ASA でのスプリット トンネリングによる AnyConnect セキュア モビリティ クライアントの設定

内容

概要

このドキュメントでは、ソフトウェア バージョン 9.3(2) を実行する Cisco 適応型セキュリティ アプライアンス（ASA）の Cisco Adaptive Security Device Manager（ASDM）で Cisco AnyConnect セキュア モビリティ クライアントを設定する方法について説明します。

前提条件

要件

Cisco AnyConnect セキュア モビリティ クライアントの Web 展開パッケージは、ASA への ASDM アクセスが可能なローカルデスクトップにダウンロードする必要があります。クライアント パッケージをダウンロードするには、Cisco AnyConnect セキュア モビリティ クライアントの Web ページを参照してください。さまざまなオペレーティングシステム（OS）用の Web 展開パッケージを ASA に同時にアップロードできます。

各種 OS 用の Web 展開ファイルの名前は次のとおりです。

- **Microsoft Windows OS**：*AnyConnect-win-<version>-k9.pkg*
- **Macintosh（MAC）OS**：*AnyConnect-macosx-i386-<version>-k9.pkg*
- **Linux OS**：*AnyConnect-linux-<version>-k9.pkg*

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。

- ASA バージョン 9.3(2)
- ASDM バージョン 7.3(1)101
- AnyConnect バージョン 3.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

このドキュメントでは、AnyConnect クライアントを設定し、スプリットトンネリングを有効にするために、ASDM を介して Cisco AnyConnect 設定ウィザードを使用する方法を、順を追って詳しく説明します。

スプリットトンネリングは、特定のトラフィックのみをトンネリングする必要があるシナリオで使用されます。これは、接続時にクライアントマシンで生成されるすべてのトラフィックが VPN を介して転送されるシナリオとは異なります。AnyConnect 設定ウィザードを使用すると、デフォルトでは ASA で *Tunnel-all が設定されます*。スプリットトンネリングは個別に設定する必要があります。これについては、このドキュメントの該当するセクションで詳しく説明します。

この設定例は、10.10.10.0/24 サブネット（ASA の背後にある LAN サブネット）のトラフィックを VPN トンネル経由で送信し、クライアントマシンからの他のトラフィックはすべて独自のインターネット回線経由で転送することを目的としています。

AnyConnect のライセンス情報

Cisco AnyConnect セキュア モビリティ クライアントのライセンスに関する役立つ情報へのリンクを次に示します。

- AnyConnect セキュア モビリティ クライアントおよび関連機能に必要なライセンスを確認するには、『AnyConnect セキュア モビリティ クライアントの機能、ライセンス、および OS - リリース 3.1』を参照してください。
- AnyConnect Apex および Plus のライセンスの詳細については、『Cisco AnyConnect 発注ガイド』を参照してください。
- IP フォンおよびモバイル接続の追加のライセンス要件については、「IP Phone およびモバイ

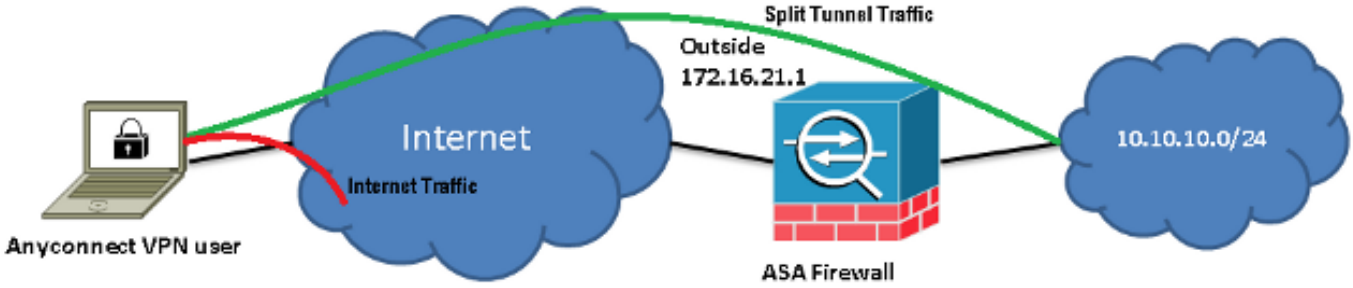
ル VPN 接続に ASA ライセンスが必要な理由」を参照してください。

設定

ここでは、ASA で Cisco AnyConnect セキュア モビリティ クライアントを設定する方法について説明します。

ネットワーク図

次の図は、このドキュメントの例で使用されるトポロジを示しています。

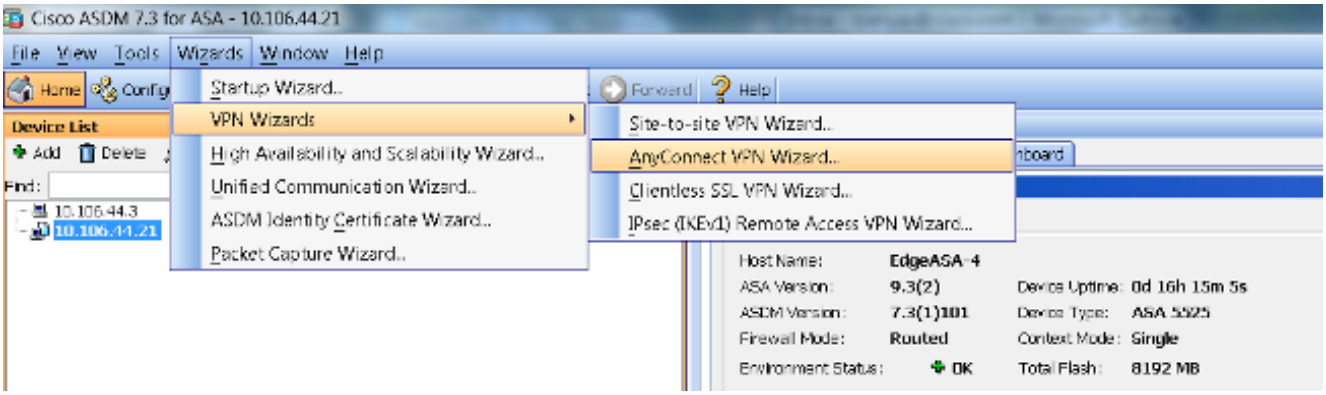


ASDM AnyConnect 構成ウィザード

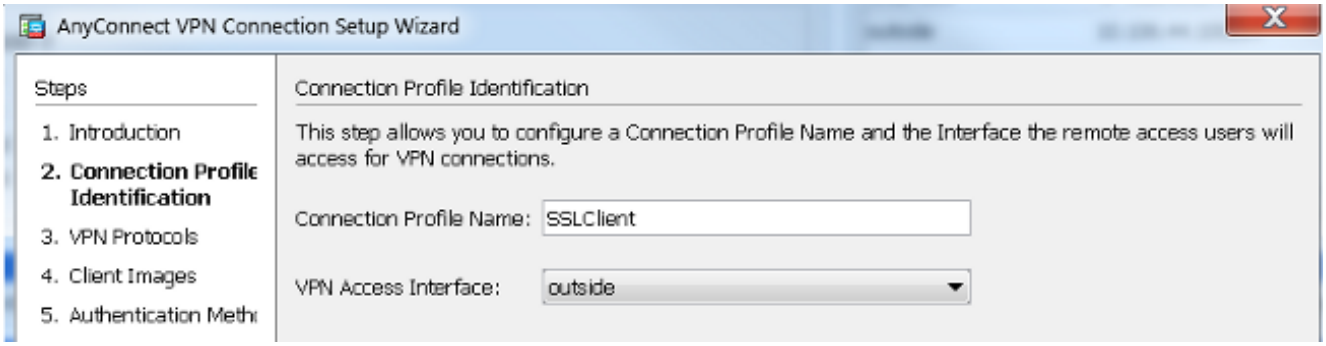
AnyConnect セキュア モビリティ クライアントの設定には、AnyConnect 設定ウィザードを使用できます。先に進む前に、AnyConnect クライアント パッケージが ASA ファイアウォールのフラッシュまたはディスクにアップロードされていることを確認します。

構成ウィザードを使用して AnyConnect セキュア モビリティ クライアントを設定するために、次の手順を実行します。

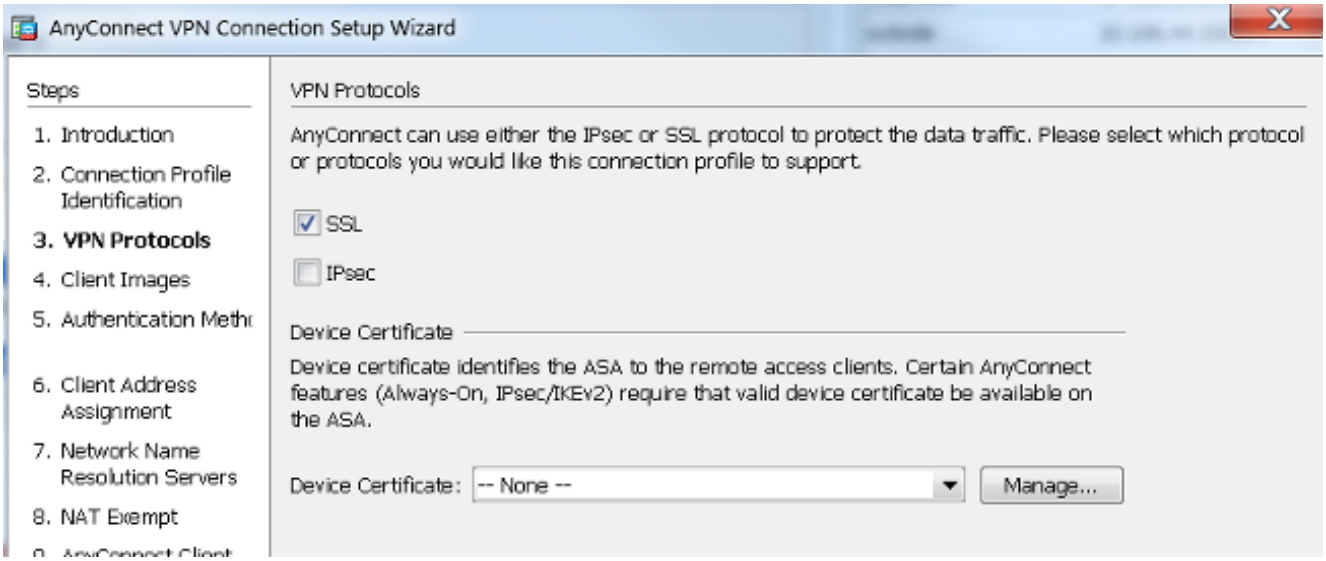
1. ASDM にログインし、**設定ウィザード**を起動して、[次へ（Next）] をクリックします。



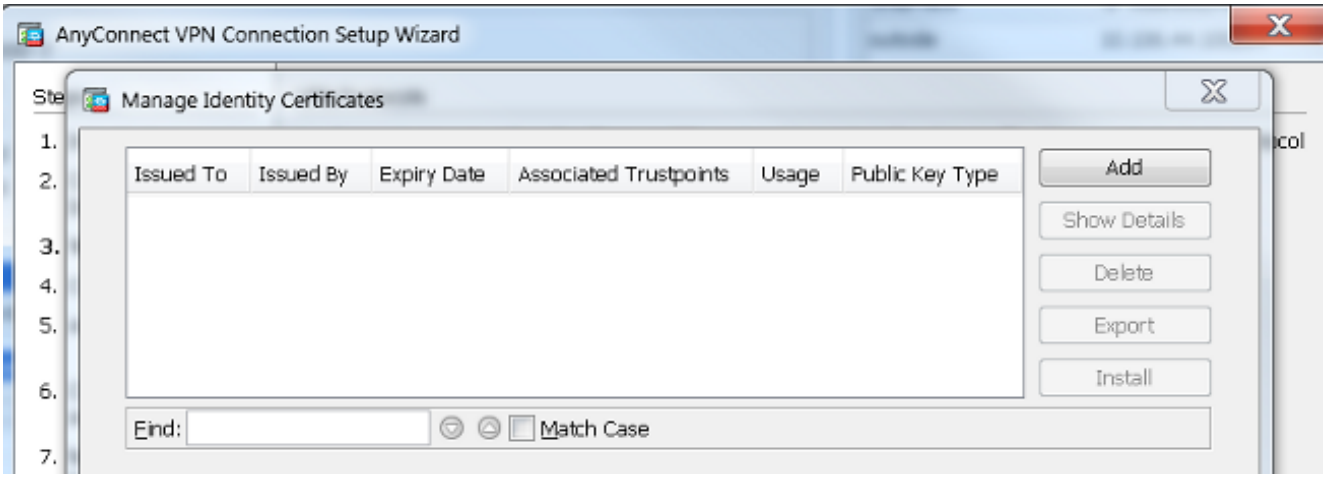
2. [接続プロファイル名（Connection Profile Name）] に接続プロファイル名を入力し、[VPNアクセスインターフェイス（VPN Access Interface）] ドロップダウンメニューから VPN を終了するインターフェイスを選択して、[次へ（Next）] をクリックします。



