 시도가

실패합니다.

ASA에서 IKEv2 프로토콜 디버그가 활성화된 경우 다음 메시지가 표시됩니다.

```
IKEv2-PROTO-1: (139): Auth exchange failed
IKEv2-PROTO-1: (140): Unsupported cert encoding found or Peer requested
   HTTP URL but never sent
HTTP_LOOKUP_SUPPORTED Notification
```

이 문제를 방지하려면 **no crypto ikev2 http-url cert** 명령을 사용하여 라우터가 ASA와 피어링될 때 라우터에서 이 기능을 비활성화합니다.

피어 ID 검증

IKE AUTH 단계 ISAKMP(Internet Security Association and Key Management Protocol) 협상 중에 피어는 서로 식별해야 합니다. 그러나 라우터와 ASA가 로컬 ID를 선택하는 방법에는 차이가 있습니다.

라우터에서 ISAKMP ID 선택

IKEv2 터널이 라우터에서 사용될 때 협상에 사용되는 로컬 ID는 **identity local** IKEv2 프로파일 아래의 명령:

```
R1(config-ikev2-profile)#identity local ?
  address  address
  dn       Distinguished Name
  email    Fully qualified email string
  fqdn     Fully qualified domain name string
  key-id   key-id opaque string - proprietary types of identification
```

기본적으로 라우터는 주소를 로컬 ID로 사용합니다.

라우터의 ISAKMP ID 검증

필요한 피어 ID도 동일한 프로파일에서 **match identity remote** 명령을 사용합니다:

```
R1(config-ikev2-profile)#match identity remote ?
  address  IP Address(es)
  any      match any peer identity
  email    Fully qualified email string [Max. 255 char(s)]
  fqdn     Fully qualified domain name string [Max. 255 char(s)]
  key-id   key-id opaque string
```

ASA에서 ISAKMP ID 선택

ASA에서 ISAKMP ID는 **crypto isakmp identity** 명령을 사용합니다:

```
ciscoasa/vpn(config)# crypto isakmp identity ?
 configure mode commands/options:
  address   Use the IP address of the interface for the identity
  auto      Identity automatically determined by the connection type: IP
            address for preshared key and Cert DN for Cert based connections
  hostname  Use the hostname of the router for the identity
  key-id    Use the specified key-id for the identity
```

기본적으로 명령 모드는 auto로 설정되며, 이는 ASA가 연결 유형별로 ISAKMP 협상을 결정함을 의미합니다.

- 사전 공유 키의 IP 주소입니다.
- 인증서 인증을 위한 인증서 고유 이름입니다.

참고: Cisco 버그 ID CSCul48099는 전역 컨피그레이션이 아닌 터널 그룹별로 구성할 수 있는 기능을 위한 개선 요청입니다.

ASA에서 ISAKMP ID 검증

원격 ID 검증은 연결 유형에 따라 자동으로 수행되며 변경할 수 없습니다. 검증은 터널 그룹별로 활성화하거나 비활성화할 수 있습니다. **peer-id-validate** 명령을 사용합니다:

```
ciscoasa/vpn(config-tunnel-ipsec)# peer-id-validate ?
 tunnel-group-ipsec mode commands/options:
  cert     If supported by certificate
  nocheck  Do not check
  req      Required
```

상호 운용성 문제

ID 선택/검증의 차이로 인해 두 가지 상호 운용성 문제가 발생합니다.

