Exemple de configuration d'AnyConnect à IOS Headend Over IPsec avec IKEv2 et certificats

Contenu

Introduction

Ce document fournit des informations sur la façon d'établir une connexion protégée par IPsec à partir d'un périphérique qui exécute un client AnyConnect sur un routeur Cisco IOS® avec authentification de certificat uniquement à l'aide de la structure FlexVPN.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FlexVPN
- AnyConnect

Components Used

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

Tête de réseau

Le routeur Cisco IOS peut être n'importe quel routeur capable d'exécuter IKEv2, exécutant au moins 15.2 version M&T. Cependant, vous devez utiliser une version plus récente (voir la section Avertissements connus), si disponible.

Client

Version AnyConnect 3.x

Autorité de certification

Dans cet exemple, l'autorité de certification exécute la version 15.2(3)T.

Il est essentiel que l'une des nouvelles versions soit utilisée en raison de la nécessité de prendre en charge l'utilisation de clé étendue (EKU).

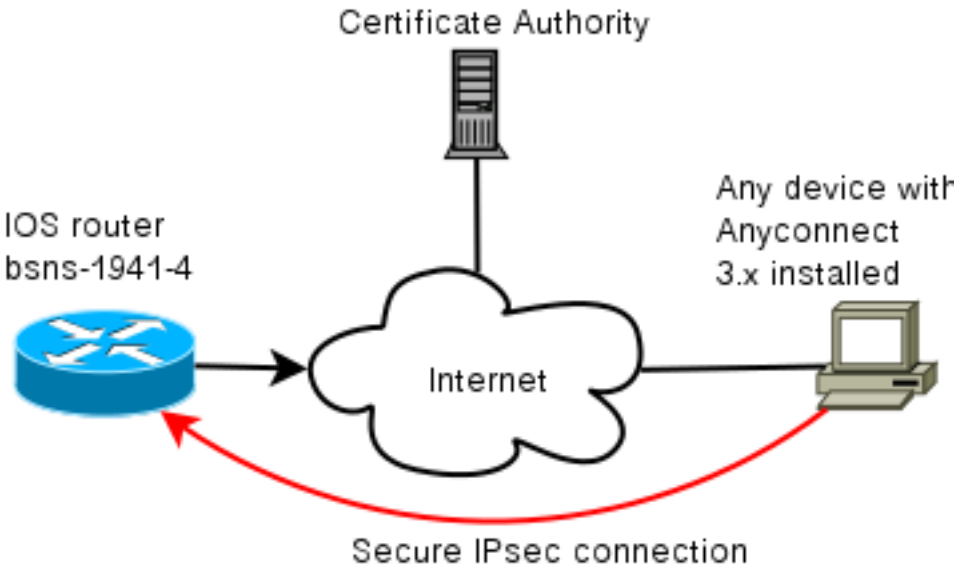
Dans ce déploiement, le routeur IOS est utilisé comme autorité de certification. Cependant, toute application CA normalisée capable d'utiliser EKU doit être correcte.

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 (facultatif)

Si vous choisissez de l'utiliser, votre routeur IOS peut agir en tant qu'autorité de certification.

Configuration de l'autorité de certification IOS

Vous devez vous rappeler que le serveur AC doit placer l'EKU correct sur les certificats client et serveur. Dans ce cas, l'EKU server-auth et client-auth ont été définis 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 l'EKU correct a été défini sur le certificat

Notez que bsns-1941-3 est le serveur AC tandis que bsns-1941-4 est la tête de réseau IPsec. Parties de la sortie omises pour plus 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 tête de réseau

La configuration de tête de réseau comprend deux parties : la partie PKI et la partie réelle flex/IKEv2.

