Cisco ASA シリーズ ファイアウォール ASDM コンフィギュレーション ガイド

ソフトウェア バージョン 7.3

リリース日：2014 年 7 月 24 日
更新日：2014 年 9 月 16 日

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
住所、電話番号、FAX 番号は 以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices。

Text Part Number: なし、オンライン専用

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。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco ASA シリーズ ファイアウォール ASDM コンフィギュレーション ガイド
Copyright © 2014 Cisco Systems, Inc. All rights reserved.

CONTENTS

このマニュアルについて xvii

マニュアルの目的 xvii

関連資料 xvii

表記法 xviii

マニュアルの入手方法およびテクニカル サポート xix

PART 1 サービス ポリシーとアクセス コントロール

CHAPTER 1 サービス ポリシー 1-1

サービス ポリシーについて 1-1

サービス ポリシーのコンポーネント 1-1

サービス ポリシーで設定される機能 1-4

機能の方向 1-4

サービス ポリシー内の機能照合 1-5

複数の機能アクションが適用される順序 1-6

特定の機能アクションの非互換性 1-7

複数のサービス ポリシーの場合の機能照合 1-7

サービス ポリシーのガイドライン 1-8

サービス ポリシーのデフォルト 1-9

デフォルトのサービス ポリシー設定 1-9

デフォルトのクラス マップ（トラフィック クラス） 1-10

サービス ポリシーの設定 1-10

通過トラフィックのサービス ポリシー ルールの追加 1-11

管理トラフィックのサービス ポリシー ルールの追加 1-14

サービス ポリシー ルールの順序の管理 1-16

サービス ポリシーの履歴 1-17

CHAPTER 2 アプリケーション インスペクションの特別なアクション（インスペクション ポリシー マップ） 2-1

インスペクション ポリシー マップに関する情報 2-1

ガイドラインと制限事項 2-2

デフォルトのインスペクション ポリシー マップ 2-3

インスペクション ポリシー マップのアクションの定義 2-3

インスペクション クラス マップ内のトラフィックの特定 2-4
次の作業 2-4
インスペクション ポリシー マップの機能履歴 2-4

CHAPTER 3 アクセス ルール 3-1
ネットワーク アクセスの制御 3-1
ルールに関する一般情報 3-2
拡張アクセス ルール 3-5
EtherType ルール 3-6
アクセス コントロールに関するガイドライン 3-7
アクセス コントロールの設定 3-7
アクセス ルールの設定 3-8
管理アクセス ルールの設定 3-11
EtherType ルールの設定（トランスペアレント モードのみ） 3-12
ICMP アクセス ルールの設定 3-13
アクセス ルールのモニタリング 3-14
アクセス ルールの syslog メッセージの評価 3-14
アクセス ルールの履歴 3-15

CHAPTER 4 公開サーバ 4-1
公開サーバに関する情報 4-1
公開サーバのライセンス要件 4-1
ガイドラインと制限事項 4-2
スタティック NAT をイネーブルにする公開サーバの追加 4-2
PAT を設定したスタティック NAT をイネーブルにする公開サーバの追加 4-3
公開サーバの設定の編集 4-3
公開サーバの機能履歴 4-4

PART 2 ネットワーク アドレス変換

CHAPTER 5 ネットワーク アドレス変換（NAT）（ASA 8.3 以降） 5-1
NAT を使用する理由 5-1
NAT の用語 5-2
NAT タイプ 5-3
NAT のタイプの概要 5-3
スタティック NAT 5-3
ダイナミック NAT 5-8

ダイナミック PAT 5-10
アイデンティティ NAT 5-12
ルーテッド モードとトランスペアレント モードの NAT 5-12
ルーテッド モードの NAT 5-13
トランスペアレント モードの NAT 5-13
NAT と IPv6 5-15
NAT の実装方法 5-15
ネットワーク オブジェクト NAT と Twice NAT の主な違い 5-15
ネットワーク オブジェクト NAT 5-16
Twice NAT 5-17
NAT ルールの順序 5-20
NAT インターフェイス 5-21
NAT パケットのルーティング 5-22
マッピング アドレスとルーティング 5-22
リモート ネットワークのトランスペアレント モード ルーティングの要件 5-25
出力インターフェイスの決定 5-25
VPN の NAT 5-26
NAT とリモート アクセス VPN 5-26
NAT およびサイトツーサイト VPN 5-28
NAT および VPN 管理アクセス 5-30
NAT と VPN のトラブルシューティング 5-32
DNS および NAT 5-32
DNS 応答修正：Outside 上の DNS サーバ 5-33
DNS 応答修正：別々のネットワーク上の DNS サーバ、ホスト、サーバ 5-34
DNS 応答修正：ホスト ネットワーク上の DNS サーバ 5-35
外部 NAT を使用する DNS64 応答修正 5-35
PTR の変更、ホスト ネットワークの DNS サーバ 5-37
次の作業 5-37

CHAPTER 6 **ネットワーク オブジェクト NAT（ASA 8.3 以降）** 6-1
ネットワーク オブジェクト NAT に関する情報 6-1
ネットワーク オブジェクト NAT のライセンス要件 6-2
ネットワーク オブジェクト NAT の前提条件 6-2
ガイドラインと制限事項 6-2
デフォルト設定 6-4
ネットワーク オブジェクト NAT の設定 6-4
ダイナミック NAT または PAT プールを使用したダイナミック PAT の設定 6-4
ダイナミック PAT（隠蔽）の設定 6-10

スタティック NAT またはポート変換を設定したスタティック NAT の設定 6-13
アイデンティティ NAT の設定 6-17
Per-Session PAT ルールの設定 6-20
ネットワーク オブジェクト NAT のモニタリング 6-21
ネットワーク オブジェクト NAT の設定例 6-22
内部 Web サーバへのアクセスの提供（スタティック NAT） 6-23
内部ホストの NAT（ダイナミック NAT）および外部 Web サーバの NAT（スタティック NAT） 6-25
複数のマッピング アドレス（スタティック NAT、1 対多）を持つ内部ロード バランサ 6-30
FTP、HTTP、および SMTP のための単一アドレス（ポート変換を設定したスタティック NAT） 6-34
マッピング インターフェイス上の DNS サーバ、実際のインターフェイス上の Web サーバ（DNS 修正を設定したスタティック NAT） 6-37
マッピング インターフェイス上の DNS サーバおよび FTP サーバ、FTP サーバが変換される（DNS 修正を設定したスタティック NAT） 6-40
マッピング インターフェイス上の IPv4 DNS サーバおよび FTP サーバ、実際のインターフェイス上の IPv6 ホスト（DNS64 修正を設定したスタティック NAT64） 6-42
ネットワーク オブジェクト NAT の機能履歴 6-47

CHAPTER 7 Twice NAT（ASA 8.3 以降） 7-1
Twice NAT に関する情報 7-1
Twice NAT のライセンス要件 7-2
Twice NAT の前提条件 7-2
ガイドラインと制限事項 7-2
デフォルト設定 7-4
Twice NAT の設定 7-4
ダイナミック NAT または PAT プールを使用したダイナミック PAT の設定 7-5
ダイナミック PAT（隠蔽）の設定 7-13
スタティック NAT またはポート変換を設定したスタティック NAT の設定 7-19
アイデンティティ NAT の設定 7-25
Per-Session PAT ルールの設定 7-31
Twice NAT のモニタリング 7-31
Twice NAT の設定例 7-32
宛先に応じて異なる変換（ダイナミック PAT） 7-32
宛先アドレスおよびポートに応じて異なる変換（ダイナミック PAT） 7-41
Twice NAT の機能履歴 7-50

PART 3 アプリケーション インスペクション

CHAPTER 8 アプリケーション レイヤ プロトコル インスペクションの準備 8-1
アプリケーション レイヤ プロトコル インスペクション 8-1
インスペクション エンジンの動作 8-1
アプリケーション プロトコル インスペクションを使用するタイミング 8-3
インスペクション ポリシー マップ 8-3
アプリケーション インスペクションのガイドライン 8-5
アプリケーション インスペクションのデフォルト 8-6
デフォルト インスペクションと NAT に関する制限事項 8-6
デフォルトのインスペクション ポリシー マップ 8-10
アプリケーション レイヤ プロトコル インスペクションの設定 8-10
正規表現の設定 8-13
正規表現の作成 8-13
正規表現クラス マップの作成 8-17
アプリケーション インスペクションの履歴 8-17

CHAPTER 9 基本インターネット プロトコルのインスペクション 9-1
DNS インスペクション 9-1
DNS インスペクションのアクション 9-2
DNS インスペクションのデフォルト 9-2
DNS インスペクションの設定 9-2
DNS インスペクションのモニタリング 9-7
FTP インスペクション 9-8
FTP インスペクションの概要 9-8
厳密な FTP 9-8
FTP インスペクションの設定 9-9
FTP インスペクションの確認とモニタリング 9-14
HTTP インスペクション 9-14
HTTP インスペクションの概要 9-14
HTTP インスペクションの設定 9-15
ICMP インスペクション 9-20
ICMP エラー インスペクション 9-20
インスタント メッセージ インスペクション 9-21
インスタント メッセージ インスペクション ポリシー マップの設定 9-21
IM インスペクション サービス ポリシーの設定 9-23
IP オプション インスペクション 9-24
IP オプション インスペクションの概要 9-24

IP オプション インスペクションのデフォルト 9-25
IP オプション インスペクションの設定 9-25
IP オプション インスペクションのモニタリング 9-27
IPsec パススルー インスペクション 9-27
IPsec パススルー インスペクションの概要 9-27
IPsec パススルー インスペクションの設定 9-28
IPv6 インスペクション 9-30
IPv6 インスペクションのデフォルト 9-30
IPv6 インスペクションの設定 9-30
NETBIOS インスペクション 9-32
インスペクション制御を追加するための NetBIOS インスペクション ポリシー マップの設定 9-33
NetBIOS インスペクション サービス ポリシーの設定 9-33
PPTP インスペクション 9-34
SMTP および拡張 SMTP 検査 9-34
SMTP および拡張 SMTP（ESMTP）のインスペクションの概要 9-35
ESMTP インスペクションのデフォルト 9-36
ESMTP インスペクションの設定 9-36
TFTP インスペクション 9-39

CHAPTER 10 音声とビデオのプロトコルのインスペクション 10-1
CTIQBE インスペクション 10-1
CTIQBE インスペクションの制限事項 10-1
H.323 インスペクション 10-2
H.323 インスペクションの概要 10-2
H.323 の動作 10-3
H.245 メッセージでの H.239 サポート 10-4
H.323 インスペクションの制限事項 10-4
H.323 インスペクションの設定 10-5
H.323 および H.225 タイムアウト値の設定 10-9
MGCP インスペクション 10-9
MGCP インスペクションの概要 10-9
MGCP インスペクションの設定 10-11
MGCP タイムアウト値の設定 10-12
RTSP インスペクション 10-13
RTSP インスペクションの概要 10-13
RealPlayer 設定要件 10-13
RSTP インスペクションの制限事項 10-14
RTSP インスペクションの設定 10-14

SIP インスペクション 10-17
SIP インスペクションの概要 10-18
SIP インスペクションの制限事項 10-18
SIP インスタント メッセージ 10-19
デフォルトの SIP インスペクション 10-20
SIP インスペクションの設定 10-20
SIP タイムアウト値の設定 10-25
Skinny（SCCP）インスペクション 10-25
SCCP インスペクションの概要 10-25
Cisco IP Phone のサポート 10-26
SCCP インスペクションの制限事項 10-26
デフォルトの SCCP インスペクション 10-26
SCCP（Skinny）インスペクションの設定 10-27
音声とビデオのプロトコル インスペクションの履歴 10-29

CHAPTER 11 データベースおよびディレクトリ プロトコルのインスペクション 11-1
ILS インスペクション 11-1
SQL*Net インスペクション 11-2
Sun RPC インスペクション 11-3
Sun RPC インスペクション 11-3
許可された Sun RPC サービスの識別 11-4

CHAPTER 12 管理アプリケーション プロトコルのインスペクション 12-1
DCERPC インスペクション 12-1
DCERPC の概要 12-1
DCERPC インスペクションの設定 12-2
GTP インスペクション 12-4
GTP インスペクションの概要 12-4
GTP インスペクションのデフォルト 12-5
GTP インスペクションの設定 12-6
RADIUS アカウンティング インスペクション 12-9
RADIUS アカウンティング インスペクションの概要 12-9
RADIUS アカウンティング インスペクションの設定 12-10
RSH インスペクション 12-12
SNMP インスペクション 12-12
XDMCP インスペクション 12-13

PART 4 接続設定と QoS

CHAPTER 13 接続設定 13-1

接続の設定に関する情報 13-1
TCP 代行受信および初期接続の制限 13-2
クライアントレス SSL 互換での管理パケットの TCP 代行受信のディセーブル化 13-2
デッド接続検出（DCD） 13-2
TCP シーケンスのランダム化 13-3
TCP の正規化 13-3
TCP ステート バイパス 13-3
接続設定のライセンス要件 13-5
ガイドラインと制限事項 13-5
デフォルト設定 13-6
接続の設定 13-6
接続設定の構成のタスク フロー 13-6
TCP マップを使用した TCP ノーマライザのカスタマイズ 13-6
接続の設定 13-8
グローバル タイムアウトの設定 13-10
接続設定の機能履歴 13-12

CHAPTER 14 QoS 14-1

QoS について 14-1
サポートされる QoS 機能 14-2
トークン バケットとは 14-2
ポリシング 14-2
プライオリティ キューイング 14-3
QoS 機能の相互作用のしくみ 14-3
DSCP（DiffServ）の保存 14-3
QoS のガイドライン 14-3
QoS の設定 14-4
プライオリティ キューのプライオリティ キューおよび TX リング制限の決定 14-4
インターフェイスのプライオリティ キューの設定 14-6
プライオリティ キューイングとポリシング用のサービス ルールの設定 14-7
QoS のモニタ 14-8
QoS ポリシーの統計情報 14-9
QoS プライオリティの統計情報 14-9
QoS プライオリティ キューの統計情報 14-9

QoS の履歴 14-10

CHAPTER 15 接続のトラブルシューティングおよびリソース 15-1

コンフィギュレーションのテスト 15-1

ASA のインターフェイスへの ping の実行 15-1

ASA のコンフィギュレーションおよび動作の検証、および ping を使用したインターフェイスのテストの実行 15-3

トレースルートによるパケット ルーティングの決定 15-6

パケット トレーサによるパケットの追跡 15-7

パフォーマンスのモニタリング 15-9

システム リソースのモニタリング 15-10

ブロック 15-10

CPU 15-11

メモリ 15-11

接続のモニタリング 15-12

プロセスごとの CPU 使用率のモニタリング 15-13

PART 5 高度なネットワーク保護

CHAPTER 16 ASA および Cisco クラウド Web セキュリティ 16-1

Cisco クラウド Web セキュリティについて 16-2

クラウド Web セキュリティへの Web トラフィックのリダイレクト 16-2

ユーザ認証およびクラウド Web セキュリティ 16-2

認証キー 16-3

ScanCenter ポリシー 16-4

クラウド Web セキュリティのアクション 16-5

ホワイトリストを使用したスキャンのバイパス 16-6

IPv4 および IPv6 のサポート 16-6

プライマリ プロキシ サーバからバックアップ プロキシ サーバへのフェールオーバー 16-7

Cisco クラウド Web セキュリティのライセンス要件 16-7

クラウド Web セキュリティの前提条件 16-7

ガイドラインと制限事項 16-8

デフォルト設定 16-9

Cisco クラウド Web セキュリティ の設定 16-9

クラウド Web セキュリティ プロキシ サーバとの通信の設定 16-9

（マルチ コンテキスト モード）セキュリティ コンテキストごとのクラウド Web セキュリティの許可 16-10

クラウド Web セキュリティにトラフィックを送信するサービス ポリシーの方法 16-10
（オプション）ホワイトリストに記載されたトラフィックの設定 16-24
（オプション）ユーザ アイデンティティ モニタを設定します 16-26
クラウド Web セキュリティ ポリシーの設定 16-27
クラウド Web セキュリティのモニタ 16-27
関連資料 16-28
Cisco クラウド Web セキュリティの機能の履歴 16-28

CHAPTER 17 脅威検出 17-1
脅威の検出 17-1
基本脅威検出統計情報 17-2
拡張脅威検出統計情報 17-2
スキャン脅威検出 17-3
脅威検出のガイドライン 17-3
脅威検出のデフォルト 17-4
脅威検出の設定 17-4
基本脅威検出統計情報の設定 17-5
拡張脅威検出統計情報の設定 17-5
スキャン脅威検出の設定 17-6
脅威検出のモニタリング 17-7
基本脅威検出統計情報のモニタリング 17-7
拡張脅威検出統計情報のモニタリング 17-7
脅威検出の履歴 17-8

PART 6 ASA モジュール

CHAPTER 18 ASA FirePOWER（SFR）モジュール 18-1
ASA FirePOWER モジュール 18-1
ASA FirePOWER モジュールを ASA と連携させる方法 18-2
ASA FirePOWER 管理アクセス 18-4
ASA の機能との互換性 18-5
ASA FirePOWER モジュールのライセンス要件 18-5
ASA FirePOWER のガイドライン 18-6
ASA FirePOWER のデフォルト 18-7
ASA FirePOWER モジュールの設定 18-7
ASA FirePOWER 管理インターフェイスの接続 18-8

（ASA 5512-X ～ 5555-X）ソフトウェア モジュールのインストールまたはイメージの再作成 18-11
ASA FirePOWER 管理 IP アドレスの変更 18-15
ASA FirePOWER CLI での基本的な ASA FirePOWER 設定値の設定 18-15
FireSIGHT 管理センター への ASA FirePOWER の追加 18-16
ASA FirePOWER モジュールでのセキュリティ ポリシーの設定 18-18
ASA FirePOWER モジュールへのトラフィックのリダイレクト 18-18
ASA FirePOWER モジュールの管理 18-19
パスワードのリセット 18-20
モジュールのリロードまたはリセット 18-20
モジュールのシャットダウン 18-20
（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュール イメージのアンインストール 18-21
（ASA 5512-X ～ ASA 5555-X）ASA からモジュールへのセッション接続 18-21
5585-X ASA FirePOWER ハードウェア モジュールのイメージの再作成 18-22
システム ソフトウェアのアップグレード 18-24
ASA FirePOWER モジュールのモニタリング 18-24
モジュール ステータスの表示 18-24
モジュールの統計情報の表示 18-25
モジュール接続のモニタリング 18-25
ASA FirePOWER モジュールの履歴 18-26

CHAPTER 19 **ASA CX モジュール** 19-1

ASA CX モジュール 19-1
ASA CX モジュールがどのように ASA と連携するか 19-2
ASA CX の管理アクセス 19-4
アクティブ認証用の認証プロキシ 19-5
ASA の機能との互換性 19-5
ASA CX モジュールのライセンス要件 19-6
ASA CX の前提条件 19-6
ASA CX のガイドライン 19-6
ASA CX のデフォルト設定 19-8
ASA CX モジュールの設定 19-8
ASA CX 管理インターフェイスの接続 19-9
（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールのインストールまたはイメージの再作成 19-12
（ASA 5585-X）ASA CX 管理 IP アドレスの変更 19-14
基本的な ASA CX 設定値の設定 19-15
ASA CX モジュールでのセキュリティ ポリシーの設定 19-16

認証プロキシ ポートの設定 19-17
ASA CX モジュールへのトラフィックのリダイレクト 19-17
ASA CX モジュールの管理 19-20
パスワードのリセット 19-20
モジュールのリロードまたはリセット 19-21
モジュールのシャットダウン 19-21
（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュール イメージのアンインストール 19-21
（ASA 5512-X ～ ASA 5555-X）ASA からモジュールへのセッション接続 19-22
ASA CX モジュールのモニタリング 19-22
モジュール ステータスの表示 19-23
モジュールの統計情報の表示 19-23
モジュール接続のモニタリング 19-23
認証プロキシでの問題のトラブルシューティング 19-24
ASA CX モジュールの履歴 19-26

CHAPTER 20 **ASA IPS モジュール** 20-1
ASA IPS モジュールに関する情報 20-1
ASA IPS モジュールがどのように ASA と連携するか 20-1
動作モード 20-2
仮想センサーの使用 20-3
管理アクセスに関する情報 20-4
ASA IPS モジュールのライセンス要件 20-5
ガイドラインと制限事項 20-5
デフォルト設定 20-6
ASA IPS モジュールの設定 20-6
ASA IPS モジュールのタスク フロー 20-7
ASA IPS 管理インターフェイスの接続 20-7
ASA からモジュールへのセッションの開始（必要な場合がある） 20-10
（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールの起動 20-11
IPS モジュールの基本的なネットワーク設定値の設定 20-13
ASA IPS モジュールでのセキュリティ ポリシーの設定 20-14
セキュリティ コンテキストへの仮想センサーの割り当て 20-16
ASA IPS モジュールへのトラフィックの誘導 20-17
ASA IPS モジュールの管理 20-19
モジュール上でのイメージのインストールおよび起動 20-19
モジュールのシャットダウン 20-21
ソフトウェア モジュール イメージのアンインストール 20-21
パスワードのリセット 20-22

モジュールのリロードまたはリセット 20-22
ASA IPS モジュールのモニタリング 20-23
ASA IPS モジュールの機能履歴 20-23

このマニュアルについて

- 「マニュアルの目的」（P.xvii）
- 「関連資料」（P.xvii）
- 「表記法」（P.xviii）
- 「マニュアルの入手方法およびテクニカル サポート」（P.xix）

マニュアルの目的

このマニュアルは、適応型セキュリティ デバイス マネージャ（ASDM）を使用して Cisco ASA シリーズのファイアウォール機能を設定する際に役立ちます。このマニュアルは、すべての機能を網羅しているわけではなく、ごく一般的なコンフィギュレーションの事例を紹介しています。

このマニュアルを通じて、「ASA」という語は、特に指定がない限り、サポートされているモデルに一般的に適用されます。

（注） ASDM では、多数の ASA バージョンをサポートしています。ASDM のマニュアルおよびオンライン ヘルプには、ASA でサポートされている最新機能がすべて含まれています。古いバージョンの ASA ソフトウェアを実行している場合、ご使用のバージョンでサポートされていない機能がこのマニュアルに含まれている場合があります。同様に、古いメジャー バージョンまたはマイナー バージョンのメンテナンス リリースに機能が追加された場合、この新機能は、以降のすべての ASA リリースで使用できない場合でも、ASDM のマニュアルに含まれています。各章の機能履歴テーブルを参照して、機能がいつ追加されたかを確認してください。各 ASA のバージョンでサポートされている ASDM の最小バージョンについては、『*Cisco ASA Series Compatibility*』を参照してください。

関連資料

詳細については、「*Navigating the Cisco ASA Series Documentation*（Cisco ASA シリーズ マニュアルのナビゲーション）」（http://www.cisco.com/go/asadocs）を参照してください。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
太字の `courier` フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字の `courier` フォント**で示しています。
イタリック体の `courier` フォント	ユーザが値を指定する引数は、*イタリック体の `courier` フォント*で示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*（*Cisco 製品資料の更新情報*）』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

PART 1

サービス ポリシーとアクセス コントロール

サービス ポリシー

リリース日：2014 年 7 月 24 日
更新日：2014 年 9 月 16 日

サービス ポリシーにより、一貫性のある柔軟な方法でASAの機能を設定できます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。サービス ポリシーは、1 つのインターフェイスに適用されるか、またはグローバルに適用される複数のアクションまたはルールで構成されます。

- 「サービス ポリシーについて」（P.1-1）
- 「サービス ポリシーのガイドライン」（P.1-8）
- 「サービス ポリシーのデフォルト」（P.1-9）
- 「サービス ポリシーの設定」（P.1-10）
- 「サービス ポリシーの履歴」（P.1-17）

サービス ポリシーについて

次の各トピックでは、サービス ポリシーの仕組みについて説明します。

- 「サービス ポリシーのコンポーネント」（P.1-1）
- 「サービス ポリシーで設定される機能」（P.1-4）
- 「機能の方向」（P.1-4）
- 「サービス ポリシー内の機能照合」（P.1-5）
- 「複数の機能アクションが適用される順序」（P.1-6）
- 「特定の機能アクションの非互換性」（P.1-7）
- 「複数のサービス ポリシーの場合の機能照合」（P.1-7）

サービス ポリシーのコンポーネント

サービス ポリシーのポイントは、許可しているトラフィックに高度なサービスを適用することです。アクセス ルールによって許可されるトラフィックにサービス ポリシーを適用することで、サービス モジュールへのリダイレクトやアプリケーション インスペクションの適用などの特別な処理を実行できます。

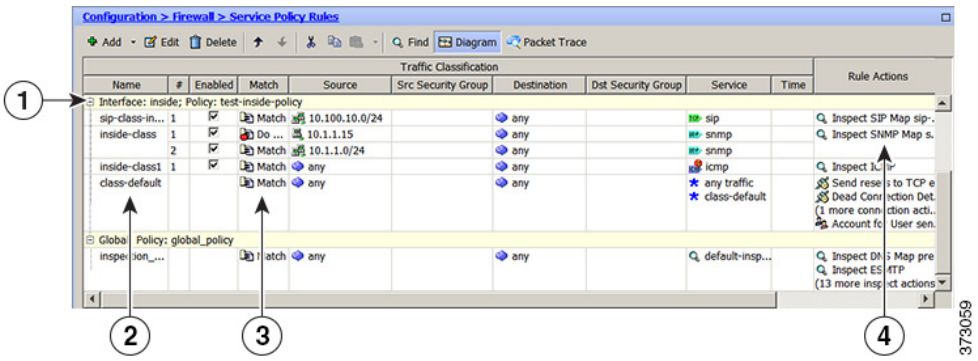
次のタイプのサービス ポリシーを使用できます。

- すべてのインターフェイスに適用される 1 つのグローバル ポリシー。
- インターフェイスごとに適用される 1 つのサービス ポリシー。このポリシーは、デバイスを通過するトラフィックと対象とするクラスと、ASA インターフェイス宛ての（インターフェイスを通過するのではない）管理トラフィックを対象とするクラスの組み合わせである場合があります。

各サービス ポリシーは、次の要素で構成されます。

1. サービス ポリシー マップ。これはルールの順序セットであり、**service-policy** コマンドで命名されます。ASDM では、ポリシー マップは [Service Policy Rules] ページにフォルダとして表示されます。
2. ルール。各ルールは、サービス ポリシー内の **class** コマンドと、および **class** コマンドに関連するコマンドで構成されます。ASDM では、各ルールは個別の行に表示され、ルールの名前はクラス名です。
   a. **class** コマンドは、ルールのトラフィック一致基準を定義します。
   b. **inspect** や **set connection timeout** などの class 関連のコマンドは、一致するトラフィックに適用するサービスと制約を定義します。inspect コマンドは、検査対象トラフィックに適用するアクションを定義するインスペクション ポリシー マップを指す場合があります。インスペクション ポリシー マップとサービス ポリシー マップは同じではないことに注意してください。

次の例では、サービス ポリシーが CLI と ASDM でどのように表示されるかを比較します。図の吹き出しと CLI の行は 1 対 1 では対応しないことに注意してください。



次の CLI は、上の図に示すルールによって生成されます。

```
: クラス マップで使用されるアクセス リスト。
: ASDM では、これらは吹き出し 3 の [Match] から [Time] までの各フィールドに対応します。
access-list inside_mpc line 1 extended permit tcp 10.100.10.0 255.255.255.0 any eq sip
access-list inside_mpc_1 line 1 extended deny udp host 10.1.1.15 any eq snmp
access-list inside_mpc_1 line 2 extended permit udp 10.1.1.0 255.255.255.0 any eq snmp
access-list inside_mpc_2 line 1 extended permit icmp any any
: SNMP インスペクションの SNMP マップ。v3 ですべてを拒否します。
: ASDM では、これは吹き出し 4 の class-inside ポリシーのルール アクションに対応します。
snmp-map snmp-v3only
  deny version 1
  deny version 2
  deny version 2c
: SIP 動作を定義するインスペクション ポリシー マップ。
: sip-high インスペクション ポリシー マップは、サービス ポリシー マップの inspect sip コマンドで
: 参照する必要があります。
: ASDM では、これは吹き出し 4 の sip-class-inside ポリシーのルール アクションに対応します。
policy-map type inspect sip sip-high
```

```
  parameters
    rtp-conformance enforce-payloadtype
    no traffic-non-sip
    software-version action mask log
    uri-non-sip action mask log
    state-checking action drop-connection log
    max-forwards-validation action drop log
    strict-header-validation action drop log
```

: inside-class ルールのトラフィック照合を定義するクラス マップ。
: ASDM では、これは吹き出し **3** の **[Match]** から **[Time]** までの各フィールドに対応します。

```
class-map inside-class
  match access-list inside_mpc_1
```

: sip-class-inside ルールのトラフィック照合を定義するクラス マップ。
: ASDM では、これは吹き出し **3** の **[Match]** から **[Time]** までの各フィールドに対応します。

```
class-map sip-class-inside
  match access-list inside_mpc
```

: inside-class1 ルールのトラフィック照合を定義するクラス マップ。
: ASDM では、これは吹き出し **3** の **[Match]** から **[Time]** までの各フィールドに対応します。

```
class-map inside-class1
  match access-list inside_mpc_2
```

: test-inside-policy というサービス ポリシー ルール セットを実際に定義するポリシー マップ。
: ASDM では、これは吹き出し **1** にあるフォルダに対応します。

```
policy-map test-inside-policy
```

: test-inside-policy の最初のルールである **sip-class-inside**。**SIP** トラフィックを検査します。
: sip-class-inside ルールは、**SIP** インスペクションに **sip-high** インスペクション ポリシー マップを適用します。
: ASDM では、各ルールは吹き出し **2** に対応します。

```
  class sip-class-inside
    inspect sip sip-high
```

: 2 番目のルールである **inside-class**。**SNMP** マップを使用して **SNMP** インスペクションを適用します。

```
  class inside-class
    inspect snmp snmp-v3only
```

: 3 番目のルールである **inside inside-class1**。**ICMP** インスペクションを適用します。

```
  class inside-class1
    inspect icmp
```

: 4 番目のルールである **class-default**。接続設定を適用し、ユーザ統計情報をイネーブルにします。

```
  class class-default
    set connection timeout embryonic 0:00:30 half-closed 0:10:00 idle 1:00:00
reset dcd 0:15:00 5
    user-statistics accounting
```

: service-policy コマンドは、**inside** インターフェイスにポリシー マップ ルール セットを適用します。
: このコマンドはポリシーをアクティブにします。

```
service-policy test-inside-policy interface inside
```

サービス ポリシーで設定される機能

次の表に、サービス ポリシーを使用して設定する機能の一覧を示します。

表 1-1　サービス ポリシーで設定される機能

機能	通過トラフィック用か	管理トラフィック用か	次を参照してください。
アプリケーション インスペクション（複数タイプ）	RADIUS アカウンティングを除く**すべて**	**RADIUS アカウンティング**のみ	• 第 8 章「アプリケーション レイヤ プロトコル インスペクションの準備」 • 第 9 章「基本インターネット プロトコルのインスペクション」 • 第 10 章「音声とビデオのプロトコルのインスペクション」 • 第 11 章「データベースおよびディレクトリ プロトコルのインスペクション」 • 第 12 章「管理アプリケーション プロトコルのインスペクション」 • 第 16 章「ASA および Cisco クラウド Web セキュリティ」
ASA IPS	**はい**	いいえ	第 20 章「ASA IPS モジュール」
ASA CX	**はい**	いいえ	第 19 章「ASA CX モジュール」
ASA FirePOWER（ASA SFR）	**はい**	いいえ	第 18 章「ASA FirePOWER（SFR）モジュール」
NetFlow セキュア イベント ロギングのフィルタリング	**はい**	**はい**	『一般的な操作のコンフィギュレーション ガイド』を参照してください。
QoS 入出力ポリシング	**はい**	いいえ	第 14 章「QoS」
QoS 標準プライオリティ キュー	**はい**	いいえ	第 14 章「QoS」
TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化	**はい**	**はい**	第 13 章「接続設定」
TCP の正規化	**はい**	いいえ	第 13 章「接続設定」
TCP ステート バイパス	**はい**	いいえ	第 13 章「接続設定」
アイデンティティ ファイアウォールのユーザ統計情報	**はい**	**はい**	『コマンド リファレンス』の **user-statistics** コマンドを参照してください。

機能の方向

アクションは、機能に応じて双方向または単方向にトラフィックに適用されます。双方向に適用される機能の場合、トラフィックが両方向のクラス マップと一致した場合に、ポリシー マップを適用するインターフェイスを出入りするすべてのトラフィックが影響を受けます。

（注）　グローバル ポリシーを使用する場合は、すべての機能が単方向です。単一インターフェイスに適用する場合に通常双方向の機能は、グローバルに適用される場合、各インターフェイスの入力にのみ適用されます。ポリシーはすべてのインターフェイスに適用されるため、ポリシーは両方向に適用され、この場合の双方向は冗長になります。

QoS プライオリティ キューなど単方向に適用される機能の場合は、ポリシー マップを適用するインターフェイスに出入りする（機能によって異なります）トラフィックだけが影響を受けます。各機能の方向については、次の表を参照してください。

表 1-2　機能の方向

機能	単一インターフェイスでの方向	グローバルでの方向
アプリケーション インスペクション（複数タイプ）	双方向	入力
ASA CSC	双方向	入力
ASA CX	双方向	入力
ASA CX 認証プロキシ	入力	入力
ASA FirePOWER（ASA SFR）	双方向	入力
ASA IPS	双方向	入力
NetFlow セキュア イベント ロギングのフィルタリング	該当なし	入力
QoS 入力ポリシング	入力	入力
QoS 出力ポリシング	出力	出力
QoS 標準プライオリティ キュー	出力	出力
TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化	双方向	入力
TCP の正規化	双方向	入力
TCP ステート バイパス	双方向	入力
アイデンティティ ファイアウォールのユーザ統計情報	双方向	入力

サービス ポリシー内の機能照合

パケットは、次のルールに従って特定のインターフェイスのポリシーの ルールに一致します。

1. パケットは、各機能タイプのインターフェイスのにだけ一致します。
2. パケットが機能タイプの ルールに一致した場合、ASA は、その機能タイプの後続の ルールとは照合しません。
3. ただし、パケットが別の機能タイプの後続の ルールと一致した場合、ASA は、後続の ルールのアクションも適用します（サポートされている場合）。サポートされていない組み合わせの詳細については、「特定の機能アクションの非互換性」（P.1-7）を参照してください。

（注）　アプリケーション インスペクションには、複数のインスペクション タイプが含まれ、ほとんどのタイプは相互に排他的です。組み合わせ可能なインスペクションの場合、各インスペクションは個々の機能と見なされます。

パケット照合の例

次に例を示します。

- パケットが接続制限値の ルールと一致し、アプリケーション インスペクションの ルールとも一致した場合、両方のクラス マップ アクションが適用されます。
- パケットが HTTP インスペクションで 1 つの ルールと一致し、HTTP インスペクションを含む別の ルールとも一致した場合、2 番目の ルールのアクションは適用されません。
- パケットが FTP インスペクションで 1 つの ルールと一致し、HTTP インスペクションを含む別の ルールとも一致した場合、HTTP および FTP インスペクションは組み合わせることができないため、2 番目の ルールのアクションは適用されません。
- パケットが HTTP インスペクションで 1 つの ルールと一致し、さらに IPv6 インスペクションを含む別の ルールとも一致した場合、IPv6 インスペクションは他のとタイプのインスペクションと組み合わせることができるため、両方のアクションが適用されます。

複数の機能アクションが適用される順序

サービス ポリシーの各種のアクションが実行される順序は、テーブル中に出現する順序とは無関係です。

アクションは次の順序で実行されます。

1. QoS 入力ポリシング
2. TCP の正規化、TCP と UDP の接続制限値とタイムアウト、TCP シーケンス番号のランダム化、および TCP ステート バイパス

   （注）　ASAがプロキシ サービス（AAA や CSC など）を実行したり、TCP ペイロード（FTP インスペクション）を変更したりするときは、TCP ノーマライザはデュアル モードで動作します。その場合、サービスを変更するプロキシやペイロードの前後で適用されます。

