FlexVPN Between a Router and an ASA with Next Generation Encryption 컨피그레이션 예

목차

소개

이 문서에서는 FlexVPN을 사용하는 라우터와 Cisco NGE(Next Generation Encryption) 알고리즘을 지원하는 ASA(Adaptive Security Appliance) 간에 VPN을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FlexVPN
- IKEv2(Internet Key Exchange version 2)
- IPSec
- ASA
- 차세대 암호화

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- **하드웨어:** 보안 라이센스를 실행하는 IOS Generation 2(G2) 라우터입니다.
- **소프트웨어:** Cisco IOS® Software 릴리스 버전 15.2-3.T2. Cisco IOS® Software 릴리스 버전 15.1.2T 이후의 릴리스에 대한 M 또는 T 릴리스는 GCM(Galois Counter Mode)의 도입과 함께 포함되어 있으므로 사용할 수 있습니다.
- **하드웨어:** NGE를 지원하는 ASA.**참고:** 멀티코어 플랫폼만 AES(Advanced Encryption Standard) GCM을 지원합니다.
- **소프트웨어:** NGE를 지원하는 ASA 소프트웨어 릴리스 9.0 이상
- OpenSSL입니다.

자세한 내용은 Cisco Feature Navigator를 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.

표기 규칙

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

동적으로 IPSec 보안 연결 생성

IOS에서 권장되는 IPSec 인터페이스는 IPsec으로 보호되는 GRE(Generic Routing Encapsulation) 인터페이스를 생성하는 VTI(Virtual Tunnel Interface)입니다. VTI의 경우 Traffic Selector(IPSec SA(Security Associations)에서 보호해야 하는 트래픽)는 터널 소스에서 터널 대상으로의 GRE 트래픽으로 구성됩니다. ASA는 GRE 인터페이스를 구현하지 않고 대신 ACL(Access Control List)에 정의된 트래픽을 기반으로 IPSec SA를 생성하므로, 라우터가 제안된 트래픽 선택기의 미러로 IKEv2 시작에 응답할 수 있는 방법을 활성화해야 합니다. FlexVPN 라우터에서 DVTI(Dynamic Virtual Tunnel Interface)를 사용하면 이 디바이스가 제공된 트래픽 선택기의 미러를 사용하여 제공된 트래픽 선택기에 응답할 수 있습니다.

이 예에서는 두 내부 네트워크 간의 트래픽을 암호화합니다. ASA에서 ASA 내부 네트워크의 트래픽 선택기를 IOS 내부 네트워크 `192.168.1.0/24`에서 `172.16.10.0/24`로 전송하면 DVTI 인터페이스는 트래픽 선택기의 미러로 응답합니다. 이는 `172.16.10.0/24 192.168.1.0/24`입니다.

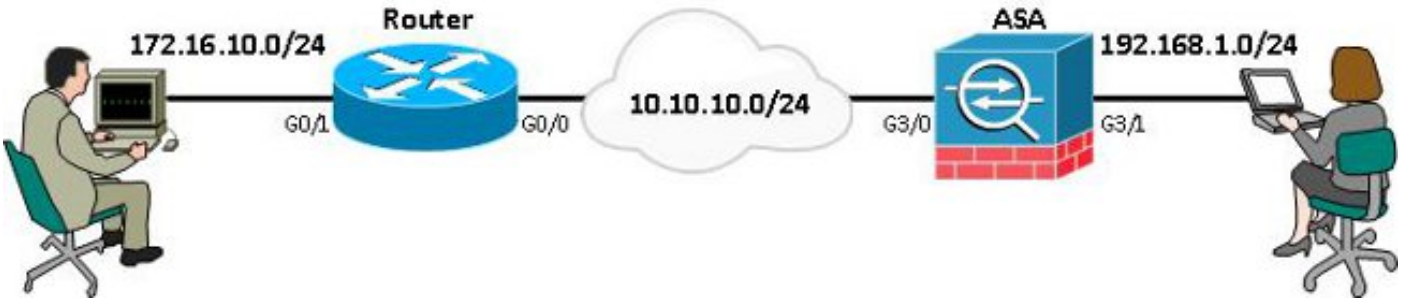
인증 기관

현재 IOS와 ASA는 Suite-B에 필요한 ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서가 있는 로컬 CA(Certificate Authority) 서버를 지원하지 않습니다. 따라서 서드파티 CA 서버를 구현해야 합니다. 예를 들어 OpenSSL을 사용하여 CA로 작동합니다.

