Configuración del acceso remoto ASA IKEv2 con EAP-PEAP y cliente nativo de Windows

Contenido

Introducción

Este documento proporciona un ejemplo de configuración para Cisco Adaptive Security Appliance (ASA) versión 9.3.2 y posteriores que permite el acceso VPN remoto para utilizar el protocolo de intercambio de claves de Internet (IKEv2) con autenticación estándar del protocolo de autenticación extensible (EAP). Esto permite que un cliente nativo de Microsoft Windows 7 (y cualquier otro IKEv2 basado en estándares) se conecte al ASA con IKEv2 y autenticación EAP.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de VPN e IKEv2
- Conocimiento básico de autenticación, autorización y contabilidad (AAA) y RADIUS
- Experiencia con la configuración de ASA VPN
- Experiencia con la configuración de Identity Services Engine (ISE)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft Windows 7
- Software Cisco ASA, versión 9.3.2 y posteriores
- Cisco ISE, versión 1.2 y posteriores

Antecedentes

Consideraciones de AnyConnect Secure Mobility Client

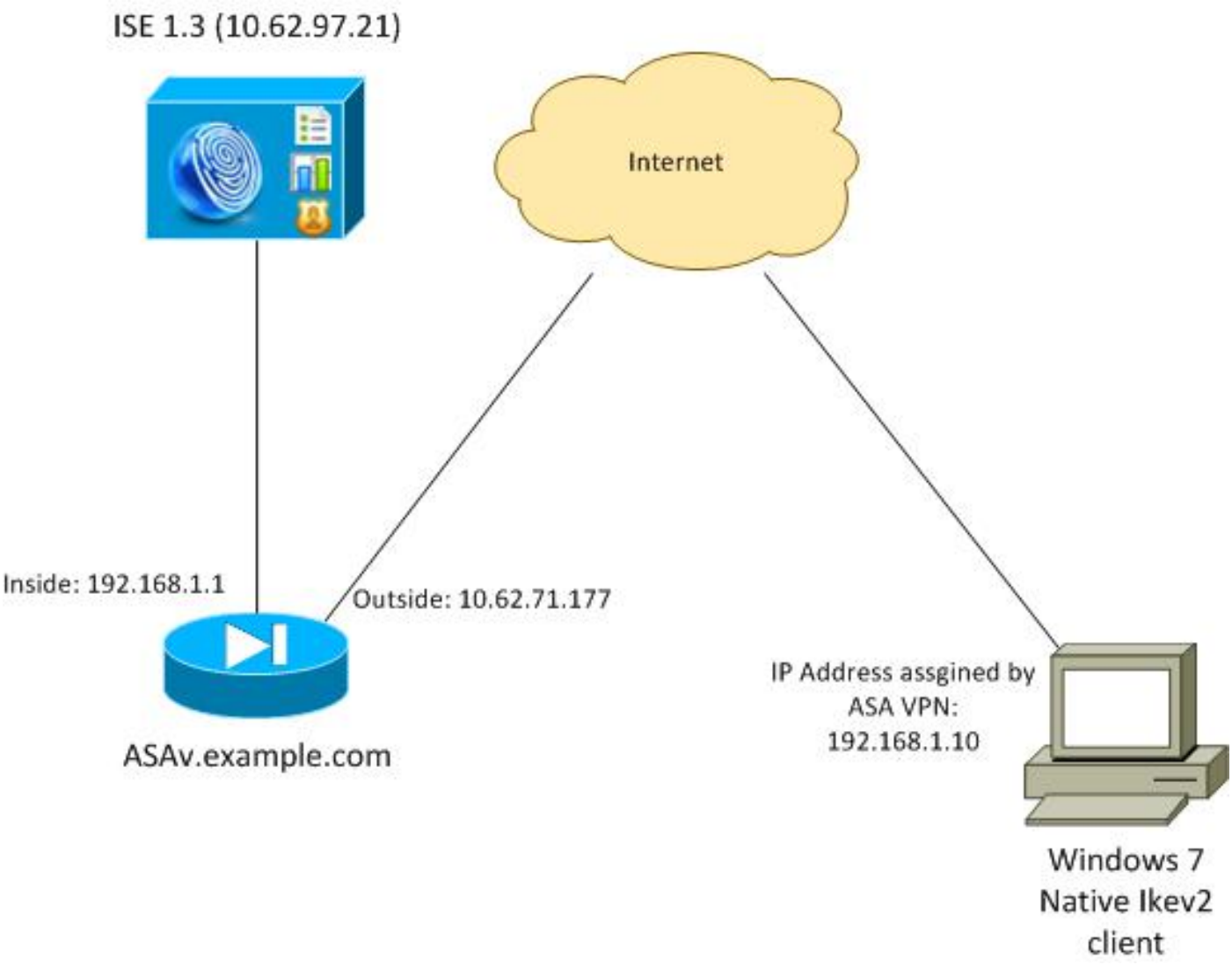
El cliente nativo de Windows IKEv2 no admite túnel dividido (no hay atributos CONF REPLY que puedan ser aceptados por el cliente de Windows 7), por lo que la única política posible con el cliente de Microsoft es tunelizar todo el tráfico (selectores de tráfico 0/0). Si se necesita una política de túnel dividido específica, se debe utilizar AnyConnect.

AnyConnect no admite métodos EAP estandarizados que se terminan en el servidor AAA (PEAP, seguridad de la capa de transporte). Si hay una necesidad de terminar las sesiones EAP en el servidor AAA, se puede utilizar el cliente de Microsoft.

Configurar

> **Nota:** Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red



El ASA está configurado para autenticarse con un certificado (el cliente necesita confiar en ese certificado). El cliente de Windows 7 está configurado para autenticarse con EAP (EAP-PEAP).

El ASA actúa como gateway VPN que finaliza la sesión IKEv2 del cliente. El ISE actúa como un servidor AAA que finaliza la sesión EAP del cliente. Los paquetes EAP se encapsulan en paquetes IKE_AUTH para el tráfico entre el cliente y ASA (IKEv2) y, a continuación, en paquetes RADIUS para el tráfico de autenticación entre el ASA y el ISE.

