Configurer l'accès à distance ASA IKEv2 avec EAP-PEAP et le client Windows natif

Contenu

Introduction

Ce document fournit un exemple de configuration pour un dispositif de sécurité adaptatif Cisco (ASA) version 9.3.2 et ultérieure qui permet à un accès VPN distant d'utiliser le protocole IKEv2 (Internet Key Exchange Protocol) avec l'authentification EAP (Extensible Authentication Protocol) standard. Cela permet à un client Microsoft Windows 7 natif (et à tout autre client IKEv2 standard) de se connecter à l'ASA avec l'authentification IKEv2 et EAP.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances VPN de base et IKEv2
- Connaissances AAA (Basic Authentication, Authorization and Accounting) et RADIUS
- Expérience avec la configuration VPN ASA
- Expérience avec la configuration ISE (Identity Services Engine)

Components Used

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

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

Informations générales

Considérations sur les clients AnyConnect Secure Mobility

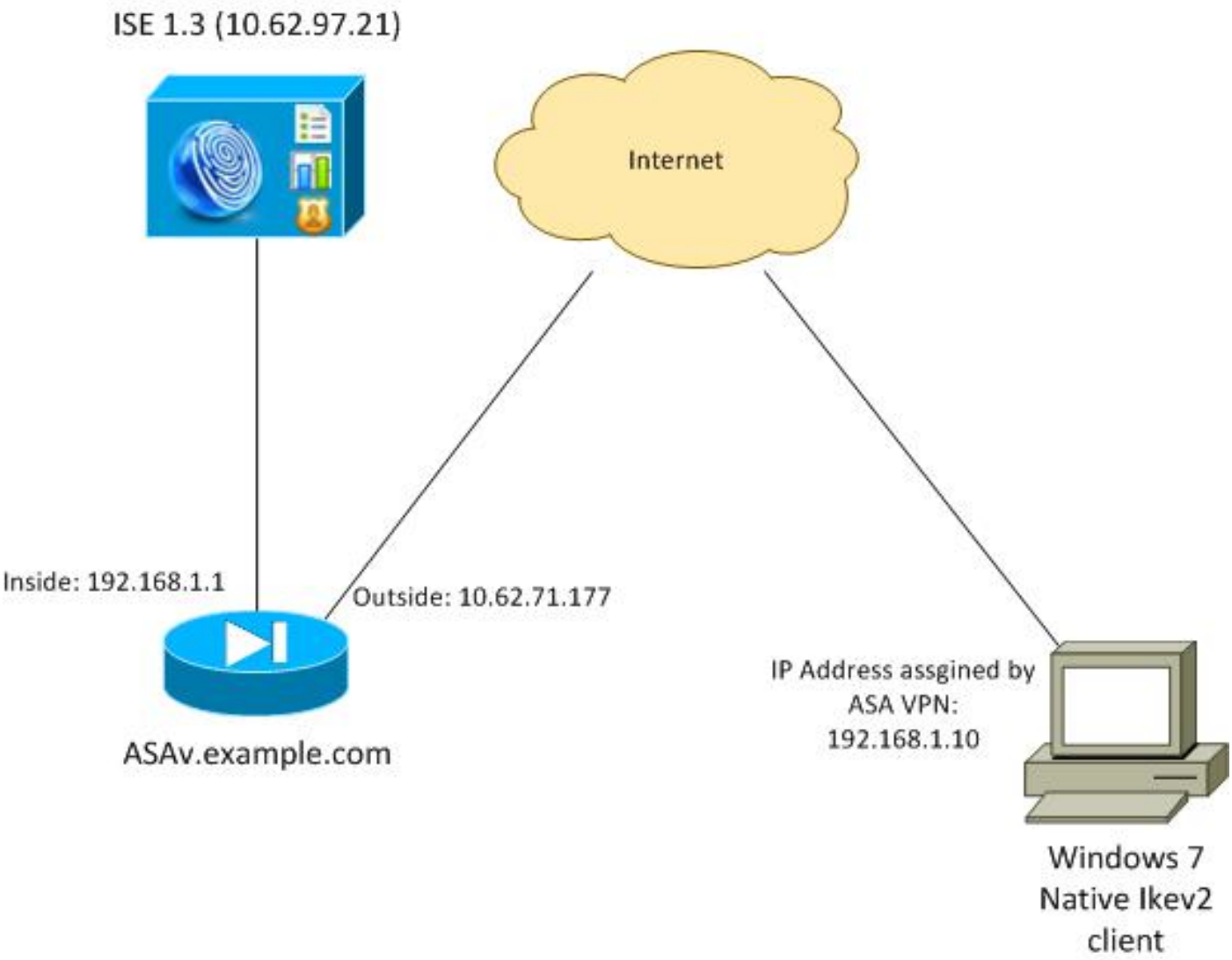
Le client natif Windows IKEv2 ne prend pas en charge le tunnel partagé (il n'y a aucun attribut CONF REPLY qui pourrait être accepté par le client Windows 7), donc la seule stratégie possible avec le client Microsoft est de tunnel tout le trafic (sélecteurs de trafic 0/0). Si une stratégie de tunnel partagé spécifique est nécessaire, AnyConnect doit être utilisé.

AnyConnect ne prend pas en charge les méthodes EAP normalisées qui sont terminées sur le serveur AAA (PEAP, Transport Layer Security). S'il est nécessaire de mettre fin aux sessions EAP sur le serveur AAA, le client Microsoft peut être utilisé.

Configuration

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

Diagramme du réseau



L'ASA est configuré pour s'authentifier avec un certificat (le client doit faire confiance à ce certificat). Le client Windows 7 est configuré pour s'authentifier avec EAP (EAP-PEAP).

