AAA 認証と証明書認証を使用した、IKEv2 による ASA への AnyConnect

目次

概要

このドキュメントでは、AnyConnect IPsec（IKEv2）、証明書、認証、認可、およびアカウンティング（AAA）を使用して PC を Cisco 適応型セキュリティ アプライアンス（ASA）に接続する方法を説明します。

> **注:** このドキュメントに記載する例には、ASA と AnyConnect との間で IKEv2 接続を確立するために使用する部分だけが示されています。 完全な設定例は、このドキュメントに記載されていません。 ネットワーク アドレス変換（NAT）またはアクセス リストの設定については説明しません。その設定は、このドキュメントでは必要になりません。

接続の準備

このセクションでは、PC を ASA に接続するために必要となる準備について説明します。

EKU が適切な証明書

重要な点として、ASA と AnyConnect の組み合わせには必須ではないものの、RFC では証明書に拡張キーの使用状況（EKU）が含まれていることを要件としています。

- ASA の証明書には EKU として **server-auth** が含まれている必要があります。
- PC の証明書には EKU として **client-auth** が含まれている必要があります。

注: 最新のソフトウェア リビジョンがインストールされた IOS ルータは、証明書に EKU を挿入できます。

ASA での設定

このセクションでは、接続を確立するために必要となる ASA 設定について説明します。

注: Cisco Adaptive Security Device Manager（ASDM）を使用すると、わずか数回のクリックで基本設定を作成できます。 間違いを避けるため、ASDM の使用を推奨します。

暗号マップの設定

次に、暗号マップの設定例を示します。

```
crypto dynamic-map DYN 1 set pfs group1
crypto dynamic-map DYN 1 set ikev2 ipsec-proposal secure
crypto dynamic-map DYN 1 set reverse-route
crypto map STATIC 65535 ipsec-isakmp dynamic DYN
crypto map STATIC interface outside
```

IPsec プロポーザル

次に、IPsec プロポーザルの設定例を示します。

```
crypto dynamic-map DYN 1 set pfs group1
crypto dynamic-map DYN 1 set ikev2 ipsec-proposal secure
crypto dynamic-map DYN 1 set reverse-route
crypto map STATIC 65535 ipsec-isakmp dynamic DYN
crypto map STATIC interface outside
```

IKEv2 ポリシー

次に、IKEv2 ポリシーの設定例を示します。

```
crypto dynamic-map DYN 1 set pfs group1
crypto dynamic-map DYN 1 set ikev2 ipsec-proposal secure
crypto dynamic-map DYN 1 set reverse-route
crypto map STATIC 65535 ipsec-isakmp dynamic DYN
crypto map STATIC interface outside
```

クライアント サービスとクライアント証明書

クライアント サービスとクライアント証明書は、適切なインターフェイスで有効にする必要があります。この例の場合、そのインターフェイスに該当するのは外部インターフェイスです。 次に設定例を示します。

```
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint OUTSIDE
ssl trust-point OUTSIDE outside
```

注: セキュア レイヤ（SSL）にも同じトラストポイントを割り当てます。これは意図的であ

り、必須の割り当てです。

AnyConnect プロファイルの有効化

ASA で AnyConnect プロファイルを有効にする必要があります。 次に設定例を示します。

```
webvpn
 enable outside
anyconnect image disk0:/anyconnect-win-3.0.5080-k9.pkg 1 regex "Windows NT"
anyconnect profiles Anyconnect disk0:/anyconnect.xml
 anyconnect enable
tunnel-group-list enable
```

ユーザ名、グループ ポリシー、トンネル グループ

次に、ASA での基本的なユーザ名、グループ ポリシー、トンネル グループの設定例を示します。

```
group-policy GroupPolicy_AC internal
group-policy GroupPolicy_AC attributes
 dns-server value 4.2.2.2
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
default-domain value cisco.com
webvpn
anyconnect profiles value Anyconnect type user
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15
tunnel-group AC type remote-access
tunnel-group AC general-attributes
address-pool VPN-POOL
 default-group-policy GroupPolicy_AC
tunnel-group AC webvpn-attributes
 authentication aaa certificate
 group-alias AC enable
 group-url https://bsns-asa5520-1.cisco.com/AC enable
 without-csd
```

