ASA Remote Access VPN 設定ガイド for Smart Phones

Date : 22 Sep 2011

tetsato@cisco.com

はじめに

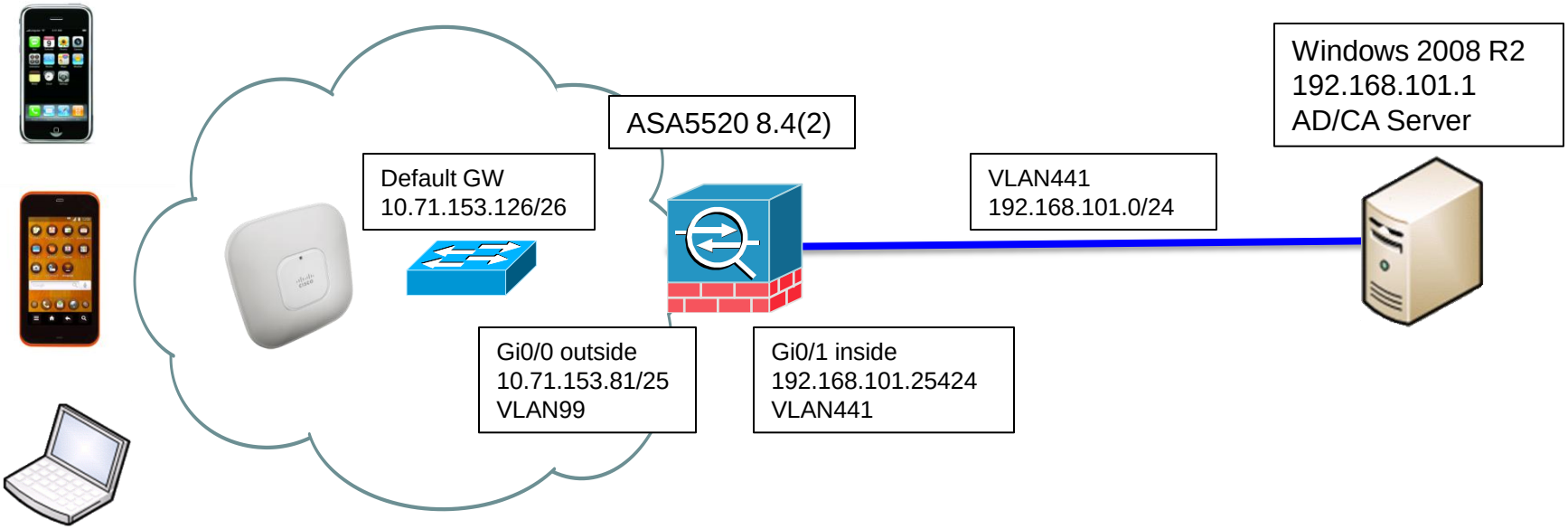
- 本ドキュメントに関する著作権は、シスコシステムズ合同会社へ独占的に帰属します。 シスコシステムズ合同会社が事前に承知している場合を除き、形態および手段を問わず本ドキュメントまたはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本ドキュメントの記述に誤りや欠落があってもシスコシステムズ合同会社はいかなる責任も負わないものとします。本ドキュメントおよびその記述内容は予告なしに変更されることがあります。

1. 基本設定 (共通)
   a) ASDM 設定 — 共通
   b) 認証設定
      I. ローカルユーザ — AnyConnect, L2TP
      II. 外部ユーザ認証 (Windows AD) — 共通
   c) 証明書 — 共通
   d) アドレスプールの設定 — 共通
2. VPN 設定
   a) AnyConnect 設定 — AnyConnect
   b) L2TP/IPSec の設定 — L2TP
3. クライアント設定
   a) AnyConnect 設定
   b) L2TP/IPSec 設定
4. 補足説明

設定フローチャート例

	AnyConnect 証明書認証	AnyConnect ADユーザ認証	L2TP/IPSec PSK Local 認証	L2TP/IPSec CRT AD認証
1. 基本設定 (共通)				
a) ASDM 設定	○	○	○	○
b) 認証設定				
I. ローカルユーザ			○	
II. 外部ユーザ認証 (Windows AD)		○		○
c) 証明書	○	○		○
d) アドレスプールの設定	○	○	○	○
2. VPN 設定				
a) AnyConnect 設定	○	○		
b) L2TP/IPsec の設定			○	○

ネットワーク構成



1. 基本設定
a) ASDM

共通

基本設定

- 基本的な設定を CLI より入力 (今回の構成での設定例)

```
!
hostname asa
domain-name bndemo.local
enable password cisco
username admin password cisco123 priv 15
!
interface gi0/0
 nameif outside
 ip address  10.71.153.80 255.255.255.128
 no shut
!
Interface gi0/1
 nameif inside
 ip address  192.168.101.254 255.255.255.0
 no shut
!
asdm image disk0:/asdm-645.bin
http server enable
http 0.0.0.0 0.0.0.0 outside
!
route outside 0.0.0.0 0.0.0.0 10.71.153.126
!
```

基本設定

共通

コンソールセットアップ例

```
Booting Up.....
                (略)
[Pre-configure Firewall now through interactive prompts [yes]? No
ciscoasa> enable
ciscoasa# conf t
ciscoasa(config)# hostname asa
asa(config)# domain-name bndemo.local
asa(config)#
asa(config)# enable password cisco
asa(config)# username admin password cisco123 priv 15


asa(config)# int gi0/1
asa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
asa(config-if)# ip address 192.168.101.254 255.255.255.0
asa(config-if)# no shut

asa(config)# int gi0/0
asa(config-if)#  nameif outside
INFO: Security level for "outside" set to 0 by default.
asa(config-if)#  ip address  10.71.153.80 255.255.255.128
asa(config-if)#  no shut
asa(config-if)#

asa(config)# route outside 0.0.0.0 0.0.0.0 10.71.153.126

asa(config-if)# asdm image disk0:/asdm-645.bin
asa(config)# http server enable
asa(config)# http 0.0.0.0 0.0.0.0 inside

asa(config)# write mem
```

セットアップウィザードを行わない

ホスト名

ドメイン名

enable password

ASDM 管理ユーザーの作成

インターフェース g0/1 にinside を割当て

192.168.101.254/24

インターフェース有効化

インターフェース g0/0 にoutside を割当て

10.71.153.80/26

インターフェース有効化

default GW の設定

利用する asdm イメージを指定

http サービス有効化

http/asdm ASDMアクセス許可

共通

基本設定 – ASDM の起動

- ASDM を起動。

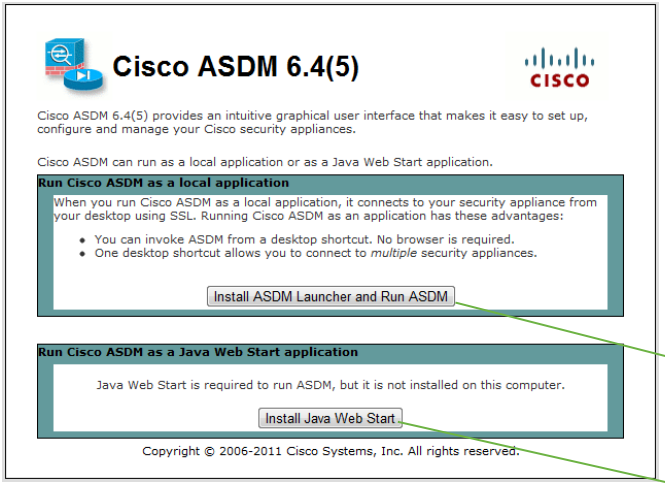
  ブラウザーより、https://<server address> https://192.168.101.254 にアクセス

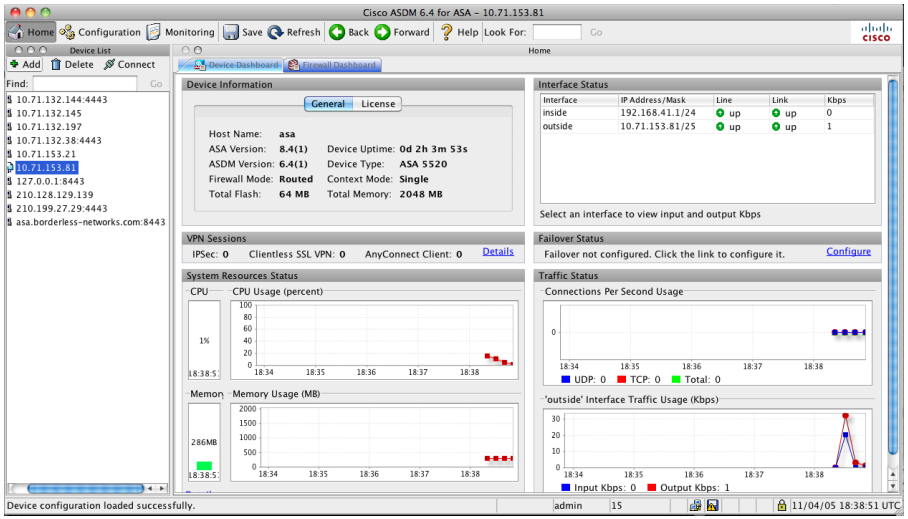
  Run ASDM をクリックし ASDM を起動

  Ex.

  ユーザ名: admin

  パスワード: cisco123





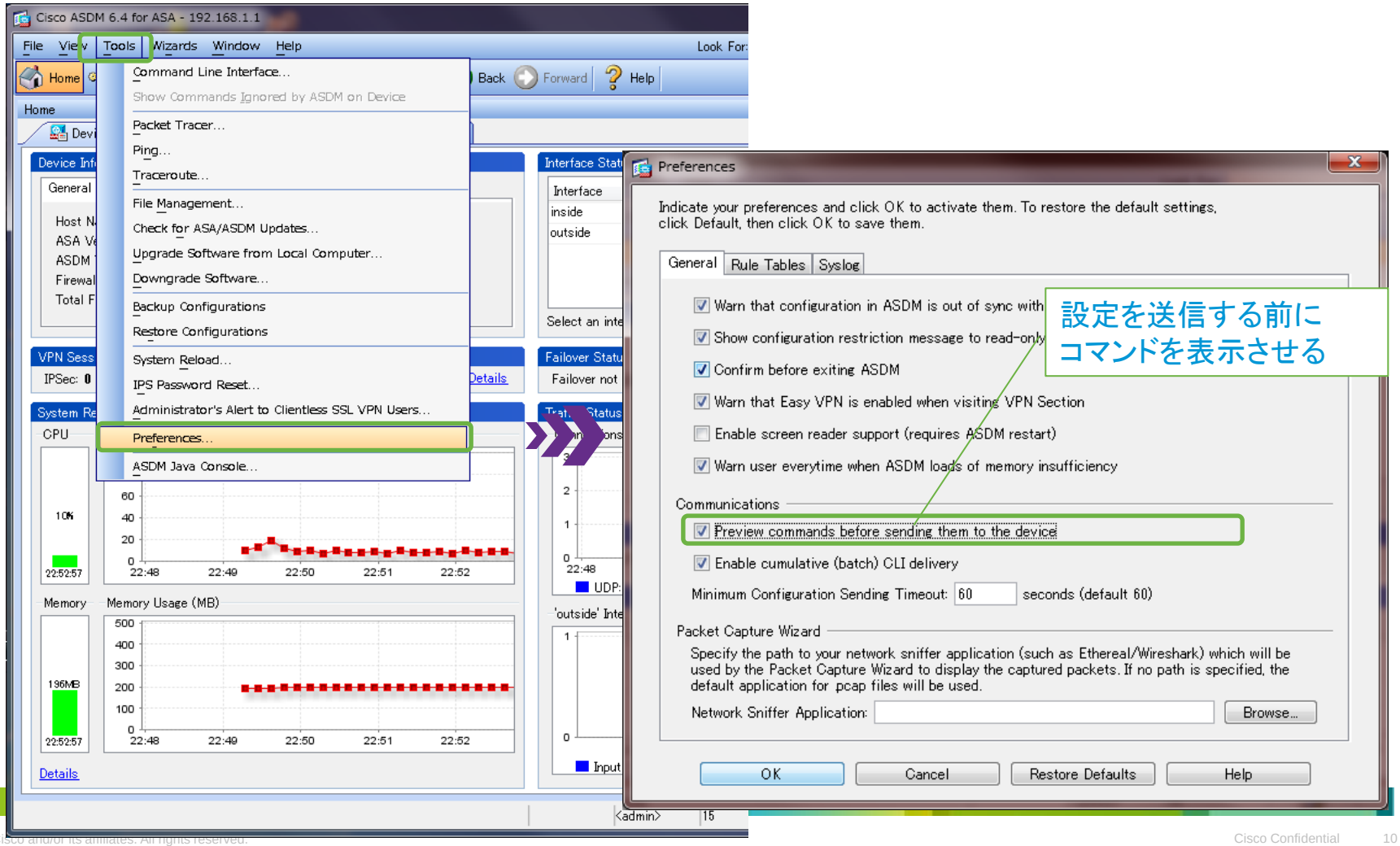
ローカルにラウンチャをインストールして実行する場合

ラウンチャをインストールせず実行する場合

基本設定
- ASDM設定内容を事前表示

共通

- ASDM で設定変更を行う際、ASA への適用時にCLI での設定内容を表示させることが可能

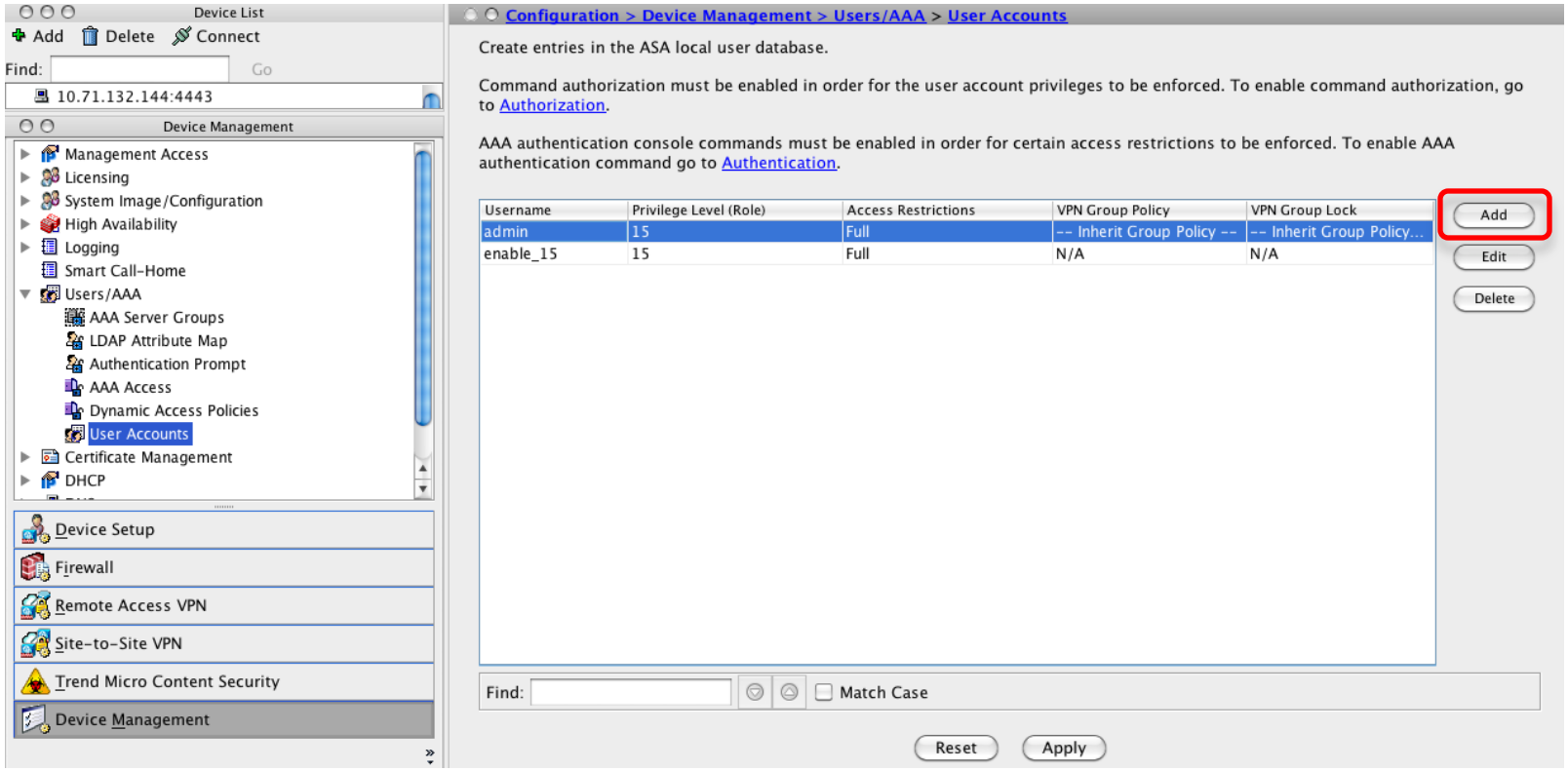


1. 基本設定
b) 認証設定

基本設定：ローカルユーザ作成

- ローカルログインユーザの作成

  Configuration -> Device Management-> Users/AAA -> Users Accounts と移動し [Add] ボタンをクリック

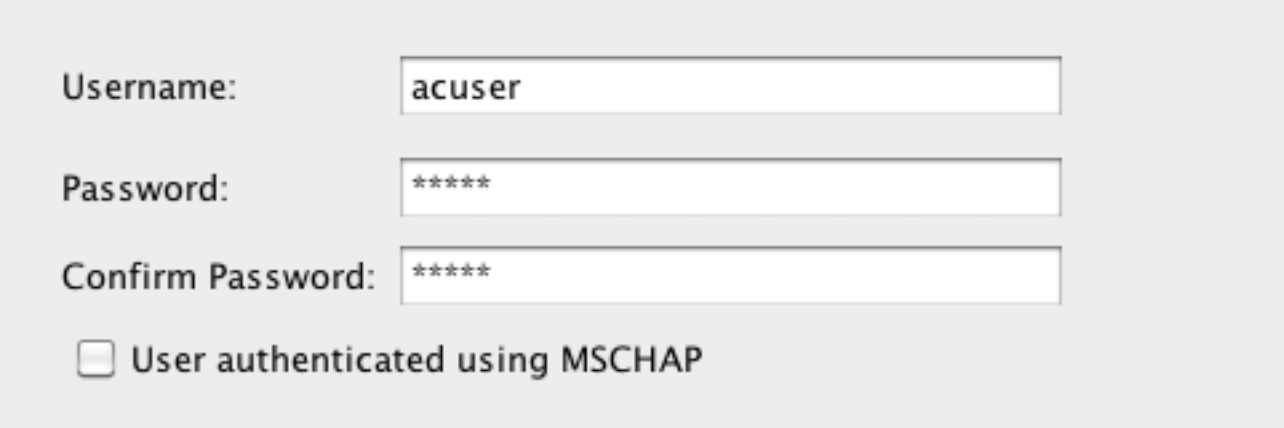


基本設定：ローカルユーザ作成 AnyConnect

- ローカルログインユーザの作成 (続き)

  [Username] に接続する際のユーザ名、[Password] にそのパスワードを入力

  Ex. Username: acuser Password: cisco



[Apply] をクリックし、設定を反映

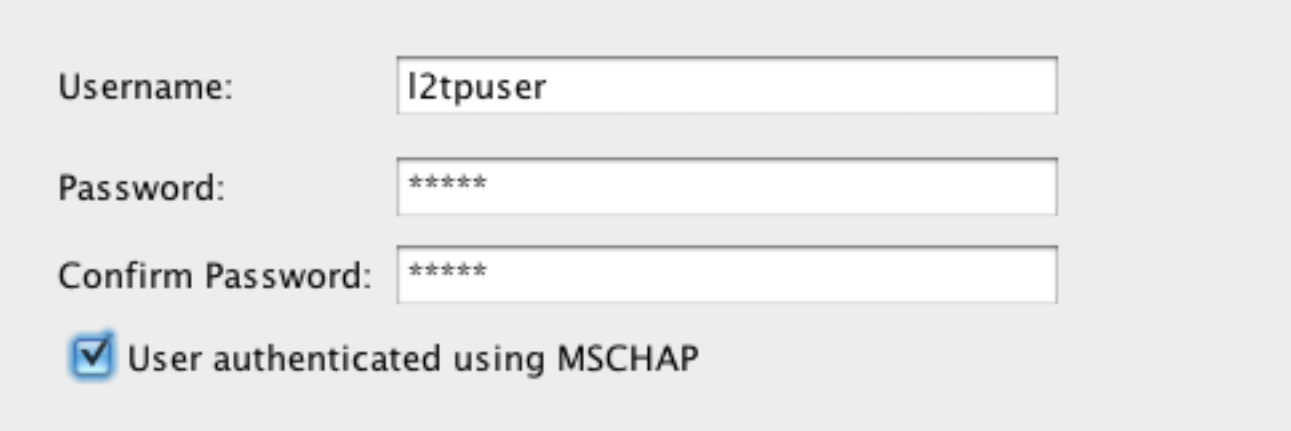
基本設定: ローカルユーザ作成 L2TP

- ローカルログインユーザの作成 (続き)

  [Username] に接続する際のユーザ名、[Password] にそのパスワードを入力

  Ex. Username: l2tpuser Password: cisco

  [User authenticated using MSCHAP] にチェックを入れ、(他は default のまま) 下の方にある [OK] ボタンをクリック



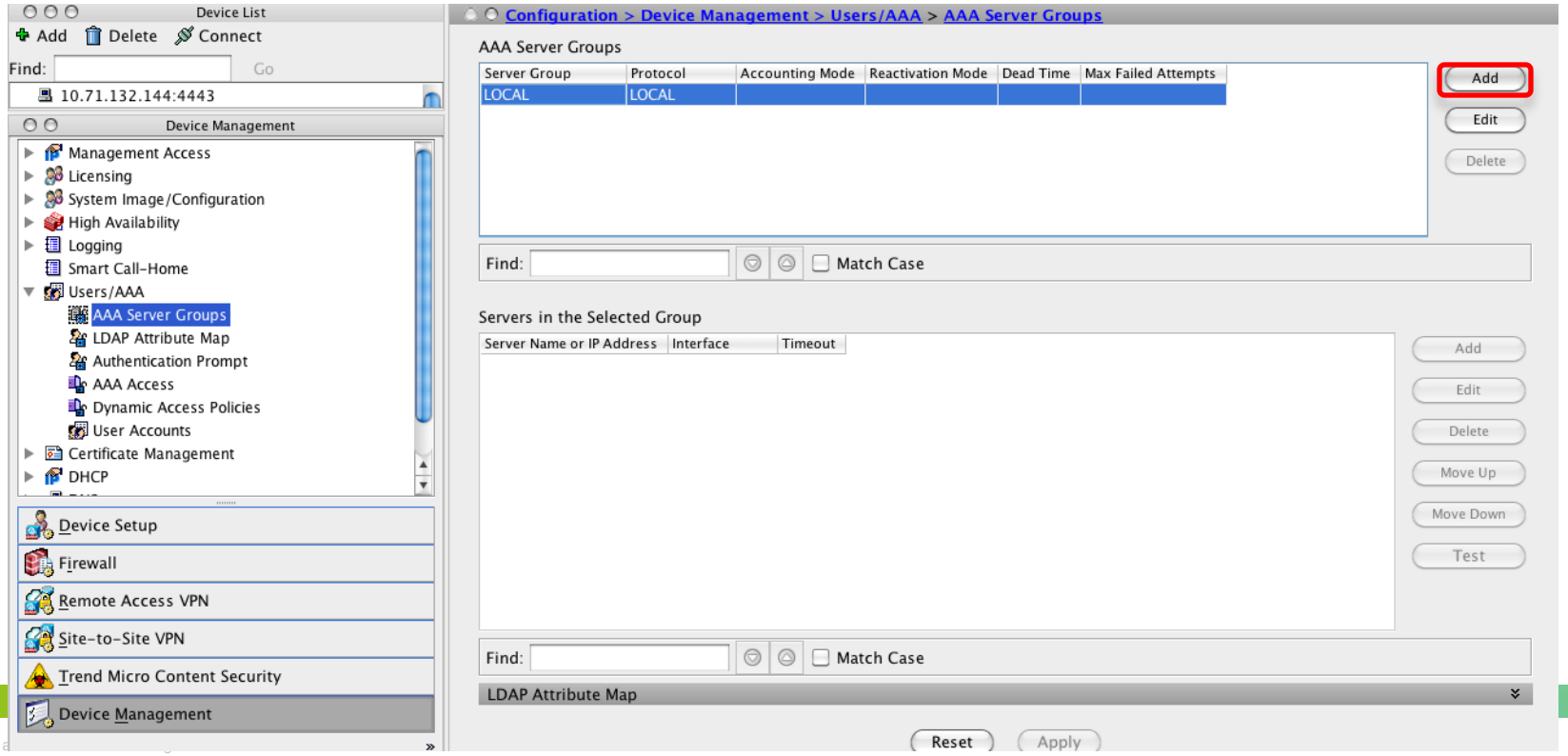
  [Apply] をクリックし、設定を反映

基本設定: Windows AD の設定

- リモートログインユーザの使用の為の設定

  外部認証データベースとして、Windows AD のユーザ情報を元に、ASA VPN の認証を行う為の設定を行います。

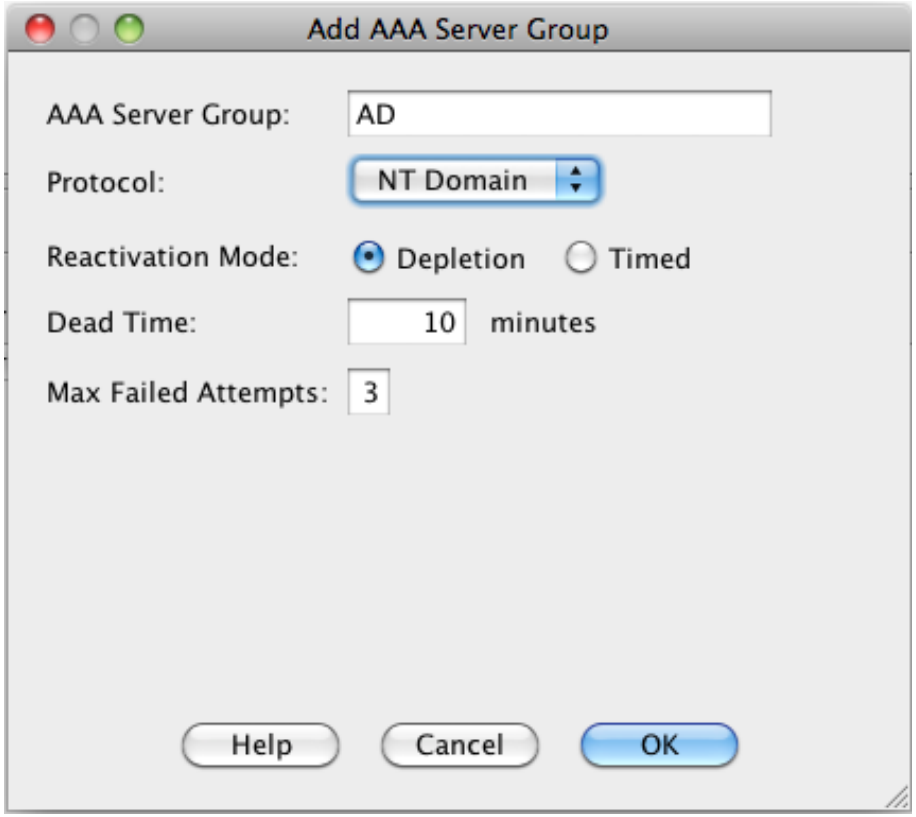
  Configuration -> Device Management-> Users/AAA -> AAA Server Groups を選択し、 [Add] ボタンをクリック。



