

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

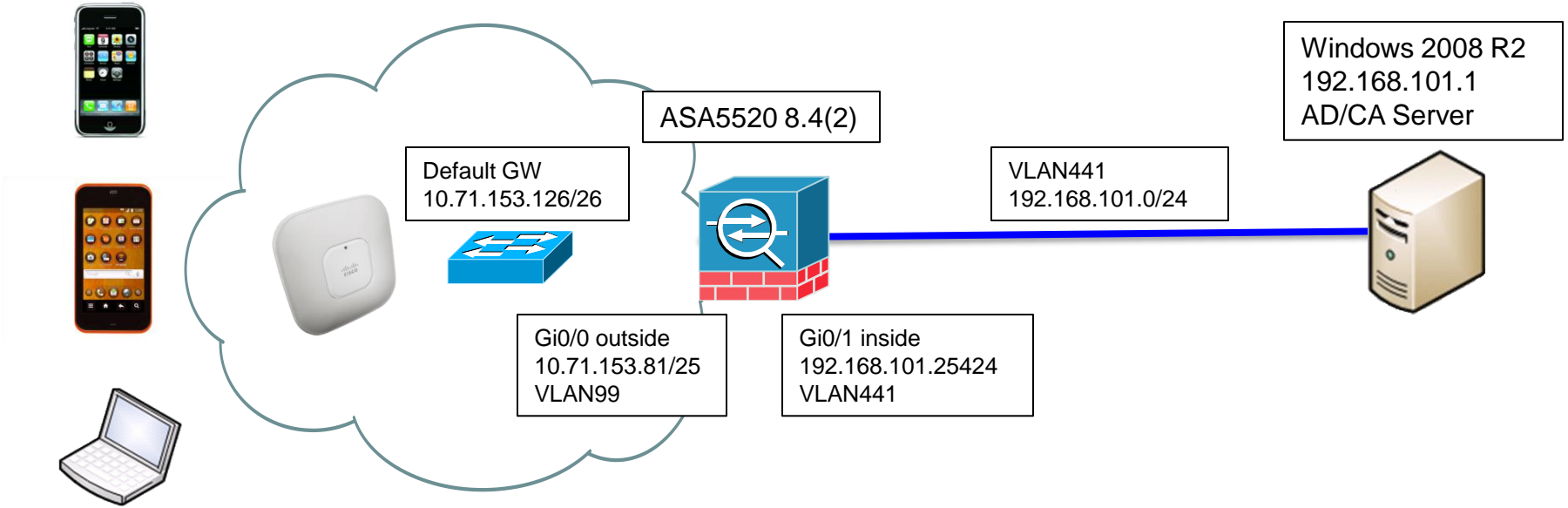
b) L2TP/IPSec 設定

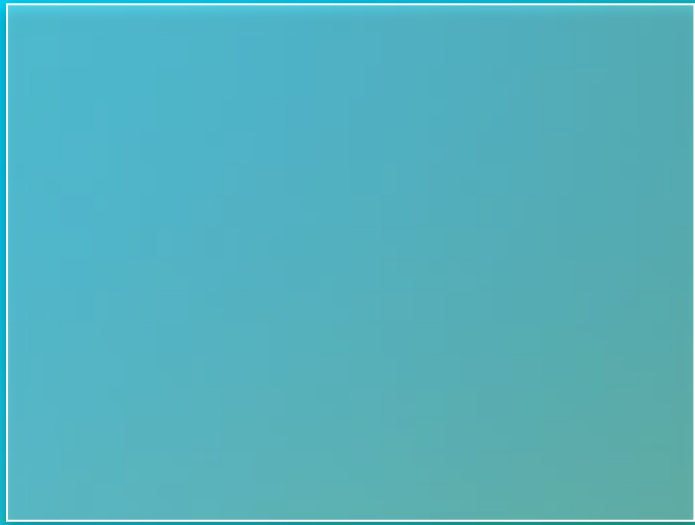
4. 補足説明

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

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

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

基本設定 - ASDM の起動

- ASDM を起動。

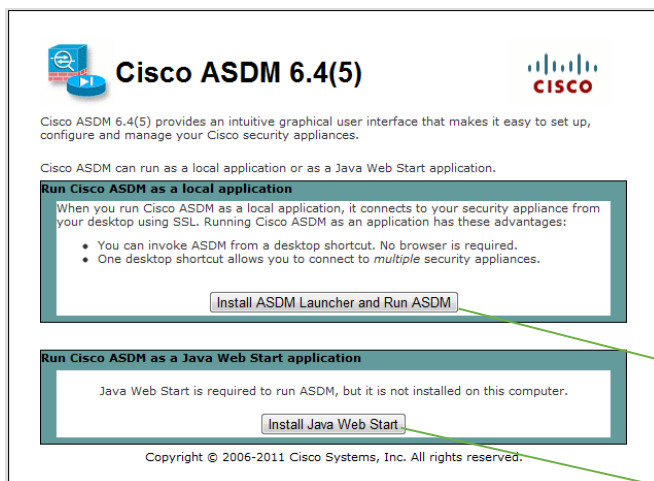
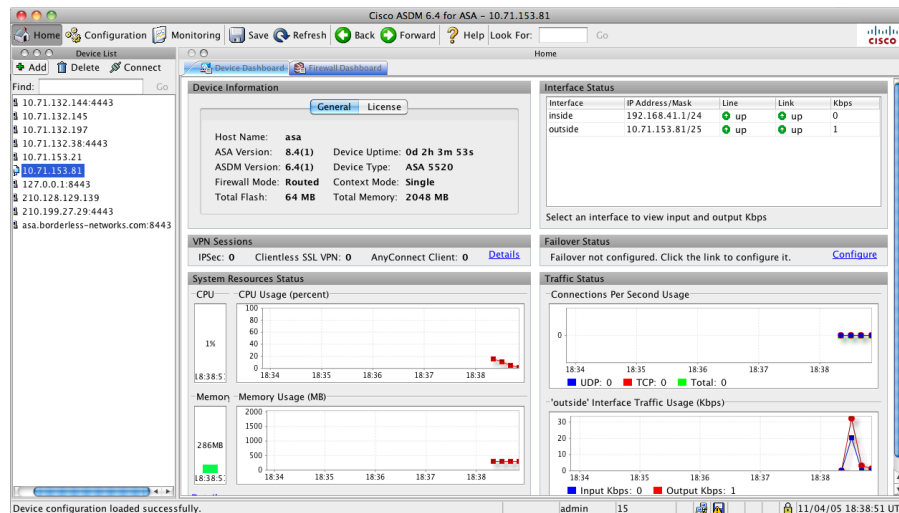
ブラウザーより、<https://<server address>> <https://192.168.101.254> にアクセス

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

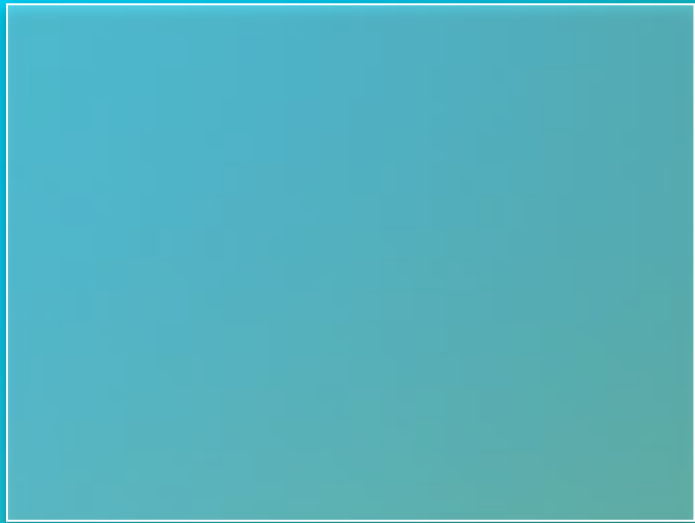
ラウンチャをインストールせず実行する場合

基本設定

- ASDM設定内容を事前表示

- 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

The screenshot displays the Cisco ASDM 6.4 for ASA interface. The 'Tools' menu is open, and the 'Preferences...' option is selected. The 'Preferences' dialog box is shown in the foreground, with the 'General' tab active. The 'Preview commands before sending them to the device' checkbox is checked and highlighted with a green box. A callout box points to this checkbox with the text '設定を送信する前にコマンドを表示させる'. The background shows the ASDM interface with various system monitors and a menu open.



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

The screenshot shows the Cisco ASA configuration interface. On the left, the 'Device List' and 'Device Management' tree are visible. The 'Device Management' tree is expanded to 'Users/AAA' > 'User Accounts'. The main pane shows the 'User Accounts' configuration page with the following table:

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
admin	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy...
enable_15	15	Full	N/A	N/A

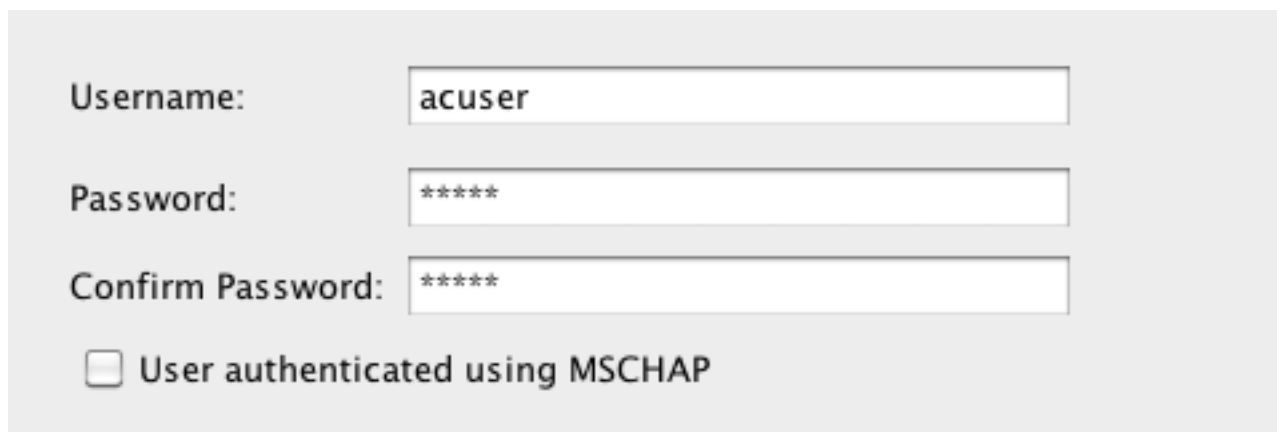
The 'Add' button is highlighted with a red box. Below the table, there is a 'Find:' search bar and 'Match Case' checkbox. At the bottom, there are 'Reset' and 'Apply' buttons.

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**



Username:

Password:

Confirm Password:

User authenticated using MSCHAP

[Apply] をクリックし、設定を反映

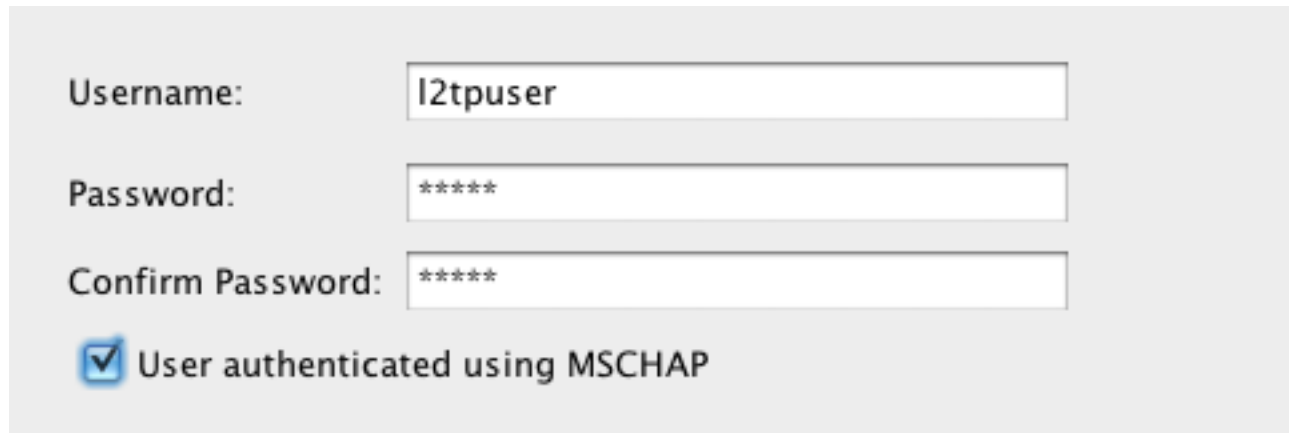
基本設定：ローカルユーザ作成 L2TP

- 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



Username:

Password:

Confirm Password:

