

# Acceso Remoto de la configuración ASA IKEv2 con EAP-PEAP y el cliente de las ventanas nativas

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Consideraciones seguras del cliente de la movilidad de AnyConnect](#)

[Configurar](#)

[Diagrama de la red](#)

[Certificados](#)

[ISE](#)

[Paso 1. Agregue el ASA a los dispositivos de red en el ISE.](#)

[Paso 2. Cree un nombre de usuario en el almacén local.](#)

[ASA](#)

[Windows 7](#)

[Paso 1. Instale el certificado de CA.](#)

[Paso 2. Configure la conexión VPN.](#)

[Verificación](#)

[Cliente de Windows](#)

[Registros](#)

[Debugs en el ASA](#)

[Paquete llano](#)

[Troubleshooting](#)

[Información Relacionada](#)

## Introducción

Este documento proporciona un ejemplo de configuración para una versión 9.3.2 y posterior adaptante del dispositivo de seguridad de Cisco (ASA) que permita que el acceso del telecontrol VPN utilice el Internet Key Exchange Protocol (IKEv2) con la autenticación estándar del Protocolo de Autenticación Extensible (EAP). Esto permite que un cliente nativo de Microsoft Windows 7 (y cualquier otro IKEv2 estándar basado) conecten con el ASA con IKEv2 y la autenticación EAP.

## Prerrequisitos

## Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico VPN e IKEv2
- Autenticación básica, autorización, y estadísticas (AAA) y conocimiento RADIUS
- Experiencia con la configuración VPN ASA
- Experiencia con la configuración del 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 de Cisco ASA, versión 9.3.2 y posterior
- Cisco ISE, libera 1.2 y posterior

## Antecedentes

### Consideraciones seguras del cliente de la movilidad de AnyConnect

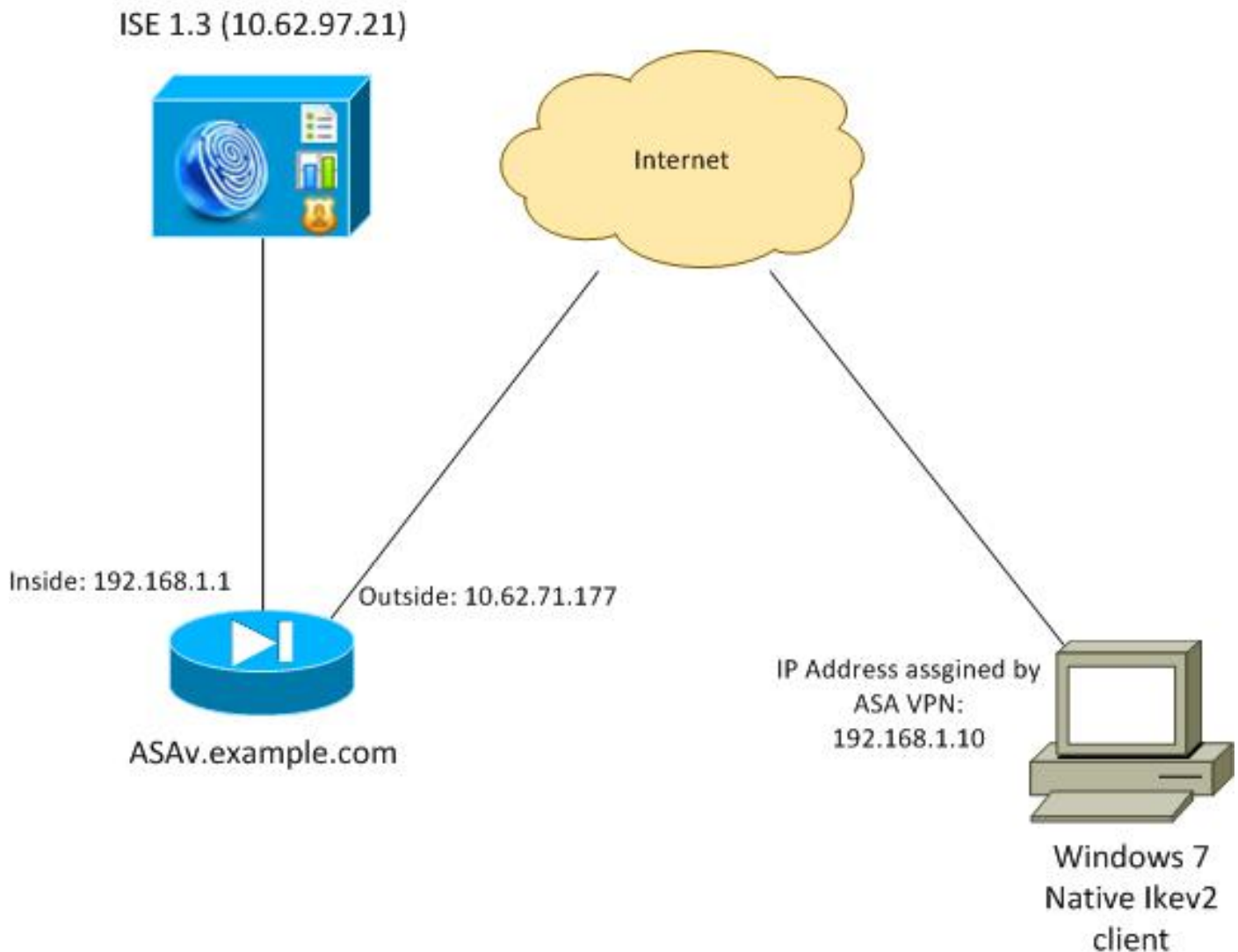
El cliente de las ventanas nativas IKEv2 no soporta el túnel dividido (no hay atributos de la CONTESTACIÓN CONF que se podrían validar por el cliente de Windows 7), así que la única directiva posible con el cliente Microsoft es hacer un túnel todo el tráfico (selectores de 0/0 tráfico). Si hay una necesidad de una directiva específica del túnel dividido, AnyConnect debe ser utilizado.

