AnyConnect met IOS Head-end over IPsec met IKEv2 en Configuratievoorbeeld voor certificaten

Inhoud

Inleiding

Dit document geeft informatie over hoe u een IPsec-beschermde verbinding kunt bereiken vanaf een apparaat dat AnyConnect-client naar een Cisco IOS® router draait met alleen certificatie door gebruik van FlexVPN-kader.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FlexVPN
- AnyConnect

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

Head-end

Cisco IOS-router kan elke router zijn die IKEv2 kan uitvoeren en die op zijn minst 15.2 M&T-release heeft. U dient echter een nieuwere release te gebruiken (zie het bekende gedeelte met voorbehouden), indien beschikbaar.

Clientclient

AnyConnect 3.x release

Certificaatinstantie

In dit voorbeeld, zal de certificeringsinstantie (CA) 15.2(3)T vrijgave uitvoeren.

Het is van cruciaal belang dat één van de nieuwe introducties wordt gebruikt vanwege de noodzaak om het gebruik van de Extended Key Use (EKU) te ondersteunen.

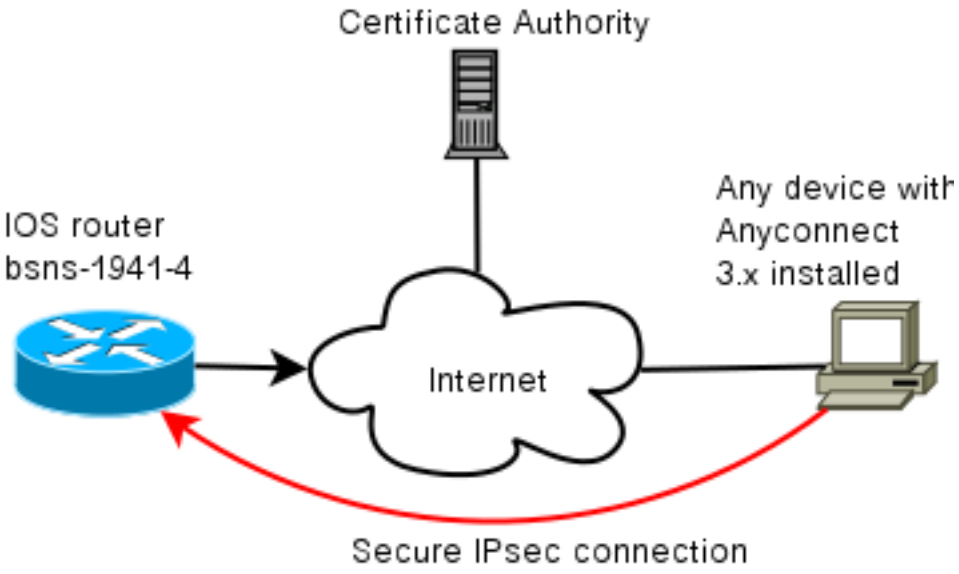
In deze plaatsing, wordt de IOS router gebruikt als CA. Een op standaarden gebaseerde CA-toepassing die gebruik kan maken van EKU moet echter wel in orde zijn.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configuratie

Netwerktopologie



Certificaat-instantie (optioneel)

Als u ervoor kiest om het te gebruiken, kan uw IOS router als CA fungeren.

IOS CA-configuratie

U moet onthouden dat de CA server de juiste EKU op de client en server certificaten moet plaatsen. In dit geval werden server-auth en client-auth EKU ingesteld voor alle certificaten.

```
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
```

Hoe werd geverifieerd of de juiste EKU op het certificaat was ingesteld

Merk op dat bsns-1941-3 de CA server is terwijl bsns-1941-4 de IPsec head-end is. Gedeelten van de output die zijn weggelaten voor de beknoptheid.

```
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...)
```

Head-end-configuratie

De configuratie van het hoofd bestaat uit twee delen: het PKI-gedeelte en de eigenlijke flex/IKEv2.