3. ASA CSC
4. 他のインスペクションと組み合わせることができるアプリケーション インスペクション：
   a. IPv6
   b. IP オプション
   c. WAAS
5. 他のインスペクションと組み合わせることができないアプリケーション インスペクション：詳細については、「特定の機能アクションの非互換性」（P.1-7）を参照してください。
6. ASA IPS
7. ASA CX
8. ASA FirePOWER（ASA SFR）

9. QoS 出力ポリシング
10. QoS 標準プライオリティ キュー

（注） NetFlow セキュア イベント ロギングのフィルタリングとアイデンティティ ファイアウォールのユーザ統計情報は順番に依存しません。

特定の機能アクションの非互換性

一部の機能は同じトラフィックに対して相互に互換性がありません。次のリストには、すべての非互換性が含まれていない場合があります。各機能の互換性については、その機能に関する章または項を参照してください。

- QoS プライオリティ キューイングと QoS ポリシングは同じトラフィックの集合に対して設定できません。
- ほとんどのインスペクションは別のインスペクションと組み合わせられないため、同じトラフィックに複数のインスペクションを設定しても、ASA は 1 つのインスペクションだけを適用します。HTTP インスペクションはクラウド Web セキュリティ インスペクションと組み合わせることができます。他の例外は、「複数の機能アクションが適用される順序」（P.1-6）に記載されています。
- トラフィックを ASA CX および ASA IPS などの複数のモジュールに送信されるように設定できません。
- HTTP インスペクションは、ASA CX または ASA FirePOWER と互換性がありません。
- クラウド ネットワーク セキュリティは、ASA CX または ASA FirePOWER と互換性がありません。

（注） デフォルト グローバル ポリシーで使用される の Default Inspection Traffic トラフィック クラスは、デフォルト ポートをすべてのインスペクションと照合する特別な CLI ショートカットです。ポリシー マップで使用すると、このクラス マップでは、トラフィックの宛先ポートに基づいて、各パケットに正しいインスペクションが適用されます。たとえば、宛先がポート 69 の UDP トラフィックが ASA に到達すると、ASA は TFTP インスペクションを適用し、宛先がポート 21 の TCP トラフィックが到着すると、ASA は FTP インスペクションを適用します。そのため、この場合に限って同じクラス マップに複数のインスペクションを設定できます。通常、ASA は、ポート番号を使用して適用するインスペクションを決定しないため、標準以外のポートなどにも柔軟にインスペクションを適用できます。

このトラフィック クラスには、クラウド Web セキュリティ インスペクション用のデフォルト ポートは含まれません（80 および 443）。

複数のサービス ポリシーの場合の機能照合

TCP および UDP トラフィック（およびステートフル ICMP インスペクションがイネーブルの場合は ICMP）の場合、サービス ポリシーはトラフィック フローに対して作用し、個々のパケットに限定されません。トラフィックが、1 つのインターフェイスのポリシーで定義されている機能に一致する既存の接続の一部である場合、そのトラフィック フローを別のインターフェイスのポリシーにある同じ機能と照合することはできません。最初のポリシーのみが使用されます。

たとえば、HTTP トラフィックが、HTTP トラフィックを検査する内部インターフェイスのポリシーと一致するときに、HTTP インスペクション用の外部インターフェイスに別のポリシーがある場合、そのトラフィックが外部インターフェイスの出力側でも検査されることはありません。同様に、その接続のリターン トラフィックが外部インターフェイスの入力ポリシーによって検査されたり、内部インターフェイスの出力ポリシーによって検査されたりすることもありません。

ステートフル ICMP インスペクションをイネーブルにしない場合の ICMP のように、フローとして扱われないトラフィックの場合は、リターン トラフィックを戻り側のインターフェイスの別のポリシー マップと照合できます。たとえば、内部および外部のインターフェイスで IPS を設定するとき、内部ポリシーでは仮想センサー 1 を使用するのに対して、外部ポリシーでは仮想センサー 2 を使用する場合、非ステートフル ping は仮想センサー 1 のアウトバウンド側を照合するだけでなく、仮想センサー 2 のインバウンド側も照合します。

サービス ポリシーのガイドライン

IPv6 のガイドライン

IPv6 は次の機能でサポートされています。

- DNS、FTP、HTTP、ICMP、ScanSafe、SIP、SMTP、IPsec-pass-thru、および IPv6 のアプリケーション インスペクション。
- ASA IPS
- ASA CX
- ASA FirePOWER
- NetFlow セキュア イベント ロギングのフィルタリング
- TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化
- TCP の正規化
- TCP ステート バイパス
- アイデンティティ ファイアウォールのユーザ統計情報

クラスマップ（トラフィック クラス）のガイドライン

すべてのタイプのクラス マップ（トラフィック クラス）の最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- レイヤ 3/4 クラスマップ（通過トラフィックと管理トラフィック向け）。
- インスペクション クラス マップ
- 正規表現クラス マップ
- インスペクション ポリシー マップ下で直接使用される **match** コマンド

この制限には、すべてのタイプのデフォルト クラス マップも含まれ、ユーザ設定のクラス マップを約 235 に制限します。「デフォルトのクラス マップ（トラフィック クラス）」（P.1-10）を参照してください。

サービス ポリシーのガイドライン

- インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、FTP インスペクションのグローバル ポリシーと、TCP 正規化のインターフェイス ポリシーがある場合、FTP インスペクションと TCP 正規化の両方がインターフェイスに適用されます。これに対し、FTP インスペクションのグローバル ポリシーと、FTP インスペクションのインターフェイス ポリシーがある場合は、インターフェイス ポリシーの FTP インスペクションだけがインターフェイスに適用されます。
- 適用できるグローバル ポリシーは 1 つだけです。たとえば、機能セット 1 が含まれたグローバル ポリシーと、機能セット 2 が含まれた別のグローバル ポリシーを作成できません。すべての機能は 1 つのポリシーに含める必要があります。
- コンフィギュレーションに対してサービス ポリシーの変更を加えた場合は、すべての *新しい* 接続で新しいサービス ポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。**show** コマンドの出力には、古い接続に関するデータは含まれません。

  たとえばインターフェイスから QoS サービス ポリシーを削除し、変更したバージョンを追加した場合、**show service-policy** コマンドには、新しいサービス ポリシーに一致する新しい接続に関連付けられた QoS カウンタだけが表示されます。古いポリシーの既存の接続はコマンド出力には表示されなくなります。

  すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。**clear conn** または **clear local-host** コマンドを使用してください。

サービス ポリシーのデフォルト

次の各トピックでは、サービス ポリシーとモジュラ ポリシー フレームワークのデフォルト設定について説明します。

- 「デフォルトのサービス ポリシー設定」（P.1-9）
- 「デフォルトのクラス マップ（トラフィック クラス）」（P.1-10）

デフォルトのサービス ポリシー設定

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーがコンフィギュレーションに含まれ、特定のインスペクションがすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。すべてのインスペクションがデフォルトでイネーブルになっているわけではありません。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します （特定の機能では、グローバル ポリシーはインターフェイス ポリシーより優先されます）。

デフォルト ポリシーには、次のアプリケーション インスペクションが含まれます。

- DNS
- FTP
- H323（H225）
- H323（RAS）
- RSH
- RTSP

- ESMTP
- SQLnet
- Skinny（SCCP）
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP
- IP オプション

デフォルトのクラス マップ（トラフィック クラス）

設定には、ASA が Default Inspection Traffic というデフォルト グローバル ポリシーで使用するデフォルトのレイヤ 3/4 クラス マップ（トラフィック クラス）が含まれます。このクラス マップは、デフォルトのインスペクション トラフィックを照合します。デフォルト グローバル ポリシーで使用されるこのクラスは、デフォルト ポートをすべてのインスペクションと照合する特別なショートカットです。

ポリシーで使用すると、このクラスでは、トラフィックの宛先ポートに基づいて、各パケットに正しいインスペクションが適用されます。たとえば、宛先がポート 69 の UDP トラフィックが ASA に到達すると、ASA は TFTP インスペクションを適用し、宛先がポート 21 の TCP トラフィックが到着すると、ASA は FTP インスペクションを適用します。そのため、この場合に限って同じクラス マップに複数のインスペクションを設定できます。通常、ASA は、ポート番号を使用して適用するインスペクションを決定しないため、標準以外のポートなどにも柔軟にインスペクションを適用できます。

デフォルト コンフィギュレーションにある別のクラス マップは、class-default と呼ばれ、すべてのトラフィックと一致します。必要であれば、Any トラフィック クラスを使用して class-default クラスを使用できます。実際、一部の機能は class-default でしか使用できません。

サービス ポリシーの設定

サービス ポリシーの設定では、インターフェイスあたりのサービス ポリシー ルール、またはグローバル ポリシーのサービス ポリシー ルールを 1 つ以上追加します。ASDM では、ウィザードを使用してサービス ポリシーを作成できます。それぞれのルールごとに、次の要素を指定します。

1. ルールを適用するインターフェイスまたはグローバル ポリシー。
2. アクションを適用するトラフィック。レイヤ 3 および 4 のトラフィックを指定できます。
3. トラフィック クラスに適用するアクション。トラフィック クラスごとに複数の競合しないアクションを適用できます。

ポリシーを作成した後にルールを追加したり、ルールやポリシーを移動、変更、または削除したりできます。次の各トピックでは、サービス ポリシーの設定方法について説明します。

- 「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）
- 「管理トラフィックのサービス ポリシー ルールの追加」（P.1-14）
- 「サービス ポリシー ルールの順序の管理」（P.1-16）

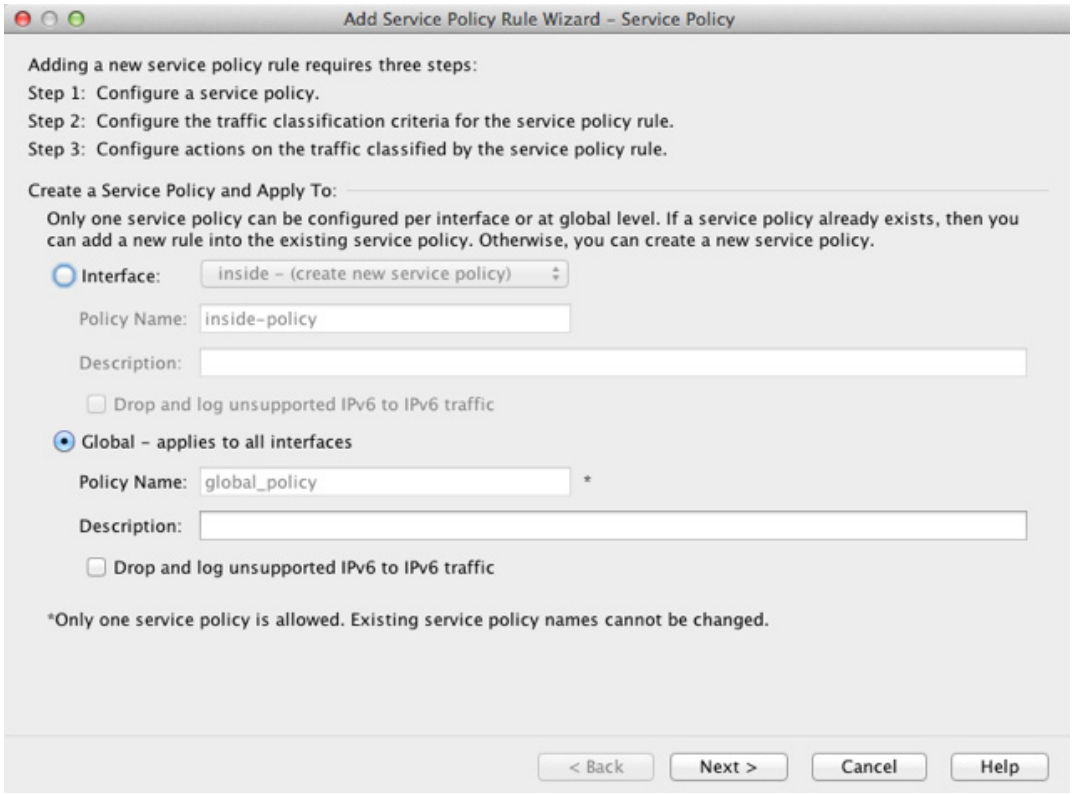
通過トラフィックのサービス ポリシー ルールの追加

通過トラフィックのサービス ポリシー ルールを追加するには、[Add Service Policy Rule Wizard] を使用します。ポリシーの適用範囲として、特定のインターフェイスまたはグローバルのいずれかを選択するように求められます。

- インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、FTP インスペクションを行うグローバル ポリシーと、TCP 接続制限を行うインターフェイス ポリシーが設定されている場合、インターフェイスには FTP インスペクションおよび TCP 接続制限がどちらも適用されます。これに対し、FTP インスペクションのグローバル ポリシーと、FTP インスペクションのインターフェイス ポリシーがある場合は、インターフェイス ポリシーの FTP インスペクションだけがインターフェイスに適用されます。
- グローバル サービス ポリシーは、すべてのインターフェイスにデフォルト サービスを提供します。インターフェイス固有のポリシーで上書きされない限り、グローバル ポリシーが適用されます。デフォルト アプリケーション インスペクションのサービス ポリシー ルールを含むグローバル ポリシーは、デフォルトで存在します。詳細については、「サービス ポリシーのデフォルト」（P.1-9）を参照してください。ウィザードを使用してルールをグローバル ポリシーに追加できます。

サービス ポリシーで設定できる機能については、「サービス ポリシーで設定される機能」（P.1-4）を参照してください。

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] を選択し、[Add] または [Add] > [Add Service Policy Rule] をクリックします。



ステップ 2　[Create a Service Policy and Apply To] 領域で次の操作を行います。

a. ポリシーを特定の**インターフェイス**に適用するか、すべてのインターフェイスに**グローバル**に適用するかを選択します。

b. [Interface] を選択した場合は、インターフェイスの名前を選択します。インターフェイスにすでにポリシーが設定されている場合は、既存のポリシーにルールを追加していることになります。

c. インターフェイスにまだサービス ポリシーが設定されていない場合は、新しいポリシーの名前を入力します。

d. （オプション）ポリシーの説明を入力します。

e. （オプション）[Drop and log unsupported IPv6 to IPv6 traffic] オプションをオンにして、IPv6 トラフィックをサポートしないアプリケーション インスペクションによってドロップされる IPv6 トラフィックの syslog（767001）を生成します。デフォルトでは、syslog が生成されません。IPv6 をサポートするインスペクションのリストについては、「IPv6 のガイドライン」（P.1-8）を参照してください。

f. [Next] をクリックします。

ステップ 3　[Traffic Classification Criteria] ページで、次のいずれかのオプションを選択してポリシー アクションを適用するトラフィックを指定し、[Next] をクリックします。

- [Create a new traffic class]。トラフィック クラスの名前を入力し、任意で説明を入力します。

  基準のいずれかを使用してトラフィックを特定します。

  – [Default Inspection Traffic]：このクラスは、ASA が検査可能なすべてのアプリケーションによって使用される、デフォルトの TCP および UDP ポートを照合します。[Next] をクリックすると、このクラスで定義されているサービスとポートが表示されます。

    デフォルト グローバル ポリシーで使用されるこのオプションは、ルール内で使用されると、トラフィックの宛先ポートに基づいて、パケットごとに正しい検査が適用されるようにします。詳細については、「デフォルトのクラス マップ（トラフィック クラス）」（P.1-10）を参照してください。

    デフォルト ポートのリストについては、「デフォルト インスペクションと NAT に関する制限事項」（P.8-6）を参照してください。ASA には、デフォルトのインスペクション トラフィックに一致して、すべてのインターフェイス上のトラフィックに共通検査を適用するデフォルト グローバル ポリシーが含まれます。Default Inspection Traffic クラスにポートが含まれているすべてのアプリケーションが、ポリシー マップにおいてデフォルトでイネーブルになっているわけではありません。

    Source and Destination IP Address(ACL を使用)クラスを Default Inspection Traffic クラスと一緒に指定して、照合されるトラフィックを絞り込むことができます。Default Inspection Traffic クラスは一致するポートとプロトコルを指定するので、アクセス リストのポートとプロトコルはすべて無視されます。

  – [Source and Destination IP Address (uses ACL)]：このクラスは拡張アクセス リストで指定されているトラフィックを照合します。ASA がトランスペアレント ファイアウォール モードで動作している場合は、EtherType ACL を使用できます。[Next] をクリックすると、アクセス コントロール エントリの属性を入力するように求められます。ウィザードによって ACL が作成されます。既存の ACL を選択することはできません。

    ACE を定義するときに [Match] オプションを選択すると、アドレスに一致するトラフィックにアクションを適用するルールが作成されます。[Do Not Match] オプションでは、トラフィックを指定したアクションの適用から免除します。たとえば、10.1.1.25 を除いて、10.1.1.0/24 のトラフィックすべてを照合し、そのトラフィックに接続制限を適用するとします。この場合は、2 つのルール（[Match] オプションを使用した 10.1.1.0/24 に対するルールおよび [Do Not Match] オプションを使用した 10.1.1.25 に対

するルール）を作成します。必ず、Do Not Match ルールが Match ルールの上になるように配置してください。順序を逆にすると、10.1.1.25 が最初に Match ルールを照合することになります。

（注） このタイプの新しいトラフィック クラスを作成する場合は、最初にアクセス コントロール エントリ（ACE）を 1 つだけ指定できます。ルールを追加した後は、同じインターフェイスまたはグローバル ポリシーに新しいルールを追加してから [Add rule to existing traffic class] を指定することによって、ACE を追加できます（以下を参照）。

- [Tunnel Group]：このクラスは、QoS を適用するトンネル グループ（接続プロファイル）のトラフィックを照合します。その他にもう 1 つのトラフィック照合オプションを指定してトラフィック照合対象をさらに絞込み、[Any Traffic]、[Source and Destination IP Address (uses ACL)]、または [Default Inspection Traffic] を排除できます。

  [Next] をクリックすると、トンネル グループを選択するように求められます（必要に応じて新しい接続グループを作成できます）。各フローをポリシングするには、[Match flow destination IP address] をオンにします。固有の IP 宛先アドレスに向かうトラフィックは、すべてフローと見なされます。

- [TCP or UDP Destination Port]：1 つのポートまたは連続する一定範囲のポートを照合します。[Next] をクリックすると、**TCP** または **UDP** のいずれかを選択してポート番号を入力するように求められます。ASDM ですでに定義されているポートを選択するには、[...] をクリックします。

ヒント 複数の非連続ポートを使用するアプリケーションの場合は、[Source and Destination IP Address (uses ACL)] を使用して各ポートを照合します。

- [RTP Range]：クラス マップは、RTP トラフィックを照合します。[Next] をクリックすると、2000 ～ 65534 の間の RTP ポート範囲を入力するように求められます。範囲内の最大ポート数は、16383 です。
- [IP DiffServ CodePoints (DSCP)]：このクラスは、IP ヘッダーの最大 8 つの DSCP 値を照合します。[Next] をクリックすると、目的の値を選択または入力する（それらの値を [Match] または [DSCP] リストに移動する）ように求められます。
- [IP Precedence]：このクラス マップは、IP ヘッダーの TOS バイトによって表される、最大 4 つの Precedence 値を照合します。[Next] をクリックすると、値を入力するように求められます。
- [Any Traffic]：すべてのトラフィックを照合します。

- [Add rule to existing traffic class]。すでに同じインターフェイスにサービス ポリシー ルールを指定している場合、またはグローバル サービス ポリシーを追加する場合は、このオプションによって既存のアクセス リストに ACE を追加できます。このインターフェイスのサービス ポリシー ルールで [Source and Destination IP Address (uses ACL)] オプションを選択した場合は、事前に作成したすべてのアクセス リストに ACE を追加できます。このトラフィック クラスでは、複数の ACE を追加する場合であっても、1 セットのルール アクションしか指定できません。この手順全体を繰り返すことによって、複数の ACE を同じトラフィック クラスに追加できます。ACE の順序の変更方法については、「サービス ポリシー ルールの順序の管理」（P.1-16）を参照してください。[Next] をクリックすると、アクセス コントロール エントリの属性を入力するように求められます。

- [Use an existing traffic class]。別のインターフェイスのルールで使用されるトラフィック クラスを作成した場合は、そのトラフィック クラス定義をこのルールで再使用できます。1 つのルールのトラフィック クラスを変更すると、その変更は同じトラフィック クラスを使用するすべてのルールに継承されます。コンフィギュレーションに CLI で入力した **class-map** コマンドが含まれている場合は、それらのトラフィック クラス名も使用できます（ただし、そのトラフィック クラスの定義を表示するには、そのルールを作成する必要があります）。
- [Use class default as the traffic class]。このオプションでは、すべてのトラフィックを照合する class-default クラスを使用します。class-default クラスは、ASA によって自動的に作成され、ポリシーの最後に配置されます。このクラスは、アクションを何も適用しない場合でも ASA によって作成されますが、内部での使用に限られます。必要に応じて、このクラスにアクションを適用できます。これは、すべてのトラフィックを照合する新しいトラフィック クラスを作成するよりも便利な場合があります。class-default クラスを使用して、このサービス ポリシーにルールを 1 つだけ作成できます。これは、各トラフィック クラスを関連付けることができるのは、サービス ポリシーごとに 1 つのルールだけであるためです。

ステップ 4　追加設定が必要なトラフィック一致基準を選択した場合は、目的のパラメータを入力して [Next] をクリックします。

ステップ 5　[Rule Actions] ページで、1 つまたは複数のルール アクションを設定します。適用できる機能およびアクション（詳細情報へのリンクを含む）については、「サービス ポリシーで設定される機能」（P.1-4）を参照してください。

ステップ 6　[Finish] をクリックします。

管理トラフィックのサービス ポリシー ルールの追加

管理目的で ASA に向けられるトラフィックのサービス ポリシー ルールを追加するには、[Add Service Policy Rule] ウィザードを使用します。ポリシーの適用範囲として、特定のインターフェイスまたはグローバルのいずれかを選択するように求められます。

- インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、RADIUS アカウンティング インスペクションを使用するグローバル ポリシーと接続制限を使用するインターフェイス ポリシーがある場合、RADIUS アカウンティングと接続制限の両方がそのインターフェイスに適用されます。ただし、RADIUS アカウンティングを使用するグローバル ポリシーと RADIUS アカウンティングを使用するインターフェイス ポリシーがある場合、インターフェイス ポリシー RADIUS アカウンティングだけがそのインターフェイスに適用されます。
- グローバル サービス ポリシーは、すべてのインターフェイスにデフォルト サービスを提供します。インターフェイス固有のポリシーで上書きされない限り、グローバル ポリシーが適用されます。デフォルト アプリケーション インスペクションのサービス ポリシー ルールを含むグローバル ポリシーは、デフォルトで存在します。詳細については、「サービス ポリシーのデフォルト」（P.1-9）を参照してください。ウィザードを使用してルールをグローバル ポリシーに追加できます。

サービス ポリシーで設定できる機能については、「サービス ポリシーで設定される機能」（P.1-4）を参照してください。

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] を選択し、[Add] または [Add] > [Add Management Service Policy Rule] をクリックします。

ステップ 2　[Create a Service Policy and Apply To] 領域で次の操作を行います。

a. ポリシーを特定の**インターフェイス**に適用するか、すべてのインターフェイスに**グローバル**に適用するかを選択します。

b. [Interface] を選択した場合は、インターフェイスの名前を選択します。インターフェイスにすでにポリシーが設定されている場合は、既存のポリシーにルールを追加していることになります。

c. インターフェイスにまだサービス ポリシーが設定されていない場合は、新しいポリシーの名前を入力します。

d. （オプション）ポリシーの説明を入力します。

e. [Next] をクリックします。

ステップ 3　[Traffic Classification Criteria] ページで、次のいずれかのオプションを選択してポリシー アクションを適用するトラフィックを指定し、[Next] をクリックします。

- [Create a new traffic class]。トラフィック クラスの名前を入力し、任意で説明を入力します。

  基準のいずれかを使用してトラフィックを特定します。

  – [Source and Destination IP Address (uses ACL)]：このクラスは拡張アクセス リストで指定されているトラフィックを照合します。ASA がトランスペアレント ファイアウォール モードで動作している場合は、EtherType ACL を使用できます。[Next] をクリックすると、アクセス コントロール エントリの属性を入力するように求められます。ウィザードによって ACL が作成されます。既存の ACL を選択することはできません。

    ACE を定義するときに [Match] オプションを選択すると、アドレスに一致するトラフィックにアクションを適用するルールが作成されます。[Do Not Match] オプションでは、トラフィックを指定したアクションの適用から免除します。たとえば、10.1.1.25 を除いて、10.1.1.0/24 のトラフィックすべてを照合し、そのトラフィックに接続制限を適用するとします。この場合は、2 つのルール（[Match] オプションを使用した 10.1.1.0/24 に対するルールおよび [Do Not Match] オプションを使用した 10.1.1.25 に対するルール）を作成します。必ず、Do Not Match ルールが Match ルールの上になるように配置してください。順序を逆にすると、10.1.1.25 が最初に Match ルールを照合することになります。

  – [TCP or UDP Destination Port]：1 つのポートまたは連続する一定範囲のポートを照合します。[Next] をクリックすると、**TCP** または **UDP** のいずれかを選択してポート番号を入力するように求められます。ASDM ですでに定義されているポートを選択するには、[...] をクリックします。

ヒント　複数の非連続ポートを使用するアプリケーションの場合は、[Source and Destination IP Address (uses ACL)] を使用して各ポートを照合します。

- [Add rule to existing traffic class]。すでに同じインターフェイスにサービス ポリシー ルールを指定している場合、またはグローバル サービス ポリシーを追加する場合は、このオプションによって既存のアクセス リストに ACE を追加できます。このインターフェイスのサービス ポリシー ルールで [Source and Destination IP Address (uses ACL)] オプションを選択した場合は、事前に作成したすべてのアクセス リストに ACE を追加できます。このトラフィック クラスでは、複数の ACE を追加する場合であっても、1 セットのルール アクションしか指定できません。この手順全体を繰り返すことによって、複数の ACE を同じトラフィック クラスに追加できます。ACE の順序の変更方法については、「サービス ポリシー ルールの順序の管理」（P.1-16）を参照してください。[Next] をクリックすると、アクセス コントロール エントリの属性を入力するように求められます。

- [Use an existing traffic class]。別のインターフェイスのルールで使用されるトラフィック クラスを作成した場合は、そのトラフィック クラス定義をこのルールで再使用できます。1 つのルールのトラフィック クラスを変更すると、その変更は同じトラフィック クラスを使用するすべてのルールに継承されます。コンフィギュレーションに CLI で入力した **class-map** コマンドが含まれている場合は、それらのトラフィック クラス名も使用できます（ただし、そのトラフィック クラスの定義を表示するには、そのルールを作成する必要があります）。

ステップ 4　追加設定が必要なトラフィック一致基準を選択した場合は、目的のパラメータを入力して [Next] をクリックします。

ステップ 5　[Rule Actions] ページで、1 つまたは複数のルール アクションを設定します。

- RADIUS アカウンティング インスペクションを設定するには、[RADIUS Accounting Map] ドロップダウン リストからインスペクション マップを選択するか、または [Configure] をクリックしてマップを追加します。詳細については、「サービス ポリシーで設定される機能」（P.1-4）を参照してください。
- 接続を設定するには、「接続の設定」（P.13-8）を参照してください。

ステップ 6　[Finish] をクリックします。

サービス ポリシー ルールの順序の管理

インターフェイス上またはグローバル ポリシー内でのサービス ポリシー ルールの順序は、トラフィックへのアクションの適用方法に影響します。パケットがサービス ポリシーのルールを照合する方法については、次のガイドラインを参照してください。

- パケットは、機能タイプごとにサービス ポリシーのルールを 1 つだけ照合できます。
- パケットが、1 つの機能タイプのアクションを含むルールを照合する場合、ASA は、その機能タイプを含む、後続のどのルールに対してもそのパケットを照合しません。
- ただし、そのパケットが異なる機能タイプの後続のルールを照合する場合、ASA は後続ルールのアクションも適用します。

たとえば、パケットが接続制限のルールを照合し、アプリケーション インスペクションのルールも照合する場合は、両方のアクションが適用されます。

パケットがアプリケーション インスペクションのルールを照合し、アプリケーション インスペクションを含む別のルールを照合する場合、2 番目のルール アクションは適用されません。

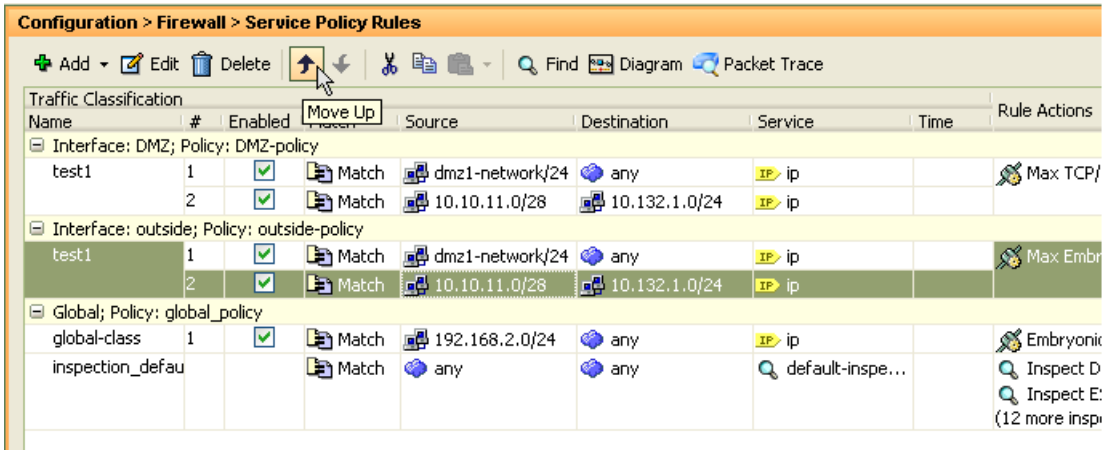
ルールに複数の ACE が組み込まれたアクセス リストが含まれる場合は、ACE の順序もパケット フローに影響します。ASA は、リストのエントリの順序に従って、各 ACE に対してパケットをテストします。一致が見つかると、ACE はそれ以上チェックされません。たとえば、すべてのトラフィックを明示的に許可する ACE を ACL の先頭に作成した場合は、残りのステートメントはチェックされません。

ルールまたはルール内での ACE の順序を変更するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] ペインで、上または下に動かすルールまたは ACE を選択します。

ステップ 2　[Move Up] または [Move Down] ボタンをクリックします。

図 1-1　　ACE の移動



（注）　複数のサービス ポリシーで使用されるアクセス リストで ACE を並べ替えると、その変更はすべてのサービス ポリシーで継承されます。

ステップ 3　ルールまたは ACE を並べ替えたら、[Apply] をクリックします。

サービス ポリシーの履歴

機能名	リリース	説明
モジュラ ポリシー フレームワーク	7.0(1)	モジュラ ポリシー フレームワークが導入されました。
RADIUS アカウンティング トラフィックで使用する管理クラス マップ	7.2(1)	RADIUS アカウンティング トラフィックで使用する管理クラス マップが導入されました。**class-map type management** コマンドおよび **inspect radius-accounting** コマンドが導入されました。
インスペクション ポリシー マップ	7.2(1)	インスペクション ポリシー マップが導入されました。**class-map type inspect** コマンドが導入されました。
正規表現およびポリシー マップ	7.2(1)	インスペクション ポリシー マップで使用される正規表現およびポリシー マップが導入されました。**class-map type regex** コマンド、**regex** コマンド、および**match regex** コマンドが導入されました。
インスペクション ポリシー マップの match any	8.0(2)	インスペクション ポリシー マップで使用される **match any** キーワードが導入されました。トラフィックを 1 つ以上の基準に照合してクラス マップに一致させることができます。以前は、**match all** だけが使用可能でした。

CHAPTER 2

アプリケーション インスペクションの特別なアクション（インスペクション ポリシー マップ）

モジュラ ポリシー フレームワークでは、多くのアプリケーション インスペクションで実行される特別なアクションを設定できます。サービス ポリシーでインスペクション エンジンをイネーブルにする場合は、*インスペクション ポリシー マップ*で定義されるアクションを必要に応じてイネーブルにすることもできます。インスペクション ポリシー マップが、インスペクション アクションを定義したサービス ポリシー内のトラフィックと一致すると、トラフィックのそのサブセットが指定したとおりに動作します（たとえば、ドロップやレート制限など）。

- 「インスペクション ポリシー マップに関する情報」（P.2-1）
- 「ガイドラインと制限事項」（P.2-2）
- 「デフォルトのインスペクション ポリシー マップ」（P.2-3）
- 「インスペクション ポリシー マップのアクションの定義」（P.2-3）
- 「インスペクション クラス マップ内のトラフィックの特定」（P.2-4）
- 「次の作業」（P.2-4）
- 「インスペクション ポリシー マップの機能履歴」（P.2-4）

インスペクション ポリシー マップに関する情報

インスペクション ポリシー マップをサポートするアプリケーションのリストについては、「アプリケーション レイヤ プロトコル インスペクションの設定」（P.8-10）を参照してください。

インスペクション ポリシー マップは、次に示す要素の 1 つ以上で構成されています。インスペクション ポリシー マップで使用可能な実際のオプションは、アプリケーションに応じて決まります。

- トラフィック照合オプション：インスペクション ポリシー マップで直接トラフィック照合オプションを定義して、アプリケーションのトラフィックを、URL 文字列などのアプリケーションに固有の基準と照合できます。一致した場合にはアクションをイネーブルにします。
  - 一部のトラフィック照合オプションでは、正規表現を指定してパケット内部のテキストを照合できます。ポリシー マップを設定する前に、正規表現クラス マップ内で、正規表現を単独またはグループで作成およびテストしておいてください。

- インスペクション クラス マップ：インスペクション クラス マップには、複数のトラフィック照合オプションが含まれます。その後、ポリシー マップでクラス マップを指定し、クラス マップのアクションを全体としてイネーブルにします。クラス マップを作成することと、インスペクション ポリシー マップ内で直接トラフィック照合を定義することの違いは、より複雑な一致基準を作成できる点と、クラス マップを再使用できる点です。ただし、異なる一致基準に対して異なるアクションを設定することはできません。**注：**すべてのアプリケーションがインスペクション クラス マップをサポートするわけではありません。
- パラメータ：パラメータは、インスペクション エンジンの動作に影響します。

ガイドラインと制限事項

- HTTP インスペクション ポリシー マップ：使用中の HTTP インスペクション ポリシー マップを変更する場合、変更を有効にするには、インスペクション ポリシー マップの アクションを削除し、再適用する必要があります。たとえば、「http-map」インスペクション ポリシー マップを修正する場合は、そのインスペクション ポリシー マップを削除し、変更を適用して、サービス ポリシーに再度追加する必要があります。
- すべてのインスペクション ポリシー マップ：使用中のインスペクション ポリシー マップを別のマップ名と交換する場合は、そのインスペクション ポリシー マップを削除し、変更を適用して、新しいインスペクション ポリシー マップをサービス ポリシーに再度追加する必要があります。
- インスペクション ポリシー マップには、複数のインスペクション クラス マップまたは直接照合を指定できます。

  1 つのパケットが複数の異なる照合 と一致する場合、ASA がアクションを適用する順序は、インスペクション ポリシー マップにアクションが追加された順序ではなく、ASA の内部ルールによって決まります。内部ルールは、アプリケーションのタイプとパケット解析の論理的進捗によって決まり、ユーザが設定することはできません。HTTP トラフィックの場合、Request Method フィールドの解析が Header Host Length フィールドの解析よりも先に行われ、Request Method フィールドに対するアクションは Header Host Length フィールドに対するアクションより先に行われます。

  アクションがパケットをドロップすると、インスペクション ポリシー マップではそれ以降のアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合、それ以降の一致基準との照合は行われません。最初のアクションがパケットのログへの記録である場合、接続のリセットなどの 2 番目のアクションは実行されます。

  パケットが、同じ複数の一致基準 と照合される場合は、ポリシー マップ内のそれらのコマンドの順序に従って照合されます。

  クラス マップは、そのクラス マップ内で重要度が最低の照合オプション（重要度は、内部ルールに基づきます）に基づいて、別のクラス マップまたは直接照合のと同じタイプであると判断されます。クラス マップに、別のクラス マップと同じタイプの重要度が最低の照合オプションがある場合、それらのクラス マップはポリシー マップに追加された順序で照合されます。クラス マップごとに最低重要度の照合が異なる場合は、最高重要度の照合オプションを持つクラス マップが最初に照合されます。

