Configurez l'Accès à distance ASA IKEv2 avec EAP-PEAP et client Windows indigène

Contenu

Introduction

Ce document fournit un exemple de configuration pour une version 9.3.2 et ultérieures de l'appliance de sécurité adaptable Cisco (ASA) qui permet l'accès VPN à distance pour utiliser l'échange de clés Internet (IKE) Protocol (IKEv2) avec l'authentification standard de Protocole EAP (Extensible Authentication Protocol). Ceci permet à un client indigène de Microsoft Windows 7 (et à toute autre conformité aux normes IKEv2) pour se connecter à l'ASA à IKEv2 et à authentification EAP.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance VPN et IKEv2 de base
- Authentification, autorisation et comptabilité (AAA) et connaissance de base de RAYON
- Expérience avec la configuration du VPN ASA
- Expérience avec la configuration du Cisco Identity Services Engine (ISE)

Composants utilisés

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

- Microsoft Windows 7
- Logiciel de Cisco ASA, version 9.3.2 et ultérieures
- Cisco ISE, version 1.2 et ultérieures

Informations générales

Considérations sécurisées de client de mobilité d'AnyConnect

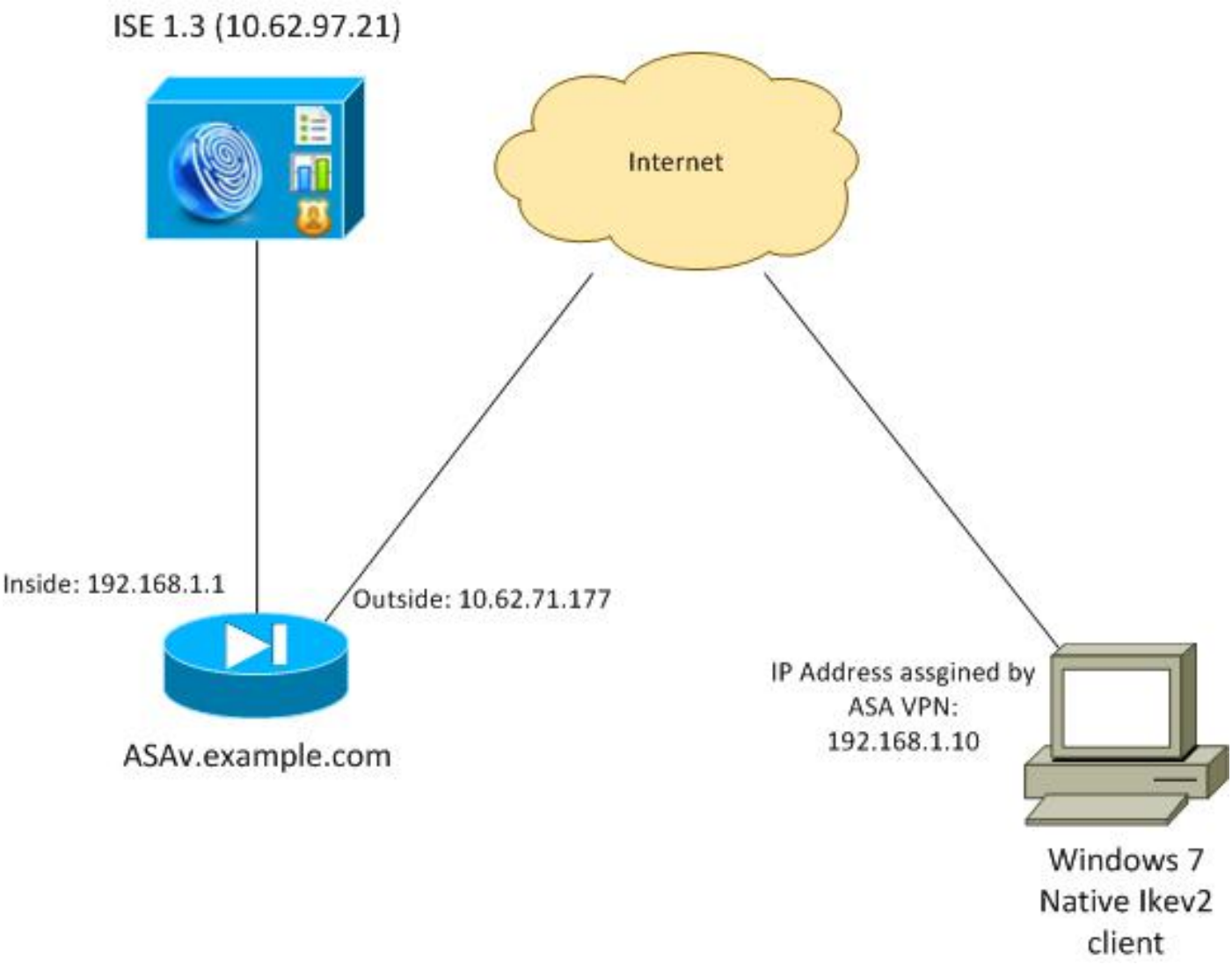
Le client indigène de Windows IKEv2 ne prend en charge pas le tunnel partagé (il n'y a aucun TÉLÉCONFÉRENCE attribut de RÉPONSE qui pourrait être reçu par le client de Windows 7), ainsi la seule stratégie possible avec le client de Microsoft est de percer un tunnel tout le trafic (sélecteurs du 0/0 trafic). S'il y a un besoin de stratégie spécifique de tunnel partagé, AnyConnect devrait être utilisé.

AnyConnect ne prend en charge pas les méthodes normalisées d'EAP qui sont terminées sur le serveur d'AAA (PEAP, Transport Layer Security). S'il y a un besoin de terminer des sessions d'EAP sur le serveur d'AAA puis le client de Microsoft peut être utilisé.

Configurez

> Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau



L'ASA est configurée pour authentifier avec un certificat (le client doit espérer que certificat). Le client de Windows 7 est configuré pour authentifier avec l'EAP (EAP-PEAP).

L'ASA agit en tant que passerelle VPN terminant la session IKEv2 du client. L'ISE agit en tant que serveur d'AAA terminant la session d'EAP du client. Des paquets d'EAP sont encapsulés en paquets IKE_AUTH pour le trafic entre le client et l'ASA (IKEv2) et puis dans des paquets RADIUS pour le trafic d'authentification entre l'ASA et l'ISE.

Certificats

Microsoft Certificate Authority (CA) a été utilisé afin de générer le certificat pour l'ASA. Les conditions requises de certificat afin d'être reçu par le client indigène de Windows 7 sont :

- L'extension étendue de l'utilisation principale (EKU) devrait inclure l'authentification de serveur (le modèle « serveur Web » a été utilisé dans cet exemple).
- Le subject-name devrait inclure le nom de domaine complet (FQDN) qui sera utilisé par le client afin de se connecter (dans cet exemple ASAv.example.com).

Pour plus de détails sur le client de Microsoft, voir dépannage des connexions VPN IKEv2.

> Remarque: Android 4.x est plus restrictif et exige le nom alternatif soumis correct selon RFC 6125. Le pour en savoir plus pour Android, voient IKEv2 d'Android strongSwan au Cisco IOS

avec l'authentification d'EAP et RSA.

Afin de générer une demande de signature de certificat sur l'ASA, cette configuration a été utilisée :

```
hostname ASAv
domain-name example.com

crypto ca trustpoint TP
enrollment terminal

crypto ca authenticate TP
crypto ca enroll TP
```

ISE

Étape 1. Ajoutez l'ASA aux périphériques de réseau sur l'ISE.

Choisissez les **périphériques de gestion > de réseau**. Placez un mot de passe preshared qui sera utilisé par l'ASA.

Étape 2. Créez un nom d'utilisateur dans la mémoire locale.

Choisissez la **gestion > les identités > les utilisateurs**. Créez le nom d'utilisateur au besoin.

Toutes autres configurations sont activées par défaut pour que l'ISE authentifie des points finaux avec EAP-PEAP (Protected Extensible Authentication Protocol).

ASA

La configuration pour l'Accès à distance est semblable pour IKEv1 et IKEv2.

```
aaa-server ISE2 protocol radius
aaa-server ISE2 (inside) host 10.62.97.21
 key cisco

group-policy AllProtocols internal
group-policy AllProtocols attributes
 vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

ip local pool POOL 192.168.1.10-192.168.1.20 mask 255.255.255.0

crypto ipsec ikev2 ipsec-proposal ipsec-proposal
 protocol esp encryption aes-256 aes-192 aes
 protocol esp integrity sha-256 sha-1 md5

crypto dynamic-map DYNMAP 10 set ikev2 ipsec-proposal ipsec-proposal
crypto map MAP 10 ipsec-isakmp dynamic DYNMAP
crypto map MAP interface outside

crypto ikev2 policy 10
 encryption 3des
 integrity sha
```

```
 group 2
 prf sha
 lifetime seconds 86400
```

Puisque le Windows 7 envoie une adresse de type IKE-ID en paquet IKE_AUTH, le **DefaultRAGroup** devrait être utilisé afin de s'assurer que la connexion débarque sur le groupe de tunnels correct. L'ASA authentifie avec un certificat (authentification locale) et s'attend à ce que le client utilise l'EAP (authentification à distance). En outre, l'ASA doit envoyer spécifiquement une demande d'identité d'EAP du client de répondre avec la réponse d'identité d'EAP (requête-identité).

```
tunnel-group DefaultRAGroup general-attributes
 address-pool POOL
 authentication-server-group ISE
 default-group-policy AllProtocols
tunnel-group DefaultRAGroup ipsec-attributes
 ikev2 remote-authentication eap query-identity
 ikev2 local-authentication certificate TP
```

En conclusion, IKEv2 doit être activé et le certificat correct être utilisé.

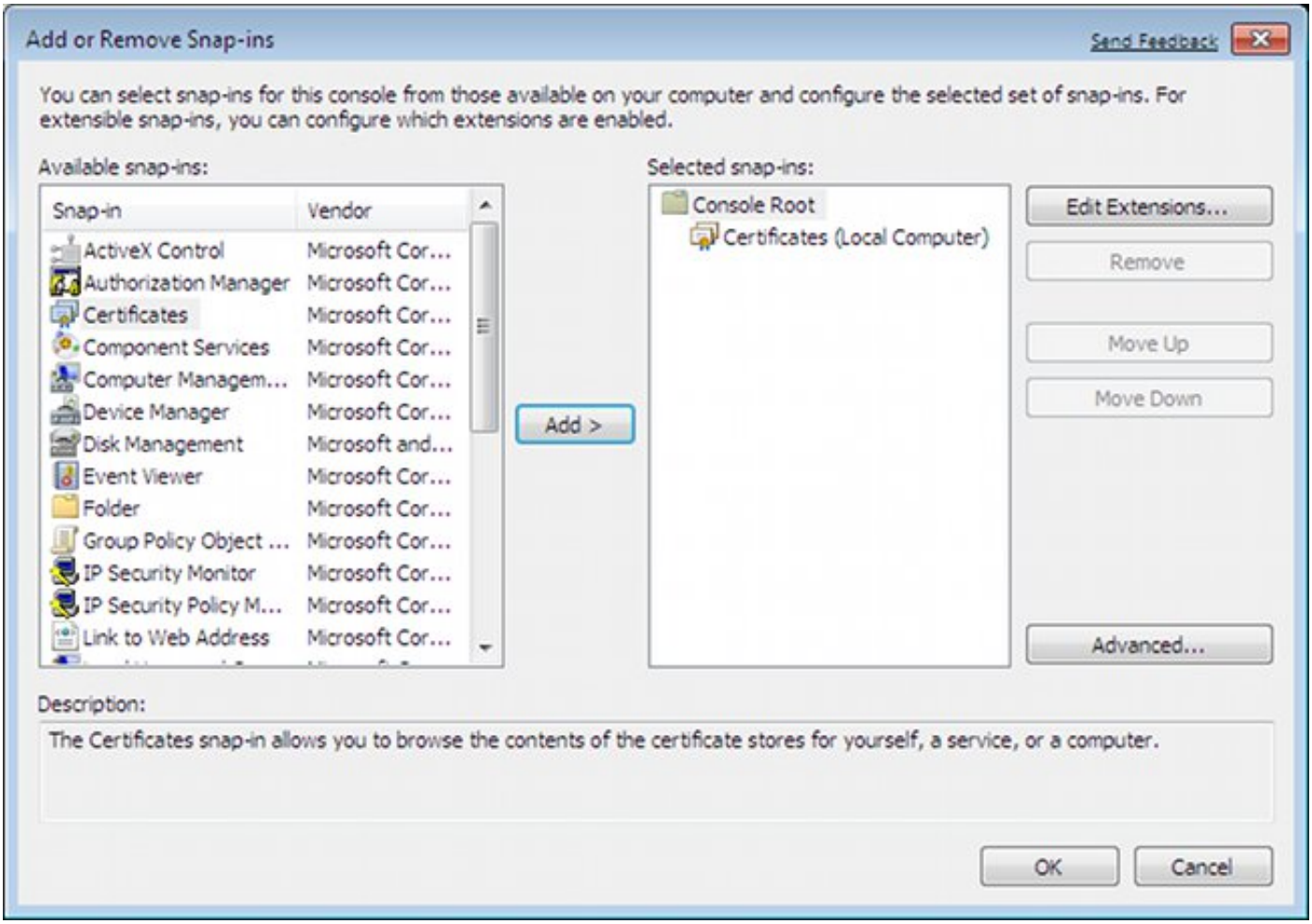
```
tunnel-group DefaultRAGroup general-attributes
 address-pool POOL
 authentication-server-group ISE
 default-group-policy AllProtocols
tunnel-group DefaultRAGroup ipsec-attributes
 ikev2 remote-authentication eap query-identity
 ikev2 local-authentication certificate TP
```

Windows 7

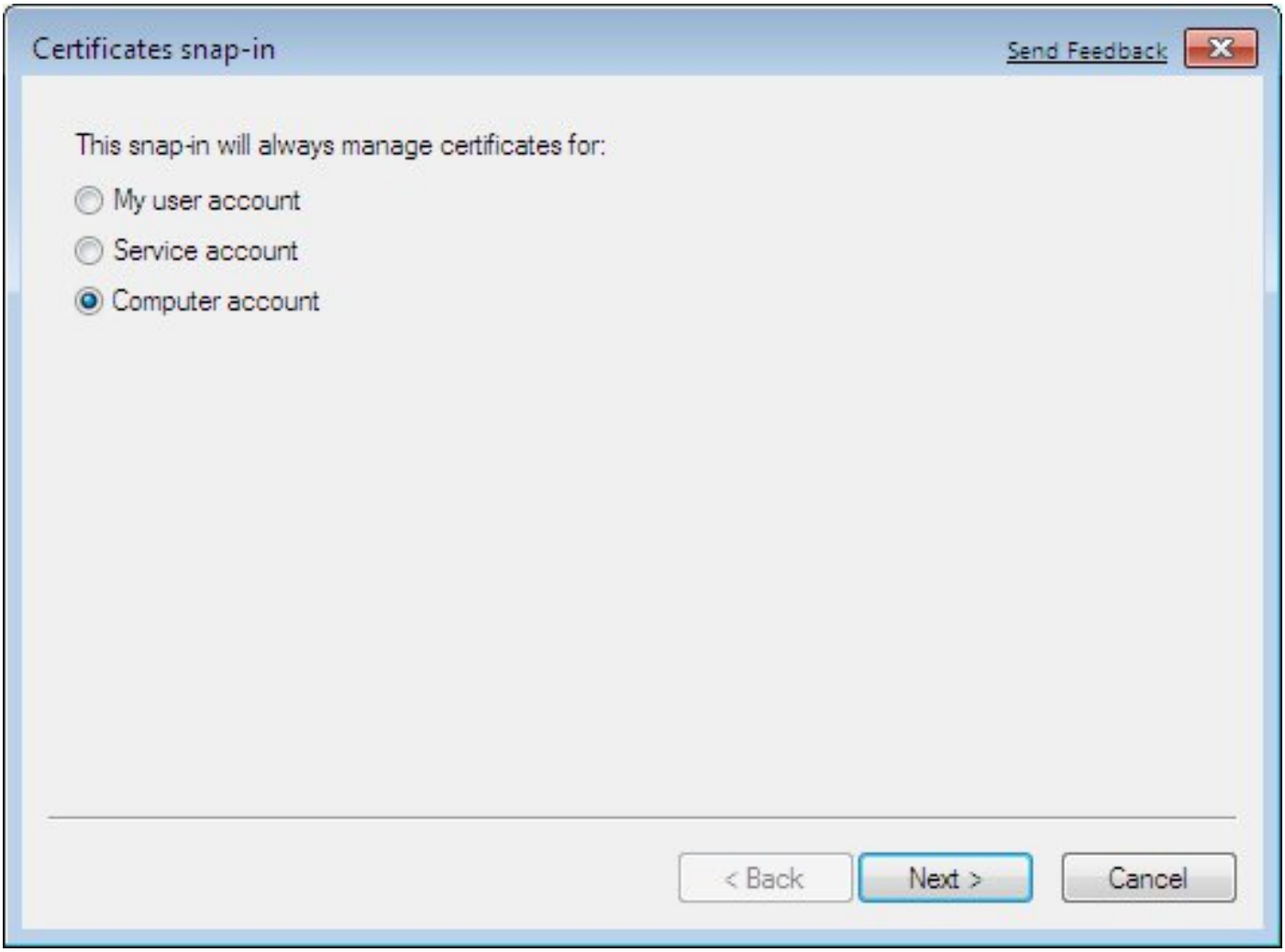
Étape 1. Installez le certificat de CA.

Afin de faire confiance au certificat présenté par l'ASA, le client Windows doit faire confiance à son CA. Ce certificat de CA devrait être ajouté à la mémoire de certificat d'ordinateur (pas la mémoire d'utilisateur). Le client Windows emploie le magasin informatique afin de valider le certificat IKEv2.

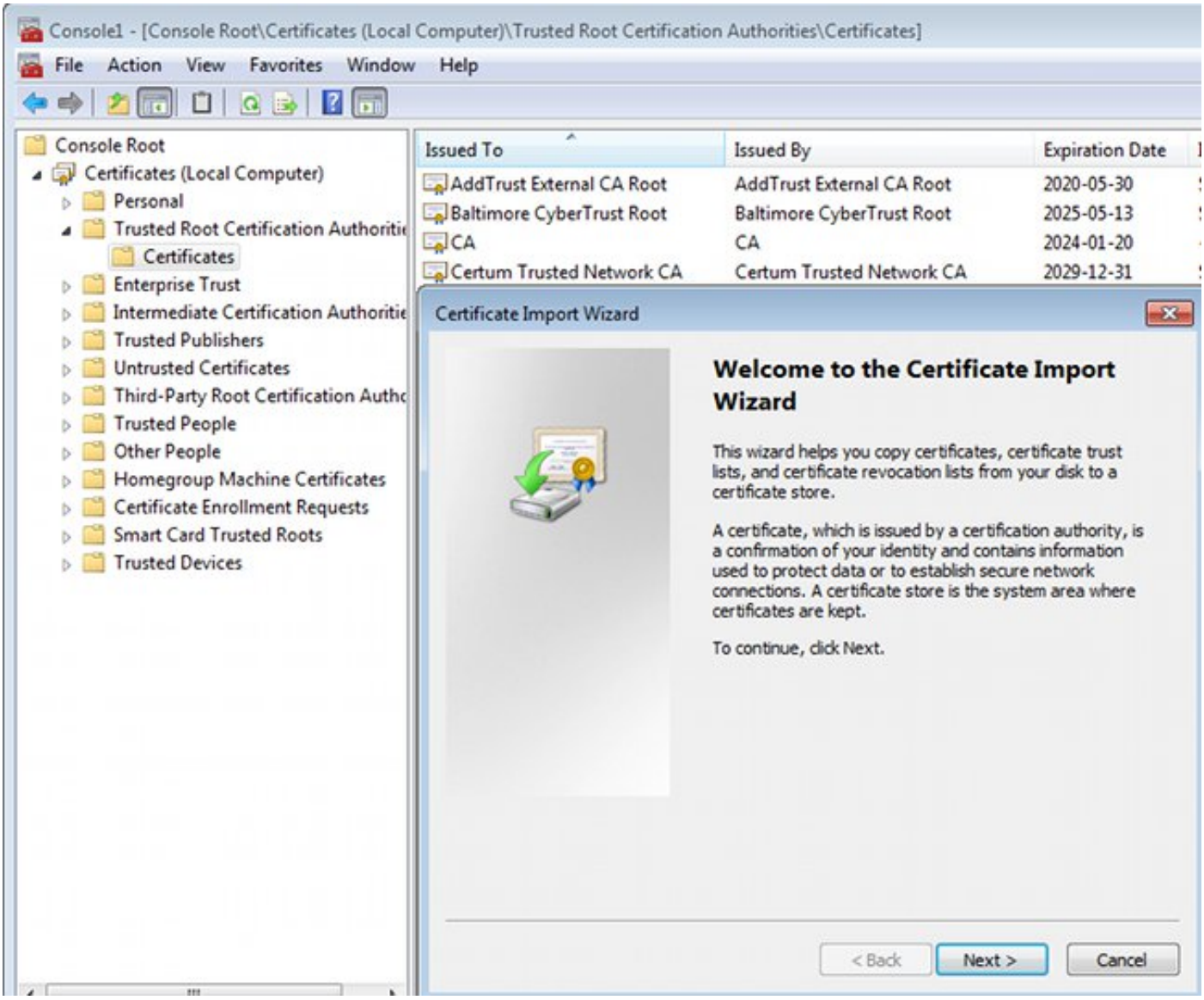
Afin d'ajouter le CA, choisissez **MMC > ajoutent ou retirent SNAP-Institut central des statistiques > Certificats**.



Cliquez sur la case d'option de **compte d'ordinateur**.



Importez le CA aux autorités de confiance de certificat racine.

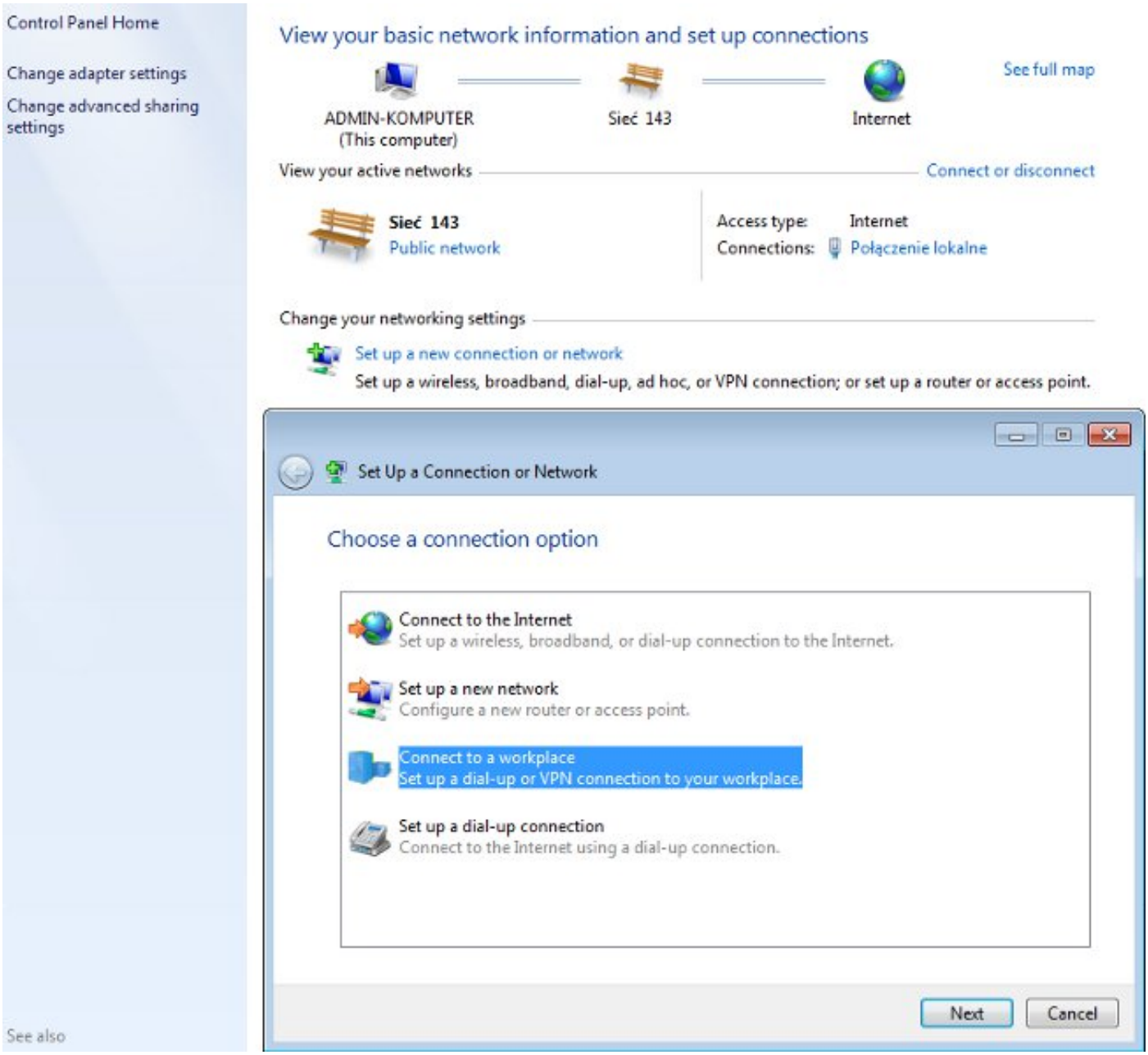


Si le client Windows ne peut pas valider le certificat présenté par l'ASA, elle signale :

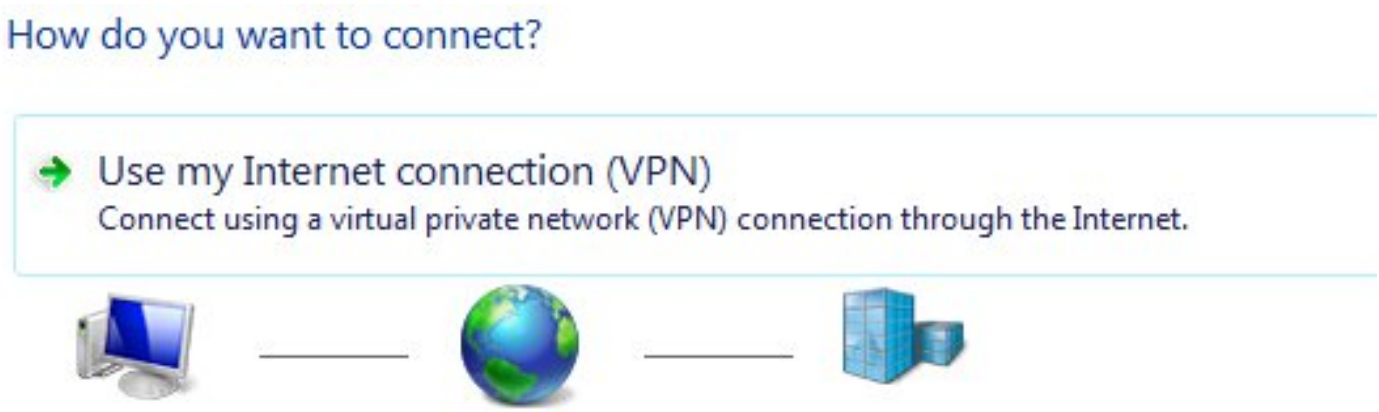
```
tunnel-group DefaultRAGroup general-attributes
 address-pool POOL
 authentication-server-group ISE
 default-group-policy AllProtocols
tunnel-group DefaultRAGroup ipsec-attributes
 ikev2 remote-authentication eap query-identity
 ikev2 local-authentication certificate TP
```

Étape 2. Configurez la connexion VPN.

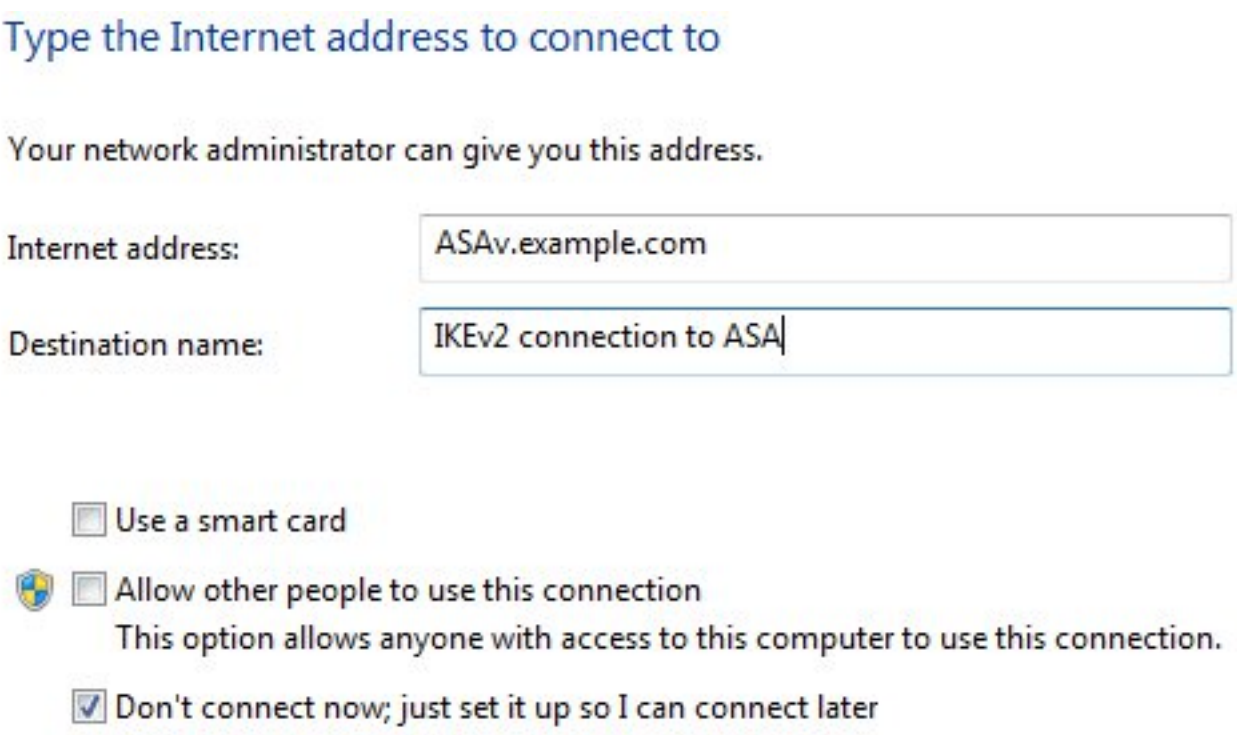
Afin de configurer la connexion VPN du réseau et du centre de partager, choisissez **se connectent à un lieu de travail** afin de créer une connexion VPN.



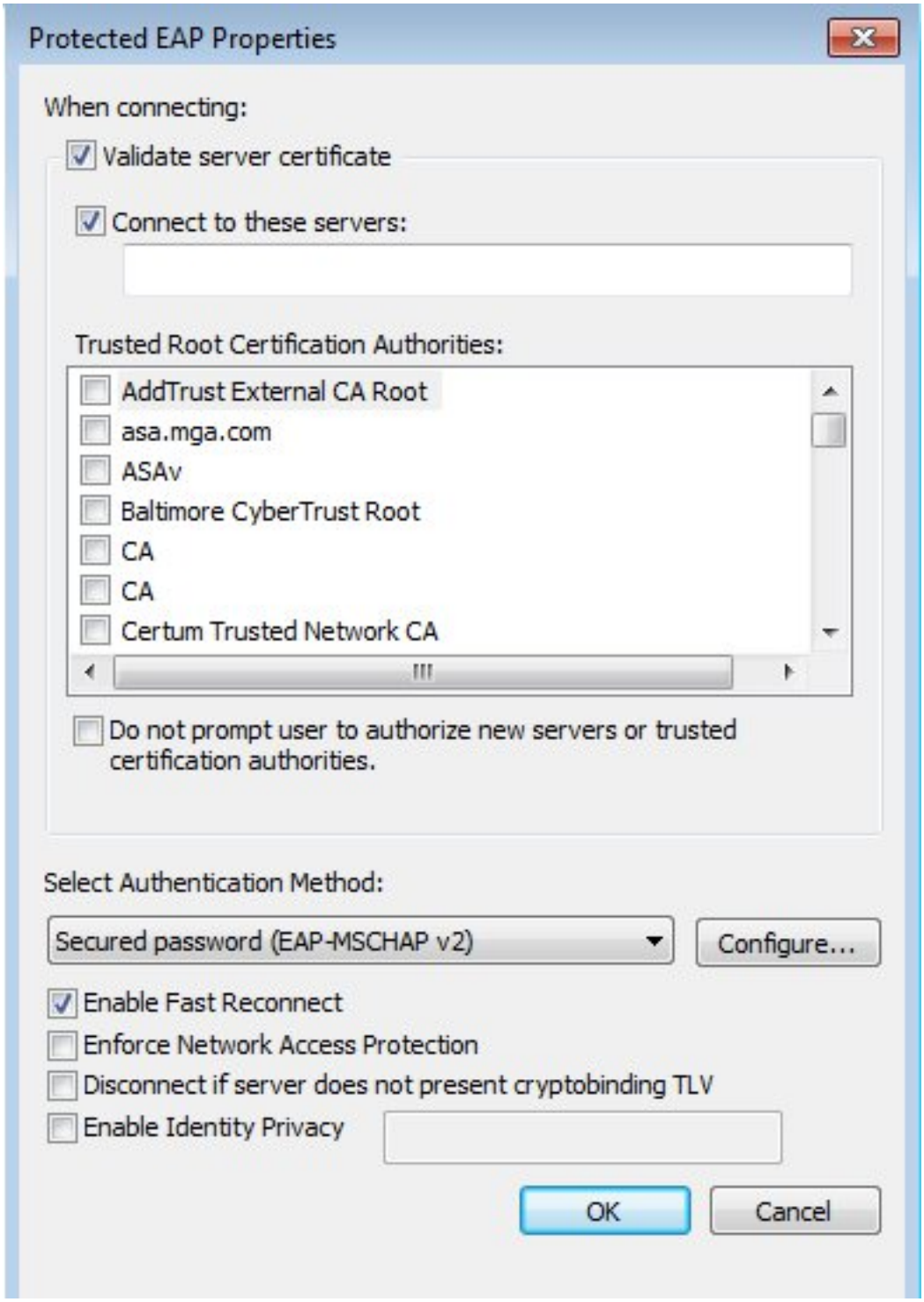
Choisissez l'**utilisation ma connexion Internet (VPN)**.



Configurez l'adresse avec un FQDN ASA. Assurez-vous qu'il est correctement résolu du Domain Name Server (DN).



S'il y a lieu, ajustez les propriétés (telles que la validation de certificat) sur la fenêtre protégée de Properties d'EAP.



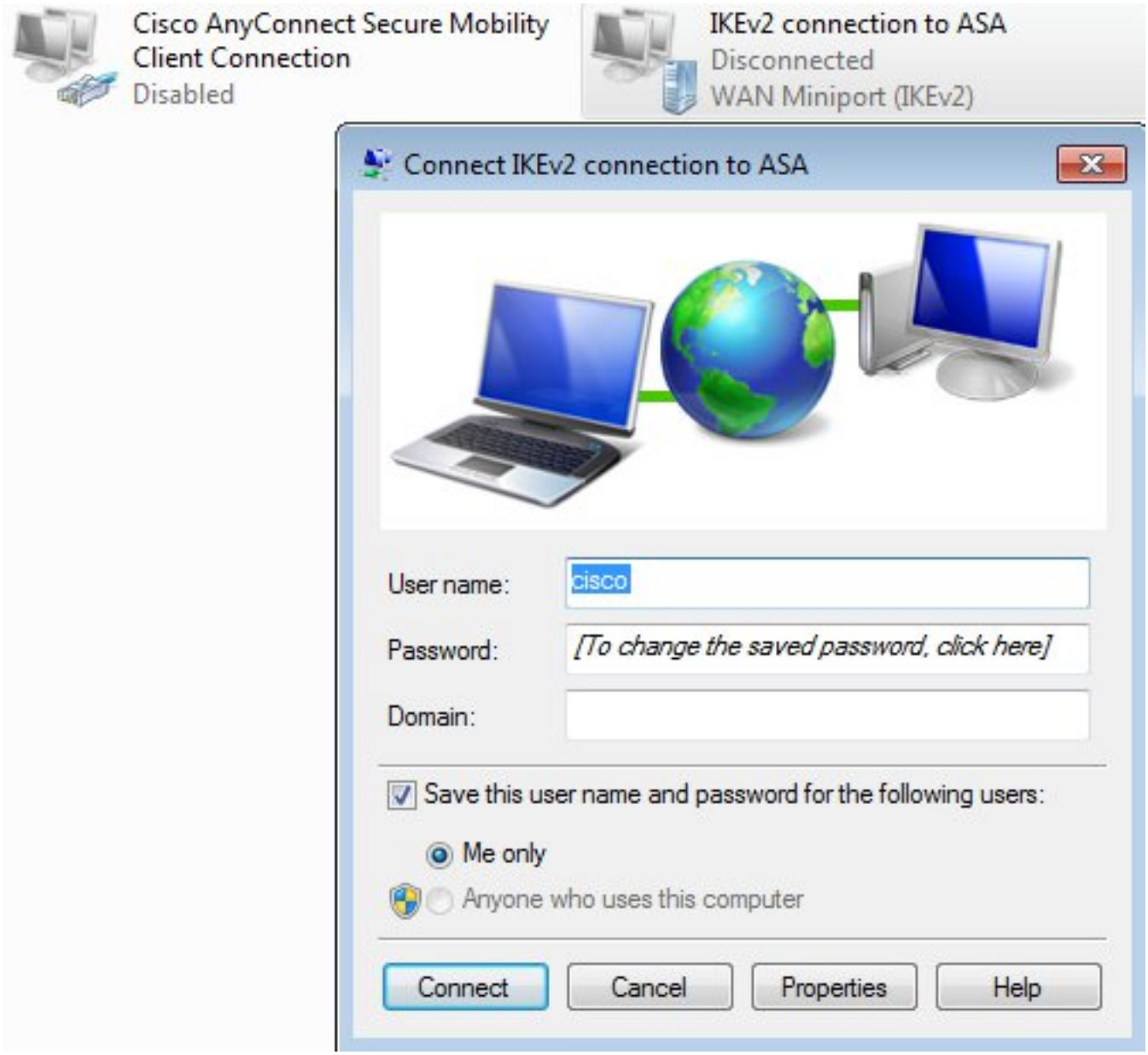
Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

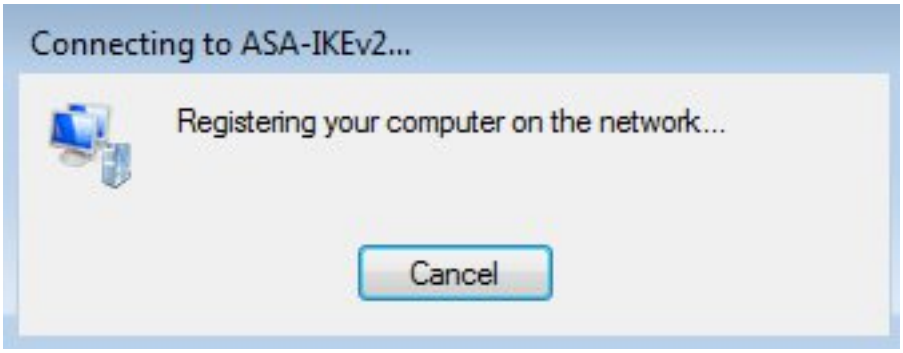
L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Client Windows

Quand vous vous connectez, entrez dans vos qualifications.



Après l'authentification réussie la configuration IKEv2 est appliquée.



La session est EN HAUSSE.

La table de routage a été mise à jour avec le default route avec l'utilisation d'une nouvelle interface avec la métrique peu élevée.

```
C:\Users\admin>route print
===========================================================================
Interface List
 41...........................IKEv2 connection to ASA
 11...08 00 27 d2 cb 54 ......Karta Intel(R) PRO/1000 MT Desktop Adapter
 1...........................Software Loopback Interface 1
 15...00 00 00 00 00 00 00 e0 Karta Microsoft ISATAP
 12...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 22...00 00 00 00 00 00 00 e0 Karta Microsoft ISATAP #4
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.68   4491
          0.0.0.0          0.0.0.0         On-link     192.168.1.10     11
    10.62.71.177  255.255.255.255     192.168.10.1    192.168.10.68   4236
       127.0.0.0        255.0.0.0         On-link         127.0.0.1   4531
       127.0.0.1  255.255.255.255         On-link         127.0.0.1   4531
 127.255.255.255  255.255.255.255         On-link         127.0.0.1   4531
    192.168.1.10  255.255.255.255         On-link      192.168.1.10    266
    192.168.10.0    255.255.255.0         On-link     192.168.10.68   4491
   192.168.10.68  255.255.255.255         On-link     192.168.10.68   4491
  192.168.10.255  255.255.255.255         On-link     192.168.10.68   4491
       224.0.0.0        240.0.0.0         On-link         127.0.0.1   4531
       224.0.0.0        240.0.0.0         On-link     192.168.10.68   4493
       224.0.0.0        240.0.0.0         On-link      192.168.1.10     11
 255.255.255.255  255.255.255.255         On-link         127.0.0.1   4531
 255.255.255.255  255.255.255.255         On-link     192.168.10.68   4491
 255.255.255.255  255.255.255.255         On-link      192.168.1.10    266
===========================================================================
```

Logs

Après l'authentification réussie les états ASA :

```
ASAv(config)# show vpn-sessiondb detail ra-ikev2-ipsec

Session Type: Generic Remote-Access IKEv2 IPsec Detailed

Username     : cisco                 Index        : 13
```

```
Assigned IP  : 192.168.1.10          Public IP    : 10.147.24.166
Protocol     : IKEv2 IPsecOverNatT
License      : AnyConnect Premium
Encryption   : IKEv2: (1)3DES  IPsecOverNatT: (1)AES256
Hashing      : IKEv2: (1)SHA1  IPsecOverNatT: (1)SHA1
Bytes Tx     : 0                     Bytes Rx     : 7775
Pkts Tx      : 0                     Pkts Rx      : 94
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : AllProtocols          Tunnel Group : DefaultRAGroup
Login Time   : 17:31:34 UTC Tue Nov 18 2014
Duration     : 0h:00m:50s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : c0a801010000d000546b8276
Security Grp : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1

IKEv2:
 Tunnel ID    : 13.1
 UDP Src Port : 4500                  UDP Dst Port : 4500
 Rem Auth Mode: EAP
 Loc Auth Mode: rsaCertificate
 Encryption   : 3DES                  Hashing      : SHA1
 Rekey Int (T): 86400 Seconds         Rekey Left(T): 86351 Seconds
 PRF          : SHA1                  D/H Group    : 2
 Filter Name  :

IPsecOverNatT:
 Tunnel ID    : 13.2
 Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 192.168.1.10/255.255.255.255/0/0
 Encryption   : AES256                Hashing      : SHA1
 Encapsulation: Tunnel
 Rekey Int (T): 28800 Seconds         Rekey Left(T): 28750 Seconds
 Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
 Bytes Tx     : 0                     Bytes Rx     : 7834
 Pkts Tx      : 0                     Pkts Rx      : 95
```

Les logs ISE indiquent l'authentification réussie avec des règles d'authentification par défaut et d'autorisation.

Les détails indiquent la méthode PEAP.

Authentication Details

Source Timestamp	2014-11-19 08:10:02.819
Received Timestamp	2014-11-19 08:10:02.821
Policy Server	ise13
Event	5200 Authentication succeeded
Failure Reason	
Resolution	
Root cause	
Username	cisco
User Type	User
Endpoint Id	10.147.24.166
Endpoint Profile	
IP Address	
Authentication Identity Store	Internal Users
Identity Group	
Audit Session Id	c0a801010001000546c424a
Authentication Method	MSCHAPV2
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Login
Network Device	ASAv
Device Type	All Device Types
Location	All Locations
NAS IP Address	10.62.71.177
NAS Port Id	
NAS Port Type	Virtual
Authorization Profile	PermitAccess

Debugs sur l'ASA

Le plus important met au point incluent :

```
ASAv# debug crypto ikev2 protocol 32
<most debugs omitted for clarity....
```

Paquet IKE_SA_INIT reçu par l'ASA (inclut les propositions IKEv2 et l'échange de clé pour le Protocole DH (Diffie-Hellman)) :

```
IKEv2-PROTO-2: Received Packet [From 10.147.24.166:500/To 10.62.71.177:500/VRF i0:f0]
Initiator SPI : 7E5B69A028355701 - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUESTIKEv2-PROTO-3: Next payload: SA,
version: 2.0 Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 528
Payload contents:
 SA  Next payload: KE, reserved: 0x0, length: 256
 last proposal: 0x2, reserved: 0x0, length: 40
 Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 4    last transform: 0x3,
reserved: 0x0: length: 8
.....
```

Réponse IKE_SA_INIT au demandeur (inclut les propositions IKEv2, l'échange de clé pour le CAD, et la demande de certificat) :

```
IKEv2-PROTO-2: (30): Generating IKE_SA_INIT message
IKEv2-PROTO-2: (30): IKE Proposal: 1, SPI size: 0 (initial negotiation),
Num. transforms: 4
(30):    3DES(30):    SHA1(30):    SHA96(30):    DH_GROUP_1024_MODP/Group
2IKEv2-PROTO-5:
Construct Vendor Specific Payload: DELETE-REASONIKEv2-PROTO-5: Construct Vendor
Specific Payload: (CUSTOM)IKEv2-PROTO-5: Construct Notify Payload:
NAT_DETECTION_SOURCE_IPIKEv2-PROTO-5: Construct Notify Payload:
NAT_DETECTION_DESTINATION_IPIKEv2-PROTO-5: Construct Vendor Specific Payload:
FRAGMENTATION(30):
IKEv2-PROTO-2: (30): Sending Packet [To 10.147.24.166:500/From
10.62.71.177:500/VRF i0:f0]
```

IKE_AUTHENTIC pour le client avec IKE-ID, demande de certificat, a proposé des jeux de transformations, la configuration demandée, et des sélecteurs du trafic :

```
IKEv2-PROTO-2: (30): Received Packet [From 10.147.24.166:4500/To 10.62.71.177:500/VRF
i0:f0]
(30): Initiator SPI : 7E5B69A028355701 - Responder SPI : 1B1A94C7A7739855 Message id: 1
(30): IKEv2 IKE_AUTH Exchange REQUESTIKEv2-PROTO-3: (30): Next payload: ENCR,
version: 2.0 (30): Exchange type: IKE_AUTH, flags: INITIATOR (30): Message id: 1,
length: 948(30):
```

Réponse IKE_AUTHENTIC de l'ASA qui inclut une demande d'identité d'EAP (premier paquet avec des extensions d'EAP). Ce paquet inclut également le certificat (s'il n'y a aucun certificat correct sur l'ASA il y a une panne) :

```
IKEv2-PROTO-2: (30): Generating EAP request
IKEv2-PROTO-2: (30): Sending Packet [To 10.147.24.166:4500/From 10.62.71.177:4500/VRF
i0:f0]
```

Réponse d'EAP reçue par l'ASA (longueur 5, charge utile : Cisco) :

```
(30): REAL Decrypted packet:(30): Data&colon; 14 bytes
(30):  EAP(30):   Next payload: NONE, reserved: 0x0, length: 14
(30):     Code: response: id: 36, length: 10
(30):     Type: identity
(30): EAP data&colon; 5 bytes
```

Alors des plusieurs paquets sont permutés comme partie d'EAP-PEAP. Le succès d'EAP est reçu par l'ASA et enfin expédié au suppliant :

```
Payload contents:
(30):  EAP(30):   Next payload: NONE, reserved: 0x0, length: 8
(30):     Code: success: id: 76, length: 4
```

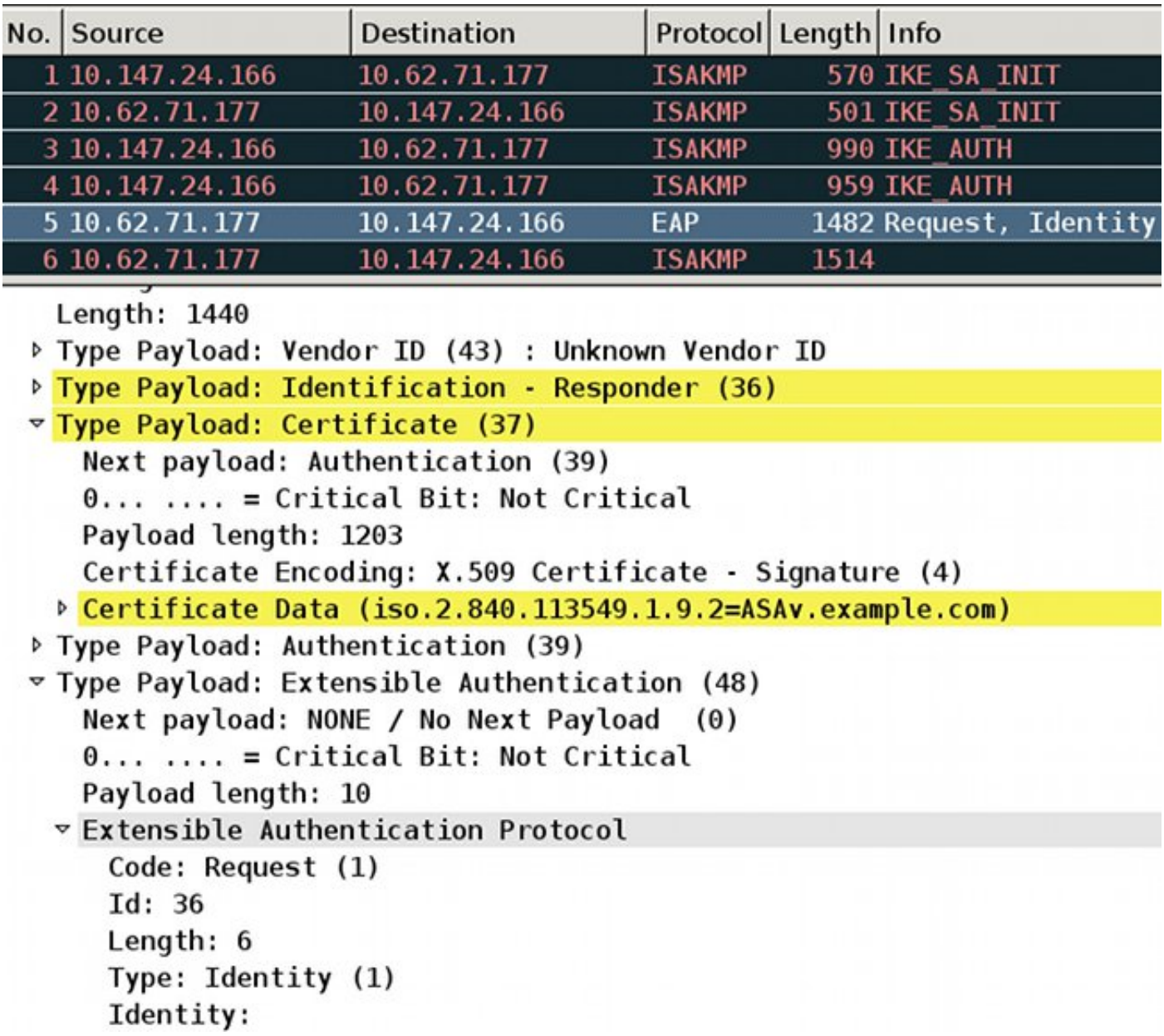
L'authentification de pair est réussie :

```
Payload contents:
(30):  EAP(30):   Next payload: NONE, reserved: 0x0, length: 8
(30):     Code: success: id: 76, length: 4
```

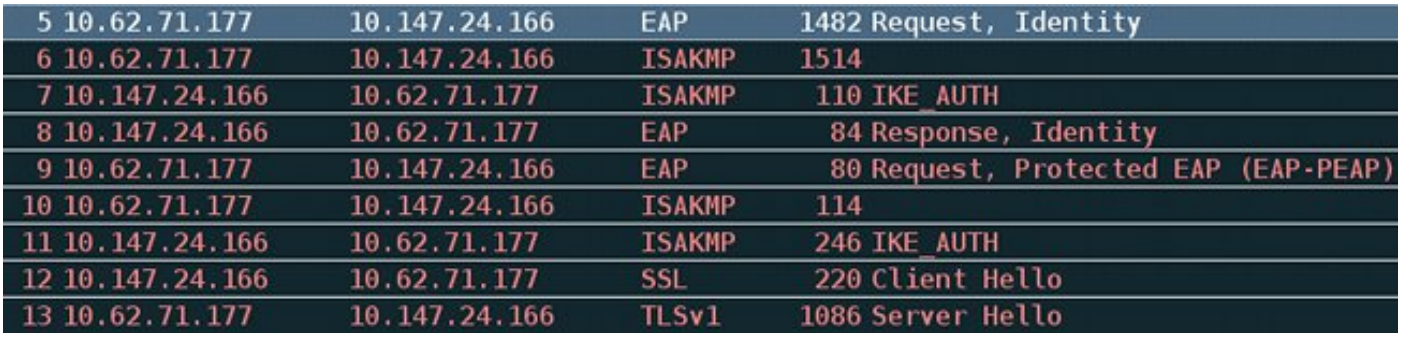
Et la session VPN est terminée correctement.

Niveau de paquet

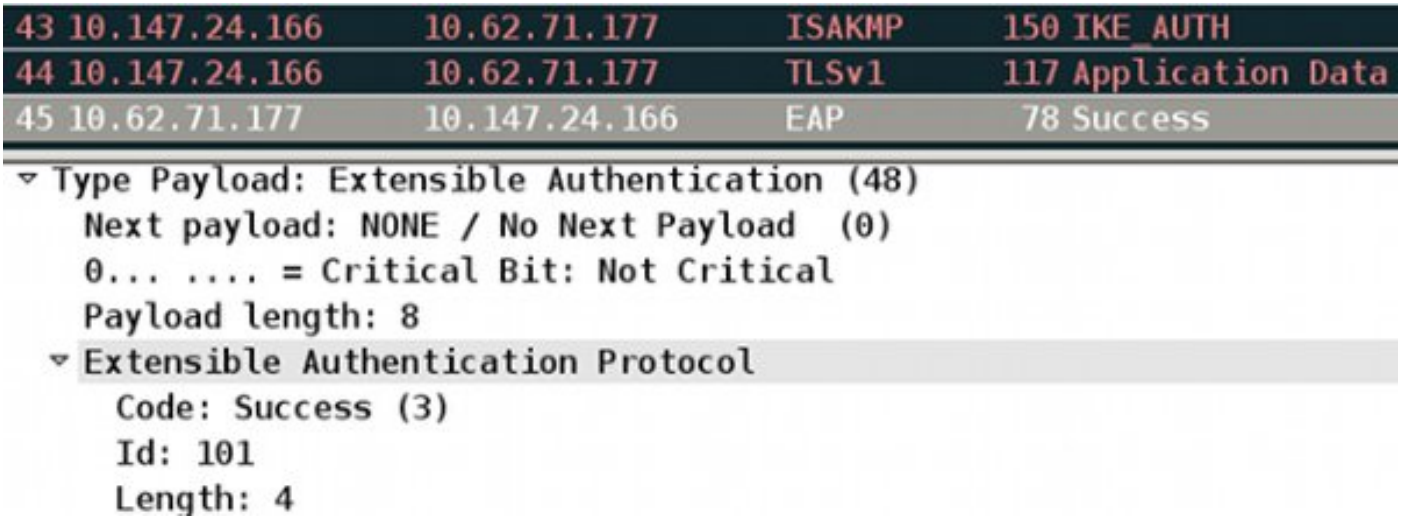
La demande d'identité d'EAP est encapsulée dans la « authentification extensible » de l'IKE_AUTH envoient par l'ASA. Avec la demande d'identité, IKE_ID et Certificats sont envoyés.



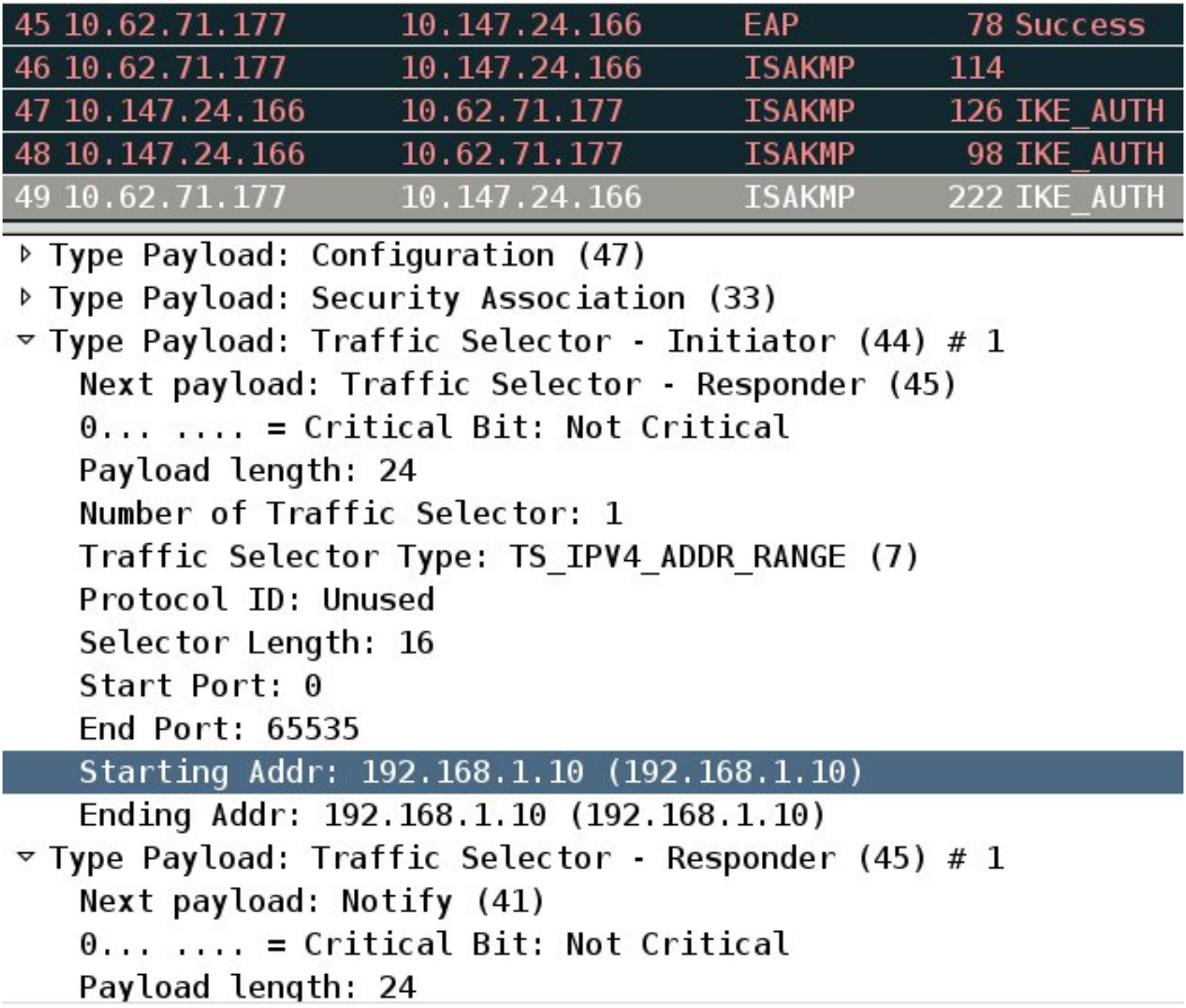
Tous les paquets ultérieurs d'EAP sont encapsulés dans IKE_AUTH. Après que le suppliant confirme la méthode (EAP-PEAP), elle commence à construire un tunnel de Secure Sockets Layer (SSL) qui protège la session MSCHAPv2 utilisée pour l'authentification.



Après que des plusieurs paquets soient permutés l'ISE confirme le succès.



La session IKEv2 est terminée par l'ASA, la configuration finale (réponse de configuration avec des valeurs telles qu'une adresse IP assignée), des jeux de transformations, et des sélecteurs du trafic sont poussés au client vpn.



Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Guide de configuration de la gamme VPN CLI de Cisco ASA, 9.3
- Guide de l'utilisateur de Logiciel Cisco Identity Services Engine, version 1.2
- Support et documentation techniques - Cisco Systems