Cisco Start Firewall

Cisco ASA 5506-X サイト間 VPN の設定

2016 年 4 月 18 日
第 1.1 版

www.networld.co.jp

株式会社ネットワールド

Networld

改訂履歴

版番号	改訂日	改訂者	改訂内容
1.0	2016 年 3 月 3 日	ネットワールド	● 新規
1.1	2016 年 4 月 18 日	ネットワールド	● ルーティング設定を追加
			●
			●

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ございません。
- 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ございません。

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
<italic>（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。

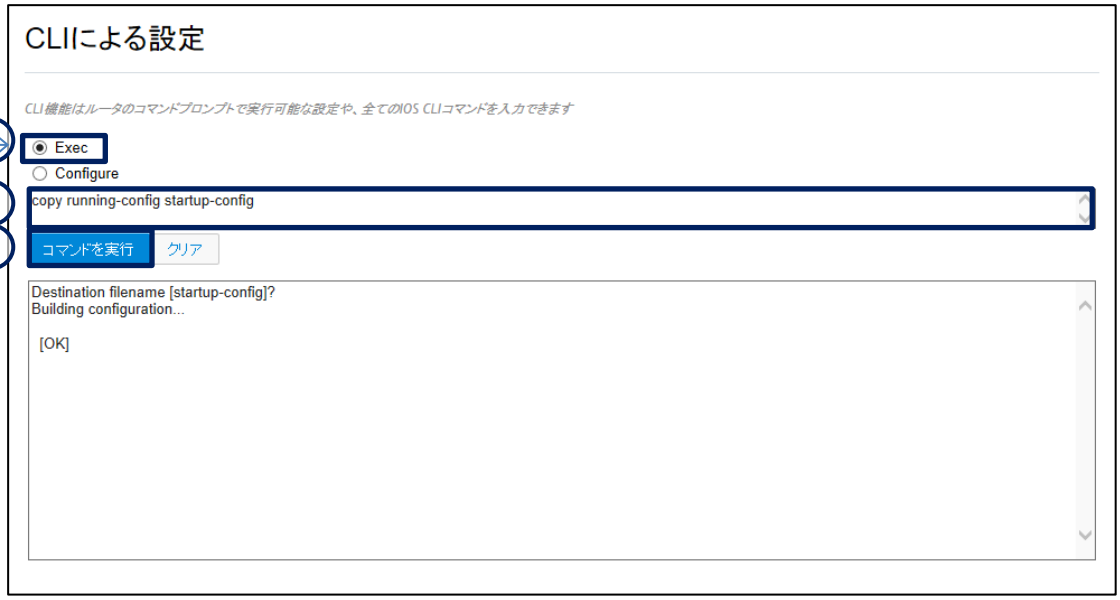
(2) テキストボックスに以下のコマンドを入力します。

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]



目次

1. はじめに

本書では Cisco ASA 5506-X におけるサイト間 VPN の設定手順について説明します。

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 サイト間 VPN について

サイト間 VPN(Virtual Private Network)とは、IPSec による暗号化および認証を使用し、Cisco ASA 5500 シリーズ等を終端装置としたトンネル技術の名称です。サイト間 VPN により、インターネットを介してオフィスネットワーク間にセキュアな通信を提供する事ができます。

2. システム構成

2.1 システム構成

本書でのサイト間 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。ASA-1 および ASA-2 は別紙「Cisco ASA 5506-X クイックスタートガイド」の内容に基づいて初期設定を行っており、各管理 PC から ASDM により ASA にアクセスできる状態および、VPN を終端する両端の ASA が互いにインターネットを介して GE1/1(outside)にアクセスできる状態を前提としています。

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)2 ASDM Version 7.5(2)153	ASA-1 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)
			ASA-2 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:172.16.2.254/24 Security level:100(デフォルト)
クライアント PC 兼管理用 PC		OS : Windows 7 ターミナルアプリケーション (Tera Term) Cisco ASDM-IDM Launcher v1.7 (0)	クライアント PC-1 インタフェース IP アドレス:172.16.1.1/24
			クライアント PC-2 インタフェース IP アドレス:172.16.2.1/24