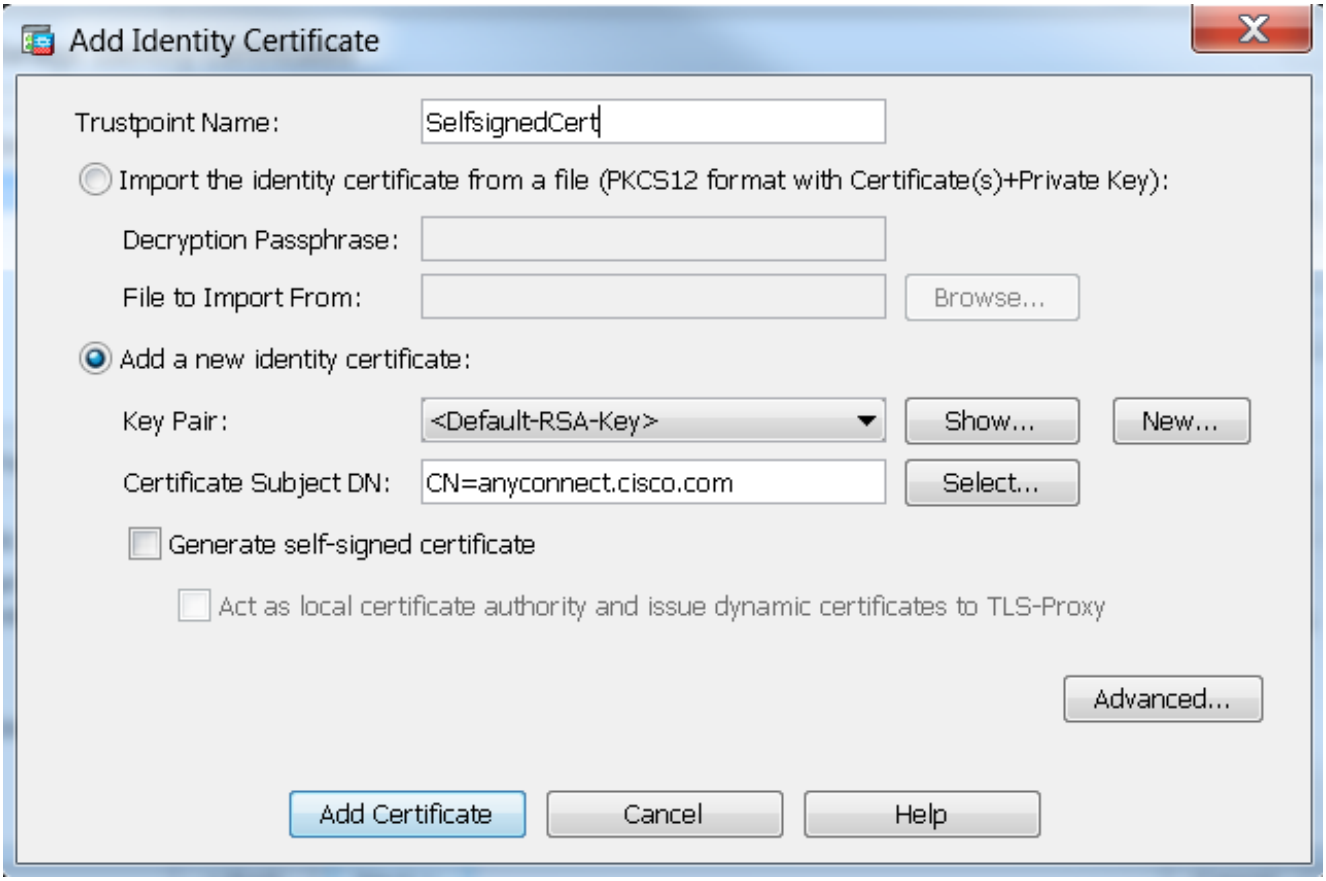
3. セキュア ソケット レイヤ（SSL）を有効にするために、[SSL] **チェックボックスにチェックを入れます。** デバイス証明書は、信頼できるサードパーティの認証局（CA）によって発行された証明書（Verisign、Entrust など）や自己署名証明書にすることができます。証明書がすでに ASA にインストールされている場合、ドロップダウン メニューから選択できます。**注：**この証明書は、提供されるサーバ側の証明書です。ASA に現在インストールされている証明書がなく、自己署名証明書を生成する必要がある場合は、[管理（Manage）] をクリックします。サードパーティの証明書をインストールするために、シスコの [ASA 8.x WebVPN で使用するサードパーティ ベンダーの証明書を手動でインストールする設定例の資料で説明されている手順を実行します。]



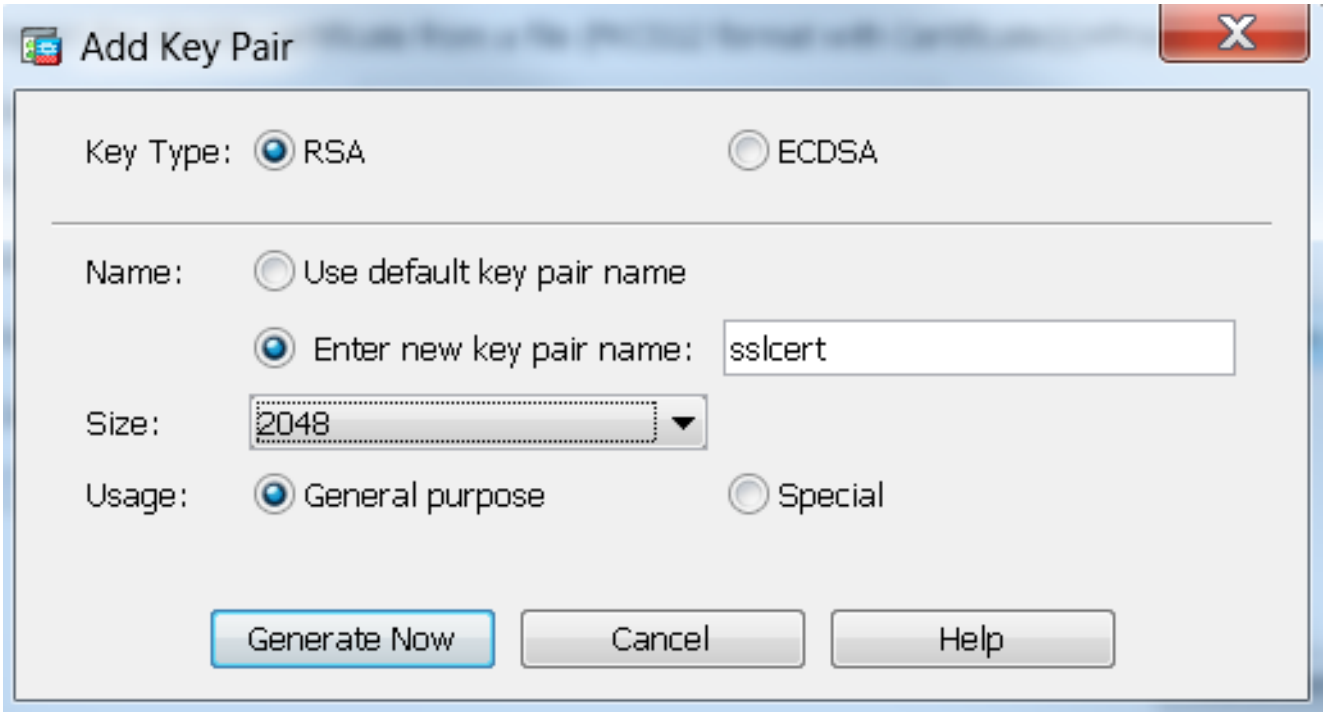
4. [追加（Add）] をクリックします。



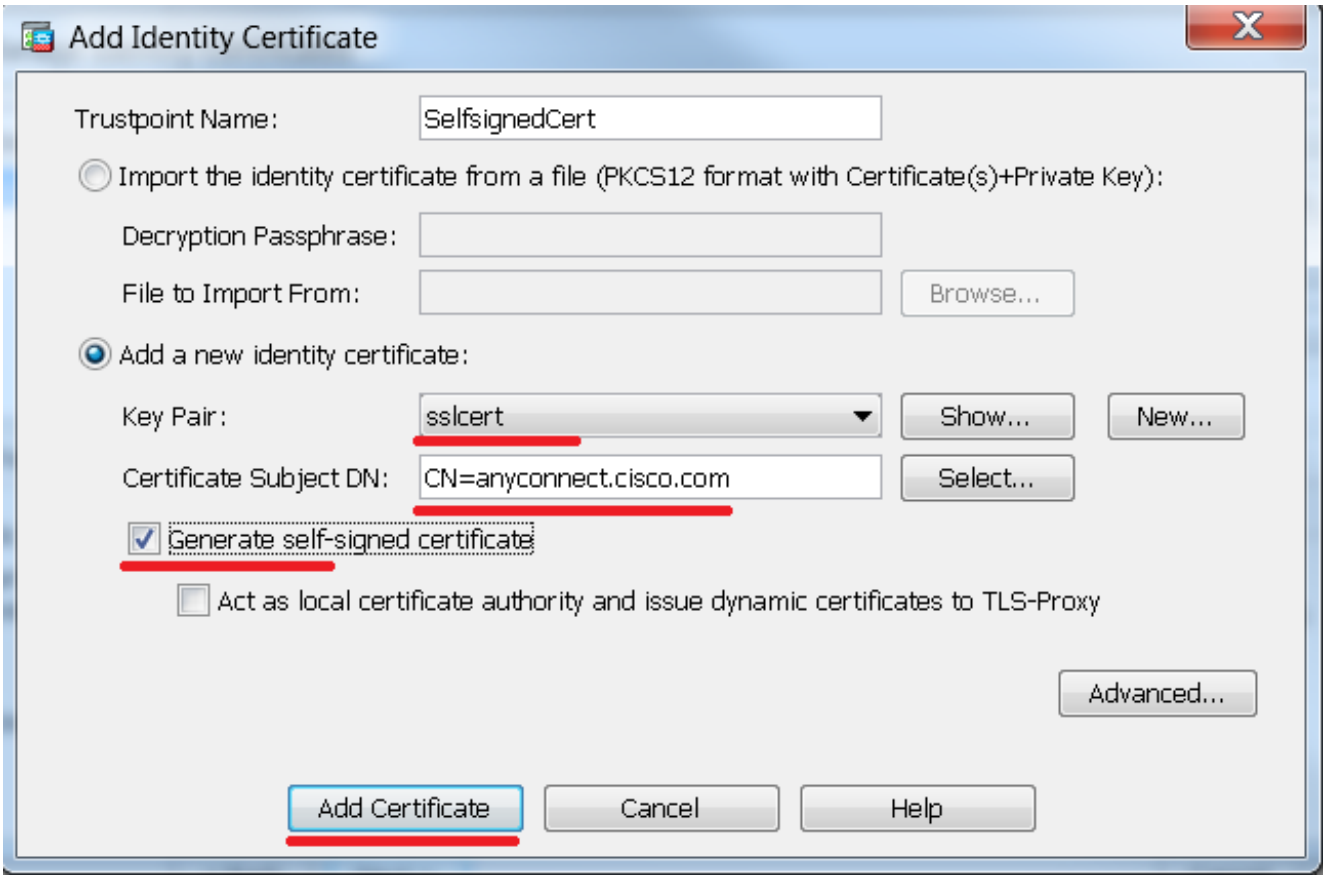
5. [トラストポイント名（Trustpoint Name）] フィールドに適切な名前を入力し、[新しいアイデンティティ証明書の追加（Add a new identity certificate）] オプションボタンをクリックします。デバイスに Rivest-Shamir-Addleman（RSA）キーペアが存在しない場合は、[新規（New）] をクリックしてキーペアを生成します。



