使用IKEv2和證書的AnyConnect to IOS Headend Over IPsec配置示例

目錄

簡介

本文提供如何使用FlexVPN框架從運行AnyConnect客戶端的裝置到僅使用證書身份驗證的Cisco IOS®路由器實現受IPsec保護的連線的資訊。

必要條件

需求

思科建議您瞭解以下主題：

- FlexVPN

- AnyConnect

採用元件

本文中的資訊係根據以下軟體和硬體版本：

頭端

Cisco IOS路由器可以是任何能夠運行IKEv2、運行至少15.2 M&T版本的路由器。但是您應該使用較新的版本(請參見已知警告部分)（如果可用）。

使用者端

AnyConnect 3.x版本

證書頒發機構

在本範例中，憑證授權單位(CA)將執行15.2(3)T版本。

使用較新的版本之一至關重要，因為需要支援擴展金鑰使用(EKU)。

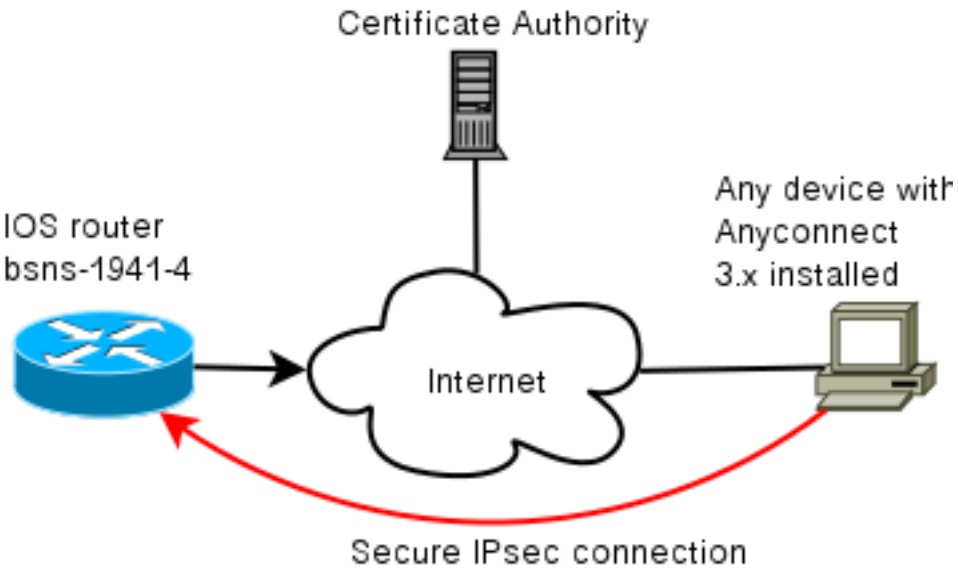
在此部署中，IOS路由器用作CA。但是，任何基於標準的、能夠使用EKU的CA應用程式都應該良好。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

組態

網路拓撲



證書頒發機構（可選）

如果您選擇使用它，您的IOS路由器可以充當CA。

IOS CA配置

您需要記住，CA伺服器必須在客戶端和伺服器證書上放置正確的EKU。在此案例中，已為所有憑證設定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
```

如何驗證證書上是否設定了正確的EKU

請注意，bsns-1941-3是CA伺服器，而bsns-1941-4是IPsec頭端。為了簡潔，部分輸出省略。

```
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...)
```

頭端配置

頭端配置由兩部分組成：PKI部分和實際flex/IKEv2。

PKI配置

您會注意到已使用bsns-1941-4.cisco.com的CN。它需要匹配正確的DNS條目，並且需要包含在<Hostname>下的AnyConnect配置檔案中。

```
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
```

Crypto/IPsec配置

請注意，建議書中的PRF/完整性設定**需要**與證書支援的內容匹配。這通常是SHA-1。

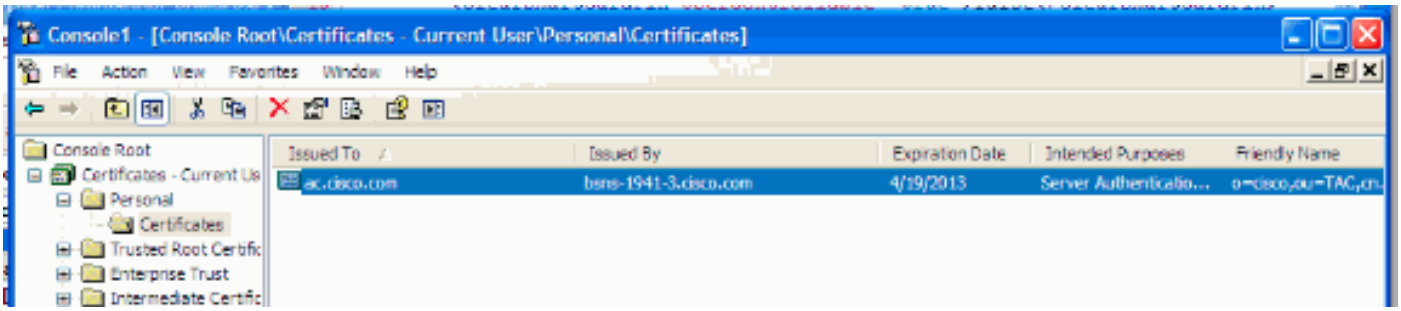
```
crypto ikev2 authorization policy AC
pool AC

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
```

使用者端

成功通過IKEv2和證書的AnyConnect連線的客戶端配置包括兩部分。

證書註冊

證書正確註冊後，您可以驗證它是否存在於電腦或個人儲存中。請記住，客戶端證書也需要具有EKU。



AnyConnect配置檔案

AnyConnect配置檔案非常冗長且非常基本。

相關部分是定義：

1. 要連線的主機
2. 通訊協定型別
3. 連線到該主機時要使用的身份驗證

使用內容：

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

在AnyConnect的連線欄位中，需要提供完整的FQDN，這是<HostName>中顯示的值。

連線驗證

為簡潔起見，省略了部分資訊。

```
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)
```

下一代加密技術

提供上述配置以供參考，以顯示最小工作配置。思科建議儘可能使用下一代加密技術(NGC)。

有關遷移的最新建議，請訪問以下網站
：http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

選擇NGC配置時，請確保客戶端軟體和頭端硬體都支援它。建議使用ISR第2代路由器和ASR 1000路由器作為前端，因為它們支援NGC。

在AnyConnect端，自AnyConnect 3.1版本起，支援NSA的Suite B演算法套件。

已知警告和問題

- 請記得在IOS頭端上配置以下線路：**no crypto ikev2 http-url cert**。IOS和AnyConnect在未配置時產生的錯誤具有很大的誤導性。
- 早期的IOS 15.2M&T軟體具有IKEv2會話，可能無法進行RSA-SIG身份驗證。此問題可能與思科錯誤ID CSCtx31294(僅限註冊客戶)有關。 確保運行最新的15.2M或15.2T軟體。
- 在某些情況下，IOS可能無法選擇正確的信任點進行身份驗證。思科知道問題，且自15.2(3)T1和15.2(4)M1版本起已修正。
- 如果AnyConnect報告類似以下內容的消息：

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

然後，您需要確保IKEv2建議中的完整性/PRF設定與您的證書可以處理的內容匹配。在上面的組態範例中，使用SHA-1。

相關資訊

- 技術支援與文件 - Cisco Systems