# FlexVPN with Next-Generation Encryption 컨피그레이션 예

## 목차



## 소개

이 문서에서는 Cisco NGE(Next-Generation Encryption) 알고리즘 집합을 지원하는 두 라우터 간에 FlexVPN을 구성하는 방법에 대해 설명합니다.

### 차세대 암호화

Cisco NGE 암호화는 구성 가능하고 잘 설정된 공용 도메인 암호화 알고리즘을 사용하는 네트워크를 통해 전송되는 정보를 보호합니다.

- 128비트 또는 256비트 키를 사용하는 AES(Advanced Encryption Standard) 기반 암호화
- 256비트 및 384비트 프라임 모듈리와 함께 곡선을 사용하는 ECDSA(Elliptic Curve Digital Signature Algorithm)를 사용하는 디지털 서명
- ECDH(Elliptic Curve Diffie-Hellman) 방법을 사용하는 키 교환
- SHA-2(Secure Hash Algorithm 2) 기반 해싱(디지털 지문)

국가안보국(NSA)은 이 네 가지 알고리즘이 결합되어 기밀 정보에 대한 적절한 정보 보증을 제공한다고 말한다.IPsec용 NSA Suite B 암호화는 RFC 6379에 표준으로 게시되었으며 업계에서 인정받았습니다.

### Suite Suite-B-GCM-128

RFC 6379에 따라 이러한 알고리즘은 Suite-B-GCM-128 제품군에 필요합니다.

이 제품군은 128비트 AES-GCM을 사용하여 ESP(Encapsulating Security Payload) 무결성 보호 및 기밀성을 제공합니다(RFC4106 참조). ESP 무결성 보호 및 암호화가 모두 필요한 경우 이 제품군을 사용해야 합니다.

**ESP**
GCM(Galois/Counter Mode)에서 128비트 키 및 168진수 무결성 검사 값(ICV)을 사용하는 암호화 AES(RFC4106)
무결성 NULL

**IKEv2**
CBC(Cipher Block Chaining) 모드에서 128비트 키를 사용하는 암호화 AES(RFC3602)
의사 난수 함수 HMAC-SHA-256(RFC4868)
무결성 HMAC-SHA-256-128(RFC4868)
Diffie-Hellman 그룹 256비트 임의 ECP 그룹(RFC5903)

Suite B 및 NGE에 대한 자세한 내용은 Next-Generation Encryption에서 확인할 수 있습니다.

# 사전 요구 사항

## 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FlexVPN
- IKEv2(Internet Key Exchange version 2)
- IPsec

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 하드웨어:보안 라이센스를 실행하는 ISR(Integrated Services Router) Generation 2(G2)
- 소프트웨어:Cisco IOS® Software 릴리스 15.2.3T2. Cisco IOS Software 릴리스 M 또는 15.1.2T 이상의 릴리스는 GCM이 도입되었기 때문에 사용할 수 있습니다.

자세한 내용은 기능 탐색기를 참조하십시오.

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

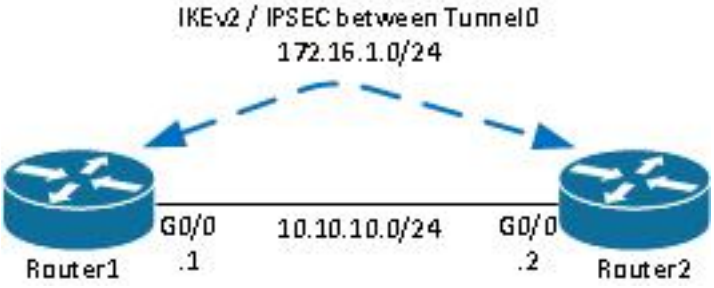
# 인증 기관

현재 Cisco IOS 소프트웨어는 Suite B에 필요한 ECDH를 실행하는 로컬 CA(Certificate Authority) 서버를 지원하지 않습니다. 서드파티 CA 서버를 구현해야 합니다.이 예에서는 Suite B PKI 기반 Microsoft CA를 사용합니다.

# 구성

## 네트워크 토폴로지

이 가이드는 이 토폴로지를 기반으로 합니다. IP 주소는 요구 사항에 맞게 수정해야 합니다.