AnyConnect no soporta los métodos EAP estandarizados que se terminan en el servidor de AAA (PEAP, Transport Layer Security). Si hay una necesidad de terminar las sesiones EAP sobre el servidor de AAA entonces el cliente Microsoft puede ser utilizado.

## 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 se configura para autenticar con un certificado (el cliente necesita confiar en ese certificado). Configuran al cliente de Windows 7 para autenticar con EAP (EAP-PEAP).

El ASA actúa como gateway de VPN que termina la sesión IKEv2 del cliente. El ISE actúa como servidor de AAA que termina la sesión EAP del cliente. Los paquetes EAP se encapsulan en los paquetes IKE\_AUTH para el tráfico entre el cliente y el ASA (IKEv2) y entonces en los paquetes RADIUS para el tráfico de la autenticación entre el ASA y el ISE.

## Certificados

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

- La extensión dominante extendida del uso (EKU) debe incluir la autenticación de servidor (la plantilla "servidor Web" se ha utilizado en ese ejemplo).
- El Tema-nombre debe incluir el nombre de dominio completo (FQDN) que será utilizado por el cliente para conectar (en este ejemplo ASAv.example.com).

Para más detalles en el cliente Microsoft, vea [resolver problemas las conexiones VPN IKEv2](#).

Nota: Android 4.x es más restrictivo y requiere el nombre alternativo sujeto correcto según el RFC 6125. Para más información para Android, vea [IKEv2 de Android strongSwan al Cisco](#)

## [IOS con el EAP y la Autenticación RSA.](#)

Para generar un pedido 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 en el ISE.**

Elija la **administración > los dispositivos de red**. Fije una contraseña del preshared que sea utilizada por el ASA.

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

Elija la **administración > las identidades > Users**. Cree el nombre de usuario como sea necesario.