Certificados

Se ha utilizado Microsoft Certificate Authority (CA) para generar el certificado para ASA. Los requisitos del certificado para ser aceptados por el cliente nativo de Windows 7 son:

- La extensión Uso de clave extendido (EKU) debe incluir la autenticación de servidor (en ese ejemplo se ha utilizado la plantilla "Servidor web").
- El nombre del asunto debe incluir el nombre de dominio completo (FQDN) que utilizará el cliente para conectarse (en este ejemplo, ASAv.example.com).

Para obtener más detalles sobre el cliente de Microsoft, vea Solución de problemas de conexiones VPN IKEv2.

Nota: Android 4.x es más restrictivo y requiere el nombre alternativo del asunto correcto

según RFC 6125. Para obtener más información sobre Android, vea IKEv2 de Android strongSwan a Cisco IOS con EAP y autenticación RSA.

Para generar una solicitud de firma de certificado en el ASA, se ha utilizado esta configuración:

```
hostname ASAv
domain-name example.com

crypto ca trustpoint TP
enrollment terminal

crypto ca authenticate TP
crypto ca enroll TP
```

ISE

Paso 1. Agregue el ASA a los dispositivos de red del ISE.

Elija **Administration > Network Devices**. Establezca una contraseña previamente compartida que será utilizada por el ASA.

Paso 2. Cree un nombre de usuario en el almacén local.

Elija **Administration > Identities > Users**. Cree el nombre de usuario según sea necesario.

El resto de la configuración se habilita de forma predeterminada para que ISE autentique los terminales con EAP-PEAP (protocolo de autenticación extensible protegido).

ASA

La configuración para el acceso remoto es similar para IKEv1 e 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
```

Dado que Windows 7 envía una dirección de tipo IKE-ID en el paquete IKE_AUTH, se debe utilizar el **DefaultRAGroup** para asegurarse de que la conexión se encuentra en el grupo de túnel correcto. El ASA se autentica con un certificado (autenticación local) y espera que el cliente utilice EAP (autenticación remota). Además, ASA necesita enviar específicamente una solicitud de identidad EAP para que el cliente responda con una respuesta de identidad 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
```

Por último, se debe habilitar IKEv2 y utilizar el certificado correcto.

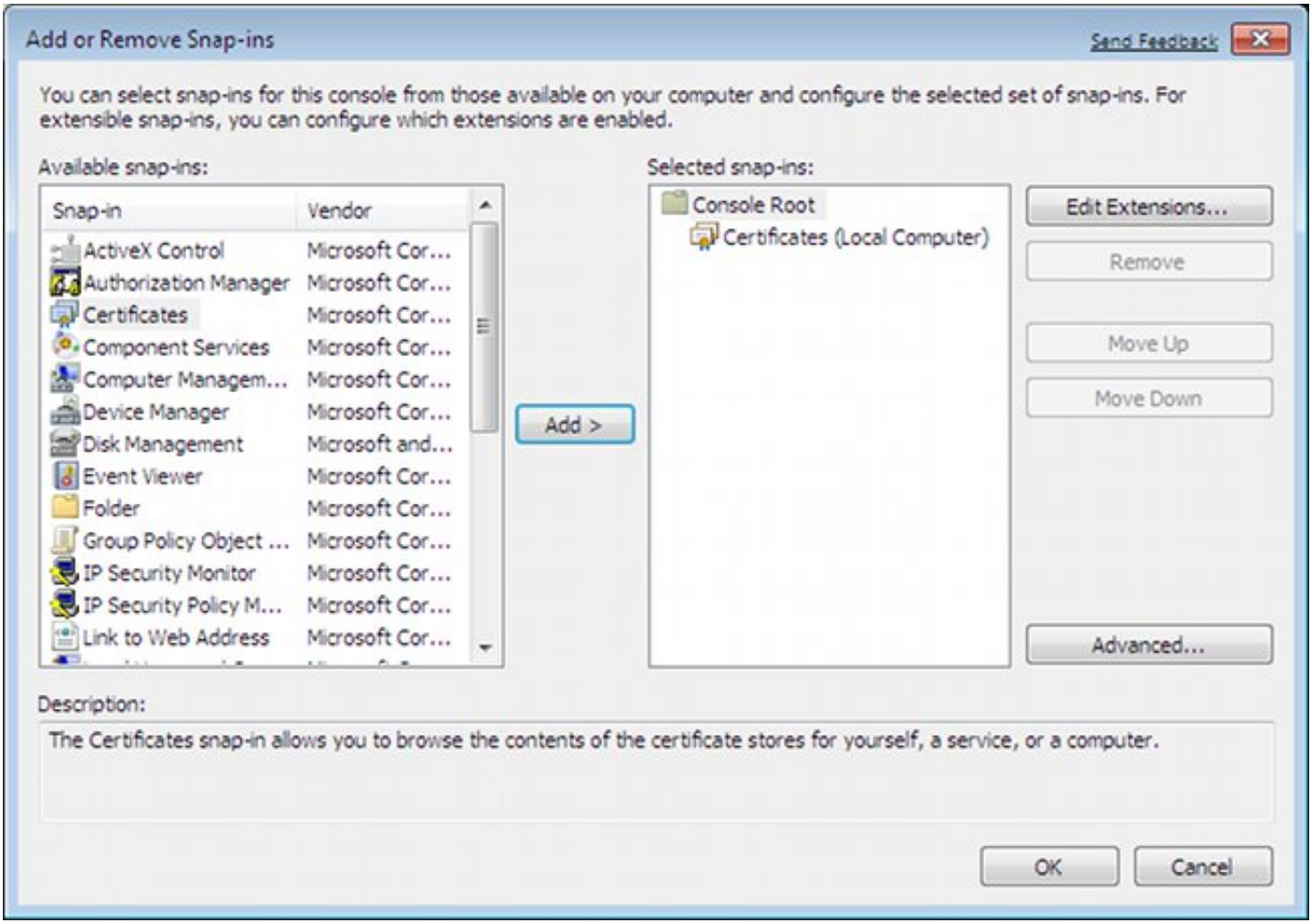
```
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint TP
```

