AnyConnect ao final do cabeçalho IO sobre o IPsec com IKEv2 e exemplo de configuração dos Certificados

Índice

Introdução

Este documento fornece a informação em como conseguir uma conexão IPsec-protegida de um dispositivo que execute o cliente de AnyConnect a um roteador do ® do Cisco IOS com somente certificado de autenticação utilizando a estrutura de FlexVPN.

Pré-requisitos

Requisitos

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:

Final do cabeçalho

O roteador do Cisco IOS pode ser todo o roteador capaz de executar IKEv2, executando pelo menos a liberação 15.2 M&T. Contudo, você deve usar uma liberação mais nova (veja a seção das advertências conhecidas), se disponível.

Cliente

Liberação de AnyConnect 3.x

Certificate Authority

Neste exemplo, o Certificate Authority (CA) estará executando a liberação 15.2(3)T.

Écrucial que uma das liberações mais novas está usado devido à necessidade de apoiar o uso chave prolongado (EKU).

Neste desenvolvimento, o IOS Router é usado como CA. Contudo, todo o aplicativo com base em padrões de CA capaz de usar o EKU deve ser fino.

Convenções

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

Configuração

Topologia de rede

Certificate Authority (opcional)

Se você escolhe a usar, seu IOS Router pode atuar como CA.

Configuração IO CA

Você precisa de recordar que o server de CA deve pôr o EKU correto sobre os Certificados de cliente e servidor. Neste caso o server-AUTH e o cliente-AUTH EKU foram ajustados 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 correto o EKU foi ajustado no certificado

Note que bsns-1941-3 é o server de CA quando bsns-1941-4 for o final do cabeçalho do IPsec. Partes da saída omitidas para a 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 final do cabeçalho

A configuração do final do cabeçalho é compreendida de duas porções: a peça PKI e o flex/IKEv2 real.

Configuração PKI

Você observará que o CN de bsns-1941-4.cisco.com está usado. Isto precisa de combinar uma entrada de DNS apropriada e precisa de ser incluído no perfil de AnyConnect sob o <hostname>.

```
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
```

Cripto/configuração IPSec

Note que seu ajuste PRF/integrity na proposta **PRECISA** de combinar que seus suportes de certificado. Este é tipicamente 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 de cliente para uma conexão bem sucedida de AnyConnect com o IKEv2 e os Certificados consiste em duas porções.

Certificado de registro

Quando o certificado é registrado corretamente, você pode verificar que esta presente na máquina ou na loja pessoal. Recorde que os certificados de cliente igualmente precisam de ter o EKU.

Perfil de AnyConnect

O perfil de AnyConnect é longo e muito básico.

A parte relevante é definir:

1. Host que você está conectando a
2. Tipo de protocolo
3. Autenticação a ser usada quando conectado 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 da conexão de AnyConnect você precisa de fornecer o FQDN completo, que é o valor visto no `<hostname>`.

Verificação da conexão

Alguma informação é omitida para a brevidade.

```
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 da próxima geração

A configuração acima é fornecida para que a referência mostre uma configuração em funcionamento mínima. Cisco recomenda usar a criptografia da próxima geração (NGC) sempre que seja possível.

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

Ao escolher a configuração NGC, certifique-se de que software do cliente e suporte a hardware do final do cabeçalho ele. A geração 2 ISR e os 1000 Router ASR são recomendados como finais do cabeçalho devido a seu suporte a hardware para NGC.

No lado de AnyConnect, até à data da versão de AnyConnect 3.1, a série do algoritmo da série B do NSA é apoiada.

Advertências conhecidas e edições

- Recorde ter esta linha configurada em seu final do cabeçalho IO: **nenhum CERT cripto do URL do HTTP ikev2**. O erro produzido por IO e por AnyConnect quando este não é configurado é bastante enganador.
- O software adiantado IO 15.2M&T com sessão IKEv2 não pôde vir acima para a autenticação RSA-SIG. Isto pode ser relacionado à identificação de bug Cisco CSCtx31294 (clientes registrados somente). Certifique-se executar o 15.2M ou o software 15.2T o mais atrasado.
- Em determinadas encenações os IO não puderam poder escolher o ponto confiável correto para autenticar. Cisco está ciente da edição, e é fixa até à data das liberações 15.2(3)T1 e

15.2(4)M1.

- Se AnyConnect está relatando uma mensagem similar a esta:

```
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)
```

Então, você precisa de certificar-se de que o ajuste integrity/PRF em seu fósforo das propostas IKEv2 o que seus Certificados podem segurar. No exemplo de configuração acima, o SHA-1 é usado.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems