FlexVPN tussen een router en een ASA met Configuratievoorbeeld van de volgende generatie

Inhoud

Inleiding

Dit document beschrijft hoe u VPN kunt configureren tussen een router met FlexVPN en een adaptieve security applicatie (ASA) die ondersteuning biedt voor de Cisco Next Generation Encryption (NGE) algoritmen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FlexVPN
- Internet Key Exchange versie 2 (IKEv2)
- IPsec
- ASA

- Cryptografie van de volgende generatie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- **Hardware:** IOS Generation 2 (G2) router die de security licentie runt.
- **in Cisco IOS®-software:** Cisco IOS®-softwarerelease versie 15.2-3.T2. Elke release van M of T voor releases later dan Cisco IOS®-softwarerelease versie 15.1.2T kan worden gebruikt omdat dit is meegeleverd met de introductie van de GCM-contramodus (GCM).
- **Hardware:** ASA die NGE ondersteunt.**Opmerking:** Alleen multi-core platforms ondersteunen Advanced Encryption Standard (AES) GCM.
- **in Cisco IOS®-software:** ASA-softwarerelease 9.0 of hoger die NGE ondersteunt.
- OpenSSL.

Raadpleeg voor meer informatie de Cisco Functie Navigator.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Dynamisch IPSec security associaties maken

De aanbevolen IPSec-interface op IOS is een Virtual Tunnel Interface (VTI), die een generieke Routing Encapsulation (GRE)-interface maakt die door IPsec wordt beschermd. Voor een VTI bestaat de Traffic Selector (welk verkeer door de IPSec security associaties (SA) moet worden beschermd) uit GRE-verkeer van de tunnelbron naar de tunnelbestemming. Omdat de ASA geen GRE-interfaces implementeert, maar in plaats daarvan IPSec SA's creëert die gebaseerd zijn op verkeer dat gedefinieerd is in een toegangscontrolelijst (ACL), moeten we een methode inschakelen die de router toestaat om op de IKEv2-initiatie te reageren met een spiegel van de voorgestelde verkeersselectors. Het gebruik van Dynamic Virtual Tunnel Interface (DVTI) op de FlexVPN-router stelt dit apparaat in staat om te reageren op de gepresenteerde Traffic Selector met een spiegel van de Traffic Selector die is gepresenteerd.

Dit voorbeeld versleutelt verkeer tussen beide interne netwerken. Wanneer de ASA de traffic selectors van het ASA interne netwerk aan het IOS interne netwerk presenteert, `192.168.1.0/24` tot `172.16.10.0/24`, reageert de DVTI interface met een spiegel van de verkeerselectie, die `172.16.10.0/24` tot `192.168.1.0/24` is.

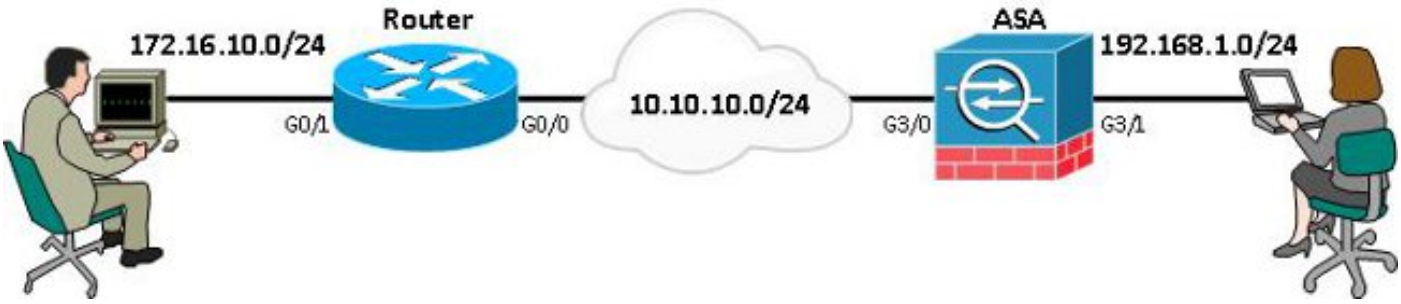
certificaatinstantie

Op dit moment ondersteunen IOS en ASA geen lokale CA-server (certificaatinstantie) met Elliptic Curve Digital Signature Algorithm (ECDSA), dat nodig is voor Suite-B. Dus moet een CA Server van derden worden geïmplementeerd. Gebruik bijvoorbeeld OpenSSL om als CA te fungeren.

