

FlexVPN の展開 : EAP-MD5 による AnyConnect IKEv2 リモート アクセス

内容

[概要](#)

[前提条件](#)

[ネットワーク図](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景](#)

[IOS の初期設定](#)

[IOS : CA](#)

[IOS : ID 証明書](#)

[IOS : AAA と Radius の設定](#)

[ACS の初期設定](#)

[IOS FlexVPN の設定](#)

[Windows の設定](#)

[Windows の信頼への CA のインポート](#)

[AnyConnect XML プロファイルの設定](#)

[テスト](#)

[確認](#)

[IOS ルータ](#)

[Windows](#)

[既知の注意事項と問題](#)

[次世代暗号化](#)

[関連情報](#)

概要

このドキュメントでは、FlexVPN ツールキットを使用して IOS でリモート アクセスを設定する方法の例について説明します。

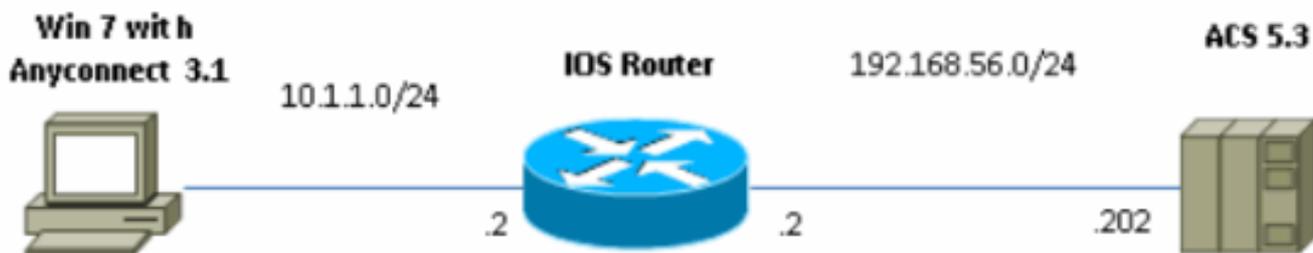
リモート アクセス VPN を使用すると、さまざまなオペレーティング システムを使用するエンドクライアントは、インターネットなどのセキュアではないメディアから企業ネットワークまたはホーム ネットワークに安全に接続できます。示されているシナリオでは、VPN トンネルは IKEv2 プロトコルを使用して Cisco IOS ルータで終了します。

このドキュメントでは、EAP-MD5 方式によって Access Control Server (ACS) を使用してユーザを認証および認可する方法を示します。

前提条件

ネットワーク図

Cisco IOS ルータには、2つのインターフェイスがあり、1つは ACS 5.3 向けです。



要件

このドキュメントに特有の要件はありません。

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。

- パッチ 6 が適用された ACS 5.3
- 15.2(4)M ソフトウェアがインストールされた IOS ルータ
- AnyConnect 3.1.01065 がインストールされた Windows 7 PC

表記法

ドキュメント表記の詳細については、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

背景

IKEv1 では、フェーズ 1.5 で XAUTH が使用され、IOS ルータでユーザをローカルに認証して、RADIUS/TACACS+ を使用してリモートでユーザを認証できます。IKEv2 では XAUTH とフェーズ 1.5 はサポートされなくなりました。これには、フェーズ IKE_AUTH で行われる EAP のサポートが組み込まれています。これの最大の利点は、IKEv2 の設計にあり、EAP は有名な標準です。

EAP では次の 2 つのモードがサポートされます。

- Tunneling : EAP-TLS、EAP/PSK、EAP-PEAP など。
- Non-tunneling : EAP-MSCHAPv2、EAP-GTC、EAP-MD5 など。

この例では、non-tunneling モードの EAP-MD5 が使用されます。これは、ACS 5.3 で現在サポートされる EAP 外部認証方式であるためです。

EAP は、発信側 (クライアント) から応答側 (この場合は IOS) の認証のみに使用できます。

IOS の初期設定

IOS : CA

最初に、認証局 (CA) を作成して、IOS ルータの ID 証明書を作成する必要があります。クライアントは、その証明書に基づいてルータの ID を確認します。

IOS での CA の設定は次のようになります。

```
crypto pki server CA
grant auto
hash sha1
eku server-auth client-auth
```

キーの拡張用途 (EAP に必要な Server-Auth。RSA-SIG では Client-Auth も必要です) を覚えておく必要があります。

crypto pki server CA で **no shutdown** コマンドを使用して CA を有効にします。

IOS : ID 証明書

次に、証明書の Simple Certificate Enrollment Protocol (SCEP) を有効にして、トラストポイントを設定します。

```
ip http server
crypto pki trustpoint CA-self
enrollment url http://10.1.1.2:80
fqdn 10.1.1.2
ip-address 10.1.1.2
subject-name cn=10.1.1.2,ou=TAC
revocation-check none
eku request server-auth client-auth
```

その後、証明書を認証して登録します。

```
(config)#crypto pki authenticate CA-self
Certificate has the following attributes:
    Fingerprint MD5: 741C671C 3202B3AE 6E05161C 694CA53E
    Fingerprint SHA1: 8C99513C 2198470F 7CB58FA2 32D8AA8D FC31D1ED
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

```
R1(config)#crypto pki enroll CA-self
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: cn=10.1.1.2,ou=TAC
% The subject name in the certificate will include: 10.1.1.2
% Include the router serial number in the subject name? [yes/no]: no
% The IP address in the certificate is 10.1.1.2
Request certificate from CA? [yes/no]: yes
```

```

% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CA-self' command
will show the fingerprint.
R1(config)#
*Dec  2 10:57:44.141: CRYPTO_PKI:  Certificate Request Fingerprint MD5:
BF8EF4B6 87FA8162 9079F917 698A5F36
*Dec  2 10:57:44.141: CRYPTO_PKI:  Certificate Request Fingerprint SHA1:
AC13FEA3 295F7AE6 7014EF60 784E33AF FD94C41D
R1(config)#
*Dec  2 10:57:44.198: %PKI-6-CERTRET: Certificate received from
Certificate Authority

```

AnyConnect でプロンプト メッセージを表示しない場合、cn は AnyConnect プロファイルで設定したホスト名/IP アドレスと等しくなければならぬことを覚えておいてください。

この例では、cn=10.1.1.2です。したがって、AnyConnect 10.1.1.2では、AnyConnect xmlプロファイルにサーバのIPアドレスとして入力されます。

IOS : AAA と Radius の設定

Radius と AAA の認証と認可を設定する必要があります。