El resto de las configuraciones se habilitan por abandono para que el ISE autentique los puntos finales con EAP-PEAP (protocolo extensible authentication 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
```

Puesto que Windows 7 envía un direccionamiento del tipo IKE-ID en el paquete IKE\_AUTH, el **DefaultRAGroup** se debe utilizar para asegurarse que la conexión aterriza en el grupo de túnel correcto. El ASA autentica con un certificado (autenticación local) y espera que el cliente utilice EAP (autenticación remota). También, el ASA necesita enviar específicamente un pedido de la identidad EAP el cliente de responder con la respuesta de la identidad EAP (interrogación-identidad).

```
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
```

Finalmente, IKEv2 necesita ser habilitado y el certificado correcto ser utilizado.

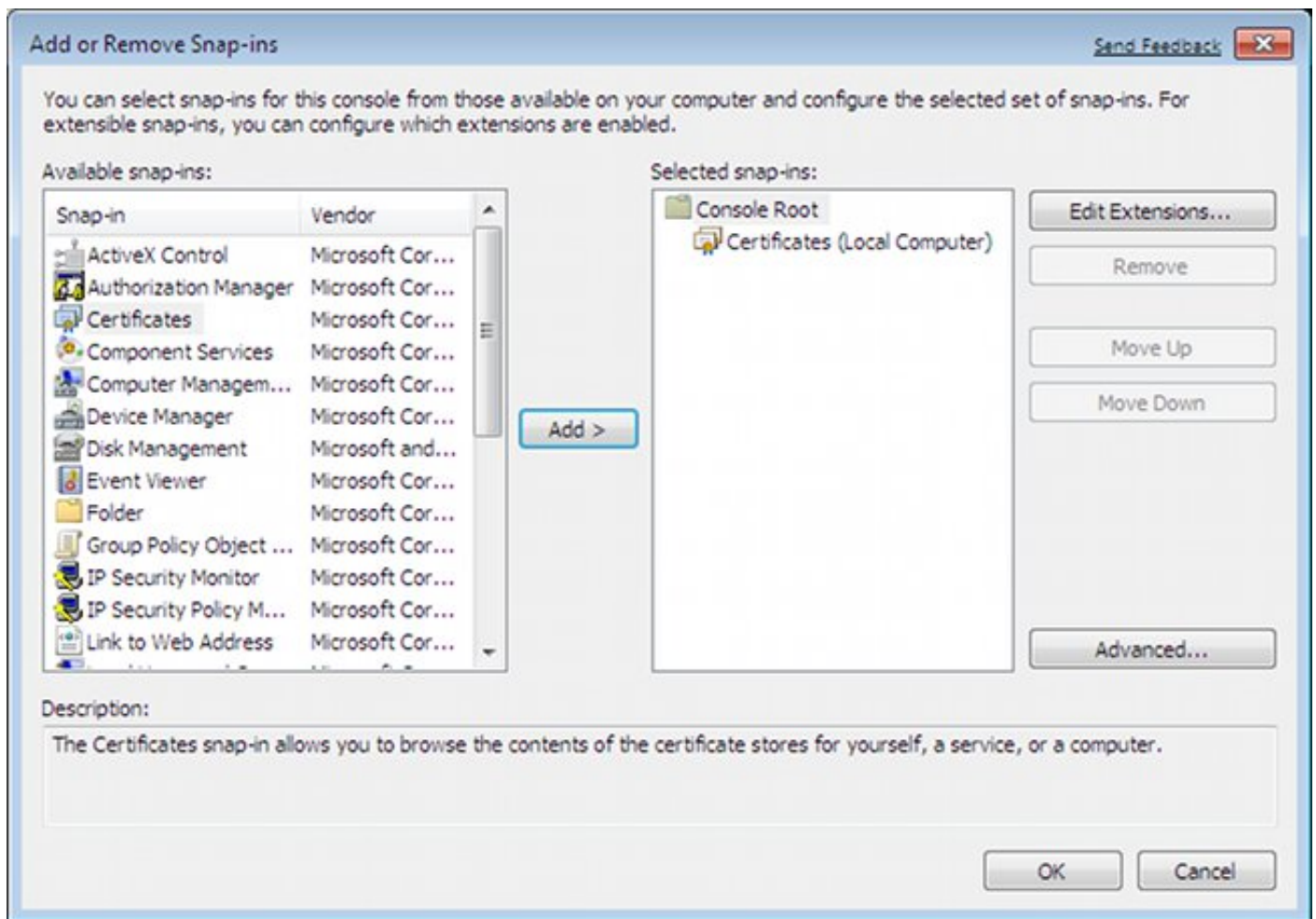
```
tunnel-group DefaultRAGroup general-attributes
address-pool POOL
authentication-server-group ISE
default-group-policy AllProtocols
tunnel-group DefaultRAGroup ipsec-attributes
ikev2 remote-authentication eap query-identity
ikev2 local-authentication certificate TP
```