基本設定: Windows AD の設定

- リモートログインユーザの使用の為の設定 (続き)

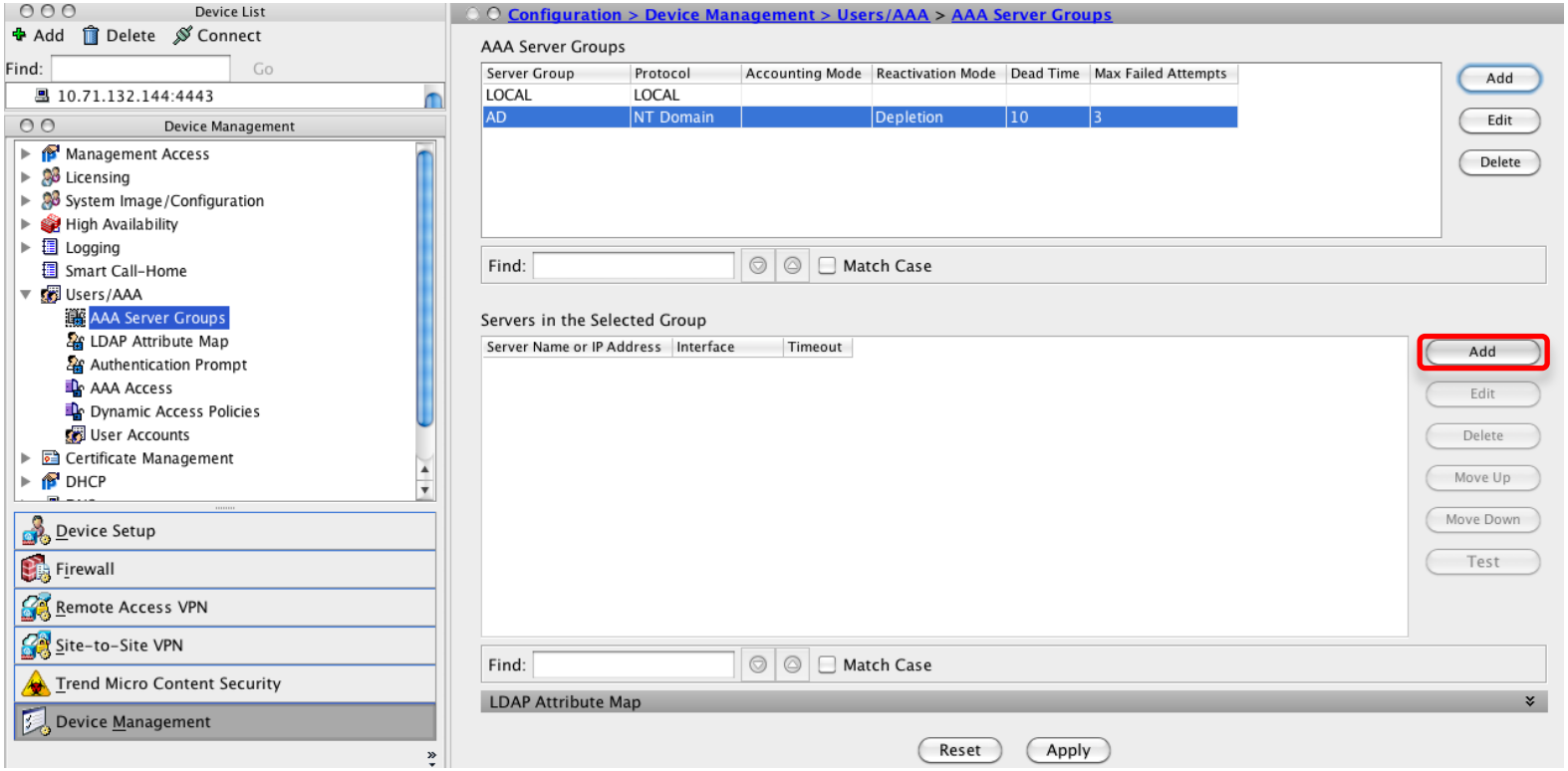
  AAA Server Group: に名前 (Ex. AD), Protocol: に NT Domain を選択し。[OK] をクリック。



基本設定: Windows AD の設定

- リモートログインユーザの使用の為の設定 (続き)

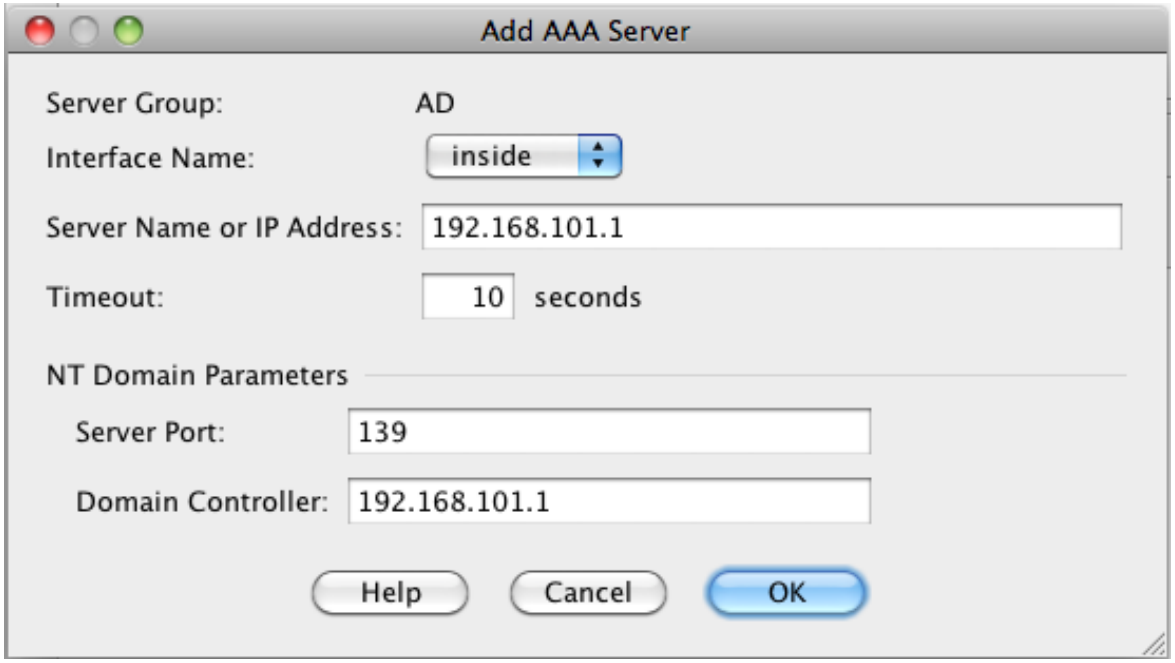
  Servers in the Selected Group AAA の [Add] をクリック。



基本設定: Windows AD の設定

- リモートログインユーザの使用の為の設定 (続き)

  Interface Name: inside を選択、Server Name or IP Address: AD Server のアドレス (Ex. 192.168.101.1), Domain Controller にも AD Server のアドレス (Ex. 192.168.101.1) を入力し、[OK] をクリック。



  [Apply] をクリックし、設定を反映

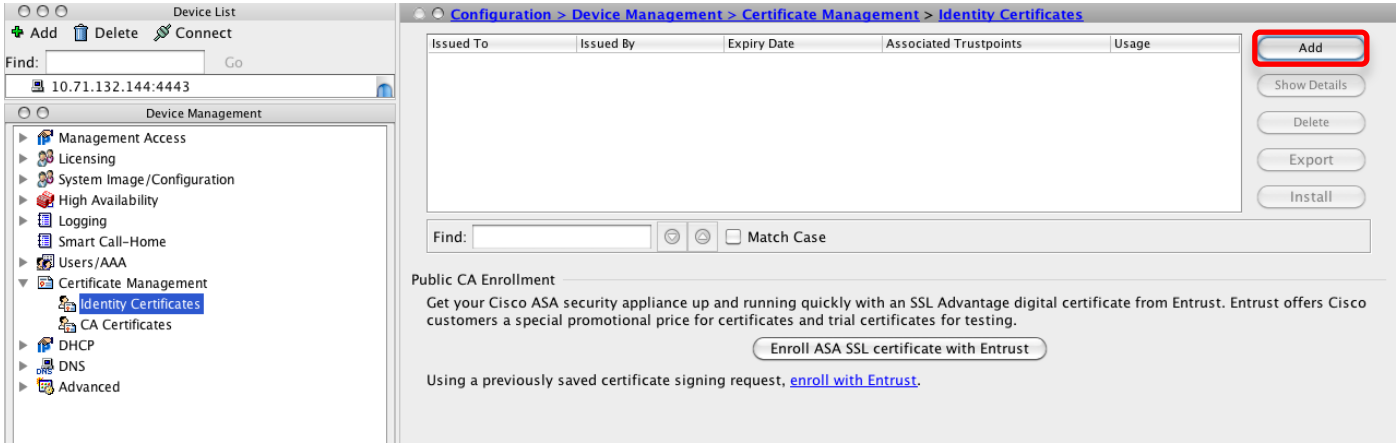
1. 基本設定
c) 証明書設定

基本設定: 証明書の設定 – CSR 作成

- 証明書の設定 – CSR 作成

  AnyConnect 証明書認証、L2TP/IPsec CRT で使用する証明書の設定を行います。

  Configuration -> Device Management-> Certificate Management -> Identity Certificates を選択し、 [Add] ボタンをクリック。



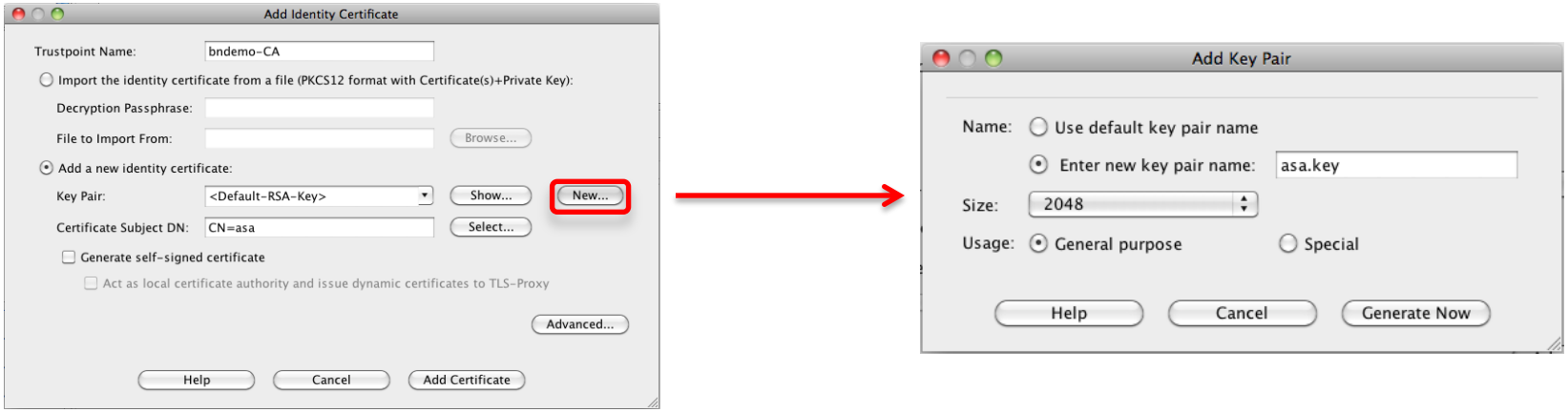
基本設定: 証明書の設定 – CSR 作成

- 証明書の設定 – CSR 作成 (続き)

  Trustpoint Name: に名前を入力 (Ex. bndemo-CA)、Add a new identity certificate: を選択します。

  [New] をクリックし、新規キーを作成します。

  Name: Enter new key pair name: を選択し、名前を入力し (Ex. asa.key)、Size: 1024 or 2048 を選択、 Usage: Generate purpose を選択し、[Generate Now] をクリック。)、

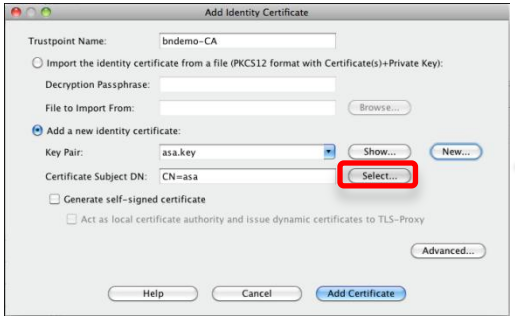


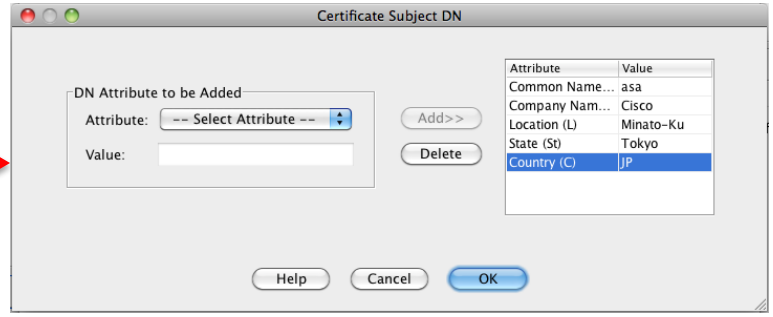
基本設定: 証明書の設定 – CSR 作成

- 証明書の設定 – CSR 作成 (続き)

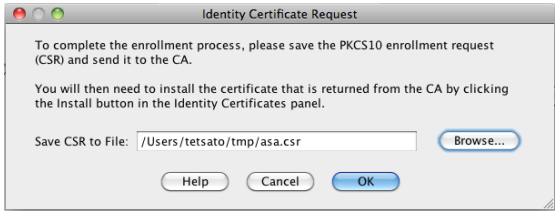
  Certificate Subject DN: [Select] をクリックし、証明書 Subject を指定します。

  Attribute: より、Attribute を選択後、Value: を入力し [Add] をクリックし、Subject を指定し、 (Ex. CN: asa, O: Cisco, L: Minato-Ku, ST: Tokyo, C: JP) [OK] をクリックします。





  [Add Certificate] をクリックし、CSR の名前を指定し (Ex. /Users/tetsato/tmp/asa.csr)、[OK] をクリックし保存します。



  作成した CSR を認証局に申請し、証明書を入手して下さい。

基本設定: 証明書の設定 – CA局に申請

- 認証局 Windows CA の場合

  ブラウザーより http://<server address>/certsrv にアクセス

  証明書を要求する > 証明書の要求の詳細設定 > 先ほど作成した CSR ファイルをテキストエディターなどで開き内容を、Base 64 エンコード 証明書要求 (CMC または PKCS #10 または PKCS #7): 内に Paste、証明書テンプレート: Web サーバーを選択し、[送信]をクリック。

  Base 64 エンコードを選択し、証明書のダウンロードをクリック。

  ダウンロードされるファイルを asa.cer として保存。

  右上にある [ホーム] > [CA 証明書、証明書チェーン、または CRL のダウンロード] と選択し、エンコード方式: Base64 を選択し、 [CA 証明書のダウンロード]をクリックし、CA 証明書を ca.cer として保存

基本設定: 証明書の設定– CA局に申請

- 認証局 CyberTrust の場合

ユーザ認証で利用する場合には、Cybertrust Shared PKI認証局に申請を行います。
機器認証用で利用する場合には、Cybertrust DeviceiD認証局に申請を行います。

ご利用の証明書発行サービスによって以下のリンクから証明書を取得してください。

Cybertrust Shared PKI認証局

https://www.cybertrust.ne.jp/shared_pki/CybertrustSharedPKIPublicCA1.crt

Cybertrust DeviceiD 認証局

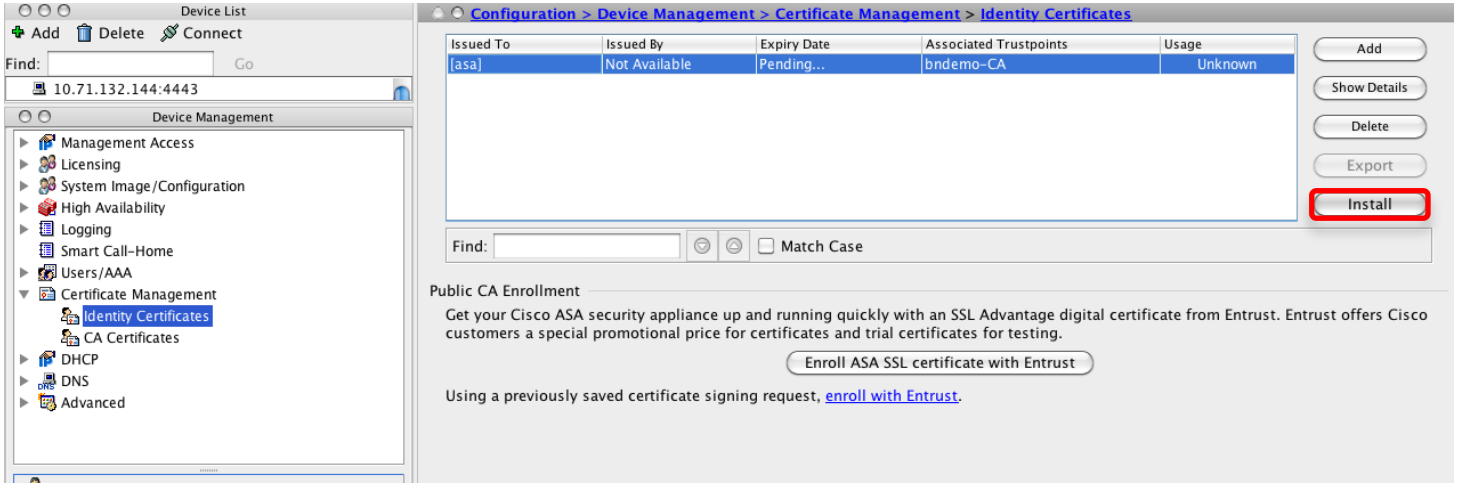
http://www.cybertrust.ne.jp/deviceid/CybertrustDeviceiDPublicCAG1.crt

詳しくは、oper@cyberturst.ne.jp までご連絡ください。

基本設定: 証明書の設定 – 証明書のインストール

- 入手した、ASAの証明書、CA 証明書をインストール

  Configuration -> Device Management-> Certificate Management -> Identity Certificates を選択し、 [Install] ボタンをクリック。

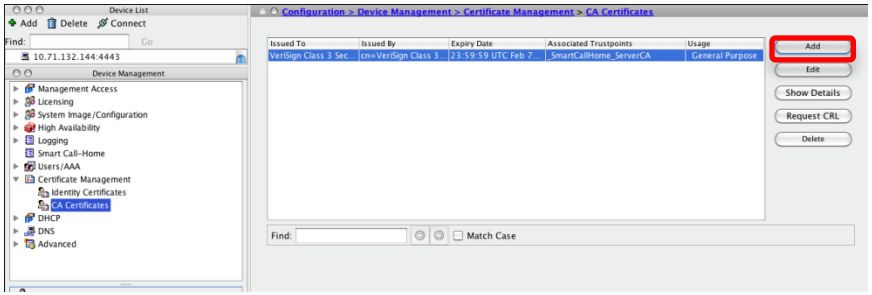


[Install from a file] で、ASA の証明を指定し、[Install Certificate] をクリック。

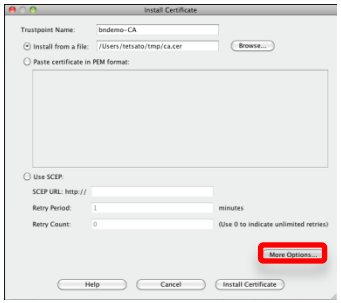
基本設定: 証明書の設定 – 証明書のインストール

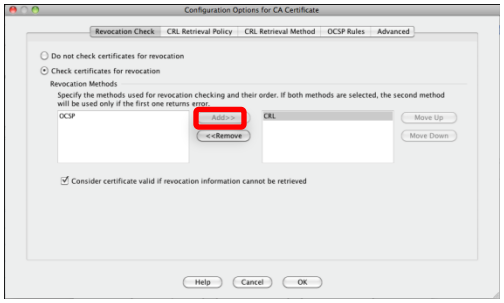
- 入手した、ASAの証明書、CA 証明書をインストール (続き)

Configuration -> Device Management-> Certificate Management -> CA Certificates を選択し、 [Add] ボタンをクリック。



TrustPoint Name: に名前を入力し (Ex. bndemo-CA)、[Install from a file:] に入手した CA 証明書ファイルを指定し、[More Options] をクリックします。





[Revocation Check] より、[Check Certificate for revocation] を選択、[Revocation Methods] にて CRL を選択し [Add] をクリック。[OK]をクリック。

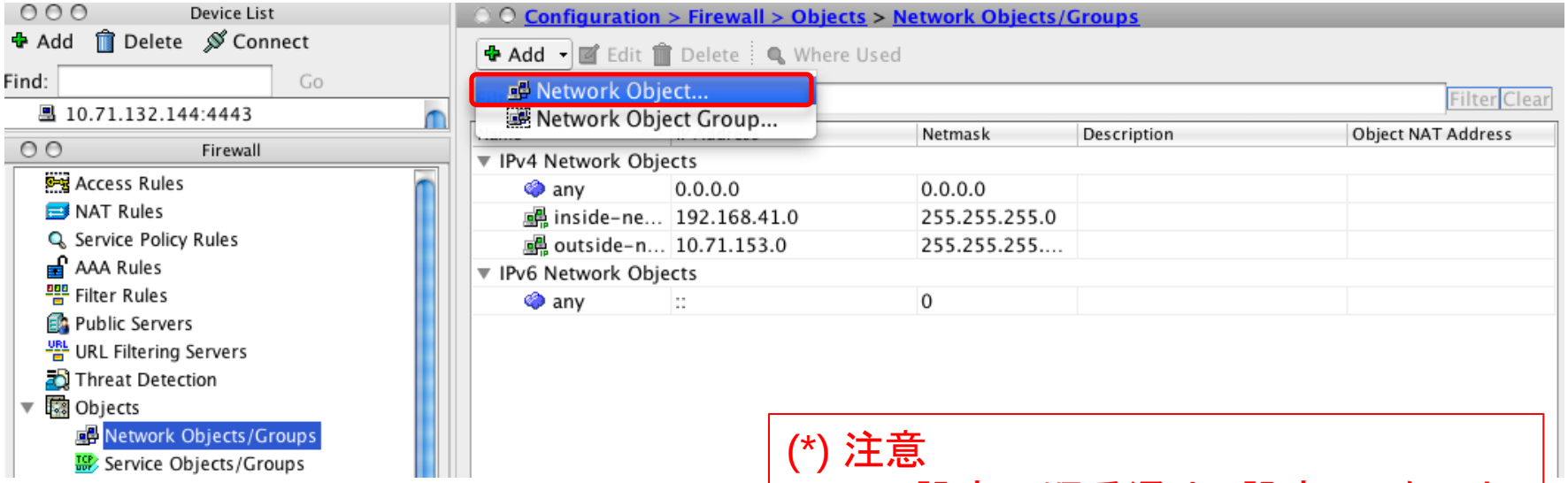
[Install Certificate] をクリック

1. 基本設定
d) アドレスプール、その他

基本設定: アドレスプール - Object

- Network Object の設定

  Configuration -> Firewall -> Objects -> Network Objects/Groups へ移動し [Add] [Network Object] をクリック