表 3 ASA 5506-X のネットワーク設定

ルーティング	ASA-1	outside で DHCP によりデフォルトルートを取得	宛先:172.16.2.0/24 ネクストホップ:ASA-2 の outside の IP アドレス
	ASA-2	outside で DHCP によりデフォルトルートを取得	宛先:172.16.1.0/24 ネクストホップ:ASA-1 の outside の IP アドレス
NAT	inside(すべてのトラフィック)→outside への PAT		

表 4 VPN のポリシー

設定機器	ピア IP アドレス	ローカルネットワーク	リモートネットワーク	Pre-shared Key	NAT 除外
ASA-1	ASA-2 の outside	172.16.1.0/24	172.16.2.0/24	cisco	inside
ASA-2	ASA-1 の outside	172.16.2.0/24	172.16.1.0/24	cisco	inside

3. サイト間 VPN の設定およびセッションの確認

3.1 サイト間 VPN の設定

本節ではサイト間 VPN の設定手順について説明します。

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

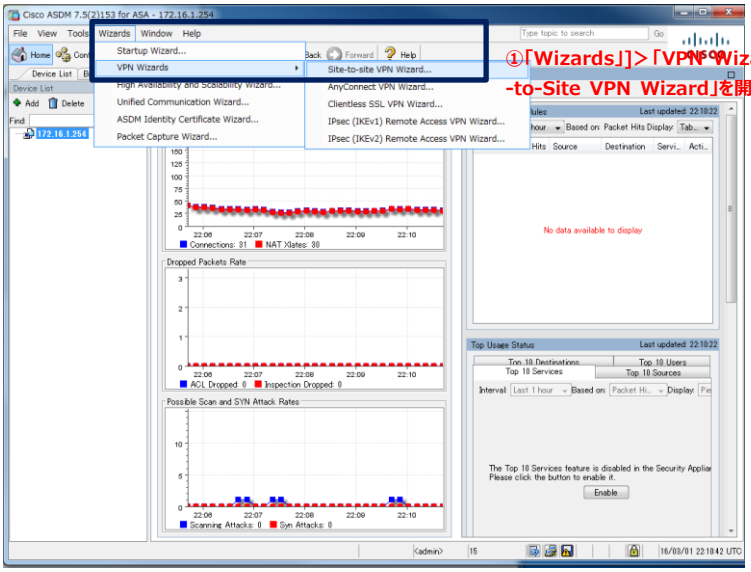


図 2 Site-to-Site VPN Wizard を開く

2) Site-to-Site VPN Wizard が開始されます。「Next」をクリックして先に進みます。

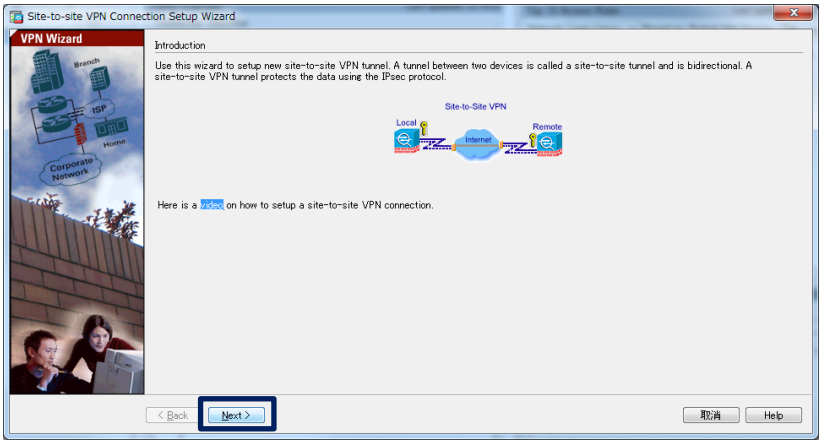


図 3 Site-to-Site VPN Wizard の開始

3) 「Peer IP Address」に VPN ピアとなる IP アドレス(ここでは ASA-2 の ouside)を入力し、「VPN Access Interface」は「Outside」を選択し、「Next」をクリックします。