User authenticated using MSCHAP

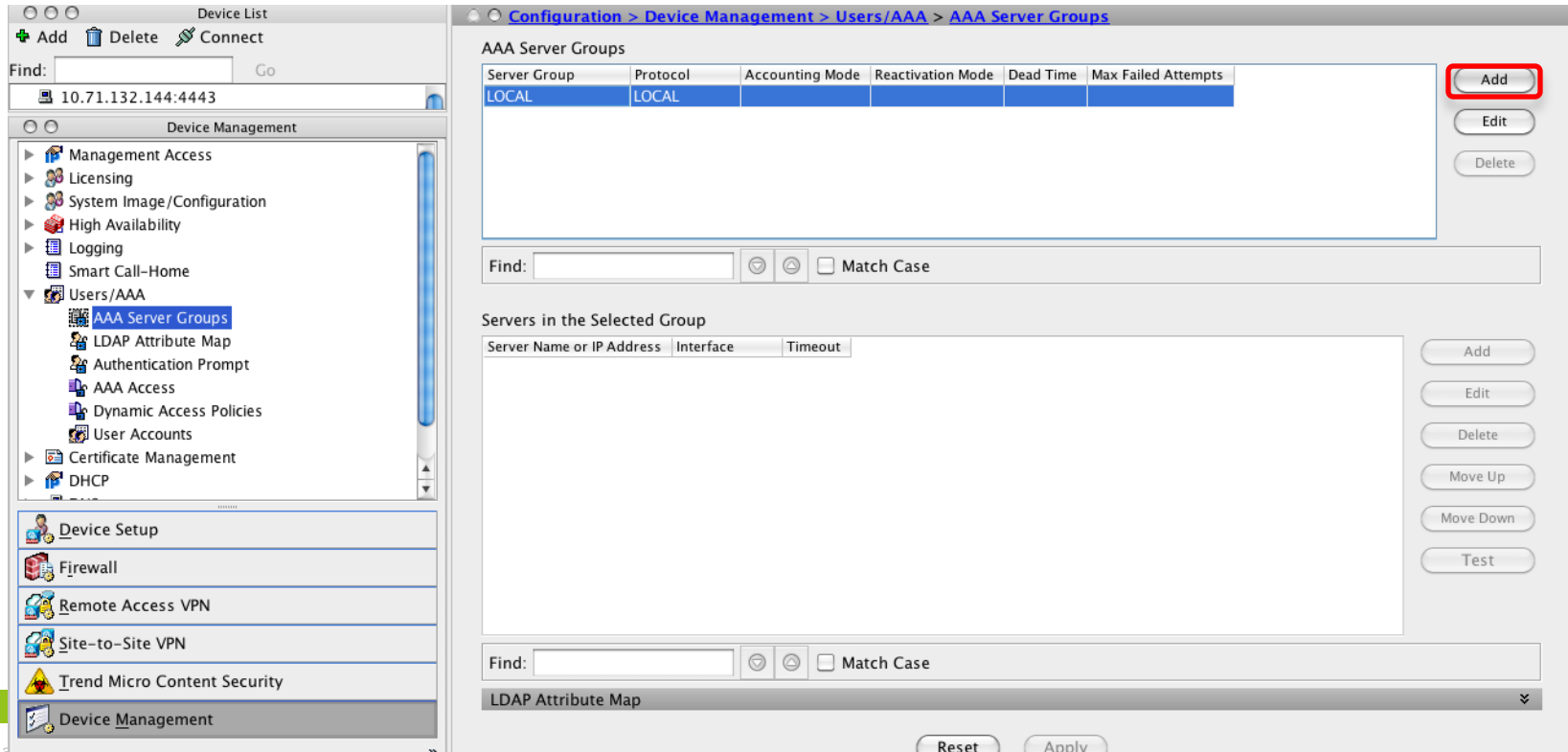
[Apply] をクリックし、設定を反映

基本設定: Windows AD の設定

- リモートログインユーザの使用のための設定

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。

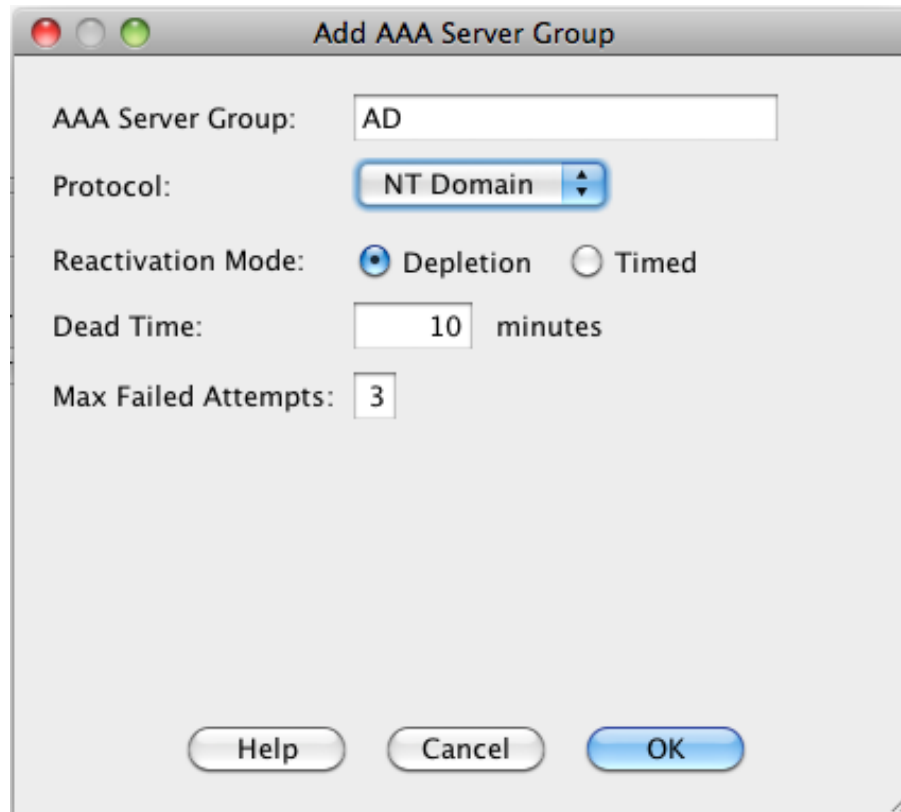
Configuration -> Device Management-> Users/AAA -> AAA Server Groups を選択し、[Add] ボタンをクリック。



基本設定: Windows AD の設定

- リモートログインユーザの使用のための設定 (続き)

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



AAA Server Group: AD

Protocol: NT Domain

Reactivation Mode: Depletion Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

Help Cancel OK

基本設定: Windows AD の設定

- リモートログインユーザの使用のための設定 (続き)

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

The screenshot shows the Cisco IOS configuration interface. On the left, the 'Device Management' tree is expanded to 'Users/AAA' > 'AAA Server Groups'. The main window displays the configuration for 'AAA Server Groups' with a table of existing groups:

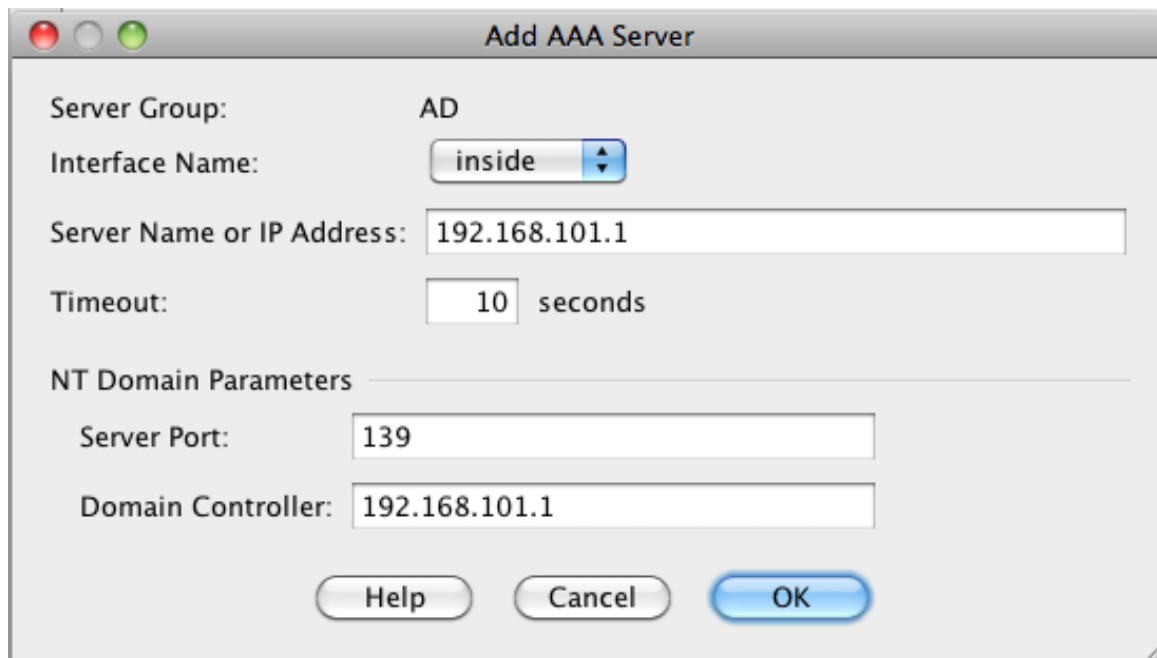
Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				
AD	NT Domain		Depletion	10	3

Below the table is a search field and a 'Match Case' checkbox. Underneath, the 'Servers in the Selected Group' section is visible, featuring an empty table with columns for 'Server Name or IP Address', 'Interface', and 'Timeout'. The 'Add' button in this section is highlighted with a red rectangle. At the bottom of the configuration window are 'Reset' and 'Apply' buttons.

基本設定: Windows AD の設定

- リモートログインユーザの使用のための設定 (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。



The screenshot shows a dialog box titled "Add AAA Server" with the following configuration:

- Server Group: AD
- Interface Name: inside
- Server Name or IP Address: 192.168.101.1
- Timeout: 10 seconds
- NT Domain Parameters section:
 - Server Port: 139
 - Domain Controller: 192.168.101.1

Buttons at the bottom: Help, Cancel, OK.

[Apply] をクリックし、設定を反映



1. 基本設定

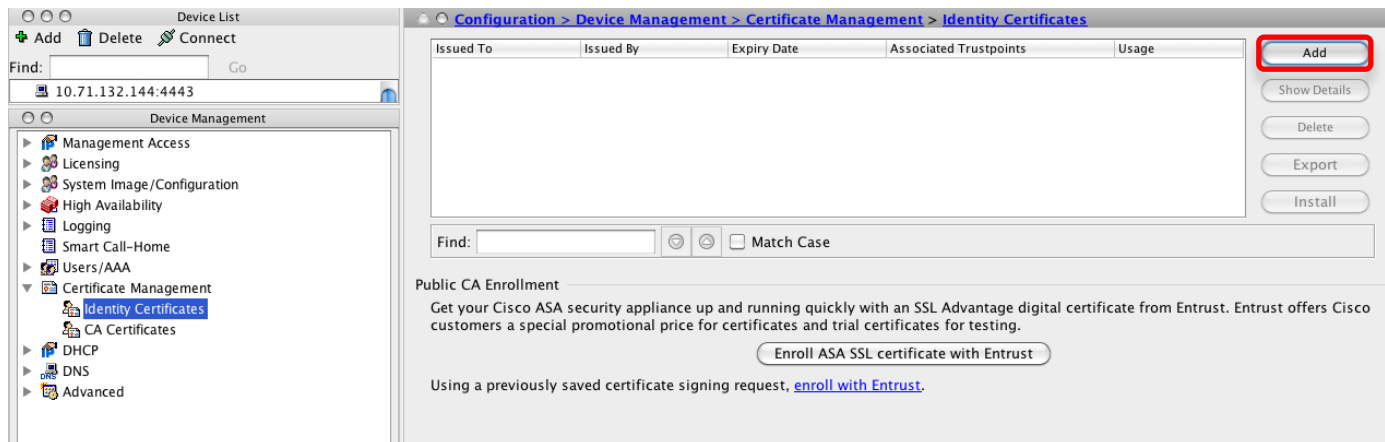
c) 証明書設定

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。



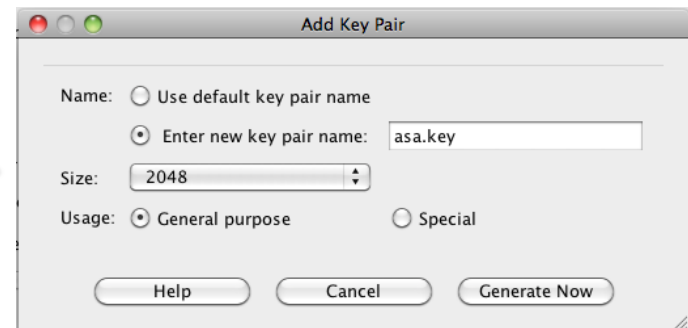
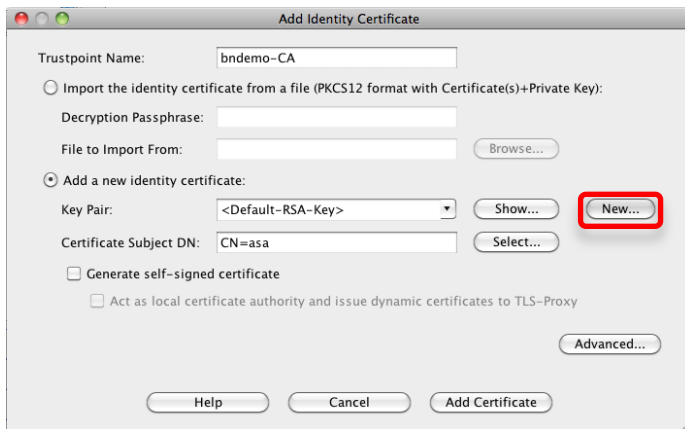
基本設定：証明書の設定 – CSR 作成

- 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。)、

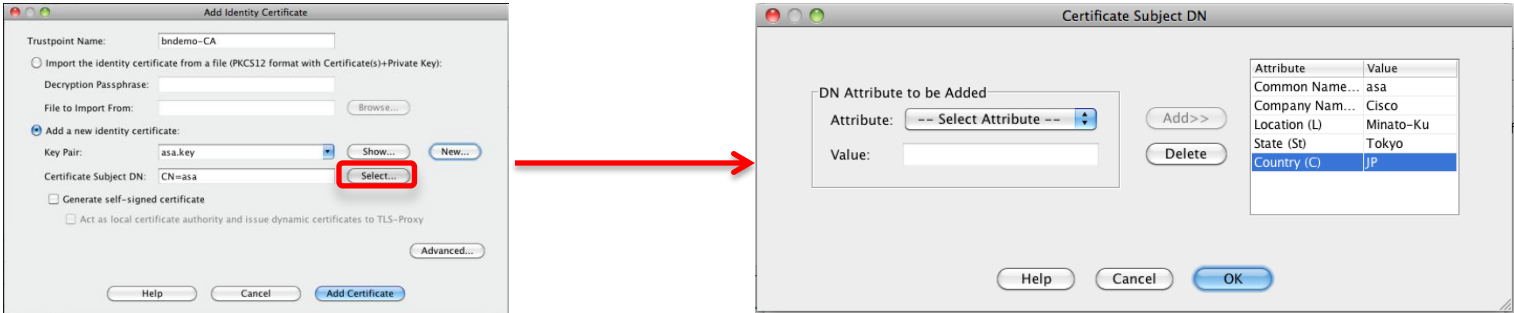


基本設定：証明書の設定 – CSR 作成

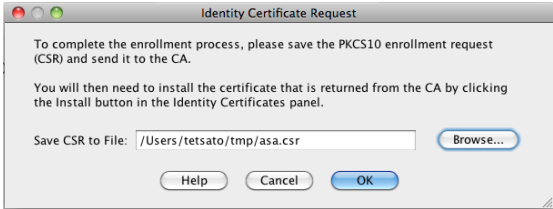
- 証明書の設定 – CSR 作成 (続き)

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、証明書を手入して下さい。

基本設定：証明書の設定 - CA局に申請

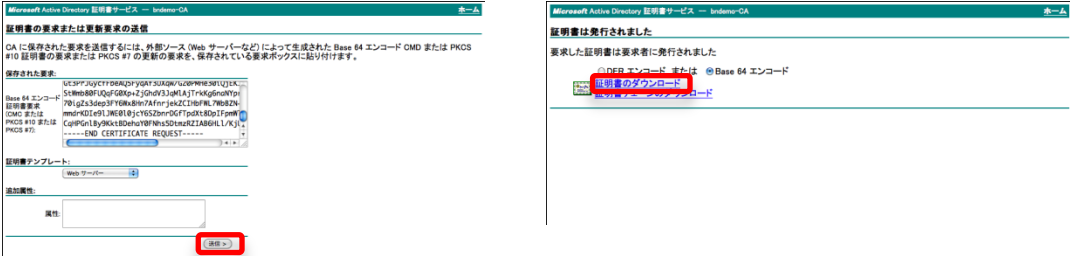
- 認証局 Windows CA の場合

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

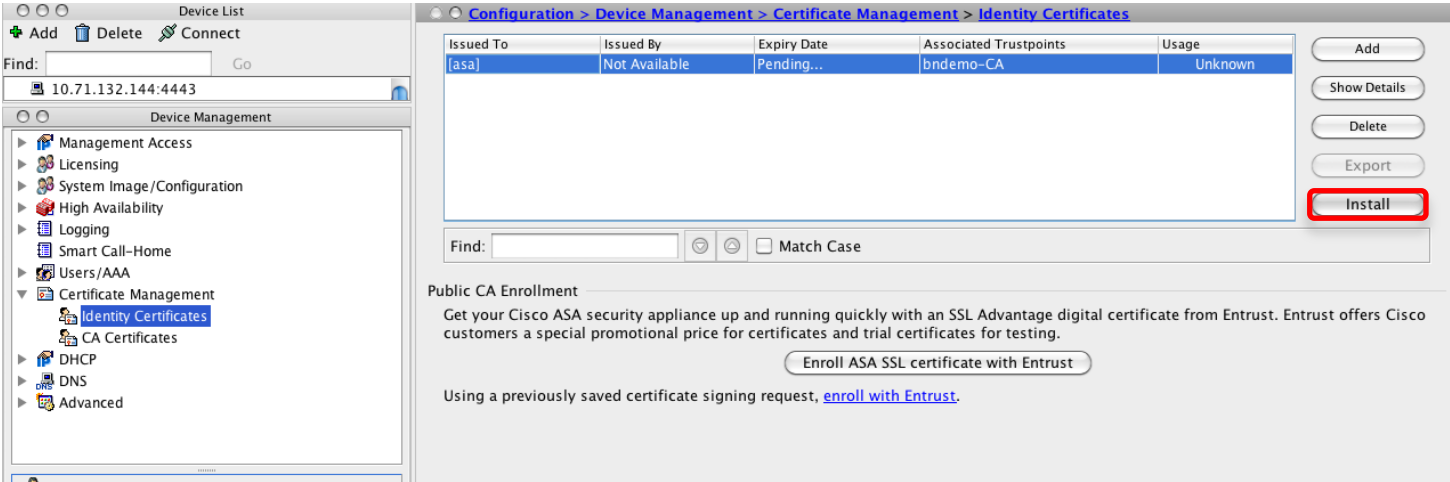
<http://www.cybertrust.ne.jp/deviceid/CybertrustDeviceIDPublicCAG1.crt>

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。

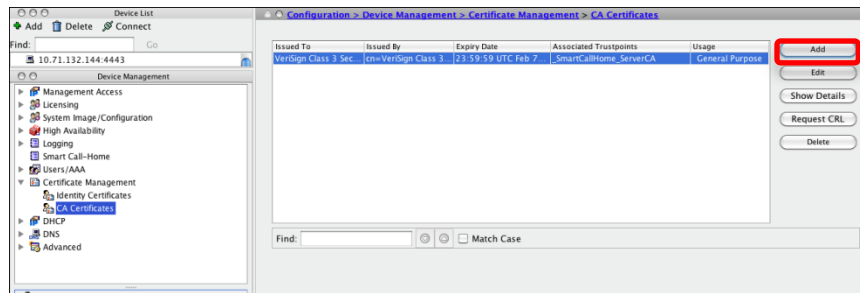


[Install from a file] で、ASA の証明を指定し、 [Install Certificate] をクリック。

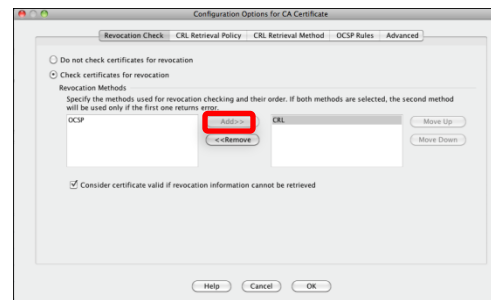
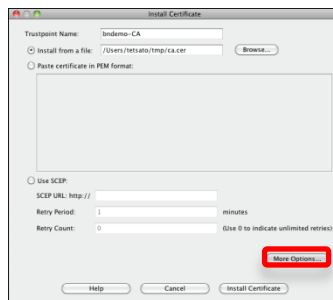
基本設定：証明書の設定 - 証明書のインストール

- 入手した、ASAの証明書、CA 証明書をインストール (続き)

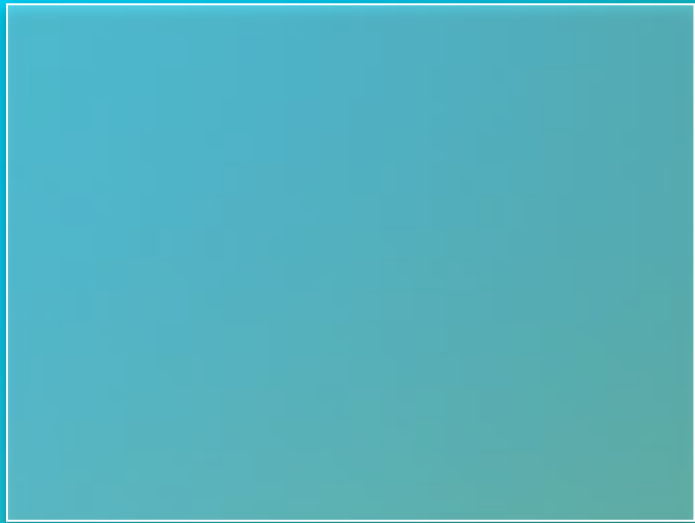
Configuration -> Device Management-> Certificate Management -> CA Certificates を選択し、[Add] ボタンをクリック。



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

		Netmask	Description	Object NAT Address
▼ IPv4 Network Objects				
any	0.0.0.0	0.0.0.0		
inside-ne...	192.168.41.0	255.255.255.0		
outside-n...	10.71.153.0	255.255.255....		
▼ IPv6 Network Objects				
any	::	0		

(*) 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](#)

The screenshot shows a dialog box titled "Add Network Object". It contains the following fields and controls:

- Name:** A text input field containing "vpn_clients".
- Type:** A dropdown menu with "Range" selected.
- Start Address:** A text input field containing "192.168.102.101".
- End Address:** A text input field containing "192.168.102.110".
- Description:** An empty text input field.
- NAT:** A dashed box containing the text "NAT" and a small downward arrow.
- Buttons:** "Help", "Cancel", and "OK" buttons at the bottom.

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

Configure named IP Address Pools. The IP Address Pools can be used in either a VPN [IPsec\(IKEv1\) Connection Profiles](#), [AnyConnect Connection Profiles](#) or [Group Policies](#) configuration.

Add Edit Delete

Pool Name	Starting Address	Ending Address/Number of Addresses	Subnet Mask/Prefix Length
-----------	------------------	------------------------------------	---------------------------

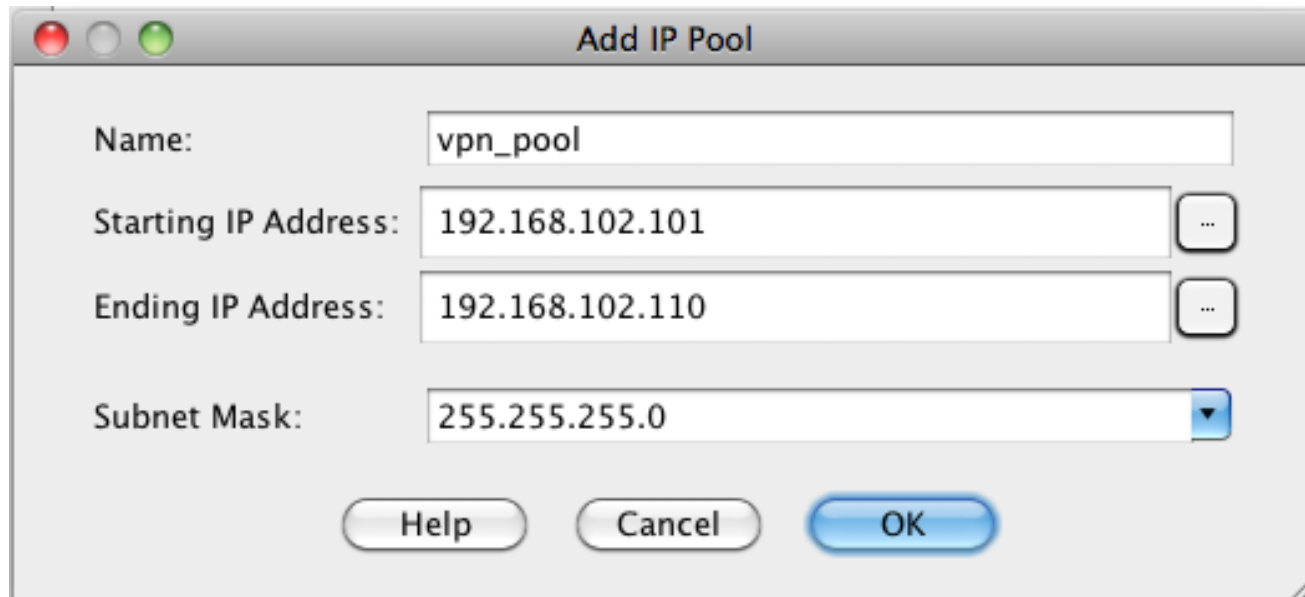
(*) 注意
以下の設定の順番通りに設定でしないと
エラーが出ます。(CSCtn96841)
Network Object の設定
アドレスプールの設定
NAT の設定

基本設定: アドレスプール – 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`



The screenshot shows a dialog box titled "Add IP Pool". It contains the following fields and values:

- Name: `vpn_pool`
- Starting IP Address: `192.168.102.101`
- Ending IP Address: `192.168.102.110`
- Subnet Mask: `255.255.255.0`

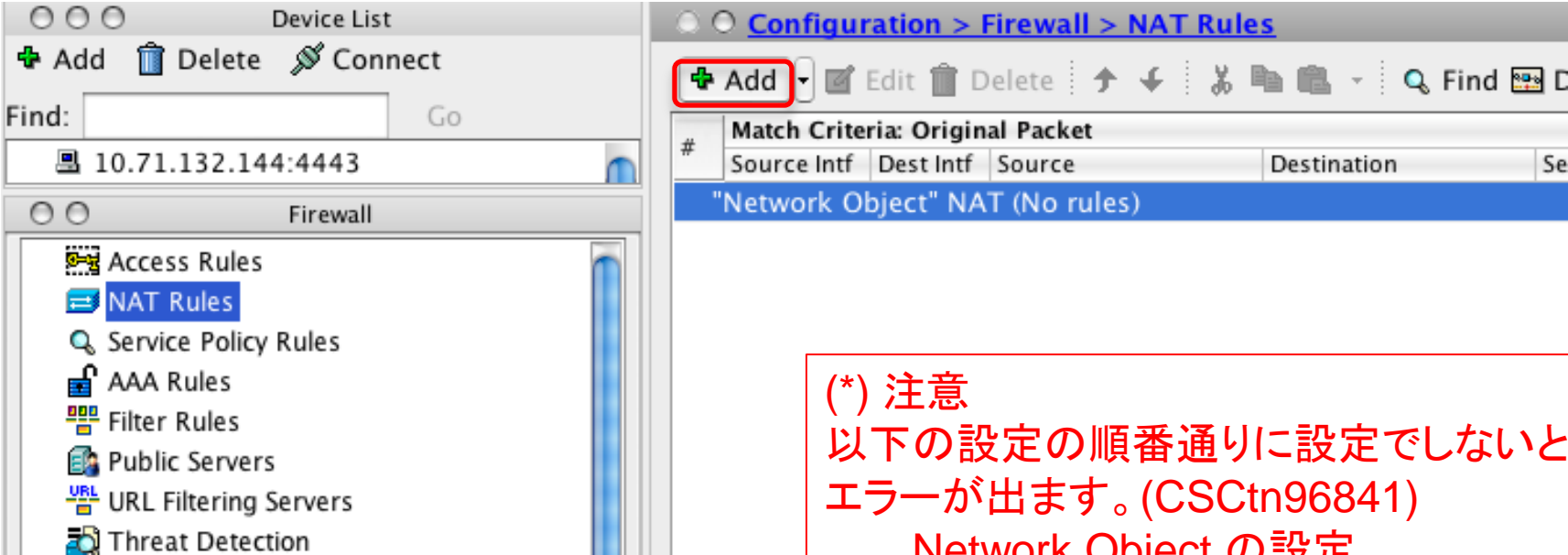
At the bottom of the dialog, there are three buttons: "Help", "Cancel", and "OK".