Windows 7

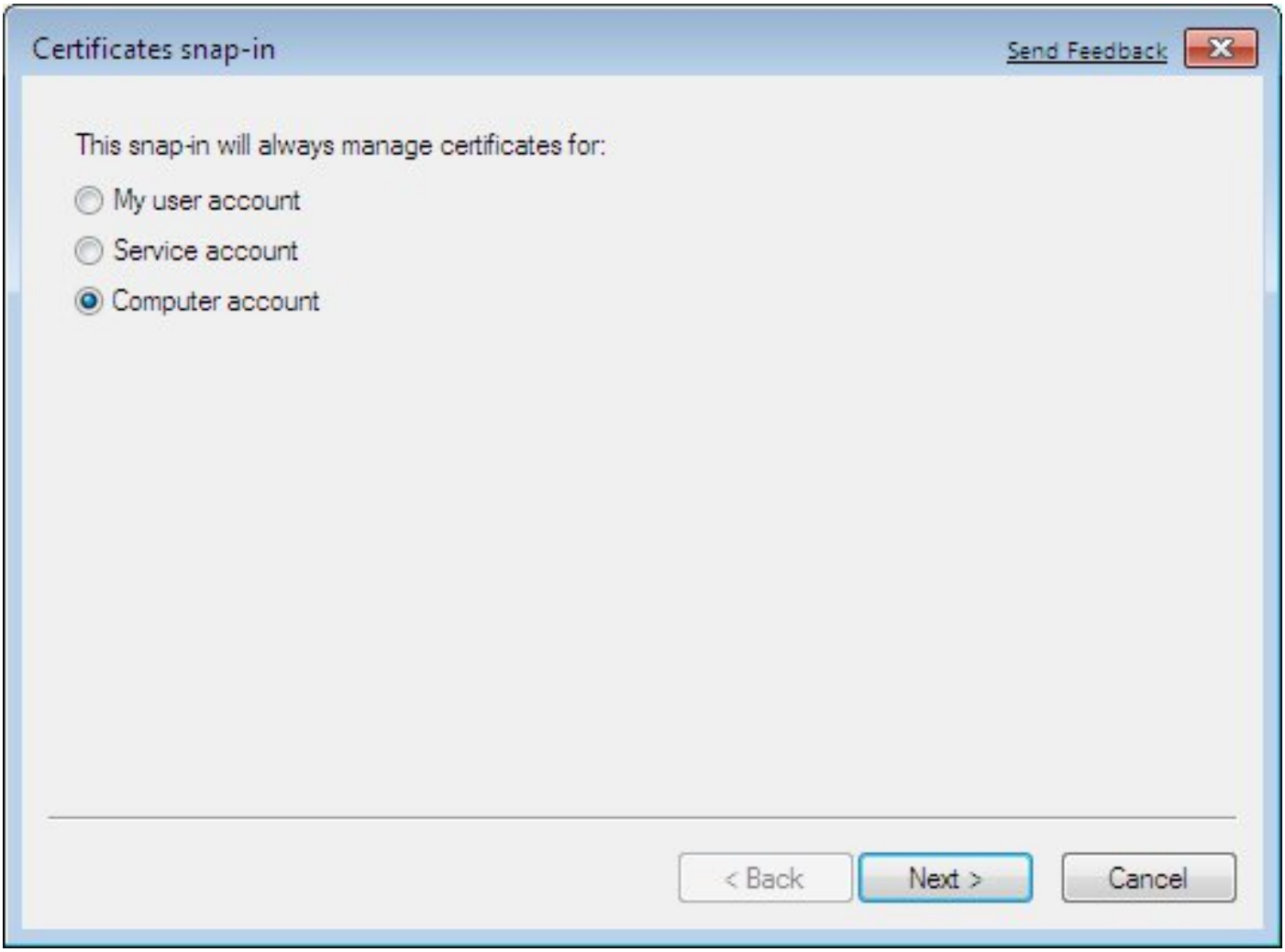
Paso 1. Instale el certificado de CA.

Para confiar en el certificado presentado por el ASA, el cliente de Windows necesita confiar en su CA. Ese certificado de CA se debe agregar al almacén de certificados del equipo (no al almacén de usuarios). El cliente de Windows utiliza el almacén del equipo para validar el certificado IKEv2.

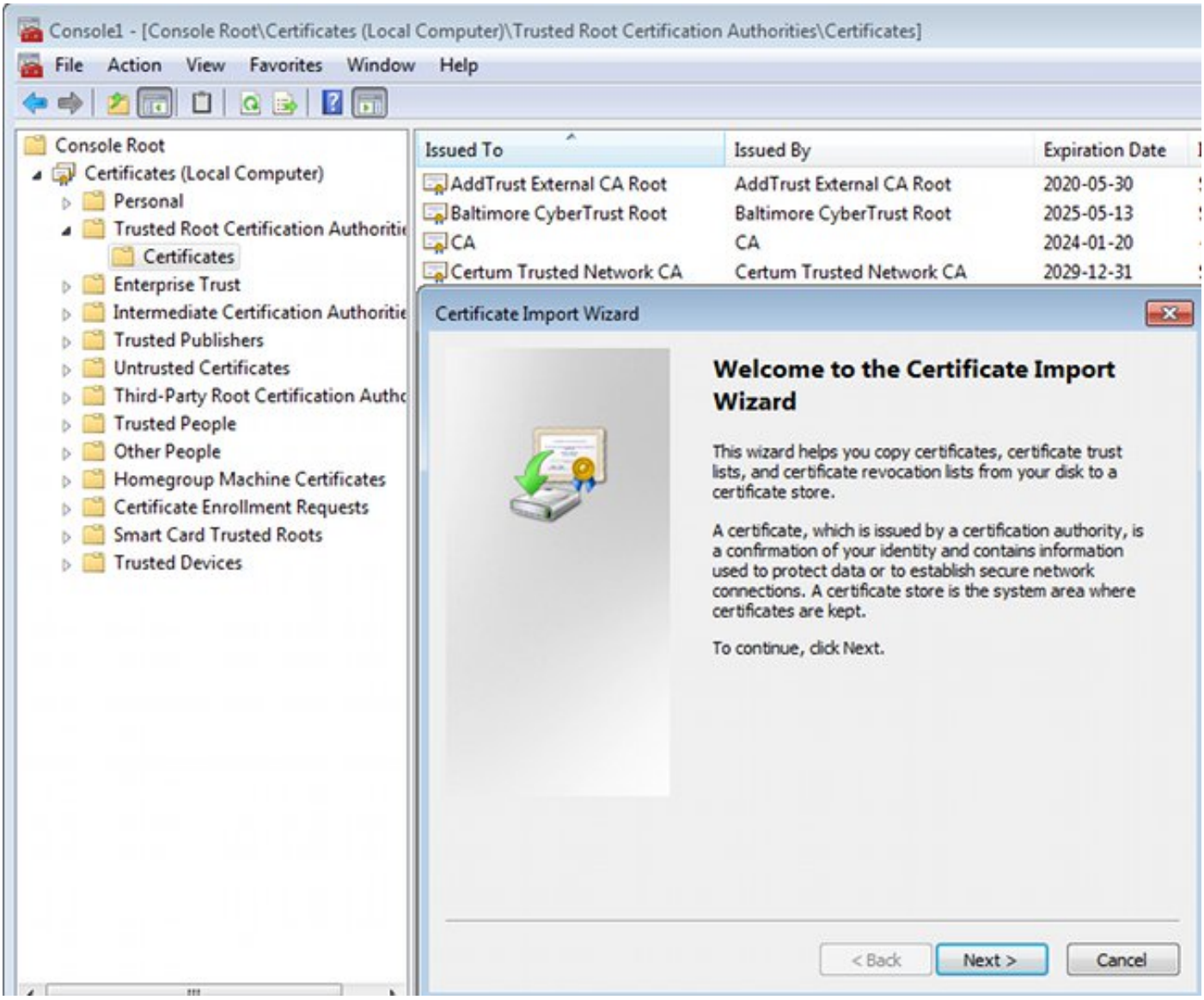
Para agregar la CA, elija **MMC > Agregar o quitar complementos > Certificados**.