```

aaa new-model
radius-server host 192.168.56.202 key cisco
aaa group server radius SERV
server 192.168.56.202
aaa authentication login eap-list group SERV
aaa authorization network eap-list group SERV

```

ACS の初期設定

最初に、新しいネットワーク デバイスを ACS に追加します ([Network Resources] > [Network Devices and AAA Clients] > [Create]) 。

The screenshot shows the configuration page for a new network device in ACS. The 'Name' field is 'H1'. Under 'Network Device Groups', 'Location' is 'All Locations' and 'Device Type' is 'All Device Types'. In the 'IP Address' section, 'Single IP Address' is selected with the IP '192.168.56.2'. The 'Authentication Options' section has 'TACACS+' and 'RADIUS' expanded. Under 'RADIUS', 'Shared Secret' is 'cisco', 'Key Input Format' is 'HEXADECIMAL', and 'Message Authenticator Code Key' is empty. A legend at the bottom left indicates that orange dots represent required fields.

ユーザを追加します ([Users and Identity Stores] > [Internal Identity Stores] > [Users] >

[Create]) 。

Users and Identity Stores > Internal Identity Stores > Users > Create

General

Name: user3 Status: Enabled 

Description:

Identity Group: All Groups

Password Information

Password must:

- Contain 4 - 32 characters

Password Type: Internal Users

Password:

Confirm Password:

Change password on next login

Enable Password Information

Password must:

- Contain 4 - 32 characters

Enable Password:

Confirm Password:

User Information

There are no additional identity attributes defined for user records

 = Pola wymagane

認可用のユーザを追加します。この例では IKETEST です。パスワードは、IOS によって送信されるデフォルトであるため「cisco」にする必要があります。

General

Name: IKETEST Status: Enabled 

Description:

Identity Group: All Groups

Password Information

Password must:

- Contain 4 - 32 characters

Password Type: Internal Users

Password:

Confirm Password:

Change password on next login

User Information

There are no additional identity attributes defined for user records

 = Pola wymagane

次に、ユーザの認可プロファイルを作成します ([Policy elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profiles] > [Create]) 。

この例では POOL です。この例では、スプリットトンネルの AV ペアを (プレフィクスとして) 入力し、接続されているクライアントに割り当てる IP アドレスとして Framed-IP-Address を入力します。サポートされるすべての AV ペアのリストは次の場所にあります。

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-apx-flex-rad.html

The screenshot shows the 'RADIUS Attributes' configuration page. It features a 'Common Tasks Attributes' table and a 'Manually Entered' table. The 'Manually Entered' table contains one entry:

Attribute	Type	Value
Framed-IP-Address cisco-av-pair	IPv4 Address String	182.168.100.200 iosec:route-set=prefix:10.1.1.0/24

Below the tables are several input fields and buttons:

- Buttons: Add A, Edit A, Replace A, Delete
- Dictionary Type: RADIUS-IPF (dropdown)
- RADIUS Attribute: (empty text field)
- Attribute Type: (empty text field)
- Attribute Value: Static (dropdown)
- Footer: = Pola wyregulacji
- Buttons: Submit, Cancel

次に、アクセス ポリシーで EAP-MD5 (認証用) と PAP/ASCII (認可用) のサポートをオンにする必要があります。この例では、デフォルトが使用されています ([Access Policies] > [Default Network Access]) 。

General **Allowed Protocols**

Process Host Lookup

Authentication Protocols

- ▶ Allow PAP/ASCII
- ▶ Allow CHAP
- ▶ Allow MS-CHAPv1
- ▶ Allow MS-CHAPv2
- ▶ Allow EAP-MD5
- ▶ Allow EAP-TLS
- ▶ Allow LEAP
- ▶ Allow PEAP
- ▶ Allow EAP-FAST

Preferred EAP protocol

Submit Cancel

アクセス ポリシーの条件を作成して、作成した認可プロファイルを割り当てます。この場合、[NDG:Location in All Locations] の条件が作成されるため、すべての Radius 認可要求で [POOL] 認可プロファイルを指定します ([Access Policies] > [Access Services] > [Default Network Access]) 。

General
Name: Rule-1 Status: Enabled ●

 The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions
 NDG:Location: in All Locations
 Time And Date: -ANY-

Results
Authorization Profiles:

POOL

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

ユーザを正常に認証できる場合、IOS ルータでテストできるはずですが。

```
R1#test aaa group SERV user3 Cisco123 new-code
User successfully authenticated
```

```
USER ATTRIBUTES
username          0   "user3"
addr              0   192.168.100.200
route-set         0   "prefix 10.1.1.0/24"
```

IOS FlexVPN の設定

IKEv2 提案とポリシーを作成する必要があります (作成する必要がないことがあります。CSCtn59317 を参照してください)。ポリシーは、この例ではいずれかの IP アドレス (10.1.1.2) 専用に作成されます。

```
crypto ikev2 proposal PROP
encryption 3des
integrity sha1
group 2
```

```
crypto ikev2 policy 5
match address local 10.1.1.2
proposal PROP
```

次に、仮想テンプレートにバインドされる IKEV2 プロファイルと IPsec プロファイルを作成します。

設定ガイドで推奨されているように、忘れずに http-url cert をオフにしてください。

```
crypto ikev2 profile PROF
match identity remote address 0.0.0.0
match identity remote key-id IKETEST
authentication remote eap query-identity
authentication local rsa-sig
pki trustpoint CA-self
aaa authentication eap eap-list
aaa authorization user eap list eap-list IKETEST
virtual-template 1
```