Configuratie

Netwerktopologie

Deze gids is gebaseerd op de topologie die in dit diagram wordt getoond. U dient IP-adressen aan te passen.



Opmerking: de instellingen omvatten een rechtstreekse verbinding van de router en ASA. Deze kunnen van elkaar worden gescheiden door vele sprongen. Als dit zo waarborgt dat er een route is om naar het IP-adres van de peer te gaan. De volgende configuratie specificeert alleen de gebruikte encryptie.

Stappen vereist om de router in staat te stellen om ECDSA te gebruiken

certificaatinstantie

1. Maak een **elliptische bocht sleutelpaar.**
   ```
   openssl ecparam -out ca.key -name secp256r1 -genkey
   ```
2. Maak een **elliptische bocht zelf-ondertekend certificaat**.
   ```
   openssl req -x509 -new -key ca.key -out ca.pem -outform PEM -days 3650
   ```

FlexVPN

1. Creëer **domeinnaam** en **hostname**, die voorwaarden zijn om een elliptische curve (EC)-sleutelpaar te maken.
   ```
   ip domain-name cisco.com
   hostname Router1
   crypto key generate ec keysize 256 label router1.cisco.com
   ```
2. Maak een lokaal **trustpunt** om een certificaat van CA te verkrijgen.
   ```
   crypto pki trustpoint ec_ca
    enrollment terminal
    subject-name cn=router1.cisco.com
    revocation-check none
    eckeypair router1.cisco.com
    hash sha256
   ```
   Opmerking: omdat de CA offline is, is herroeping van de controle uitgeschakeld. herroepingscontrole moet mogelijk worden gemaakt om in een productieomgeving een maximale veiligheid te waarborgen .
3. Verifieer het **vertrouwenspunt**. Dit verkrijgt een kopie van het certificaat van de CA, dat de openbare sleutel bevat.
   ```
   crypto pki authenticate ec_ca
   ```

4. U wordt dan gevraagd het standaard 64 gecodeerde certificaat van de CA in te voeren. Dit is het bestand ca.pem, dat met OpenSSL is gemaakt. Om dit bestand te kunnen weergeven, opent u het bestand in een editor of met de OpenSSL-opdracht **openssl x509 - in ca.pem**. Typ **stop** als je dit plakt. Typ het **ja** om het te aanvaarden.
5. Geef de router op aan de Public Key Infrastructure (PKI) op de CA.
```
crypto pki enrol ec_ca
```
6. De uitvoer die u ontvangt, moet worden gebruikt om een certificaataanvraag bij de CA in te dienen. Dit kan als een tekstbestand (flex.csr) worden opgeslagen en met de OpenSSL-opdracht worden ondertekend.
```
openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in flex.csr -out flex.pem
```
7. Importeer het certificaat, dat deel uitmaakt van flex.pem, dat uit de CA is gegenereerd, in de router nadat u deze opdracht hebt ingevoerd. Ga dan **ontslag** na voltooiing.
```
crypto pki import ec_ca certificate
```