デフォルトのインスペクション ポリシー マップ

DNS インスペクションは、preset_dns_map インスペクション クラス マップを使用して、デフォルトでイネーブルになります。

- 最大 DNS メッセージ長は、512 バイトです。
- 最大クライアント DNS メッセージ長は、リソース レコードに一致するように自動的に設定されます。
- DNS ガードはイネーブルになり、ASA によって DNS 応答が転送されるとすぐに、ASA は DNS クエリーに関連付けられている DNS セッションを切断します。ASA はまた、メッセージ交換をモニタして DNS 応答の ID が DNS クエリーの ID と一致することを確認します。
- NAT の設定に基づく DNS レコードの変換はイネーブルです。
- プロトコルの強制はイネーブルであり、DNS メッセージ形式チェックが行われます。ドメイン名の長さが 255 文字以下、ラベルの長さが 63 文字、圧縮、ループ ポインタのチェックなどです。

（注）　**_default_esmtp_map** など、デフォルトのインスペクション ポリシー マップはほかにもあります。たとえば、ESMTP インスペクション ルールはポリシー マップ「_default_esmtp_map」を暗黙的に使用します。

インスペクション ポリシー マップのアクションの定義

サービス ポリシーでインスペクション エンジンをイネーブルにする場合は、インスペクション ポリシー マップで定義されるアクションを必要に応じてイネーブルにすることもできます。

手順の詳細

ステップ 1　（オプション）インスペクション クラス マップを作成します。または、ポリシー マップ内でトラフィックを直接特定できます。「インスペクション クラス マップ内のトラフィックの特定」（P.2-4）を参照してください。

ステップ 2　（オプション）正規表現をサポートするポリシー マップ タイプの場合は、正規表現を作成します。『一般的な操作のコンフィギュレーション ガイド』を参照してください。

ステップ 3　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] を選択します。

ステップ 4　設定するインスペクション タイプを選択します。

ステップ 5　[Add] をクリックして、新しいインスペクション ポリシー マップを追加します。

ステップ 6　インスペクションの章の該当するインスペクション タイプの手順に従います。

インスペクション クラス マップ内のトラフィックの特定

このタイプのクラス マップを使用して、アプリケーション固有の基準と照合できます。たとえば DNS トラフィックの場合は、DNS クエリー内のドメイン名と照合可能です。

クラス マップは、複数のトラフィック照合をグループ化します（match-all クラス マップ）。あるいはクラス マップで、照合リストのいずれかを照合できます（match-any クラス マップ）。クラス マップを作成することと、インスペクション ポリシー マップ内で直接トラフィック照合を定義することの違いは、クラス マップを使用して複数の match コマンドをグループ化できる点と、クラス マップを再使用できる点です。このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップで、接続のドロップ、リセット、またはロギングなどのアクションを指定できます。タイプの異なるトラフィックで異なるアクションを実行する場合は、ポリシー マップで直接トラフィックを指定してください。

制限事項

すべてのアプリケーションがインスペクション クラス マップをサポートするわけではありません。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Class Maps] を選択します。

ステップ 2　設定するインスペクション タイプを選択します。

ステップ 3　[Add] をクリックして、新しいインスペクション クラス マップを追加します。

ステップ 4　インスペクションの章の該当するインスペクション タイプの手順に従います。

次の作業

インスペクション ポリシーを使用するには、第 1 章「サービス ポリシー」を参照してください。

インスペクション ポリシー マップの機能履歴

表 2-1 に、この機能のリリース履歴を示します。

表 2-1　　サービス ポリシーの機能履歴

機能名	リリース	機能情報
インスペクション ポリシー マップ	7.2(1)	インスペクション ポリシー マップが導入されました。**class-map type inspect** コマンドが導入されました。
正規表現およびポリシー マップ	7.2(1)	インスペクション ポリシー マップで使用される正規表現およびポリシー マップが導入されました。**class-map type regex** コマンド、**regex** コマンド、および**match regex** コマンドが導入されました。

表 2-1　　サービス ポリシーの機能履歴 （続き）

機能名	リリース	機能情報
インスペクション ポリシー マップの match any	8.0(2)	インスペクション ポリシー マップで使用される **match any** キーワードが導入されました。トラフィックを 1 つ以上の基準に照合してクラス マップに一致させることができます。以前は、**match all** だけが使用可能でした。

インスペクション ポリシー マップの機能履歴

アクセス ルール

この章では、アクセス ルールを使用して ASA へのネットワーク アクセスや ASA を通過するネットワーク アクセスを制御する方法について説明します。ルーテッド ファイアウォール モードの場合もトランスペアレント ファイアウォール モードの場合も、ネットワーク アクセスを制御するには、アクセス ルールを使用します。トランスペアレント モードでは、アクセス ルール（レイヤ 3 トラフィックの場合）と EtherType ルール（レイヤ 2 トラフィックの場合）の両方を使用できます。

（注） また、ASA インターフェイスに管理アクセスの目的でアクセスするには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。『一般的な操作のコンフィギュレーション ガイド』に従って管理アクセスを設定することだけが必要です。

- 「ネットワーク アクセスの制御」（P.3-1）
- 「アクセス コントロールに関するガイドライン」（P.3-7）
- 「アクセス コントロールの設定」（P.3-7）
- 「アクセス ルールのモニタリング」（P.3-14）
- 「アクセス ルールの履歴」（P.3-15）

ネットワーク アクセスの制御

アクセス ルールは、ASA の通過を許可するトラフィックを定義したものです。複数の異なるレイヤのルールを組み合わせてアクセス コントロール ポリシーを実装できます。

- インターフェイスに割り当てられる拡張アクセス ルール（レイヤ 3 以上のトラフィック）：インバウンド方向とアウトバウンド方向のそれぞれで異なるルール セット（ACL）を適用できます。拡張アクセス ルールでは、送信元と宛先のトラフィックの基準に基づいてトラフィックが許可または拒否されます。
- グローバルに割り当てられる拡張アクセス ルール：デフォルトのアクセス コントロールとして使用する単一のグローバル ルール セットを作成できます。グローバル ルールはインターフェイス ルールの後に適用されます。
- 管理アクセス ルール（レイヤ 3 以上のトラフィック）：インターフェイス宛てのトラフィック（通常は管理トラフィック）を対象とする単一のルール セットを適用できます。これらのルールは、CLI の「コントロール プレーン」アクセス グループに相当します。デバイス宛ての ICMP トラフィックについては、代わりに ICMP ルールを設定できます。

- インターフェイスに割り当てられる EtherType ルール（レイヤ 2 のトラフィック）（トランスペアレント ファイアウォール モードのみ）：インバウンド方向とアウトバウンド方向のそれぞれで異なるルール セットを適用できます。EtherType ルールは、IP 以外のトラフィックのネットワーク アクセスを制御するルールです。EtherType ルールでは、EtherType に基づいてトラフィックが許可または拒否されます。

トランスペアレント ファイアウォール モードでは、拡張アクセス ルール、管理アクセス ルール、および EtherType ルールを組み合わせて同じインターフェイスに適用できます。

- 「ルールに関する一般情報」（P.3-2）
- 「拡張アクセス ルール」（P.3-5）
- 「EtherType ルール」（P.3-6）

ルールに関する一般情報

この項では、アクセス ルールと EtherType ルールの両方について説明します。次の項目を取り上げます。

- 「インターフェイス アクセス ルールとグローバル アクセス ルール」（P.3-2）
- 「インバウンド ルールとアウトバウンド ルール」（P.3-2）
- 「ルールの順序」（P.3-3）
- 「暗黙的な許可」（P.3-4）
- 「暗黙的な拒否」（P.3-4）
- 「NAT とアクセス ルール」（P.3-4）

インターフェイス アクセス ルールとグローバル アクセス ルール

アクセス ルールを特定のインターフェイスに適用するか、またはアクセス ルールをすべてのインターフェイスにグローバルに適用できます。インターフェイス アクセス ルールと一緒にグローバル アクセス ルールを設定できます。この場合、特定のインバウンド インターフェイス アクセス ルールが常に汎用のグローバル アクセス ルールよりも先に処理されます。グローバル アクセス ルールは、インバウンド トラフィックにだけ適用されます。

インバウンド ルールとアウトバウンド ルール

トラフィックの方向に基づいてアクセス ルールを設定できます。

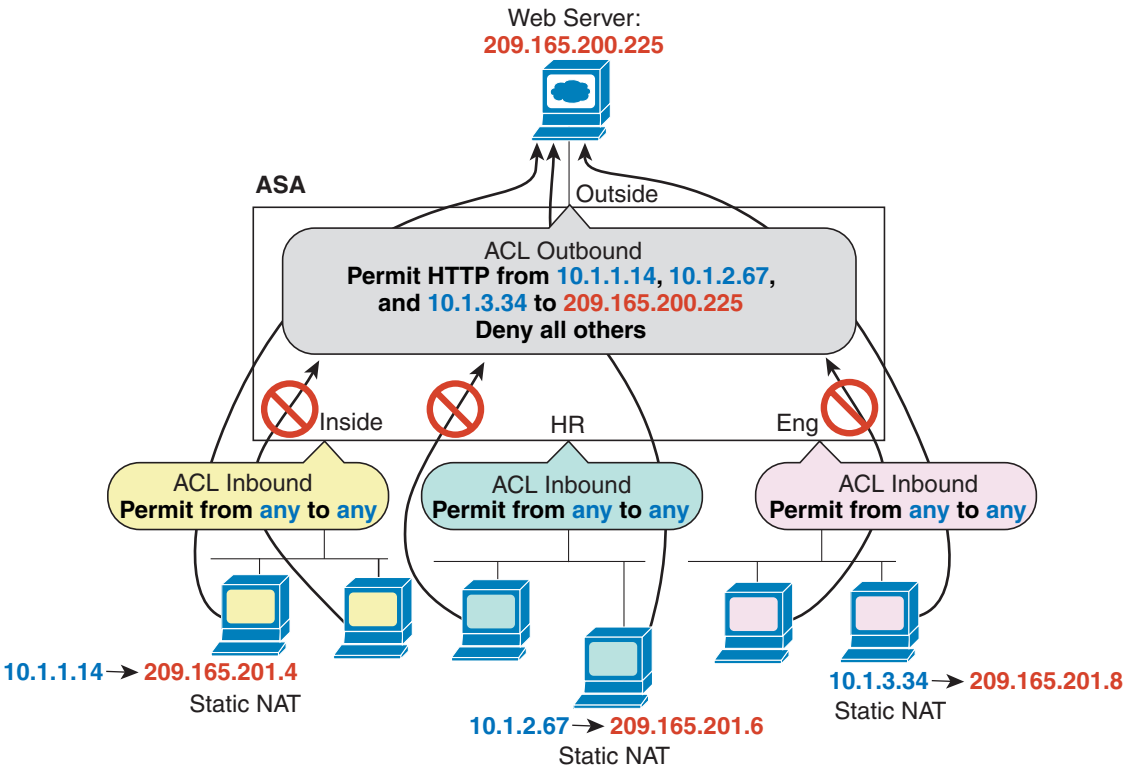
- インバウンド：インバウンド アクセス ルールは、インターフェイスに入ってくるトラフィックに適用されます。グローバル アクセス ルールおよび管理アクセス ルールは常にインバウンド ルールになります。
- アウトバウンド：アウトバウンド ルールは、インターフェイスから送信されるトラフィックに適用されます。

（注）　「インバウンド」および「アウトバウンド」は、インターフェイスにおける ACL の適用対象を表したもので、前者は、インターフェイスにおいて ASA により受信されるトラフィックに ACL が適用されることを表し、後者はインターフェイスにおいて ASA から送信されるトラフィックに ACL が適用されることを表しています。これらの用語は、一般にインバウンドと

呼ばれる、低セキュリティ インターフェイスから高セキュリティ インターフェイスへのトラフィックの移動や、一般にアウトバウンドと呼ばれる、高セキュリティ インターフェイスから低セキュリティ インターフェイスへのトラフィックの移動を意味しません。

たとえば、内部ネットワーク上の特定のホストに限って、外部ネットワーク上の Web サーバにアクセスできるようにする場合などには、アウトバウンド ACL が有用です。複数のインバウンド ACL を作成してアクセスを制限することもできますが、指定したホストだけアクセスを許可するアウトバウンド ACL を 1 つだけ作成する方が効率的です （次の図を参照）。このアウトバウンド ACL を使用すれば、その他のホストが外部ネットワークへアクセスすることもできなくなります。

図 3-1　　アウトバウンド ACL



ルールの順序

ルールの順序が重要です。ASA において、パケットを転送するかドロップするかの判断が行われる場合、ASA では、パケットと各ルールとの照合が、適用される ACL におけるそれらのルールの並び順に従って行われます。いずれかのルールに合致した場合、それ以降のルールはチェックされません。たとえば、先頭に作成したアクセス ルールが、インターフェイスに対してすべてのトラフィックを明示的に許可するものであれば、それ以降のルールはチェックされません。

暗黙的な許可

ルーテッド モードの場合、デフォルトでは次のタイプのトラフィックが許可されます。

- 高セキュリティ インターフェイスから低セキュリティ インターフェイスへの IPv4 および IPv6 のユニキャスト トラフィック。

トランスペアレント モードの場合、デフォルトでは次のタイプのトラフィックが許可されます。

- 高セキュリティ インターフェイスから低セキュリティ インターフェイスへの IPv4 および IPv6 のユニキャスト トラフィック。
- 双方向の ARP。ARP トラフィックの制御には ARP インスペクションを使用します。アクセス ルールでは制御できません。
- 双方向の BPDU。

他のトラフィックには、拡張アクセス ルール（IPv4 および IPv6）、または EtherType ルール（非 IP）のいずれかを使用する必要があります。

暗黙的な拒否

ACL の最後で暗黙的な拒否が設定されるため、明示的に許可しない限り、トラフィックは通過できません。たとえば、特定のアドレスを除くすべてのユーザに、ASA を通過してネットワークにアクセスすることを許可する場合、特定のアドレスを拒否したうえで、他のすべてのユーザを許可します。

EtherType ACL の場合、ACL の末尾にある暗黙的な拒否は、IP トラフィックや ARP には影響しません。たとえば、EtherType 8037 を許可する場合、ACL の末尾にある暗黙的な拒否によって、拡張 ACL で以前許可（または高セキュリティ インターフェイスから低セキュリティ インターフェイスへ暗黙的に許可）した IP トラフィックがブロックされることはありません。ただし、EtherType ルールですべてのトラフィックを明示的に拒否した場合は、IP と ARP のトラフィックが拒否され、物理的なプロトコルのトラフィック（自動ネゴシエーションなど）だけが許可されます。

グローバル アクセス ルールを設定すると、暗黙的な拒否はグローバル ルールが処理された*後*になります。次の動作の順序を参照してください。

1. インターフェイス アクセス ルール。
2. グローバル アクセス ルール。
3. 暗黙的な拒否。

NAT とアクセス ルール

アクセス ルールは、NAT を設定している場合でも、アクセス ルールの一致を決定する際に常に実際の IP アドレスを使用します。たとえば、内部サーバ 10.1.1.5 用の NAT を設定して、パブリックにルーティング可能な外部の IP アドレス 209.165.201.5 をこのサーバに付与する場合は、この内部サーバへのアクセスを外部トラフィックに許可するアクセス ルールの中で、サーバのマッピング アドレス（209.165.201.5）ではなく実際のアドレス（10.1.1.5）を参照する必要があります。

拡張アクセス ルール

この項では、拡張アクセス ルールについて説明します。

- 「リターン トラフィックに対する拡張アクセス ルール」（P.3-5）
- 「アクセス ルールを使用したトランスペアレント ファイアウォールを介したブロードキャストとマルチキャスト トラフィックの許可」（P.3-5）
- 「管理アクセス ルール」（P.3-6）

リターン トラフィックに対する拡張アクセス ルール

ルーテッド モードとトランスペアレント モードの両方に対する TCP 接続および UDP 接続については、リターン トラフィックを許可するためのアクセス ルールは必要ありません。ASA は、確立された双方向接続のリターン トラフィックをすべて許可します。

ただし、ICMP などのコネクションレス型プロトコルについては、ASA は単方向セッションを確立します。したがって、（ACL を送信元インターフェイスと宛先インターフェイスに適用することで）アクセス ルールで双方向の ICMP を許可するか、ICMP インスペクション エンジンをイネーブルにする必要があります。ICMP インスペクション エンジンは、ICMP セッションを双方向接続として扱います。

アクセス ルールを使用したトランスペアレント ファイアウォールを介したブロードキャストとマルチキャスト トラフィックの許可

ルーテッド ファイアウォール モードでは、ブロードキャストとマルチキャスト トラフィックは、アクセス ルールで許可されている場合でもブロックされます。これには、サポートされていないダイナミック ルーティング プロトコルおよび DHCP（DHCP リレーを設定している場合を除く）が含まれます。トランスペアレント ファイアウォール モードでは、すべての IP トラフィックの通過を許可できます。

（注）　これらの特殊なタイプのトラフィックはコネクションレス型であるため、アクセス ルールを両方のインターフェイスに適用して、リターン トラフィックの通過を許可する必要があります。

次の表に、トランスペアレント ファイアウォールの通過を許可できる一般的なトラフィック タイプを示します。

表 3-1　トランスペアレント ファイアウォールの特殊トラフィック

トラフィック タイプ	プロトコルまたはポート	注意
DHCP	UDP ポート 67 および 68	DHCP サーバがイネーブルの場合、ASA は DHCP パケットの通過を拒否します。
EIGRP	プロトコル 88	—
OSPF	プロトコル 89	—
マルチキャスト ストリーム	UDP ポートは、アプリケーションによって異なります。	マルチキャスト ストリームは、常に Class D アドレス（224.0.0.0 ～ 239.x.x.x）に送信されます。
RIP（v1 または v2）	UDP ポート 520	—

管理アクセス ルール

ASA 宛ての管理トラフィックを制御するアクセス ルールを設定できます。to-the-box 管理トラフィック（インターフェイスへの HTTP、Telnet、SSH などによる接続）に対するアクセス コントロール ルールは、管理アクセス ルールよりも優先されます。したがって、このような許可された管理トラフィックは、to-the-box ACL で明示的に拒否されている場合でも着信が許可されます。

また、デバイスへの ICMP トラフィックは、ICMP ルールを使用して制御できます。デバイスを通過する ICMP トラフィックの制御には、通常の拡張アクセス ルールを使用します。

EtherType ルール

この項では、EtherType ルールについて説明します。

- 「サポートされている EtherType およびその他のトラフィック」（P.3-6）
- 「リターン トラフィックに対する EtherType ルール」（P.3-6）
- 「MPLS の許可」（P.3-6）

サポートされている EtherType およびその他のトラフィック

EtherType ルールは次を制御します。

- 一般的なタイプの IPX および MPLS ユニキャストまたはマルチキャストを含む、16 ビットの 16 進数値で示された EtherType。
- イーサネット V2 フレーム。
- デフォルトで許可される BPDU。BPDU は、SNAP でカプセル化されており、ASA は特別に BPDU を処理するように設計されています。
- トランク ポート（シスコ専用）BPDU。トランク BPDU のペイロードには VLAN 情報が含まれるので、BPDU を許可すると、ASA により、発信 VLAN を使用してペイロードが修正されます。
- Intermediate System to Intermediate System（IS-IS）。

次のタイプのトラフィックはサポートされていません。

- 802.3 形式フレーム：type フィールドではなく length フィールドが使用されるため、ルールでは処理されません。

リターン トラフィックに対する EtherType ルール

EtherType はコネクションレス型であるため、トラフィックを両方向に通過させる必要がある場合は、両方のインターフェイスにルールを適用する必要があります。

MPLS の許可

MPLS を許可する場合は、ラベル配布プロトコルおよびタグ配布プロトコルの TCP 接続が ASA を経由して確立されるようにしてください。これには、ASA インターフェイス上の IP アドレスを LDP セッションまたは TDP セッションの router-id として使用するように、ASA に接続されている両方の MPLS ルータを設定します（LDP および TDP を使用することにより、MPLS ルータは、転送するパケットに使用するラベル（アドレス）をネゴシエートできるようになります）。

Cisco IOS ルータで、使用プロトコル（LDP または TDP）に適したコマンドを入力します。*interface* は、ASA に接続されているインターフェイスです。

```
hostname(config)# mpls ldp router-id interface force
```

または

```
hostname(config)# tag-switching tdp router-id interface force
```

アクセス コントロールに関するガイドライン

IPv6 のガイドライン

IPv6 をサポートします。（9.0 以降）送信元アドレスと宛先アドレスには IPv4 アドレスと IPv6 アドレスの組み合わせを含めることができます。9.0 よりも前のバージョンでは、別の IPv6 アクセス ルールを作成する必要があります。

ユーザごとの ACL のガイドライン

- ユーザごとの ACL では、**timeout uauth** コマンドの値が使用されますが、この値は AAA のユーザごとのセッション タイムアウト値で上書きできます。
- ユーザごとの ACL のためにトラフィックが拒否された場合、syslog メッセージ 109025 がログに記録されます。トラフィックが許可された場合、syslog メッセージは生成されません。ユーザごとの ACL の **log** オプションの効果はありません。

その他のガイドラインと制限事項

- オブジェクト グループ検索をイネーブルにすると、ルックアップのパフォーマンスは低下しますが、アクセス ルールの検索に必要なメモリを抑えることができます。オブジェクト グループ検索をイネーブルにした場合、ネットワーク オブジェクトは拡張されませんが、それらのグループの定義に基づいて一致するアクセス ルールが検索されます。このオプションを設定するには、アクセス ルール テーブルの下ある [Advanced] ボタンをクリックします。
- アクセス グループにトランザクション コミット モデルを使用することで、システムのパフォーマンスと信頼性を高めることができます。詳細については、『一般的な操作のコンフィギュレーション ガイド』の基本設定の章を参照してください。このオプションは、[Configurations] > [Device Management] > [Advanced] > [Rule Engine] にあります。
- ASDM では、ACL のルールの前にあるアクセス リストのコメントに基づいてルールの説明が設定されます。ASDM で新しいルールを作成した場合も、関連するルールの前にあるコメントが説明として設定されます。ただし、ASDM のパケット トレーサは、CLI の照合ルール後に設定されたコメントに一致します。

アクセス コントロールの設定

ここでは、アクセス コントロールを設定する方法について説明します。

- 「アクセス ルールの設定」（P.3-8）
- 「管理アクセス ルールの設定」（P.3-11）
- 「EtherType ルールの設定（トランスペアレント モードのみ）」（P.3-12）
- 「ICMP アクセス ルールの設定」（P.3-13）

アクセス ルールの設定

アクセス ルールを適用するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Firewall] > [Access Rules] の順に選択します。

ルールはインターフェイスおよび方向別に構成され、グローバル ルールはそれらとは別のグループにまとめられています。管理アクセス ルールを設定する場合は、このページで繰り返されます。これらのグループが、作成されてアクセス グループとしてインターフェイスまたはグローバルに割り当てられた拡張 ACL に相当します。それらの ACL も [ACL Manager] ページに表示されます。

ステップ 2　次のいずれかを実行します。

- 新しいルールを追加するには、[Add] > [Add Access Rule] の順に選択します。
- コンテナ内の特定の場所にルールを挿入するには、追加する場所の下にある既存のルールを選択して [Add] > [Insert] の順に選択するか、[Add] > [Insert After] の順に選択します。
- ルールを編集するには、ルールを選択し、[Edit] をクリックします。

ステップ 3　ルールのプロパティを入力します。選択する主なオプションを次に示します。

- [Interface]：ルールを適用するインターフェイスを指定します。グローバル ルールを作成する場合は [Any] を選択します。
- [Action]：[Permit] または [Deny]：対象のトラフィックを許可するか拒否（破棄）するかを指定します。
- [Source Criteria]/[Destination Criteria]：送信元（送信元アドレス）と宛先（トラフィック フローの送信先アドレス）を定義します。通常は、ネットワーク オブジェクトまたはネットワーク オブジェクト グループを使用して、ホストまたはサブネットの IPv4 アドレスまたは IPv6 アドレスを設定します。送信元については、ユーザ名またはユーザ グループ名を指定することも可能です。また、[Service] フィールドでトラフィックの種類を指定すると、すべての IP トラフィックではなく、特定のトラフィックを対象とするルールを作成できます。Trustsec を実装している場合は、セキュリティ グループを使用して送信元と宛先を定義できます。

使用可能なすべてのオプションの詳細については、「アクセス ルールのプロパティ」（P.3-8）を参照してください。

ルールの定義が完了したら、[OK] をクリックしてルール テーブルに追加します。

ステップ 4　[Apply] をクリックし、アクセス ルールを設定に保存します。

アクセス ルールのプロパティ

アクセス ルールを追加または編集するときに設定できるプロパティを次に示します。多くのフィールドでは、編集ボックスの右にある [...] ボタンをクリックして、そのフィールドに対応するオブジェクトを選択、作成、編集できます。

- [Interface]：ルールを適用するインターフェイスを指定します。グローバル ルールを作成する場合は [Any] を選択します。
- [Action]：[Permit] または [Deny]：対象のトラフィックを許可するか拒否（破棄）するかを指定します。

- [Source Criteria]：照合するトラフィックの送信元の特性を定義します。[Source] は必須ですが、それ以外のプロパティは省略可能です。
  - [Source]：送信元の IPv4 アドレスまたは IPv6 アドレスを指定します。デフォルトは **any** で、すべての IPv4 アドレスと IPv6 アドレスが対象になります。IPv4 だけを対象にするには **any4**、IPv6 だけを対象にするには **any6** を使用します。単一のホスト アドレス（10.100.10.5 や 2001:DB8::0DB8:800:200C:417A など）、サブネット（10.100.10.0/24 や 10.100.10.0/255.255.255.0 の形式、IPv6 の場合は 2001:DB8:0:CD30::/60）、ネットワーク オブジェクトまたはネットワーク オブジェクト グループの名前、インターフェイスの名前を指定できます。
  - [User]：アイデンティティ ファイアウォールをイネーブルにしている場合に、トラフィックの送信元としてユーザまたはユーザ グループを指定できます。ユーザが現在使用している IP アドレスがルールに一致します。ユーザ名（DOMAIN\user）、ユーザ グループ（DOMAIN\\group、グループ名の前に \ を 2 つ入力）、またはユーザ オブジェクト グループを指定できます。このフィールドでは、[...] をクリックすると、AAA サーバ グループから名前を選択できます。直接入力するよりもはるかに簡単です。
  - [Security Group]：Cisco TrustSec をイネーブルにしている場合に、セキュリティ グループの名前またはタグ（1 ～ 65533）、あるいはセキュリティ グループを指定できます。
  - [More Options] > [Source Service]：宛先サービスとして TCP または UDP を指定した場合に、必要に応じて、TCP、UDP、または TCP-UDP の事前定義済みのサービス オブジェクトを指定できます（独自のオブジェクトを使用することもできます）。通常は、宛先サービスだけを定義し、送信元サービスは定義しません。送信元サービスを定義する場合は、宛先サービスのプロトコルと一致する必要があることに注意してください（たとえば、ポートの定義に関係なく、どちらも TCP にするなど）。
- [Destination Criteria]：照合するトラフィックの送信先の特性を定義します。[Destination] は必須ですが、それ以外のプロパティは省略可能です。
  - [Destination]：送信先の IPv4 アドレスまたは IPv6 アドレスを指定します。デフォルトは **any** で、すべての IPv4 アドレスと IPv6 アドレスが対象になります。IPv4 だけを対象にするには **any4**、IPv6 だけを対象にするには **any6** を使用します。単一のホスト アドレス（10.100.10.5 や 2001:DB8::0DB8:800:200C:417A など）、サブネット（10.100.10.0/24 や 10.100.10.0/255.255.255.0 の形式、IPv6 の場合は 2001:DB8:0:CD30::/60）、ネットワーク オブジェクトまたはネットワーク オブジェクト グループの名前、インターフェイスの名前を指定できます。
  - [Security Group]：Cisco TrustSec をイネーブルにしている場合に、セキュリティ グループの名前またはタグ（1 ～ 65533）、あるいはセキュリティ グループを指定できます。
  - [Service]：トラフィックのプロトコル（IP、TCP、UDP など）を指定します。TCP および UDP の場合は、必要に応じてポートも指定します。デフォルトは IP ですが、特定のプロトコルを選択することで対象のトラフィックを絞り込むことができます。通常は、サービス オブジェクトのタイプを選択します。TCP および UDP の場合はポートも指定できます。たとえば、tcp/80、tcp/http、tcp/10-20（ポートの範囲）、tcp-udp/80（ポート 80 の TCP と UDP のすべてのトラフィック）のように指定できます。
- [Description]：ルールの目的の説明を入力します。1 行の最大文字数は 100 文字までで、複数行を入力できます。CLI では、各行がコメントとして追加され、ルールの前に配置されます。

（注） 1 つのプラットフォーム（Windows など）上で英語以外の文字でコメントを追加し、それらの文字を別のプラットフォーム（Linux など）から削除しようとした場合、元の文字が正しく認識されないため編集や削除を実行できない可能性があります。この制限は、各種言語の文字をさまざまな方法でエンコードするプラットフォームの依存性によるものです。

- [Enable Logging]、[Logging Level]、[More Options] > [Logging Interval]：ルールに対する syslog メッセージの生成方法を定義します。これらのロギング オプションは、次のように実装できます。
  - [Enable Logging] を選択解除：ルールのロギングがディセーブルになります。このルールに一致するトラフィックに対して、どのタイプの syslog メッセージも発行されません。
  - [Enable Logging] を選択、[Logging Level] が [Default]：ルールに対してデフォルトのロギングが行われます。パケットが拒否されるたびに、syslog メッセージ 106023 が発行されます。アプライアンスが攻撃を受けると、このメッセージが頻繁に発行され、サービスに影響を及ぼす可能性があります。
  - [Enable Logging] を選択、[Logging Level] が [Default] 以外 : syslog メッセージ 106023 の代わりに、まとめて 106100 が発行されます。メッセージ 106100 は、最初のヒットがあったときに発行され、それ以降は [More Options] > [Logging Interval] で設定された間隔（デフォルトは 300 秒、1 ～ 600 秒の範囲で指定可能）で発行されてその間のヒット数を示します。推奨されるロギング レベルは [Informational] です。

    拒否メッセージをまとめることで、攻撃による影響を軽減し、メッセージを分析しやすくなります。サービス拒否攻撃を受けた場合、メッセージ 106100 のヒット数を特定するために使用される拒否フローのキャッシュ数が間隔あたりの最大数を超えたことを示すメッセージ 106101 が表示されることがあります。この場合、攻撃を軽減するために、次の間隔の開始時点まで統計情報の収集が停止されます。
- [More Options] > [Traffic Direction]：ルールの方向（[In] または [Out]）を指定します。デフォルトは [In] で、グローバル アクセス ルールと管理アクセス ルールではこのオプションしか選択できません。
- [More Options] > [Enable Rule]：ルールをデバイスでアクティブにするかどうかを指定します。ディセーブルにしたルールは、ルール テーブルに取り消し線付きで表示されます。ルールをディセーブルにすると、削除せずにトラフィックへの適用を停止できるので、後で必要になったときに再度イネーブルにすることができます。
- [More Options] > [Time Range]：ルールをアクティブにする時間帯や曜日を定義した時間範囲オブジェクトの名前を指定します。時間範囲を指定しない場合、ルールは常にアクティブになります。

アクセス ルールの詳細オプションの設定

アクセス ルールの詳細オプションを使用して、ルールの動作の一部をカスタマイズすることができます。ただし、これらのオプションは、ほとんどの場合に適切に動作するようにデフォルトで設定されています。

ステップ 1　[Configuration] > [Firewall] > [Access Rules] の順に選択します。

ステップ 2　ルール テーブルの下にある [Advanced] ボタンをクリックします。

ステップ 3　次のオプションを必要に応じて設定します。

- [Advanced Logging Settings]：デフォルト以外のロギングを設定すると、メッセージ 106100 の統計情報を得るために拒否フローがキャッシュされます（「アクセス ルールの syslog メッセージの評価」（P.3-14）を参照）。メモリおよび CPU リソースが無制限に消費されないようにするために、ASA は同時拒否フロー数に制限を設定します。これは、拒否フローが攻撃を示している可能性があるためです。この制限に達すると、メッセージ 106101 が発行されます。106101 について以下を設定できます。
  - [Maximum Deny-flows]：ASA によりフローのキャッシュが停止される前に許可される拒否フローの最大数を、1 ～ 4096 の範囲で指定します。デフォルトは 4096 です。

– [Alert Interval]：拒否フローが最大数に達したことを示すシステム ログ メッセージ 106101 が発行される時間間隔（1 ～ 3600 秒）を指定します。デフォルトは 300 秒です。

- [Per User Override] テーブル：ユーザの認証用に RADIUS サーバからダウンロードしたダイナミック ユーザ ACL をインターフェイスに割り当てられた ACL よりも優先するかどうかを指定します。たとえば、インターフェイス ACL が 10.0.0.0 からのトラフィックをすべて拒否し、ダイナミック ACL が 10.0.0.0 からのトラフィックをすべて許可する場合、そのユーザに関しては、ダイナミック ACL によってインターフェイス ACL が上書きされます。ユーザの上書きを許可する各インターフェイスについて、[Per User Override] チェックボックスをオンにします（インバウンド方向のみ）。ユーザごとの上書き機能がディセーブルになると、RADIUS サーバによって提供されるアクセス ルールは、そのインターフェイス上で設定されたアクセス ルールと結合されます。

  デフォルトでは、VPN リモート アクセス トラフィックはインターフェイス ACL と照合されません。ただし、[Enable inbound VPN sessions to bypass interface access lists] 設定（[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] ペイン）の選択を解除した場合は、グループ ポリシーで VPN フィルタが適用されているかどうか（[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [General] > [More Options] > [Filter] フィールド）、および [Per User Override] オプションを設定しているかどうかによって動作が異なります。

  – [Per User Override] なし、VPN フィルタなし：トラフィックはインターフェイス ACL と照合されます。

  – [Per User Override] なし、VPN フィルタ：トラフィックはまずインターフェイス ACL と照合され、次に VPN フィルタと照合されます。

  – [Per User Override]、VPN フィルタ：トラフィックは VPN フィルタのみと照合されます。

- [Object Group Search Setting]：[Enable Object Group Search Algorithm] を選択すると、ルックアップのパフォーマンスは低下しますが、オブジェクト グループを使用するアクセス ルールの検索に必要なメモリを抑えることができます。オブジェクト グループ検索をイネーブルにした場合、ネットワーク オブジェクトは拡張されませんが、それらのグループの定義に基づいて一致するアクセス ルールが検索されます。

ステップ 4　[OK] をクリックします。

管理アクセス ルールの設定

特定のピア（または複数のピア）から ASA への to-the-box 管理トラフィックを制御するインターフェイス ACL を設定できます。このタイプの ACL は、IKE DoS（サービス拒絶）攻撃をブロックする場合などに有用です

to-the-box トラフィックのパケットを許可または拒否する拡張 ACL を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [Management Access Rules] を選択します。

ルールはインターフェイス別に構成されています。各グループが、作成されてコントロール プレーン ACL としてインターフェイスに割り当てられた拡張 ACL に相当します。それらの ACL も [Access Rules] ページおよび [ACL Manager] ページに表示されます。

ステップ 2　次のいずれかを実行します。

- 新しいルールを追加するには、[Add] > [Add Management Access Rule] の順に選択します。

- コンテナ内の特定の場所にルールを挿入するには、追加する場所の下にある既存のルールを選択して [Add] > [Insert] の順に選択するか、[Add] > [Insert After] の順に選択します。
- ルールを編集するには、ルールを選択し、[Edit] をクリックします。

ステップ 3　ルールのプロパティを入力します。選択する主なオプションを次に示します。

- [Interface]：ルールを適用するインターフェイスを指定します。
- [Action]：[Permit] または [Deny]：対象のトラフィックを許可するか拒否（破棄）するかを指定します。
- [Source Criteria]/[Destination Criteria]：送信元（送信元アドレス）と宛先（トラフィック フローの送信先アドレス）を定義します。通常は、ネットワーク オブジェクトまたはネットワーク オブジェクト グループを使用して、ホストまたはサブネットの IPv4 アドレスまたは IPv6 アドレスを設定します。送信元については、ユーザ名またはユーザ グループ名を指定することも可能です。また、[Service] フィールドでトラフィックの種類を指定すると、すべての IP トラフィックではなく、特定のトラフィックを対象とするルールを作成できます。Trustsec を実装している場合は、セキュリティ グループを使用して送信元と宛先を定義できます。

使用可能なすべてのオプションの詳細については、「アクセス ルールのプロパティ」（P.3-8）を参照してください。

ルールの定義が完了したら、[OK] をクリックしてルール テーブルに追加します。

ステップ 4　[Apply] をクリックし、ルールを設定に保存します。

EtherType ルールの設定（トランスペアレント モードのみ）

EtherType ルールは、トランスペアレント ファイアウォール モードの IP 以外のレイヤ 2 トラフィックに適用されます。これらのルールを使用して、レイヤ 2 パケット内の EtherType 値に基づいてトラフィックを許可または破棄できます。EtherType ルールでは、ASA を経由する IP 以外のトラフィックのフローを制御できます。

トランスペアレント モードでは、拡張アクセス ルールと EtherType アクセス ルールの両方をインターフェイスに適用できます。EtherType ルールは、拡張アクセス ルールに優先されます。

EtherType ルールを追加するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [EtherType Rules] を選択します。

ルールはインターフェイスおよび方向別に構成されています。各グループが、作成されてインターフェイスに割り当てられた EtherType ACL に相当します。

ステップ 2　次のいずれかを実行します。

- 新しいルールを追加するには、[Add] > [Add EtherType Rule] の順に選択します。
- コンテナ内の特定の場所にルールを挿入するには、追加する場所の下にある既存のルールを選択して [Add] > [Insert] の順に選択するか、[Add] > [Insert After] の順に選択します。
- ルールを編集するには、ルールを選択し、[Edit] をクリックします。

ステップ 3　ルールのプロパティを入力します。選択する主なオプションを次に示します。

- [Interface]：ルールを適用するインターフェイスを指定します。
- [Action]：[Permit] または [Deny]：対象のトラフィックを許可するか拒否（破棄）するかを指定します。

- [EtherType]：次のオプションを使用してトラフィックを照合できます。
  - **ipx**：Internet Packet Exchange（IPX）。
  - **bpdu**：ブリッジ プロトコル データ ユニット。デフォルトで許可されます。
  - **mpls-multicast**：MPLS マルチキャスト。
  - **mpls-unicast**：MPLS ユニキャスト。
  - **isis**：Intermediate System to Intermediate System（IS-IS）。
  - **any**：すべてのトラフィック。
  - *hex_number*：16 ビットの 16 進数値（0x600 ～ 0xffff）で示された任意の EtherType。EtherType のリストについては、http://www.ietf.org/rfc/rfc1700.txt にアクセスして、RFC 1700「Assigned Numbers」を参照してください。
- [Description]：ルールの目的の説明を入力します。1 行の最大文字数は 100 文字までで、複数行を入力できます。CLI では、各行がコメントとして追加され、ルールの前に配置されます。
- [More Options] > [Direction]：ルールの方向（[In] または [Out]）を指定します。デフォルトは [In] です。

ルールの定義が完了したら、[OK] をクリックしてルール テーブルに追加します。

ステップ 4　[Apply] をクリックし、ルールを設定に保存します。

ICMP アクセス ルールの設定

デフォルトでは、IPv4 または IPv6 を使用して任意の ASA インターフェイスに ICMP パケットを送信できます。ただし、次の例外があります。

- ASA は、ブロードキャスト アドレス宛ての ICMP エコー要求に応答しません。
- ASAは、トラフィックが着信するインターフェイス宛ての ICMP トラフィックにのみ応答します。ICMP トラフィックは、インターフェイス経由で離れたインターフェイスに送信できません。

デバイスを攻撃から保護するために、ICMP ルールを使用して、ASA インターフェイスへの ICMP アクセスを特定のホスト、ネットワーク、または ICMP タイプに限定できます。ICMP ルールにはアクセス ルールと同様に順序があり、パケットに最初に一致したルールの処理が適用されます。

インターフェイスに対して any ICMP ルールを設定すると、ICMP ルールのリストの最後に暗黙の deny ICMP ルールが追加され、デフォルトの動作が変更されます。そのため、一部のメッセージ タイプだけを拒否する場合は、残りのメッセージ タイプを許可するように ICMP ルールのリストの最後に permit any ルールを含める必要があります。

ICMP 到達不能メッセージ タイプ（タイプ 3）の権限を常に付与することを推奨します。ICMP 到達不能メッセージを拒否すると、ICMP パス MTU ディスカバリがディセーブルになって、IPSec および PPTP トラフィックが停止することがあります。また、IPv6 の ICMP パケットは、IPv6 のネイバー探索プロセスに使用されます。パス MTU ディスカバリの詳細については、RFC 1195 および RFC 1435 を参照してください。

手順

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [ICMP] を選択します。

ステップ 2　ICMP ルールを設定します。

a. ルールを追加する（[Add] > [Rule]、[Add] > [IPv6 Rule]、または [Add] > [Insert]）か、ルールを選択して編集します。

b. 制御する ICMP タイプを選択します。すべてのタイプに適用する場合は **any** を選択します。

c. ルールを適用するインターフェイスを選択します。各インターフェイスに対して個別にルールを作成する必要があります。

d. 一致したトラフィックに対してアクセスを許可するか拒否するかを選択します。

e. すべてのトラフィックにルールを適用する場合は、[Any Address] を選択します。特定のホストまたはネットワークを制御する場合は、アドレスとマスク（IPv4 の場合）またはアドレスとプレフィックス長（IPv6 の場合）を入力します。

f. [OK] をクリックします。

ステップ 3　（オプション）ICMP の到達不能メッセージに対する制限は、次の各オプションを使用して設定します。ASA をホップの 1 つとして表示するトレース ルートに対して ASA の通過を許可するためには、サービス ポリシーで [Decrement time to live for a connection] オプション（[Configuration] > [Firewall] > [Service Policy Rules] > [Rule Actions] > [Connection Settings] ダイアログボックス）をイネーブルにするほか、レート制限を大きくする必要があります。

- [Rate Limit]：到達不能メッセージのレート制限を、1 秒あたり 1 ～ 100 の範囲で設定します。デフォルトは、1 秒あたり 1 メッセージです。
- [Burst Size]：バースト レートを 1 ～ 10 の範囲で設定します。このキーワードは、現在システムで使用されていないため、任意の値を選択できます。

ステップ 4　[Apply] をクリックします。

アクセス ルールのモニタリング

[Access Rules] ページに各ルールのヒット数が表示されます。ヒット数にカーソルを合わせると、その更新時間と間隔が表示されます。ヒット数をリセットするには、ルールを右クリックして [Clear Hit Count] を選択します。これを実行すると、同じ方向の同じインターフェイスに適用されているすべてのルールのヒット数が消去されることに注意してください。

アクセス ルールの syslog メッセージの評価

アクセス ルールに関するメッセージは、syslog イベントのビューア（ASDM のビューアなど）を使用して確認できます。

デフォルトのロギングを使用している場合、明示的に拒否されたフローに対する syslog メッセージ 106023 だけが表示されます。ルールのリストの最後にある「暗黙の deny」に一致するトラフィックは記録されません。

ASA が攻撃を受けた場合、拒否されたパケットを示す syslog メッセージの数が非常に大きくなることがあります。代わりに、syslog メッセージ 106100 を使用するロギングをイネーブルにすることをお勧めします。このメッセージは各ルール（許可ルールも含む）の統計情報を示すもので、これを使用することにより、生成される syslog メッセージの数を制限できます。また、特定のルールについて、すべてのロギングをディセーブルにする方法もあります。

メッセージ 106100 のロギングがイネーブルで、パケットが ACE と一致した場合、ASA はフロー エントリを作成して、指定された時間内で受信したパケットの数を追跡します。ASA は、最初のヒットがあったとき、および各間隔の終わりに syslog メッセージを生成し、その間隔におけるヒットの合計数と最後のヒットのタイムスタンプを示します。各間隔の終わりに、ASA はヒット数を 0 にリセットします。1 つの間隔内で ACE と一致するパケットがなかった場合、ASA はそのフロー エントリを削除します。ルールのロギングの設定では、それぞれのルールについて、ログ メッセージの間隔のほか、重大度も制御することができます。

フローは、送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびポートで定義されます。同じ 2 つのホスト間の新しい接続では、送信元ポートが異なる場合があるため、接続のための新しいフローが作成されると、同じフローの増加は示されない場合があります。

確立された接続に属する、許可されたパケットを ACL でチェックする必要はありません。最初のパケットだけがロギングされ、ヒット数に含められます。ICMP などのコネクションレス型プロトコルの場合は、許可されているパケットもすべてロギングされ、拒否されたパケットはすべてロギングされます。

これらのメッセージの詳細については、*syslog メッセージ ガイド*を参照してください。

ヒント　メッセージ 106100 のロギングがイネーブルで、パケットが ACE と一致した場合、ASA はフロー エントリを作成して、指定された時間内で受信したパケットの数を追跡します。ASA では、ACE 用のロギング フローを最大 32 K 保持できます。どの時点でも大量のフローが同時に存在する可能性があります。メモリおよび CPU リソースが無制限に消費されないようにするために、ASA は同時*拒否*フロー数に制限を設定します。この制限は、拒否フローに対してだけ設定されます（許可フローには設定されません）。これは、拒否フローは攻撃を示している可能性があるためです。制限に達すると、ASA は既存の拒否フローが期限切れになるまでロギング用の新しい拒否フローを作成せず、メッセージ 106101 を発行します。このメッセージの頻度、および拒否フローのキャッシュの最大数は、詳細設定で制御できます。「アクセス ルールの詳細オプションの設定」（P.3-10）を参照してください。

アクセス ルールの履歴

機能名	プラットフォーム リリース	説明
インターフェイス アクセス ルール	7.0(1)	ACL を使用した、ASA 経由のネットワーク アクセスの制御。 次の画面が導入されました。[Configuration] > [Firewall] > [Access Rules]。
グローバル アクセス ルール	8.3(1)	グローバル アクセス ルールが導入されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Access Rules]。

機能名	プラットフォーム リリース	説明
アイデンティティ ファイアウォールのサポート	8.4(2)	アイデンティティ ファイアウォールのユーザおよびグループを発信元と宛先に使用できるようになりました。アイデンティティ ファイアウォール ACL はアクセス ルールや AAA ルールとともに、および VPN 認証に使用できます。
EtherType ACL が IS-IS トラフィックをサポート	8.4(5)、9.1(2)	トランスペアレント ファイアウォール モードでは、ASA が EtherType ACL を使用して IS-IS トラフィックを渡すことができるようになりました。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [EtherType Rules]。
TrustSec のサポート	9.0(1)	TrustSec セキュリティ グループを送信元と宛先に使用できるようになりました。アイデンティティ ファイアウォール ACL をアクセス ルールとともに使用できます。
IPv4 および IPv6 の統合 ACL	9.0(1)	ACL で IPv4 および IPv6 アドレスがサポートされるようになりました。送信元および宛先に対して IPv4 および IPv6 アドレスの組み合わせも指定できます。**any** キーワードは、IPv4 および IPv6 トラフィックを表すように変更されました。IPv4 のみのトラフィックを表す **any4** キーワードと、IPv6 のみのトラフィックを表す **any6** キーワードが追加されました。IPv6 固有の ACL は非推奨です。既存の IPv6 ACL は拡張 ACL に移行されます。移行の詳細については、リリース ノートを参照してください。 次の画面が変更されました。 [Configuration] > [Firewall] > [Access Rules] [Configuration] > [Remote Access VPN] > [Network（Client）Access] > [Group Policies] > [General] > [More Options]
ICMP コードによって ICMP トラフィックをフィルタリングするための拡張 ACL とオブジェクト機能拡張	9.0(1)	ICMP コードに基づいて ICMP トラフィックの許可または拒否ができるようになりました。 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] [Configuration] > [Firewall] > [Access Rule]
アクセス グループ ルール エンジンのトランザクション コミット モデル	9.1(5)	イネーブルにすると、ルールのコンパイルの完了後に、ルールの照合パフォーマンスに影響を及ぼすことなくルールの更新が適用されます。 次の画面が導入されました。[Configuration] > [Device Management] > [Advanced] > [Rule Engine]。

公開サーバ

ここでは、公開サーバを設定する方法について説明します。

- 「公開サーバに関する情報」（P.4-1）
- 「公開サーバのライセンス要件」（P.4-1）
- 「ガイドラインと制限事項」（P.4-2）
- 「スタティック NAT をイネーブルにする公開サーバの追加」（P.4-2）
- 「PAT を設定したスタティック NAT をイネーブルにする公開サーバの追加」（P.4-3）
- 「公開サーバの設定の編集」（P.4-3）
- 「公開サーバの機能履歴」（P.4-4）

公開サーバに関する情報

[Public Servers] ペインを使用して、管理者は内部ユーザおよび外部ユーザにさまざまなアプリケーション サーバへのアクセスを提供できます。このペインには公開サーバのリスト、内部および外部アドレス、内部および外部アドレスが適用されるインターフェイス、アドレスを変換する機能、および公開されるサービスが表示されます。既存の公開サーバを追加、編集、削除、または変更できます。

公開サーバのライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

スタティック NAT をイネーブルにする公開サーバの追加

スタティック NAT をイネーブルにする公開サーバを追加し、実際のアドレスからマッピング アドレスへの固定変換を作成するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Public Servers] ペインで、[Add] をクリックして新しいサーバを追加します。

[Add Public Server] ダイアログボックスが表示されます。

ステップ 2　[Private Interface] ドロップダウン メニューで、実サーバの接続先であるプライベート インターフェイスの名前を選択します。

ステップ 3　[Private IP address] フィールドに、サーバの実際の IP アドレスを入力します（IPv4 のみ）。

ステップ 4　[Private Service] フィールドで、[Browse] をクリックして [Browse Service] ダイアログボックスを表示し、外部に公開される実際のサービスを選択して、[OK] をクリックします。

必要に応じて、[Browse Service] ダイアログボックスで [Add] をクリックして、新しいサービスまたはサービス グループを作成できます。各種ポートから複数のサービスを外部に開くことができます。サービス オブジェクトおよびサービス グループの詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

ステップ 5　[Public Interface] ドロップダウン メニューで、外部のユーザが実サーバにアクセスするために使用するインターフェイスを入力します。

ステップ 6　[Public Address] フィールドで、サーバのマッピング IP アドレスを入力します。これは外部ユーザに表示されるアドレスです。

ステップ 7　（オプション）スタティック PAT をイネーブルにするには、[Specify if Public Service is different from private service] チェックボックスをオンにします。

ステップ 8　[OK] をクリックします。メイン ペインに設定内容が表示されます。

ステップ 9　[Apply] をクリックして、スタティック NAT およびトラフィック フローの対応するアクセス ルールを生成し、設定を保存します。

スタティック NAT の詳細については、「スタティック NAT について」（P.5-3）を参照してください。

PAT を設定したスタティック NAT をイネーブルにする公開サーバの追加

実際のプロトコルとマッピング プロトコル（TCP または UDP）を指定できる公開サーバを追加するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Public Servers] を選択して、[Add] をクリックします。

[Add Public Server] ダイアログボックスが表示されます。

ステップ 2　[Private Interface] ドロップダウン メニューで、実サーバの接続先であるプライベート インターフェイスの名前を選択します。

ステップ 3　[Private IP address] フィールドに、サーバの実際の IP アドレスを入力します（IPv4 のみがサポートされます）。

ステップ 4　[Private Service] フィールドで、[Browse] をクリックして [Browse Service] ダイアログボックスを表示します。

ステップ 5　外部に公開される実際のサービスを選択して、[OK] をクリックします。

必要に応じて、[Browse Service] ダイアログボックスで [Add] をクリックして、新しいサービスまたはサービス グループを作成します。各種ポートから複数のサービスを外部に開くことができます。サービス オブジェクトおよびサービス グループの詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

ステップ 6　[Public Interface] ドロップダウン メニューで、外部のユーザが実サーバにアクセスするために使用するインターフェイスを入力します。

ステップ 7　[Public Address] フィールドで、サーバのマッピング IP アドレスを入力します。これは外部ユーザに表示されるアドレスです。

ステップ 8　[Specify Public Service if different from Private Service] チェックボックスをオンにして、スタティック PAT をイネーブルにします。

ステップ 9　[Public Service] フィールドで、マッピング プロトコル（TCP または UDP のみ）を入力するか、[Browse] をクリックしてリストからプロトコルを選択します。

ステップ 10　[OK] をクリックします。

ステップ 11　[Apply] をクリックして、PAT が設定されたスタティック NAT およびトラフィック フローの対応するアクセス ルールを生成し、設定を保存します。

ポート アドレス変換が設定されたスタティック NAT の詳細については、「ポート変換を設定したスタティック NAT」（P.5-4）を参照してください。

公開サーバの設定の編集

公開サーバの設定を編集するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Public Servers] の順に選択し、既存の公開サーバを選択して、[Edit] をクリックします。

[Edit Public Server] ダイアログボックスが表示されます。

ステップ 2　次の設定に必要な変更を行います。

- [Private Interface]：実サーバが接続されるインターフェイスです。
- [Private IP Address]：サーバの実際の IP アドレスです。
- [Private Service]：実サーバで実行されている実際のサービスです。
- [Public Interface]：外部ユーザが実サーバにアクセスするために使用するインターフェイスです。
- [Public Address]：外部ユーザに表示される IP アドレスです。
- [Public Service]：変換後のアドレスで実行されているサービスです。サポートされる公共サービスに関する情報を表示するには、[Information] アイコンをクリックします。

ステップ 3　[OK]、[Apply] の順にクリックし、変更内容を保存します。

公開サーバの機能履歴

表 4-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 4-1　公開サーバの機能履歴

機能名	プラットフォーム リリース	機能情報
公開サーバ	8.3(1)	公開サーバでは、内部ユーザおよび外部ユーザにさまざまなアプリケーション サーバへのアクセスを提供します。 次の画面が導入されました。 [Configuration] > [Firewall] > [Public Servers]

PART 2

ネットワーク アドレス変換

CHAPTER 5

ネットワーク アドレス変換（NAT）（ASA 8.3 以降）

この章では、ネットワーク アドレス変換（NAT）が ASA でどのように機能するかについて説明します。

- 「NAT を使用する理由」（P.5-1）
- 「NAT の用語」（P.5-2）
- 「NAT タイプ」（P.5-3）
- 「ルーテッド モードとトランスペアレント モードの NAT」（P.5-12）
- 「NAT と IPv6」（P.5-15）
- 「NAT の実装方法」（P.5-15）
- 「NAT ルールの順序」（P.5-20）
- 「NAT インターフェイス」（P.5-21）
- 「NAT パケットのルーティング」（P.5-22）
- 「VPN の NAT」（P.5-26）
- 「DNS および NAT」（P.5-32）
- 「次の作業」（P.5-37）

（注） NAT の設定を開始するには、第 6 章「ネットワーク オブジェクト NAT（ASA 8.3 以降）」または第 7 章「Twice NAT（ASA 8.3 以降）」を参照してください。

NAT を使用する理由

IP ネットワーク内の各コンピュータおよびデバイスには、ホストを識別する固有の IP アドレスが割り当てられています。パブリック IPv4 アドレスが不足しているため、これらの IP アドレスの大部分はプライベートであり、プライベートの企業ネットワークの外部にルーティングできません。RFC 1918 では、アドバタイズされない、内部で使用できるプライベート IP アドレスが次のように定義されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

NAT の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。NAT は、プライベート IP アドレスをパブリック IP に置き換え、内部プライベート ネットワーク内のプライベート アドレスをパブリック インターネットで使用可能な正式の、ルーティング可能なアドレスに変換します。このようにして、NAT はパブリック アドレスを節約します。これは、ネットワーク全体に対して 1 つのパブリック アドレスだけを外部に最小限にアドバタイズするように NAT を設定できるからです。

NAT の他の機能は、次のとおりです。

- セキュリティ：内部 IP アドレスを隠蔽し、直接攻撃を防止します。
- IP ルーティング ソリューション：NAT を使用する際は、重複 IP アドレスが問題になりません。
- 柔軟性 : 外部で使用可能なパブリック アドレスに影響を与えずに、内部 IP アドレッシング スキームを変更できます。たとえば、インターネットにアクセス可能なサーバの場合、インターネット用に固定 IP アドレスを維持できますが、内部的にはサーバのアドレスを変更できます。
- IPv4 と IPv6（ルーテッド モードのみ）の間の変換（バージョン 9.0(1) 以降）：IPv4 ネットワークに IPv6 ネットワークを接続する場合は、NAT を使用すると、2 つのタイプのアドレス間で変換を行うことができます。

（注） NAT は必須ではありません。特定のトラフィック セットに NAT を設定しない場合、そのトラフィックは変換されませんが、セキュリティ ポリシーはすべて通常どおりに適用されます。

NAT の用語

このマニュアルでは、次の用語を使用しています。

- 実際のアドレス/ホスト/ネットワーク/インターフェイス：実際のアドレスとは、ホストで定義されている、変換前のアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、内部ネットワークが「実際の」ネットワークになります。内部ネットワークだけではなく、ASA に接続されている任意のネットワークを変換できます。したがって、外部アドレスを変換するように NAT を設定した場合、「実際の」は、外部ネットワークが内部ネットワークにアクセスしたときの外部ネットワークを指します。
- マッピング アドレス/ホスト/ネットワーク/インターフェイス：マッピング アドレスとは、実際のアドレスが変換されるアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、外部ネットワークが「マッピング」ネットワークになります。

（注） アドレスの変換中、ASA のインターフェイスに存在する IP アドレスは変換されません。

- 双方向の開始：スタティック NAT では、*双方向に*開始できます。つまり、ホストへの接続とホストからの接続の両方を開始できます。
- 送信元および宛先の NAT：任意のパケットについて、送信元 IP アドレスと宛先 IP アドレスの両方を NAT ルールと比較し、1 つまたは両方を変換する、または変換しないことができます。スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。

NAT タイプ

次のトピックで、さまざまなタイプの NAT について説明します。

- 「NAT のタイプの概要」（P.5-3）
- 「スタティック NAT」（P.5-3）
- 「ダイナミック NAT」（P.5-8）
- 「ダイナミック PAT」（P.5-10）
- 「アイデンティティ NAT」（P.5-12）

NAT のタイプの概要

NAT は、次の方法を使用して実装できます。

- スタティック NAT：実際の IP アドレスとマッピング IP アドレスとの間での一貫したマッピング。双方向にトラフィックを開始できます。「スタティック NAT」（P.5-3）を参照してください。
- ダイナミック NAT：実際の IP アドレスのグループが、（通常は、より小さい）マッピング IP アドレスのグループに先着順でマッピングされます。実際のホストだけがトラフィックを開始できます。「ダイナミック NAT」（P.5-8）を参照してください。
- ダイナミック ポート アドレス変換（PAT）：実際の IP アドレスのグループが、1 つの IP アドレスにマッピングされます。この IP アドレスの一意の送信元ポートが使用されます。「ダイナミック PAT」（P.5-10）を参照してください。
- アイデンティティ NAT：実際のアドレスが同一アドレスにスタティックに変換され、基本的に NAT をバイパスします。大規模なアドレスのグループを変換するものの、小さいアドレスのサブセットは免除する場合は、NAT をこの方法で設定できます。「アイデンティティ NAT」（P.5-12）を参照してください。

スタティック NAT

次のトピックでは、スタティック NAT について説明します。

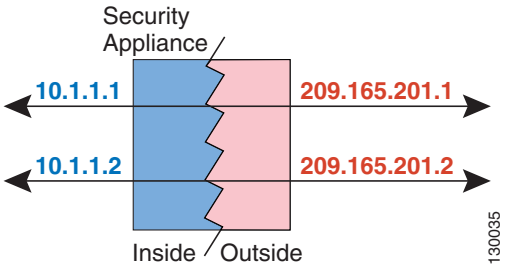
- 「スタティック NAT について」（P.5-3）
- 「ポート変換を設定したスタティック NAT」（P.5-4）
- 「1 対多のスタティック NAT」（P.5-6）
- 「他のマッピング シナリオ（非推奨）」（P.5-7）

スタティック NAT について

スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。マッピング アドレスは連続する各接続で同じなので、スタティック NAT では、双方向の接続（ホストへの接続とホストからの接続の両方）を開始できます（接続を許可するアクセス ルールが存在する場合）。一方、ダイナミック NAT および PAT では、各ホストが以降の各変換に対して異なるアドレスまたはポートを使用するので、双方向の開始はサポートされません。

次の図に、一般的なスタティック NAT のシナリオを示します。この変換は常にアクティブなので、実際のホストとリモート ホストの両方が接続を開始できます。

図 5-1　スタティック NAT



（注）　必要に応じて、双方向をディセーブルにできます。

ポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT では、実際のプロトコルとマッピング プロトコル（TCP または UDP）およびポートを指定できます。

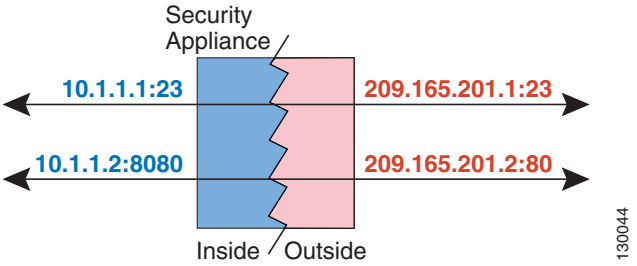
- 「ポート アドレス変換を設定したスタティック NAT について」（P.5-4）
- 「アイデンティティ ポート変換を設定したスタティック NAT」（P.5-5）
- 「標準以外のポートのポート変換を設定したスタティック NAT」（P.5-5）
- 「ポート変換を設定したスタティック インターフェイス NAT」（P.5-6）

ポート アドレス変換を設定したスタティック NAT について

スタティック NAT を使用してポートを指定する場合、ポートまたは IP アドレスを同じ値にマッピングするか、別の値にマッピングするかを選択できます。

次の図に、ポート変換が設定された一般的なスタティック NAT のシナリオを示します。自身にマッピングしたポートと、別の値にマッピングしたポートの両方を示しています。いずれのケースでも、IP アドレスは別の値にマッピングされています。この変換は常にアクティブなので、変換されたホストとリモート ホストの両方が接続を開始できます。

図 5-2　ポート変換を設定したスタティック NAT の一般的なシナリオ

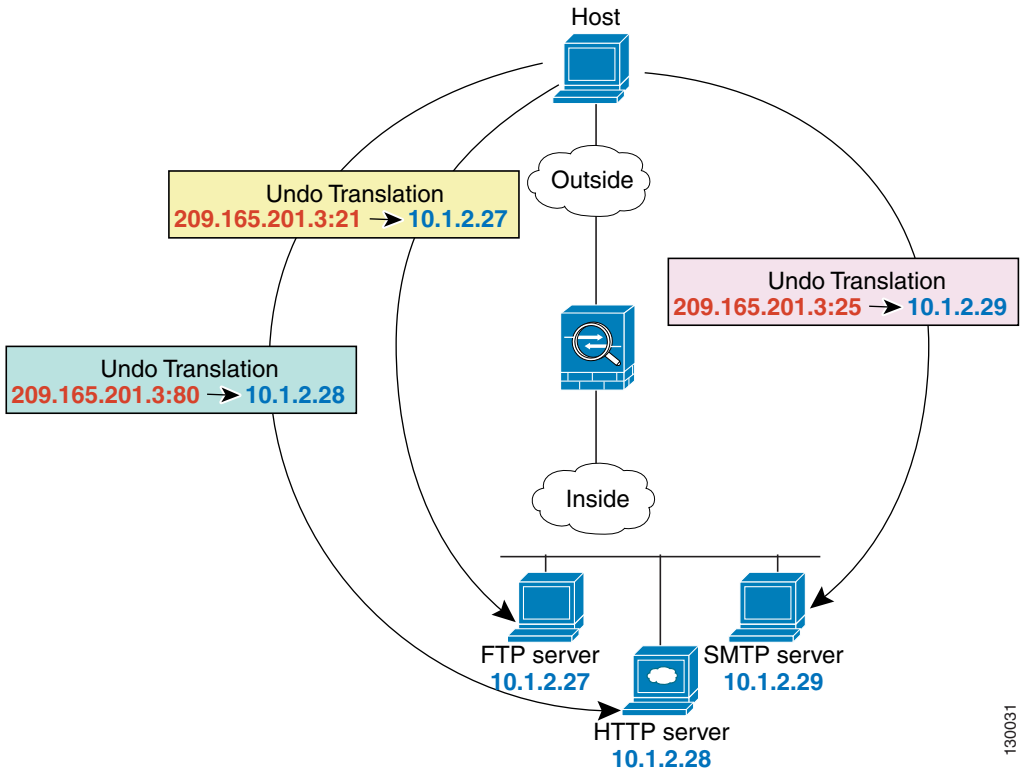


（注）　セカンダリ チャネルのアプリケーション インスペクションが必要なアプリケーション（FTP、VoIP など）を使用する場合は、ASA が自動的にセカンダリ ポートを変換します。

アイデンティティ ポート変換を設定したスタティック NAT

次のポート変換を設定したスタティック NAT の例では、リモート ユーザが FTP、HTTP、および SMTP にアクセスするための単一のアドレスを提供します。実際にはこれらのサーバは、実際のネットワーク上の異なるデバイスですが、各サーバに対して、異なるポートでも同じマッピング IP アドレスを使用するというポート変換ルールを設定したスタティック NAT を指定できます

図 5-3　　ポート変換を設定したスタティック NAT



標準以外のポートのポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT を使用すると、予約済みポートから標準以外のポートへの変換や、その逆の変換も実行できます。たとえば、内部 Web サーバがポート 8080 を使用する場合、ポート 80 に接続することを外部ユーザに許可し、その後、変換を元のポート 8080 に戻すことができます。同様に、セキュリティをさらに高めるには、Web ユーザに標準以外のポート 6785 に接続するように指示し、その後、変換をポート 80 に戻すことができます。

ポート変換を設定したスタティック インターフェイス NAT

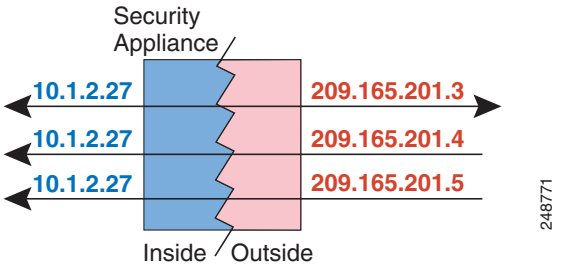
スタティック NAT は、実際のアドレスをインターフェイス アドレスとポートの組み合わせにマッピングするように設定できます。たとえば、ASA の outside インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を ASA のインターフェイス アドレス/ポート 23 にマッピングできます （ASA への Telnet では最低セキュリティのインターフェイスは許可されませんが、インターフェイス ポート変換が設定されたスタティック NAT は、その Telnet セッションを拒否するのではなく、リダイレクトします）。

1 対多のスタティック NAT

通常、スタティック NAT は 1 対 1 のマッピングで設定します。しかし場合によっては、1 つの実際のアドレスを複数のマッピング アドレスに設定することがあります（1 対多）。1 対多のスタティック NAT を設定する場合、実際のホストがトラフィックを開始すると、常に最初のマッピング アドレスが使用されます。しかし、ホストに向けて開始されたトラフィックの場合、任意のマッピング アドレスへのトラフィックを開始でき、1 つの実際のアドレスには変換されません。

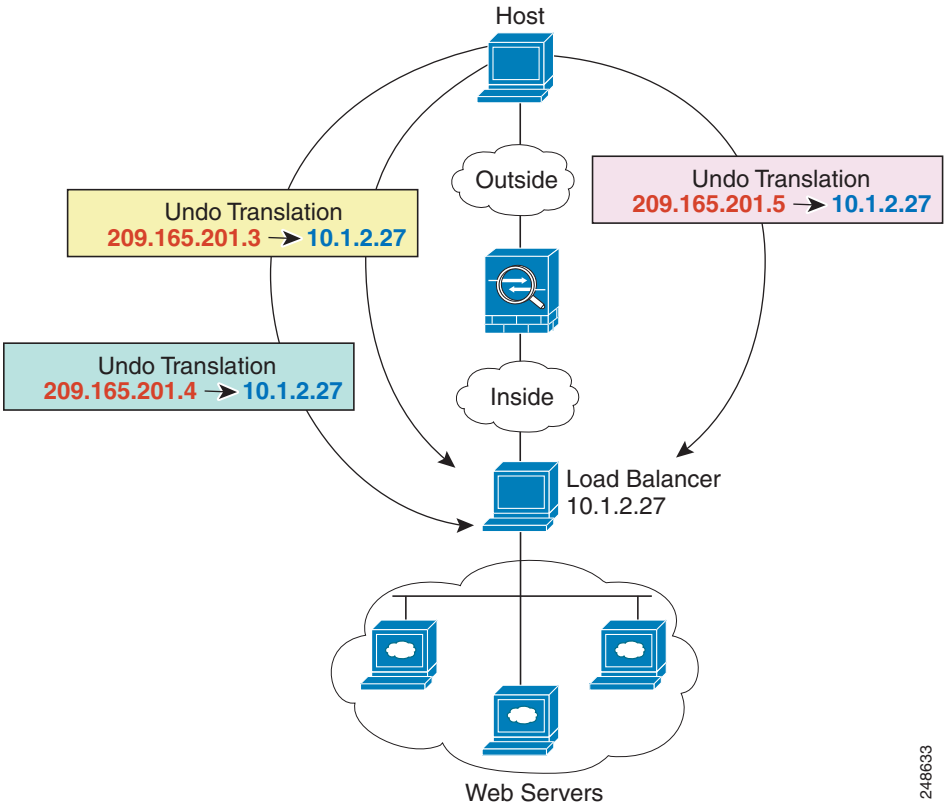
図 5-4 に、一般的な 1 対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピング アドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 5-4　　1 対多のスタティック NAT



たとえば、10.1.2.27 にロード バランサが存在するとします。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。

図 5-5　　1 対多のスタティック NAT の例



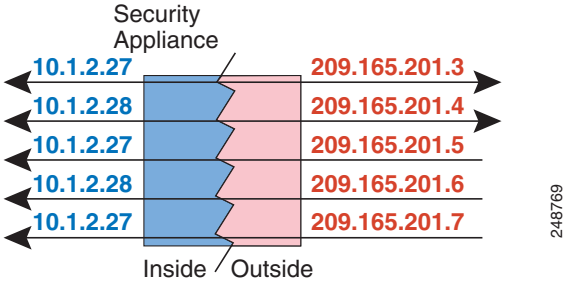
他のマッピング シナリオ（非推奨）

ASA には、1 対 1、1 対多だけではなく、少対多、多対少、多対 1 など任意の種類のスタティック マッピング シナリオを使用できるという柔軟性があります。1 対 1 マッピングまたは 1 対多マッピングだけを使用することをお勧めします。これらの他のマッピング オプションは、予期しない結果が発生する可能性があります。

機能的には、少対多は、1 対多と同じです。しかし、コンフィギュレーションが複雑化して、実際のマッピングが一目では明らかでない場合があるため、必要とする実際の各アドレスに対して 1 対多のコンフィギュレーションを作成することを推奨します。たとえば、少対多のシナリオでは、少数の実際のアドレスが多数のマッピング アドレスに順番にマッピングされます（A は 1、B は 2、C は 3）。すべての実際のアドレスがマッピングされたら、次にマッピングされるアドレスは、最初の実際のアドレスにマッピングされ、すべてのマッピング アドレスがマッピングされるまで続行されます（A は 4、B は 5、C は 6）。この結果、実際の各アドレスに対して複数のマッピング アドレスが存在することになります。1 対多のコンフィギュレーションのように、最初のマッピングだけが双方向であり、以降のマッピングでは、実際のホストへのトラフィックを開始できますが、実際のホストからのすべてのトラフィックは、送信元の最初のマッピング アドレスだけを使用できます。

次の図に、一般的な少対多のスタティック NAT シナリオを示します。

図 5-6　　少対多のスタティック NAT

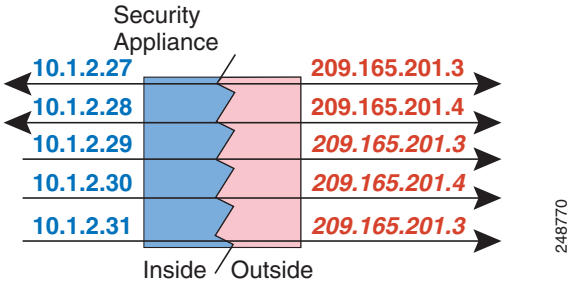


多対少または多対 1 コンフィギュレーションでは、マッピング アドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足するよりも前に、マッピング アドレスが不足します。双方向の開始を実現できるのは、最下位の実際の IP アドレスとマッピングされたプールの間でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターン トラフィックは、接続の固有の 5 つのタプル（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。

（注）　多対少または多対 1 の NAT は PAT ではありません。2 つの実際のホストが同じ送信元ポート番号を使用して同じ外部サーバおよび同じ TCP 宛先ポートにアクセスする場合は、両方のホストが同じ IP アドレスに変換されると、アドレスの競合がある（5 つのタプルが一意でない）ため、両方の接続がリセットされます。

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 5-7　　多対少のスタティック NAT



このようにスタティック ルールを使用するのではなく、双方向の開始を必要とするトラフィックに 1 対 1 のルールを作成し、残りのアドレスにダイナミック ルールを作成することをお勧めします。

ダイナミック NAT

次のトピックでは、ダイナミック NAT について説明します。

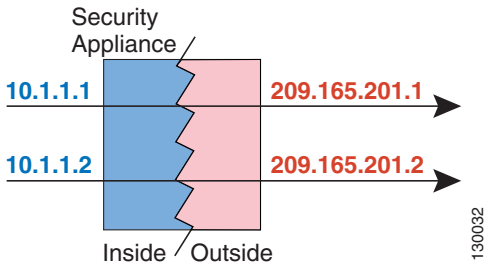
- 「ダイナミック NAT について」（P.5-9）
- 「ダイナミック NAT の欠点と利点」（P.5-10）

ダイナミック NAT について

ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピング アドレスのプールに変換されます。マッピングされたプールにあるアドレスは、通常、実際のグループより少なくなります。変換対象のホストが宛先ネットワークにアクセスすると、ASA は、マッピングされたプールから IP アドレスをそのホストに割り当てます。変換は、実際のホストが接続を開始したときにだけ作成されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセス ルールでその接続が許可されている場合でも、宛先ネットワークのユーザは、ダイナミック NAT を使用するホストへの確実な接続を開始できません。

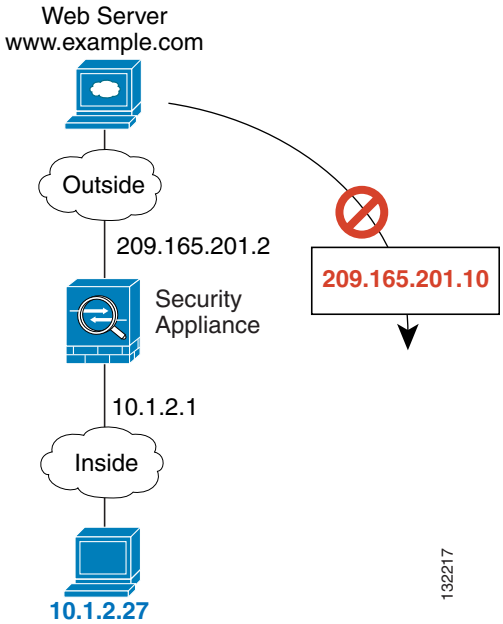
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

図 5-8　ダイナミック NAT



次の図に、マッピング アドレスへの接続開始を試みているリモート ホストを示します。このアドレスは、現時点では変換テーブルにないため、ASA はパケットをドロップしています。

図 5-9　マッピング アドレスへの接続開始を試みているリモート ホスト



（注）　変換が継続している間、アクセス ルールで許可されていれば、リモート ホストは変換済みホストへの接続を開始できます。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。

ダイナミック NAT の欠点と利点

ダイナミック NAT には、次の欠点があります。

- マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。

  PAT では、1 つのアドレスのポートを使用して 64,000 を超える変換を処理できるため、このイベントが頻繁に発生する場合は、PAT または PAT のフォールバック方式を使用します。
- マッピング プールではルーティング可能なアドレスを多数使用する必要があるのに、ルーティング可能なアドレスは多数用意できない場合があります。

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、PAT は次の場合は機能しません。

- GRE バージョン 0 などのように、オーバーロードするためのポートがない IP プロトコルでは機能しません。
- 一部のマルチメディア アプリケーションなどのように、1 つのポート上にデータ ストリームを持ち、別のポート上に制御パスを持ち、公開規格ではないアプリケーションでも機能しません。

NAT および PAT のサポートの詳細については、「デフォルト インスペクションと NAT に関する制限事項」（P.8-6）を参照してください。

ダイナミック PAT

次のトピックでは、ダイナミック PAT について説明します。

- 「ダイナミック PAT について」（P.5-10）
- 「Per-Session PAT と Multi-Session PAT（バージョン 9.0(1) 以降）」（P.5-11）
- 「ダイナミック PAT の欠点と利点」（P.5-11）

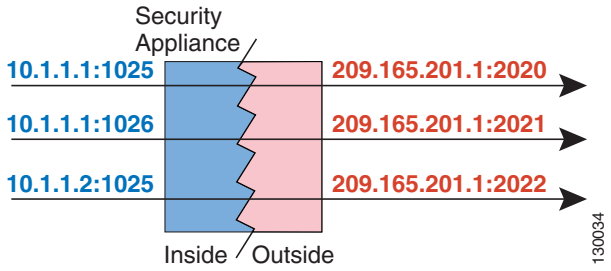
ダイナミック PAT について

ダイナミック PAT では、実際のアドレスおよび送信元ポートが 1 つのマッピング アドレスおよび固有のポートに変換されることによって、複数の実際のアドレスが 1 つのマッピング IP アドレスに変換されます。使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。下位ポート範囲を使用するトラフィックが数多くある場合は、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。

送信元ポートが接続ごとに異なるため、各接続には別の変換セッションが必要です。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

次の図に、一般的なダイナミック PAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。マッピング アドレスはどの変換でも同じですが、ポートがダイナミックに割り当てられます。

図 5-10　ダイナミック PAT



接続の有効期限が切れると、ポート変換も有効期限切れになります。Multi-Session PAT では、デフォルトで 30 秒の PAT タイムアウトが使用されます。Per-Session PAT（9.0(1) 以降）の場合、xlate が即座に削除されます。宛先ネットワークのユーザは、PAT を使用するホストへの接続を確実には開始できません（アクセス ルールでその接続が許可されている場合も同じです）。

（注）　変換が継続している間、アクセス ルールで許可されていれば、リモート ホストは変換済みホストへの接続を開始できます。実際のポート アドレスおよびマッピング ポート アドレスはどちらも予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。

Per-Session PAT と Multi-Session PAT（バージョン 9.0(1) 以降）

Per-Session PAT によって PAT のスケーラビリティが向上し、クラスタリングの場合に各メンバ ユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、マスター ユニットに転送してマスター ユニットを所有者とする必要があります。Per-Session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンド ノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。

「ヒットエンドラン」トラフィック、たとえば HTTP や HTTPS の場合は、Per-Session PAT によって、1 アドレスでサポートされる接続率が大幅に増加することがあります。Per-Session PAT を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。Per-Session PAT を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/*平均ライフタイム*です。

デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-Session PAT xlate を使用します。H.323、SIP、Skinny など、Multi-Session PAT による利点があるトラフィックの場合、Per-Session PAT 拒否ルールを作成して、Per-Session PAT をディセーブルにできます。「Per-Session PAT ルールの設定」（P.6-20）を参照してください。

ダイナミック PAT の欠点と利点

ダイナミック PAT では、1 つのマッピング アドレスを使用できるため、ルーティング可能なアドレスが節約されます。さらに、ASA インターフェイスの IP アドレスを PAT アドレスとして使用できます。

ダイナミック PAT は、制御パスとは異なるデータ ストリームを持つ一部のマルチメディア アプリケーションでは機能しません。NAT および PAT のサポートの詳細については、「デフォルト インスペクションと NAT に関する制限事項」（P.8-6）を参照してください。

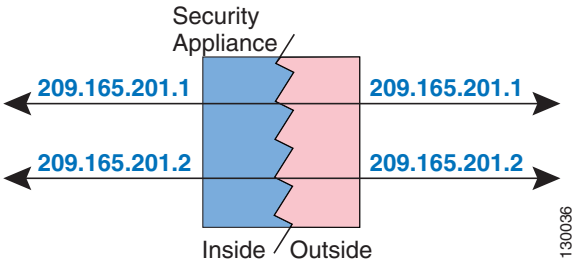
ダイナミック PAT によって、単一の IP アドレスから送信されたように見える数多くの接続が作成されることがあります。この場合、このトラフィックはサーバで DoS 攻撃として解釈される可能性があります。（8.4(2)/8.5(1) 以降）アドレスの PAT プールを設定し、PAT アドレスのラウンドロビン割り当てを使用すると、この状況を緩和できます。

アイデンティティ NAT

IP アドレスを自身に変換する必要のある NAT コンフィギュレーションを設定できます。たとえば、NAT を各ネットワークに適用するものの、1 つのネットワークを NAT から除外するという広範なルールを作成する場合、スタティック NAT ルールを作成して、アドレスを自身に変換することができます。アイデンティティ NAT は、NAT からクライアント トラフィックを除外する必要のある、リモート アクセス VPN で必要です。

次の図に、一般的なアイデンティティ NAT のシナリオを示します。

図 5-11　アイデンティティ NAT



ルーテッド モードとトランスペアレント モードの NAT

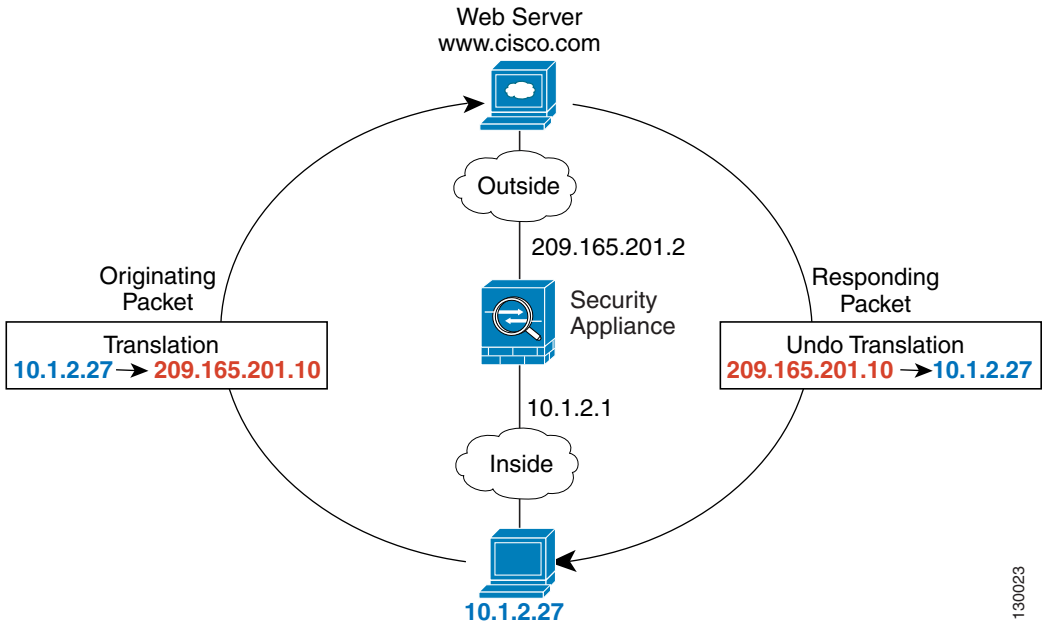
NAT は、ルーテッド モードおよびトランスペアレント ファイアウォール モードの両方に設定できます。この項では、各ファイアウォール モードの一般的な使用方法について説明します。

- 「ルーテッド モードの NAT」（P.5-13）
- 「トランスペアレント モードの NAT」（P.5-13）

ルーテッド モードの NAT

次の図は、内部にプライベート ネットワークを持つ、ルーテッド モードの一般的な NAT の例を示しています。

図 5-12　NAT の例：ルーテッド モード



1. 内部ホスト 10.1.2.27 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.2.27 はマッピング アドレス 209.165.201.10 に変更されます。
2. サーバが応答すると、マッピング アドレス 209.165.201.10 に応答を送信し、ASA がそのパケットを受信します。これは、ASA がプロキシ ARP を実行してパケットを要求するためです。
3. ASA はその後、パケットをホストに送信する前に、マッピング アドレス 209.165.201.10 を変換し、実際のアドレス 10.1.2.27 に戻します。

トランスペアレント モードの NAT

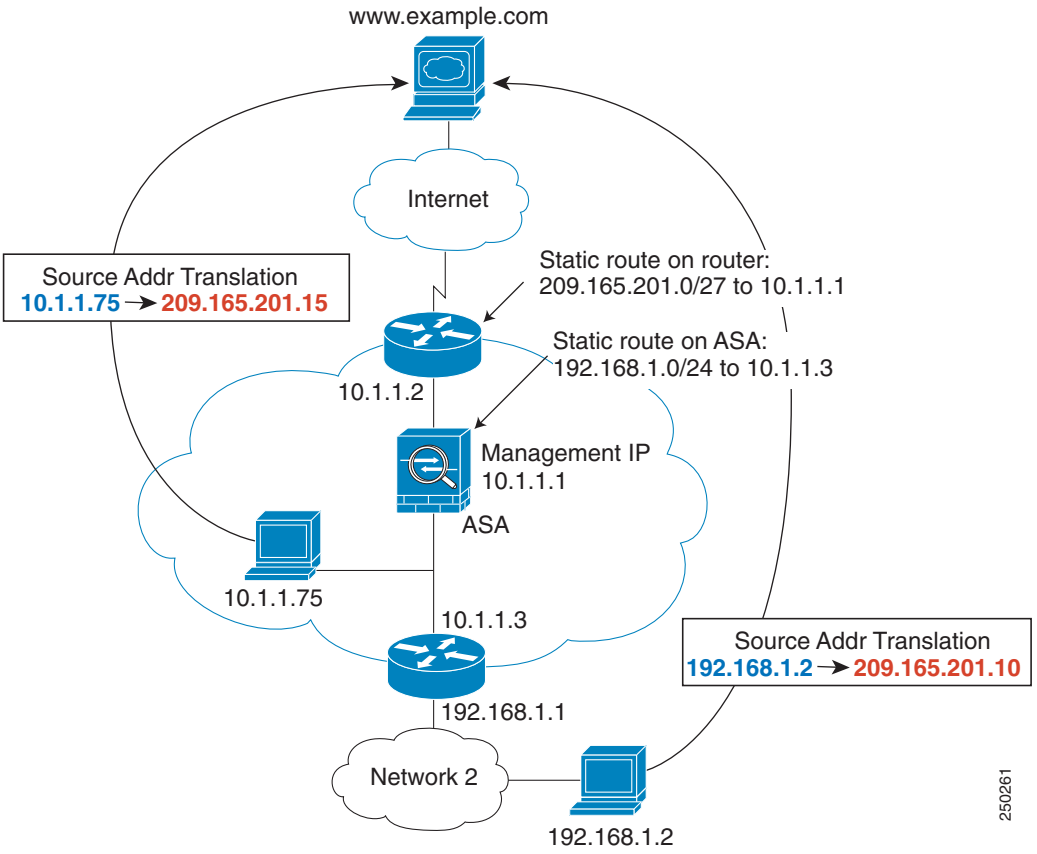
NAT をトランスペアレント モードで使用すると、ネットワークで NAT を実行するためのアップストリーム ルータまたはダウンストリーム ルータが必要なくなります。

トランスペアレント モードの NAT には、次の要件および制限があります。

- トランスペアレント ファイアウォールにはインターフェイス IP アドレスがないため、インターフェイス PAT を使用できません。
- ARP インスペクションはサポートされていません。また、何らかの理由で、一方の ASA のホストがもう一方の ASA のホストに ARP 要求を送信し、開始ホストの実際のアドレスが同じサブネットの別のアドレスにマッピングされる場合、実際のアドレスは ARP 要求で可視のままになります。
- IPv4 および IPv6 ネットワークの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。

次の図に、インターフェイス内部と外部に同じネットワークを持つ、トランスペアレント モードの一般的な NAT のシナリオを示します。このシナリオのトランスペアレント ファイアウォールは NAT サービスを実行しているため、アップストリーム ルータは NAT を実行する必要がありません。

図 5-13　NAT の例：トランスペアレント モード



1. 内部ホスト 10.1.1.75 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.1.75 はマッピング アドレス 209.165.201.15 に変更されます。
2. サーバが応答すると、マッピング アドレス 209.165.201.15 に応答を送信し、ASA がそのパケットを受信します。これは、アップストリーム ルータには、ASA の管理 IP アドレスに転送されるスタティック ルートのこのマッピング ネットワークが含まれるためです。必要なルートの詳細については、「マッピング アドレスとルーティング」（P.5-22）を参照してください。
3. その後、ASA はマッピング アドレス 209.165.201.15 を変換して実際のアドレス 10.1.1.1.75 に戻します。実際のアドレスは直接接続されているため、ASA はそのアドレスを直接ホストに送信します。
4. ホスト 192.168.1.2 の場合も、リターン トラフィックを除き、同じプロセスが発生します。ASA はルーティング テーブルでルートを検索し、192.168.1.0/24 の ASA スタティック ルートに基づいてパケットを 10.1.1.3 にあるダウンストリーム ルータに送信します。必要なルートの詳細については、「リモート ネットワークのトランスペアレント モード ルーティングの要件」（P.5-25）を参照してください。

NAT と IPv6

NAT を使用すると、IPv6 ネットワーク間、さらに IPv4 および IPv6 ネットワークの間で変換できます（ルーテッド モードのみ）。次のベスト プラクティスを推奨します。

- NAT66（IPv6-to-IPv6）：スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（Twice NAT のみ）。
- NAT46（IPv4-to-IPv6）：スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいので、容易にスタティック変換に対応できます。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（Twice NAT のみ）。IPv6 サブネットに変換する場合（/96 以下）、結果のマッピング アドレスはデフォルトで IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます（混合表記で表示）。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。また、任意で、ネット間のアドレスを変換できます。この場合、最初の IPv6 アドレスに最初の IPv4 アドレス、2 番目の IPv6 アドレスに 2 番目の IPv4 アドレス、のようにマッピングします。
- NAT64（IPv6-to-IPv4）：IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

特定の実装のガイドラインおよび制約事項については、設定の章を参照してください。

NAT の実装方法

ASA は、*ネットワーク オブジェクト NAT* および *Twice NAT* という 2 種類の方法でアドレス変換を実装できます。

- 「ネットワーク オブジェクト NATと Twice NAT の主な違い」（P.5-15）
- 「ネットワーク オブジェクト NAT」（P.5-16）
- 「Twice NAT」（P.5-17）

ネットワーク オブジェクト NATと Twice NAT の主な違い

これら 2 つの NAT タイプの主な違いは、次のとおりです。

- 実際のアドレスの定義方法
  - ネットワーク オブジェクト NAT : NAT をネットワーク オブジェクトのパラメータとして定義します。ネットワーク オブジェクトは、IP ホスト、範囲、またはサブネットの名前を指定するので、実際の IP アドレスではなく、NAT コンフィギュレーション内のオブジェクトを使用できます。ネットワーク オブジェクトの IP アドレスが実際のアドレスとして機能します。この方法では、ネットワーク オブジェクトがコンフィギュレーションの他の部分ですでに使用されていても、そのネットワーク オブジェクトに NAT を容易に追加できます。

  - Twice NAT：実際のアドレスとマッピング アドレスの両方のネットワーク オブジェクトまたはネットワーク オブジェクト グループを識別します。この場合、NAT はネットワーク オブジェクトのパラメータではありません。ネットワーク オブジェクトまたはグループが、NAT コンフィギュレーションのパラメータです。実際のアドレスのネットワーク オブジェクト *グループ*を使用できることは、Twice NAT がよりスケーラブルであることを意味します。

- 送信元および宛先 NAT の実装方法
  - ネットワーク オブジェクト NAT：各ルールは、パケットの送信元または宛先のいずれかに適用できます。つまり、送信元 IP アドレスに 1 つ、宛先 IP アドレスに 1 つと、2 つのルールが使用されることがあります。これらの 2 つのルールを相互に結び付けて、送信先と宛先の組み合わせに特定の変換を適用することはできません。
  - Twice NAT：1 つのルールが送信元と宛先の両方を変換します。一致するパケットは、1 つのルールだけに一致します。これ以外のルールはチェックされません。Twice NAT にオプションの宛先アドレスを設定しない場合でも、一致するパケットは、1 つの Twice NAT ルールだけに一致します。送信元および宛先は相互に結び付けられるので、送信元と宛先の組み合わせに応じて、異なる変換を適用できます。たとえば、sourceA/destinationA には、sourceA/destinationB とは異なる変換を設定できます。
- NAT ルールの順序
  - ネットワーク オブジェクト NAT：NAT テーブルで自動的に順序付けされます。
  - Twice NAT：NAT テーブルで、手動で順序付けします（ネットワーク オブジェクト NAT ルールの前または後）。

  詳細については、「NAT ルールの順序」（P.5-20）を参照してください。

Twice NAT の追加機能を必要としない場合は、ネットワーク オブジェクト NAT を使用することをお勧めします。ネットワーク オブジェクト NAT は設定が容易で、Voice over IP（VoIP）などの用途では、信頼性が高い場合があります （Twice NAT は 2 つのオブジェクト間だけに適用可能であるため、VoIP では、いずれのオブジェクトにも属さない間接アドレスの変換が失敗することがあります）。

ネットワーク オブジェクト NAT

ネットワーク オブジェクトのパラメータとして設定されているすべての NAT ルールは、*ネットワーク オブジェクト NAT* ルールと見なされます。ネットワーク オブジェクト NAT は、1 つの IP アドレス、アドレスの範囲、またはサブネットであるネットワーク オブジェクトの NAT を設定するための迅速かつ容易な方法です。

ネットワーク オブジェクトを設定すると、このオブジェクトのマッピング アドレスをインライン アドレスとして、または別のネットワーク オブジェクトやネットワーク オブジェクト グループのいずれかとして識別できるようになります。

パケットが ASA に入ると、送信元 IP アドレスと宛先 IP アドレスの両方がネットワーク オブジェクト NAT ルールと照合されます。個別の照合が行われる場合、パケット内の送信元 IP アドレスと宛先 IP アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはないので、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定することはできません。この種の機能には、Twice NAT を使用します（Twice NAT を使用すると、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます）。

ネットワーク オブジェクト NAT の設定を開始するには、第 6 章「ネットワーク オブジェクト NAT（ASA 8.3 以降）」を参照してください。

Twice NAT

Twice NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定できます。

宛先アドレスはオプションです。宛先アドレスを指定する場合、宛先アドレスを自身にマッピングするか（アイデンティティ NAT）、別のアドレスにマッピングできます。宛先マッピングは、常にスタティック マッピングです。

Twice NAT では、ポート変換が設定されたスタティック NAT のサービス オブジェクトを使用できます。ネットワーク オブジェクト NAT は、インライン定義だけを受け入れます。

Twice NAT の設定を開始するには、第 7 章「Twice NAT（ASA 8.3 以降）」を参照してください。

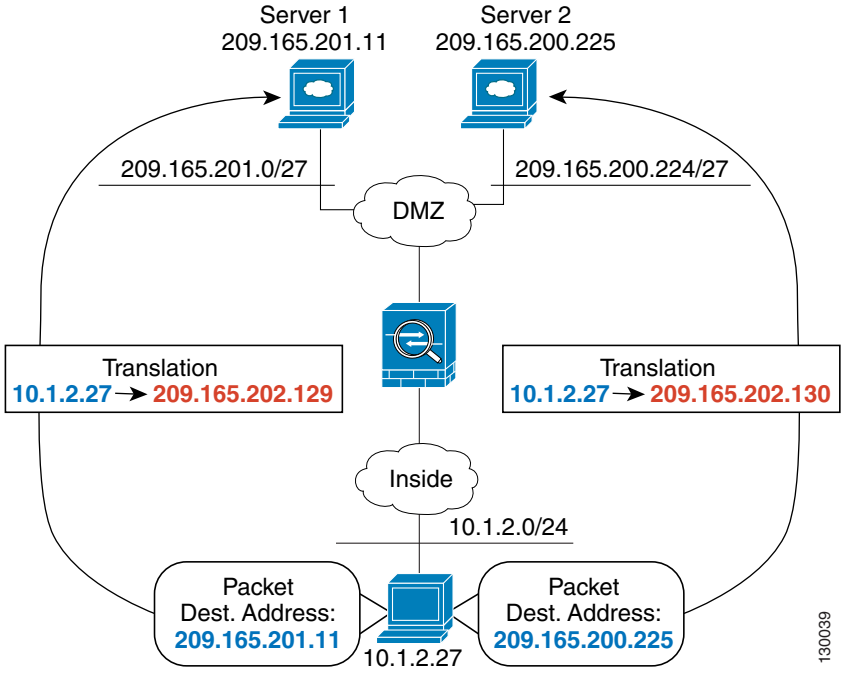
次のトピックで、Twice NAT の例を示します。

- 「例：異なる宛先アドレスを使用する Twice NAT」（P.5-17）
- 「例：異なる宛先ポートを使用する Twice NAT」（P.5-18）
- 「例：宛先アドレス変換が設定された Twice NAT」（P.5-19）

例：異なる宛先アドレスを使用する Twice NAT

次の図に、2 台の異なるサーバにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129 に変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130 に変換されます。

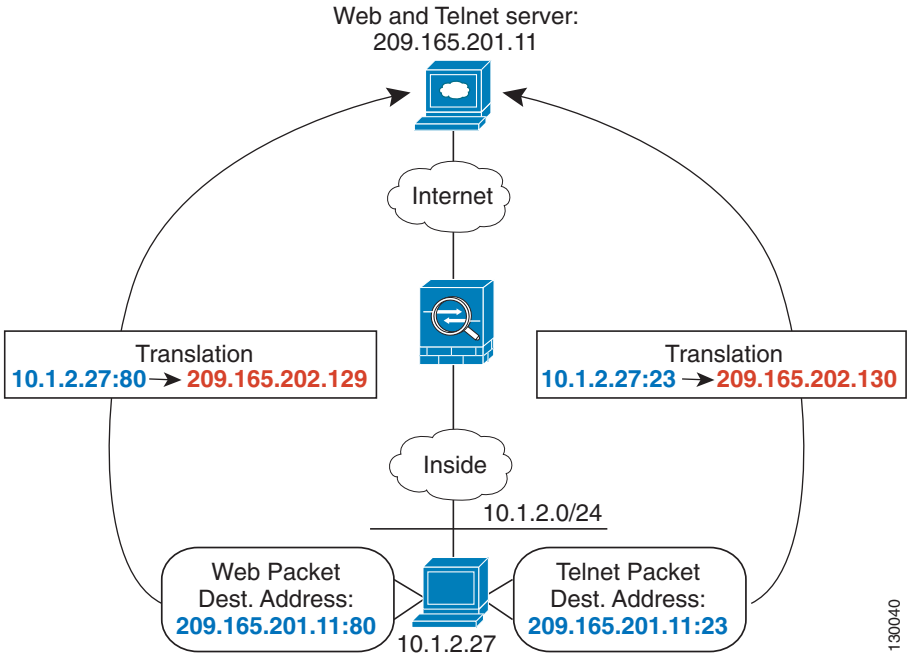
図 5-14　異なる宛先アドレスを使用する Twice NAT



例：異なる宛先ポートを使用する Twice NAT

次の図に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Web サービスを求めてサーバにアクセスすると、実際のアドレスは 209.165.202.129 に変換されます。ホストが Telnet サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130 に変換されます。

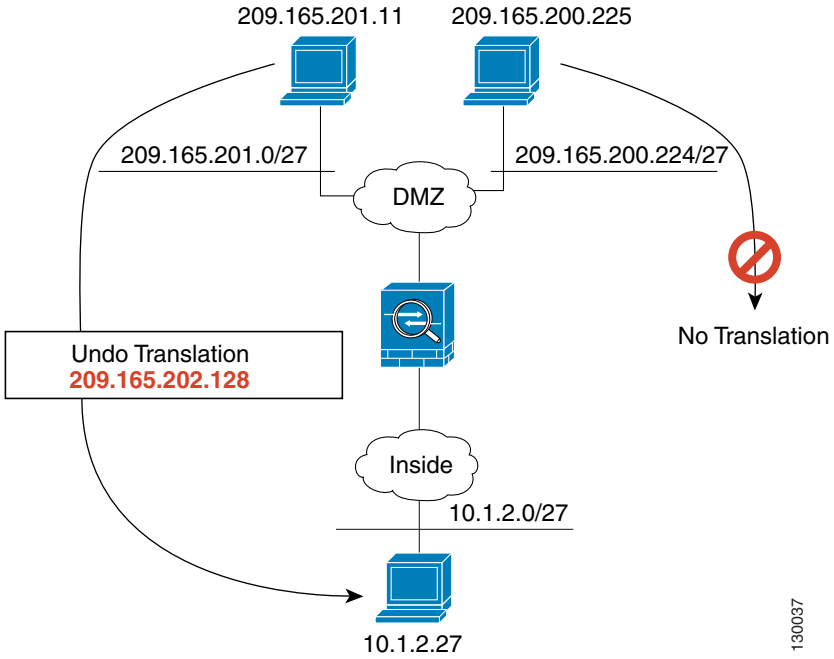
図 5-15　異なる宛先ポートを使用する Twice NAT



例：宛先アドレス変換が設定された Twice NAT

次の図に、マッピングされるホストに接続するリモート ホストを示します。マッピングされるホストには、209.165.201.0/27 ネットワークが起点または終点となるトラフィックに限り実際のアドレスを変換するスタティック Twice NAT 変換が設定されています。209.165.200.224/27 ネットワーク用の変換は存在しません。したがって、変換済みのホストはそのネットワークに接続できず、そのネットワークのホストも変換済みのホストに接続できません。

図 5-16　宛先アドレス変換が設定されたスタティック Twice NAT



NAT ルールの順序

ネットワーク オブジェクト NAT ルールおよび Twice NAT ルールは、3 セクションに分割される 1 つのテーブルに保存されます。最初にセクション 1 のルール、次にセクション 2、最後にセクション 3 というように、一致が見つかるまで順番に適用されます。たとえば、セクション 1 で一致が見つかった場合、セクション 2 とセクション 3 は評価されません。次の表に、各セクション内のルールの順序を示します。

表 5-1　NAT ルール テーブル

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 1	Twice NAT	コンフィギュレーションに登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に特殊なルールが来るようにする必要があります。そうしない場合、特殊なルールを期待どおりに適用できない可能性があります。デフォルトでは、Twice NAT ルールはセクション 1 に追加されます。 **（注）** Easy VPN Remote を設定する場合、ASA はこのセクションの末尾に非表示の NAT ルールをダイナミックに追加します。非表示のルールではなく、VPN トラフィックに一致する Twice NAT ルールは、このセクションで設定しないでください。NAT エラーのために VPN が機能しない場合は、このセクションではなく、セクション 3 に Twice NAT ルールを追加することを検討してください。
セクション 2	ネットワーク オブジェクト NAT	セクション 1 で一致が見つからない場合、ASA によって自動的に判断され、セクション 2 のルールが次の順序で適用されます。 1. スタティック ルール 2. ダイナミック ルール **各ルール タイプでは、次の順序ガイドラインが使用されます。** 1. 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。 2. 数量が同じ場合には、IP アドレス番号（低から高の順）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。 3. 同じ IP アドレスが使用される場合、ネットワーク オブジェクトの名前がアルファベット順で使用されます。たとえば、abracadabra は catwoman よりも先に評価されます。
セクション 3	Twice NAT	まだ一致が見つからない場合、セクション 3 のルールがコンフィギュレーションに登場する順に、最初の一致ベースで適用されます。このセクションには、最も一般的なルールを含める必要があります。このセクションにおいても、一般的なルールの前に特殊なルールが来るようにする必要があります。そうしない場合、一般的なルールが適用されます。Twice NAT ルールを追加するときには、このルールをセクション 3 に追加するかどうかを指定できます。

たとえばセクション 2 のルールでは、ネットワーク オブジェクト内に定義されている次の IP アドレスがあるとします。

192.168.1.0/24（スタティック）

192.168.1.0/24（ダイナミック）

10.1.1.0/24（スタティック）

192.168.1.1/32（ダイナミック）

172.16.1.0/24（ダイナミック）（オブジェクト def）

172.16.1.0/24（ダイナミック）（オブジェクト abc）

この結果、使用される順序は次のとおりです。

192.168.1.1/32（ダイナミック）

10.1.1.0/24（スタティック）

192.168.1.0/24（スタティック）

172.16.1.0/24（ダイナミック）（オブジェクト abc）

172.16.1.0/24（ダイナミック）（オブジェクト def）

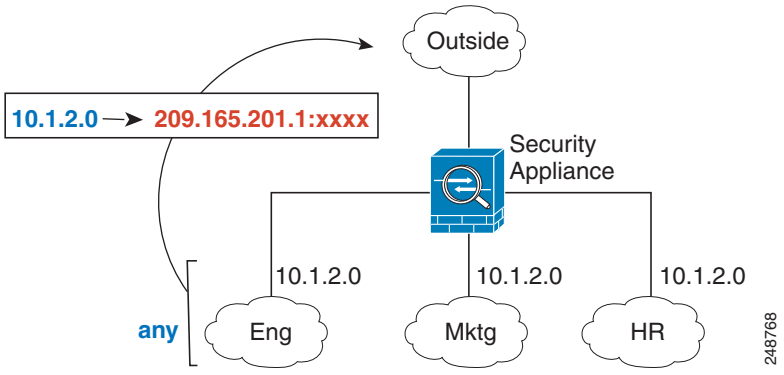
192.168.1.0/24（ダイナミック）

NAT インターフェイス

NAT ルールを設定して任意のインターフェイス（つまり、すべてのインターフェイス）に適用できます。または、特定の実際のインターフェイスおよびマッピング インターフェイスを識別できます。実際のアドレスには任意のインターフェイスを指定できます。マッピング アドレスには特定のインターフェイスを指定できます。または、その逆も可能です。

たとえば、複数のインターフェイスで同じプライベート アドレスを使用し、外部へのアクセス時にはすべてのインターフェイスを同じグローバル プールに変換する場合、実際のアドレスに任意のインターフェイスを指定し、マッピング アドレスには outside インターフェイスを指定します。

図 5-17　　任意のインターフェイスの指定



（注）　トランスペアレント モードの場合は、特定の送信元インターフェイスおよび宛先インターフェイスを選択する必要があります。

NAT パケットのルーティング

ASA は、マッピング アドレスに送信されたすべてのパケットの宛先となる必要があります。ASA は、マッピング アドレス宛てに送信されるすべての受信パケットの出力インターフェイスを決定する必要があります。この項では、ASA が NAT を使用してパケットの受信および送信を処理する方法について説明します。

- 「マッピング アドレスとルーティング」（P.5-22）
- 「リモート ネットワークのトランスペアレント モード ルーティングの要件」（P.5-25）
- 「出力インターフェイスの決定」（P.5-25）

マッピング アドレスとルーティング

実際のアドレスをマッピング アドレスに変換する場合は、選択したマッピング アドレスによって、マッピング アドレスのルーティング（必要な場合）を設定する方法が決定されます。

マッピング IP アドレスに関するその他のガイドラインについては、第 6 章「ネットワーク オブジェクト NAT（ASA 8.3 以降）」および第 7 章「Twice NAT（ASA 8.3 以降）」を参照してください。

次のトピックでは、マッピング アドレスのタイプについて説明します。

- 「マッピング インターフェイスと同じネットワーク上のアドレス」（P.5-22）
- 「固有のネットワーク上のアドレス」（P.5-23）
- 「実際のアドレスと同じアドレス（アイデンティティ NAT）」（P.5-23）

マッピング インターフェイスと同じネットワーク上のアドレス

マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、ASA はプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することによって、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法では、ASA がその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。このソリューションは、外部ネットワークに十分な数のフリー アドレスが含まれている場合に最も適しており、ダイナミック NAT またはスタティック NAT などの 1:1 変換を使用している場合は考慮が必要です。ダイナミック PAT ではアドレス数が少なくても使用できる変換の数が大幅に拡張されるので、外部ネットワークで使用できるアドレスが少ししかない場合でも、この方法を使用できます。PAT では、マッピング インターフェイスの IP アドレスも使用できます。

