与下一代加密配置示例的FlexVPN

目录

简介

本文描述如何配置在支持Cisco NEXT-GENERATION加密的两路由器之间的FlexVPN (NGE)套算法。

下一代加密

思科NGE加密算法在网络使用四可配置，源远流长和公共领域加密算法移动的安全信息：

- 根据高级加密标准(AES)的加密，使用128-bit或256-bit密钥
- 与椭圆曲线数字签名算法(ECDSA)的数字签名该使用弯曲与256-bit和384-bit头等模数
- 使用椭圆曲线Diffie-Hellman的密钥交换(ECDH)方法
- 根据安全散列算法(数字指纹)的切细2 (SHA-2)

国家安全局(NSA)阐明，在组合的这四种算法提供适当信息保证对于分级信息。NSA IPsec的套件B加密算法发布作为在RFC 6379的一个标准和得到了在行业的接受。

套件Suite-B-GCM-128

根据RFC 6379，这些算法为套件Suite-B-GCM-128要求。

此套件提供封装安全有效载荷(ESP)完整性保护和机密性128-bit AES-GCM (请参阅RFC4106)。此套件，当ESP完整性保护和加密两个必要时，应该使用。

ESP
与128-bit密钥的加密AES和在Galois/计数器模式(GCM) (RFC4106)的16八位字节总校验值(ICV)
完整性NULL

IKEv2
与128-bit密钥的加密AES在密码链块(CBC)模式(RFC3602)
伪随机功能HMAC-SHA-256 (RFC4868)
完整性HMAC-SHA-256-128 (RFC4868)
迪菲–赫尔曼组256-bit随机的ECP组(RFC5903)

关于套件B和NGE的更多信息可以在下一代加密找到。

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:集成服务路由器(ISR)运行安全许可证的生成2 (G2)该。
- 软件：Cisco IOS软件版本15.2.3T2。可以使用所有版本Cisco IOS软件版本M或15.1.2T或者以后，因为这是，当GCM介绍。

关于详细信息，参考功能导航。

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。

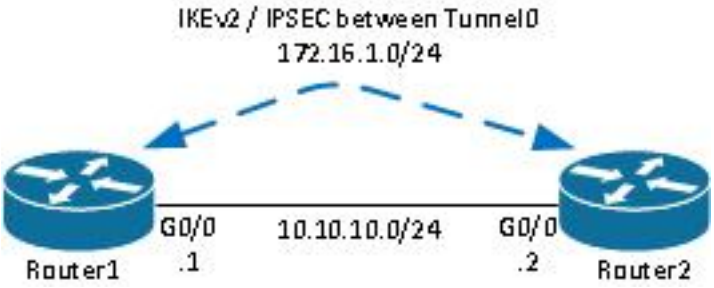
认证中心

目前， Cisco IOS软件不支持运行ECDH，为套件B.要求的一个本地Certificate Authority (CA)服务器。 必须实现第三方CA服务器。此示例使用根据套件的Microsoft CA B PKI

配置

网络拓扑

此指南根据此图示拓扑。 应该修正IP地址适合您的需求。



注意：

设置包括连接的两路由器，也许由许多跳分离。 如果那样，请保证有路由达到对端IP地址。此配置只选派使用的加密。 IKEv2应该在IPSec VPN实现路由或路由协议。

要求的步骤使路由器使用椭圆曲线数字签名算法

1. 创建域名和主机名，是创建EC密钥对的前提条件。

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

Note:除非运行版本以Cisco Bug ID的CSCue59994修正，路由器不会允许您登记与keysize的一证书少于768。

2. 创建一本地信任点为了获取从CA的一证书。

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

Note:因为CA脱机，撤销检查禁用。 应该为在生产环境的最大安全性启用撤销检查。

3. 验证信任点(这得到包含公共密钥) CA证书的复制。

```
crypto pki authenticate ecdh
```

4. 进入CA的base64编码的证书在提示符。 输入**离开**然后输入**是**接受。

5. 登记路由器到在CA的PKI。

```
crypto pki enrol ecdh
```

6. 显示的输出用于为了提交证书请求到CA。对于Microsoft CA，请连接对CA的Web接口并且选

择**提交证书请求**。

7. 导入从CA接收的证书到路由器。一旦证书导入，请输入**离开**。

```
crypto pki import ecdh certificate
```

配置

提供的配置此处是为Router1。Router2要求在隧道接口的仅IP地址是唯一配置的镜像。

1. 创建证书地图匹配对等设备的证书。

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

2. 配置IKEv2提议对于套件B。

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

Note:IKEv2聪明的默认实现在默认IKEv2建议内的一定数量的预先配置的算法。因为aes-cbc-128和sha256为套件Suite-B-GCM-128要求，您必须删除aes-cbc-256、sha384和sha512在这些算法内。对此的原因是IKEv2选择最强的算法，当提交与选择。最大安全性、使用aes-cbc-256和sha512。然而，这没有为Suite-B-GCM-128要求。为了查看已配置的IKEv2建议，输入**显示crypto ikev2建议**命令。

3. 配置IKEv2配置文件匹配证书地图和以定义的信任点使用ECDSA前。

```
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转换使用GCM。

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

5. 配置与配置的参数的IPSec简档前。

```
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
```

验证连接

使用本部分可确认配置能否正常运行。

1. 验证ECDSA密钥顺利地生成。

```
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. 验证证书顺利地导入，并且使用ECDH。

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

3. 验证IKEv2 SA顺利地创建并且使用套件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顺利地创建并且使用套件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)
```

Note:在此输出中，不同于在互联网密钥交换版本1 (IKEv1)，完整转发安全性(PFS) Diffie-Hellman (DH)组的值显示作为**PFS是/否：N， DH组：什么都**在第一隧道协商时，然而，在重新生成密钥发生后，正确的值不显示。这不是bug，即使行为在Cisco Bug ID CSCug67056描述。 在IKEv1和IKEv2之间的区别是作为验证交换一部分，在后者，儿童安全关联(SA)创建。在重新生成密钥期间， DH组配置在加密映射下仅使用。因此，您看到**PFS是/否：N， DH组：什么都**直到第一不重新生成密钥。但是与IKEv1，您看到一种不同的行为，因为SA儿童创建发生在快速模式期间，并且CREATE_CHILD_SA消息做好准备为指定DH参数派生一新建的共享机密的传送密钥交换有效负载。

故障排除

目前没有针对此配置的故障排除信息。

结论

在NGE定义的高效和强加密算法提供长期保证机要数据和完整性提供并且被维护在低成本处理。NGE可能容易地实现与FlexVPN，提供套件B标准加密算法。

关于套件B的思科的实施的更多信息可以在下一代加密找到。