L'ASA agit comme une passerelle VPN qui termine la session IKEv2 à partir du client. L'ISE agit comme un serveur AAA qui termine la session EAP du client. Les paquets EAP sont encapsulés dans des paquets IKE_AUTH pour le trafic entre le client et l'ASA (IKEv2), 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 exigences de certificat afin d'être acceptées par le client natif Windows 7 sont les suivantes :

- L'extension Extended Key Usage (EKU) doit inclure l'authentification du serveur (le modèle « serveur Web » a été utilisé dans cet exemple).
- Le nom de sujet doit 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 d'informations sur le client Microsoft, consultez Dépannage des connexions VPN IKEv2.

> **Note**: Android 4.x est plus restrictif et nécessite le bon nom de remplacement de sujet, conformément à la RFC 6125. Pour plus d'informations sur Android, consultez IKEv2

d'Android strongSwan à Cisco IOS avec EAP et RSA Authentication.

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 réseau de l'ISE.

Choisissez **Administration > Network Devices**. Définissez un mot de passe pré-partagé qui sera utilisé par l'ASA.

Étape 2. Créez un nom d'utilisateur dans le magasin local.

Choisissez **Administration > Identités > Utilisateurs**. Créez le nom d'utilisateur si nécessaire.

Tous les autres paramètres sont activés par défaut pour que l'ISE authentifie les points de terminaison avec EAP-PEAP (Protected Extensible Authentication Protocol).

ASA

La configuration de l'accès distant est similaire 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 Windows 7 envoie une adresse de type IKE-ID dans le paquet IKE_AUTH, le **DefaultRAGroup** doit être utilisé afin de s'assurer que la connexion atterrit sur le groupe de tunnels correct. L'ASA s'authentifie avec un certificat (authentification locale) et attend du client qu'il utilise EAP (authentification à distance). En outre, l'ASA doit spécifiquement envoyer une demande d'identité EAP pour que le client réponde avec une réponse d'identité EAP (query-identity).

```
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
```

Enfin, IKEv2 doit être activé et le certificat correct utilisé.

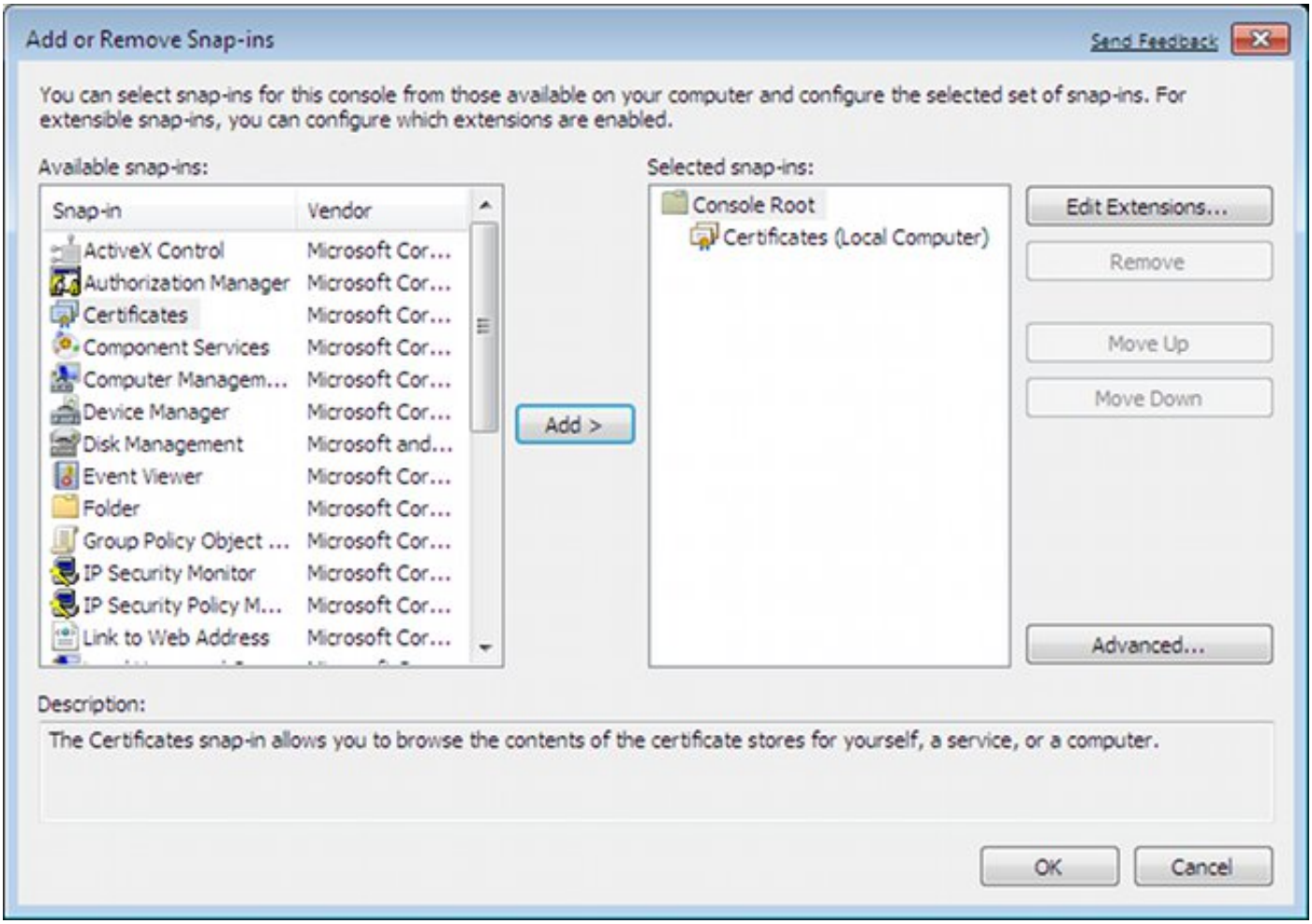
```
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint TP
```