（注） マッピング インターフェイスを任意のインターフェイスとして設定し、マッピング インターフェイスの 1 つとして同じネットワーク上のマッピング アドレスを指定すると、そのマッピング アドレスの ARP 要求を*別の*インターフェイスで受信する場合、入力インターフェイスでそのネットワークの ARP エントリを手動で設定し、その MAC アドレスを指定する必要があります（[Configuration] > [Device Management] > [Advanced] > [ARP] > [ARP Static Table] を参照）。通常、マッピング インターフェイスに任意のインターフェイスを指定して、マッピング アドレスの固有のネットワークを使用すると、この状況は発生しません。

固有のネットワーク上のアドレス

マッピング インターフェイスで使用可能なアドレスより多くのアドレスが必要な場合は、別のサブネット上のアドレスを指定できます。アップストリーム ルータには、ASA を指しているマッピング アドレスのスタティック ルートが必要です。また、ルーテッド モードの場合、宛先ネットワーク上の IP アドレスをゲートウェイとして使用して、マッピング アドレスの ASA にスタティック ルートを設定し、ルーティング プロトコルを使用してルートを再配布することができます。たとえば、内部ネットワーク（10.1.1.0/24）に NAT を使用し、マッピング IP アドレス 209.165.201.5 を使用する場合、次のスタティック ルートを設定して再配布することができます。

```
route inside 209.165.201.5 255.255.255.255 10.1.1.99
```

トランスペアレント モードの場合は、実際のホストが直接接続されてる場合は、ASA をポイントするようにアップストリーム ルータのスタティック ルートを設定します。8.3 では、グローバルな管理 IP アドレスを指定します。8.4(1) 以降では、ブリッジ グループの IP アドレスを指定します。トランスペアレント モードのリモート ホストの場合は、アップストリーム ルータのスタティック ルートで、代わりにダウンストリーム ルータの IP アドレスを指定できます。

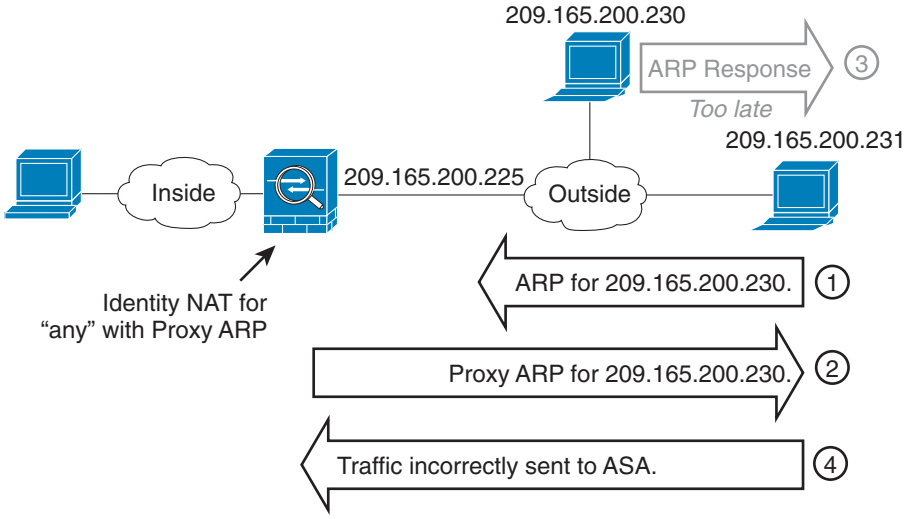
実際のアドレスと同じアドレス（アイデンティティ NAT）

（8.3(1)、8.3(2)、8.4(1)）アイデンティティ NAT のデフォルト動作で、プロキシ ARP はディセーブルにされます。これは設定できません。

（8.4(2) 以降）アイデンティティ NAT のデフォルト動作で、プロキシ ARP はイネーブルにされ、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP をディセーブルにできます。必要に応じて標準スタティック NAT のプロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの適切なルートがあることを確認する必要があります。

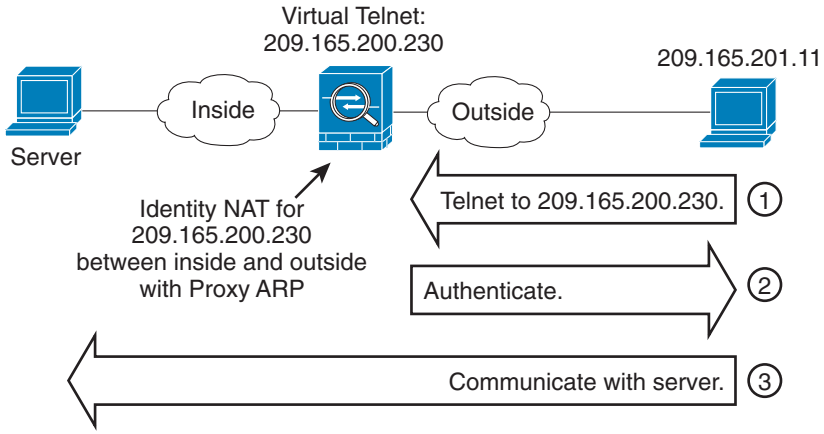
アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。たとえば、任意の IP アドレスの広範なアイデンティティ NAT ルールを設定した場合、プロキシ ARP をイネーブルのままにしておくと、マッピング インターフェイスに直接接続されたネットワーク上のホストの問題を引き起こすことがあります。この場合、マッピング ネットワークのホストが同じネットワークの他のホストと通信すると、ARP 要求内のアドレスは（任意のアドレスと一致する）NAT ルールと一致します。このとき、実際には ASA 向けのパケットでない場合でも、ASA はこのアドレスの ARP をプロキシします （この問題は、Twice NAT ルールが設定されている場合にも発生します。NAT ルールは送信元と宛先のアドレス両方に一致する必要がありますが、プロキシ ARP 判定は「送信元」アドレスに対してのみ行われます）。実際のホストの ARP 応答の前に ASA の ARP 応答を受信した場合、トラフィックは誤って ASA に送信されます（図 5-18 を参照）。

図 5-18　アイデンティティ NAT に関するプロキシ ARP の問題



まれに、アイデンティティ NAT に対してプロキシ ARP が必要になります（仮想 Telnet など）。ネットワーク アクセスに AAA を使用する場合、ホストは他のトラフィックが通過する前に Telnet のようなサービスを使用して ASA で認証を受ける必要があります。ASA に仮想 Telnet サーバを設定すると、必要なログインを提供できます。仮想 Telnet アドレスに外部からアクセスする場合は、特にプロキシ ARP 機能用のアドレスのアイデンティティ NAT ルールを設定する必要があります。仮想 Telnet の内部プロセスにより、プロキシ ARP を使用すると ASA が NAT ルールに従って送信元インターフェイスからトラフィックを送信せず、トラフィックを仮想 Telnet アドレス宛のままにすることができます （図 5-19 を参照）。

図 5-19　プロキシ ARP と仮想 Telnet



リモート ネットワークのトランスペアレント モード ルーティングの要件

トランスペアレント モードで NAT を使用する場合、一部のタイプのトラフィックには、スタティック ルートが必要になります。詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

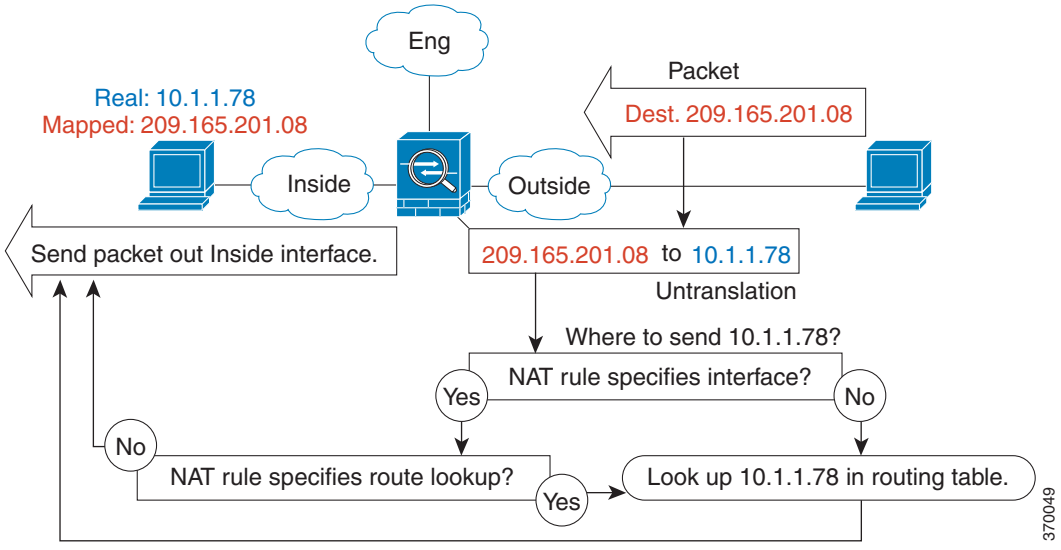
出力インターフェイスの決定

ASA がマッピング アドレスのトラフィックを受信する場合、ASA は NAT ルールに従って宛先アドレスを変換解除し、実際のアドレスにパケットを送信します。ASA は、次の方法でパケットの出力インターフェイスを決定します。

- トランスペアレント モード：ASA は NAT ルールを使用して実際のアドレスの出力インターフェイスを決定します。NAT ルールの一部として送信元インターフェイスと宛先インターフェイスを指定する必要があります。
- ルーテッド モード：ASA は、次のいずれかの方法で出力インターフェイスを決定します。
  - NAT ルールでインターフェイスを設定する：ASA は NAT ルールを使用して出力インターフェイスを決定します。（8.3(1) ～ 8.4(1)）唯一の例外はアイデンティティ NAT です。アイデンティティ NAT では、NAT コンフィギュレーションに関係なく、常にルート ルックアップが使用されます。（8.4(2) 以降）アイデンティティ NAT の場合、デフォルト動作は NAT コンフィギュレーションを使用することです。ただし、代わりにオプションとして常にルート ルックアップを使用することもできます。一部のシナリオでは、ルート ルックアップの上書きが必要になる場合があります。たとえば、「NAT および VPN 管理アクセス」（P.5-30）を参照してください。
  - NAT ルールでインターフェイスを設定しない：ASA はルート ルックアップを使用して出力インターフェイスを決定します。

次の図に、ルーテッド モードでの出力インターフェイスの選択方法を示します。ほとんどの場合、ルート ルックアップは NAT ルールのインターフェイスと同じです。ただし、一部のコンフィギュレーションでは、2 つの方法が異なる場合があります。

図 5-20　ルーテッド モードでの出力インターフェイスの選択



VPN の NAT

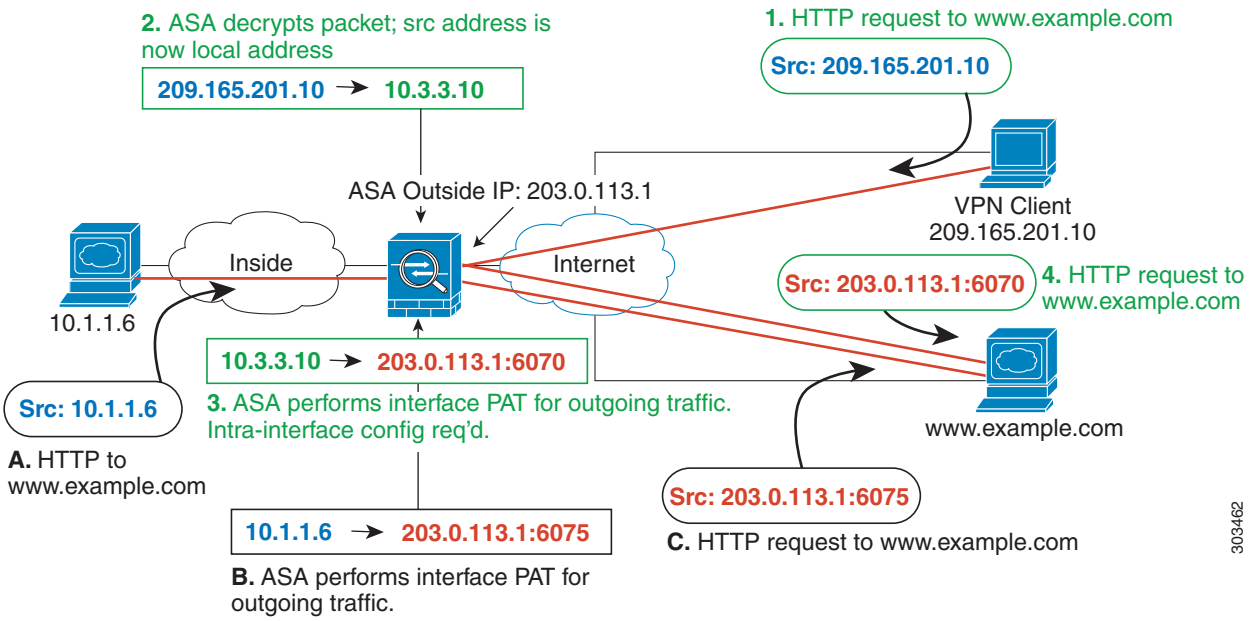
次のトピックでは、さまざまなタイプの VPN を用いた NAT の使用例について説明します。

- 「NAT とリモート アクセス VPN」（P.5-26）
- 「NAT およびサイトツーサイト VPN」（P.5-28）
- 「NAT および VPN 管理アクセス」（P.5-30）
- 「NAT と VPN のトラブルシューティング」（P.5-32）

NAT とリモート アクセス VPN

次の図に、内部サーバ（10.1.1.6）とインターネットにアクセスする VPN クライアント（209.165.201.10）の両方を示します。VPN クライアント用のスプリット トンネリング（指定したトラフィックのみが VPN トンネル上でやりとりされる）を設定しない限り、インターネット バインドされた VPN トラフィックも ASA を経由する必要があります。VPN トラフィックが ASA に渡されると、ASA はパケットを復号化し、得られたパケットには送信元として VPN クライアント ローカル アドレス（10.3.3.10）が含まれています。内部ネットワークと VPN クライアント ローカル ネットワークの両方で、インターネットにアクセスするために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。VPN トラフィックが、入ってきたインターフェイスと同じインターフェイスから出て行けるようにするには、インターフェイス内通信（別名「ヘアピン ネットワーキング」）をイネーブルにする必要があります。

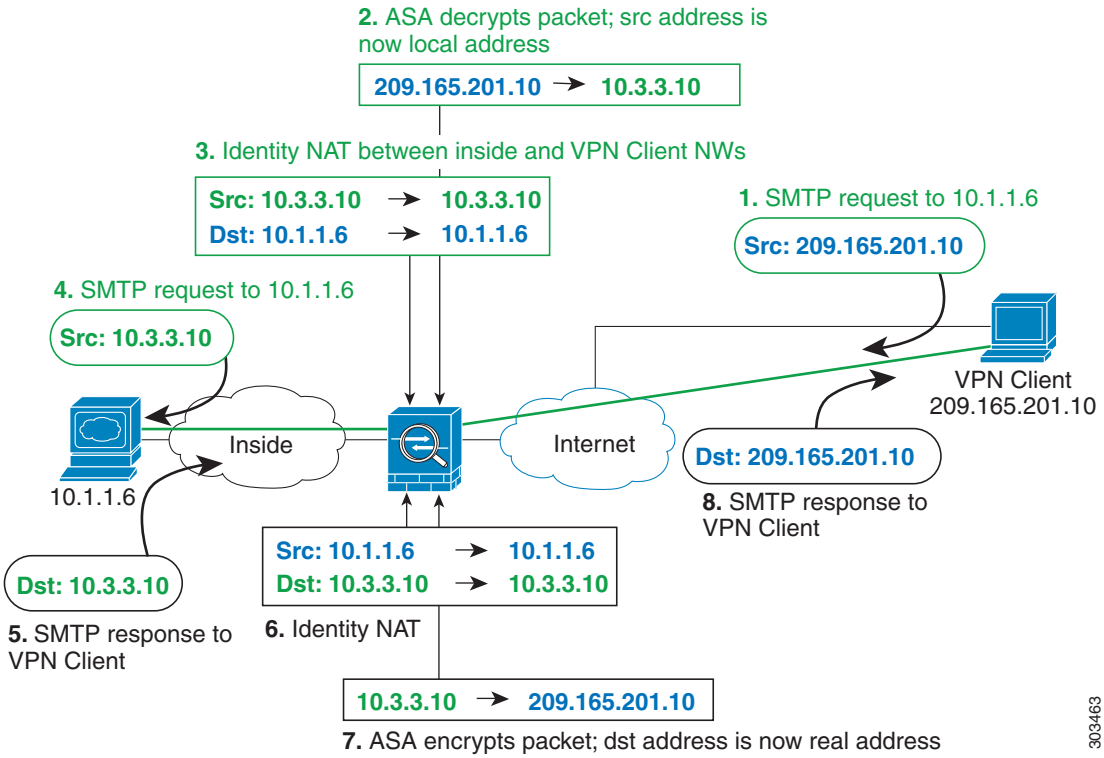
図 5-21　インターネット宛 VPN トラフィックのインターフェイス PAT（インターフェイス内）



次の図に、内部のメール サーバにアクセスする VPN クライアントを示します。ASA は、内部ネットワークと外部ネットワークの間のトラフィックが、インターネット アクセス用に設定したインターフェイス PAT ルールに一致することを期待するので、VPN クライアント（10.3.3.10）から SMTP サーバ（10.1.1.6）へのトラフィックは、リバース パス障害が原因で廃棄されます。10.3.3.10 から 10.1.1.6 へのトラフィックは、NAT ルールに一致しませんが、10.1.1.6 から 10.3.3.10

へのリターン トラフィックは、送信トラフィックのインターフェイス PAT ルールに一致する*必要があります*。順方向および逆方向のフローが一致しないため、ASA は受信時にパケットをドロップします。この障害を回避するには、それらのネットワーク間のアイデンティティ NAT ルールを使用して、インターフェイス PAT ルールから VPN クライアント内部のトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスにアドレスを変換します。

図 5-22　　VPN クライアントのアイデンティティ NAT



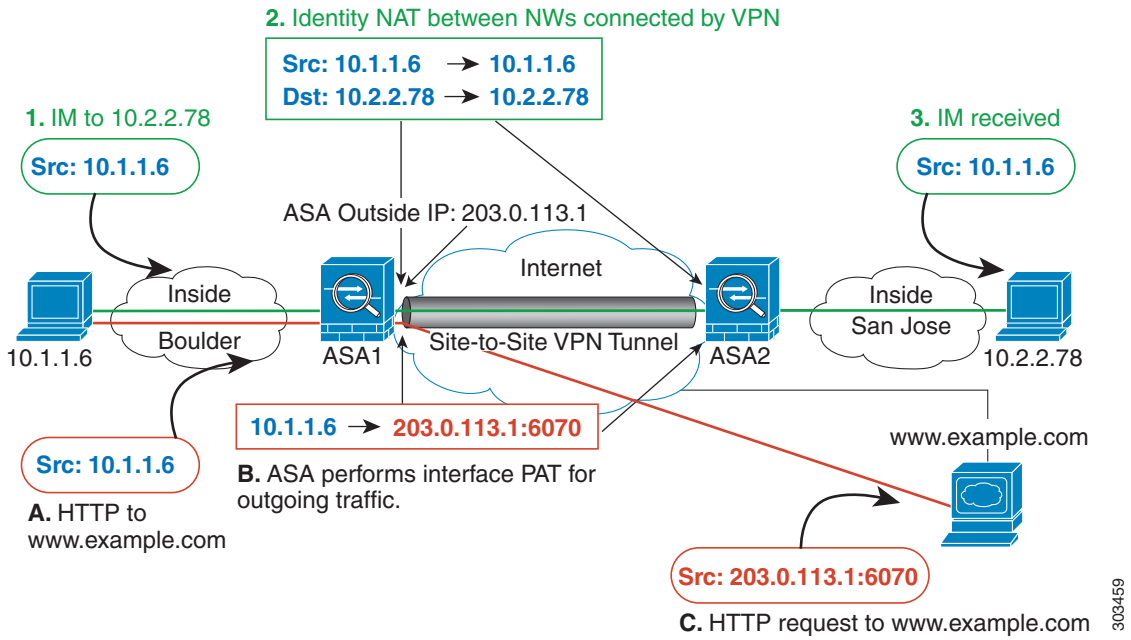
上記のネットワークのための次のサンプル NAT の設定を参照してください。

```
!Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

!Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0
    nat (outside,outside) dynamic interface

!Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
    subnet 10.1.1.0 255.255.255.0
    nat (inside,outside) dynamic interface

!Use twice NAT to pass traffic between the inside network and the VPN client without
!address translation (identity NAT):
nat (inside,outside) source static inside_nw inside_nw destination static vpn_local
vpn_local
```

NAT およびサイトツーサイト VPN

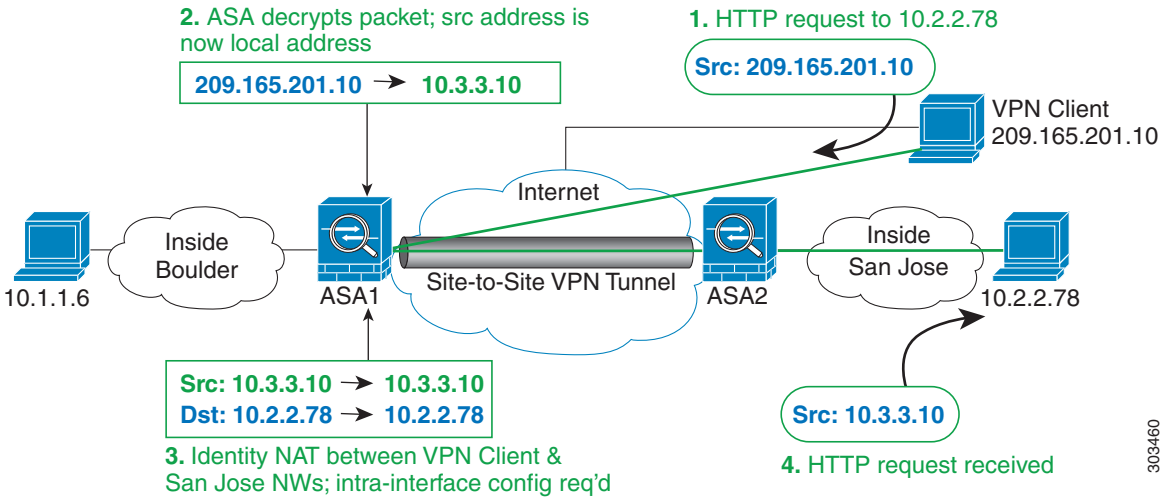
次の図に、ボールダーとサンノゼのオフィスを接続するサイトツーサイト トンネルを示します。インターネットに渡すトラフィックについて（たとえばボールダーの 10.1.1.6 から www.example.com へ）、インターネットへのアクセスのために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。ただし、VPN トンネルを経由するトラフィックについては（たとえば、ボールダーの 10.1.1.6 からサンノゼの 10.2.2.78 へ）、NAT を実行しません。そのため、アイデンティティ NAT ルールを作成して、そのトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスにアドレスを変換します。

図 5-23　サイトツーサイト VPN のためのインターフェイス PAT およびアイデンティティ NAT



次の図に、ASA1（ボールダー）に接続する VPN クライアントと、ASA1 と ASA2（サンノゼ）間のサイトツーサイト トンネル上でアクセス可能なサーバ（10.2.2.78）に対する Telnet 要求を示します。これはヘアピン接続であるため、VPN クライアントからの非スプリット トンネルのインターネット宛トラフィックにも必要な、インターフェイス内通信をイネーブルにする必要があります。アウトバウンド NAT ルールからこのトラフィックを除外するため、VPN に接続された各ネットワーク間で行うのと同様に、VPN クライアントとボールダーおよびサンノゼのネットワーク間でアイデンティティ NAT を設定する必要もあります。

図 5-24　サイト ツーサイト VPN への VPN クライアント アクセス



ASA1（ボールダー）については、次の NAT の設定例を参照してください。

```
!Enable hairpin for VPN client traffic:
same-security-traffic permit intra-interface

!Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0
    nat (outside,outside) dynamic interface

!Identify inside Boulder network, & perform object interface PAT when going to Internet:
object network boulder_inside
    subnet 10.1.1.0 255.255.255.0
    nat (inside,outside) dynamic interface

!Identify inside San Jose network for use in twice NAT rule:
object network sanjose_inside
    subnet 10.2.2.0 255.255.255.0

!Use twice NAT to pass traffic between the Boulder network and the VPN client without
!address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside destination static
vpn_local vpn_local

!Use twice NAT to pass traffic between the Boulder network and San Jose without
!address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside destination static
sanjose_inside sanjose_inside

!Use twice NAT to pass traffic between the VPN client and San Jose without
!address translation (identity NAT):
nat (outside,outside) source static vpn_local vpn_local destination static sanjose_inside
sanjose_inside
```

ASA2（サンノゼ）については、次の NAT の設定例を参照してください。

```
!Identify inside San Jose network, & perform object interface PAT when going to Internet:
object network sanjose_inside
    subnet 10.2.2.0 255.255.255.0
    nat (inside,outside) dynamic interface

!Identify inside Boulder network for use in twice NAT rule:
```

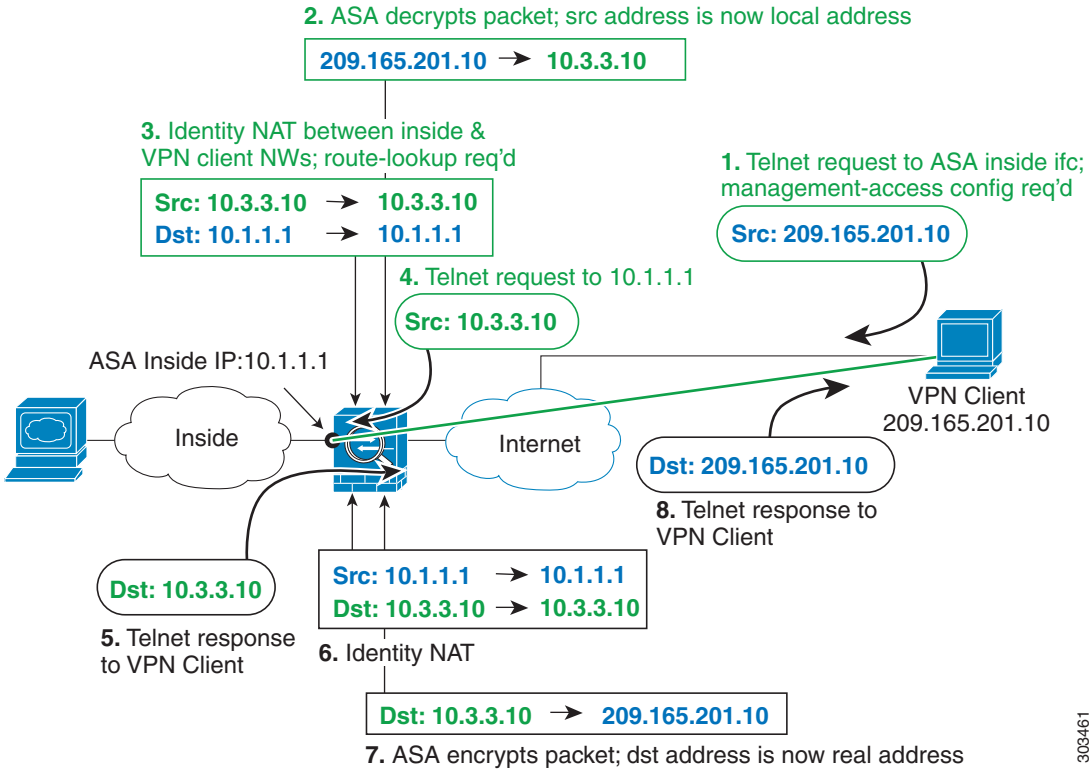
```
object network boulder_inside
    subnet 10.1.1.0 255.255.255.0

!Identify local VPN network for use in twice NAT rule:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0

!Use twice NAT to pass traffic between the San Jose network and Boulder without
!address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside destination static
boulder_inside boulder_inside

!Use twice NAT to pass traffic between the San Jose network and the VPN client without
!address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside destination static
vpn_local vpn_local
```

NAT および VPN 管理アクセス

VPN を使用する場合、ASA を開始したインターフェイス以外のインターフェイスへの管理アクセスを許可することができます。たとえば、外部インターフェイスから ASA を開始する場合、管理アクセス機能では、ASDM、SSH、Telnet、または SNMP を使用して内部インターフェイスに接続することが可能です。または、内部インターフェイスに ping を実行できます。

次の図に、ASA の内部インターフェイスに Telnet 接続する VPN クライアントを示します。管理アクセス インターフェイスを使用し、「NAT とリモート アクセス VPN」（P.5-26）または「NAT およびサイトツーサイト VPN」（P.5-28）に従ってアイデンティティ NAT を設定する場合、ルート ルックアップ オプションを使用して NAT を設定する必要があります。ルート ルックアップがない場合、ASA は、ルーティング テーブルの内容に関係なく、NAT コマンドで指定されたインターフェイスからトラフィックを送信します。次の例では、出力インターフェイスは内部インターフェイスです。ASA で、内部ネットワークに管理トラフィックを送信しません。これは、内部インターフェイスの IP アドレスには戻りません。ルート ルックアップ オプションを使用すると、ASA は、内部ネットワークの代わりに内部インターフェイスの IP アドレスに直接トラフィックを送信できます。VPN クライアントから内部ネットワーク上のホストへのトラフィックの場合、ルート ルックアップ オプションがあっても正しい出力インターフェイス（内部）になるため、通常のトラフィック フローは影響を受けません。ルート ルックアップ オプションの詳細については、「出力インターフェイスの決定」（P.5-25）を参照してください。

図 5-25　VPN 管理アクセス



上記のネットワークのための次のサンプル NAT の設定を参照してください。

```
!Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

!Enable management access on inside ifc:
management-access inside

!Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0
    nat (outside,outside) dynamic interface

!Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
    subnet 10.1.1.0 255.255.255.0
    nat (inside,outside) dynamic interface

!Use twice NAT to pass traffic between the inside network and the VPN client without
!address translation (identity NAT), w/route-lookup:
nat (outside,inside) source static vpn_local vpn_local destination static inside_nw
inside_nw route-lookup
```

NAT と VPN のトラブルシューティング

VPN を使用した NAT の問題をトラブルシューティングするためには、次の監視ツールを参照してください。

- パケット トレーサ：正しく使用した場合、パケット トレーサは、パケットが該当している NAT ルールを表示します。
- **show nat detail**：特定の NAT ルールのヒット カウントおよび変換解除されたトラフィックを表示します。
- **show conn all**：ボックス トラフィックとの間の接続を含むアクティブ接続を表示します。

非動作設定と動作設定に習熟するには、次の手順を実行します。

1. アイデンティティ NAT を使用しない VPN を設定します。
2. **show nat detail** と **show conn all** を入力します。
3. アイデンティティ NAT の設定を追加します。
4. **show nat detail** と **show conn all** を繰り返します。

DNS および NAT

応答内のアドレスを NAT コンフィギュレーションと一致するアドレスに置き換えて、DNS 応答を修正するように ASA を設定することが必要になる場合があります。DNS 修正は、各変換ルールを設定するときに設定できます。

この機能は、NAT ルールに一致する DNS クエリーと応答のアドレスをリライトします（たとえば、IPv4 の A レコード、IPv6 の AAAA レコード、または逆引き DNS クエリーの PTR レコード）。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答では、A レコードはマップされた値から実際の値へリライトされます。逆に、任意のインターフェイスからマッピング インターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へリライトされます。

次に DNS リライトの制限事項を示します。

- 個々の A レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS リライトは PAT には適用されません。
- Twice NAT ルールを設定する場合、送信元アドレスおよび宛先アドレスを指定すると、DNS 修正を設定できません。これらの種類のルールでは、A と B に向かった場合に 1 つのアドレスに対して異なる変換が行われる可能性があります。したがって、ASA は、DNS 応答内の IP アドレスを適切な Twice NAT ルールに一致させることができません。DNS 応答には、DNS 要求を求めたパケット内の送信元アドレスと宛先アドレスの組み合わせに関する情報が含まれません。
- DNS リライトでは、デフォルトでオンになっている DNS アプリケーション インスペクションをイネーブルにする必要があります。詳細については、「DNS インスペクション」（P.9-1）を参照してください。
- 実際には、DNS リライトは NAT ルールではなく xlate エントリで実行されます。したがって、ダイナミック ルールに xlate がない場合、リライトが正しく実行されません。スタティック NAT の場合は、同じような問題は発生しません。

次のトピックで、DNS リライトの例を示します。

- 「DNS 応答修正：Outside 上の DNS サーバ」（P.5-33）
- 「DNS 応答修正：別々のネットワーク上の DNS サーバ、ホスト、サーバ」（P.5-34）

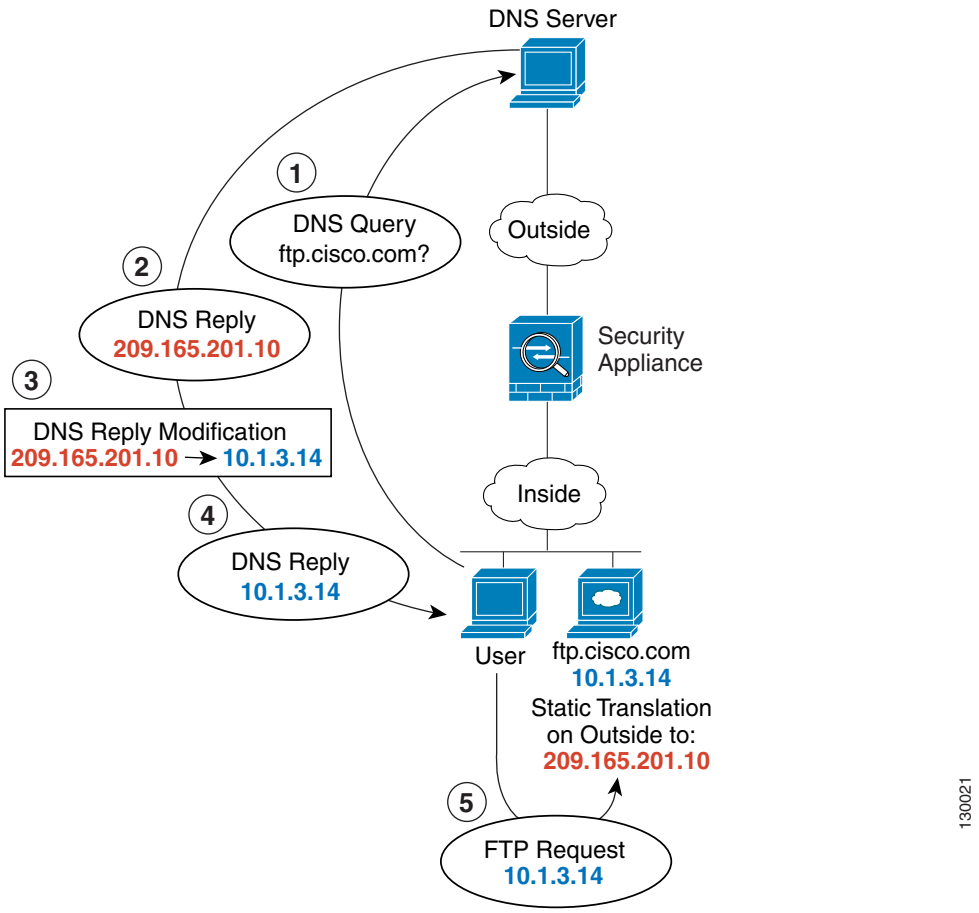
- 「DNS 応答修正：ホスト ネットワーク上の DNS サーバ」（P.5-35）
- 「外部 NAT を使用する DNS64 応答修正」（P.5-35）
- 「PTR の変更、ホスト ネットワークの DNS サーバ」（P.5-37）

DNS 応答修正：Outside 上の DNS サーバ

次の図に、外部インターフェイスからアクセス可能な DNS サーバを示します。ftp.cisco.com というサーバが内部インターフェイス上にあります。ftp.cisco.com の実際のアドレス（10.1.3.14）を、外部ネットワーク上で可視のマッピング アドレス（209.165.201.10）にスタティックに変換するように、ASA を設定します

