使用下一代加密的路由器和ASA之間的FlexVPN配置示例

目錄

簡介

本文檔介紹如何在使用FlexVPN的路由器與支援思科下一代加密(NGE)演算法的自適應安全裝置(ASA)之間配置VPN。

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
- ASA
- 下一代加密技術

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IOS第2代(G2)路由器。
- **軟體**：Cisco IOS®軟體版本15.2-3.T2。任何低於Cisco IOS®軟體版本15.1.2T的M或T版本均可使用，因為此版本隨伽羅瓦計數器模式(GCM)的引入而包含。
- **硬體**：支援NGE的ASA。**注意**：只有多核平台支援高級加密標準(AES)GCM。
- **軟體**：支援NGE的ASA軟體9.0版或更高版本。
- OpenSSL。

有關詳細資訊，請參閱思科功能導航器。

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。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

動態建立IPSec安全關聯

IOS上建議的IPSec介面是虛擬通道介面(VTI)，其會建立受IPsec保護的通用路由封裝(GRE)介面。對於VTI，流量選擇器(哪些流量應受IPSec安全關聯(SA)保護)由從通道來源到通道目的地的GRE流量組成。因為ASA不實施GRE介面，而是根據訪問控制清單(ACL)中定義的流量建立IPSec SA，因此我們必須啟用允許路由器使用建議的流量選擇器的映象響應IKEv2啟動的方法。在FlexVPN路由器上使用動態虛擬通道介面(DVTI)允許此裝置使用提供的流量選擇器的映象來響應提供的流量選擇器。

此範例會加密兩個內部網路之間的流量。當ASA向IOS內部網路`192.168.1.0/24`到`172.16.10.0/24`呈現ASA內部網路的流量選擇器時，DVTI介面將響應流量選擇器的映象，即`172.16.10.0/24`到`192.168.1.0/24`。

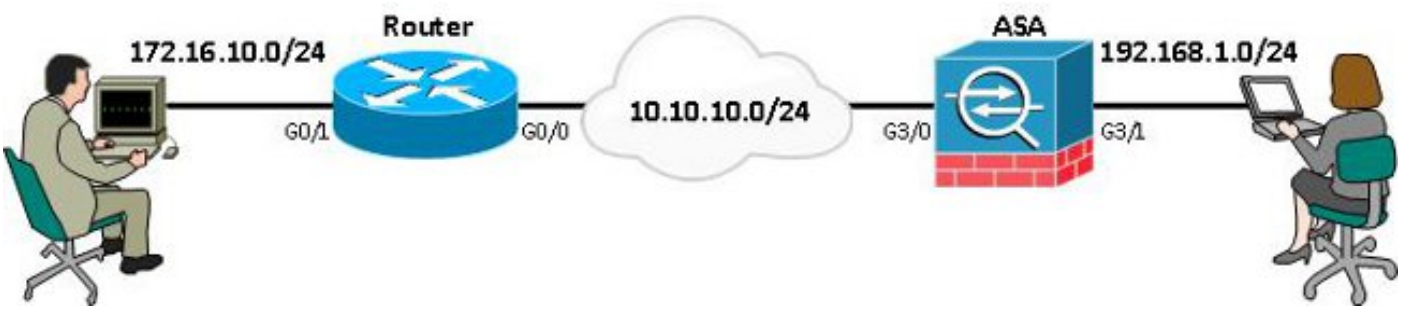
證書頒發機構

目前，IOS和ASA不支援具有橢圓曲線數位簽章演算法(ECDSA)證書的本地證書頒發機構(CA)伺服器，這是Suite-B所必需的。因此必須實施第三方CA伺服器。例如，使用OpenSSL充當CA。

組態

網路拓撲

本指南基於此圖中所示的拓撲。您應該修改IP地址以適應。



注意：設定包括直接連線路由器和ASA。它們之間可以隔出許多跳。如果是，請確儲存在到達對等IP地址的路由。以下配置僅詳細說明了使用的加密。

啟用路由器使用ECDSA所需的步驟

證書頒發機構

1. 建立橢圓**曲線金鑰對**。
```
openssl ecparam -out ca.key -name secp256r1 -genkey
```
2. 建立一**個橢圓曲線自簽名證書**。
```
openssl req -x509 -new -key ca.key -out ca.pem -outform PEM -days 3650
```