[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

Match Criteria: Original Packet

Source Interface: outside Destination Interface: inside

Source Address: vpn_clients Destination Address: any

Service: any

Action: Translated Packet

Source NAT Type: Static

Source Address: -- Original -- Destination Address: -- Original --

PAT Pool Translated Address: Service: -- Original --

Round Robin

Fall through to interface PAT

Options

Enable rule

Translate DNS replies that match this rule

Disable Proxy ARP on egress interface

Lookup route table to locate egress interface

Direction: Both

Description:

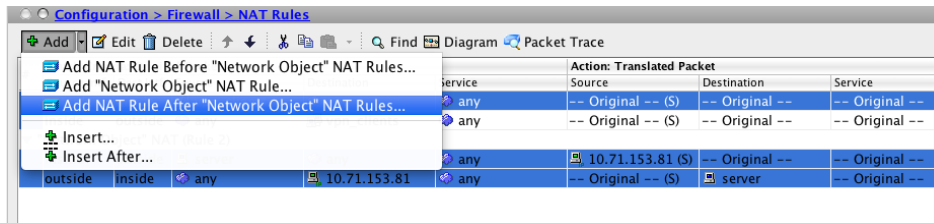
Help Cancel OK

[Apply] をクリックし、設定を反映

基本設定: NAT (Option)

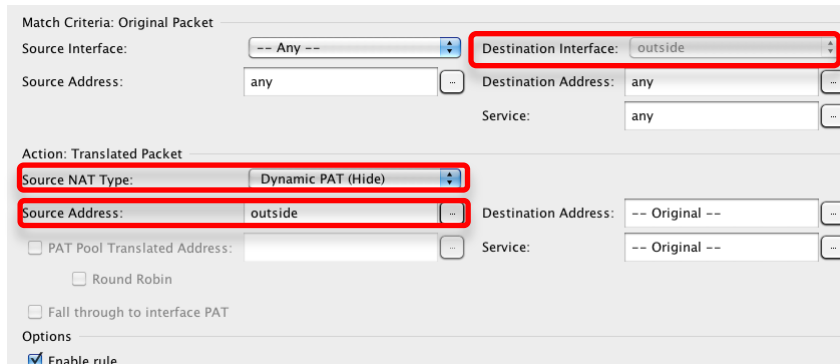
- 内部からの通信を NAT する為の設定 (Option)

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。

The screenshot shows the Cisco configuration interface. On the left, the 'Device Setup' menu is visible with 'Interfaces' selected. The main area displays a table of interfaces with the following data:

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Type
GigabitEthernet0/0	outside	Enabled	0	10.71.153.80	255.255.255...		Hardware
GigabitEthernet0/1	inside	Enabled	100	192.168.101.254	255.255.255.0		Hardware
GigabitEthernet0/2		Disabled					Hardware
GigabitEthernet0/3		Disabled					Hardware
Management0/0		Disabled					Hardware

At the bottom of the interface, there are two checkboxes:

- Enable traffic between two or more interfaces which are configured with same security levels
- Enable traffic between two or more hosts connected to the same interface

[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。

The screenshot shows the Cisco configuration interface. On the left, the 'Device List' window shows a search for '10.71.132.144:4443'. Below it, the 'Device Setup' window shows a tree view with 'Routing' expanded and 'Static Routes' selected. The main window is titled 'Configuration > Device Setup > Routing > Static Routes' and contains the following content:

Specify static routes.
Filter: Both IPv4 only IPv6 only

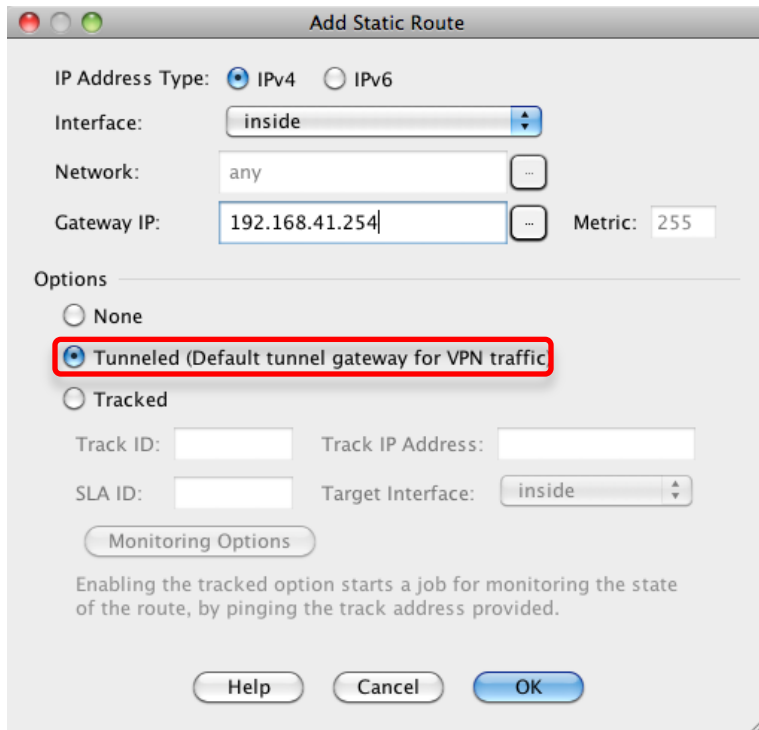
Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options
inside	192.168.0.0	255.255.0.0	192.168.41.254	1	None
outside	0.0.0.0	0.0.0.0	10.71.153.126	1	None

On the right side of the main window, there are three buttons: 'Add' (highlighted with a red box), 'Edit', and 'Delete'.

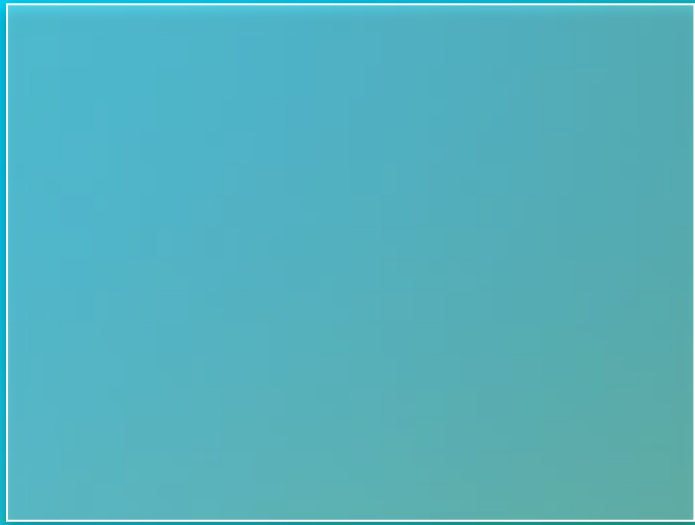
基本設定: トンネルルート (Option)

- 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



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Settings

AnyConnect Client Images

Cisco AnyConnect Client packages can be downloaded from the Cisco Web using the search string 'AnyConnect VPN Client'. The regular expression is used to match the user-agent of a browser to an image.

You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

Note: The Cisco AnyConnect 2.5 Client can be downloaded from this link after log on to CCO: [AnyConnect 2.5 download](#)

+ Add Replace Delete Up Down

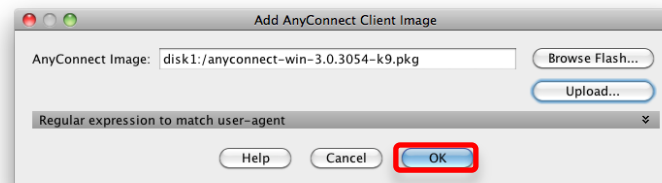
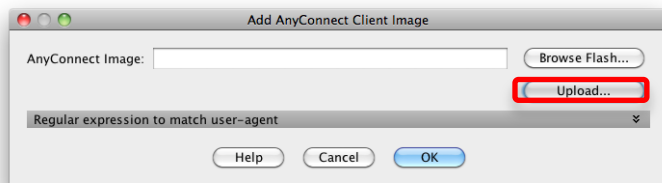
Image	Regular expression to match user-agent
-------	--

(*)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

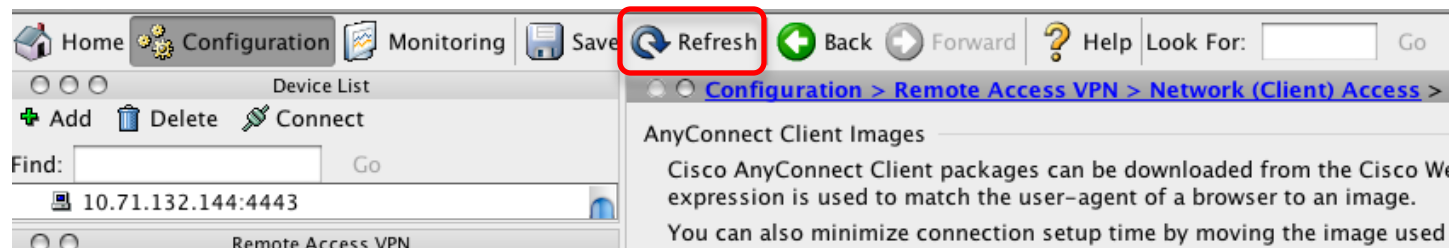
- AnyConnect の設定 - Image (続き)

[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

The screenshot shows the configuration interface for AnyConnect. On the left, a tree view under 'Remote Access VPN' shows 'Network (Client) Access' expanded, with 'Group Policies' selected. The main pane displays the 'Group Policies' configuration page. At the top, there is a description: 'Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts. To enforce authorization attributes from an LDAP server you must use an [LDAP attribute map](#).' Below this is a toolbar with buttons for 'Add', 'Edit', 'Delete', and 'Assign'. The 'Add' button is highlighted with a red box. Below the toolbar is a table with the following data:

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultWEBV...

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。

The screenshot shows the configuration page for a Group Policy. The left sidebar has 'General' selected. The main area has the following settings:

- Name: GroupPolicyAC
- Banner: Inherit
- SCEP forwarding URL: Inherit
- Address Pools: Inherit, vpn_pool (selected)
- IPv6 Address Pools: Inherit
- More Options:
 - Tunneling Protocols: Inherit, Clientless SSL VPN, SSL VPN Client, IPsec IKEv1, IPsec IKEv2, L2TP/IPsec
 - IPv4 Filter: Inherit

[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。

The screenshot shows the configuration page for AnyConnect Connection Profiles. The 'Access Interfaces' section is highlighted with a red box, containing the following table:

Interface	SSL Access	Enable DTLS	IPsec (IKEv2) Access	Allow Access	Enable Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The 'Device Certificate...' button is highlighted with a red box, and a red arrow points to the 'Specify Device Certificate' dialog box. The dialog box shows the following information:

Device certificate is a digital certificate that identifies this ASA to the clients.
 Device Certificate: `bndemo-CA:cn=asa, o=Cisco, l=Minato-Ku, st=Tokyo, ...`
 Buttons: Help, Cancel, OK

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。

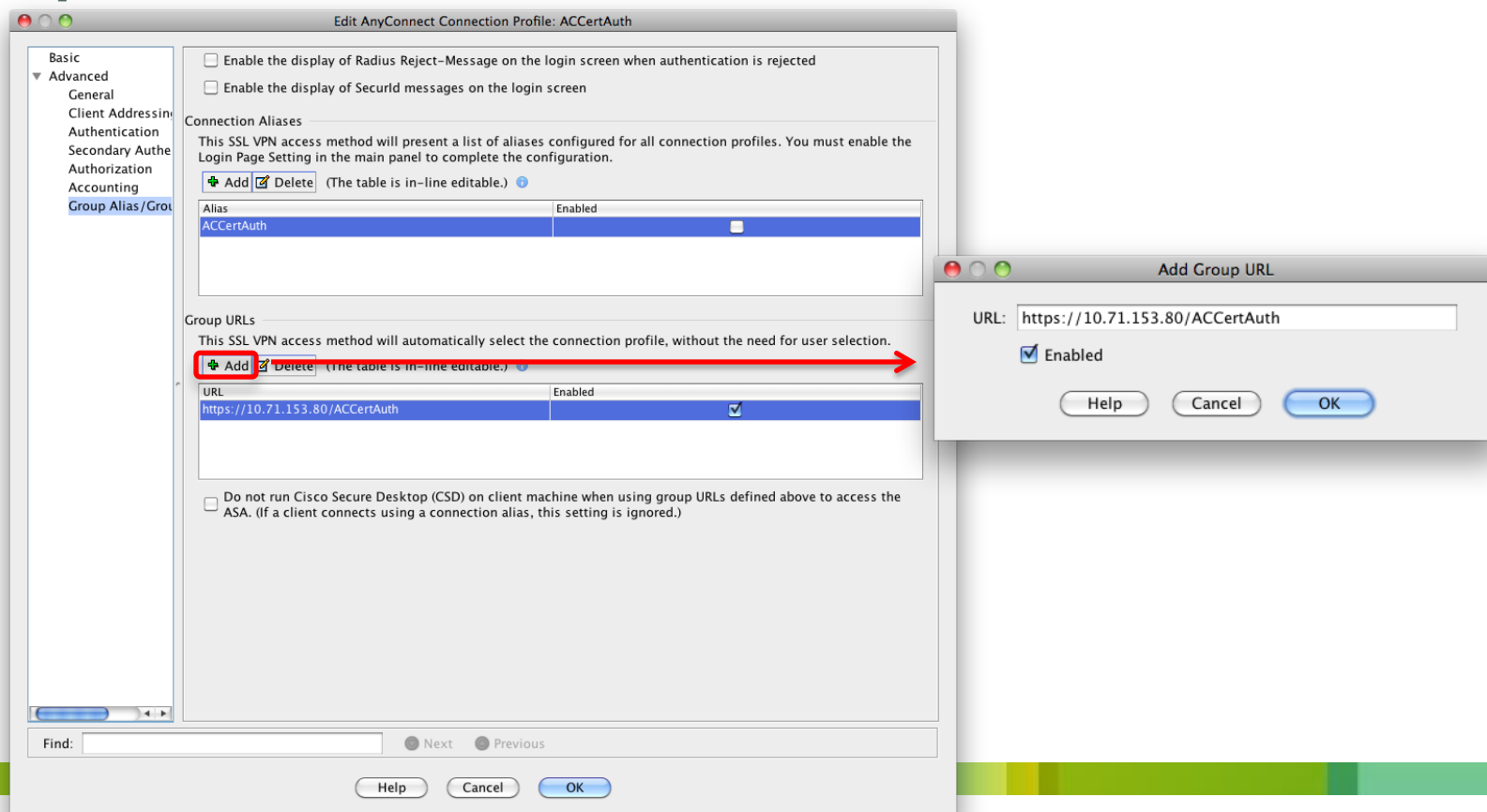
The screenshot shows the 'Edit AnyConnect Connection Profile: ACCertAuth' window. The 'Basic' tab is selected, and the 'Advanced' tab is collapsed. The configuration fields are as follows:

