带下一代加密的FlexVPN配置示例

目录

简介

本文档介绍如何在支持思科下一代加密(NGE)算法集的两台路由器之间配置FlexVPN。

下一代加密

思科NGE加密保护通过使用四个可配置、已建立且公共域加密算法的网络传输的信息：

- 基于高级加密标准(AES)的加密，该标准使用128位或256位密钥
- 使用椭圆曲线数字签名算法(ECDSA)的数字签名，该算法使用带256位和384位素模的曲线
- 使用椭圆曲线Diffie-Hellman(ECDH)方法的密钥交换
- 基于安全散列算法2(SHA-2)的散列（数字指纹）

美国国家安全局(NSA)指出，这四种算法结合起来为保密信息提供了充分的信息保障。NSA Suite B IPsec加密已作为RFC 6379中的标准发布，并已在业界得到认可。

套件 — B-GCM-128

根据RFC 6379,Suite Suite-B-GCM-128需要这些算法。

此套件通过128位AES-GCM（请参阅RFC4106）提供封装安全负载(ESP)完整性保护和机密性保护。 当同时需要ESP完整性保护和加密时，应使用此套件。

ESP
加密AES，在Galois/Counter模式(GCM)(RFC4106)下，使用128位密钥和16个八位组完整性检查值(ICV)
完整性NULL

IKEv2
加密AES，在密码块链(CBC)模式(RFC3602)下使用128位密钥
伪随机函数HMAC-SHA-256(RFC4868)
完整性HMAC-SHA-256-128(RFC4868)
Diffie-Hellman组256位随机ECP组(RFC5903)

有关Suite B和NGE的详细信息，请参阅下一代加密。

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

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Hardware:运行安全许可证的第2代集成多业务路由器(ISR)(G2)。
- 软件：Cisco IOS®软件版本15.2.3T2。Cisco IOS软件版本M或15.1.2T或更高版本可以使用，因为GCM引入时就是这个版本。

有关详细信息，请参阅功能导航器。

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。

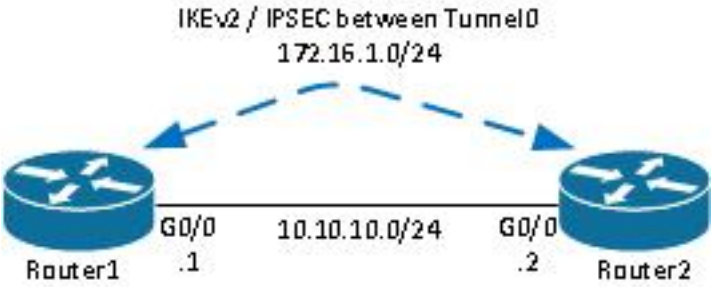
认证中心

目前，Cisco IOS软件不支持运行ECDH的本地证书颁发机构(CA)服务器，这是Suite B所必需的。必须实施第三方CA服务器。此示例使用基于Suite B PKI的Microsoft CA

配置

网络拓扑

本指南基于此图示拓扑。应根据您的要求修改IP地址。



注意：

设置由两台直接连接的路由器组成，路由器之间可能分隔许多跳。如果是，请确保有到达对等IP地址的路由。此配置仅详细说明所使用的加密。IKEv2路由或路由协议应通过IPSec VPN实施。

使路由器能够使用椭圆曲线数字签名算法所需的步骤

1. 创建域名和主机名，这是创建EC密钥对的先决条件。

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

注意：除非您运行的版本包含Cisco Bug ID CSCue59994的修复，否则路由器将不允许您注册密钥大小小于768的证书。

2. 创建本地信任点以从CA获取证书。

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

注意：由于CA处于脱机状态，因此已禁用撤销检查。应启用撤销检查以在生产环境中实现最高安全性。

3. 验证信任点（这将获取包含公钥的CA证书的副本）。

```
crypto pki authenticate ecdh
```

4. 在提示符后输入CA的base 64编码证书。 输入**quit**，然后输入yes接受。

5. 将路由器注册到CA上的PKI。

```
crypto pki enrol ecdh
```

6. 显示的输出用于向CA提交证书请求。对于Microsoft CA，连接到CA的Web界面并选择“提**交证书请求**”。

7. 将从CA收到的证书导入路由器。导入证**书**后输入quit。

```
crypto pki import ecdh certificate
```

配置

此处提供的配置适用于Router1。Router2需要配置镜像，其中只有隧道接口上的IP地址是唯一的。

1. 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
```

2. 为Suite B配置IKEv2建议。

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

注意：IKEv2智能默认值在默认IKEv2建议中实施许多预配置算法。由于套件Suite-B-GCM-128需要aes-cbc-128和sha256，因此您必须在这些算法中删除aes-cbc-256、sha384和sha512。原因是IKEv2在提供选择时选择最强的算法。为获得最高安全性，请使用aes-cbc-256和sha512。但是，Suite-B-GCM-128不需要这些。要查看已配置的IKEv2建议，请输入**show crypto ikev2 proposal**命令。

3. 配置IKEv2配置文件以匹配证书映射并使用ECDSA与之前定义的信任点。

```
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转换以使用GCM。

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

5. 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
```

6. 配置隧道接口。

```
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
```

检验连接

使用本部分可确认配置能否正常运行。

1. 验证ECDSA密钥是否已成功生成。

```
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. 验证证书已成功导入且已使用ECDH。

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

3. 验证IKEv2 SA已成功创建并使用Suite B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. 验证IKEv2 SA已成功创建并使用Suite B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)
```

注意：在此输出中，与Internet密钥交换版本1(IKEv1)不同，完全向前保密(PFS)Diffie-Hellman(DH)组值显示为**PFS(Y/N):N，DH组：第**一次隧道协商期间无，但在重新生成密钥后，显示正确的值。虽然Cisco Bug ID CSCug67056中描述了此行为，但这不是Bug。IKEv1和IKEv2之间的区别在于，在IKEv1和IKEv2中，子安全关联(SA)是作为AUTH交换本身的一部分创建的。仅在重新生成密钥时，才使用在加密映射下配置的DH组。因此，您会看**到PFS(Y/N):N，DH组：直到**第一次重新键。但是，使用IKEv1时，您会看到不同的行为，因为子SA创建在快速模式期间发生，并且CREATE_CHILD_SA消息具有用于承载指定DH参数以派生新共享密钥的密钥交换负载的设置。

故障排除

目前没有针对此配置的故障排除信息。

结论

NGE中定义的高效和强大的加密算法提供长期保证，以低处理成本提供和维护数据机密性和完整性。NGE可以通过提供Suite B标准加密的FlexVPN轻松实施。

有关思科实施Suite B的详细信息，请参阅下一代加密。