- ASA에서 인증서 인증이 사용될 때 ASA는 수신된 인증서의 SAN(Subject Alternative Name)에서 피어 ID의 검증을 시도합니다. 피어 ID 검증이 활성화되고 ASA에서 IKEv2 플랫폼 디버그가 활성화된 경우 이러한 디버그가 표시됩니다.

```
IKEv2-PROTO-3: (172): Getting configured policies
```

```
IKEv2-PLAT-3: attempting to find tunnel group for ID: 172.16.1.1
IKEv2-PLAT-3: mapped to tunnel group 172.16.1.1 using phase 1 ID
IKEv2-PLAT-3: (172) tg_name set to: 172.16.1.1
IKEv2-PLAT-3: (172) tunn grp type set to: L2L
IKEv2-PLAT-3: Peer ID check started, received ID type: IPv4 address
IKEv2-PLAT-2: Peer ID check: failed to retreive IP from SAN
IKEv2-PLAT-2: Peer ID check: failed to retreive DNS name from SAN
IKEv2-PLAT-2: Peer ID check: failed to retreive RFC822 name from SAN
IKEv2-PLAT-1: retrieving SAN for peer ID check
IKEv2-PLAT-1: Peer ID check failed
IKEv2-PROTO-1: (172): Failed to locate an item in the database
IKEv2-PROTO-1: (172):
IKEv2-PROTO-5: (172): SM Trace-> SA: I_SPI=833D2323FCB46093
   R_SPI=F0B4D318DDDDB783 (I) MsgID = 00000001 CurState: I_PROC_AUTH
   Event: EV_AUTH_FAIL
IKEv2-PROTO-3: (172): Verify auth failed
IKEv2-PROTO-5: (172): SM Trace-> SA: I_SPI=833D2323FCB46093
   R_SPI=F0B4D318DDDDB783 (I) MsgID = 00000001 CurState: AUTH_DONE
   Event: EV_FAIL
IKEv2-PROTO-3: (172): Auth exchange failed
```

이 문제는 인증서의 IP 주소를 피어 인증서에 포함하거나 피어 ID 검증을 ASA에서 비활성화해야 합니다.

- 마찬가지로, 기본적으로 ASA는 로컬 ID를 자동으로 선택하므로, 인증서 인증을 사용할 경우 ID로 DN(Distinguished Name)을 전송합니다. 라우터가 원격 ID로 주소를 수신하도록 구성된 경우 라우터에서 피어 ID 검증이 실패합니다. 라우터에서 IKEv2 디버그가 활성화된 경우 다음 디버그가 표시됩니다.

```
Nov 30 22:49:14.464: IKEv2:(SESSION ID = 172,SA ID = 1):SM Trace-> SA:
   I_SPI=E9E4B7FD0A336C97 R_SPI=F2CF438C0CCA281C (R) MsgID = 1 CurState:
   R_WAIT_AUTH Event: EV_GET_POLICY_BY_PEERID
Nov 30 22:49:14.464: IKEv2:(SESSION ID = 172,SA ID = 1):Searching policy
   based on peer's identity 'hostname=asa.cisco.com' of type 'DER ASN1 DN'
Nov 30 22:49:14.464: IKEv2:%Profile could not be found by peer certificate.
Nov 30 22:49:14.468: IKEv2:% IKEv2 profile not found
Nov 30 22:49:14.468: IKEv2:(SESSION ID = 172,SA ID = 1):: Failed to
   locate an item in the database
```

이 문제의 경우 FQDN(정규화된 도메인 이름)을 검증하기 위해 라우터를 구성하거나 주소를 ISAKMP ID로 사용하기 위해 ASA를 구성합니다.

참고: 라우터에서 DN을 인식하려면 IKEv2 프로파일에 연결된 인증서 맵을 구성해야 합니다. 설정 방법에 대한 자세한 내용은 IPsec VPN에 대한 인터넷 키 교환 구성 가이드, Cisco IOS XE 릴리스 3S Cisco 문서의 ISAKMP 프로파일 매핑에 대한 인증서 섹션을 참조하십시오.

인증 페이로드 크기

인증에 사전 공유 키가 아닌 인증서가 사용되는 경우 인증 페이로드가 훨씬 큽니다. 이 경우 일반적으로 프래그먼트가 발생하여 경로에서 프래그먼트가 손실되거나 삭제될 경우 인증이 실패할 수 있습니다. 인증 페이로드의 크기 때문에 터널이 나타나지 않으면 일반적인 원인은 다음과 같습니다.

- Control Plane Policing 패킷을 차단할 수 있는 라우터에 있습니다.
- MTU(Maximum Transition Unit) 협상이 잘못되었습니다. **crypto ikev2 fragmentation mtu** *size* 명령을 실행합니다.