Haga clic en el botón de opción **Cuenta de equipo**.



Importe la CA a las autoridades de certificados raíz de confianza.

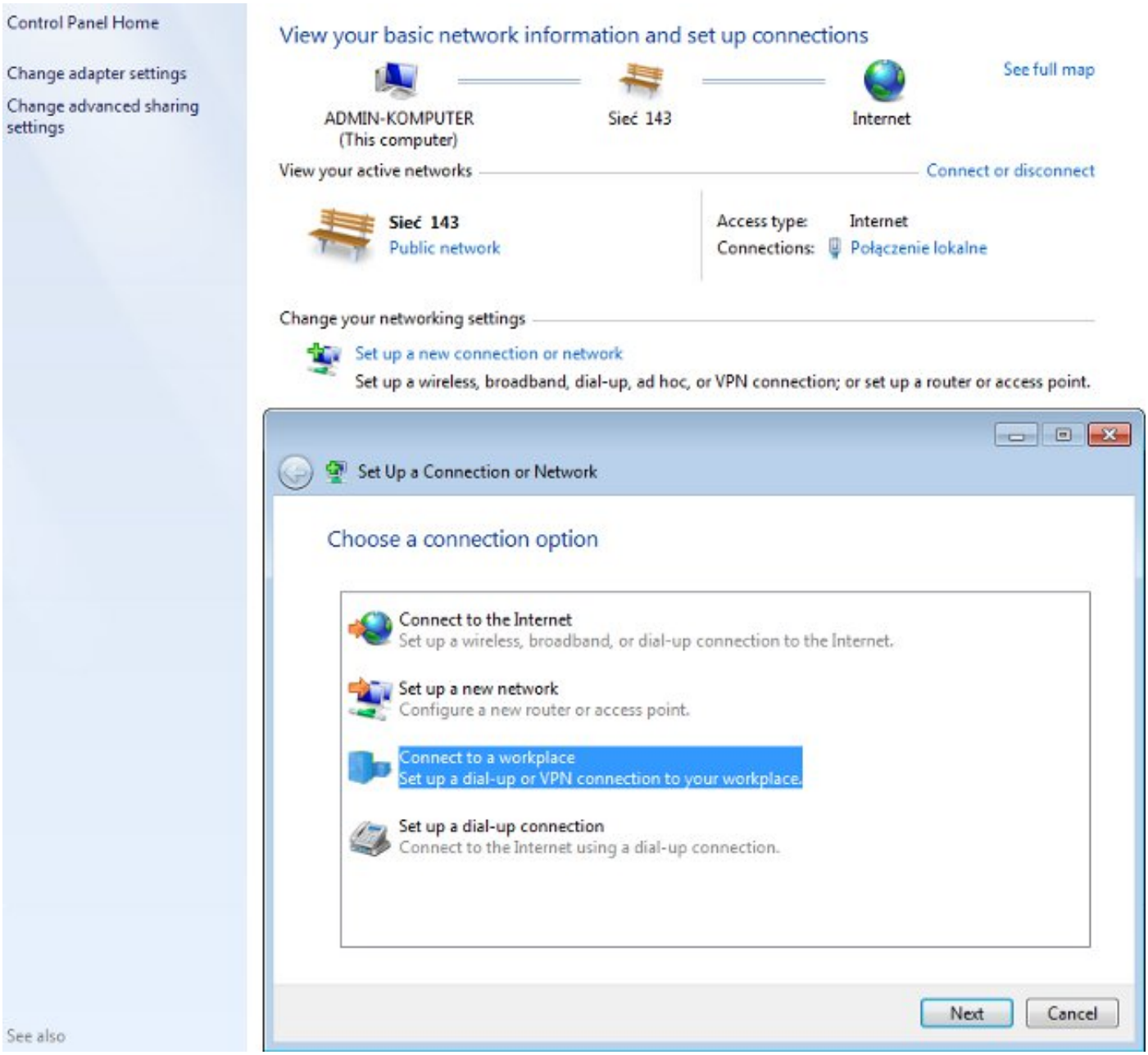


Si el cliente de Windows no puede validar el certificado presentado por el ASA, informa:

