

EAP-PEAP とネイティブ Windows クライアントによる ASA IKEv2 リモート アクセスの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[AnyConnect セキュア モビリティ クライアントの考慮事項](#)

[設定](#)

[ネットワーク図](#)

[証明書](#)

[ISE](#)

[手順 1 : ASA を ISE 上のネットワーク デバイスに追加する。](#)

[手順 2 : ローカル ストアにユーザ名を作成する。](#)

[ASA](#)

[Windows 7](#)

[手順 1 : CA 証明書をインストールする。](#)

[手順 2 : VPN 接続を設定する。](#)

[確認](#)

[Windows クライアント](#)

[ログ](#)

[ASA でのデバッグ](#)

[パケット レベル](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、リモート VPN アクセスで標準規格の Extensible Authentication Protocol (EAP; 拡張可能認証プロトコル) 認証による Internet Key Exchange Protocol (IKEv2) の使用を可能にする Cisco 適応型セキュリティ アプライアンス (ASA) バージョン 9.3.2 以降の設定例を示します。この設定を使用すれば、ネイティブの Microsoft Windows 7 クライアント (および他のすべての標準ベースの IKEv2) で IKEv2 と EAP 認証を使用して ASA に接続できます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- VPN および IKEv2 に関する基本的な知識
- 認証、認可、およびアカウントテイング (AAA)、および RADIUS に関する基本的な知識
- ASA VPN 設定の経験
- Identity Services Engine (ISE) 設定の経験

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Microsoft Windows 7
- Cisco ASA ソフトウェア バージョン 9.3.2 以降
- Cisco ISE リリース 1.2 以降

背景説明

AnyConnect セキュア モビリティ クライアントの考慮事項

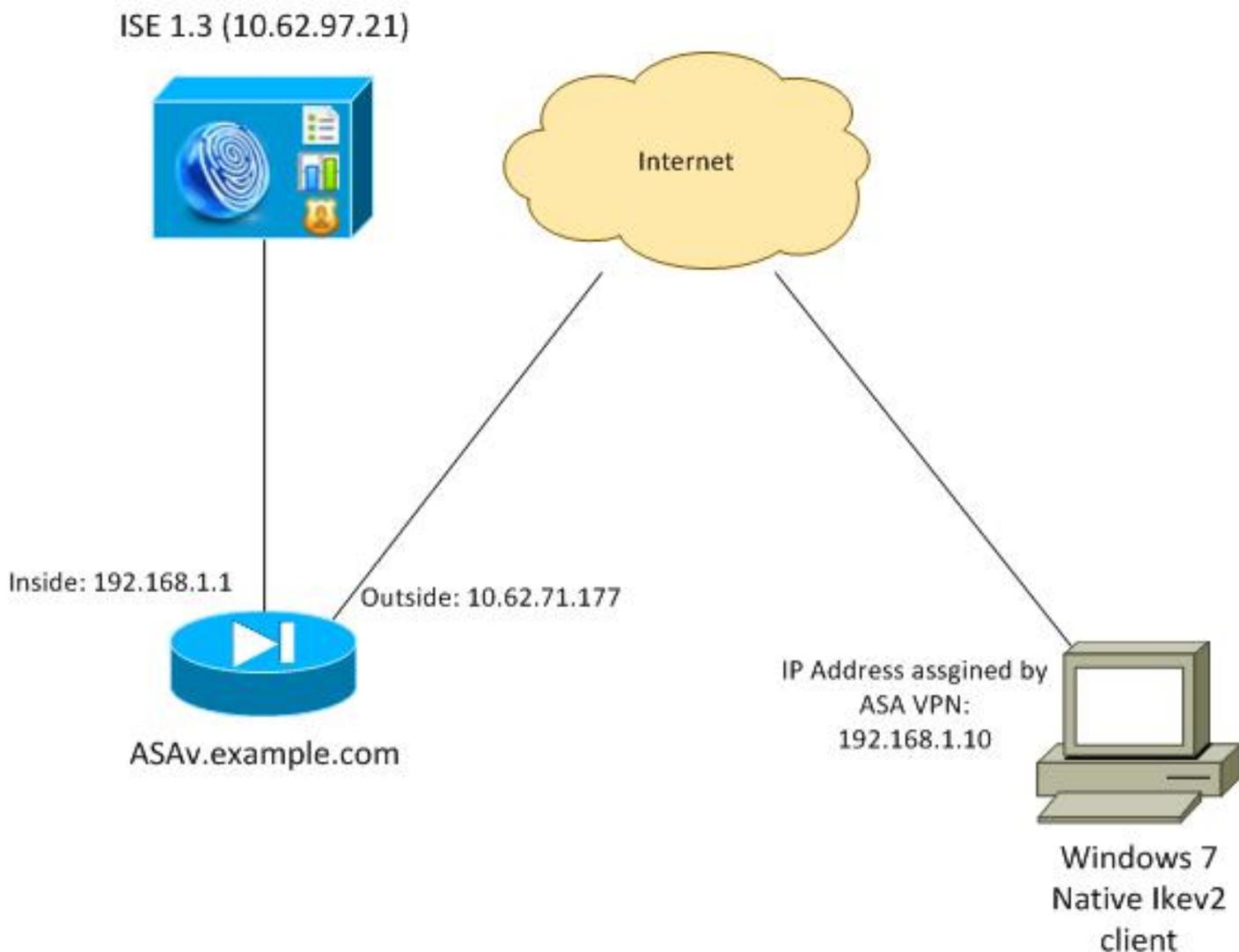
ネイティブの Windows IKEv2 クライアントでは、スプリット トンネルがサポートされない (Windows 7 クライアントで受け入れられる CONF REPLY 属性がありません) ため、Microsoft クライアントで可能な唯一のポリシーはすべてのトラフィックをトンネリングする (0/0 トラフィック セレクタ) ことです。固有のスプリット トンネル ポリシーが必要な場合は、AnyConnect を使用する必要があります。

