

# Configurar o acesso remoto ASA IKEv2 com EAP-PEAP e cliente Windows nativo

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Considerações do AnyConnect Secure Mobility Client](#)

[Configurar](#)

[Diagrama de Rede](#)

[Certificados](#)

[ISE](#)

[Etapa 1. Adicione o ASA aos dispositivos de rede no ISE.](#)

[Etapa 2. Crie um nome de usuário no repositório local.](#)

[ASA](#)

[Windows 7](#)

[Etapa 1. Instale o certificado CA.](#)

[Etapa 2. Configure a conexão VPN.](#)

[Verificar](#)

[Cliente Windows](#)

[Logs](#)

[Depurações no ASA](#)

[Nível do pacote](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## Introduction

Este documento fornece um exemplo de configuração para um Cisco Adaptive Security Appliance (ASA) versão 9.3.2 e posterior que permite o acesso remoto à VPN para usar o Internet Key Exchange Protocol (IKEv2) com a autenticação padrão do Extensible Authentication Protocol (EAP). Isso permite que um cliente nativo do Microsoft Windows 7 (e qualquer outro IKEv2 baseado em padrão) se conecte ao ASA com autenticação IKEv2 e EAP.

## Prerequisites

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico de VPN e IKEv2
- Autenticação básica, autorização e contabilidade (AAA) e conhecimento RADIUS
- Experiência com a configuração do ASA VPN
- Experiência com a configuração do Identity Services Engine (ISE)

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft Windows 7
- Software Cisco ASA, versão 9.3.2 e posterior
- Cisco ISE, versão 1.2 e posterior

## Informações de Apoio

### Considerações do AnyConnect Secure Mobility Client

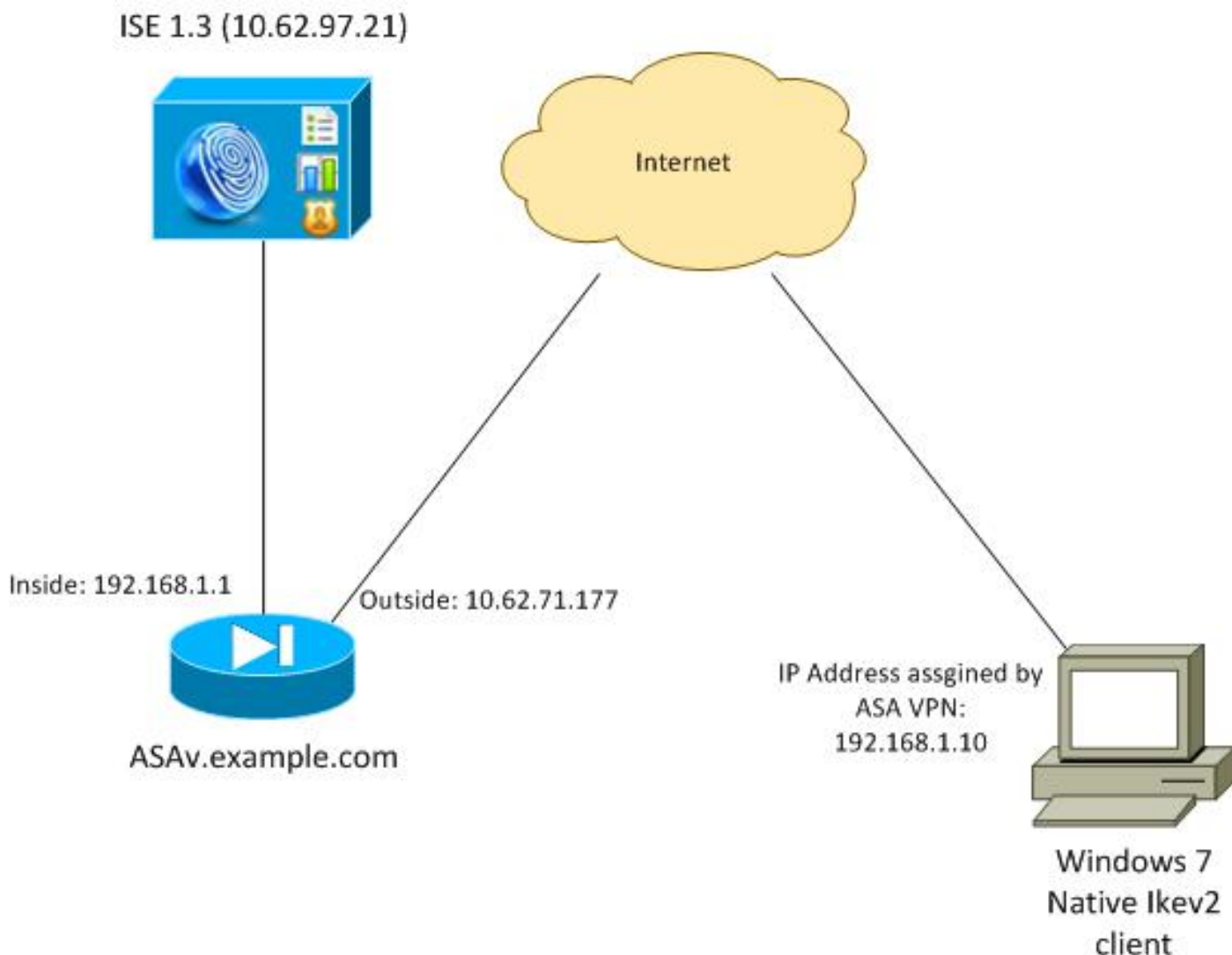
O cliente Windows IKEv2 nativo não suporta o túnel dividido (não há atributos CONF REPLY que possam ser aceitos pelo cliente Windows 7), portanto, a única política possível com o cliente Microsoft é o túnel de todo o tráfego (selecionadores de tráfego 0/0). Se houver necessidade de uma política de túnel dividido específica, o AnyConnect deve ser usado.

O AnyConnect não suporta métodos EAP padronizados que são terminados no servidor AAA (PEAP, Transport Layer Security). Se houver necessidade de encerrar sessões EAP no servidor AAA, o cliente Microsoft poderá ser usado.

## Configurar

**Note:** Use a [Command Lookup Tool \(somente clientes registrados\)](#) para obter mais informações sobre os comandos usados nesta seção.

## Diagrama de Rede



O ASA é configurado para autenticar com um certificado (o cliente precisa confiar nesse certificado). O cliente Windows 7 é configurado para autenticação com EAP (EAP-PEAP).

O ASA atua como gateway VPN terminando a sessão IKEv2 do cliente. O ISE atua como um servidor AAA terminando sessão EAP a partir do cliente. Os pacotes EAP são encapsulados em pacotes IKE\_AUTH para tráfego entre o cliente e o ASA (IKEv2) e, em seguida, em pacotes RADIUS para tráfego de autenticação entre o ASA e o ISE.

## Certificados

A Autoridade de Certificação da Microsoft (AC) foi usada para gerar o certificado para o ASA. Os requisitos de certificado para serem aceitos pelo cliente nativo do Windows 7 são:

- A extensão EKU (Extended Key Usage, uso de chave estendida) deve incluir a Autenticação de servidor (o modelo "servidor Web" foi usado nesse exemplo).
- O nome do assunto deve incluir o nome de domínio totalmente qualificado (FQDN) que será usado pelo cliente para se conectar (neste exemplo, ASAv.example.com).

Para obter mais detalhes sobre o cliente Microsoft, consulte [Troubleshooting de Conexões VPN IKEv2](#).

**Note:** O Android 4.x é mais restritivo e exige o nome alternativo de assunto correto de

acordo com o RFC 6125. Para obter mais informações sobre Android, consulte [IKEv2 de Android strongSwan para Cisco IOS com EAP e autenticação RSA](#).

Para gerar uma solicitação de assinatura de certificado no ASA, esta configuração foi usada:

```
hostname ASAv
domain-name example.com

crypto ca trustpoint TP
enrollment terminal

crypto ca authenticate TP
crypto ca enroll TP
```

## ISE

### Etapa 1. Adicione o ASA aos dispositivos de rede no ISE.

Escolha **Administração > Dispositivos de rede**. Defina uma senha pré-compartilhada que será usada pelo ASA.

### Etapa 2. Crie um nome de usuário no repositório local.

Escolha **Administração > Identidades > Usuários**. Crie o nome de usuário conforme necessário.

Todas as outras configurações são habilitadas por padrão para que o ISE autentique endpoints com EAP-PEAP (Protected Extensible Authentication Protocol).

## ASA

A configuração para acesso remoto é semelhante 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
```

Como o Windows 7 envia um endereço do tipo IKE-ID no pacote IKE\_AUTH, o **DefaultRAGgroup** deve ser usado para garantir que a conexão aterre no grupo de túneis correto. O ASA autentica com um certificado (autenticação local) e espera que o cliente use EAP (autenticação remota). Além disso, o ASA precisa enviar especificamente uma solicitação de identidade EAP para que o cliente responda com resposta de identidade EAP (identidade de consulta).

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

Finalmente, o IKEv2 precisa ser ativado e o certificado correto usado.

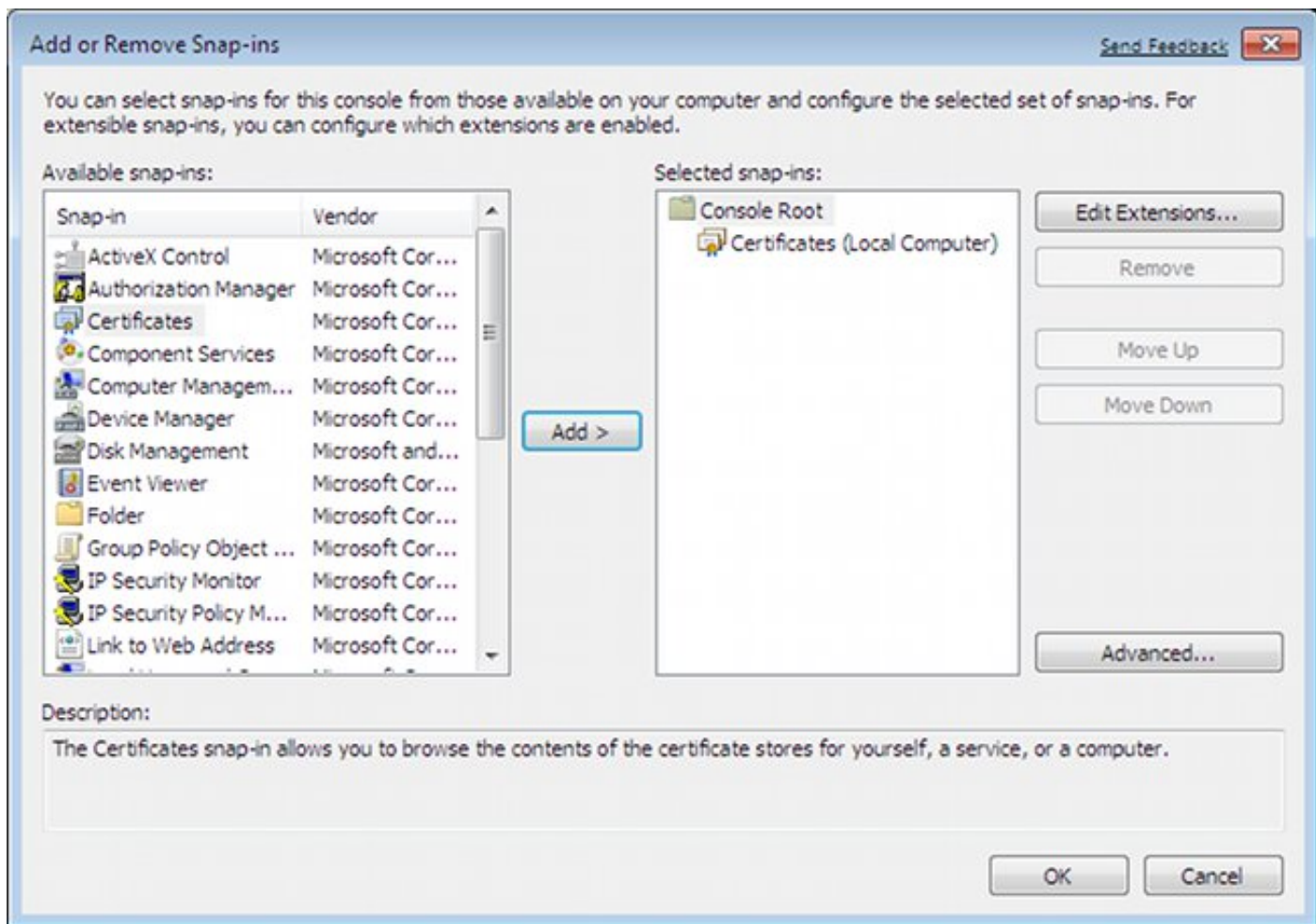
```
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint TP
```

## Windows 7

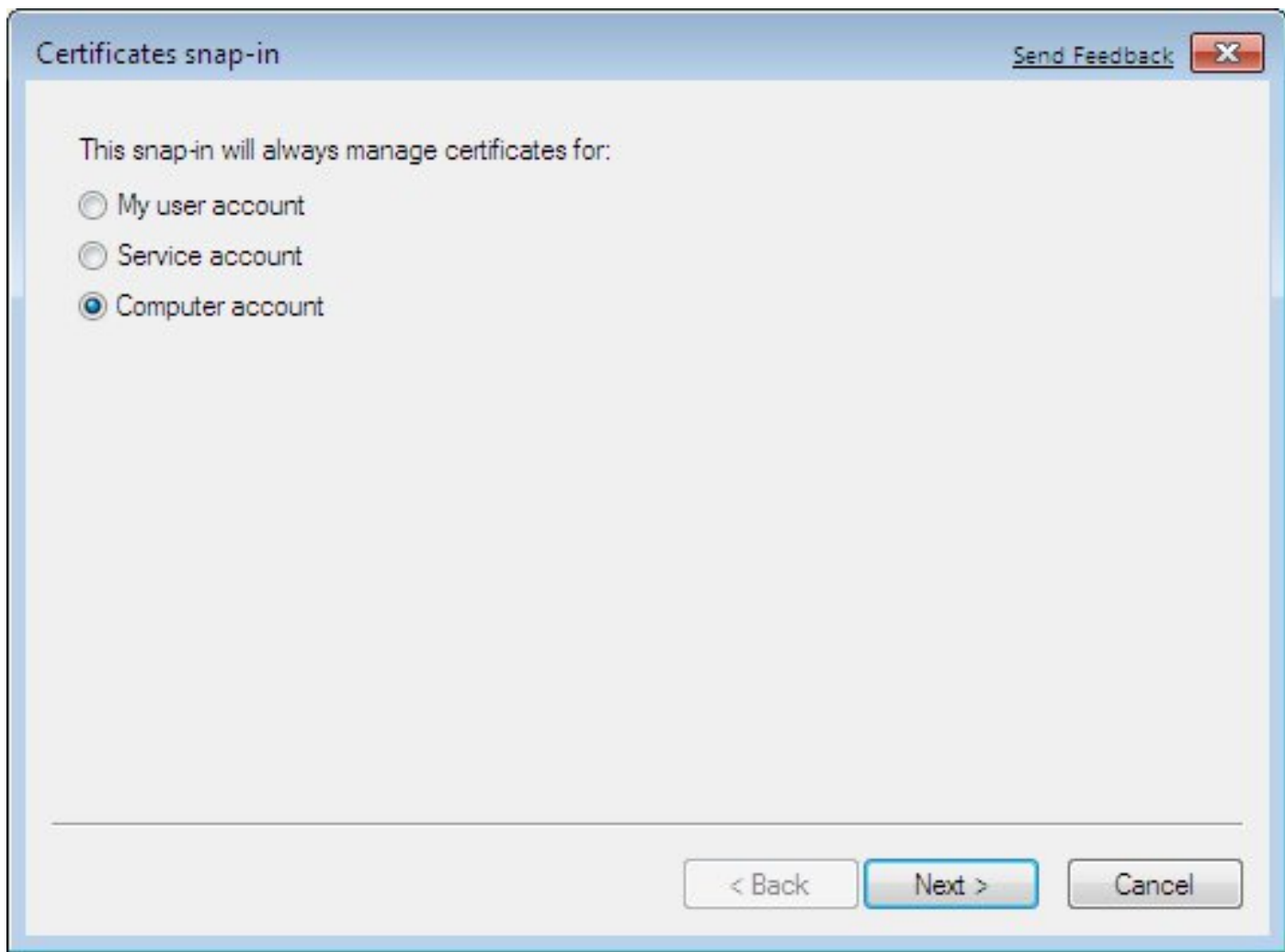
### Etapa 1. Instale o certificado CA.

Para confiar no certificado apresentado pelo ASA, o cliente Windows precisa confiar em sua CA. Esse certificado CA deve ser adicionado ao repositório de certificados do computador (não ao repositório de usuários). O cliente Windows usa o armazenamento do computador para validar o certificado IKEv2.

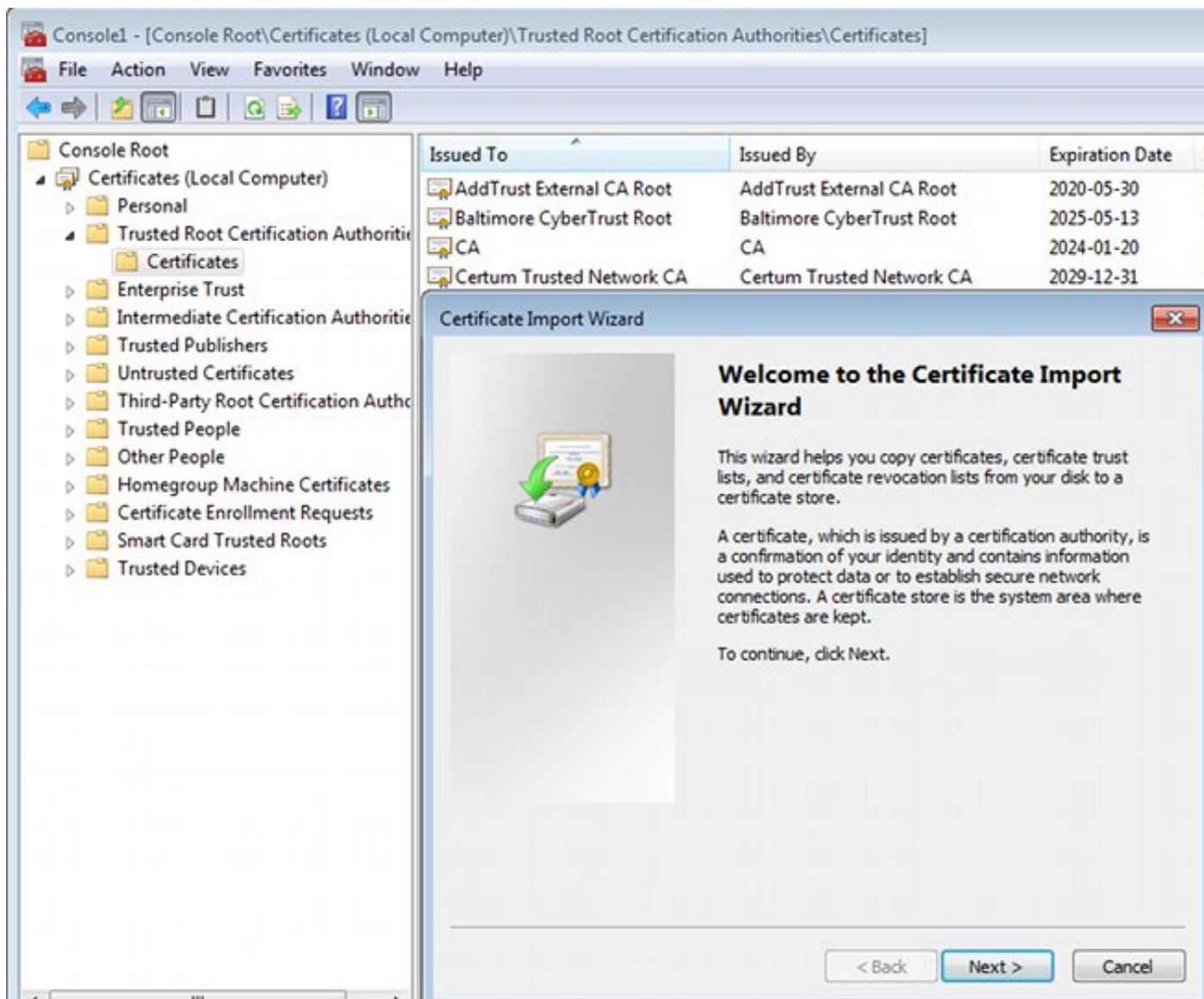
Para adicionar a CA, escolha **MMC > Adicionar ou remover snap-ins > Certificados**.



Clique no botão de opção **Conta do computador**.



Importar a AC para as Autoridades de Certificado Raiz Confiáveis.



Se o cliente Windows não puder validar o certificado apresentado pelo ASA, ele relata:

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

## Etapa 2. Configure a conexão VPN.

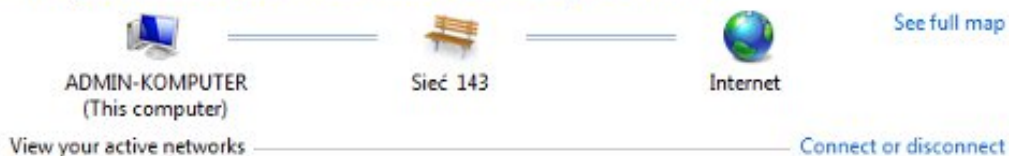
Para configurar a conexão VPN do Centro de Rede e Compartilhamento, escolha **Conectar a um local de trabalho** para criar uma conexão VPN.



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

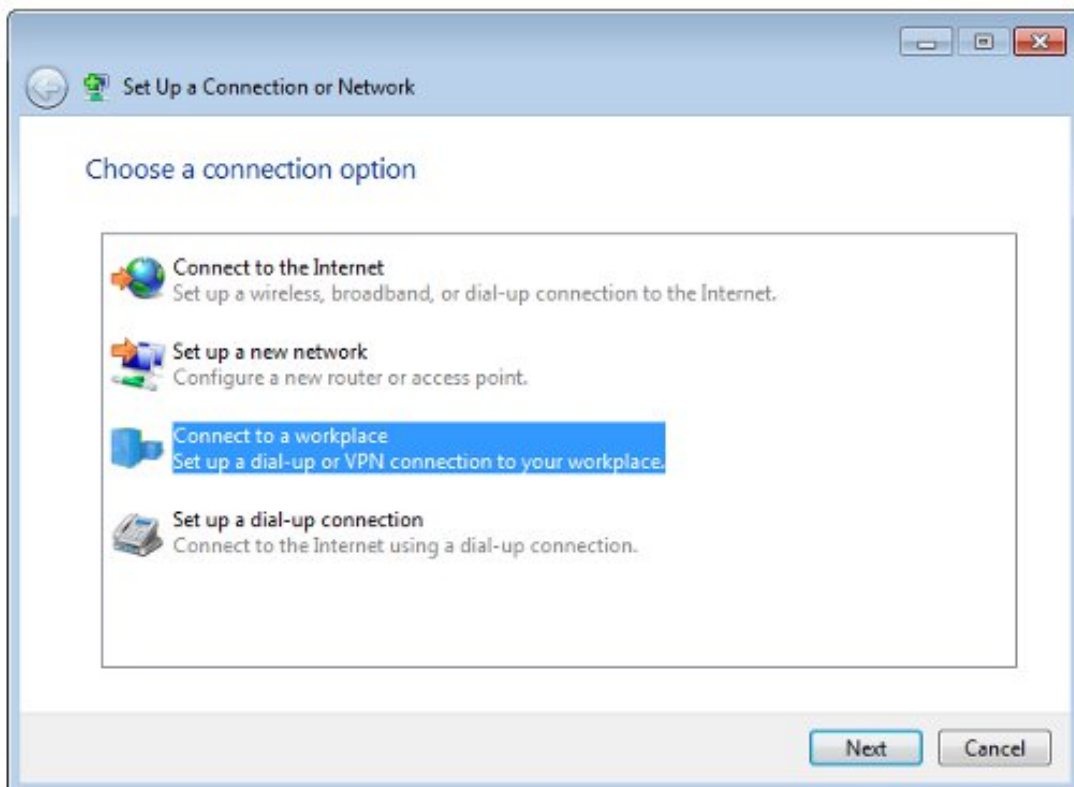
Access type: Internet  
Connections: Połączenie lokalne

## 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.



Escolha Usar minha conexão com a 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 o endereço com um FQDN ASA. Verifique se ele foi resolvido corretamente pelo Domain Name Server (DNS).


## Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

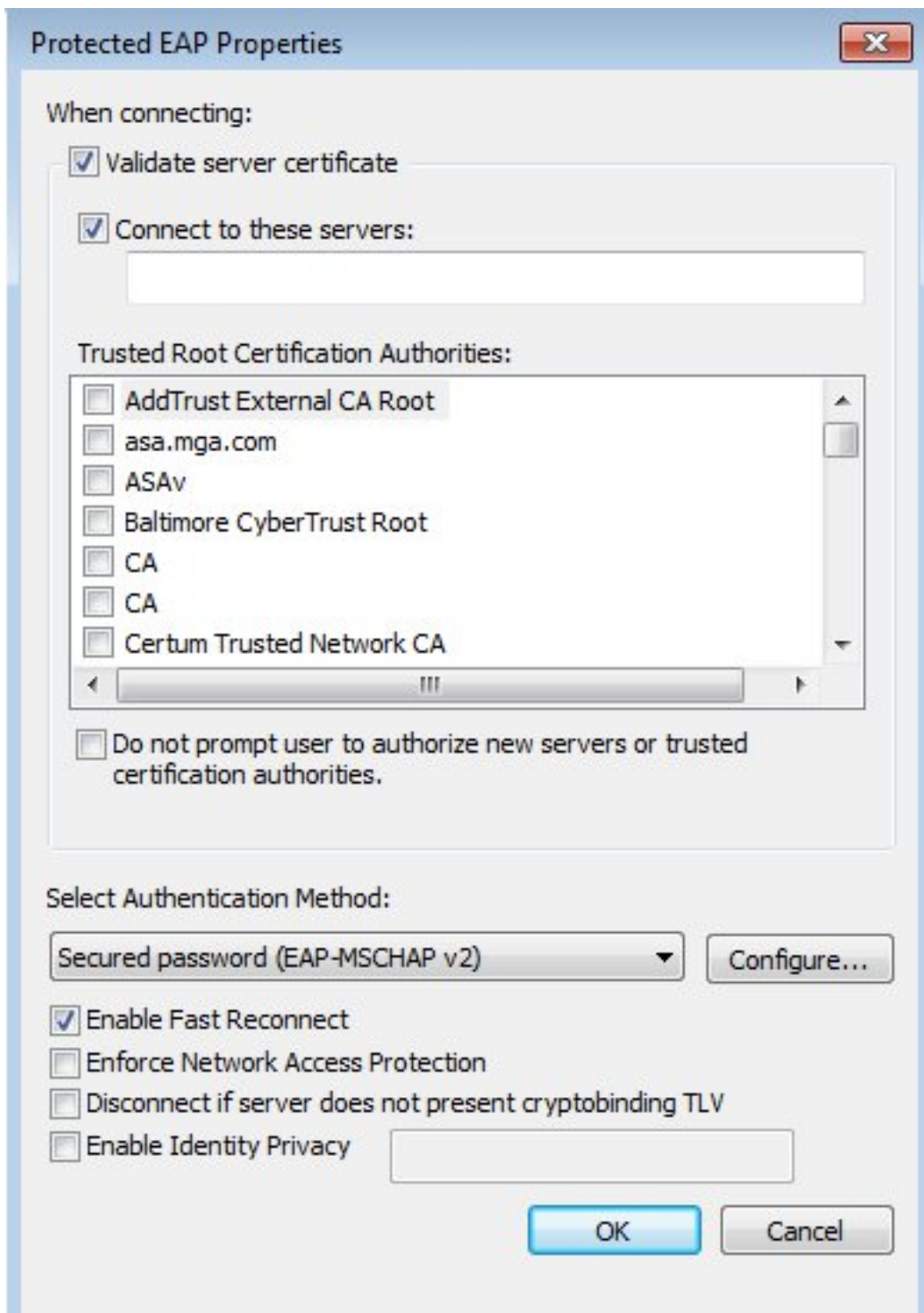
Use a smart card

  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

Se necessário, ajuste as propriedades (como validação de certificado) na janela Propriedades do EAP Protegido.



## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

## Cliente Windows

Ao conectar-se, digite suas credenciais.



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

Após a autenticação bem-sucedida, a configuração do IKEv2 é aplicada.

Connecting to ASA-IKEv2...



Registering your computer on the network...

A sessão está ativa.

## Internet ▶ Network Connections ▶

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)

A tabela de roteamento foi atualizada com a rota padrão com o uso de uma nova interface com a métrica baixa.

```
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 e0 Karta Microsoft ISATAP  
12...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface  
22...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

Após a autenticação bem-sucedida, o ASA relata:

```
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

```

Os registros ISE indicam autenticação bem-sucedida com as regras de autenticação e autorização padrão.

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 the navigation, there are several status indicators: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (6), and Client Stopped (0). The main part of the screenshot is a table of authentication logs. The table has columns for Time, Status, Identity, Endpoint ID, Authorization Policy, Authorization Profiles, and Network Device. The first row shows a successful authentication for user 'cisco' at IP '10.147.24.166' at 2014-11-18 18:31:34. The second row shows a successful authentication for user 'cisco' at IP '10.147.24.166' at 2014-11-18 17:52:07, with the authorization policy 'Default >> Basic\_Authenticated\_Access' and authorization profile 'PermitAccess' on network device 'ASAv'.

Time	Status	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device
2014-11-18 18:31:34...	<span style="color: blue;">i</span>	cisco	10.147.24.166			
2014-11-18 17:52:07...	<span style="color: green;">✓</span>	cisco	10.147.24.166	Default >> Basic_Authenticated_Access	PermitAccess	ASAv

Os detalhes indicam o 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

## Depurações no ASA

As depurações mais importantes incluem:

ASAv# **debug crypto ikev2 protocol 32**

<most debugs omitted for clarity....

**Pacote IKE\_SA\_INIT recebido pelo ASA (inclui propostas IKEv2 e troca de chaves 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
.....
```

**Resposta IKE\_SA\_INIT ao iniciador (inclui propostas IKEv2, troca de chave para DH e solicitação 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 cliente com IKE-ID, solicitação de certificado, conjuntos de transformação propostos, configuração solicitada e seletores de tráfego:**

```
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):
```

**Resposta IKE\_AUTH do ASA que inclui uma solicitação de identidade EAP (primeiro pacote com extensões EAP). Esse pacote também inclui o certificado (se não houver certificado correto no ASA, há uma falha):**

```
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]
```

**Resposta EAP recebida pelo ASA (comprimento 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
```



Em seguida, vários pacotes são trocados como parte do EAP-PEAP. Finalmente, o sucesso do EAP é recebido pelo ASA e encaminhado ao requerente:

Payload contents:

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

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

A autenticação de peer foi bem-sucedida:

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

E a sessão VPN foi concluída corretamente.

## Nível do pacote

A solicitação de identidade EAP é encapsulada em "Autenticação extensível" do IKE\_AUTH enviado pelo ASA. Juntamente com a solicitação de identidade, IKE\_ID e certificados são enviados.

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 os pacotes EAP subsequentes são encapsulados em IKE\_AUTH. Depois que o requerente confirmar o método (EAP-PEAP), ele começa a criar um túnel SSL (Secure Sockets Layer) que protege a sessão MSCHAPv2 usada para autenticação.

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

Depois que vários pacotes são trocados, o ISE confirma o sucesso.

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
  
```

A sessão IKEv2 é concluída pelo ASA, a configuração final (resposta de configuração com valores como um endereço IP atribuído), os conjuntos de transformação e os seletores de tráfego são enviados ao 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

## Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## Informações Relacionadas

- [Guia de configuração de CLI para VPN da Cisco ASA Series, 9.3](#)
- [Manual do usuário do Cisco Identity Services Engine, versão 1.2](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)