ASA

1. Creëer **domeinnaam** en **hostname**, die voorwaarden zijn om een EC-sleutelpaar te creëren.
```
domain-name cisco.com
hostname ASA1
crypto key generate ecdsa label asa1.cisco.com elliptic-curve 256
```
2. Maak een lokaal **trustpunt** om een certificaat te verkrijgen van CA.
```
crypto ca trustpoint ec_ca
 enrollment terminal
 subject-name cn=asa1.cisco.com
 revocation-check none
 keypair asa1.cisco.com
```
Opmerking: omdat de CA offline is, is herroeping van de controle uitgeschakeld. herroepingscontrole moet mogelijk worden gemaakt om in een productieomgeving een maximale veiligheid te waarborgen .
3. Verifieer het **vertrouwenspunt**. Dit verkrijgt een kopie van het certificaat van de CA, dat de openbare sleutel bevat.
```
crypto ca authenticate ec_ca
```
4. U wordt dan gevraagd het standaard 64 gecodeerde certificaat van de CA in te voeren. Dit is het bestand ca.pem, dat met OpenSSL is gemaakt. Om dit bestand te kunnen weergeven, opent u het bestand in een editor of met de OpenSSL-opdracht **openssl x509 - in ca.pem**. Typ **stop** wanneer u dit bestand plakt en type **ja** om het te accepteren.
5. Inrol de ASA in de PKI op de CA.
```
crypto ca enrol ec_ca
```
6. De uitvoer die u ontvangt, moet worden gebruikt om een certificaataanvraag bij de CA in te dienen. Dit kan als een tekstbestand (asa.csr) worden opgeslagen en met de OpenSSL-opdracht worden ondertekend.
```
openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in asa.csr -out asa.pem
```
7. Importeer het certificaat, dat in het bestand als a.pem aanwezig is en dat van de CA is gegenereerd in de router nadat deze opdracht is ingevoerd. Ga dan na voltooiing ontslag in.
```
crypto ca import ec_ca certificate
```

Configuratie

FlexVPN

Maak een certificaatkaart die overeenkomt met het certificaat van het peer-apparaat.

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

Voer deze opdrachten in voor IKEv2 Proposal for Suite-B configuratie:

Opmerking: Voor maximale veiligheid, configureer dan met de **AES-cbc-256 met de** opdracht **sha512 hash**.

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

Stem het IKEv2-profiel af op de certificaatkaart en gebruik ECDSA met het eerder gedefinieerde **trustpunt**.

```
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
```

Configureer de IPSec-transformator die is ingesteld om de GCM-contrastmodus (GCM) te gebruiken.

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

Configureer het IPSec-profiel met de eerder ingestelde parameters.

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

Configuratie van de tunnelinterface:

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

Hier is de interfaceconfiguratie:

```
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

Gebruik deze interfaceconfiguratie:

```
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
```

Typ deze opdracht in de toegangslijst om het te versleutelen verkeer te definiëren:

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

Voer deze opdracht van IPSec-voorstel in bij NGE:

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

Opdrachten voor cryptografie-plattegronden:

```
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
```

Deze opdracht vormt het IKEv2-beleid met NGE:

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

Tunnelgroep ingesteld voor peer opdrachten:

```
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
```

Connection-verificatie

Controleer dat de ECDSA-toetsen met succes zijn gegenereerd.

```
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...>
```

Controleer dat het certificaat is ingevoerd en dat ECDSA wordt gebruikt.

```
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...>
```

Controleer dat de IKEv2 SA met succes is gemaakt en gebruikt de geconfigureerde NGE-algoritmen.

```
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
```

Controleer dat de IPSec SA met succes wordt gemaakt en gebruikt de geconfigureerde NGE-algoritmen.

Opmerking: FlexVPN kan IPSec-verbindingen afsluiten van niet-IOS klanten die zowel de IKEv2- als IPSec-protocollen ondersteunen.

```
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, }
```

Raadpleeg het Witboek over encryptie van de volgende generatie voor meer informatie over de implementatie van Cisco van Suite-B.

Raadpleeg de pagina Encryption Solution van de volgende generatie om meer te weten te komen over de implementatie van Cisco van Next-Generation Encryption.

Gerelateerde informatie

- Whitepaper over encryptie van de volgende generatie
- Pagina voor encryptie van de volgende generatie
- Secure Shell (SSH)
- IPsec-onderhandeling/IKE-protocollen
- ASA IKEv2-debugs voor Site-to-Site VPN met PSKs TechNotes

- ASA IPSec and IKE-debugs (IKEv1 hoofdmodus) voor probleemoplossing Technische opmerking
- IOS IPSec- en IKE-implementaties - IKEv1 hoofdmodus voor probleemoplossing
- ASA IPSec and IKE-implementaties - IKEv1 aggregation mode TechNotes
- Technische ondersteuning en documentatie – Cisco Systems