AnyConnect では、AAA サーバ上で終了される標準化された EAP 方式 (PEAP、Transport Layer Security) はサポートされていません。AAA サーバ上で EAP セッションを終了する必要がある場合、Microsoft クライアントを使用できます。

設定

注：このセクションで使用されるコマンドの詳細については、[Command Lookup Tool \(登録ユーザ専用 \)](#) を使用してください。

ネットワーク図



ASA は、証明書を使用して認証するように設定されます (クライアントではその証明書を信頼する必要があります)。Windows 7 クライアントは、EAP (EAP-PEAP) を使用して認証するように設定されます。

ASA は、クライアントからの IKEv2 セッションを終了する VPN ゲートウェイとして機能します。ISE は、クライアントからの EAP セッションを終了する AAA サーバとして機能します。EAP パケットは、クライアントと ASA (IKEv2) 間のトラフィック用の IKE_AUTH パケットでカプセル化された後、ASA と ISE 間の認証トラフィック用の RADIUS パケットでカプセル化されます。

証明書

ASA の証明書を生成するために、Microsoft Certificate Authority (CA) が使用されました。Windows 7 のネイティブ クライアントで受け入れられるための証明書の要件は、次のとおりです。

- 拡張キー使用法 (EKU) 拡張に、Server Authentication (サーバ認証) (この例では、テンプレートの「Web server」が使用されました) が含まれている必要があります。
- サブジェクト名には、クライアントによって接続のために使用される完全修飾ドメイン名 (FQDN) (この例では、ASAv.example.com) が含まれている必要があります。

Microsoft クライアントの詳細については、「[Troubleshooting IKEv2 VPN Connections](#)」を参照してください。

注：Android 4.x はより制限的で、RFC 6125 に準拠した正しいサブジェクト代替名が必要です。Android の詳細については、「[EAP 認証および RSA 認証を使用した Android strongSwan から Cisco IOS への IKEv2](#)」を参照してください。

ASA で証明書署名要求を生成するために、次の設定が使用されました。

```
hostname ASAv
domain-name example.com

crypto ca trustpoint TP
enrollment terminal

crypto ca authenticate TP
crypto ca enroll TP
```

ISE

手順 1：ASA を ISE 上のネットワーク デバイスに追加する。

[Administration] > [Network Devices] を選択します。ASA で使用される事前共有パスワードを設定します。

手順 2：ローカル ストアにユーザ名を作成する。

[Administration] > [Identities] > [Users] を選択します。必要に応じてユーザ名を作成します。

他のすべての設定は、ISE で EAP-PEAP (Protected Extensible Authentication Protocol) を使用してエンドポイントを認証するために、デフォルトで有効になっています。