Windows 7

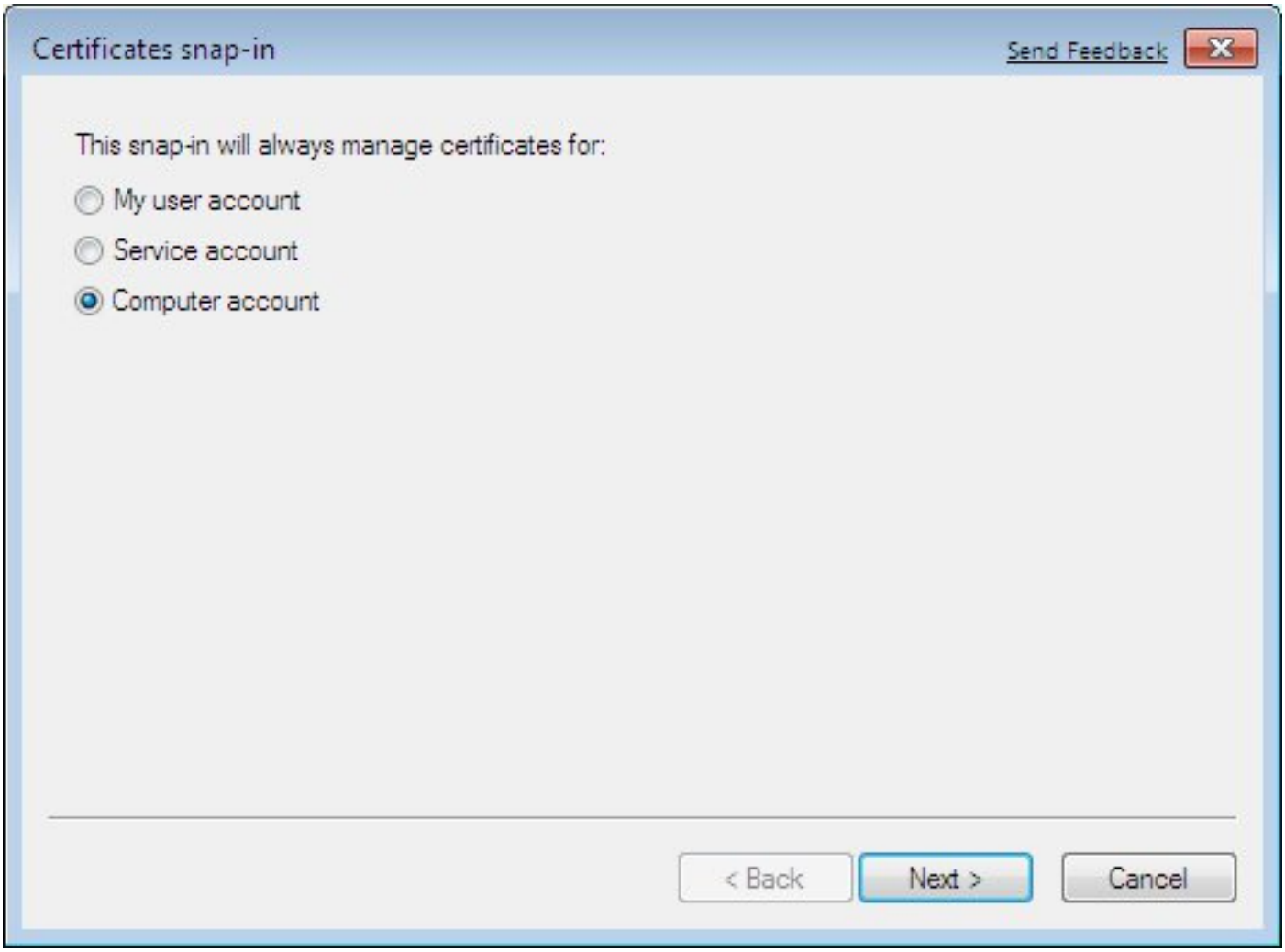
Étape 1. Installez le certificat CA.

Pour faire confiance au certificat présenté par l'ASA, le client Windows doit faire confiance à son autorité de certification. Ce certificat d'autorité de certification doit être ajouté au magasin de certificats de l'ordinateur (et non au magasin d'utilisateurs). Le client Windows utilise le magasin d'ordinateurs afin de valider le certificat IKEv2.

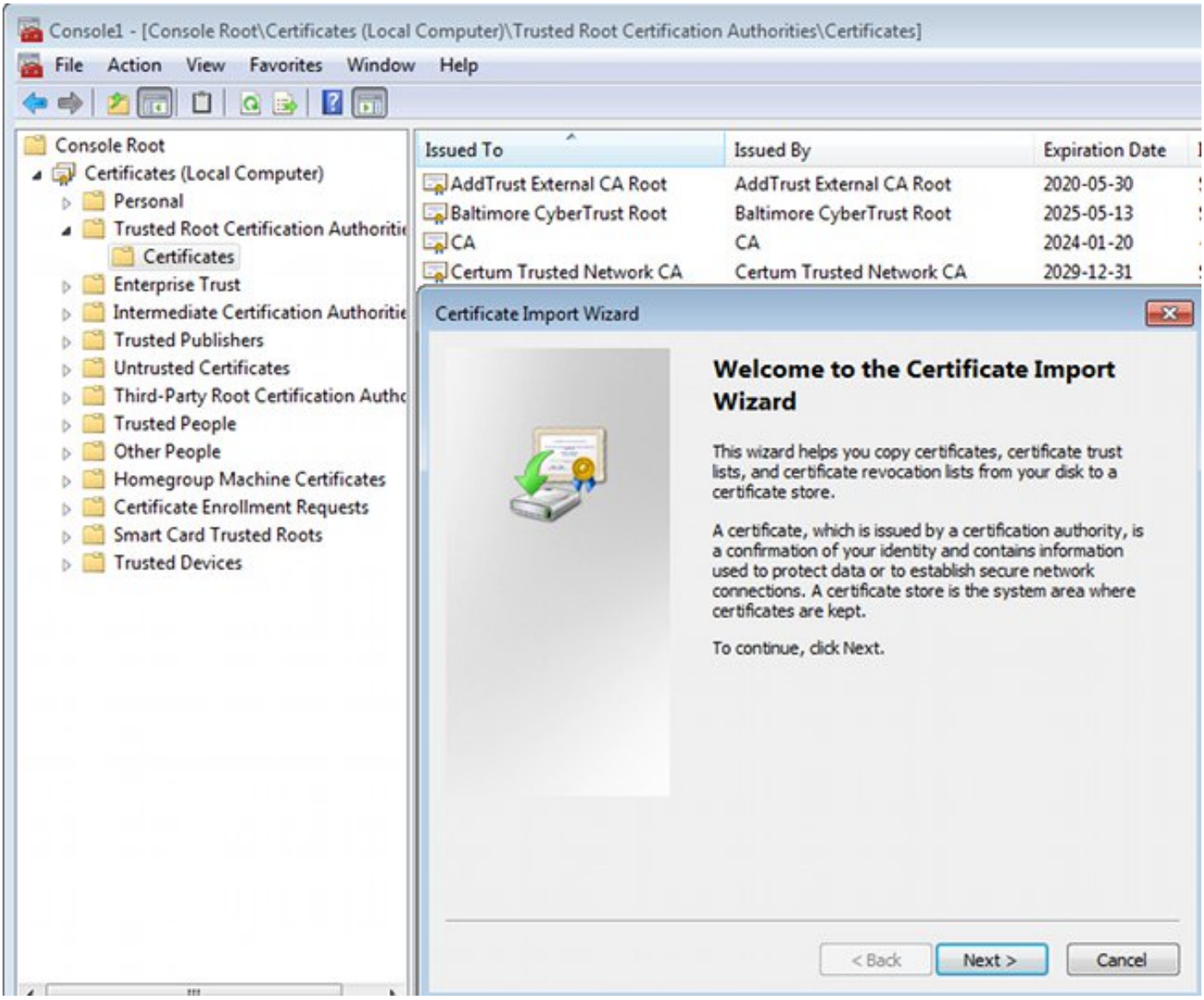
Afin d'ajouter l'autorité de certification, choisissez **MMC > Ajouter ou supprimer des composants logiciels enfichables > Certificats**.



Cliquez sur la case d'option **Compte d'ordinateur**.



Importez l'autorité de certification dans les autorités de certification racine de confiance.

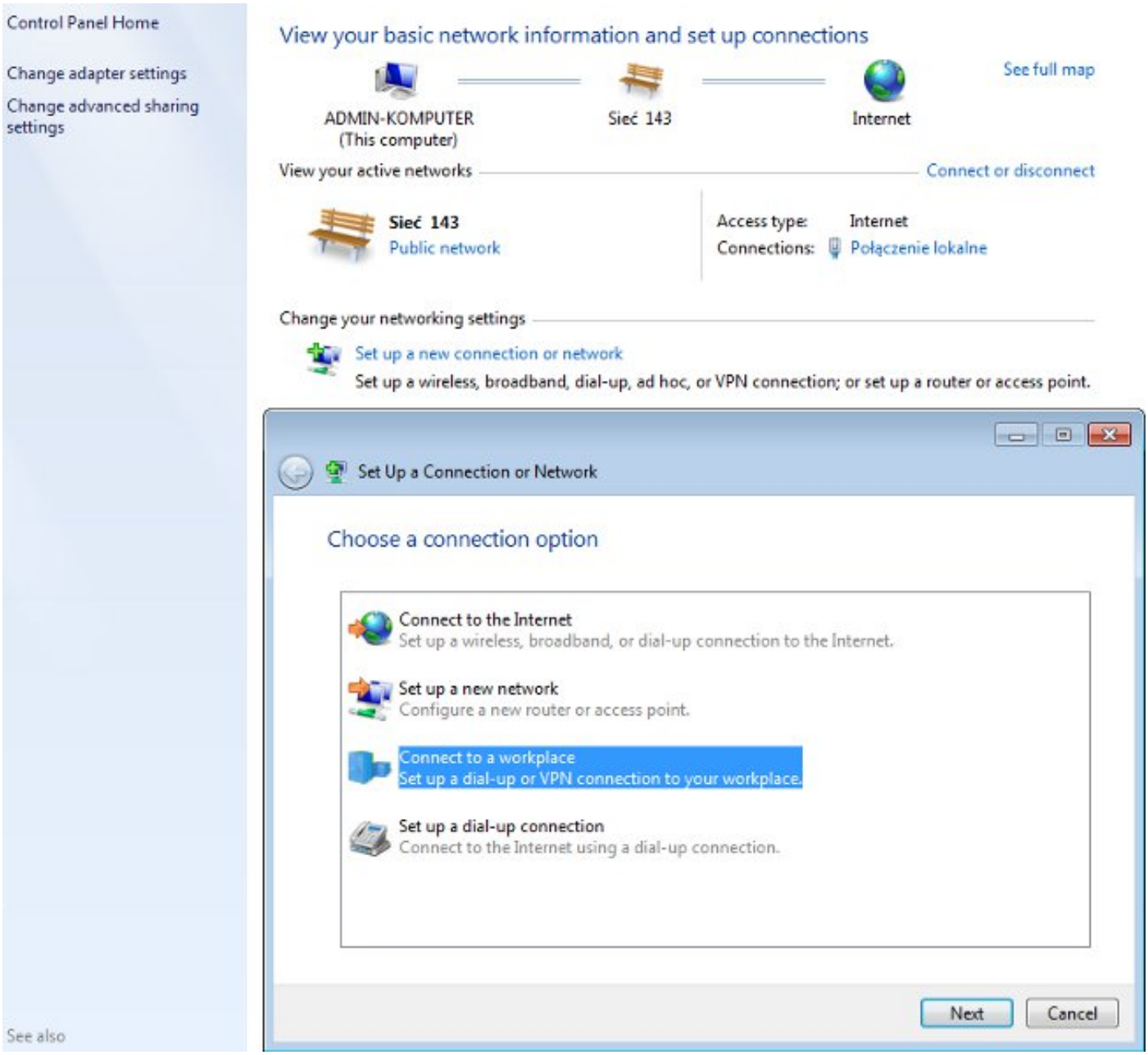


Si le client Windows ne peut pas valider le certificat présenté par l'ASA, il signale :

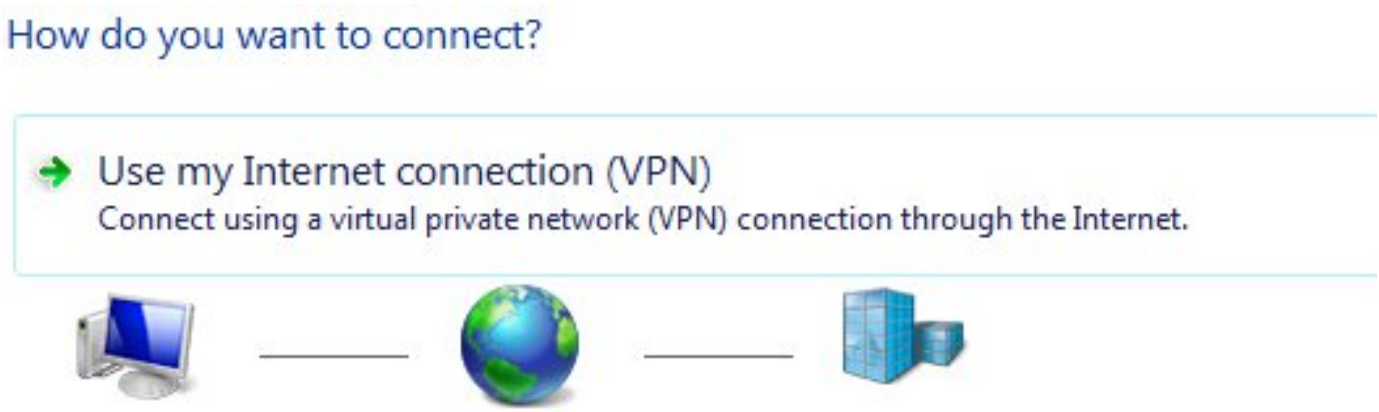
```
13801: IKE authentication credentials are unacceptable
```

Étape 2. Configurez la connexion VPN.

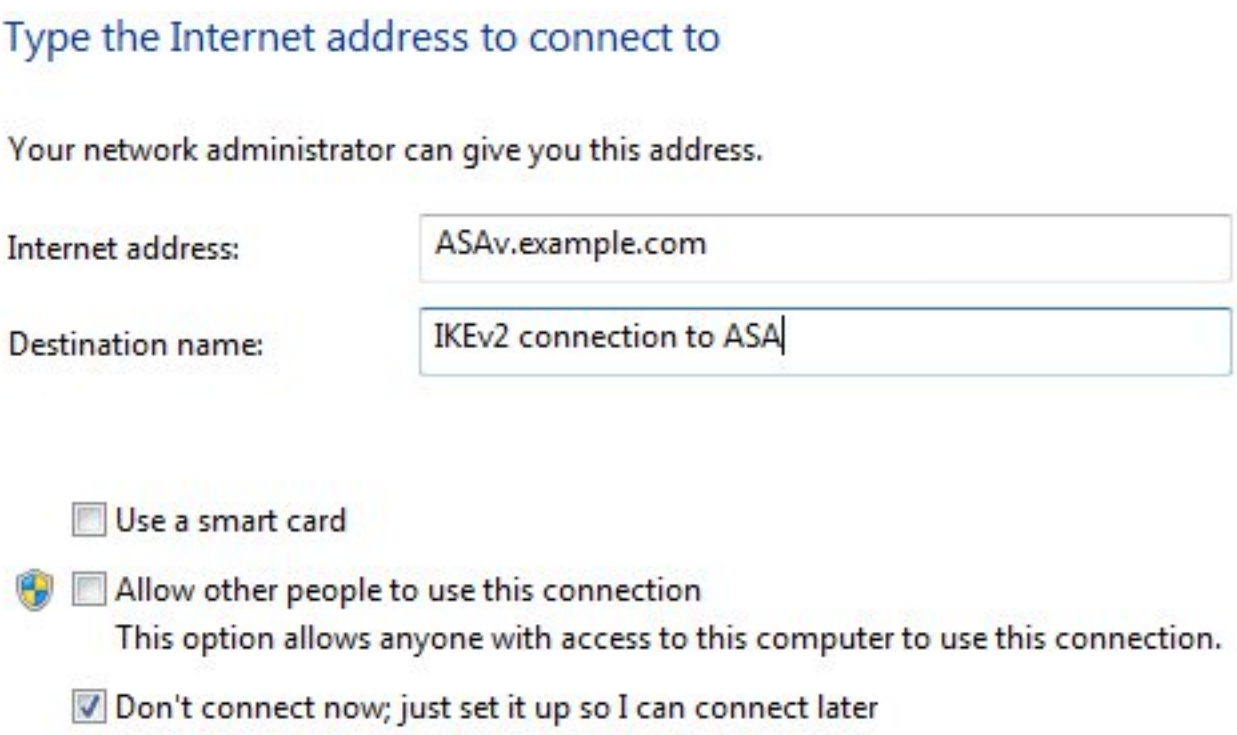
Afin de configurer la connexion VPN à partir du Centre Réseau et Partage, choisissez **Se connecter à un lieu de travail** afin de créer une connexion VPN.