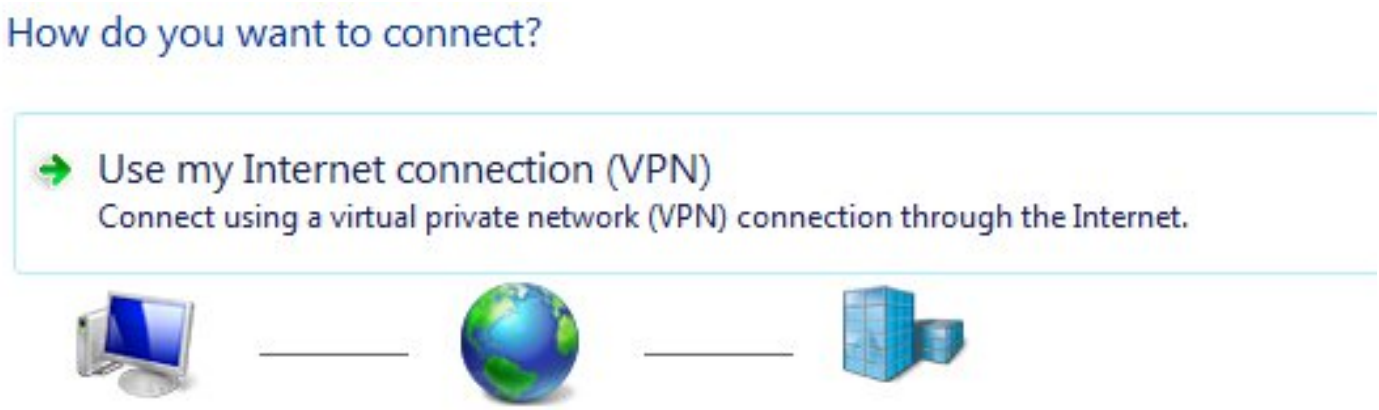
```
13801: IKE authentication credentials are unacceptable
```

Paso 2. Configure la conexión VPN.

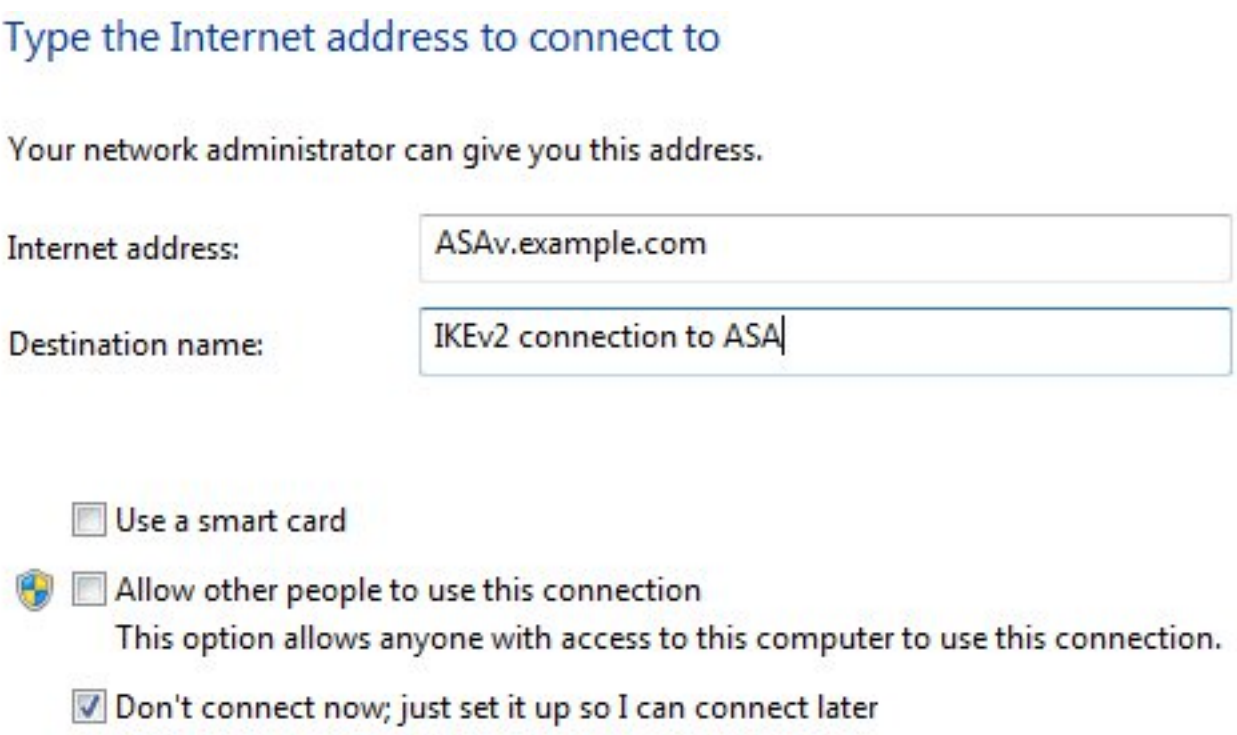
Para configurar la conexión VPN desde el Centro de Red y Uso Compartido, elija **Conectar a un lugar de trabajo** para crear una conexión VPN.