```
no crypto ikev2 http-url cert
crypto ipsec transform-set transform1 esp-3des esp-sha-hmac
crypto ipsec profile PROF
set transform-set transform1
set ikev2-profile PROF
interface Virtual-Templatel type tunnel
ip unnumbered Ethernet0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
```

この例では、認可は、ACS 設定で作成されたユーザ IKETEST に基づいて設定されます。

Windows の設定

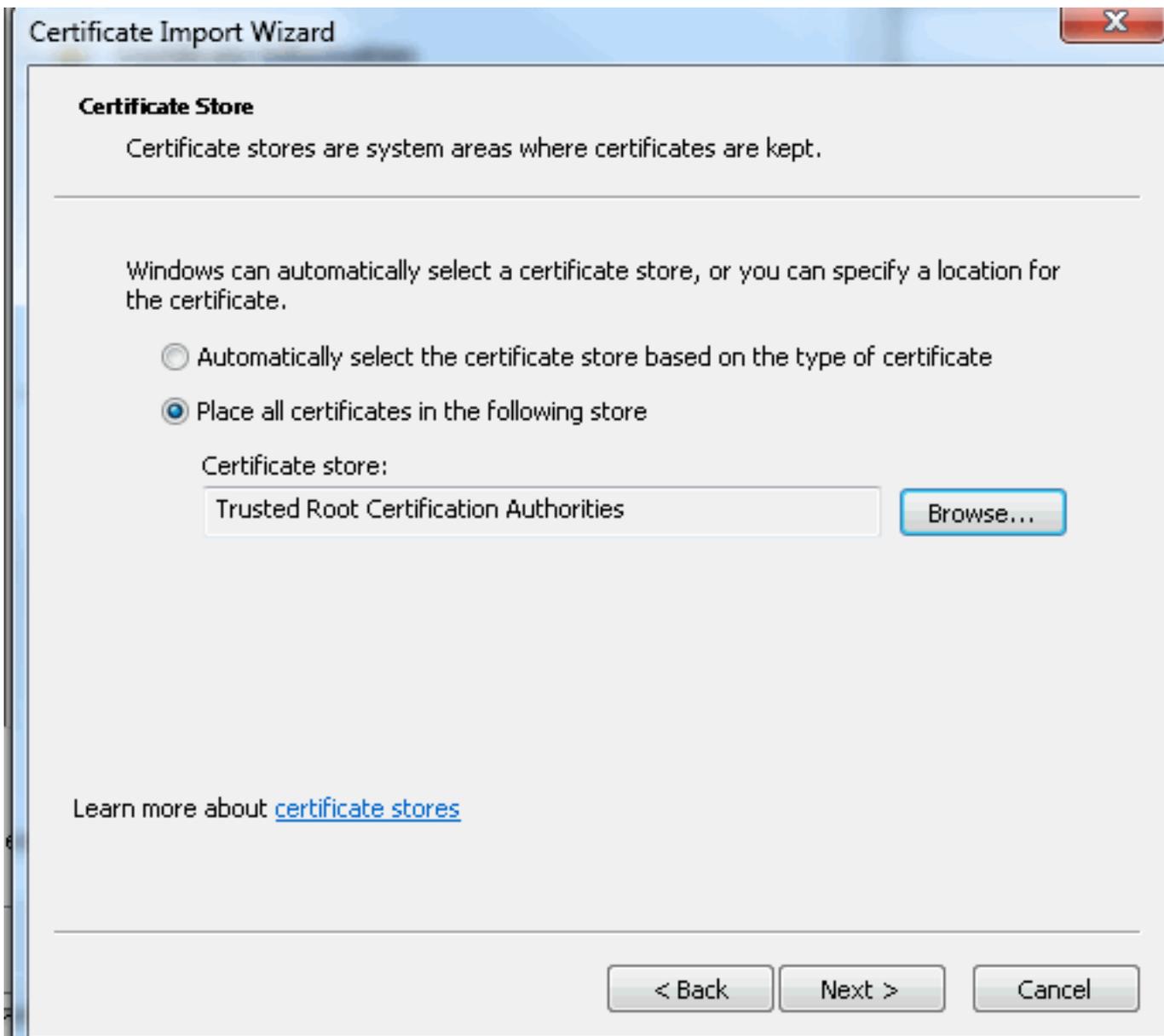
Windows の信頼への CA のインポート

IOS で CA 証明書をエクスポートします (ID 証明書をエクスポートして、最初の部分のみを使用してください)。