ASA에서 다중 컨텍스트 모드의 리소스 할당

ASA 버전 9.0부터 ASA는 다중 컨텍스트 모드의 VPN을 지원합니다. 그러나 다중 컨텍스트 모드에서 VPN을 구성할 때는 VPN이 구성된 시스템에 적절한 리소스를 할당해야 합니다.

자세한 내용은 CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.8의 Information About Resource Management 섹션을 참조하십시오.

인증서 해지 목록의 유효성 검사

CRL(Certificate Revocation List)은 지정된 CA에서 발급하고 이후에 폐기된 폐기된 인증서의 목록입니다. 다음과 같은 여러 가지 이유로 인증서를 취소할 수 있습니다.

- 지정된 인증서를 사용하는 디바이스의 장애 또는 손상.
- 인증서에서 사용하는 키 쌍의 손상.
- ID가 잘못되었거나 이름 변경을 수용해야 하는 등의 발급된 인증서 내의 오류

인증서 취소에 사용되는 메커니즘은 CA에 따라 다릅니다. 폐기된 인증서는 CRL에 일련 번호로 표시됩니다. 네트워크 디바이스가 인증서의 유효성을 확인하려고 하면 현재 CRL에서 제공된 인증서의 일련 번호를 다운로드하고 검사합니다. 따라서 어느 한 피어에서 CRL 검증이 활성화된 경우 ID 인증서의 유효성을 확인할 수 있도록 적절한 CRL URL도 구성해야 합니다.

CRL에 대한 자세한 내용은 Public Key Infrastructure Configuration Guide, Cisco IOS XE Release 3S의 What a CRL 섹션을 참조하십시오.

인증서 체인 검증

ASA가 중간 CA가 있는 인증서로 구성되어 있고 해당 피어에 동일한 중간 CA가 없는 경우, 라우터에 전체 인증서 체인을 보내도록 ASA를 명시적으로 구성해야 합니다. 라우터는 기본적으로 이를 수행합니다. 이렇게 하려면 암호화 맵 아래에서 신뢰 지점을 정의할 때 다음과 같이 chain 키워드를 추가합니다.

```
crypto map outside-map 1 set trustpoint ios-ca chain
```

이렇게 하지 않으면 ASA가 응답자인 경우에만 터널이 협상됩니다. Initiator인 경우 터널 협상이 실

패하고 라우터의 PKI 및 IKEv2 디버깅에 다음 내용이 표시됩니다.

```
2328304: Jun  8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):
Get peer's authentication method
2328305: Jun  8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):
Peer's authentication method is 'RSA'
2328306: Jun  8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):
SM Trace-> SA: I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1
 CurState: R_VERIFY_AUTH Event: EV_CHK_CERT_ENC
2328307: Jun  8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):
SM Trace-> SA: I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1
 CurState: R_VERIFY_AUTH Event: EV_VERIFY_X509_CERTS
2328308: Jun  8 19:14:38.051 GMT: CRYPTO_PKI: (A16A8) Adding peer certificate
2328309: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: Added x509 peer certificate -(1359) bytes
2328310: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: ip-ext-val: IP extension validation
 not required
2328311: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: create new ca_req_context type
 PKI_VERIFY_CHAIN_CONTEXT,ident 4177
2328312: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8)validation path has 1 certs
2328313: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8) Check for identical certs
2328314: Jun  8 19:14:38.055 GMT: CRYPTO_PKI : (A16A8) Validating non-trusted cert
2328315: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8) Create a list of suitable
 trustpoints
2328316: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: Unable to locate cert record by
 issuername
2328317: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: No trust point for cert issuer,
 looking up cert chain
2328318: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8) No suitable trustpoints found
2328319: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):: Platform
 errors
2328320: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):SM Trace-> SA:
 I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1 CurState:
 R_VERIFY_AUTH Event: EV_CERT_FAIL
2328321: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):Verify cert
 failed
2328322: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):
SM Trace-> SA: I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1 CurState:
 R_VERIFY_AUTH Event: EV_AUTH_FAIL
2328323: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68)
:Verification of peer's authentication data FAILED
```

