Exemplo de Configuração do AnyConnect to IOS Headend Over IPsec com IKEv2 e Certificados

Contents

Introduction

Este documento fornece informações sobre como obter uma conexão protegida por IPsec de um dispositivo que executa o cliente AnyConnect para um roteador Cisco IOS® com somente autenticação de certificado utilizando a estrutura FlexVPN.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- FlexVPN
- AnyConnect

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

Headend

O roteador Cisco IOS pode ser qualquer roteador capaz de executar IKEv2, executando pelo menos 15,2 versão M&T. No entanto, deve utilizar uma versão mais recente (ver a seção advertências conhecidas), se disponível.

Cliente

Versão do AnyConnect 3.x

Autoridade de certificação

Neste exemplo, a autoridade de certificação (CA) executará a versão 15.2(3)T.

Écrucial que uma das versões mais recentes seja usada devido à necessidade de suporte ao EKU (Extended Key Usage, uso de chave estendida).

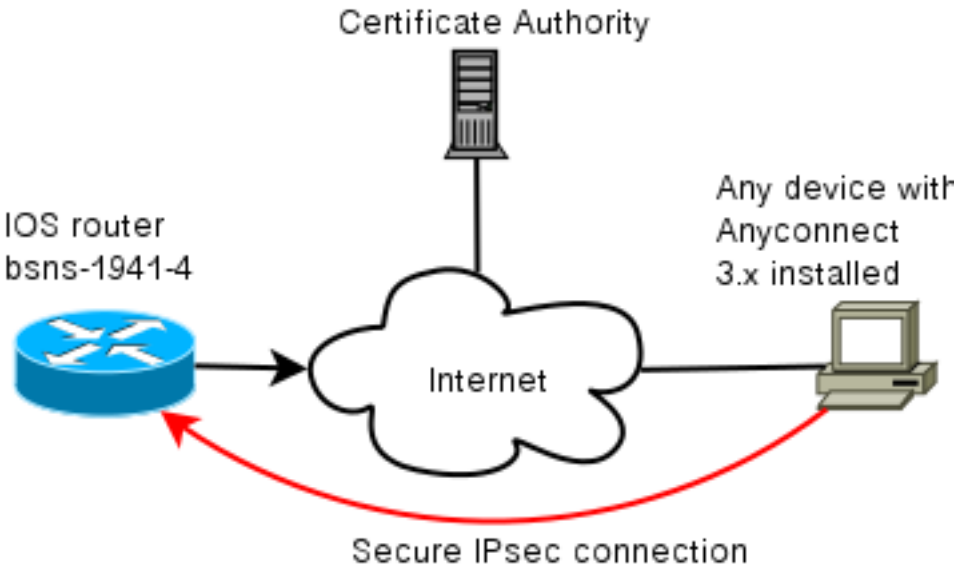
Nesta implantação, o roteador IOS é usado como CA. No entanto, qualquer aplicação CA baseada em padrões capaz de utilizar EKU deve ser aceitável.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configuração

Topologia de rede



Autoridade de certificação (opcional)

Se você optar por usá-lo, o roteador do IOS poderá atuar como uma CA.

configuração de CA do IOS

Lembre-se de que o servidor CA deve colocar o EKU correto nos certificados do cliente e do servidor. Nesse caso, EKU de autenticação de servidor e autenticação de cliente foram definidas para todos os certificados.

```
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
```

Como verificar se a EKU correta foi definida no certificado

Observe que bsns-1941-3 é o servidor CA, enquanto bsns-1941-4 é o headend IPsec. Partes da saída omitidas para brevidade.

```
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...)
```

Configuração do Headend

A configuração do headend é composta por duas partes: a parte PKI e o flex/IKEv2 real.

configuração de PKI

Você observará que o CN do bsns-1941-4.cisco.com é usado. Isso precisa corresponder a uma entrada de DNS apropriada e precisa ser incluído no perfil do AnyConnect em <Nome do host>.

```
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
```