- Name: ACCertAuth
- Aliases: (empty)
- Authentication Method: Certificate (selected), AAA, Both
- AAA Server Group: LOCAL (dropdown), Manage...
- Use LOCAL if Server Group fails: (unchecked)
- Client Address Assignment: DHCP Servers: (empty)
- Client Address Pools: None (selected), DHCP Link, DHCP Subnet
- Client IPv6 Address Pools: (empty), Select...
- IPv6 address pool is only supported for SSL.
- Default Group Policy: Group Policy: GroupPolicyAC (dropdown), Manage...
- (Following fields are attributes of the group policy selected above.)
- Enable SSL VPN client protocol: (checked)
- Enable IPsec(IKEv2) client protocol: (unchecked)
- DNS Servers: 192.168.101.1
- WINS Servers: (empty)
- Domain Name: bndemo.local

At the bottom, there is a 'Find:' field, 'Next' and 'Previous' buttons, and 'Help', 'Cancel', and 'OK' buttons.

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。

The screenshot shows the 'Edit AnyConnect Connection Profile: ACUserAuthLocal' window. The 'Basic' tab is selected, and the 'Advanced' section is expanded. The configuration is as follows:

- Name:** ACUserAuthLocal
- Aliases:** ACUserAuthLocal
- Authentication Method:** AAA (selected), Certificate, Both
- AAA Server Group:** LOCAL (selected), with a 'Manage...' button and a checkbox for 'Use LOCAL if Server Group fails'.
- Client Address Assignment:**
 - DHCP Servers:** (empty field)
 - Client Address Pools:** (empty field) with a 'Select...' button.
 - Client IPv6 Address Pools:** (empty field) with a 'Select...' button.
 - Note: IPv6 address pool is only supported for SSL.
- Default Group Policy:**
 - Group Policy:** GroupPolicyAC (selected), with a 'Manage...' button.
 - (Following fields are attributes of the group policy selected above.)
 - Enable SSL VPN client protocol
 - Enable IPsec(IKEv2) client protocol
 - DNS Servers:** 192.168.101.1
 - WINS Servers:** (empty field)
 - Domain Name:** bndemo.local

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。

The screenshot displays the configuration window for 'Edit AnyConnect Connection Profile: ACUserAuthLocal'. The left sidebar shows the navigation tree with 'Group Alias/Group URL' selected. The main panel is divided into sections: 'Basic', 'Advanced', 'Client Addressing', 'Authentication', 'Secondary Authentication', 'Authorization', 'Accounting', and 'Group Alias/Group URL'. The 'Group URLs' section is active, showing a table with one entry: 'https://10.71.153.80/ACUserAuthLocal' with the 'Enabled' checkbox checked. A red arrow points to the 'Add' button in the 'Group URLs' section. An 'Add Group URL' dialog box is overlaid on top, with the URL field containing 'https://10.71.153.80/ACUserAuthLocal' and the 'Enabled' checkbox checked. The dialog box has 'Help', 'Cancel', and 'OK' buttons.

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。

Basic
▶ Advanced

Name: ACUserAD
Aliases: ACUserAD

Authentication
Method: AAA Certificate Both
AAA Server Group: AD
 Use LOCAL if Server Group fails

Client Address Assignment
DHCP Servers:
 None DHCP Link DHCP Subnet
Client Address Pools:
Client IPv6 Address Pools:
IPv6 address pool is only supported for SSL.

Default Group Policy
Group Policy: GroupPolicyAC
(Following fields are attributes of the group policy selected above.)
 Enable SSL VPN client protocol
 Enable IPsec(IKEv2) client protocol
DNS Servers: 192.168.101.1
WINS Servers:
Domain Name: bndemo.local

Find: Next Previous

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。

The screenshot displays the 'Edit AnyConnect Connection Profile: ACUserAD' window. The left sidebar shows the navigation menu with 'Group Alias/Group URL' selected. The main panel is divided into two sections: 'Connection Aliases' and 'Group URLs'. The 'Group URLs' section has a red box around the 'Add' button, with a red arrow pointing to the 'Add Group URL' dialog box. The dialog box shows the URL 'https://10.71.153.80/ACUserAuthAD' and the 'Enabled' checkbox checked. The 'Add Group URL' dialog box has 'Help', 'Cancel', and 'OK' buttons.

Basic

- Advanced
 - General
 - Client Addressing
 - Authentication
 - Secondary Authentication
 - Authorization
 - Accounting
 - Group Alias/Group URL

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

+ Add [x] Delete (The table is in-line editable.)

Alias	Enabled
ACUserAD	<input checked="" type="checkbox"/>

Group URLs

This SSL VPN access method will automatically select the connection profile, without the need for user selection.

+ Add [x] Delete (The table is in-line editable.)

URL	Enabled
https://10.71.153.80/ACUserAuthAD	<input checked="" type="checkbox"/>

Do not run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored.)

Find: [] ● Next ● Previous

Help Cancel OK

Add Group URL

URL: https://10.71.153.80/ACUserAuthAD

Enabled

Help Cancel OK

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。

Login Page Setting

Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

+ Add Edit Delete Find: Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
ACCertAuth	<input checked="" type="checkbox"/>	<input type="checkbox"/>		Certificate	GroupPolicyAC
ACUserAuthLocal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ACUserAuthLocal	AAA(LOCAL)	GroupPolicyAC
ACUserAD	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ACUserAD	AAA(AD)	GroupPolicyAC
L2TPGroup	<input type="checkbox"/>	<input type="checkbox"/>		AAA(AD)	GroupPolicyL2TP

Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile matches the certificate map will be used.

Reset Apply

[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

Device List
+ Add Delete Connect
Find: Go

Remote Access VPN

- Dynamic Access Policies
- Group Policies
- IPsec(IKEv1) Connection
- Secure Mobility Solution
- Address Assignment
- Advanced
 - Endpoint Security
 - SSL VPN
 - IPsec
 - Crypto Maps
 - IKE Policies**
 - IKE Parameters

Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Policies

Configure specific Internet Key Exchange (IKE) algorithms and parameters, within the IPsec Internet Security Association Key Management Protocol (ISAKMP) framework, for the AH and ESP IPsec protocols.

IKEv1 Policies

+ Add Edit Delete

Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime (seconds)
------------	------------	------	-----------	----------------	--------------------

IKEv2 Policies

+ Add Edit Delete

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: 65335, Authentication: pre-share, Encryption: 3des, D-H Group: 2, Hash: sha

The screenshot shows the 'Add IKE Policy' dialog box with the following settings:

- Priority: 65335
- Authentication: pre-share
- Encryption: 3des
- D-H Group: 2
- Hash: sha
- Lifetime: Unlimited 86400 seconds

Buttons: Help, Cancel, OK

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

The screenshot shows the 'Add IKE Policy' dialog box with the following settings:

- Priority: 65530
- Authentication: rsa-sig
- Encryption: 3des
- D-H Group: 2
- Hash: sha
- Lifetime: Unlimited, 86400, seconds

Buttons: Help, Cancel, OK

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

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

The screenshot shows the Cisco VPN configuration interface. On the left, the 'Remote Access VPN' tree view is expanded to 'IPsec' > 'IPsec Proposals (Transform Sets)'. The main pane shows the configuration for 'Specify Transform Sets' under 'IKE v1 IPsec Proposals (Transform Sets)'. The 'Add' button is highlighted with a red box. Below it is a table with columns: Name, Mode, ESP Encryption, and ESP Authentication. The 'Add' button is also present for 'IKE v2 IPsec Proposals'.

Name	Mode	ESP Encryption	ESP Authentication
------	------	----------------	--------------------

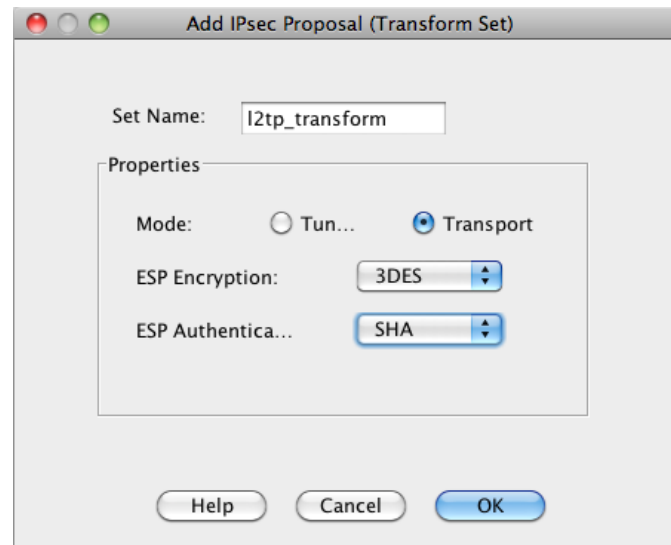
Name	Encryption	Integrity Hash
------	------------	----------------

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

The screenshot shows the Cisco configuration interface. On the left, the 'Remote Access VPN' tree is expanded to 'IPsec' > 'Crypto Maps'. On the right, the configuration page for 'Crypto Maps' is displayed, with the breadcrumb path 'Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps'. The 'Add' button is highlighted with a red box. Below the breadcrumb, there is a toolbar with 'Add', 'Edit', 'Delete', and other icons. A table with columns for 'Type:Priority', 'Traffic Selection' (including '#', 'Source', 'Destination', 'Service', 'Action'), 'Transform Set (IKEv1)', and 'IPsec Proposal (I)' is visible.

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

Tunnel Policy (Crypto Map) - Basic | Tunnel Policy (Crypto Map) - Advanced | Traffic Selection

Interface: Policy Type: Priority:

IPsec Proposals (Transform Sets)

IKE v1 IPsec Proposal:

IKE v2 IPsec Proposal:

[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

The screenshot shows the Cisco configuration interface for 'Group Policies'. The breadcrumb navigation is 'Configuration > Remote Access VPN > Network (Client) Access > Group Policies'. The page title is 'Configuration > Remote Access VPN > Network (Client) Access > Group Policies'. The main content area contains the following text:

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an [LDAP attribute map](#).

Buttons: **Add** (highlighted), Edit, Delete

Name	Type	Tunneling Protocol	AAA Server Group
DfltGrpPolicy (System Default)	Internal	ikev1,ikev2,ssl-clientless,l2tp-ipsec	-- N/A --

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。

The screenshot shows the configuration page for a Group Policy named "GroupPolicyL2TP". The "General" tab is selected, and the "Advanced" section is expanded. The "Name" field contains "GroupPolicyL2TP". Under "Banner:", "SCEP forwarding URL:", and "IPv6 Address Pools:", the "Inherit" checkbox is checked. Under "Address Pools:", the "Inherit" checkbox is unchecked, and "vpn_pool" is selected in the dropdown menu, with a "Select..." button to its right. The "More Options" section is expanded, showing "Tunneling Protocols:" with "Inherit" unchecked and "L2TP/IPsec" checked. Other options like "Clientless SSL VPN", "SSL VPN Client", "IPsec IKEv1", and "IPsec IKEv2" are unchecked. The "IPv4 Filter:" field has "Inherit" checked.

[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

The screenshot shows the Cisco IOS configuration interface. The left pane displays the navigation tree with 'IPsec(IKEv1) Connection Profiles' selected. The right pane shows the configuration for 'IPsec(IKEv1) Connection Profiles'. Under 'Access Interfaces', the 'outside' interface has 'Allow Access' checked. Under 'Connection Profiles', the 'DefaultRAGroup' profile is selected, and the 'Edit' button is highlighted.

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow Access
outside	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

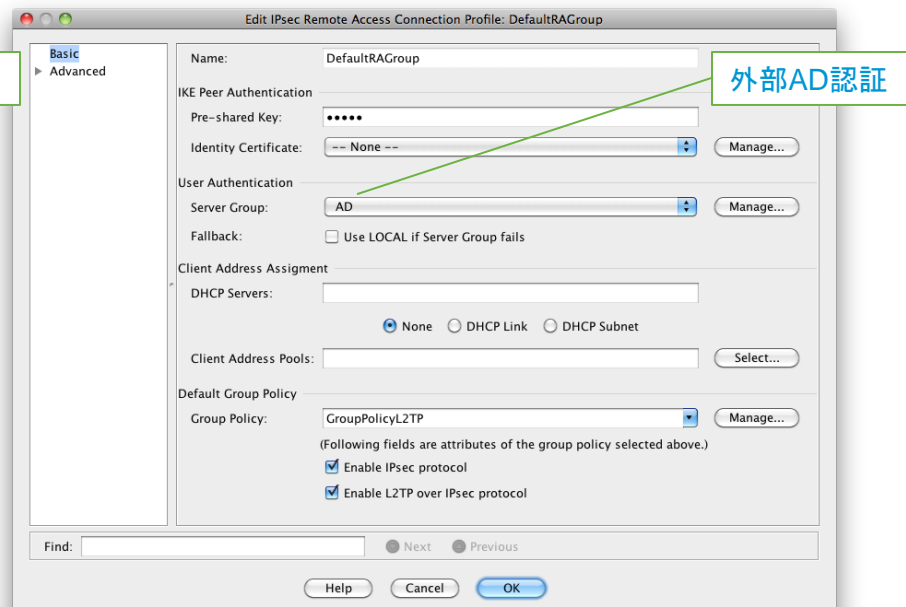
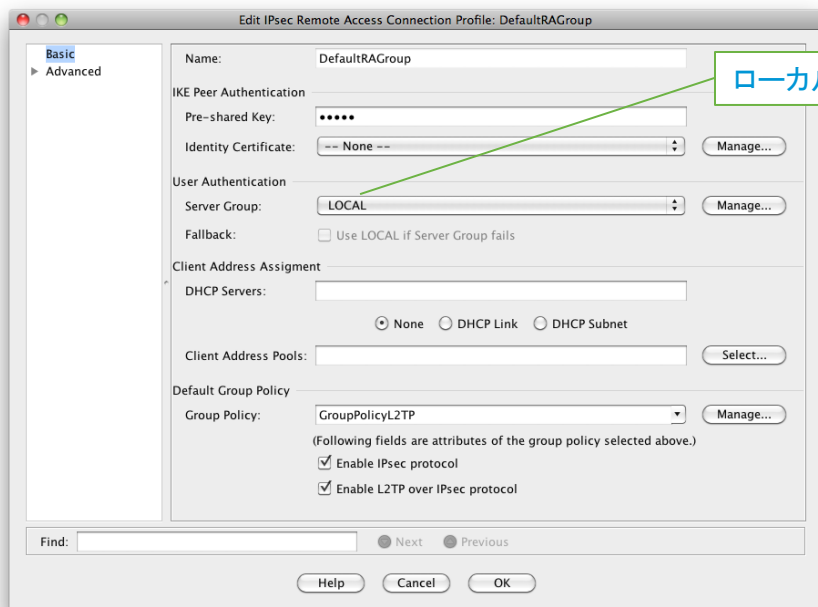
+ Add **Edit** Delete

Name	IPsec Enabled	L2TP/IPsec Enabled	Authentication Server Group	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LOCAL	DfltGrpPolicy
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LOCAL	DfltGrpPolicy

設定例 – L2TP/IPsec PSK

• コネクションプロファイルの設定 (続き)

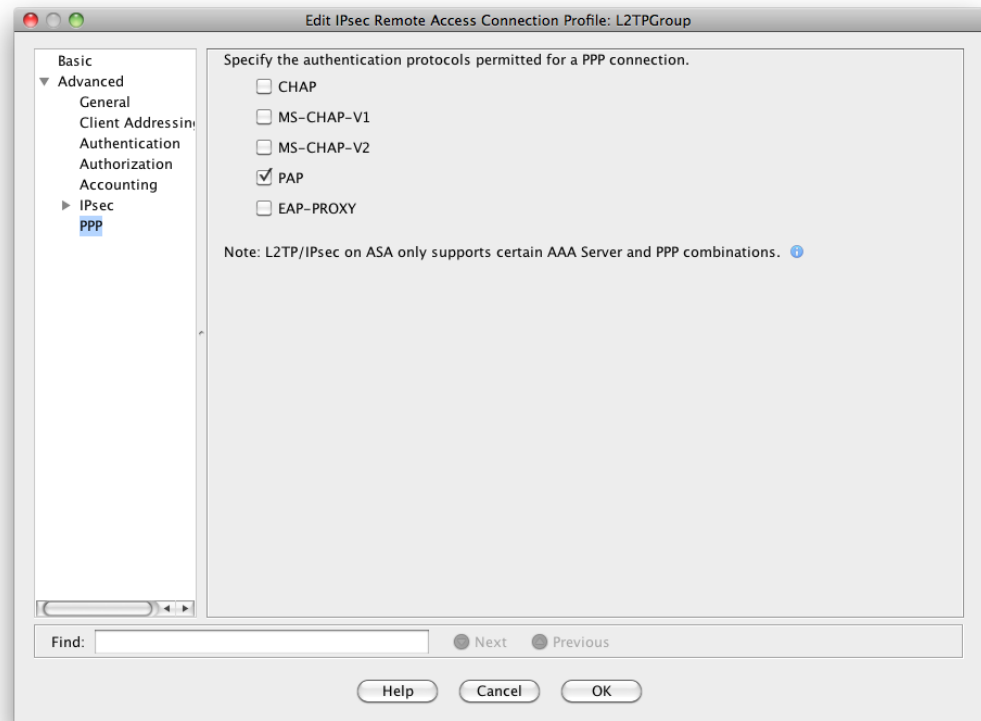
Pre-shared Key (Ex. Pre-shared Key: **cisco**) を入力、Server Group: LOCAL を選択 (→ ローカル認証) もしくは、AD を選択 (→ 外部認証)、Group Policy: に作成したものを選択 (Ex. **GroupPolicyL2TP**)、 “Enable IPsec proposal” 及び “Enable L2TP over IPsec proposal” にチェックがある事を確認する。



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

The screenshot shows the Cisco IOS configuration interface. The left pane displays the configuration tree with 'IPsec(IKEv1) Connection Profiles' selected under 'Network (Client) Access'. The right pane shows the configuration for 'IPsec(IKEv1) Connection Profiles'. The 'Access Interfaces' section has a table for enabling interfaces for IPsec access. The 'Connection Profiles' section has a table for existing profiles and an 'Add' button highlighted with a red box.

Device List
+ Add Delete Connect
Find: Go
10.71.132.144:4443

Remote Access VPN

- Introduction
- Network (Client) Access
 - AnyConnect Connection Profiles
 - AnyConnect Customization/Localization
 - AnyConnect Client Profile
 - AnyConnect Client Settings
 - Dynamic Access Policies
 - Group Policies
 - IPsec(IKEv1) Connection Profiles**
 - Secure Mobility Solution
 - Address Assignment
 - Advanced
 - Clientless SSL VPN Access
 - AAA/Local Users

Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow Access
outside	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

+ Add Edit Delete

Name	IPsec Enabled	L2TP/IPsec Enabled	Authentication Server Group	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LOCAL	DfltGrpPolicy
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LOCAL	DfltGrpPolicy

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

Basic
Advanced

Name: L2TPGroup

IKE Peer Authentication
Pre-shared Key:

Identity Certificate: bndemo-CA:cn=asa,o=Cisco,l=Minato-ku,st=Tokyo,... Manage...

User Authentication
Server Group: LOCAL Manage...
Fallback: Use LOCAL if Server Group fails

Client Address Assignment
DHCP Servers:

None DHCP Link DHCP Subnet

Client Address Pools: Select...

Default Group Policy
Group Policy: GroupPolicyL2TP Manage...
(Following fields are attributes of the group policy selected above.)
 Enable IPsec protocol
 Enable L2TP over IPsec protocol

Find: Next Previous

Help Cancel OK

Basic
Advanced

Name: L2TPGroup

IKE Peer Authentication
Pre-shared Key:

Identity Certificate: bndemo-CA:cn=asa,o=Cisco,l=Minato-ku,st=Tokyo,... Manage...

User Authentication
Server Group: AD Manage...
Fallback: Use LOCAL if Server Group fails

Client Address Assignment
DHCP Servers:

None DHCP Link DHCP Subnet

Client Address Pools: Select...

Default Group Policy
Group Policy: GroupPolicyL2TP Manage...
(Following fields are attributes of the group policy selected above.)
 Enable IPsec protocol
 Enable L2TP over IPsec protocol

Find: Next Previous

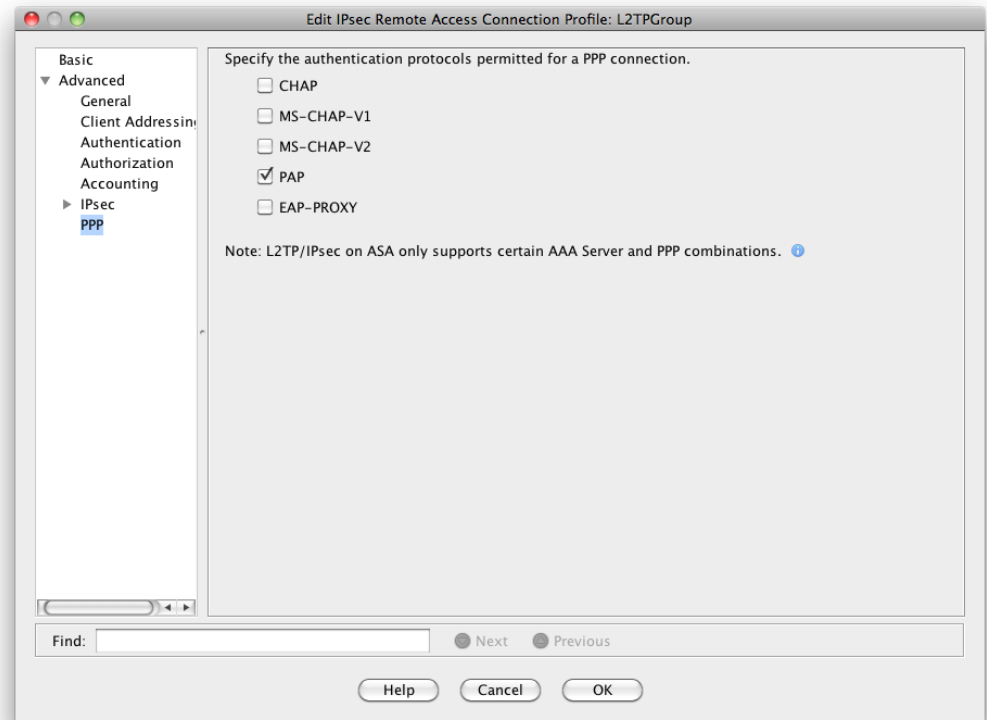
Help Cancel OK

[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

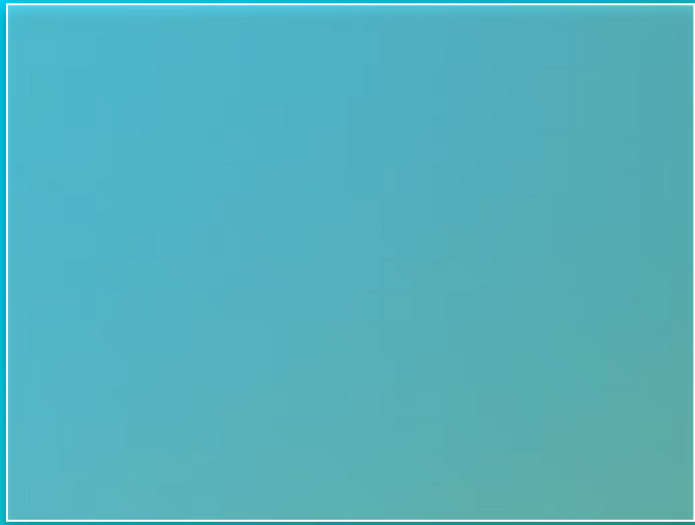
```
snmp-server enable traps snmp authentication linkup linkdown
coldstart warmstart
crypto ipsec ikev1 transform-set l2tp_transform esp-3des esp-sha-
hmac
crypto ipsec ikev1 transform-set l2tp_transform mode transport
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set
l2tp_transform
crypto 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 14e87d8f00000000000004
  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 XIAPE6POhu0IQN1OczHpog== 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



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

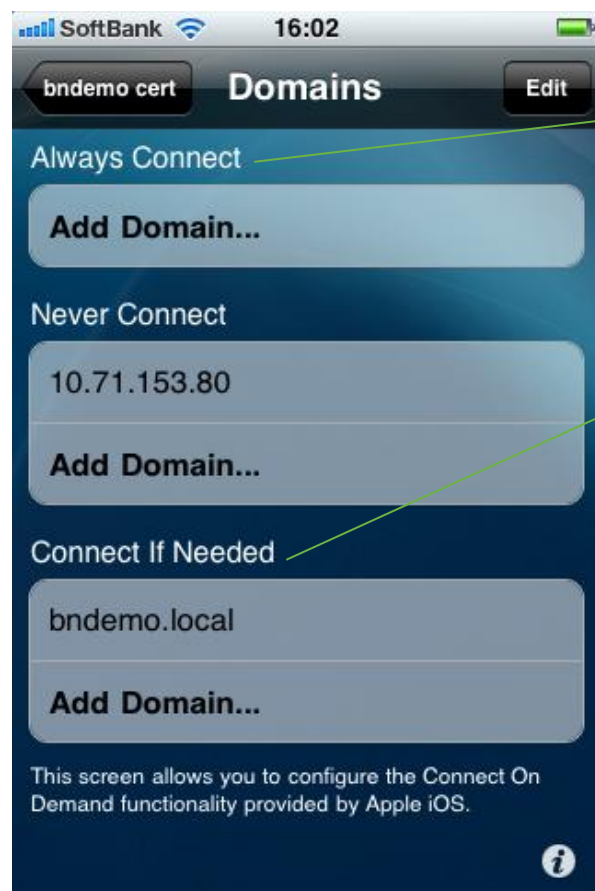
Domain List: 次ページ

Android

iPhone

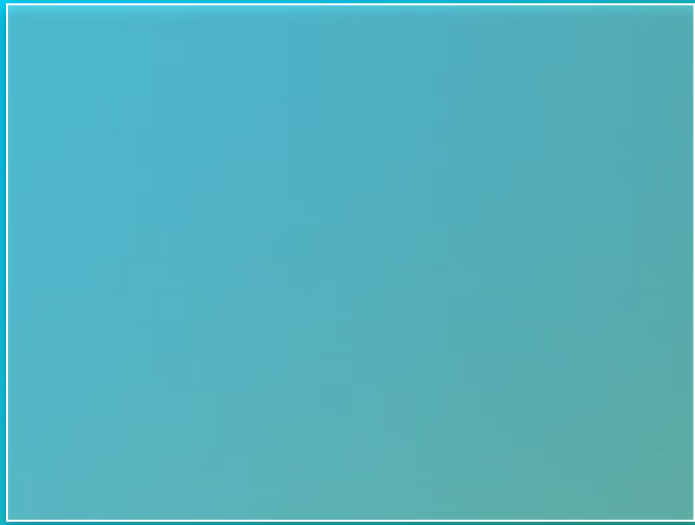
クライアント設定: AnyConnect

- 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

SoftBank 17:03 58%

キャンセル 構成を追加 保存

L2TP PPTP IPSec

説明 L2TP psk AD

サーバ 10.71.153.80

アカウント aduser

RSA SecurID オフ

パスワード 毎回確認

シークレット ●●●●●

すべての信号を送信 オン

プロキシ

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&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

(*) 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 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



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
```