AnyConnect プロファイル

次に、プロファイルの例を示します。関連する部分は**太字**で示されています。

```
<?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>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="true">Automatic
 </RSASecurIDIntegration>
<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>bsns-asa5520-1</HostName>
<HostAddress>bsns-asa5520-1.cisco.com</HostAddress>
<UserGroup>AC</UserGroup>
<PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

この設定例についての重要な注意点は次のとおりです。

- プロファイルを作成する際は、IKEv2 に使用する証明書に設定された証明書名（CN）と一致する [HostAddress] を定義する必要があります。 これを定義するには、**crypto ikev2 remote-access trustpoint** コマンドを入力します。

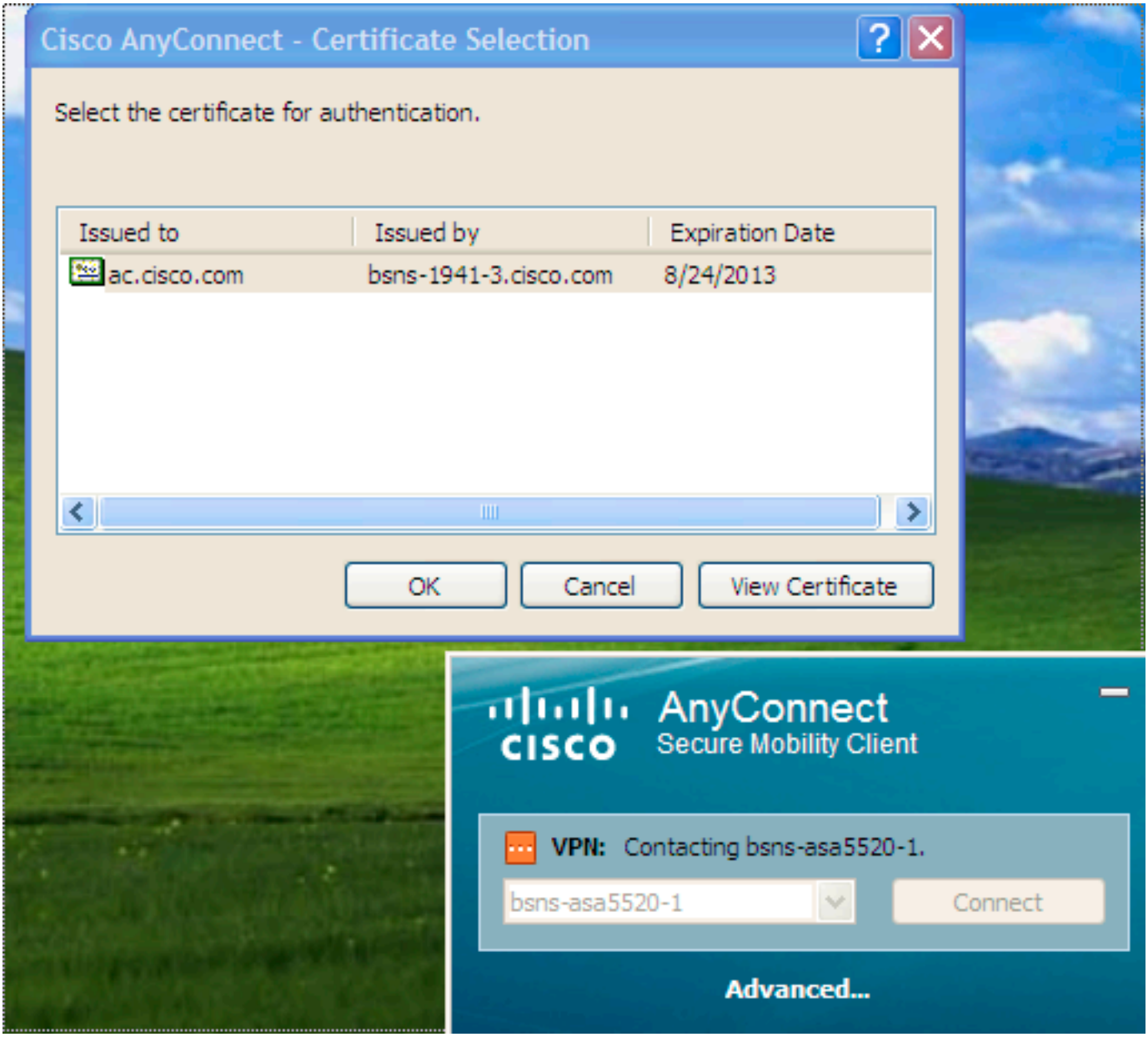