```
R1(config)#crypto pki export CA-self pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB8zCCAbygAwIBAgIBATANBgkqhkiG9w0BAQUFADANMQswCQYDVQQDEwJDQTAe
Fw0xMjExMjYxNzZlMzZlMzZlMzZlMzZlMzZlMzZlMzZlMzZlMzZlMzZlMzZlMzZl
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvDR4lH0crj42QfHpRuNu4EyFrLR8H
TbPanXYV+GdCBmu53pDILE00ASEHByD6DYBx01EZuDsioLJ7t2MPTguB+YZe6V40
JbtayyxtZGmF7+eDqRegQHHC394adQQWl2oJgQiuTHERDTqDJR8i5gN2Ee+K0sr3
+OjnHjUmXb/I6QIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQE
AwIBhjAfBgNVHSMEGDAwBTH5Sdh69q4HAJulLQYlBYH0Nk9zzAdBgNVHQ4EFgQU
x+UnYevauBwCbP50GC22B9DZPc8wDQYJKoZIhvcNAQEFBQADgYEADtBLiNXnl+LC
PIgJ0nl/jH5p2IwVlZwbPbZcOsZ9mn54QaqrhmhbHnmqKQJl/20+JPE6p+4noICq
VBrxoiX2KYQlOwmEScPpQ2XJ9vhGqtQ4Xcx3g20HhxxFDfp2XuW7hwU0W8dTCmZw
4vodj47qEXKI6pGuzauw9MN1xhkNarc=
-----END CERTIFICATE-----
```

BEGIN CERTIFICATE と END CERTIFICATE の間の部分をコピーして、Windows のメモ帳に貼り付けて、ファイル CA.crt として保存します。

これは、信頼されたルート機関としてインストールする必要があります ([file] > [Install Certificate] > [Place all certificates in the following store] > [Trusted Root Certification Authorities] をダブルクリックします)。



[AnyConnect XML プロファイルの設定](#)

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile に、ファイル「whatever.xml」を作成して、次を貼り付けます。

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
  <ClientInitialization>
    <UseStartBeforeLogon UserControllable="true">>false</UseStartBeforeLogon>
    <AutomaticCertSelection UserControllable="true">
      false</AutomaticCertSelection>
    <ShowPreConnectMessage>>false</ShowPreConnectMessage>
    <CertificateStore>All</CertificateStore>
    <CertificateStoreOverride>>false</CertificateStoreOverride>
    <ProxySettings>Native</ProxySettings>
    <AllowLocalProxyConnections>>true</AllowLocalProxyConnections>
    <AuthenticationTimeout>12</AuthenticationTimeout>
    <AutoConnectOnStart UserControllable="true">>false</AutoConnectOnStart>
    <MinimizeOnConnect UserControllable="true">>true</MinimizeOnConnect>
    <LocalLanAccess UserControllable="true">>false</LocalLanAccess>
```