## Windows 7

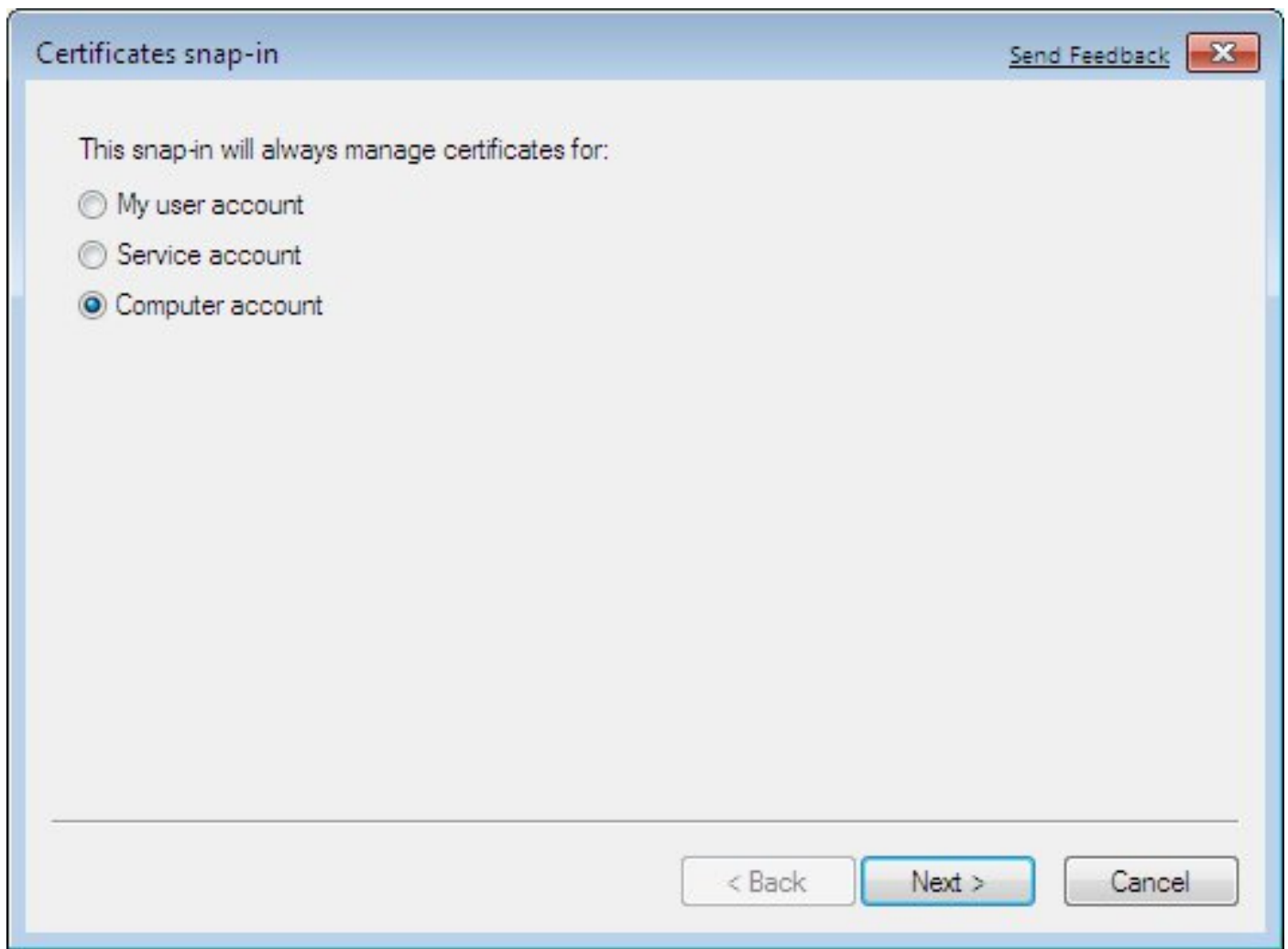
### Paso 1. Instale el certificado de CA.

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 (no el almacén del usuario). El cliente de Windows utiliza a las tiendas de computación para validar el certificado IKEv2.

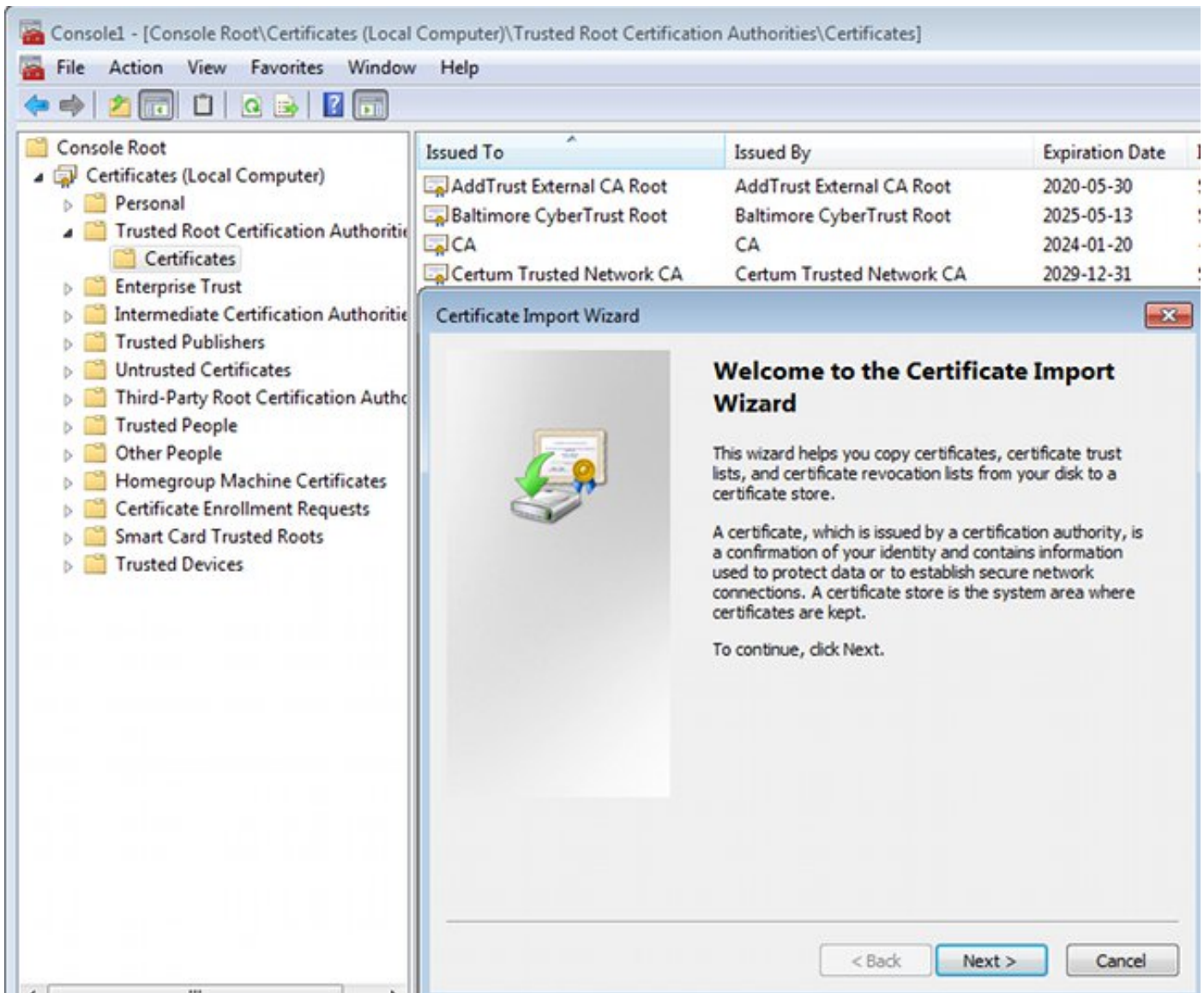
Para agregar CA, elija el **MMC > Add o quítelo Broche-INS > los Certificados**.



Haga clic el botón de radio de la **cuenta de la Computadora**.



Importe CA a las autoridades de certificación de la Raíz confiable.



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