PKI-configuratie

Het zal jullie opvallen dat CN van bsns-1941-4.cisco.com wordt gebruikt. Dit moet overeenkomen met een juiste DNS-ingang en moet in het AnyConnect-profiel onder **<Hostname>** worden opgenomen.

```
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
```

Configuratie Crypto/IPsec

Merk op dat uw PRF/integriteitsinstelling in het voorstel overeenkomt met wat uw certificaat ondersteunt. Dit is doorgaans 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
```

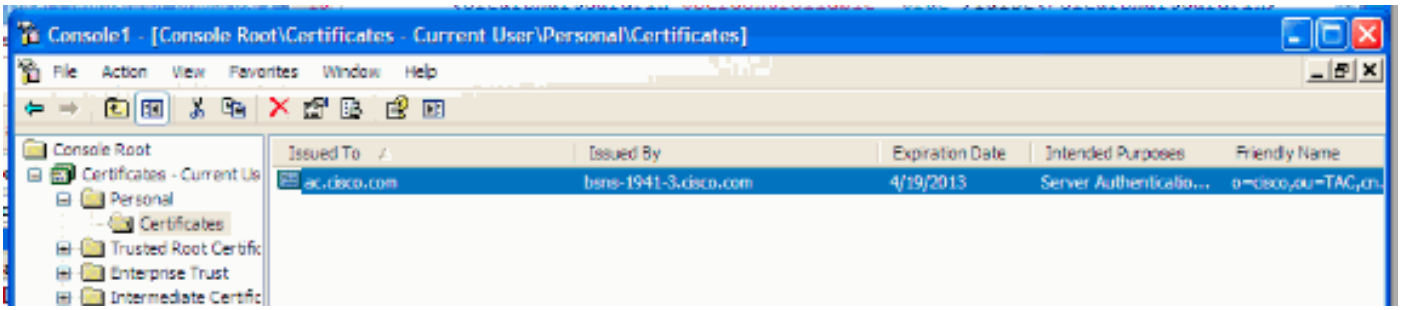
```
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint CISCO2
aaa authorization group cert list default AC
virtual-template 1

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
```

Clientclient

Clientconfiguratie voor een succesvolle AnyConnect-verbinding met IKEv2 en certificaten bestaat uit twee delen.

Certificaatinschrijving

Wanneer het certificaat naar behoren wordt ingevoerd, kunt u controleren of het in machine- of persoonlijke winkel is. Denk eraan dat ook EKU voor cliëntencertificaten nodig is.



AnyConnect-profiel

Het AnyConnect-profiel is lang en zeer eenvoudig.

Het relevante deel is het definiëren van:

1. Host waarop u een verbinding maakt
2. Type protocol
3. Verificatie die moet worden gebruikt bij aansluiting op die host

Wat wordt gebruikt:

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

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

In het verbindingsveld van AnyConnect moet u de volledige FQDN leveren, de waarde die in `<HostName>` wordt gezien.

Verificatie van aansluiting

Sommige informatie wordt weggelaten vanwege de beknoptheid.

```
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)
```

volgende generatie cryptografie

De bovenstaande configuratie is voorzien om een minimale werkconfiguratie te tonen. Cisco raadt het gebruik van cryptografie van de volgende generatie (NGC) aan wanneer mogelijk.

De huidige aanbevelingen voor migratie zijn hier te vinden: http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Zorg er bij het kiezen van een NGC-configuratie voor dat zowel de clientsoftware als de head-end hardware deze ondersteunen. Routers voor ISR-generatie 2 en ASR 1000 worden aanbevolen als head-end vanwege hun hardwareondersteuning voor NGC.

Aan de AnyConnect-zijde wordt, zoals beschreven in de AnyConnect 3.1-versie, de Suite B-algoritmische reeks van de NSA ondersteund.

Bekende voorbehouden en kwesties

- Vergeet niet deze lijn op uw IOS-head-end te hebben ingesteld: **geen crypto ikev2 http-url cert**. De fout die door IOS en AnyConnect wordt gemaakt wanneer dit niet wordt geconfigureerd is misleidend.
- Eerdere IOS 15.2M&T-software met IKEv2-sessie kan mogelijk niet voor RSA-SIG verificatie verschijnen. Dit kan worden gerelateerd aan Cisco bug-ID CSCtx31294 (alleen geregistreerde klanten). Draai de nieuwste 15.2M- of 15.2T-software.
- In bepaalde scenario's kan IOS niet het juiste betrouwbare punt kiezen om authentiek te verklaren. Cisco is zich bewust van het probleem en het is vastgesteld op 15.2(3)T1 en 15.2(4)M1 releases.
- Als AnyConnect een vergelijkbaar bericht meldt:
  ```
  The client certificate's cryptographic service provider(CSP)
  does not support the sha512 algorithm
  ```

Vervolgens moet u ervoor zorgen dat de instellingen voor integriteit/PRF in uw IKEv2-voorstellen overeenkomen met wat uw certificaten kunnen verwerken. In het bovenstaande configuratievoorbeeld wordt SHA-1 gebruikt.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems