Cisco ASA 5500 シリーズ スタートアップ ガイド

Cisco ASA 5500 Series Getting Started Guide

Cisco ASA 5510、ASA 5520、ASA 5540、ASA 5550

ソフトウェア バージョン 8.3

Text Part Number: 78-19186-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

Cisco ASA 5500 シリーズ スタートアップ ガイド
© 2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2010, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

CHAPTER 1

始める前に

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの実装に必要な設置および設定の手順を確認するには、次の表を使用してください。

このマニュアルに記載されている適応型セキュリティ アプライアンスの実装内容は、次のとおりです。

ASA 5500

実行内容	参照先
シャーシの取り付け	第 4 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 の取り付け」
インターフェイス ケーブルの接続	第 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームにおけるインターフェイス ケーブルの接続」
適応型セキュリティ アプライアンスの初期セットアップの実行	第 7 章「適応型セキュリティ アプライアンスの設定」
各実装内容に応じた適応型セキュリティ アプライアンスの設定	第 8 章「シナリオ：DMZ 設定」 第 9 章「シナリオ：IPsec リモート アクセス VPN 設定」 第 10 章「シナリオ：Cisco AnyConnect VPN クライアント用接続の設定」 第 11 章「シナリオ：SSL VPN クライアントレス接続」 第 12 章「シナリオ：サイトツーサイト VPN 設定」
オプション機能および拡張機能の設定	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』
日常のシステム動作	『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series System Log Messages*』

AIP SSM 搭載 ASA 5500

実行内容	参照先
シャーシの取り付け	第 4 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 の取り付け」
AIP SSM の取り付け	第 5 章「オプションの SSM の取り付け」
インターフェイス ケーブルの接続	第 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームにおけるインターフェイス ケーブルの接続」
適応型セキュリティ アプライアンスの初期セットアップの実行	第 7 章「適応型セキュリティ アプライアンスの設定」
AIP SSM に対する適応型セキュリティ アプライアンスの設定	第 9 章「シナリオ：IPsec リモートアクセス VPN 設定」
侵入防御のための IPS ソフトウェアの設定	『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*』
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』 『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series System Log Messages*』

CSC SSM 搭載 ASA 5500

実行内容	参照先
シャーシの取り付け	第 4 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 の取り付け」
CSC SSM の取り付け	第 5 章「オプションの SSM の取り付け」
インターフェイス ケーブルの接続	第 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームにおけるインターフェイス ケーブルの接続」
適応型セキュリティ アプライアンスの初期セットアップの実行	第 7 章「適応型セキュリティ アプライアンスの設定」
コンテンツ セキュリティのための適応型セキュリティ アプライアンスの設定	第 14 章「CSC SSM の設定」
CSC SSM の設定	『*Cisco Content Security and Control SSM Administrator Guide*』
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』 『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series System Log Messages*』

4GE SSM 搭載 ASA 5500

実行内容	参照先
シャーシの取り付け	第 4 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 の取り付け」
4GE SSM の取り付け	第 5 章「オプションの SSM の取り付け」
インターフェイス ケーブルの接続	第 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームにおけるインターフェイス ケーブルの接続」
適応型セキュリティ アプライアンスの初期セットアップの実行	第 7 章「適応型セキュリティ アプライアンスの設定」
光ファイバ モジュールの取り付け	第 5 章「オプションの SSM の取り付け」
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』 『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series System Log Messages*』

ASA 5550

実行内容	参照先
シャーシの取り付け 光ファイバ モジュールの取り付け（存在する場合） インターフェイス ケーブルの接続	第 3 章「ASA 5550 の取り付け」
適応型セキュリティ アプライアンスの初期セットアップの実行	第 7 章「適応型セキュリティ アプライアンスの設定」
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』 『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series System Log Messages*』

関連ドキュメント

詳細については、次のマニュアルを参照してください。

- 『*Documentation Roadmap for the Cisco ASA 5500 Series*』
- 『*Cisco ASA 5500 Series Release Notes*』
- 『*Release Notes for Cisco ASDM*』
- 『*Cisco ASA 5500 Series Command Reference*』
- 『*Cisco ASA 5500 Series Configuration Guide using the CLI*』
- 『*Cisco ASA 5500 Series System Log Messages*』
- 『*Migrating to ASA for VPN 3000 Series Concentrator Administrators*』
- 『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』
- 『*Open Source Software Licenses for ASA and PIX Security Appliances*』

CHAPTER 2

ASA 5550 のスループットの最大化

（注） この章の内容は、Cisco ASA 5550 にだけ適用されます。

Cisco ASA 5550 適応型セキュリティ アプライアンスは、この章で説明するガイドラインに従って設定する時にスループットが最大になるように設計されています。

この章は、次の項で構成されています。

組み込みネットワーク インターフェイス

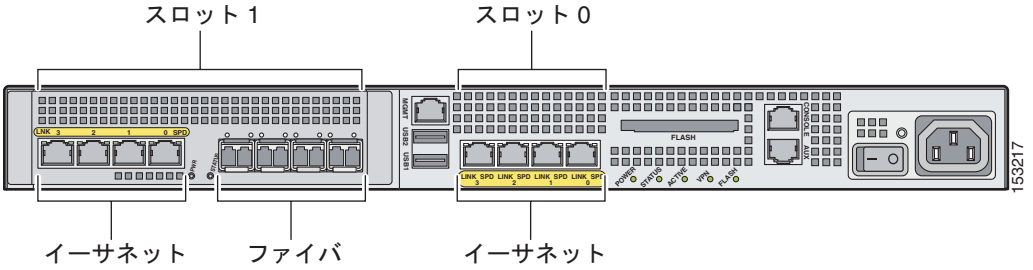
適応型セキュリティ アプライアンスは、銅線ギガビット イーサネットおよびファイバ ギガビット イーサネット接続を可能とする 2 つの内部バスを備えています。

- スロット 0（バス 0 に対応）には、4 つの組み込み銅線ギガビット イーサネット ポートが用意されています。
- スロット 1（バス 1 に対応）には、4 つの組み込み銅線ギガビット イーサネット ポートと、ファイバ ギガビット イーサネット接続をサポートする 4 つの組み込み SFP が用意されています。

（注） 適応型セキュリティ アプライアンス上でファイバ接続を確立するには、使用するファイバ ポートごとに SFP モジュールを注文してインストールする必要があります。ファイバ ポートと SFP モジュールの詳細については、「SFP モジュールの取り付け」（P.3-6）を参照してください。

図 2-1 に、Cisco ASA 5550 の組み込みポートを示します。

図 2-1　ASA 5550 の組み込みポート



（注） スロット 1 には、4 つの銅線イーサネット ポートと、4 つのファイバ イーサネット ポートが用意されていますが、一度に使用できるスロット 1 のポートは 4 つまでです。たとえば、2 つのスロット 1 銅線ポートと 2 つのファイバ ポートを使用できますが、すでに 4 つのスロット 1 銅線ポートをすべて使用している場合、ファイバ ポートは使用できません。

スループットを最大化するためのトラフィックのバランシング

トラフィックのスループットを最大化するには、トラフィックがデバイス内の 2 つのバス間で均等に分配されるように適応型セキュリティ アプライアンスを設定する必要があります。そのためには、すべてのトラフィックがバス 0（スロット 0）とバス 1（スロット 1）の両方を通過し、入力は片方のバス、出力はもう片方のバスを通るようにネットワークを設計します。

図 2-2 と図 2-3 では、すべてのトラフィックがデバイス内の両方のバスを通過し、適応型セキュリティ アプライアンスがスループットを最大化できるように、ネットワークのトラフィックが分散されています。

図 2-2　スループットを最大化するために均等に分配されたトラフィック（銅線から銅線へ）

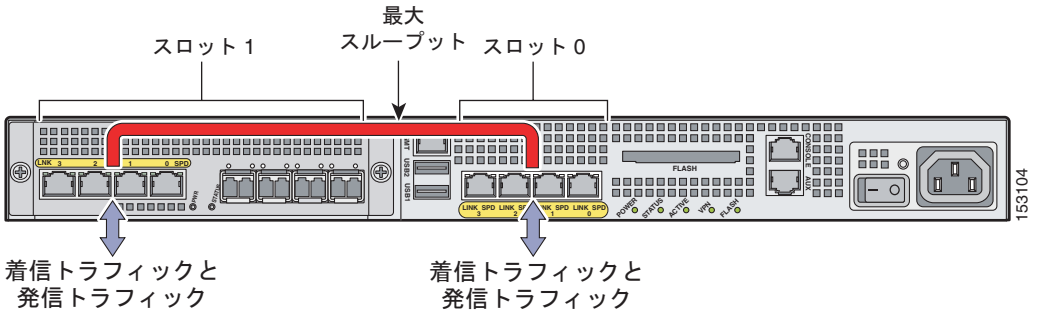


図 2-3　スループットを最大化するために均等に分配されたトラフィック（銅線からファイバへ）

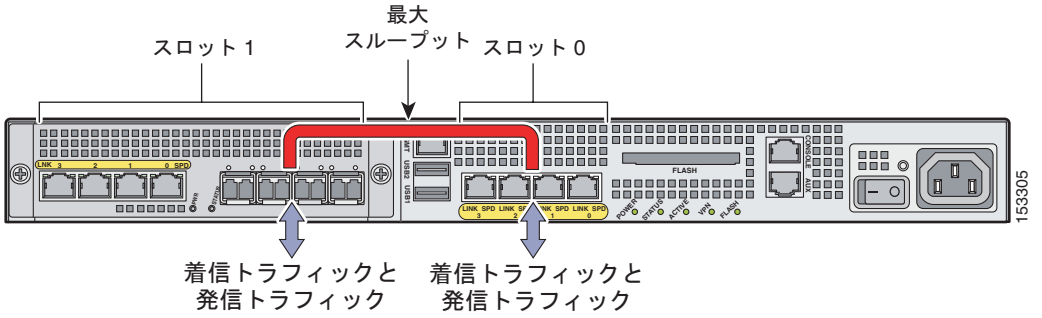
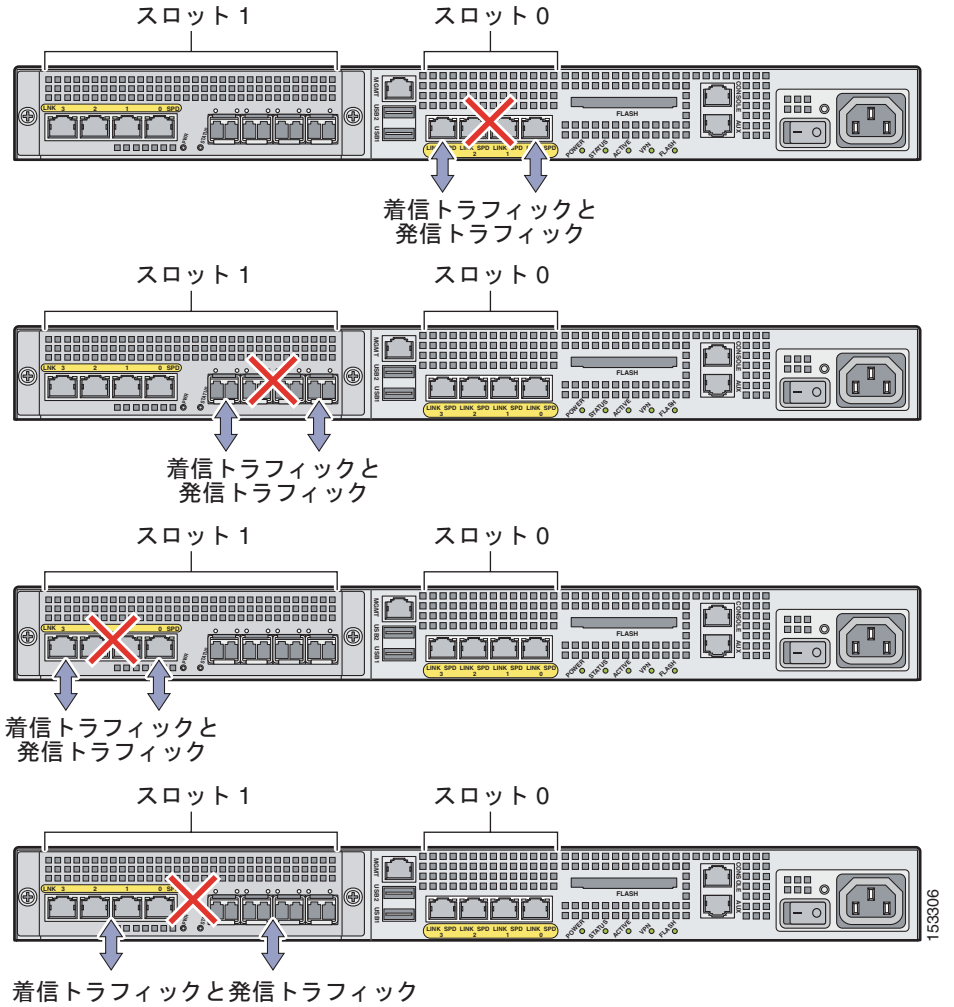


図 2-4 に、ネットワーク トラフィックがデバイスの片方のバスしか通過しないために、適応型セキュリティ アプライアンスがスループットを最大化できない設定をいくつか示します。

図 2-4　スループットを最大化できない設定



（注）　**show traffic** コマンドを使用すれば、各バスにおけるトラフィックのスループットを確認できます。このコマンドの使用に関する詳細については、『*Cisco ASA 5500 Series Command Reference*』を参照してください。

次の作業

第 3 章「ASA 5550 の取り付け」に進みます。

CHAPTER 3

ASA 5550 の取り付け

注意 これらの手順を実行するときは、『*Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*』の安全に関する警告を読み、適切な安全手順に従ってください。

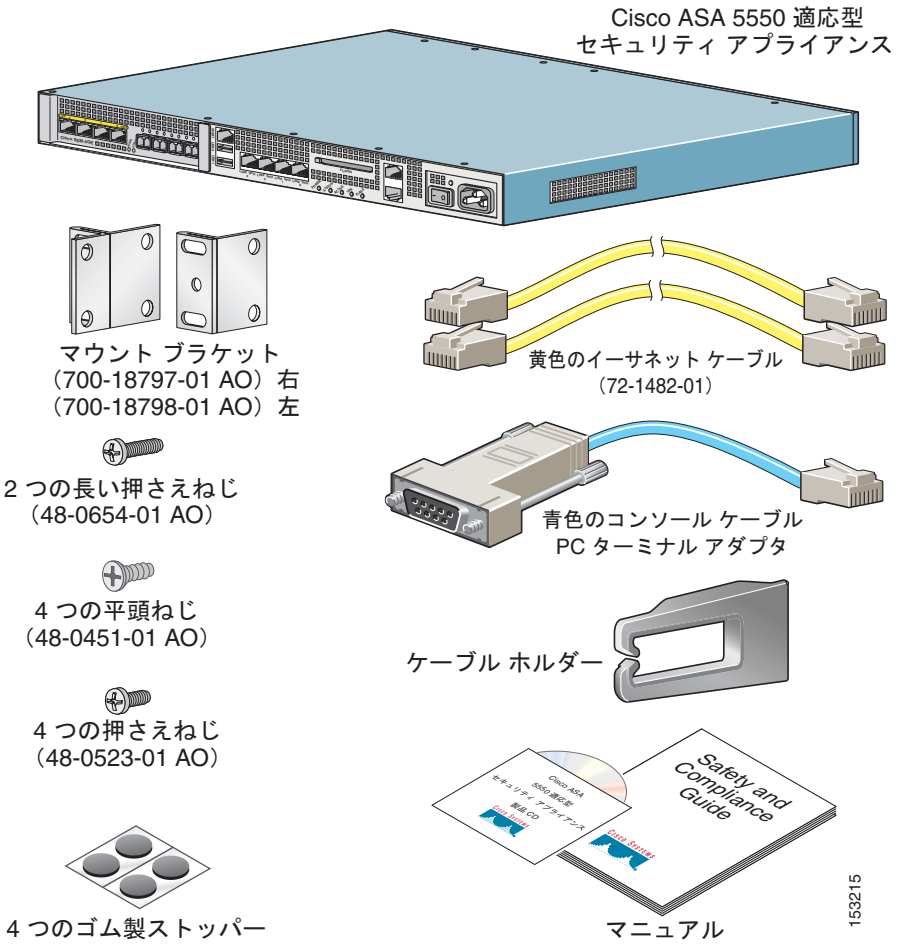
警告 **この装置の 設置、交換、保守は、訓練を受けた相応の資格のある人が行ってください。**ステートメント 49

この章では、ASA 5550 適応型セキュリティ アプライアンス、および適応型セキュリティ アプライアンスのラックマウント手順と取り付け手順について説明します。この章は、次の項で構成されています。

パッケージ内容の確認

図 3-1 に示すように、パッケージの内容をチェックし、Cisco ASA 5550 を取り付けるために必要な品目がすべてそろっていることを確認します。

図 3-1　ASA 5550 パッケージの内容



シャーシの取り付け

この項では、適応型セキュリティ アプライアンスのラックマウントおよび設置の手順について説明します。適応型セキュリティ アプライアンスは、19 インチ ラック（開口部は 17.5 または 17.75 インチ）にマウントできます。

警告　ラックにこの装置をマウントしたり、ラック上の装置の作業を行うときは、ケガをしないように、装置が安定した状態に置かれていることを十分に確認してください。安全に関するガイドラインは次のとおりです。

次の情報は、ラックへの機器の取り付けを計画する場合に役立ちます。

- ラックの周囲に、メンテナンスに必要な空間を確保します。
- 閉鎖型ラックに装置をマウントする場合は、換気が十分に行われるようにします。閉鎖型ラックに装置を詰め込みすぎないようにしてください。各装置で熱が発生するため、ラック内に装置を詰め込みすぎないように注意してください。
- 開放型ラックに装置をマウントする場合、ラックのフレームで吸気口や排気口をふさがないように注意してください。
- ラックに装置を 1 つだけマウントする場合は、ラックの一番下にマウントします。
- すでに別の装置がこのラックに取り付けられている場合は、最も重い装置をラックの一番下に取り付け、重い順にラックの下から上へと設置します。
- ラックにスタビライザが付属している場合、スタビライザを取り付けてから、ラックへの装置の取り付けまたはラックでの作業を行います。

警告　次の手順を実行する前に、電源が切れていることを確認してください（AC または DC）。DC 回路に電気が流れていないことを確認するには、パネル ボード上で DC 回路に対応している回路ブレーカーを確認して、回路ブレーカーを OFF の位置に切り替え、回路ブレーカーのスイッチ ハンドルを OFF の位置のままテープで固定します。

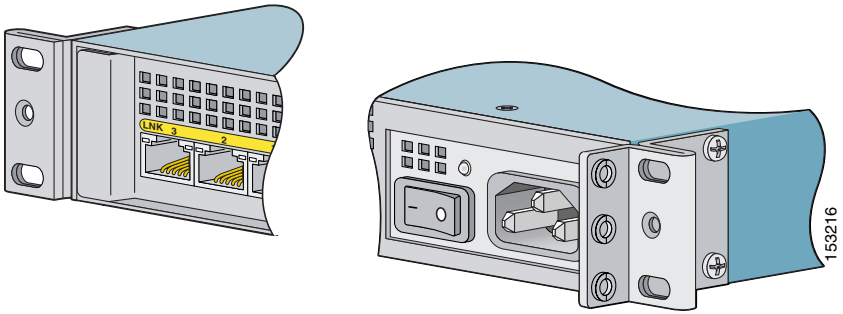
シャーシのラックマウント

シャーシをラックマウントするには、次の手順に従います。

（注）　マウント ブラケットを使用して、シャーシの前面パネルまたは背面パネルが外側に向くように、シャーシをラックの前面または背面にマウントできます。

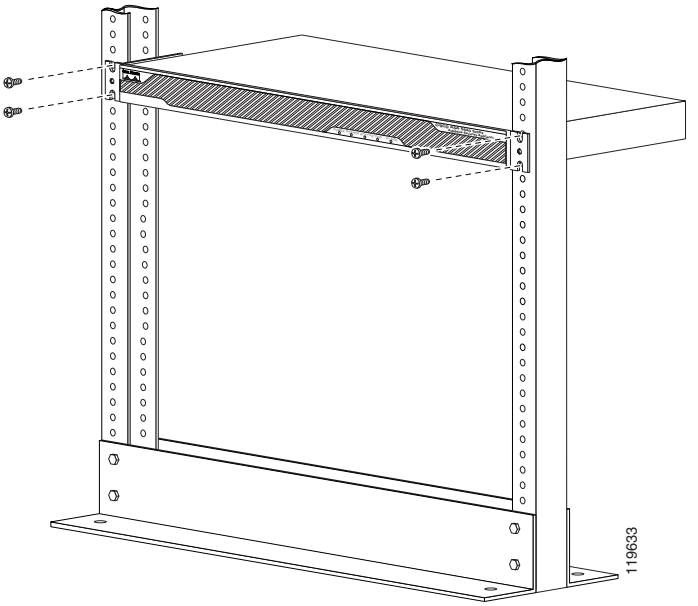
ステップ 1　付属のネジを使用して、シャーシにラックマウント ブラケットを取り付けます。ブラケットを穴に取り付けます（図 3-2 を参照）。ブラケットをシャーシに固定すると、ラックマウントできるようになります。

図 3-2　　左ブラケットと右ブラケットの取り付け



ステップ 2　付属のネジを使用して、シャーシをラックに取り付けます（図 3-3 を参照）。

図 3-3　シャーシのラックマウント



（注）　図 3-2 には、ラックマウント ブラケットをシャーシの背面に取り付けた図を、図 3-3 には、シャーシの前面に取り付けた図を示します。前面パネルまたは背面パネルを外側に向けて、シャーシの前面または背面にマウント ブラケットを取り付けます。

図 3-2 は、ブラケットを背面に取り付けた場合の構成、図 3-3 は、ブラケットを前面に取り付けた場合の構成を示しています。ステップ 1 と ステップ 2 では、ブラケットを背面に取り付けるか、前面に取り付けるかのどちらかを選択します。両方を実行するわけではありません。

ラックからシャーシを取り外すには、シャーシをラックに取り付けているネジを外してから、シャーシを取り外します。

SFP モジュールの取り付け

適応型セキュリティ アプライアンスは、ファイバ ギガビット イーサネット接続の確立に現場交換可能な SFP モジュールを使用します。

この項では、適応型セキュリティ アプライアンスの SFP モジュールの着脱方法について説明します。この項は、次の内容で構成されています。

SFP モジュール

Small Form-Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）モジュールは、ファイバ ポートに接続するホットスワップ可能入力/出力デバイスです。

（注） スイッチの電源を投入した後に SFP モジュールを取り付ける場合、適応型セキュリティ アプライアンスをリロードして SFP モジュールをイネーブルにする必要があります。

表 3-1 に、適応型セキュリティ アプライアンスによってサポートされている SFP モジュールを示します。

表 3-1　サポートされる SFP モジュール

SFP モジュール	接続タイプ	シスコ製品番号
1000BASE-LX/LH	ファイバ	GLC-LH-SM=
1000BASE-SX	ファイバ	GLC-SX-MM=

1000BASE-LX/LH モジュールおよび 1000BASE-SX SFP モジュールは、ファイバ接続を確立するために使用します。LC コネクタが付いた光ファイバ ケーブルを使用して、SFP モジュールに接続してください。SFP モジュールは、850 ～ 1550 nm の公称波長をサポートします。ケーブルの長さは、信頼できる通信の要件であるケーブル長を超えることはできません。表 3-2 に、ケーブル長の要件を示します。

表 3-2　光ファイバ SFP モジュールのケーブル要件

SFP モジュール	62.5/125 ミクロン マルチモード 850 nm ファイバ	50/125 ミクロン マルチモード 850 nm ファイバ	62.5/125 ミクロン マルチモード 1310 nm ファイバ	50/125 ミクロン マルチモード 1310 nm ファイバ	9/125 ミクロン マルチモード 1310 nm ファイバ
LX/LH	—	—	500 Mhz-km で 550 m	400 Mhz-km で 550 m	10 km
SX	200 Mhz-km で 275 m	500 Mhz-km で 550 m	—	—	—

適応型セキュリティ アプライアンス上では、シスコ認定の SFP モジュールだけを使用してください。SFP モジュールにはそれぞれ、セキュリティ情報で符号化された内部シリアル EEPROM があります。この符号化によって、SFP モジュールが適応型セキュリティ アプライアンスの要件を満たしていることを、シスコが識別して検証できます。

（注） 適応型セキュリティ アプライアンス でサポートされるのは、シスコによって認定された SFP モジュールのみです。

注意 ケーブルを SFP から抜き出した後は、汚れのないポート プラグを SFP に挿入することによって、SFP モジュールを保護してください。別の SFP モジュールの光ボアにファイバ ケーブルを再接続する前に、ケーブルの受光面が汚れていないことを確認してください。SFP モジュールの光ボアにホコリやその他汚染物質が入り込まないようにしてください。光ボアにホコリが詰まると、正しく動作しません。

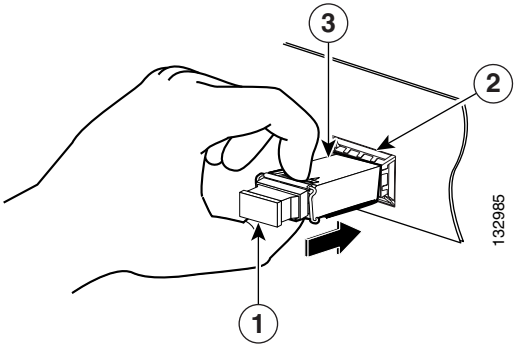
警告 **ケーブルが接続されていない場合、ポートの開口部からは目に見えないレーザー光が放射されている可能性があります。レーザー光に当たらないようにし、開口部をのぞきこまないでください。**ステートメント 70

SFP モジュールの取り付け

SFP モジュールをスロット 1 のファイバ ポートに取り付けるには、次の手順に従います。

ステップ 1　SFP モジュールをポートの位置に合せ、ロックする位置までポート スロット内にスライドさせます（図 3-4 を参照）。

図 3-4　SFP モジュールの取り付け



1	ポート プラグ	**3**	SFP モジュール
2	ポート スロット		

注意　ケーブルを接続する準備ができるまでは、SFP モジュールからポート プラグを取り外さないでください。

ステップ 2　ポート プラグを取り外します。次にネットワーク ケーブルを SFP モジュールに接続します。

ステップ 3　ケーブルのもう一方の端をネットワークに接続します。ケーブル接続の詳細については、第 3 章「インターフェイス ケーブルの接続」を参照してください。

注意　多数の SFP モジュールで使用されているラッチ機構により、ケーブルを接続するとそれらが所定の位置にロックされます。SFP を取り外そうとしてケーブル配線を引っ張らないでください。

ポートおよび LED

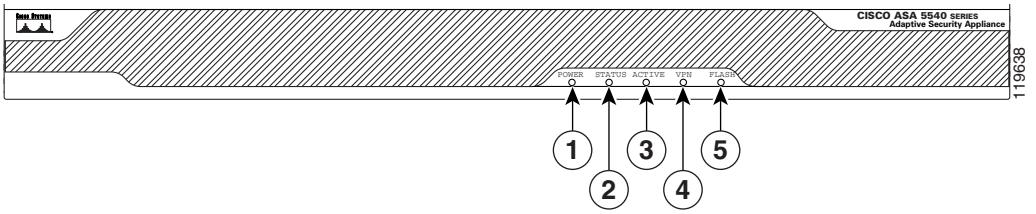
この項では、前面パネルと背面パネルについて説明します。図 3-5 に前面パネルの LED を示します。この項は、次の内容で構成されています。

- 「前面パネルの LED」（P.3-10）
- 「スロット 0 の背面パネル LED とポート」（P.3-11）
- 「スロット 1 のポートおよび LED」（P.3-13）

前面パネルの LED

図 3-5 に、適応型セキュリティ アプライアンスの前面パネルの LED を示します。

図 3-5　前面パネルの LED

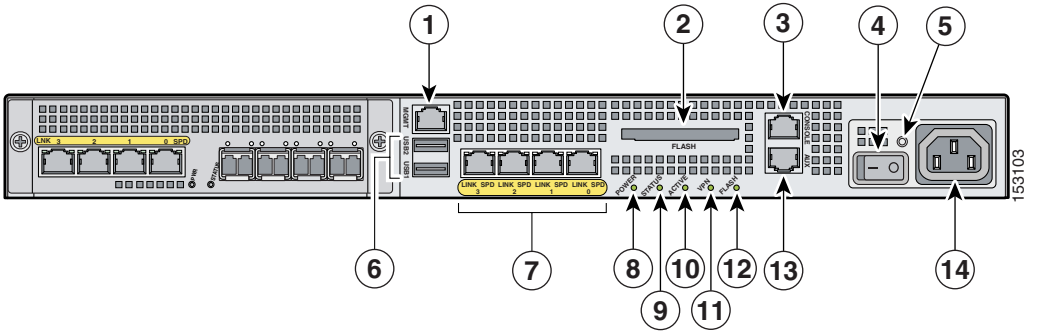


	LED	色	状態	説明
1	電源	緑	点灯	システムは通電状態です。
2	ステータス	緑	点滅	電源投入診断を実行中か、システムがブート中です。
			点灯	システムは電源投入診断に合格しました。
		オレンジ	点灯	電源投入診断に合格しませんでした。
3	アクティブ	緑	点滅	ネットワーク アクティビティが発生しています。
4	VPN	緑	点灯	VPN トンネルが確立されています。
5	点滅	緑	点灯	CompactFlash にアクセス中です。

スロット 0 の背面パネル LED とポート

図 3-6 に、スロット 0 の背面パネル LED とポートを示します。

図 3-6　スロット 0 の背面パネル LED とポート（AC 電源モデルを表示）



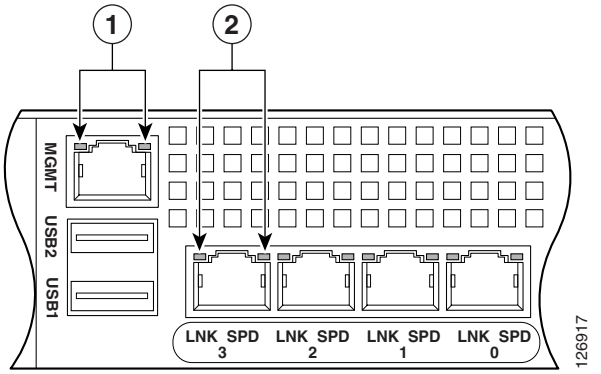
1	管理ポート[1]	**6**	USB 2.0 インターフェイス[2]	**11**	VPN LED
2	外部 CompactFlash スロット	**7**	ネットワーク インターフェイス[3]	**12**	フラッシュ LED
3	シリアル コンソール ポート	**8**	電源インジケータ LED	**13**	補助ポート
4	電源スイッチ	**9**	ステータスインジケータ LED	**14**	電源コネクタ
5	電源インジケータ LED	**10**	アクティブ LED		

1. 管理 0/0 インターフェイスは、管理トラフィック専用のファースト イーサネット インターフェイスです。
2. 今後のリリース用に確保されています。
3. GigabiteEthernet インターフェイス（右から左）、GigabitEthernet 0/0、GigabitEthernet 0/1、GigabitEthernet 0/2、および GigabitEthernet 0/3。

管理ポートの詳細については、『*Cisco ASA 5500 Series Command Reference*』の **management-only** コマンドに関する項を参照してください。

図 3-7 に適応型セキュリティ アプライアンス の背面パネルの LED を示します。

図 3-7　背面パネルのリンクおよび速度のインジケータ LED



1	MGMT インジケータ LED	**2**	インターフェイス LED

表 3-3 に、背面の MGMT およびネットワーク インターフェイスの LED を示します。

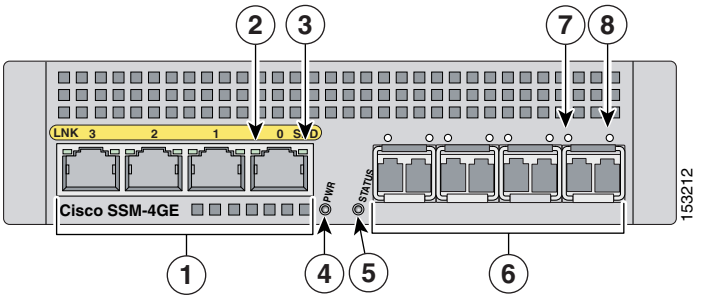
表 3-3　リンクおよび速度の LED

インジケータ	色	説明
左側	緑（点灯）	物理リンク
	緑（点滅）	ネットワーク アクティビティ
右側	消灯	10 Mbps
	緑	100 Mbps
	オレンジ	1000 Mbps

スロット 1 のポートおよび LED

図 3-8 に、スロット 1 のポートと LED を示します。

図 3-8　スロット 1 のポートおよび LED



1	銅線イーサネット ポート	5	ステータス LED
2	RJ-45 リンク LED	6	ファイバ イーサネット ポート
3	RJ-45 速度 LED	7	SFP リンク LED
4	電源 LED	8	SFP 速度 LED

（注） 図 3-8 に、ファイバ イーサネット ポートに取り付けられた SFP モジュールを示します。ファイバ イーサネット接続を確立する場合は、SFP モジュールを注文して取り付ける必要があります。ファイバ ポートと SFP モジュールの詳細については、「SFP モジュールの取り付け」（P.3-6）を参照してください。

表 3-4 では、スロット 1 の LED について説明しています。

表 3-4　　バス G1 の LED

	LED	色	状態	説明
2, 7	リンク	緑	点灯	イーサネット リンクがあります。
			点滅	イーサネット アクティビティが発生しています。
3, 8	速度	消灯	10 MB	ネットワーク アクティビティは発生していません。
		緑	100 MB	100 Mbps でネットワーク アクティビティが発生しています。
		オレンジ	1000 MB（GigE）	1000 Mbps でネットワーク アクティビティが発生しています。
4	電源	緑	点灯	システムは通電状態です。
5	ステータス	緑	点滅	システムはブート中です。
		緑	点灯	システムは正常にブートされました。
		オレンジ	点灯	システムの診断が失敗しました。

インターフェイス ケーブルの接続

この項では、コンソール ポート、補助ポート、管理ポート、銅線イーサネット ポート、およびファイバ イーサネット ポートへの適切なケーブルの接続方法について説明します。

ネットワーク インターフェイスにケーブルを接続するには、次の手順を実行します。

ステップ 1　安定した平らな面か、またはラック内（ラックマウントする場合）にシャーシを置きます。

ステップ 2　管理ポートに接続します。

適応型セキュリティ アプライアンスには、Management0/0 ポートと呼ばれるデバイス管理専用のインターフェイスがあります。Management0/0 ポートは、ファスト イーサネット インターフェイスです。このポートはコンソール ポートに似ていますが、適応型セキュリティ アプライアンスへの着信トラフィックを受け入れるのは Management0/0 ポートだけです。

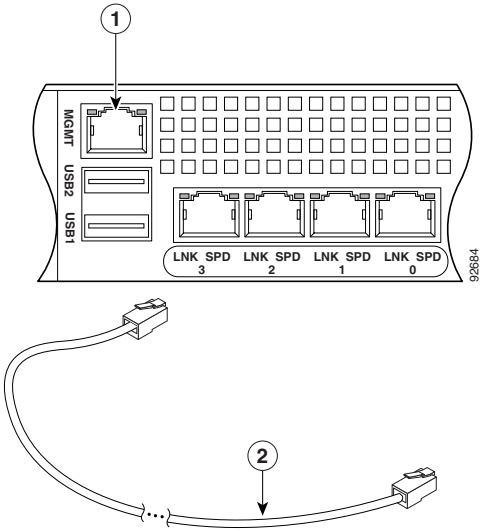
（注）　**management-only** コマンドを使用することで、任意のインターフェイスを管理専用インターフェイスとして設定できます。管理インターフェイスの管理専用モードをディセーブルにすることもできます。このコマンドの詳細については、『*Cisco ASA 5500 Series Command Reference*』の **management-only** コマンドの説明を参照してください。

a. 両端に RJ-45 コネクタがついているイーサネット ケーブルを用意します。

b. RJ-45 コネクタの一方を管理 0/0 ポートに接続します（図 3-9 を参照）。

c. イーサネット ケーブルの逆側の端子をコンピュータまたは管理ネットワークのイーサネット ポートに接続します。

図 3-9　　管理ポートへの接続



1	管理ポート	**2**	RJ-45/RJ-45 イーサネット ケーブル

ステップ 3　コンソール ポートに接続します。

a. コンピュータまたはターミナルをポートに接続する前に、シリアル ポートのボー レートを確認し、判断します。コンピュータまたはターミナルのボー レートは、適応型セキュリティ アプライアンスのコンソール ポートのデフォルト ボー レート（9600 ボー）と一致している必要があります。

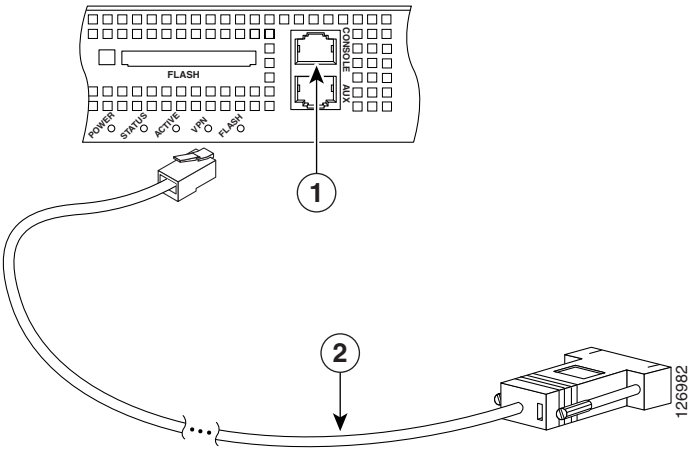
ターミナルを次のように設定します。9600 ボー（デフォルト）、8 データ ビット、パリティなし、1 ストップ ビット、Flow Control（FC; フロー制御）＝ハードウェア。

b. シリアル コンソール ケーブルを見つけてください。このケーブルは、一方の端が RJ-45 コネクタで、もう一方の端が、ご使用のコンピュータのシリアル ポートに接続するための DB-9 コネクタとなっています。

c. 図 3-10 に示すように、RJ-45 コネクタを適応型セキュリティ アプライアンスのコンソール ポートに接続します。

d. DB-9 コネクタを、ご使用のコンピュータのコンソール ポートに接続します。

図 3-10　コンソール ケーブルの接続



1	RJ-45 コンソール ポート	2	RJ-45/DB-9 コンソール ケーブル

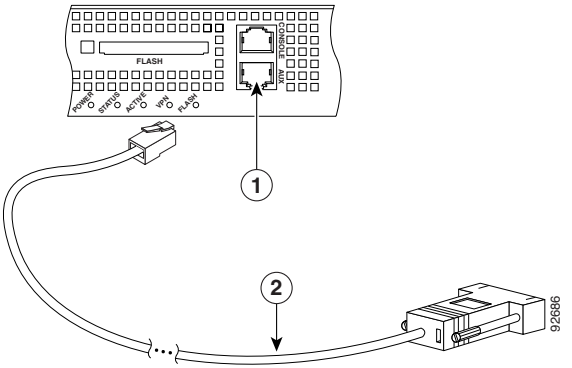
ステップ 4　（AUX というラベルが付いた）補助ポートに接続します。

a. シリアル コンソール ケーブルを見つけてください。このケーブルは、一方の端が RJ-45 コネクタで、もう一方の端が、ご使用のコンピュータのシリアル ポートに接続するための DB-9 コネクタとなっています。

b. 図 3-11 に示すように、ケーブルの RJ-45 コネクタを適応型セキュリティ アプライアンスの（AUX というラベルが付いた）補助ポートに接続します。

c. ケーブルのもう一方の端（DB-9 コネクタ）をコンピュータのシリアル ポートに接続します。

図 3-11　補助ポートへの接続



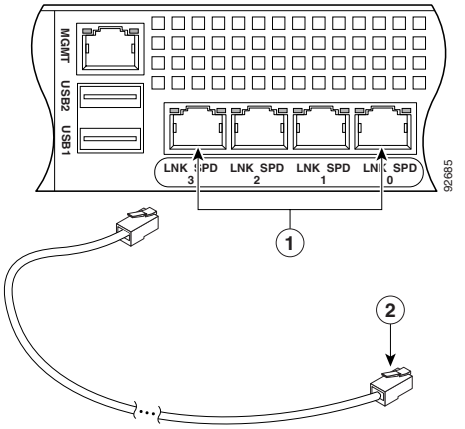
1	RJ-45 補助ポート	**2**	RJ-45/DB-9 コンソール ケーブル

ステップ 5　ネットワーク接続に使用する銅線イーサネット ポートに接続します。銅線イーサネット ポートは、スロット 0 とスロット 1 両方で使用できます。

（注）　内部インターフェイスにはスロット 0 のポート、外部インターフェイスにはスロット 1 のポートを使用する必要があります。

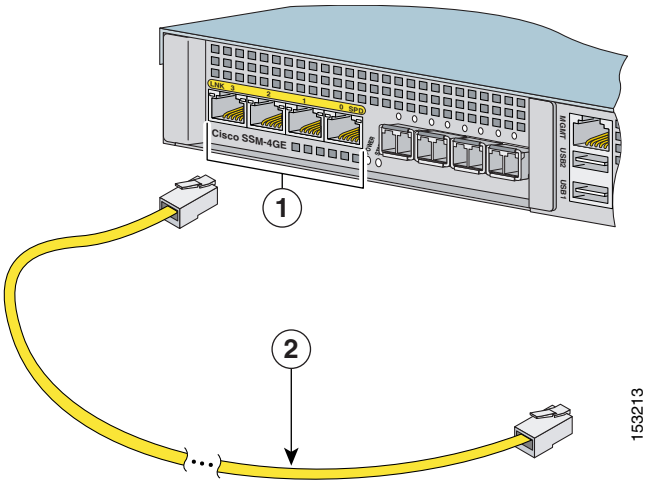
a.　図 3-12 および図 3-13 に示すように、イーサネット ケーブルの一方の端子を銅線イーサネット ポートに接続します。

図 3-12　スロット 0 の銅線イーサネット インターフェイスへの接続



1	銅線イーサネット ポート	**2**	RJ-45 コネクタ

図 3-13　スロット 1 の銅線イーサネット インターフェイスへの接続



1	銅線イーサネット ポート	2	RJ-45 コネクタ

b. イーサネット ケーブルのもう一方の端を、ルータ、スイッチ、またはハブなどのネットワーク デバイスに接続します。

ステップ 6　ネットワーク接続に使用するファイバ イーサネット ポートに接続します。

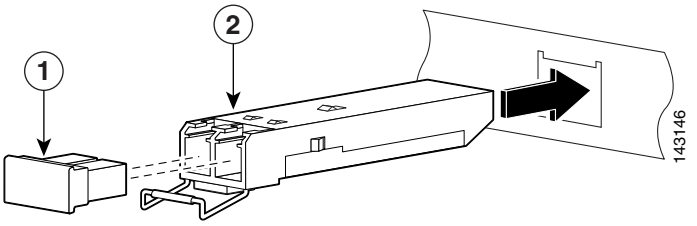
（注） スロット 1 には 4 つの銅線イーサネット ポートと 4 つのファイバ イーサネット ポートがあります。両方のタイプのポートを使用できますが、一度に使用できるスロット 1 ポートの合計数は 4 つです。たとえば、銅線イーサネット ポートを 2 つ、ファイバ イーサネット ポートを 2 つ使用できます。

