

Cisco Start Firewall

Cisco ASA 5506-X AnyConnect VPN の設定

2016 年 2 月 16 日

第 1.0 版



www.networld.co.jp

株式会社ネットワールド



Networld



Cisco Start Firewall

Cisco ASA 5506-X AnyConnect VPN の設定



改訂履歴

版番号	改訂日	改訂者	改訂内容
1.0	2016 年 2 月 16 日	ネットワーク	● 新規
			●
			●
			●



免責事項

- 本書のご利用は、お客様ご自身の責任において行われるものとします。本書に記載する情報については、株式会社ネットワールド（以下 弊社）が慎重に作成および管理いたしますが、弊社がすべての情報の正確性および完全性を保証するものではありません。
- 弊社は、お客様が本書からご入手された情報により発生したあらゆる損害に関して、一切の責任を負いません。また、本書および本書にリンクが設定されている他の情報元から取得された各種情報のご利用によって生じたあらゆる損害に関しても、一切の責任を負いません。
- 弊社は、本書に記載する内容の全部または一部を、お客様への事前の告知なしに変更または廃止する場合がございます。なお、弊社が本書を更新することをお約束するものではありません。



表記規則

表記	表記の意味
「」 (括弧記号)	キー、テキストボックス、ラジオボタンなどのオブジェクト
bold (ボールド文字)	入力または選択するシステム定義値
<i><italic></i> (イタリック文字)	入力または選択するユーザー定義値
□ (囲み線)	入力または選択するオブジェクト
"" (二重引用符記号)	表示されるメッセージ
■ (蛍光マーカー)	確認するメッセージ

表記の例)

(1) 「Exec」ラジオボタンを選択します。

(2) テキストボックスに以下のコマンドを入力します。

copy running-config <file name>

(3) 「コマンドを実行」ボタンをクリックします。正常に実行されれば、画面に「[OK]」が表示されます。

Destination filename [startup-config]?

Building configuration...

[OK]

CLIによる設定

CLI機能はルータのコマンドプロンプトで実行可能な設定や、全てのIOS CLIコマンドを入力できます

1
2
3

☒ Exec
☐ Configure

copy running-config startup-config

コマンドを実行

クリア

Destination filename [startup-config]?
Building configuration...

[OK]



目次

1. はじめに.....	1
1.1 対象機器.....	1
1.2 AnyConnect VPN について.....	1
1.3 事前に用意するもの	1
2. システム構成	2
2.1 システム構成	2
3. AnyConnect VPN の設定	3
3.1 AnyConnect VPN のポリシー設定	3
3.2 クライアント PC の AnyConnect VPN 設定	17
3.2.1 AnyConnect Secure Mobility Client のインストール	17
3.2.2 AnyConnect VPN の接続	21



1. はじめに

本書は Cisco ASA 5506-X における AnyConnect VPN の設定手順について説明しています。

1.1 対象機器

本書で対象としている機器は以下になります。

表 1 本書の対象機器

ASA 5506-X (ASA5506-K9)	ASA 5506W-X (ASA5506W-Q-K9)
☑	☑

1.2 AnyConnect VPN について

AnyConnect VPN とは、Cisco ASA 5500 シリーズ等を終端装置として、PC などのリモート端末から VPN 接続を行う際にクライアントとなるソフトウェアおよび機能の名称です。

AnyConnect VPN を行うためには、AnyConnect Plus ライセンスまたは AnyConnect Apex ライセンスを購入し、ASA 本体でアクティベーション(有効化)する必要があります。ライセンスのアクティベーション手順については別紙「Cisco ASA 5506-X AnyConnect ライセンスアクティベーション」を参照して下さい。

1.3 事前に実施しておく事

- AnyConnect Plus ライセンスまたは AnyConnect Apex ライセンスのアクティベーション
- AnyConnect Secure Mobility Client のイメージファイル (Windows 用、Web deploy) を Cisco.com よりダウンロードし、ASA の Flash へのコピーしておきます。ダウンロード時には Cisco.com ID に AnyConnect Plus ライセンスまたは AnyConnect Apex ライセンスの契約番号が紐づいている必要があります



2. システム構成

2.1 システム構成

本書での AnyConnect VPN 設定手順は以下のシステム構成に基づいて行われます。設定状態は別紙「Cisco ASA 5506-X クイックスタートガイド」の設定完了後となり、管理 PC の ASDM から ASA に接続でき、インターネットへもアクセスできる状態を想定しています。また、ASA の outside のインタフェース(GE1/1)に対してクライアント PC からインターネット越しにアクセスできることが前提となります。



図 1 システム構成図

表 2 本書で使用した機材およびそれらのシステム環境

機器	機器名	OS およびアプリケーション	ネットワーク設定
Firewall	ASA 5506W-X	OS Version 9.5(2) ASDM Version 7.5(2)153 AnyConnect Secure Mobility Client Version 4.2.01035※ AnyConnect Plus ライセンス	GE1/1 nameif:outside (デフォルト) IP アドレス:DHCP(デフォルト) security level:0(デフォルト) GE1/2 nameif:inside (デフォルト) IP アドレス:172.16.1.254/24 Security level:100(デフォルト)
管理用 PC		OS : Windows 7 ターミナルアプリケーション (Tera Term) Web ブラウザ(Internet Explorer11)	インタフェース IP アドレス:172.16.1.1/24
クライアント PC		OS : Windows 7 Web ブラウザ(Internet Explorer11)	インタフェース IP アドレス:DHCP

※AnyConnect Secure Mobility Client のイメージファイルはデフォルトでは ASA の Flash に入っていないため、事前に Cisco.com よりダウンロードして Flash に入れておく必要があります

表 3 ASA 5506-X のネットワーク設定

ルーティング	・インターネット側へデフォルトルート を DHCP により取得
NAT	・any→outside への PAT (デフォルト)

表 4 AnyConnect VPN のポリシー

VPN アクセス インタフェース	VPN プロトコル	AnyConnect クライアント イメージ	IP Address プール (プ ール名)	NAT 除外ルール	スプリットトンネリ ング(ACL 名)
outside	SSL	anyconnect-win-4. 2.01035-k9.pkg	192.168.1.1-250/24 (Pool)	inside, 172.16.1.0/24	172.16.1.0/24 (split)



3. AnyConnect VPN の設定

3.1 AnyConnect VPN のポリシー設定

本節では、AnyConnect VPN のポリシー設定手順を説明します。

- 1) 管理 PC から ASDM により ASA にアクセスし、「Wizards」>「VPN Wizards」>「AnyConnect VPN Wizard」を開きます。

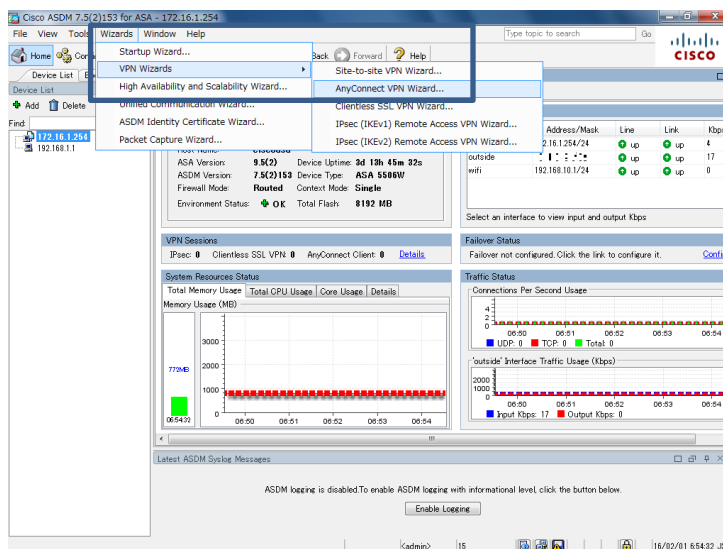


図 2 AnyConnect VPN Wizard を開く

- 2) AnyConnect VPN Connection Setup Wizard が開始されます。「Next」をクリックします。

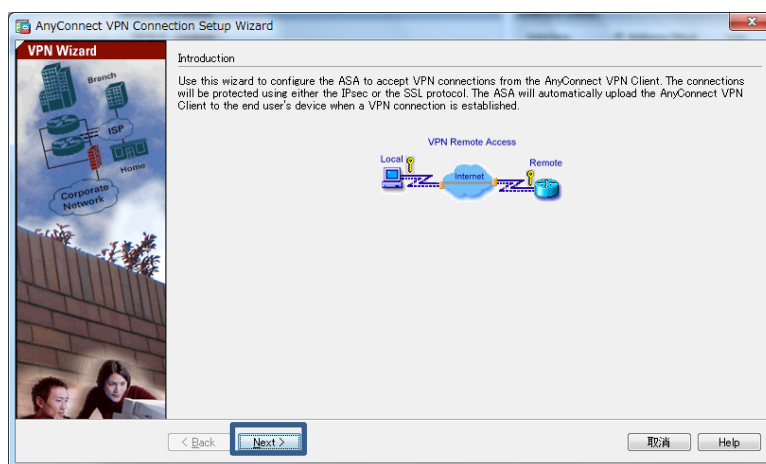


図 3 AnyConnect VPN Connection setup Wizard の開始



- 3) 「Connection Profile Name」および「VPN Access Interface」を設定して「Next」をクリックします。

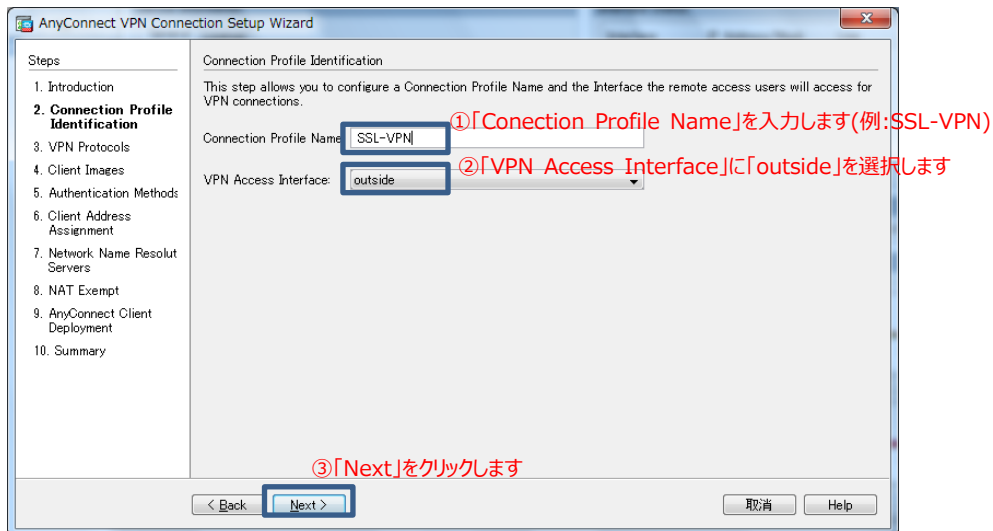


図 4 Connection Profile の作成

- 4) 使用する VPN を選択し、「Next」をクリックします。

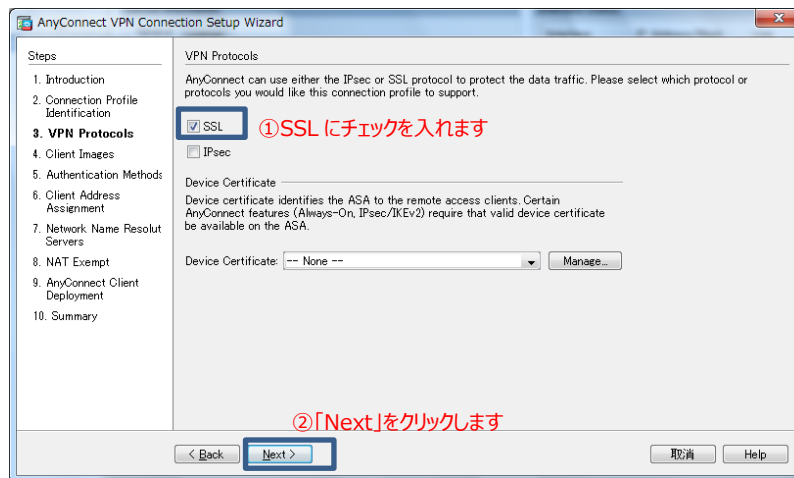


図 5 VPN の選択



5) 「Add」をクリックして Client Image の指定に進みます。

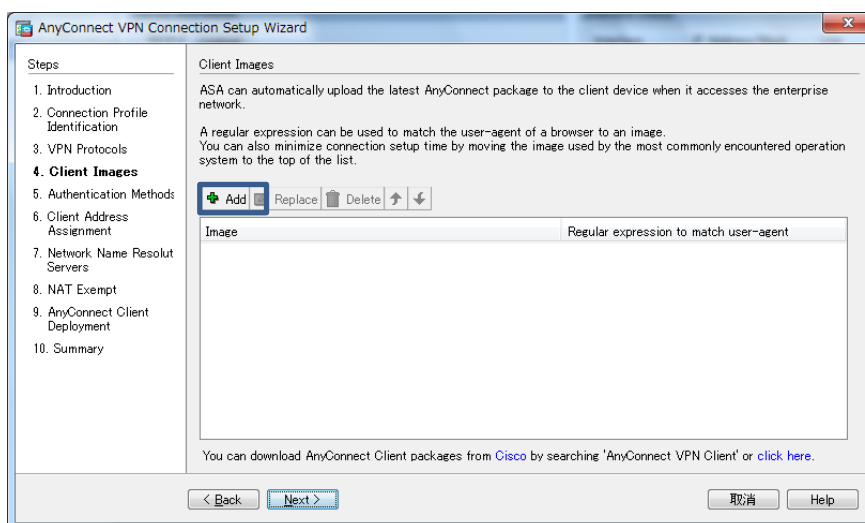


図 6 Client Image の指定(1)

6) 「Browse Flash」をクリックします。

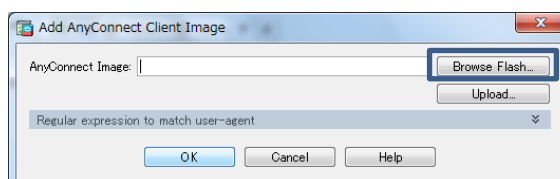


図 7 Client Image の指定(2)

7) AnyConnect Client Image を指定し、「OK」をクリックします。

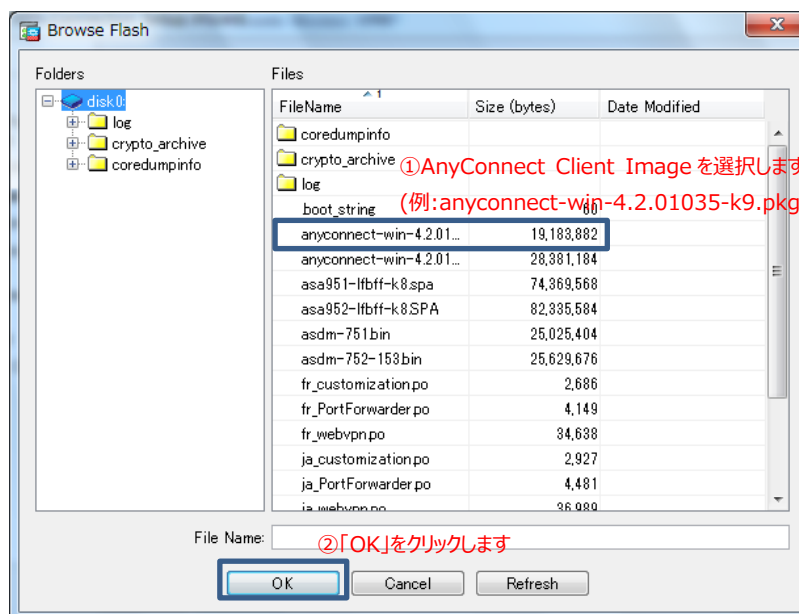


図 8 Client Image の指定(3)



8) 「OK」をクリックして Client Image の指定を完了します。

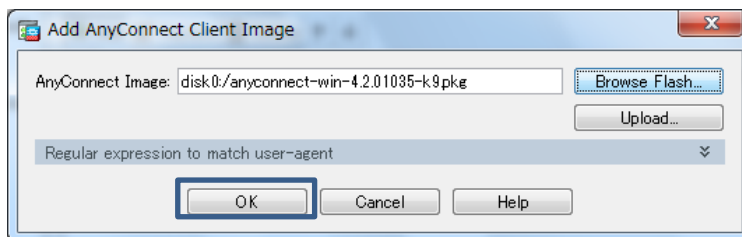


図 9 Client Image の指定(4)

9) 「Next」をクリックして先に進みます。

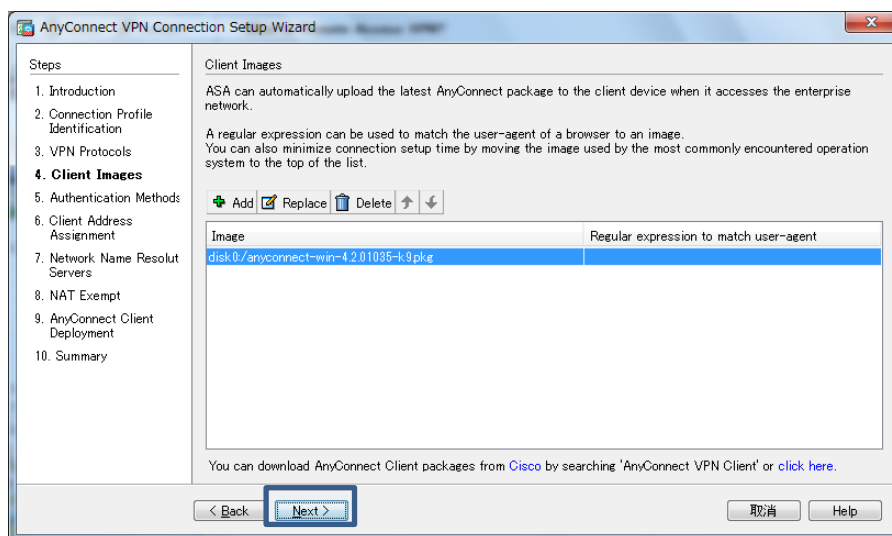


図 10 Client Image の指定(5)

10) AnyConnect VPN で接続するクライアントを認証するためのユーザアカウントを追加し、「Next」をクリックします。

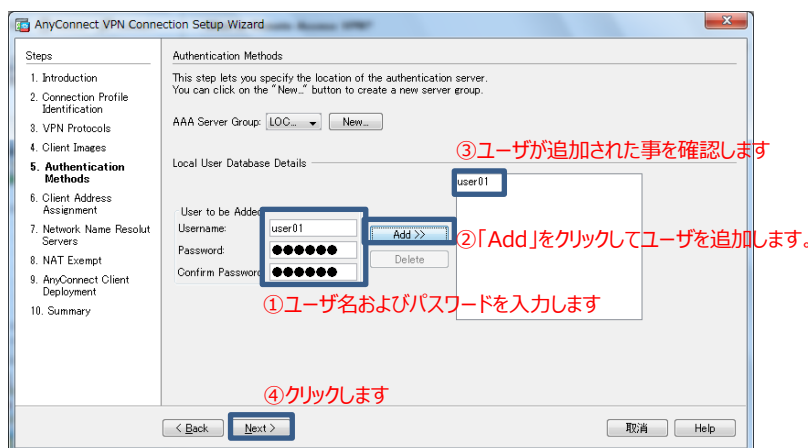


図 11 AnyConnect VPN ユーザアカウントの追加



- 11) VPN で接続するクライアント端末に割り当てる IP アドレスプールを作成するため、「New」をクリックします。

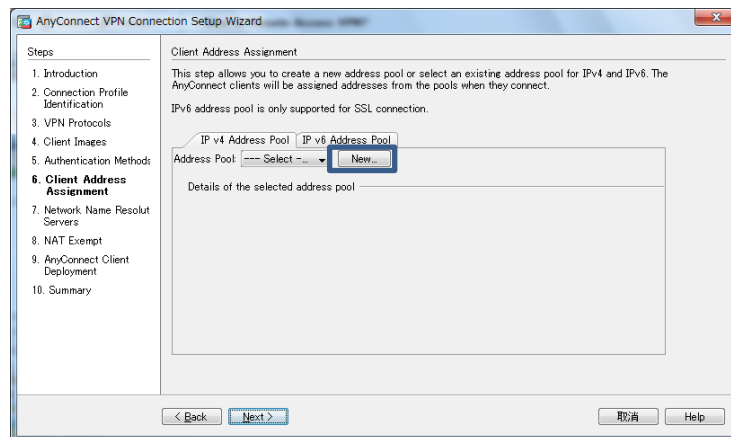


図 12 IP Address Pool の作成(1)

- 12) IP アドレスプールの設定を入力し、「OK」をクリックします。

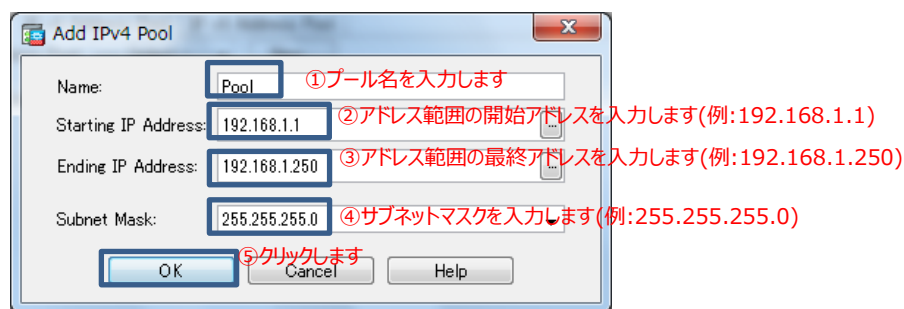


図 13 IP Address Pool の作成(2)

- 13) 先ほど作成した Pool を選択し、「Next」をクリックします。

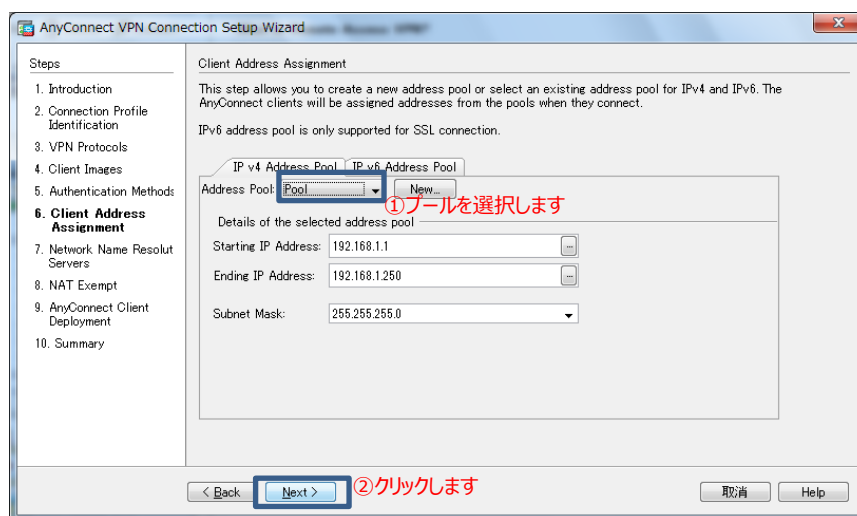
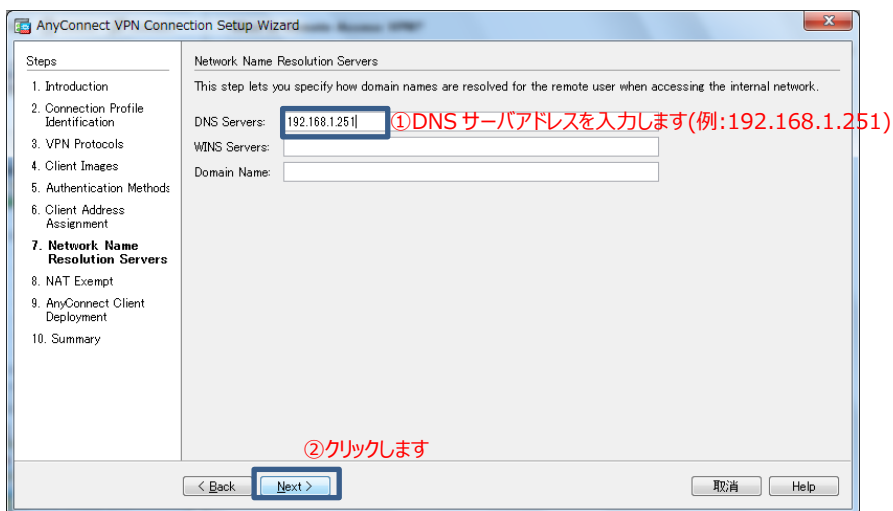


図 14 IP Address Pool の作成(3)



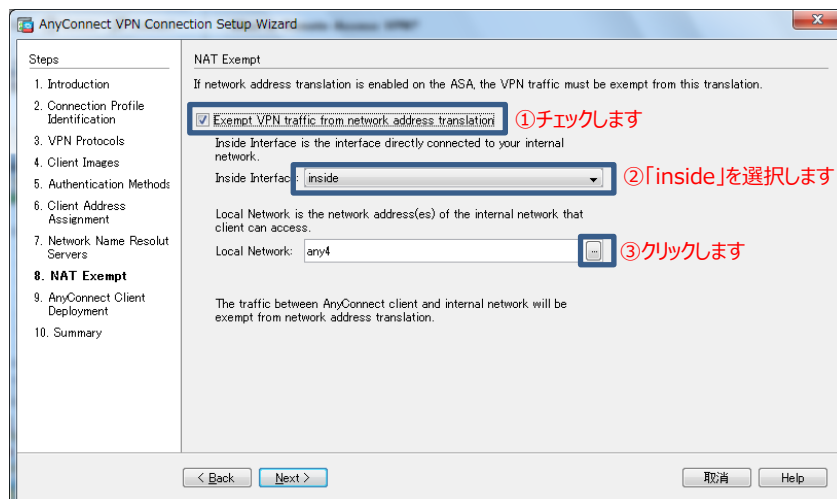
14) クライアント端末が使用する DNS サーバのアドレスを入力し、「Next」をクリックします。



The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window, specifically the 'Network Name Resolution Servers' step. The left sidebar lists steps 1 through 10, with step 7, 'Network Name Resolution Servers', highlighted. The main area contains the following text: 'This step lets you specify how domain names are resolved for the remote user when accessing the internal network.' Below this, there are three input fields: 'DNS Servers:' with the value '192.168.1.251', 'WINS Servers:', and 'Domain Name:'. A red annotation '①DNS サーバアドレスを入力します(例:192.168.1.251)' points to the 'DNS Servers' field. At the bottom, a red annotation '②クリックします' points to the 'Next >' button. The 'Back' button is disabled, and the 'Cancel' and 'Help' buttons are also present.

図 15 DNS サーバアドレスの設定

15) NAT 除外のルールを作成します。



The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window, specifically the 'NAT Exempt' step. The left sidebar lists steps 1 through 10, with step 8, 'NAT Exempt', highlighted. The main area contains the following text: 'If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.' Below this, there is a checkbox labeled 'Exempt VPN traffic from network address translation' which is checked. A red annotation '①チェックします' points to this checkbox. Below the checkbox, there is a dropdown menu for 'Inside Interface' with the value 'inside'. A red annotation '②「inside」を選択します' points to this dropdown. Below the dropdown, there is a text field for 'Local Network' with the value 'any4'. A red annotation '③クリックします' points to the 'Next >' button. The 'Back' button is disabled, and the 'Cancel' and 'Help' buttons are also present.

図 16 NAT 除外ルールの設定(1)



16) NAT の除外となる Local Network を選択し、「OK」をクリックします。

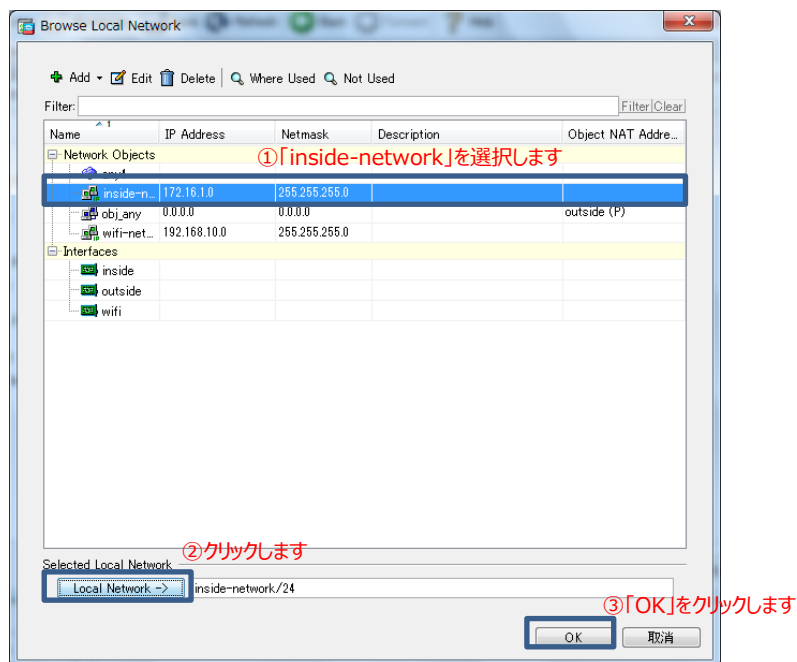


図 17 NAT 除外ルールの設定(2)

17) 「Next」をクリックして先に進みます。

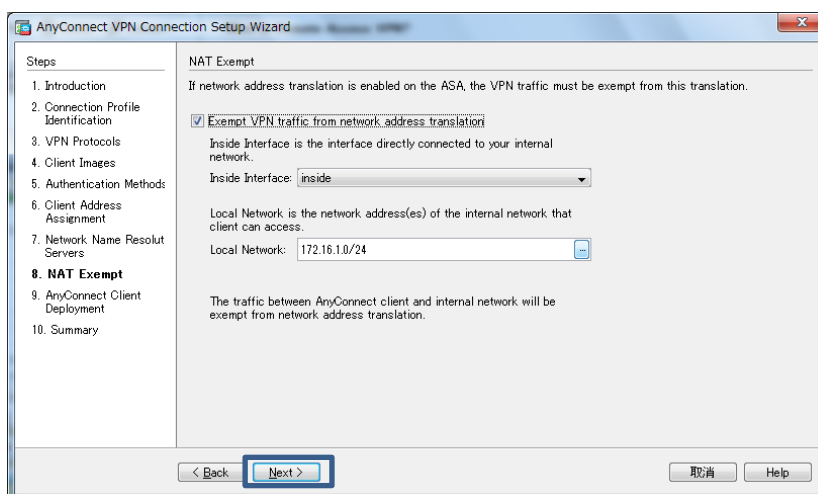


図 18 NAT 除外ルールの設定(3)



18) 「Next」をクリックして先に進みます。

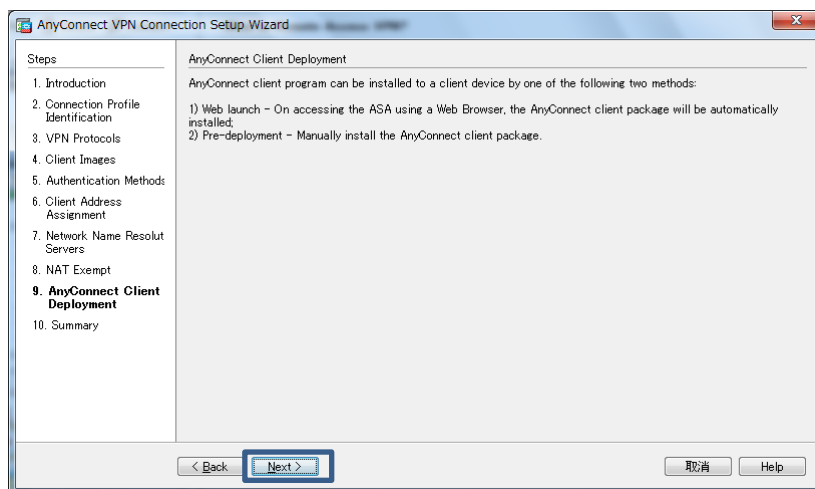


図 19 AnyConnect VPN Client のインストール方法

19) 「Finish」をクリックして Wizard を完了します。

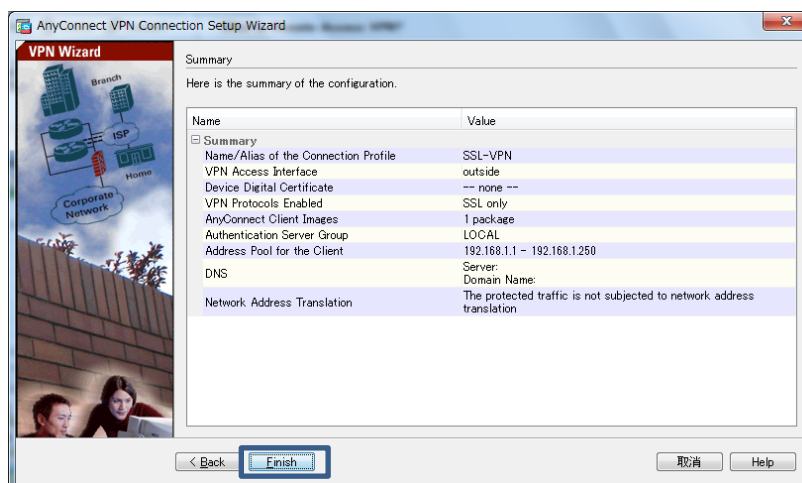


図 20 Wizard の完了



20) ASA に実行されるコマンドのプレビューが表示されるので、「Send」をクリックして実行します。

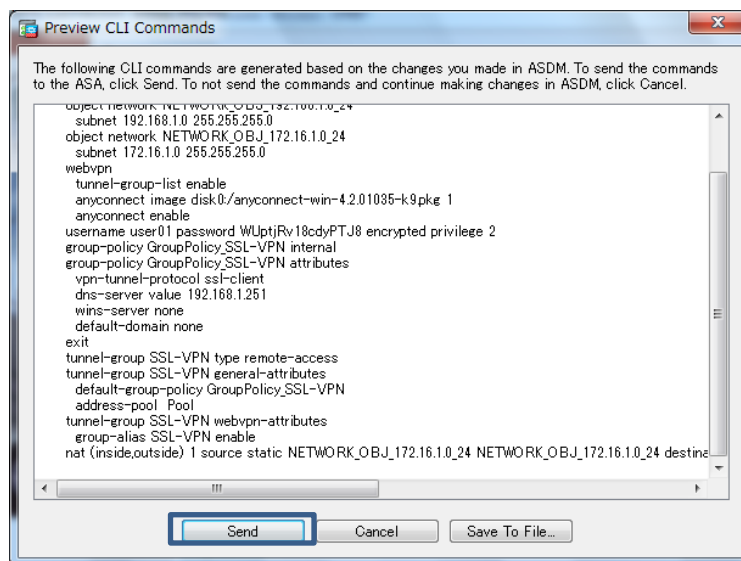


図 21 コマンドのプレビュー

21) 「Configuration」>「Remote Access VPN」>「Network (Client) Access」> Group Policiesを開き、「GroupPolicy_SSL-VPN」を選択し、「Edit」をクリックします。

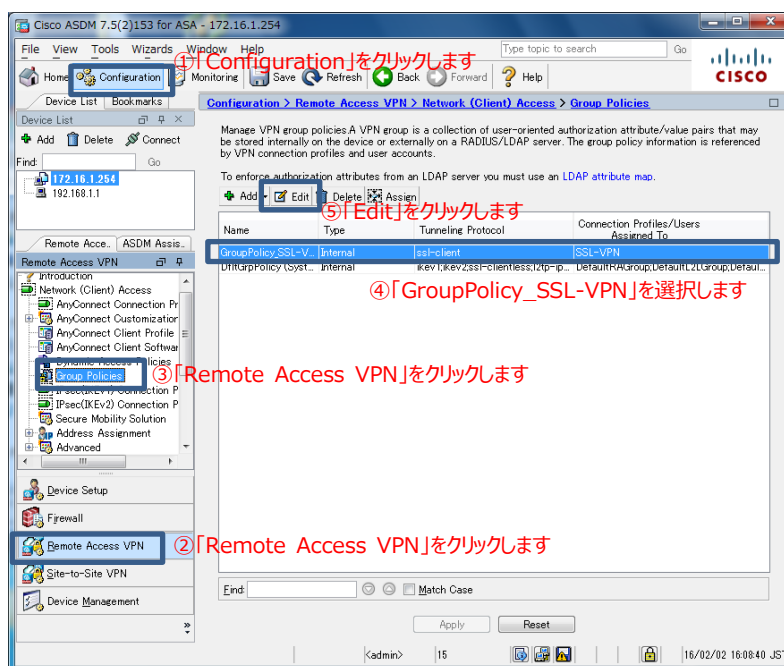


図 22 Group Policy の設定



- 22) スプリットトンネリングの設定を行います。スプリットトンネリングにより、VPN クライアントは VPN へ接続または切断することなく、セキュリティ保護されたサイトおよび保護されていないサイトの両方に接続することができます。

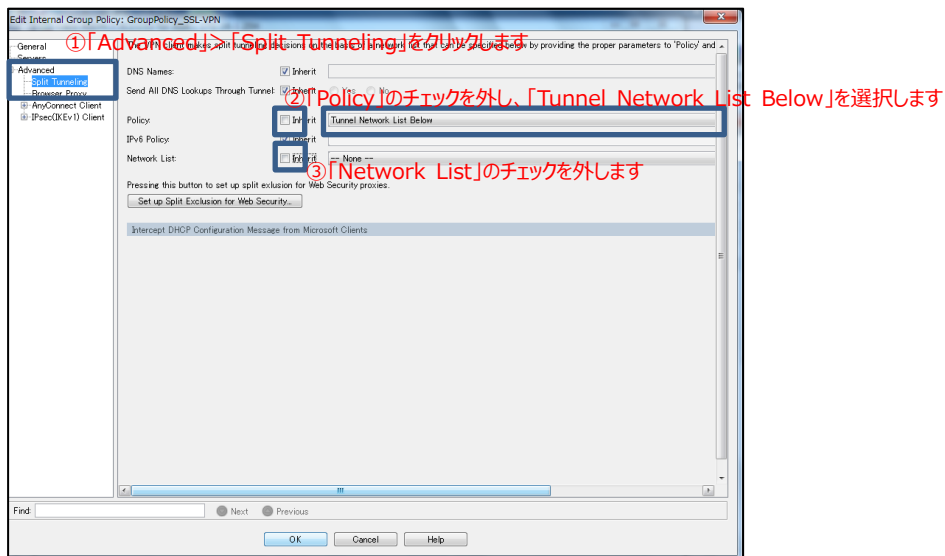


図 23 スプリットトンネリングの設定(1)

- 23) 右にスクロールし、「Manage」をクリックします。

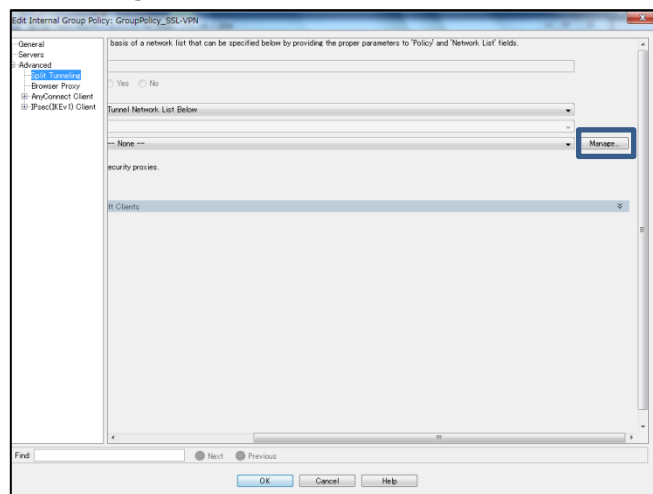


図 24 スプリットトンネリングの設定(2)



24) 「Add」>「Add ACL」を開きます。

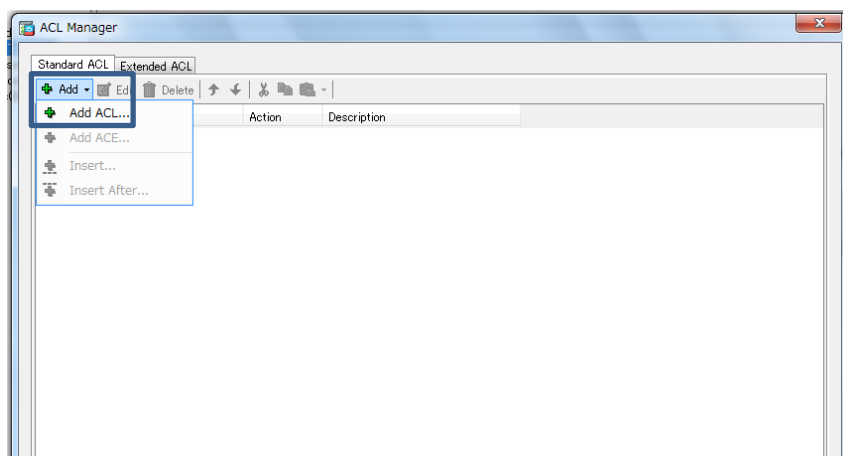


図 25 ACL の設定(1)

25) 「ACL Name」を入力し、「OK」をクリックします。

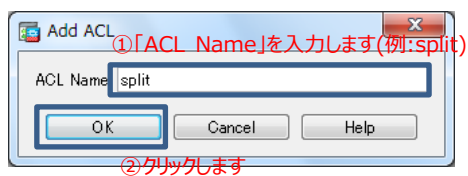


図 26 ACL の設定(2)

26) 「Add」>「Add ACE」を開きます。

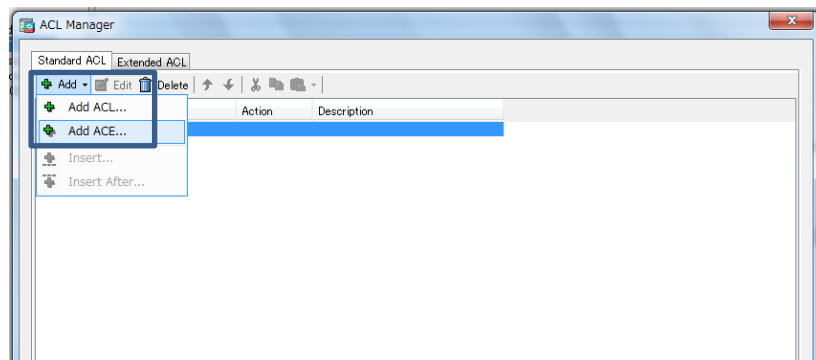


図 27 ACE の設定(1)



27) ACE の設定をします。

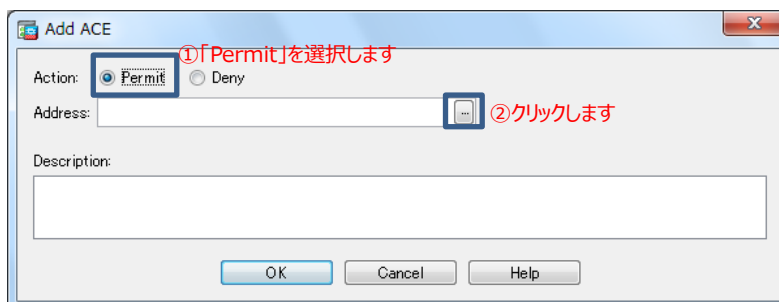


図 28 ACE の設定(2)

28) 「inside-network」を選択し、「OK」をクリックします。

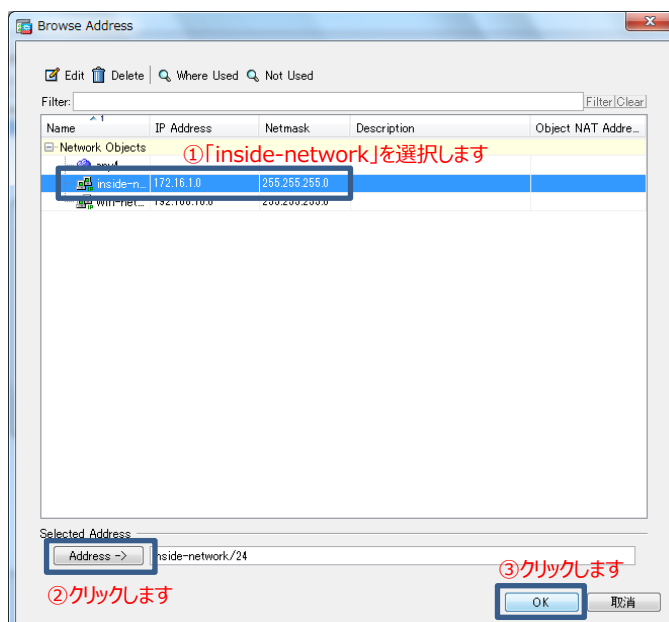


図 29 ACE の設定(3)

29) 「OK」をクリックして先に進みます。

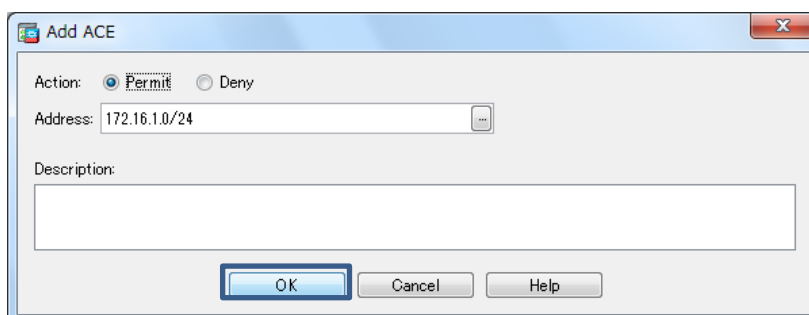


図 30 ACE の設定の完了



30) 「OK」をクリックして ACL の設定を完了します。

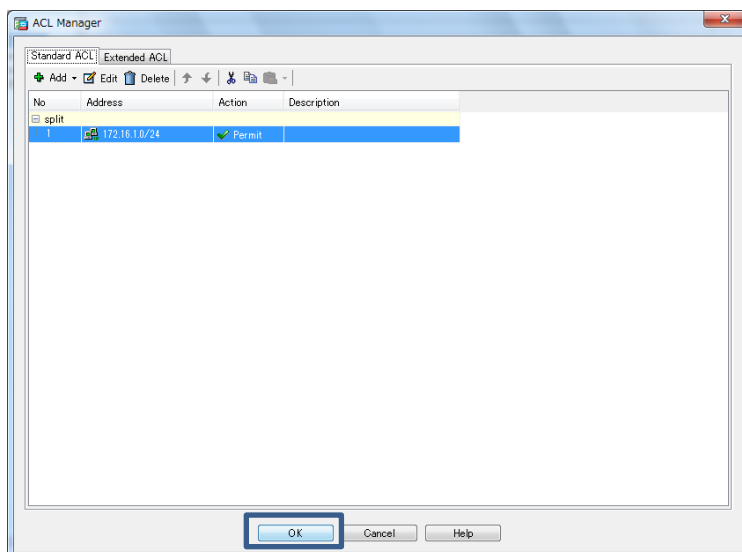


図 31 ACL の設定の完了

31) 「OK」をクリックし、スプリットトンネリングの設定を完了します。

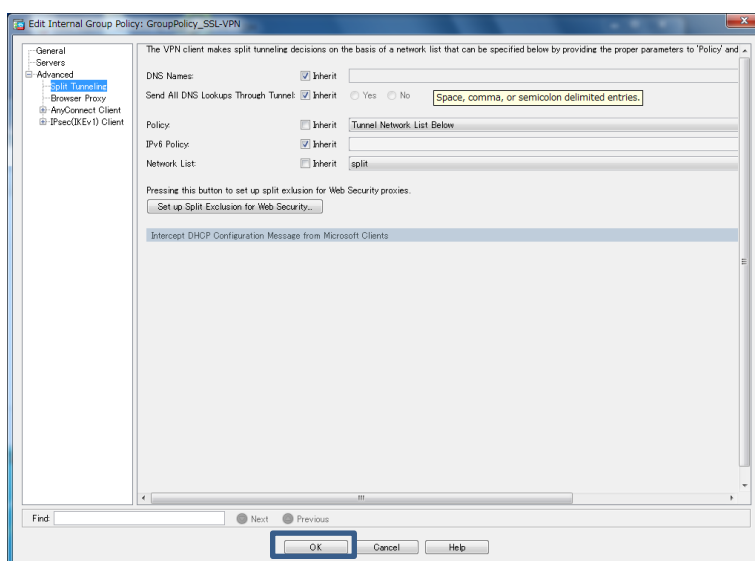


図 32 スプリットトンネリングの設定の完了



32) 「Apply」をクリックして ASA に設定を反映します。

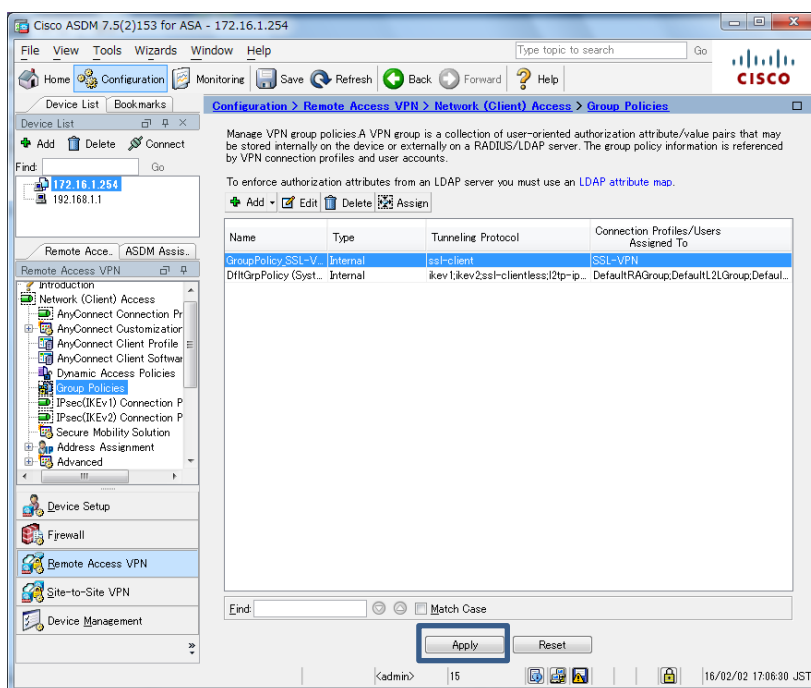


図 33 Group Policy の設定完了と設定の反映

33) ASA に実行されるコマンドのプレビューが表示されるので、「Send」をクリックして実行します。

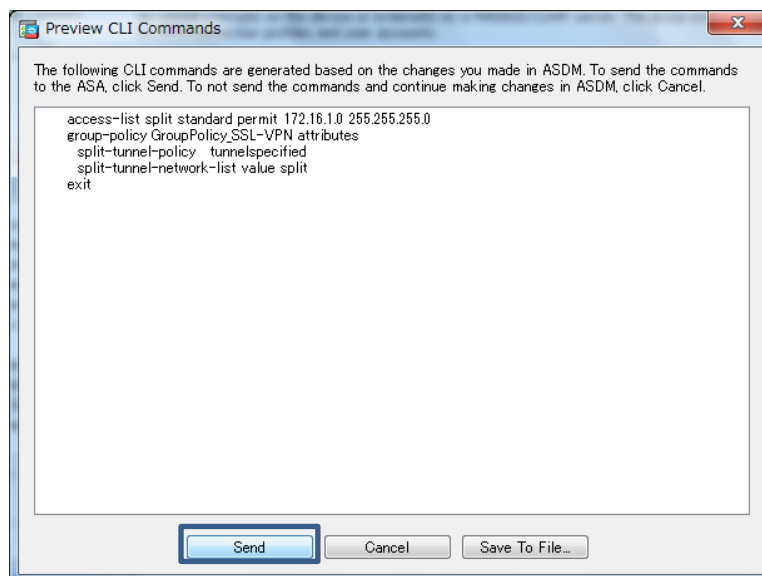


図 34 コマンドのプレビュー



3.2 クライアント PC の AnyConnect VPN 設定

本節ではクライアント PC で AnyConnect VPN を設定する手順について説明します。

3.2.1 AnyConnect Secure Mobility Client のインストール

- 1) クライアント PC で WEB ブラウザを起動し、URL に「http://<ASA の outside の IP アドレス>」を入力し、ASA にアクセスします。図 35 のように表示されるので、「このサイトの閲覧を続行する」をクリックして先に進みます。

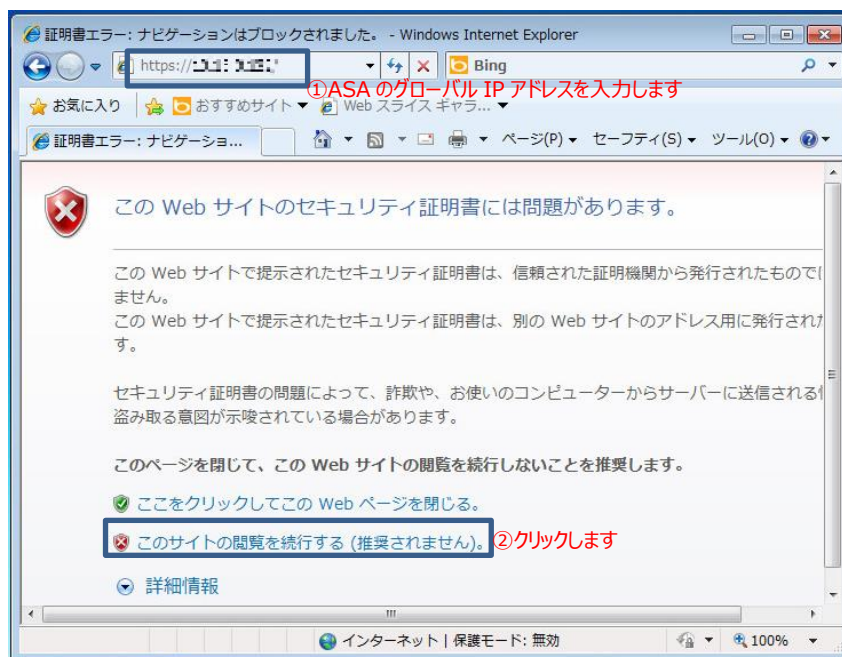


図 35 クライアント PC から ASA へのアクセス

- 2) ASA で設定した VPN クライアントのユーザ名とパスワードを入力してログインします。



図 36 ログイン画面



- 3) AnyConnect Secure Mobility Clientのインストールを行います。図 37 の画面で「skip」をクリックします。

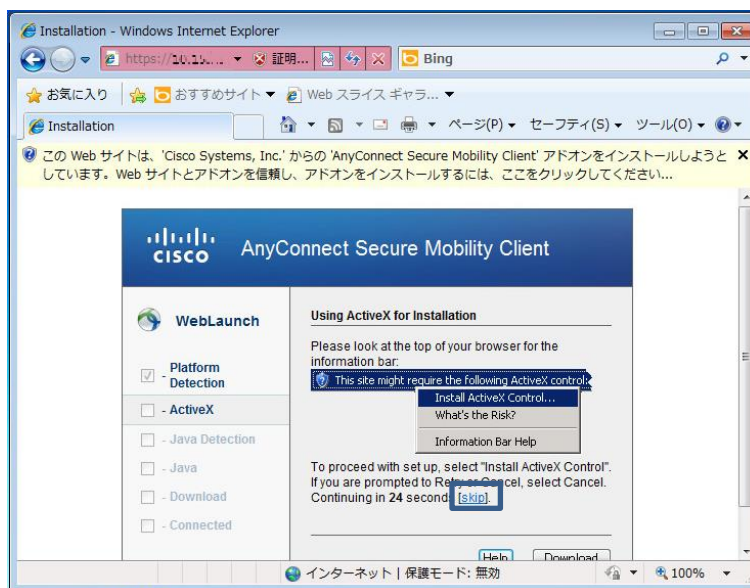


図 37 AnyConnect Secure Mobility Client のインストール(1)

- 4) 図 38 の画面が表示されますが、しばらく待ち、「Manual Installation」に進みます。



図 38 AnyConnect Secure Mobility Client のインストール(2)



5) 「AnyConnect VPN」をクリックします。

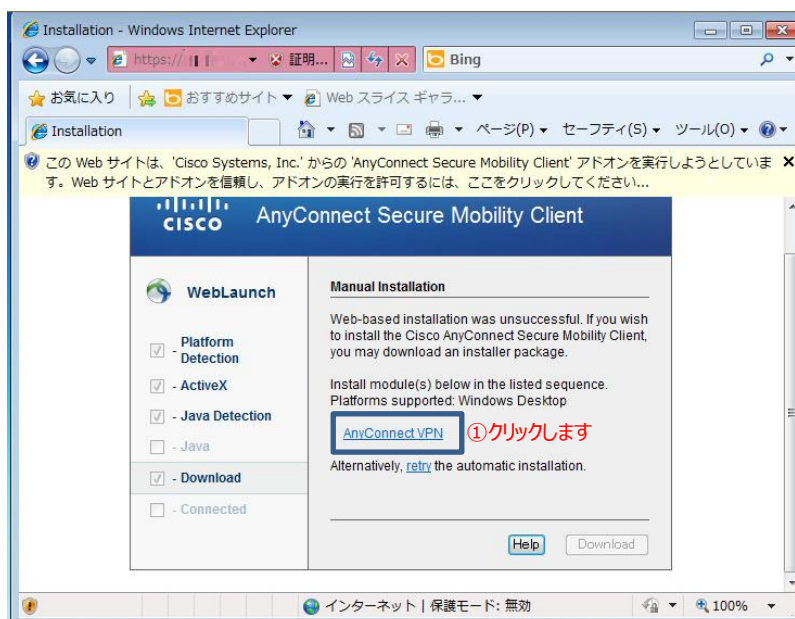


図 39 AnyConnect Secure Mobility Client のインストール(3)

6) 「実行」をクリックします。



図 40 AnyConnect Secure Mobility Client のインストール(4)

7) 「実行する」をクリックします。



図 41 AnyConnect Secure Mobility Client のインストール(5)



- 8) End-User License Agreementにおいて「I accept the terms in the License Agreement」にチェックを要れ、「Next」をクリックします。



図 42 AnyConnect Secure Mobility Client のインストール(6)

- 9) 「Install」をクリックします。

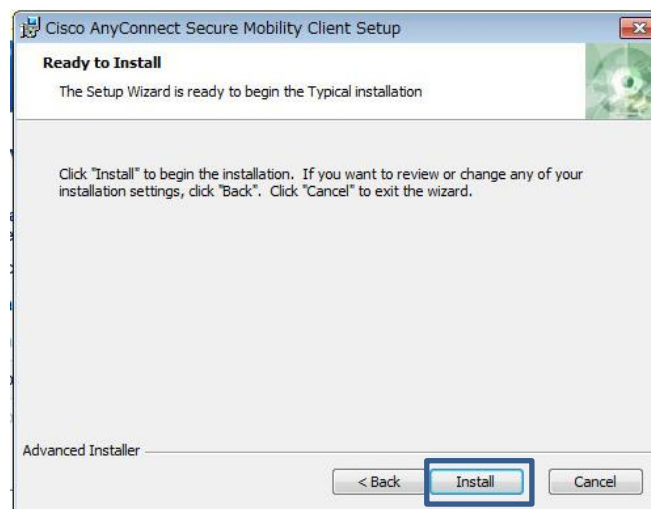


図 43 AnyConnect Secure Mobility Client のインストール(7)



10) 「Finish」をクリックしてインストールを完了します。



図 44 AnyConnect Secure Mobility Client のインストールの完了

3.2.2 AnyConnect VPN の接続

1) Windows のスタートメニューから「Cisco AnyConnect Secure Mobility Client」を起動します。

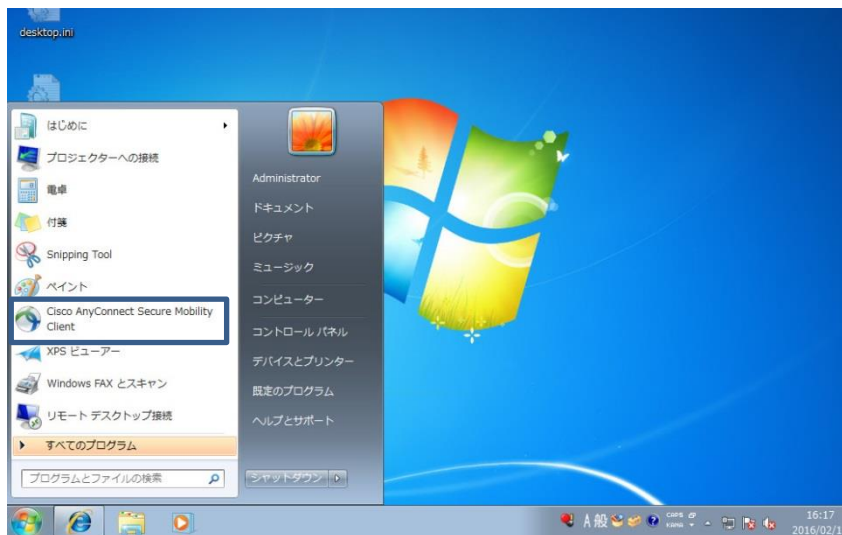


図 45 Cisco AnyConnect Secure Mobility Client の起動



- 2) Cisco AnyConnect Secure Mobility Client が起動したら、VPN の接続先である ASA の outside の IP アドレスを入力し、「Connect」をクリックします。