(*) 注意
以下の設定の順番通りに設定でしないとエラーが出ます。(CSCtn96841)
- Network Object の設定
- アドレスプールの設定
- NAT の設定

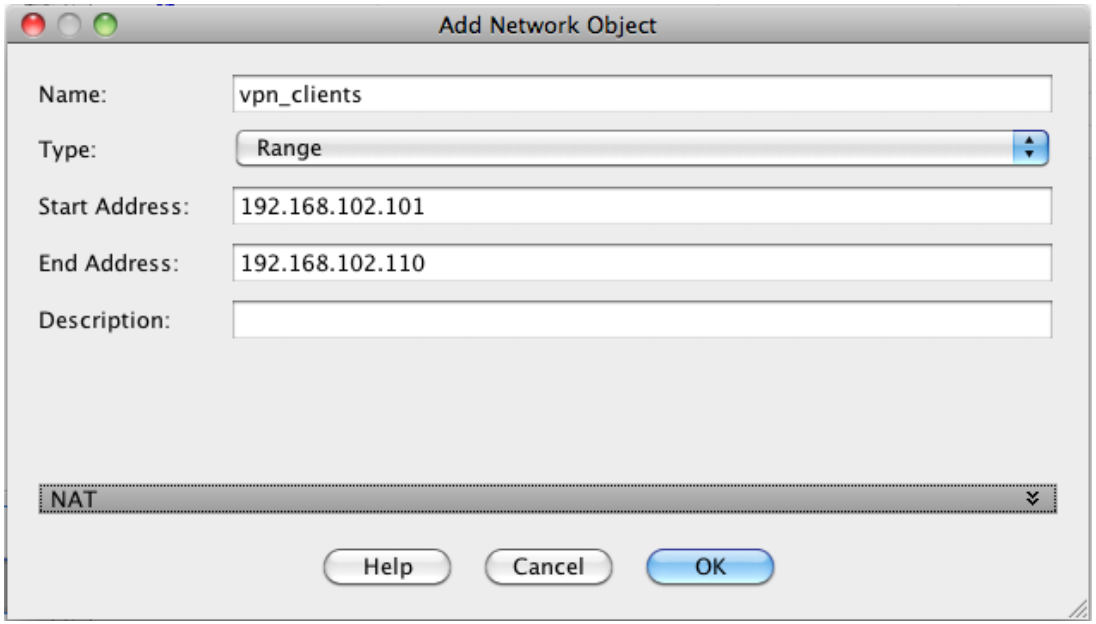
基本設定: アドレスプール - Object

- Network Object の設定 (続き)

  Name: に名前 (Ex. vpn_clients), Type に Range を選択。 Start Address, End Address を入力。(アドレスプールを作成する際に使用するものと同じものを指定)

  [OK] をクリック。

  Ex. Start Address: 192.168.102.101, End Address: 192.168.102.110

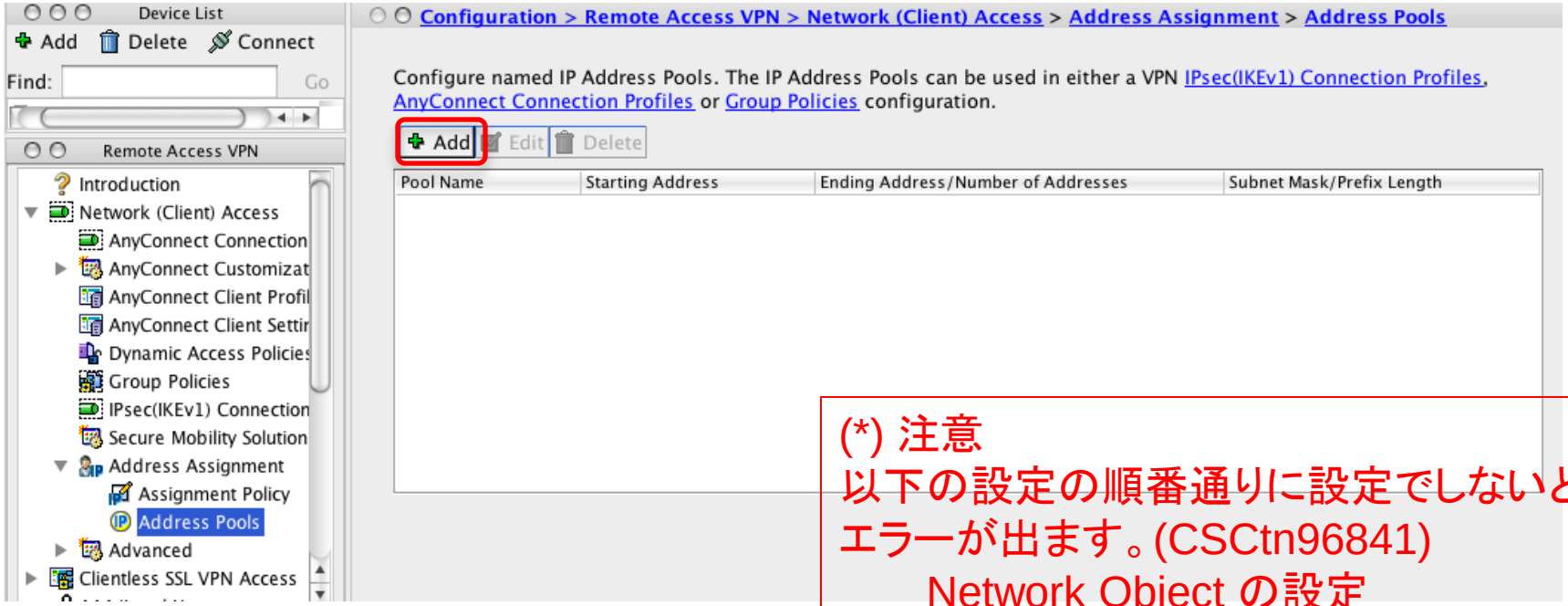


基本設定: アドレスプール – アドレスプール指定

- アドレスプールの作成

  Configuration -> Remote Access VPN -> Network (Client) Access

  -> Address Assignment -> Address Pools と移動し [Add] をクリック



(*) 注意
以下の設定の順番通りに設定でしないとエラーが出ます。(CSCtn96841)

- Network Object の設定
- アドレスプールの設定
- NAT の設定

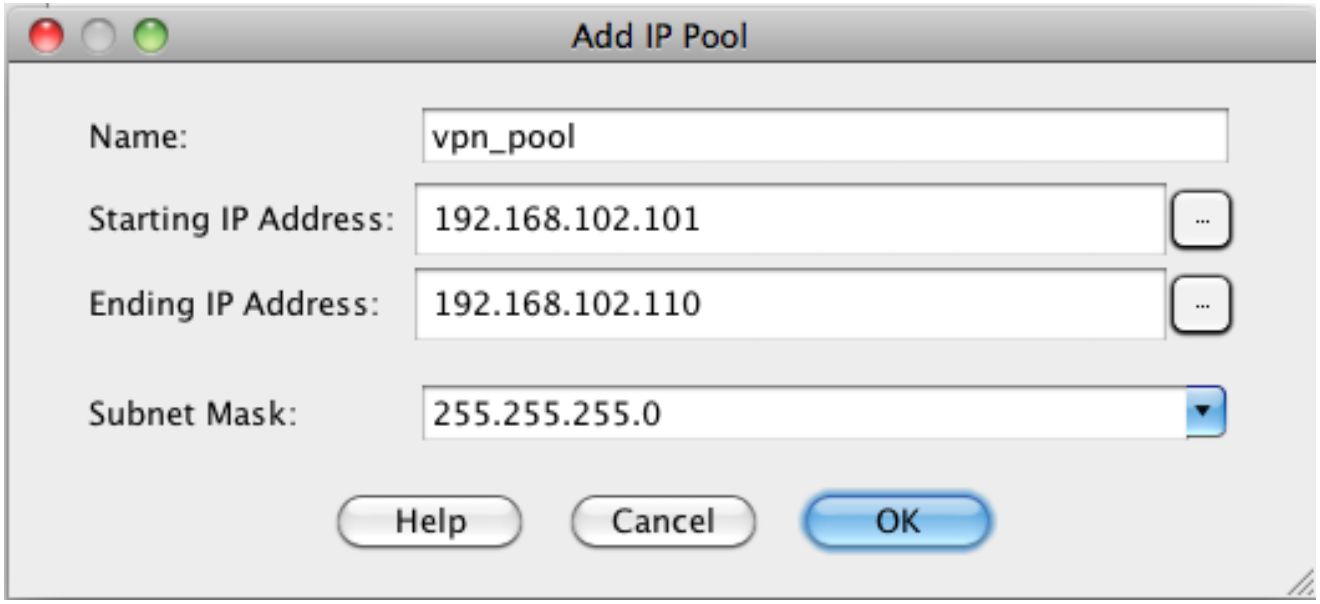
共通

基本設定: アドレスプール – アドレスプール指定

- アドレスプールの作成 (続き)

  アドレスプールの名前、開始アドレス、終了アドレス、サブネットマスクを入力し [OK] をクリック

  Ex. Name: vpn_pool, Starting IP Address: 192.168.102.101, Ending IP Address: 192.168.102.110, Subnet Mask: 255.255.255.0



  [Apply] をクリックし、設定を反映

基本設定: アドレスプール - NAT

- NAT の設定

  Configuration -> Firewall -> NAT Rules へ移動し [Add] をクリック

(*) 注意
以下の設定の順番通りに設定でしないとエラーが出ます。(CSCtn96841)
- Network Object の設定
- アドレスプールの設定
- NAT の設定

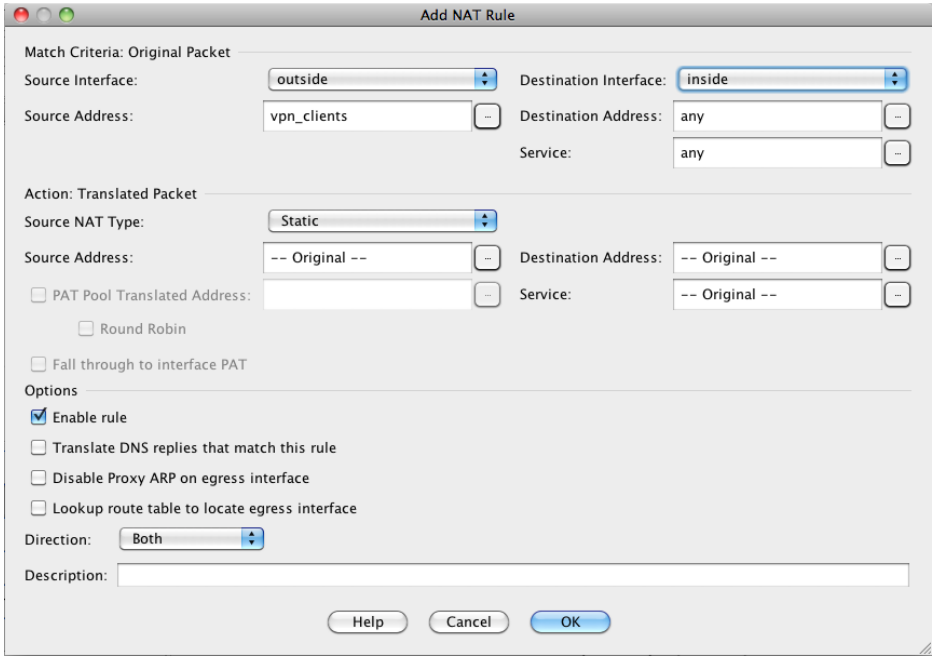
VPNクライアント以外の NAT 設定は、別途適宜行って下さい。

基本設定: アドレスプール - NAT

- NAT の設定 (続き)

  Source Interface: に outside、Source Address に先ほど作成した Network Object (Ex. vpn_clients) を選択。Destination interface: に inside を選択。

  他の設定は Default のまま[OK] をクリック

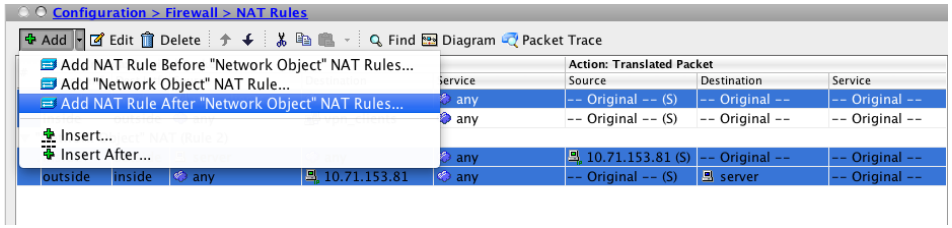


  [Apply] をクリックし、設定を反映

基本設定: NAT (Option)

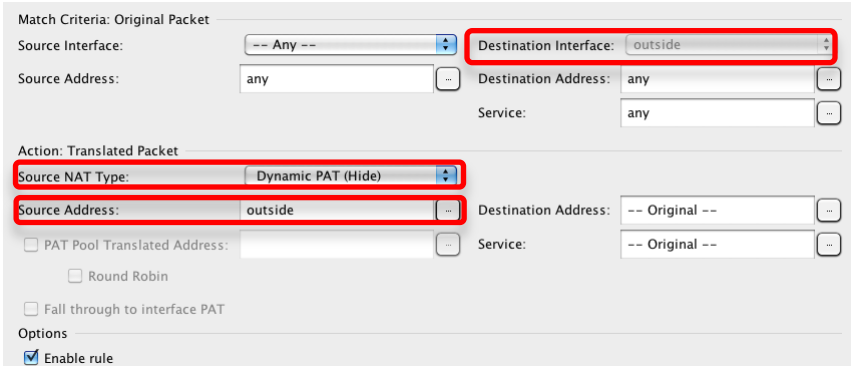
- 内部からの通信を NAT する為の設定 (Option)

  Configuration > Firewall > NAT Rules と移動し、[Add] より、Add NAT Rule After “Network Object NAT Rules をクリック。



  Match Criteria: Original Packet, Destination Interface: outside を選択。

  Action: Translated Packet, Source NAT Type: Dynamic PAT (Hide) を選択、Source Address: outside を選択し、[OK] をクリック。

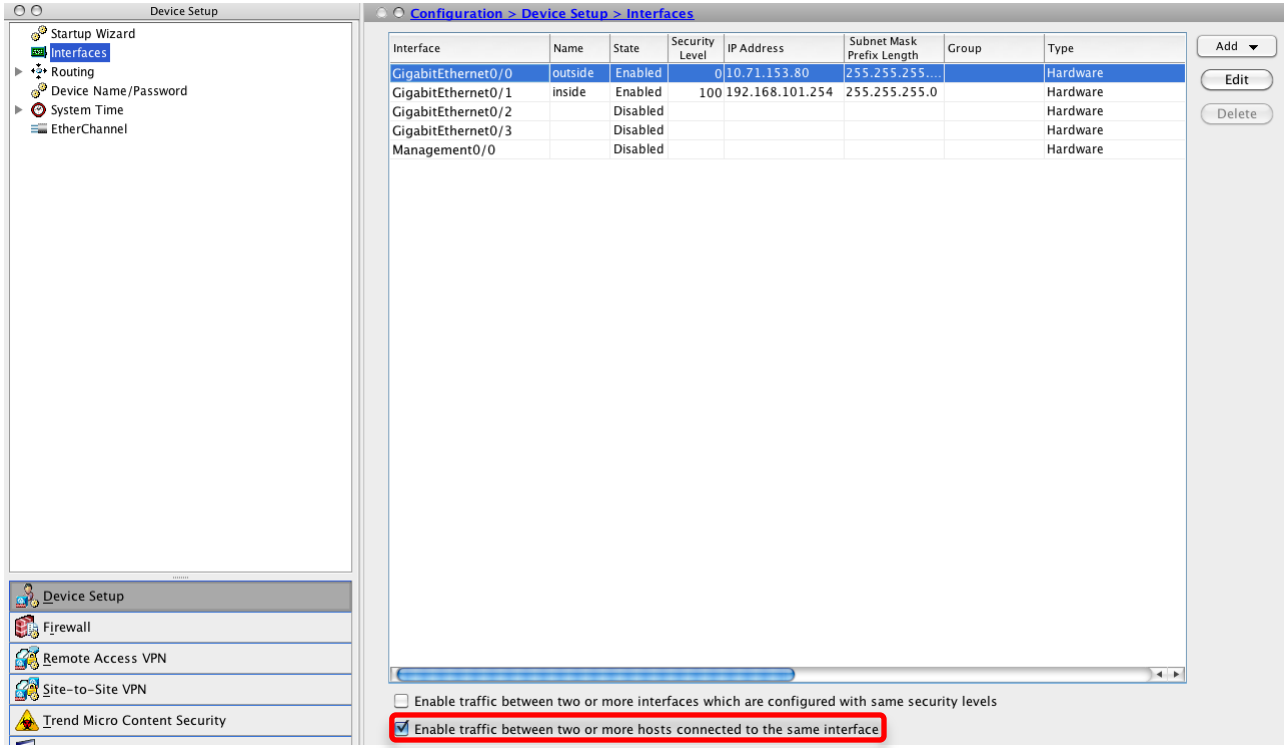


  [Apply] をクリックし、設定を反映

基本設定: VPN Traffic を外部に許可 (Option)

- VPN Traffic を外部へアクセスを許可する為の設定

  Configuration > Device Setup > Interfaces へ移動し、Enable traffic between two or more hosts connected on the same interface にチェックを入れる。

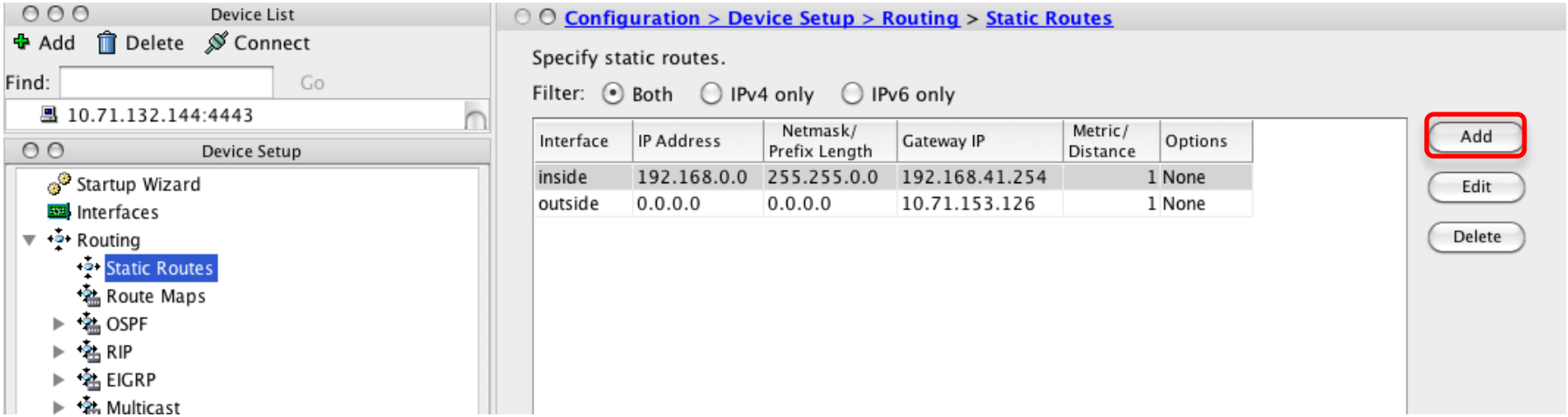


[Apply] をクリックし、設定を反映

基本設定: トンネルルート (Option)

- トンネルルートの追加

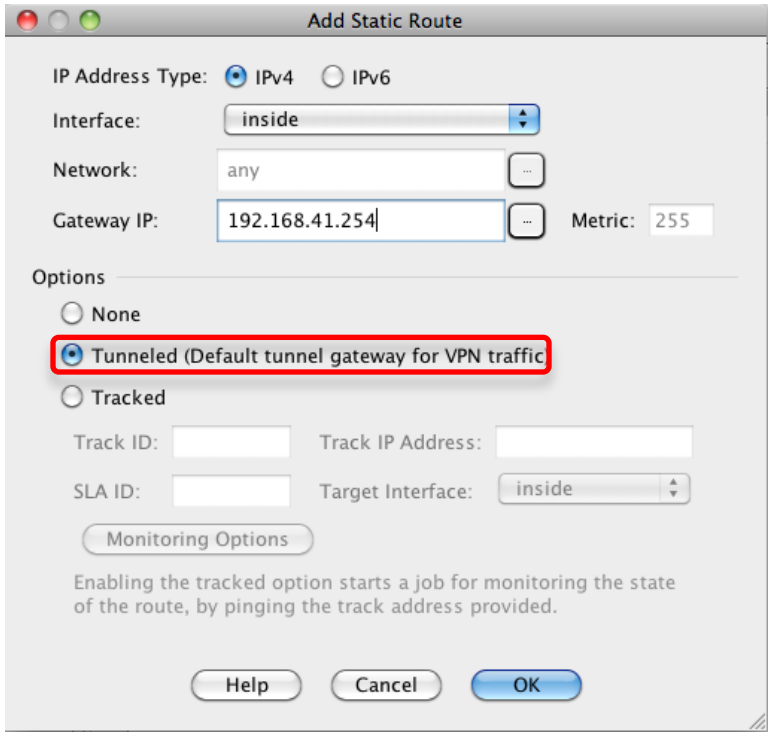
  Configuration -> Device Setup -> Routing -> Static Routes へ移動し [Add] をクリック。



基本設定: トンネルルート (Option)

- トンネルゲートウェイの追加 (続き)

  Option: Tunneled (Default tunnel gateway for VPN traffic) にチェックを入れ、Gateway IP: に Gateway のアドレス (Ex. 192.168.41.254) を入力し [OK] をクリック



  [Apply] をクリックし、設定を反映

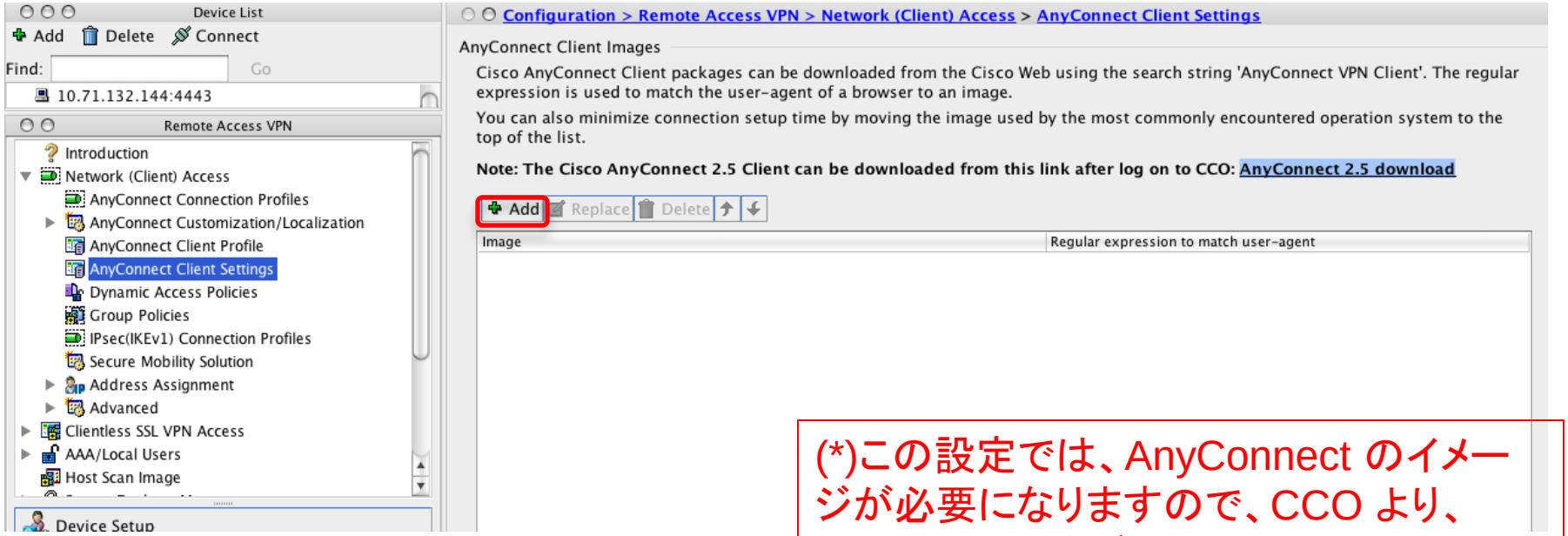
2. VPN 設定

a) AnyConnect

VPN 設定: AnyConnect

- AnyConnect の設定 – Image

  Configuration -> Remote Access VPN -> Network (Client) Access -> AnyConnect Client Settings へ移動し [Add] をクリック