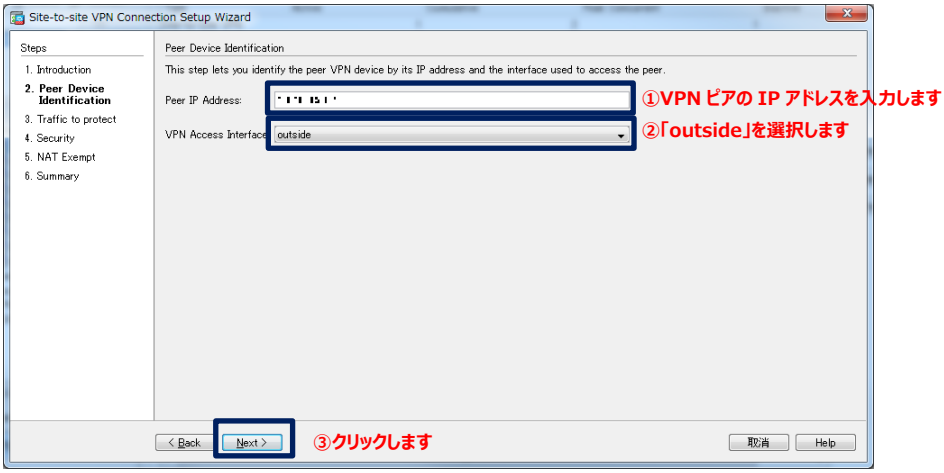


図 4 VPN ピアの設定

4) 「Local Network」にローカルのネットワークセグメント(ここでは ASA-1 の LAN)を、「Remote Network」に対向側のネットワークセグメント(ここでは ASA-2 の LAN)を入力し、「Next」をクリックします。