使用するファイバ ポートごとに、次の手順に従います。

a. SFP モジュールを取り付けます。

- SFP モジュールを、カチッという音が聞こえるまでファイバ ポートに差し込み、スライドさせます。カチッという音がすれば、SFP モジュールがポートにロックされています。
- 図 3-14 に示すように、取り付けた SFP からポート プラグを取り外します。

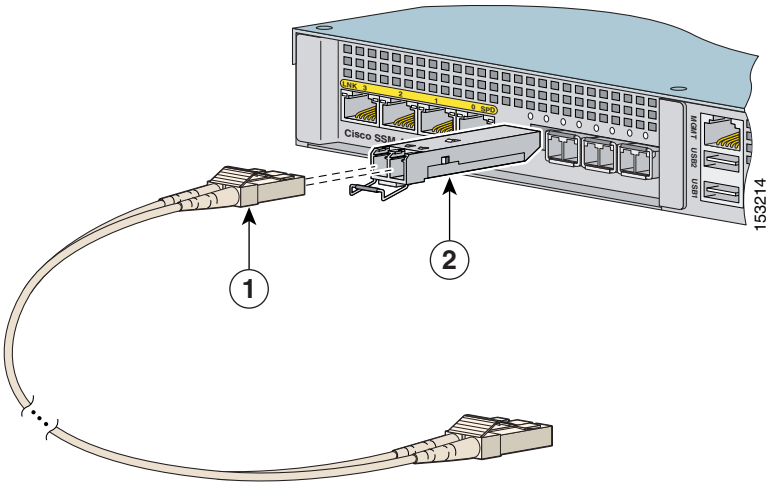
図 3-14　ファイバ ポート プラグの取り外し



1	ポート プラグ	**2**	SFP モジュール

b. LC コネクタを SFP モジュールに接続します（図 3-15 を参照）。

図 3-15　LC コネクタの接続



1	LC コネクタ	**2**	SFP モジュール

c. ケーブルのもう一方の端を、ルータ、スイッチ、またはハブなどのネットワーク デバイスに接続します。

ステップ 7　電源コードを適応型セキュリティ アプライアンスに接続し、もう一方の端を電源に差し込みます。

ステップ 8　シャーシの電源を入れます。

次の作業

第 7 章「適応型セキュリティ アプライアンスの設定」に進みます。

CHAPTER 4

ASA 5500、ASA 5510、ASA 5520、および ASA 5540 の取り付け

（注） 本章の内容は、ASA 5550 には適用されません。

警告 **この装置の 設置、交換、保守は、訓練を受けた相応の資格のある人が行ってください。**ステートメント 49

注意 これらの手順を実行するときは、『*Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*』の安全に関する警告を読み、適切な安全手順に従ってください。

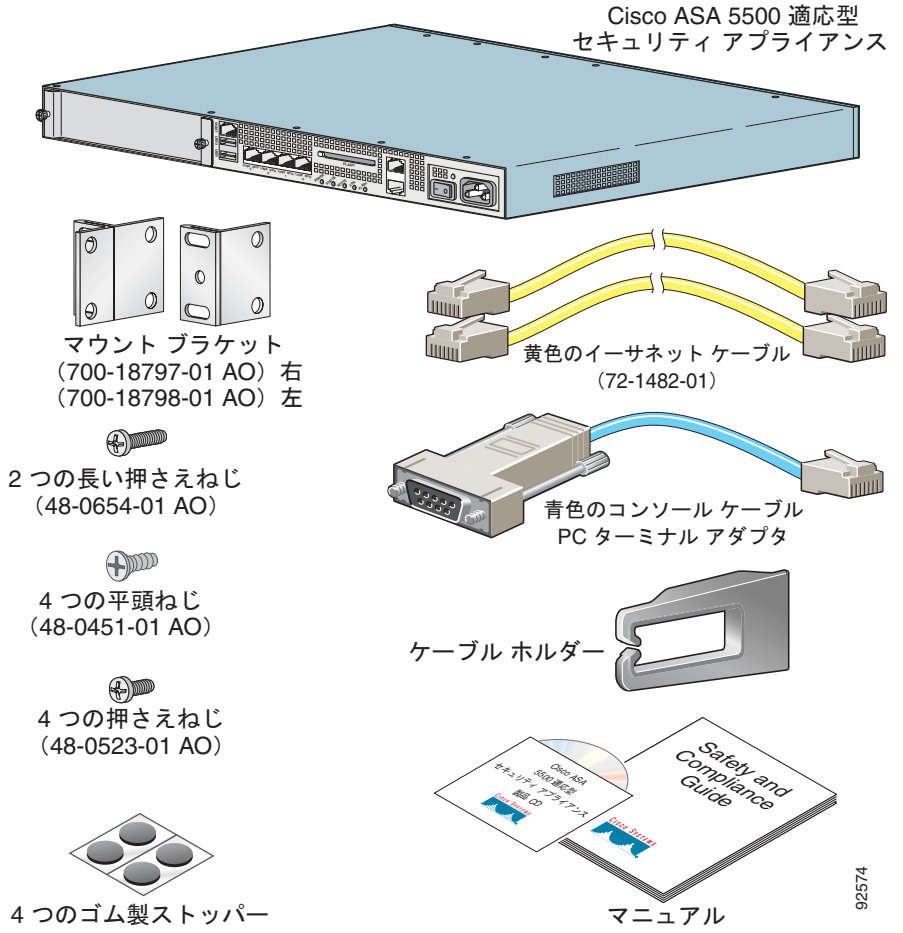
本章では、製品概要と、適応型セキュリティ アプライアンスのメモリ要件、ラックマウント、および取り付け手順について説明します。この章は、次の項で構成されています。

（注） このマニュアル内の各図は、Cisco ASA 5540 適応型セキュリティ アプライアンスを示します。Cisco ASA 5510 適応型セキュリティ アプライアンスと Cisco ASA 5520 適応型セキュリティ アプライアンスは、まったく同じものであり、同じ背面パネル機能とインジケータからなっています。

パッケージ内容の確認

パッケージの箱の内容をチェックし、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスを取り付けるために必要な品目がすべてそろっていることを確認します。

図 4-1　　ASA 5500 パッケージの内容



シャーシの取り付け

この項では、適応型セキュリティ アプライアンスのラックマウントおよび設置の手順について説明します。適応型セキュリティ アプライアンスは、19 インチ ラック（開口部は 17.5 または 17.75 インチ）にマウントできます。

警告　ラックにこの装置をマウントしたり、ラック上の装置の作業を行うときは、ケガをしないように、装置が安定した状態に置かれていることを十分に確認してください。安全に関するガイドラインは次のとおりです。

次の情報は、ラックへの機器の取り付けを計画する場合に役立ちます。

- ラックの周囲に、メンテナンスに必要な空間を確保します。
- 閉鎖型ラックに装置をマウントする場合は、換気が十分に行われるようにします。閉鎖型ラックに装置を詰め込みすぎないようにしてください。各装置で熱が発生するため、ラック内に装置を詰め込みすぎないように注意してください。
- 開放型ラックに装置をマウントする場合、ラックのフレームで吸気口や排気口をふさがないように注意してください。
- ラックに装置を 1 つだけマウントする場合は、ラックの一番下にマウントします。
- すでに別の装置がこのラックに取り付けられている場合は、最も重い装置をラックの一番下に取り付け、重い順にラックの下から上へと設置します。
- ラックにスタビライザが付属している場合、スタビライザを取り付けてから、ラックへの装置の取り付けまたはラックでの作業を行います。

警告　手順を実行する前に、DC 回路に電気が流れていないことを確認してください。すべての電源を確実に切断するには、パネル ボード上で DC 回路に対応している回路ブレーカーを確認して、回路ブレーカーを OFF の位置に切り替え、回路ブレーカーのスイッチ ハンドルを OFF の位置のままテープで固定します。

シャーシのラックマウント

シャーシをラックマウントするには、次の手順に従います。

（注）　マウント ブラケットを使用して、シャーシの前面パネルまたは背面パネルが外側に向くように、シャーシをラックの前面または背面にマウントできます。

ステップ 1　付属のネジを使用して、シャーシにラックマウント ブラケットを取り付けます。図 4-2 と図 4-3 に示すように、ブラケットを穴に取り付けます。ブラケットをシャーシに固定すると、ラックマウントできるようになります。

図 4-2　シャーシの背面パネルへの左側ブラケットの取り付け

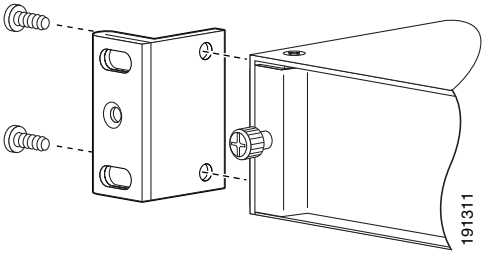
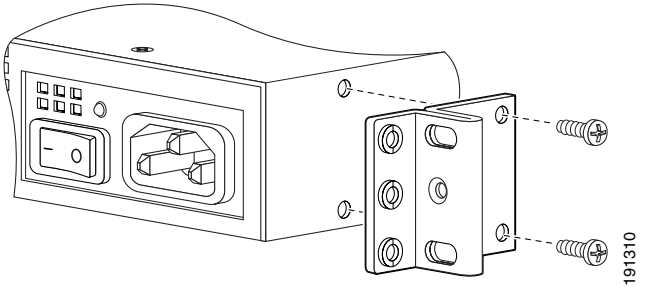
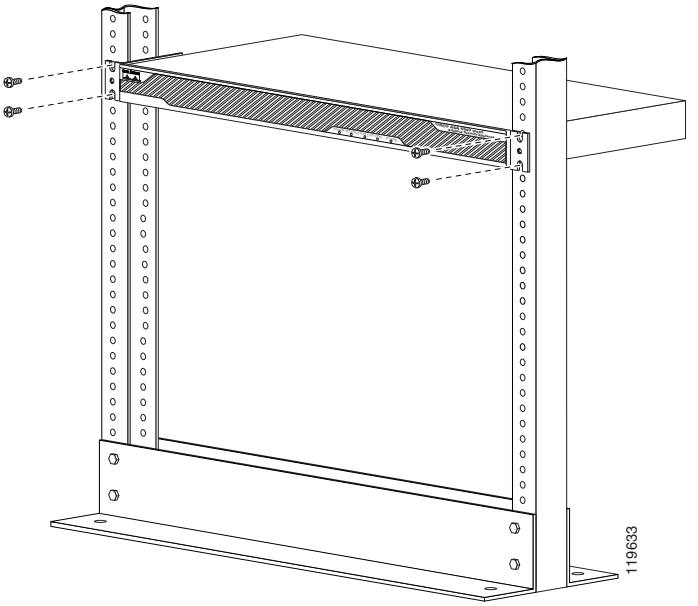


図 4-3　シャーシの背面パネルへの右側ブラケットの取り付け



ステップ 2　付属のネジを使用して、シャーシをラックに取り付けます（図 4-4 を参照）。

図 4-4　　シャーシのラックマウント



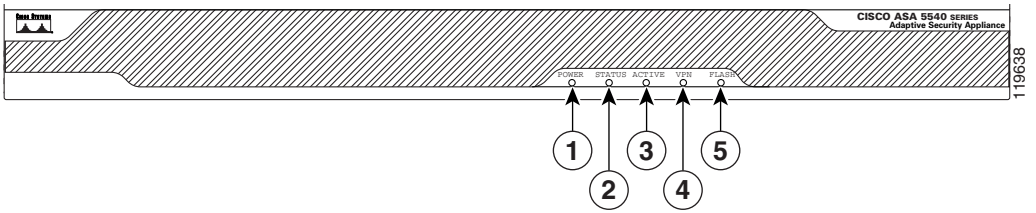
（注）　図 4-2 と図 4-3 は、シャーシの背面へのラックマウント ブラケットの取り付けを示し、図 4-4 は、シャーシの前面へのラックマウント ブラケットの取り付けを示しています。前面パネルまたは背面パネルを外側に向けて、シャーシの前面または背面にマウント ブラケットを取り付けます。
図 4-2 と図 4-3 は、背面へのブラケットの取り付けを、その配置がわかるように示しています。図 4-4 は、前面へのブラケットの取り付けを、その配置がわかるように示しています。ステップ 1 と ステップ 2 では、ブラケットを背面に取り付けるか、前面に取り付けるかのどちらかを選択します。両方を実行するわけではありません。

ラックからシャーシを取り外すには、シャーシをラックに取り付けているネジを外してから、シャーシを取り外します。

ポートおよび LED

この項では、前面パネルと背面パネルについて説明します。図 4-5 に前面パネルの LED を示します。

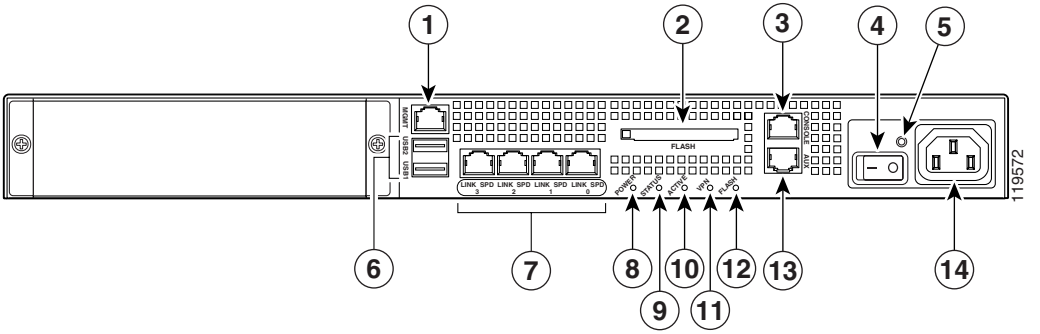
図 4-5　前面パネルの LED



	LED	色	状態	説明
1	電源	緑	点灯	システムは通電状態です。
2	ステータス	緑	点滅	電源投入診断を実行中か、システムがブート中です。
			点灯	システムは電源投入診断に合格しました。
		オレンジ	点灯	電源投入診断に合格しませんでした。
3	アクティブ	緑	点灯	アクティブ フェールオーバー デバイス
		オレンジ	点灯	スタンバイ フェールオーバー デバイス
4	VPN	緑	点灯	VPN トンネルが確立されています。
5	点滅	緑	点灯	CompactFlash にアクセス中です。

図 4-6 に、適応型セキュリティ アプライアンスの背面パネルの機能を示します。

図 4-6　背面パネルの LED とポート（AC 電源モジュール モデルの場合）



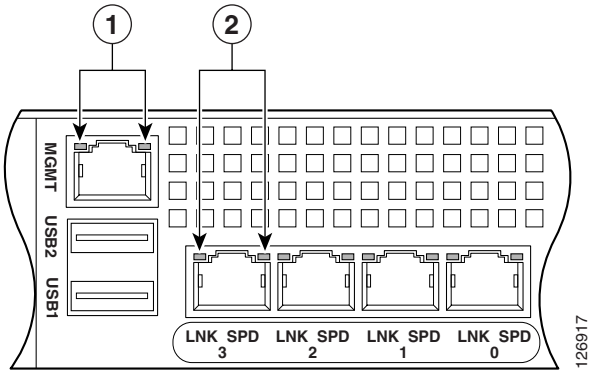
1	管理ポート[1]	**6**	USB 2.0 インターフェイス[2]	**11**	VPN LED
2	外部 CompactFlash スロット	**7**	ネットワーク インターフェイス[3]	**12**	フラッシュ LED
3	シリアル コンソール ポート	**8**	電源インジケータ LED	**13**	補助ポート
4	電源スイッチ	**9**	ステータスインジケータ LED	**14**	電源コネクタ
5	電源インジケータ LED	**10**	アクティブ LED		

1. 管理 0/0 インターフェイスは、管理トラフィック専用のファースト イーサネット インターフェイスです。
2. 現時点ではサポートされていません。
3. GigabiteEthernet インターフェイス（右から左）、GigabitEthernet 0/0、GigabitEthernet 0/1、GigabitEthernet 0/2、および GigabitEthernet 0/3。

管理ポートの詳細については、『*Cisco ASA 5500 Series Command Reference*』の「Management-Only」の項を参照してください。

図 4-7 に適応型セキュリティ アプライアンス の背面パネルの LED を示します。

図 4-7　背面パネルのリンクおよび速度のインジケータ LED



1	MGMT インジケータ LED	**2**	インターフェイス LED

表 4-1 に、背面の MGMT およびネットワーク インターフェイスの LED を示します。

表 4-1　リンクおよび速度の LED

インジケータ	色	説明
左側	緑（点灯）	物理リンク
	緑（点滅）	ネットワーク アクティビティ
右側	消灯	10 Mbps
	緑	100 Mbps
	オレンジ	1000 Mbps

（注） ASA 5510 適応型セキュリティ アプライアンスがサポートしているのは、10/100BaseTX だけです。ASA 5520 適応型セキュリティ アプライアンス と ASA 5540 適応型セキュリティ アプライアンス は、1000BaseT をサポートします。

次の作業

次のいずれかの章に進みます。

実行内容	参照先
購入したがまた取り付けていない SSM の取り付け	第 5 章「オプションの SSM の取り付け」
インターフェイス ケーブルの接続	第 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームにおけるインターフェイス ケーブルの接続」

CHAPTER 5

オプションの SSM の取り付け

（注） 本章の内容は、ASA 5550 には適用されません。

本章では、オプションの Security Services Module（SSM; セキュリティ サービス モジュール）、およびそのコンポーネントの取り付けに関して説明します。オプションの SSM を購入し、まだ取り付けていない場合、本章の手順だけで十分です。

この章は、次の項で構成されています。

Cisco 4GE SSM

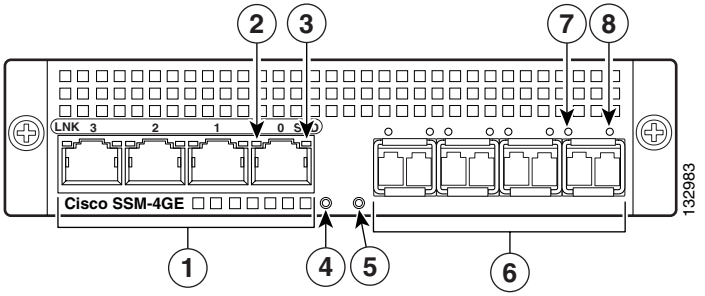
4GE SSM には、8 個のイーサネット ポートがあります。10/100/1000 Mbps 用、銅線の RJ-45 ポートが 4 個、オプションの 1000 Mbps 用、着脱可能小型フォーム ファクタ（SFP）ファイバ ポートが 4 個です。

この項では、適応型セキュリティ アプライアンスにおける Cisco 4GE SSM の取り付けおよび取り換え方法について説明します。この項は、次の内容で構成されています。

4GE SSM コンポーネント

図 5-1 に、Cisco 4GE SSM ポートと LED を示します。

図 5-1　Cisco 4GE SSM ポートと LED



1	RJ-45 ポート	5	ステータス LED
2	RJ-45 リンク LED	6	SFP ポート
3	RJ-45 速度 LED	7	SFP リンク LED
4	電源 LED	8	SFP 速度 LED

（注） 図 5-1 は、ポート スロットに取り付けられた SFP モジュールを示しています。この機能を使用する場合は、SFP モジュールを注文し、取り付ける必要があります。SFP ポートとモジュールの詳細については、「SFP Module の取り付け」（P.5-5）を参照してください。

表 5-1 で、各種 Cisco 4GE SSMLED について説明します。

表 5-1　Cisco 4GE SSM LED

	LED	色	状態	説明
2, 7	リンク	緑	点灯	イーサネット リンクがあります。
			点滅	イーサネット アクティビティが発生しています。
3, 8	速度	消灯	10 MB	ネットワーク アクティビティは発生していません。
		緑	100 MB	100 Mbps でネットワーク アクティビティが発生しています。
		オレンジ	1000 MB（GigE）	1000 Mbps でネットワーク アクティビティが発生しています。
4	電源	緑	点灯	システムは通電状態です。
5	ステータス	緑	点滅	システムはブート中です。
		緑	点灯	システムは正常にブートされました。
		オレンジ	点灯	システムの診断が失敗しました。

Cisco 4GE SSM の取り付け

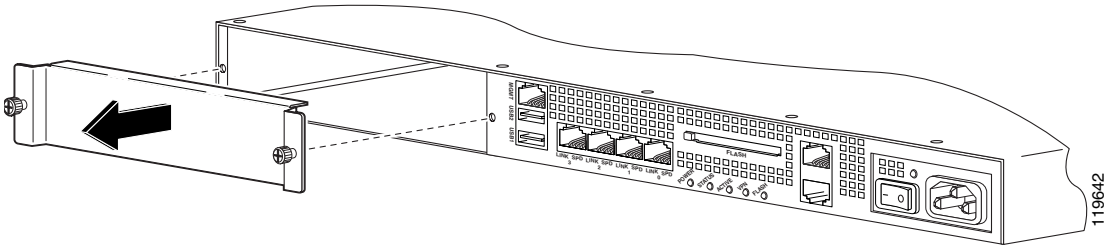
新しい Cisco 4GE SSM を初めて取り付けるには、次の手順に従います。

ステップ 1　適応型セキュリティ アプライアンスの電源を切ります。

ステップ 2　アクセサリ キットからアース ストラップを取り出して、肌に密着するように、ストラップの一端を手首に固定します。もう一方の端をシャーシに接続します。

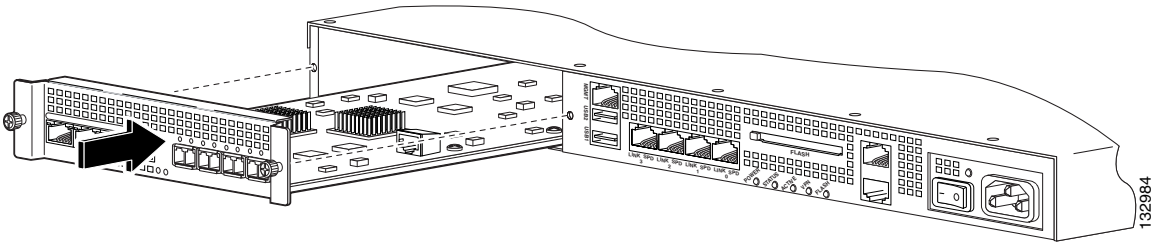
ステップ 3　シャーシ背面左端の 2 個のネジを外し（図 5-2 を参照）、スロット カバーを取り外します。

図 5-2　　スロット カバーのネジの取り外し



ステップ 4　スロット開口部に Cisco 4GE SSM を差し込みます（図 5-3 を参照）。

図 5-3　　スロットへの Cisco 4GE SSM の差し込み



ステップ 5　ネジを取り付けて、Cisco 4GE SSM をシャーシに固定します。

ステップ 6　適応型セキュリティ アプライアンスの電源を入れます。

ステップ 7　LED を確認します。Cisco 4GE SSM が適切に取り付けられると、ステータス LED が点滅（ブート アップ中の場合）、または点灯（操作可能になった場合）します。

ステップ 8　RJ-45 ケーブルの一方の端をポートに接続し、もう一方の端をネットワーク デバイスに接続します。詳細については、第 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームにおけるインターフェイス ケーブルの接続」を参照してください。

SFP Module の取り付け

Small Form-Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）は、SFP ポートに接続するホットスワップ可能入力 / 出力デバイスです。次の SFP モジュール タイプがサポートされています。

- 長波長 / ロング ホール 1000BASE-LX/LH（GLC-LH-SM=）
- 短波長 1000BASE-SX（GLC-SX-MM=）

この項では、光ギガビット イーサネット接続を使用できるように、適応型セキュリティ アプライアンスで SFP モジュールの取り付けと取り外しを行う方法について説明します。この項は、次の内容で構成されています。

- 「SFP モジュール」（P.5-5）
- 「SFP モジュールの取り付け」（P.5-7）

SFP モジュール

適応型セキュリティ アプライアンスは、現場交換可能な SFP モジュールを使用して、ギガビット接続を確立します。

（注） スイッチの電源を投入した後に SFP モジュールを取り付ける場合、適応型セキュリティ アプライアンスをリロードして SFP モジュールをイネーブルにする必要があります。

表 5-2 に、適応型セキュリティ アプライアンスによってサポートされている SFP モジュールを示します。

表 5-2　サポートされる SFP モジュール

SFP モジュール	接続タイプ	シスコ製品番号
1000BASE-LX/LH	光ファイバ	GLC-LH-SM=
1000BASE-SX	光ファイバ	GLC-SX-MM=

1000BASE-LX/LH と 1000BASE-SX SFP モジュールは、光ファイバ接続の確立に使用されます。SFP モジュールに接続するには、LC コネクタに光ファイバケーブルを使用します。SFP モジュールは、850 ～ 1550 nm の公称波長をサポートします。ケーブルの長さは、信頼できる通信の要件であるケーブル長を超えることはできません。表 5-3 に、ケーブル長の要件を示します。

表 5-3　光ファイバ SFP モジュールのケーブル要件

SFP モジュール	62.5/125 ミクロン マルチモード 850 nm ファイバ	50/125 ミクロン マルチモード 850 nm ファイバ	62.5/125 ミクロン マルチモード 1310 nm ファイバ	50/125 ミクロン マルチモード 1310 nm ファイバ	9/125 ミクロン マルチモード 1310 nm ファイバ
LX/LH	—	—	500 Mhz-km で 550 m	400 Mhz-km で 550 m	10 km
SX	200 Mhz-km で 275 m	500 Mhz-km で 550 m	—	—	—

適応型セキュリティ アプライアンスには、シスコ認定の SFP モジュールのみを使用します。SFP モジュールにはそれぞれ、セキュリティ情報で符号化された内部シリアル EEPROM があります。この符号化によって、SFP モジュールが適応型セキュリティ アプライアンスの要件を満たしていることを、シスコが識別して検証できます。

（注） 適応型セキュリティ アプライアンス でサポートされるのは、シスコによって認定された SFP モジュールのみです。

注意 SFP からケーブルを外した後は、清潔なダスト プラグを SFP に差し込んで SFP モジュールを保護します。光ファイバケーブルの光学面に汚れがないことを確認してから、別の SFP モジュールの光ボアに接続し直してください。SFP モジュールの光ボアにホコリやその他汚染物質が入り込まないようにしてください。光ボアにホコリが詰まると、正しく動作しません。

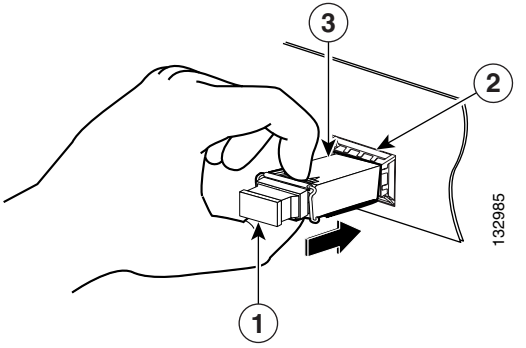
警告 **ケーブルが接続されていない場合、ポートの開口部からは目に見えないレーザー光が放射されている可能性があります。レーザー光に当たらないようにし、開口部をのぞきこまないでください。ステートメント 70**

SFP モジュールの取り付け

Cisco 4GE SSM に SFP モジュールを取り付けるには、次の手順に従います。

ステップ 1　SFP モジュールをポートの位置に合せ、ロックする位置までポート スロット内にスライドさせます（図 5-4 を参照）。

図 5-4　SFP モジュールの取り付け



1	光ポート プラグ	**3**	SFP モジュール
2	SFP ポート スロット		

注意　ケーブルを接続する準備ができるまでは、SFP から光ポート プラグを取り外さないでください。

ステップ 2　光ポート プラグを取り外し、ネットワーク ケーブルを SFP モジュールに接続します。

ステップ 3　ケーブルのもう一方の端をネットワークに接続します。ケーブル接続の詳細については、第 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームにおけるインターフェイス ケーブルの接続」を参照してください。

注意　多くの SFP で使用されているラッチ メカニズムによって、ケーブルが接続されると SPF がロックされます。SFP を取り外す際にはケーブルを引っ張らないようにしてください。

Cisco AIP SSM および CSC SSM

ASA 5500 シリーズの適応型セキュリティ アプライアンスでは、AIP SSM（Advanced Inspection and Prevention Security Services Module）と CSC SSM（Content Security Control Security Services Module）がサポートされています。これらはインテリジェント SSM とも呼ばれます。

AIP SSM によって、セキュリティ検査を提供する高度な IPS ソフトウェアが実行されます。AIP SSM には、AIP SSM 10 と AIP SSM 20 の 2 つのモデルがあります。両方のタイプはまったく同じように見えますが、AIP SSM 20 は、AIP SSM 10 より、プロセッサが高速でメモリ容量も大きくなっています。スロットに入れられるモジュールは一度に 1 つだけです（AIP SSM 10 または AIP SSM 20）。

表 5-4 に、AIP SSM 10 と AIP SSM 20 のメモリ仕様を示します。

表 5-4　SSM メモリ仕様

SSM	CPU	DRAM
AIP SSM 10	2.0 GHz Celeron	1.0 GB
AIP SSM 20	2.4 GHz Pentium 4	2.0 GB

AIP SSM の詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

CSC SSM は、Content Security and Control ソフトウェアを実行します。CSC SSM は、ウイルス、スパイウェア、スパムなどの好ましくないトラフィックを予防します。CSC SSM の詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

この項では、適応型セキュリティ アプライアンスにおける SSM の取り付けおよび取り換え方法について説明します。図 5-5 に、各種 SSM LED を示します。

図 5-5　SSM LED

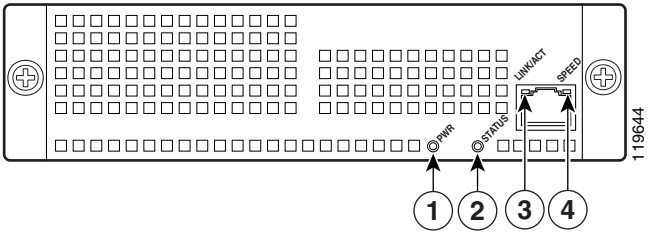


表 5-5 で、各種SSM LED について説明します。

表 5-5　SSM LED

	LED	色	状態	説明
1	電源	緑	点灯	システムは通電状態です。
2	ステータス	緑	点滅	システムはブート中です。
			点灯	システムは電源投入診断に合格しました。
3	リンク/アクティブ	緑	点灯	イーサネット リンクがあります。
			点滅	イーサネット アクティビティが発生しています。
4	速度	緑 オレンジ	100 MB	ネットワーク アクティビティが発生しています。
			1000 MB（GigE）	ネットワーク アクティビティが発生しています。

SSM の取り付け

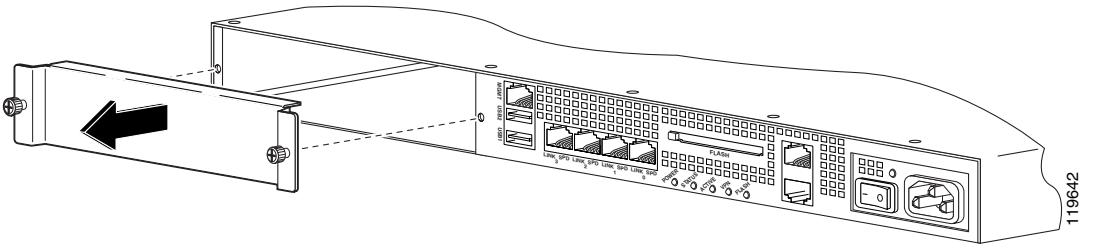
新しい SSM を取り付けるには、次の手順に従います。

ステップ 1　適応型セキュリティ アプライアンスの電源を切ります。

ステップ 2　アクセサリ キットからアース ストラップを取り出して、肌に密着するように、ストラップの一端を手首に固定します。もう一方の端をシャーシに接続します。

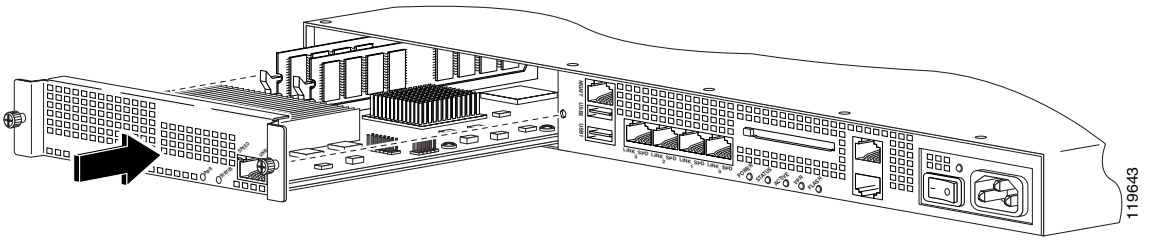
ステップ 3　シャーシ背面左端の 2 個のネジを外し（図 5-6 を参照）、スロット カバーを取り外します。

図 5-6　スロット カバーのネジの取り外し



ステップ 4　図 5-7 に示すように、SSM をスロットの開口部に挿入します。

図 5-7　スロットへの SSM の差し込み



ステップ 5　ネジを取り付けて、SSM をシャーシに固定します。

ステップ 6　適応型セキュリティ アプライアンスの電源を入れます。LED を確認します。SSM が適切に取り付けられると、電源 LED が緑色に点灯し、ステータス LED が緑色に点滅します。

ステップ 7　RJ-45 ケーブルの一方の端をポートに接続し、もう一方の端をネットワーク デバイスに接続します。

次の作業

第 6 章「ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームにおけるインターフェイス ケーブルの接続」に進みます。

CHAPTER 6

ASA 5500、ASA 5510、ASA 5520、および ASA 5540 プラットフォームにおけるインターフェイス ケーブルの接続

（注） 本章の内容は、ASA 5550 には適用されません。

本章では、コンソール ポート、補助ポート、管理ポート 4GE SSM、および SSM ポートへのケーブルの接続方法について説明します。このマニュアルでは、SSM とは、インテリジェント SSM、AIP SSM、または CSC SSM を指します。

（注） 4GE SSM、AIP SSM、および CSC SSM は、オプションのセキュリティ サービス モジュールです。ご使用の適応型セキュリティ アプライアンスに、これらのモジュールがない場合は、第 7 章「適応型セキュリティ アプライアンスの設定」を参照してください。

警告 **この装置の 設置、交換、保守は、訓練を受けた相応の資格のある人が行ってください。**ステートメント 49

注意 これらの手順を実行するときは、『*Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*』の安全に関する警告を読み、適切な安全手順に従ってください。

この章は、次の項で構成されています。

インターフェイス ケーブルの接続

この項では、コンソール ポート、補助ポート、管理ポート、銅線イーサネット ポート、およびファイバ イーサネット ポートへの適切なケーブルの接続方法について説明します。

ネットワーク インターフェイスにケーブルを接続するには、次の手順を実行します。

ステップ 1　安定した平らな面か、またはラック内（ラックマウントする場合）にシャーシを置きます。

ステップ 2　管理ポートに接続します。

適応型セキュリティ アプライアンスには、Management0/0 ポートと呼ばれるデバイス管理専用のインターフェイスがあります。Management0/0 ポートは、ファスト イーサネット インターフェイスです。このポートはコンソール ポートに似ていますが、適応型セキュリティ アプライアンスへの着信トラフィックを受け入れるのは Management0/0 ポートだけです。

（注）　**management-only** コマンドを使用することで、任意のインターフェイスを管理専用インターフェイスとして設定できます。管理インターフェイスの管理専用モードをディセーブルにすることもできます。このコマンドの詳細については、『*Cisco ASA 5500 Series Command Reference*』の **management-only** コマンドの説明を参照してください。

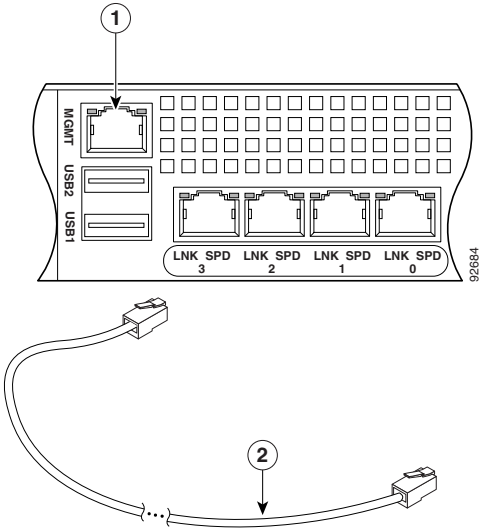
a.　両端に RJ-45 コネクタがついているイーサネット ケーブルを用意します。

b.　RJ-45 コネクタの一方を管理 0/0 ポートに接続します（図 6-1 を参照）。

c. イーサネット ケーブルの逆側の端子をコンピュータまたは管理ネットワークのイーサネット ポートに接続します。

（注） 適応型セキュリティ アプライアンス上の管理ポートにコンピュータを直接接続する場合は、クロスオーバ イーサネット ケーブルを使用してください。ハブやスイッチを経由して適応型セキュリティ アプライアンスにコンピュータを接続する場合は、ストレート スルー イーサネット ケーブルを使用して、そのハブやスイッチを管理ポートに接続してください。

図 6-1　管理ポートへの接続



1	管理ポート	**2**	RJ-45/RJ-45 イーサネット ケーブル

ステップ 3　コンソール ポートへ接続します。

a. コンピュータまたはターミナルをポートに接続する前に、シリアル ポートのボー レートを確認し、判断します。ボー レートは、適応型セキュリティ アプライアンスのコンソール ポートのデフォルト ボー レート（9600 ボー）と一致している必要があります。

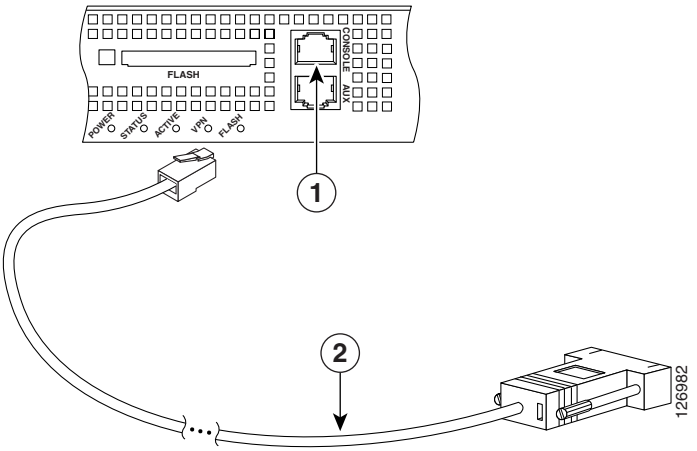
ターミナルを次のように設定します。9600 ボー（デフォルト）、8 データ ビット、パリティなし、1 ストップ ビット、Flow Control（FC; フロー制御）＝ハードウェア。

b. シリアル コンソール ケーブルを見つけてください。このケーブルは、一方の端が RJ-45 コネクタで、もう一方の端が、ご使用のコンピュータのシリアル ポートに接続するための DB-9 コネクタとなっています。

c. 図 6-2 に示すように、RJ-45 コネクタを適応型セキュリティ アプライアンスのコンソール ポートに接続します。

d. DB-9 コネクタを、ご使用のコンピュータのコンソール ポートに接続します。

図 6-2　コンソール ケーブルの接続



1	RJ-45 コンソール ポート	**2**	RJ-45/DB-9 コンソール ケーブル

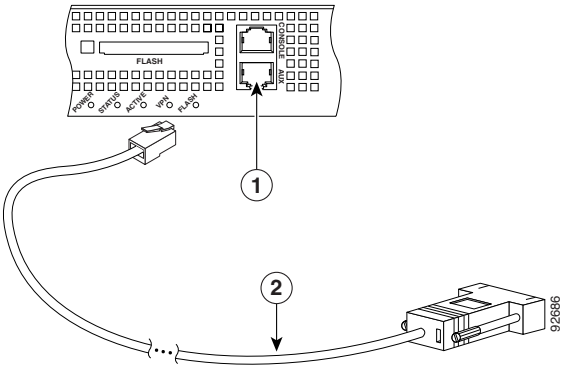
ステップ 4　（AUX というラベルが付いた）補助ポートに接続します。

a. シリアル コンソール ケーブルを見つけてください。このケーブルは、一方の端が RJ-45 コネクタで、もう一方の端が、ご使用のコンピュータのシリアル ポートに接続するための DB-9 コネクタとなっています。

b. 図 6-3 に示すように、ケーブルの RJ-45 コネクタを適応型セキュリティ アプライアンスの（AUX というラベルが付いた）補助ポートに接続します。

c. ケーブルのもう一方の端（DB-9 コネクタ）をコンピュータのシリアル ポートに接続します。

図 6-3　補助ポートへの接続



1	RJ-45 補助ポート	**2**	RJ-45/DB-9 コンソール ケーブル

SSM への接続

SSM はオプションです。この手順は、適応型セキュリティ アプライアンスに SSM を取り付けた場合にだけ必要となります。

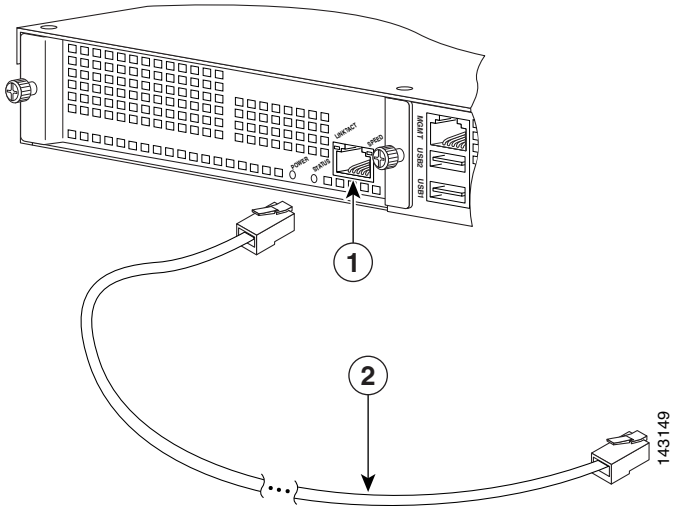
（注） この手順は、4GE SSM には適用されません。4GE SSM への接続の詳細については、「4GE SSM への接続」（P.6-8）を参照してください。

SSM に接続するには、次の手順に従います。

ステップ 1　図 6-4 に示すように、RJ-45 コネクタを SSM の管理ポートに接続します。

ステップ 2　RJ-45 ケーブルのもう一方の端をネットワーク デバイスに接続します。

図 6-4　SSM 管理ポート への接続



1	SSM 管理ポート	2	RJ-45/RJ-45 ケーブル

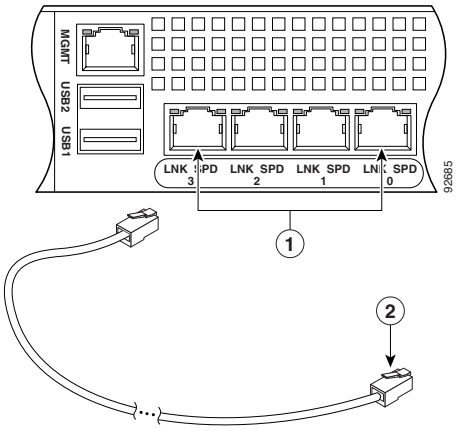
ステップ 3　ネットワーク接続に使用されるイーサネット ポートに接続します。

a. RJ-45 コネクタをイーサネット ポートに接続します。

b. イーサネット ケーブルのもう一方の端をネットワーク デバイス（ルータ、スイッチ、ハブなど）に接続します。

（注） 装置上のイーサネット インターフェイスは、使用されていなければどれでも、フェールオーバー リンクとして使用できます。フェールオーバー リンク インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー リンクとしてのみ使用されます。LAN ベースのフェールオーバー リンクを接続するには、そのリンク上にホストもルータもない専用スイッチを使用することも、装置を直接リンクするクロスオーバー イーサネット ケーブルを使用することもできます。詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』の「Configuring Failover」の章を参照してください。また、イーサネット インターフェイスについては、第 4 章「ポートおよび LED」も参照してください。

図 6-5　ネットワーク インターフェイスへのケーブルの接続



1	RJ-45 イーサネット ポート	2	RJ-45 コネクタ

4GE SSM への接続

4GE SSM はオプションです。そのため、この手順は、適応型セキュリティ アプライアンスに 4GE SSM を取り付けた場合にだけ必要となります。

4GE SSM に接続するには、次の手順に従います。

ステップ 1　ネットワーク接続に使用する銅線イーサネット ポートに接続します。

a. イーサネット ケーブルの一方の端を、銅線イーサネット ポートに接続します。

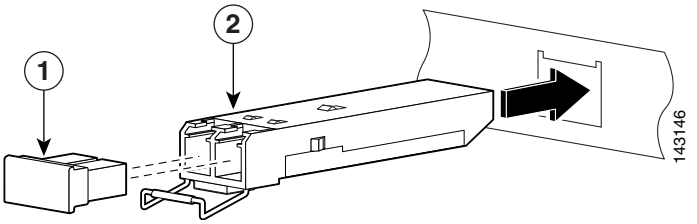
b. イーサネット ケーブルのもう一方の端を、ルータ、スイッチ、またはハブなどのネットワーク デバイスに接続します。

ステップ 2　ネットワーク接続に使用するファイバ イーサネット ポートに接続します。使用するファイバ ポートごとに、次の手順に従います。

a. SFP モジュールを取り付けます。

- SFP モジュールを、カチッという音が聞こえるまでファイバ ポートに差し込み、スライドさせます。カチッという音がすれば、SFP モジュールがポートにロックされています。
- 図 6-6 に示すように、取り付けた SFP からポート プラグを取り外します。

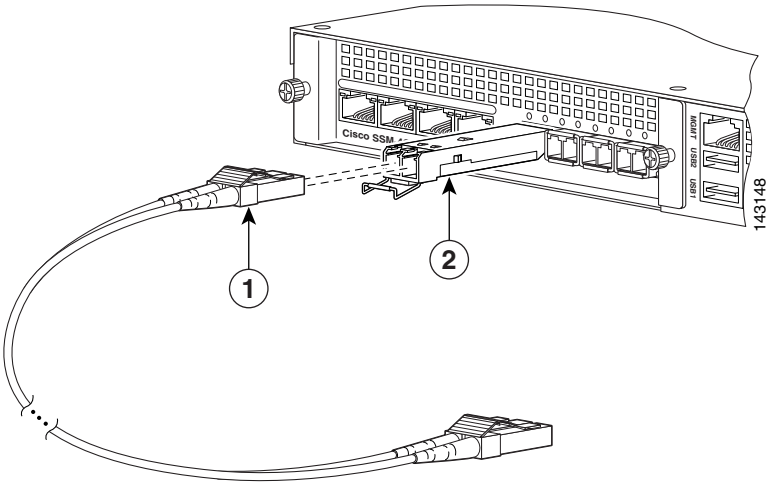
図 6-6　ファイバ ポート プラグの取り外し



1	ポート プラグ	**2**	SFP モジュール

– LC コネクタを SFP モジュールに接続します（図 6-7 を参照）。

図 6-7　　LC コネクタの接続



b. ケーブルのもう一方の端を、ルータ、スイッチ、またはハブなどのネットワーク デバイスに接続します。

適応型セキュリティ アプライアンスの電源投入

適応型セキュリティ アプライアンス の電源を入れるには、次の手順に従います。

ステップ 1　電源コードを適応型セキュリティ アプライアンスに接続し、もう一方の端を電源に差し込みます。

ステップ 2　シャーシの電源を入れます。

次の作業

第 7 章「適応型セキュリティ アプライアンスの設定」に進みます。

CHAPTER 7

適応型セキュリティ アプライアンスの設定

この章では、適応型セキュリティ アプライアンスの初期設定について説明します。設定手順を実行するには、ブラウザベースの Cisco Adaptive Security Device Manager（ASDM）またはコマンドライン インターフェイス（CLI）のいずれかを使用します。この章の手順では、ASDM を使用して適応型セキュリティ アプライアンスを設定する方法を説明します。

この章は、次の項で構成されています。

工場出荷時のデフォルト設定について

Cisco 適応型セキュリティ アプライアンスは、すぐに使用を開始できるように工場でデフォルト設定されて出荷されます。ASA 5500 シリーズ は次のように事前設定されています

- 2 つの VLAN：VLAN 1 と VLAN2。
- VLAN 1 のプロパティは次のとおりです。
  - 名前：「inside」
  - 割り当てられているスイッチ ポート：Ethernet 0/1 から Ethernet 0/7
  - セキュリティ レベル：100
  - 割り当てられているスイッチ ポート：Ethernet 0/1 から 0/7
  - IP アドレス：192.168.1.1 255.255.255.0
- VLAN2 のプロパティは次のとおりです。
  - 名前：「outside」
  - 割り当てられているスイッチ ポート：Ethernet 0/0
  - セキュリティ レベル：0
  - DHCP を使用して IP アドレスを取得するように設定済み
- デバイスに接続し、ASDM を使用して設定を入力するための内部インターフェイス。

デフォルトでは、適応型セキュリティ アプライアンスの内部インターフェイスには、デフォルト DHCP アドレス プールが組み込まれています。この設定により、内部ネットワークのクライアントは、適応型セキュリティ アプライアンスに接続するためにアプライアンスから DHCP アドレスを取得できます。このため、管理者は ASDM を使用して適応型セキュリティ アプライアンスを設定および管理できます。

CLI を使用した設定

適応型セキュリティ アプライアンスは、ASDM Web コンフィギュレーション ツールだけでなく、コマンドライン インターフェイスを使用しても設定できます。

vpnsetup ipsec-remote-access steps コマンドおよび **vpnsetup site-to-site steps** コマンドを使用すれば、CLI 自体の中で基本的なリモート アクセスおよび LAN 間接続を設定する方法の、段階を追った例を取得できます。これらのコマンドの詳細については、『*Cisco ASA 5500 Series Command Reference*』を参照してください。

適応型セキュリティ アプライアンスのすべての機能領域に関する段階を追った手順については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

Adaptive Security Device Manager を使用した設定

Adaptive Security Device Manager（ASDM）は、適応型セキュリティ アプライアンスを管理および監視できる、豊富な機能を持つグラフィカル インターフェイスです。Web ベースの設計によってセキュアなアクセスが実現されるため、Web ブラウザを使用して、どこからでも適応型セキュリティ アプライアンスに接続し、管理することができます。

設定と管理の機能がそろっているだけでなく、ASDM には適応型セキュリティ アプライアンスの導入を簡素化および促進するインテリジェント ウィザードが搭載されています。

この項は、次の内容で構成されています。

ASDM を使用するための準備

ASDM を使用する前に、次の手順に従います。

ステップ 1　まだ行っていない場合、イーサネット ケーブルを使用して、MGMT インターフェイスをスイッチまたはハブに接続します。同じスイッチに、適応型セキュリティ アプライアンスを設定する PC を接続します。

ステップ 2　DHCP を使用するように PC を設定します（適応型セキュリティ アプライアンス から自動的に IP アドレスを受信するため）。この設定により、PC が 適応型セキュリティ アプライアンス およびインターネットと通信できるようになるだけでなく、ASDM を実行して設定および管理のタスクを行えます。

または、192.168.1.0 サブネットの中からアドレスを選択して、スタティック IP アドレスを使用中の PC に割り当てることもできます （有効なアドレスは 192.168.1.2 ～ 192.168.1.254 で、255.255.255.0 のマスクと 192.168.1.1 のデフォルト ルートがあります）。

他のデバイスを任意の内部ポートに接続する場合は、同じ IP アドレスが使用されていないことを確認します。

（注）　適応型セキュリティ アプライアンスの MGMT インターフェイスには、デフォルトで 192.168.1.1 が割り当てられています。そのため、このアドレスは使用できません。

ステップ 3　MGMT インターフェイス上の LINK LED を確認します。

接続が確立されると、適応型セキュリティ アプライアンスのリンク LED インターフェイス、およびスイッチまたはハブ上の対応する LINK LED が緑色に点灯します。

初期セットアップの設定情報の収集

ASDM Startup Wizard で使用する次の情報を収集します。

- ネットワーク上の適応型セキュリティ アプライアンスを識別する一意のホスト名。
- ドメイン名。
- 設定する外部インターフェイス、内部インターフェイス、およびその他のインターフェイスの IP アドレス。
- ASDM の HTTPS、SSH、または Telnet を使用して、このデバイスに管理アクセスできるホストの IP アドレス。
- 管理アクセス用の特権モードのパスワード。
- NAT または PAT アドレス変換に使用する IP アドレス（存在する場合）。
- DHCP サーバの IP アドレス範囲。
- WINS サーバの IP アドレス。
- 設定するスタティック ルート。
- DMZ を作成する場合、3 つ目の VLAN を作成して、その VLAN にポートを割り当てる必要があります （デフォルトでは、2 つの VLAN が設定されています）。
- インターフェイスの設定情報。つまり、同じセキュリティ レベルのインターフェイス間でトラフィックを許可するかどうか、同じインターフェイスのホスト間でトラフィックを許可するかどうか。
- Easy VPN ハードウェア クライアントを設定する場合は、プライマリおよびセカンダリの Easy VPN サーバの IP アドレス、クライアントをクライアント モードまたはネットワーク拡張モードで実行するかどうか、プライマリおよびセカンダリの Easy VPN サーバに設定されたユーザおよびグループ ログイン認定証に一致するそれぞれの認定証。

ASDM Launcher のインストール

ASDM は次の 2 つの方法のいずれかで起動できます。ASDM が PC でローカルに実行されるように ASDM Launcher ソフトウェアをダウンロードする方法か、Web ブラウザ内で Java および JavaScript をイネーブルにして、ASDM に PC からリモートでアクセスする方法です。ここでの手順は、ASDM をローカルで実行するようにシステムを設定する方法について説明するものです。

ASDM Launcher をインストールするには、次の手順に従います。

ステップ 1　スイッチまたはハブに接続された PC で、インターネット ブラウザを起動します。

a. ブラウザのアドレス フィールドに、**https://192.168.1.1/admin** という URL を入力します。

（注） 適応型セキュリティ アプライアンスは、192.168.1.1 のデフォルト IP アドレスが設定されて出荷されます。「**https**」の「**s**」を付け忘れると、接続は失敗します。HTTPS（HTTP over SSL）を使用すると、ブラウザと適応型セキュリティ アプライアンスとの間の安全な接続が可能になります。

Cisco ASDM のスプラッシュ画面が表示されます。

b. [Install ASDM Launcher and Run ASDM] をクリックします。

c. ユーザ名とパスワードの入力を求めるダイアログボックスで、どちらのフィールドも空のままにします。[OK] をクリックします。

d. [Yes] をクリックして、証明書を受け入れます。後続の認証および証明書に関するすべてのダイアログボックスで、[Yes] をクリックします。

e. [File Download] ダイアログボックスがオープンしたら、[Open] をクリックして、インストール プログラムを直接実行します。ハード ドライブにインストール ソフトウェアを保存する必要はありません。

f. InstallShield Wizard が表示されたら、指示に従って ASDM Launcher ソフトウェアをインストールします。

ステップ 2　デスクトップから、Cisco ASDM Launcher ソフトウェアを起動します。

ダイアログボックスが表示されます。

ステップ 3　適応型セキュリティ アプライアンスの IP アドレスまたはホスト名を入力します。

ステップ 4　適応型セキュリティ アプライアンスの IP アドレスまたはホスト名を入力します。

ステップ 5　[Username] フィールドと [Password] フィールドは空白のままにします。

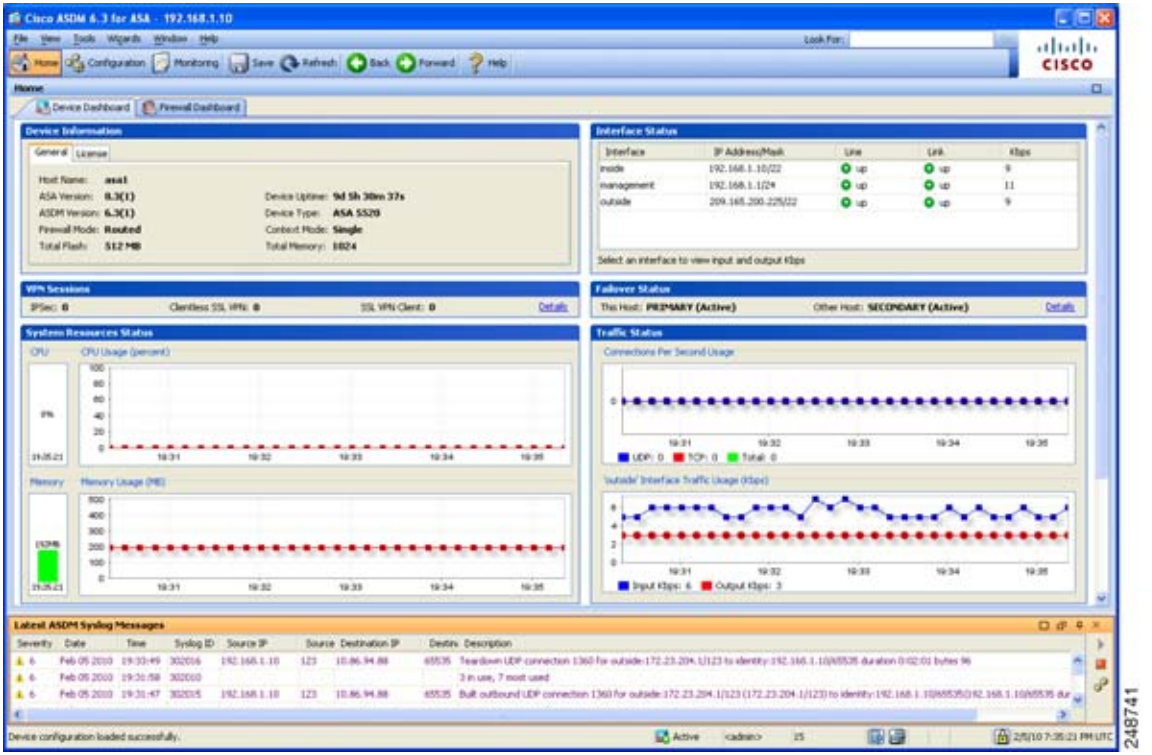
（注）　デフォルトでは、Cisco ASDM Launcher に対してユーザ名およびパスワードは設定されていません。

ステップ 6　[OK] をクリックします。

ステップ 7　証明書を受け入れる要求を含むセキュリティ警告を受信したら、[Yes] をクリックします。

ASA によって、更新されたソフトウェアがあるかどうかが確認され、あった場合、そのソフトウェアが自動的にダウンロードされます。

メイン ASDM ウィンドウが表示されます。



ASDM が開始され、メイン ウィンドウが表示されます。

Web ブラウザを使用した ASDM の開始

Web ブラウザで ASDM を実行するには、アドレス フィールドに工場出荷時のデフォルト IP アドレス **https://192.168.1.1/admin/** を入力します。

（注） 「**https**」の「**s**」を付け忘れると、接続は失敗します。HTTP over SSL（HTTP）を使用すると、ブラウザと適応型セキュリティ アプライアンスとの間の安全な接続が可能になります。

メイン ASDM ウィンドウが表示されます。

ASDM Startup Wizard の実行

ASDM には、適応型セキュリティ アプライアンスの初期設定を簡素化する Startup Wizard が用意されています。Startup Wizard を使用すると、わずかな手順で、内部ネットワークと外部ネットワーク間でパケットが安全に流れるように適応型セキュリティ アプライアンスを設定できます。

Startup Wizard を使用して適応型セキュリティ アプライアンスの基本設定をセットアップするには、次の手順に従います。

ステップ 1　[ASDM] ウィンドウ上部にある [Wizards] メニューから、[Startup Wizard] を選択します。

ステップ 2　Startup Wizard の手順に従って適応型セキュリティ アプライアンスを設定します。

Startup Wizard のフィールドの詳細を確認するには、ウィンドウ下部にある [Help] ボタンをクリックします。

（注） DES ライセンスまたは 3DES-AES ライセンスを要求するエラー メッセージが表示された場合は、付録 A「3DES/AES ライセンスの取得」を参照してください。

（注） また、ネットワークのセキュリティ ポリシーに基づいて、外部インターフェイス、または必要なその他すべてのインターフェイスを経由する ICMP トラフィックをすべて拒否するように適応型セキュリティ アプライアンスを設定することを検討する必要もあります。このアクセス コントロール ポリシーは、ASDM を使用して設定できます。ASDM のメインページから、[Configuration] > [Properties] > [ICMP Rules] をクリックします。外部インターフェイス用のエントリを追加します。IP アドレスを 0.0.0.0 に、ネットマスクを 0.0.0.0 に、Action を拒否にそれぞれ設定します。

次の作業

次の 1 つ以上の章を参照して、それぞれの構成に応じた適応型セキュリティ アプライアンスを設定します。

実行内容	参照先
DMZ Web サーバを保護するための適応型セキュリティ アプライアンスの設定	第 8 章「シナリオ : DMZ 設定」
リモートアクセス VPN 用の適応型セキュリティ アプライアンスの設定	第 9 章「シナリオ : IPsec リモートアクセス VPN 設定」
ソフトウェア クライアントを使用した SSL VPN 接続のための適応型セキュリティ アプライアンスの設定	第 10 章「シナリオ : Cisco AnyConnect VPN クライアント用接続の設定」
Web ブラウザを使用した SSL VPN 接続のための適応型セキュリティ アプライアンスの設定	第 11 章「シナリオ : SSL VPN クライアントレス接続」
サイトツーサイト VPN 用の適応型セキュリティ アプライアンスの設定	第 12 章「シナリオ : サイトツーサイト VPN 設定」

CHAPTER 8

シナリオ：DMZ 設定

非武装地帯（DMZ）は、プライベート（内部）ネットワークとパブリック（外部）ネットワークとの間の中立帯に位置する単独のネットワークです。

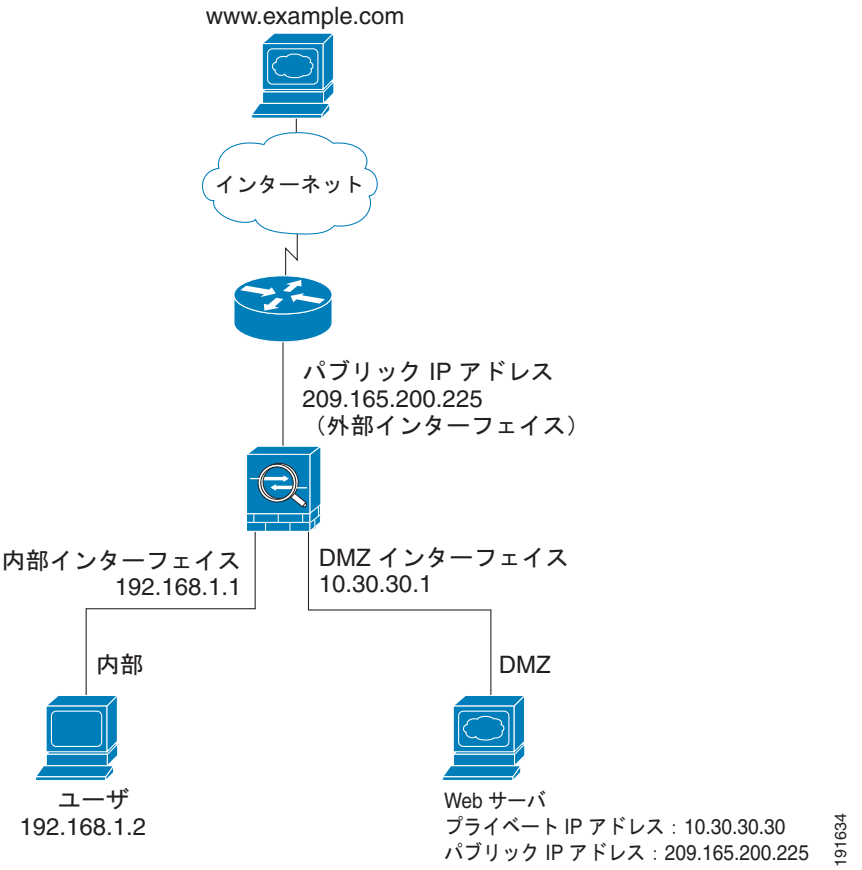
この章は、次の項で構成されています。

DMZ ネットワーク トポロジの例

この章では、図 8-1 に示すように適応型セキュリティ アプライアンスの DMZ 構成の設定方法について説明します。

この例では、Web サーバは DMZ インターフェイス上にあり、内部ネットワークおよび外部ネットワークの両方の HTTP クライアントが Web サーバにアクセスできます。

図 8-1　DMZ 設定シナリオのネットワーク レイアウト



このシナリオ例には、次の特徴があります。

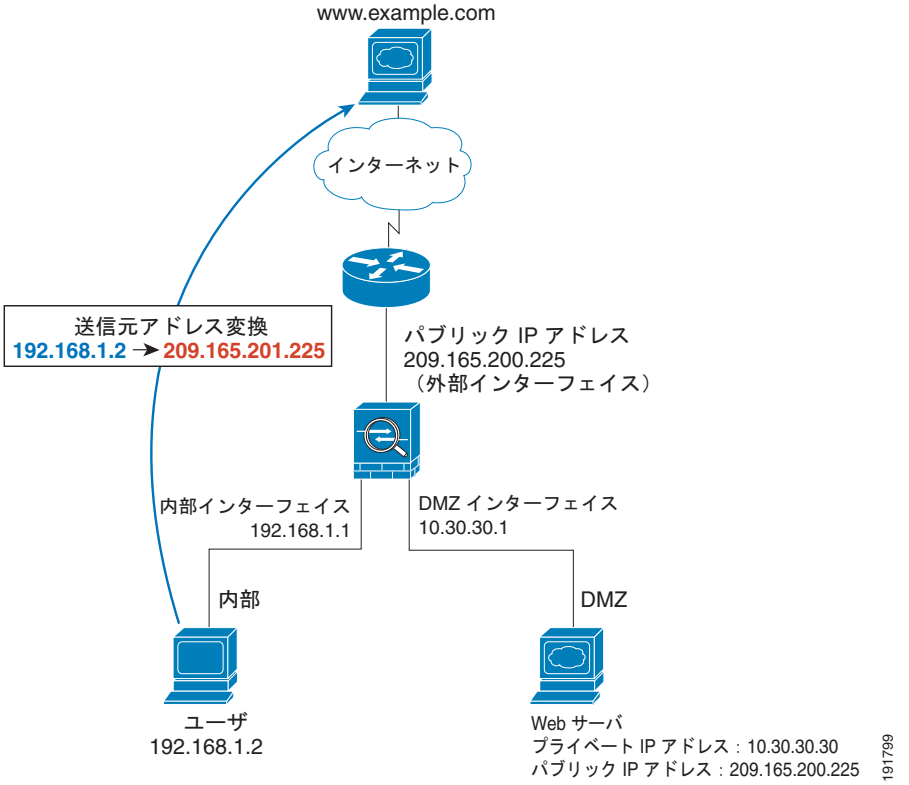
- Web サーバは、適応型セキュリティ アプライアンスの DMZ インターフェイス上に存在します。
- 内部ネットワーク上のクライアントは、DMZ 内の Web サーバにアクセスでき、インターネット上のデバイスとも通信できます。
- インターネット上のクライアントは、DMZ Web サーバへの HTTP アクセスが許可され、インターネットからのその他のトラフィックはすべて拒否されます。
- ネットワークには、だれでも使用できる IP アドレスが 1 つあります。これは、適応型セキュリティ アプライアンスの外部インターフェイスです（209.165.200.225）。このパブリック アドレスは適応型セキュリティ アプライアンスと DMZ Web サーバで共有されます。

この項は、次の内容で構成されています。

インターネットで Web サーバにアクセスする内部ユーザ

図 8-2 に、内部ユーザがインターネットの Web サーバから HTTP ページを要求している場合の、適応型セキュリティ アプライアンスを経由したトラフィック フローを示します。

図 8-2　インターネット Web サーバにアクセスする内部ユーザ



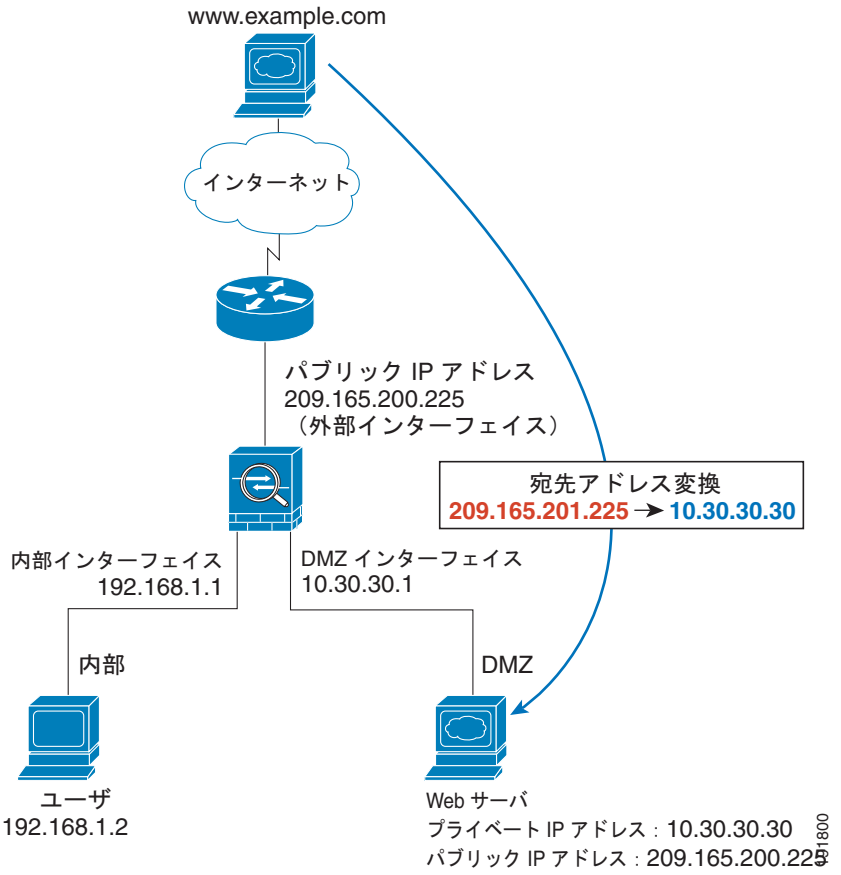
内部ユーザがインターネットの Web サーバから HTTP ページを要求している場合、データは次のように適応型セキュリティ アプライアンスを経由して移動します。

1. 内部ネットワークのユーザが、www.example.com から Web ページを要求します。
2. 適応型セキュリティ アプライアンスはパケットを受信し、新しいセッションであるため、パケットが許可されていることを確認します。
3. 適応型セキュリティ アプライアンスは Network Address Translation（NAT; ネットワーク アドレス変換）を行い、ローカルな送信元アドレス（192.168.1.2）を外部インターフェイスのパブリック アドレス（209.165.200.225）に変換します。
4. 適応型セキュリティ アプライアンスは、セッションか確立されていることを記録し、外部インターフェイスからパケットを転送します。
5. www.example.com が要求に応答すると、確立されたセッションを使用して、パケットは適応型セキュリティ アプライアンスを通過します。
6. 適応型セキュリティ アプライアンスは NAT を使用して、パブリック宛先（209.165.200.225）アドレスをローカル ユーザ アドレス（192.168.1.2）に変換します。
7. 適応型セキュリティ アプライアンスはパケットを内部ユーザに転送します。

DMZ Web サーバにアクセスするインターネット ユーザ

図 8-3 に、インターネット上のユーザが DMZ Web サーバから Web ページを要求している場合の、適応型セキュリティ アプライアンスを経由したトラフィック フローを示します。

図 8-3　DMZ Web サーバにアクセスする外部ユーザ



インターネット上のユーザが DMZ Web サーバから HTTP ページを要求している場合、トラフィックは次のように適応型セキュリティ アプライアンスを流れます。

1. 外部ネットワークのユーザは、適応型セキュリティ アプライアンスのパブリック IP アドレス（外部インターフェイスの IP アドレスである 209.165.200.225）を使用して、DMZ Web サーバから Web ページを要求します。
2. 適応型セキュリティ アプライアンスはパケットを受信し、新しいセッションであるため、パケットが許可されていることを確認します。
3. 適応型セキュリティ アプライアンスは、宛先アドレスを DMZ Web サーバのローカル アドレス（10.30.30.30）に変換し、DMZ インターフェイスを通してパケットを転送します。
4. DMZ Web サーバが要求に応答すると、適応型セキュリティ アプライアンスは DMZ Web サーバのローカル アドレス（10.30.30.30）を DMZ Web サーバのパブリック アドレス（209.165.200.225）に変換します。
5. 適応型セキュリティ アプライアンスはパケットを外部ユーザに転送します。

DMZ Web サーバにアクセスする内部ユーザ

図 8-4 に、DMZ Web サーバにアクセスしている内部ユーザを示します。

図 8-4　DMZ で Web サーバにアクセスする内部ユーザ

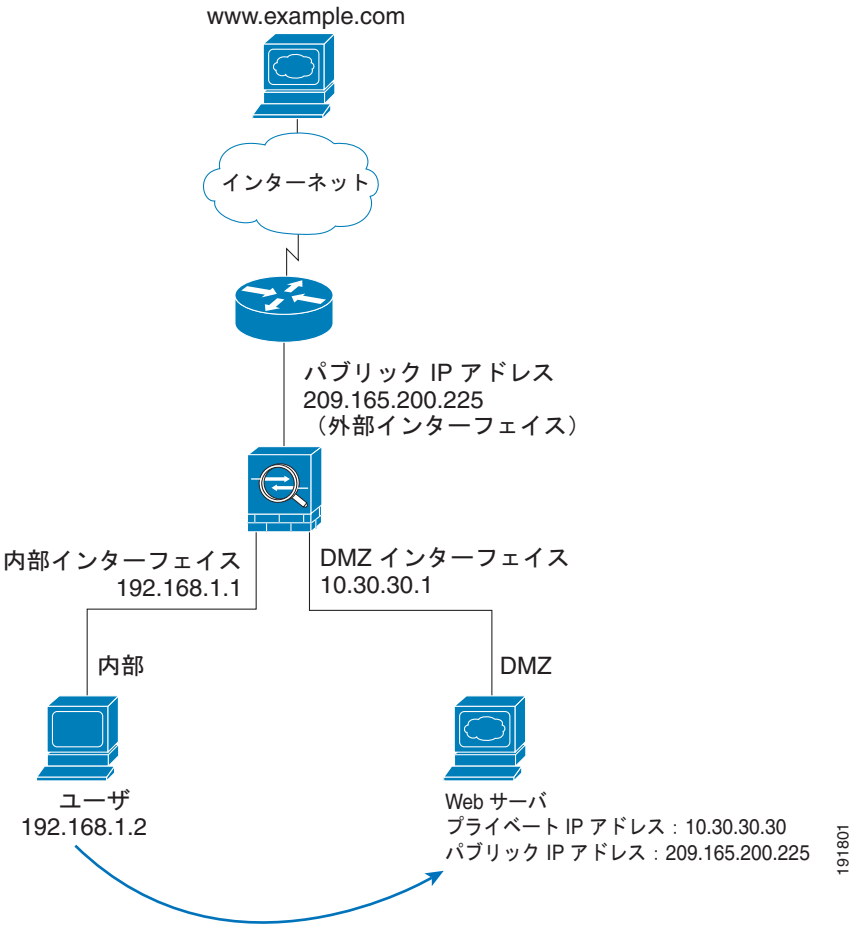


図 8-4 では、適応型セキュリティ アプライアンスは内部クライアントから DMZ Web サーバ宛の HTTP トラフィックを許可します。内部ネットワークには DNS サーバがないので、DMZ Web サーバへの内部クライアントの要求は、次のように処理されます。

1. ルックアップ要求が ISP の DNS サーバに送信されます。DMZ Web サーバのパブリック IP アドレスがクライアントに返されます。
2. 内部クライアントは、DMZ Web サーバのパブリック IP アドレスから Web ページを要求します。適応型セキュリティ アプライアンスは、その内部インターフェイス上の要求を受信します。
3. 適応型セキュリティ アプライアンスは、DMZ Web サーバのパブリック IP アドレスをその実アドレスに変換し（209.165.200.225 -> 10.30.30.30）、要求をその DMZ インターフェイスから Web サーバへ転送します。
4. DMZ Web サーバが要求に応答すると、適応型セキュリティ アプライアンスはその DMZ インターフェイス上のデータを受信し、その内部インターフェイスからユーザにデータを転送します。

この設定を作成する手順については、この章の後半部分で説明します。

DMZ 構成用の適応型セキュリティ アプライアンスの設定

この項では、ASDM を使用して、図 8-1 に示されている設定シナリオ用に適応型セキュリティ アプライアンスを設定する方法について説明します。手順では、シナリオに基づいたサンプル パラメータを使用します。

この設定手順では、適応型セキュリティ アプライアンスにはすでに内部インターフェイス、外部インターフェイス、および DMZ インターフェイスとして設定されているインターフェイスがあることを前提とします。DMZ インターフェイスのセキュリティ レベルを 0 ～ 100 の間に設定していることを確認します（通常は 50）。

（注） 適応型セキュリティ アプライアンスにインターフェイスをセットアップする必要がある場合、ASDM の Startup Wizard を使用できます。Startup Wizard の使用方法の詳細については、第 7 章「適応型セキュリティ アプライアンスの設定」を参照してください。

この項は、次の内容で構成されています。

この章の後半部分では、この設定を実装する方法について説明します。

設定要件

適応型セキュリティ アプライアンスのこの DMZ 構成では、次のような設定ルールが必要です。

目的	対象となるルール
内部クライアントが、インターネット上の Web サーバから情報を要求できる	適応型セキュリティ アプライアンスに備わった、内部クライアントによるインターネット上のデバイスへのアクセスを許可するデフォルト設定。設定を追加する必要はありません。
内部クライアントが、DMZ Web サーバから情報を要求できる	• DMZ Web サーバの実際の IP アドレスをパブリック IP アドレスに変換する（10.30.30.30 から 209.165.200.225 へ）、DMZ インターフェイスと内部インターフェイス間の NAT ルール。 • 内部クライアント ネットワークの実際のアドレスを変換する、内部インターフェイスと DMZ インターフェイス間の NAT ルール。このシナリオでは、内部ネットワークの実 IP アドレスはその実アドレス自体に「変換」されます。つまり、内部ネットワークの実 IP アドレスは、内部クライアントが DMZ Web サーバ（10.30.30.30）と通信するときに使用されます。
外部クライアントが、DMZ Web サーバから情報を要求できる	• DMZ Web サーバのパブリック IP アドレスをそのプライベート IP アドレスに変換する（209.165.200.225 から 10.30.30.30 へ）、外部インターフェイスと DMZ インターフェイス間のアドレス変換ルール。 • DMZ Web サーバ宛の着信 HTTP トラフィックを許可するアクセス コントロール ルール。

収集する情報

この設定手順を開始する前に、次の情報を収集します。

- パブリック ネットワーク上のクライアントに対して使用可能にする DMZ 内のサーバの内部 IP アドレス（このシナリオでは Web サーバ）。
- DMZ 内のサーバのために使用されるパブリック IP アドレス （パブリック ネットワーク上のクライアントはパブリック IP アドレスを使用して DMZ 内のサーバにアクセスします）。
- 発信トラフィックで内部 IP アドレスの代わりになるクライアント IP アドレス（このシナリオでは、外部インターフェイスの IP アドレス）。内部 IP アドレスが公開されないように、発信クライアント トラフィックはこのアドレスから発信されたように表示されます。

内部クライアントとインターネット上のデバイスとの通信を可能にする

内部クライアントによるインターネット上のデバイスからのコンテンツの要求を許可するには、適応型セキュリティ アプライアンスが内部クライアントの実際の IP アドレスを外部インターフェイスの外部アドレス（つまり適応型セキュリティ アプライアンスのパブリック IP アドレス）に変換します。発信トラフィックは、このアドレスから発信されたように表示されます。

内部クライアントと DMZ Web サーバとの通信を可能にする

この手順では、内部クライアントが DMZ 内の Web サーバと安全に通信できるように、適応型セキュリティ アプライアンスを設定します。この手順を実行するには、変換ルールを設定する必要があります。

DMZ Web サーバの実際の IP アドレスをそのパブリック IP アドレスに変換する（10.30.30.30 から 209.165.200.225 へ）、DMZ インターフェイスと内部インターフェイス間の NAT ルールを設定します。

このルールが必要なのは、内部クライアントが DNS ルックアップ要求を送信したときに、DNS サーバが DMZ Web サーバのパブリック IP アドレスを返すためです。

（注）　内部ネットワーク上には DNS サーバがないため、DNS 要求は適応型セキュリティ アプライアンスから出て、インターネット上の DNS サーバによって解決されなければなりません。

この項は、次の内容で構成されています。

内部インターフェイスと DMZ インターフェイス間の内部クライアント IP アドレスの変換

内部インターフェイスと DMZ インターフェイス間で内部クライアント IP アドレスを変換するように NAT を設定するには、次の手順に従います。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] ペインの順にクリックし、緑色の +（プラス）アイコンをクリックし、[Add "Network Object" NAT Rule] を選択します。

[Add Network Object] ダイアログボックスが表示されます。

ステップ 2　次の値を入力します。

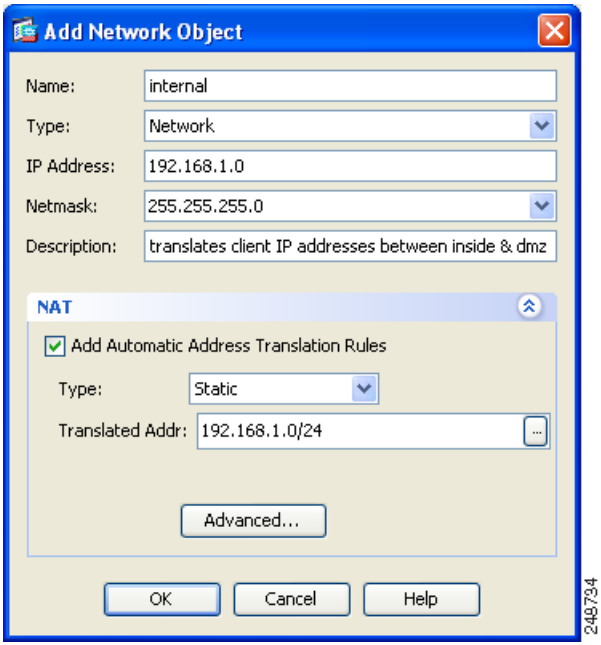
- [Name] フィールドに、オブジェクト名を入力します。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。
- [Type] ドロップダウン リストから、[Network] を選択します。
- [IP Address] フィールドに、クライアントまたはネットワークの実際の IP アドレスを入力します。このシナリオでは、ネットワークの IP アドレスは 192.168.1.0 です。
- [Netmask] フィールドに、IP アドレスが IPv4 アドレスである場合はサブネット マスクを入力し、IP アドレスが IPv6 アドレスである場合はプレフィクスを入力します。
- （オプション）[Description] フィールドに、ネットワーク オブジェクトの説明を入力します（最大 200 文字）。

（注）　[NAT] セクションが表示されていない場合は、[NAT] をクリックしてセクションを展開します。

ステップ 3　[Add Automatic Translation Rules] チェックボックスをオンにします。

ステップ 4　[Type] ドロップダウン リストから、[Static] を選択します。

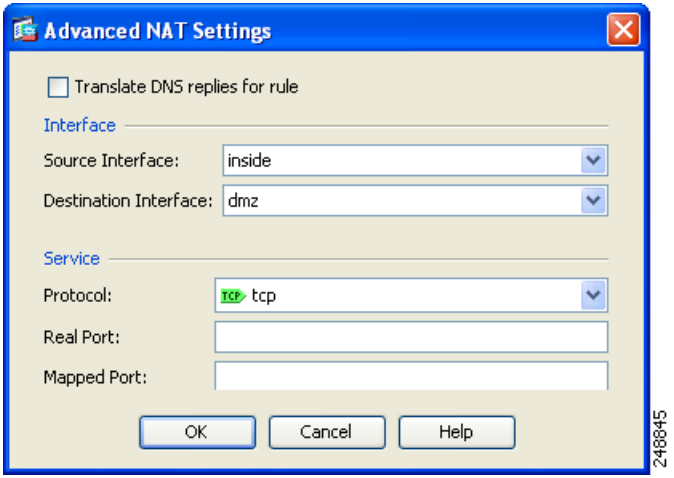
ステップ 5　[Translated Addr.] フィールドに、内部クライアントまたはネットワークの IP アドレスを入力します。または、[...] をクリックし、[Browse Translated Addr] ダイアログボックスからアドレスを選択します。[IP Address] フィールドに、ネットワークの IP アドレスを入力します。このシナリオでは、ネットワークの IP アドレスは 192.168.1.0 です。



ステップ 6　[Advanced] をクリックし、[Advanced NAT Settings] ダイアログボックスで次のオプションを設定します。

- [Source Interface] ドロップダウン リストで、[inside] インターフェイスを選択します。
- [Destination Interface] ドロップダウン リストから、[DMZ] インターフェイスを選択します。

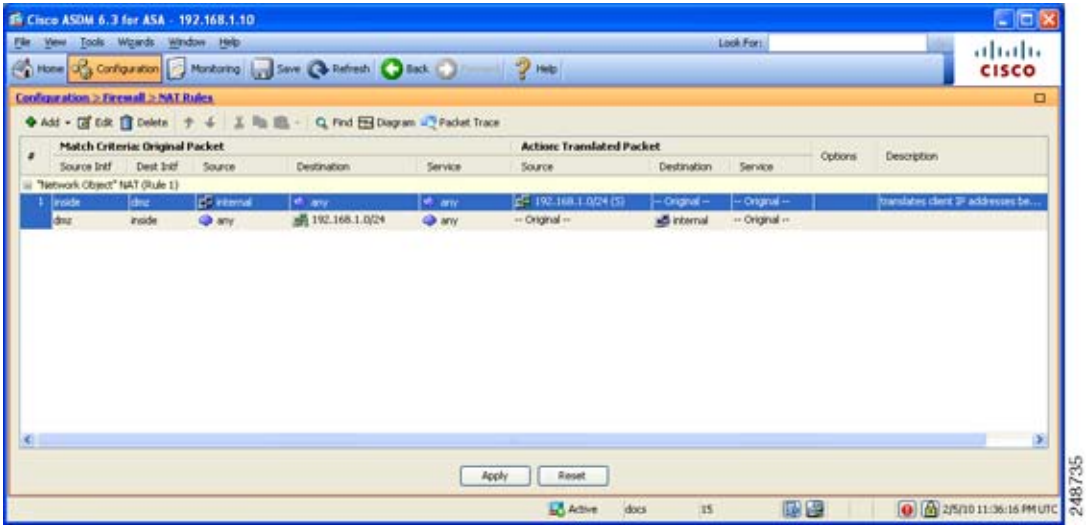
  この 2 つの設定により、NAT ルールを適用する実際のインターフェイスとマップされるインターフェイスを指定したことになります。



ステップ 7　[OK] をクリックします。[Add Network Object] ダイアログボックスに戻ります。

ステップ 8　[OK] をクリックしてルールを追加し、Address Translation Rules のリストに戻ります。

ルールが、意図したとおりに作成されたことを確認します。表示される設定は次のようになります。



ステップ 9　[Apply] をクリックして、適応型セキュリティ アプライアンスの設定変更を終了します。

内部インターフェイスでの Web サーバのパブリック アドレスのその実アドレスへの変換

Web サーバのパブリック IP アドレスをその実際の IP アドレスに変換する NAT ルールを設定するには、次の手順に従います。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] ペインの順にクリックし、緑色の +（プラス）アイコンをクリックし、[Add "Network Object" NAT Rule] を選択します。

[Add Network Object] ダイアログボックスが表示されます。

ステップ 2　次の値を入力します。

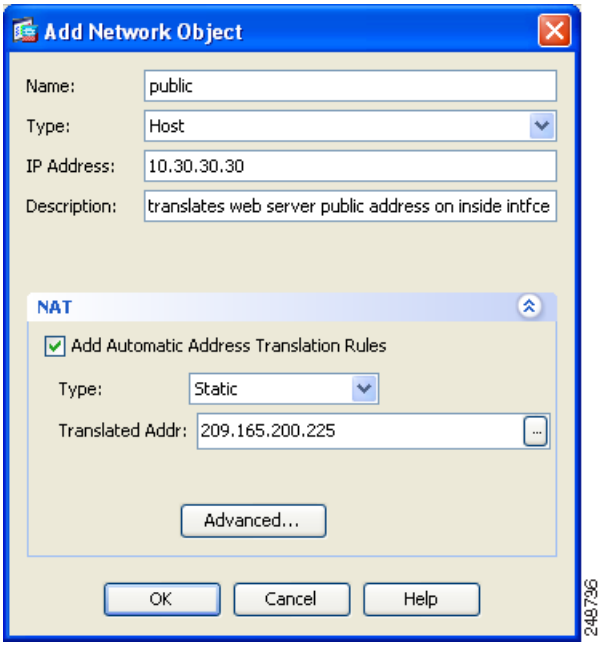
- [Name] フィールドに、オブジェクト名を入力します。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。
- [Type] ドロップダウン リストから、[Host] を選択します。
- [IP Address] フィールドに、DMZ Web サーバの実際の（プライベート）アドレスを入力します。このシナリオでは、IP アドレスは 10.30.30.30 です。
- （オプション）[Description] フィールドに、ネットワーク オブジェクトの説明を入力します（最大 200 文字）。

（注）　[NAT] セクションが表示されていない場合は、[NAT] をクリックしてセクションを展開します。

ステップ 3　[Add Automatic Translation Rules] チェックボックスをオンにします。

ステップ 4　[Type] ドロップダウン リストから、[Static] を選択します。

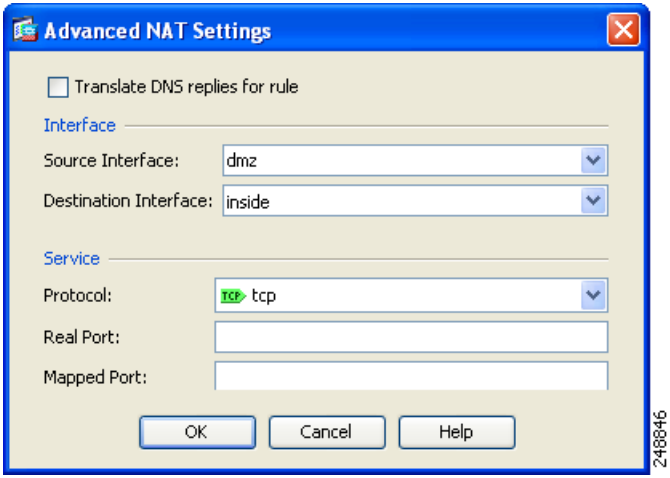
ステップ 5　[Translated Addr.] フィールドに、DMZ Web サーバのパブリック アドレス（またはマップ アドレス）を入力します。または、[...] をクリックし、[Browse Translated Addr] ダイアログボックスからアドレスを選択します。このシナリオでは、IP アドレスは 209.165.200.225 です。



ステップ 6　[Advanced] をクリックし、[Advanced NAT Settings] ダイアログボックスで次のオプションを設定します。

- [Source Interface] ドロップダウン リストで、[DMZ] インターフェイスを選択します。
- [Destination Interface] ドロップダウン リストで、[inside] インターフェイスを選択します。

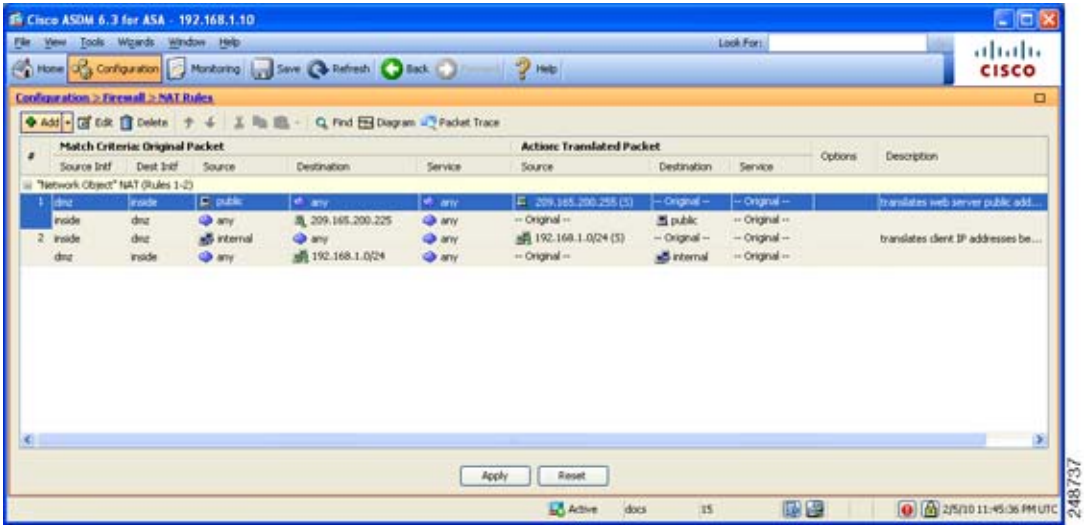
  この 2 つの設定により、NAT ルールを適用する実際のインターフェイスとマップされるインターフェイスを指定したことになります。



ステップ 7　[OK] をクリックします。[Add Network Object] ダイアログボックスに戻ります。

ステップ 8　[OK] をクリックしてルールを追加し、Address Translation Rules のリストに戻ります。

ルールが、意図したとおりに作成されたことを確認します。表示される設定は次のようになります。



ステップ 9　[Apply] をクリックして、適応型セキュリティ アプライアンスの設定変更を終了します。

DMZ Web サーバへのパブリック アクセスのためのスタティック PAT の設定（ポート フォワーディング）

DMZ Web サーバは、インターネット上のすべてのホストからアクセスできる必要があります。この設定では、DMZ Web サーバのプライベート IP アドレスをパブリック IP アドレスに変換し、外部 HTTP クライアントが適応型セキュリティ アプライアンスを認識せずに Web サーバにアクセスできるようにする必要があります。このシナリオでは、DMZ Web サーバで、パブリック IP アドレスと適応型セキュリティ アプライアンスの外部インターフェイスが共有されています（209.165.200.225）。

実際の Web サーバの IP アドレス（10.30.30.30）をパブリック IP アドレス（209.165.200.225）にスタティックにマッピングするには、次の手順に従います。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] ペインの順にクリックし、緑色の +（プラス）アイコンをクリックし、[Add "Network Object" NAT Rule] を選択します。

[Add Network Object] ダイアログボックスが表示されます。

ステップ 2　次の値を入力します。

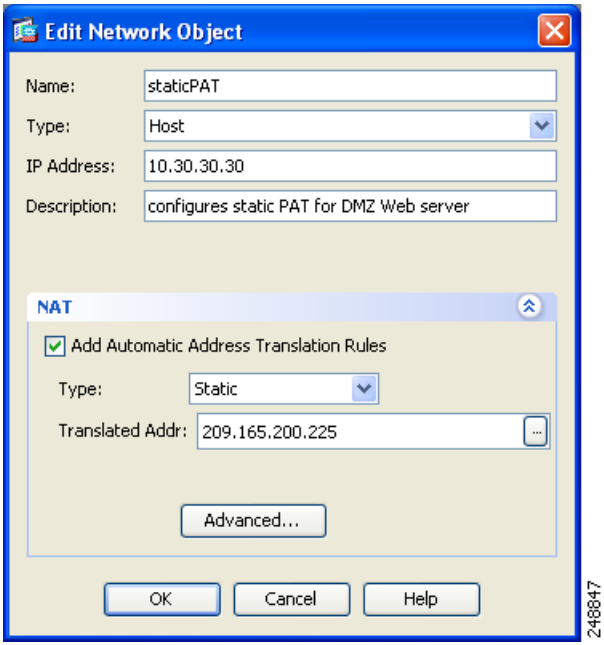
- [Name] フィールドに、オブジェクト名を入力します。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。
- [Type] ドロップダウン リストから、[Host] を選択します。
- [IP Address] フィールドに、DMZ Web サーバの実際の IP アドレスを入力します。このシナリオでは、IP アドレスは 10.30.30.30 です。
- （オプション）[Description] フィールドに、ネットワーク オブジェクトの説明を入力します（最大 200 文字）。

（注）　[NAT] セクションが表示されていない場合は、[NAT] をクリックしてセクションを展開します。

ステップ 3　[Add Automatic Translation Rules] チェックボックスをオンにします。

ステップ 4　[Type] ドロップダウン リストから、[Static] を選択します。

ステップ 5　[Translated Addr.] フィールドに、Web サーバで使用されるパブリック IP アドレスを入力します。これは、指定したインターフェイス（この場合は外部インターフェイス）の IP アドレスです。または、[...] をクリックし、[Browse Translated Addr] ダイアログボックスからアドレスを選択します。

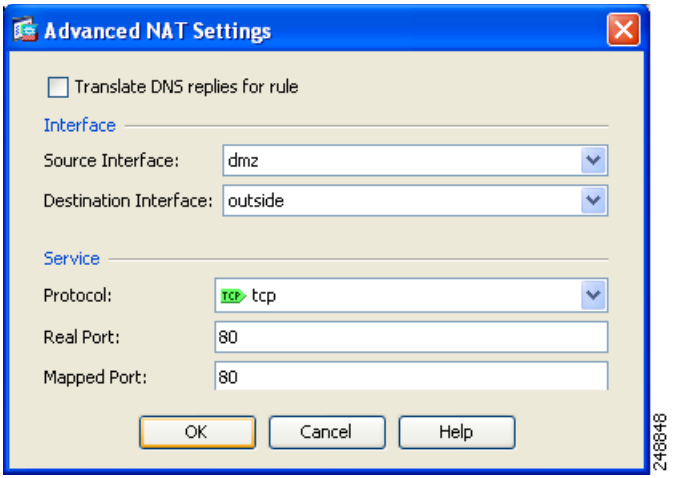


ステップ 6　[Advanced] をクリックし、[Advanced NAT Settings] ダイアログボックスで次のオプションを設定します。

- [Source Interface] ドロップダウン リストで、[DMZ] インターフェイスを選択します。
- [Destination Interface] ドロップダウン リストから、[Outside] インターフェイスを選択します。

  この 2 つの設定により、NAT ルールを適用する実際のインターフェイスとマップされるインターフェイスを指定したことになります。
- ポート変換を設定したスタティック NAT を設定するには、[Service] の [Protocol] ドロップダウン リストから [tcp] を選択します。
- [Real Port] フィールドに 80 と入力します。

- [Mapped Port] フィールドに 80 と入力します。

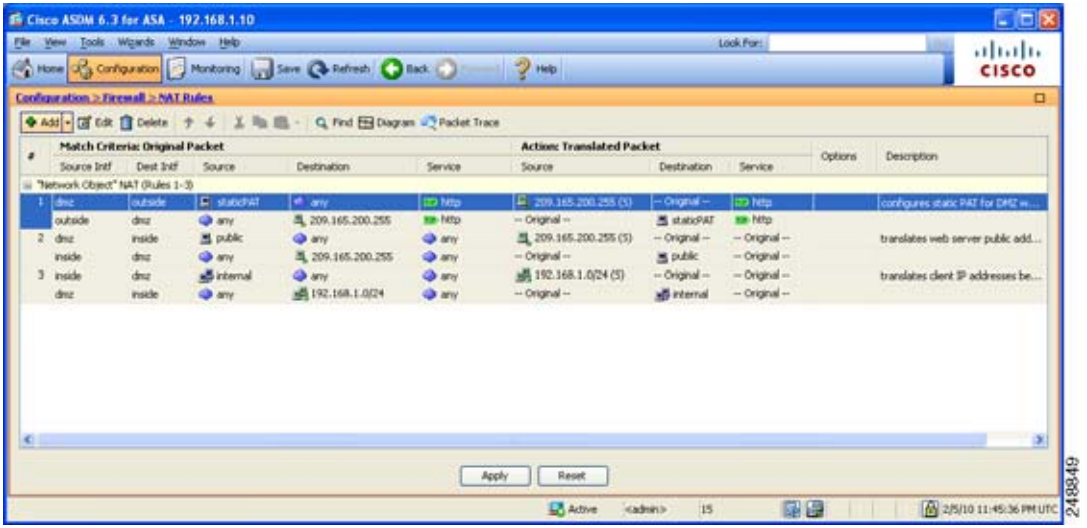


パブリック IP アドレスは 1 つだけなので、Port Address Translation を使用して、DMZ Web サーバの IP アドレスを適応型セキュリティ アプライアンスのパブリック IP アドレス（外部インターフェイスの IP アドレス）に変換する必要があります。

ステップ 7　[OK] をクリックします。[Add Network Object] ダイアログボックスに戻ります。

ステップ 8　[OK] をクリックしてルールを追加し、Address Translation Rules のリストに戻ります。

ルールが、意図したとおりに作成されたことを確認します。表示される設定は次のようになります。



ステップ 9　[Apply] をクリックして、適応型セキュリティ アプライアンスの設定変更を終了します。

DMZ Web サーバへのパブリック HTTP アクセスの提供

デフォルトでは、適応型セキュリティ アプライアンスは、パブリック ネットワークから着信するトラフィックをすべて拒否します。インターネットから DMZ Web サーバにアクセスするトラフィックを許可するには、DMZ Web サーバ宛の着信 HTTP トラフィックを許可するアクセス コントロール ルールを設定する必要があります。

このアクセス コントロール ルールは、トラフィックを処理する適応型セキュリティ アプライアンスのインターフェイスに対して、トラフィックが着信されるかどうか、トラフィックの発信元および宛先、および許可するトラフィック プロトコルとサービスのタイプを指定します。

この項では、トラフィックの宛先が DMZ ネットワークの Web サーバである場合に、インターネット上のホストまたはネットワークから発信される着信 HTTP トラフィックを許可するアクセス ルールを作成します。パブリック ネットワークから着信する他のすべてのトラフィックは拒否されます。

アクセス コントロール ルールを設定するには、次の手順に従います。

ステップ 1　メイン ASDM ウィンドウで、次の内容を実行します。

a. [Configuration] ツールをクリックします。

b. [Firewall] ペインで、[Access Rules] をクリックします。

c. 緑色のプラス アイコンをクリックし、[Add Access Rule] を選択します。

[Add Access Rule] ダイアログボックスが表示されます。

ステップ 2　[Add Access Rule] ダイアログボックスで、次の内容を実行します。

a. [Interface] ドロップダウン リストから、[Outside] を選択します。

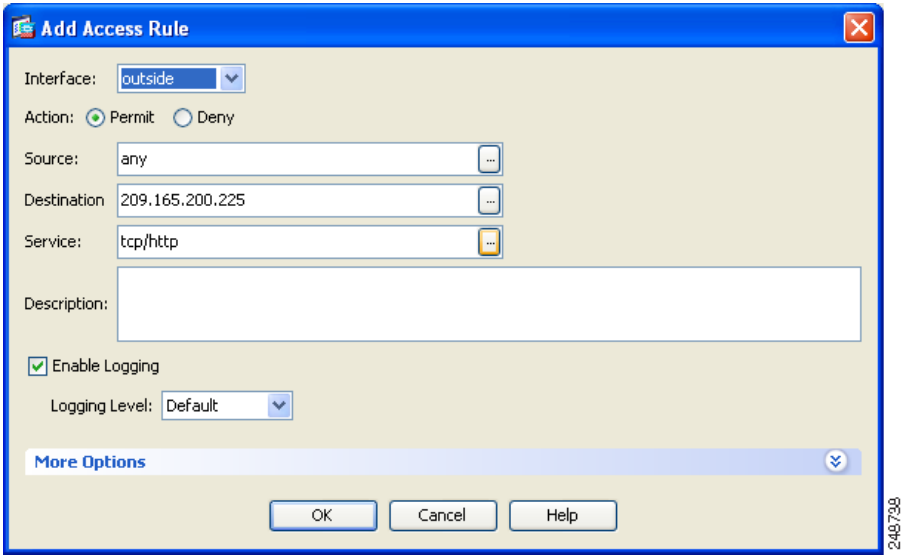
b. [Permit Action] オプション ボタンをクリックします。

c. [Source] フィールドに Any と入力します。

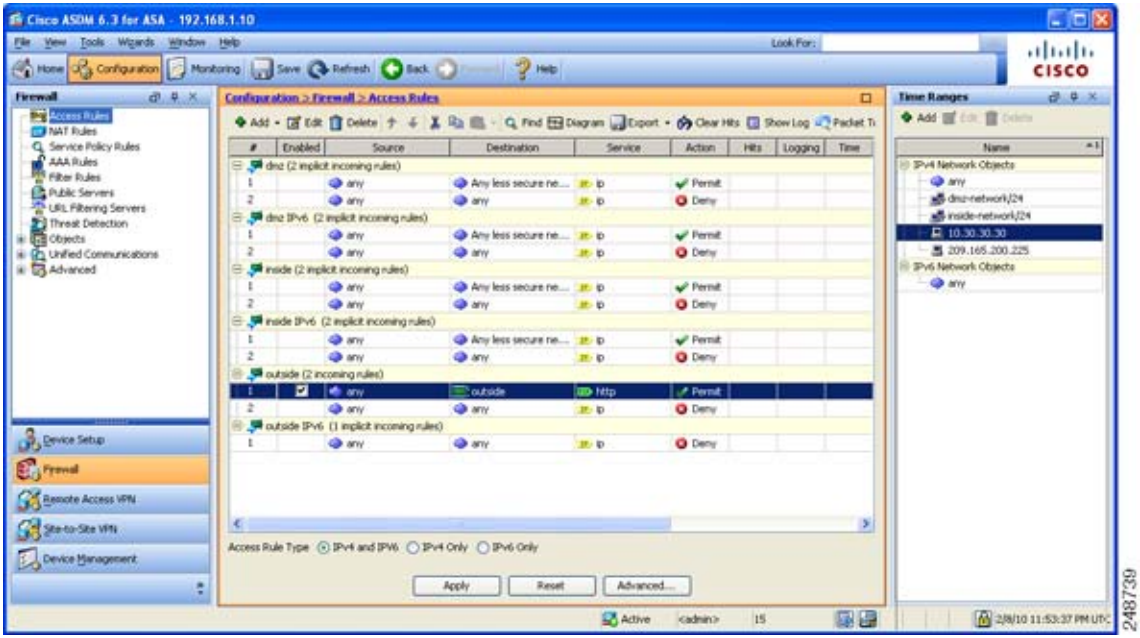
d. [Destination] フィールドに、Web サーバのパブリック IP アドレス（209.165.200.225）を入力します。

e. [Service] フィールドに TCP/HTTP と入力します。

この時点で、[Add Access Rule] ダイアログボックスのエントリは次のようになります。



f. [OK] をクリックして、[Security Policy] > [Access Rules] ペインに戻ります。表示される設定は次のようになります。



入力した情報が正しいことを確認します。

[Apply] をクリックし、適応型セキュリティ アプライアンスが現在実行している設定に変更を保存します。

プライベート ネットワークに存在するクライアントは、DMZ Web サーバからのコンテンツに対する HTTP 要求を解決できるだけでなく、プライベート ネットワークの安全性を保持できます。

ステップ 3　次にデバイスを起動するときに適用されるように、設定変更をスタートアップ コンフィギュレーションに保存する場合は、[File] メニューから [Save] をクリックします。

または、ASDM を終了するときに設定変更を半永久的に保存するように求められます。

設定変更を保存しない場合は、次にデバイスを起動するときに変更前の設定がそのまま適用されます。

次の作業

DMZ 内の Web サーバを保護するためだけに適応型セキュリティ アプライアンスを配置する場合は、これで初期設定が完了しました。次の追加の手順を実行することもできます。

実行内容	参照先
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』
日常的な運用について	『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series System Log Messages*』

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できます。次の項では、適応型セキュリティ アプライアンスの他の一般的なアプリケーションの設定手順について説明します。

実行内容	参照先
リモートアクセス VPN の設定	第 9 章「シナリオ：IPsec リモートアクセス VPN 設定」
Cisco AnyConnect ソフトウェア クライアントの SSL VPN の設定	第 10 章「シナリオ：Cisco AnyConnect VPN クライアント用接続の設定」
ブラウザ ベース SSL VPN の設定	第 11 章「シナリオ：SSL VPN クライアントレス接続」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN 設定」

CHAPTER 9

シナリオ：IPsec リモートアクセス VPN 設定

この章では、適応型セキュリティ アプライアンスを使用して、リモートアクセス IPsec VPN 接続を受け入れる方法について説明します。リモートアクセス VPN を使用すると、インターネットを越えてセキュアな接続（トンネル）を作成でき、オフサイトのユーザにセキュアなアクセスを提供できます。このタイプの VPN 設定では、リモート ユーザは、Cisco VPN クライアントを実行して、適応型セキュリティ アプライアンスに接続する必要があります。

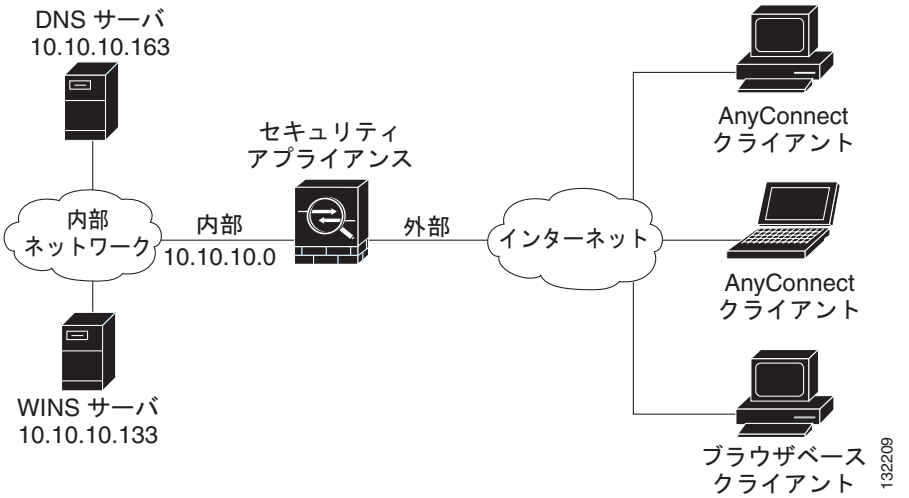
Easy VPN ソリューションを実装する場合、この章では、Easy VPN サーバ（別名、ヘッドエンド デバイス）を設定する方法について説明します。

この章は、次の項で構成されています。

IPsec リモートアクセス VPN ネットワーク トポロジの例

図 9-1 に、インターネットを越えて Cisco Easy VPN ソフトウェア クライアントまたはハードウェア クライアントなどの VPN クライアントからの要求を受け入れ、VPN クライアントとの IPsec 接続を確立するように設定された適応型セキュリティ アプライアンスを示します。

図 9-1　リモート アクセス VPN シナリオのネットワーク レイアウト



IPsec リモートアクセス VPN シナリオの実装

この項では、リモート クライアントおよびデバイスから IPsec VPN 接続を受け入れるように適応型セキュリティ アプライアンスを設定する方法について説明します。Easy VPN ソリューションを実装する場合、この項では、Easy VPN サーバ（別名、ヘッドエンド デバイス）を設定する方法について説明します。

設定内容の例で使われる値は、図 9-1 に示すリモートアクセス シナリオのものです。

この項は、次の内容で構成されています。

収集する情報

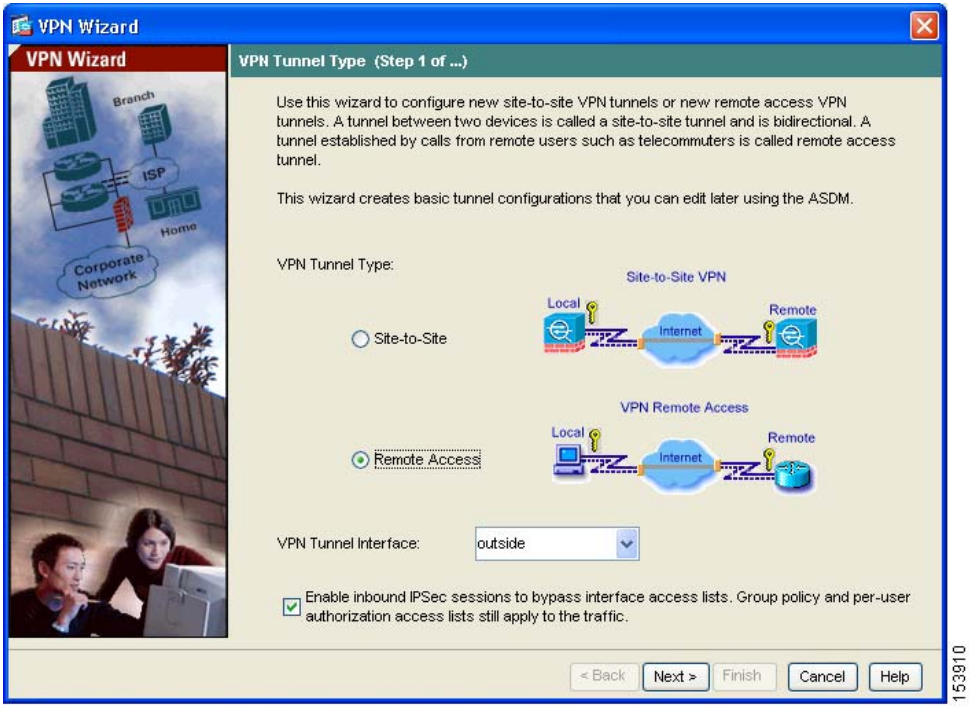
リモート アクセス IPsec VPN 接続を受け入れるように適応型セキュリティ アプライアンスを設定する手順を開始する前に、次の情報を手元に用意してください。

- IP プールで使用する IP アドレスの範囲。これらのアドレスは、正常に接続されると、リモート VPN クライアントに割り当てられます。
- ローカル認証データベースを作成するときに使用するユーザのリスト（認証用に AAA サーバを使用している場合を除く）。
- VPN に接続する場合に、リモート クライアントが使用するネットワーキング情報。内容は次のとおりです。
  - プライマリおよびセカンダリの DNS サーバの IP アドレス
  - プライマリおよびセカンダリの WINS サーバの IP アドレス
  - デフォルトのドメイン名
  - 認証されたリモート クライアントにアクセスできるローカル ホスト、グループ、およびネットワークの IP アドレスのリスト

IPsec リモートアクセス VPN の設定

リモートアクセス VPN を設定するには、次の手順に従います。

ステップ 1　ASDM メイン ウィンドウで、[Wizards] ドロップダウン メニューから [VPN Wizard] を選択します。VPN Wizard の Step 1 画面が表示されます。



ステップ 2　VPN Wizard の Step 1 で、次の手順に従います。

a.　[Remote Access] オプション ボタンをクリックします。

b.　ドロップダウン リストから、着信 VPN トンネルで有効なインターフェイスとして [Outside] を選択します。

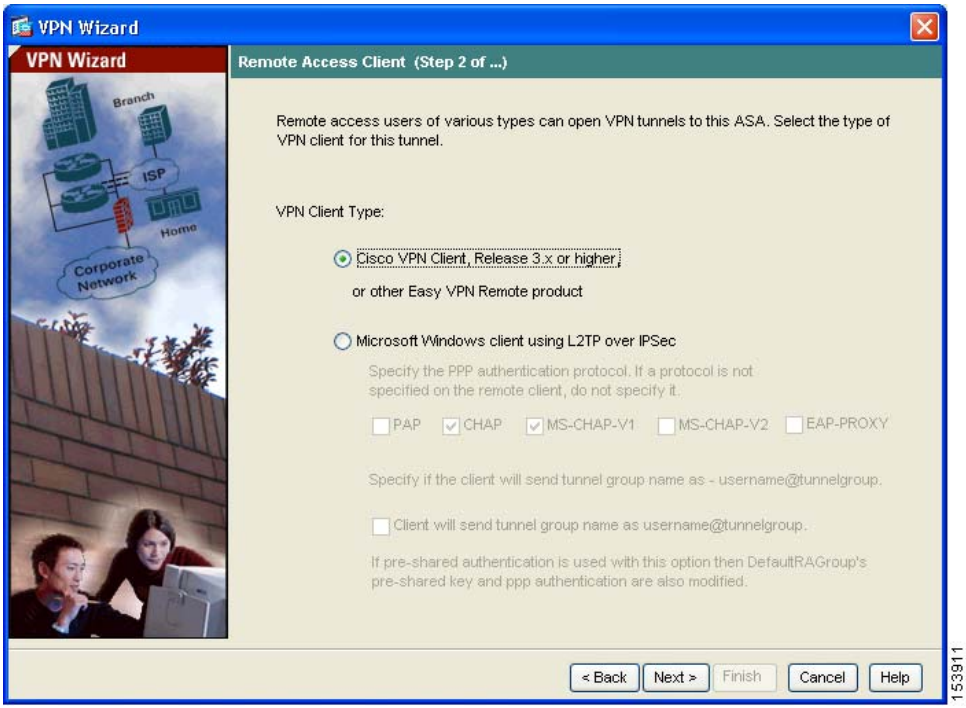
c.　[Next] をクリックして続行します。

VPN クライアント タイプの選択

VPN Wizard の Step 2 で、次の手順に従います。

ステップ 1　この適応型セキュリティ アプライアンスに接続するリモート ユーザを有効にする VPN クライアントのタイプを指定します。このシナリオでは、[Cisco VPN Client] オプション ボタンをクリックします。

その他の Cisco Easy VPN リモート製品も使用できます。



ステップ 2　[Next] をクリックして続行します。

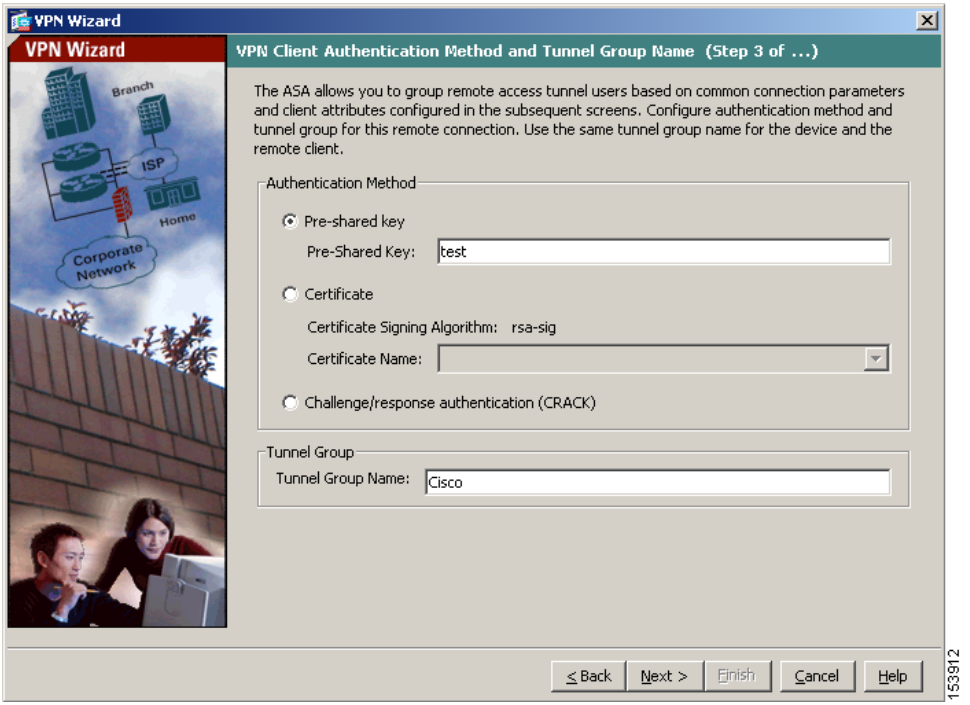
VPN トンネル グループ名と認証方式の指定

VPN Wizard の Step 3 で、次の手順に従います。

ステップ 1　次のいずれかの操作を実行して、使用する認証のタイプを指定します。

- 認証にスタティック事前共有キーを使用するには、[Pre-Shared Key] オプション ボタンをクリックし、事前共有キー（たとえば、「Cisco」）を入力します。このキーは、IPsec ネゴシエーションで使用されます。
- 認証にデジタル証明書を使用するには、[Certificate] オプション ボタンをクリックし、ドロップダウン リストから証明書署名アルゴリズムを選択し、次に、事前設定されているトラストポイント名をドロップダウン リストから選択します。

  認証にデジタル証明書を使用する予定で、まだトラストポイント名を設定していない場合は、他の 2 つのオプションのいずれかを使用してウィザードを続行できます。認証設定は、標準 ASDM ウィンドウを使用して後で修正できます。
- [Challenge/Response Authentication (CRACK)] オプション ボタンをクリックすると、この認証方式を使用できます。



ステップ 2　共通の接続パラメータおよびクライアント アトリビュートを使用して、この適応型セキュリティ アプライアンスに接続する複数ユーザのセットのトンネル グループ名（たとえば、「Cisco」）を入力します。

ステップ 3　[Next] をクリックして続行します。

ユーザ認証方式の指定

ユーザの認証は、ローカル認証データベース、または外部の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバを使用して実行できます（AAA サーバには RADIUS、TACACS+、SDI、NT、Kerberos、および LDAP があります）。

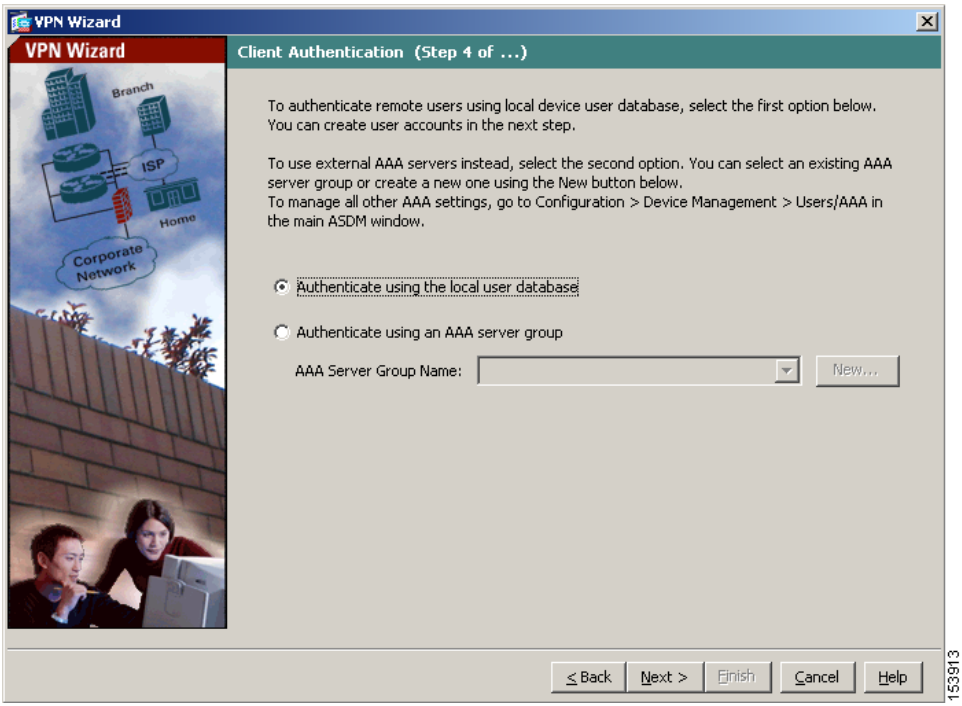
VPN Wizard の Step 4 で、次の手順に従います。

ステップ 1　適応型セキュリティ アプライアンスにユーザ データベースを作成してユーザを認証するには、[Authenticate Using the Local User Database] オプション ボタンをクリックします。

ステップ 2　外部 AAA サーバ グループを使用してユーザを認証する場合は、次の手順に従います。

a. [Authenticate Using an AAA Server Group] オプション ボタンをクリックします。

b. 事前設定されているサーバ グループを [Authenticate using an AAA Server Group] ドロップダウン リストから選択するか、[New] をクリックして新しい AAA サーバ グループを追加します。



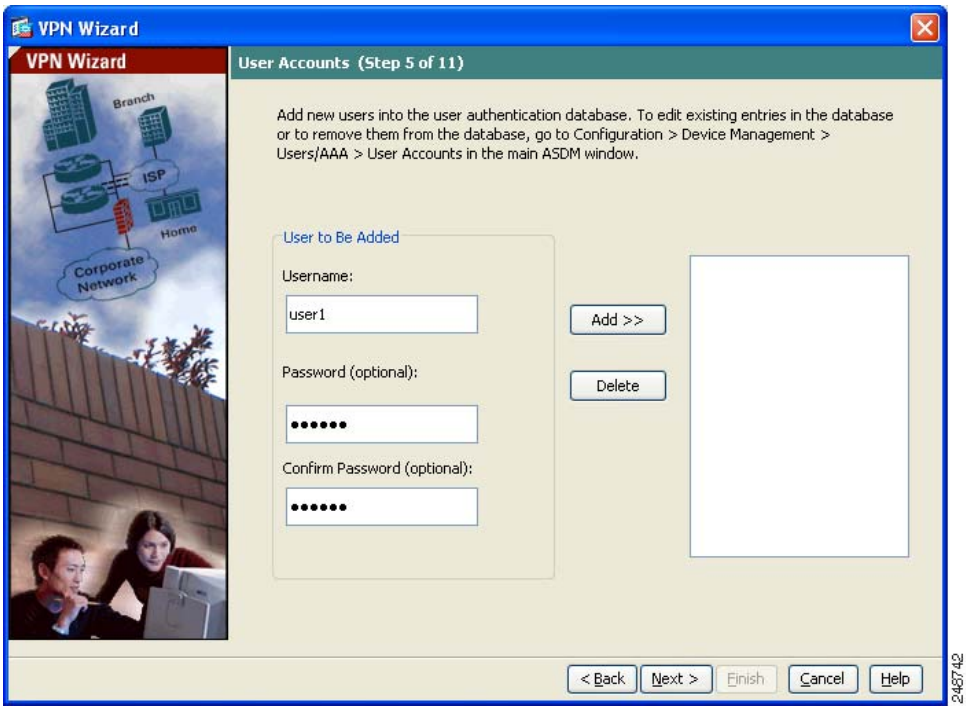
ステップ 3　[Next] をクリックして続行します。

（オプション）ユーザ アカウントの設定

ローカル ユーザ データベースを使用してユーザを認証する場合、次の手順で新しいユーザ アカウントを作成できます。ASDM 設定インターフェイスを使用して、後でユーザを追加することもできます。

VPN Wizard の Step 5 で、次の手順に従います。

ステップ 1　新しいユーザを追加するには、ユーザ名とパスワードを入力し、[Add] をクリックします。



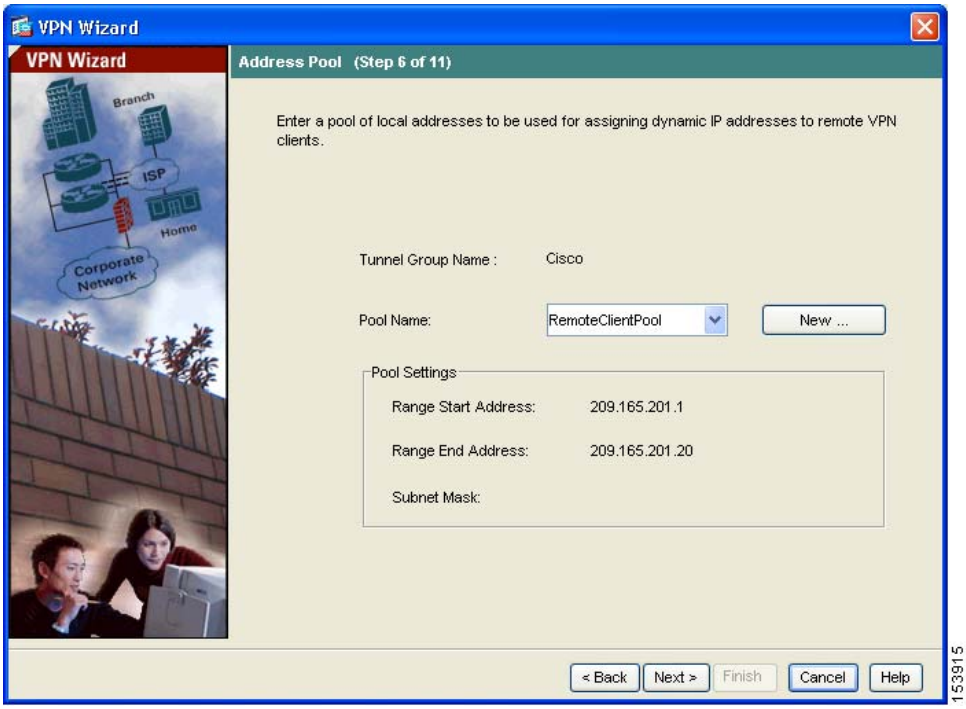
ステップ 2　新しいユーザの追加が終了したら、[Next] をクリックして続行します。

アドレス プールの設定

リモート クライアントがネットワークにアクセスするには、接続に成功したときにリモート VPN クライアントに割り当てる IP アドレスのプールを設定する必要があります。このシナリオでは、プールは 209.165.201.1 ～ 209.166.201.20 の範囲の IP アドレスを使用するように設定します。

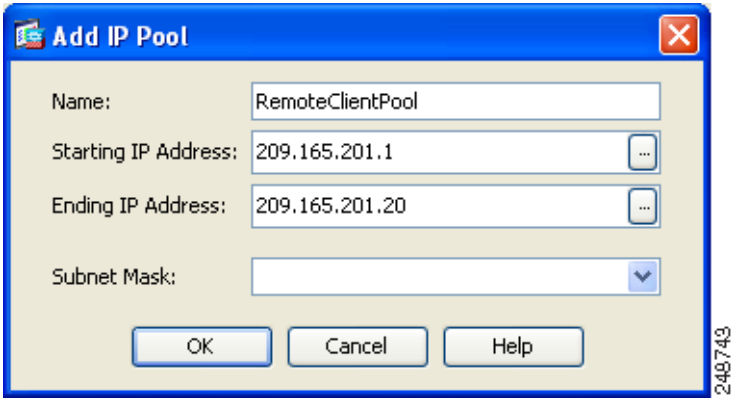
VPN Wizard の Step 6 で、次の手順に従います。

ステップ 1　プール名を入力するか、事前設定されているプールを [Pool Name] ドロップダウン リストから選択します。



または、[New] をクリックして、新しいアドレス プールを作成します。

[Add IP Pool] ダイアログボックスが表示されます。



ステップ 2　[Add IP Pool] ダイアログボックスで、次の内容を実行します。

a. 範囲の開始 IP アドレスと終了 IP アドレスを入力します。

b. （オプション）サブネット マスクを入力するか、[Subnet Mask] ドロップダウン リストから IP アドレス範囲のサブネット マスクを選択します。

c. [OK] をクリックして、VPN Wizard の Step 6 に戻ります。

ステップ 3　[Next] をクリックして続行します。

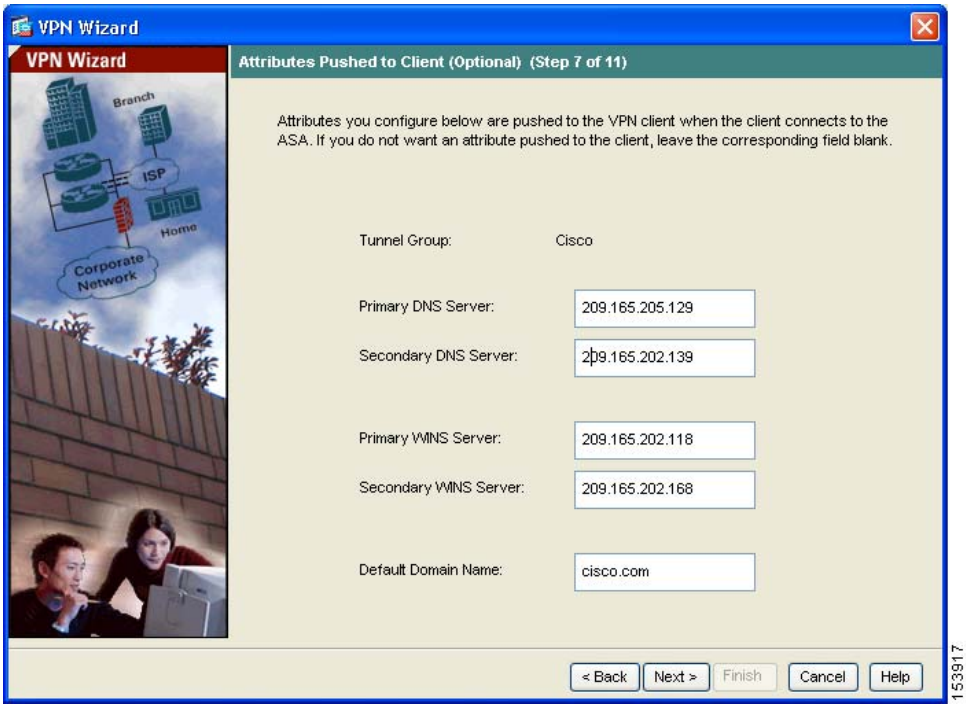
クライアント アトリビュートの設定

各リモート アクセス クライアントがネットワークにアクセスするには、使用する DNS サーバと WINS サーバ、デフォルトのドメイン名などの基本的なネットワーク設定情報が必要です。各リモート クライアントを個々に設定するのではなく、ASDM にクライアント情報を設定できます。接続が確立されると、適応型セキュリティ アプライアンスは、この情報をリモート クライアントまたは Easy VPN ハードウェア クライアントに適用します。

必ず正しい値を指定してください。値が正しくない場合、リモート クライアントが解決に DNS 名を使用できない、または Windows ネットワーキングを使用できないという問題が発生します。

VPN Wizard の Step 7 で、次の手順に従います。

ステップ 1　リモート クライアントに適用するネットワーク設定情報を入力します。



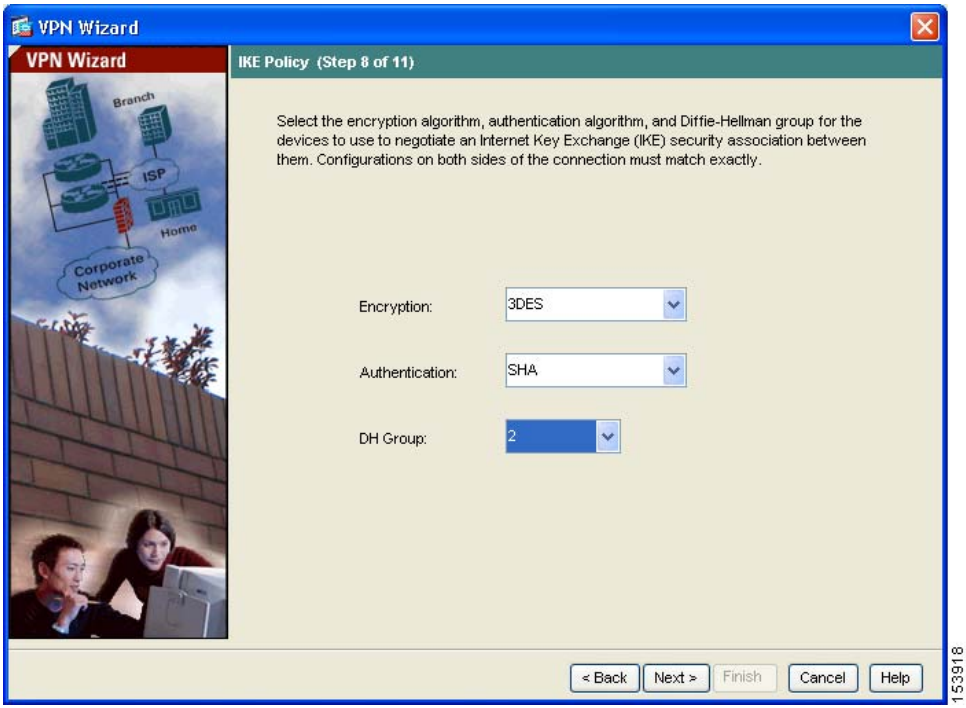
ステップ 2　[Next] をクリックして続行します。

IKE ポリシーの設定

IKE は、データを保護しプライバシーを保証する暗号化方式を含むネゴシエーション プロトコルで、ピアの ID を確認する認証方式でもあります。ほとんどの場合、ASDM のデフォルト値を使用すれば、十分にセキュアな VPN トンネルを確立できます。

VPN Wizard の Step 8 で IKE ポリシーを指定するには、次の手順に従います。

ステップ 1　IKE セキュリティ アソシエーションにおいて適応型セキュリティ アプライアンスが使用する暗号化アルゴリズム（DES、3DES、または AES）、認証アルゴリズム（MD5 または SHA）、および Diffie-Hellman グループ（1、2、5、または 7）を選択します。



ステップ 2　[Next] をクリックして続行します。

アドレス変換の例外およびスプリット トンネリングの指定

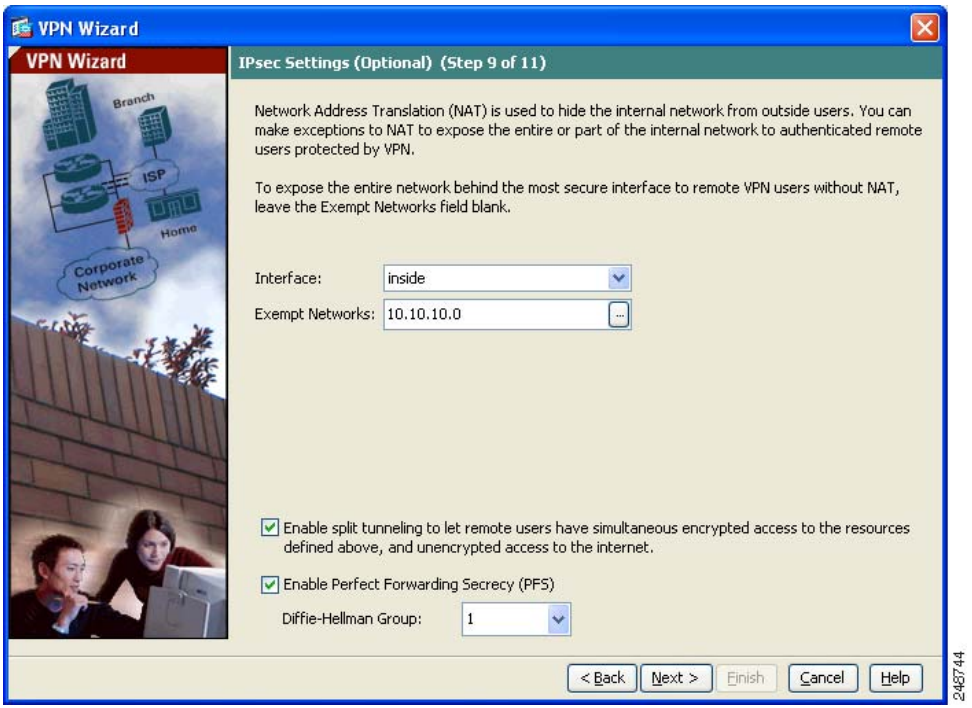
スプリット トンネリングを使用すると、リモートアクセス IPsec クライアントは、パケットを条件によって、IPsec トンネル経由で送信すること（暗号化形式）や、ネットワーク インターフェイスに送信すること（テキスト形式）ができます。

適応型セキュリティ アプライアンスは、Network Address Translation（NAT; ネットワーク アドレス変換）を使用して、内部 IP アドレスが外部に公開されないようにしています。認証されたリモート ユーザにアクセスを許可するローカル ホストおよびネットワークを特定することで、このネットワーク保護に例外を設定できます。

VPN Wizard の Step 9 で、次の手順に従います。

ステップ 1　認証されたリモート ユーザにアクセスを許可する内部リソースのリストに入れるホスト、グループ、およびネットワークを指定します。

[Selected Hosts/Networks] 領域のホスト、グループ、およびネットワークを動的に追加するには [Add]、動的に削除するには [Delete] をクリックします。



ステップ 2　スプリット トンネリングをイネーブルにするには、[Enable Split Tunneling] チェック ボックスをオンにします。スプリット トンネリングを使用すると、設定したネットワークの外部のトラフィックは、暗号化された VPN トンネルを経由せずにインターネットに直接送信されます。

ステップ 3　PFS をイネーブルにするには、[Enable Perfect Forwarding Secrecy] チェック ボックスをオンにします。PFS をイネーブルにすると、フェーズ 2 IPsec キーの生成で使用する番号のサイズが設定されます。

PFS は、新しいキーはすべて、あらゆる過去のキーと関係しないという暗号化コンセプトです。IPsec ネゴシエーションでは、PFS がイネーブルになるまで、フェーズ 2 キーはフェーズ 1 キーに基づいています。PFS では、キーの生成にデフィーヘルマン方式が採用されています。PFS によって、秘密キーの 1 つが将来解読されても、一連の長期公開キーおよび秘密キーから派生したセッション キーは解読されなくなります。

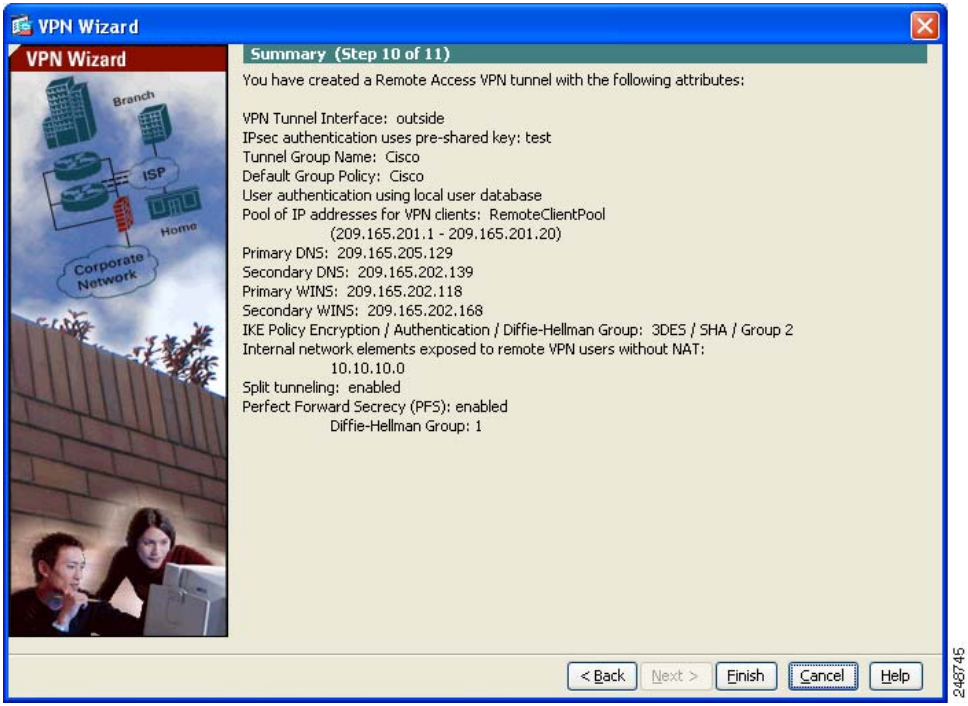
（注）　PFS は、接続の両側でイネーブルにする必要があります。

ステップ 4　デフィーヘルマン グループ ID を選択します。この ID は、2 つの IPsec ピアが、互いに転送することなく共有秘密を導き出すために使用します。デフォルトの Group 2（1024 ビット デフィーヘルマン）は、Group 5（1536 ビット）と比較して、CPU の実行時間は短いですが、安全性は低くなります。Group 7 は、Movian VPN クライアントと共に使用しますが、Group 7（ECC）をサポートするすべてのピアと共に動作します。

ステップ 5　[Next] をクリックして続行します。

リモートアクセス VPN 設定の確認

VPN Wizard の Step 10 で、新しい VPN トンネルの設定アトリビュートを確認します。表示される設定は次のようになります。



適切に設定されている場合は [Finish] をクリックして、適応型セキュリティ アプライアンスに変更内容を適用します。

次にデバイスを起動するときに適用されるように、設定変更をスタートアップ コンフィギュレーションに保存する場合は、[File] メニューから [Save] をクリックします。または、ASDM を終了するときに設定変更を半永久的に保存するように求められます。

設定変更を保存しない場合は、次にデバイスを起動するときに変更前の設定がそのまま適用されます。

次の作業

モバイル従業員またはテレワーカー向けの安全な接続用にエンドツーエンドの暗号化 VPN トンネルを確立するには、Cisco VPN クライアント ソフトウェアを入手します。

Cisco Systems VPN クライアントの詳細については、http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html を参照してください。

リモートアクセス VPN 環境だけに適応型セキュリティ アプライアンスを配置する場合は、これで初期設定が終了しました。さらに、次の手順を実行することもできます。

実行内容	参照先
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』
日常的な運用について	『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series System Log Messages*』

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できます。次の項では、適応型セキュリティ アプライアンスの他の一般的なアプリケーションの設定手順について説明します。

実行内容	参照先
Cisco AnyConnect ソフトウェア クライアントの SSL VPN の設定	第 10 章「シナリオ：Cisco AnyConnect VPN クライアント用接続の設定」
クライアントレス（ブラウザベース）SSL VPN の設定	第 10 章「シナリオ：Cisco AnyConnect VPN クライアント用接続の設定」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN 設定」

次の作業

CHAPTER 10

シナリオ：Cisco AnyConnect VPN クライアント用接続の設定

この章では、リモート ユーザが、Cisco AnyConnect VPN クライアントを使用して SSL 接続を確立できるように適応型セキュリティ アプライアンスを設定する方法について説明します。

この章は、次の項で構成されています。

SSL VPN クライアント接続について

SSL VPN クライアント（AnyConnect）の使用を開始するには、リモート ユーザはブラウザに、適応型セキュリティ アプライアンスの SSL VPN インターフェイスの IP アドレスまたは FQDN を入力します。ブラウザは SSL VPN が有効になっているインターフェイスに接続し、ログイン画面を表示します。

（注） Cisco AnyConnect VPN クライアントを初めてインストールまたはダウンロードする際には、管理者権限が必要となります。

ダウンロードが終わると、クライアントは自動的にインストールおよび設定され、次に、安全な SSL 接続が確立されます。接続が終了すると、クライアント ソフトウェアは、適応型セキュリティ アプライアンスの設定に従って、そのまま残るか自動的にアンインストールされます。

リモート ユーザが過去に SSL VPN 接続を確立したことがあり、クライアント ソフトウェアが自動的にアンインストールされる設定になっていない場合、ユーザ認証時に、適応型セキュリティ アプライアンスによってクライアントのバージョンが確認され、必要に応じてアップグレードされます。

Cisco AnyConnect VPN クライアント ソフトウェアの取得

AnyConnect VPN クライアント ソフトウェアは、適応型セキュリティ アプライアンスによってシスコの Web サイトから取得されます。この章では、設定ウィザードを使用した SSL VPN の設定手順について説明します。Cisco SSL VPN ソフトウェアは、設定プロセス中にダウンロードできます。

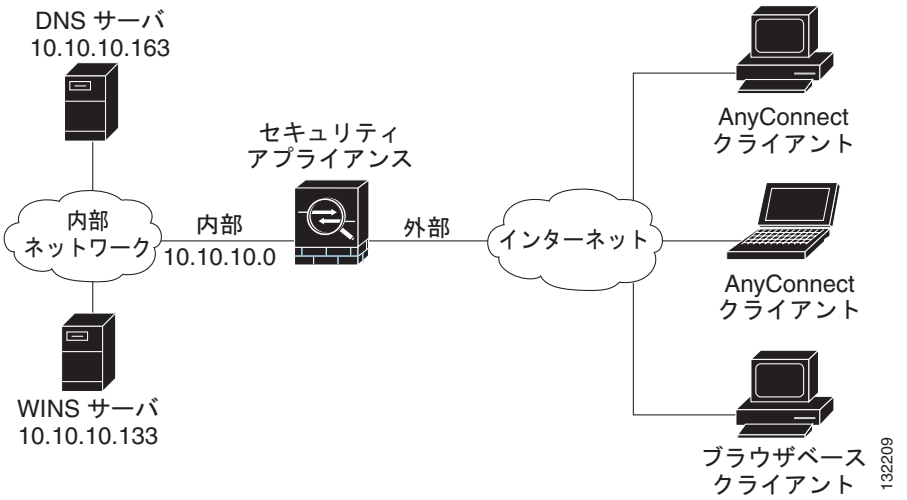
AnyConnect VPN クライアントは、ユーザが適応型セキュリティ アプライアンスからダウンロードするか、システム管理者が手動でリモート PC にインストールできます。手動によるクライアント ソフトウェアのインストールに関する詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

適応型セキュリティ アプライアンスでは、グループ ポリシーまたは接続を確立するユーザのユーザ名アトリビュートに基づいて、クライアント ソフトウェアが適用されます。適応型セキュリティ アプライアンスを、ユーザが接続を確立する度にクライアントが自動的に適用されるように、あるいは、ユーザに対してクライアントをダウンロードするかどうか指定することを求めるように設定できます。後者においては、ユーザが応答しなかった場合に、タイムアウト期間が過ぎた後にクライアントが自動的に適用されるか、あるいは、SSL VPN ログイン画面が表示されるように適応型セキュリティ アプライアンスを設定できます。

AnyConnect SSL VPN クライアントを使用したトポロジの例

図 10-1 に、AnyConnect SSL VPN ソフトウェアが実行されているクライアントの要求を受け付け、そのクライアントからの SSL 接続を確立するように設定された適応型セキュリティ アプライアンスを示します。適応型セキュリティ アプライアンスは、AnyConnect VPN ソフトウェアが実行されているクライアントと、ブラウザベースのクライアントの両方に対応できます。

図 10-1　　SSL VPN シナリオのネットワーク レイアウト



Cisco SSL VPN シナリオの実装

この項では、Cisco AnyConnect SSL VPN 接続を受け入れるように適応型セキュリティ アプライアンスを設定する方法について説明します。設定内容の例で使われる値は、図 10-1 に示す SSL VPN シナリオのものです。

この項は、次の内容で構成されています。

収集する情報

AnyConnect SSL VPN 接続を受け入れるように適応型セキュリティ アプライアンスを設定する手順を開始する前に、次の情報を手元に用意してください。

- リモート ユーザが接続する適応型セキュリティ アプライアンスのインターフェイス名。
- デジタル証明書。

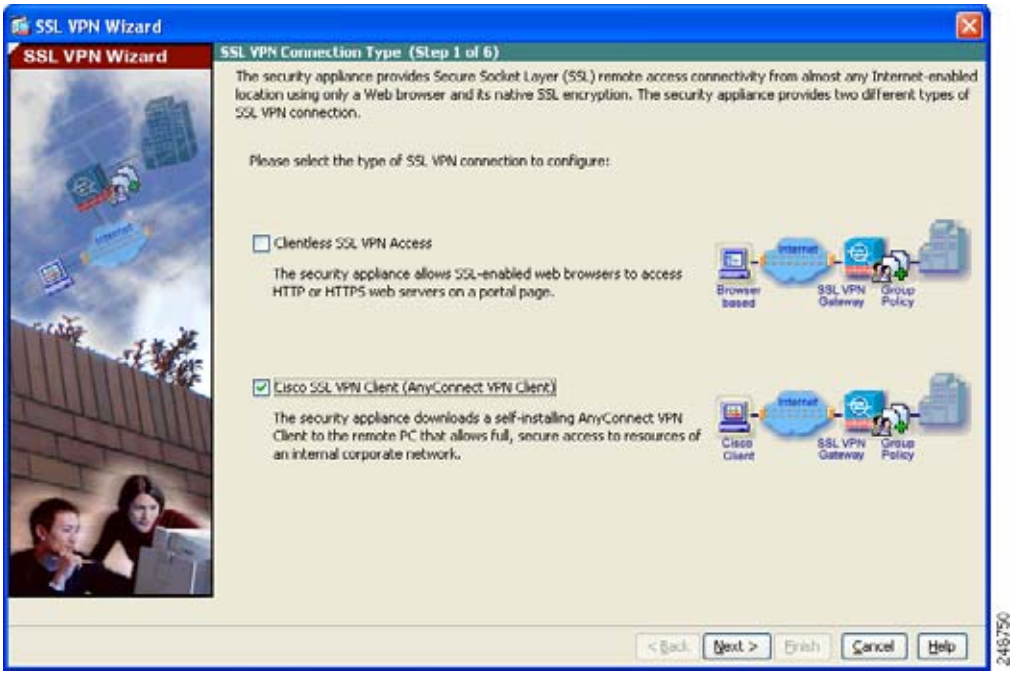
  デフォルトでは、適応型セキュリティ アプライアンスによって自己署名証明書が生成されます。しかし、セキュリティを強化するために、公的に信頼された SSL VPN 証明書を購入してからシステムを実稼動環境に移行することもできます。
- IP プールで使用する IP アドレスの範囲。これらのアドレスは、正常に接続されると、SSL AnyConnect VPN クライアントに割り当てられます。
- ローカル認証データベースを作成するときに使用するユーザのリスト（認証用に AAA サーバを使用している場合を除く）。

- 認証に AAA サーバを使用する場合は、次の情報を手元に用意してください。
  - AAA サーバのグループ名
  - 使用する認証プロトコル（TACACS、SDI、NT、Kerberos、LDAP）
  - AAA サーバの IP アドレス
  - 認証に使用する適応型セキュリティ アプライアンスのインターフェイス
  - AAA サーバで認証を行うための秘密キー

Cisco AnyConnect VPN クライアントの適応型セキュリティ アプライアンスの設定

設定プロセスを始めるには、次の手順に従います。

ステップ 1　ASDM メイン ウィンドウで、[Wizards] ドロップダウン メニューから [SSL VPN Wizard] を選択します。SSL VPN Wizard の Step 1 の画面が表示されます。



ステップ 2　SSL VPN Wizard の Step 1 で、次の手順に従います。

a. [Cisco SSL VPN Client] チェックボックスをオンにします。

b. [Next] をクリックして続行します。

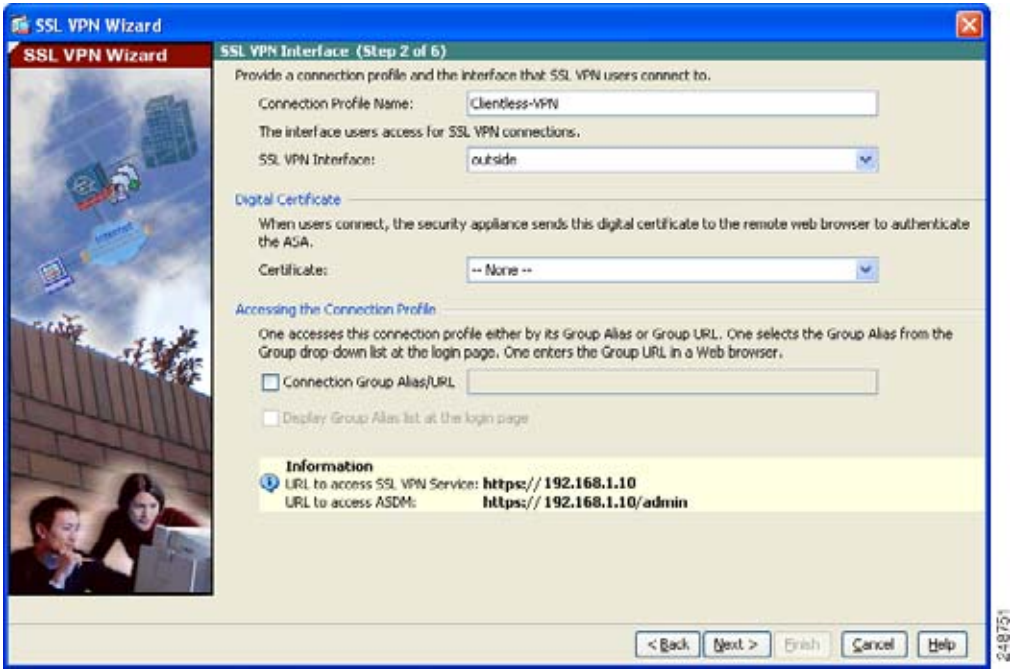
SSL VPN インターフェイスの指定

SSL VPN Wizard の Step 2 で、次の手順に従います。

ステップ 1　リモート ユーザが接続する接続名を指定します。

ステップ 2　[SSL VPN Interface] ドロップダウン リストから、リモート ユーザが接続するインターフェイスを選択します。ユーザがこのインターフェイスへの接続を確立すると、SSL VPN のポータル ページが表示されます。

ステップ 3　[Certificate] ドロップダウン リストから、適応型セキュリティ アプライアンスを認証するために適応型セキュリティ アプライアンスによってリモート ユーザに送信される証明書を選択します。



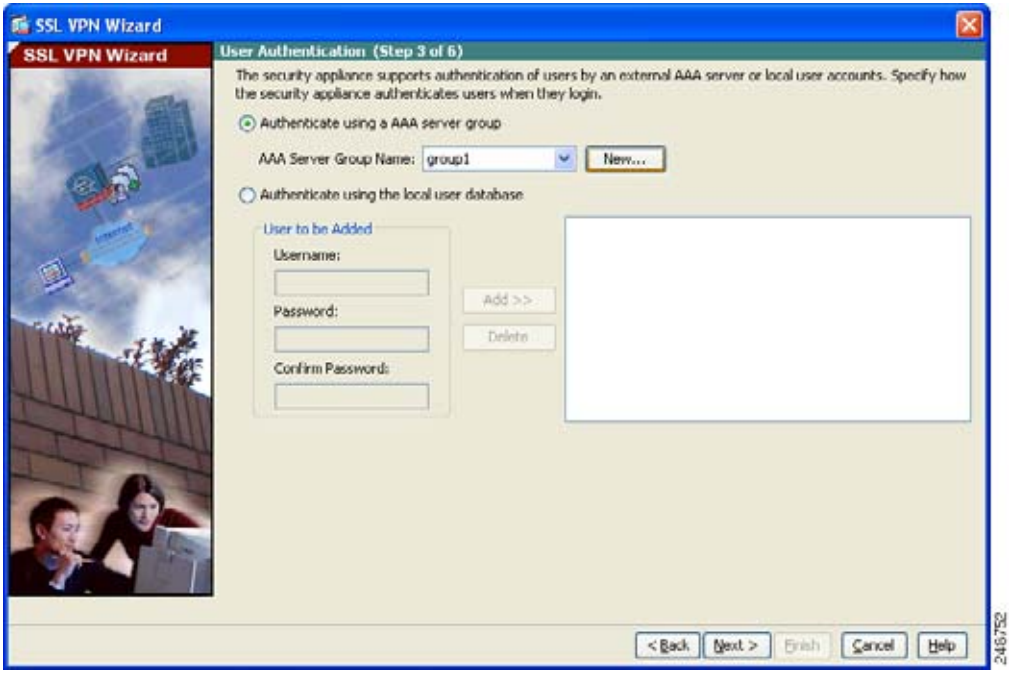
ステップ 4　[Next] をクリックして続行します。

ユーザ認証方式の指定

SSL VPN Wizard の Step 3 で、次の手順に従います。

ステップ 1　認証に AAA サーバまたはサーバ グループを使用する場合、次の手順に従います。

a. [Authenticate using a AAA server group] オプション ボタンをクリックします。



b. AAA サーバ グループ名を指定します。

c. ドロップダウン リストから、既存の AAA サーバ グループ名を選択するか、[New] をクリックして新しいサーバ グループを作成できます。

新しい AAA サーバ グループを作成するには、[New] をクリックします。[New Authentication Server Group] ダイアログボックスが表示されます。

このダイアログボックスで、次の項目を指定します。

- サーバ グループ名
- 使用する認証プロトコル（RADIUS、TACACS、SDI、NT、Kerberos、LDAP）
- AAA サーバの IP アドレス
- 適応型セキュリティ アプライアンス のインターフェイス
- AAA サーバとの通信時に使用する秘密キー

d. [OK] をクリックします。

ステップ 2　ローカル ユーザ データベースを使用してユーザを認証する場合、次の手順で新しいユーザ アカウントを作成できます。ASDM 設定インターフェイスを使用して、後でユーザを追加することもできます。

新しいユーザを追加するには、ユーザ名とパスワードを入力し、[Add] をクリックします。

ステップ 3　新しいユーザの追加が終了したら、[Next] をクリックして続行します。

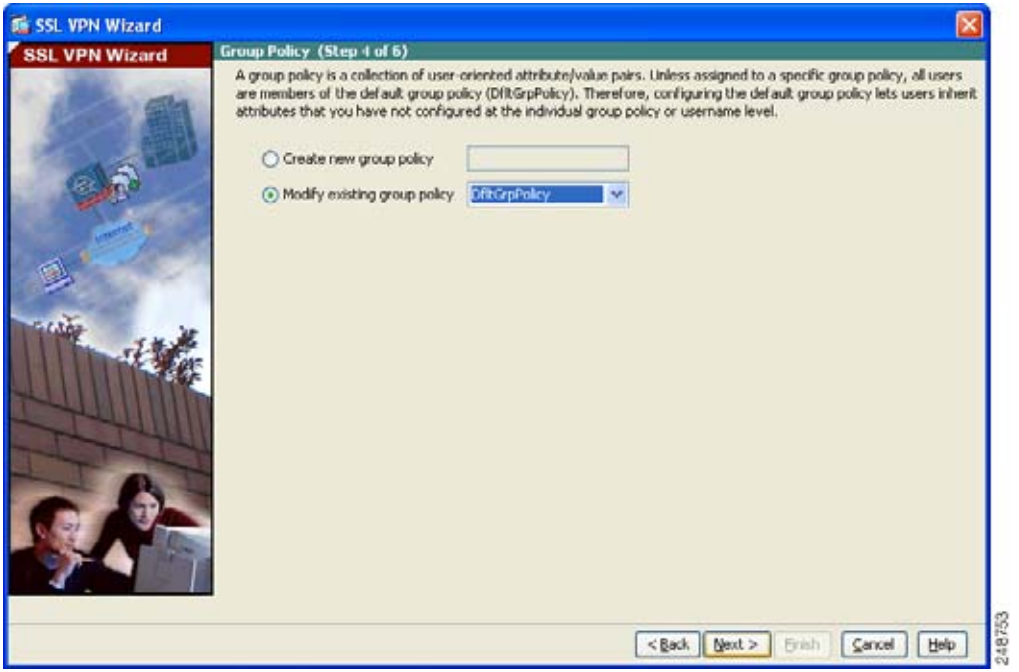
グループ ポリシーの指定

SSL VPN Wizard の Step 4 で、次の手順に従ってグループ ポリシーを指定します。

ステップ 1　[Create new group policy] オプション ボタンをクリックして、グループ名を指定します。

または、

[Modify an existing group policy] オプション ボタンをクリックして、ドロップダウン リストからグループを選択します。



ステップ 2　[Next] をクリックします。

ステップ 3　SSL VPN Wizard の Step 5 が表示されます。このステップは AnyConnect VPN クライアント接続には関係ないので、再度 [Next] をクリックします。

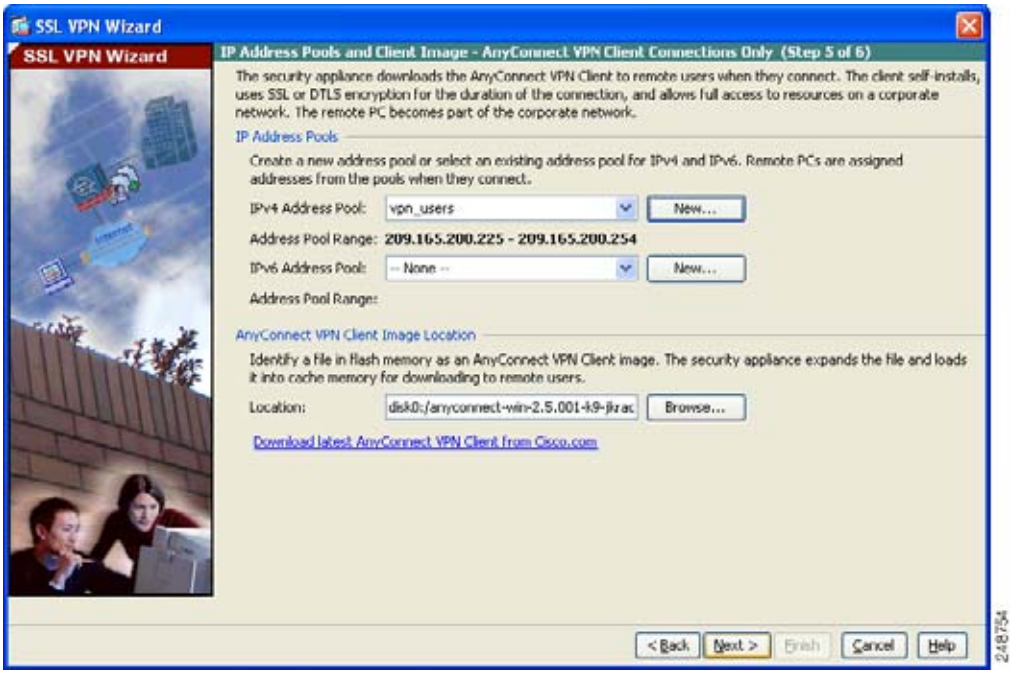
Cisco AnyConnect VPN クライアントの設定

リモート クライアントが Cisco AnyConnect VPN クライアントを使用してネットワークにアクセスできるようにするには、接続に成功した時にリモート VPN クライアントに割り当て可能な IP アドレスのプールを設定する必要があります。このシナリオでは、プールは 209.165.200.225 ～ 209.165.200.254 の範囲の IP アドレスを使用するように設定します。

適応型セキュリティ アプライアンスによってユーザに割り当てられるように、AnyConnect ソフトウェアの場所も指定する必要があります。

SSL VPN Wizard の Step 6 で、次の手順に従います。

ステップ 1　事前に設定されたアドレス プールを使用するには、[IPv4 Address Pool] ドロップダウン リストまたは [IPv6 Address Pool] ドロップダウン リストからプール名を選択します。



ステップ 2　または、[New] をクリックして、新しいアドレス プールを作成します。

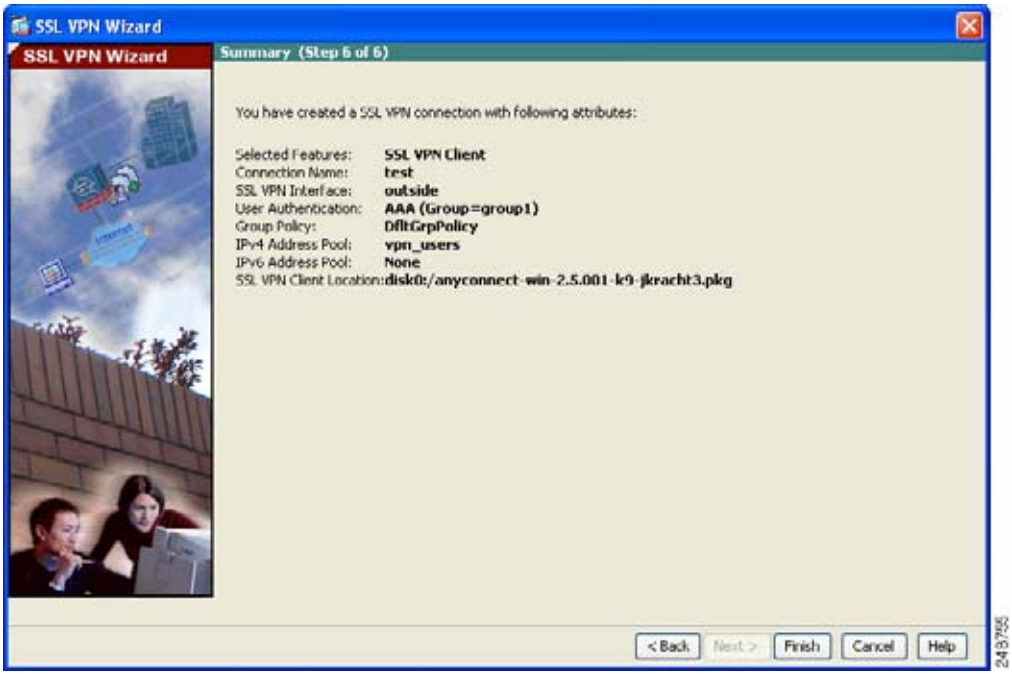
ステップ 3　AnyConnect VPN クライアント ソフトウェア イメージの場所を指定します。

最新バージョンのソフトウェアを取得するには、[Download Latest AnyConnect VPN Client from cisco.com] をクリックします。これにより、クライアント ソフトウェアが PC にダウンロードされます。

ステップ 4　[Next] をクリックして続行します。

リモートアクセス VPN 設定の確認

SSL VPN Wizard の Step 7 で、設定内容が正しいことを確認します。表示される設定は次のようになります。



適切に設定されている場合は [Finish] をクリックして、適応型セキュリティ アプライアンスに変更内容を適用します。

次にデバイスを起動するときに適用されるように、設定変更をスタートアップ コンフィギュレーションに保存する場合は、[File] メニューから [Save] をクリックします。または、ASDM を終了するときに設定変更を半永久的に保存するように求められます。

設定変更を保存しない場合は、次にデバイスを起動するときに変更前の設定がそのまま適用されます。

次の作業

AnyConnect VPN 接続をサポートするためだけに適応型セキュリティ アプライアンスを配置する場合は、これで初期設定が完了しました。さらに、次の手順を実行することもできます。

実行内容	参照先
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』
日常的な運用について	『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series System Log Messages*』

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できます。次の項では、適応型セキュリティ アプライアンスの他の一般的なアプリケーションの設定手順について説明します。

実行内容	参照先
クライアントレス（ブラウザベース）SSL VPN の設定	第 11 章「シナリオ：SSL VPN クライアントレス接続」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN 設定」
リモートアクセス IPSec VPN の設定	第 9 章「シナリオ：IPsec リモートアクセス VPN 設定」

CHAPTER 11

シナリオ：SSL VPN クライアントレス接続

この章では、適応型セキュリティ アプライアンスを使用して、ソフトウェア クライアントを使用しない（クライアントレス）でリモート アクセス SSL VPN 接続を受け入れる方法について説明します。クライアントレス SSL VPN を使用すると、Web ブラウザを使用する、インターネットを介したセキュアな接続、つまりトンネルを作成できます。これにより、ソフトウェア クライアントまたはハードウェア クライアントを使用していないオフサイトのユーザにセキュアなアクセスを提供できます。

この章は、次の項で構成されています。

クライアントレス SSL VPN について

クライアントレス SSL VPN 接続によって、インターネット上のほぼすべてのコンピュータから、さまざまな Web リソースおよび Web 対応アプリケーションに対する、セキュアで簡単なアクセスが可能になります。アクセスできるものには次のものがあります。

- 内部 Web サイト
- Web 対応アプリケーション
- NT/Active Directory および FTP ファイル共有
- POP3S、IMAP4S、および SMTPS などの E メール プロキシ
- MS Outlook Web Access
- MAPI
- アプリケーション アクセス（他の TCP ベースのアプリケーションにアクセスするためのポート フォワーディング）およびスマート トンネル

クライアントレス SSL VPN では、Secure Sockets Layer（SSL）プロトコルとその後継プロトコルである Transport Layer Security（TLSI）を使用することで、リモート ユーザと、中央サイトで設定した特定のサポート対象のリソース間のセキュアな接続を実現しています。適応型セキュリティ アプライアンスが、プロキシする必要がある接続を認識し、HHTP サーバが認証サブシステムと情報をやりとりしてユーザを認証します。

ネットワーク管理者は、グループ単位でクライアントレス SSL VPN のユーザにリソースへのアクセス権限を付与します。

クライアントレス SSL VPN 接続に関するセキュリティ上の考慮事項

適応型セキュリティ アプライアンス上のクライアントレス SSL VPN 接続は、特に SSL 対応サーバと情報をやりとりする方法と、証明書の確認に関して、リモート アクセス IPsec 接続とは異なります。

クライアントレス SSL VPN 接続では、適応型セキュリティ アプライアンスが、エンド ユーザの Web ブラウザとターゲット Web サーバ間のプロキシとなります。ユーザが SSL 対応 Web サーバに接続すると、適応型セキュリティ アプライアンスによってセキュアな接続が確立され、サーバの SSL 証明書が確認されま

す。エンド ユーザのブラウザが提示された証明書を受け取ることはありません。そのため、エンド ユーザのブラウザによってその証明書を検証および確認はできません。

適応型セキュリティ アプライアンス上のクライアントレス SSL VPN の現在の実装では、有効期限が切れた証明書を提示するサイトとの通信は許可されません。また、適応型セキュリティ アプライアンスによって、信頼されている CA 証明書が確認されることもありません。そのためユーザは、SSL 対応 Web サーバと通信する前に同サーバが提示する証明書を分析できません。

SSL 証明書に関するリスクを最小限に抑えるには、次を実行します。

1. クライアントレス SSL VPN アクセスを必要とするすべてのユーザで構成されるグループ ポリシーを設定し、そのグループ ポリシーに関してだけ、そのアクセスをイネーブルにする。
2. ユーザがクライアントレス SSL VPN 接続を使用してアクセスできるリソースを制限するなどして、クライアントレス SSL VPN ユーザのインターネット アクセスに制限を加える。そのために、ユーザのインターネット上の一般的なコンテンツへのアクセスを制限することも可能です。その場合、クライアントレス SSL VPN のユーザにアクセスを許可したい内部ネットワーク上の特定のターゲットへのリンクをすることも可能です。
3. ユーザを教育する。SSL 対応サイトがプライベート ネットワーク内にない場合、ユーザがクライアントレス SSL VPN 接続を介してそのサイトにアクセスすることを禁止する必要があります。ユーザは、別のブラウザ ウィンドウを開いてこのサイトにアクセスし、そのブラウザを使用して提示された証明書を表示する必要があります。

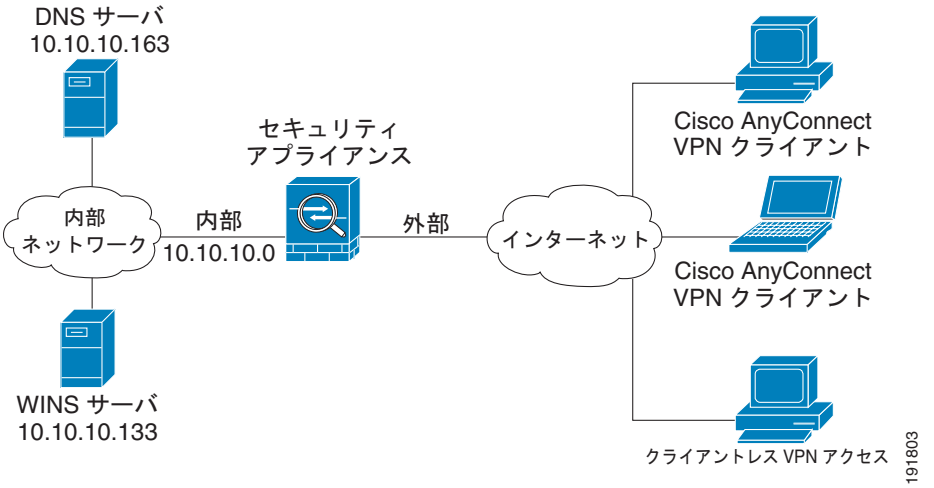
適応型セキュリティ アプライアンスは、クライアントレス SSL VPN 接続の次の機能についてはサポートしていません。

- NAT（IP アドレスがグローバルに一意である必要性を減少させる）
- PAT（複数のアウトバウンド セッションが単一の IP アドレスから発信されているように見せることが可能）

ブラウザベースの SSL VPN アクセスを使用したネットワークの例

図 11-1 に、Web ブラウザを使用してインターネットを介した SSL VPN 接続を受け入れるように設定された適応型セキュリティ アプライアンスを示します。

図 11-1　SSL VPN 接続のネットワーク レイアウト



クライアント SSL VPN シナリオの実装

この項では、Web ブラウザからの SSL VPN 要求を受け入れるように適応型セキュリティ アプライアンスを設定する方法について説明します。設定内容の例で使われる値は、図 11-1 に示すリモートアクセス シナリオのものです。

この項は、次の内容で構成されています。

- 「収集する情報」（P.11-5）
- 「ブラウザベースの SSL VPN 接続のための適応型セキュリティ アプライアンスの設定」（P.11-6）
- 「SSL VPN インターフェイスの指定」（P.11-7）

収集する情報

リモート アクセス IPsec VPN 接続を受け入れるように適応型セキュリティ アプライアンスを設定する手順を開始する前に、次の情報を手元に用意してください。

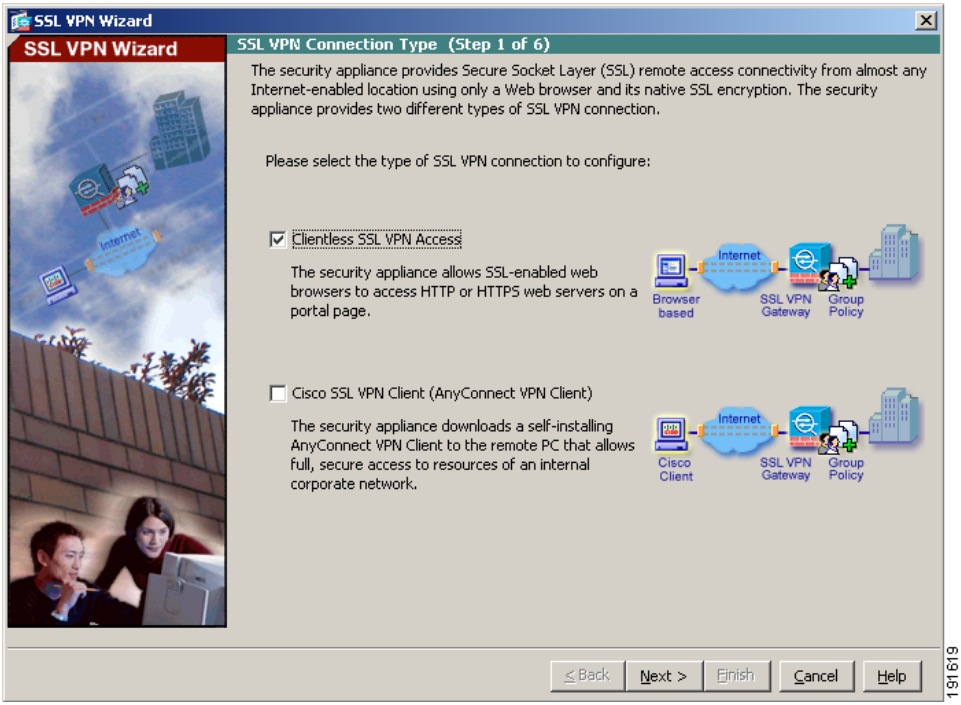
- リモート ユーザが接続する適応型セキュリティ アプライアンスのインターフェイス名。リモート ユーザがこのインターフェイスに接続すると、SSL VPN ポータル ページが表示されます。
- デジタル証明書。

  デフォルトでは、ASA 5500 シリーズによって自己署名証明書が生成されます。セキュリティを強化し、ブラウザの警告メッセージが表示されないようにするために、公的に信頼された SSL VPN 証明書を購入してからシステムを実稼動環境に移行することもできます。
- ローカル認証データベースを作成するときに使用するユーザのリスト（認証用に AAA サーバを使用している場合を除く）。
- AAA サーバ グループ名（認証に AAA サーバを使用する場合）。
- AAA サーバ上のグループ ポリシーに関する次の情報。
  - サーバ グループ名
  - 使用する認証プロトコル（TACACS、SDI、NT、Kerberos、LDAP）
  - AAA サーバの IP アドレス
  - 認証に使用する適応型セキュリティ アプライアンスのインターフェイス
  - AAA サーバで認証を行うための秘密キー
- リモート ユーザが接続を確立した時に SSL VPN ポータル ページに表示させる内部 Web サイトまたはページのリスト。これは、ユーザが最初に接続を確立した時に目にするページなので、リモート ユーザにとって最も頻繁に使用するターゲットが表示されている必要があります。

ブラウザベースの SSL VPN 接続のための適応型セキュリティ アプライアンスの設定

ブラウザベースの SSL VPN の設定プロセスを開始するには、次の手順に従います。

ステップ 1　ASDM メイン ウィンドウで、[Wizards] ドロップダウン メニューから [SSL VPN Wizard] を選択します。SSL VPN 機能の Step 1 の画面が表示されます。



ステップ 2　SSL VPN Wizard の Step 1 で、次の手順に従います。

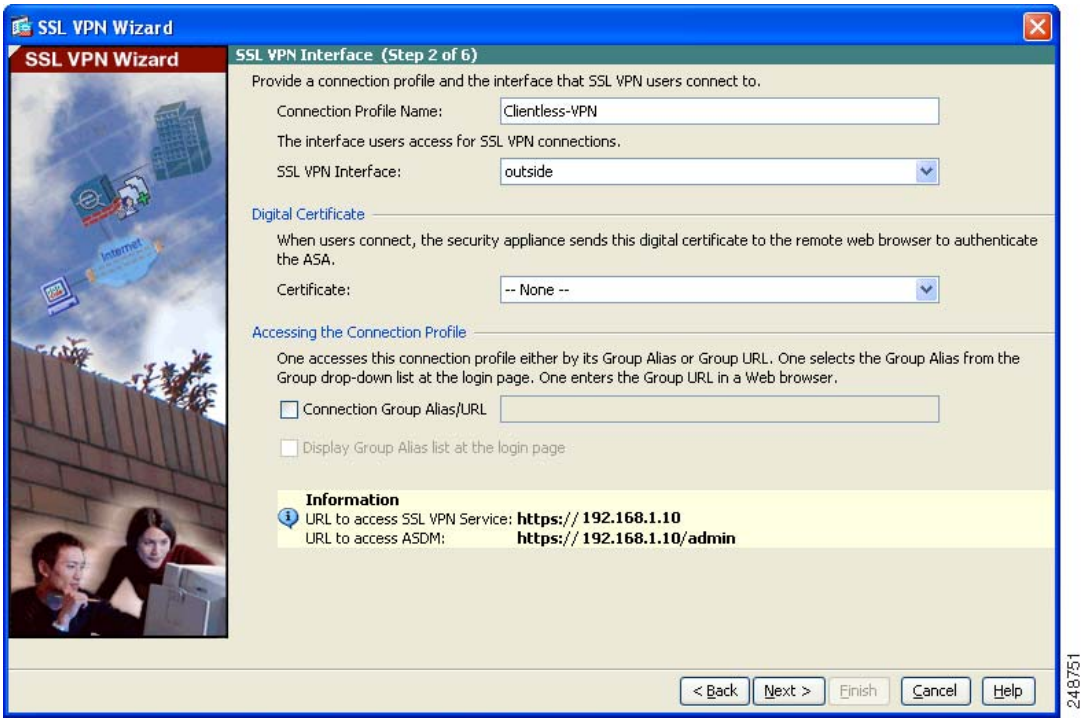
a.　[Browser-based SSL VPN (Web VPN)] チェックボックスをオンにします。

b.　[Next] をクリックして続行します。

SSL VPN インターフェイスの指定

SSL VPN Wizard の Step 2 で、次の手順に従います。

ステップ 1　リモート ユーザが接続する接続名を指定します。



ステップ 2　[SSL VPN Interface] ドロップダウン リストから、リモート ユーザが接続するインターフェイスを選択します。ユーザがこのインターフェイスへの接続を確立すると、SSL VPN のポータル ページが表示されます。

ステップ 3　[Certificate] ドロップダウン リストから、適応型セキュリティ アプライアンスを認証するために適応型セキュリティ アプライアンスによってリモート ユーザに送信される証明書を選択します。

（注）　デフォルトでは、ASA 5500 シリーズによって自己署名証明書が生成されます。セキュリティを強化し、ブラウザの警告メッセージが表示されないようにするために、公的に信頼された SSL VPN 証明書を購入してからシステムを実稼動環境に移行することもできます。

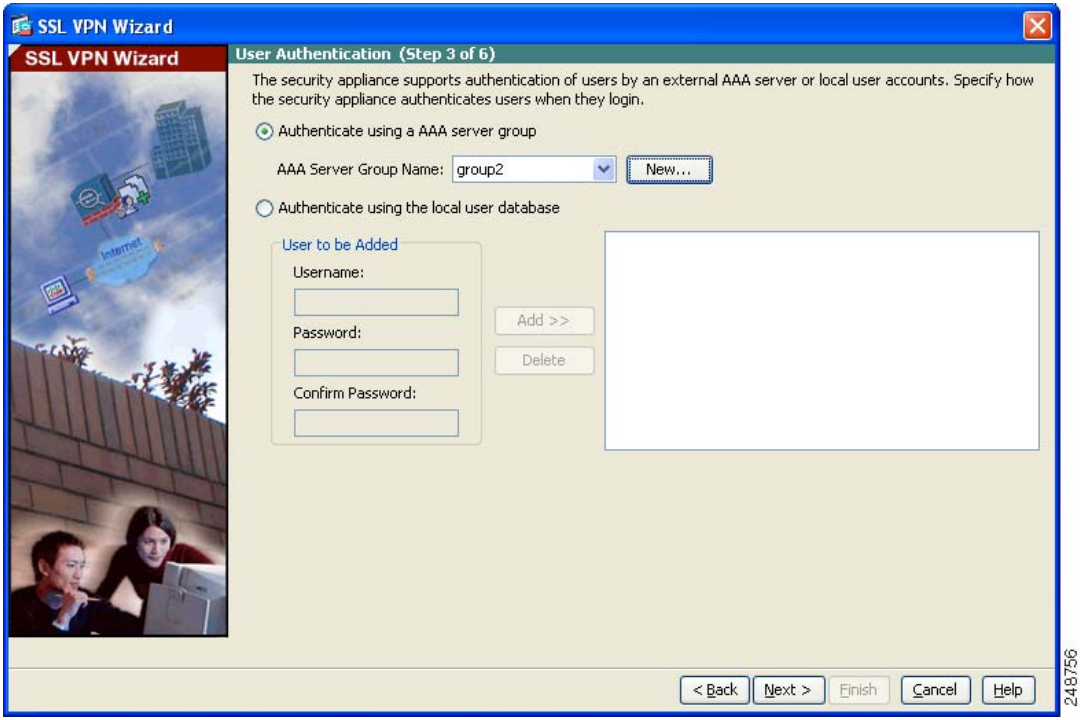
ユーザ認証方式の指定

ユーザの認証は、ローカル認証データベース、または外部の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバを使用して実行できます（AAA サーバには RADIUS、TACACS+、SDI、NT、Kerberos、および LDAP があります）。

SSL VPN Wizard の Step 3 で、次の手順に従います。

ステップ 1　認証に AAA サーバまたはサーバ グループを使用する場合、次の手順に従います。

a.　[Authenticate using a AAA server group] オプション ボタンをクリックします。



b. 事前設定されているサーバ グループを [Authenticate using an AAA Server Group] ドロップダウン リストから選択するか、[New] をクリックして新しい AAA サーバ グループを追加します。

新しい AAA サーバ グループを作成するには、[New] をクリックします。[New Authentication Server Group] ダイアログボックスが表示されます。

このダイアログボックスで、次の項目を指定します。

- サーバ グループ名
- 使用する認証プロトコル（TACACS、SDI、NT、Kerberos、LDAP）
- AAA サーバの IP アドレス
- 適応型セキュリティ アプライアンス のインターフェイス
- AAA サーバとの通信時に使用する秘密キー

[OK] をクリックします。

ステップ 2　ローカル ユーザ データベースを使用してユーザを認証する場合、次の手順で新しいユーザ アカウントを作成できます。ASDM 設定インターフェイスを使用して、後でユーザを追加することもできます。

新しいユーザを追加するには、ユーザ名とパスワードを入力し、[Add] をクリックします。

ステップ 3　新しいユーザの追加が終了したら、[Next] をクリックして続行します。

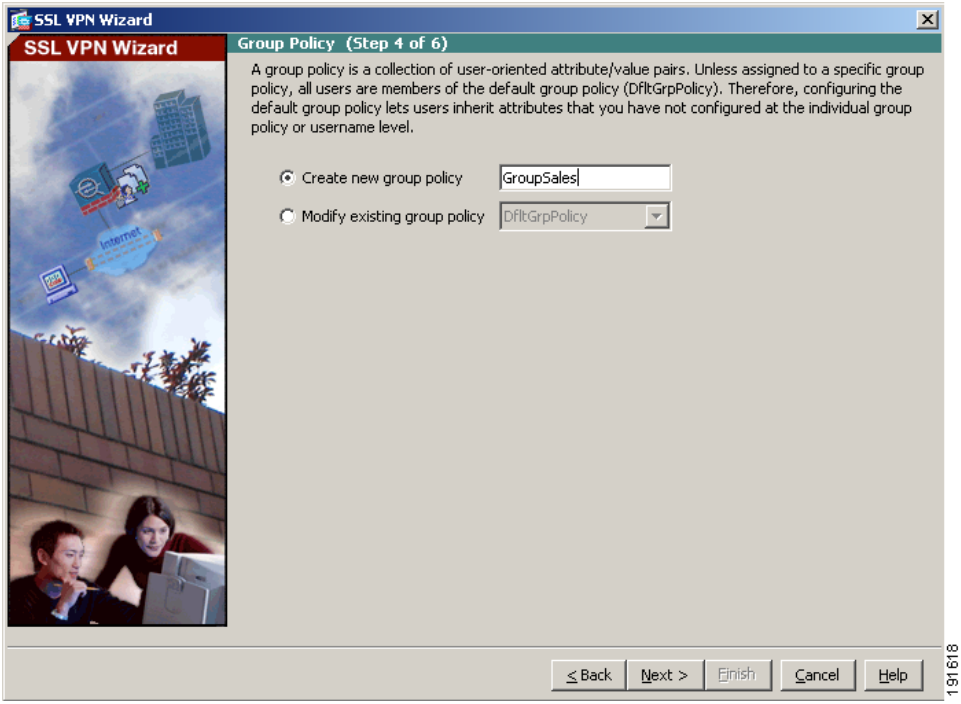
グループ ポリシーの指定

SSL VPN Wizard の Step 4 で、次の手順に従ってグループ ポリシーを指定します。

ステップ 1　[Create new group policy] オプション ボタンをクリックして、グループ名を指定します。

または、

[Modify an existing group policy] オプション ボタンをクリックして、ドロップダウン リストからグループを選択します。



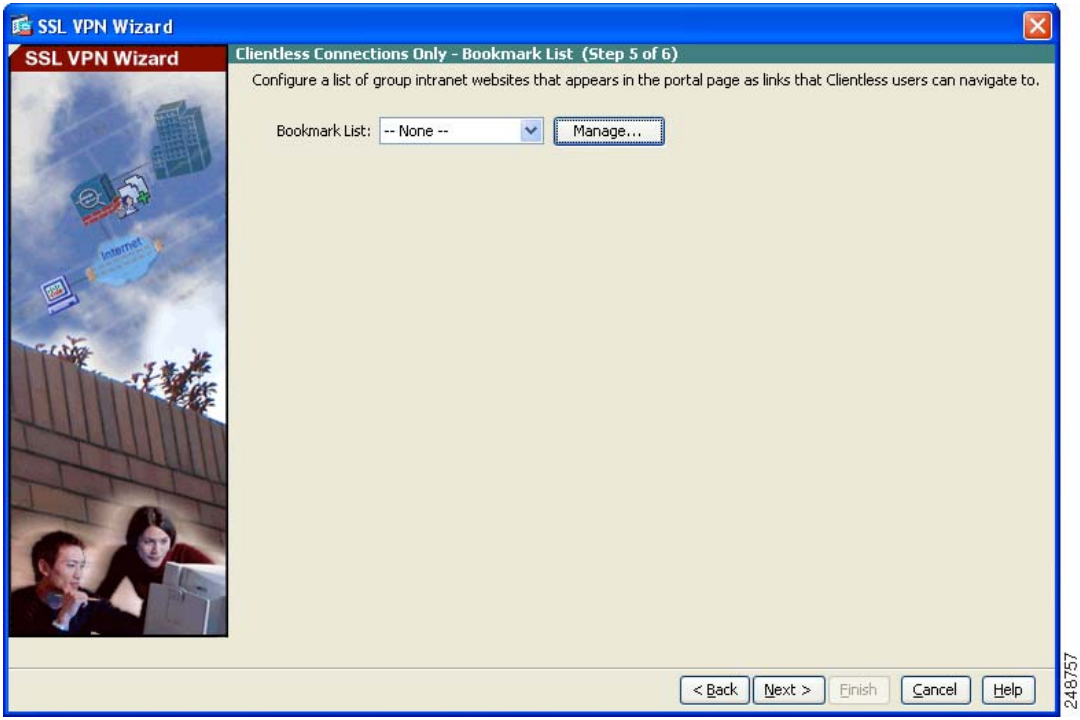
ステップ 2　[Next] をクリックします。

リモート ユーザのブックマーク リストの作成

ユーザが簡単にアクセスできる URL のリストを指定することによって、ポータル ページ、つまりブラウザベースのクライアントが適応型セキュリティ アプライアンスへの VPN 接続を確立した時に表示される特別な Web ページを作成できます。

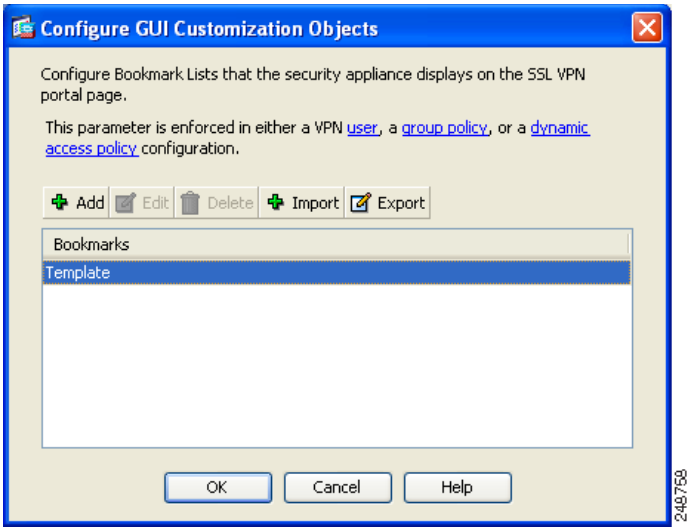
SSL VPN Wizard の Step 5 で、次の手順に従って VPN ポータル ページに表示する URL を指定します。

ステップ 1　既存のブックマーク リストを指定するには、ドラップダウン リストからブックマーク リストの名前を選択します。



新しいリストを追加したり、既存のリストを編集したりするには、[Manage] をクリックします。

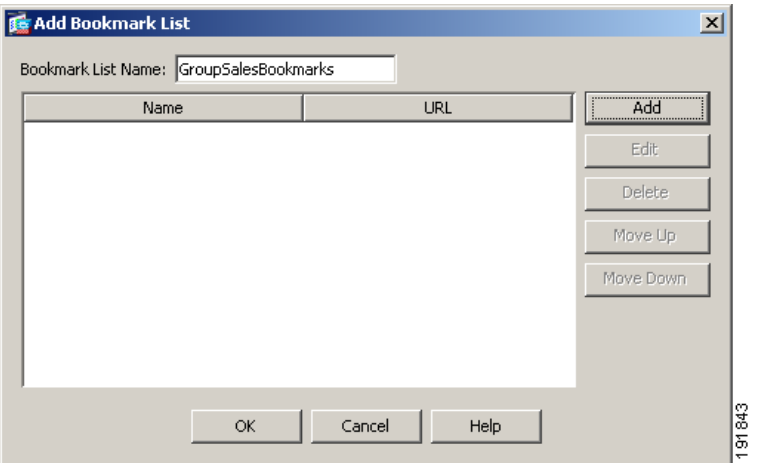
[Configure GUI Customization Objects] ダイアログボックスが表示されます。



ステップ 2　新しいブックマーク リストを作成するには、[Add] をクリックします。

既存のブックマーク リストを編集するには、編集するリストを選択して、[Edit] をクリックします。

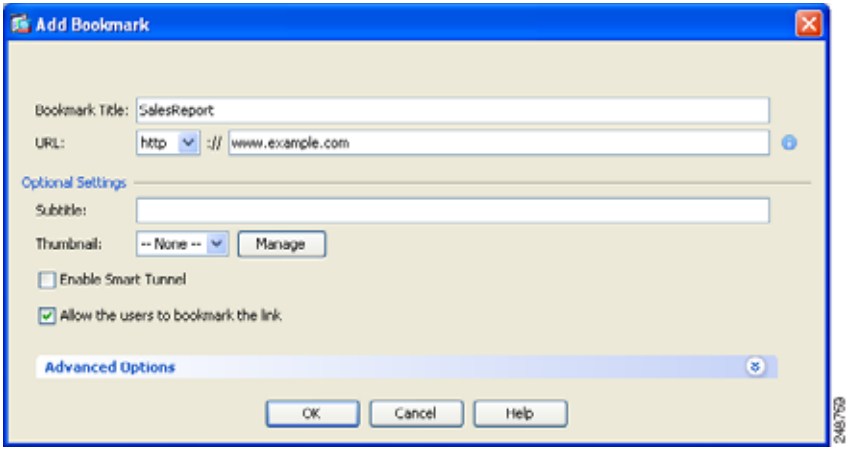
[Add Bookmark List] ダイアログボックスが表示されます。



ステップ 3　[URL List Name] フィールドで、作成するブックマークのリスト名を指定します。このリスト名が VPN ポータル ページのタイトルになります。

ステップ 4　[Add] をクリックして、ブックマーク リストに新しい URL を追加します。

[Add Bookmark Entry] ダイアログボックスが表示されます。



ステップ 5　[Bookmark Title] フィールドで、リストのタイトルを指定します。

ステップ 6　[URL Value] ドロップダウン リストから、指定する URL の種類を指定します。たとえば、http、https、ftp などを選択します。

次に、ページの完全 URL を指定します。

ステップ 7　[OK] をクリックして、[Add Bookmark List] ダイアログボックスに戻ります。

ステップ 8　ブックマーク リストの追加が終了した場合、[OK] をクリックして [Configure GUI Customization Objects] ダイアログボックスに戻ります。

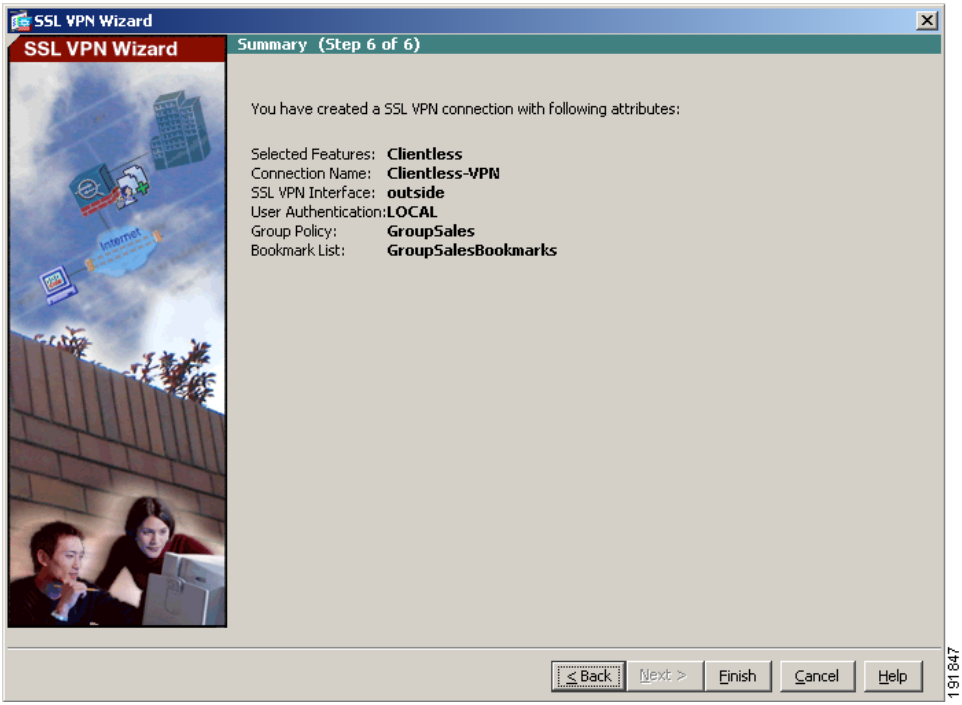
ステップ 9　ブックマーク リストの追加および編集が終了したら、[OK] をクリックして SSL VPN Wizard の Step 5 に戻ります。

ステップ 10　[Bookmark List] ドロップダウン リストから、この VPN グループのブックマーク リストの名前を選択します。

ステップ 11　[Next] をクリックして続行します。

設定内容の確認

SSL VPN Wizard の Step 7 で、設定内容が正しいことを確認します。表示される設定は次のようになります。



適切に設定されている場合は [Finish] をクリックして、適応型セキュリティ アプライアンスに変更内容を適用します。

次にデバイスを起動するときに適用されるように、設定変更をスタートアップ コンフィギュレーションに保存する場合は、[File] メニューから [Save] をクリックします。または、ASDM を終了するときに設定変更を半永久的に保存するように求められます。

設定変更を保存しない場合は、次にデバイスを起動するときに変更前の設定がそのまま適用されます。

次の作業

クライアントレス SSL VPN 環境だけに適応型セキュリティ アプライアンスを配置する場合は、これで初期設定が終了しました。さらに、次の手順を実行することもできます。

実行内容	参照先
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』
日常的な運用について	『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series System Log Messages*』

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できます。次の項では、適応型セキュリティ アプライアンスの他の一般的なアプリケーションの設定手順について説明します。

実行内容	参照先
DMZ 内の Web サーバを保護するための適応型セキュリティ アプライアンスの設定	第 8 章「シナリオ：DMZ 設定」
リモートアクセス VPN の設定	第 9 章「シナリオ：IPsec リモートアクセス VPN 設定」
AnyConnect VPN の設定	第 10 章「シナリオ：Cisco AnyConnect VPN クライアント用接続の設定」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN 設定」

次の作業

CHAPTER 12

シナリオ：サイトツーサイト VPN 設定

この章では、適応型セキュリティ アプライアンスを使用して、サイトツーサイト VPN を作成する方法について説明します。

適応型セキュリティ アプライアンスに備わっているサイトツーサイト VPN 機能を使用すると、企業はネットワーク セキュリティを維持したまま、ネットワークを拡張してビジネス パートナーや世界中のリモート オフィスとの間で低コストのパブリック インターネット接続を実現できます。VPN 接続では、セキュアな接続、つまりトンネル経由で 1 つの場所から別の場所へデータを送信できます。これは、まず接続の両端を認証し、次に 2 つのサイト間で送信されるすべてのデータを自動的に暗号化することによって可能になります。

この章は、次の項で構成されています。

サイトツーサイト VPN ネットワーク トポロジの例

図 12-1 に、2 台の適応型セキュリティ アプライアンス間の VPN トンネルの例を示します。

図 12-1　サイトツーサイト VPN 設定シナリオのネットワーク レイアウト

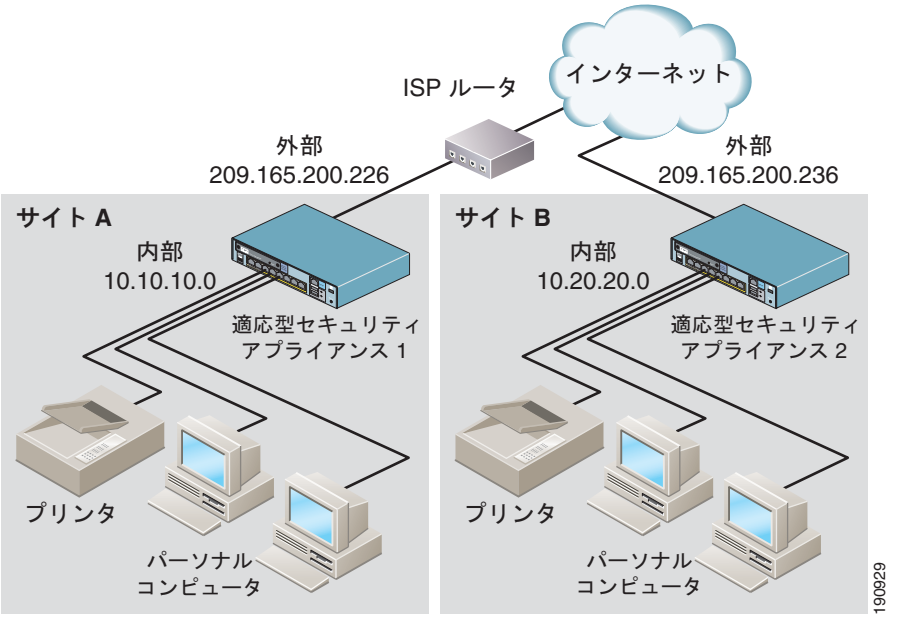


図 12-1 のような VPN サイトツーサイト構成を作成するには、2 台の適応型セキュリティ アプライアンスを設定する必要があります（接続のそれぞれの側に 1 台ずつ）。

サイトツーサイト シナリオの実装

この項では、図 12-1 に表示されているリモートアクセス シナリオのパラメータ例を使用して、サイトツーサイト VPN 構成に適応型セキュリティ アプライアンスを設定する方法について説明します。

この項は、次の内容で構成されています。

収集する情報

この設定手順を開始する前に、次の情報を取得します。

- リモートの適応型セキュリティ アプライアンス ピアの IP アドレス
- リモート サイトのリソースとの通信にトンネルを使用することが許可されたローカル ホストとネットワークの IP アドレス
- ローカル リソースとの通信にトンネルを使用することが許可されたリモート ホストとネットワークの IP アドレス

サイトツーサイト VPN の設定

ここでは、ASDM VPN Wizard を使用してサイトツーサイト VPN 用に適応型セキュリティ アプライアンスを設定する方法について説明します。

この項は、次の内容で構成されています。

次の項では、各設定手順を実行する方法を詳細に説明します。

ローカル サイトでのセキュリティ アプライアンスの設定

（注）　このシナリオでは、最初のサイトの適応型セキュリティ アプライアンスを Security Appliance 1 と呼びます。

Security Appliance 1 を設定するには、次の手順に従います。

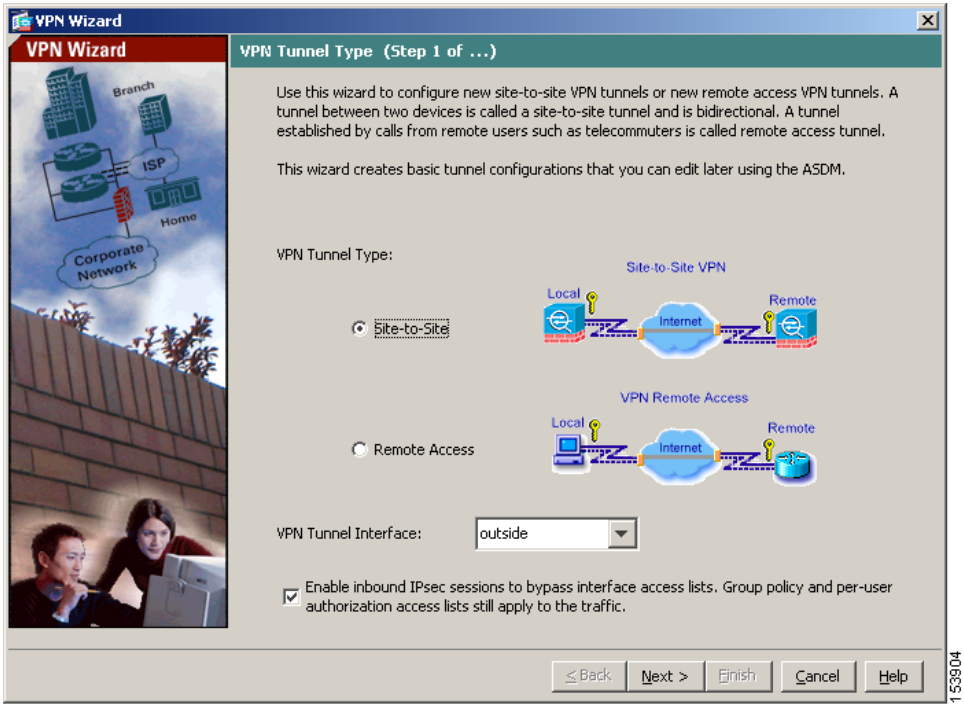
ステップ 1　ASDM メイン ウィンドウで、[Wizards] ドロップダウン メニューから [VPN Wizard] を選択します。ASDM で、最初の VPN Wizard 画面が開きます。

VPN Wizard の Step 1 で、次の手順に従います。

a. [VPN Tunnel Type] 領域で、[Site-to-Site] オプション ボタンをクリックします。

（注）　[Site-to-Site VPN] オプションを選択すると、2 つの IPsec セキュリティ ゲートウェイが接続されますが、これには適応型セキュリティ アプライアンス、VPN コンセントレータ、またはサイトツーサイト IPsec 接続をサポートするその他のデバイスが含まれる可能性があります。

b. [VPN Tunnel Interface] ドロップダウン リストから、現在の VPN トンネルで有効なインターフェイスとして [Outside] を選択します。



c. [Next] をクリックして続行します。

リモート VPN ピアに関する情報の入力

VPN ピアは、設定している接続のもう一方の端にあるシステムで、通常はリモート サイトにあります。

（注） このシナリオでは、リモート VPN ピアを Security Appliance 2 と呼びます。

VPN Wizard の Step 2 で、次の手順に従います。

ステップ 1　ピアの IP アドレス（このシナリオでは、Security Appliance 2 の IP アドレス、209.165.200.236）と、トンネル グループ名（たとえば「Cisco」）を入力します。

ステップ 2　次のいずれかの認証方式を選択して、使用する認証のタイプを指定します。

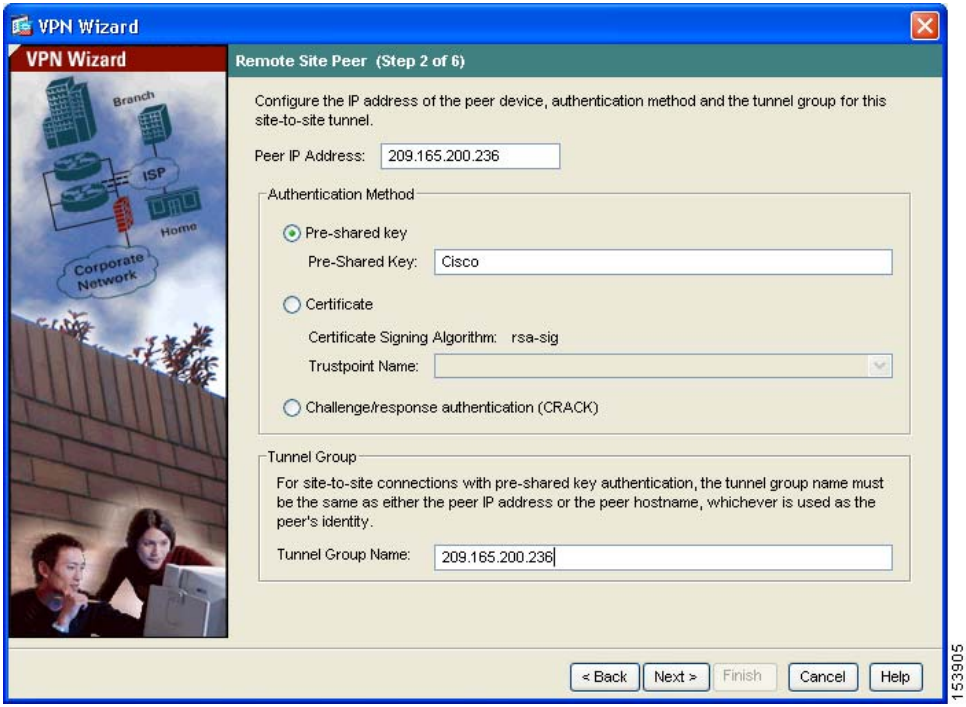
- 認証にスタティック事前共有キーを使用するには、[Pre-Shared Key] オプション ボタンをクリックし、事前共有キー（たとえば、「Cisco」）を入力します。このキーは、適応型セキュリティ アプライアンス間の IPsec ネゴシエーションで使用されます。

  （注） 事前共有キー認証を使用する場合、トンネル グループ名はピアの IP アドレスにする必要があります。

- 認証にデジタル証明書を使用するには、[Certificate] オプション ボタンをクリックし、[Certificate Signing Algorithm] ドロップダウン リストから証明書署名アルゴリズムを選択し、次に、事前設定されているトラストポイント名を [Trustpoint Name] ドロップダウン リストから選択します。

  認証にデジタル証明書を使用する予定で、まだトラストポイント名を設定していない場合は、他の 2 つのオプションのいずれかを使用してウィザードを続行できます。認証設定は、標準 ASDM 画面を使用して後で修正できます。