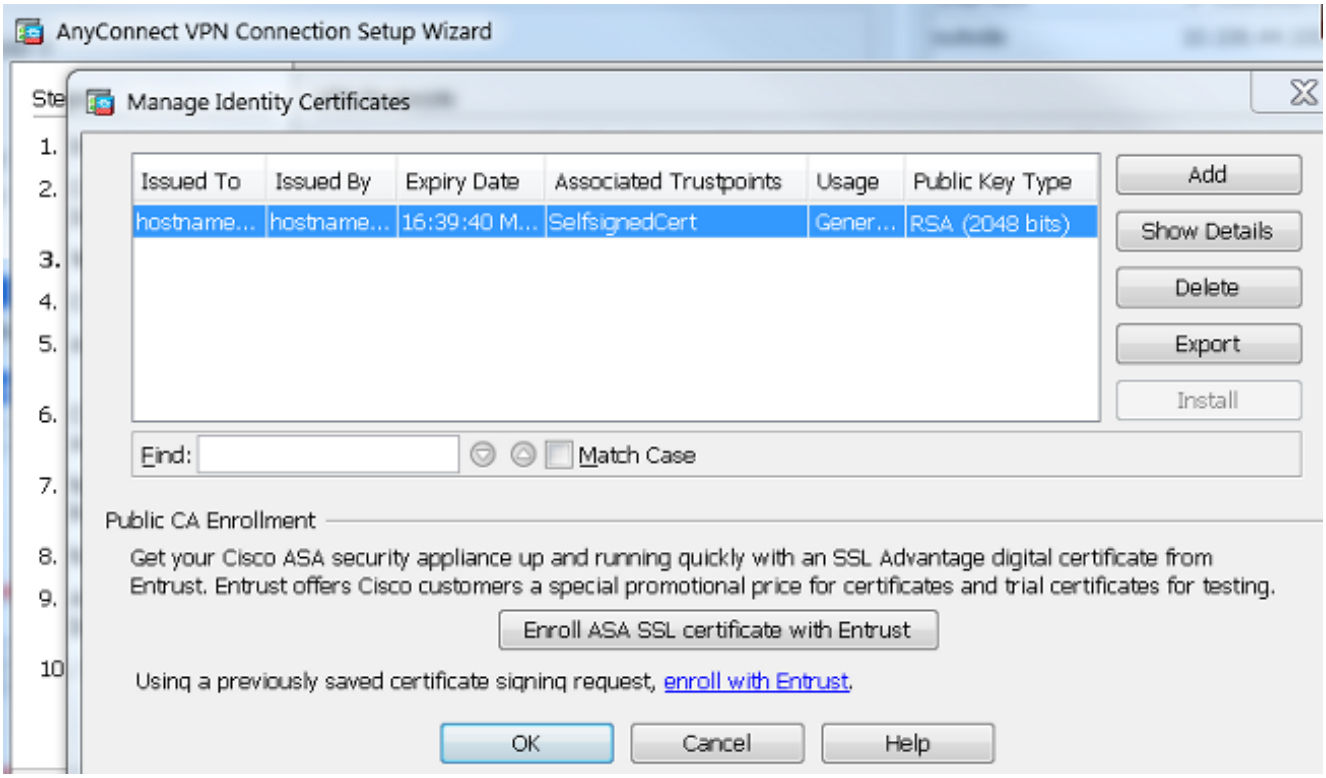
6. [デフォルトのキーペア名を使用（Use default key pair name）] オプションボタンをクリックするか、[新しいキーペア名を入力（Enter new key pair name）] オプションボタンをクリックして新しい名前を入力します。キーのサイズを選択し、[今すぐ生成（Generate Now）] をクリックします。



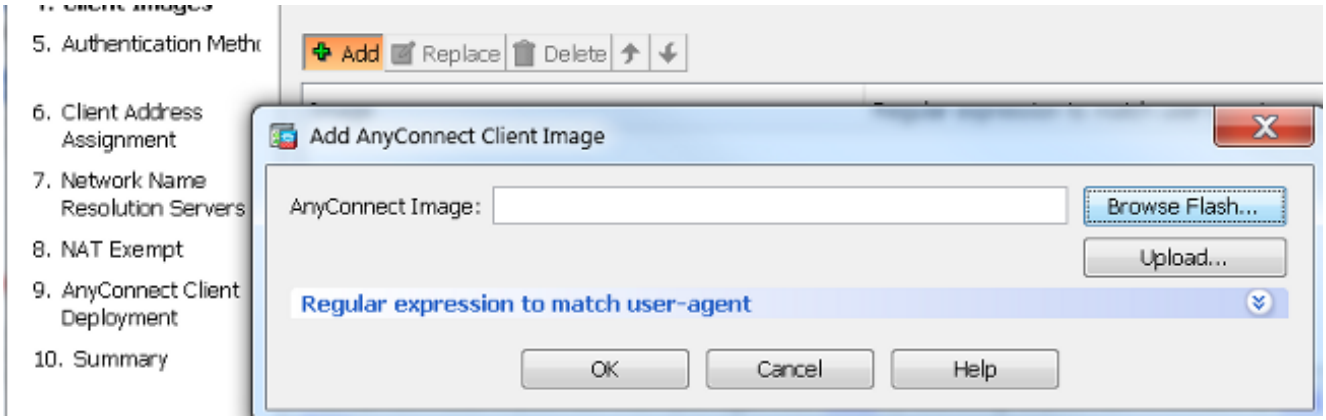
7. RSA キーペアが生成されたら、そのキーを選択し、[自己署名証明書の生成（Generate self-signed certificate）] チェックボックスをオンにします。[証明書サブジェクト DN（Certificate Subject DN）] フィールドに目的のサブジェクトドメイン名（DN）を入力し、[証明書の追加（Add Certificate）] をクリックします。

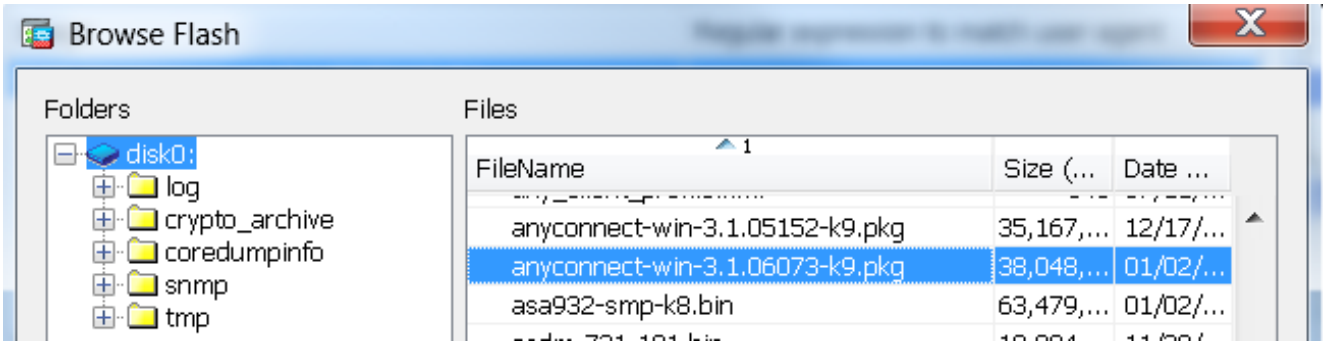


8. 登録が完了したら、[OK]、[OK]、[次へ（Next）] の順にクリックします。

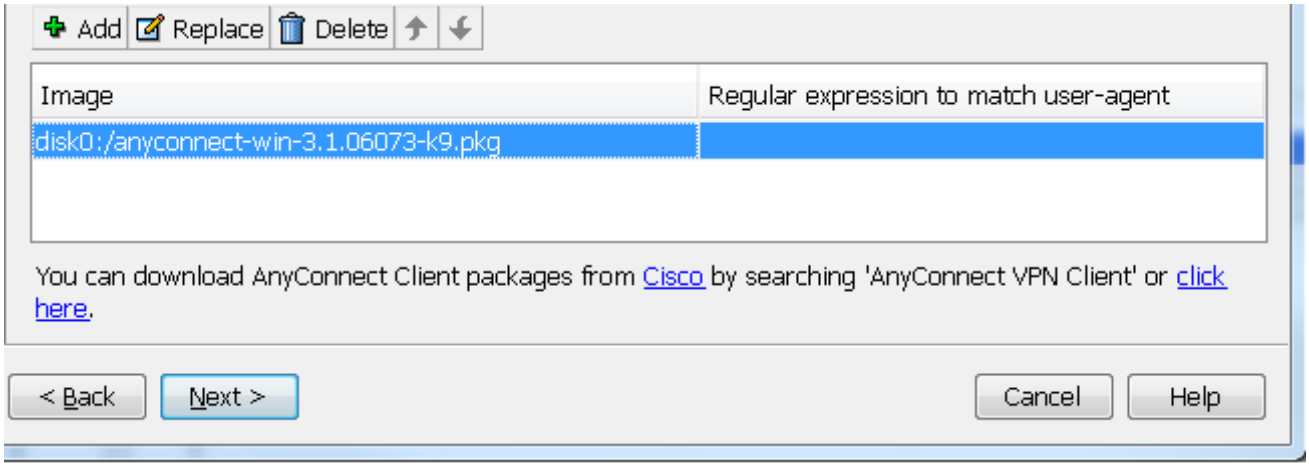


9. PC またはフラッシュから AnyConnect クライアントイメージ（ *.pkg ファイル* ）を追加するために、*[追加（Add）]* をクリックします。[フラッシュの参照（Browse Flash）] をクリックしてフラッシュドライブからイメージを追加するか、[アップロード（Upload）] をクリックしてホストマシンから直接イメージを追加します。

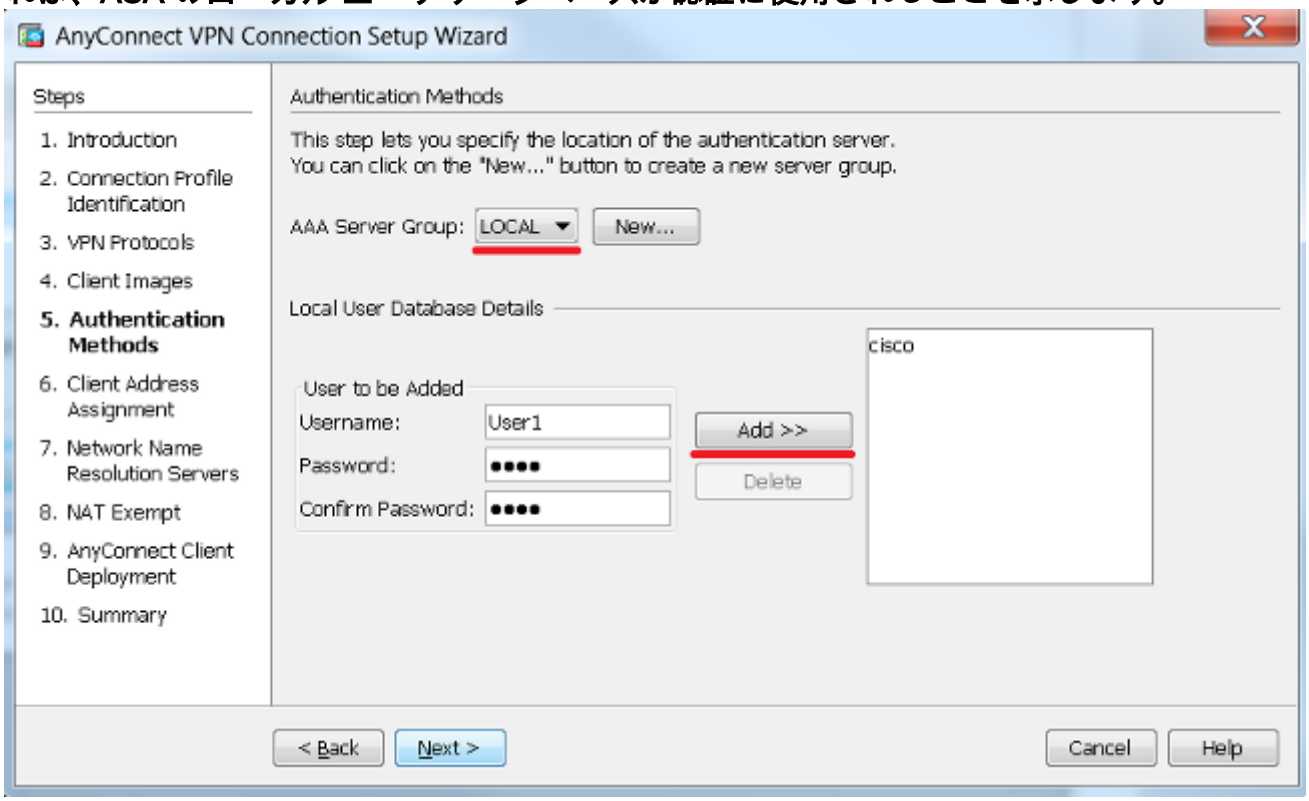




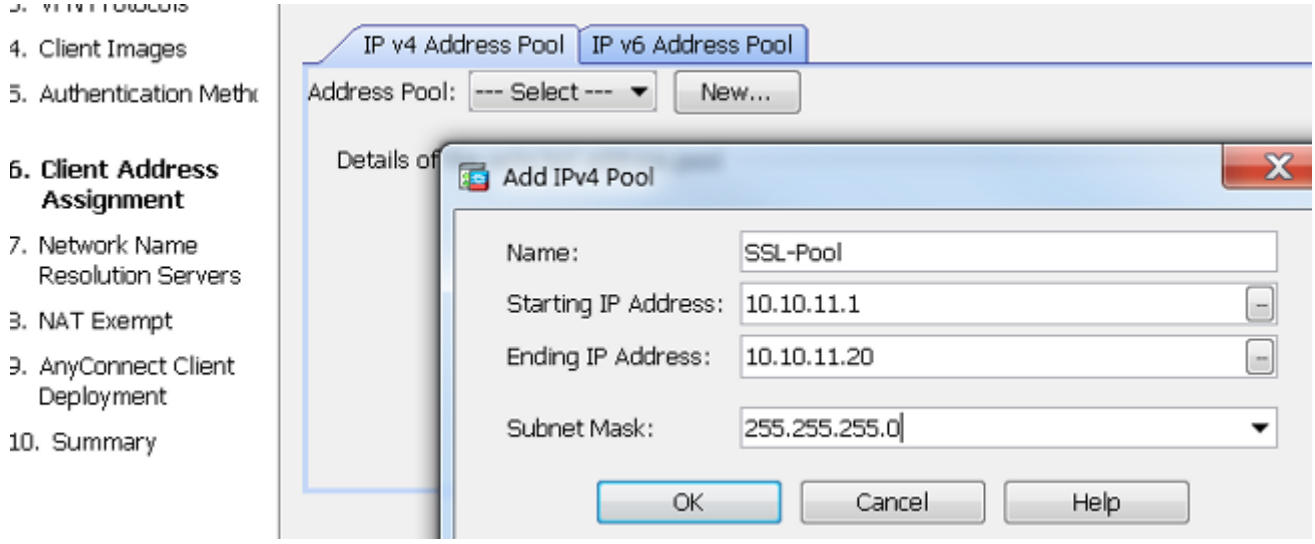
10. イメージが追加されたら、[次へ（Next）] をクリックします。



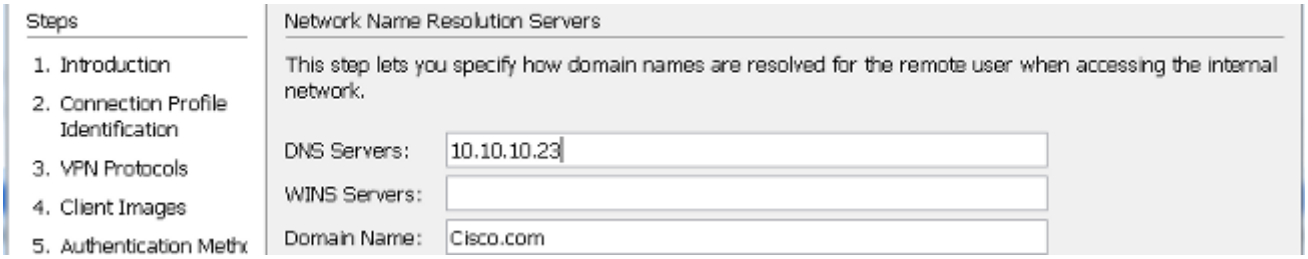
11. ユーザ認証は認証、許可、およびアカウンティング（AAA）サーバ グループを介して実行できます。ユーザーがすでに設定されている場合は、[ローカル（LOCAL）] を選択し、[次へ（Next）] をクリックします。 **注：この例では、ローカル認証が設定されています。これは、ASA のローカル ユーザ データベースが認証に使用されることを示します。**



12. VPN クライアントのアドレスプールが設定されている必要があります。すでに設定されている場合は、それをドロップダウンメニューから選択します。まだ設定されていない場合は、[新規（New）] をクリックして新しく設定します。 完了したら、[OK] をクリックします。

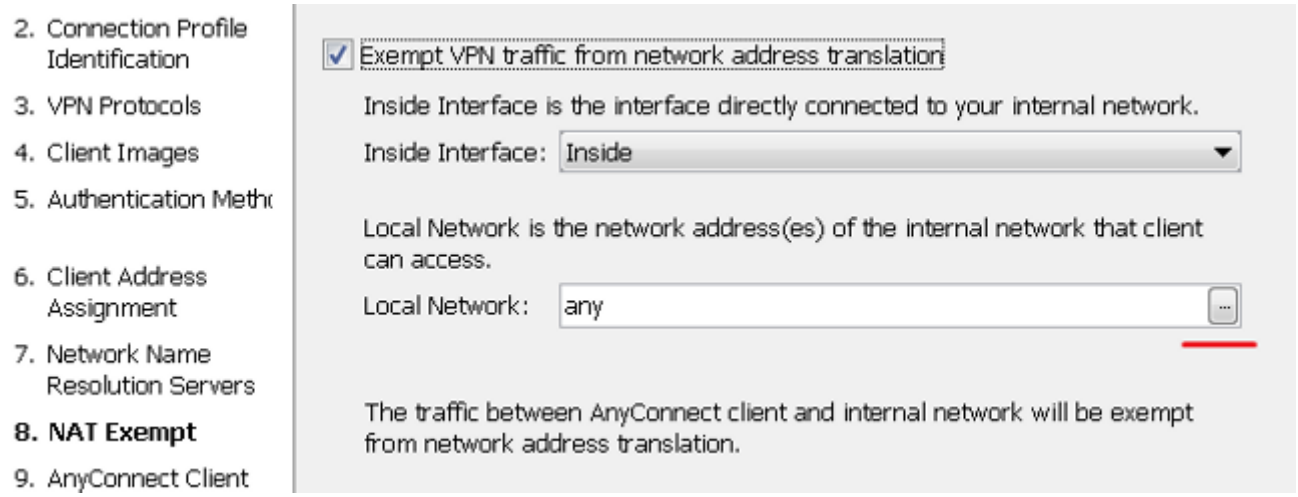


13. ドメインネームシステム（DNS）サーバと DN を [DNS] フィールドと [ドメイン名（Domain Name）] フィールドに適切に入力し、[次へ（Next）] をクリックします。

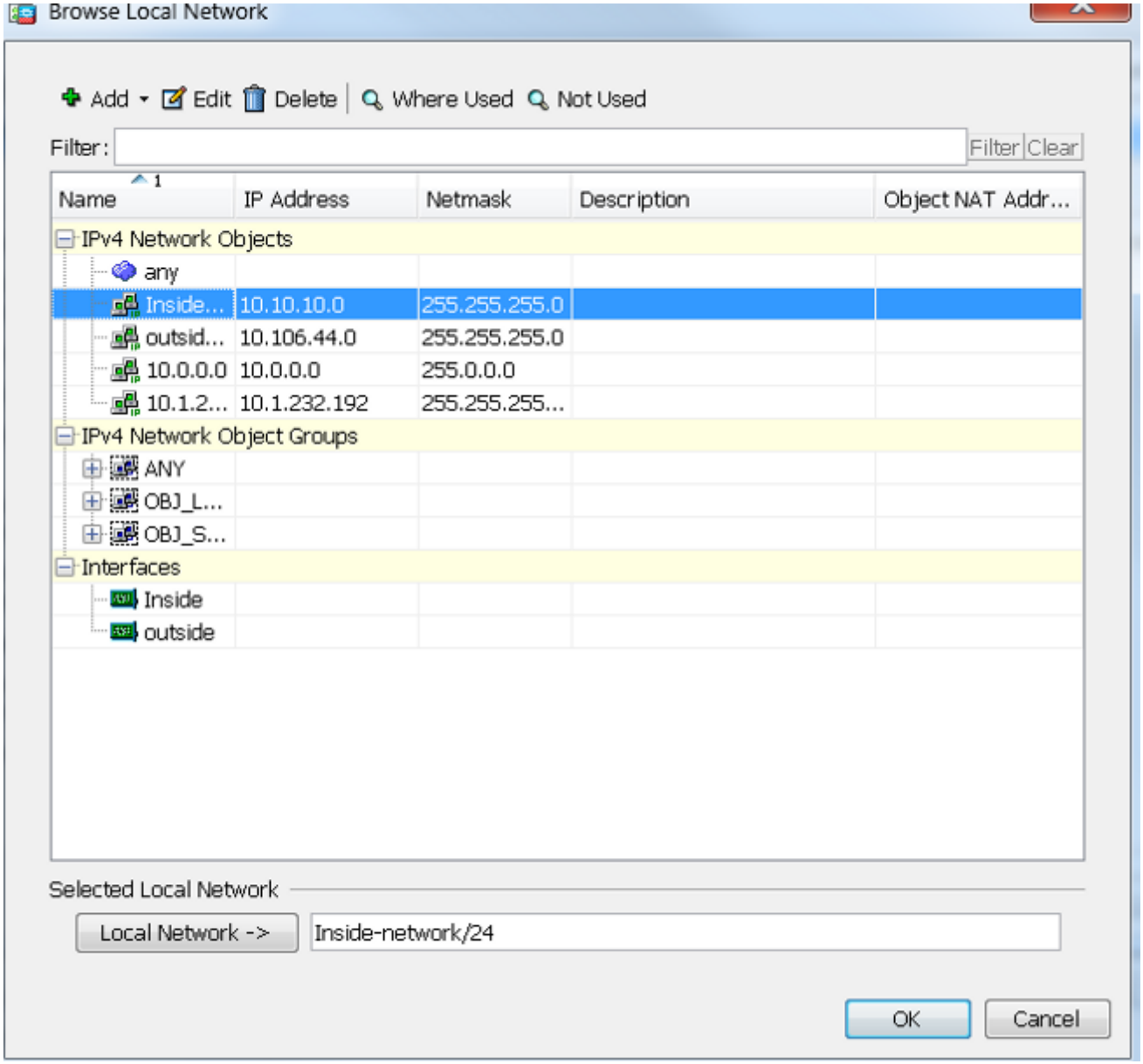


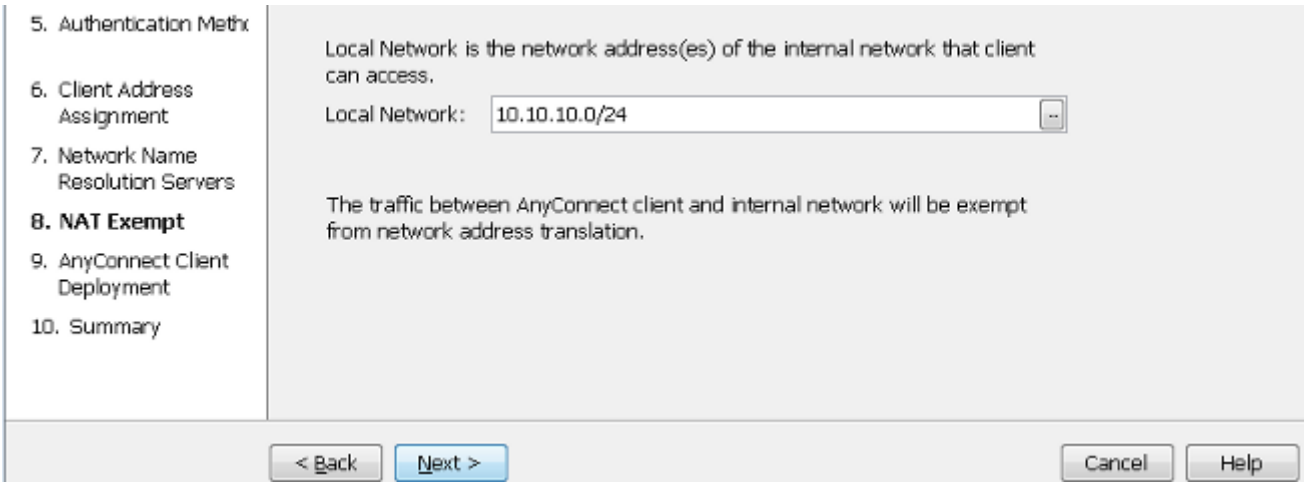
14. このシナリオの目的は、ASA の背後にある*内部（または LAN）サブネットとして設定されている* **10.10.10.0/24 ネットワークへの VPN 経由のアクセスを制限することです。**クライアントと内部サブネットの間のトラフィックは、動的なネットワークアドレス変換（NAT）から除外する必要があります。

[ネットワークアドレス変換からVPNトラフィックを除外（Exempt VPN traffic from network address translation）] チェックボックスをオンにして、除外に使用される LAN および WAN インターフェイスを設定します。



15. 除外する必要があるローカルネットワークを選択します。





16. [次へ（Next）]、[次へ（Next）]、[完了（Finish）] の順にクリックします。

これで、AnyConnect クライアントの設定が完了しました。ただし、設定ウィザードを使用して AnyConnect を設定すると、*スプリットトンネル*ポリシーがデフォルトで「**Tunnel-all**」に設定されます。特定のトラフィックだけをトンネリングするには、*スプリットトンネリングを実装する必要があります。*

注：スプリットトンネリングが設定されていない場合、スプリットトンネルポリシーはデフォルトのグループポリシー（DfltGrpPolicy）から継承されます（デフォルトでは Tunnelall に設定される）。これは、クライアントが VPN を介して接続されるとすべてのトラフィック（Web へのトラフィックを含む）がトンネルを介して送信されることを意味します。

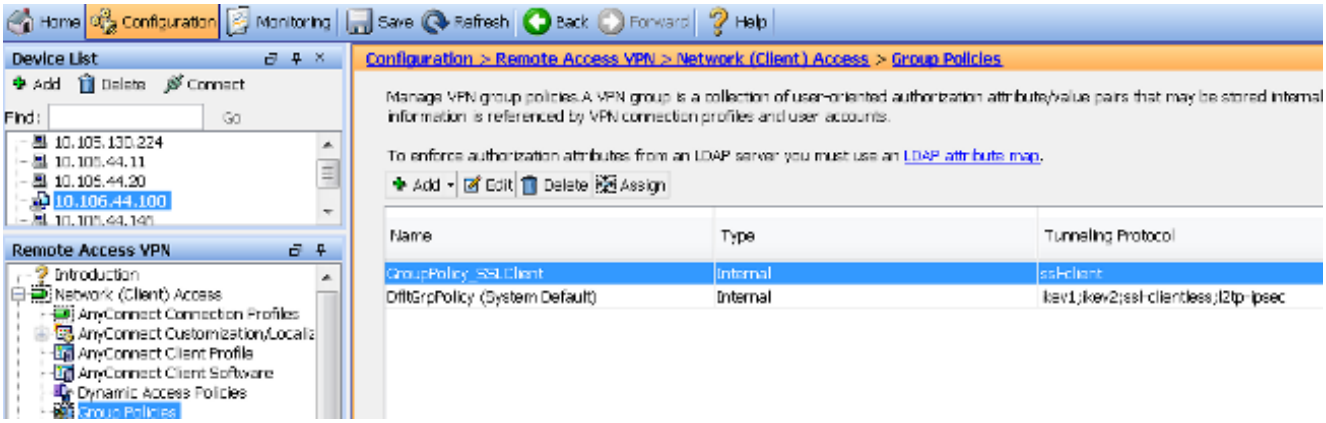
ASA WAN（または*外部*）IP アドレス宛てのトラフィックのみがクライアントマシンでのトンネリングをバイパスします。これは、Microsoft Windowsマシンでの **route print コマンドの出力で確認できます。**

Split-tunnel 設定

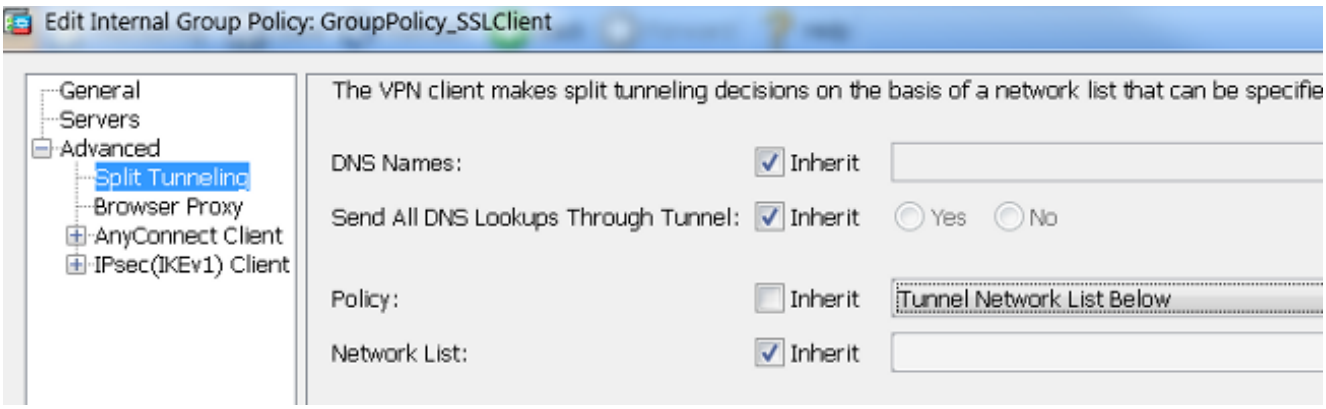
スプリットトンネリングは、暗号化する必要があるサブネットまたはホストのトラフィックを定義するために使用できる機能です。これには、この機能に関連付けられるアクセスコントロールリスト（ACL）の設定が含まれます。この ACL で定義されたサブネットまたはホストのトラフィックは、クライアント側からのトンネルを介して暗号化され、これらのサブネットのルートは PC ルーティングテーブルにインストールされます。

Tunnel-all 設定から Split-tunnel 設定に移行するには、次の手順に従います。

1. [設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [グループポリシー（Group Policies）] に移動します。

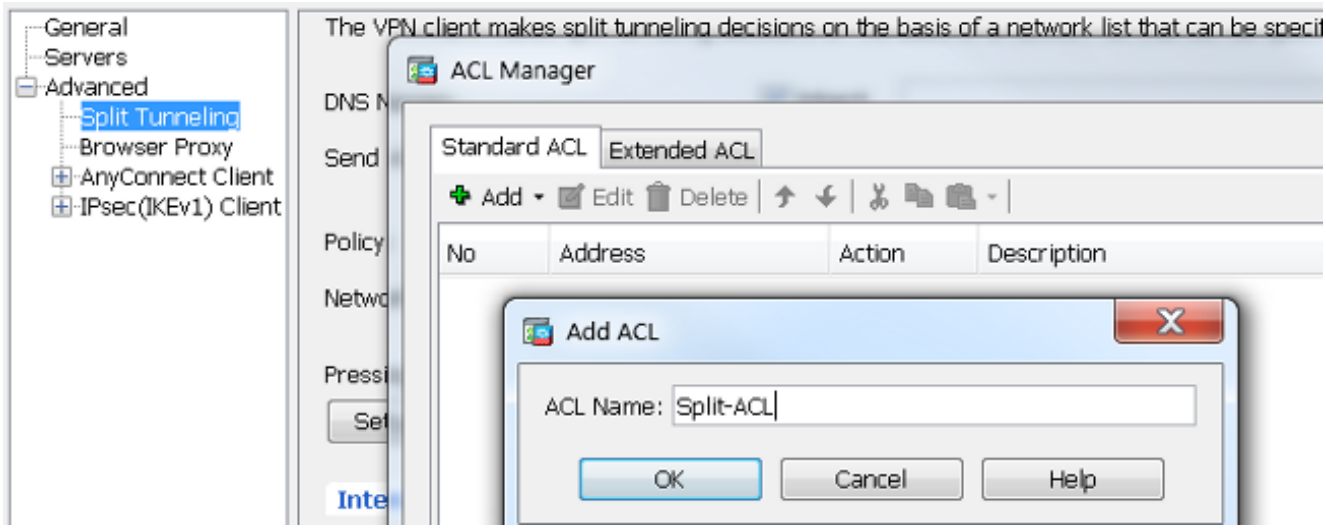


2. [編集（Edit）] をクリックし、ナビゲーションツリーを使用して [詳細（Advanced）] > [スプリットトンネリング（Split Tunneling）] に移動します。[ポリシー（Policy）] セクションの [継承（Inherit）] チェックボックスをオフにして、ドロップダウンメニューから [以下のネットワークリストをトンネリング（Tunnel Network List Below）] を選択します。

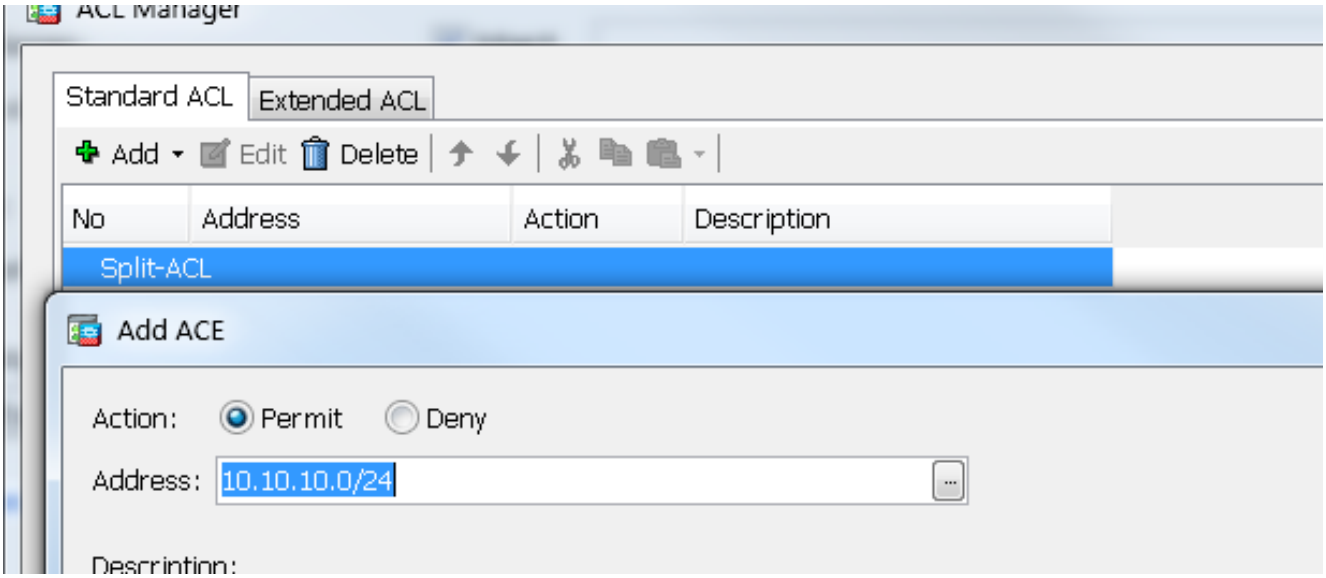


3. [ネットワークリスト（Network List）] セクションの [継承（Inherit）] チェックボックスをオフにして、[管理（Manage）] をクリックし、クライアントがアクセスする必要のある LAN ネットワークを指定する ACL を選択します。

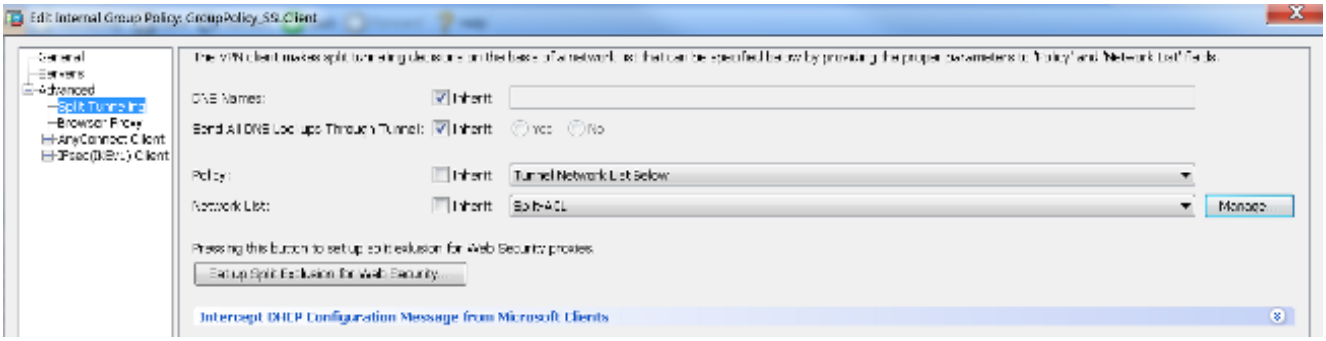
4. [標準ACL（Standard ACL）]、[追加（Add）]、[ACLの追加（Add ACL）]、[ACL名（ACL Name）] の順にクリックします。



5. [追加（Add）] をクリックしてルールを追加します。



6. [OK] をクリックします。



7. [Apply] をクリックします。

接続されると、Split-ACL に含まれるサブネットまたはホストのルートがクライアントマシンのルーティングテーブルに追加されます。Microsoft Windowsマシンでは、これを route print コマンドの出力で確認できます。これらのルートのネクストホップは、クライアント IP プールサブネットからの IP アドレス (通常、サブネットの最初の IP アドレス) です。

```
C:\Users\admin>route print
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 10.106.44.1 10.106.44.243 261
10.10.10.0      255.255.255.0    10.10.11.2  10.10.11.1     2

!! This is the split tunnel route.

10.106.44.0 255.255.255.0 On-link 10.106.44.243 261
172.16.21.1    255.255.255.255     On-link    10.106.44.243  6

!! This is the route for the ASA Public IP Address.
```

MAC OS マシンでは、netstat -r コマンドを入力して PC ルーティングテーブルを表示します。

```
$ netstat -r
Routing tables
Internet:
Destination Gateway Flags Refs Use Netif Expire
default hsrp-64-103-236-1. UGSc 34 0 en1
10.10.10/24        10.10.11.2         UGSc    0   44   utun1

!! This is the split tunnel route.

10.10.11.2/32 localhost UGSc 1 0 lo0
172.16.21.1/32     hsrp-64-103-236-1. UGSc    1   0    en1

!! This is the route for the ASA Public IP Address.
```

AnyConnect クライアントのダウンロードとインストール

Cisco AnyConnect セキュア モビリティ クライアントは次の 2 つの方法でユーザマシンに展開できます。

- Web 展開
- スタンドアロン展開

これらの方法の両方について、以下のセクションで詳しく説明します。

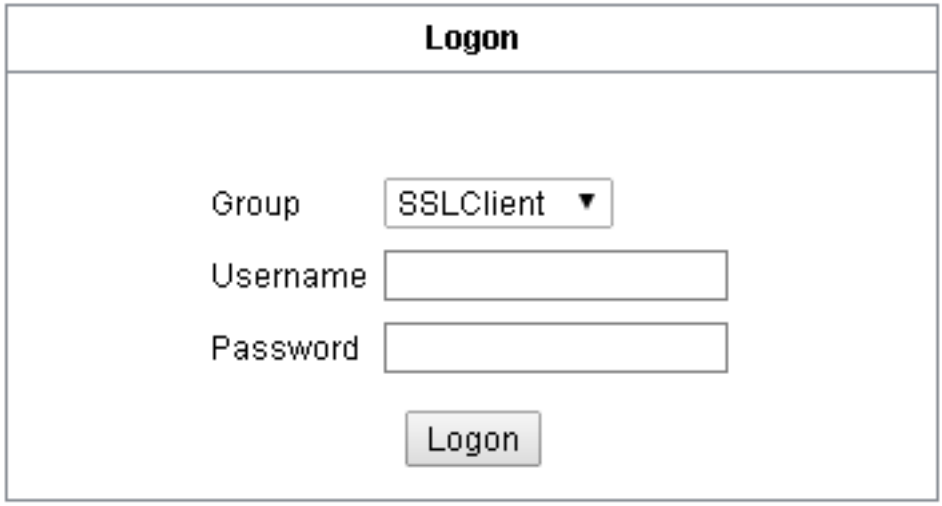
Web 展開

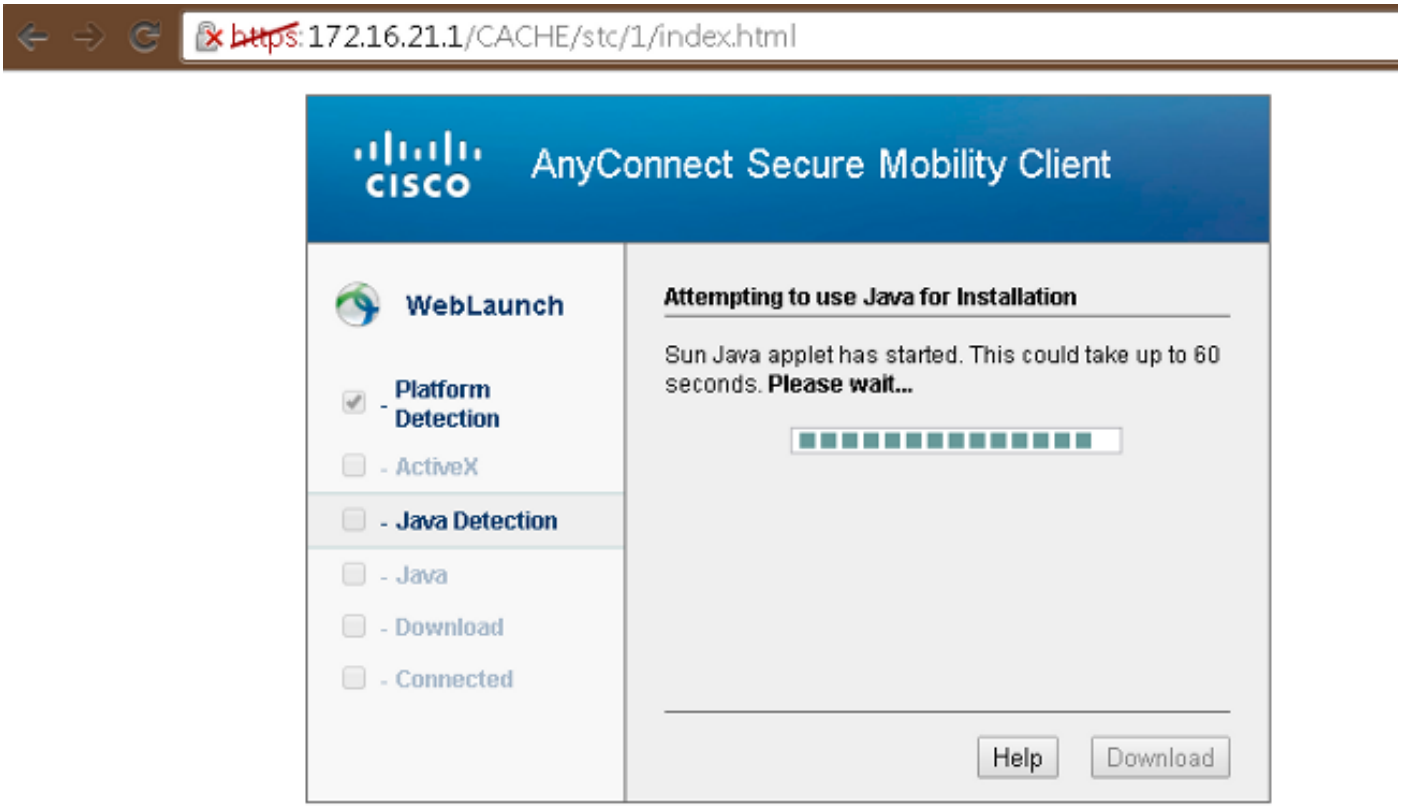
Web 展開方式を使用するには、クライアントマシンのブラウザに **https://<ASA's FQDN> または <ASA's IP>**URL を入力して *WebVPN* ポータルページを表示します。

> **注：**Internet Explorer（IE）を使用する場合は、Java を強制的に使用する設定になっていなければ、インストールのほとんどが ActiveX を介して完了します。他のすべてのブラウザでは Java が使用されます。

ページにログインすると、クライアントマシンへのインストールが開始され、インストールの完了後にクライアントが ASA に接続します。

> **注：**ActiveX または Java を実行する権限を求められる場合があります。インストールを続行するには、これを許可する必要があります。

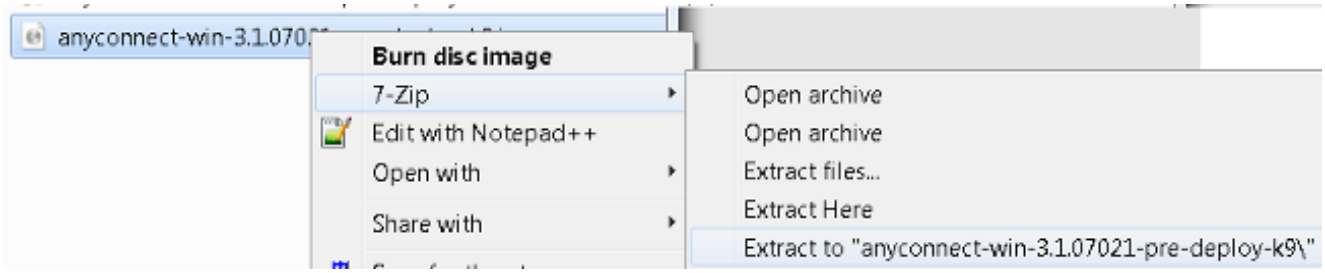




スタンドアロンでの導入

スタンドアロン展開の方法を使用するには、次の手順に従います。

1. シスコの Web サイトから AnyConnect クライアントのイメージをダウンロードします。ダウンロードするイメージを正しく選択するには、Cisco AnyConnect セキュア モビリティ クライアントの Web ページを参照してください。このページにダウンロードリンクがあります。 ダウンロードページに移動し、適切なバージョンを選択します。 「**Full installation package - Windows / Standalone installer (ISO)**」を検索してください。 **注**：ISO インストーライメージ（ *anyconnect-win-3.1.06073-pre-deploy-k9.iso* など）がダウンロードされます。
2. *WinRar または 7-Zip を使用して ISO パッケージの内容を抽出します。*



3. 内容が抽出されたら、**Setup.exe ファイルを実行し、Cisco AnyConnect セキュア モビリティ クライアントと同時にインストールする必要があるモジュールを選択します。**

   ヒント：VPN の追加設定を指定するには、『*Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6*』の「Configuring AnyConnect VPN Client Connections」を参照してください。

CLI での設定

ここでは、参考までに Cisco AnyConnect セキュア モビリティ クライアントの CLI 設定の例を示します。

```
ASA Version 9.3(2)
!
hostname PeerASA-29
enable password 8Ry2YjIyt7RRXU24 encrypted
ip local pool SSL-Pool 10.10.11.1-10.10.11.20 mask 255.255.255.0
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.21.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!
boot system disk0:/asa932-smp-k8.bin
ftp mode passive
object network NETWORK_OBJ_10.10.10.0_24
subnet 10.10.10.0 255.255.255.0
object network NETWORK_OBJ_10.10.11.0_27
subnet 10.10.11.0 255.255.255.224

access-list all extended permit ip any any

!***********Split ACL configuration***********

access-list Split-ACL standard permit 10.10.10.0 255.255.255.0
no pager
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-721.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected

!************** NAT exemption Configuration *****************
!This will exempt traffic from Local LAN(s) to the
!Remote LAN(s) from getting NATted on any dynamic NAT rule.

nat (inside,outside) source static NETWORK_OBJ_10.10.10.0_24 NETWORK_OBJ_10.10.10.0_24
destination static NETWORK_OBJ_10.10.11.0_27 NETWORK_OBJ_10.10.11.0_27 no-proxy-arp
route-lookup
access-group all in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.21.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
```

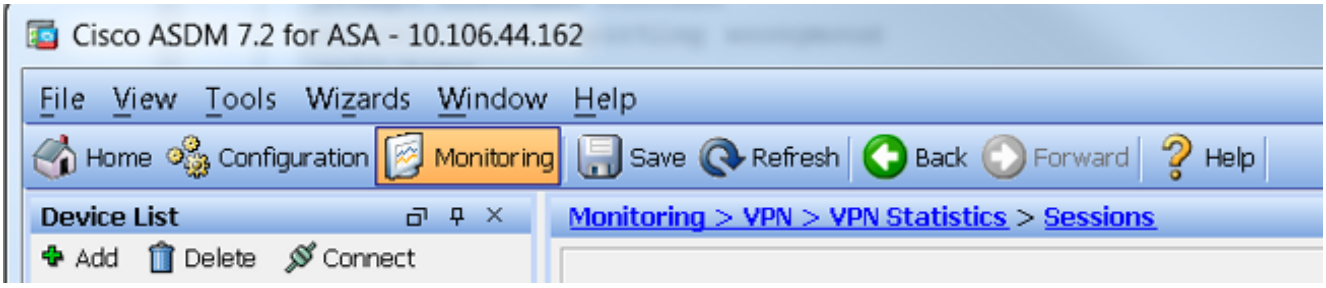
```
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact

!********** Trustpoint for Selfsigned certificate**********
!Genarate the key pair and then configure the trustpoint
!Enroll the trustpoint genarate the self-signed certificate

crypto ca trustpoint SelfsignedCert
enrollment self
subject-name CN=anyconnect.cisco.com
keypair sslcert
crl configure
crypto ca trustpool policy
crypto ca certificate chain SelfsignedCert
certificate 4748e654
308202f0 308201d8 a0030201 02020447 48e65430 0d06092a 864886f7 0d010105
0500303a 311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e
636f6d31 19301706 092a8648 86f70d01 0902160a 50656572 4153412d 3239301e
170d3135 30343032 32313534 30375a17 0d323530 33333032 31353430 375a303a
311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e 636f6d31
19301706 092a8648 86f70d01 0902160a 50656572 4153412d 32393082 0122300d
06092a86 4886f70d 01010105 00038201 0f003082 010a0282 010100f6 a125d0d0
55a975ec a1f2133f 0a2c3960 0da670f8 bcb6dad7 efefe50a 482db3a9 7c6db7c4
ed327ec5 286594bc 29291d8f 15140bad d33bc492 02f5301e f615e7cd a72b60e0
7877042b b6980dc7 ccaa39c8 c34164d9 e2ddeea1 3c0b5bad 5a57ec4b d77ddb3c
75930fd9 888f92b8 9f424fd7 277e8f9e 15422b40 071ca02a 2a73cf23 28d14c93
5a084cf0 403267a6 23c18fa4 fca9463f aa76057a b07e4b19 c534c0bb 096626a7
53d17d9f 4c28a3fd 609891f7 3550c991 61ef0de8 67b6c7eb 97c3bff7 c9f9de34
03a5e788 94678f4d 7f273516 c471285f 4e23422e 6061f1e7 186bbf9c cf51aa36
19f99ab7 c2bedb68 6d182b82 7ecf39d5 1314c87b ffddff68 8231d302 03010001
300d0609 2a864886 f70d0101 05050003 82010100 d598c1c7 1e4d8a71 6cb43296
c09ea8da 314900e7 5fa36947 c0bc1778 d132a360 0f635e71 400e592d b27e29b1
64dfb267 51e8af22 0a6a8378 5ee6a734 b74e686c 6d983dde 54677465 7bf8fe41
daf46e34 bd9fd20a bacf86e1 3fac8165 fc94fe00 4c2eb983 1fc4ae60 55ea3928
f2a674e1 8b5d651f 760b7e8b f853822c 7b875f91 50113dfd f68933a2 c52fe8d9
4f9d9bda 7ae2f750 313c6b76 f8d00bf5 1f74cc65 7c079a2c 8cce91b0 a8cdd833
900a72a4 22c2b70d 111e1d92 62f90476 6611b88d ff58de5b fdaa6a80 6fe9f206
3fe4b836 6bd213d4 a6356a6c 2b020191 bf4c8e3d dd7bdd8b 8cc35f0b 9ad8852e
b2371ee4 23b16359 ba1a5541 ed719680 ee49abe8
quit
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ssl server-version tlsv1-only
ssl encryption des-sha1 3des-sha1 aes128-sha1 aes256-sha1

!******** Bind the certificate to the outside interface********
ssl trust-point SelfsignedCert outside

!********Configure the Anyconnect Image and enable Anyconnect***
webvpn
enable outside
```

```
anyconnect image disk0:/anyconnect-win-3.1.06073-k9.pkg 1
anyconnect enable
tunnel-group-list enable

!*******Group Policy configuration*********
!Tunnel protocol, Spit tunnel policy, Split
!ACL, etc. can be configured.

group-policy GroupPolicy_SSLClient internal
group-policy GroupPolicy_SSLClient attributes
wins-server none
dns-server value 10.10.10.23
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Split-ACL
default-domain value Cisco.com

username User1 password PfeNk7qp9b4LbLV5 encrypted
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15

!*******Tunnel-Group (Connection Profile) Configuraiton*****
tunnel-group SSLClient type remote-access
tunnel-group SSLClient general-attributes
address-pool SSL-Pool
default-group-policy GroupPolicy_SSLClient
tunnel-group SSLClient webvpn-attributes
group-alias SSLClient enable
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:8d492b10911d1a8fbcc93aa4405930a0
: end
```

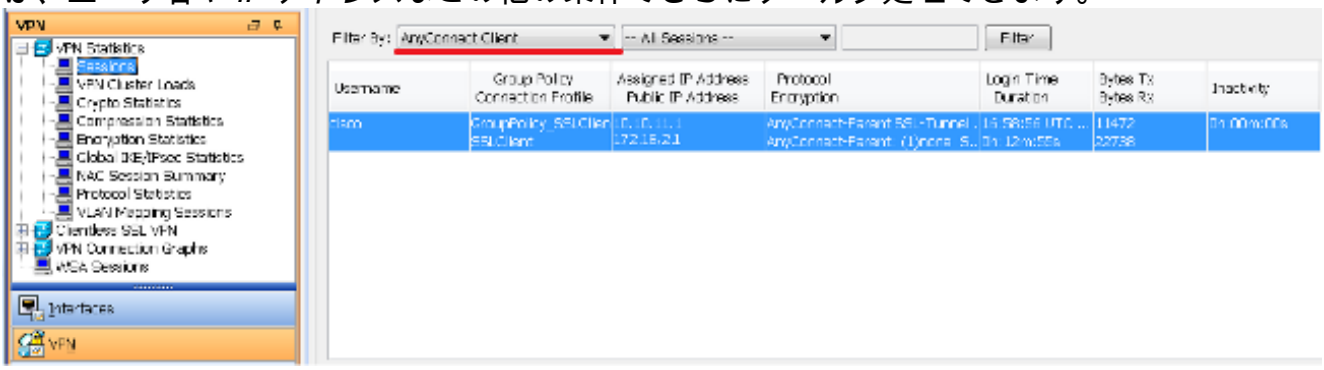
確認

クライアント接続とその接続に関連付けられているさまざまなパラメータを確認するには、次の手順に従います。

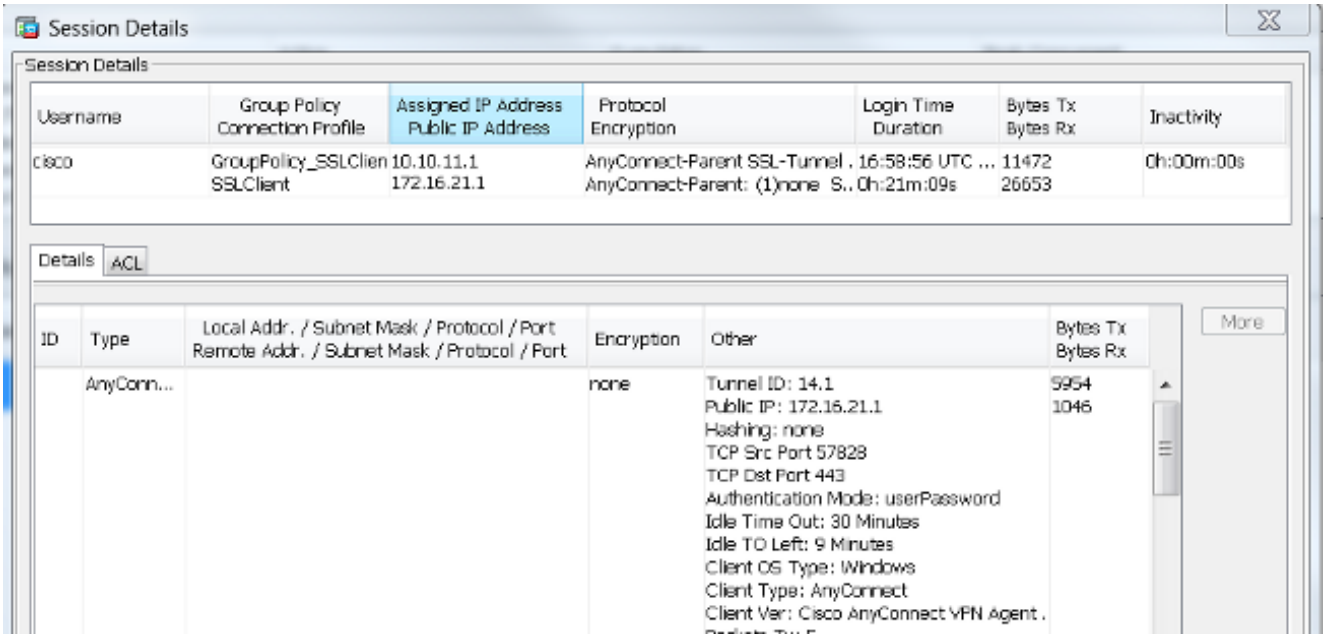
1. ASDMで [モニタリング（Monitoring）] > [VPN] に移動します。



2. [次でフィルタ処理（Filter By）] オプションを使用すると VPN のタイプをフィルタ処理できます。ドロップダウンメニューから [AnyConnectクライアント（AnyConnect Client）] を選択し、すべての AnyConnect クライアントセッションを選択します。 **ヒント**：セッションは、ユーザ名や *IP アドレス*などの他の条件でさらにフィルタ処理できます。



3. 特定のセッションの詳細情報を取得するには、そのセッションをダブルクリックします。



4. CLI に **show vpn-sessiondb anyconnect コマンドを入力してセッションの詳細情報を取得します。**

```
# show vpn-sessiondb anyconnect
Session Type : AnyConnect
Username : cisco Index : 14
Assigned IP : 10.10.11.1   Public IP : 172.16.21.1
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
```

```
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11472 Bytes Rx : 39712
Group Policy : GroupPolicy_SSLClient   Tunnel Group : SSLClient
Login Time : 16:58:56 UTC Mon Apr 6 2015
Duration : 0h:49m:54s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

5. 他のフィルタオプションを使用して結果を絞り込むことができます。

```
# show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed

Username : cisco Index : 19
Assigned IP : 10.10.11.1    Public IP : 10.106.44.243
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11036 Bytes Rx : 4977
Pkts Tx : 8 Pkts Rx : 60
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_SSLClient  Tunnel Group : SSLClient
Login Time   : 20:33:34 UTC Mon Apr 6 2015
Duration : 0h:01m:19s

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 19.1
Public IP : 10.106.44.243
Encryption : none Hashing : none
TCP Src Port : 58311 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : AnyConnect
Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 5518 Bytes Rx : 772
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 19.2
Assigned IP : 10.10.11.1 Public IP : 10.106.44.243
Encryption : 3DES Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 58315
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 5518 Bytes Rx : 190
Pkts Tx : 4 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 19.3
```

```
Assigned IP : 10.10.11.1 Public IP : 10.106.44.243
Encryption : DES Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 58269
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 0 Bytes Rx : 4150
Pkts Tx : 0 Pkts Rx : 59
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

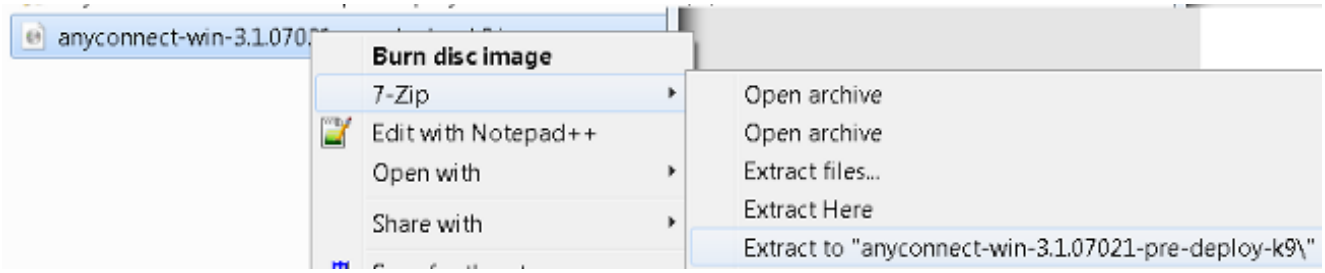
トラブルシュート

AnyConnect Diagnostics and Reporting Tool（DART）を使用すると、AnyConnect のインストールと接続に関する問題のトラブルシューティングに役立つデータを収集できます。 DART ウィザードは、AnyConnect が稼働するコンピュータで使用します。DART によってログ、ステータス、および診断情報が収集され、それを Cisco Technical Assistance Center（TAC）での分析に使用できます。クライアントマシンで実行するために管理者権限は不要です。