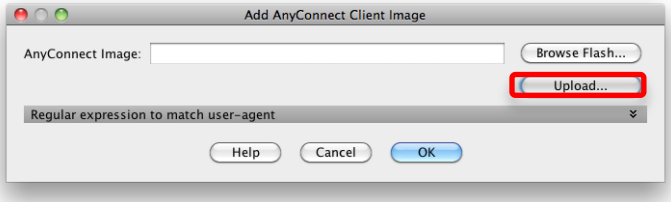


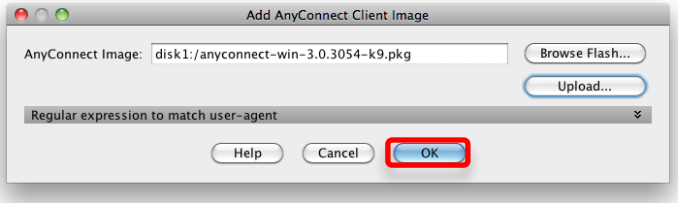
(*)この設定では、AnyConnect のイメージが必要になりますので、CCO より、AnyConnect をダウンロードしておいて下さい。
(Ex. anyconnect-win-3.0.3054-k9.pkg)

VPN 設定: AnyConnect

- AnyConnect の設定 – Image (続き)

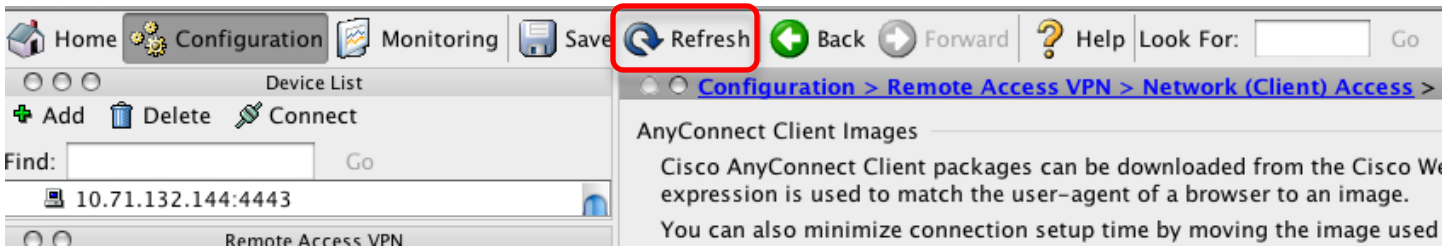
  [Upload] をクリックし、AnyConnect イメージを指定し [Upload File] をクリックします。アップロード完了後、[OK]をクリックします。





  [Apply] をクリックし、設定を反映。

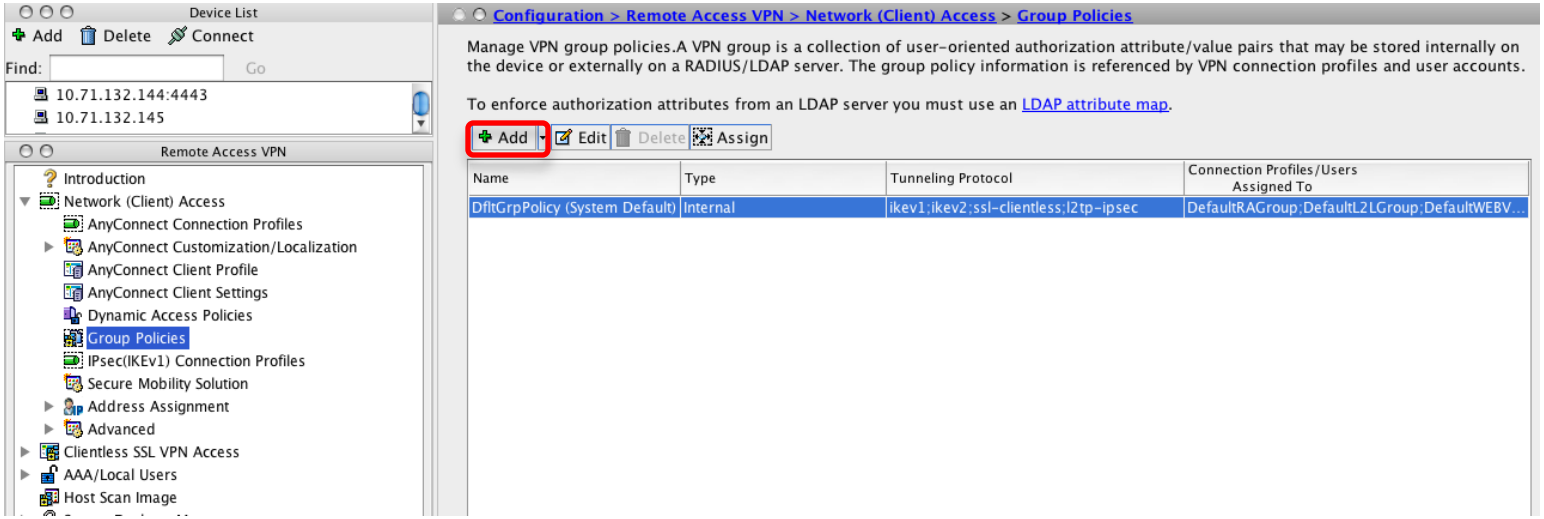
  [Refresh] をクリックし、設定の再読み込み。



VPN 設定: AnyConnect

- AnyConnect の設定 – Group Policy

  Configuration -> Remote Access VPN -> Network (Client) Access -> Group Policies へ移動し [Add] をクリック

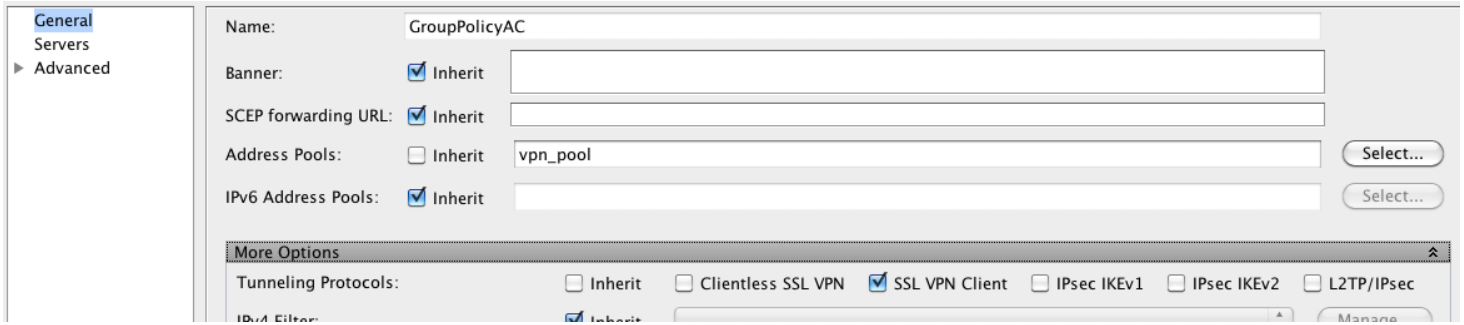


VPN 設定: AnyConnect

- AnyConnect の設定 – Group Policy (続き)

  左側の Pane より、General を選択。Name: に名前を入力 (Ex. GroupPolicyAC)、Address Pools: の Inherit のチェックを外し、[Select] をクリックし、先ほど作成したアドレスプールを選択 (Ex. vpn_pool)、[More Option] をクリックし、More Option 部を表示させ、Tunneling Protocols: の Inherit のチェックを外し、SSL VPN Client にチェックを入れる。

  ページ下にある [OK] をクリック。



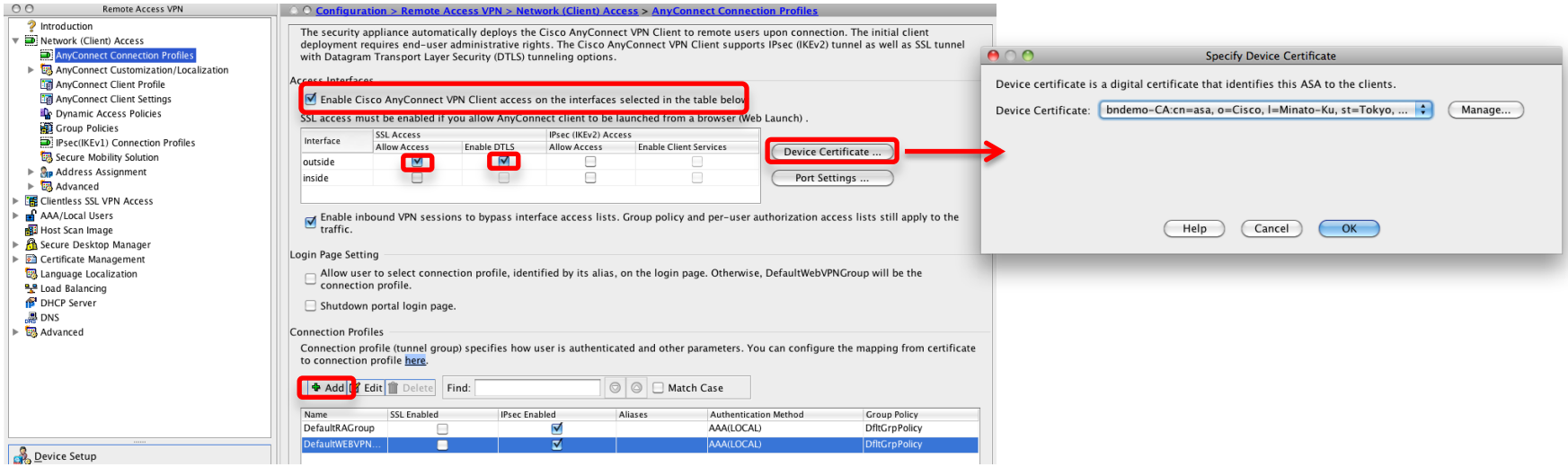
  [Apply] をクリックし、設定を反映

VPN 設定: AnyConnect

- AnyConnect の設定 – AnyConnect 有効化

  Configuration -> Remote Access VPN -> Network (Client) Access -> AnyConnect Connection Profiles へ移動し、Enable Cisco AnyConnect VPN Client access or on the interfaces selected in the table below にチェックし、Interface outside の SSL Access, Allow Access と Enable DTLS にチェック。

  [Device Certificate] をクリックし、先ほどインストールした証明書を指定し (Ex. bndemo-CA)、[OK] をクリック。

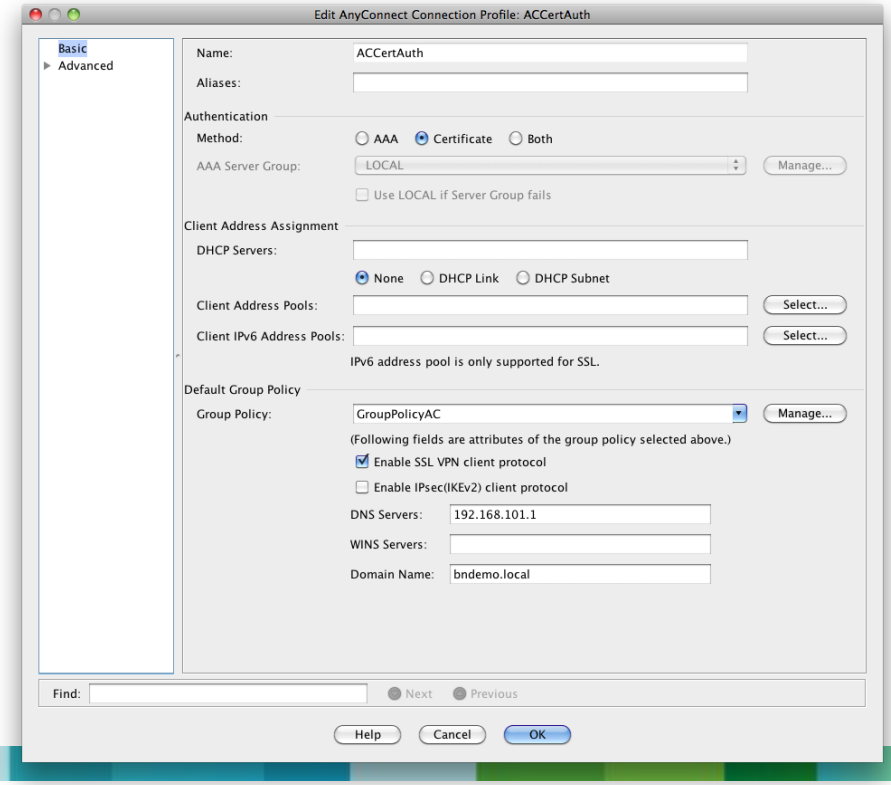


Connection Profiles 内の [Add] をクリック

VPN 設定: AnyConnect

- AnyConnect の設定 – Connection Profile 作成:証明書認証

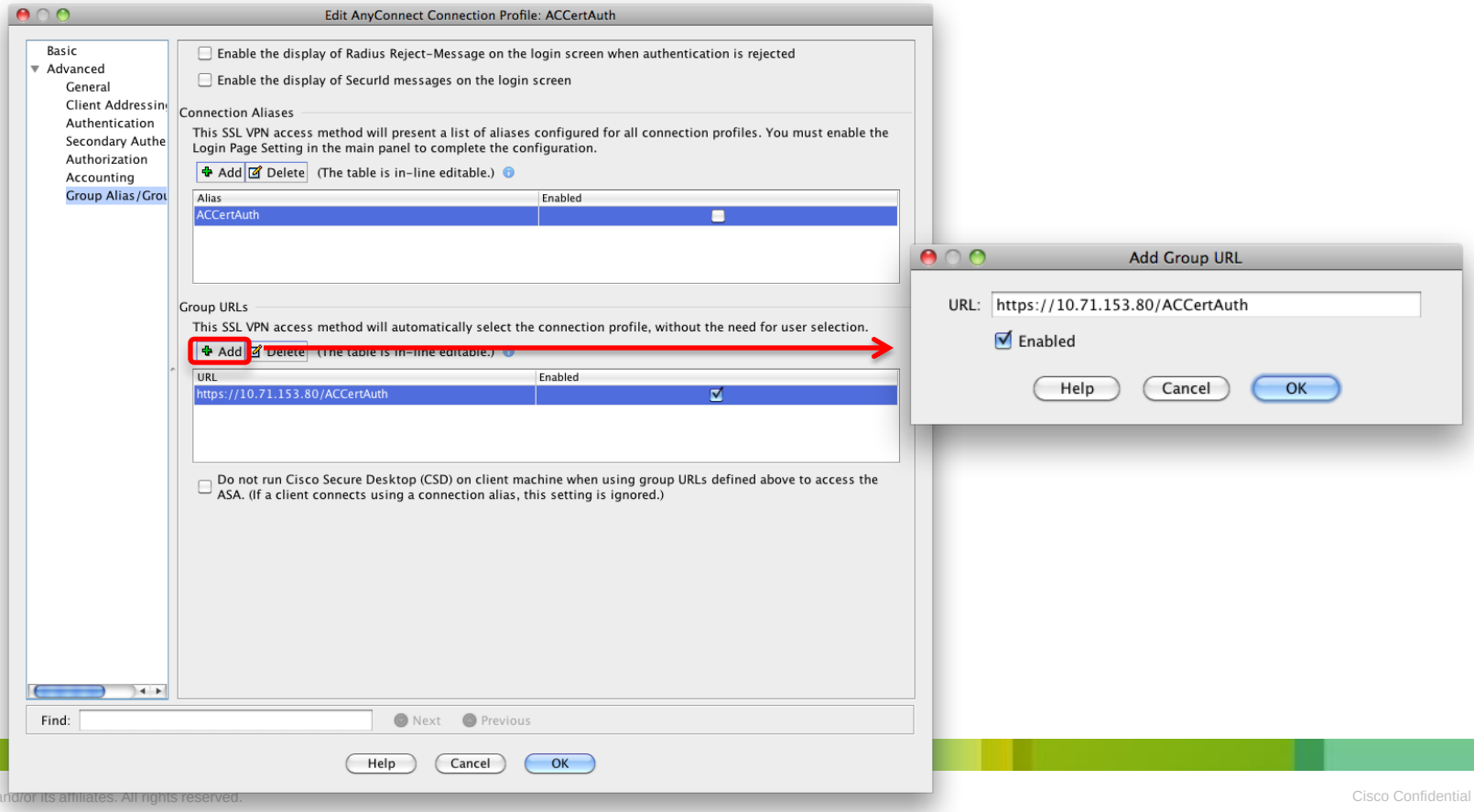
  Name: 及び Alias: に名前を入力し (Ex. ACCertAuth)、Authentication Method: で Certificate を選択。Default Group Policy, Group Policy: に先ほど作成した Group Policy を選択 (Ex. GroupPolicyAC)、Enable SSL VPN client protocol のみにチェックを入れ、DNS Servers: (Ex. 192.168.101.1)、WINS Servers: (Ex. なし)、Domain Name: (Ex. bndemo.local) を入力する。



VPN 設定: AnyConnect

- AnyConnect の設定 – Connection Profile 作成:証明書認証 (続き)

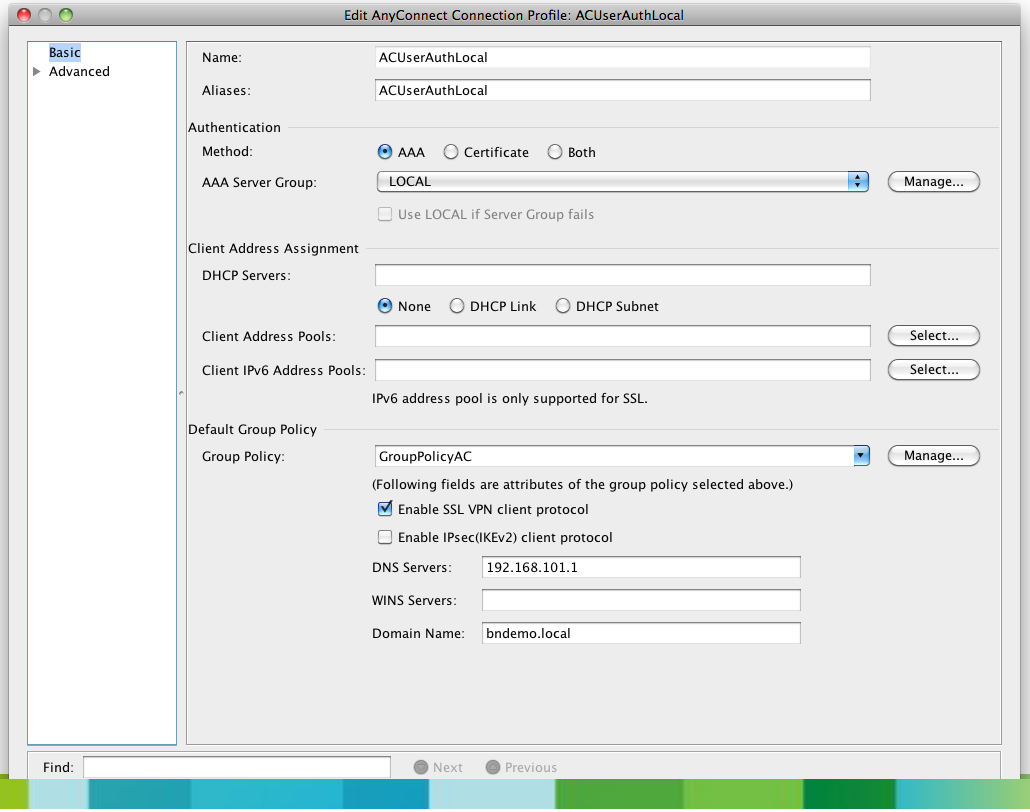
  左側の Pane より、Advanced > Group Alias/Group URL と移動し、”Group URLs” の Add をクリックし、Group URL を入力 (Ex. https://10.71.153.80/ACCertAuth)、Enable にチェックを入れる。その後、[OK] をクリック。



VPN 設定: AnyConnect

- AnyConnect の設定 – Connection Profile 作成:ユーザ認証(ローカル)

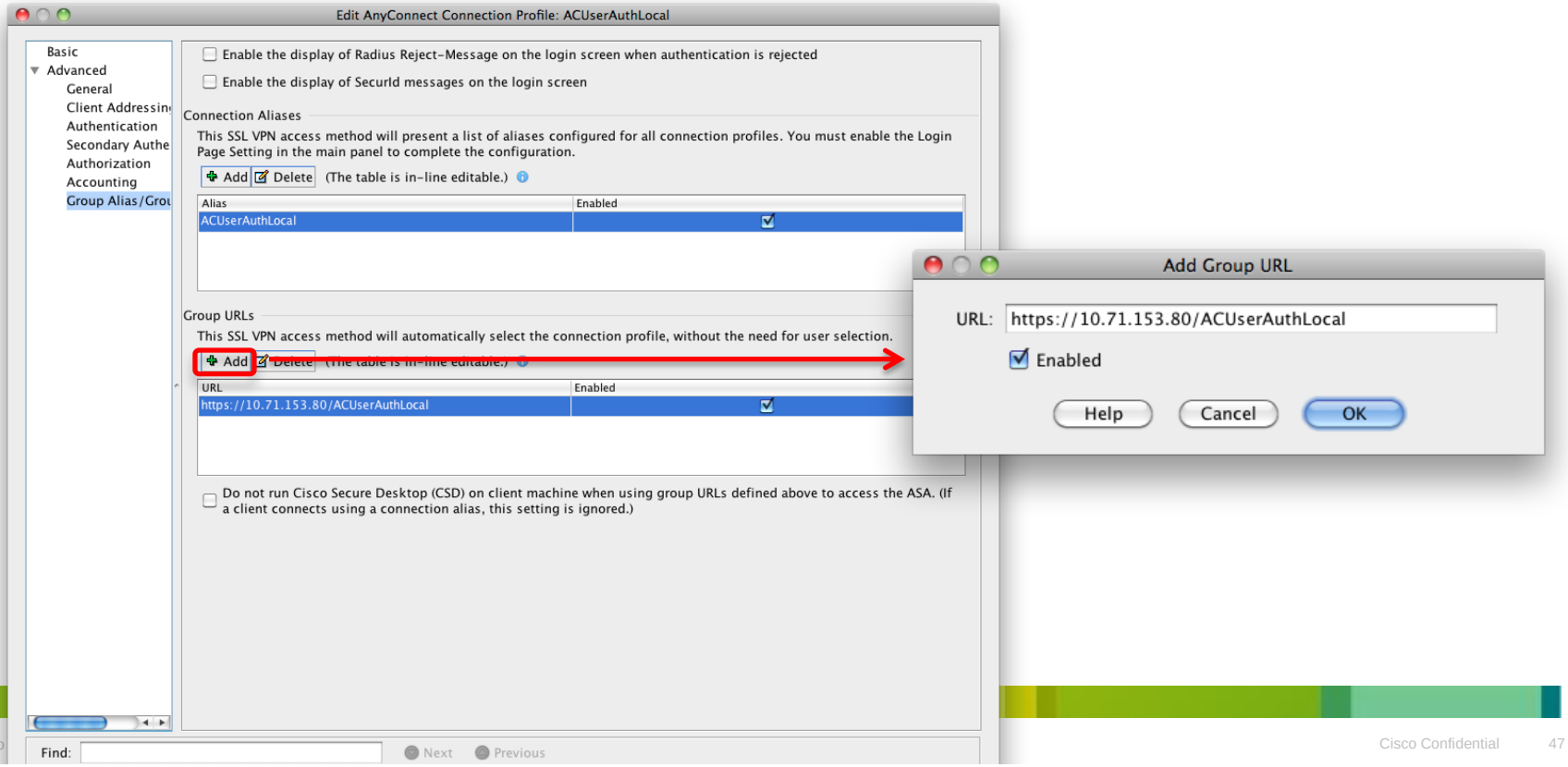
  Name: 及び Alias:に名前を入力し (Ex. ACUserAuthLocal)、Authentication Method: で AAAを選択、AAA Server Group で LOCAL を選択。Default Group Policy, Group Policy: に先ほど作成した Group Policy を選択 (Ex. GroupPolicyAC)、Enable SSL VPN client protocol のみにチェックを入れ、DNS Servers: (Ex. 192.168.101.1)、WINS Servers: (Ex. なし)、Domain Name: (Ex. bndemo.local) を入力しする。



VPN 設定: AnyConnect

- AnyConnect の設定 – Connection Profile 作成:ユーザ認証(ローカル)

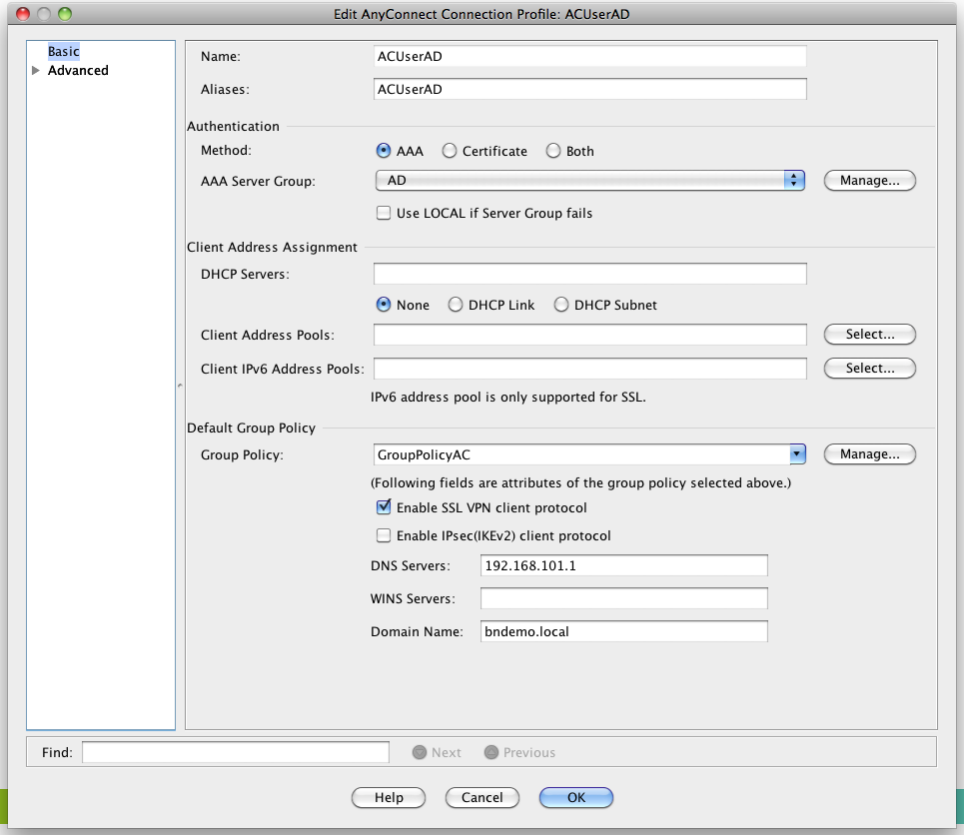
  左側の Pane より、Advanced > Group Alias/Group URL と移動し、”Group URLs” の Add をクリックし、Group URL を入力 (Ex. https://10.71.153.80/ACUserAuthLocal)、Enable にチェックを入れる。その後、[OK] をクリック。



VPN 設定: AnyConnect

- AnyConnect の設定 – Connection Profile 作成:ユーザ認証(AD)

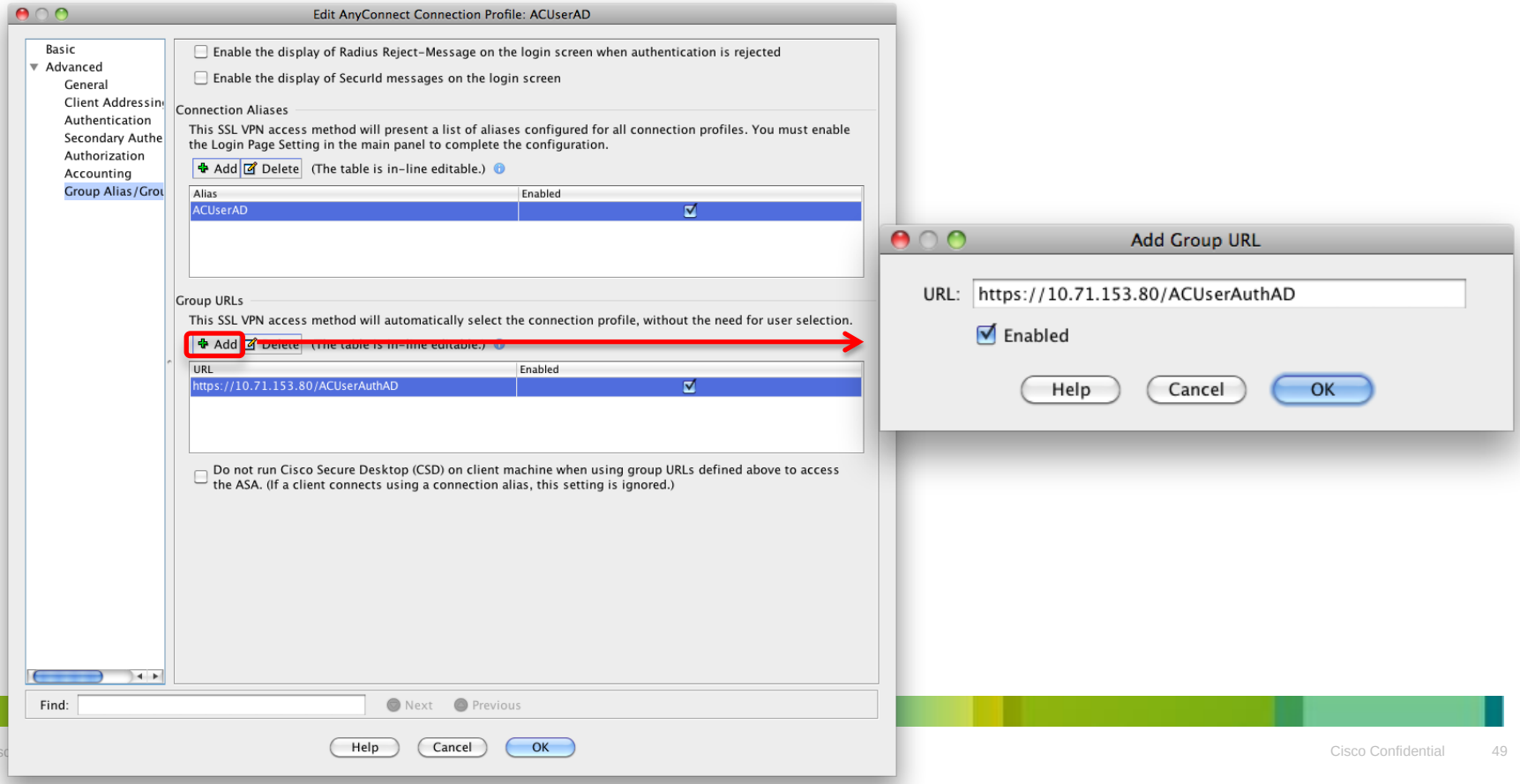
  Name: 及び Alias: に名前を入力し (Ex. ACUserAuthAD)、Authentication Method: で AAAを選択、AAA Server Group で AD を選択。Default Group Policy, Group Policy: に先ほど作成した Group Policy を選択 (Ex. GroupPolicyAC)、Enable SSL VPN client protocol のみにチェックを入れ、DNS Servers: (Ex. 192.168.101.1)、WINS Servers: (Ex. なし)、Domain Name: (Ex. bndemo.local) を入力する。



VPN 設定: AnyConnect

- AnyConnect の設定 – Connection Profile 作成:ユーザ認証(AD)

  左側の Pane より、Advanced > Group Alias/Group URL と移動し、”Group URLs” の Add をクリックし、Group URL を入力 (Ex. https://10.71.153.80/ACUserAuthAD)、Enable にチェックを入れる。その後、[OK] をクリック。

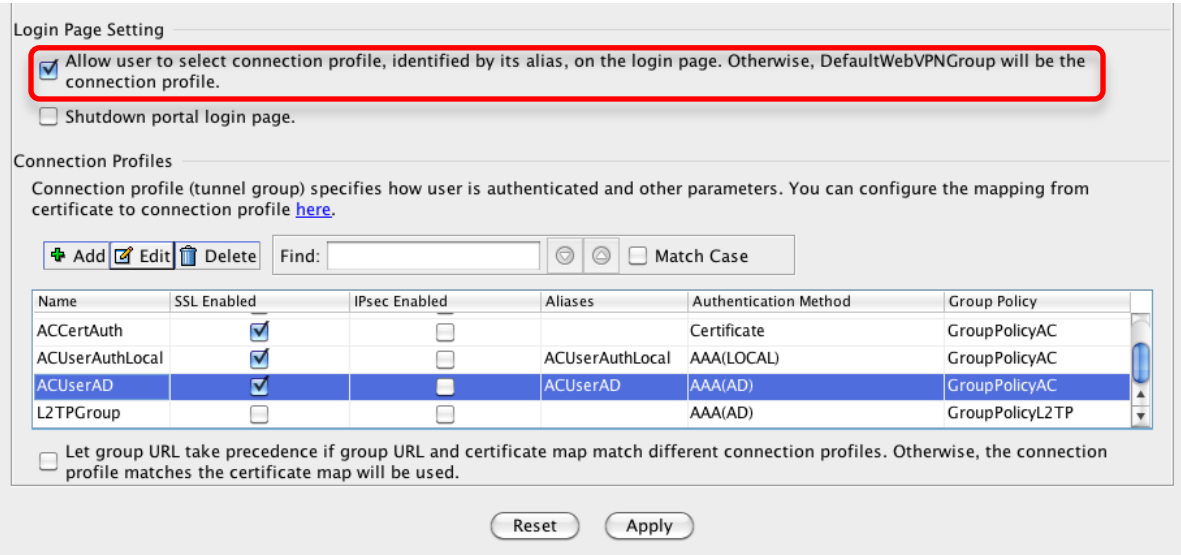


VPN 設定: AnyConnect (Option)

- AnyConnect の設定 – Connection Profile

  SSLVPN Login Page 上に、コネクションプロファイルのリストを表示させる設定

  “Login Page Setting” の “Allow user to select connection profile, identified by its alias, on login page. Otherwise, DefaultWebVPNGroup will be the connection profile” にチェックを入れる。



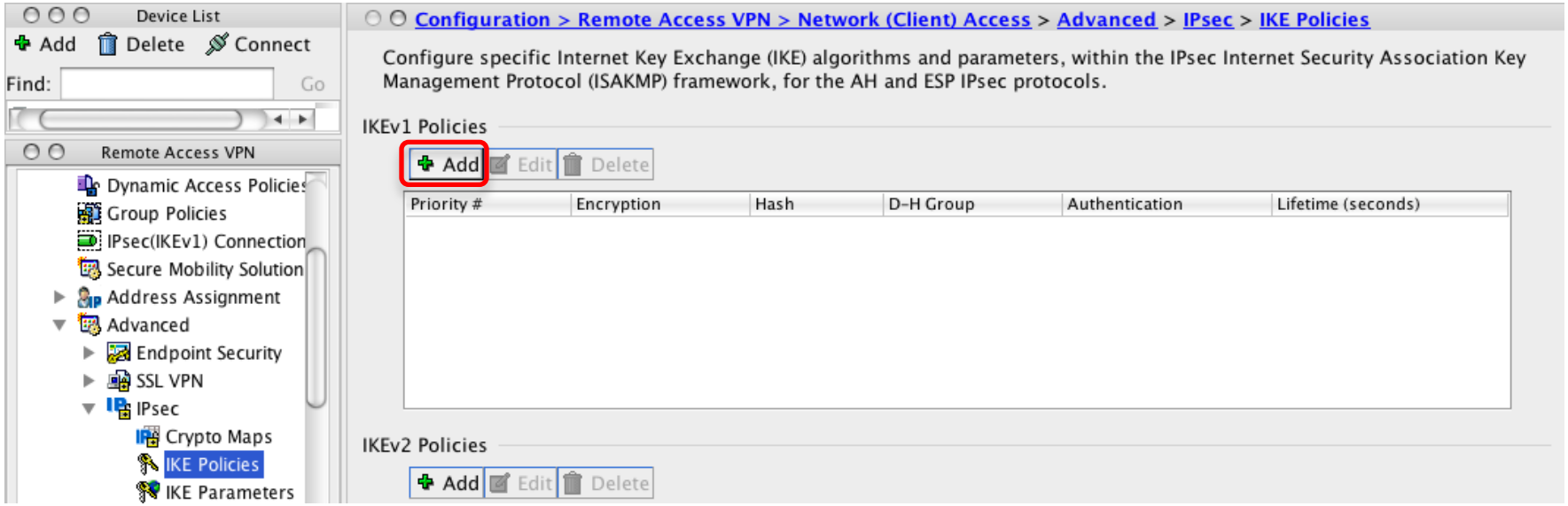
  [Apply] をクリックし、設定を反映

2. VPN 設定
b) L2TP/IPSec

VPN 設定: L2TP/IPSec – IKE ポリシー

- IKE ポリシーの設定

  Configuration -> Remote Access VPN -> Network (Client) Access -> Advanced -> IPSec -> IKE Policies と移動し、IKEv1 Policies の [Add] をクリック

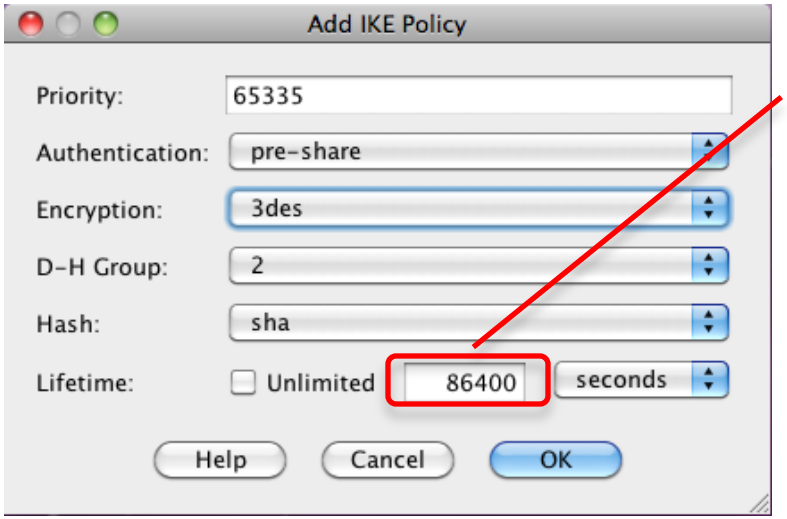


VPN 設定: L2TP/IPSec – IKE ポリシー

- IKE ポリシーの設定 (続き) – L2TP/IPSec PSK

  Priority 番号、Authentication, Encryption, D-H Group, Hash タイプの選択を選択し、[OK] をクリック

  Ex. Priority: 65535, Authentication: pre-share, Encryption: 3des, D-H Group: 2, Hash: sha



断末側で wifi/3G 断となった場合、
ISAKMP rekey もしくは、l2tp tunnel hello (デフォルト６０秒) の早い方のタイミングで、L2TP/IPSec トンネルが切断されます。
ISAKMP の Rekey の設定はこの画面より変更可能。

l2tp tunnel hello は、 CLI にて設定変更可能。
Ex. 30秒に設定する場合

```
asa# conf t
asa(config)# l2tp tunnel hello 30
asa(config)#
```

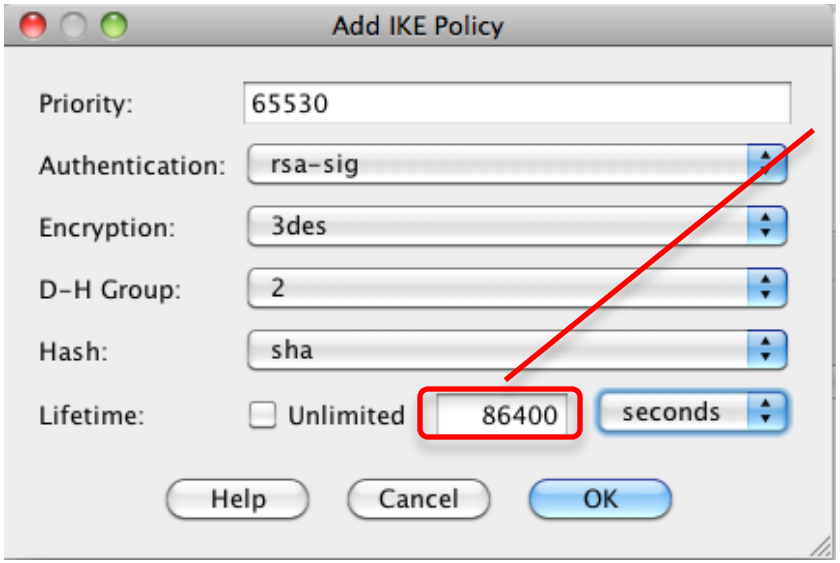
[Apply] をクリックし、設定を反映

設定例 VPN 設定: L2TP/IPSec – IKE ポリシー

- IKE ポリシーの設定 (続き) – L2TP/IPSec CRT

  Priority 番号、Authentication, Encryption, D-H Group, Hash タイプの選択を選択し、[OK] をクリック

  Ex. Priority: 65530, Authentication: rsa-sig, Encryption: 3des, D-H Group: 2, Hash: sha



断末側で wifi/3G 断となった場合、
ISAKMP rekey もしくは、l2tp tunnel hello (デフォルト６０秒) の早い方のタイミングで、L2TP/IPSec トンネルが切断されます。
ISAKMP の Rekey の設定はこの画面より変更可能。

l2tp tunnel hello は、 CLI にて設定変更可能。
Ex. 30秒に設定する場合

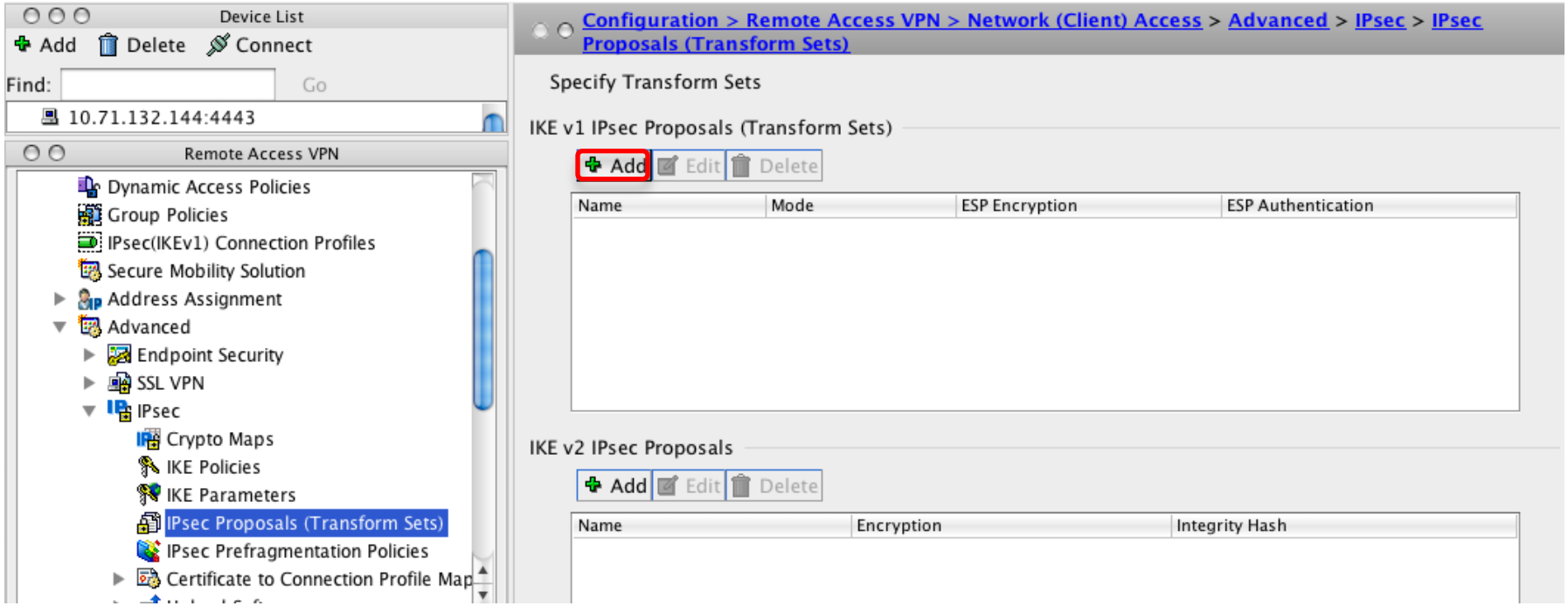
```
asa# conf t
asa(config)# l2tp tunnel hello 30
asa(config)#
```

  [Apply] をクリックし、設定を反映

VPN 設定: L2TP/IPSec – トランスフォーム

- トランスフォームセットの設定

  Configuration -> Remote Access VPN -> Network (Client) Access -> Advanced -> IPSec -> IPSec Proposals (Transform Set) に移動し IKEv1 IPSec Proposals (Transform Sets) の [Add] をクリック

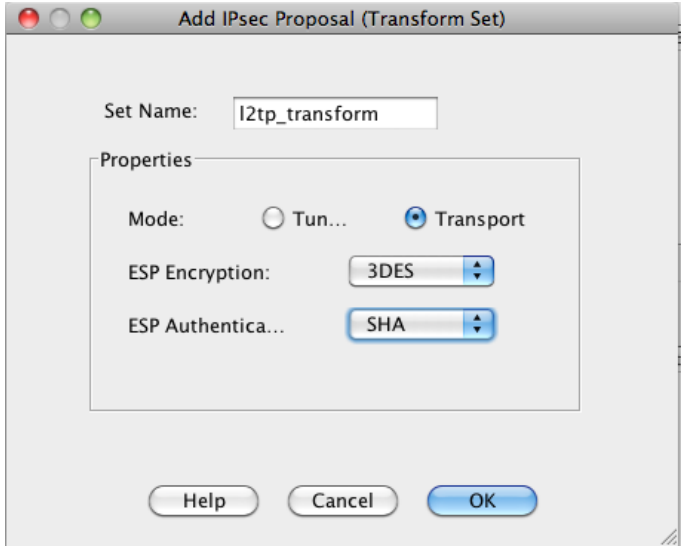


VPN 設定: L2TP/IPSec – トランスフォーム

- トランスフォームセットの設定 (続き)

  Name: [任意のなまえ], Mode: Transport, ESP Encryption & Authentication を入力し [OK] をクリック。

  Ex. Set Name: l2tp_transform, Mode: Transport, ESP Encryption: 3DES, ESP Authentication: SHA