図 46 VPN の接続

- 3) セキュリティ警告のメッセージが表示されますが、「Connect Anyway」をクリックします。



図 47 警告メッセージ

- 4) ASA で設定した VPN クライアントのユーザ名とパスワードを入力して VPN に接続します。

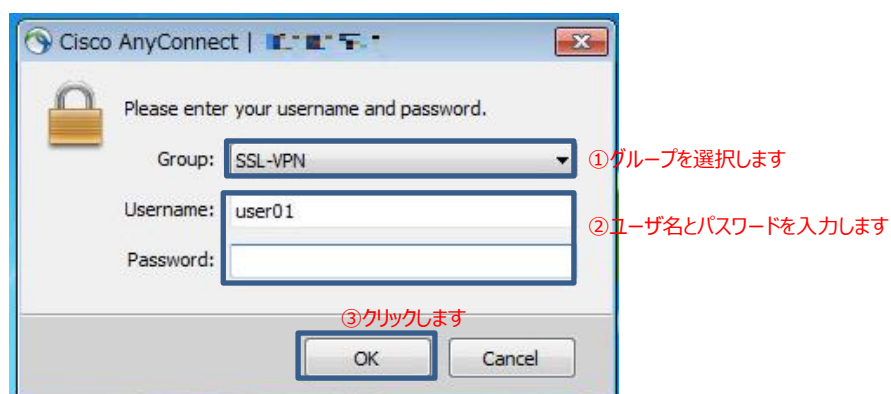


図 48 VPN ユーザーの認証



- 5) VPN に接続できると、右下のアイコンに鍵マークが表示され、これをクリックすると Cisco AnyConnect Secure Mobility Client が起動します。次に「VPN」またはををクリックします。左下のアイコンをクリックします。

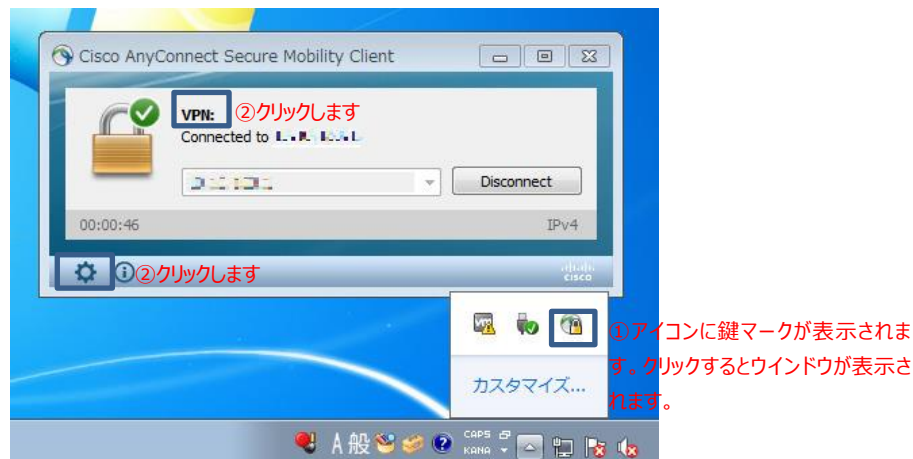


図 49 VPN 接続の完了

- 6) 統計情報などのステータスが確認できます。

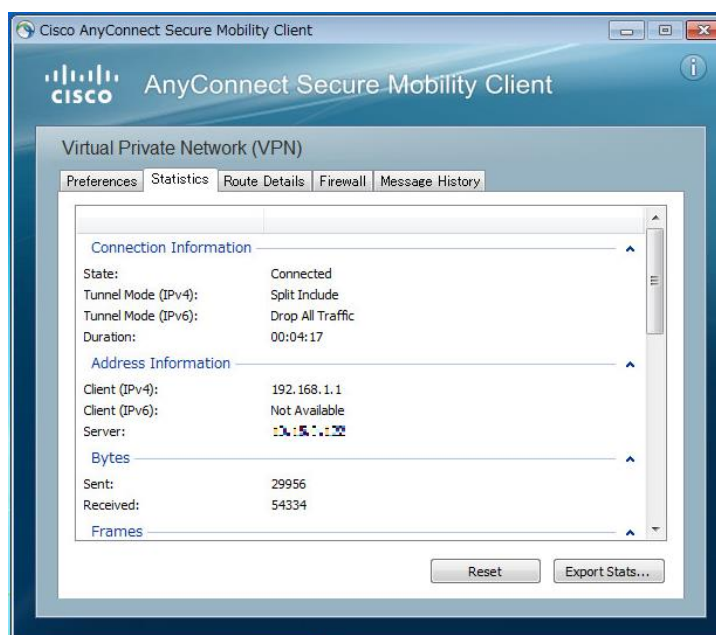


図 50 VPN クライアントの統計情報



- 7) ASDM で「Monitoring」>「VPN」>「VPN Statistics」>「Sessions」を開き、VPN クライアントのセッションを確認します。

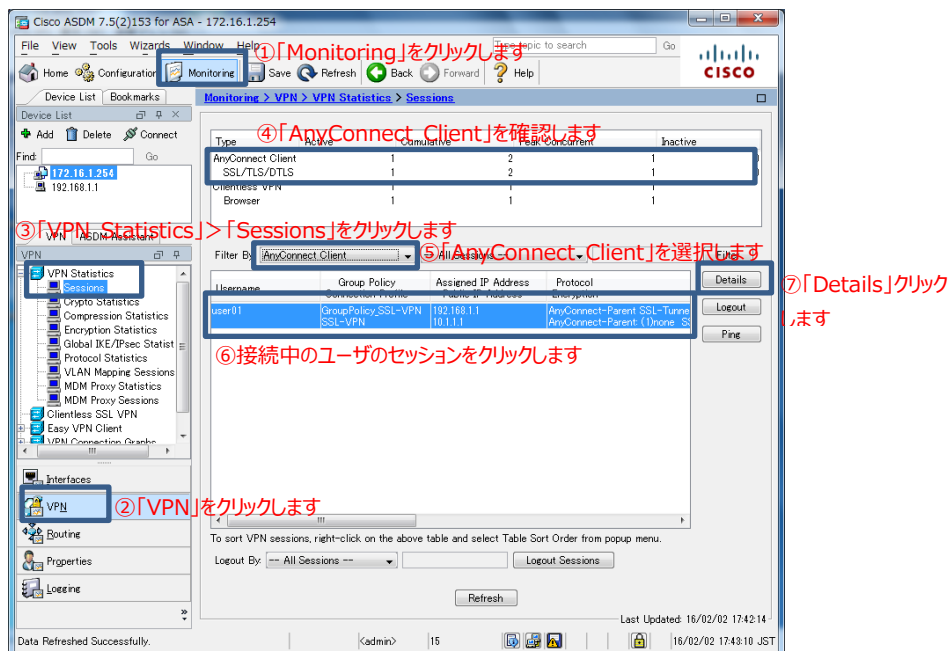


図 51 VPN クライアントセッションの確認

- 8) 接続中のユーザのセッションの詳細情報が確認できます。

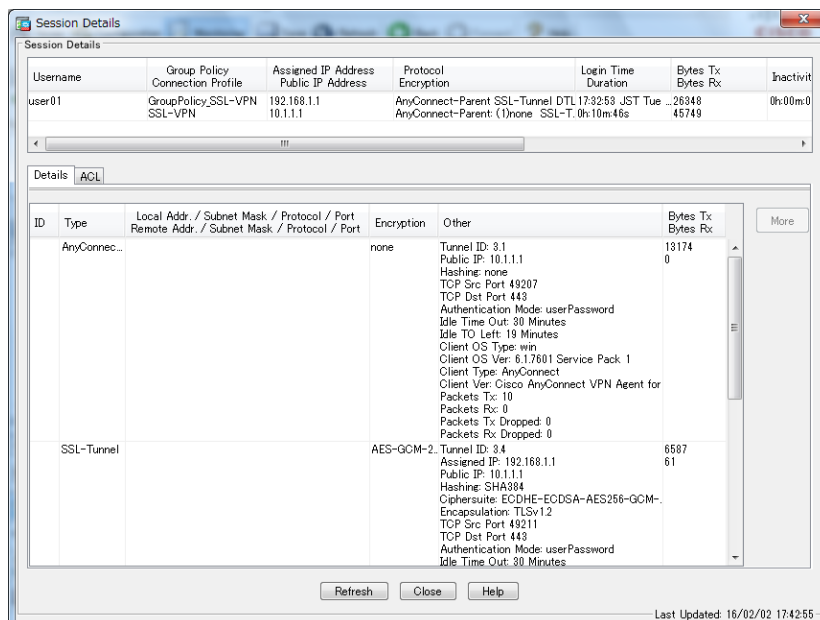


図 52 VPN セッションの詳細情報

お問い合わせ

Q 製品のご購入に関するお問い合わせ

<https://info-networld.smartseminar.jp/public/application/add/152>

Q ご購入後の製品導入に関するお問い合わせ

弊社担当営業にご連絡ください。

Q 製品の保守に関するお問い合わせ

保守開始案内に記載されている連絡先にご連絡ください。

本書に記載されているロゴ、会社名、製品名、サービス名は、一般に各社の登録商標または商標です。
本書では、®、™、©マークを省略しています。

www.networld.co.jp

株式会社ネットワーク