샘플 ASA 컨피그레이션

```
domain-name cisco.com
!
interface outside
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!
interface CA
 nameif CA
 security-level 50
 ip address 192.168.0.1 255.255.255.0
!
```

```
! acl which defines crypto domains, must be mirror images on both peers
!
access-list cryacl extended permit ip 192.168.0.0 255.255.255.0 172.16.2.0
   255.255.255.0
pager lines 24
logging console debugging
mtu outside 1500
mtu CA 1500
mtu backbone 1500
route outside 172.16.2.0 255.255.255.0 172.16.1.1 1
route CA 192.168.254.254 255.255.255.255 192.168.0.254 1
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto map outside-map 1 match address cryacl
crypto map outside-map 1 set pfs
crypto map outside-map 1 set peer 172.16.1.1
crypto map outside-map 1 set ikev2 ipsec-proposal DES AES256
crypto map outside-map 1 set trustpoint ios-ca chain
crypto map outside-map interface outside
crypto ca trustpoint ios-ca
 enrollment url http://192.168.254.254:80
 fqdn asa.cisco.com
 keypair ios-ca
 crl configure
crypto ca certificate chain ios-ca
 certificate ca 01
    3082020f 30820178 a0030201 02020101 300d0609 2a864886 f70d0101 04050030
    1b311930 17060355 04031310 696f732d 63612e63 6973636f 2e636f6d 301e170d
    31333131 31353231 33353533 5a170d31 33313231 35323133 3535335a 301b3119
    30170603 55040313 10696f73 2d63612e 63697363 6f2e636f 6d30819f 300d0609
    2a864886 f70d0101 01050003 818d0030 81890281 81009ebb 48957c44 c940236f
    a1cda758 aa930e8c 91390734 b8ef814d 0bf7aec9 7ec40379 7749d3c6 154f6a32
    00738655 33b20207 037a9e15 3229fa72 478424fb 409f518d b13d328d e761be08
    8023b4ff f4100054b 4423156d 66c99788 69ab5956 966d5e1b 4d1c1120 a05ad08c
    f036a134 3b2fc425 e4a2524f 36e0a129 2c8f6cee 971d0203 010001a3 63306130
    0f060355 1d130101 ff040530 030101ff 300e0603 551d0f01 01ff0404 03020186
    301f0603 551d2304 18301680 14082896 b9f4af20 75514321 d072f161 d09d2ec8
    aa301d06 03551d0e 04160414 082896b9 f4af2075 514321d0 72f161d0 9d2ec8aa
    300d0609 2a864886 f70d0101 04050003 81810087 a06d354a f7423e0e 64a7c5ec
    6006fbde 914d7bfd f86ada50 b1a00d17 0bf06ec1 5423d514 fbeb0a76 986eb63f
    f7fce99a 81c4b112 61fd69ce a2ce750e b1b3a6f9 84e92490 8f213613 451dd9a8
    3fc3406a 854b20ed 27e4ddd8 62f6dea5 dd8b4396 1879b3e7 651cb9d1 3dd46b8b
    32796963 9f6854f1 389f0060 aa0d1b8d f83e09
  quit
 certificate 08
    3082028e 308201f7 a0030201 02020108 300d0609 2a864886 f70d0101 04050030
    1b311930 17060355 04031310 696f732d 63612e63 6973636f 2e636f6d 301e170d
    31333131 31383136 31383130 5a170d31 33313132 38313631 3831305a 301e311c
    301a0609 2a864886 f70d0109 02160d61 73612e63 6973636f 2e636f6d 30819f30
    0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c38ee5 75215237
    2728cffd 3519cd15 ebcaab2c 48d63b92 7562d2fc f7db60bc ecb03b2c 4e4dff07
    47ad5122 80899055 37f346d7 d10962e9 1e5edb06 8985ee7e 8a6da977 2460f82e
    53679457 ed10372a 9ff2946e 449214e4 9be95cab 51d7681c 2db0382b 048fe807
    1d1bb9b0 e4bd9de6 c99cafea c279e943 1e1f5d1b d1e6010c b7020301 0001a381
    de3081db 30310603 551d2504 2a302806 082b0601 05050703 0106082b 06010505
    07030506 082b0601 05050703 0606082b 06010505 07030730 3c060355 1d1f0435
    30333031 a02fa02d 862b6874 74703a2f 2f313932 2e313638 2e323534 2e323534
```

```
    2f696f73 2d636163 64702e69 6f732d63 612e6372 6c301806 03551d11 0411300f
    820d6173 612e6369 73636f2e 636f6d30 0e060355 1d0f0101 ff040403 0205a030
    1f060355 1d230418 30168014 082896b9 f4af2075 514321d0 72f161d0 9d2ec8aa
    301d0603 551d0e04 1604145b 76de9ef0 d3255efe f4bc551b 69cd8398 d1596c30
    0d06092a 864886f7 0d010104 05000381 81003fb0 ec7719cd 4f6162b2 90727db4
    da5606f2 61441dc6 094fb3a6 defe62ef 5ff8f140 3bc3448c e0b42d26 07647607
    fd7518cb 034139d3 e3648fd2 9d93b5e4 db3b828b 16d50dd5 3e18cdd6 74855de4
    88a159d6 6ef51718 cf6cc4e4 53c2aca3 36442ff0 bb4b8493 22f0e632 a8b32b36
    f287801f 8d47637f e4e9ee6a b4555094 c092
  quit
!
! manually select the ISAKMP identity to use address on the ASA
crypto isakmp identity address
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 14 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 10
 encryption aes-192
 integrity sha256 sha
 group 14 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 30
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside
!
! to allow pings from the CA interface that will bring up the tunnel during
    testing.
!
management-access CA
!
group-policy GroupPolicy2 internal
group-policy GroupPolicy2 attributes
 vpn-idle-timeout 30
 vpn-tunnel-protocol ikev1 ikev2
tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 general-attributes
 default-group-policy GroupPolicy2
tunnel-group 172.16.1.1 ipsec-attributes
!
! disable peer-id validation
!
 peer-id-validate nocheck
 ikev2 remote-authentication certificate
 ikev2 local-authentication certificate ios-ca
: end
! NTP configuration
ntp trusted-key 1
ntp server 192.168.254.254
```