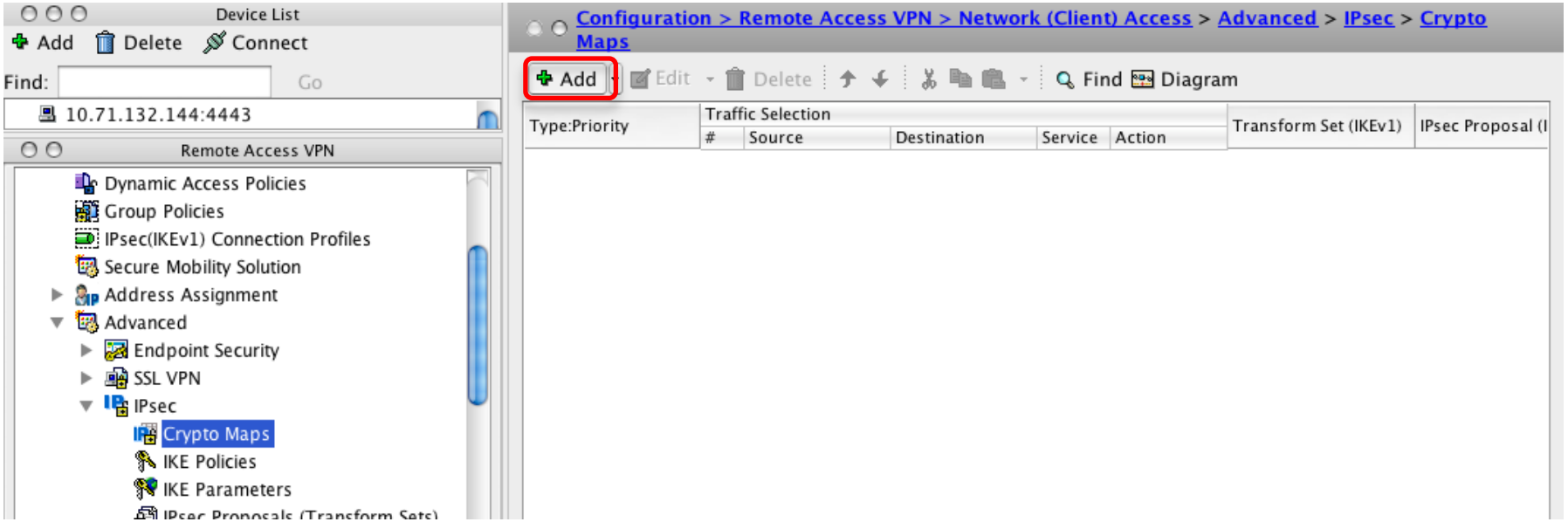


[Apply] をクリックし、設定を反映

VPN 設定: L2TP/IPSec – Crypto Map

- Crypto Map の設定

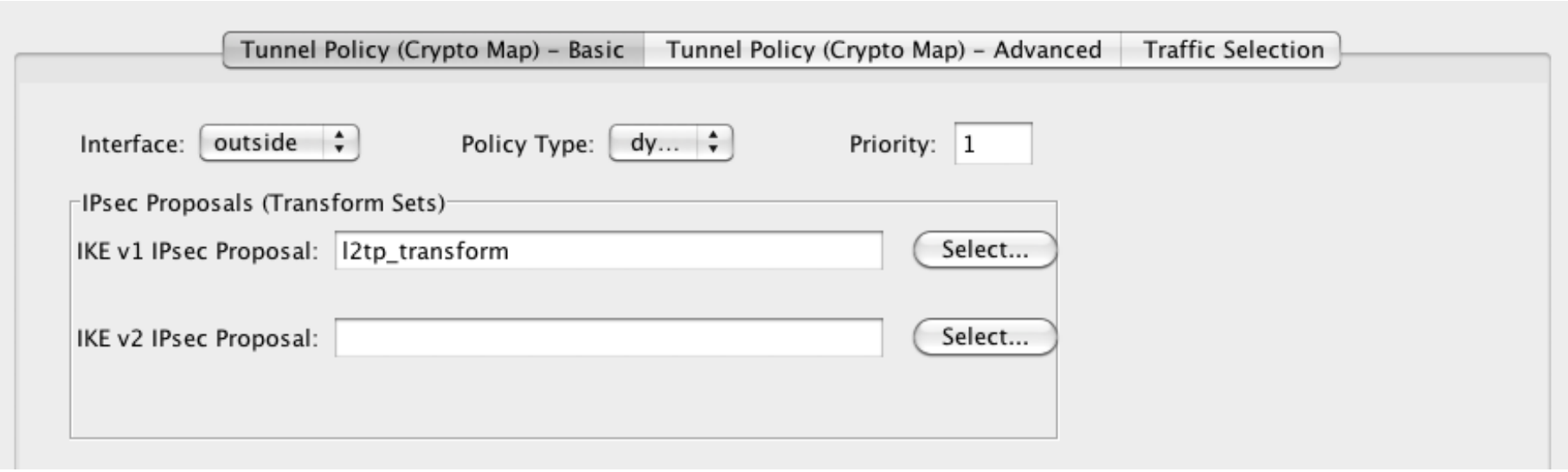
  Configuration -> Remote Access VPN -> Network (Client) Access -> Advanced -> IPSec -> Crypto Maps へ移動し [Add] をクリック



VPN 設定: L2TP/IPSec – Crypto Map

- Crypto Map の設定 (続き)

  Interface: outside, Policy Type: dynamic を選択。IKE v1 IPsec Proposal: に先ほど作成したもの (Ex. l2tp_transform) を指定し [OK] をクリック

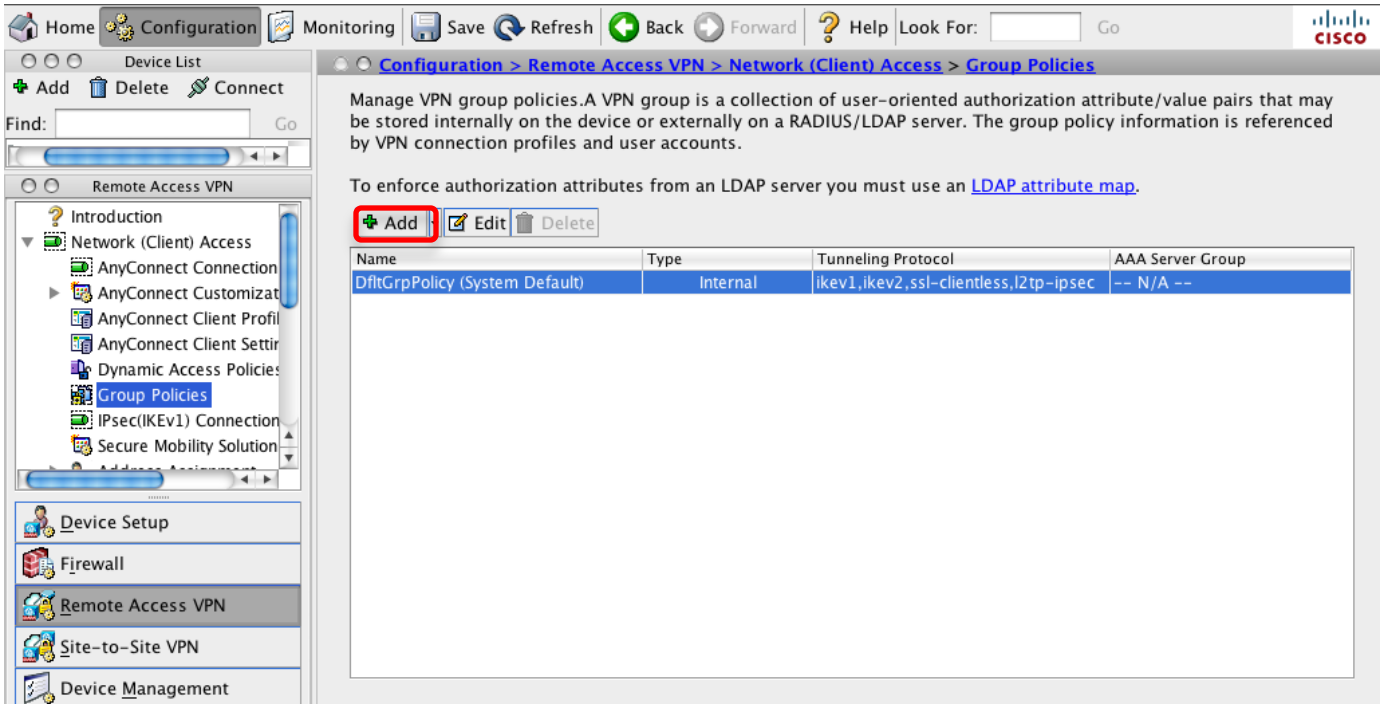


[Apply] をクリックし、設定を反映

VPN 設定: L2TP/IPSec - グループポリシー設定

- グループポリシーの作成

  Configuration > Remote Access VPN > Network (Client) Access > Group Policies へ移動し [Add] をクリック

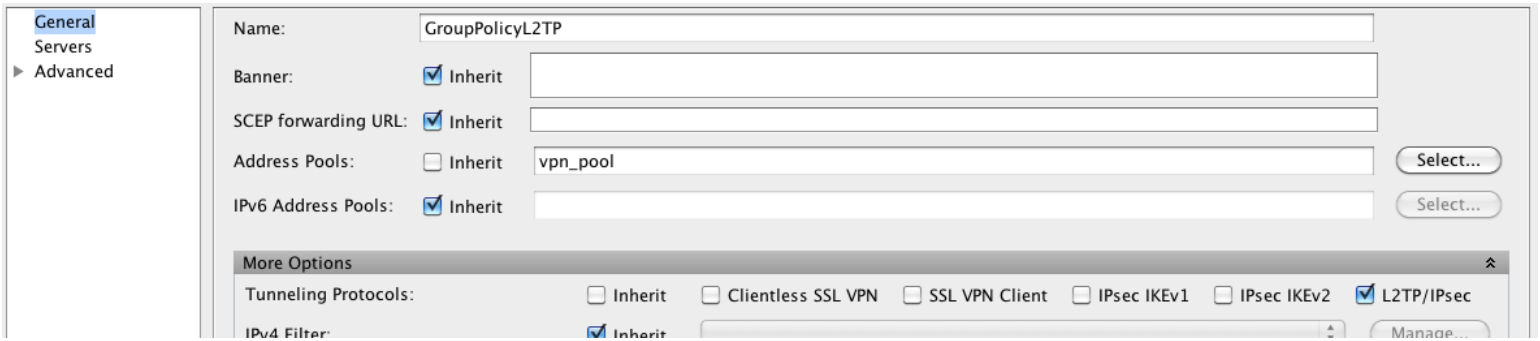


設定例 – L2TP/IPsec - グループポリシー設定

- グループポリシーの作成 (続き)

  [Name:] に名前を入力 (Ex. GroupPolicyL2TP)、Address Pools: の Inherit のチェックを外し、[Select] をクリックし、先ほど作成したアドレスプールを選択 (Ex. vpn_pool)、[More Option] をクリックし、More Option 部を表示させ、Tunneling Protocols: の Inherit のチェックを外し、SSL VPN Client にチェックを入れる。

  ページ下にある [OK] をクリック。



  [Apply] をクリックし、設定を反映

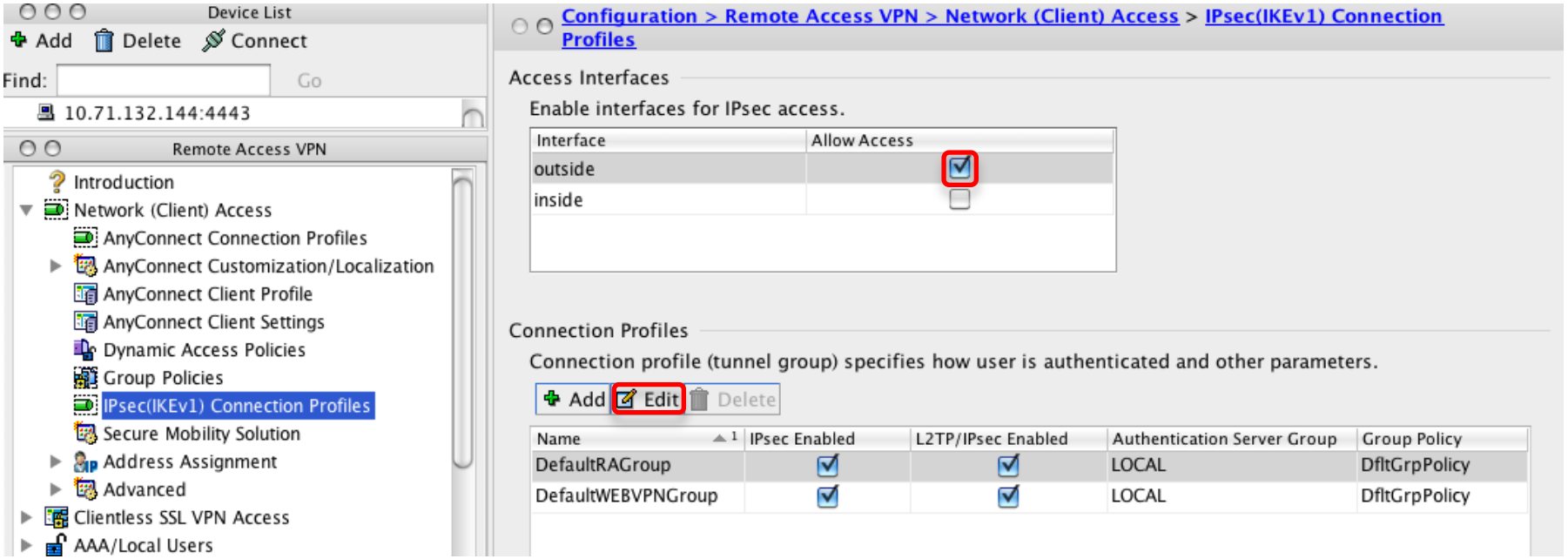
設定例 – L2TP/IPsec PSK

- コネクションプロファイルの設定

  Configuration -> Remote Access VPN -> Network (Client) Access -> IPSec(IKEv1) Connection Profiles へ移動

  Access Interfaces: outside の Allow Access にチェックを入れる

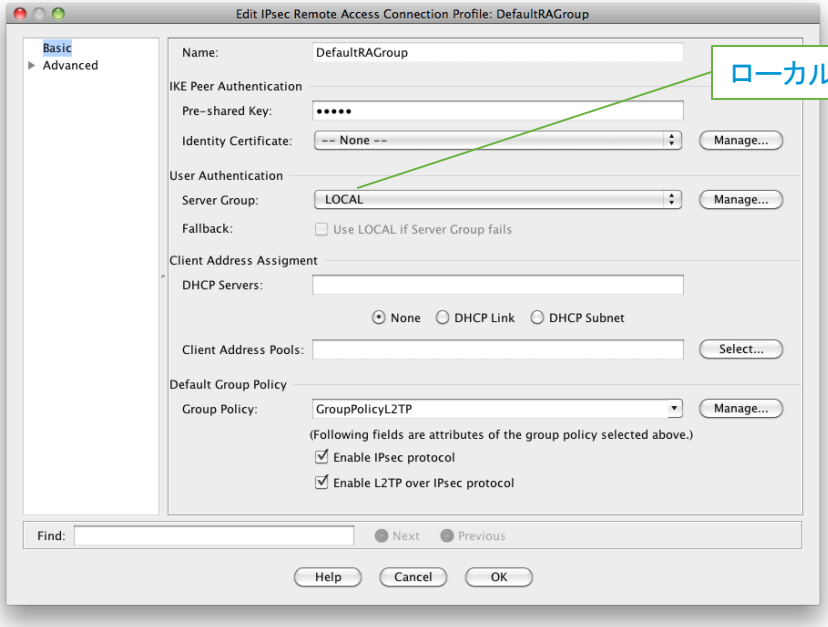
  Connection Profiles で DefaultRAGroup を選び [Edit] をクリック

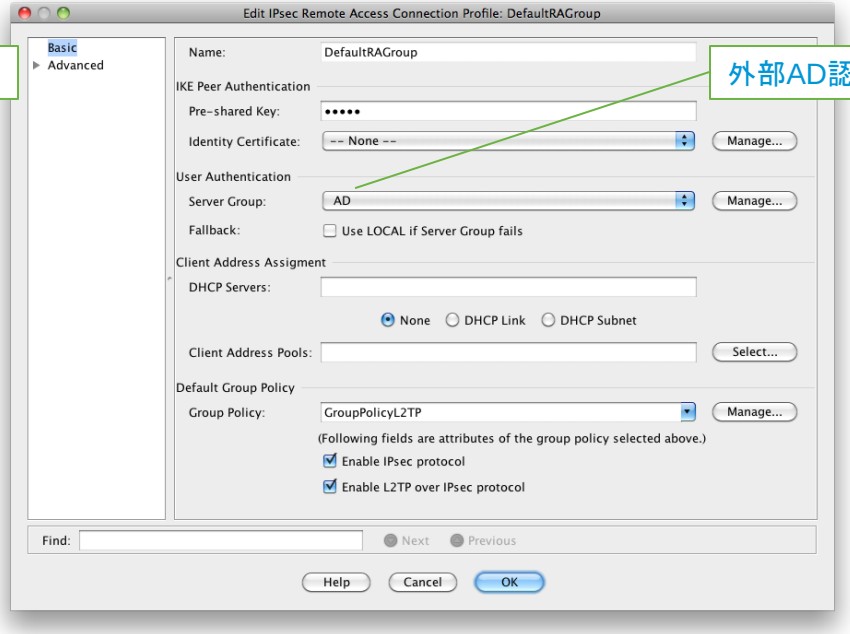


設定例 – L2TP/IPsec PSK

- コネクションプロファイルの設定 (続き)

  Pre-shared Key (Ex. Pre-shared Key: cisco) を入力、Server Group: LOCAL を選択 (➔ ローカル認証) もしくは、AD を選択 (➔ 外部認証)、Group Policy: に作成したものを選択 (Ex. GroupPolicyL2TP)、 “Enable IPsec proposal” 及び “Enable L2TP over IPSec proposal” にチェックがある事を確認する。

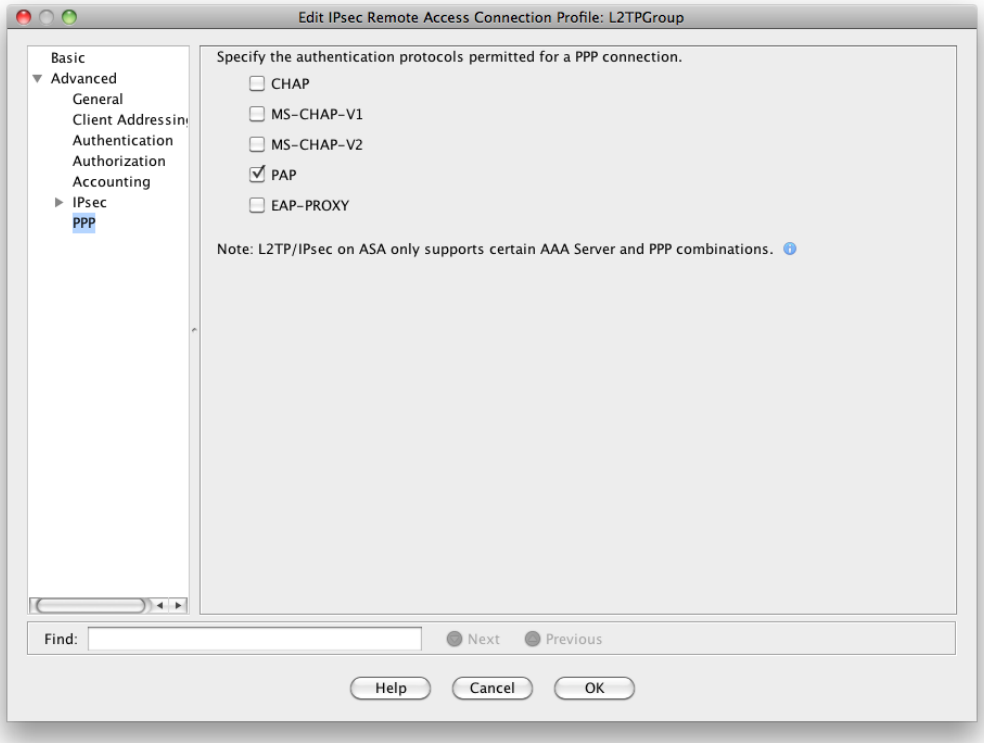




設定例 – L2TP/IPsec PSK

- コネクションプロファイルの設定 (続き)

  左側の Pane より、Advanced > PPP と移動し、”Specify the authentication protocol permitted for a PPP connection” で “PAP” のみにチェックを入れ、[OK] をクリック。



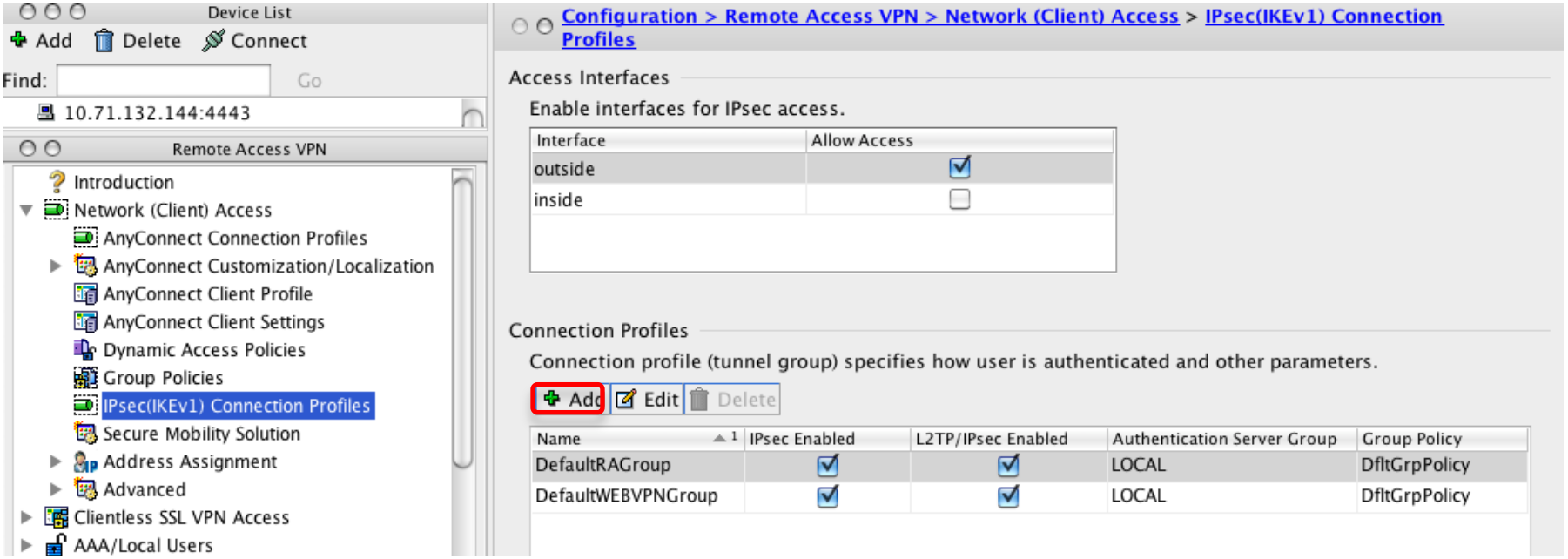
  [Apply] をクリックし、設定を反映

設定例 – L2TP/IPsec CRT

- コネクションプロファイルの作成

  Configuration -> Remote Access VPN -> Network (Client) Access -> IPSec(IKEv1) Connection Profiles へ移動

  Connection Profiles [Add] をクリック

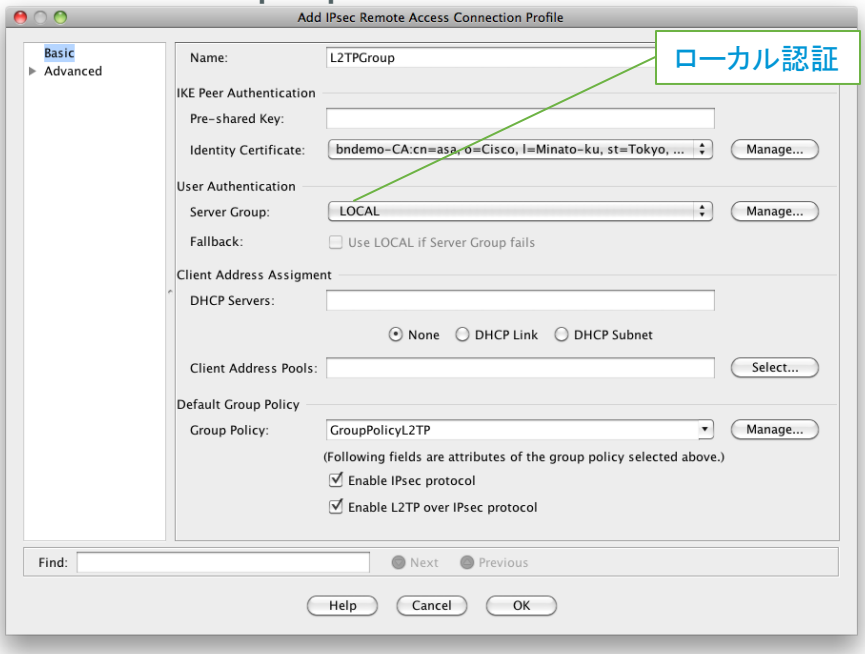


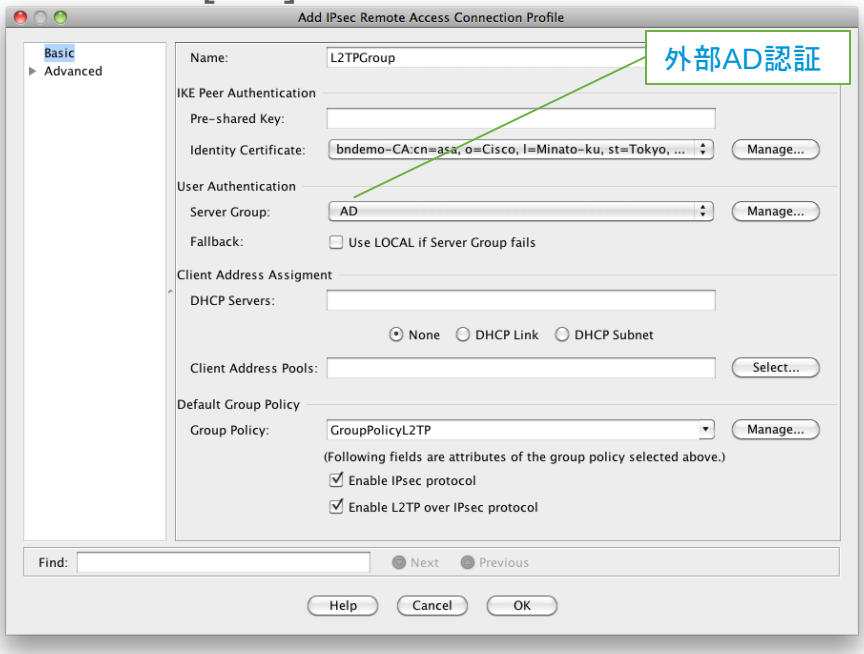
設定例 – L2TP/IPsec CRT

- コネクションプロファイルの設定 (続き)