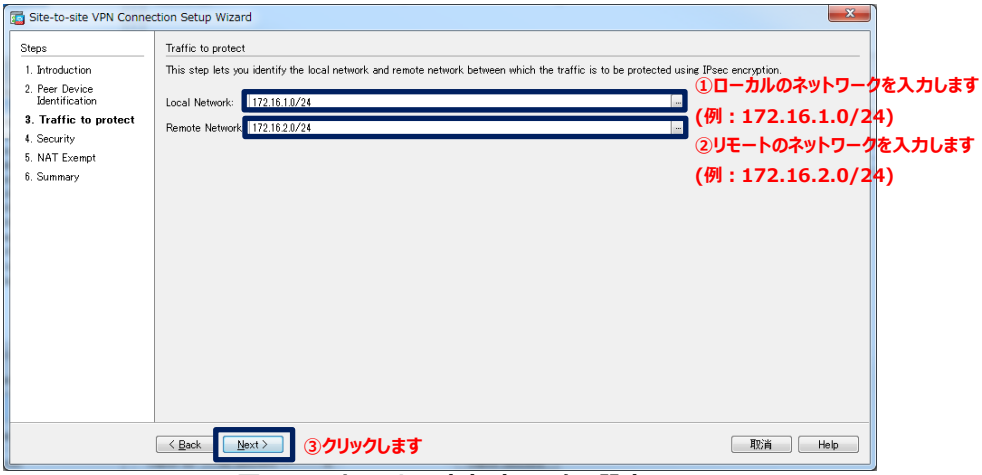


図 5 ローカル・リモートネットワークの設定

5) Pre-shared Key (事前共有鍵)を入力し、「Next」をクリックします。

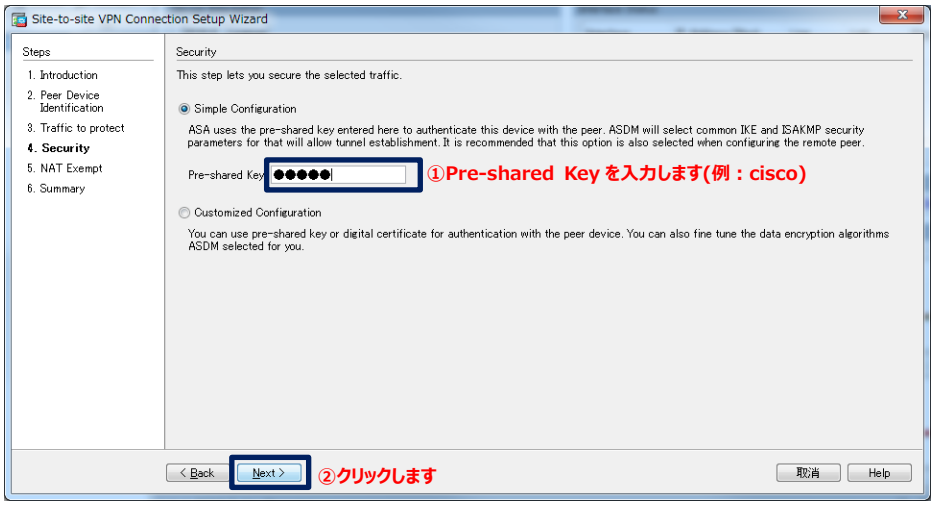


図 6 Pre-shared Key の設定

6) NAT 除外の設定を入力し、「Next」をクリックします。

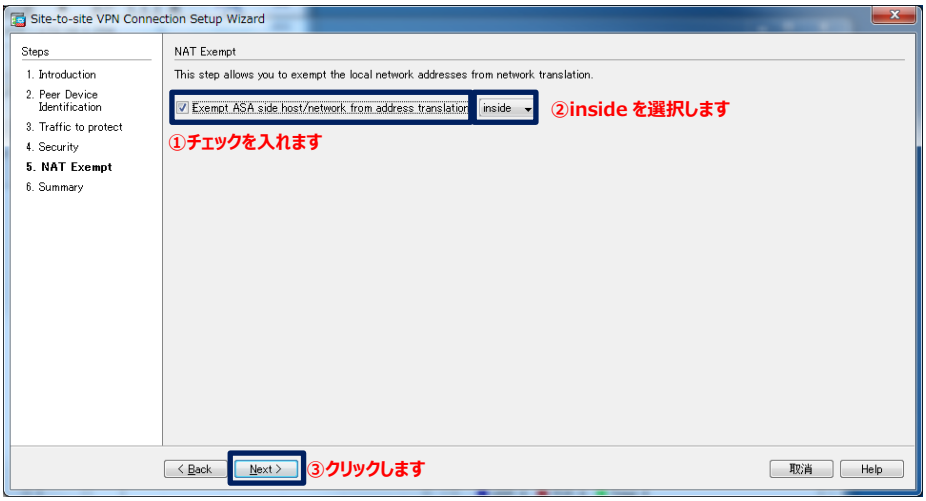


図 7 NAT 除外の設定

7) 「Finish」をクリックし、設定を完了します。

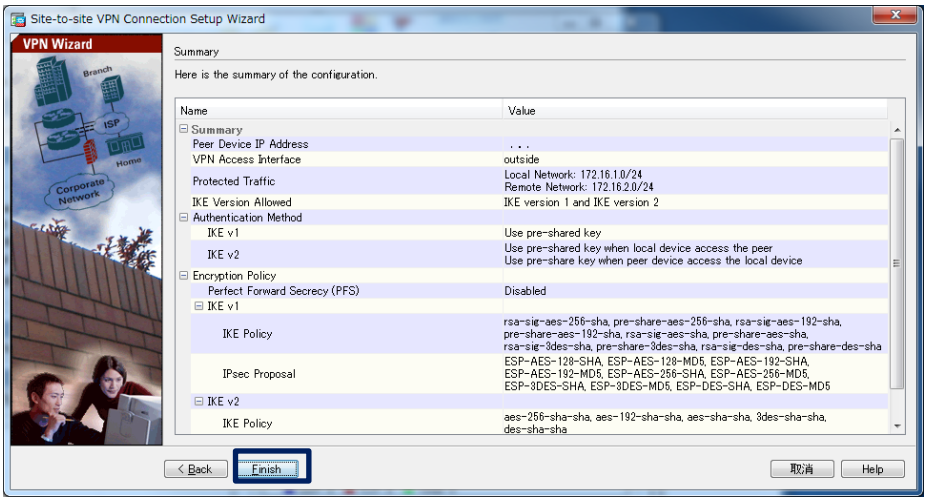


図 8 設定の完了