참고:

설정은 두 개의 라우터가 직접 연결되어 있으며 여러 홉으로 구분될 수 있습니다. 이렇게 하면 피어 IP 주소에 연결할 경로가 있는지 확인하십시오.이 컨피그레이션은 사용된 암호화에 대해서만 자세히 설명합니다. IPSec VPN을 통해 IKEv2 라우팅 또는 라우팅 프로토콜을 구현해야 합니다.

## 라우터가 EC 디지털 서명 알고리즘을 사용하도록 설정하는 단계

1. EC 키 쌍을 만들기 위한 사전 요구 사항인 도메인 이름 및 호스트 이름을 만듭니다.

```
ip domain-name cisco.com
hostname Router1
crypto key generate ec keysize 256 label Router1.cisco.com
```

**참고:**Cisco 버그 ID CSCue59994에 대한 수정 버전을 실행하지 않는 경우, 라우터는 키 크기가 768보다 작은 인증서를 등록할 수 없습니다.

2. CA에서 인증서를 얻기 위해 로컬 신뢰 지점을 생성합니다.

```
crypto pki trustpoint ecdh
 enrollment terminal
 revocation-check none
 eckeypair Router1.cisco.com
```

**참고:**CA가 오프라인 상태이므로 해지 검사를 사용할 수 없습니다. 프로덕션 환경에서 최대 보안을 유지하려면 해지 검사를 사용해야 합니다.

3. 신뢰 지점을 인증합니다(공개 키가 포함된 CA 인증서의 복사본을 얻음).

```
crypto pki authenticate ecdh
```

4. 프롬프트에서 CA의 기본 64로 인코딩된 인증서를 입력합니다. quit를 입력한 다음 **yes를** 입력하여 수락합니다.

5. CA의 PKI에 라우터를 등록합니다.

```
crypto pki enrol ecdh
```

6. 표시된 출력은 CA에 인증서 요청을 제출하는 데 사용됩니다.Microsoft CA의 경우 CA의 웹 인터페이스에 연결하고 **인증서 요청 제출을** 선택합니다.

7. CA에서 받은 인증서를 라우터로 가져옵니다.인증서를 가져오면 quit을 입력합니다.

```
crypto pki import ecdh certificate
```

## 구성

여기에 제공된 컨피그레이션은 Router1에 대한 것입니다. Router2에는 터널 인터페이스의 IP 주소만 고유한 컨피그레이션의 미러가 필요합니다.

1. 피어 디바이스의 인증서와 매칭할 인증서 맵을 만듭니다.

```
crypto pki certificate map certmap 10
 subject-name co cisco.com
```

2. Suite B에 대한 IKEv2 제안서를 구성합니다.

```
crypto ikev2 proposal default
 encryption aes-cbc-128
 integrity sha256
 group 19
```

**참고:**IKEv2 Smart Defaults는 기본 IKEv2 제안서 내에서 미리 구성된 다수의 알고리즘을 구현합니다.Suite Suite-B-GCM-128에는 aes-cbc-128 및 sha256이 필요하므로 이러한 알고리즘 내에서 aes-cbc-256, sha384 및 sha512를 제거해야 합니다.그 이유는 IKEv2가 선택사항이 있을 때 가장 강력한 알고리즘을 선택했기 때문입니다.보안을 극대화하려면 aes-cbc-256 및 sha512를 사용합니다. 그러나 Suite-B-GCM-128에는 필요하지 않습니다. 구성된 IKEv2 제안을 보려면 **show crypto ikev2 proposal** 명령을 입력합니다.