  Name: にユーザ証明書で指定する OU と同じもの (Ex. L2TPGroup)

  Identity Certificate を選択 (Ex. bndemo-CA)、Group Policy: に作成したものを選択 (Ex. GroupPolicyL2TP)、 “Enable IPsec proposal” 及び “Enable L2TP over IPSec proposal” にチェックがある事を確認し [OK] をクリック



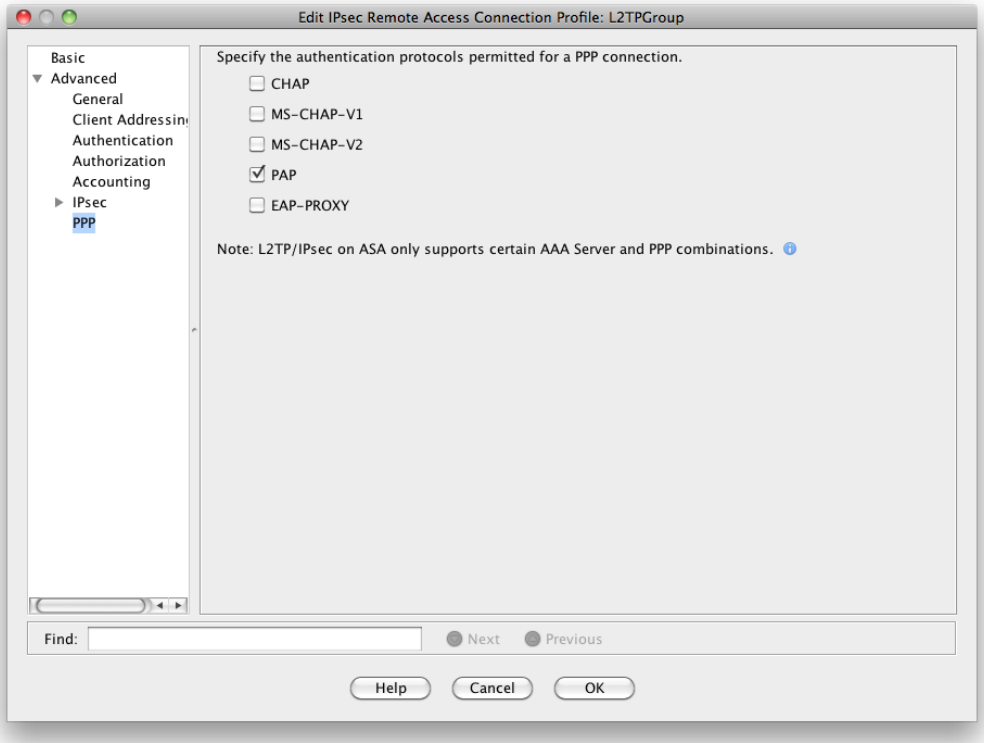


  [Apply] をクリックし、設定を反映

設定例 – L2TP/IPsec CRT

- コネクションプロファイルの設定 (続き)

  左側の Pane より、Advanced > PPP と移動し、”Specify the authentication protocol permitted for a PPP connection” で “PAP” のみにチェックを入れ、[OK] をクリック。



[Apply] をクリックし、設定を反映

ASA Sample Config

```
!
hostname asa
domain-name bndemo.local
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.71.153.80 255.255.255.128
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.101.254 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
dns server-group DefaultDNS
 domain-name bndemo.local
same-security-traffic permit intra-interface
object network server
 host 192.168.101.1
```

```
object network vpn_cleints
 range 192.168.102.101 192.168.102.110
access-list outside_access_in extended permit ip any object server
pager lines 24
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
ip local pool vpn_pool 192.168.102.101-192.168.102.110 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-645.bin
no asdm history enable
arp timeout 14400
nat (outside,inside) source static vpn_cleints vpn_cleints
!
object network server
 nat (any,any) static 10.71.153.81
!
nat (any,outside) after-auto source dynamic any interface
access-group outside_access_in in interface outside
route outside 0.0.0.0 0.0.0.0 10.71.153.126 1
timeout xlate 3:00:00
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
aaa-server AD protocol nt
aaa-server AD (inside) host 192.168.101.1
 nt-auth-domain-controller 192.168.101.1
user-identity default-domain LOCAL
http server enable
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
```

ASA Sample Config - Cont

```
snmp-server enable traps snmp authentication linkup linkdown
coldstart warmstart
crypto ipsec ikev1 transform-set l2tp_transform esp-3des esp-sha-
hmac
crypto ipsec ikev1 transform-set l2tp_transform mode transport
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set
l2tp_transform
crypto map outside_map 65535 ipsec-isakmp dynamic
outside_dyn_map
crypto map outside_map interface outside
crypto ca trustpoint bndemo-CA
 revocation-check crl none
 enrollment terminal
 subject-name CN=asa,O=Cisco,C=JP,St=Tokyo,L=Minato-ku
 keypair asa.key
 crl configure
  policy static
  url 1 http://192.168.101.1/CertEnroll/bndemo-CA.crl
  no protocol ldap
  no protocol scep
crypto ca certificate chain bndemo-CA
 certificate ca 344679022a7810924c265fb083e460de
    30820361 30820249 a0030201 02021034 4679022a 7810924c
265fb083 e460de30
    0d06092a 864886f7 0d010105 05003043 31153013 060a0992
268993f2 2c640119
    16056c6f 63616c31 16301406 0a099226 8993f22c 64011916
06626e64 656d6f31
!
! <snip>
!
 quit
 certificate 14e87d8f000000000004
    3082054a 30820432 a0030201 02020a14 e87d8f00 00000000
04300d06 092a8648
    86f70d01 01050500 30433115 3013060a 09922689 93f22c64
01191605 6c6f6361
!
! <snip>
!
 quit
```

```
crypto ikev2 remote-access trustpoint bndemo-CA
crypto ikev1 enable outside
crypto ikev1 policy 65530
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ssl trust-point bndemo-CA outside
webvpn
 enable outside
 anyconnect-essentials
 anyconnect image disk1:/anyconnect-win-3.0.3054-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
group-policy GroupPolicyAC internal
group-policy GroupPolicyAC attributes
 wins-server none
 dns-server value 192.168.101.1
 vpn-tunnel-protocol ssl-client
 default-domain value bndemo.local
 address-pools value vpn_pool
group-policy GroupPolicyL2TP internal
group-policy GroupPolicyL2TP attributes
 vpn-tunnel-protocol ikev1 l2tp-ipsec
 address-pools value vpn_pool
username acuser password j39fuvcRZNDqQeK7 encrypted
username admin password e1z89R3cZe9Kt6Ib encrypted privilege
15
username l2tpuser password XIAPE6POhu0lQN1OczHpog== nt-
encrypted
```

ASA Sample Config - Cont

```
tunnel-group DefaultRAGroup general-attributes
 authentication-server-group AD
 default-group-policy GroupPolicyL2TP
tunnel-group DefaultRAGroup ipsec-attributes
 ikev1 pre-shared-key *****
tunnel-group DefaultRAGroup ppp-attributes
 authentication pap
 no authentication chap
 no authentication ms-chap-v1
tunnel-group ACCertAuth type remote-access
tunnel-group ACCertAuth general-attributes
 default-group-policy GroupPolicyAC
tunnel-group ACCertAuth webvpn-attributes
 authentication certificate
 group-alias ACCertAuth disable
 group-url https://10.71.153.80/ACCertAuth enable
tunnel-group ACUserAuthLocal type remote-access
tunnel-group ACUserAuthLocal general-attributes
 default-group-policy GroupPolicyAC
tunnel-group ACUserAuthLocal webvpn-attributes
 group-alias ACUserAuthLocal enable
 group-url https://10.71.153.80/ACUserAuthLocal enable
tunnel-group ACUserAD type remote-access
tunnel-group ACUserAD general-attributes
 authentication-server-group AD
 default-group-policy GroupPolicyAC
tunnel-group ACUserAD webvpn-attributes
 group-alias ACUserAD enable
 group-url https://10.71.153.80/ACUserAuthAD enable
tunnel-group L2TPGroup type remote-access
tunnel-group L2TPGroup general-attributes
 authentication-server-group AD
 default-group-policy GroupPolicyL2TP
 password-management
tunnel-group L2TPGroup ipsec-attributes
 ikev1 trust-point bndemo-CA
tunnel-group L2TPGroup ppp-attributes
 authentication pap
 no authentication chap
 no authentication ms-chap-v1
!
```

```
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 h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
call-home reporting anonymous prompt 2
call-home
 profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
: end
```

3. クライアント設定
a) AnyConnect

クライアント設定: AnyConnect

- AnyConnect アプリをダウンロードします。

  iPhone/iPad

  http://itunes.apple.com/jp/app/cisco-anyconnect/id392790924?mt=8

  Android

  AnyConnect for Samsung

  https://market.android.com/details?id=com.cisco.anyconnect.vpn.android&hl=ja

  AnyConnect for Rooted Device

  https://market.android.com/details?id=com.cisco.anyconnect.vpn.android.rooted&hl=ja

クライアント設定: AnyConnect

1. ユーザ証明書、CA 証明書をデバイスにインストール

   iPhone/iPad

   CA、ユーザ証明書をデバイスにインストール。

   Android

   CA 証明書: デバイスにインストール。

   ユーザ証明書: AnyConnect アプリにインストールする必要がある為、URI Handler (*) を使用。

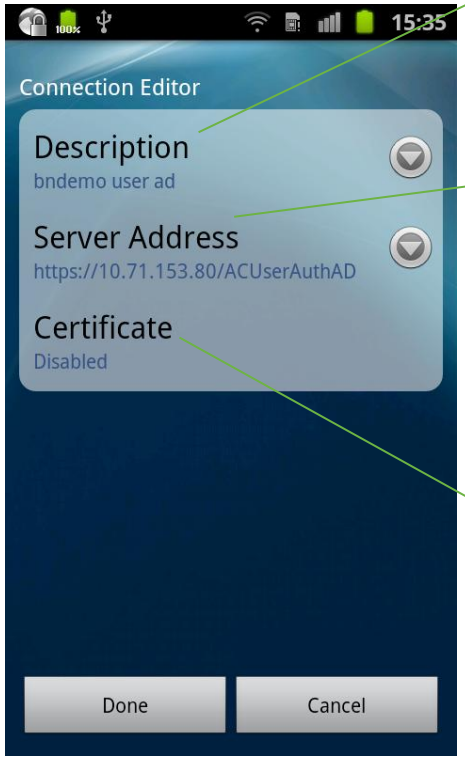
   (*) http://www.cisco.com/en/US/partner/docs/security/vpn_client/anyconnect/anyconnect24/release/notes/rn-ac2.4-android.html#wp1082290

2. AnyConnect Connection 設定

   Add VPN Connection より設定を入力

クライアント設定: AnyConnect

- 設定サンプル



Android

Description: 任意の名前

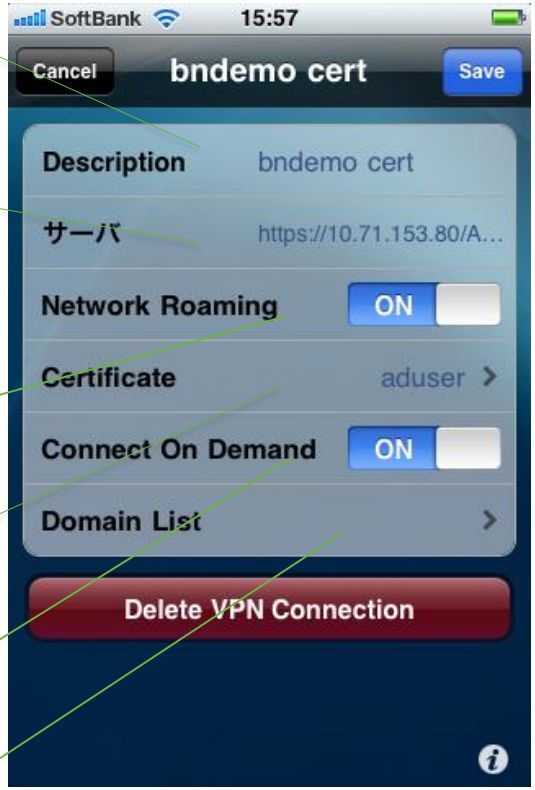
Server Address:
コネクションプロファイル Group URL で作成したものを入力
Ex:
https://10.71.153.80/ACCertAuth
https://10.71.153.80/ACUserAuthLocal
https://10.71.153.80/ACUserAuthAD

Network Roaming: 3G <-> wifi Roaming 有効
iPhone/iPad のみ

Certificate: 証明書認証時に証明書を指定

Connect On Demand:
設定を行う場合、On
証明書必須
iPhone/iPad のみ

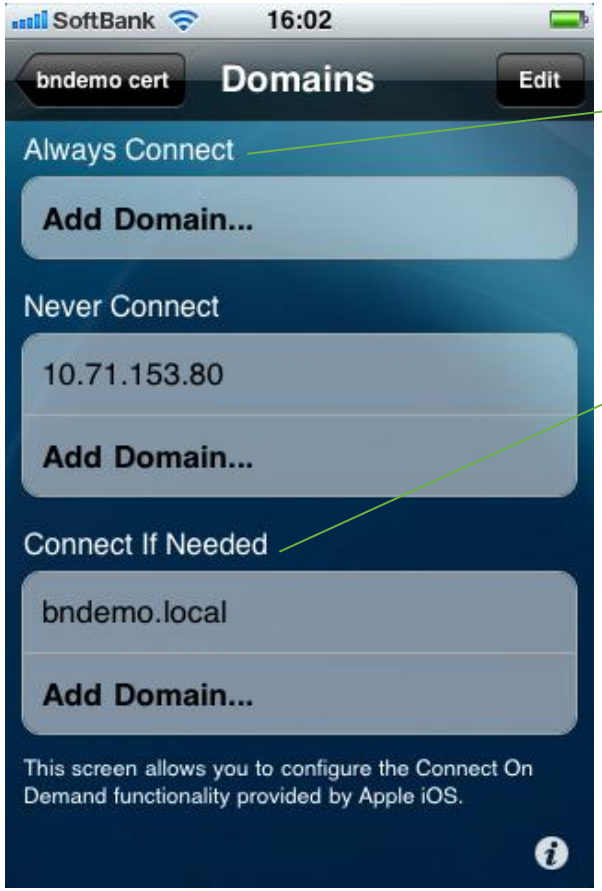
Domain List: 次ページ



iPhone

クライアント設定: AnyConnect

- 設定サンプル (続き) – Connect On Demand



Always Connect:
指定したドメインに一致するアドレスがある場合は、そのための VPN 接続 を開始。

Always Connect:
DNS ルックアップが失敗した後でのみ、指定したドメインと一致するアド レスで VPN 接続を開始。

3. クライアント設定
b) L2TP/IPSec

クライアント設定: L2TP/IPSec – iPhone/iPad

- iPhone/iPad (L2TP/IPSec PSK のみ)

  設定 > VPN > VPN 構成を追加

説明: 任意の名前

サーバ: 接続先サーバ名 or アドレス
Ex) 10.71.153.80

アカウント: 接続するユーザ名
Ex) aduser

シークレット: プリシェアキー
Ex) cisco

クライアント設定: L2TP/IPSec PSK - Android

- Android

(*) 機種によってはメニューが違う場合があります。

設定 > 無線とネットワーク > VPN設定 > VPNの追加 (*)

L2TP/IPSec PSK VPNを追加

各項目を入力

VPN名 ： 任意の名前

(Ex. L2TP PSK AD)

VPNサーバーの設定:接続先サーバ名 or アドレス

(Ex. 10.71.153.80)

IPSec事前共有鍵の設定: ASA で設定した pre-share-key

(Ex. cisco)

L2TPセキュリティ保護を有効にする: チェックなし

クライアント設定: L2TP/IPSec CRT - Android

- 必要なもの
  - ユーザ（端末）証明書 (.p12)
  - CA 証明書 (.cer) [Private CA の場合]
- 証明書のインストール方法
  - ユーザ証明書
    - 証明書 (.p12) を Android 端末 SDカードのルート(一番上のフォルダーに)置く。
    - 設定 > セキュリティー＆位置情報 > SDカードからインストール(*)
    - 証明書 (.p12) の export パスワードを入力し、証明書をインストール
  - CA 証明書
    - Web サーバーなどに CA 証明書 (.cer) を置き、Android のブラウザーからアクセスしインストール

(*) 機種によってはメニューが違う場合があります。

クライアント設定: L2TP/IPSec CRT - Android

- Android

  設定 > 無線とネットワーク > VPN設定 > VPNの追加 (*)

  L2TP/IPSec CRT VPNを追加

  各項目を入力

  VPN名 ： 任意の名前

  (Ex. L2TP CRT AD)

  VPNサーバーの設定: ASA の Outside IF アドレス

  (Ex. 10.71.153.80)

  ユーザ証明書の設定: ユーザ証明書

  認証局証明書の設定: CA 証明書

(*) 機種によってはメニューが違う場合があります。

補足

ユーザ証明書作成手順 Windows CA Server

- ユーザ証明書の作成

  PC ブラウザーより http://<CA server>/certsrv にアクセス

  証明書を要求する > 証明書の要求の詳細設定 > このCA への要求を作成し送信する

  名前、会社等入力

  (注：ここで指定する「部署名」がコネクションプロファイル名と同じもの)

  「エクスポート可能なキーとしてマーク」にチェックを入れる

  「送信」をクリック

  「この証明書をインストール」をクリック

  「ファイル名を指定して実行」より mmc を実行

  「ファイル」 > 「スナップインの追加と削除」 > 「証明書」 (ユーザアカウント) を追加

  「コンソールルート」 > 「証明書 – 現在のユーザ」 > 「個人」 > 「証明書」 より先ほどインストールした証明書を選択し、右クリック 「すべてのタスク」 > 「エクスポート」

  秘密キーをエクスポートを選び、PKCS#12 を選択、パスワード、ファイル名を指定しエクスポート。

  エクスポートしたファイル xxx.pfx を xxx.p12 のように拡張子を変更。

IAS (Radius) サーバ設定方法

- リファレンス:

  http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00806de37e.shtml#configuringthemicrosoftserverwithias

- ASA Config for Radius:

  aaa-server AD protocol radius

  aaa-server AD (inside) host x.x.x.x

  key cisco

  tunnel-group DefaultRAGroup general-attributes

  authentication-server-group AD

- ASA radius Test Command:

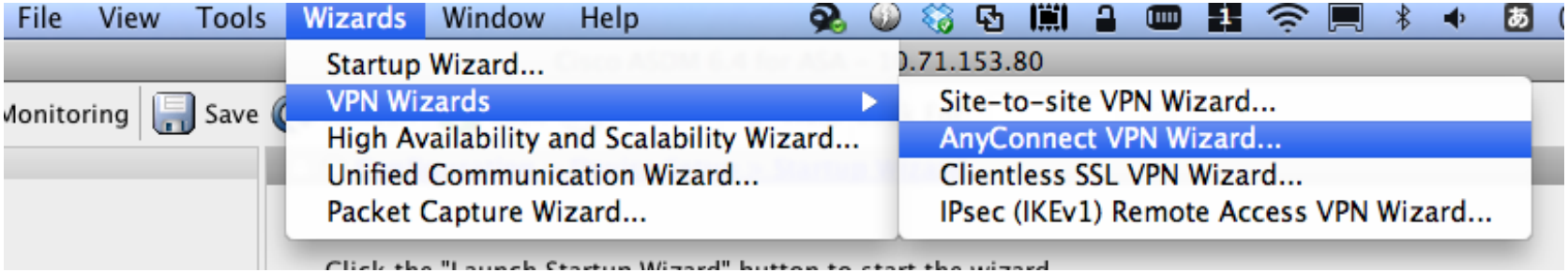
  test aaa-server authentication AD host x.x.x.x user aduser pass cisco123

VPN 設定
AnyConnect Wizard

VPN 設定: AnyConnect

- Wizard を使用しての AnyConnect の設定

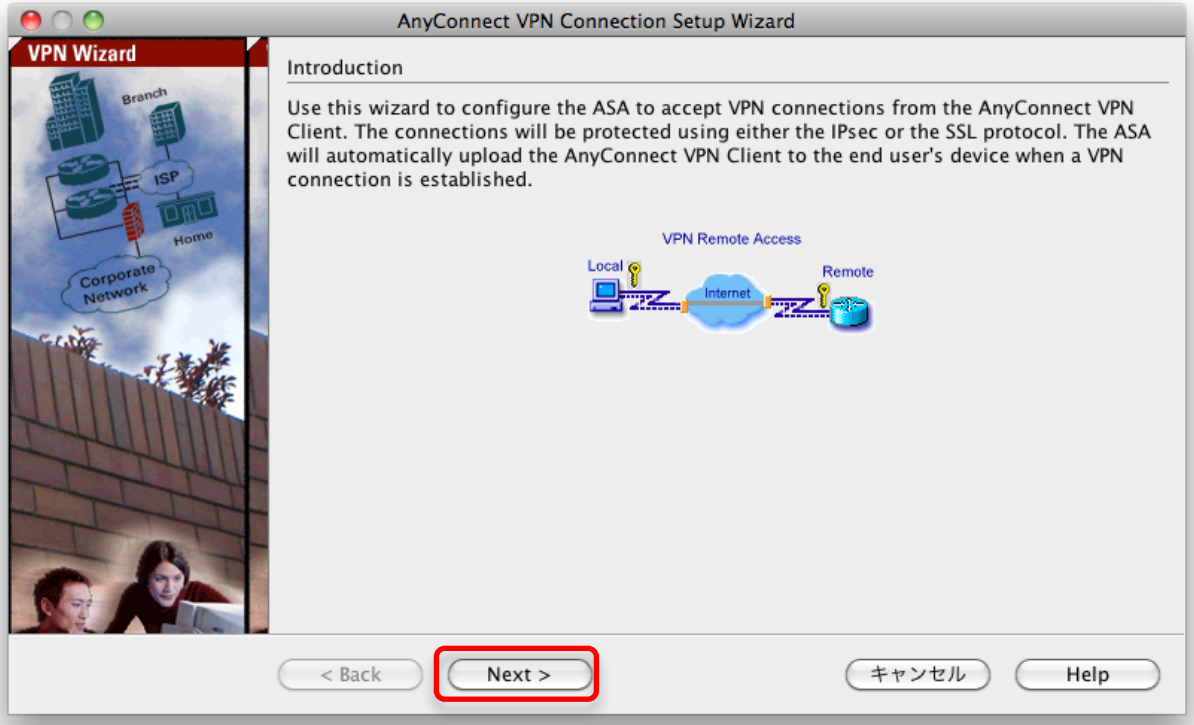
  上部のメニューより、Wizards > VPN Wizard > AnyConnect VPN Wizard と進みます。



(*)この設定では、AnyConnect のイメージが必要になりますので、CCO より、AnyConnect をダウンロードしておいて下さい。
(Ex. anyconnect-win-3.0.3054-k9.pkg)

VPN 設定: AnyConnect

- Wizard を使用しての AnyConnect の設定 (続き)
  [Next] をクリックします。



VPN 設定: AnyConnect

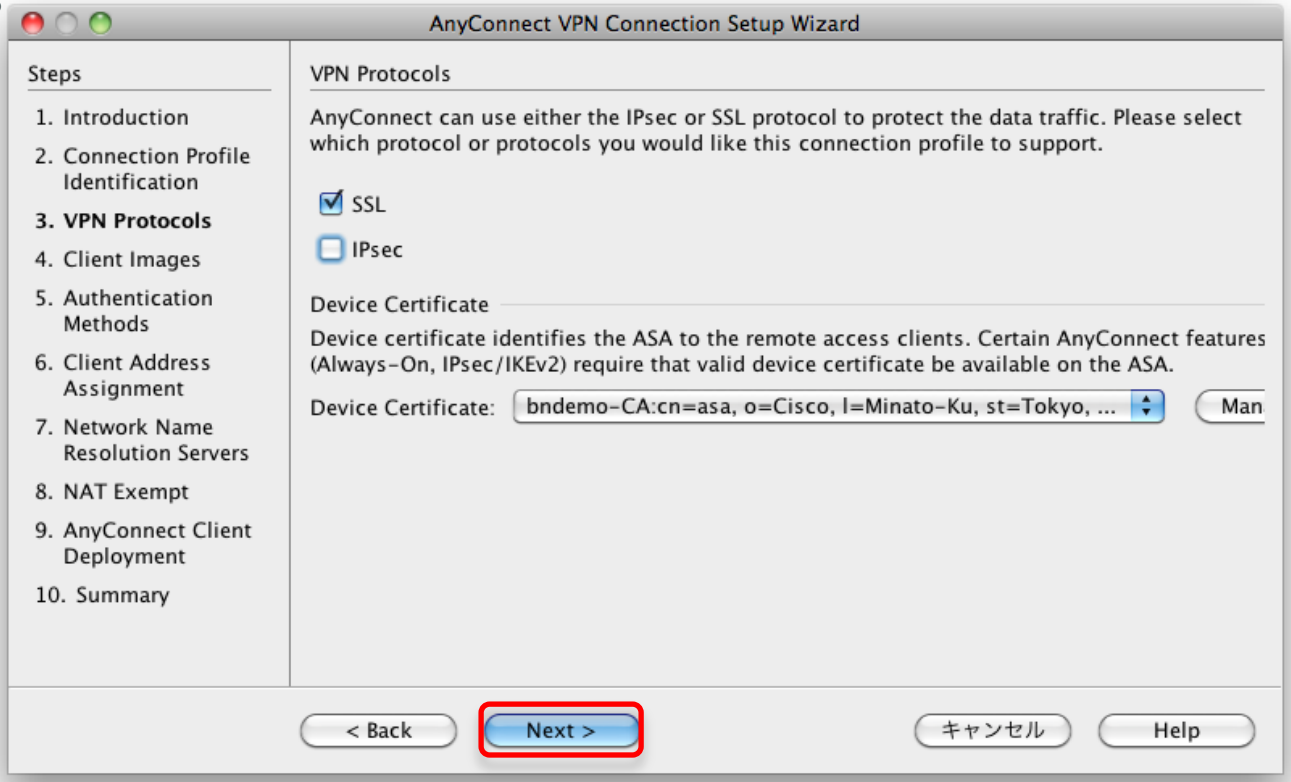
- Wizard を使用しての AnyConnect の設定 (続き)

