使用IKEv2和证书通过IPsec连接到IOS头端的配置示例

目录

简介

本文档提供有关如何通过使用FlexVPN框架从运行AnyConnect客户端的设备到仅使用证书身份验证的Cisco IOS®路由器实现受IPsec保护的连接的信息。

先决条件

要求

Cisco 建议您了解以下主题：

- FlexVPN

- AnyConnect

使用的组件

本文档中的信息基于以下软件和硬件版本：

头端

Cisco IOS路由器可以是任何能够运行IKEv2且运行至少15.2 M&T版本的路由器。但是，您应使用较新的版本(请参阅已知警告部分)（如果可用）。

客户端

AnyConnect 3.x版本

认证中心

在本例中，证书颁发机构(CA)将运行15.2(3)T版本。

由于需要支持扩展密钥使用(EKU)，因此使用其中一个较新版本至关重要。

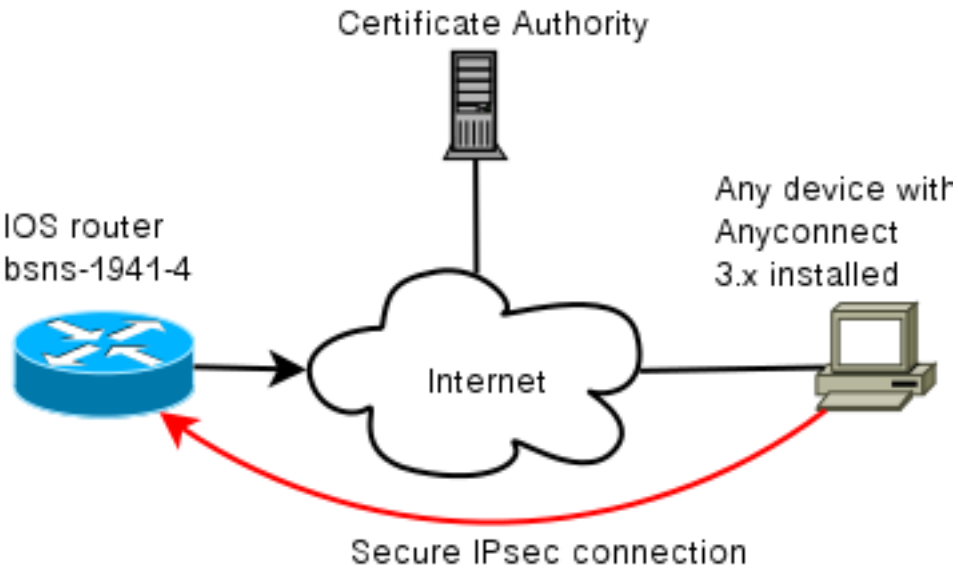
在此部署中，IOS路由器用作CA。但是，任何能够使用EKU的基于标准的CA应用都应该良好。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

网络拓扑



证书颁发机构（可选）

如果您选择使用它，则IOS路由器可以充当CA。

IOS CA配置

您需要记住，CA服务器必须在客户端和服务器证书上放置正确的EKU。在这种情况下，为所有证书设置了server-auth和client-auth EKU。

```
bsns-1941-3#show run | s crypto pki
crypto pki server CISCO
database level complete
database archive pem password 7 00071A1507545A545C
issuer-name cn=bsns-1941-3.cisco.com,ou=TAC,o=cisco
grant auto rollover ca-cert
grant auto
auto-rollover
eku server-auth client-auth
```

如何验证证书上是否设置了正确的EKU

请注意，bsns-1941-3是CA服务器，而bsns-1941-4是IPsec头端。为简洁起见，省略了部分输出。

```
BSNS-1941-4#show crypto pki certificate verbose
Certificate
(...omitted...)

Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: C3D52BE9 1EE97559 C7323995 3C51DC53
Fingerprint SHA1: 76BC7CD4 F298F8D9 A95338DC E5AF7602 9B57BE31
X509v3 extensions:
X509v3 Key Usage: A0000000
Digital Signature
Key Encipherment
X509v3 Subject Key ID: 83647B09 D3300A97 577C3E2C AAE7F47C F2D88ADF
X509v3 Authority Key ID: B3CC331D 7159C3CD 27487322 88AC02ED FAF2AE2E
Authority Info Access:
Extended Key Usage:
Client Auth
Server Auth
Associated Trustpoints: CISCO2
Storage: nvram:bsns-1941-3c#5.cer
Key Label: BSNS-1941-4.cisco.com
Key storage device: private config

CA Certificate
(...omitted...)
```

头端配置

头端配置由两部分组成：PKI部分和实际flex/IKEv2。

PKI配置

您会注意到已使用bsns-1941-4.cisco.com的CN。这需要匹配正确的DNS条目，并且需要包括在<Hostname>下的AnyConnect配置文件中。

```
crypto pki trustpoint CISCO2
enrollment url http://10.48.66.14:80
serial-number
ip-address 10.48.66.15
subject-name cn=bsns-1941-4.cisco.com,ou=TAC,o=cisco
revocation-check none

crypto pki certificate map CMAP 10
subject-name co cisco
```

