对IOS数据转发器的AnyConnect在与IKEv2和证书配置示例的IPsec

Contents

Introduction

本文提供信息关于怎样达到从运行AnyConnect客户端到Cisco IOS路由器与仅证书验证通过使用FlexVPN框架的设备的IPSec保护的连接。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- FlexVPN

- AnyConnect

Components Used

本文档中的信息基于以下软件和硬件版本：

数据转发器

Cisco IOS路由器可以是所有路由器能够运行IKEv2，运行至少15.2 M&T版本。然而，您应该使用新版本(请参阅已知Caveats部分)若有。

客户端

AnyConnect 3.x版本

认证机关

在本例中， Certificate Authority (CA)运行15.2(3)T版本。

是关键的一个更新的版本使用由于需要支持延长的密钥用法(EKU)。

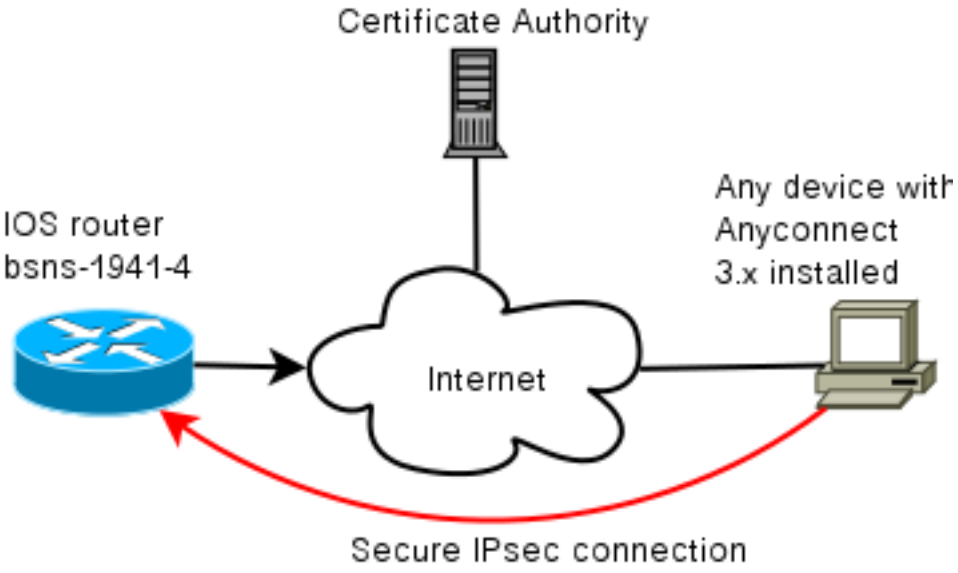
在此配置， IOS路由器使用作为CA。然而，所有基于标准的CA应用程序能够使用EKU应该是细致的。

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

配置

网络拓扑



认证机关(可选)

如果选择使用它，您的IOS路由器能作为CA。

IOS CA配置

您需要记得CA服务器在客户端和服务器证书必须放置正确的EKU。在这种情况下服务器auth和客户端auth EKU为所有证书设置。

```
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
```

如何验证正确EKU是否在认证设置

注意bsns-1941-3是CA服务器，当bsns-1941-4是IPsec数据转发器时。为简要起见被省略的输出的部分。

```
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...)
```

数据转发器配置

数据转发器配置包括两部分：PKI零件和实际flex/IKEv2。

PKI配置

您注意使用bsns-1941-4.cisco.com CN。这在AnyConnect配置文件需要匹配一个适当的DNS条目并且需要包括在<hostname>下。

```
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

注意您的在建议的PRF/integrity设置需要匹配什么您的证书支持。这典型地是SHA-1。

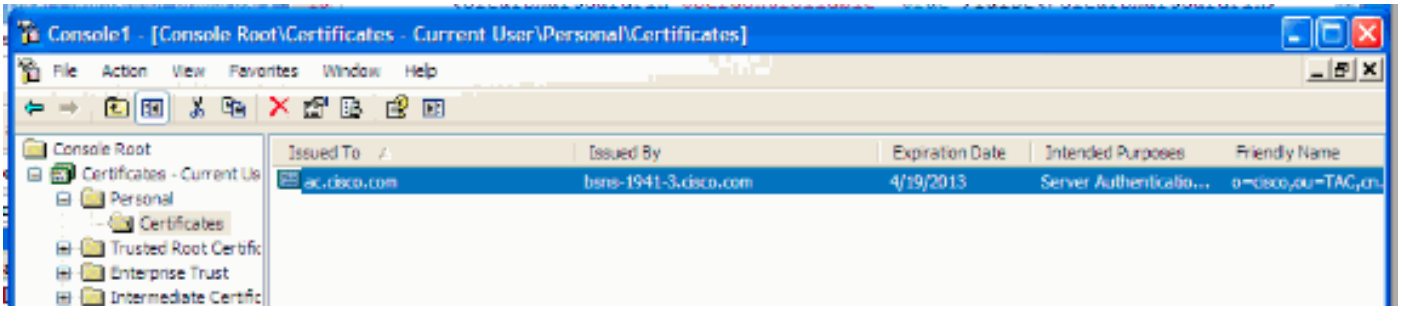
```
crypto ikev2 authorization policy AC
pool AC

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

成功的AnyConnect连接的客户端配置与IKEv2和证书包括两部分。

证书登记

当认证适当地被登记时，您能验证是存在机器或私有存储。切记客户端证书也需要有EKU。



AnyConnect配置文件

AnyConnect配置文件是较和非常基本的。

相关部分将定义：

1. 您连接的主机
2. 协议的类型
3. 将使用的认证，当连接到该主机

使用什么：

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

在AnyConnect的连接字段您需要提供充分的FQDN，是在<hostname>看到的值。

连接验证

一些信息为简要起见被省略。

```
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)
```

下一代密码学

上述配置提供供参考显示一个最小的工作配置。Cisco推荐尽可能使用下一代密码学(NGC)。

可以找到对迁移的当前推荐这里
：http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

当选择NGC配置时，请切记客户端软件和数据转发器硬件技术支持它。ISR生成2和ASR 1000路由器建议使用作为数据转发器由于他们的NGC的硬件技术支持。

在AnyConnect边，根据AnyConnect 3.1版本， NSA的套件B支持算法套件。

已知警告和问题

- 切记有在您的IOS数据转发器配置的此线路：**没有crypto ikev2 http URL cert**。IOS和

AnyConnect产生的错误，当没有配置时这是相当令人误解的。

- 与IKEv2会话的早期的IOS 15.2M&T软件也许不为RSA-SIG认证出来。这能与Cisco Bug ID CSCtx31294 (仅限注册用户)有关。保证运行最新的15.2M或15.2T软件。
- 在某些情况下IOS也许不能选择正确的信任点验证。Cisco知道问题，并且自15.2(3)T1和15.2(4)M1版本是固定的。
- 如果AnyConnect报告消息类似于此：

```
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)
```

然后，您需要确信，在您的IKEv2建议匹配的integrity/PRF设置什么您的证书能处理。在以上的配置示例中，使用SHA-1。

Related Information

- Technical Support & Documentation - Cisco Systems