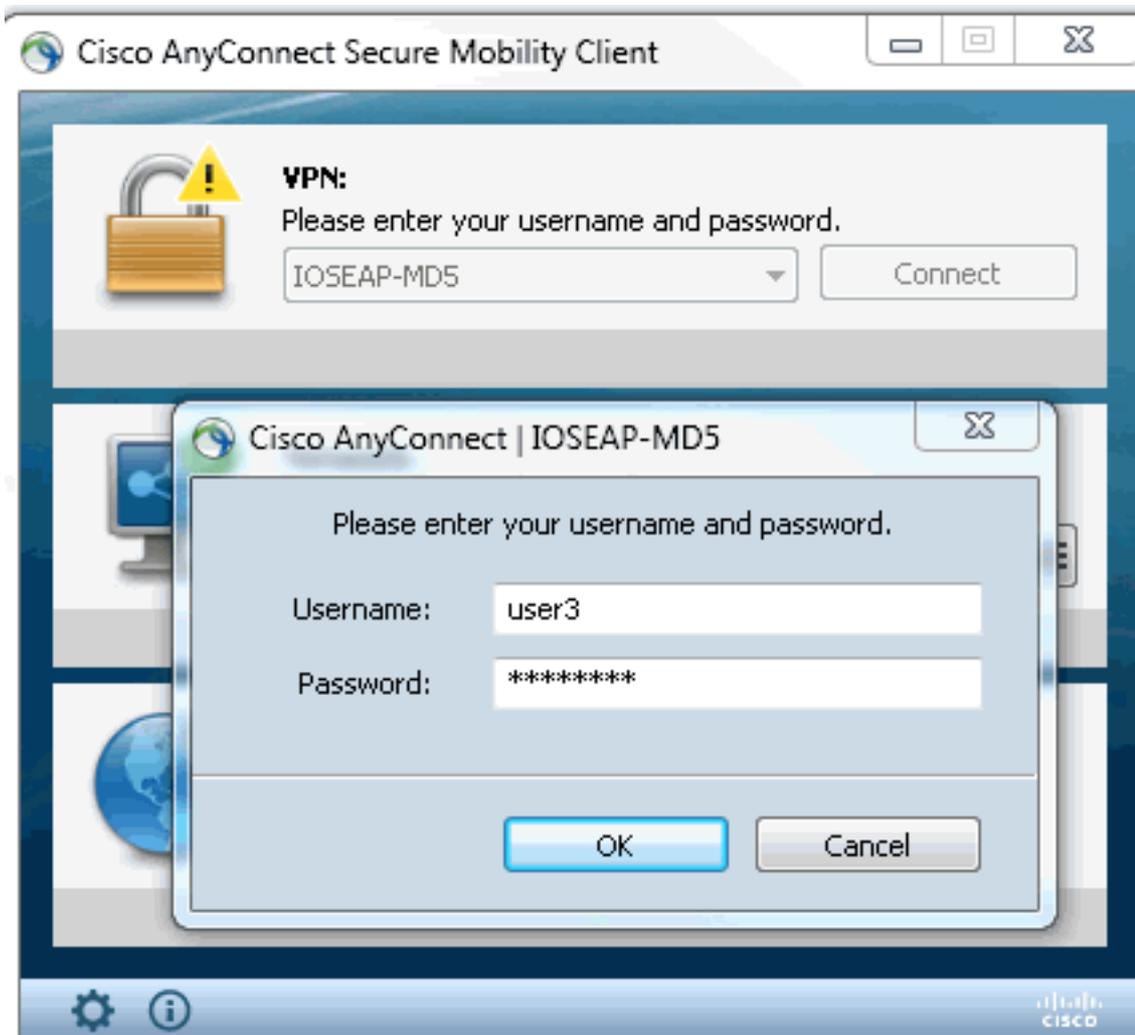
```
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
  <AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
  </AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSA SecurIDIntegration UserControllable="false">
  Automatic</RSA SecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPEXclusion UserControllable="false">Disable
  <PPPEXclusionServerIP UserControllable="false"></PPPEXclusionServerIP>
</PPPEXclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
  <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
</ClientInitialization>
<ServerList>
  <HostEntry>
    <HostName>IOSEAP-MD5</HostName>
    <HostAddress>10.1.1.2</HostAddress>
    <PrimaryProtocol>IPsec
      <StandardAuthenticationOnly>true
        <AuthMethodDuringIKENegotiation>EAP-MD5</AuthMethodDuringIKENegotiation>
        <IKEIdentity>IKETEST</IKEIdentity>
      </StandardAuthenticationOnly>
    </PrimaryProtocol>
  </HostEntry>
</ServerList>
</AnyConnectProfile>
```

10.1.1.2 エントリは、ID 証明書で入力した CN=10.1.1.2 と完全に同じにしてください。

テスト

このシナリオでは、SSL VPN は使用されないため、HTTP サーバが IOS で無効になっていることを確認します (no ip http server)。そうしないと、「Use a browser to gain access」というエラーメッセージが AnyConnect で表示されます。