- [Challenge/Response Authentication] オプション ボタンをクリックして、この認証方式を使用できます。



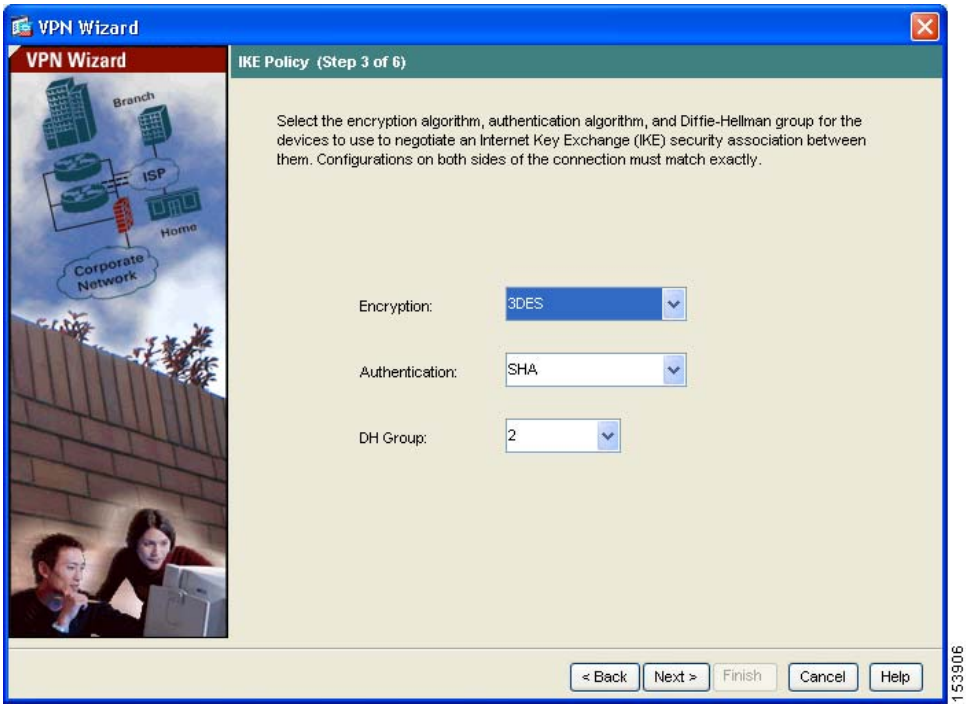
ステップ 3　[Next] をクリックして続行します。

IKE ポリシーの設定

IKE は、データを保護しプライバシーを保証する暗号化方式を含むネゴシエーション プロトコルで、ピアの ID を確認する認証機能も提供されます。ほとんどの場合、ASDM のデフォルト値を使用すれば、十分にセキュアな VPN トンネルを 2 つのピア間に確立できます。

VPN Wizard の Step 3 で、次の手順に従います。

ステップ 1　IKE セキュリティ アソシエーションにおいて適応型セキュリティ アプライアンスが使用する暗号化アルゴリズム（DES、3DES、または AES）、認証アルゴリズム（MD5 または SHA）、および Diffie-Hellman グループ（1、2、または 5）をクリックします。



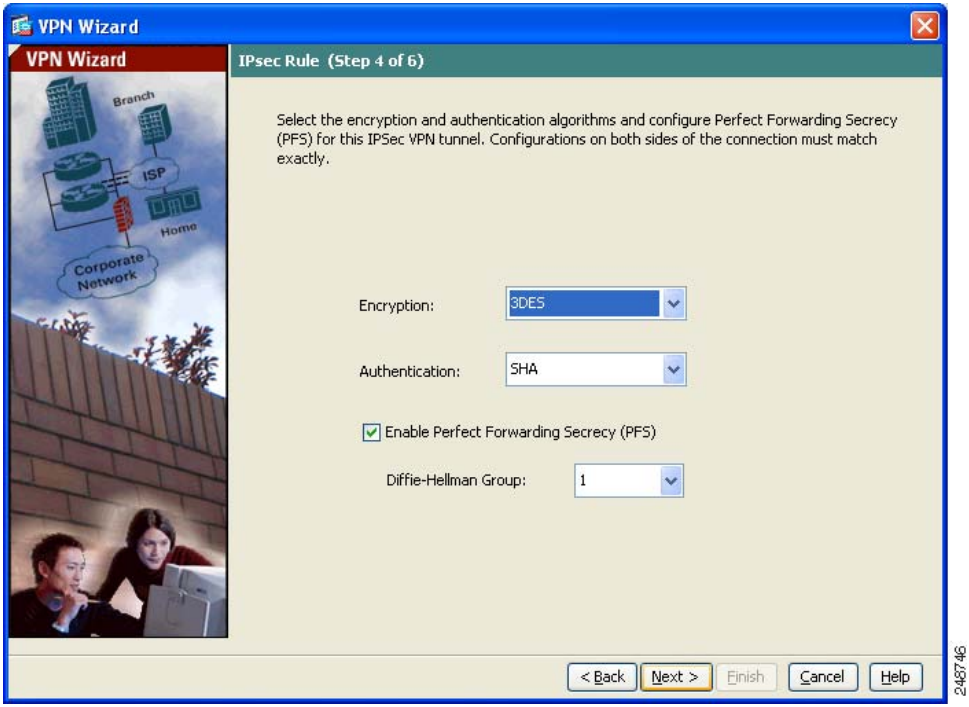
（注）　Security Appliance 2 を設定する場合は、Security Appliance 1 で選択した各オプションと同じ値を正確に入力します。VPN トンネルが失敗し、処理速度を低下させる一般的な原因は、暗号化の不整合です。

ステップ 2　[Next] をクリックして続行します。

IPsec Encryption パラメータおよび Authentication パラメータの設定

VPN Wizard の Step 4 で、次の手順に従います。

ステップ 1　[Encryption] ドロップダウン リストから暗号化アルゴリズム（DES、3DES、または AES）を、[Authentication] ドロップダウン リストから認証アルゴリズム（MD5 または SHA）を選択します。



ステップ 2　[Enable Perfect Forwarding Secrecy (PFS)] チェックボックスをオンにして、フェーズ 2 IPsec キーの生成において、PFS を使用するかどうかを指定し、[Diffie-Hellman Group] ドロップダウン リストから使用する番号のサイズを指定します。

PFS は、新しいキーはすべて、あらゆる過去のキーと関係しないという暗号化コンセプトです。IPsec ネゴシエーションでは、PFS がイネーブルになるまで、フェーズ 2 キーはフェーズ 1 キーに基づいています。PFS では、キーの生成にデフィーヘルマン方式が採用されています。

ステップ 3　[Next] をクリックして続行します。

ホストおよびネットワークの指定

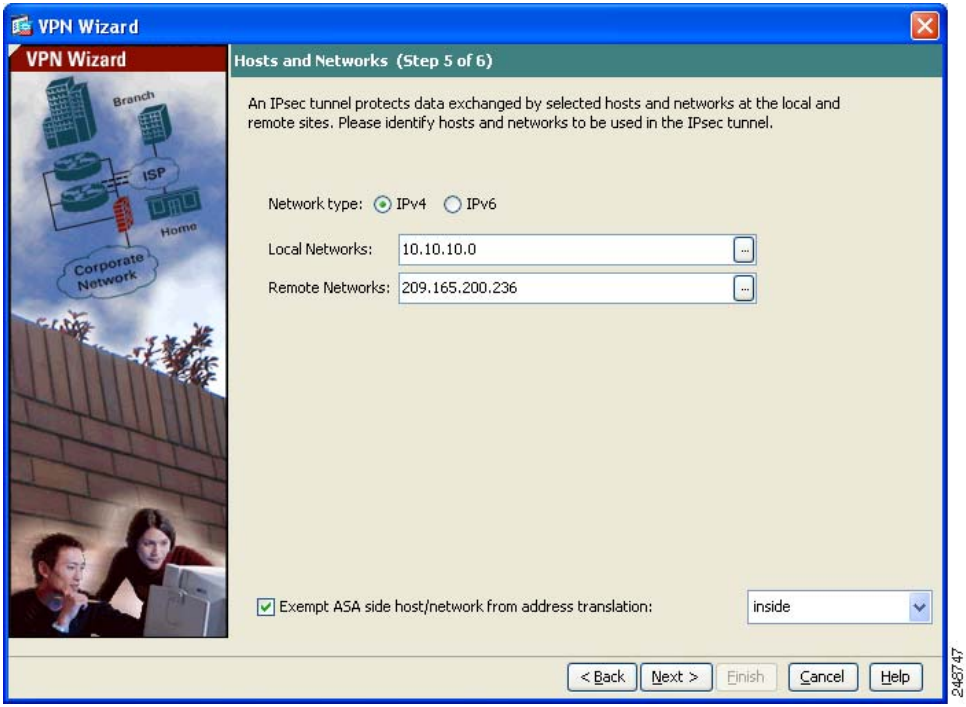
トンネルの反対側のホストおよびネットワークとの通信にこの IPsec トンネルを使用することが許可されたローカル サイトのホストおよびネットワークを指定します。[Add] または [Delete] をクリックして、トンネルへのアクセスが許可されたホストおよびネットワークを指定します。現在のシナリオでは、ネットワーク A（10.10.10.0）からのトラフィックは Security Appliance 1 によって暗号化され、VPN トンネル経由で送信されます。

さらに、ローカル ホストおよびネットワークへのアクセスにこの IPsec トンネルを使用することを許可するリモート サイトのホストおよびネットワークを指定します。ホストおよびネットワークを動的に追加するには [Add]、削除するには [Delete] をクリックします。このシナリオにおいて、Security Appliance 1 では、リモート ネットワークはネットワーク B（10.20.20.0）で、このネットワークからの暗号化されたトラフィックはトンネル経由で許可されます。

VPN Wizard の Step 5 で、次の手順に従います。

ステップ 1　保護する、または保護を解除するローカル ネットワークの IP アドレスを入力するか、省略（...）ボタンをクリックして、ホストとネットワークのリストから選択します。

ステップ 2　保護する、または保護を解除するリモート ネットワークの IP アドレスを入力するか、省略（...）ボタンをクリックして、ホストとネットワークのリストから選択します。

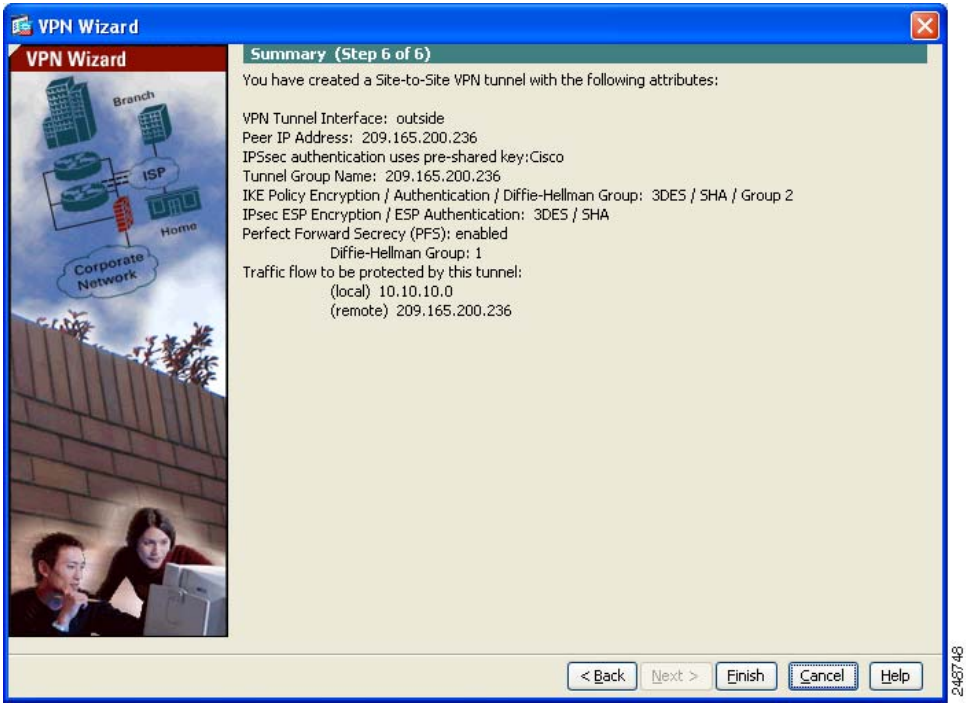


ステップ 3　NAT または PAT を使用していない場合は、[Exempt ASA side host network from address translation] チェックボックスをオンにして、ドロップダウン リストから [Inside] インターフェイスを選択します。

ステップ 4　[Next] をクリックして続行します。

VPN アトリビュートの表示とウィザードの終了

VPN Wizard の Step 6 では、作成した VPN トンネルの設定リストを確認します。



適切に設定されている場合は [Finish] をクリックして、適応型セキュリティ アプライアンスに変更内容を適用します。

次にデバイスを起動するときに適用されるように、設定変更をスタートアップ コンフィギュレーションに保存する場合は、[File] メニューから [Save] をクリックします。

または、ASDM を終了するときに設定変更を半永久的に保存するように求められます。

設定変更を保存しない場合は、次にデバイスを起動するときに変更前の設定がそのまま適用されます。

この操作により、Security Appliance 1 の設定プロセスが終了します。

VPN 接続の反対側の設定

これで、ローカルの適応型セキュリティ アプライアンスの設定は完了しました。次は、リモート サイトで適応型セキュリティ アプライアンスを設定する必要があります。

リモート サイトでは、VPN ピアとしての役割を果たす 2 つ目の適応型セキュリティ アプライアンスを設定します。ローカルの適応型セキュリティ アプライアンスを設定したときと同じ手順を使用します。「ローカル サイトでのセキュリティ アプライアンスの設定」（P.12-4）から開始し、「VPN アトリビュートの表示とウィザードの終了」（P.12-12）で終了します。

（注）　Security Appliance 2 を設定する場合、ローカル ホストおよびネットワークを除いて、Security Appliance 1 で選択した各オプションと同じ値を使用します。VPN 構成が失敗する一般的な原因は、不整合です。

サイトツーサイト VPN の設定の確認またはトラブルシューティングについては、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』の「Troubleshooting the Security Appliance」の項を参照してください。

個々のトラブルシューティング問題については、次のサイトにある「Troubleshooting Technotes」を参照してください。

http://www.cisco.com/en/US/products/ps6120/prod_tech_notes_list.html

ヘルプ トラブルシューティング コンフィギュレーション問題については、次のサイトの「Configuration Examples and TechNotes」を参照してください。

http://www.cisco.com/en/US/products/ps6120/prod_configuration_examples_list.html

特に、「Troubleshooting Technotes」にある、ASA を使用したサイトツーサイト VPN（L2L）に関する TECHNOTE を参照してください。「Troubleshooting Technotes」では、次に示すような、サイトツーサイト VPN 設定のトラブルシューティングを行うためのコマンドについて説明しています。

- **show run isakmp**
- **show run ipsec**
- **show run tunnel-group**
- **show run crypto map**

- **debug crypto ipsec sa**
- **debug crypto isakmp sa**

これらのコマンドの詳細にいては、『*Cisco ASA 5500 Series Command Reference*』を参照してください。

次の作業

サイトツーサイト VPN 環境だけに適応型セキュリティ アプライアンスを配置する場合は、これで初期設定が完了しました。さらに、次の手順を実行することもできます。

実行内容	参照先
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』
日常的な運用について	『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series System Log Messages*』

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できます。次の項では、適応型セキュリティ アプライアンスの他の一般的なアプリケーションの設定手順について説明します。

実行内容	参照先
リモートアクセス VPN の設定	第 9 章「シナリオ：IPsec リモートアクセス VPN 設定」
クライアントレス（ブラウザベース）SSL VPN の設定	第 11 章「シナリオ：SSL VPN クライアントレス接続」
Cisco AnyConnect ソフトウェア クライアントの SSL VPN の設定	第 10 章「シナリオ：Cisco AnyConnect VPN クライアント用接続の設定」

CHAPTER 13

AIP SSM の設定

オプションの AIP SSM は、インライン モードまたは混合モードで追加のセキュリティ検査を提供する高度な IPS ソフトウェアを実行します。適応型セキュリティ アプライアンスは、パケットが出力インターフェイスから送信される直前（または VPN 暗号化が設定されている場合は暗号化が行われる前）、および他のファイアウォール ポリシーが適用された後に、パケットを AIP SSM に転送します。たとえば、アクセス リストによってブロックされたパケットは、AIP SSM に転送されません。

AIP SSM を購入された場合は、この章で示す手順を使用して次の作業を実行します。

- AIP SSM に転送するトラフィックを指定するように適応型セキュリティ アプライアンスを設定する
- AIP SSM へのセッションを確立し、セットアップを実行する

（注） AIP SSM は、Cisco ASA 5500 シリーズ ソフトウェア バージョン 7.0（1）以降でサポートされています。

AIP SSM を ASA 5500 シリーズ適応型セキュリティ アプライアンスに取り付けられます。AIP SSM は、ワームやネットワーク ウイルスなど悪意があるトラフィックをネットワークに影響を与える前に止めるため、予防的な、フル機能を備えた侵入防御システムを提供する高度な IPS ソフトウェアを実行します。この章は、次の項で構成されています。

AIP SSM について

この項は、次の内容で構成されています。

適応型セキュリティ アプライアンスとの AIP SSM の動作

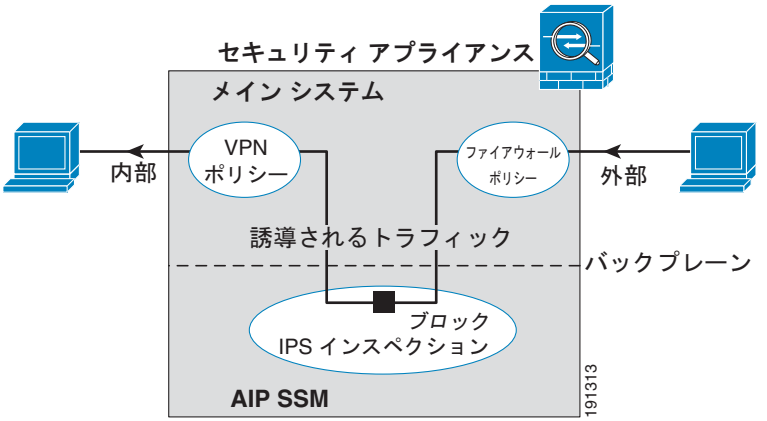
AIP SSM は、適応型セキュリティ アプライアンスから別のアプリケーションを実行します。ただし、そのアプリケーションは適応型セキュリティ アプライアンスのトラフィック フローに統合されます。AIP SSM 自体には、管理インターフェイスを除き、外部インターフェイスは入っていません。IPS 検査のため適応型セキュリティ アプライアンスでトラフィックを指定する場合、トラフィックは適応型セキュリティ アプライアンスと AIP SSM を通して次のように流れます。

1. トラフィックが適応型セキュリティ アプライアンスに入ります。
2. ファイアウォール ポリシーが適用されます。
3. バックプレーンからトラフィックが AIP SSM に送信されます。

   トラフィックのコピーの AIP SSM への送信だけについては、「動作モード」（P.13-3）を参照してください。
4. AIP SSM はそのセキュリティ ポリシーをトラフィックに適用して、適切な処理を行います。
5. 有効なトラフィックはバックプレーンを通って適応型セキュリティ アプライアンスに返信されます。AIP SSM がそのセキュリティ ポリシーに従ってあるトラフィックをブロックする場合、そのトラフィックは渡されません。
6. VPN ポリシーが適用されます（設定されている場合）。
7. トラフィックが適応型セキュリティ アプライアンスから出ます。

図 13-1 は、AIP SSM をインライン モードで動作している場合のトラフィック フローを示します。この例では、AIP SSM は攻撃と見なしたトラフィックを自動的にブロックしています。その他のトラフィックはすべて適応型セキュリティ アプライアンスを経由して転送されています。

図 13-1　適応型セキュリティ アプライアンスの AIP SSM トラフィック フロー: インライン モード

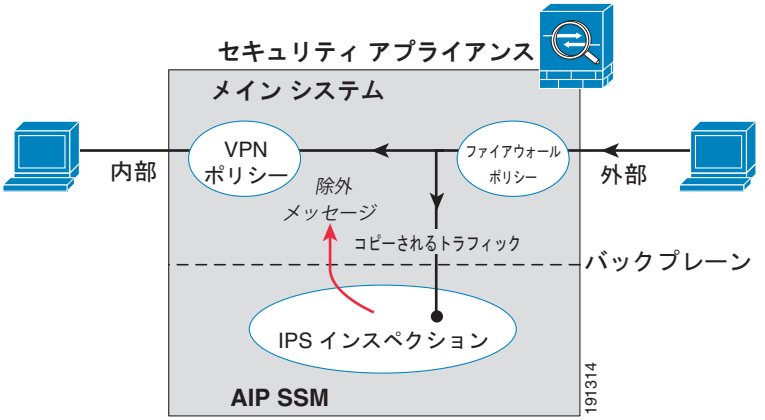


動作モード

次のいずれかのモードを使用して、トラフィックを AIP SSM に送信できます。

- インライン モード：このモードでは、AIP SSM はトラフィック フローに直接配置されます（図 13-1 を参照）。IPS 検査に指定したトラフィックが適応型セキュリティ アプライアンスを経由するには、まず AIP SSM を通り、その検査を受ける必要があります。検査に指定するあらゆるパケットが通過を許可される前に分析されるため、このモードが最も安全です。また、AIP SSM では、パケットごとにブロッキング ポリシーを実装できます。ただし、このモードはスループットに影響を与える可能性があります。
- 混合モード：このモードでは、トラフィックの重複したストリームが AIP SSM に送信されます。このモードは安全性は劣りますが、トラフィックのスループットにはほとんど影響を与えません。インライン モードとは異なり、混合モードでは、AIP SSM は適応型セキュリティ アプライアンスにトラフィックを回避するか、適応型セキュリティ アプライアンスへの接続をリセットするよう指示することでだけ、トラフィックをブロックできます。また、AIP SSM がトラフィックを分析している間、AIP SSM がトラフィックを回避する前に少量のトラフィックが適応型セキュリティ アプライアンスを通過する場合があります。図 13-2 は混合モードの AIP SSM を示しています。この例では、AIP SSM は脅威として指定されたトラフィックに対して適応型セキュリティ アプライアンスに回避メッセージを送信します。

図 13-2　適応型セキュリティ アプライアンスの AIP SSM トラフィック フロー: 混合モード



仮想センサーの使用

IPS ソフトウェア バージョン 6.0 以降を実行している AIP SSM は複数の仮想センサーを実行できます。つまり、AIP SSM で複数のセキュリティ ポリシーを設定できます。1 つまたは複数の仮想センサーに各コンテキストまたはシングル モードの適応型セキュリティ アプライアンスを割り当てたり、複数のセキュリティ コンテキストを同じ仮想センサーに割り当てられます。サポートされている最大センサー数など、仮想センサーの詳細については、IPS マニュアルを参照してください。

図 13-3 は、（インライン モードの）仮想センサー 1 つが 1 つのセキュリティ コンテキストとペアになり、同時に 2 つのセキュリティ コンテキストが同じ仮想センサーを共有しているところを示しています。

図 13-3　セキュリティ コンテキストと仮想センサー

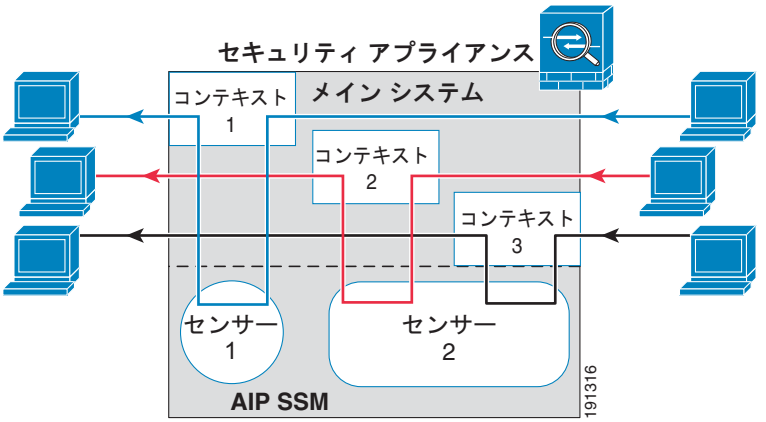
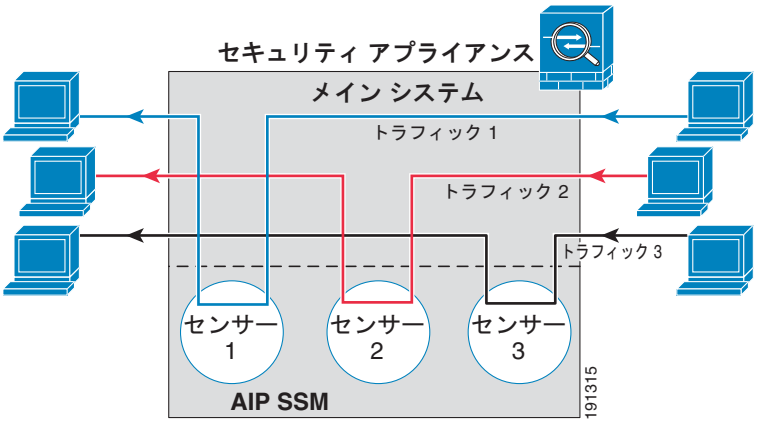


図 13-4 は、（インライン モードの）複数の仮想センサーがシングル モードの適応型セキュリティ アプライアンスとペアになり、定義されたトラフィック フローがそれぞれ異なるセンサーに流れているところを示しています。

図 13-4　シングル モードのセキュリティ アプライアンスと複数の仮想センサー



AIP SSM の設定

この項は、次の内容で構成されています。

AIP SSM 手順の概要

AIP SSM の設定は、AIP SSM を設定してから ASA 5500 シリーズ適応型セキュリティ アプライアンスを設定するプロセスです。

1. 適応型セキュリティ アプライアンスから AIP SSM にセッションを確立します。「AIP SSM へのセッション確立」（P.13-7）を参照してください。
2. AIP SSM で、検査および保護ポリシーを設定します。これにより、トラフィックの検査方法と浸入が検出されたときに行う作業が決まります。マルチ センサー モードで AIP SSM を実行する場合は、各仮想センサーに対して検査および保護ポリシーを設定します。「AIP SSM でのセキュリティ ポリシーの設定」（P.13-8）を参照してください。
3. マルチ コンテキスト モードの ASA 5500 シリーズ適応型セキュリティ アプライアンスで、各コンテキストに使用できる IPS 仮想センサーを指定します（仮想センサーを設定した場合）。「仮想センサーのセキュリティ コンテンツへの割り当て」（P.13-9）を参照してください。
4. ASA 5500 シリーズ適応型セキュリティ アプライアンスで、AIP SSM に転送するトラフィックを指定します。「トラフィックの AIP SSM への転送」（P.13-12）を参照してください。

AIP SSM へのセッション確立

AIP SSM の設定を開始するには、適応型セキュリティ アプライアンスから AIP SSM へセッションを確立します（SSH または Telnet を使用して AIP SSM 管理インターフェイスに直接接続することもできます）。

適応型セキュリティ アプライアンスから AIP SSM にセッションを確立するには、次の手順に従います。

ステップ 1　ASA 5500 シリーズ適応型セキュリティ アプライアンスから AIP SSM にセッションを確立するには、次のコマンドを入力します。

```
hostname# session 1

Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

ステップ 2　ユーザ名とパスワードを入力します。デフォルトのユーザ名とパスワードは「cisco」です。

（注）　AIP SSM に初めてログインしたとき、デフォルトのパスワードを変更するよう求められます。パスワードは、8 文字以上で、意味を持たない言葉である必要があります。

```
login: cisco
Password:
Last login: Fri Sep  2 06:21:20 from xxx.xxx.xxx.xxx
***NOTICE***
This product contains cryptographic features and is subject to United
States
and local country laws governing import, export, transfer and use.
Delivery
of Cisco cryptographic products does not imply third-party authority
to import,
export, distribute or use encryption. Importers, exporters,
distributors and
users are responsible for compliance with U.S. and local country laws.
By using
this product you agree to comply with applicable laws and regulations.
If you
are unable to comply with U.S. and local laws, return this product
immediately.
```

```
A summary of U.S. laws governing Cisco cryptographic products may be
found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email
to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
AIP SSM#
```

（注） （一部のソフトウェア バージョンだけに表示される）前回のライセンス通知が表示された場合、AIP SSM のシグニチャ ファイルのアップグレードが必要になるまでメッセージを無視してかまいません。有効なライセンス キーがインストールされるまで、AIP SSM は現在のシグニチャ レベルで動作します。ライセンス キーは後でインストールできます。ライセンス キーは AIP SSM の現在の機能に影響を与えません。

AIP SSM でのセキュリティ ポリシーの設定

AIP SSM で、トラフィックの検査方法と侵入が検出されたときに行う作業を決定する検査および保護ポリシーを設定するには、次の手順に従います。適応型セキュリティ アプライアンスから AIP SSM へセッションを確立するには、「AIP SSM へのセッション確立」（P.13-7）を参照してください。

AIP SSM でのセキュリティ ポリシーを設定するには、次の手順に従います。

ステップ 1　AIP SSM の初期設定用のセットアップ ユーティリティを実行するには、次のコマンドを入力します。

```
sensor# setup
```

ステップ 2　IPS セキュリティ ポリシーを設定します。IPS バージョン 6.0 以降で仮想センサーを設定する場合、いずれかのセンサーをデフォルトとして指定します。ASA 5500 シリーズ適応型セキュリティ アプライアンスが設定中に仮想センサー名を指定していない場合は、デフォルト センサーが使用されます。

AIP SSM で実行される IPS ソフトウェアは、このマニュアルではそれらの機能について説明していないため、詳細な設定情報については次のマニュアルを参照してください。

- 『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*』
- 『*Command Reference for Cisco Intrusion Prevention System*』

ステップ 3　AIP SSM の設定が完了したら、次のコマンドを入力して IPS ソフトウェアを終了します。

```
sensor# exit
```

適応型セキュリティ アプライアンスから AIP SSM にセッションを確立した場合、適応型セキュリティ アプライアンスプロンプトに戻ります。

仮想センサーのセキュリティ コンテンツへの割り当て

適応型セキュリティ アプライアンスがマルチ コンテキスト モードの場合、1 つまたは複数の IPS 仮想センサーを各コンテキストに割り当てられます。次に、トラフィックを AIP SSM に送信するようコンテキストを設定する場合、コンテキストに割り当てられるセンサーを指定できます。コンテキストに割り当てなかったセンサーは指定できません。センサーをコンテキストに割り当てない場合、AIP SSM で設定されたデフォルト センサーが使用されます。同じセンサーを複数のコンテキストに割り当てることができます。

（注）　仮想センサーを使用するのにマルチ コンテキスト モードである必要はありません。シングル モードでも、異なるトラフィック フローに異なるセンサーを使用できます。

1 つまたは複数のセンサーをセキュリティ コンテキストに割り当てるには、次の手順に従います。

ステップ 1　コンテキスト設定モードに入るには、システム実行スペースで次のコマンドを入力します。

```
hostname(config)# context name
hostname(config-ctx)#
```

ステップ 2　仮想センサーをコンテキストに割り当てるには、次のコマンドを入力します。

```
hostname(config-ctx)# allocate-ips sensor_name [mapped_name] [default]
```

コンテキストに割り当てるセンサーごとにこのコマンドを入力します。

sensor _name 引数は AIP SSM で設定されたセンサー名です。AIP SSM で設定されたセンサーを表示するには、**allocate-ips ?** コマンドを入力します。利用可能なすべてのセンサーがリストされます。**show ips** コマンドを入力することもできます。**show ips** コマンドは、システム実行スペースにすべての利用可能なセンサーをリストします。コンテキストでそのコマンドを入力すると、コンテキストにすでに割り当てられたセンサーが表示されます。まだ AIP SSM にないセンサー名を指定すると、エラーになりますが、**allocate-ips** コマンドはそのまま入力されます。AIP SSM にその名前のセンサーを作成するまで、コンテキストによりセンサーがダウンしていると見なされます。

コンテキスト内で使用できるセンサー名のエイリアスとして、実際のセンサー名ではなく *mapped_name* 引数を使用します。マップ名を指定しない場合、センサー名がコンテキスト内で使用されます。セキュリティを考慮すると、どのセンサーがコンテキストで使用されているかをコンテキスト アドミニストレータに知られたくない場合があります。または、コンテキスト設定の一般名を使用する場合があります。たとえば、すべてのコンテキストで「sensor1」と「sensor2」というセンサーを使用したい場合、コンテキスト A で「highsec」センサーと「lowsec」センサーを sensor1 と sensor2 にマップし、コンテキスト B では「medsec」センサーと「lowsec」センサーを sensor1 と sensor2 にマップできます。

default キーワードを指定すると、コンテキストごとに 1 つのセンサーがデフォルト センサーとして設定されます。コンテキスト設定でセンサー名が指定されていない場合、コンテキストではこのデフォルト センサーが使用されます。コンテキスト 1 つにつき、1 つのデフォルト センサーしか設定できません。デフォルト センサーを変更する場合、**no allocate-ips** *sensor_name* コマンドを入力して、現在のデフォルト センサーを削除してから、新しいデフォルト センサーを割り当てます。センサーをデフォルトとして指定していないためコンテキスト設定にセンサー名が含まれていない場合、トラフィックは AIP SSM でデフォルト センサーを使用します。

ステップ 3　コンテキストごとにステップ 1 とステップ 2 を繰り返します。

ステップ 4　コンテキスト IPS ポリシーを設定するには、次のコマンドを使用してコンテキスト実行スペースに移ります。

```
hostname(config-ctx)# changeto context context_name
```

ここで *context_name* 引数は、設定するコンテキストの名前です。「トラフィックの AIP SSM への転送」（P.13-12）に記載されているように、各コンテキストに移り、IPS セキュリティ ポリシーを設定します。

次の例では、sensor1 と sensor2 がコンテキスト A に、sensor1 と sensor3 がコンテキスト B に割り当てられています。どちらのコンテキストもセンサー名を「ips1」と「ips2」にマップしています。コンテキスト A では、sensor1 はデフォルト センサーとして設定されていますが、コンテキスト B では AIP SSM で設定されているデフォルトが使用されるよう、デフォルトは設定されていません。

```
hostname(config-ctx)# context A
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface
gigabitethernet0/0.110-gigabitethernet0/0.115 int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1 default
hostname(config-ctx)# allocate-ips sensor2 ips2
hostname(config-ctx)# config-url
ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface
gigabitethernet0/1.230-gigabitethernet0/1.235 int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1
hostname(config-ctx)# allocate-ips sensor3 ips2
hostname(config-ctx)# config-url
ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver

hostname(config-ctx)# changeto context A
...
```

トラフィックの AIP SSM への転送

適応型セキュリティ アプライアンスから AIP SSM へトラフィックを転送するよう指定するには、次の手順に従います。マルチ コンテキスト モードで、各コンテキスト実行スペースでこれらの手順を行います。

ステップ 1　AIP SSM で検査するトラフィックを指定するには、**class-map** コマンドを使用して 1 つまたは複数のクラス マップを追加します。

たとえば、次のコマンドを使用してすべてのトラフィックを一致させることができます。

```
hostname(config)# class-map IPS
hostname(config-cmap)# match any
```

特定のトラフィックを一致させるため、アクセス リストを一致させることができます。

```
hostname(config)# access list IPS extended permit ip any 10.1.1.1
255.255.255.255
hostname(config)# class-map IPS
hostname(config-cmap)# match access-list IPS
```

ステップ 2　AIP SSM にトラフィックを転送するよう処理を設定するポリシー マップを追加したり、編集するには、次のコマンドを入力します。

```
hostname(config)# policy-map name
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

ここで *class_map_name* はステップ 1 からのクラス マップです。

次の例を参考にしてください。

```
hostname(config)# policy-map IPS
hostname(config-pmap)# class IPS
```

ステップ 3　AIP SSM にトラフィックを転送するには、次のコマンドを入力します。

```
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close |
fail-open} [sensor {sensor_name | mapped_name}]
```

ここで **inline** キーワードと **promiscuous** キーワードは AIP SSM の動作モードを制御します。詳細については、「動作モード」（P.13-3）を参照してください。

fail-close キーワードを指定すると、AIP SSM が使用できない場合、適応型セキュリティ アプライアンスはすべてのトラフィックをブロックするように設定されます。

fail-open キーワードを指定すると、AIP SSM が使用できない場合、適応型セキュリティ アプライアンスはすべてのトラフィックの通過を検査なしで許可するように設定されます。

AIP SSM で仮想センサーを使用する場合、**sensor** *sensor_name* 引数を使用してセンサー名を指定できます。利用可能なセンサー名を表示するには、**ips ... sensor ?** コマンドを入力します。利用可能なセンサーがリストされます。**show ips** コマンドを使用することもできます。適応型セキュリティ アプライアンスでマルチ コンテキスト モードを使用する場合、コンテキストに割り当てたセンサーだけ指定できます（「仮想センサーのセキュリティ コンテンツへの割り当て」（P.13-9）を参照）。コンテキストで設定されている場合は、*mapped_name* を使用します。センサー名を指定しない場合、トラフィックはデフォルト センサーを使用します。マルチ コンテキスト モードでは、コンテキストのデフォルト センサーを指定できます。シングル モード、またはマルチ モードでデフォルト センサーを指定しない場合、トラフィックは AIP SSM で設定されているデフォルト センサーを使用します。まだ AIP SSM にない名前を入力するとエラーになり、コマンドは拒否されます。

ステップ 4　（オプション）別のクラスのトラフィックを AIP SSM に転送し、IPS ポリシーを設定するには、次のコマンドを入力します。

```
hostname(config-pmap-c)# class class_map_name2
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close |
fail-open} [sensor sensor_name]
```

ここで *class_map_name2* 引数は、IPS 検査を実行する別のクラス マップの名前です。コマンド オプションの詳細については、ステップ 3 を参照してください。

トラフィックは、同じ処理タイプについて複数のクラス マップを一致させることはできません。したがって、ネットワーク A を sensorA に送信し、他のすべてのトラフィックを sensorB に送信する場合は、ネットワーク A に **class** コマンドを入力してから、すべてのトラフィックに **class** コマンドを入力する必要があります。そうしないと、（ネットワーク A を含む）すべてのトラフィックが最初の **class** コマンドと一致し、sensorB に送信されます。

ステップ 5　1 つまたは複数のインターフェイスでポリシー マップを有効にするには、次のコマンドを入力します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global |
interface interface_ID]
hostname
```

ここで *policy_map_name* はステップ 2 で設定されたポリシー マップです。このポリシー マップをすべてのインターフェイスのトラフィックに適用するには、**global** キーワードを使用します。ポリシー マップを特定のインターフェイスのトラフィックに適用するには、**interface** *interface_ID* オプションを使用します。ここで *interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

使用できるグローバル ポリシーは、1 つに限られます。インターフェイスのグローバル ポリシーを無効にするには、そのインターフェイスにサービス ポリシーを適用します。各インターフェイスに適用できるポリシー マップは、1 つだけです。

次の例では、すべての IP トラフィックは AIP SSM に混合モードで転送され、何らかの原因で AIP SSM カードに障害が発生した場合、IP トラフィックはすべてブロックされます。

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

次の例では、10.1.1.0 ネットワークと 10.2.1.0 ネットワークに宛てられたすべての IP トラフィックはインライン モードで AIP SSM に転送され、何らかの原因で AIP SSM カードに障害が発生した場合、すべてのトラフィックが通過できます。my-ips-class トラフィックの場合 sensor1 が使用され、my-ips-class2 トラフィックの場合 sensor2 が使用されます。

```
hostname(config)# access-list my-ips-acl permit ip any 10.1.1.0
255.255.255.0
hostname(config)# access-list my-ips-acl2 permit ip any 10.2.1.0
255.255.255.0
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list my-ips-acl
hostname(config)# class-map my-ips-class2
```