FlexVPN

1. 建立**domain-name**和**hostname**，這些是建立橢圓曲線(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
```
2. 建立本地**信任點**以便從CA獲取證書。
```
crypto pki trustpoint ec_ca
 enrollment terminal
 subject-name cn=router1.cisco.com
 revocation-check none
 eckeypair router1.cisco.com
 hash sha256
```
注意：由於CA處於離線狀態，因此吊銷檢查處於禁用狀態；應在生產環境中啟用吊銷檢查以實現最大安全性。
3. 驗證信**任點**。這會獲取CA證書的副本，其中包含公鑰。
```
crypto pki authenticate ec_ca
```
4. 然後提示您輸入CA的base 64編碼憑證。這是使用OpenSSL建立的ca.pem檔案。若要檢視此檔案，請在編輯器中或使用OpenSSL指令**openssl x509 -in ca.pem**將其開啟。貼上此內容時輸入**quit**。然後鍵入**yes**接受。
5. 將路由器註冊到CA上的公開金鑰基礎架構(PKI)。
```
crypto pki enrol ec_ca
```
6. 您收到的輸出需要用於向CA提交證書請求。這可儲存為文字檔案(flex.csr)，並使用OpenSSL指令進行簽名。
```
openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in flex.csr -out flex.pem
```
7. 輸入此命令後，將包含在CA產生的flex.pem檔案中的憑證匯入路由器。然後，完成時輸入**quit**。
```
crypto pki import ec_ca certificate
```

ASA

1. 建立**domain-name**和**hostname**，它們是建立EC金鑰對的先決條件。
```
domain-name cisco.com
hostname ASA1
crypto key generate ecdsa label asa1.cisco.com elliptic-curve 256
```
2. 建立本地**信任點**，以便從CA獲取證書。
```
crypto ca trustpoint ec_ca
 enrollment terminal
 subject-name cn=asa1.cisco.com
 revocation-check none
 keypair asa1.cisco.com
```

注意：由於CA處於離線狀態，因此吊銷檢查處於禁用狀態；應在生產環境中啟用吊銷檢查以實現最大安全性。

3. 驗證信**任點**。這會獲取CA證書的副本，其中包含公鑰。
   ```
   crypto ca authenticate ec_ca
   ```
4. 然後提示您輸入CA的base 64編碼憑證。這是使用OpenSSL建立的ca.pem檔案。若要檢視此檔案，請在編輯器中或使用OpenSSL指令**openssl x509 -in ca.pem**將其開啟。貼上此檔案時輸入**quit**，然後鍵入**yes**接受。
5. 將ASA註冊到CA上的PKI中。
   ```
   crypto ca enrol ec_ca
   ```
6. 您必須使用收到的輸出向CA提交證書請求。這可儲存為文本檔案(asa.csr)，然後使用OpenSSL命令進行簽名。
   ```
   openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in asa.csr -out asa.pem
   ```
7. 輸入此命令後，將從CA產生的憑證以a.pem形式匯入路由器中。完成後，輸入**quit**。
   ```
   crypto ca import ec_ca certificate
   ```

組態

FlexVPN

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
```

為Suite-B配置的IKEv2建議輸入以下命令：

註：為獲得最大的安全性，請使**用aes-cbc-256 with sha512 hash命令進行**配置。

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

將IKEv2配置檔案與證書對映進行匹配，然後將ECDSA與先前定義的**信任點**配合使用。

```
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
```

配置IPSec轉換集以使用伽羅瓦計數器模式(GCM)。

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

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
```
設定通道介面：

```
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel source GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```
以下是介面組態：

```
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

使用以下介面配置：

```
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
```
輸入以下存取清單命令，以定義要加密的流量：

```
access-list 100 extended permit ip 192.168.1.0 255.255.255.0 172.16.10.0 255.255.255.0
```
輸入帶NGE的以下IPSec proposal命令：

```
crypto ipsec ikev2 ipsec-proposal prop1
 protocol esp encryption aes-gcm
 protocol esp integrity null
```
加密對映命令：

```
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
```
此命令使用NGE配置IKEv2策略：

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

```
crypto ikev2 enable outside
```

為對等命令配置的隧道組：

```
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
```

連線驗證

驗證ECDSA金鑰是否已成功生成。

```
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...>
```

確認已成功匯入證書並且使用了ECDSA。

```
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...>
```

確認已成功建立IKEv2 SA並使用配置的NGE演算法。

```
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
```

確認已成功建立IPSec SA並使用配置的NGE演算法。

注意：FlexVPN可以從同時支援IKEv2和IPSec協定的非IOS客戶端終止IPSec連線。

```
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, }
```

有關思科實施Suite-B的詳細資訊，請參閱下一代加密白皮書。

請參閱下一代加密解決方案頁面，以瞭解更多有關思科實施下一代加密的資訊。

相關資訊

- 下一代加密白皮書
- 「下一代加密解決方案」頁
- 安全殼層 (SSH)
- IPSec 協商/IKE 通訊協定
- 適用於採用PSK的站點到站點VPN的ASA IKEv2調試技術說明
- ASA IPSec和IKE調試（IKEv1主模式）故障排除技術說明
- IOS IPSec和IKE調試 — IKEv1主模式故障排除技術說明
- ASA IPSec和IKE調試 — IKEv1主動模式技術說明
- 技術支援與文件 - Cisco Systems