8) 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。

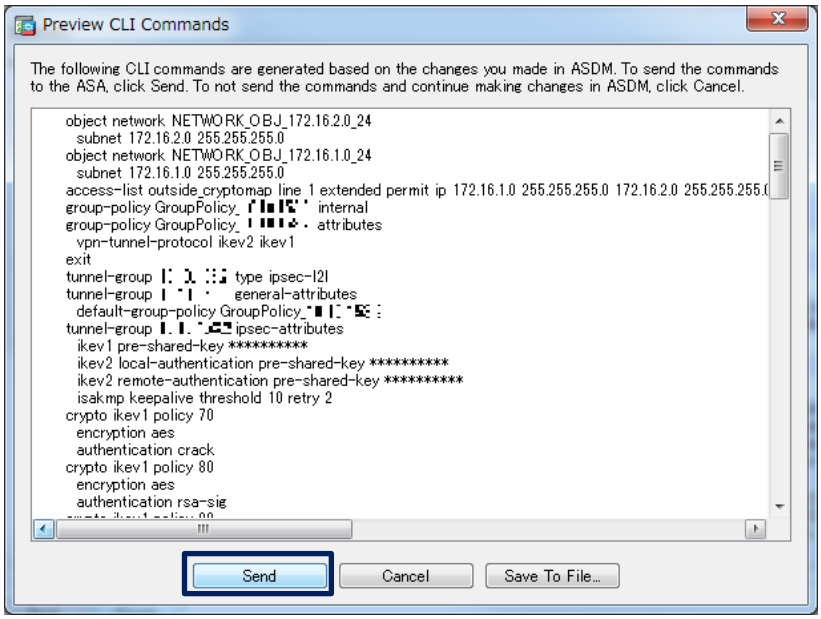


図 9 コマンドのプレビュー

9) 既にサポートされていないコマンドに対するエラーが表示される場合があり、「Close」をクリックします。

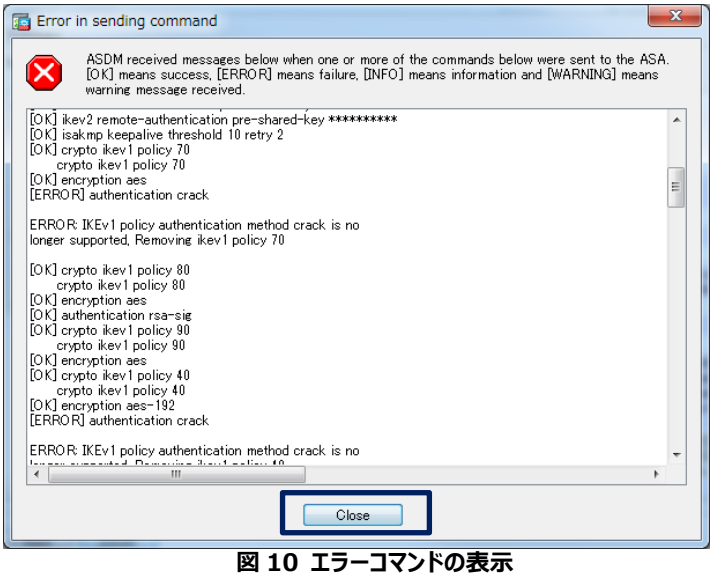
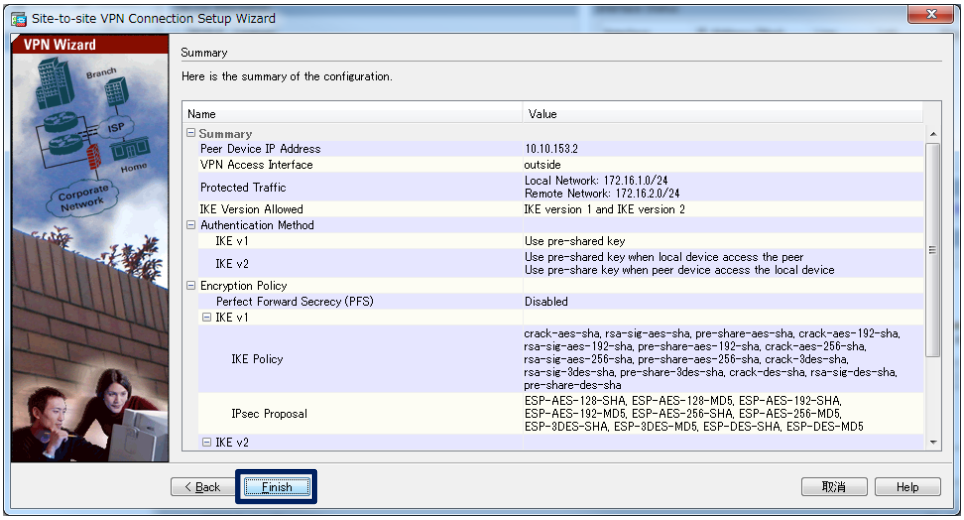


図 10 エラーコマンドの表示

10) 再度コマンドの実行を求められる場合があります。



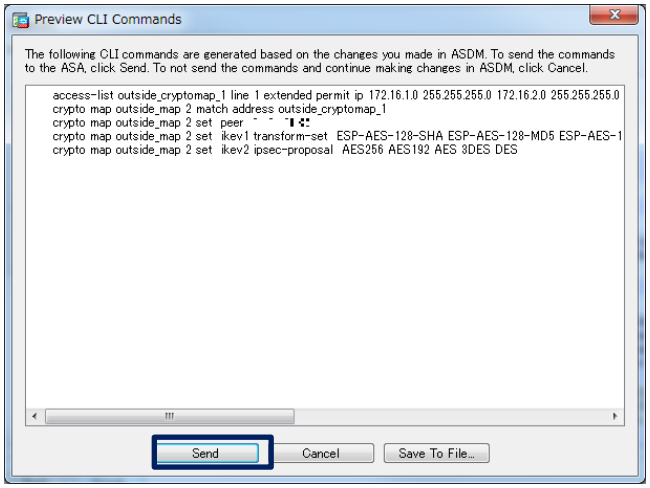


図 11 コマンドの再実行

11) CLI のグローバルコンフィグレーションモードで、対向のリモートネットワーク(inside 側のネットワーク)に対するルーティングの設定を行います。

asa-1(config)#route outside 172.16.2.0 255.255.255.0 <ASA-2 の outside の IP アドレス>

12) 同様の設定を ASA-2 でも行い、PC-1 と PC-2 の間で通信が成功したら設定完了となります。

3.2 サイト間 VPN セッションの確認

本節ではサイト間 VPN のセッション情報の確認方法について説明します。

1) ASDM で「Monitoring」>「VPN」>「VPN Statistics」>「Sessions」を開き、VPN セッションの詳細情報を確認します。(PC 間で通信を発生させないとセッションは表示されません)