```
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
```

## Paso 2. Configure la conexión VPN.

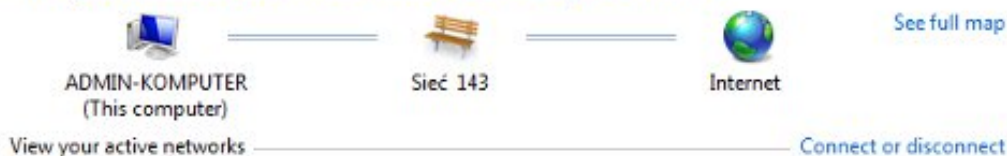
Para configurar la conexión VPN de la red y del centro de la distribución, elija **conectan con un lugar de trabajo** para crear una conexión VPN.



Control Panel Home  
Change adapter settings  
Change advanced sharing settings

See also

## View your basic network information and set up connections



Sieć 143  
Public network

Access type: Internet  
Connections: Połączenie lokalne

## Change your networking settings



Set up a new connection or network

Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Set Up a Connection or Network

Choose a connection option

- Connect to the Internet  
Set up a wireless, broadband, or dial-up connection to the Internet.
- Set up a new network  
Configure a new router or access point.
- Connect to a workplace  
Set up a dial-up or VPN connection to your workplace.
- Set up a dial-up connection  
Connect to the Internet using a dial-up connection.

Next Cancel

Elija el uso mi conexión de Internet (VPN).

## How do you want to connect?

Use my Internet connection (VPN)  
Connect using a virtual private network (VPN) connection through the Internet.



Configure el direccionamiento con un ASA FQDN. Asegurese lo es resuelto correctamente por el Domain Name Server (DNS).


## Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