  Connection Profile Name: に名前を入力 (Ex. ACUserAD [*] この例ではADを使用したユーザ認証の設定で使用するのでこのような名前にしました)、VPN Access Interface: に outside を選択し [Next] をクリックします。

VPN 設定: AnyConnect

- Wizard を使用しての AnyConnect の設定 (続き)

  VPN Protocols には、SSL のみにチェックを入れ、Device Certificate には、証明書設定の所でインストールした、証明書を選択し、[Next] をクリックします。

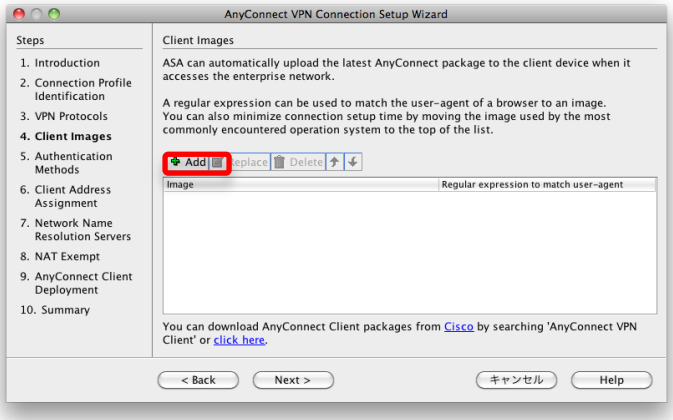


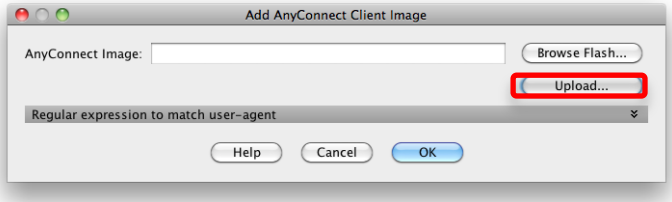
VPN 設定: AnyConnect

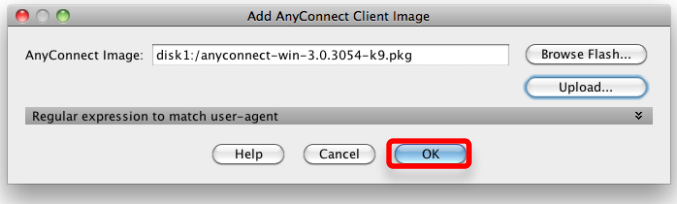
- Wizard を使用しての AnyConnect の設定 (続き)

  [Add] をクリックし、ダウンロードしておいた AnyConnect イメージをアップロードします。

  [Upload] をクリックし、AnyConnect イメージを指定し [Upload File] をクリックします。アップロード完了後、[OK]をクリックします。







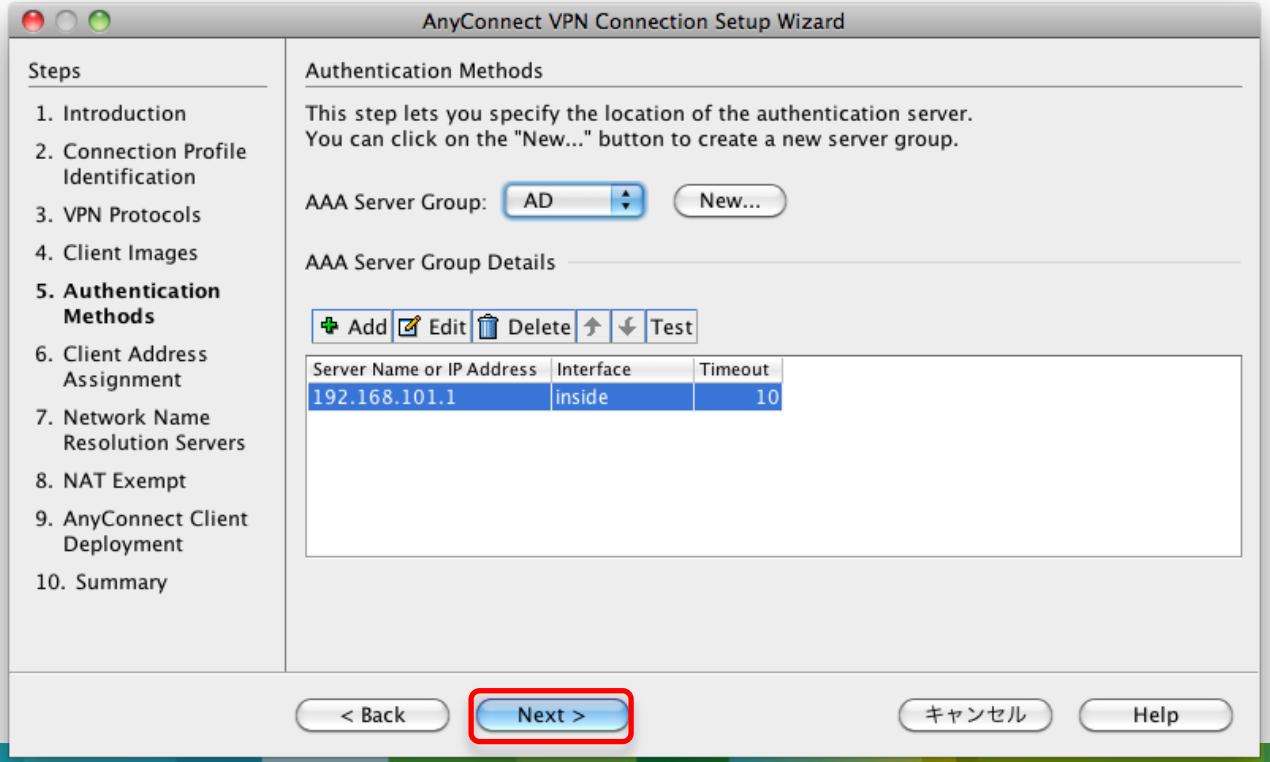
[Next] をクリックし、次のページに進みます。

VPN 設定: AnyConnect

- Wizard を使用しての AnyConnect の設定 (続き)

  AAA Server Group: で、前で作成した外部ユーザー認証 (Ex. AD) を選択し、

  [Next] をクリックし、次のページに進みます。

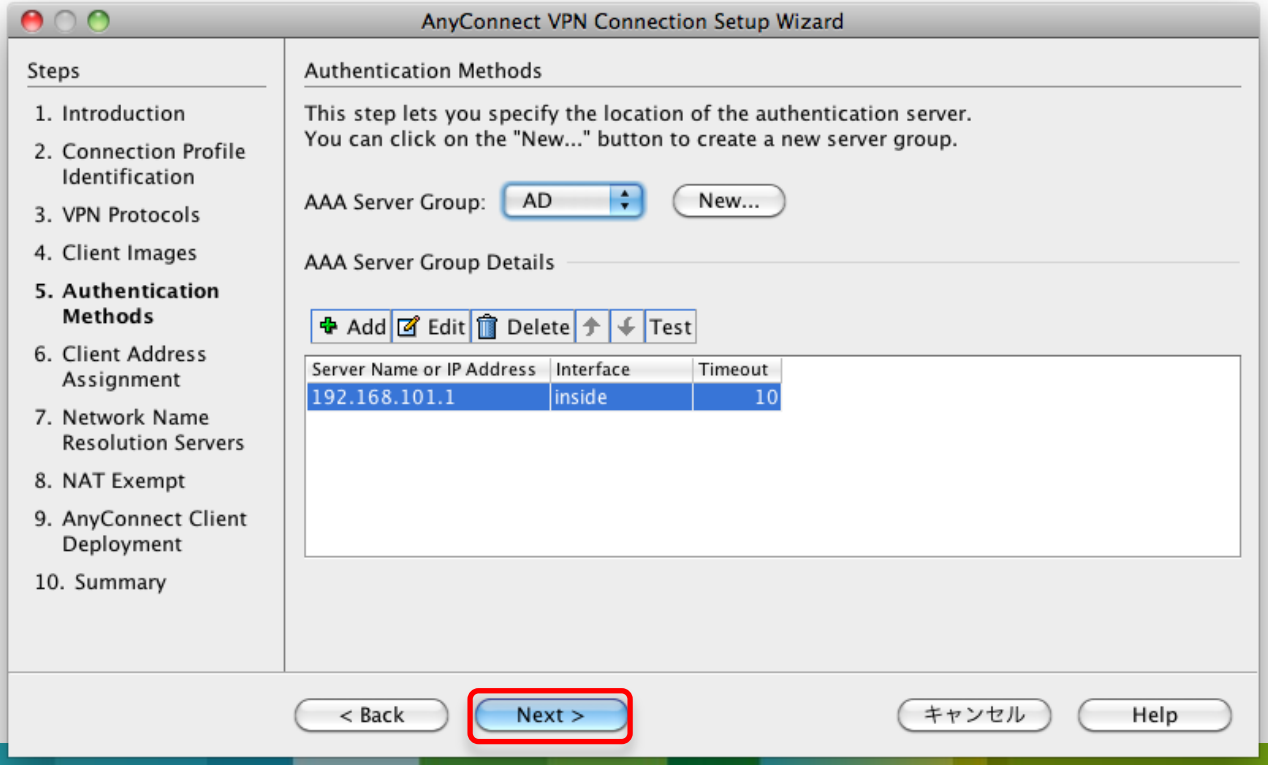


VPN 設定: AnyConnect

- Wizard を使用しての AnyConnect の設定 (続き)

  IP v4 Address Pool で、前で作成したアドレスプール (Ex. vpn_pool) を選択し、

  [Next] をクリックし、次のページに進みます。

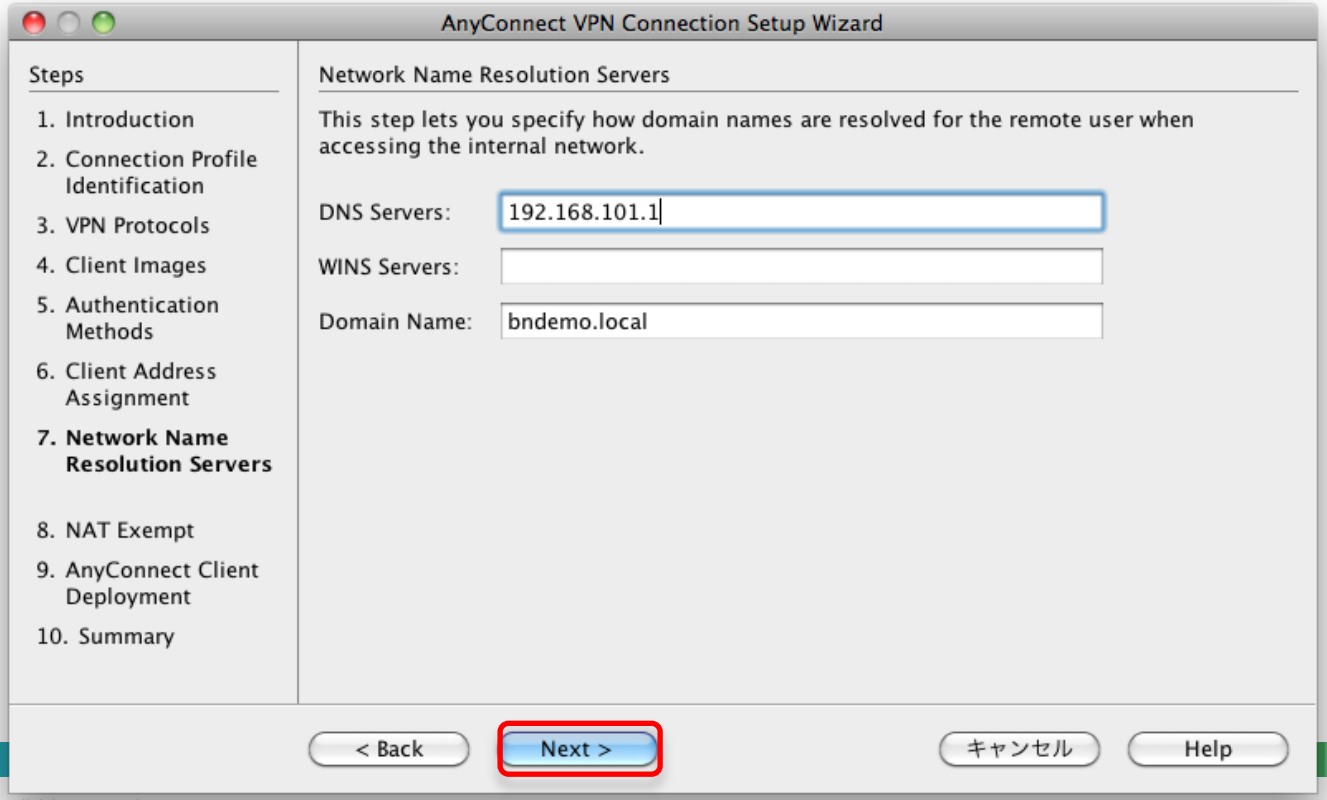


VPN 設定: AnyConnect

- Wizard を使用しての AnyConnect の設定 (続き)

  DNS Servers: (Ex. 192.168.101.1)、WINS Servers: (Ex. なし)を入力し、

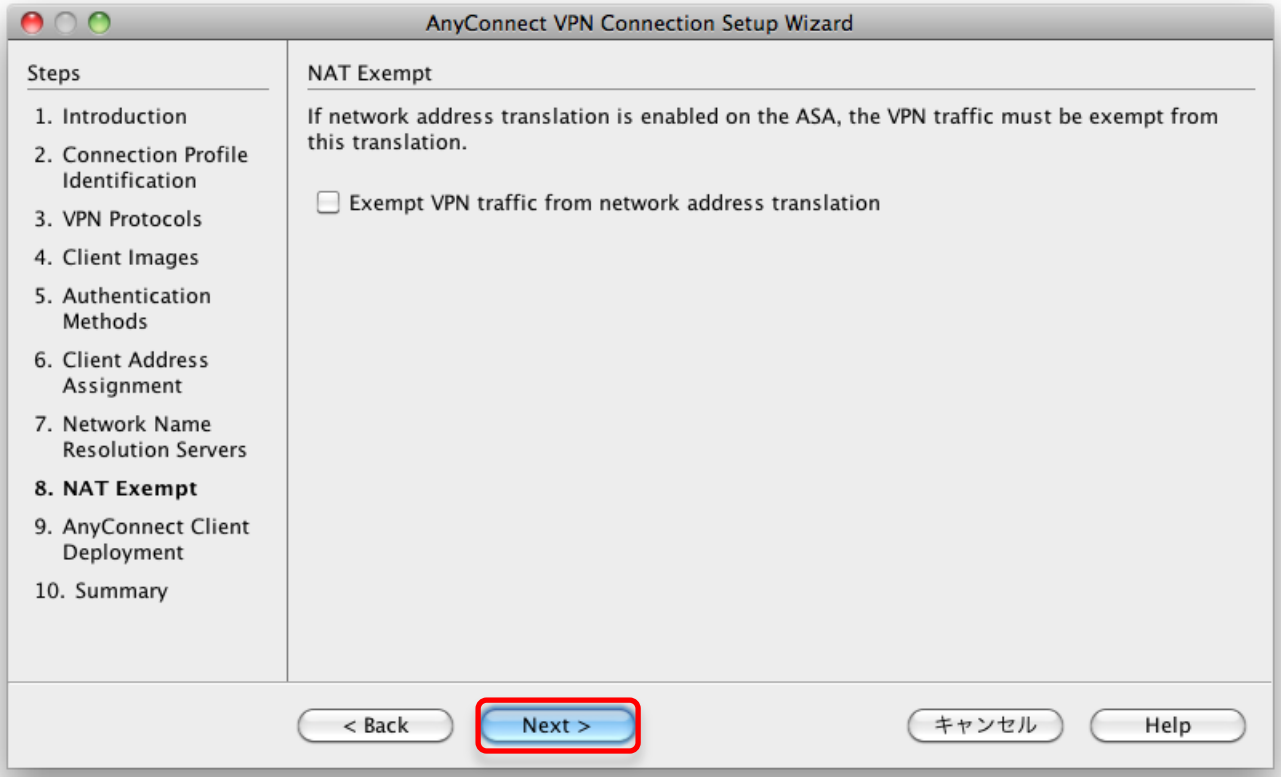
  [Next] をクリックし、次のページに進みます。



VPN 設定: AnyConnect

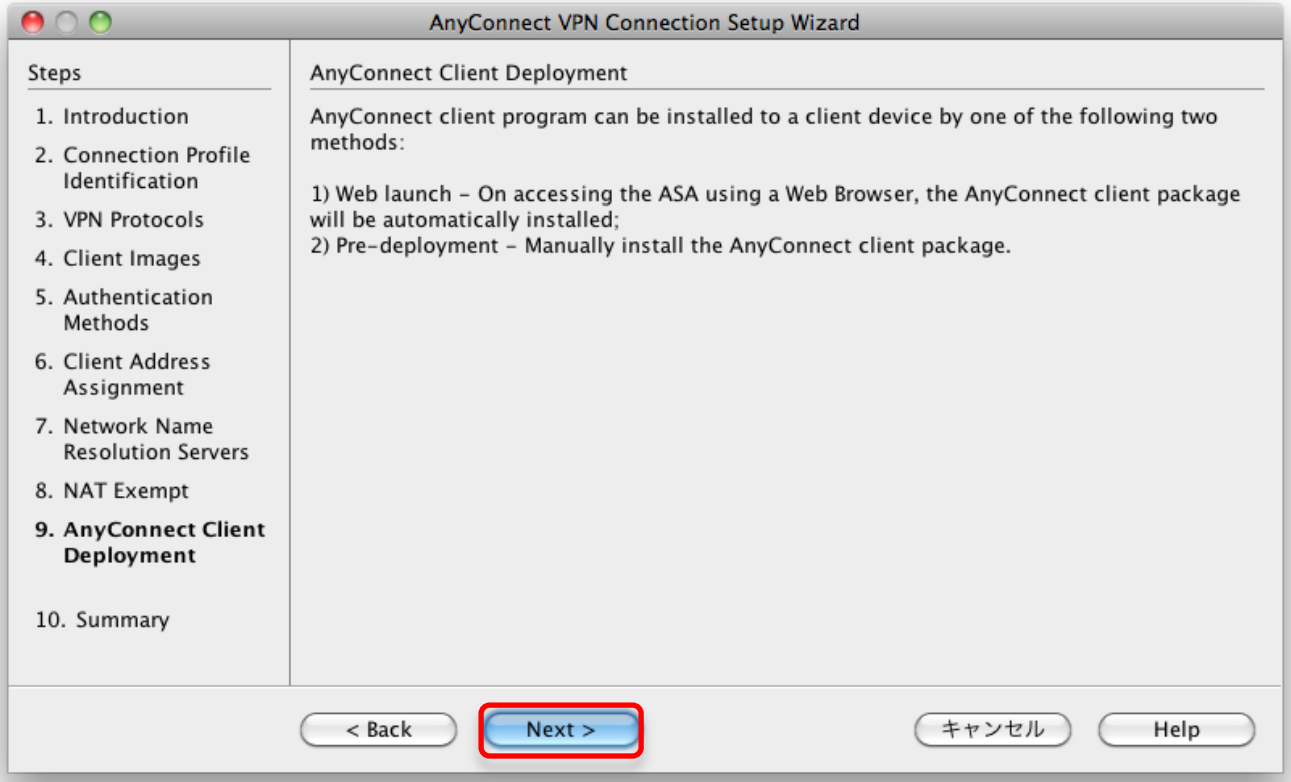
- Wizard を使用しての AnyConnect の設定 (続き)

  既に、NAT の設定は完了しているので今回はこのまま [Next] をクリックし、次のページに進みます。



VPN 設定: AnyConnect

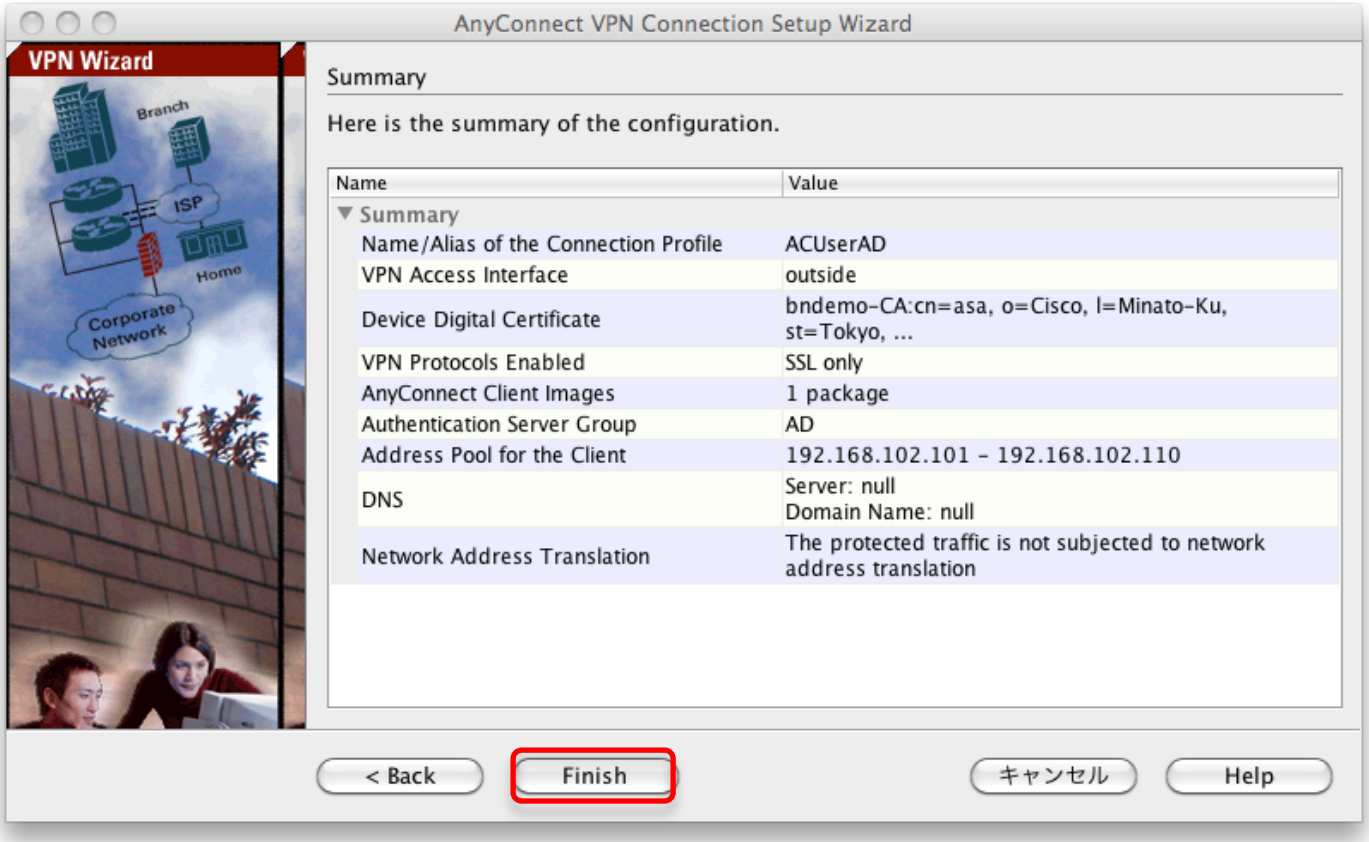
- Wizard を使用しての AnyConnect の設定 (続き)
  AnyConnect Client が記載されたページが表示されます。
  [Next] をクリックし、次のページに進みます。



VPN 設定: AnyConnect

- Wizard を使用しての AnyConnect の設定 (続き)

  最後に確認ページが表示されます。 [Finish] をクリックし、設定を完了します。



Thank you.