AnyConnect での接続時に、パスワードを求められます。この例では、作成した User3 です。



その後、ユーザが接続されます。

確認

IOS ルータ

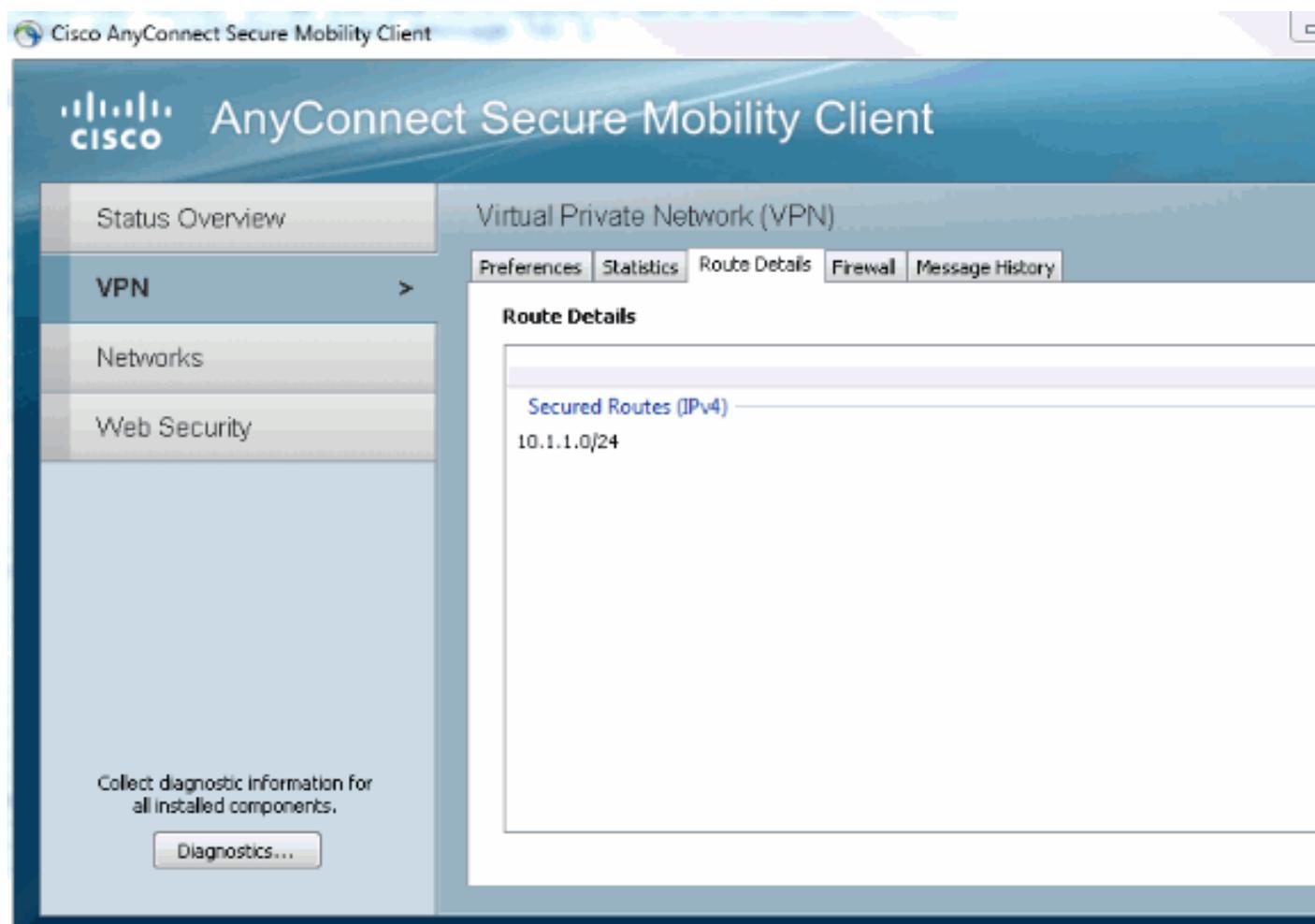
```
R1#show ip inter brief | i Virtual
Virtual-Access1    10.1.1.2  YES unset  up  up
Virtual-Templatel 10.1.1.2  YES unset  up  down
R1# show ip route 192.168.100.200
Routing entry for 192.168.100.200/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via Virtual-Access1
    Route metric is 0, traffic share count is 1
R1#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA
Tunnel-id Local Remote fvr/ivrf Status
1 10.1.1.2/4500 110.1.1.100/61021 none/none READY
  Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: RSA, Auth verify: EAP
  Life/Active Time: 86400/94 sec
IPv6 Crypto IKEv2 SA
R1#show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
```

```
X - IKE Extended Authentication, F - IKE Fragmentation
Interface: Virtual-Access1
Uptime: 00:04:06
Session status: UP-ACTIVE
Peer: 192.168.56.1 port 61021 fvrf: (none) ivrf: (none)
  Phase1_id: IKETEST
  Desc: (none)
  IKEv2 SA: local 10.1.1.2/4500 remote 10.1.1.100/61021 Active
    Capabilities:(none) connid:1 lifetime:23:55:54
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 192.168.100.200
    Active SAs: 2, origin: crypto map
    Inbound:  #pkts dec'ed 1 drop 0 life (KB/Sec) 4160122/3353
    Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4160123/3353
```