Configuração de criptografia/IPsec

Observe que sua configuração de PRF/integridade na proposta PRECISA corresponder ao que seu certificado suporta. Normalmente é 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
```

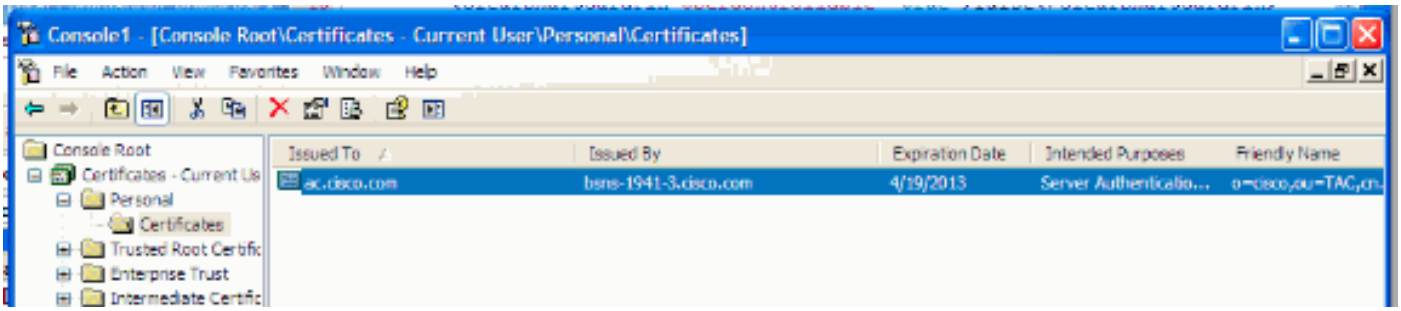
```
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint CISCO2
aaa authorization group cert list default AC
virtual-template 1

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
```

Cliente

A configuração do cliente para uma conexão bem-sucedida do AnyConnect com IKEv2 e certificados consiste em duas partes.

Inscrição de certificado

Quando o certificado estiver corretamente inscrito, você poderá verificar se ele está presente na máquina ou no armazenamento pessoal. Lembre-se de que os certificados de cliente também precisam ter EKU.



perfil do AnyConnect

O perfil do AnyConnect é longo e muito básico.

A parte relevante é definir:

1. Host ao qual você está se conectando
2. Tipo de protocolo
3. Autenticação a ser usada quando conectada a esse host

O que é usado:

```
<ServerList>
<HostEntry>
<HostName>bsns-1941-4.cisco.com</HostName>
<PrimaryProtocol>IPsec
```

```
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>
IKE-RSA
</AuthMethodDuringIKENegotiation>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

No campo de conexão do AnyConnect, você precisa fornecer o FQDN completo, que é o valor visto em `<HostName>`.

Verificação de conexão

Algumas informações são omitidas para ser breve.

```
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)
```

Criptografia de próxima geração

A configuração acima é fornecida como referência para mostrar uma configuração de trabalho mínima. A Cisco recomenda o uso da criptografia de próxima geração (NGC) onde possível.

As recomendações atuais para migração podem ser encontradas aqui: http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Ao escolher a configuração da NGC, certifique-se de que o software cliente e o hardware de headend o suportem. Os roteadores ISR geração 2 e ASR 1000 são recomendados como headends devido ao suporte de hardware para NGC.

No lado do AnyConnect, a partir da versão 3.1 do AnyConnect, o conjunto de algoritmos Suite B da NSA é suportado.

Problemas conhecidos

- Lembre-se de ter esta linha configurada no headend do IOS: **no crypto ikev2 http-url cert**. O erro produzido pelo IOS e pelo AnyConnect quando não está configurado é bastante enganador.
- O software IOS 15.2M&T anterior com sessão IKEv2 pode não aparecer para autenticação RSA-SIG. Isso pode estar relacionado à ID de bug da Cisco CSCtx31294 (somente clientes registrados) . Execute o software 15.2M ou 15.2T mais recente.
- Em determinados cenários, o IOS pode não ser capaz de escolher o ponto de confiança correto para autenticar. A Cisco está ciente do problema e ele é corrigido a partir das versões 15.2(3)T1 e 15.2(4)M1.
- Se o AnyConnect estiver relatando uma mensagem semelhante a esta:
  ```
  The client certificate's cryptographic service provider(CSP)
  does not support the sha512 algorithm
  ```

Em seguida, você precisa certificar-se de que a configuração de integridade/PRF em suas propostas de IKEv2 corresponda ao que seus certificados podem lidar. No exemplo de configuração acima, SHA-1 é usado.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems