Konfigurationsbeispiel für FlexVPN mit Verschlüsselung der nächsten Generation

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie ein FlexVPN zwischen zwei Routern konfigurieren, die den Algorithmussatz von Cisco Next-Generation Encryption (NGE) unterstützen.

Verschlüsselungstechnologie der nächsten Generation

Die Cisco NGE-Verschlüsselung sichert Informationen, die über Netzwerke übertragen werden und vier konfigurierbare, etablierte und allgemein zugängliche Kryptografiealgorithmen verwenden:

- Verschlüsselung basierend auf dem Advanced Encryption Standard (AES), der 128-Bit- oder 256-Bit-Schlüssel verwendet
- Digitale Signaturen mit dem Elliptic Curve Digital Signature Algorithm (ECDSA), der Kurven mit 256-Bit- und 384-Bit-Primärkanälen verwendet
- Schlüsselaustausch, der die Elliptic Curve Diffie-Hellman-Methode (ECDH) verwendet
- Hashing (digitale Fingerabdrücke) basierend auf dem Secure Hash Algorithm 2 (SHA-2)

Die National Security Agency (NSA) erklärt, dass diese vier Algorithmen zusammen eine angemessene Informationssicherung für Verschlusssachen bieten. Die Verschlüsselung der NSA Suite B für IPsec wurde standardmäßig in RFC 6379 veröffentlicht und hat sich in der Branche

etabliert.

Suite-B-GCM-128

Gemäß RFC 6379 sind diese Algorithmen für Suite-B-GCM-128 erforderlich.

Diese Suite bietet mit 128-Bit AES-GCM den Schutz und die Vertraulichkeit der ESP-Integrität (Encapsulating Security Payload) (siehe RFC4106). Diese Suite sollte verwendet werden, wenn sowohl ESP-Integritätsschutz als auch Verschlüsselung erforderlich sind.

ESP
Verschlüsselungs-AES mit 128-Bit-Schlüsseln und 16-Oktett Integrity Check Value (ICV) im Galois/Counter Mode (GCM) (RFC4106)
Integrität NULL

IKEv2
Verschlüsselungs-AES mit 128-Bit-Schlüsseln im CBC-Modus (Cipher Block Chaining) (RFC3602)
Pseudozufallsfunktion HMAC-SHA-256 (RFC4868)
Integrität HMAC-SHA-256-128 (RFC4868)
Diffie-Hellman-Gruppe, 256-Bit, zufällige ECP-Gruppe (RFC5903)

Weitere Informationen zu Suite B und NGE finden Sie unter Verschlüsselung der nächsten Generation.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

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

Verwendete Komponenten

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

- Hardware: Integrated Services Router (ISR) Generation 2 (G2), auf denen die Sicherheitslizenz ausgeführt wird.
- Software: Cisco IOS® Softwareversion 15.2.3T2 Jede Version der Cisco IOS Software, Version M oder 15.1.2T oder höher, kann verwendet werden, da GCM eingeführt wurde.

Weitere Informationen finden Sie im 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.

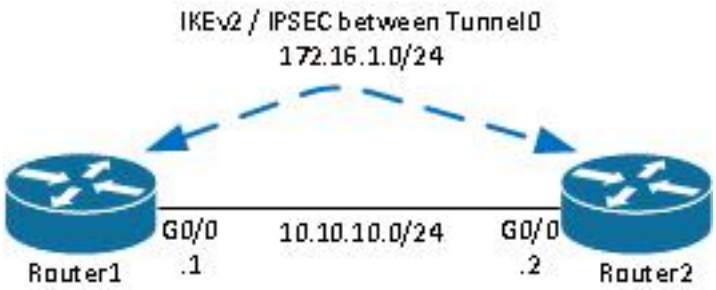
Zertifizierungsstelle

Derzeit unterstützt die Cisco IOS-Software keinen lokalen CA-Server (Certificate Authority), der ECDH ausführt. Dies ist für Suite B erforderlich. Ein CA-Server eines Drittanbieters muss implementiert werden. In diesem Beispiel wird eine Microsoft CA basierend auf Suite B PKI verwendet.

Konfigurieren

Netzwerktopologie

Dieser Leitfaden basiert auf dieser abgebildeten Topologie. IP-Adressen sollten an Ihre Anforderungen angepasst werden.



Hinweise:

Die Konfiguration besteht aus zwei direkt miteinander verbundenen Routern, die durch viele Hops voneinander getrennt sein können. Wenn ja, stellen Sie sicher, dass eine Route zur Peer-IP-Adresse vorhanden ist. In dieser Konfiguration wird nur die verwendete Verschlüsselung angegeben. IKEv2-Routing oder ein Routing-Protokoll sollten über das IPSec-VPN implementiert werden.

Schritte erforderlich, um dem Router die Verwendung des Elliptic Curve Digital Signature Algorithm zu ermöglichen

1. Erstellen Sie den Domänennamen und den Hostnamen, die Voraussetzung für die Erstellung eines EC-Tastenfelds sind.

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

Hinweis: Wenn Sie keine Version mit der Behebung für die Cisco Bug-ID CSCue59994

ausführen, können Sie mit dem Router kein Zertifikat mit einem Keysize-Wert unter 768 registrieren.

2. Erstellen Sie einen lokalen Vertrauenspunkt, um ein Zertifikat von der CA zu erhalten.

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

Hinweis: Da die CA offline war, wurden die Widerrufsprüfungen deaktiviert. Widerrufskontrollen sollten aktiviert werden, um in einer Produktionsumgebung maximale Sicherheit zu gewährleisten.

3. Authentifizieren des Vertrauenspunkts (erhält eine Kopie des Zertifikats der Zertifizierungsstelle, das den öffentlichen Schlüssel enthält).

```
crypto pki authenticate ecdh
```

4. Geben Sie an der Eingabeaufforderung das Base-64-kodierte Zertifikat der CA ein. Geben Sie **quit (Beenden)** und dann **yes (Ja** akzeptieren) ein.

5. Registrieren Sie den Router bei der PKI der CA.

```
crypto pki enrol ecdh
```

6. Die angezeigte Ausgabe wird verwendet, um eine Zertifikatsanforderung an die Zertifizierungsstelle zu senden. Stellen Sie für die Microsoft CA eine Verbindung zur Webschnittstelle der CA her, und wählen Sie **Zertifikatsanforderung einreichen aus**.

7. Importieren Sie das Zertifikat, das Sie von der CA erhalten haben, in den Router. Geben Sie **quit** ein, sobald das Zertifikat importiert wurde.

```
crypto pki import ecdh certificate
```

Konfiguration

Die hier bereitgestellte Konfiguration gilt für Router1. Router2 erfordert einen Spiegel der Konfiguration, in dem nur die IP-Adressen auf der Tunnelschnittstelle eindeutig sind.

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

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

2. Konfigurieren Sie das IKEv2-Angebot für Suite B.

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

Hinweis: IKEv2 Smart Defaults implementiert eine Reihe vorkonfigurierter Algorithmen im IKEv2-Standardvorschlag. Da aes-cbc-128 und sha256 für Suite-B-GCM-128 erforderlich sind, müssen Sie in diesen Algorithmen aes-cbc-256, sha384 und sha512 entfernen. Der Grund dafür ist, dass IKEv2 den stärksten Algorithmus wählt, wenn eine Auswahl getroffen wird. Verwenden Sie für maximale Sicherheit aes-cbc-256 und sha512. Dies ist jedoch nicht für Suite-B-GCM-128 erforderlich. Um den konfigurierten IKEv2-Vorschlag anzuzeigen, geben Sie den Befehl **show crypto ikev2 Proposal ein**.

3. Konfigurieren Sie das IKEv2-Profil so, dass es der Zertifikatszuordnung entspricht, und verwenden Sie ECDSA mit dem zuvor definierten Trustpoint.

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

4. Konfigurieren Sie die IPSec-Transformation für die Verwendung von GCM.

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

5. 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
```

6. Konfigurieren Sie die Tunnelschnittstelle.

```
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
```

Verbindung überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

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

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

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

3. Überprüfen Sie, ob die IKEv2 SA erfolgreich erstellt wurde, und verwenden Sie die Suite B-Algorithmen.

```
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. Überprüfen Sie, ob die IKEv2 SA erfolgreich erstellt wurde, und verwenden Sie die Suite B-Algorithmen.

```
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)
```

Hinweis: In dieser Ausgabe wird im Gegensatz zu Internet Key Exchange Version 1 (IKEv1) der perfekte Forward Secrecy (PFS) Diffie-Hellman (DH)-Gruppenwert als **PFS (Y/N)** angezeigt**: N, DH-Gruppe: Keine** während der ersten Tunnelverhandlung, aber nach einem erneuten Auftreten werden die richtigen Werte angezeigt. Dies ist kein Fehler, obwohl das Verhalten in der Cisco Bug-ID CSCug67056 beschrieben wird. Der Unterschied zwischen IKEv1 und IKEv2 besteht darin, dass in letzterem die untergeordneten Sicherheitszuordnungen (SAs) als Teil des AUTH-Austauschs selbst erstellt werden. Die unter der Crypto Map konfigurierte DH-Gruppe wird nur während des rekey verwendet. Daher sehen Sie **PFS (J/N): N, DH-Gruppe: keine** bis zum ersten Wiederaufflammen. Bei IKEv1 wird jedoch ein anderes Verhalten angezeigt, da die Erstellung der untergeordneten SA während des Schnellmodus erfolgt und die CREATE_CHILD_SA-Nachricht eine Rückstellung für das Tragen der Key Exchange-Payload enthält, die die DH-Parameter angibt, um einen neuen gemeinsamen geheimen Schlüssel abzuleiten.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Schlussfolgerung

Die in NGE definierten effizienten und leistungsstarken kryptografischen Algorithmen bieten langfristig die Sicherheit, dass Daten vertraulich und integer zu geringen Kosten bereitgestellt und verwaltet werden. NGE kann problemlos mit FlexVPN implementiert werden, das Suite B-Standardkryptografie bietet.

Weitere Informationen zur Implementierung von Suite B durch Cisco finden Sie unter Verschlüsselung der nächsten Generation.