ASA

リモート アクセスの設定は、IKEv1 と IKEv2 で類似しています。

```
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
```

Windows 7はIKE-IDタイプアドレスをIKE_AUTHパケットで送信するため、接続が正しいトンネルグループに到達することを確認するためにDefaultRAGroupを使用する必要があります。ASAは証明書（ローカル認証）で認証し、クライアントがEAPを使用します。また、ASAではクライアントがEAP ID（アイデンティティ）応答（query-identity）で応答するために、EAP ID（アイデンティティ）要求を明示的に送信する必要もあります。

```
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
```

また、IKEv2 が有効になっており、正しい証明書を使用している必要があります。

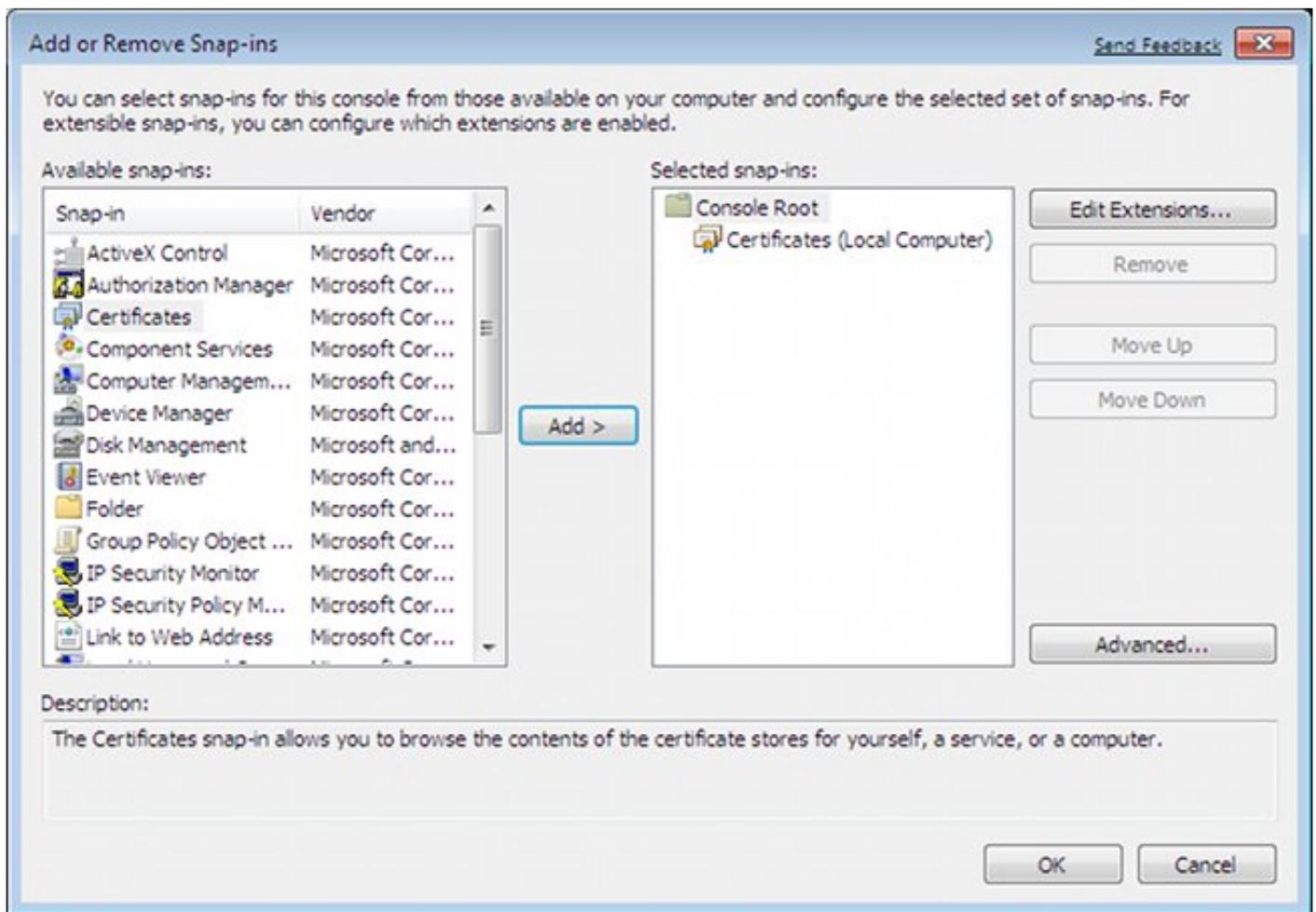
```
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint TP
```