3. IKEv2 프로필을 구성하여 인증서 맵과 일치시키고 이전에 정의된 신뢰 지점에서 ECDSA를 사용합니다.

```
crypto ikev2 profile default
 match certificate certmap
 identity local dn
 authentication remote ecdsa-sig
 authentication local ecdsa-sig
 pki trustpoint ecdh
```

4. GCM을 사용하도록 IPSec 변환을 구성합니다.

```
crypto ipsec transform-set ESP_GCM esp-gcm
 mode transport
```

5. 앞에서 구성한 매개변수를 사용하여 IPSec 프로파일을 구성합니다.

```
crypto ipsec profile default
 set transform-set ESP_GCM
 set pfs group19
 set ikev2-profile default
```

6. 터널 인터페이스를 구성합니다.

```
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 tunnel source Gigabit0/0 tunnel destination 10.10.10.2
 tunnel protection ipsec profile default
```

# 연결 확인

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

1. ECDSA 키가 생성되었는지 확인합니다.

```
Router1#show crypto key mypubkey ec
% Key pair was generated at: 04:05:07 JST Jul 6 2012
Key name: Router1.cisco.com
Key type: EC KEYS
 Storage Device: private-config
 Usage: Signature Key
 Key is not exportable.
 Key Data&colon;
 30593013 06072A86 48CE3D02 0106082A 8648CE3D 03010703 4200048F 2B0B5B5E
(...omitted...)
```

2. 인증서가 성공적으로 가져오기되었으며 ECDH가 사용되는지 확인합니다.

```
Router1#show crypto pki certificates verbose ecdh
Certificate
 Status: Available
 Version: 3
 Certificate Serial Number (hex): 6156E3D5000000000009
(...omitted...)
```

3. IKEv2 SA가 성공적으로 생성되었고 Suite B 알고리즘을 사용하는지 확인합니다.

```
Router1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA
```

```
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.10.10.1/500        10.10.10.2/500        none/none            READY
     Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:19, Auth sign: ECDSA, Auth verify:
ECDSA
     Life/Active Time: 86400/20 sec
```

4. IKEv2 SA가 성공적으로 생성되었고 Suite B 알고리즘을 사용하는지 확인합니다.

```
Router1#show crypto ipsec sa

interface: Tunnel0
   Crypto map tag: Tunnel0-head-0, local addr 10.10.10.1

(...omitted...)

    local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2
    plaintext mtu 1466, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0xAC5845E1(2891466209)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0xAEF7FD9C(2935487900)
       transform: esp-gcm ,
       in use settings ={Transport, }
       conn id: 6, flow_id: SW:6, sibling_flags 80000000, crypto map: Tunnel0-head-0
       sa timing: remaining key lifetime (k/sec): (4341883/3471)
       IV size: 8 bytes
       replay detection support: N
       Status: ACTIVE(ACTIVE)
```

**참고:**이 출력에서는 IKEv1(Internet Key Exchange version 1)과 달리 PFS(Perfect Forward Secrecy) DH(Diffie-Hellman) 그룹 값이 **PFS(Y/N)**로 표시됩니다.**N, DH 그룹:**첫 번째 터널 협상 중에는 **없음**이 표시되지만 rekey가 발생한 후에는 오른쪽 값이 표시됩니다.Cisco 버그 ID CSCug67056에 동작이 설명되어 있지만 이 버그는 아닙니다. IKEv1과 IKEv2의 차이점은 후자의 SA(Child Security Associations)가 AUTH 교환 자체의 일부로 생성된다는 것입니다.암호화 맵에 구성된 DH 그룹은 키 재설정 동안에만 사용됩니다.따라서 PFS**(Y/N)가 표시됩니다.N, DH 그룹:**첫 번째 키 다시 **키**가 올 때까지 없음그러나 IKEv1에서는 하위 SA 생성이 빠른 모드 중에 발생하고 CREATE_CHILD_SA 메시지에는 새 공유 암호를 파생하기 위해 DH 매개변수를 지정하는 키 교환 페이로드를 전달하기 위한 프로비저닝이 있기 때문에 다른 동작이 표시됩니다.

# 문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

# 결론

NGE에 정의된 효율적이고 강력한 암호화 알고리즘은 데이터 기밀성과 무결성을 낮은 처리 비용으로 제공하고 유지 관리한다는 장기적 보장을 제공합니다.NGE는 Suite B 표준 암호화를 제공하는 FlexVPN을 통해 손쉽게 구현할 수 있습니다.

Cisco가 Suite B를 구현하는 방법에 대한 자세한 내용은 Next-Generation Encryption에서 확인할 수 있습니다.