구성

네트워크 토폴로지

이 가이드는 이 다이어그램에 표시된 토폴로지를 기반으로 합니다. IP 주소를 적절하게 수정해야 합니다.



참고: 설정에는 라우터와 ASA의 직접 연결이 포함됩니다. 여러 홉으로 분리될 수 있습니다. 이 경우 피어 IP 주소에 연결할 경로가 있는지 확인합니다. 다음 컨피그레이션에서는 사용된 암호화에 대해서만 자세히 설명합니다.

라우터가 ECDSA를 사용하도록 설정하는 단계

인증 기관

1. 타원 **곡선 키 쌍을 만듭니다.**
   ```
   openssl ecparam -out ca.key -name secp256r1 -genkey
   ```
2. **타원 곡선 자체 서명 인증서를** 만듭니다.
   ```
   openssl req -x509 -new -key ca.key -out ca.pem -outform PEM -days 3650
   ```

FlexVPN

1. EC(Elliptic **Curve**) 키 쌍을 생성하기 위한 필수 조건인 **domain-name** 및 **hostname**을 생성합니다.
   ```
   ip domain-name cisco.com
   hostname Router1
   crypto key generate ec keysize 256 label router1.cisco.com
   ```
2. CA에서 인증서를 얻기 위해 로컬 신뢰 지점을 생성합니다.
   ```
   crypto pki trustpoint ec_ca
    enrollment terminal
    subject-name cn=router1.cisco.com
    revocation-check none
    eckeypair router1.cisco.com
    hash sha256
   ```
   참고: CA가 오프라인이므로 해지 검사가 비활성화됩니다. 프로덕션 환경에서 최대 보안을 위해 해지 검사를 활성화해야 합니다.
3. 신뢰 지점을 **인증합니다**. 이렇게 하면 공개 키가 포함된 CA 인증서의 복사본을 가져옵니다.
   ```
   crypto pki authenticate ec_ca
   ```
4. 그런 다음 CA의 기본 64로 인코딩된 인증서를 입력하라는 메시지가 표시됩니다. OpenSSL로 생성된 ca.pem 파일입니다. 이 파일을 보려면 편집기 또는 ca.pem에서 OpenSSL 명령 openssl **x509 -in ca.pem을 사용하여 파일을 엽니다**. 붙여넣을 때 quit를 입력합니다. 그런 다음 **yes를** 입력하여 수락합니다.
5. CA의 PKI(Public Key Infrastructure)에 라우터를 등록합니다.
   ```
   crypto pki enrol ec_ca
   ```
6. CA에 인증서 요청을 제출하려면 수신하는 출력을 사용해야 합니다. 텍스트 파일(flex.csr)로 저장되고 OpenSSL 명령으로 서명될 수 있습니다.
   ```
   openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in flex.csr -out flex.pem
   ```
7. 이 명령을 입력한 후 CA에서 생성된 flex.pem 파일에 포함된 인증서를 라우터로 가져옵니다. 그런 다음 완료되면 quit를 입력합니다.
   ```
   crypto pki import ec_ca certificate
   ```