Windows 7

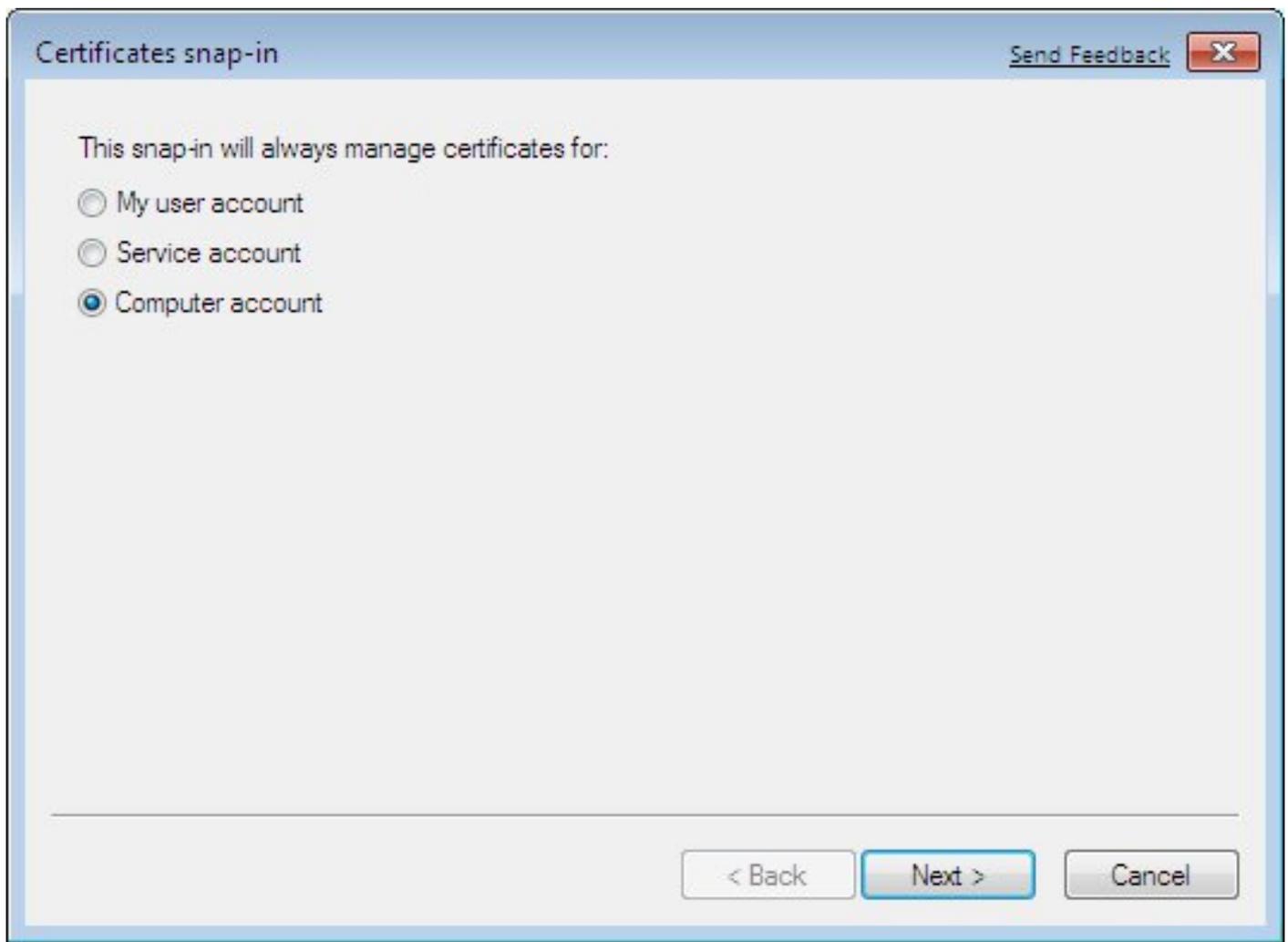
手順 1：CA 証明書をインストールする。

ASA から提示された証明書を信頼するために、Windows クライアントはその CA を信頼する必要があります。この CA 証明書をコンピュータの証明書ストア（ユーザストアではなく）に追加する必要があります。