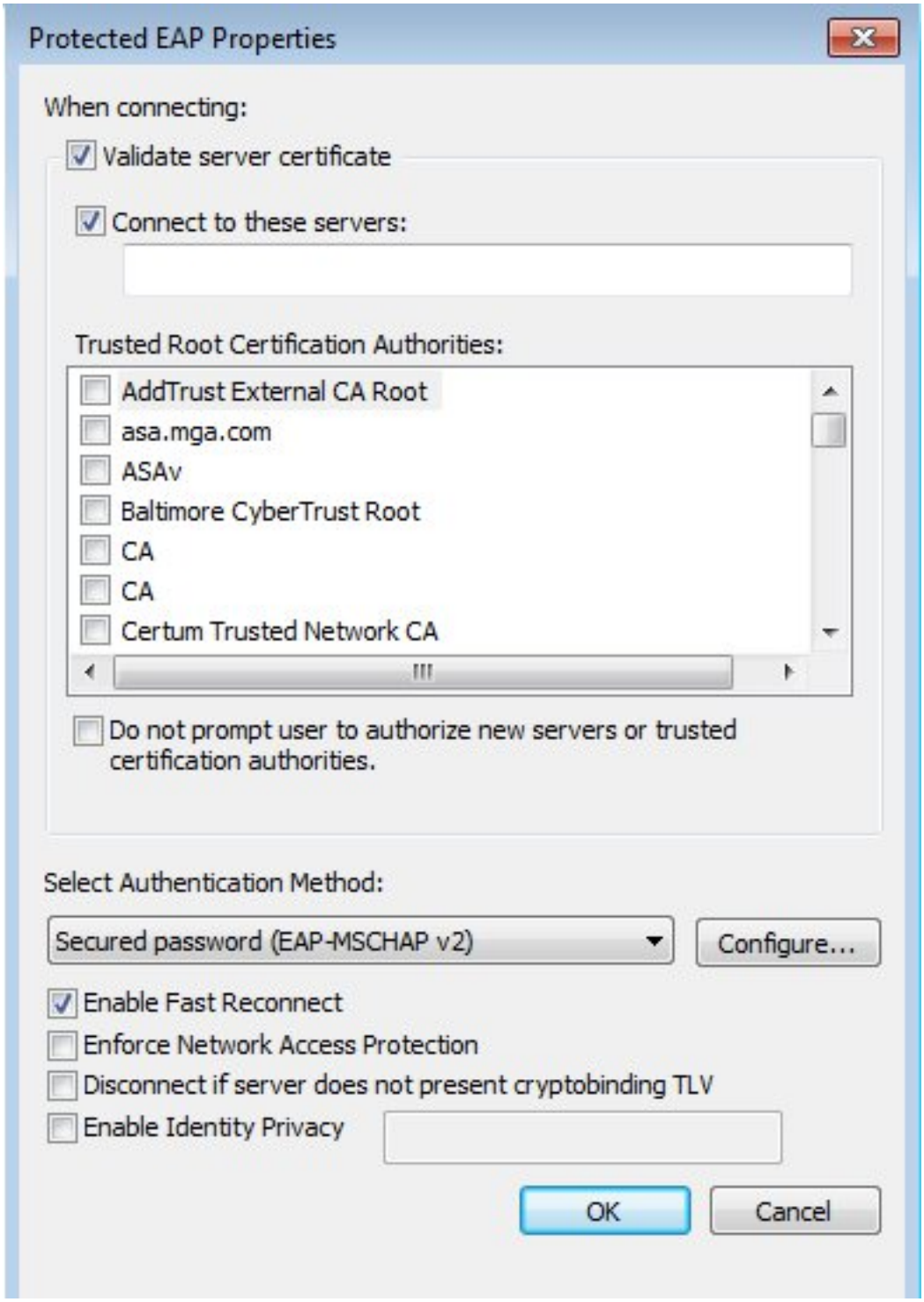
Elija **Usar mi conexión a Internet (VPN)**.



Configure la dirección con un FQDN de ASA. Asegúrese de que el servidor de nombres de dominio (DNS) lo resuelva correctamente.



Si es necesario, ajuste las propiedades (como la validación de certificados) en la ventana Propiedades EAP protegidas.



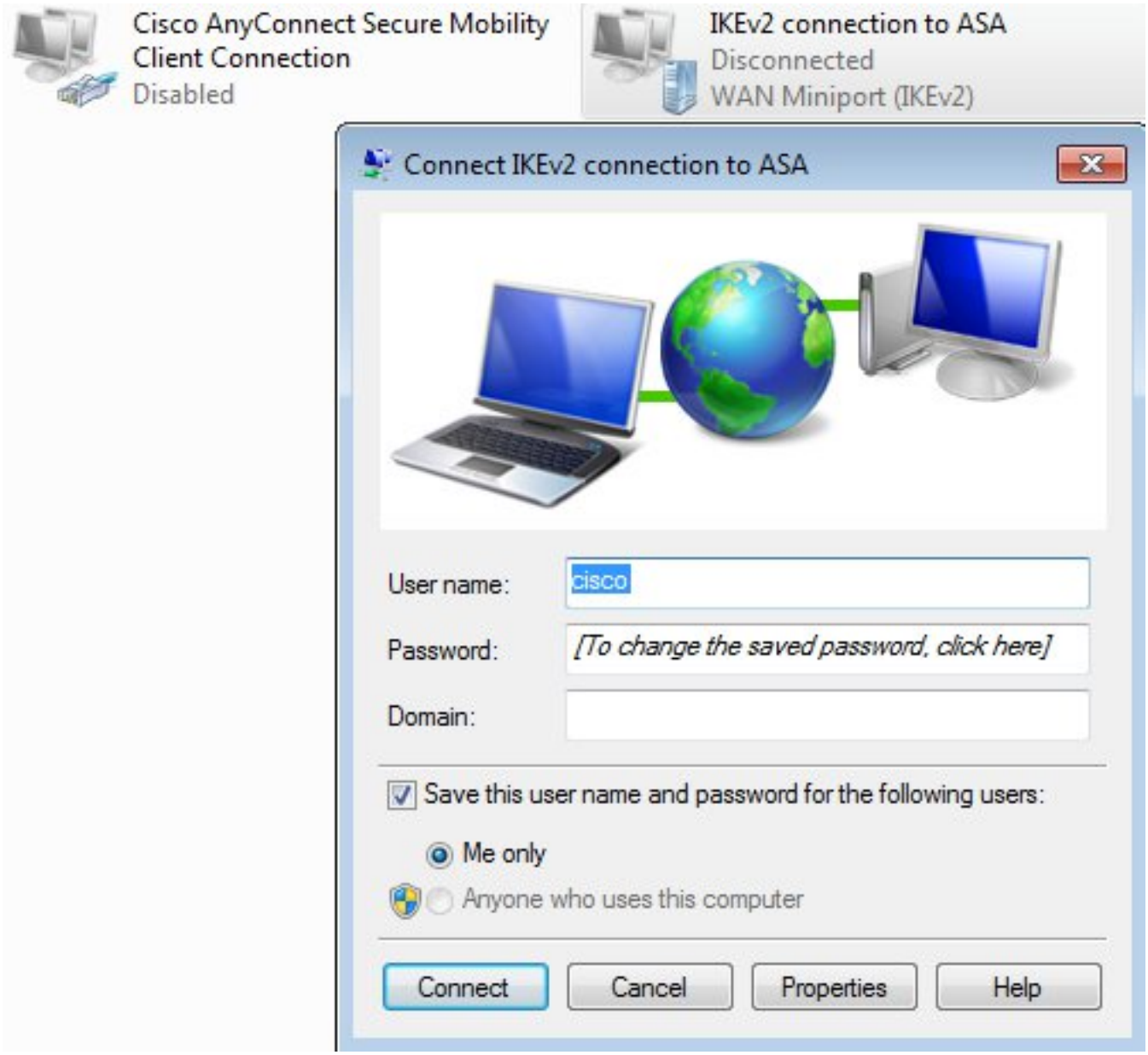
Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