ASA

1. EC 키 쌍을 생성하기 위한 사전 요구 사항인 **domain-name** 및 **hostname**을 생성합니다.
   ```
   domain-name cisco.com
   hostname ASA1
   crypto key generate ecdsa label asa1.cisco.com elliptic-curve 256
   ```
2. CA에서 인증서를 얻기 위해 로컬 신뢰 지점을 생성합니다.
   ```
   crypto ca trustpoint ec_ca
    enrollment terminal
    subject-name cn=asa1.cisco.com
    revocation-check none
    keypair asa1.cisco.com
   ```
   참고: CA가 오프라인이므로 해지 검사가 비활성화됩니다. 프로덕션 환경에서 최대 보안을 위해 해지 검사를 활성화해야 합니다.
3. 신뢰 지점을 **인증합니다**. 이렇게 하면 공개 키가 포함된 CA 인증서의 복사본을 가져옵니다.
   ```
   crypto ca authenticate ec_ca
   ```
4. 그런 다음 CA의 기본 64로 인코딩된 인증서를 입력하라는 메시지가 표시됩니다. OpenSSL로 생성된 ca.pem 파일입니다. 이 파일을 보려면 편집기 또는 ca.pem에서 OpenSSL 명령 openssl **x509 -in ca.pem을 사용하여 파일을 엽니다**. 이 파일을 붙여넣을 때 quit을 입력한 다음 **yes**를 입력하여 수락합니다.
5. CA의 PKI에 ASA를 등록합니다.
   ```
   crypto ca enrol ec_ca
   ```
6. CA에 인증서 요청을 제출하려면 수신하는 출력을 사용해야 합니다. 텍스트 파일(asa.csr)로 저장한 다음 OpenSSL 명령으로 서명할 수 있습니다.
   ```
   openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in asa.csr -out asa.pem
   ```
7. 이 명령을 입력한 후 CA에서 생성된 a.pem 파일에 포함된 인증서를 라우터로 가져옵니다. 그런 다음 완료되면 quit를 입력합니다.
   ```
   crypto ca import ec_ca certificate
   ```

구성

FlexVPN

피어 디바이스의 인증서와 매칭할 인증서 맵을 만듭니다.

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

IKEv2 Proposal for Suite-B 컨피그레이션에 다음 명령을 입력합니다.

참고: 보안을 극대화하려면 sha512 hash 명령을 사용하여 aes**-cbc-256을** 구성합니다.

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

IKEv2 프로필을 인증서 맵에 일치시키고 이전에 정의된 **신뢰 지점**과 ECDSA를 사용합니다.

```
crypto ikev2 profile default
 match certificate certmap
 identity local dn
```

```
 authentication remote ecdsa-sig
 authentication local ecdsa-sig
 pki trustpoint ec_ca
 virtual-template 1
```

GCM(Galois Counter Mode)을 사용하도록 IPSec 변형 집합을 구성합니다.

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

이전에 구성한 매개변수를 사용하여 IPSec 프로파일을 구성합니다.

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

터널 인터페이스를 구성합니다.

```
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel source GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

다음은 인터페이스 컨피그레이션입니다.

```
interface GigabitEthernet0/0
 ip address 10.10.10.1 255.255.255.0
interface GigabitEthernet0/1
 ip address 172.16.10.1 255.255.255.0
```

ASA

이 인터페이스 컨피그레이션 사용:

```
interface GigabitEthernet3/0
 nameif outside
 security-level 0
 ip address 10.10.10.2 255.255.255.0
interface GigabitEthernet3/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
```

암호화할 트래픽을 정의하려면 다음 액세스 목록 명령을 입력합니다.

```
access-list 100 extended permit ip 192.168.1.0 255.255.255.0 172.16.10.0 255.255.255.0
```

NGE와 함께 이 IPSec proposal 명령을 입력합니다.

```
crypto ipsec ikev2 ipsec-proposal prop1
 protocol esp encryption aes-gcm
 protocol esp integrity null
```

암호화 맵 명령:

```
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 10.10.10.1
crypto map mymap 10 set ikev2 ipsec-proposal prop1
crypto map mymap 10 set trustpoint ec_ca
crypto map mymap interface outside
```

이 명령은 NGE로 IKEv2 정책을 구성합니다.

```
crypto ikev2 policy 10
 encryption aes
 integrity sha256
 group 19
 prf sha256
 lifetime seconds 86400
crypto ikev2 enable outside
```

피어 명령에 대해 구성된 터널 그룹:

```
tunnel-group 10.10.10.1 type ipsec-l2l
tunnel-group 10.10.10.1 ipsec-attributes
 peer-id-validate cert
 ikev2 remote-authentication certificate
 ikev2 local-authentication certificate ec_ca
```

연결 확인

ECDSA 키가 생성되었는지 확인합니다.