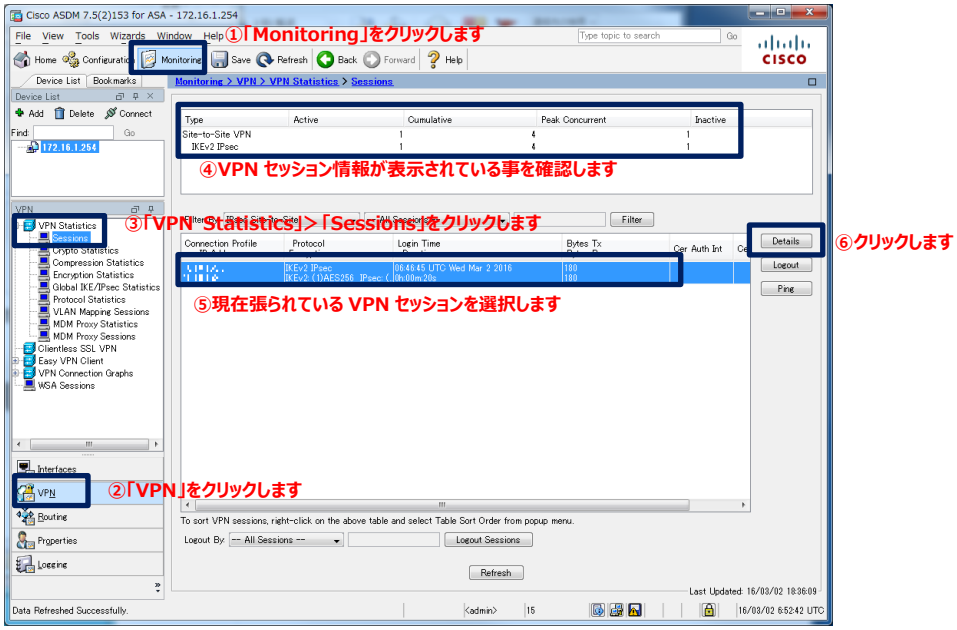


図 12 サイト間 VPN セッション情報の表示

2) セッションの詳細情報が表示されます。

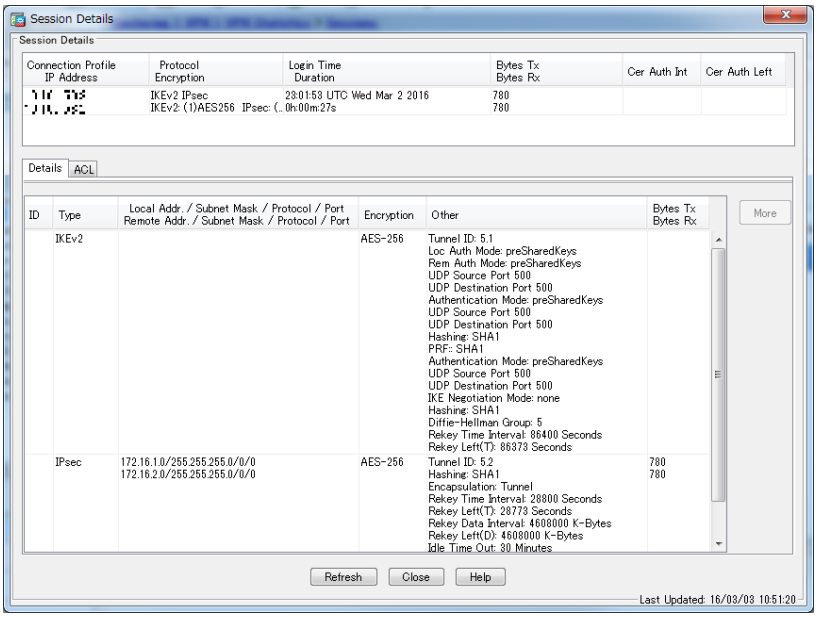


図 13 セッション情報の詳細

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。

www.networld.co.jp

株式会社ネットワールド

Networld