Konfigurationsbeispiel für FlexVPN zwischen einem Router und einer ASA mit Verschlüsselung der nächsten Generation

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie ein VPN zwischen einem Router mit FlexVPN und einer Adaptive Security Appliance (ASA) konfigurieren, die die Cisco NGE-Algorithmen (Next Generation Encryption) unterstützt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- FlexVPN
- Internet Key Exchange Version 2 (IKEv2)
- IPSec
- ASA

- Verschlüsselung der nächsten Generation

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- **Hardware:** IOS Generation 2 (G2) Router, auf dem die Sicherheitslizenz ausgeführt wird.
- **Software:** Cisco IOS® Softwareversion 15.2-3.T2. Jede Version von M oder T für Versionen, die älter als die Version 15.1.2T der Cisco IOS® Software sind, kann verwendet werden, da diese Version mit der Einführung des Galois Counter Mode (GCM) integriert ist.
- **Hardware:** ASA mit NGE-Unterstützung**Hinweis:** Nur Multicore-Plattformen unterstützen Advanced Encryption Standard (AES) GCM.
- **Software:** ASA Software Version 9.0 oder höher, die NGE unterstützt.
- OpenSSL

Weitere Informationen finden Sie im Cisco Feature Navigator.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Dynamisches Erstellen von IPSec-Sicherheitszuordnungen

Die empfohlene IPSec-Schnittstelle in IOS ist eine Virtual Tunnel Interface (VTI), die eine generische GRE-Schnittstelle (Routing Encapsulation) erstellt, die durch IPsec geschützt ist. Für ein VTI besteht der Datenverkehrsauswahl (welcher Datenverkehr durch die IPSec-Sicherheitszuordnungen (SA) geschützt werden soll) aus GRE-Datenverkehr von der Tunnelquelle zum Tunnelziel. Da die ASA keine GRE-Schnittstellen implementiert, sondern stattdessen IPSec-SAs erstellt, die auf dem in einer Zugriffskontrollliste (ACL) definierten Datenverkehr basieren, muss eine Methode aktiviert werden, die es dem Router ermöglicht, auf die IKEv2-Initiierung mit einer Spiegelung der vorgeschlagenen Datenverkehrsauswahl zu reagieren. Durch die Verwendung von DVTI (Dynamic Virtual Tunnel Interface) auf dem FlexVPN-Router kann dieses Gerät auf den angezeigten Datenverkehrsauswahlanzeiger mit einem Spiegel des angezeigten Datenverkehrsauswahl reagieren.

In diesem Beispiel wird der Datenverkehr zwischen beiden internen Netzwerken verschlüsselt. Wenn die ASA dem internen IOS-Netzwerk die Datenverkehrsselektoren des ASA-Netzwerks `192.168.1.0/24` bis `172.16.10.0/24` vorstellt, reagiert die DVTI-Schnittstelle mit einem Spiegel der Datenverkehrsselektoren, der `172.16.10.0/24` bis `192.168.1.0/24` ist.

Zertifizierungsstelle

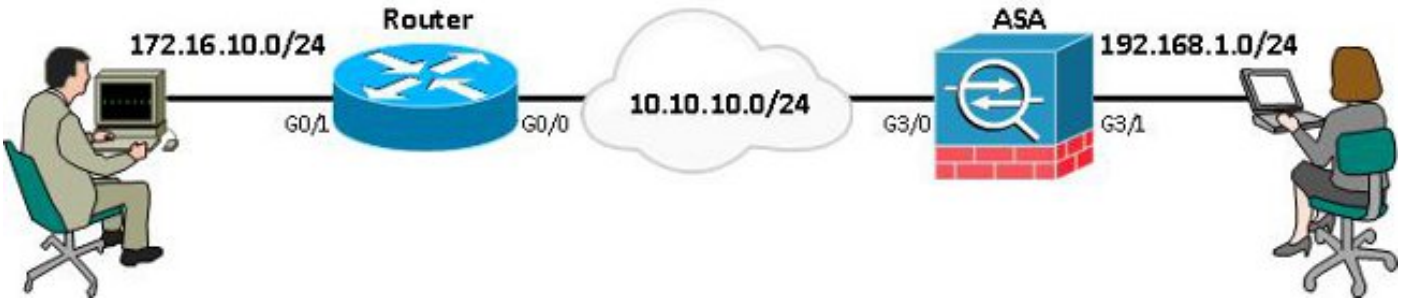
Derzeit unterstützen IOS und ASA keinen lokalen CA-Server (Certificate Authority) mit ECDSA-

Zertifikaten (Elliptic Curve Digital Signature Algorithm), was für Suite-B erforderlich ist. Daher muss ein CA-Server eines Drittanbieters implementiert werden. Verwenden Sie beispielsweise OpenSSL, um als CA zu fungieren.