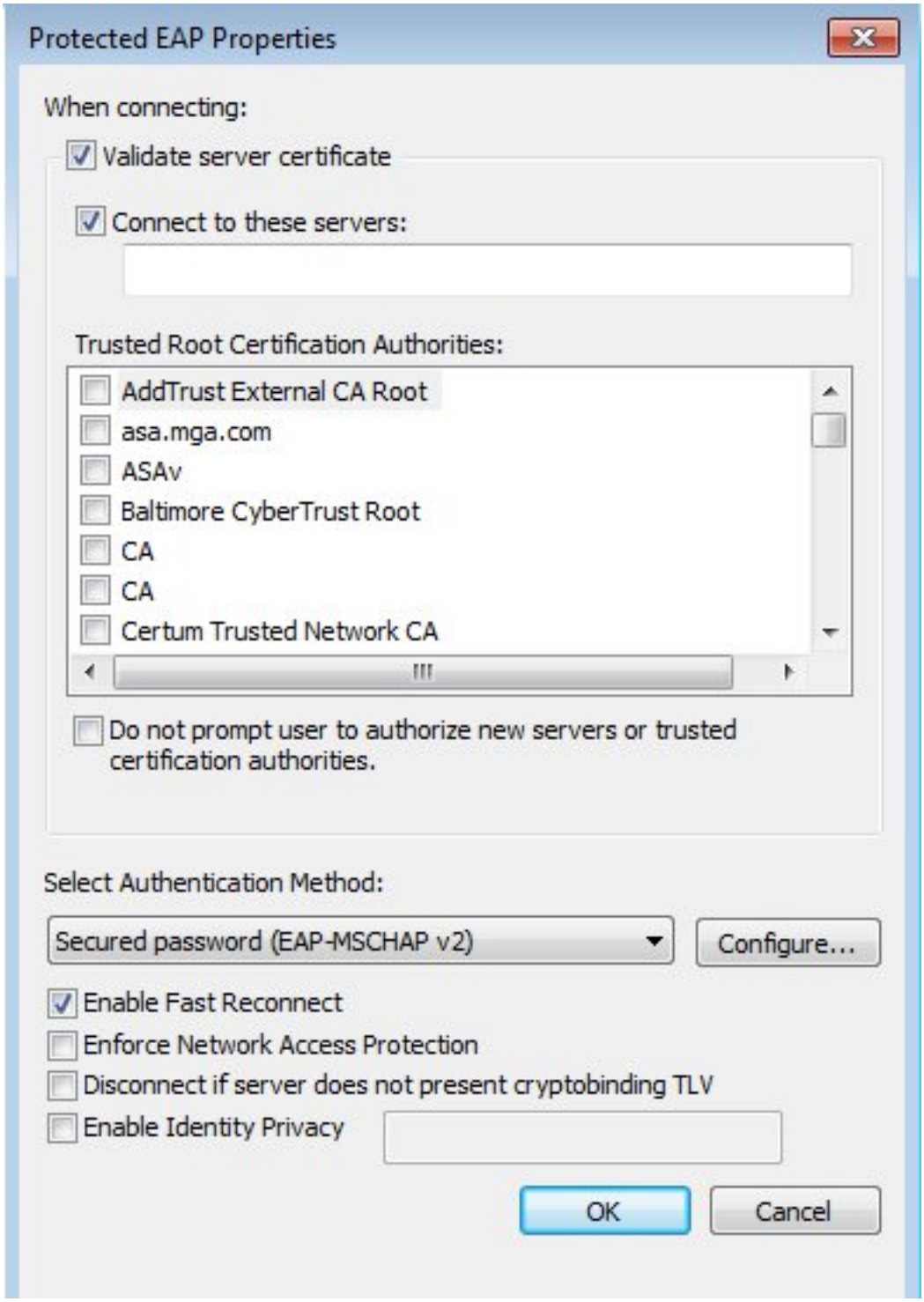
Choisissez **Utiliser ma connexion Internet (VPN)**.



Configurez l'adresse avec un FQDN ASA. Assurez-vous qu'elle est correctement résolue par le serveur de noms de domaine (DNS).



Si nécessaire, ajustez les propriétés (telles que la validation du certificat) dans la fenêtre Propriétés EAP protégées.