```
hostname(config-cmap)# match access-list my-ips-acl2
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips inline fail-open sensor sensor1
hostname(config-pmap)# class my-ips-class2
hostname(config-pmap-c)# ips inline fail-open sensor sensor2
hostname(config-pmap-c)# service-policy my-ips-policy interface
outside
```

次の作業

これで、適応型セキュリティ アプライアンスに侵入防御を設定する準備ができました。次のマニュアルを使用して、各実装内容に応じた適応型セキュリティ アプライアンスの設定を続けます。

実行内容	参照先
IPS センサーの設定	『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*』
より効率的なサービス ポリシーを作成することによる AIP SSM と CSC SSM のパフォーマンスの最適化	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』

IPS センサーと AIP SSM ソフトウェアを設定したら、次の追加の手順を実行することもできます。

実行内容	参照先
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』
日常的な運用について	『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series System Log Messages*』
ハードウェア メンテナンスおよびトラブルシューティング情報の確認	『*Cisco ASA 5500 Series Hardware Installation Guide*』

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できます。次の項では、適応型セキュリティ アプライアンスの他の一般的なアプリケーションの設定手順について説明します。

実行内容	参照先
DMZ Web サーバの保護設定	第 8 章「シナリオ：DMZ 設定」
リモートアクセス VPN の設定	第 9 章「シナリオ：IPsec リモートアクセス VPN 設定」
ソフトウェア クライアントのリモートアクセス SSL 接続設定	第 10 章「シナリオ：Cisco AnyConnect VPN クライアント用接続の設定」
ブラウザベースのリモートアクセス SSL 接続設定	第 11 章「シナリオ：SSL VPN クライアントレス接続」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN 設定」

CHAPTER 14

CSC SSM の設定

ASA 5500 シリーズ 適応型セキュリティ アプライアンスは、Content Security および Control ソフトウェアを実行する CSC SSM をサポートしています。CSC SSM は、適応型セキュリティ アプライアンスが CSC SSM に転送する FTP、HTTP、POP3、および SMTP の各トラフィックをスキャンすることで、ウイルス、スパイウェア、スパム、およびその他の迷惑なトラフィックに対して保護します。

（注） CSC SSM には Cisco ASA 5500 シリーズ ソフトウェア バージョン 7.1（1）以降が必要です。

この章は、次の項で構成されています。

CSC SSM について

CSC SSM は、Trend Micro 社のアップデート サーバから定期的に更新される、疑わしいコンテンツのシグニチャ プロファイルが入ったファイルを維持します。CSC SSM は適応型セキュリティ アプライアンスから受信されるトラフィックをスキャンし、それを Trend Micro 社から受け取るコンテンツ プロファイルと比較します。次に、正規のコンテンツを適応型セキュリティ アプライアンスに転送してルーティングしたり、疑わしいコンテンツをブロックして報告します。

Trend Micro 社からコンテンツ プロファイルを受け取るだけでなく、システム アドミニストレータが、CSC SSM が追加のトラフィック タイプや場所をスキャンするよう、設定をカスタマイズすることもできます。たとえば、システム アドミニストレータは特定の URL をブロックまたはフィルタしたり、FTP および E メール パラメータをスキャンするよう CSC SSM を設定できます。

CSC SSM のシステム セットアップや監視には ASDM を使用します。CSC SSM ソフトウェアでコンテンツ セキュリティ ポリシーの高度な設定をするには、ASDM 内でリンクをクリックして、CSC SSM の Web ベースの GUI にアクセスします。

この章では、適応型セキュリティ アプライアンスを設定して構成する方法について説明します。CSC SSM GUI の使用方法については、『*Cisco Content Security and Control SSM Administrator Guide*』に記載されています。

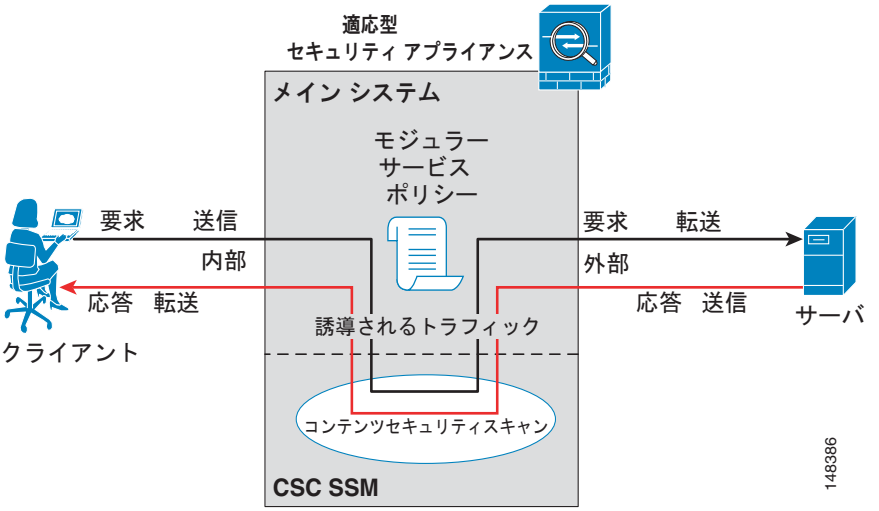
CSC SSM 搭載の適応型セキュリティ アプライアンスの構成について

適応型セキュリティ アプライアンスが CSC SSM とともに構成されているネットワークでは、CSC SSM にスキャンしたいトラフィックのタイプだけ送信するよう適応型セキュリティ アプライアンスを設定します。

図 14-1 に、企業ネットワーク、適応型セキュリティ アプライアンスおよび CSC SSM、またインターネット間の基本的なトラフィック フローを示します。図 14-1 に図示されたネットワークには次のものがあります。

- CSC SSM がインストールされ、設定されている適応型セキュリティ アプライアンス
- どのトラフィックが CSC SSM に転送されてスキャンされるかを指定する適応型セキュリティ アプライアンス上のサービス ポリシー

図 14-1　CSC SSM のトラフィック フロー



この例では、クライアントは Web サイトにアクセスし、FTP サーバからファイルをダウンロードし、または POP3 サーバからメールを受信するネットワーク ユーザと考えられます。

この設定では、トラフィック フローは次のようになります。

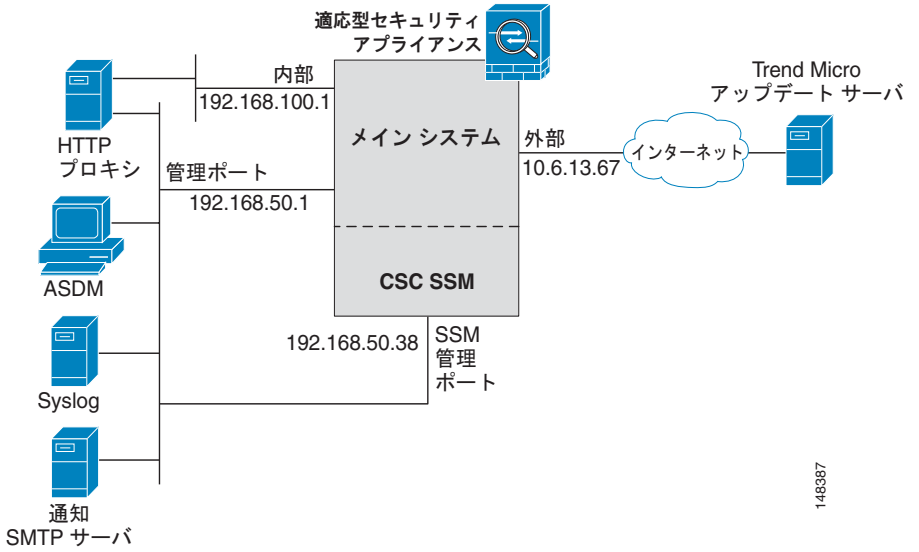
1. クライアントが要求を出します。
2. 適応型セキュリティ アプライアンスがその要求を受信し、インターネットに転送します。
3. 要求されたコンテンツを取得すると、適応型セキュリティ アプライアンスは、そのサービス ポリシーがこのコンテンツ タイプを CSC SSM に転送してスキャンすべきコンテンツとして定義しているどうか判断し、適宜、転送してスキャンします。
4. CSC SSM は適応型セキュリティ アプライアンスからコンテンツを受信し、スキャンして、その Trend Micro コンテンツ フィルタの最新アップデートと比較します。
5. コンテンツが疑わしい場合、CSC SSM はコンテンツをブロックし、イベントを報告します。コンテンツが疑わしくない場合は、CSC SSM は、ルーティングのため要求されたコンテンツを適応型セキュリティ アプライアンスに転送します。

（注）　CSC SSM は、SMTP トラフィックを他のコンテンツ タイプとは異なる方法で処理します。CSC SSM は SMTP トラフィックを受信してスキャンした後、ルーティングのためにトラフィックを適応型セキュリティ アプライアンスには転送しません。代わりに、CSC SSM は SMTP トラフィックを適応型セキュリティ アプライアンスで保護された SMTP サーバに直接転送します。

シナリオ：コンテンツ セキュリティのため CSC SSM を搭載したセキュリティ アプライアンス

図 14-2 に、CSC SSM を搭載した適応型セキュリティ アプライアンスの一般的な構成を示します。

図 14-2　CSC SSM 構成シナリオ



このシナリオでは、お客様はコンテンツ セキュリティのため CSC SSM を搭載した適応型セキュリティ アプライアンスを構成しています。特に興味深いのは次の点です。

- 適応型セキュリティ アプライアンスは専用管理ネットワーク上にあります。専用管理ネットワークの使用は必須ではありませんが、セキュリティを考え、使用することを推奨します。
- この適応型セキュリティ アプライアンス設定には 2 つの管理ポートがあります。1 つは適応型セキュリティ アプライアンス自体用、もう 1 つは CSC SSM 用です。すべての管理ホストは両方の IP アドレスにアクセスできることが必要です。
- HTTP プロキシ サーバは、内部ネットワークと専用管理ネットワーク両方に接続されています。これにより CSC SSM は、Trend Micro 社のアップデート サーバから更新されたコンテンツ セキュリティ フィルタを取得できます。
- アドミニストレータに CSC SSM イベントを通知できるよう、管理ネットワークには SMTP サーバが含まれています。管理ネットワークには、CSC SSM により生成されたログを保存するため syslog サーバも含まれています。

この項は、次の内容で構成されています。

- 「設定要件」（P.14-5）
- 「コンテンツ セキュリティのための CSC SSM の設定」（P.14-6）

設定要件

適応型セキュリティ アプライアンスの構成を計画する場合、ネットワークが次の要件を満たしていることが重要です。

- SSM 管理ポートの IP アドレスは、ASDM の実行で使用されるホストによりアクセスできなければなりません。ただし、SSM 管理ポートおよび適応型セキュリティ アプライアンス管理インターフェイスの IP アドレスは異なるサブネットにある場合があります。
- SSM 管理ポートは、CSC SSM が Trend Micro アップデート サーバに到達できるよう、インターネットに接続できなければなりません。

コンテンツ セキュリティのための CSC SSM の設定

オプションの CSC SSM モジュールとともに適応型セキュリティ アプライアンスを注文した場合、初期設定を完了するまでに、いくつか必要な手順があります。適応型セキュリティ アプライアンスで行う設定手順もあれば、CSC SSM で実行しているソフトウェアで行う手順もあります。

このマニュアルのこれよりも前の章の手順に従っている場合、この時点で、ライセンス ソフトウェアにより適応型セキュリティ アプライアンス システムが動作しており、Startup Wizard を使用して基本システム値が入力されています。次に、コンテンツ セキュリティ構成のために適応型セキュリティ アプライアンスを設定します。

基本的な手順は次のとおりです。

1. Cisco.com からソフトウェア アクティベーション キーを入手します。
2. CSC SSM の設定に必要な情報を収集します。
3. ASDM を使用して、時間設定を確認します。
4. ASDM で、CSC 設定ウィザードを実行し、CSC SSM を設定します。
5. ASDM を使用してトラフィックを CSC SSM に転送し、スキャンするよう適応型セキュリティ アプライアンスを設定します。

これらの手順の詳細は、次の項に記載されています。

この項は、次の内容で構成されています。

Cisco.com からのソフトウェア アクティベーション キーの入手

CSC SSM により、Product Authorization Key（PAK）を受信しているはずです。PAK を使用して、次の URL で CSC SSM を登録します。

http://www.cisco.com/go/license

登録後、E メールでアクティベーション キーを受信します。「CSC Setup Wizard の実行」（P.14-8）に記載された手順を完了する前に、アクティベーション キーが必要です。

情報の収集

適応型セキュリティ アプライアンスと CSC SSM を設定する前に、次の情報を収集します。

- CSC SSM 管理ポートの IP アドレスとネットマスク、ゲートウェイの IP アドレスとネットマスク。適応型セキュリティ アプライアンスの IP アドレスは、付録 A「3DES/AES ライセンスの取得」に記載されているように Startup Wizard を完了したときに割り当てられました。

（注）　SSM 管理ポートの IP アドレスは、ASDM の実行で使用されるホストによりアクセスできなければなりません。SSM 管理ポートおよび適応型セキュリティ アプライアンス管理インターフェイスの IP アドレスは異なるサブネットにある場合があります。

- CSC SSM に使用するホスト名とドメイン名
- DNS サーバの IP アドレス
- HTTP プロキシ サーバの IP アドレス（インターネットへの HTTP アクセスにネットワークでプロキシが使用されている場合）
- E メール通知に使用する E メール アドレスおよび SMTP サーバの IP アドレスとポート番号
- CSC SSM への管理アクセスを許可するためのホストとネットワークの IP アドレス

時間設定の確認

時間帯など、適応型セキュリティ アプライアンスの時間設定の精度を確認します。ライセンスには時間的制約があるため、セキュリティ イベントの記録、CSC SSM のコンテンツ フィルタ リストの自動アップデート、またライセンシングには時間は正確であることが重要です。

時間設定の精度を確認するには、次の手順に従います。

- 時間設定を手動で制御する場合、クロック設定を確認します。ASDM で、[Configuration] > [Device Setup] > [System Time] > [Clock] の順に選択します。
- NTP を使用して時間設定を制御している場合は、NTP 設定を確認します。ASDM で、[Configuration] > [Device Setup] > [System Time] > [NTP] の順に選択します。

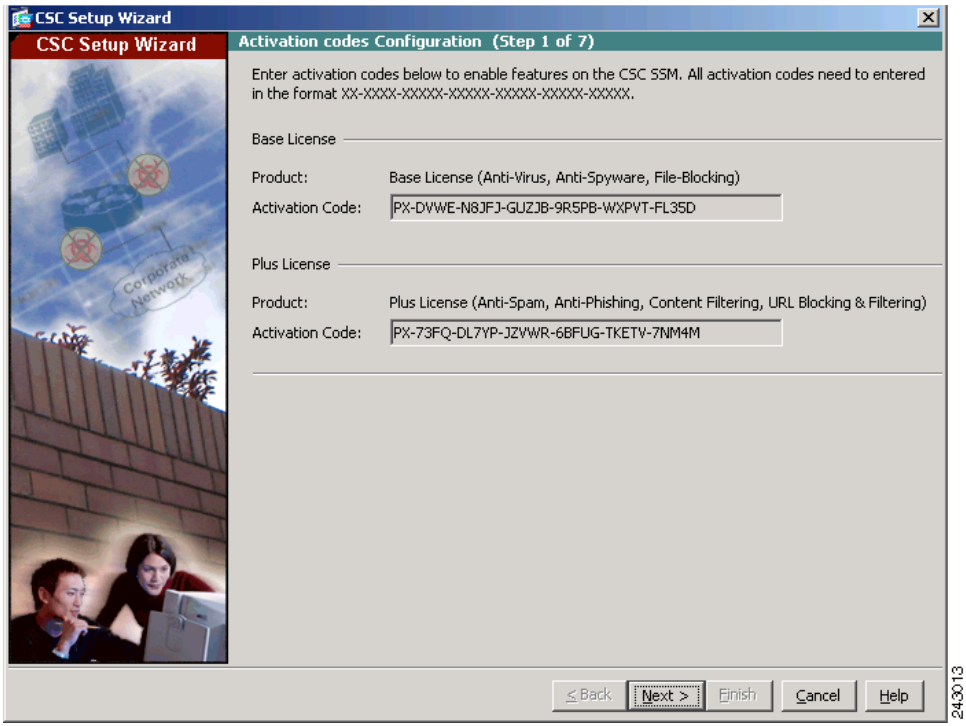
CSC Setup Wizard の実行

CSC 設定ウィザードを実行するには、次の手順に従います。

ステップ 1　ASDM メイン アプリケーション ウィンドウで、[Configuration] > [Trend Micro Content Security] > [Wizard Setup] > [Launch Wizard Setup] の順に選択します。

[CSC Setup Wizard] 画面が表示されます。

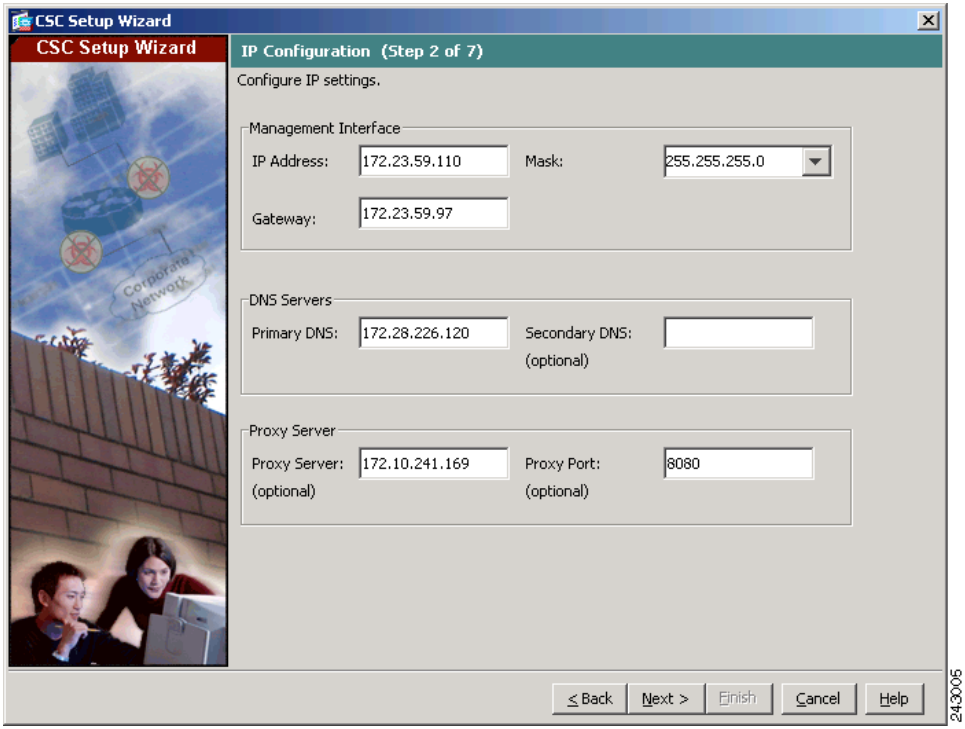
ステップ 2　CSC Setup Wizard の Step 1 で、[Base License] および、該当する場合は [Plus License] のプロダクト アクティベーション コードを入力します。[Plus License] のアクティベーション コードは CSC SSM の初期設定後に入力できます。



ステップ 3　[Next] をクリックします。

ステップ 4　CSC Setup Wizard の Step 2 で、次の情報を入力します。

- CSC 管理インターフェイスの IP アドレス、ネットワーク マスク、およびゲートウェイ IP アドレス
- Primary DNS サーバの IP アドレス
- （オプション）HTTP プロキシ サーバの IP アドレスおよびプロキシ ポート（ネットワークで HTTP プロキシ サーバを使用して HTTP 要求をインターネットに送信している場合）



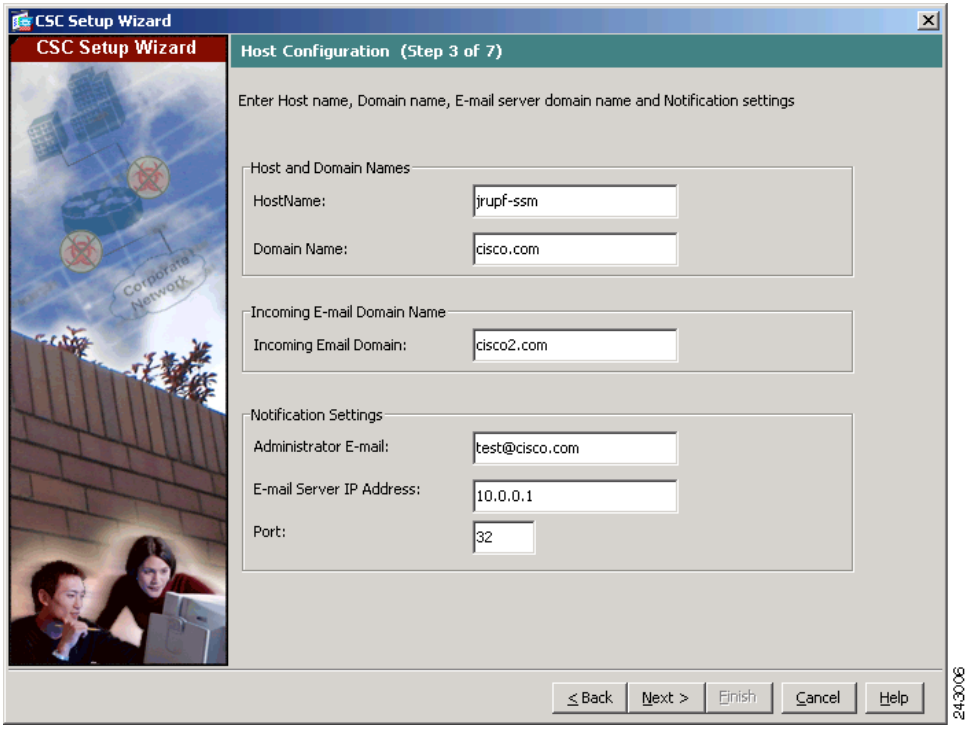
ステップ 5　[Next] をクリックします。

ステップ 6　CSC Setup Wizard の Step 3 で、次の情報を入力します。

- CSC SSM のホスト名とドメイン名
- ローカル メール サーバにより着信ドメインとして使用されているドメイン名

（注）　アンチスパム ポリシーは、このドメインに入る E メール トラフィックにだけ適用されます。

- 通知用のアドミニストレータの E メール アドレス、E メール サーバの IP アドレス、およびポート



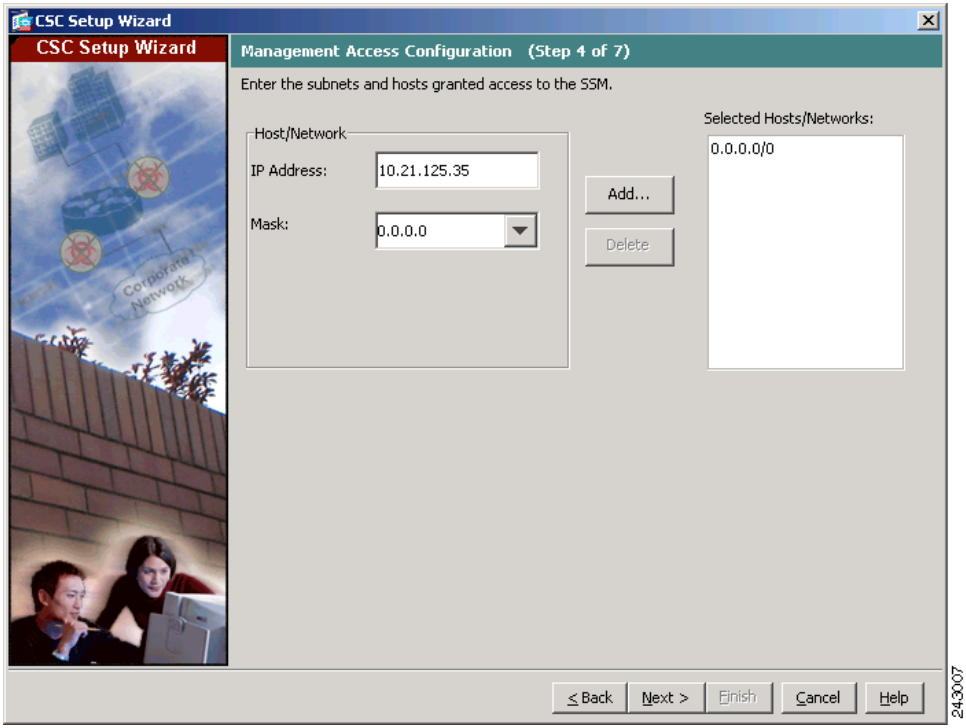
ステップ 7　[Next] をクリックします。

ステップ 8　CSC Setup Wizard の Step 4 で、次の情報を入力します。

- CSC SSM への管理アクセス権を持っているはずの、各サブネットおよびホストの IP アドレスとネットワーク マスク デフォルトでは、すべてのネットワークに CSC SSM への管理アクセス権があります。

（注）　セキュリティを考え、特定のサブネットや管理ホストへのアクセスを制限することを推奨します。

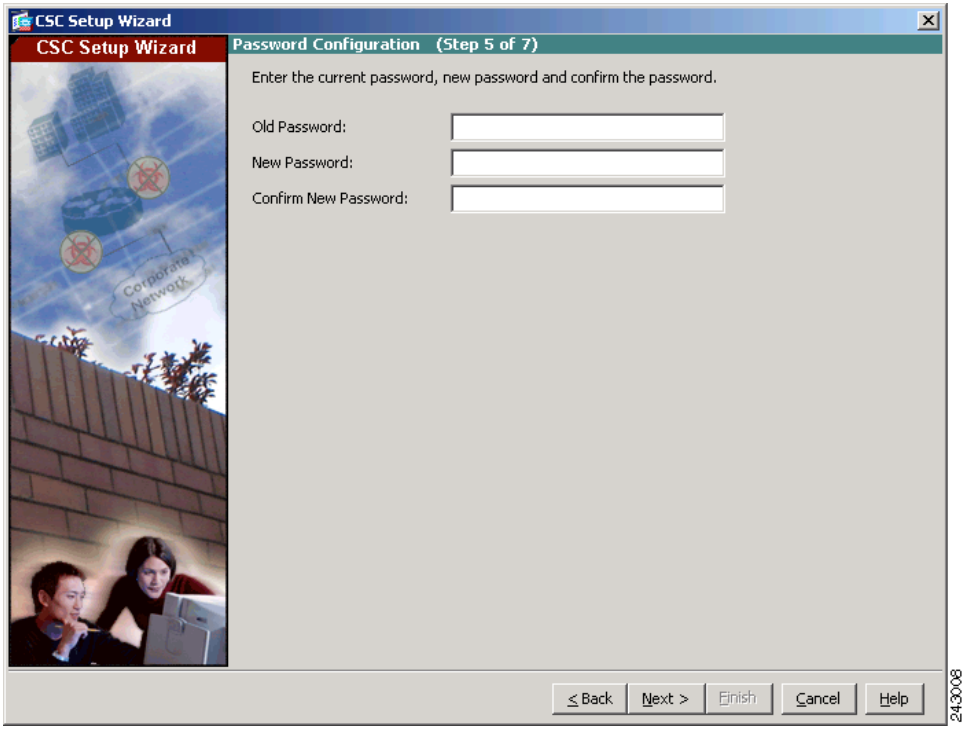
- ホストとネットワークの新しい組み合せを入力するには、[Add] をクリックします。
- 既存のホストとネットワークの組み合せを削除するには、[Selected Hosts/Networks] リストから 1 つ選択し、[Delete] をクリックします。



ステップ 9　[Next] をクリックします。

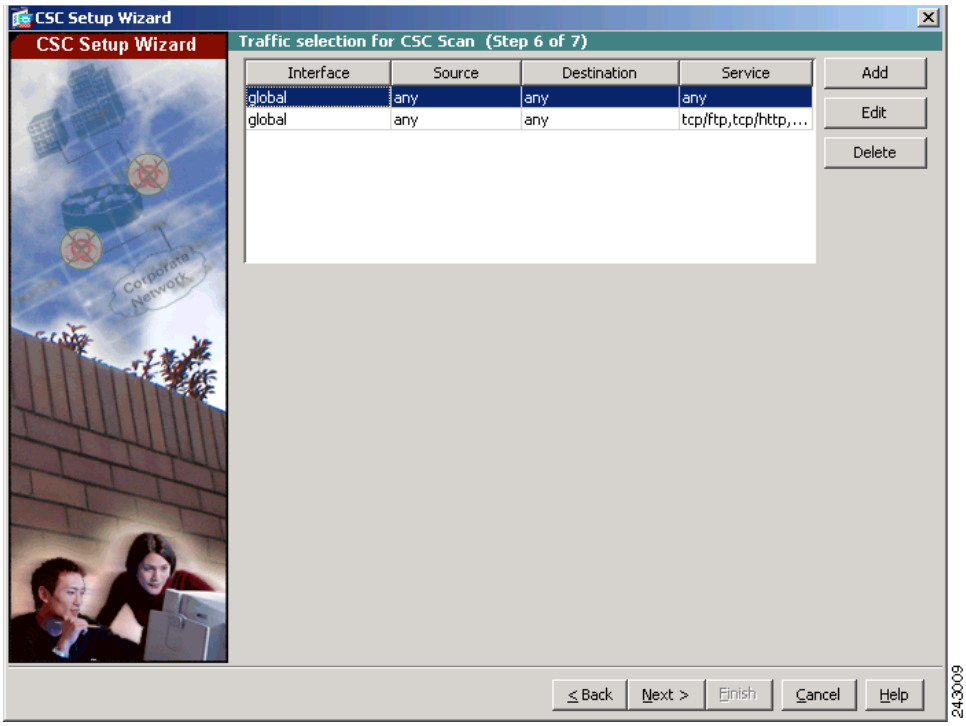
ステップ 10　CSC Setup Wizard の Step 5 で、次の情報を入力します。

- 工場出荷時のデフォルト パスワード「cisco」
- 管理アクセス用の新規パスワード
- 新規パスワードの確認

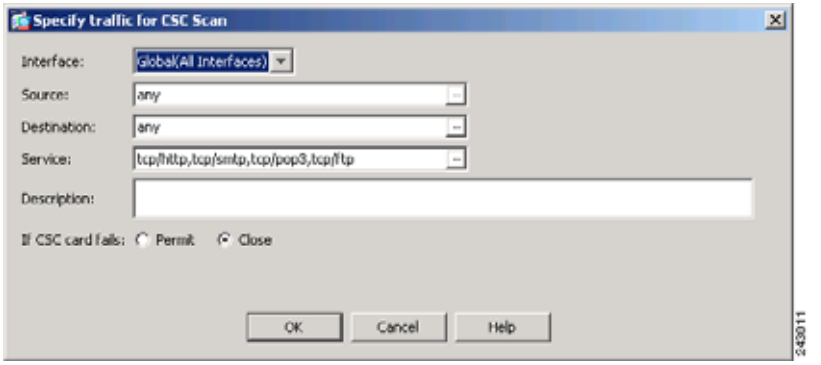


ステップ 11　[Next] をクリックします。

ステップ 12　CSC Setup Wizard の Step 6 で、CSC スキャンのためのトラフィック選択肢を定義します。[Add] をクリックします。



[Specify Traffic for CSC Scan] ダイアログボックスが表示されます。



ステップ 13　ドロップダウン リストからインターフェイスを選択します。利用可能なオプションは、[global (all interfaces)]、[inside]、[management]、および [ssm management] です。

ステップ 14　[IPv4 Network Objects] リストからネットワーク トラフィックの発信元を選択し、[OK] をクリックします。

ステップ 15　スキャンのため CSC のネットワーク トラフィックの宛先を指定するには、省略記号をクリックし、[Browse Destination] ダイアログボックスを表示します。

ステップ 16　[IPv4 Network Objects] リストからネットワーク トラフィックの宛先を選択し、[OK] をクリックします。

ステップ 17　スキャンのため CSC のサービスのタイプを指定するには、省略記号をクリックし、[Browse Service] ダイアログボックスを表示します。

ステップ 18　リストからサービス（複数の場合もあり）を選択し、[OK] をクリックします。

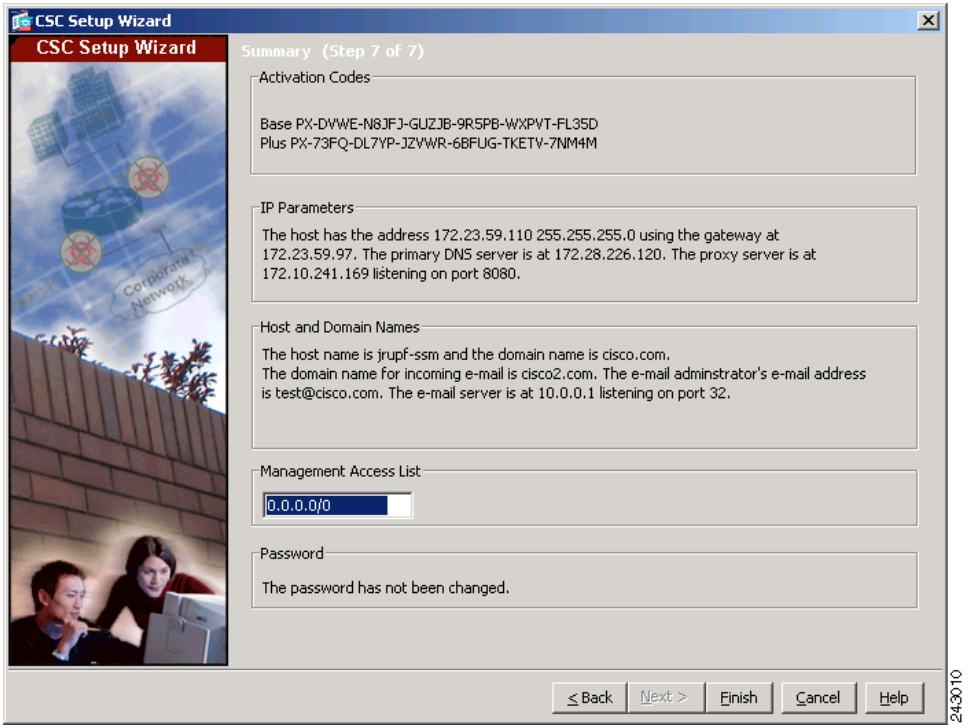
ステップ 19　CSC でスキャンするネットワーク トラフィックの説明を指定のフィールドに入力します。

ステップ 20　スキャンに失敗した場合に CSC でネットワーク トラフィックをスキャンできるかどうか指定する場合は、次の内容を実行します。

- スキャンせずにトラフィックの通過を許可する場合は、[Permit] をクリックします。
- スキャンせずにトラフィックが通過しないようにするには、[Deny] をクリックします。
- 設定を保存するには、[OK] をクリックします。追加されたトラフィックの詳細が [Traffic Selection for CSC Scan] 画面に表示されます。
- これらの設定を廃棄し、[Traffic Selection for CSC Scan] 画面に戻るには、[Cancel] をクリックします。[Cancel] をクリックすると、ASDM により決定を確認するダイアログボックスが表示されます。

ステップ 21　[Next] をクリックします。

ステップ 22　CSC Setup Wizard の Step 7 で、[Summary] 画面で CSC SSM に入力した設定内容を確認します。



ステップ 23　適切に設定されている場合は、[Finish] をクリックします。設定を変更するには、変更する設定が表示されている画面になるまで [Back] をクリックします。

CSC SSM がアクティブであることを示す情報メッセージが表示されます。

デフォルトでは、CSC SSM は、（アンチウイルス、アンチスパム、アンチフィッシング、およびコンテンツ フィルタリングを含む場合がある）購入したライセンスにしたがって有効になったコンテンツ セキュリティをスキャンするよう設定されています。また、Trend Micro 社のアップデート サーバから定期的にアップデートを入手するよう設定されています。

Plus ライセンスを購入した場合は、URL ブロッキングおよび URL フィルタリングだけでなく、E メール パラメータや FTP パラメータのカスタム設定を作成できます。詳細については、『*Cisco Content Security and Control SSM Administrator Guide*』を参照してください。

次の作業

これで、Trend Micro Interscan for Cisco CSC SSM ソフトウェアを設定する準備ができました。次のマニュアルを使用して、各実装内容に応じた適応型セキュリティ アプライアンスの設定を続けます。

作業内容	参照先
高度なセキュリティ ポリシーなど CSC SSM ソフトウェアの設定	『*Cisco Content Security and Control SSM Administrator Guide*』
コンテンツ フィルタリングなど、ASDM での追加 CSC SSM 機能の設定	ASDM オンライン ヘルプ
より効率的なサービス ポリシーを作成することによる AIP SSM と CSC SSM のパフォーマンスの最適化	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』

CSC SSM ソフトウェアを設定したら、次の追加の手順を実行することもできます。

作業内容	参照先
既存の詳細な設定およびオプション機能と拡張機能の設定	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』
日常的な運用について	『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series System Log Messages*』
ハードウェア メンテナンスおよびトラブルシューティング情報の確認	『*Cisco ASA 5500 Series Hardware Installation Guide*』

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できます。次の章では、適応型セキュリティ アプライアンスの他の一般的なアプリケーションの設定手順について説明します。

作業内容	参照先
DMZ Web サーバの保護設定	第 8 章「シナリオ：DMZ 設定」
リモートアクセス VPN の設定	第 9 章「シナリオ：IPsec リモートアクセス VPN 設定」
ソフトウェア クライアントのリモートアクセス SSL 接続設定	第 10 章「シナリオ：Cisco AnyConnect VPN クライアント用接続の設定」
ブラウザベースのリモートアクセス SSL 接続設定	第 11 章「シナリオ：SSL VPN クライアントレス接続」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN 設定」

次の作業

CHAPTER 15

ファイバ向け 4GE SSM の設定

4GE SSM（セキュリティ サービス モジュール）には、イーサネット ポートが 4 つあり、各ポートには SFP（Small Form-Factor Pluggable）ファイバまたは RJ 45 という 2 種類のメディア タイプ オプションがあります。同じ 4GE SSM カードを使用して、銅線ポートとファイバ ポートを混合させることができます。

（注） 4GE SSM には Cisco ASA 5500 シリーズ ソフトウェア バージョン 7.1（1）以降が必要です。

この章は、次の項で構成されています。

（注） デフォルトのメディア タイプ設定はイーサネットであるため、イーサネット インターフェイスを使用する場合はメディア タイプ設定を変更する必要はありません。

4GE SSM インターフェイスのケーブル接続

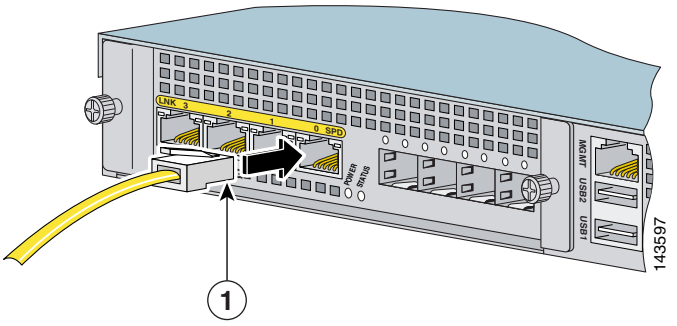
4GE SSM インターフェイスをケーブル接続するには、ネットワーク デバイスに接続するポートごとに次の手順に従います。

ステップ 1　RJ-45（イーサネット）インターフェイスをネットワーク デバイスに接続するには、インターフェイスごとに次の作業を実行します。

a. アクセサリ キットから黄色のイーサネット ケーブルを見つけます。

b. ケーブルの一方の端を 4GE SSM のイーサネット ポートに接続します（図 15-1 を参照）。

図 15-1　イーサネット ポートへの接続



1	RJ-45（イーサネット）ポート

c. ケーブルのもう一方の端をネットワーク デバイスに接続します。

ステップ 2　（オプション）SFP（光ファイバ）ポートを使用する場合は、SFP モジュールを取り付け、ケーブル接続します（図 15-2 を参照）。

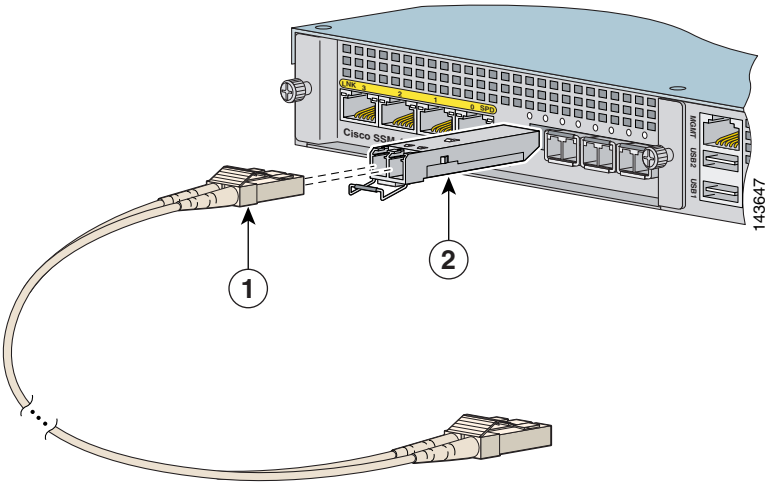
a. SFP モジュールを SFP ポートに差し込み、カチッと音がするまでスライドさせます。カチッという音がすれば、SFP モジュールがポートにロックされています。

b. 取り付けた SFP から光ポート プラグを取り外します。

c. 4GE SSM のアクセサリ キットから LC コネクタ（光ファイバ ケーブル）を見つけます。

d. LC コネクタを SFP ポートに接続します。

図 15-2　　LC コネクタの接続



1	LC コネクタ	2	SFP モジュール

e. LC コネクタのもう一方の端をネットワーク デバイスに接続します。

SFP ポートをネットワーク デバイスに接続したら、各 SFP インターフェイスのメディア タイプ設定も変更する必要があります。「ファイバ インターフェイスの 4GE SSM メディア タイプの設定（オプション）」の手順を実行します。

ファイバインターフェイスの 4GE SSM メディア タイプの設定（オプション）

ファイバ インターフェイスを使用している場合は、各 SFP インターフェイスに対して、メディア タイプ設定をデフォルト設定（イーサネット）からファイバ コネクタに変更する必要があります。

（注） デフォルトのメディア タイプ設定はイーサネットであるため、イーサネット インターフェイスを使用する場合はメディア タイプ設定を変更する必要はありません。

ASDM を使用する SFP インターフェイスのメディア タイプを設定するには、メイン ASDM ウィンドウから始まる次の手順に従います。

ステップ 1　ASDM ウィンドウの最上部で、[Configuration] タブをクリックします。

ステップ 2　ASDM ウィンドウの左側で、[Interfaces] タブをクリックします。

ステップ 3　[4GE SSM] インターフェイスをクリックして、[Edit] をクリックします。[Edit Interface] ダイアログボックスが表示されます。

ステップ 4　[Configure Hardware Properties] をクリックします。[Hardware Properties] ダイアログボックスが表示されます。

ステップ 5　[Media Type] ドロップダウン リストから、[Fiber Connector] を選択します。

ステップ 6　[OK] をクリックして [Edit Interfaces] ダイアログボックスに戻り、次に [OK] をクリックしてインターフェイス設定のダイアログボックスに戻ります。

ステップ 7　この手順を、各 SFP インターフェイスに対して繰り返します。

メディア タイプはコマンドラインから設定することもできます。詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』の「Configuring Ethernet Settings and Subinterfaces」を参照してください。

次の作業

これで初期設定が終了しました。次の追加の手順を実行することもできます。

実行内容	参照先
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』
日常的な運用について	『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series System Log Messages*』
ハードウェア メンテナンスおよびトラブルシューティング情報の確認	『*Cisco ASA 5500 Series Hardware Installation Guide*』

次の作業

APPENDIX A

3DES/AES ライセンスの取得

Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンスには、暗号化を提供する DES ライセンスが付属しています。セキュア リモート管理（SSH、ASDM など）、サイトツーサイト VPN、リモート アクセス VPN などの特定の機能をイネーブルにする暗号化テクノロジーを提供する 3DES/AES ライセンスを取得できます。このライセンスをイネーブルにするには、暗号化ライセンス キーが必要です。

Cisco.com の登録ユーザの場合、3DES/AES 暗号化ライセンスを入手するには、次の Web サイトにアクセスしてください。

http://www.cisco.com/go/license

Cisco.com の登録ユーザでない場合は、次の Web サイトにアクセスしてください。

https://tools.cisco.com/SWIFT/Licensing/RegistrationServlet

姓名、電子メールアドレス、および **show version** コマンド出力で表示される適応型セキュリティ アプライアンスのシリアル番号を入力してください。

（注） ライセンス アップグレードを請求すると、2 時間以内に、適応型セキュリティ アプライアンスの新しいアクティベーション キーが送信されます。

アクティベーション キーの例またはソフトウェアのアップグレードの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

アクティベーション キーを使用するには、次の手順に従います。

	コマンド	目的
ステップ 1	hostname# **show version**	ソフトウェア リリース、ハードウェア コンフィギュレーション、ライセンス キー、および関連の動作期間データを表示します。
ステップ 2	hostname# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	hostname(config)# **activation-key** *activation-5-tuple-key*	*activation-4-tuple-key* 変数を新しいライセンスで取得したアクティベーション キーに置き換えて、暗号化アクティベーション キーを更新します。*activation-5-tuple-key* 変数は 5 つの要素で構成される 16 進数文字列で、各要素間には 1 つずつスペースがあります。たとえば、0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e です。「0x」はオプションです。すべての値は 16 進数であると見なされます。
ステップ 4	hostname(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 5	hostname# **copy running-config startup-config**	設定を保存します。
ステップ 6	hostname# **reload**	適応型セキュリティ アプライアンスをリブートし、設定をリロードします。