加密/IPsec配置

请注意，建议书中的PRF/完整性设置**需要**与证书支持的内容匹配。这通常是SHA-1。

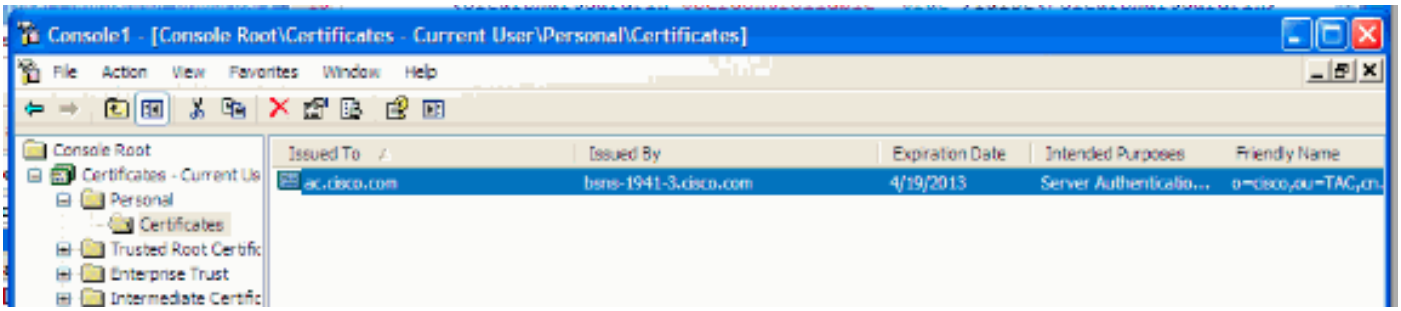
```
crypto ikev2 authorization policy AC
pool AC

crypto ikev2 proposal PRO
encryption 3des aes-cbc-128
integrity sha1
group 5 2

crypto ikev2 policy POL
match fvrf any
proposal PRO

crypto ikev2 profile PRO
match certificate CMAP
identity local dn
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint CISCO2
aaa authorization group cert list default AC
virtual-template 1

no crypto ikev2 http-url cert
crypto ipsec transform-set TRA esp-3des esp-sha-hmac

crypto ipsec profile PRO
set transform-set TRA
set ikev2-profile PRO

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

客户端

与IKEv2和证书成功进行AnyConnect连接的客户端配置由两部分组成。

证书注册

正确注册证书后，您可以验证证书是否存在于计算机或个人存储中。请记住，客户端证书还需要有EKU。



AnyConnect配置文件

AnyConnect配置文件冗长且基本。

相关部分定义：

1. 要连接的主机
2. 协议类型
3. 连接到该主机时要使用的身份验证

使用内容：

```
<ServerList>
<HostEntry>
<HostName>bsns-1941-4.cisco.com</HostName>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>
IKE-RSA
</AuthMethodDuringIKENegotiation>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

在AnyConnect的连接字段中，您需要提供完整的FQDN，该值在<HostName>。

连接验证

为简洁起见，省略了一些信息。

```
BSNS-1941-4#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA
Tunnel-id Local Remote fvrf/ivrf Status
2    10.48.66.15/4500    10.55.193.212/65311    none/none    READY
Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:5,
Auth sign: RSA, Auth verify: RSA
Life/Active Time: 86400/180 sec
```

```
IPv6 Crypto IKEv2 SA

BSNS-1941-4#show crypto ipsec sa

interface: Virtual-Access1
Crypto map tag: Virtual-Access1-head-0, local addr 10.48.66.15

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/0/0)
current_peer 10.55.193.212 port 65311
PERMIT, flags={origin_is_acl,}
#pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
#pkts decaps: 26, #pkts decrypt: 26, #pkts verify: 26

local crypto endpt.: 10.48.66.15, remote crypto endpt.: 10.55.193.212
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0x5C171095(1545015445)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8283D0F0(2189676784)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel UDP-Encaps, }
conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000040,
crypto map: Virtual-Access1-head-0
sa timing: remaining key lifetime (k/sec): (4215478/3412)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound esp sas:
spi: 0x5C171095(1545015445)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel UDP-Encaps, }
conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000040,
crypto map: Virtual-Access1-head-0
sa timing: remaining key lifetime (k/sec): (4215482/3412)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

下一代加密

上述配置被提供以用于显示最小工作配置。思科建议尽可能使用下一代加密(NGC)。

有关迁移的当前建议，请访问
：http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

选择NGC配置时，请确保客户端软件和头端硬件都支持它。建议将ISR第2代和ASR 1000路由器作为头端，因为它们对NGC的硬件支持。

在AnyConnect端，从AnyConnect 3.1版开始，支持NSA的Suite B算法套件。

已知警告和问题

- 请记住，在IOS头端上配置此线路：**无crypto ikev2 http-url证书**。IOS和AnyConnect在未配置时产生的错误具有相当的误导性。
- 早期的IOS 15.2M&T软件（带IKEv2会话）可能未启用RSA-SIG身份验证。这可能与Cisco Bug ID CSCtx31294(仅限注册客户)相关。 确保运行最新的15.2M或15.2T软件。
- 在某些情况下，IOS可能无法选择正确的信任点进行身份验证。思科已意识到此问题，自15.2(3)T1和15.2(4)M1版本起，思科已修复此问题。
- 如果AnyConnect报告的消息类似于以下内容：

```
The client certificate's cryptographic service provider(CSP)
does not support the sha512 algorithm
```

然后，您需要确保IKEv2提议中的完整性/PRF设置与证书可以处理的内容匹配。在上述配置示例中，使用SHA-1。

相关信息

- 技术支持和文档 - Cisco Systems