デバッグを実行できます (debug crypto ikev2)。

Windows

AnyConnect の [VPN] の [Advanced] オプションで、[Route Details] を調べて、スプリットトンネリング ネットワークを確認できます。



既知の注意事項と問題

- IKEv2 でのシグニチャ ハッシュと整合性ポリシーでいつ SHA1 を使用したかを覚えておきます (Cisco Bug ID [CSCtn59317](#) ([登録ユーザ専用](#)) を参照)。
- IOS ID 証明書内の CN は、ACS XML プロファイル内のホスト名と等しい必要があります。
- 認証中に渡される Radius AV ペアを使用し、グループの認可をまったく使用しない場合、

IKEv2 プロファイルで次を使用できます。

```
aaa authorization user eap cached
```

- 認可は、常にグループまたはユーザの認可にパスワード「cisco」を使用します。これは、次を使用する場合はわかりにくいことがあります。

```
aaa authorization user eap list SERV (without any paramaters)
```

これは、AnyConnect で渡されたユーザをユーザとパスワード「cisco」として使用しようとしませんが、このパスワードはユーザのパスワードではない可能性があるためです。

- 問題が発生した場合に、分析して Cisco TAC に提供できる出力があります。debug crypto ikev2debug crypto ikev2 internalDART 出力
- SSL VPN を使用していない場合、忘れずに ip http server を無効にしてください (no ip http server)。 そうしないと、AnyConnect は HTTP サーバに接続して、結果「Use a browser to gain access」を表示しようとしています。

次世代暗号化

上の構成は、最小主義の動作設定を示すための参照として提供されています。

Cisco では、可能な場合は次世代暗号化 (NGC) を使用することをお勧めします。

移行の現在の推奨事項は、以下を参照してください。

http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

NGC 設定を選択するときに、クライアント ソフトウェアとヘッドエンド ハードウェアの両方がその設定をサポートすることを確認します。NGC のハードウェア サポートがあるため、ISR Generation 2 と ASR 1000 ルータをヘッドエンドとしてお勧めします。

AnyConnect 3.1 バージョンの時点では、AnyConnect 側で NSA の Suite B アルゴリズムスイートがサポートされます。

関連情報

- [Cisco ASA IKEv2 PKI サイト間 VPN](#)
- [IOS での IKEv2 サイト間デバッグ](#)
- [FlexVPN/IKEv2 : Windows 7 Built-in-Client : IOS ヘッドエンド : パート 1 : 証明書認証](#)
- [FlexVPN およびインターネット キー エクスチェンジ \(IKE \) バージョン 2 コンフィギュレーション ガイド、Cisco IOS リリース 15.2M&T](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)