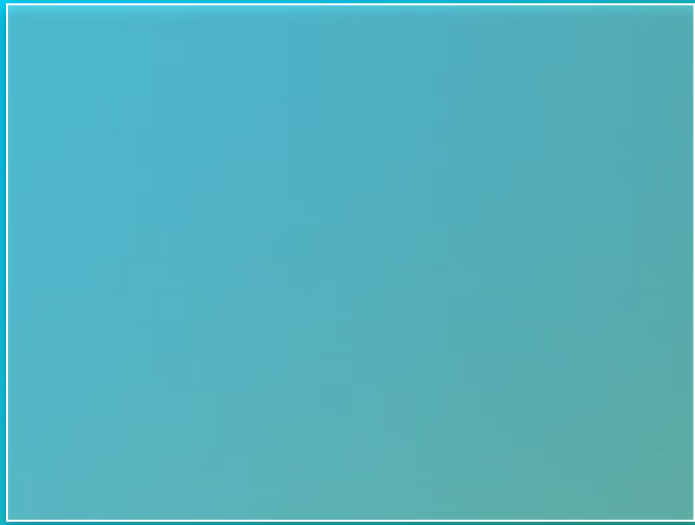
```
key cisco
```

```
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
```

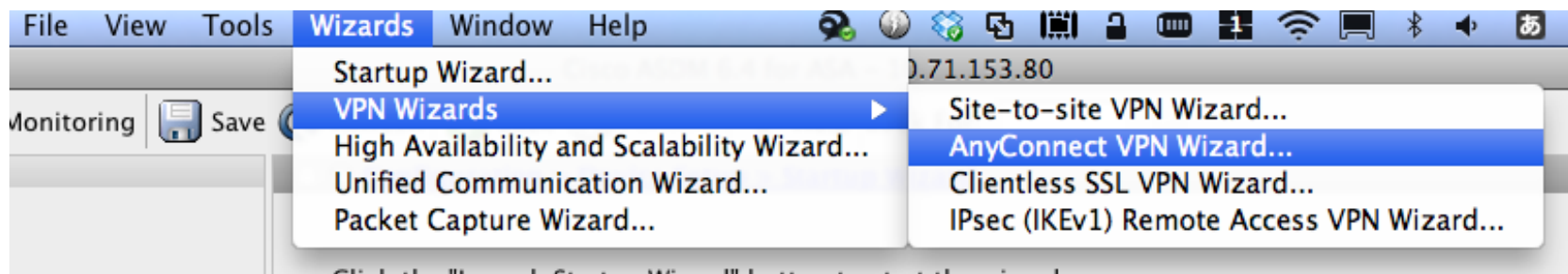


VPN 設定

AnyConnect Wizard

VPN 設定: AnyConnect

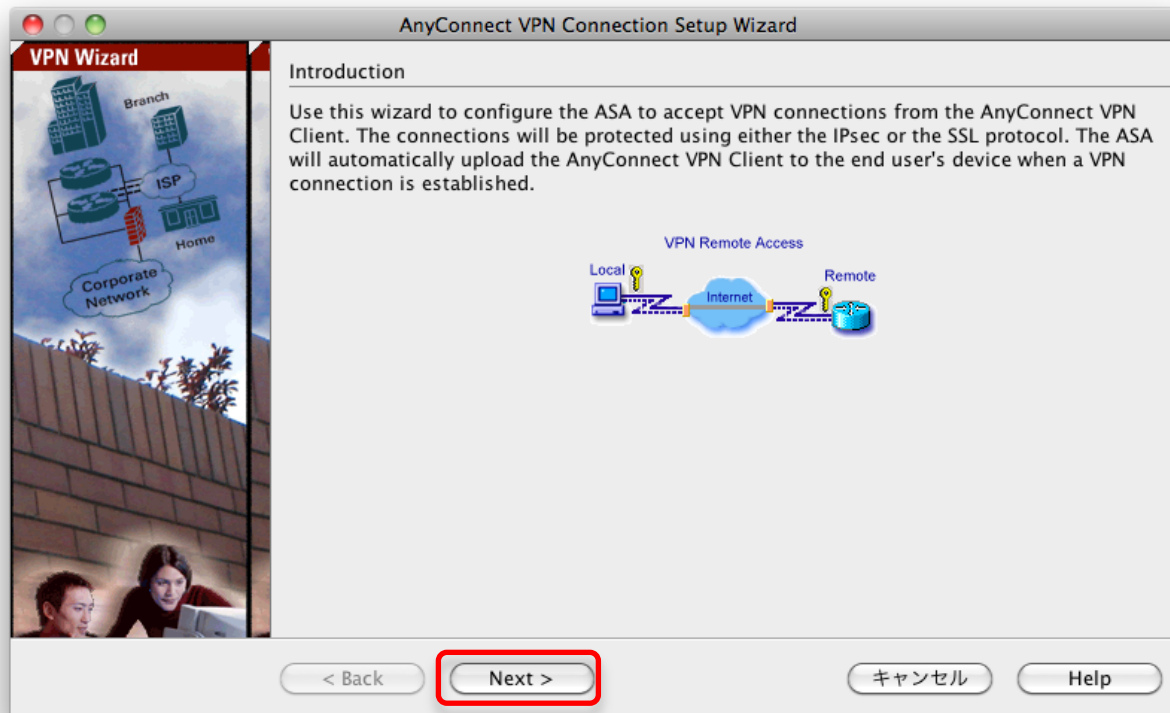
- Wizard を使用しての AnyConnect の設定
上部のメニューより、Wizards > VPN Wizard > AnyConnect VPN Wizard と進みます。



(*)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。

AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. **Connection Profile Identification**
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Connection Profile Identification

This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections.

Connection Profile Name:

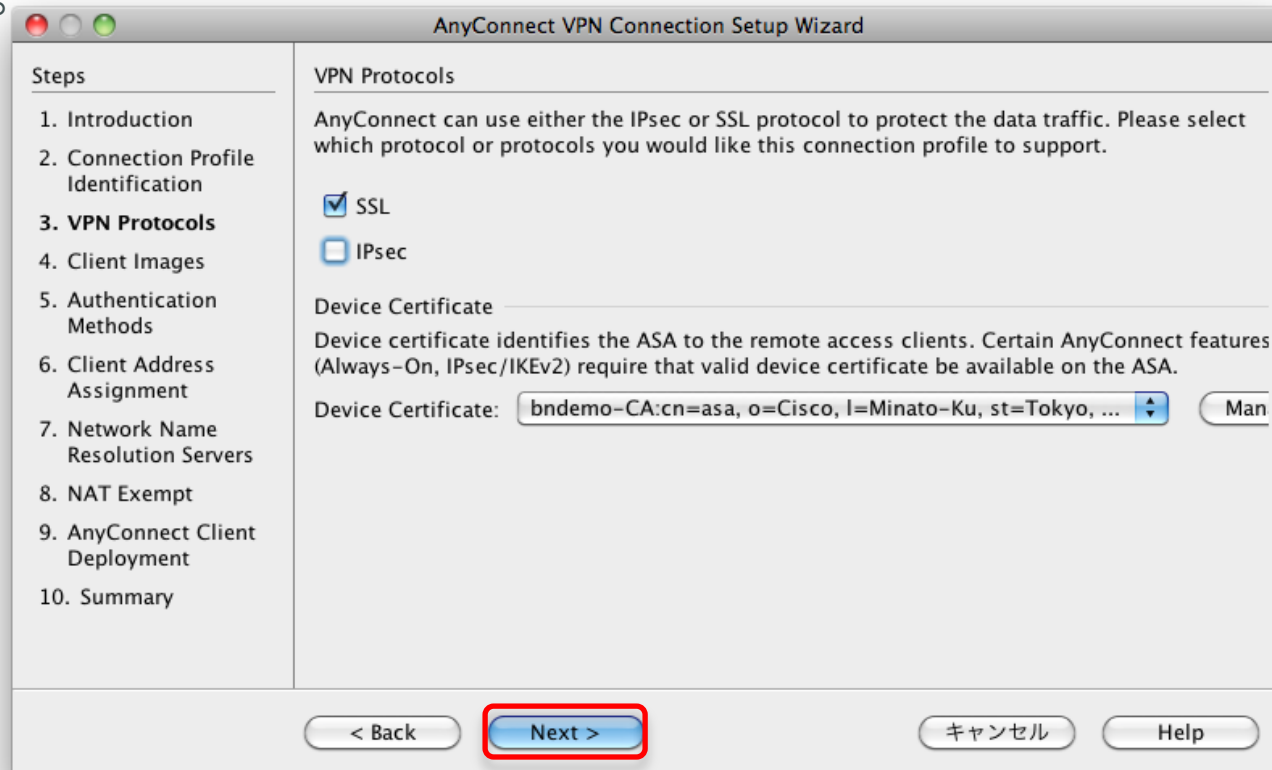
VPN Access Interface:

< Back **Next >** キャンセル Help

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。

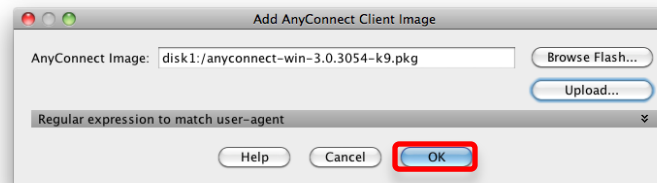
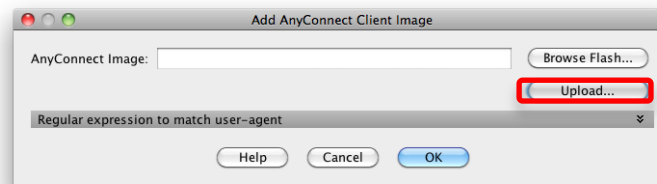
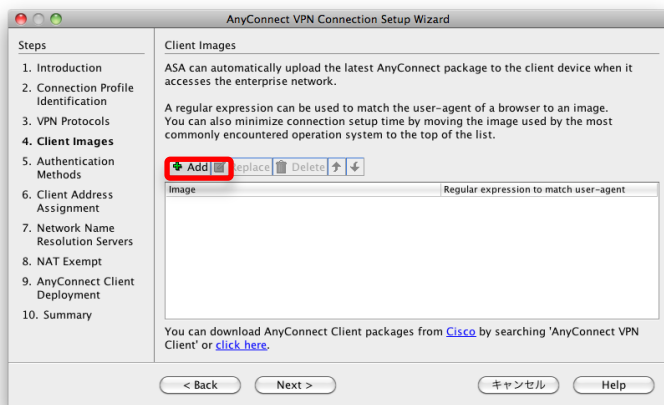


VPN 設定: AnyConnect

- 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。

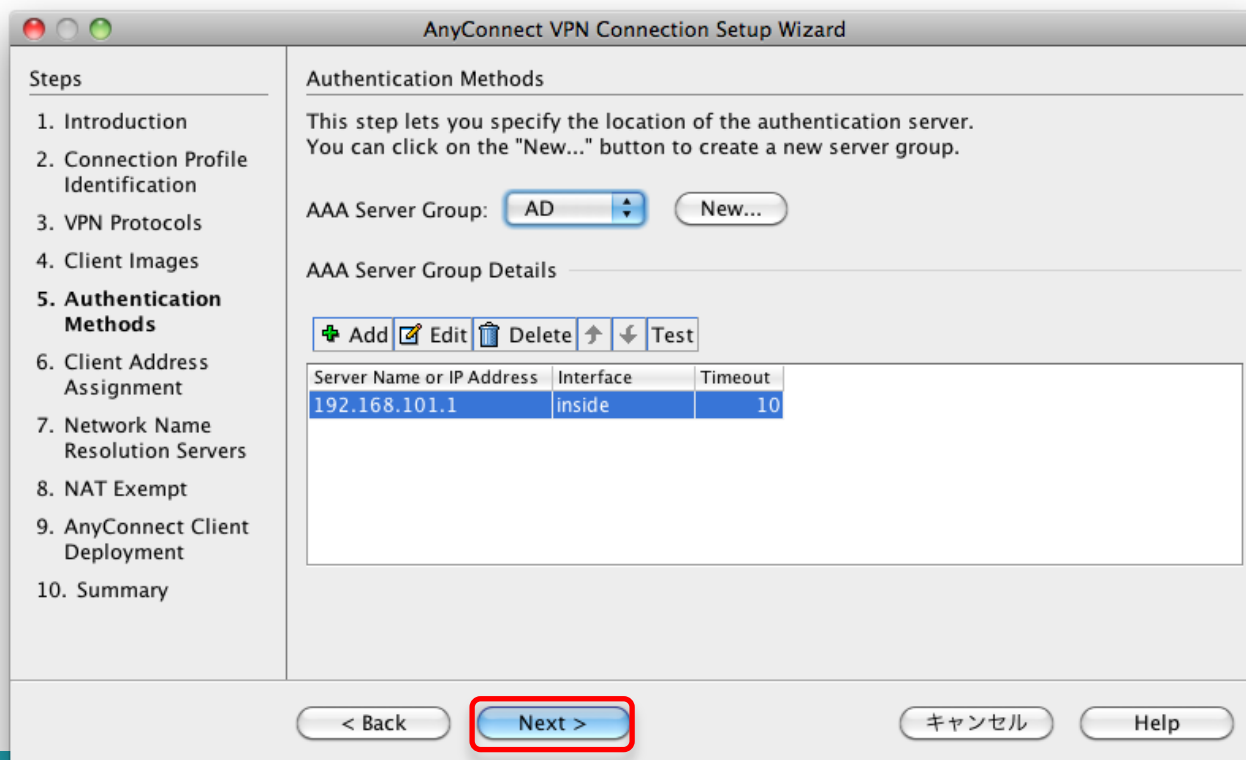
[Upload] をクリックし、AnyConnect イメージを指定し [Upload File] をクリックします。アップロード完了後、[OK]をクリックします。