- IKEv2 接続が属するトンネル グループの名前と一致する [UserGroup] を定義する必要があります。 一致していないと、接続が頻繁に失敗し、デバッグに Diffie-Hellman（DH）グループ不一致または同様の検出漏れが示されます。

接続の確立

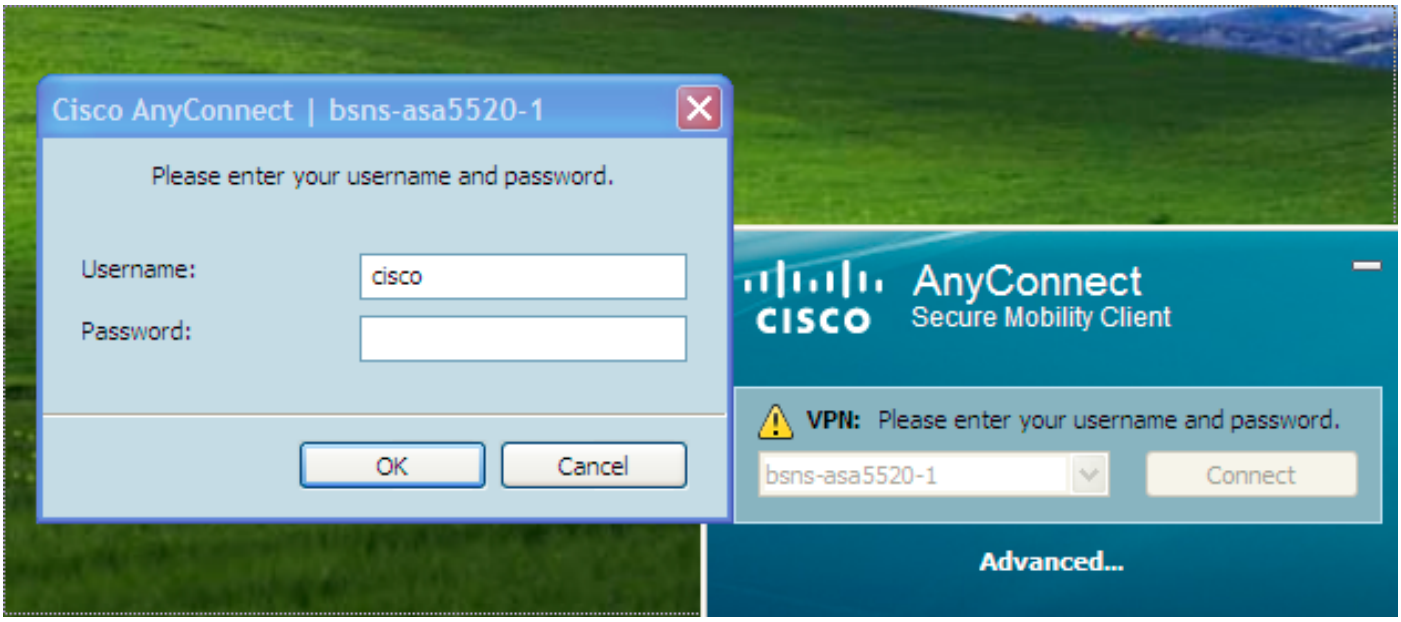
このセクションでは、プロファイルがすでに存在する場合の PC と ASA 間の接続について説明します。

> **注:** GUI に入力する接続情報は、AnyConnect プロファイルに設定されている <HostName> 値です。 この場合、完全修飾ドメイン名（FQDN）ではなく **bsns-asa5520-1** と入力します。

AnyConnect から 1 回目の接続試行を行うと、ゲートウェイから証明書を選択するよう求められます（自動証明書選択が無効にされている場合）。

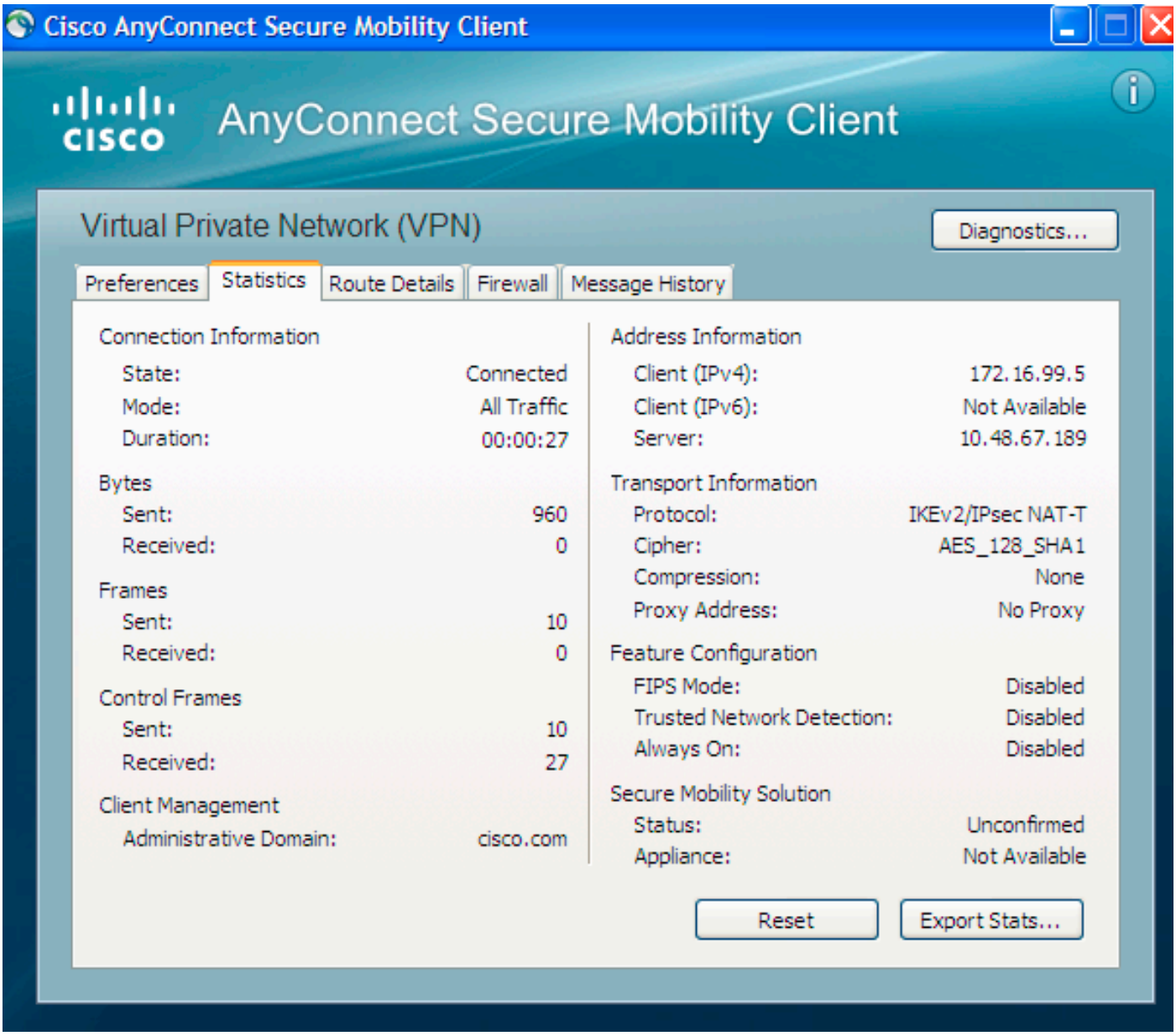


次に、ユーザ名とパスワードを入力する必要があります。



ユーザ名とパスワードが受け入れられると、接続が成功し、AnyConnect の統計情報を確認でき

ます。



ASA での確認

接続で IKEv2、AAA、証明書認証が使用されていることを確認するには、ASA で次のコマンドを入力します。

