採用下一代加密的FlexVPN配置示例

目錄

簡介

本文描述如何在支援思科下一代加密(NGE)演算法集的兩台路由器之間配置FlexVPN。

下一代加密

Cisco NGE加密技術可保護使用四種可配置、完善的公共域加密演算法的網路傳輸的資訊：

- 基於高級加密標準(AES)的加密，使用128位或256位金鑰
- 使用具有256位和384位素模數的曲線的橢圓曲線數位簽章演算法(ECDSA)的數位簽章
- 使用橢圓曲線Diffie-hellman(ECDH)方法的金鑰交換
- 基於安全雜湊演算法2(SHA-2)的雜湊（數字指紋）

美國國家安全域性(NSA)表示，這四種演算法結合起來為機密資訊提供了充分的資訊保證。用於IPsec的NSA套件B加密技術已作為RFC 6379中的標準發佈，並已得到業界的認可。

Suite Suite-B-GCM-128

根據RFC 6379，套件Suite-B-GCM-128需要這些演算法。

此套件使用128位AES-GCM提供封裝安全負載(ESP)完整性保護和保密性(請參閱RFC4106)。 當同時需要ESP完整性保護和加密時，應使用此套件。

ESP
加密AES(在加洛瓦/計數器模式(GCM)下具有128位金鑰和16個八位組完整性檢查值(ICV))(RFC4106)
完整性NULL

IKEv2
在密碼區塊鏈結(CBC)模式下使用128位金鑰的加密AES(RFC3602)
偽隨機函式HMAC-SHA-256(RFC4868)
完整性HMAC-SHA-256-128(RFC4868)
Diffie-Hellman群組256位隨機ECP群組(RFC5903)

有關Suite B和NGE的詳細資訊，請參閱下一代加密。

必要條件

需求

思科建議您瞭解以下主題：

- FlexVPN
- 網際網路金鑰交換版本2(IKEv2)
- IPsec

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 硬體：運行安全許可證的整合多業務路由器(ISR)第2代(G2)。
- 軟體：Cisco IOS®軟體版本15.2.3T2。任何Cisco IOS軟體版本M或15.1.2T或更新版本均可使用，因為這是在引入GCM時。

有關詳細資訊，請參閱功能導航器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

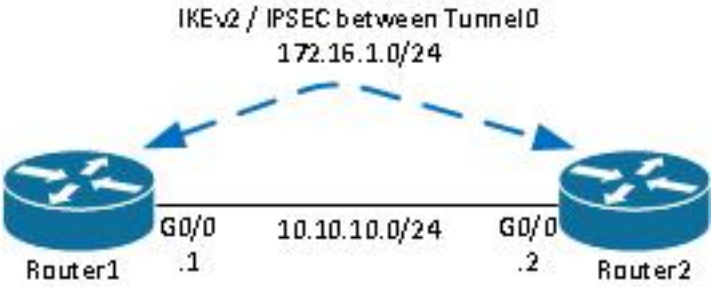
證書頒發機構

目前，Cisco IOS軟體不支援執行ECDH的本地憑證授權單位(CA)伺服器，套件B需要該伺服器。必須實作第三方CA伺服器。本示例使用基於Suite B PKI的Microsoft CA

設定

網路拓撲

本指南基於此圖示拓撲。應修改IP地址以滿足您的要求。



附註：

安裝程式由兩個直接連線的路由器組成，這些路由器之間可能有多個躍點。如果是，請確儲存在到達對等IP地址的路由。此配置僅詳細介紹使用的加密。應通過IPSec VPN實施IKEv2路由或路由協定。

啟用路由器使用橢圓曲線數位簽章演算法所需的步驟

1. 建立域名和主機名，這是建立EC金鑰對的先決條件。

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

附註：除非使用修正思科錯誤ID CSCue5994的版本運行該版本，否則路由器將不允許您註冊金鑰大小小於768的證書。

2. 建立本機信任點以便從CA取得憑證。

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

附註：由於CA處於離線狀態，因此已禁用吊銷檢查。應在生產環境中啟用吊銷檢查以實現最大安全性。

3. 對信任點進行身份驗證（這將獲取包含公鑰的CA證書的副本）。

```
crypto pki authenticate ecdh
```

4. 在提示時輸入CA的base 64編碼證書。 輸入**quit**，然後輸入**yes**接受。

5. 將路由器註冊到CA上的PKI中。

```
crypto pki enrol ecdh
```

6. 顯示的輸出用於向CA提交證書請求。對於Microsoft CA，連線到CA的Web介面，然後選擇**Submit a certificate request**。

7. 將從CA接收的憑證匯入路由器。匯入證書後輸入**quit**。

```
crypto pki import ecdh certificate
```

組態

此處提供的配置用於Router1。Router2需要配置映象，其中只有通道介面上的IP位址是唯一的。

1. 建立證書對映以匹配對等裝置的證書。

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

2. 為套件B配置IKEv2方案。

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

附註：IKEv2 Smart Defaults在預設IKEv2建議內實現許多預配置的演算法。由於套件Suite-B-GCM-128需要aes-cbc-128和sha256，因此必須在這些演算法中移除aes-cbc-256、sha384和sha512。其原因在於，IKEv2在有選擇的情況下會選擇最強的演算法。為了獲得最大的安全性，請使用aes-cbc-256和sha512。但是，Suite-B-GCM-128不需要此功能。要檢視配置的IKEv2提議，請輸入**show crypto ikev2 proposal**命令。

3. 配置IKEv2配置檔案以匹配證書對映並使用帶有之前定義的信任點的ECDSA。

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

4. 配置IPSec轉換以使用GCM。

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

5. 使用之前配置的引數配置IPSec配置檔案。

```
crypto ipsec profile default
 set transform-set ESP_GCM
```

```
 set pfs group19
 set ikev2-profile default
```

6. 配置隧道介面。

```
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
```

驗證連線

使用本節內容，確認您的組態是否正常運作。

1. 驗證ECDSA金鑰是否成功生成。

```
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. 驗證憑證是否成功匯入且是否使用ECDH。

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

3. 驗證是否已成功建立IKEv2 SA並使用套件B演算法。

```
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. 驗證是否已成功建立IKEv2 SA並使用套件B演算法。

```
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)
```

附註：在此輸出中，與網際網路金鑰交換版本1(IKEv1)不同，完全向前保密(PFS)Diffie-hellman(DH)群組值顯示為**PFS(Y/N):否，DH組：在首**次通道交涉期間無，但重新設定金鑰後，會顯示正確的值。這不是錯誤，即使Cisco錯誤ID CSCug67056中介紹了該行為。IKEv1和IKEv2之間的區別在於，在後一種情況下，子級安全關聯(SA)是作為AUTH交換本身的一部分建立的。在加密對映下配置的DH組僅在重新生成金鑰期間使用。因此，您會**看到PFS(Y/N):否，DH組：直到第**一個重新生成金鑰為止。但是對於IKEv1，您會看到不同的行為，因為子SA建立發生在快速模式期間，而CREATE_CHILD_SA消息具有攜帶金鑰交換有效載荷的設定，該有效載荷指定DH引數以派生新的共用金鑰。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

結論

在NGE中定義的高效和強大的加密演算法以低成本提供和維護資料保密和完整性的長期保證。NGE可以通過FlexVPN輕鬆實現，FlexVPN提供Suite B標準加密。

有關思科實施Suite B的詳細資訊，請參閱下一代加密。