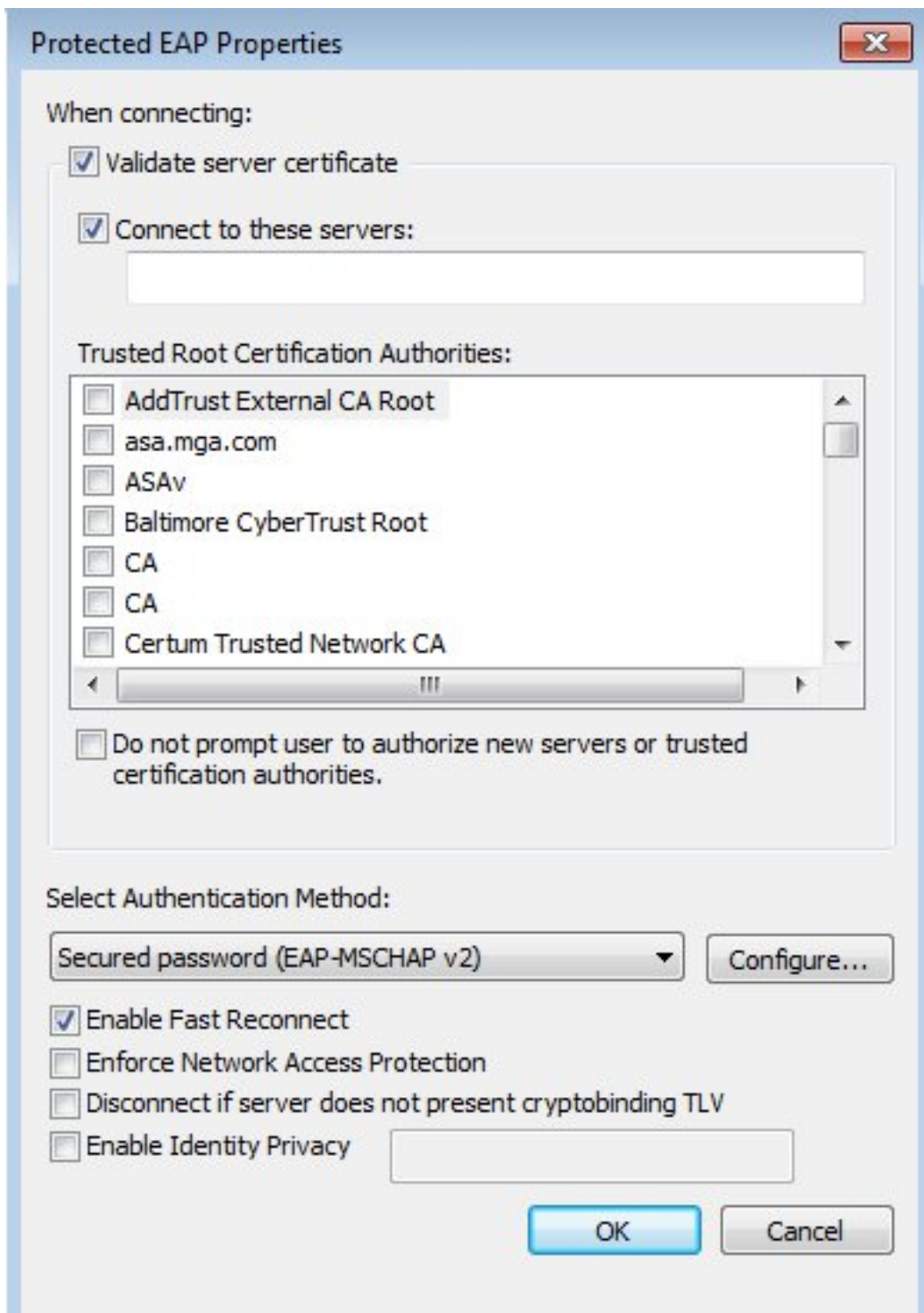
Use a smart card

  Allow other people to use this connection

This option allows anyone with access to this computer to use this connection.

Don't connect now; just set it up so I can connect later

Si procede, ajuste las propiedades (tales como validación de certificado) en la ventana de pPropiedades protegida EAP.



## Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta del Output Interpreter \(clientes registrados solamente\)](#) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

## Cliente de Windows

Cuando usted conecta, ingrese sus credenciales.



Cisco AnyConnect Secure Mobility  
Client Connection  
Disabled



Ikev2 connection to ASA  
Disconnected  
WAN Miniport (Ikev2)

Connect IKEv2 connection to ASA



User name:

Password:

Domain:


Save this user name and password for the following users:

Me only

Anyone who uses this computer

Después de la autenticación satisfactoria la configuración IKEv2 es aplicada.

Connecting to ASA-Ikev2...



Registering your computer on the network...

La sesión está activada.

Rename this connection

View status of this connection

Delete this connection



Cisco AnyConnect Secure Mobility  
Client Connection  
Disabled



IKEv2 connection to ASA  
IKEv2 connection to ASA  
WAN Miniport (IKEv2)

La tabla de ruteo se ha puesto al día con la ruta predeterminado con el uso de una nueva interfaz con el valor bajo de la medición.