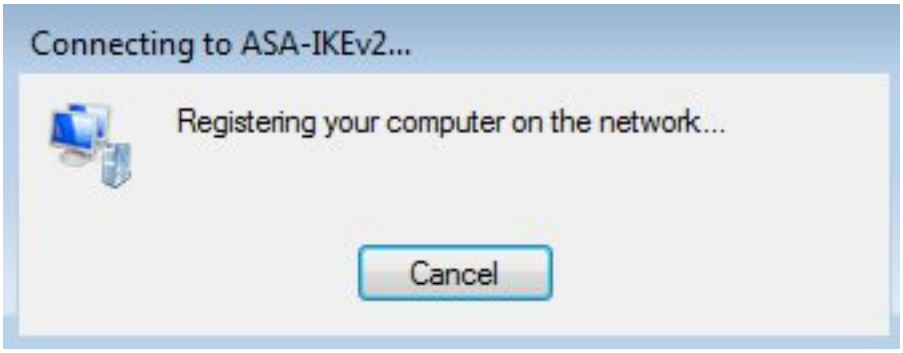
La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Cliente de Windows

Cuando se conecte, introduzca sus credenciales.



Después de una autenticación exitosa, se aplica la configuración IKEv2.



La sesión está activada.

La tabla de ruteo se ha actualizado con la ruta predeterminada con el uso de una nueva interfaz con la métrica baja.

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

Registros

Después de una autenticación exitosa, ASA informa:

```
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
```

Los registros de ISE indican una autenticación correcta con reglas de autenticación y autorización predeterminadas.

Los detalles indican el método 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

Depuraciones en ASA

Las depuraciones más importantes incluyen:

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

Paquete IKE_SA_INIT recibido por ASA (incluye propuestas IKEv2 e intercambio de claves para 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
.....
```

Respuesta IKE_SA_INIT al iniciador (incluye propuestas IKEv2, intercambio de claves para DH y solicitud de certificado):

```
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 para el cliente con IKE-ID, solicitud de certificado, conjuntos de transformación propuestos, configuración solicitada y selectores de tráfico:

```
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):
```

respuesta IKE_AUTH del ASA que incluye una solicitud de identidad EAP (primer paquete con extensiones EAP). Ese paquete también incluye el certificado (si no hay un certificado correcto en el ASA hay una falla):

```
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]
```