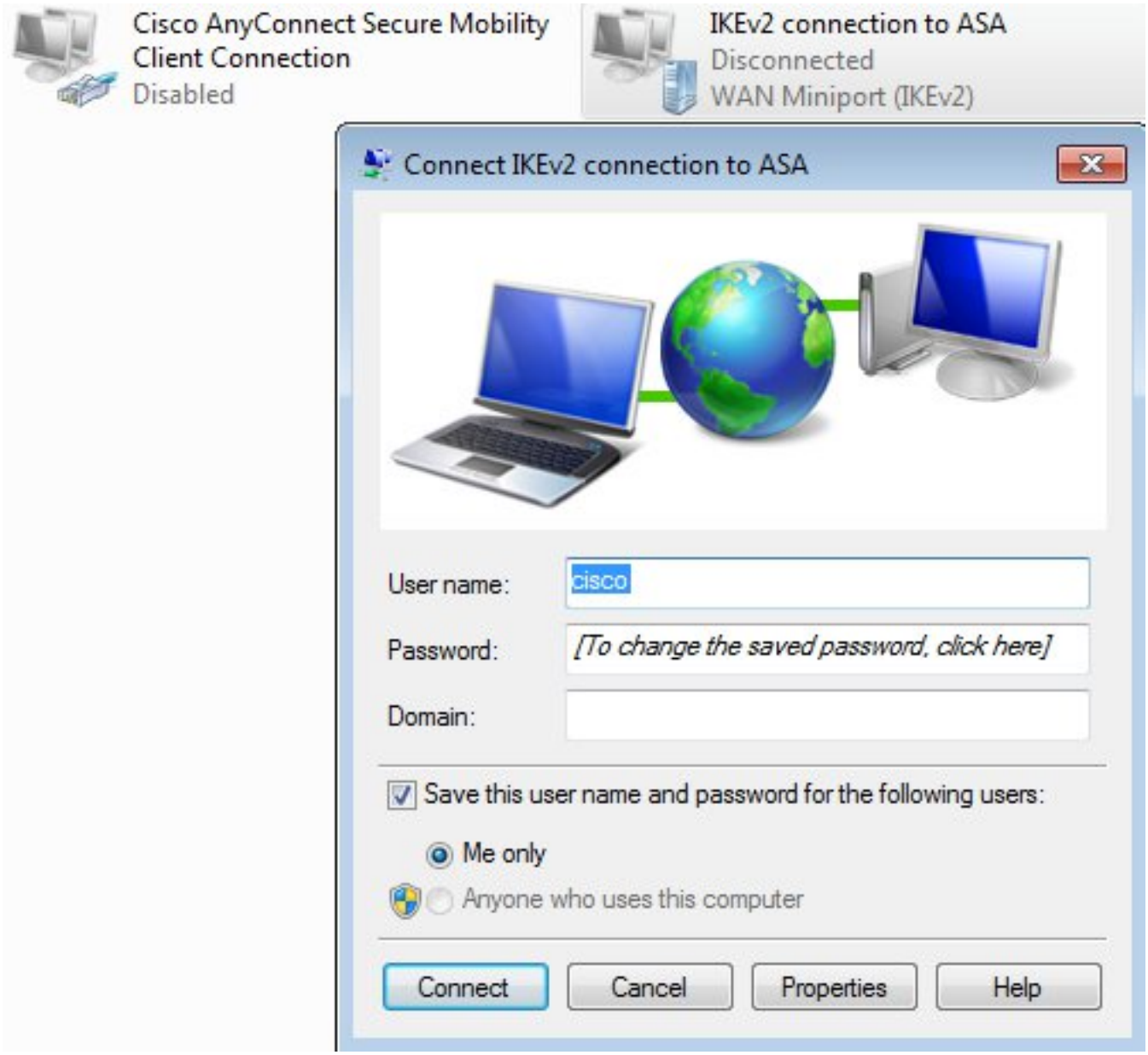
Vérification

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

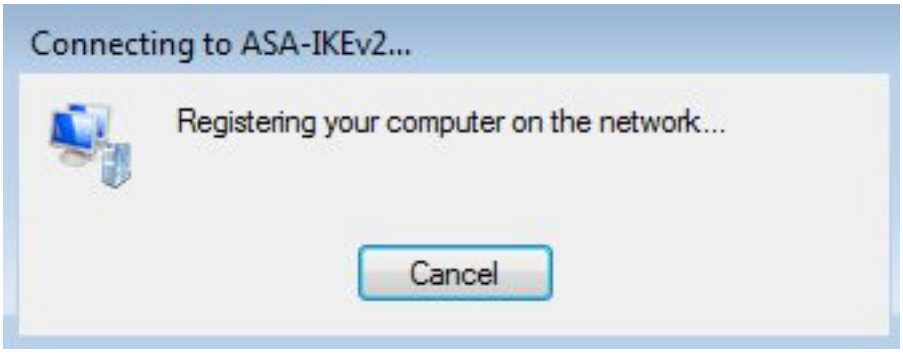
L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines **commandes d'affichage.** Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Client Windows

Lorsque vous vous connectez, saisissez vos informations d'identification.



Après authentification réussie, la configuration IKEv2 est appliquée.



La session est UP.

La table de routage a été mise à jour avec la route par défaut avec l'utilisation d'une nouvelle interface avec la métrique basse.

```
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
===========================================================================
```

Journaux

Après l'authentification réussie, l'ASA signale :

```
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 journaux ISE indiquent une authentification réussie avec des règles d'authentification et d'autorisation par défaut.

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

Débogues sur ASA

Les débogages les plus importants sont les suivants :

```
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 clés pour Diffie-Hellman (DH)) :

```
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 à l'initiateur (inclut les propositions IKEv2, l'échange de clés pour DH 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_AUTH pour le client avec IKE-ID, demande de certificat, jeux de transformation proposés, configuration demandée et sélecteurs de 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_AUTH de l'ASA qui inclut une demande d'identité EAP (premier paquet avec des extensions EAP). Ce paquet inclut également le certificat (s'il n'y a pas de certificat correct sur l'ASA, il y a une défaillance) :

```
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 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
```

Ensuite, plusieurs paquets sont échangés dans le cadre du protocole EAP-PEAP. Enfin, le succès du PAE est reçu par l'ASA et transmis au demandeur :

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

L'authentification homologue a réussi :

```
IKEv2-PROTO-2: (30): Verification of peer's authenctication data PASSED
```

Et la session VPN est terminée correctement.

Niveau de paquet

La demande d'identité EAP est encapsulée dans « Extensible Authentication » de l'IKE_AUTH envoyé par l'ASA. En plus de la demande d'identité, IKE_ID et les certificats sont envoyés.

No.	Source	Destination	Protocol	Length	Info
1	10.147.24.166	10.62.71.177	ISAKMP	570	IKE_SA_INIT
2	10.62.71.177	10.147.24.166	ISAKMP	501	IKE_SA_INIT
3	10.147.24.166	10.62.71.177	ISAKMP	990	IKE_AUTH
4	10.147.24.166	10.62.71.177	ISAKMP	959	IKE_AUTH
5	10.62.71.177	10.147.24.166	EAP	1482	Request, Identity
6	10.62.71.177	10.147.24.166	ISAKMP	1514	