この場合、このスタティック ルールで DNS 応答修正をイネーブルにする必要があります。これにより、実際のアドレスを使用して ftp.cisco.com にアクセスすることを許可されている内部ユーザは、マッピング アドレスではなく実際のアドレスを DNS サーバから受信できるようになります。内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバは応答でマッピング アドレス（209.165.201.10）を示します。ASA は、内部サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正をイネーブルにしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックを送信することを試みます。

図 5-26　DNS 応答修正：Outside 上の DNS サーバ

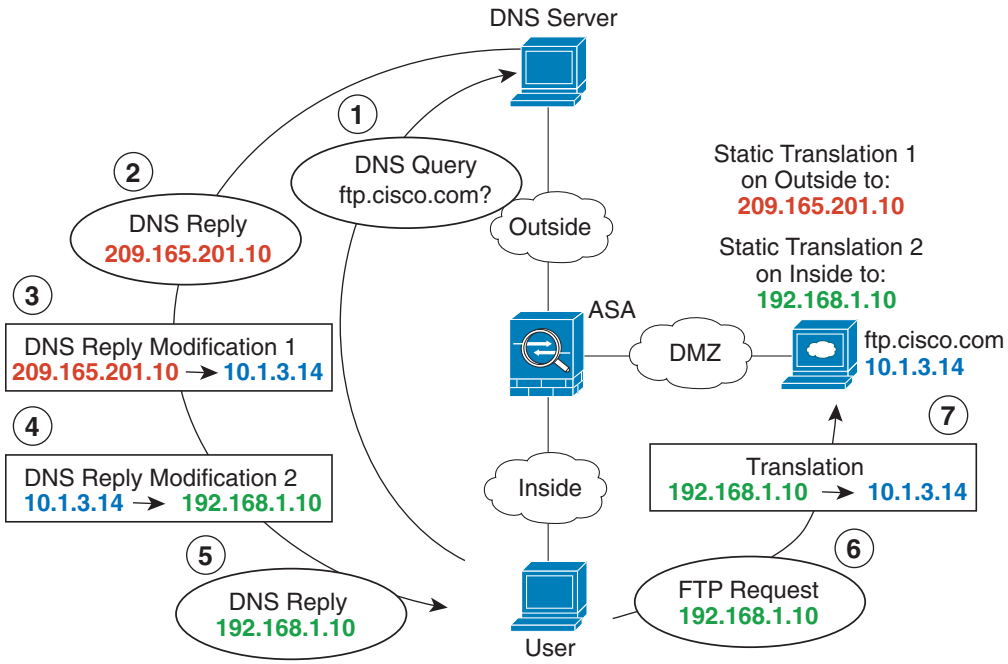


DNS 応答修正：別々のネットワーク上の DNS サーバ、ホスト、サーバ

次の図に、外部 DNS サーバから DMZ ネットワークにある ftp.cisco.com の IP アドレスを要求する内部ネットワークのユーザを示します。DNS サーバは、ユーザが DMZ ネットワーク上に存在しない場合でも、外部と DMZ 間のスタティック ルールに従って応答でマッピング アドレス（209.165.201.10）を示します。ASA は、DNS 応答内のアドレスを 10.1.3.14 に変換します。

ユーザが実際のアドレスを使用して ftp.cisco.com にアクセスする必要がある場合、これ以上の設定は必要ありません。内部と DMZ 間にもスタティック ルールがある場合は、このルールに対して DNS 応答修正もイネーブルにする必要があります。このとき、DNS 応答は 2 回修正されます。この場合、ASA は内部と DMZ 間のスタティック ルールに従って、DNS 応答内のアドレスを再度 192.168.1.10 に変換します。

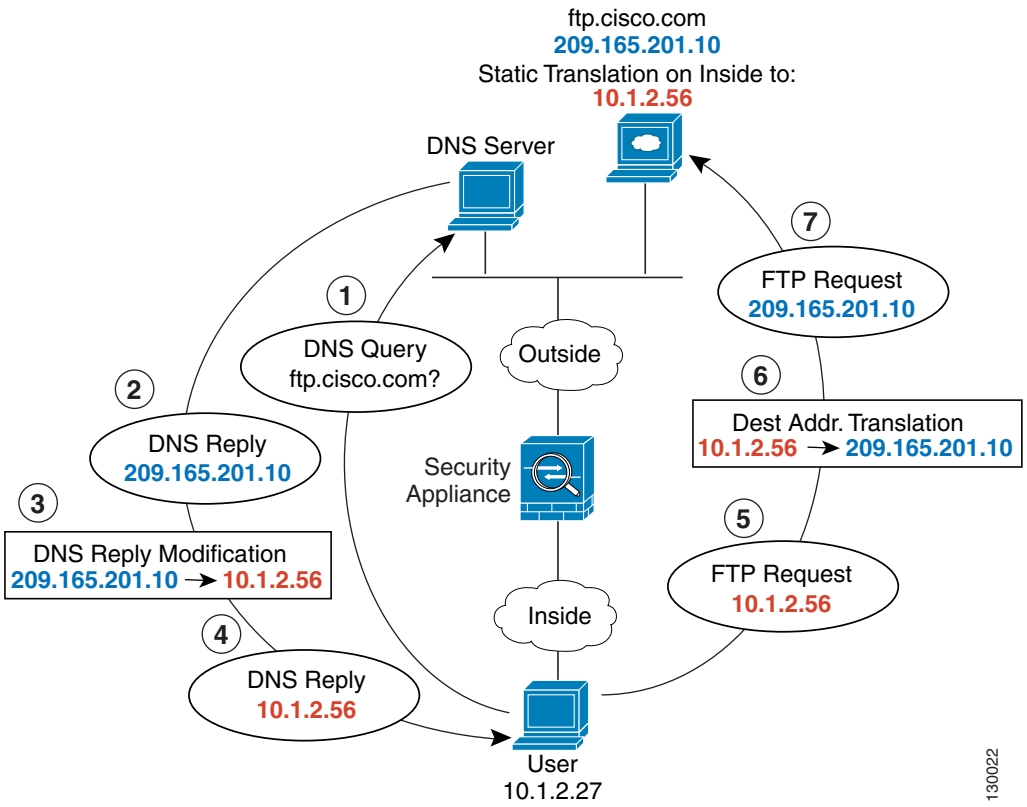
図 5-27　DNS 応答修正：別々のネットワーク上の DNS サーバ、ホスト、サーバ



DNS 応答修正：ホスト ネットワーク上の DNS サーバ

次の図に、外部の FTP サーバと DNS サーバを示します。ASA には、外部サーバ用のスタティック変換があります。この場合、ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答で実際のアドレス 209.165.20.10 を示します。ftp.cisco.com のマッピング アドレス（10.1.2.56）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。

図 5-28　DNS 応答修正：ホスト ネットワーク上の DNS サーバ

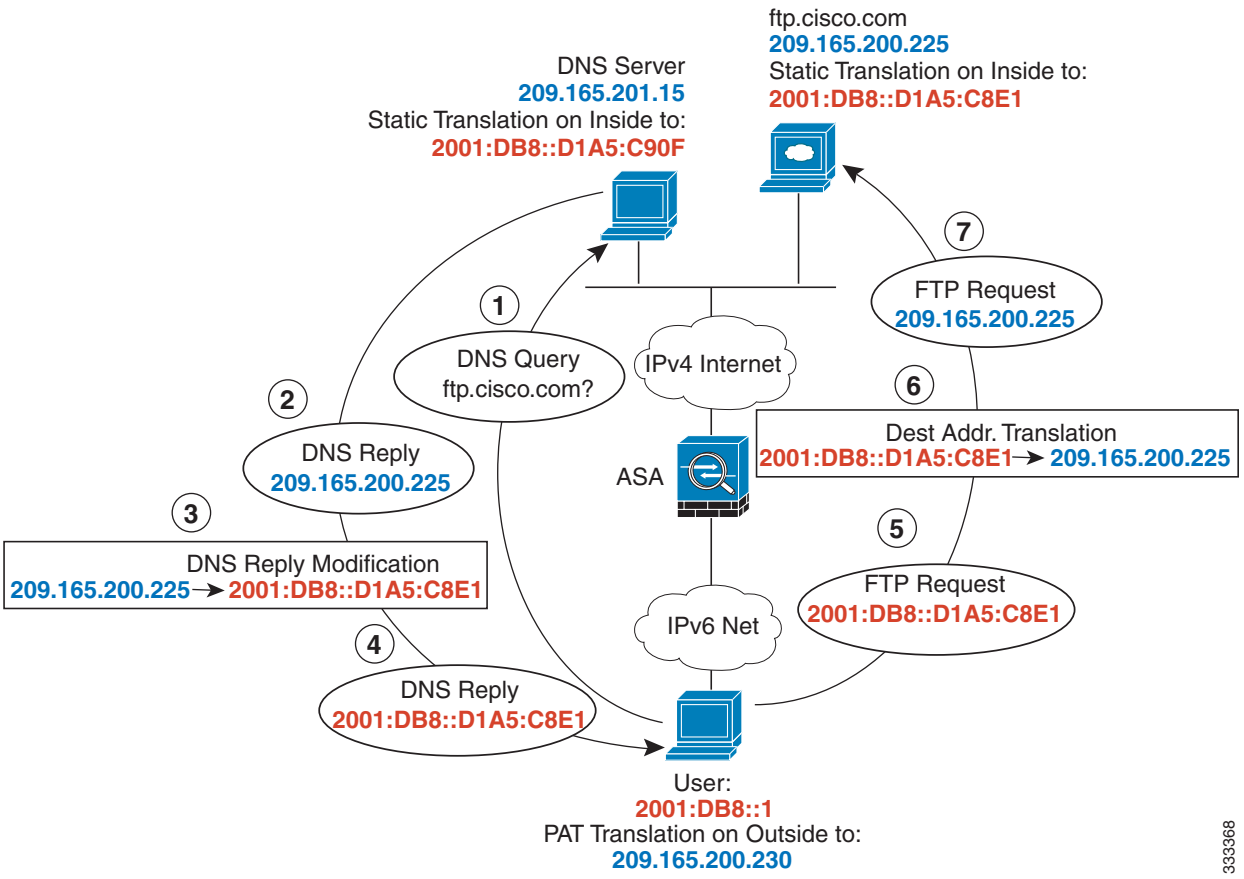


外部 NAT を使用する DNS64 応答修正

次の図に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。ASA には、外部サーバ用のスタティック変換があります。この場合に、内部 IPv6 ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答として実際のアドレス 209.165.200.225 を返します。

ftp.cisco.com のマッピング アドレス（2001:DB8::D1A5:C8E1）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。この例には、DNS サーバのスタティック NAT 変換、および内部 IPv6 ホストの PAT ルールも含まれています。

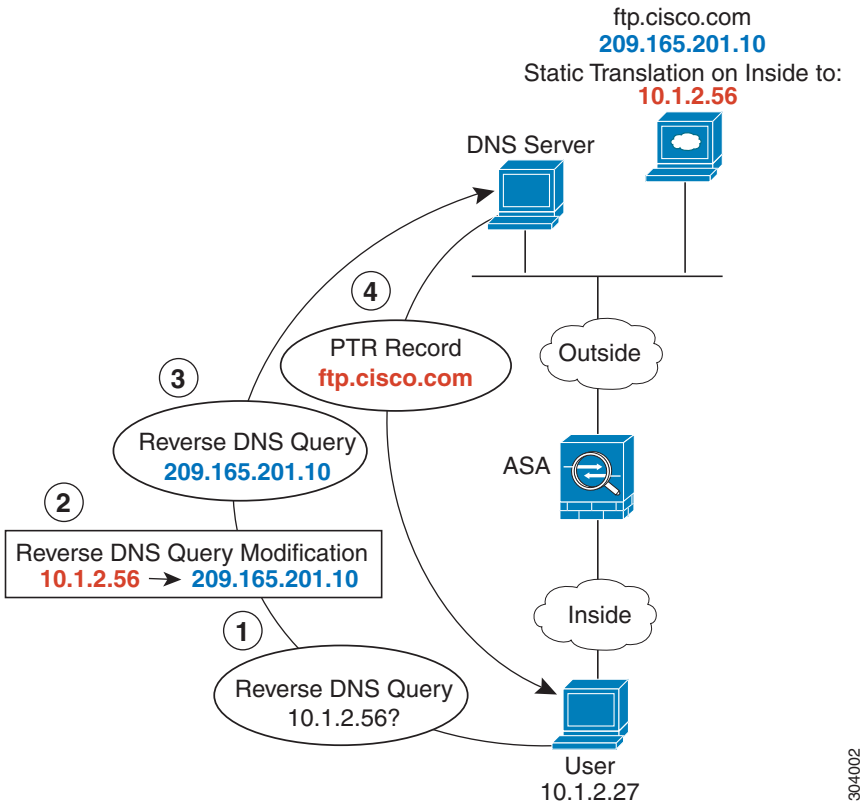
図 5-29　外部 NAT を使用する DNS64 応答修正



PTR の変更、ホスト ネットワークの DNS サーバ

次の図に、外部の FTP サーバと DNS サーバを示します。ASA には、外部サーバ用のスタティック変換があります。この場合、内部のユーザが 10.1.2.56 の逆引き DNS ルックアップを実行する場合、ASA は実際のアドレスを使用して逆引き DNS クエリーを変更し、DNS サーバはサーバ名、ftp.cisco.com を使用して応答します。

図 5-30　PTR の変更、ホスト ネットワークの DNS サーバ



次の作業

ネットワーク オブジェクト NAT を設定するには、第 6 章「ネットワーク オブジェクト NAT（ASA 8.3 以降）」を参照してください。

Twice NAT を設定するには、第 7 章「Twice NAT（ASA 8.3 以降）」を参照してください

次の作業

CHAPTER 6

ネットワーク オブジェクト NAT（ASA 8.3 以降）

ネットワーク オブジェクトのパラメータとして設定されているすべての NAT ルールは、*ネットワーク オブジェクト NAT* ルールと見なされます。ネットワーク オブジェクト NAT は、1 つの IP アドレス、アドレスの範囲、またはサブネットに対して NAT を設定するための迅速かつ容易な方法です。ネットワーク オブジェクトを設定したら、このオブジェクトのマッピング アドレスを識別できます。

この章では、ネットワーク オブジェクト NAT 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。

- 「ネットワーク オブジェクト NAT に関する情報」（P.6-1）
- 「ネットワーク オブジェクト NAT のライセンス要件」（P.6-2）
- 「ネットワーク オブジェクト NAT の前提条件」（P.6-2）
- 「ガイドラインと制限事項」（P.6-2）
- 「デフォルト設定」（P.6-4）
- 「ネットワーク オブジェクト NAT の設定」（P.6-4）
- 「ネットワーク オブジェクト NAT のモニタリング」（P.6-21）
- 「ネットワーク オブジェクト NAT の設定例」（P.6-22）
- 「ネットワーク オブジェクト NAT の機能履歴」（P.6-47）

（注） NAT の機能の詳細については、第 5 章「ネットワーク アドレス変換（NAT）（ASA 8.3 以降）」を参照してください。

ネットワーク オブジェクト NAT に関する情報

パケットが ASA に入ると、送信元 IP アドレスと宛先 IP アドレスの両方がネットワーク オブジェクト NAT ルールと照合されます。個別の照合が行われる場合、パケット内の送信元 IP アドレスと宛先 IP アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはありません。したがって、宛先 X に向かう場合は送信元アドレスが A と変換され、宛先 Y に向かう場合は B と変換されるように指定することはできません。この種の機能には、Twice NAT を使用します（Twice NAT を使用すると、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます）。

Twice NAT とネットワーク オブジェクト NAT の違いの詳細については、「NAT の実装方法」（P.5-15）を参照してください。

ネットワーク オブジェクト NAT ルールは、NAT ルール テーブルのセクション 2 に追加されます。NAT の順序付けの詳細については、「NAT ルールの順序」（P.5-20）を参照してください。

ネットワーク オブジェクト NAT のライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

ネットワーク オブジェクト NAT の前提条件

コンフィギュレーションによっては、必要に応じてマッピング アドレスをインラインで設定したり、マッピング アドレスの別のネットワーク オブジェクトまたはネットワーク オブジェクト グループを作成したりできます。ネットワーク オブジェクト グループは、非連続的な IP アドレス範囲または複数のホストやサブネットで構成されるマッピング アドレスを作成する場合に特に便利です。ネットワーク オブジェクトまたはグループを作成するには、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

オブジェクトおよびグループに関する特定のガイドラインについては、設定する NAT タイプの設定の項を参照してください。「ガイドラインと制限事項」（P.6-2）も参照してください。

ガイドラインと制限事項

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

- ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。
- トランスペアレント モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定する必要があります。--Any-- は使用できません。
- トランスペアレント モードでは、インターフェイス PAT を設定できません。トランスペアレント モードのインターフェイスには、IP アドレスが設定されていないためです。管理 IP アドレスもマッピング アドレスとして使用できません。
- トランスペアレント モードでは、IPv4 ネットワークと IPv6 ネットワークとの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。

IPv6 のガイドライン

- IPv6 をサポートします。「NAT と IPv6」（P.5-15）も参照してください。
- ルーテッド モードの場合は、IPv4 と IPv6 との間の変換もできます。
- トランスペアレント モードの場合は、IPv4 ネットワークと IPv6 ネットワークとの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。
- トランスペアレント モードの場合は、PAT プールは IPv6 に対してはサポートされません。
- スタティック NAT の場合は、/64 までの IPv6 サブネットを指定できます。これよりも大きいサブネットはサポートされません。
- FTP を NAT46 とともに使用する場合は、IPv4 FTP クライアントが IPv6 FTP サーバに接続するときに、クライアントは拡張パッシブ モード（EPSV）または拡張ポート モード（EPRT）を使用する必要があります。PASV コマンドおよび PORT コマンドは IPv6 ではサポートされません。

その他のガイドライン

- 定義できる NAT ルールは 1 つのオブジェクトに対して 1 つだけです。1 つのオブジェクトに対して複数の NAT ルールを設定する場合は、複数のオブジェクトを作成する必要があります。それぞれに異なる名前を付け、IP アドレスは同じものを指定します。たとえば、**object network obj-10.10.10.1-01**、**object network obj-10.10.10.1-02** などとします。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT コンフィギュレーションが使用されるようにするには、**clear xlate** コマンドを使用して変換テーブルを消去します。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

（注） ダイナミック NAT または PAT ルールを削除し、次に削除したルールに含まれるアドレスと重複するマッピング アドレスを含む新しいルールを追加すると、新しいルールは、削除されたルールに関連付けられたすべての接続がタイムアウトするか、**clear xlate** コマンドを使用してクリアされるまで使用されません。この予防手段のおかげで、同じアドレスが複数のホストに割り当てられないようにできます。

- NAT で使用されるオブジェクトおよびオブジェクト グループを未定義にすることはできません。IP アドレスを含める必要があります。
- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。
- 同じマッピング オブジェクトやグループを複数の NAT ルールで使用できます。
- マッピング IP アドレス プールは、次のアドレスを含むことができません。
  - マッピング インターフェイスの IP アドレス。ルールに --Any-- インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT（ルーテッド モードのみ）の場合、IP アドレスの代わりにインターフェイス名を使用します。
  - （トランスペアレント モード）管理 IP アドレス。
  - （ダイナミック NAT）VPN がイネーブルの場合は、スタンバイ インターフェイスの IP アドレス。
  - 既存の VPN プールのアドレス。

- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- NAT や PAT に伴うアプリケーション インスペクションの制限については、第 8 章「アプリケーション レイヤ プロトコル インスペクションの準備」の「デフォルト インスペクションと NAT に関する制限事項」（P.8-6）を参照してください。

デフォルト設定

- （ルーテッド モード）デフォルトの実際のインターフェイスおよびマッピング インターフェイスは Any で、すべてのインターフェイスにルールが適用されます。
- （8.3(1)、8.3(2)、8.4(1)）アイデンティティ NAT のデフォルト動作で、プロキシ ARP はディセーブルにされます。これは設定できません。（8.4(2) 以降）アイデンティティ NAT のデフォルト動作で、プロキシ ARP はイネーブルにされ、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP をディセーブルにできます。詳細については、「NAT パケットのルーティング」（P.5-22）を参照してください。
- オプションのインターフェイスを指定する場合、ASA によって NAT コンフィギュレーションが使用されて、出力インターフェイスが決定されます。（8.3(1) ～ 8.4(1)）唯一の例外はアイデンティティ NAT です。アイデンティティ NAT では、NAT コンフィギュレーションに関係なく、常にルート ルックアップが使用されます。（8.4(2) 以降）アイデンティティ NAT の場合、デフォルト動作は NAT コンフィギュレーションの使用ですが、代わりにルート ルックアップを常に使用するオプションがあります。詳細については、「NAT パケットのルーティング」（P.5-22）を参照してください。

ネットワーク オブジェクト NAT の設定

この項では、ネットワーク オブジェクト NAT を設定する方法について説明します。

- 「ダイナミック NAT または PAT プールを使用したダイナミック PAT の設定」（P.6-4）
- 「ダイナミック PAT（隠蔽）の設定」（P.6-10）
- 「スタティック NAT またはポート変換を設定したスタティック NAT の設定」（P.6-13）
- 「アイデンティティ NAT の設定」（P.6-17）
- 「Per-Session PAT ルールの設定」（P.6-20）

ダイナミック NAT または PAT プールを使用したダイナミック PAT の設定

この項では、ダイナミック NAT または PAT プールを使用するダイナミック PAT のためのネットワーク オブジェクト NAT を設定する方法について説明します。詳細については、「ダイナミック NAT」（P.5-8）または「ダイナミック PAT」（P.5-10）を参照してください。

ガイドライン

PAT プールの場合：

- 使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。したがって、1024 未満のポートに使用できるのは、小さな PAT プール 1 つだけです。（8.4(3) 以降、8.5(1) または 8.6(1) を除く）下位ポート範囲を使用するトラフィックが数多くある場合は、PAT プールに対して、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。1024 ～ 65535 または 1 ～ 65535 です。
- 同じ PAT プール オブジェクトを 2 つの異なるルールの中で使用する場合は、必ず同じオプションを各ルールに指定してください。たとえば、1 つのルールで拡張 PAT およびフラットな範囲が指定される場合は、もう一方のルールでも拡張 PAT およびフラットな範囲が指定される必要があります。

PAT プールに対する拡張 PAT の場合：

- 多くのアプリケーション インスペクションでは、拡張 PAT はサポートされていません。サポート対象外のインスペクションの完全な一覧については、第 8 章「アプリケーション レイヤ プロトコル インスペクションの準備」の「デフォルト インスペクションと NAT に関する制限事項」（P.8-6）を参照してください。
- ダイナミック PAT ルールに対して拡張 PAT をイネーブルにする場合は、PAT プール内のアドレスを、ポート変換ルールを設定した別のスタティック NAT の PAT アドレスとしても使用することはできません。たとえば、PAT プールに 10.1.1.1 が含まれている場合、PAT アドレスとして 10.1.1.1 を使用する、ポート変換ルールを設定したスタティック NAT は作成できません。
- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。
- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。

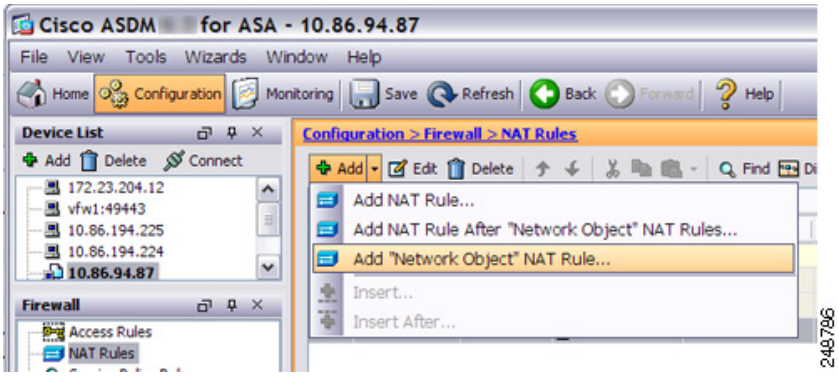
PAT プールのラウンドロビンの場合：

- ホストに既存の接続がある場合は、そのホストからの以降の接続は同じ PAT IP アドレスを使用します（ポートが使用可能である場合）。**注**：この「粘着性」は、フェールオーバーが発生すると失われます。ASA がフェールオーバーすると、ホストからの後続の接続では最初の IP アドレスが使用されない場合があります。
- ラウンドロビンでは、特に拡張 PAT と組み合わせた場合に、大量のメモリが消費されます。NAT プールはマッピングされるプロトコル/IP アドレス/ポート範囲ごとに作成されるため、ラウンドロビンでは数多くの同時 NAT プールが作成され、メモリが使用されます。拡張 PAT では、さらに多くの同時 NAT プールが作成されます。

手順の詳細

ステップ 1　新規または既存のネットワーク オブジェクトに NAT を追加します。

- 新しいネットワーク オブジェクトを追加するには、[Configuration] > [Firewall] > [NAT Rules] を選択し、[Add] > [Add Network Object NAT Rule] をクリックします。



- 既存のネットワーク オブジェクトに NAT を追加するには、[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] を選択し、ネットワーク オブジェクトをダブルクリックします。

詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

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

ステップ 2　新しいオブジェクトの場合は、次のフィールドに値を入力します。

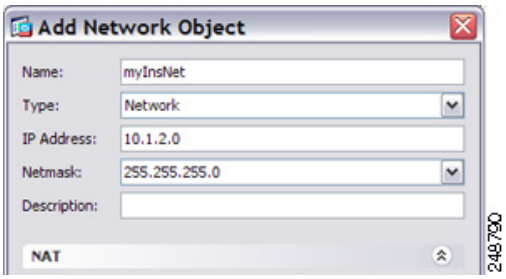
a. [Name]：オブジェクト名。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。

b. [Type]：ホスト、ネットワーク、または範囲。

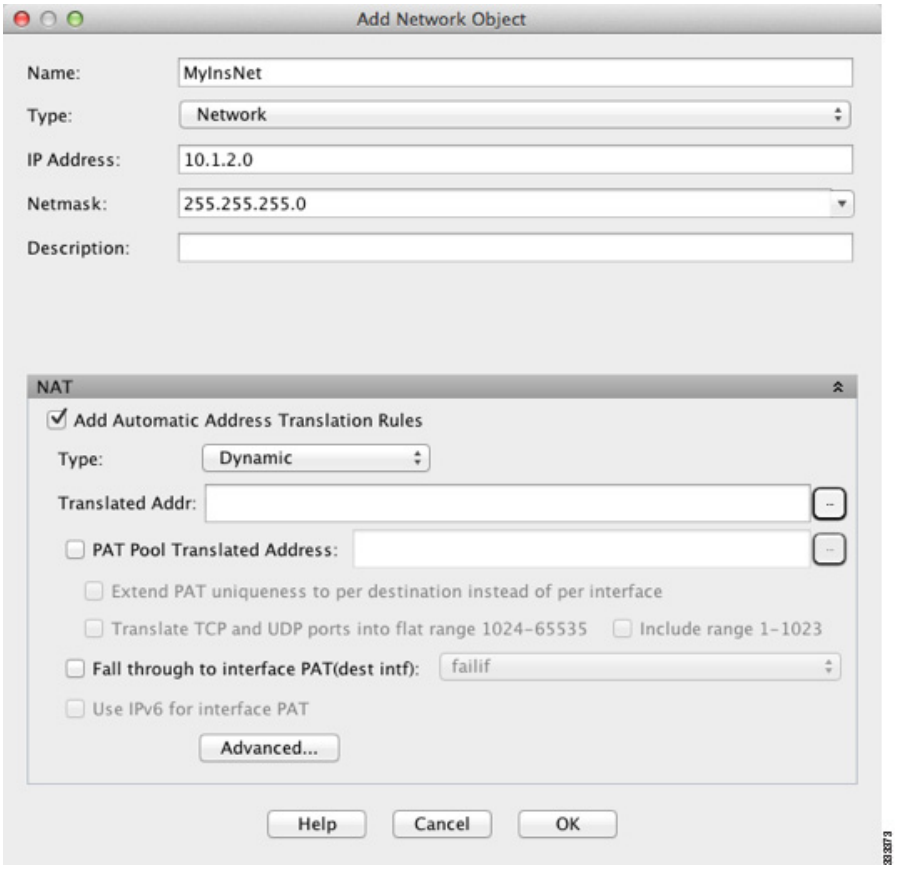
c. [IP Address] : IPv4 または IPv6 アドレス。オブジェクト タイプとして [Range] を選択した場合は、[IP Address] フィールドは、開始アドレスと終了アドレスを入力できるように変更されます。

d. [Netmask/Prefix Length]：サブネット マスクまたはプレフィックス長を入力します。

e. [Description]：（オプション）ネットワーク オブジェクトの説明（最大 200 文字）。



ステップ 3　[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。

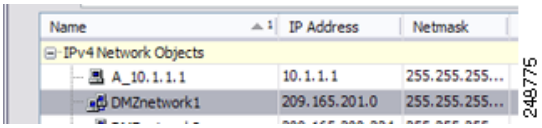


ステップ 4　[Add Automatic Translation Rules] チェックボックスをオンにします。

ステップ 5　[Type] ドロップダウン リストから、[Dynamic] を選択します。PAT プールを使用するダイナミック PAT を設定する場合であっても、[Dynamic] を選択してください。

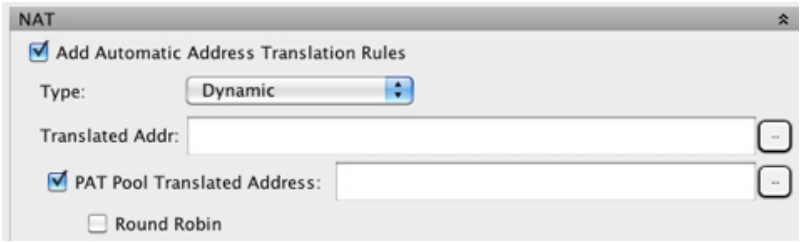
ステップ 6　ダイナミック NAT、または PAT プールを使用するダイナミック PAT を設定します。

- ダイナミック NAT：[Translated Addr] フィールドの右の参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスで、既存のネットワーク オブジェクトを選択するか新しいオブジェクトを作成します。



（注）　オブジェクトまたはグループは、サブネットを含むことはできません。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。

- PAT プールを使用したダイナミック PAT：フォールバックの PAT プールを有効にします。



a. [Translated Addr] フィールドには値を入力 せず、空白のままにしてください。

b. [PAT Pool Translated Address] チェックボックスをオンにしてから、参照ボタンをクリックして、[Browse Translated PAT Pool Address] ダイアログボックスで既存のネットワーク オブジェクトを選択するか新しいネットワーク オブジェクトを作成します。

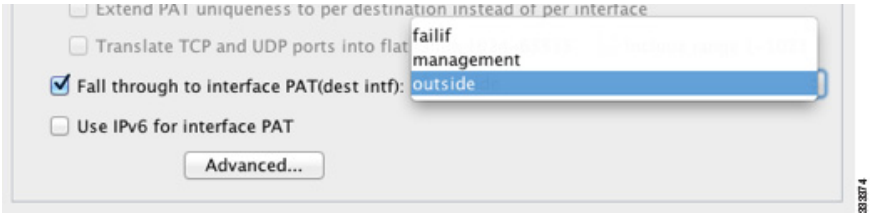
（注）　PAT プール オブジェクトまたはグループには、サブネットを含むことはできません。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。

c. （オプション）アドレス/ポートをラウンドロビン方式で割り当てるには、[Round Robin] チェックボックスをオンにします。デフォルトではラウンドロビンは使用されず、1 つの PAT アドレスのポートがすべて割り当てられると次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレス/ポートが割り当てられると最初のアドレスに戻り、次に 2 番目のアドレスというように順に使用されます。

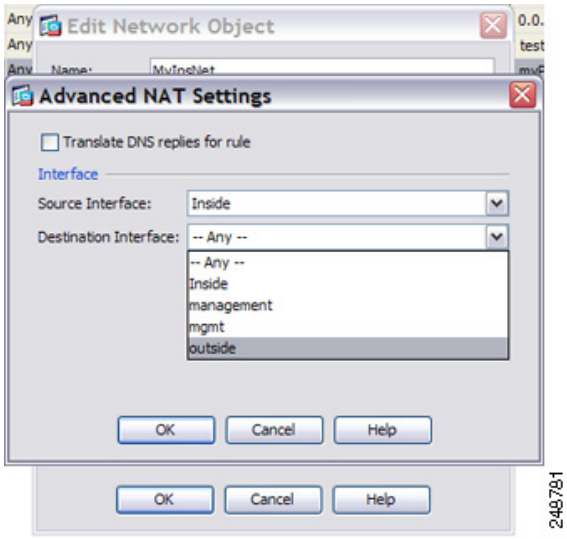
d. （任意、8.4(3) 以降、ただし 8.5(1) と 8.6(1) を除く）拡張 PAT を使用する場合は、[Extend PAT uniqueness to per destination instead of per interface] チェックボックスをオンにします。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、*サービス*ごとに 65535 個のポートが使用されます。通常は、PAT 変換を作成するときに宛先ポートとアドレスは考慮されないため、PAT アドレスごとに 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。

e. （任意、8.4(3) 以降、ただし 8.5(1) と 8.6(1) を除く）ポートを割り当てるときに 1024 ～ 65535 のポート範囲を 1 つのフラット範囲として使用するには、[Translate TCP or UDP ports into flat range (1024-65535)] チェックボックスをオンにします。変換のマッピング ポート番号を選択するときに、ASA によって、使用可能な場合は実際の送信元ポート番号が使用されます。ただし、このオプションを設定しないと、実際のポートが使用 *できない* 場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の全範囲を使用するには、[Include range 1 to 1023] チェックボックスもオンにします。

ステップ 7　（任意、ルーテッド モードのみ）他のマッピング アドレスがすべて割り当て済みの場合にインターフェイス IP アドレスをバックアップ方法として使用するには、[Fall through to interface PAT (dest intf)] チェックボックスをオンにして、インターフェイスをドロップダウン リストから選択します。インターフェイスの IPv6 アドレスを使用するには、[Use IPv6 for interface PAT] チェックボックスをオンにします。



ステップ 8　（オプション）[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。



- [Translate DNS replies for rule]：DNS 応答内の IP アドレスを変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。詳細については、「DNS および NAT」（P.5-32）を参照してください。
- （トランスペアレント ファイアウォール モードの場合に必須）[Source Interface]：この NAT ルールを適用する実際のインターフェイスを指定します。デフォルトでは、ルールはすべてのインターフェイスに適用されます。
- （トランスペアレント ファイアウォール モードの場合に必須）[Destination Interface]：この NAT ルールが適用されるマッピング インターフェイスを指定します。デフォルトでは、ルールはすべてのインターフェイスに適用されます。

入力が終わったら、[OK] をクリックします。[Add/Edit Network Object] ダイアログボックスに戻ります。

ステップ 9　[OK] をクリックし、さらに [Apply] をクリックします。

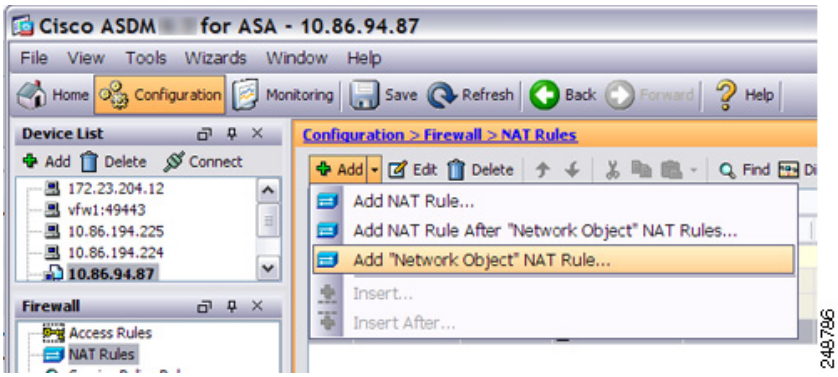
ダイナミック PAT（隠蔽）の設定

この項では、ダイナミック PAT（隠蔽）のためのネットワーク オブジェクト NAT の設定方法について説明します。PAT プールを使用するダイナミック PAT については、この項ではなく、「ダイナミック NAT または PAT プールを使用したダイナミック PAT の設定」（P.6-4）を参照してください。詳細については、「ダイナミック PAT」（P.5-10）を参照してください。

手順の詳細

ステップ 1　新規または既存のネットワーク オブジェクトに NAT を追加します。

- 新しいネットワーク オブジェクトを追加するには、[Configuration] > [Firewall] > [NAT Rules] を選択し、[Add] > [Add Network Object NAT Rule] をクリックします。



