AnyConnect au-dessus d'IKEv2 à l'ASA avec l'AAA et l'authentification de certificat

Contenu

Introduction

Ce document décrit comment connecter un PC à une appliance de sécurité adaptable Cisco (ASA) à l'utilisation d'AnyConnect IPsec (IKEv2) aussi bien que le délivrer un certificat et authentification d'Authentification, autorisation et comptabilité (AAA).

> **Note**: L'exemple qui est fourni dans ce document décrit seulement les éléments pertinents qui sont utilisés afin d'obtenir une connexion IKEv2 entre l'ASA et l'AnyConnect. Un exemple de configuration complète n'est pas fourni. Le Traduction d'adresses de réseau (NAT) ou la configuration de liste d'accès n'est pas décrit ou est exigé dans ce document.

Préparez-vous à la connexion

Cette section décrit les perparations qui sont exigés avant que vous puissiez connecter votre PC à l'ASA.

Certificats avec EKU approprié

Il est important de noter que quoiqu'on ne l'exige pas pour la combinaison ASA et d'AnyConnect, le RFC exige que les Certificats ont étendu l'utilisation principale (EKU) :

- Le certificat pour l'ASA doit contenir le **serveur-auth** EKU.
- Le certificat pour le PC doit contenir le **client-auth** EKU.

Note: Un routeur IOS avec la révision de logiciel récente peut placer EKUs sur des Certificats.

Configuration sur l'ASA

Cette section décrit les configurations ASA qui sont exigées avant que la connexion se produise.

Note: Le Cisco Adaptive Security Device Manager (ASDM) te permet pour créer la configuration de base avec seulement quelques clics. Cisco recommande que vous l'employiez afin d'éviter des erreurs.

Configuration de crypto map

Voici un exemple de configuration de crypto map :

```
crypto dynamic-map DYN 1 set pfs group1
crypto dynamic-map DYN 1 set ikev2 ipsec-proposal secure
crypto dynamic-map DYN 1 set reverse-route
crypto map STATIC 65535 ipsec-isakmp dynamic DYN
crypto map STATIC interface outside
```

Propositions d'IPsec

Voici un exemple de configuration de proposition d'IPsec :

```
crypto dynamic-map DYN 1 set pfs group1
crypto dynamic-map DYN 1 set ikev2 ipsec-proposal secure
crypto dynamic-map DYN 1 set reverse-route
crypto map STATIC 65535 ipsec-isakmp dynamic DYN
crypto map STATIC interface outside
```

Stratégies IKEv2

Voici un exemple de configuration de la stratégie IKEv2 :

```
crypto dynamic-map DYN 1 set pfs group1
crypto dynamic-map DYN 1 set ikev2 ipsec-proposal secure
crypto dynamic-map DYN 1 set reverse-route
crypto map STATIC 65535 ipsec-isakmp dynamic DYN
crypto map STATIC interface outside
```

Services clientèle et certificat

Vous devez activer des services clientèle et des Certificats sur l'interface appropriée, qui est l'interface extérieure dans ce cas. Voici un exemple de configuration :

```
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint OUTSIDE
ssl trust-point OUTSIDE outside
```

Note: Le même point de confiance est également assigné pour Secure Sockets Layer (SSL),

qui est destiné et exigé.

Profil d'AnyConnect d'enable

Vous devez activer le profil d'AnyConnect sur l'ASA. Voici un exemple de configuration :

```
webvpn
 enable outside
anyconnect image disk0:/anyconnect-win-3.0.5080-k9.pkg 1 regex "Windows NT"
anyconnect profiles Anyconnect disk0:/anyconnect.xml
 anyconnect enable
tunnel-group-list enable
```

Nom d'utilisateur, stratégie de groupe, et groupe de tunnels

Voici un exemple de configuration pour un nom d'utilisateur, une stratégie de groupe, et un groupe de tunnels de base sur l'ASA :

```
group-policy GroupPolicy_AC internal
group-policy GroupPolicy_AC attributes
 dns-server value 4.2.2.2
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
default-domain value cisco.com
webvpn
anyconnect profiles value Anyconnect type user
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15
tunnel-group AC type remote-access
tunnel-group AC general-attributes
address-pool VPN-POOL
 default-group-policy GroupPolicy_AC
tunnel-group AC webvpn-attributes
 authentication aaa certificate
 group-alias AC enable
 group-url https://bsns-asa5520-1.cisco.com/AC enable
 without-csd
```

Profil d'AnyConnect

Voici un profil d'exemple avec les éléments pertinents affichés en **gras** :

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation=
 "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false
 </AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
```

```
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="true">Automatic
 </RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>bsns-asa5520-1</HostName>
<HostAddress>bsns-asa5520-1.cisco.com</HostAddress>
<UserGroup>AC</UserGroup>
<PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

Voici quelques informations importantes au sujet de cet exemple de configuration :

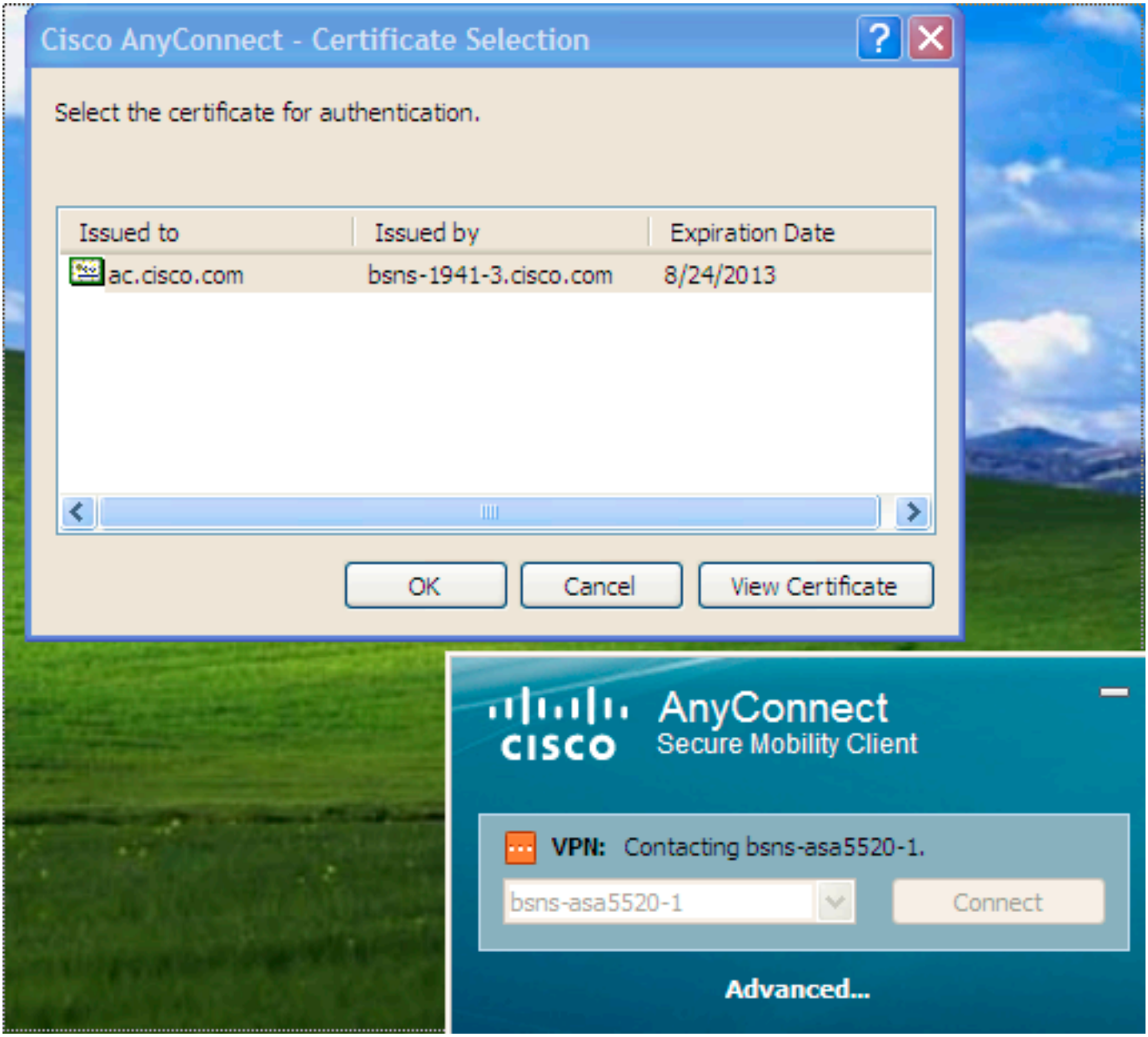
- Quand vous créez le profil, le host address doit apparier le nom de certificat (NC) sur le certificat qui est utilisé pour IKEv2. Sélectionnez la **crypto** commande de **point de confiance de la remote-access ikev2** afin de définir ceci.
- L'usergroup doit apparier le nom du tunnelgroup auquel la connexion IKEv2 tombe. S'ils ne s'assortissent pas, la connexion échoue souvent et met au point indiquent une non-concordance de groupe de Protocole DH (Diffie-Hellman) ou un faux négatif semblable.

Établissez le rapport

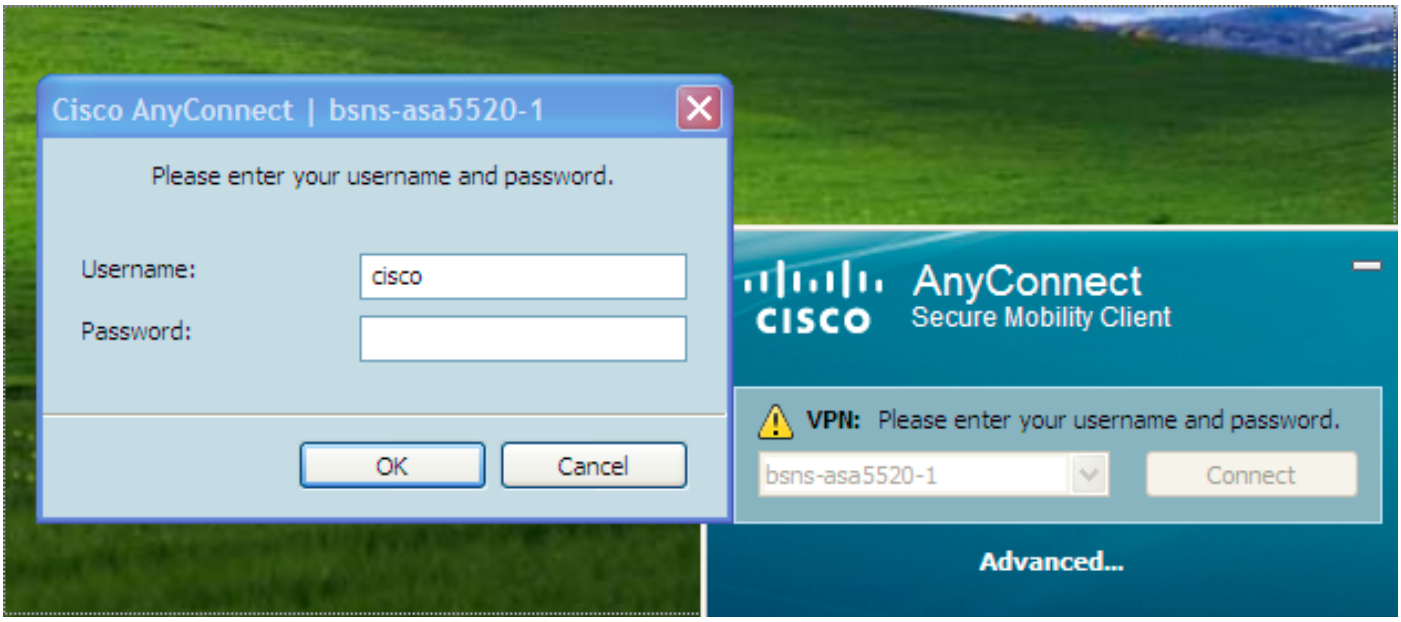
Cette section décrit la connexion PC-à-ASA quand le profil est déjà présent.

> **Note**: Les informations que vous entrez dans le GUI afin de se connecter sont la valeur de <HostName> qui est configurée dans le profil d'AnyConnect. Dans ce cas, **bsns-asa5520-1** n'est écrit, pas le nom de domaine complet complet (FQDN).

Quand vous premier essai de se connecter par AnyConnect, la passerelle vous incite à sélectionner le certificat (si automatique la sélection de certificat est désactivée) :

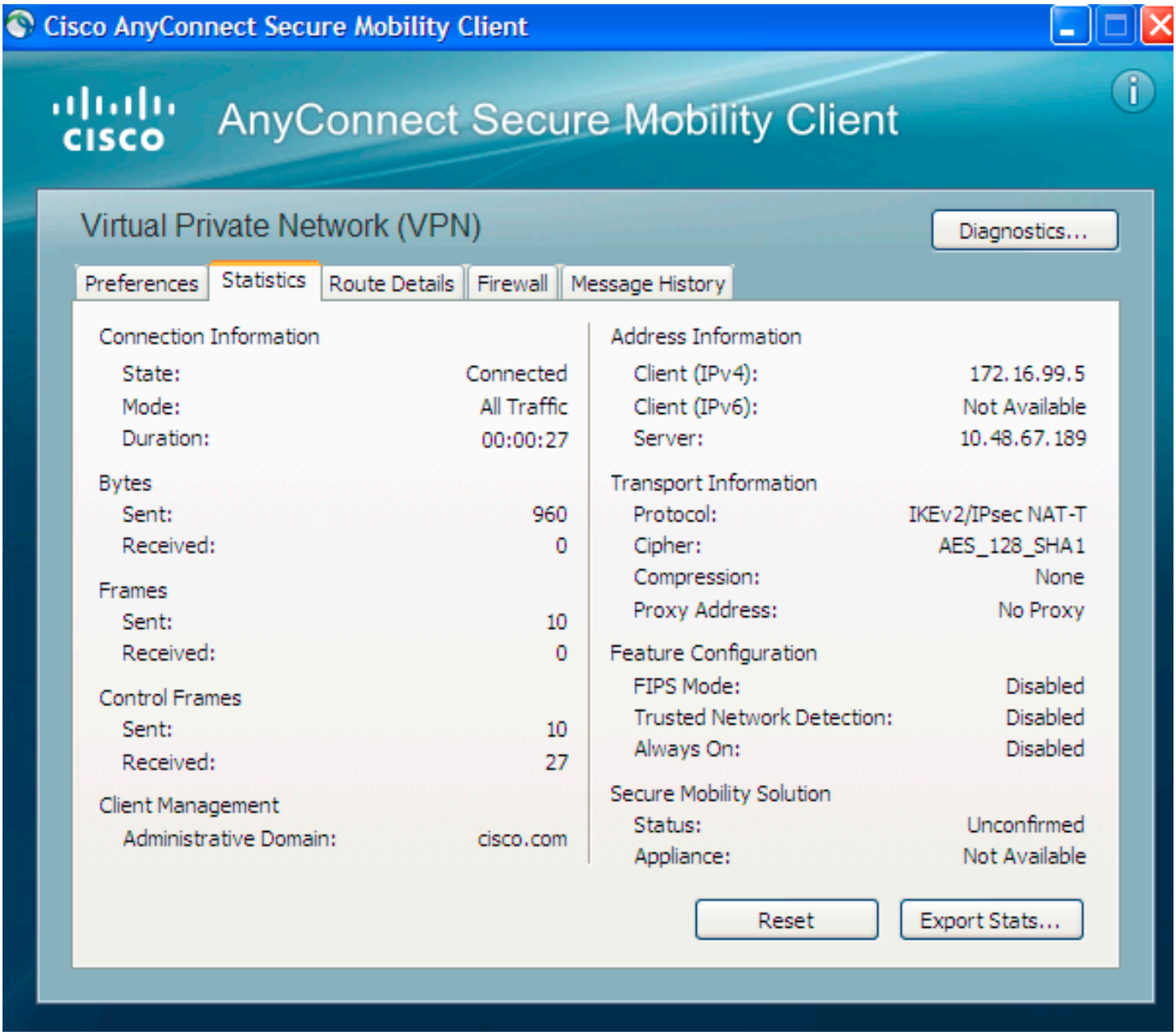


Vous devez alors écrire le nom d'utilisateur et mot de passe :



Une fois que le nom d'utilisateur et mot de passe sont reçus, la connexion est réussie et les

statistiques d'AnyConnect peuvent être vérifiées :



Vérification sur l'ASA

Sélectionnez cette commande sur l'ASA afin de vérifier que les utilisations IKEv2 de connexion aussi bien qu'AAA et authentification de certificat :

```
bsns-asa5520-1# show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed
Username : cisco Index : 6
Assigned IP : 172.16.99.5 Public IP : 1.2.3.4
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : AES256 AES128 Hashing : none SHA1 SHA1
Bytes Tx : 0 Bytes Rx : 960
Pkts Tx : 0 Pkts Rx : 10
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_AC Tunnel Group : AC
Login Time : 15:45:41 UTC Tue Aug 28 2012
Duration : 0h:02m:41s
```

```
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1
AnyConnect-Parent:
Tunnel ID : 6.1
Public IP : 1.2.3.4
Encryption : none Auth Mode : Certificate and userPassword
 Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client Type : AnyConnect
Client Ver : 3.0.08057
IKEv2:
Tunnel ID : 6.2
UDP Src Port : 60468 UDP Dst Port : 4500
Rem Auth Mode: Certificate and userPassword
 Loc Auth Mode: rsaCertificate
 Encryption : AES256 Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86238 Seconds
PRF : SHA1 D/H Group : 5
Filter Name :
Client OS : Windows
IPsecOverNatT:
Tunnel ID : 6.3
Local Addr : 0.0.0.0/0.0.0.0/0/0
Remote Addr : 172.16.99.5/255.255.255.255/0/0
Encryption : AES128 Hashing : SHA1\
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 28638 Seconds
Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Bytes Tx : 0 Bytes Rx : 960
Pkts Tx : 0 Pkts Rx : 10
```

Mises en garde connues

Ce sont les mises en garde et les questions connues qui sont liées aux informations qui sont décrites dans ce document :

- L'IKEv2 et les points de confiance SSL doivent être identique.
- Cisco recommande que vous utilisiez le FQDN comme NC pour les Certificats d'ASA-side. Assurez-vous que vous mettez en référence le même FQDN pour le <HostAddress> dans le profil d'AnyConnect.
- Souvenez-vous pour insérer la valeur de <HostName> du profil d'AnyConnect quand vous vous connectez.
- Même dans la configuration IKEv2, quand AnyConnect se connecte à l'ASA, il télécharge des mises à jour de profil et de binaire au-dessus de SSL, mais pas IPsec.
- La connexion d'AnyConnect au-dessus d'IKEv2 à l'ASA utilise l'eap-AnyConnect, un mécanisme de propriété industrielle qui permet une implémentation plus simple.