샘플 라우터 컨피그레이션

```
ip domain name cisco.com
!
crypto pki trustpoint tp_ikev2
 enrollment url http://192.168.254.254:80
 usage ike
 fqdn R1.cisco.com
!
! necessary only in this example as no crl has been configured on the IOS CA.
   On the ASA this is enabled by default. When using proper 3rd party
   certificates this is not necessary.
!
 revocation-check none
 rsakeypair ikev2_cert
 eku request server-auth
!
crypto pki certificate chain tp_ikev2
 certificate 0B
 308202F4 3082025D A0030201 0202010B 300D0609 2A864886 F70D0101 05050030
 1B311930 17060355 04031310 696F732D 63612E63 6973636F 2E636F6D 301E170D
 31333131 32353233 35363537 5A170D31 33313230 35323335 3635375A 301D311B
 30190609 2A864886 F70D0109 02160C52 312E6369 73636F2E 636F6D30 82012230
 0D06092A 864886F7 0D010101 05000382 010F0030 82010A02 82010100 A1032A61
 A3F14539 87816C22 8C66A170 3A9661EA 4AF6F063 3FC305B8 E525B84D AA74A9CE
 666B1BF5 3C7DF025 31FEB161 CE49845F 3EC2DE7B D3FCC685 D6F80C8C 0AA12772
 1B4AB15C 90C04446 068A0DBA 7BFA4E40 E978364F A2B07F7C 02C691A8 921A5481
 A4AF07B4 BA0C9DBA D35F4566 6CB70553 DAF09A45 F2948C5A 1621E5D2 98508D49
 A2EF61D3 AAF3A9DB 87F2D763 89AD0BBE 916A6CF8 1B59C426 7960013B 061AA0A5
 F6870319 87A35ABA 8C1B5CF5 42976739 B8C936D3 24276E56 F59E3CFD 9B9B4A0D
 2E5294AB C4470376 5D96915F 275CBC78 586D6755 F45C7592 62DCA916 CEC1A450
 3FF090A9 15088CD2 13B90391 B0795263 071C7002 8CBF98F2 89788A0B 02030100
 01A381C1 3081BE30 3C060355 1D1F0435 30333031 A02FA02D 862B6874 74703A2F
 2F313932 2E313638 2E323534 2E323534 2F696F73 2D636163 64702E69 6F732D63
 612E6372 6C303106 03551D25 042A3028 06082B06 01050507 03010608 2B060105
 05070305 06082B06 01050507 03060608 2B060105 05070307 300B0603 551D0F04
 04030205 A0301F06 03551D23 04183016 80140828 96B9F4AF 20755143 21D072F1
 61D09D2E C8AA301D 0603551D 0E041604 14C63949 4CA10DBB 2BBB6F98 BAFF0EE2
 B3716CEE 3B300D06 092A8648 86F70D01 01050500 03818100 3080FEF6 9160357B
 6F28ED60 428BA6CE 203706F6 F91DA273 AF6E81D3 46539E13 B4C89A9A 19E1F0BC
 A631A418 C30DFC8E 0585039D EB07D35D E719F5FE A4EE47B5 CED31B12 745C9EE8
 5B6B0F17 67C3B965 C927B379 C674933F 84E7A1F7 851A6CF0 8775B1C5 3A033D90
 75965DCA 86E4A842 E2C35AC0 6BFA8144 699B1582 C094BF35
 quit
 certificate ca 01
 3082020F 30820178 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 1B311930 17060355 04031310 696F732D 63612E63 6973636F 2E636F6D 301E170D