```
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 la autenticación satisfactoria los informes 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**  
**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 ISE indican la autenticación satisfactoria con las reglas de la autenticación predeterminada y de la autorización.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there are navigation tabs: Home, Operations, Policy, Guest Access, and Administration. Below these are sub-tabs: Authentications, Reports, Endpoint Protection Service, and Troubleshoot. A summary bar displays four metrics: Misconfigured Suppliants (0), Misconfigured Network Devices (0), RADIUS Drops (6), and Client Stopped (0). Below this is a table of live sessions with columns for Time, Status, Det..., Repeat C..., Identity, Endpoint ID, Authorization Policy, Authorization Profiles, and Network Device. Two sessions are listed: one at 2014-11-18 18:31:34 with status 'All' and identity 'cisco', and another at 2014-11-18 17:52:07 with status 'All' and identity 'cisco'.

Time	Status	Det...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device
2014-11-18 18:31:34...	All			cisco	10.147.24.166			
2014-11-18 17:52:07...	All			cisco	10.147.24.166	Default >> Basic_Authenticated_Access	PermitAccess	ASAv

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	c0a8010100010000546c424a
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 en el ASA

Los debugs más importantes incluyen:

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

Paquete IKE\_SA\_INIT recibido por el ASA (incluye las ofertas IKEv2 y el intercambio de claves para el 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 las ofertas IKEv2, el intercambio de claves para el DH, y el pedido 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\_AUTHENTIC para el cliente con IKE-ID, pedido de certificado, propuesto transforman los conjuntos, configuración pedida, y los selectores del 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\_AUTHENTIC del ASA que incluye una petición de la identidad EAP (primer paquete con las Extensiones EAP). Ese paquete también incluye el certificado (si no hay certificado correcto en el ASA allí es un error):

```
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 el ASA (longitud 5, payload: Cisco):

```
(30): REAL Decrypted packet:(30): Data: 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: 5 bytes
```

Entonces los paquetes múltiples se intercambian como parte de EAP-PEAP. Finalmente el éxito EAP es recibido por el ASA y remitido al supplicant:

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



La autenticación de peer es acertada:

Payload contents:

(30): EAP(30): Next payload: NONE, reserved: 0x0, length: 8

(30): Code: success: id: 76, length: 4

Y acaban a la sesión de VPN correctamente.

## Paquete llano

La petición de la identidad EAP se encapsula en la “autenticación ampliable” del IKE\_AUTH envía por el ASA. Junto con la petición de la identidad, se envían IKE\_ID y los 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 supplicant confirme el método (EAP-PEAP), comienza a construir un túnel de Secure Sockets Layer (SSL) que proteja la sesión del MSCHAPv2 usada para la autenticación.

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

Después de que se intercambien los paquetes múltiples el ISE confirma el éxito.

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 sesión IKEv2 es completada por el ASA, la configuración final (contestación de la configuración con los valores tales como un IP Address asignado), transforma los conjuntos, y los selectores del tráfico se avanzan al cliente VPN.

45	10.62.71.177	10.147.24.166	EAP	78 Success
46	10.62.71.177	10.147.24.166	ISAKMP	114
47	10.147.24.166	10.62.71.177	ISAKMP	126 IKE_AUTH
48	10.147.24.166	10.62.71.177	ISAKMP	98 IKE_AUTH
49	10.62.71.177	10.147.24.166	ISAKMP	222 IKE_AUTH

- Type Payload: Configuration (47)
- Type Payload: Security Association (33)
- ▾ Type Payload: Traffic Selector - Initiator (44) # 1
  - Next payload: Traffic Selector - Responder (45)
  - 0... .. = Critical Bit: Not Critical
  - Payload length: 24
  - Number of Traffic Selector: 1
  - Traffic Selector Type: TS\_IPV4\_ADDR\_RANGE (7)
  - Protocol ID: Unused
  - Selector Length: 16
  - Start Port: 0
  - End Port: 65535

Starting Addr: 192.168.1.10 (192.168.1.10)

Ending Addr: 192.168.1.10 (192.168.1.10)

- ▾ Type Payload: Traffic Selector - Responder (45) # 1
  - Next payload: Notify (41)
  - 0... .. = Critical Bit: Not Critical
  - Payload length: 24

## Troubleshooting

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

## Información Relacionada

- [Guía de configuración CLI de la serie VPN de Cisco ASA, 9.3](#)
- [Guía del usuario del Cisco Identity Services Engine, versión 1.2](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)