DART のインストール

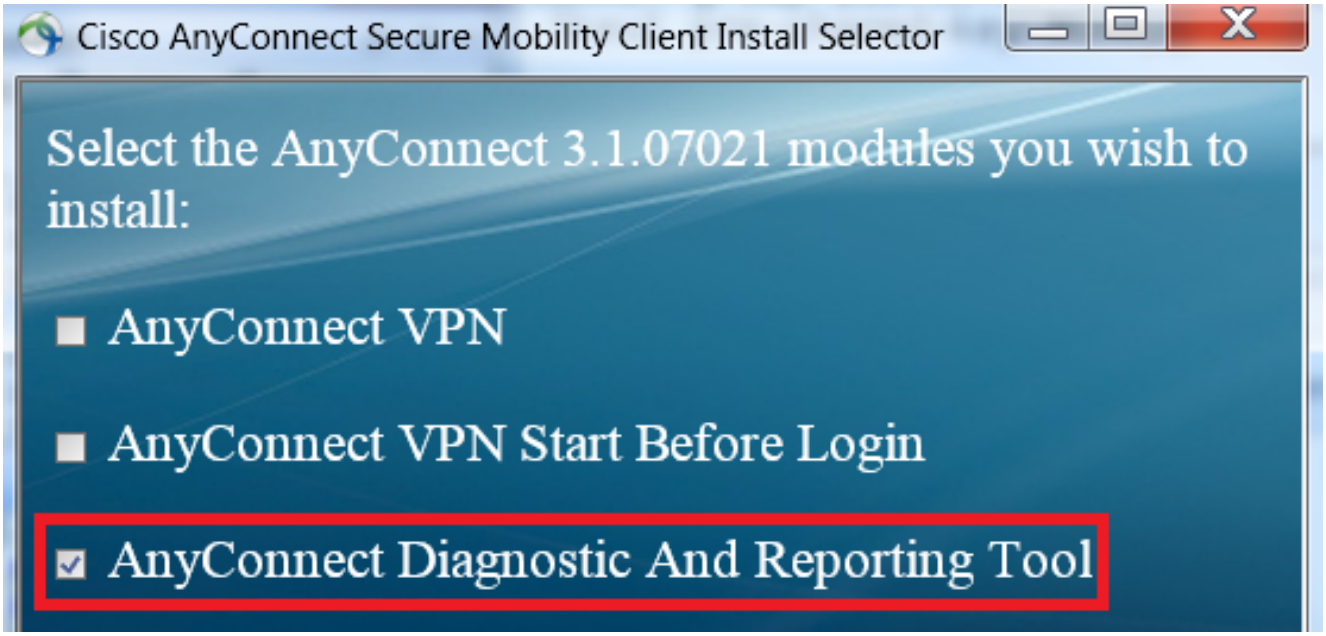
DART をインストールするには、次の手順に従います。

1. シスコの Web サイトから AnyConnect クライアントのイメージをダウンロードします。ダウンロードするイメージを正しく選択するには、Cisco AnyConnect セキュア モビリティ クライアントの Web ページを参照してください。このページにダウンロードリンクがあります。 ダウンロードページに移動し、適切なバージョンを選択します。「**Full installation package - Windows / Standalone installer (ISO)**」を検索してください。 **注**：ISO インストーライメージ（*anyconnect-win-3.1.06073-pre-deploy-k9.iso* など）がダウンロードされます。
2. *WinRar または 7-Zip を使用して ISO パッケージの内容を抽出します。*



3. 内容が抽出されたフォルダを参照します。

4. **Setup.exe** ファイルを実行し、[Anyconnect Diagnostic And Reporting Tool] のみを選択します。



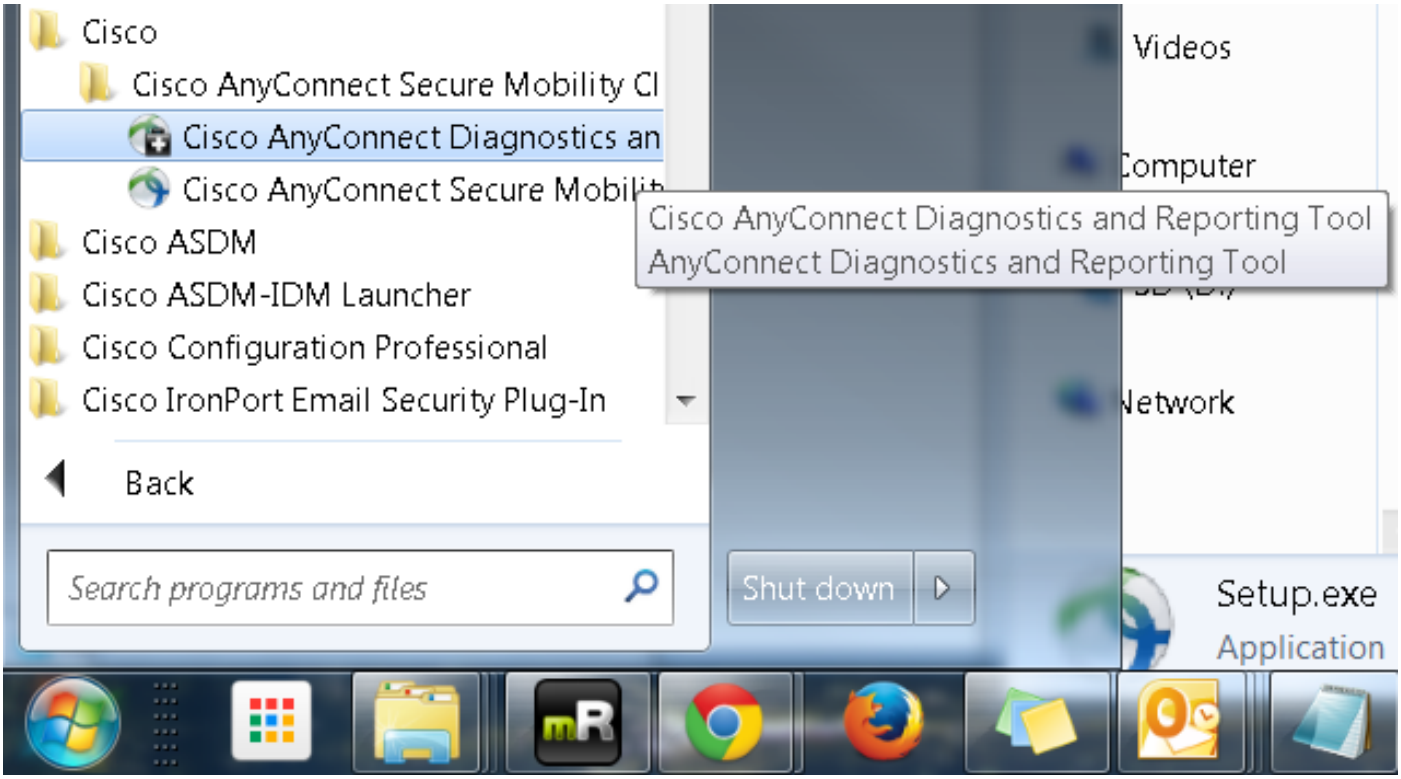
DART の実行

DART を実行する前に考慮する必要がある重要な情報は、次のとおりです。

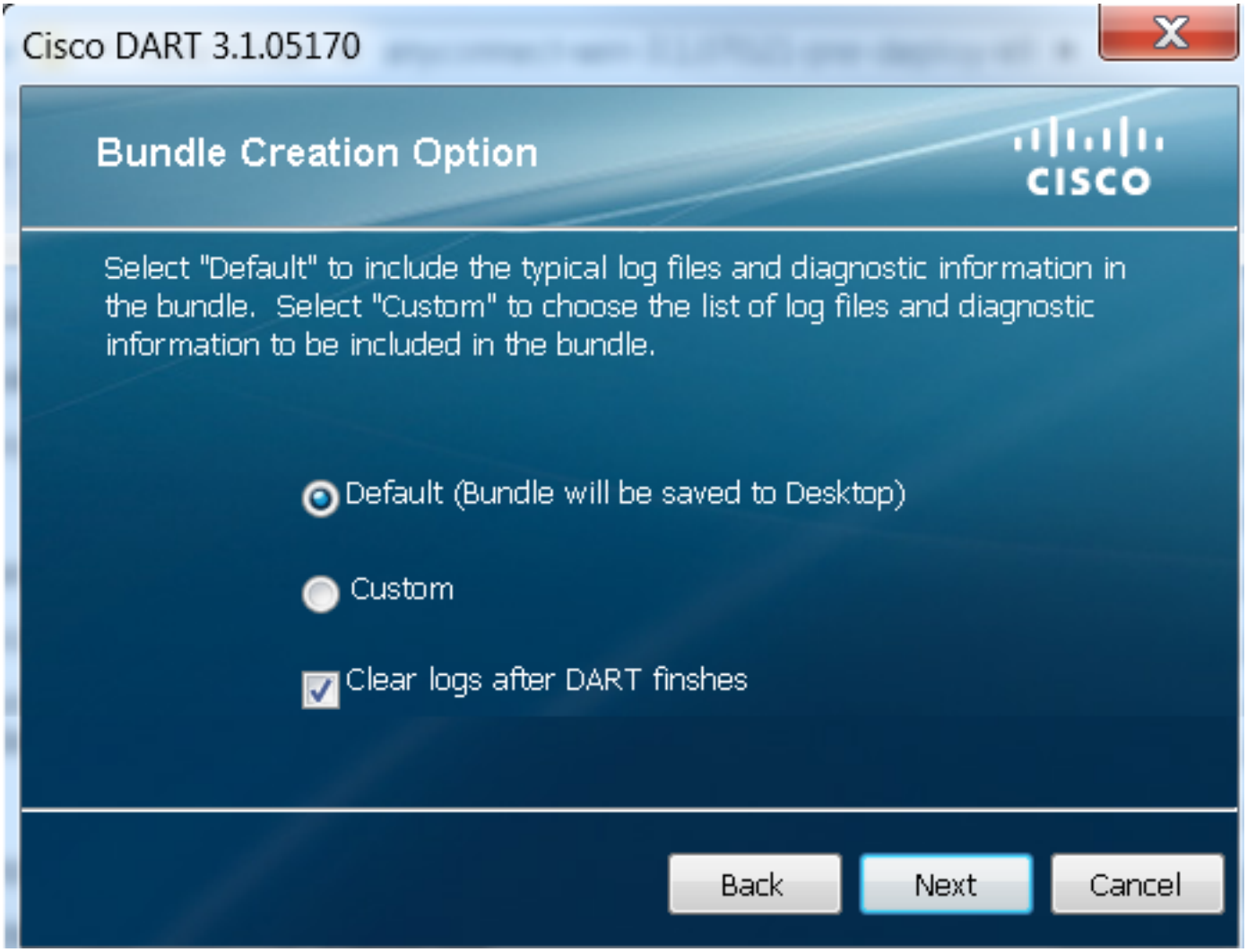
- DART を実行する前に、少なくとも 1 回は問題を再現する必要があります。

- 問題が再現されたときに、ユーザマシンの日付と時刻を記録する必要があります。

クライアントマシンの [スタート（Start）]メニューから DART を実行します。



[デフォルト（Default）] モードまたは [カスタム（Custom）] モードを選択できます。DART をデフォルトモードで実行することをお勧めします。これにより、すべての情報を 1 回のスクリーンショットでキャプチャできます。



完了すると、DART バンドルの *.zip ファイルがクライアントデスクトップに保存されます。*このバンドルを、さらなる分析のために TAC に電子メールで送信できます（TAC のケースをオープンした後）。

関連情報

- AnyConnect VPN クライアントのトラブルシューティング ガイド - 一般的な問題
- AnyConnect、CSD/Hostscan、および WebVPN による Java 7 の問題 - トラブルシューティング ガイド
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。