FlexVPN-configuratievoorbeeld met encryptie van de volgende generatie

Inhoud

Inleiding

Dit document beschrijft hoe u een FlexVPN kunt configureren tussen twee routers die de Cisco Next-Generation Encryption (NGE) reeks algoritmen ondersteunen.

Encryptie van de volgende generatie

Cisco NGE-cryptografie garandeert informatie die over netwerken reist die vier configureerbare, gevestigde en openbare cryptografische algoritmen gebruiken:

- Encryptie op basis van de Advanced Encryption Standard (AES), die 128-bits of 256-bits toetsen gebruikt
- Digitale handtekeningen met het Elliptic Curve Digital Signature Algorithm (ECDSA), die curves met 256-bits en 384-bits Prime moduli gebruiken
- Key exchange die de Elliptic Curve Diffie-Hellman (ECDH) methode gebruikt
- Hashing (digitale vingerafdrukken) op basis van het Secure Hash Algorithm 2 (SHA-2)

Het National Security Agency (NSA) verklaart dat deze vier algoritmes in combinatie adequate informatie-verzekering bieden voor gerubriceerde informatie. NSA Suite B-cryptografie voor IPsec is gepubliceerd als een standaard in RFC 6379 en heeft acceptatie binnen de sector verworven.

Suite Suite-B-GCM-128

Volgens RFC 6379 zijn deze algoritmen vereist voor reeks Suite-B-GCM-128.

Deze suite biedt bescherming en vertrouwelijkheid bij ingesloten security payload (ESP) met 128-bits AES-GCM (zie RFC4106). Deze suite moet worden gebruikt wanneer ESP bescherming en encryptie nodig zijn.

ESP
Encryptie AES met 128-bits en 16-poorts 16-octet Integrity Control Value (ICV) in Galois/Counter Mode (GCM) (RFC4106)
Integratie NULL

IKEv2
Encryptie AES met 128-bits toetsen in Cipher Block Chaining (CBC) modus (RFC3602)
Pseudo-willekeurige functie HMAC-SHA-256 (RFC4868)
Integriteit HMAC-SHA-256-128 (RFC4868)
Diffie-Hellman groep 256-bits willekeurige ECP-groep (RFC5903)

Meer informatie over Suite B en NGE is te vinden op Next-generation encryptie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

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

- Hardware: Geïntegreerde services routers (ISR) generatie 2 (G2) die de beveiligingslicentie uitvoeren.
- Software: Cisco IOS-softwarerelease 15.2.3T2. Elke release van Cisco IOS-softwarerelease M of 15.1.2T of hoger kan worden gebruikt omdat dit is wanneer GCM is geïntroduceerd.

Zie voor meer informatie de 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.

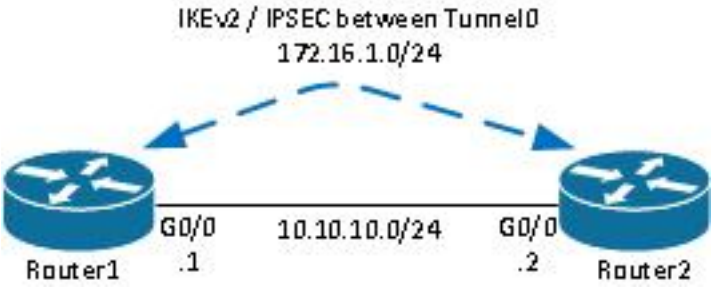
certificaatinstantie

Momenteel ondersteunt Cisco IOS-software geen lokale CA-server (certificaatautoriteit) die ECDH draait, wat vereist is voor Suite B. Een CA-server van derden moet worden geïmplementeerd. Dit voorbeeld gebruikt een Microsoft CA gebaseerd op Suite B PKI

Configureren

Netwerktopologie

Deze handleiding is gebaseerd op deze geïllustreerde topologie. IP-adressen moeten aan uw vereisten worden aangepast.



Opmerkingen:

De installatie bestaat uit twee direct aangesloten routers, die door veel hops van elkaar zouden kunnen worden gescheiden. Als dit zo is, zorg er dan voor dat er een route is om naar het IP-adres van de peer te gaan. Deze configuratie details alleen de gebruikte encryptie. IKEv2-routing of een routingprotocol moet via IPSec VPN worden geïmplementeerd.