```
Router1#show crypto key mypubkey ec router1.cisco.com
% Key pair was generated at: 21:28:26 UTC Feb 19 2013
Key name: router1.cisco.com
Key type: EC KEYS
 Storage Device: private-config
 Usage: Signature Key
 Key is not exportable.
 Key Data&colon;
<...omitted...>

ASA-1(config)#show crypto key mypubkey ecdsa
Key pair was generated at: 21:11:24 UTC Feb 19 2013
Key name: asa1.cisco.com
 Usage: General Purpose Key
 EC Size (bits): 256
 Key Data&colon;
<...omitted...>
```

인증서를 성공적으로 가져왔으며 ECDSA가 사용되는지 확인합니다.

```
Router1#show crypto pki certificates verbose
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 0137
  Certificate Usage: General Purpose
  Issuer:
<...omitted...>
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
```

```
    EC Public Key:  (256 bit)
  Signature Algorithm: SHA256 with ECDSA


ASA-1(config)#show crypto ca certificates
CA Certificate
  Status: Available
  Certificate Serial Number: 00a293f1fe4bd49189
  Certificate Usage: General Purpose
  Public Key Type: ECDSA (256 bits)
  Signature Algorithm: SHA256 with ECDSA Encryption
 <...omitted...>
```

IKEv2 SA가 성공적으로 생성되었고 구성된 NGE 알고리즘을 사용하는지 확인합니다.

```
Router1#show crypto ikev2 sa  detailed
 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: SHA384, DH Grp:19, Auth sign: ECDSA,
        Auth verify: ECDSA
      Life/Active Time: 86400/94 sec


ASA-1#show crypto ikev2 sa detail

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                 Local                 Remote     Status         Role
268364957        10.10.10.2/500        10.10.10.1/500      READY    INITIATOR
      Encr: AES-CBC, keysize: 128, Hash: SHA384, DH Grp:19, Auth sign: ECDSA,
        Auth verify: ECDSA
      <...omitted...>
Child sa: local selector  192.168.1.0/0 - 192.168.1.255/65535
          remote selector 172.16.10.0/0 - 172.16.10.255/65535
          ESP spi in/out: 0xe847d8/0x12bce4d
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 128, esp_hmac: N/A
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

IPSec SA가 성공적으로 생성되었고 구성된 NGE 알고리즘을 사용하는지 확인합니다.

참고: FlexVPN은 IKEv2 및 IPSec 프로토콜을 모두 지원하는 비 IOS 클라이언트에서 IPSec 연결을 종료할 수 있습니다.

```
Router1#show crypto ipsec sa

interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 10.10.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 10.10.10.2 port 500
     PERMIT, flags={origin_is_acl,}
<...omitted...>

     inbound esp sas:
```

```
      spi: 0x12BCE4D(19648077)
        transform: esp-gcm ,
        in use settings ={Tunnel, }

ASA-1#show crypto ipsec sa detail
interface: outside
    Crypto map tag: mymap, seq num: 10, local addr: 10.10.10.2

      access-list 100 extended permit ip 192.168.1.0 255.255.255.0 172.16.10.0
        255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
      current_peer: 10.10.10.1
<...omitted...>


    inbound esp sas:
      spi: 0x00E847D8 (15222744)
         transform: esp-aes-gcm esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
```

Cisco의 Suite-B 구현에 대한 자세한 내용은 Next Generation Encryption 백서를 참조하십시오.

Cisco의 Next Generation Encryption 구현에 대한 자세한 내용은 차세대 암호화 솔루션 페이지를 참조하십시오.

관련 정보

- Next Generation Encryption 백서
- 차세대 암호화 솔루션 페이지
- SSH(Secure Shell)
- IPSec 협상/IKE 프로토콜
- PSK가 포함된 Site-to-Site VPN용 ASA IKEv2 디버그 TechNote
- ASA IPSec 및 IKE 디버깅(IKEv1 기본 모드) 문제 해결 TechNote
- IOS IPSec 및 IKE 디버깅 - IKEv1 기본 모드 문제 해결 TechNote
- ASA IPSec 및 IKE 디버깅 - IKEv1 Aggressive Mode TechNote
- 기술 지원 및 문서 – Cisco Systems