Windows クライアントでは、コンピュータのストアを使用して IKEv2 証明書を検証します。

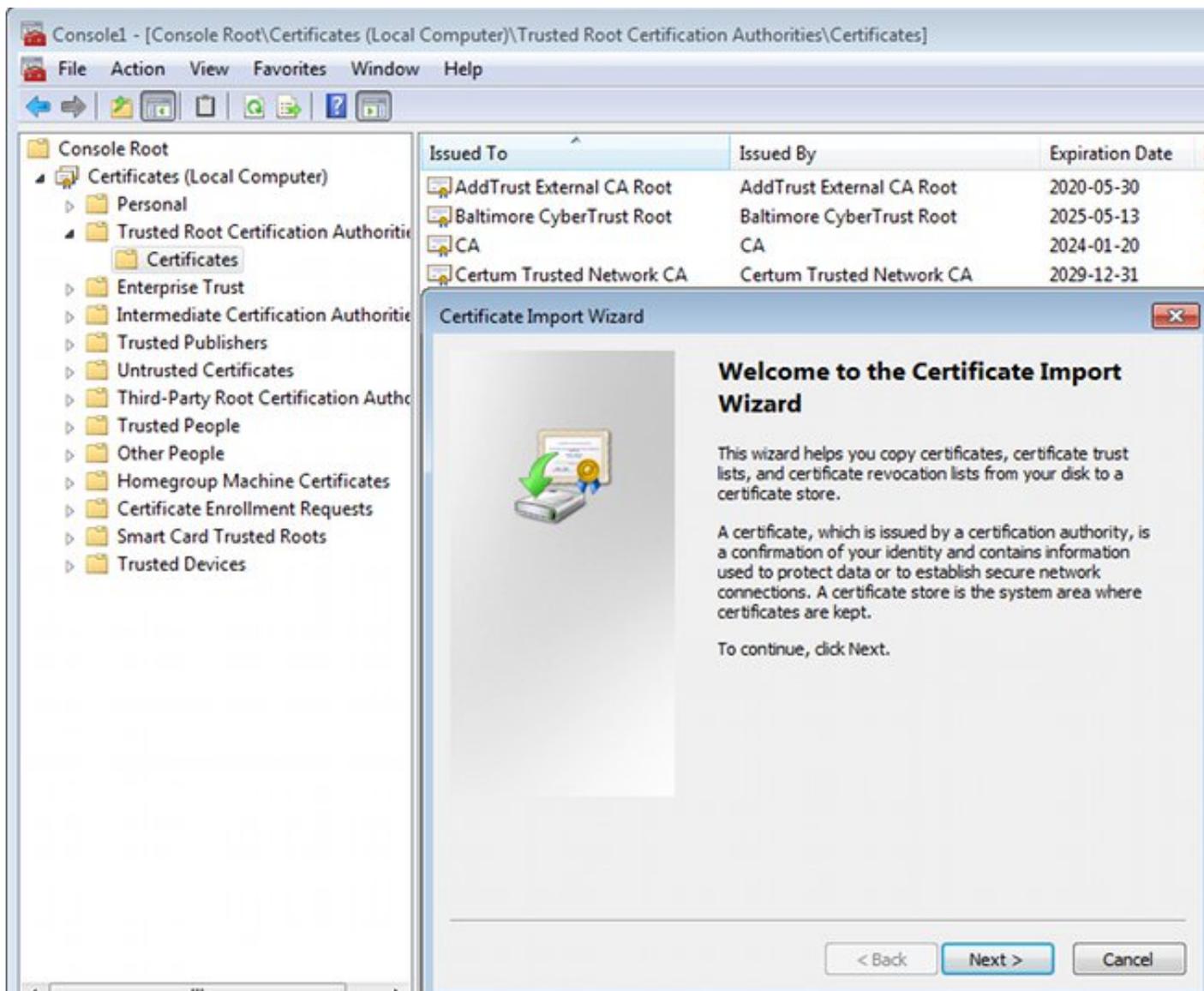
この CA を追加するには、[MMC] > [Add or Remove Snap-ins] > [Certificates] を選択します。



[Computer account] オプション ボタンをクリックします。



CA を [Trusted Root Certificate Authorities] にインポートします。



Windows クライアントで ASA から提示された証明書を検証できない場合、次のように報告されます。

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

手順 2 : VPN 接続を設定する。

[Network and Sharing Center] で VPN 接続を設定するには、VPN 接続を作成するために [Connect to a workplace] を選択します。

Control Panel Home
Change adapter settings
Change advanced sharing settings

See also

View your basic network information and set up connections



[See full map](#)

View your active networks [Connect or disconnect](#)



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

[Use my Internet connection (VPN)] を選択します。

How do you want to connect?

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



ASA の FQDN を使用してアドレスを設定します。このアドレスがドメイン ネーム サーバ (DNS) によって正しく解決されることを確認します。

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

Use a smart card

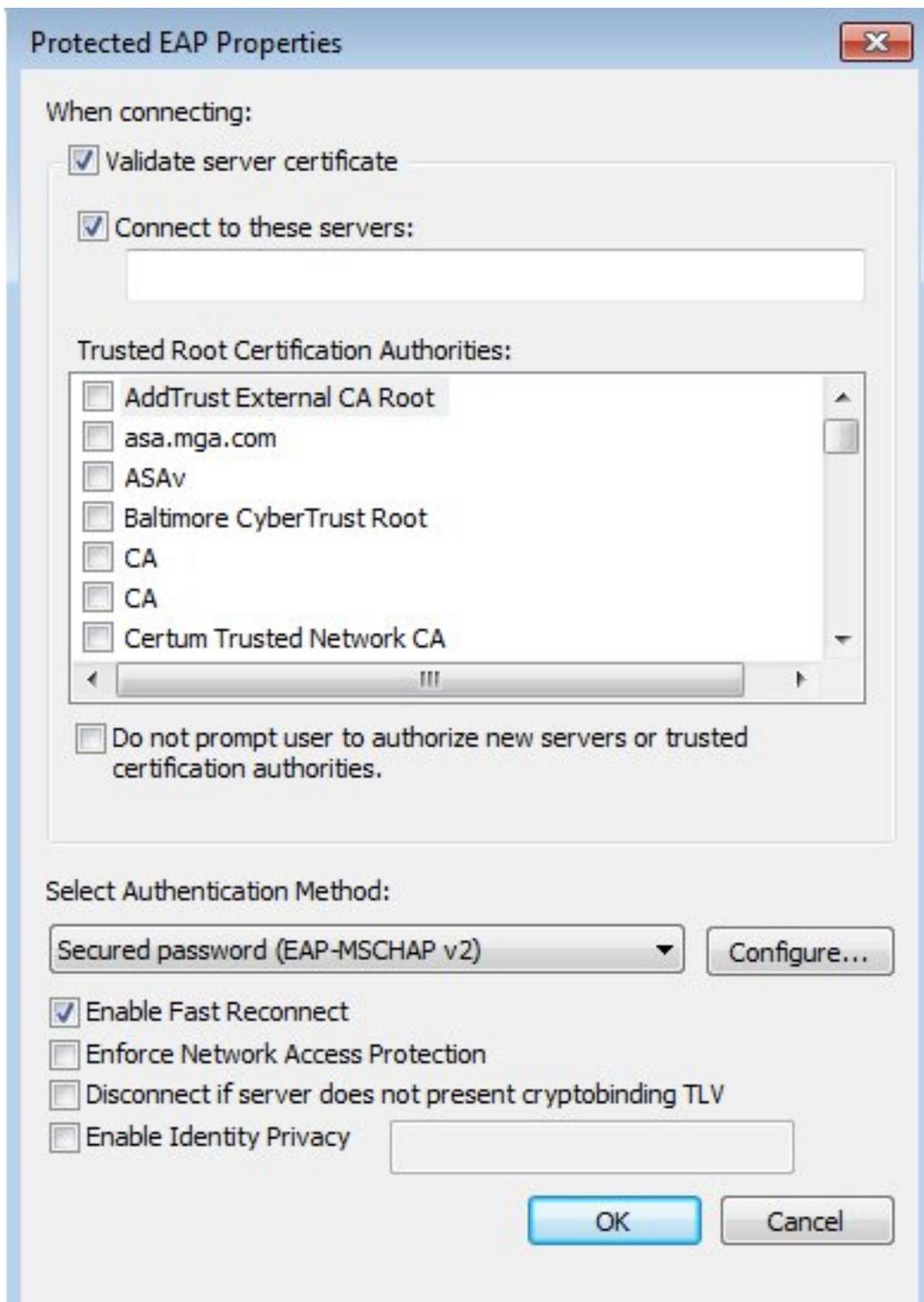


Allow other people to use this connection

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

必要な場合、[Protected EAP Properties] ウィンドウでプロパティ (証明書の検証など) を調整します。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

[アウトプット インタープリタ ツール \(登録ユーザ専用 \)](#) は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

Windows クライアント

接続する際は、クレデンシャル (資格情報) を入力します。



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

認証に成功すると、IKEv2 の設定が適用されます。

Connecting to ASA-IKEv2...



Registering your computer on the network...

セッションがアップします。

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)

ルーティング テーブルは、低いメトリックの新しいインターフェイスを使用してデフォルト ルートですでに更新されています。

```
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  
=====
```

ログ

認証に成功すると、ASA では次のように報告します。

```
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

```

ISE のログには、デフォルトの認証ルールと許可ルールとともに認証の成功が示されます。

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

詳細には PEAP 方式が示されます。

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

ASA でのデバッグ

最も重要な debug には、次のものがあります。

ASAv# **debug crypto ikev2 protocol 32**

<most debugs omitted for clarity....

ASA で受信された IKE_SA_INIT パケット (IKEv2 プロポーザルや Diffie-Hellman (DH) のキー交換など) :

```
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
```

.....

イニシエータへの IKE_SA_INIT 応答 (IKEv2 プロポーザル、DH のキー交換、証明書の要求など) :

```
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-ID のクライアント、証明書の要求、プロポーズされたトランスフォーム セット、要求された設定、およびトラフィック セレクタの IKE_AUTH :

```
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):
```

EAP ID 要求 (EAP 拡張を持つ最初のパケット) が含まれた ASA からの IKE_AUTH 応答。このパケットには、証明書も含まれます (ASA 上に正しい証明書がない場合、失敗があります)。

```
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]
```

ASA で受信された EAP 応答 (長さ 5、ペイロード : 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
```

この後、複数のパケットが EAP-PEAP の一環として交換されます。最後に次のように EAP の成

功が ASA で受信され、サブリカントに転送されます。

Payload contents:

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

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

ピアの認証が次のように成功します。

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

そして VPN のセッションが正常に終了します。

パケット レベル

EAP ID 要求が ASA によって送信される IKE_AUTH の「Extensible Authentication」にカプセル化されます。ID 要求とともに、IKE_ID と証明書が送信されます。

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:

後続のすべての EAP パケットは、IKE_AUTH にカプセル化されます。サブリカントで方式 (EAP-PEAP) を確認した後、認証に使用される MSCHAPv2 セッションを保護するセキュアソ

ケットレイヤ (SSL) トンネルの作成を開始します。

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

複数のパケットが交換された後、ISE で成功を確認します。

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

IKEv2 セッションが ASA によって完了され、最終的な設定 (設定では、割り当てられた IP アドレスなどの値で応答します)、トランスフォーム セット、およびトラフィック セレクタが、VPN クライアントにプッシュされます。

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

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [Cisco ASA シリーズ VPN CLI コンフィギュレーション ガイド 9.3](#)
- 『[Cisco Identity Services Engine User Guide, Release 1.2 \(Cisco Identity Services Engine ユーザガイド リリース 1.2 \)](#)』
- [テクニカル サポートとドキュメント - Cisco Systems](#)