Stappen vereist om de router in staat te stellen om het Elliptic Curve Digital Signature Algorithm te gebruiken

1. Creëer de domeinnaam en hostname, die voorwaarden zijn om een EC-sleutelpaar te creëren.

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

   Opmerking: Tenzij u een versie met de oplossing voor Cisco bug-ID CSCue5994 gebruikt, is het met de router niet mogelijk om een certificaat in te schrijven met een maximale grootte van 768.
2. Maak een lokaal trustpunt om een certificaat van CA te verkrijgen.

```
crypto pki trustpoint ecdh
 enrollment terminal
```

```
 revocation-check none
 eckeypair Router1.cisco.com
```

Opmerking: Aangezien de VK offline was, werden herroepingscontroles uitgeschakeld. Rerozingscontroles zouden worden ingeschakeld voor maximale veiligheid in een productieomgeving.

3. Verifieer het trustpunt (dit verkrijgt een kopie van het certificaat van CA dat de openbare sleutel bevat).

```
crypto pki authenticate ecdh
```

4. Voer het basiscertificaat 64 van de CA in bij de prompt. Typ **stop** en **bevestig** het voor **instemming**.

5. Installeer de router in de PKI op de CA.

```
crypto pki enrol ecdh
```

6. De weergegeven uitvoer wordt gebruikt om een certificaataanvraag bij de CA in te dienen. Voor de Microsoft CA, sluit u de verbinding aan op de web interface van de CA en selecteer **Een certificaataanvraag indienen**.

7. Importeer het certificaat dat van de CA is ontvangen in de router. Typ de **stop** zodra het certificaat is geïmporteerd.

```
crypto pki import ecdh certificate
```

Configuratie

De configuratie hier beschikbaar is voor Router1. Router2 vereist een spiegel van de configuratie waar alleen de IP adressen op de tunnelinterface uniek zijn.

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

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

2. Configureer het IKEv2 voorstel voor Suite B.

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

Opmerking: IKEv2 Smart Default implementeert een aantal vooraf geconfigureerd algoritmen

in het standaard IKEv2-voorstel. Aangezien es-cbc-128 en sha256 nodig zijn voor de reeks Suite-B-GCM-128, moet u aes-cbc-256, sha384 en sha512 binnen deze algoritmen verwijderen. De reden hiervoor is dat IKEv2 het sterkste algoritme kiest wanneer het een keuze heeft. Gebruik voor maximale veiligheid aes-cbc-256 en sha512. Dit is echter niet nodig voor Suite-B-GCM-128. Om het geconfigureerde IKEv2-voorstel te kunnen bekijken, dient u de opdracht **showcrypto ikev2-voorstel** in te voeren.

3. Configureer het IKEv2-profiel zodat het overeenkomt met 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 ecdh
```

4. Configuratie van de transformatie van IPSec om GCM te gebruiken.

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

5. Configureer het IPSec-profiel met de parameters die eerder zijn ingesteld.

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

6. Configuratie van de tunnelinterface.

```
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
```

Controleer de verbinding

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

1. Controleer dat de ECDSA-toetsen met succes zijn gegenereerd.

```
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. Controleer dat het certificaat is ingevoerd en dat het ECDH wordt gebruikt.

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

3. Controleer dat de IKEv2 SA met succes is gemaakt en gebruik de Suite B algoritmen.

```
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. Controleer dat de IKEv2 SA met succes is gemaakt en gebruik de Suite B algoritmen.

```
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)
```

Opmerking: In deze output, anders dan in Internet Key Exchange versie 1 (IKEv1), toont de perfecte forward geheim (PFS) Diffie-Hellman (DH) - groepswaarde als **PFS (Y/N): N, DH-groep: geen** tijdens de eerste tunnelonderhandeling , maar na een nieuwe start tonen de juiste waarden . Dit is geen bug, ook al wordt het gedrag in Cisco bug-ID CSCug67056 beschreven. Het verschil tussen IKEv1 en IKEv2 is dat in het laatste geval de Child Security Associations (SA's) zijn gemaakt als onderdeel van de AUTH-uitwisseling zelf. De DH Group die onder de crypto map is ingesteld, wordt alleen tijdens het programma gebruikt. Daarom

zie je **PFS (Y/N): N, DH-groep: niet** tot de eerste rekey . Maar met IKEv1 zie je een ander gedrag omdat de creatie van het Kind SA tijdens de Snelle Modus gebeurt en het CREATE_CHILD_SA bericht heeft een voorziening voor het dragen van de Key Exchange lading die de DH parameters specificeert om een nieuw gedeeld geheim af te leiden.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Conclusie

De efficiënte en sterke cryptografische algoritmen die in NGE zijn gedefinieerd, bieden een garantie op de lange termijn dat gegevens vertrouwelijk en integer worden verstrekt en onderhouden tegen lage verwerkingskosten. NGE kan eenvoudig worden geïmplementeerd met FlexVPN, dat Suite B standaard cryptografie biedt.

Nadere informatie over de implementatie van Cisco van Suite B is te vinden op Encryptie van de volgende generatie.