Configuration PKI

Vous remarquerez que le CN de bsns-1941-4.cisco.com est utilisé. Cela doit correspondre à une entrée DNS correcte et doit être inclus dans le profil AnyConnect sous **<Nom d'hôte>**.

```
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 paramètre PRF/intégrité dans la proposition **DOIT** correspondre à ce que votre certificat prend en charge. Il s'agit généralement de 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
```

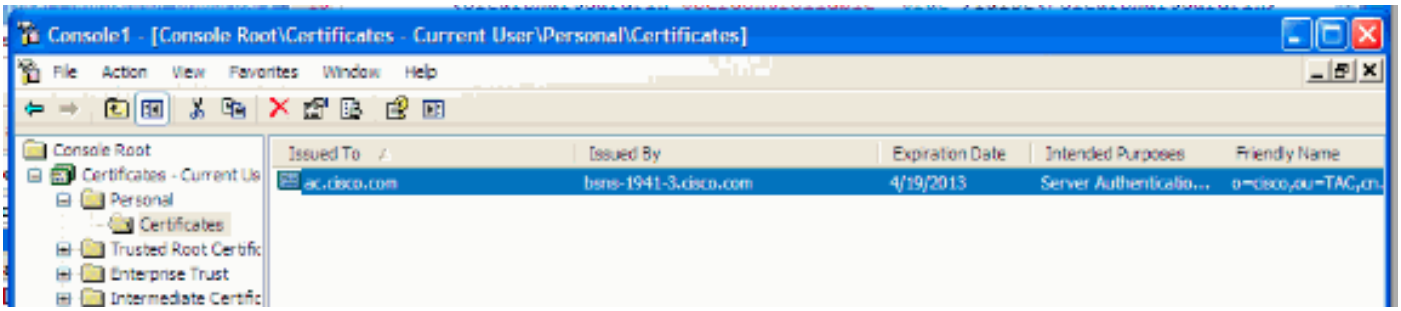
```
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint CISCO2
aaa authorization group cert list default AC
virtual-template 1

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 du client pour une connexion AnyConnect réussie avec IKEv2 et les certificats se compose de deux parties.

Inscription de certificat

Lorsque le certificat est correctement inscrit, vous pouvez vérifier qu'il est présent dans l'ordinateur ou dans le magasin personnel. N'oubliez pas que les certificats clients doivent également avoir EKU.



Profil AnyConnect

Le profil AnyConnect est long et très basique.

La partie pertinente est de définir :

1. Hôte auquel vous vous connectez
2. Type de protocole
3. Authentification à utiliser lors de la connexion 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 champ de connexion d'AnyConnect, vous devez fournir le nom de domaine complet (FQDN), qui correspond à la valeur affichée dans `<HostName>`.

Vérification de la connexion

Certaines 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)
```

Cryptographie de nouvelle génération

La configuration ci-dessus est fournie à titre de référence pour montrer une configuration de travail minimale. Cisco recommande d'utiliser la cryptographie de nouvelle génération (NGC) dans la mesure du possible.

Les recommandations actuelles concernant la migration sont disponibles ici : http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Lors du choix de la configuration NGC, assurez-vous que le logiciel client et le matériel de tête de réseau le prennent en charge. Les routeurs ISR de 2e génération et ASR 1000 sont recommandés comme têtes de réseau en raison de leur prise en charge matérielle des NGC.

Du côté d'AnyConnect, depuis la version 3.1 d'AnyConnect, la suite d'algorithmes de la suite B de NSA est prise en charge.

Causes et problèmes connus

- N'oubliez pas que cette ligne est configurée sur votre tête de réseau IOS : **no crypto ikev2 http-url cert**. L'erreur produite par IOS et AnyConnect lorsqu'elle n'est pas configurée est tout à fait trompeuse.
- Les premiers logiciels IOS 15.2M&T avec la session IKEv2 risquent de ne pas être disponibles pour l'authentification RSA-SIG. Ceci peut être lié à l'ID de bogue Cisco CSCtx31294 (clients enregistrés uniquement). Assurez-vous d'exécuter le dernier logiciel 15.2M ou 15.2T.
- Dans certains scénarios, IOS peut ne pas être en mesure de sélectionner le point de confiance correct à authentifier. Cisco est au courant du problème et il est corrigé à partir des versions 15.2(3)T1 et 15.2(4)M1.
- Si AnyConnect signale un message similaire à celui-ci :
  ```
  The client certificate's cryptographic service provider(CSP)
  does not support the sha512 algorithm
  ```

Ensuite, vous devez vous assurer que le paramètre intégrité/PRF de vos propositions IKEv2 correspond à ce que vos certificats peuvent gérer. Dans l'exemple de configuration ci-dessus, SHA-1 est utilisé.

Informations connexes

- Support et documentation techniques - Cisco Systems