[Next] をクリックし、次のページに進みます。

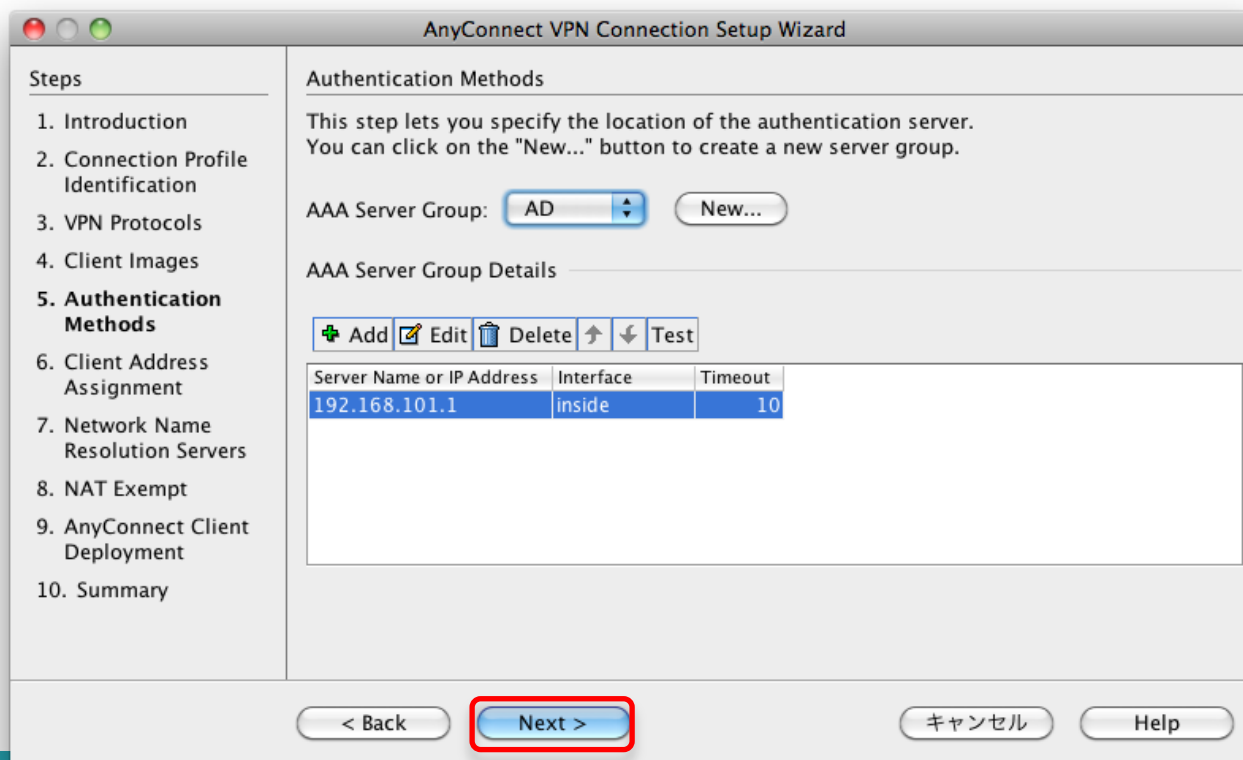
VPN 設定: AnyConnect

- 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。

AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
- 7. Network Name Resolution Servers**
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Network Name Resolution Servers

This step lets you specify how domain names are resolved for the remote user when accessing the internal network.

DNS Servers:

WINS Servers:

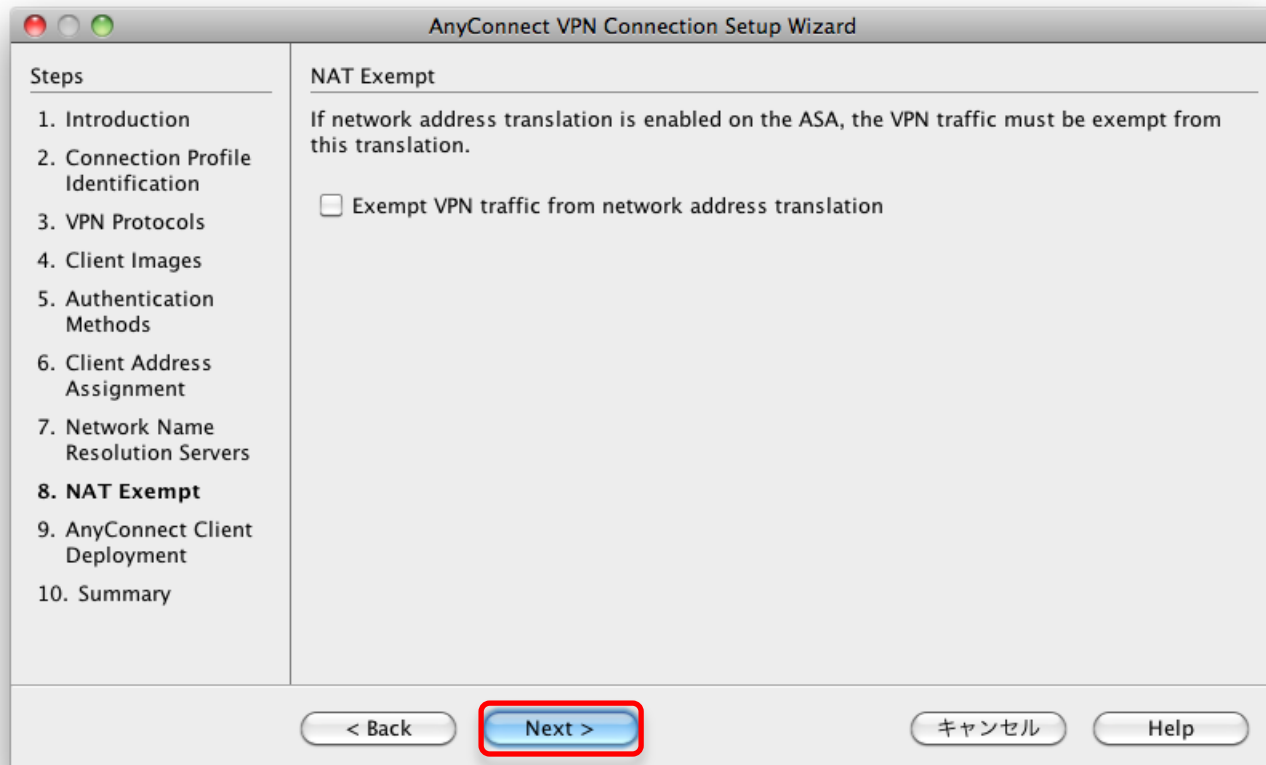
Domain Name:

< Back **Next >** キャンセル Help

VPN 設定: AnyConnect

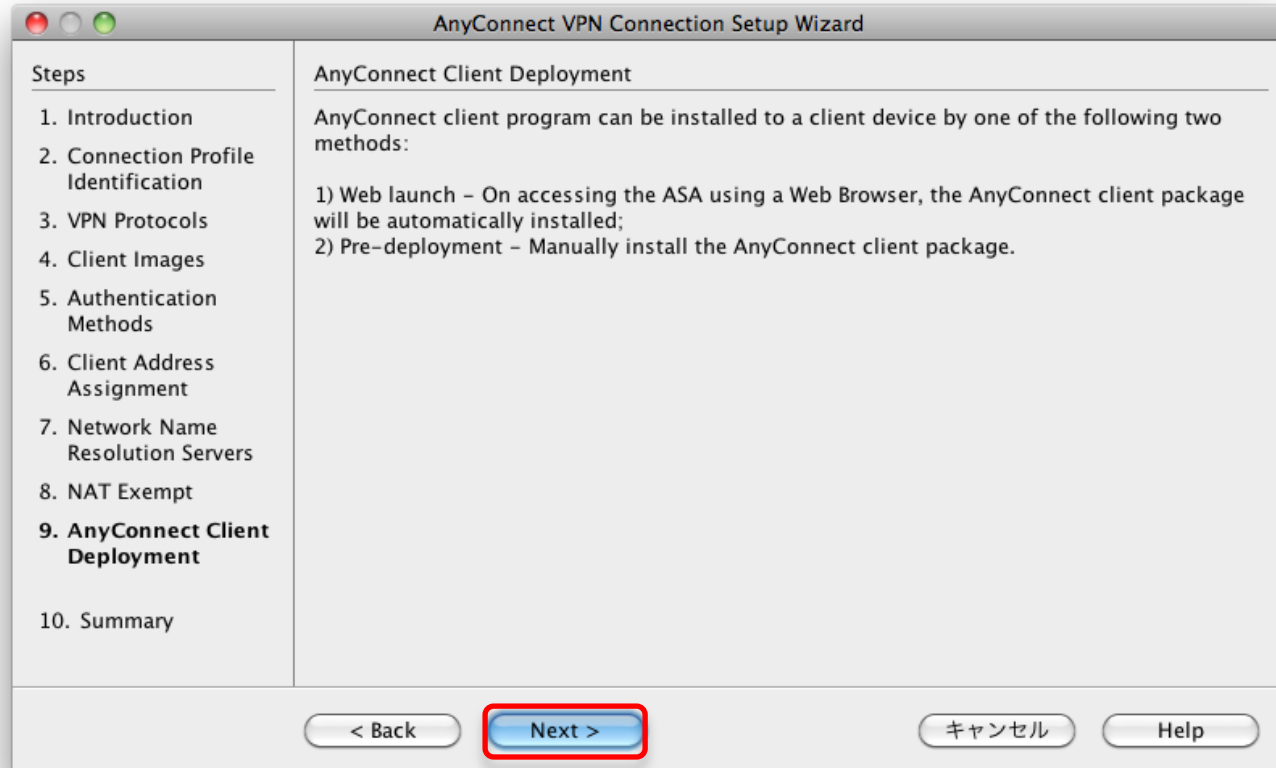
- Wizard を使用しての AnyConnect の設定 (続き)

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。



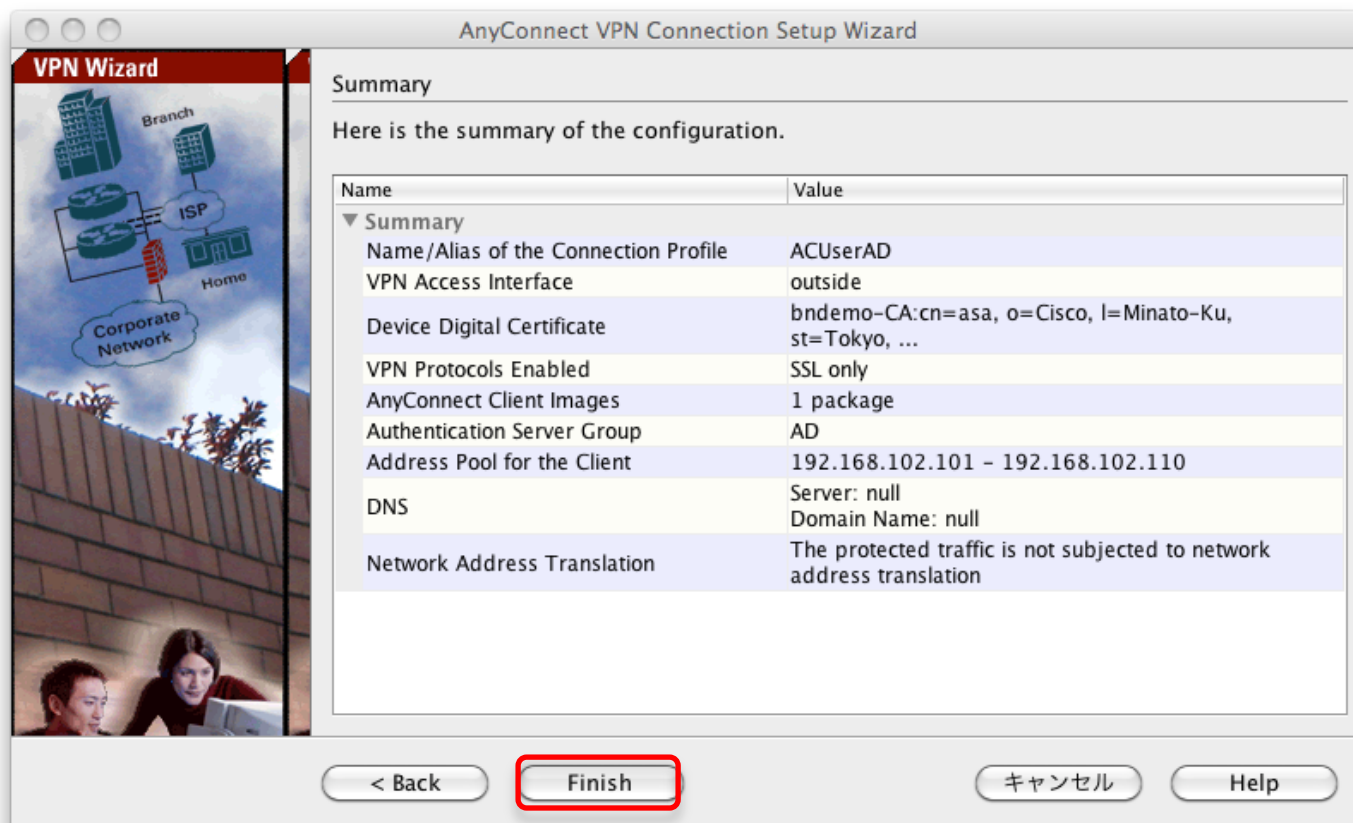
VPN 設定: AnyConnect

- 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.