```
bsns-asa5520-1# show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed
Username : cisco Index : 6
Assigned IP : 172.16.99.5 Public IP : 1.2.3.4
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : AES256 AES128 Hashing : none SHA1 SHA1
Bytes Tx : 0 Bytes Rx : 960
Pkts Tx : 0 Pkts Rx : 10
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_AC Tunnel Group : AC
Login Time : 15:45:41 UTC Tue Aug 28 2012
Duration : 0h:02m:41s
```

```
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1
AnyConnect-Parent:
Tunnel ID : 6.1
Public IP : 1.2.3.4
Encryption : none Auth Mode : Certificate and userPassword
 Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client Type : AnyConnect
Client Ver : 3.0.08057
IKEv2:
Tunnel ID : 6.2
UDP Src Port : 60468 UDP Dst Port : 4500
Rem Auth Mode: Certificate and userPassword
 Loc Auth Mode: rsaCertificate
 Encryption : AES256 Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86238 Seconds
PRF : SHA1 D/H Group : 5
Filter Name :
Client OS : Windows
IPsecOverNatT:
Tunnel ID : 6.3
Local Addr : 0.0.0.0/0.0.0.0/0/0
Remote Addr : 172.16.99.5/255.255.255.255/0/0
Encryption : AES128 Hashing : SHA1\
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 28638 Seconds
Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Bytes Tx : 0 Bytes Rx : 960
Pkts Tx : 0 Pkts Rx : 10
```

既知の警告

このドキュメントで説明した情報には、次の既知の問題および警告があります。

- IKEv2 と SSL のトラストポイントは同一でなければなりません。
- ASA 側の証明書には、FQDN を CN として使用することを推奨します。 AnyConnect プロファイルの <HostAddress> でも、同じ FQDN を参照するようにしてください。
- 接続する際は、AnyConnect プロファイル内の <HostName> 値を入力することに注意してください。
- IKEv2 設定でも、AnyConnect が ASA に接続する際は、IPsec ではなく SSL を使用してプロファイルとバイナリ アップデートをダウンロードします。
- IKEv2 による ASA への AnyConnect 接続では、実装が簡素な独自のメカニズムである EAP-AnyConnect が利用されます。