Respuesta EAP recibida por ASA (longitud 5, carga útil: 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
```

Luego se intercambian varios paquetes como parte de EAP-PEAP. Finalmente, el ASA recibe el éxito de EAP y se reenvía al solicitante:

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

La autenticación de par se realiza correctamente:

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

Y la sesión VPN ha finalizado correctamente.

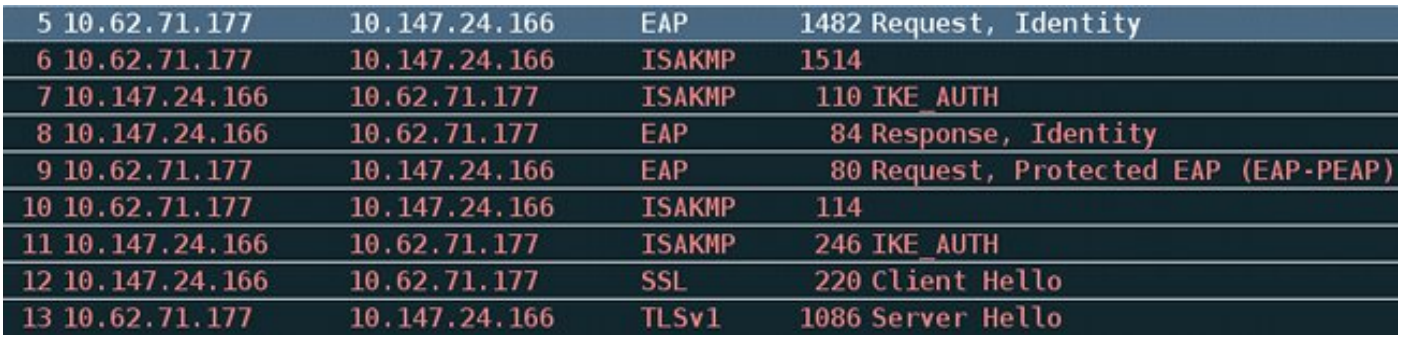
Nivel de paquete

La solicitud de identidad EAP se encapsula en "Extensible Authentication" (Autenticación extensible) de IKE_AUTH enviada por ASA. Junto con la solicitud de identidad, se envían IKE_ID y certificados.

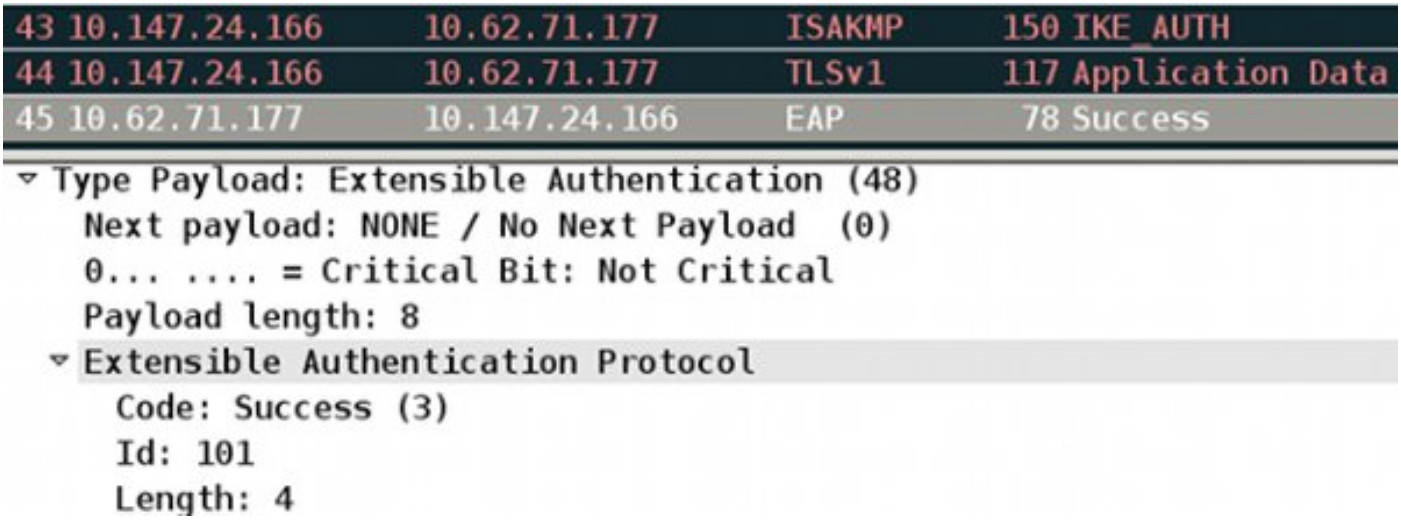
No.	Source	Destination	Protocol	Length	Info
1	10.147.24.166	10.62.71.177	ISAKMP	570	IKE_SA_INIT
2	10.62.71.177	10.147.24.166	ISAKMP	501	IKE_SA_INIT
3	10.147.24.166	10.62.71.177	ISAKMP	990	IKE_AUTH
4	10.147.24.166	10.62.71.177	ISAKMP	959	IKE_AUTH
5	10.62.71.177	10.147.24.166	EAP	1482	Request, Identity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

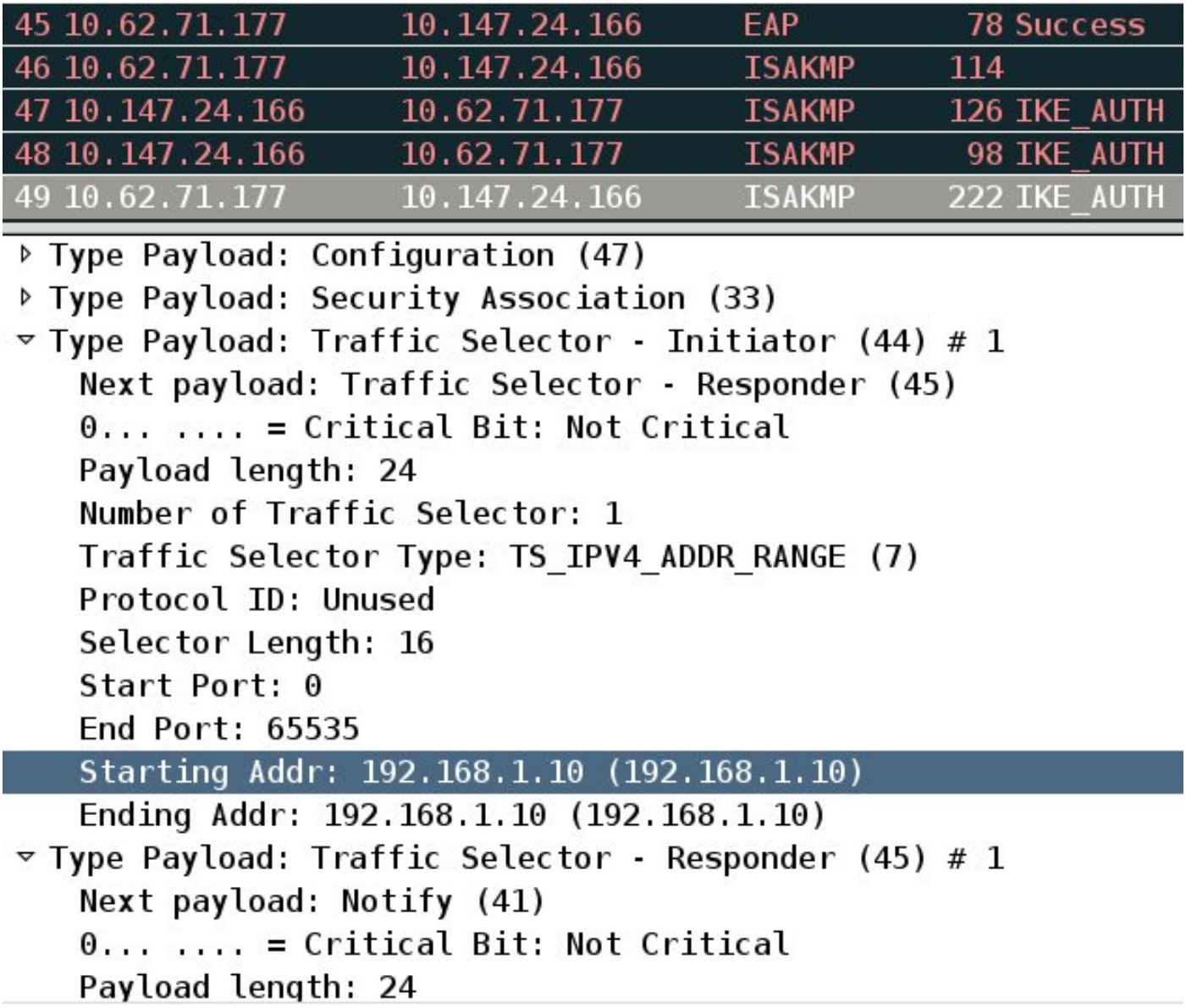
Todos los paquetes EAP subsiguientes se encapsulan en IKE_AUTH. Después de que el solicitante confirme el método (EAP-PEAP), comienza a crear un túnel de capa de sockets seguros (SSL) que protege la sesión MSCHAPv2 utilizada para la autenticación.



Después de intercambiar varios paquetes, ISE confirma el éxito.



ASA completa la sesión IKEv2, la configuración final (respuesta de configuración con valores como una dirección IP asignada), los conjuntos de transformación y los selectores de tráfico se envían al cliente VPN.



Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Guía de configuración CLI VPN Cisco Serie ASA, 9.3
- Guía de usuario de Cisco Identity Services Engine, versión 1.2
- Soporte Técnico y Documentación - Cisco Systems