AnyConnect au Headend IOS au-dessus d'IPsec avec IKEv2 et exemple de configuration de Certificats

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Configuration
Topologie du réseau
Autorité de certification (facultative)
Configuration IOS CA
Comment vérifier si correct EKU a été placé sur le certificat
Configuration de Headend
Configuration de PKI
Configuration crypto/IPsec
Client
Inscription de certificat
Profil d'AnyConnect
Vérification de connexion
Chiffrement de nouvelle génération
Mises en garde et questions connues
Informations connexes

Introduction

Ce document fournit des informations sur la façon dont réaliser une connexion IPsec-protégée d'un périphérique qui exécute le client d'AnyConnect à un routeur de Cisco IOS® avec seulement l'authentification de certificat en utilisant le cadre de FlexVPN.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FlexVPN
- AnyConnect

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

Headend

Le routeur Cisco IOS peut être n'importe quel routeur capable d'exécuter IKEv2, exécutant au moins la release 15.2 M&T. Cependant, vous devriez utiliser une plus nouvelle release (voyez la section connue de mises en garde), si disponible.

Client

Release d'AnyConnect 3.x

Autorité de certification

Dans cet exemple, l'Autorité de certification (CA) exécutera la release 15.2(3)T.

Il est crucial qu'une des releases plus nouvelles soit utilisée en raison de la nécessité de prendre en charge l'utilisation principale étendue (EKU).

Dans ce déploiement, le routeur IOS est utilisé comme CA. Cependant, n'importe quelle application basée sur des standards CA capable d'utiliser EKU devrait être bon.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration

Topologie du réseau

Autorité de certification (facultative)

Si vous choisissez de l'utiliser, votre routeur IOS peut agir en tant que CA.

Configuration IOS CA

Vous devez se souvenir que le serveur CA doit mettre l'EKU correct sur les Certificats de client et serveur. Dans ce cas le serveur-auth et le client-auth EKU ont été placés pour tous les Certificats.

```
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
```

Comment vérifier si correct EKU a été placé sur le certificat

Notez que bsns-1941-3 est le serveur CA tandis que bsns-1941-4 est le headend d'IPsec. Parties de sortie omises par souci de concision.

```
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...)
```

Configuration de Headend

La configuration de Headend est composée de deux parts : la pièce et l'effectif flex/IKEv2 de PKI.

Configuration de PKI

Vous noterez que la NC de bsns-1941-4.cisco.com est utilisée. Ceci doit apparier une entrée DNS appropriée et doit être inclus dans le profil d'AnyConnect sous le <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
```

Configuration crypto/IPsec

Notez que votre configuration PRF/integrity dans la proposition **DOIT** apparier ce que votre certificat prend en charge. C'est typiquement 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
```

Client

La configuration de client pour une connexion réussie d'AnyConnect avec IKEv2 et Certificats se compose de deux parts.

Inscription de certificat

Quand le certificat est correctement inscrit, vous pouvez vérifier qu'il est présent dans l'ordinateur ou la mémoire personnelle. Souvenez-vous que les certificats client doivent également avoir EKU.

Profil d'AnyConnect

Le profil d'AnyConnect est prolongé et très de base.

L'élément pertinent doit définir :

1. Hôte que vous connectez à
2. Type de protocole
3. Authentification à utiliser une fois connecté à cet hôte

Ce qui est utilisé :

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

Dans le domaine de connexion d'AnyConnect vous devez fournir le plein FQDN, qui est la valeur vue dans le `<HostName>`.

Vérification de connexion

Quelques informations sont omises par souci de concision.

```
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)
```

Chiffrement de nouvelle génération

La configuration ci-dessus est donnée pour la référence pour afficher une configuration en cours minimale. Cisco recommande utilisant le chiffrement de nouvelle génération (NGC) si possible.

Des recommandations en cours pour le transfert peuvent être trouvées ici : http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

En choisissant la configuration NGC, assurez-vous que logiciel client et support matériel de headend il. Les Routeurs 2 et ASR 1000 de génération ISR sont recommandés comme headends en raison de leur support matériel pour NGC.

Du côté d'AnyConnect, en date de la version d'AnyConnect 3.1, la suite d'algorithme de la suite B du NSA est prise en charge.

Mises en garde et questions connues

- Souvenez-vous pour avoir cette ligne configurée sur votre headend IOS : **aucun crypto CERT HTTP-URL ikev2**. L'erreur produite par l'IOS et l'AnyConnect quand ceci n'est pas configuré est tout à fait fallacieuse.
- Le logiciel tôt IOS 15.2M&T avec la session IKEv2 ne pourrait pas être soulevé pour l'authentification RSA-SIG. Ceci peut être lié à l'ID de bogue Cisco CSCtx31294 (clients enregistrés seulement). Veillez à exécuter le dernier 15.2M ou logiciel 15.2T.
- Dans certains scénarios l'IOS ne pourrait pas pouvoir sélectionner le point de confiance correct pour authentifier. Cisco se rend compte de la question, et elle est réparée en date des releases 15.2(3)T1 et 15.2(4)M1.
- Si AnyConnect signale un message semblable à ceci :
  ```
  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)
```

Puis, vous devez s'assurer que la configuration integrity/PRF dans votre correspondance des propositions IKEv2 ce que vos Certificats peuvent manipuler. Dans l'exemple de configuration ci-dessus, SHA-1 est utilisé.

Informations connexes

- Support et documentation techniques - Cisco Systems