 31333131 31353231 33353533 5A170D31 33313231 35323133 3535335A 301B3119
 30170603 55040313 10696F73 2D63612E 63697363 6F2E636F 6D30819F 300D0609
 2A864886 F70D0101 01050003 818D0030 81890281 81009EBB 48957C44 C940236F
 A1CDA758 AA930E8C 91390734 B8EF814D 0BF7AEC9 7EC40379 7749D3C6 154F6A32
 00738655 33B20207 037A9E15 3229FA72 478424FB 409F518D B13D328D E761BE08
 8023B4FF F4100054B 4423156D 66C99788 69AB5956 966D5E1B 4D1C1120 A05AD08C
 F036A134 3B2FC425 E4A2524F 36E0A129 2C8F6CEE 971D0203 010001A3 63306130
 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186
 301F0603 551D2304 18301680 14082896 B9F4AF20 75514321 D072F161 D09D2EC8
 AA301D06 03551D0E 04160414 082896B9 F4AF2075 514321D0 72F161D0 9D2EC8AA
 300D0609 2A864886 F70D0101 04050003 81810087 A06D354A F7423E0E 64A7C5EC
 6006FBDE 914D7BFD F86ADA50 B1A00D17 0BF06EC1 5423D514 FBEB0A76 986EB63F
 F7FCE99A 81C4B112 61FD69CE A2CE750E B1B3A6F9 84E92490 8F213613 451DD9A8
 3FC3406A 854B20ED 27E4DDD8 62F6DEA5 DD8B4396 1879B3E7 651CB9D1 3DD46B8B
 32796963 9F6854F1 389F0060 AA0D1B8D F83E09
 quit
!
```

```
crypto ikev2 proposal aes-cbc-256-proposal
 encryption aes-cbc-256
 integrity sha1
 group 5 2 14
!
crypto ikev2 policy policy1
 match address local 172.16.1.1
 proposal aes-cbc-256-proposal
!
crypto ikev2 profile profile1
 description IKEv2 profile
!
! router configured to use address as the remote identity. By default local
   identity is address
!
 match address local 172.16.1.1
 match identity remote address 172.16.1.2 255.255.255.255
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint tp_ikev2
!
! disable http-url based cert lookup
!
no crypto ikev2 http-url cert
!
crypto ipsec transform-set ESP-AES-SHA esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
 set peer 172.16.1.2
 set transform-set ESP-AES-SHA
 set pfs group2
 set ikev2-profile profile1
 match address 103
!
interface Loopback0
 ip address 172.16.2.1 255.255.255.255
!
interface GigabitEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
 crypto map SDM_CMAP_1
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
ip route 192.168.0.0 255.255.255.0 172.16.1.2
ip route 192.168.254.254 255.255.255.255 192.168.1.254
!
! access list that defines crypto domains, must be mirror images on both peers.
!
access-list 103 permit ip 172.16.2.0 0.0.0.255 192.168.0.0 0.0.0.255
!
! ntp configuration
!
ntp trusted-key 1
ntp server 192.168.254.254
!
end
```

