具有下一代加密的路由器和ASA之间的FlexVPN配置示例

目录

简介

本文档介绍如何在使用FlexVPN的路由器与支持思科下一代加密(NGE)算法的自适应安全设备(ASA)之间配置VPN。

先决条件

要求

Cisco 建议您了解以下主题：

- FlexVPN
- 互联网密钥交换版本2(IKEv2)
- IPsec
- ASA
- 下一代加密

使用的组件

本文档中的信息基于以下软件和硬件版本：

- **Hardware:**运行安全许可证的IOS第2代(G2)路由器。
- **软件**：Cisco IOS®软件版本15.2-3.T2。M或T版本在Cisco IOS®软件版本15.1.2T之后的版本中，可以使用任何版本的M或T，因为Galois计数器模式(GCM)的引入中也包含了此版本。
- **Hardware:**支持NGE的ASA。**注意**：只有多核平台支持高级加密标准(AES)GCM。
- **软件**：支持NGE的ASA软件版本9.0或更高版本。
- OpenSSL。

有关详细信息，请参阅Cisco Feature Navigator。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

动态创建IPSec安全关联

IOS上推荐的IPSec接口是虚拟隧道接口(VTI)，它创建受IPsec保护的通用路由封装(GRE)接口。对于VTI，流量选择器(哪些流量应受IPSec安全关联(SA)保护)包括从隧道源到隧道目标的GRE流量。由于ASA不实施GRE接口，而是根据访问控制列表(ACL)中定义的流量创建IPSec SA，因此我们必须启用一种方法，允许路由器使用建议的流量选择器的镜像响应IKEv2启动。在FlexVPN路由器上使用动态虚拟隧道接口(DVTI)可让此设备使用所显示流量选择器的镜像响应显示的流量选择器。

此示例加密两个内部网络之间的流量。当ASA向IOS内部网络(192.168.1.0/24到`172.16.10.0/24`)显示ASA内部网络的流量选择器时，DVTI接口会以流量选择器的镜像(即`172.16.10.0/24` `192`.168.1.0/24)作出响应

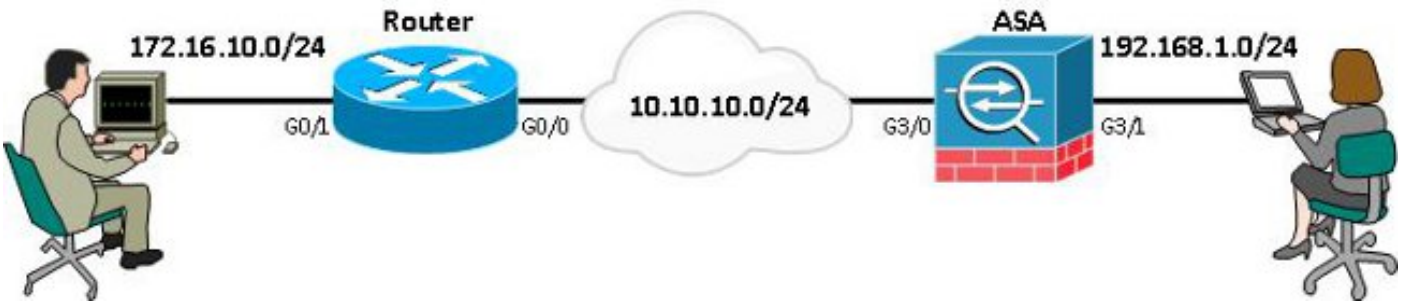
认证中心

目前，IOS和ASA不支持具有Elliptic Curve数字签名算法(ECDSA)证书的本地证书颁发机构(CA)服务器，这是Suite-B所需的。因此，必须实施第三方CA服务器。例如，使用OpenSSL作为CA。

配置

网络拓扑

本指南基于此图中所示的拓扑。您应该修改IP地址。



注意：设置包括路由器和ASA的直接连接。这些路由可以分为多跳。如果是，请确保有到达对等IP地址的路由。以下配置仅详细说明使用的加密。

启用路由器以使用ECDSA所需的步骤

认证中心

1. 创建一个**椭圆曲线键对。**
```
openssl ecparam -out ca.key -name secp256r1 -genkey
```
2. 创建一个**椭圆曲线自签名证书。**
```
openssl req -x509 -new -key ca.key -out ca.pem -outform PEM -days 3650
```

FlexVPN

1. 创**建域名**和**主机名**，这是创建椭圆曲线(EC)密钥对的必备条件。
```
ip domain-name cisco.com
hostname Router1
crypto key generate ec keysize 256 label router1.cisco.com
```
2. 创建本**地信**任点以从CA获取证书。
```
crypto pki trustpoint ec_ca
 enrollment terminal
 subject-name cn=router1.cisco.com
 revocation-check none
 eckeypair router1.cisco.com
 hash sha256
```
注意：由于CA处于脱机状态，因此撤销检查被禁用；应启用撤销检查，以在生产环境中实现最大安全性。
3. 验证信**任点**。这将获取包含公钥的CA证书的副本。
```
crypto pki authenticate ec_ca
```
4. 然后，系统将提示您输入CA的基64编码证书。这是使用OpenSSL创建的文件ca.pem。要查看此文件，请在编辑器中或使用OpenSSL命令openssl x509 -in ca.pem打**开此文件**。粘贴此**项时**输入quit。然后键入**yes**接受。
5. 将路由器注册到CA上的公钥基础设施(PKI)。
```
crypto pki enrol ec_ca
```
6. 您收到的输出需要用于向CA提交证书请求。这可以另存为文本文件(flex.csr)并使用OpenSSL命令签名。
```
openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in flex.csr -out flex.pem
```
7. 输入此命令后，将包含在从CA生成的flex.pem文件中的证书导入路由器。然后，在完成**后输**入quit。
```
crypto pki import ec_ca certificate
```

ASA

1. 创**建域名**和**主机名**，这是创建EC密钥对的必备条件。
```
domain-name cisco.com
hostname ASA1
crypto key generate ecdsa label asa1.cisco.com elliptic-curve 256
```
2. 创建本地**信任**点以从CA获取证书。
```
crypto ca trustpoint ec_ca
 enrollment terminal
 subject-name cn=asa1.cisco.com
 revocation-check none
 keypair asa1.cisco.com
```

注意：由于CA处于脱机状态，因此撤销检查被禁用；应启用撤销检查，以在生产环境中实现最大安全性。

3. 验证信**任点**。这将获取包含公钥的CA证书的副本。
   ```
   crypto ca authenticate ec_ca
   ```
4. 然后，系统将提示您输入CA的基64编码证书。这是使用OpenSSL创建的文件ca.pem。要查看此文件，请在编辑器中或使用OpenSSL命令openssl x509 -in ca.pem打**开此文件**。在粘贴**此**文件时输入quit，然后键入**yes**接受。
5. 将ASA注册到CA上的PKI。
   ```
   crypto ca enrol ec_ca
   ```
6. 您收到的输出必须用于向CA提交证书请求。这可以另存为文本文件(asa.csr)，然后使用OpenSSL命令签名。
   ```
   openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in asa.csr -out asa.pem
   ```
7. 输入此命令后，将文件中包含的证书作为a.pem从CA生成的证书导入路由器。然后**在完**成时输入quit。
   ```
   crypto ca import ec_ca certificate
   ```

配置

FlexVPN

创建证书映射以匹配对等设备的证书。

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

为Suite-B的IKEv2建议配置输入以下命令：

注意：为了实现最大安全性，请使用**aes-cbc-256 with sha512 hash命令进行**配置。

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

将IKEv2配置文件与证书映射匹配，并将ECDSA与之前定义的**信任点**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转换集以使用Galois计数器模式(GCM)。

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

使用之前配置的参数配置IPSec配置文件。

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

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

配置隧道接口：

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

接口配置如下：

```
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

使用此接口配置：

```
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
```

输入以下访问列表命令以定义要加密的流量：

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

输入此IPSec建议命令和NGE:

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

加密映射命令：

```
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
```

为对等命令配置的隧道组：

```
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
```

连接验证

验证ECDSA密钥已成功生成。

```
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...>
```

验证证书已成功导入且已使用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...>
```

验证IKEv2 SA已成功创建并使用已配置的NGE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
```

验证IPSec SA已成功创建并使用已配置的NGE算法。

注意：FlexVPN可以终止来自同时支持IKEv2和IPSec协议的非IOS客户端的IPSec连接。

```
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, }
```

有关思科实施Suite-B的详细信息，请参阅下一代加密白皮书。

有关思科实施下一代加密的详细信息，请参阅下一代加密解决方案页面。

相关信息

- 下一代加密白皮书
- 下一代加密解决方案页
- Secure Shell (SSH)
- IPsec 协商/IKE 协议
- 使用PSK的站点到站点VPN的ASA IKEv2调试技术说明
- ASA IPSec和IKE调试（IKEv1主模式）故障排除技术说明
- IOS IPSec和IKE调试 — IKEv1主模式故障排除技术说明
- ASA IPSec和IKE调试 — IKEv1主动模式技术说明
- 技术支持和文档 - Cisco Systems