Konfiguration

Netzwerktopologie

Dieser Leitfaden basiert auf der in diesem Diagramm gezeigten Topologie. Sie sollten die IP-Adressen entsprechend ändern.



Hinweis: Das Setup umfasst eine direkte Verbindung zwischen Router und ASA. Diese können durch viele Hopfen getrennt werden. Wenn ja, stellen Sie sicher, dass eine Route zur Peer-IP-Adresse vorhanden ist. In der folgenden Konfiguration wird nur die verwendete Verschlüsselung angegeben.

Erforderliche Schritte zur Aktivierung der ECDSA-Funktion für den Router

Zertifizierungsstelle

1. Erstellen Sie eine **elliptische Kurve keypair.**
   ```
   openssl ecparam -out ca.key -name secp256r1 -genkey
   ```
2. Erstellen Sie ein **selbstsigniertes Zertifikat** für **die elliptische Kurve**.
   ```
   openssl req -x509 -new -key ca.key -out ca.pem -outform PEM -days 3650
   ```

FlexVPN

1. Erstellen Sie **Domänennamen** und **Hostnamen**, die Voraussetzung für die Erstellung einer elliptischen Kurve (EC)-Tastenkombination sind.
   ```
   ip domain-name cisco.com
   hostname Router1
   crypto key generate ec keysize 256 label router1.cisco.com
   ```
2. Erstellen Sie einen lokalen **Vertrauenspunkt**, um ein Zertifikat von der CA zu erhalten.
   ```
   crypto pki trustpoint ec_ca
    enrollment terminal
    subject-name cn=router1.cisco.com
    revocation-check none
    eckeypair router1.cisco.com
    hash sha256
   ```
   Hinweis: Da die CA offline ist, ist die Widerrufsüberprüfung deaktiviert. Die Widerrufsüberprüfung sollte aktiviert werden, um in einer Produktionsumgebung maximale

Sicherheit zu gewährleisten.

3. Authentifizierung des **Vertrauenspunkts**. Hiermit wird eine Kopie des Zertifikats der Zertifizierungsstelle erworben, das den öffentlichen Schlüssel enthält.
   ```
   crypto pki authenticate ec_ca
   ```
4. Sie werden dann aufgefordert, das Base-64-verschlüsselte Zertifikat der CA einzugeben. Dies ist die Datei ca.pem, die mit OpenSSL erstellt wurde. Um diese Datei anzuzeigen, öffnen Sie sie in einem Editor oder mit dem OpenSSL-Befehl **openssl x509 -in ca.pem**. Geben Sie **quit ein**, wenn Sie dieses einfügen. Geben Sie dann **yes** zum Akzeptieren ein.
5. Registrieren Sie den Router für die Public Key Infrastructure (PKI) der CA.
   ```
   crypto pki enrol ec_ca
   ```
6. Die Ausgabe, die Sie erhalten, muss verwendet werden, um eine Zertifikatsanforderung an die Zertifizierungsstelle zu senden. Diese kann als Textdatei (flex.csr) gespeichert und mit dem OpenSSL-Befehl signiert werden.
   ```
   openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in flex.csr -out flex.pem
   ```
7. Importieren Sie das Zertifikat, das in der Datei flex.pem enthalten ist und von der CA generiert wird, nach Eingabe dieses Befehls in den Router. Geben Sie anschließend **quit (Beenden)** ein.
   ```
   crypto pki import ec_ca certificate
   ```

ASA

1. Erstellen Sie **Domänenname** und **Hostname**, die Voraussetzung für die Erstellung eines EC-Tastenfeldes sind.
   ```
   domain-name cisco.com
   hostname ASA1
   crypto key generate ecdsa label asa1.cisco.com elliptic-curve 256
   ```
2. Erstellen Sie einen lokalen **Vertrauenspunkt**, um ein Zertifikat von der Zertifizierungsstelle zu erhalten.
   ```
   crypto ca trustpoint ec_ca
    enrollment terminal
    subject-name cn=asa1.cisco.com
    revocation-check none
    keypair asa1.cisco.com
   ```
   Hinweis: Da die CA offline ist, ist die Widerrufsüberprüfung deaktiviert. Die Widerrufsüberprüfung sollte aktiviert werden, um in einer Produktionsumgebung maximale Sicherheit zu gewährleisten.
3. Authentifizierung des **Vertrauenspunkts**. Hiermit wird eine Kopie des Zertifikats der Zertifizierungsstelle erworben, das den öffentlichen Schlüssel enthält.
   ```
   crypto ca authenticate ec_ca
   ```
4. Sie werden dann aufgefordert, das Base-64-verschlüsselte Zertifikat der CA einzugeben. Dies ist die Datei ca.pem, die mit OpenSSL erstellt wurde. Um diese Datei anzuzeigen, öffnen Sie sie in einem Editor oder mit dem OpenSSL-Befehl **openssl x509 -in ca.pem**. Geben Sie **quit** ein, wenn Sie diese Datei einfügen, und geben Sie dann **yes** to accept ein.
5. Registrieren Sie die ASA bei der PKI der CA.
   ```
   crypto ca enrol ec_ca
   ```
6. Die Ausgabe, die Sie erhalten, muss verwendet werden, um eine Zertifikatsanforderung an die Zertifizierungsstelle zu senden. Dies kann als Textdatei (asa.csr) gespeichert und dann mit dem OpenSSL-Befehl signiert werden.
   ```
   openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in asa.csr -out asa.pem
   ```
7. Importieren Sie das Zertifikat, das in der Datei als a.pem enthalten ist, das von der CA generiert wurde, in den Router, nachdem dieser Befehl eingegeben wurde. **Geben** Sie dann

quit (Beenden) ein.

```
crypto ca import ec_ca certificate
```

Konfiguration

FlexVPN

Erstellen Sie eine Zertifikatszuordnung, die mit dem Zertifikat des Peer-Geräts übereinstimmt.

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

Geben Sie die folgenden Befehle für die Konfiguration des IKEv2-Angebots für Suite-B ein:

Hinweis: Konfigurieren Sie für maximale Sicherheit mit dem **Hash-**Befehl **aes-cbc-256 mit sha512**.

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

Ordnen Sie das IKEv2-Profil der Zertifikatszuordnung zu, und verwenden Sie ECDSA mit dem zuvor definierten **Vertrauenspunkt**.

```
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
```

Konfigurieren Sie den IPSec-Transformationssatz für die Verwendung des Galois Counter Mode (GCM).

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

Konfigurieren Sie das IPSec-Profil mit den zuvor konfigurierten Parametern.

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

Konfigurieren Sie die Tunnelschnittstelle:

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

Die Schnittstellenkonfiguration sieht folgendermaßen aus:

```
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

Verwenden Sie diese Schnittstellenkonfiguration:

```
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
```

Geben Sie diesen Befehl für die Zugriffsliste ein, um den zu verschlüsselnden Datenverkehr zu definieren:

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

Geben Sie diesen IPSec-Angebotsbefehl mit NGE ein:

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

Befehle der Kryptografiezuordnung:

```
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
```

Mit diesem Befehl wird die IKEv2-Richtlinie mit NGE konfiguriert:

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

Für Peer-Befehle konfigurierte Tunnelgruppe:

```
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
```

Verbindungsprüfung

Überprüfen Sie, ob die ECDSA-Schlüssel erfolgreich generiert wurden.

```
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...>
```

Überprüfen Sie, ob das Zertifikat erfolgreich importiert wurde und ECDSA verwendet wird.

```
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...>
```

Überprüfen Sie, ob die IKEv2 SA erfolgreich erstellt wurde und die konfigurierten NGE-Algorithmen verwendet.

```
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
```

Überprüfen Sie, ob die IPSec SA erfolgreich erstellt wurde und die konfigurierten NGE-Algorithmen verwendet.

Hinweis: FlexVPN kann IPSec-Verbindungen von Nicht-IOS-Clients terminieren, die sowohl das IKEv2- als auch das IPSec-Protokoll unterstützen.

```
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, }
```

Weitere Informationen zur Implementierung der Suite-B durch Cisco finden Sie im Whitepaper Next Generation Encryption.

Auf der Seite Verschlüsselungslösung der nächsten Generation erfahren Sie mehr über die Implementierung von Verschlüsselungstechnologie der nächsten Generation durch Cisco.

Zugehörige Informationen

- Whitepaper zum Thema Verschlüsselung der nächsten Generation
- Seite "Encryption Solution" der nächsten Generation
- Secure Shell (SSH)
- IPSec-Aushandlung/IKE-Protokolle
- ASA IKEv2-Debugger für Site-to-Site-VPN mit PSKs - Technische Anmerkung
- ASA IPSec- und IKE-Debugging (IKEv1-Hauptmodus) Problembehandlung TechHinweis
- IOS IPSec- und IKE-Debug - IKEv1 Main Mode Troubleshooting TechNote
- ASA IPSec- und IKE-Debug - IKEv1 Aggressive Mode TechNote
- Technischer Support und Dokumentation - Cisco Systems