샘플 Cisco IOS CA 컨피그레이션

```
ip domain name cisco.com
!
! CA server configuration
!
crypto pki server ios-ca
 database archive pkcs12 password 7 02050D4808095E731F
 issuer-name CN=ios-ca.cisco.com
 grant auto
 lifetime certificate 10
 lifetime ca-certificate 30
 cdp-url http://192.168.254.254/ios-cacdp.ios-ca.crl
 eku server-auth ipsec-end-system ipsec-tunnel ipsec-user
!
! this trustpoint is generated automatically when the CA server is enabled.
!
crypto pki trustpoint ios-ca
 revocation-check crl
 rsakeypair ios-ca
!
!
crypto pki certificate chain ios-ca
 certificate ca 01
 3082020F 30820178 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 1B311930 17060355 04031310 696F732D 63612E63 6973636F 2E636F6D 301E170D
 31333131 31353231 33353533 5A170D31 33313231 35323133 3535335A 301B3119
 30170603 55040313 10696F73 2D63612E 63697363 6F2E636F 6D30819F 300D0609
 2A864886 F70D0101 01050003 818D0030 81890281 81009EBB 48957C44 C940236F
 A1CDA758 AA930E8C 91390734 B8EF814D 0BF7AEC9 7EC40379 7749D3C6 154F6A32
 00738655 33B20207 037A9E15 3229FA72 478424FB 409F518D B13D328D E761BE08
 8023B4FF F410054B 4423156D 66C99788 69AB5956 966D5E1B 4D1C1120 A05AD08C
 F036A134 3B2FC425 E4A2524F 36E0A129 2C8F6CEE 971D0203 010001A3 63306130
 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186
 301F0603 551D2304 18301680 14082896 B9F4AF20 75514321 D072F161 D09D2EC8
 AA301D06 03551D0E 04160414 082896B9 F4AF2075 514321D0 72F161D0 9D2EC8AA
 300D0609 2A864886 F70D0101 04050003 81810087 A06D354A F7423E0E 64A7C5EC
 6006FBDE 914D7BFD F86ADA50 B1A00D17 0BF06EC1 5423D514 FBEB0A76 986EB63F
 F7FCE99A 81C4B112 61FD69CE A2CE750E B1B3A6F9 84E92490 8F213613 451DD9A8
 3FC3406A 854B20ED 27E4DDD8 62F6DEA5 DD8B4396 1879B3E7 651CB9D1 3DD46B8B
 32796963 9F6854F1 389F0060 AA0D1B8D F83E09
 quit
voice-card 0
!
!
interface Loopback0
 ip address 192.168.254.254 255.255.255.255
!
interface GigabitEthernet0/0
 ip address 192.168.0.254 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.254 255.255.255.0
 duplex auto
 speed auto
!
```

```
! http-server needs to be enabeld for SCEP
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.122.162.129
ip route 172.18.108.26 255.255.255.255 10.122.162.129
!
! ntp configuration
!
ntp trusted-key 1
ntp master 1
!
end
```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

이 명령은 ASA와 라우터 모두에서 작동합니다.

- **show crypto ikev2 sa** - 1단계 SA(Security Association)의 상태를 표시합니다.
- **show crypto ipsec sa** - 2단계 SA의 상태를 표시합니다.

> 참고: 이 출력에서는 IKEv1과 달리 PFS(Perfect Forwarding Secrecy) DH(Diffie-Hellman) 그룹 값이 첫 번째 터널 협상 중에 'PFS(Y/N): N, DH group: none'으로 표시됩니다. rekey가 발생하면 올바른 값이 표시됩니다. 이는 버그가 아니라 예상 동작입니다.
>
> IKEv1과 IKEv2의 차이점은 IKEv2에서 하위 SA는 AUTH 교환 자체의 일부로 생성된다는 점입니다. 암호화 맵 아래에 구성된 DH 그룹은 키 재설정 중에만 사용됩니다. 따라서 첫 번째 키 재지정 전까지는 'PFS (Y/N): N, DH group: none'이 표시됩니다. IKEv1에서는 하위 SA가 빠른 모드 중에 생성되고 CREATE_CHILD_SA 메시지에 키 교환 페이로드를 전달하는 프로비전이 있으므로 다른 동작이 표시됩니다. 이 페이로드는 새 공유 암호를 파생하기 위한 DH 매개변수를 지정합니다.

1단계 확인

이 절차에서는 1단계 활동을 확인합니다.

1. 다음을 입력합니다. **show crypto ikev2 sa** 라우터의 명령:

```
R1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf    Status
1         172.16.1.1/500        172.16.1.2/500        none/none    READY
      Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:14, Auth sign: RSA,
```

```
         Auth verify: RSA
      Life/Active Time: 86400/53 sec
 IPv6 Crypto IKEv2  SA
```

2. 다음을 입력합니다. **show crypto ikev2 sa** ASA의 명령:

```
ciscoasa/vpn(config)# show crypto ikev2 sa

IKEv2 SAs:

Session-id:138, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                Status       Role
45926289  172.16.1.2/500        172.16.1.1/500        READY        INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:14, Auth sign: RSA,
         Auth verify: RSA
      Life/Active Time: 86400/4 sec
Child sa: local selector  192.168.0.0/0 - 192.168.0.255/65535
          remote selector 172.16.2.0/0 - 172.16.2.255/65535
          ESP spi in/out: 0xa84caabb/0xf18dce57
```

2단계 검증

이 절차에서는 두 피어에서 SPI(Security Parameter Index)가 올바르게 협상되었는지 확인하는 방법에 대해 설명합니다.

1. 다음을 입력합니다. **show crypto ipsec sa | i spi** 라우터의 명령:

```
R1#show crypto ipsec sa | i spi
     current outbound spi: 0xA84CAABB(2823596731)
      spi: 0xF18DCE57(4052602455)
      spi: 0xA84CAABB(2823596731)
```

2. 다음을 입력합니다. **show crypto ipsec sa | i spi** ASA의 명령:

```
ciscoasa/vpn(config)# show crypto ipsec sa | i spi
      current outbound spi: F18DCE57
      current inbound spi : A84CAABB
      spi: 0xA84CAABB (2823596731)
      spi: 0xF18DCE57 (4052602455)
```

이 절차에서는 트래픽이 터널을 통과하는지 여부를 확인하는 방법에 대해 설명합니다.

1. 다음을 입력합니다. **show crypto ipsec sa | i pkts** 라우터의 명령:

```
R1#show crypto ipsec sa | i pkts
    #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
    #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
```

2. 다음을 입력합니다. **show crypto ipsec sa | i pkts** ASA의 명령:

```
ciscoasa/vpn(config)# show crypto ipsec sa | i pkts
      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp
         failed: 0
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

참고: Debug 명령에 대한 중요한 정보를 참조한 후 사용하십시오. **debug** 명령을 사용합니다.

ASA에서 디버깅

주의: ASA에서는 다양한 디버그 레벨을 설정할 수 있습니다. 기본적으로 레벨 1이 사용됩니다. 디버그 수준을 변경하면 디버그의 세부 정도가 증가할 수 있습니다. 특히 프로덕션 환경에서는 이 작업을 신중하게 수행해야 합니다.

터널 협상을 위한 ASA 디버깅은 다음과 같습니다.

- **debug crypto ikev2 protocol**
- **debug crypto ikev2 platform**

인증서 인증을 위한 ASA 디버그:

- **debug crypto ca**

라우터의 디버깅

터널 협상을 위한 라우터 디버깅은 다음과 같습니다.

- **debug crypto ikev2**

- **debug crypto ikev2 error**
- **debug crypto ikev2 internal**

인증서 인증을 위한 라우터 디버깅은 다음과 같습니다.

- **debug cry pki validation**
- **debug cry pki transaction**
- **debug cry pki messages**

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.