```
  Length: 1440
▷ Type Payload: Vendor ID (43) : Unknown Vendor ID
▷ Type Payload: Identification - Responder (36)
▽ Type Payload: Certificate (37)
    Next payload: Authentication (39)
    0... .... = Critical Bit: Not Critical
    Payload length: 1203
    Certificate Encoding: X.509 Certificate - Signature (4)
  ▷ Certificate Data (iso.2.840.113549.1.9.2=ASAv.example.com)
▷ Type Payload: Authentication (39)
▽ Type Payload: Extensible Authentication (48)
    Next payload: NONE / No Next Payload  (0)
    0... .... = Critical Bit: Not Critical
    Payload length: 10
  ▽ Extensible Authentication Protocol
      Code: Request (1)
      Id: 36
      Length: 6
      Type: Identity (1)
      Identity:
```

Tous les paquets EAP suivants sont encapsulés dans IKE_AUTH. Une fois que le demandeur a

confirmé la méthode (EAP-PEAP), il commence à construire un tunnel SSL (Secure Sockets Layer) qui protège la session MSCHAPv2 utilisée pour l'authentification.

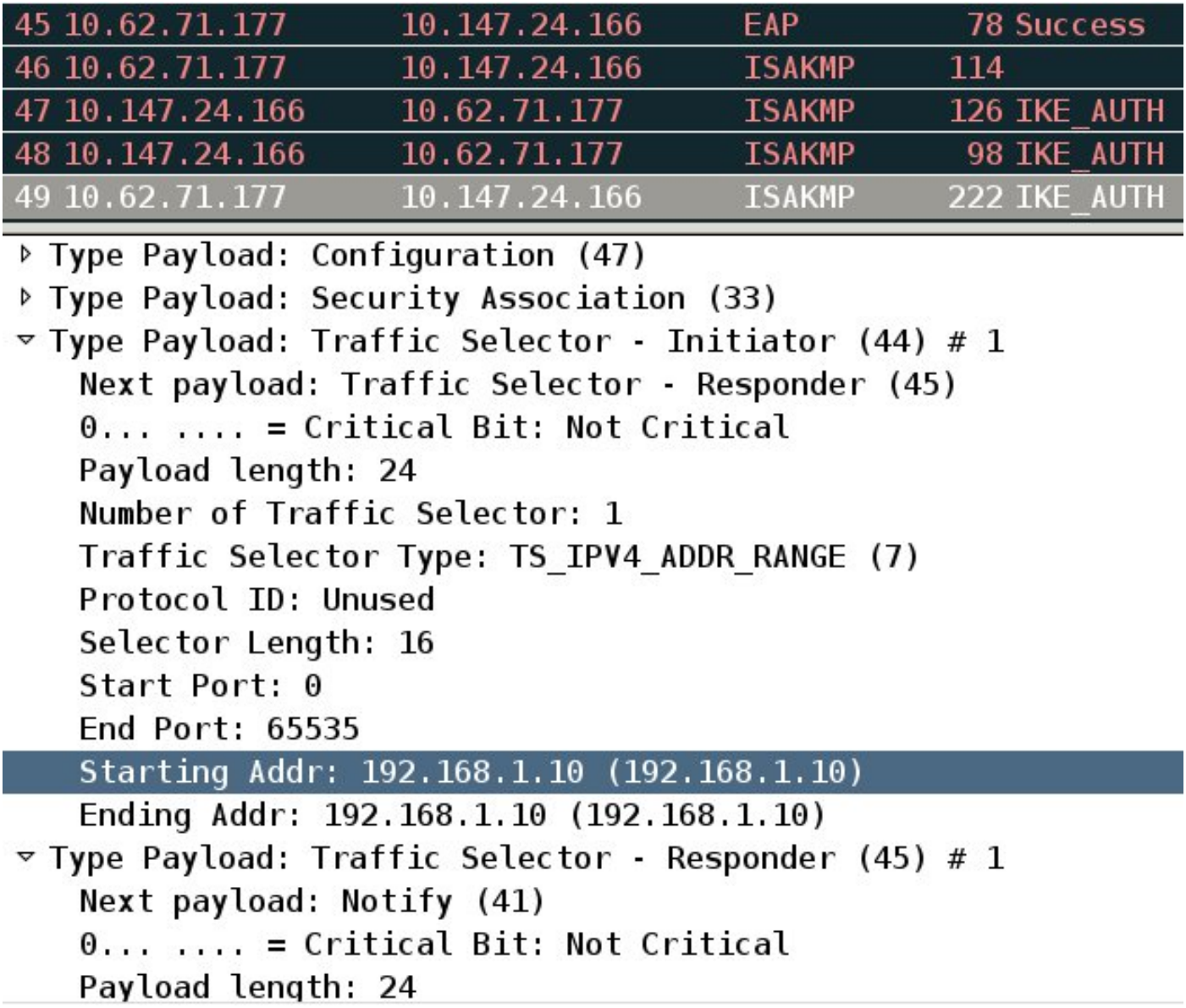
5	10.62.71.177	10.147.24.166	EAP	1482	Request, Identity
6	10.62.71.177	10.147.24.166	ISAKMP	1514	
7	10.147.24.166	10.62.71.177	ISAKMP	110	IKE_AUTH
8	10.147.24.166	10.62.71.177	EAP	84	Response, Identity
9	10.62.71.177	10.147.24.166	EAP	80	Request, Protected EAP (EAP-PEAP)
10	10.62.71.177	10.147.24.166	ISAKMP	114	
11	10.147.24.166	10.62.71.177	ISAKMP	246	IKE_AUTH
12	10.147.24.166	10.62.71.177	SSL	220	Client Hello
13	10.62.71.177	10.147.24.166	TLSv1	1086	Server Hello

Après l'échange de plusieurs paquets, ISE confirme la réussite.

43	10.147.24.166	10.62.71.177	ISAKMP	150	IKE_AUTH
44	10.147.24.166	10.62.71.177	TLSv1	117	Application Data
45	10.62.71.177	10.147.24.166	EAP	78	Success

```
▾ Type Payload: Extensible Authentication (48)
    Next payload: NONE / No Next Payload  (0)
    0... .... = Critical Bit: Not Critical
    Payload length: 8
  ▾ Extensible Authentication Protocol
      Code: Success (3)
      Id: 101
      Length: 4
```

La session IKEv2 est terminée par l'ASA, la configuration finale (réponse de configuration avec des valeurs telles qu'une adresse IP attribuée), les jeux de transformation et les sélecteurs de trafic sont transmis au client VPN.



Dépannage

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

Informations connexes

- Guide de configuration du CLI VPN de la série Cisco ASA, 9.3
- Guide de l'utilisateur de la plateforme de services d'identité de Cisco, version 1.2
- Support et documentation techniques - Cisco Systems