- 既存のネットワーク オブジェクトに NAT を追加するには、[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] を選択し、ネットワーク オブジェクトをダブルクリックします。

詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

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

ステップ 2　新しいオブジェクトの場合は、次のフィールドに値を入力します。

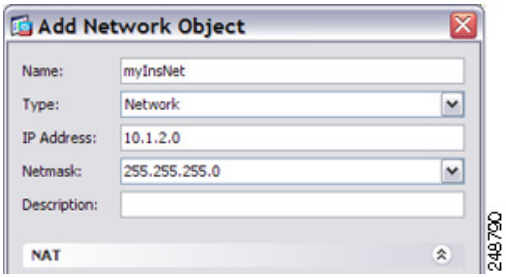
a. [Name]：オブジェクト名。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。

b. [Type]：ホスト、ネットワーク、または範囲。

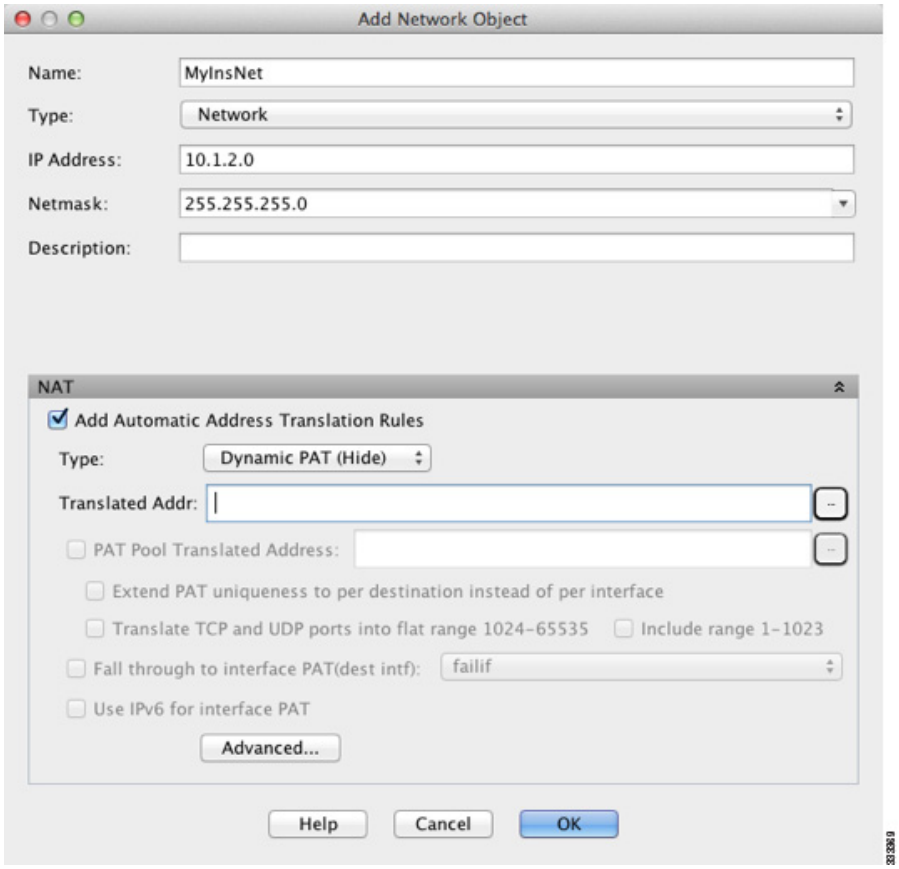
c. [IP Address]：IPv4 または IPv6 アドレス。オブジェクト タイプとして [Range] を選択した場合は、[IP Address] フィールドは、開始アドレスと終了アドレスを入力できるように変更されます。

d. [Netmask/Prefix Length]：サブネット マスクまたはプレフィックス長を入力します。

e. [Description]：（オプション）ネットワーク オブジェクトの説明（最大 200 文字）。



ステップ 3　[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 4　[Add Automatic Translation Rules] チェックボックスをオンにします。

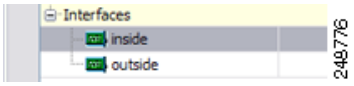
ステップ 5　[Type] ドロップダウン リストから、[Dynamic PAT (Hide)] を選択します。

（注）　1 つのアドレスの代わりに PAT プールを使用してダイナミック PAT を設定する方法については、「ダイナミック NAT または PAT プールを使用したダイナミック PAT の設定」（P.6-4）を参照してください。

ステップ 6　マッピング アドレスを 1 つだけ指定します。[Translated Addr] フィールドには、次のいずれかの方法で、マッピング IP アドレスを指定します。

- ホスト IP アドレスを入力します。

- インターフェイス名を入力するか、または参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスでインターフェイスを選択します。

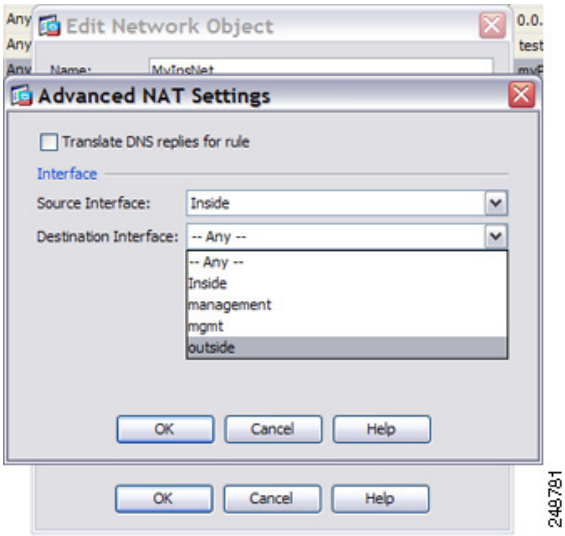


インターフェイス名を指定する場合は、*インターフェイス PAT* をイネーブルにしてください。このときに指定したインターフェイス IP アドレスがマッピング アドレスとして使用されます。IPv6 インターフェイス アドレスを使用するには、[Use IPv6 for interface PAT] もオンにする必要があります。インターフェイス PAT を使用する場合は、NAT ルールが適用されるのは指定したマッピング インターフェイスのみとなります（インターフェイス PAT を使用しない場合は、ルールはデフォルトですべてのインターフェイスに適用されます）。実際のインターフェイスも [--Any--] ではなく特定のインターフェイスとなるように設定する方法については、ステップ 7 を参照してください。

（注） トランスペアレント モードでは、インターフェイスを指定することはできません。

- 参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスで既存のホスト アドレスを選択します。
- 参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスで新しい名前付きオブジェクトを作成します。

ステップ 7　（オプション）[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。



- [Translate DNS replies for rule]：DNS 応答内の IP アドレスを変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。詳細については、「DNS および NAT」（P.5-32）を参照してください。
- （トランスペアレント ファイアウォール モードの場合に必須）[Source Interface]：この NAT ルールを適用する実際のインターフェイスを指定します。デフォルトでは、ルールはすべてのインターフェイスに適用されます。

- （トランスペアレント ファイアウォール モードの場合に必須）[Destination Interface]：この NAT ルールが適用されるマッピング インターフェイスを指定します。デフォルトでは、ルールはすべてのインターフェイスに適用されます。

入力が終わったら、[OK] をクリックします。[Add/Edit 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、さらに [Apply] をクリックします。

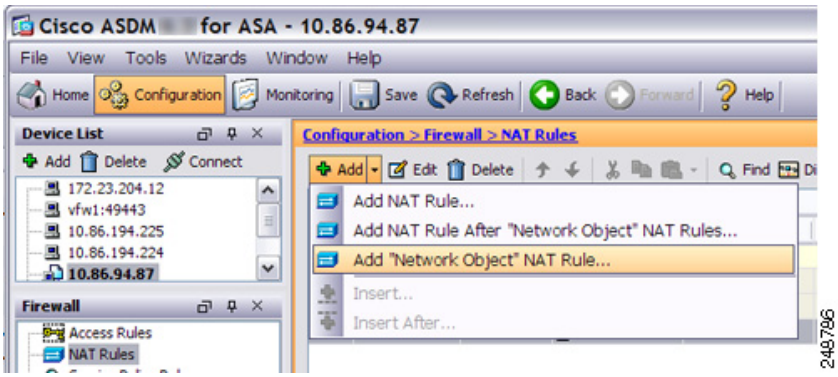
スタティック NAT またはポート変換を設定したスタティック NAT の設定

この項では、ネットワーク オブジェクト NAT を使用してスタティック NAT ルールを設定する方法について説明します。詳細については、「スタティック NAT」（P.5-3）を参照してください。

手順の詳細

ステップ 1　新規または既存のネットワーク オブジェクトに NAT を追加します。

- 新しいネットワーク オブジェクトを追加するには、[Configuration] > [Firewall] > [NAT Rules] を選択し、[Add] > [Add Network Object NAT Rule] をクリックします。



- 既存のネットワーク オブジェクトに NAT を追加するには、[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] を選択し、ネットワーク オブジェクトをダブルクリックします。

詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

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

ステップ 2　新しいオブジェクトの場合は、次のフィールドに値を入力します。

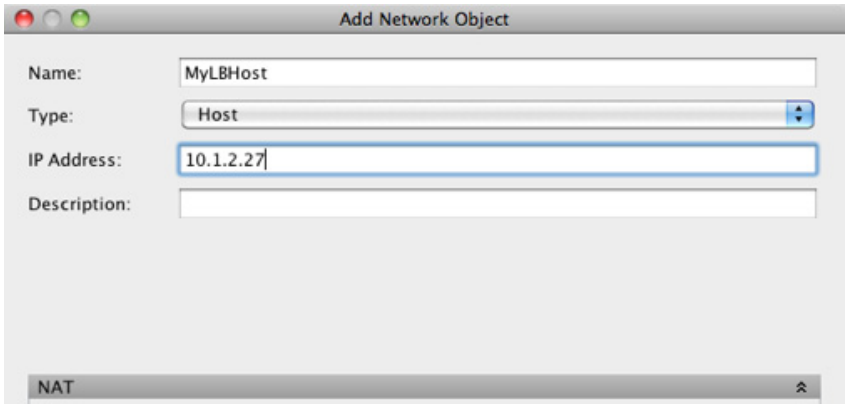
a.　[Name]：オブジェクト名。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。

b.　[Type]：ネットワーク、ホスト、または範囲。

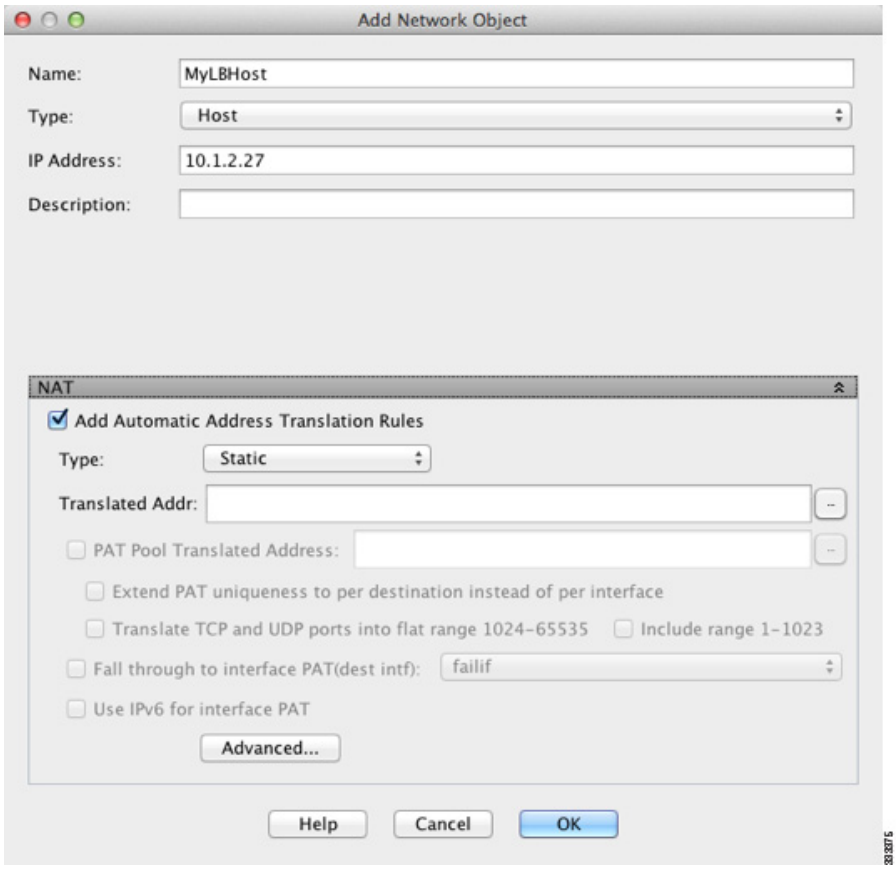
c.　[IP Address] : IPv4 または IPv6 アドレス。オブジェクト タイプとして [Range] を選択した場合は、[IP Address] フィールドは、開始アドレスと終了アドレスを入力できるように変更されます。

d.　[Netmask/Prefix Length]：サブネット マスクまたはプレフィックス長を入力します。

e. [Description]：（オプション）ネットワーク オブジェクトの説明（最大 200 文字）。



ステップ 3　[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 4　[Add Automatic Translation Rules] チェックボックスをオンにします。

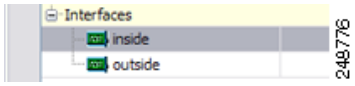
ステップ 5　[Type] ドロップダウン リストから、[Static] を選択します。

ステップ 6　[Translated Addr] フィールドで、次のいずれかを実行します。

- IP アドレスを入力します。

  IP アドレスを入力すると、マッピングされるネットワークのネットマスクや範囲は、実際のネットワークのものと同一になります。たとえば、実際のネットワークがホストの場合、このアドレスは、ホスト アドレスです。範囲の場合、マッピング アドレスには、実際の範囲と同じ数のアドレスが含まれます。たとえば、実際のアドレスが 10.1.1.1 ～ 10.1.1.6 の範囲として定義され、172.20.1.1 をマッピング アドレスとして指定する場合、マッピング範囲には、172.20.1.1 ～ 172.20.1.6 が含まれます。

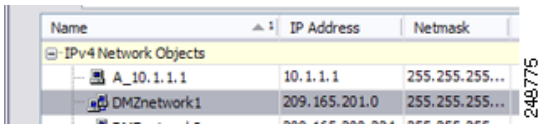
- （ポート変換を設定したスタティック NAT の場合のみ）インターフェイス名を入力するか、参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスでインターフェイス名を選択します。



  IPv6 インターフェイス アドレスを使用するには、[Use IPv6 for interface PAT] もオンにする必要があります。[Advanced NAT Settings] ダイアログボックスでのサービスの設定も必ず行ってください（ステップ 8 を参照）。（トランスペアレント モードでは、インターフェイスを指定することはできません）。

- 参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスで既存のアドレスを選択します。

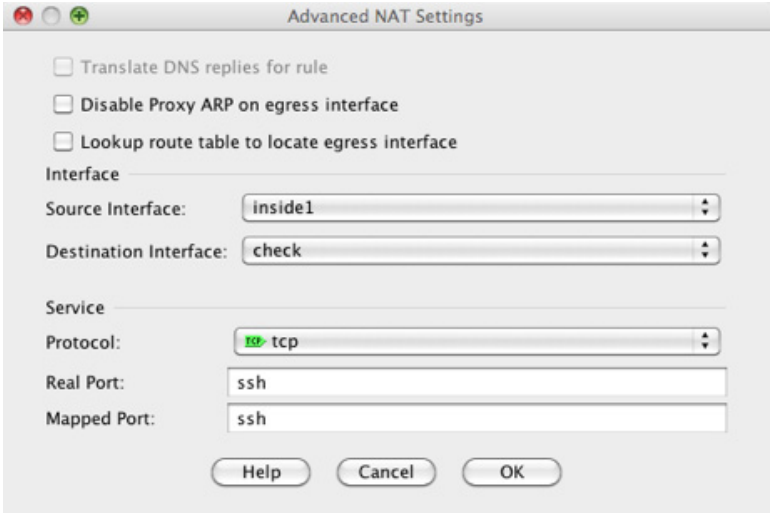
- 参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスで新しいアドレスを作成します。



通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。詳細については、「スタティック NAT」（P.5-3）を参照してください。

ステップ 7　（オプション）NAT46 の場合、[Use one-to-one address translation] をオンにします。NAT 46 の場合、最初の IPv4 アドレスを最初の IPv6 アドレス、2 番目の IPv4 アドレスを 2 番目の IPv6 アドレス、以下同様に 1 対 1 で順に変換するように指定します。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このキーワードを使用する必要があります。

ステップ 8　（オプション）[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。

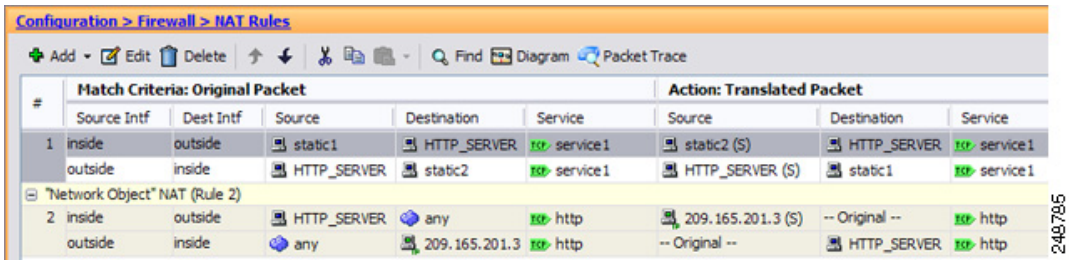


- [Translate DNS replies for rule]：DNS 応答内の IP アドレスを変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。詳細については、「DNS および NAT」（P.5-32）を参照してください。
- [Disable Proxy ARP on egress interface]：マッピング IP アドレスへの着信パケットのプロキシ ARP をディセーブルにします。詳細については、「マッピング アドレスとルーティング」（P.5-22）を参照してください。
- （トランスペアレント ファイアウォール モードの場合に必須）[Interface]：
  - [Source Interface]：この NAT ルールを適用する実際のインターフェイスを指定します。デフォルトでは、ルールはすべてのインターフェイスに適用されます。
  - [Destination Interface]：この NAT ルールが適用されるマッピング インターフェイスを指定します。デフォルトでは、ルールはすべてのインターフェイスに適用されます。
- [Service]：
  - [Protocol]：ポート変換を設定したスタティック NAT を設定します。[tcp] または [udp] を選択します。
  - [Real Port]：ポート番号または予約済みポートの名前（たとえば「ftp」）のいずれかを入力できます。
  - [Mapped Port]：ポート番号または予約済みポートの名前（たとえば「ftp」）のいずれかを入力できます。

入力が終わったら、[OK] をクリックします。[Add/Edit Network Object] ダイアログボックスに戻ります。

ステップ 9　[OK] をクリックし、さらに [Apply] をクリックします。

スタティック ルールが二方向である（開始を実際のホストの間で許可する）ため、NAT ルール テーブルは各スタティック ルールに対して、各方向に 1 つずつ 2 つの行を表示します。



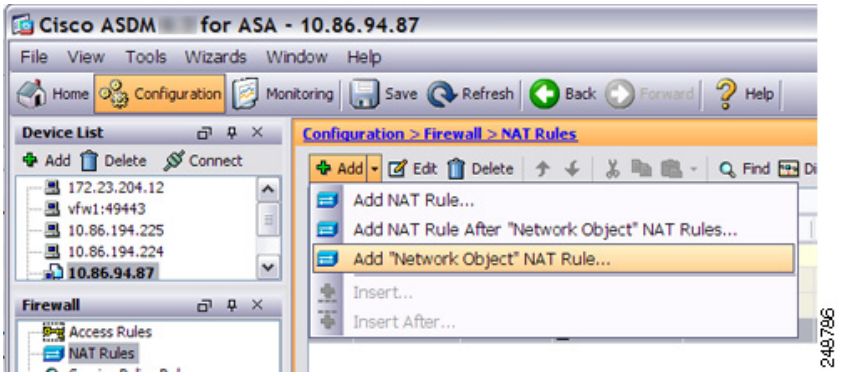
アイデンティティ NAT の設定

この項では、ネットワーク オブジェクト NAT を使用してアイデンティティ NAT ルールを設定する方法について説明します。詳細については、「アイデンティティ NAT」（P.5-12）を参照してください。

手順の詳細

ステップ 1　新規または既存のネットワーク オブジェクトに NAT を追加します。

- 新しいネットワーク オブジェクトを追加するには、[Configuration] > [Firewall] > [NAT Rules] を選択し、[Add] > [Add Network Object NAT Rule] をクリックします。



- 既存のネットワーク オブジェクトに NAT を追加するには、[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] を選択し、ネットワーク オブジェクトをダブルクリックします。

詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

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

ステップ 2　新しいオブジェクトの場合は、次のフィールドに値を入力します。

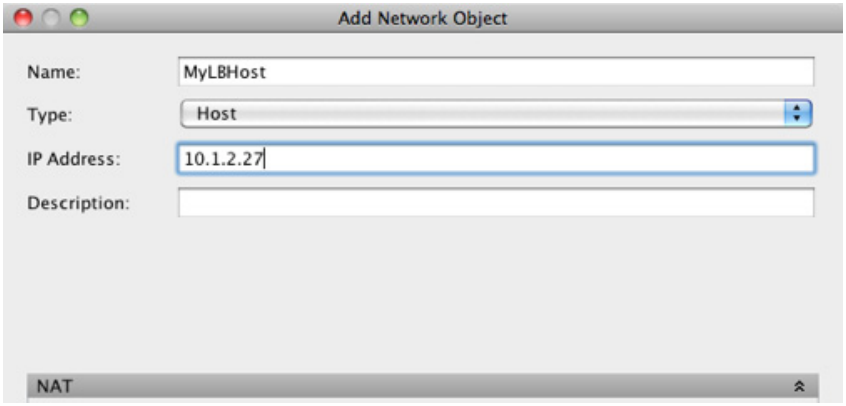
a. [Name]：オブジェクト名。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。

b. [Type]：ネットワーク、ホスト、または範囲。

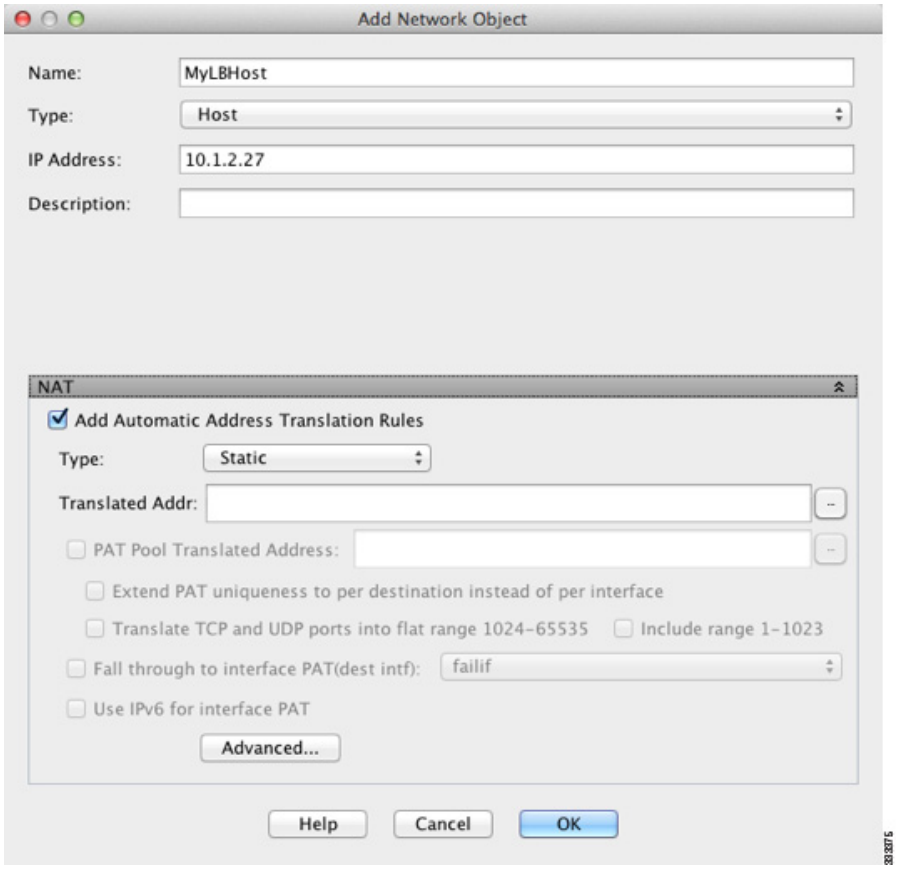
c. [IP Address]：IPv4 または IPv6 アドレス。オブジェクト タイプとして [Range] を選択した場合は、[IP Address] フィールドは、開始アドレスと終了アドレスを入力できるように変更されます。

d. [Netmask/Prefix Length]：サブネット マスクまたはプレフィックス長を入力します。

e. [Description]：（オプション）ネットワーク オブジェクトの説明（最大 200 文字）。



ステップ 3　[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。



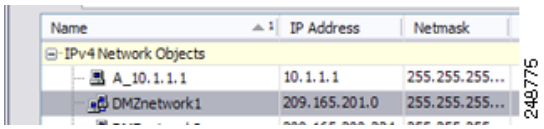
ステップ 4　[Add Automatic Translation Rules] チェックボックスをオンにします。

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

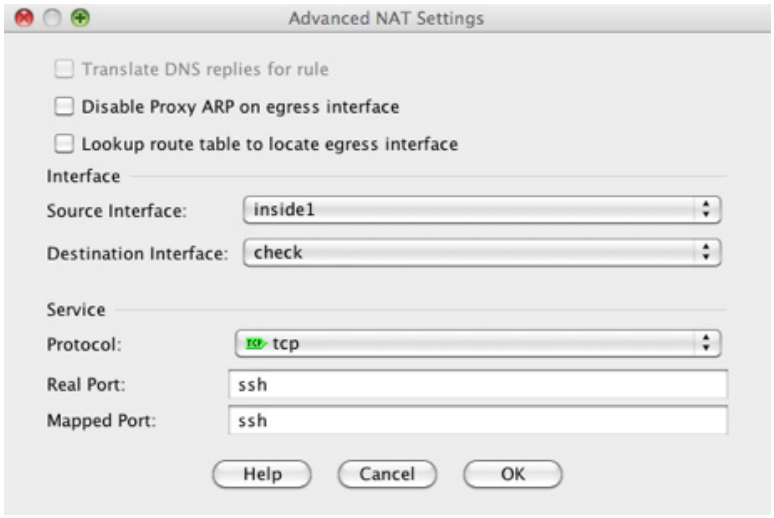
ステップ 6　[Translated Addr] フィールドで、次のいずれかを実行します。

- 実際のアドレスに使用したのと同じ IP アドレスを入力します。

- 参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスで、一致する IP アドレス定義を持つネットワーク オブジェクトを選択します。
- 参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスで、一致する IP アドレス定義を持つネットワーク オブジェクトを作成します。



ステップ 7　（オプション）[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。

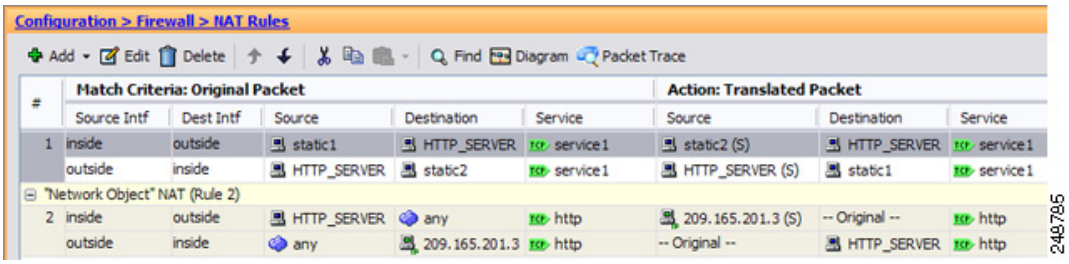


- [Disable Proxy ARP on egress interface]：マッピング IP アドレスへの着信パケットのプロキシ ARP をディセーブルにします。詳細については、「マッピング アドレスとルーティング」（P.5-22）を参照してください。
- （ルーテッド モード、インターフェイスを指定）[Lookup route table to locate egress interface]：NAT コマンドに指定したインターフェイスを使用する代わりに、ルート ルックアップを使用して出力インターフェイスを決定します。詳細については、「出力インターフェイスの決定」（P.5-25）を参照してください。
- （トランスペアレント ファイアウォール モードの場合に必須）[Interface]：
  - [Source Interface]：この NAT ルールを適用する実際のインターフェイスを指定します。デフォルトでは、ルールはすべてのインターフェイスに適用されます。
  - [Destination Interface]：この NAT ルールが適用されるマッピング インターフェイスを指定します。デフォルトでは、ルールはすべてのインターフェイスに適用されます。

このダイアログボックスのその他の設定は変更しないでください。入力が終わったら、[OK] をクリックします。[Add/Edit 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、さらに [Apply] をクリックします。

スタティック ルールが二方向である（開始を実際のホストの間で許可する）ため、NAT ルール テーブルは各スタティック ルールに対して、各方向に 1 つずつ 2 つの行を表示します。



Per-Session PAT ルールの設定

デフォルトでは、すべての TCP PAT トラフィックおよびすべての UDP DNS トラフィックが Per-Session PAT を使用します。トラフィックに Multi-Session PAT を使用するには、Per-Session PAT ルールを設定します。許可ルールで Per-Session PAT を使用し、拒否ルールで Multi-Session PAT を使用します。Per-Session PAT と Multi-Session PAT の詳細については、「Per-Session PAT と Multi-Session PAT（バージョン 9.0(1) 以降）」（P.5-11）を参照してください。

デフォルト

デフォルトでは、次のルールがインストールされます。

- any（IPv4 および IPv6）から any（IPv4 および IPv6）への TCP を許可する
- any（IPv4 および IPv6）からドメインへの UDP を許可する

これらのルールは、ルール テーブルに表示されません。

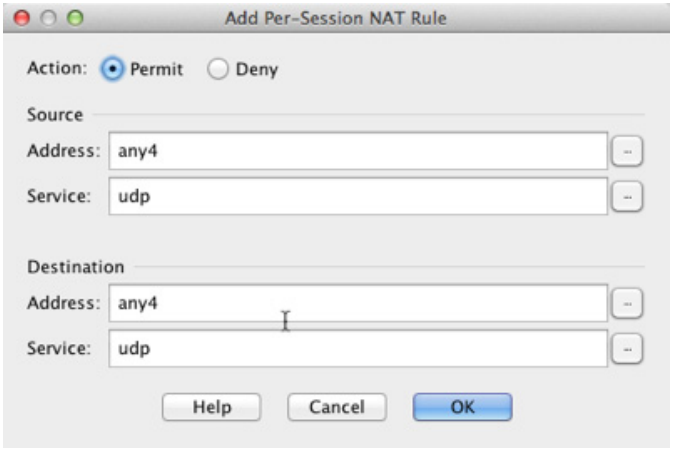
（注）　これらのルールは削除できません。これらのルールは常に、手動作成されたルールの後に存在します。ルールは順番に評価されるので、デフォルト ルールを無効にすることができます。たとえば、これらのルールを完全に反転させるには、次のものを追加します。

- any（IPv4 および IPv6）から any（IPv4 および IPv6）への TCP を拒否する
- any（IPv4 および IPv6）からドメインへの UDP を拒否する

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Advanced] > [Per-Session NAT Rules] を選択し、[Add] > [Add Per-Session NAT Rule] をクリックします。

ステップ 2　[Permit] または [Deny] をクリックします。



許可ルールは、per-session PAT を使用し、拒否ルールは multi-session PAT を使用します。

ステップ 3　アドレスを入力するか、または [...] ボタンをクリックし、オブジェクトを選択して、送信元アドレスを指定します。

ステップ 4　送信元サービスに UDP または TCP を指定します。通常は宛先ポートだけを指定しますが、任意で送信元ポートを指定できます。[UDP/port] または [TCP/port] に入力するか、[...] ボタンをクリックして、共通の値またはオブジェクトを選択します。

ステップ 5　アドレスを入力するか、または [...] ボタンをクリックし、オブジェクトを選択して、宛先アドレスを指定します。

ステップ 6　宛先サービスに UDP または TCP を指定します。これは送信元サービスと一致する必要があります。任意で宛先ポートを指定できます。[UDP/port] または [TCP/port] に入力するか、[...] ボタンをクリックして、共通の値またはオブジェクトを選択します。

ステップ 7　[OK] をクリックします。

ステップ 8　[Apply] をクリックします。

ネットワーク オブジェクト NAT のモニタリング

[Monitoring] > [Properties] > [Connection Graphs] > [Xlates] ペインでは、アクティブなネットワーク アドレス変換をグラフィック形式で表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs]：グラフ化できるコンポーネントを一覧表示します。
  - [Xlate Utilization]：ASA の NAT の使用状況を表示します。
- [Graph Window Title]：グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add]：[Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove]：[Selected Graphs] リストから選択したエントリを削除するには、このフィールドをクリックします。

- [Show Graphs]：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

[Monitoring] > [Properties] > [Connection Graphs] > [Perfmon] ペインでは、パフォーマンス情報をグラフィック形式で表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs]：グラフ化できるコンポーネントを一覧表示します。
  - [AAA Perfmon]：ASA の AAA パフォーマンス情報を表示します。
  - [Inspection Perfmon]：ASA の検査パフォーマンス情報を表示します。
  - [Web Perfmon]：URL アクセスおよび URL サーバ要求などの ASA の Web パフォーマンス情報を表示します。
  - [Connections Perfmon]：ASA の接続パフォーマンス情報を表示します。
  - [Xlate Perfmon]：ASA の NAT パフォーマンス情報を表示します。
- [Graph Window Title]：グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add]：[Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove]：[Selected Graphs] リストから選択した統計タイプを削除するには、このフィールドをクリックします。
- [Show Graphs]：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

ネットワーク オブジェクト NAT の設定例

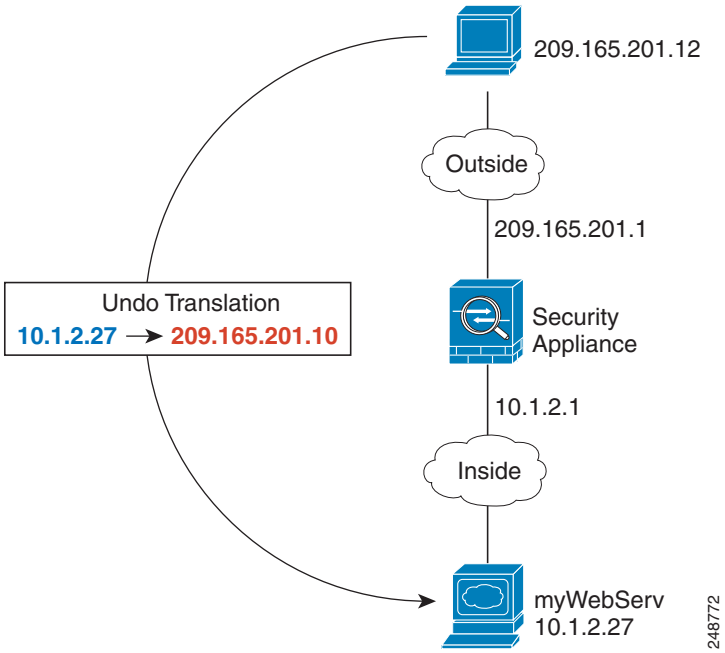
ここでは、次の設定例を示します。

- 「内部 Web サーバへのアクセスの提供（スタティック NAT）」（P.6-23）
- 「内部ホストの NAT（ダイナミック NAT）および外部 Web サーバの NAT（スタティック NAT）」（P.6-25）
- 「複数のマッピング アドレス（スタティック NAT、1 対多）を持つ内部ロード バランサ」（P.6-30）
- 「FTP、HTTP、および SMTP のための単一アドレス（ポート変換を設定したスタティック NAT）」（P.6-34）
- 「マッピング インターフェイス上の DNS サーバ、実際のインターフェイス上の Web サーバ（DNS 修正を設定したスタティック NAT）」（P.6-37）
- 「マッピング インターフェイス上の DNS サーバおよび FTP サーバ、FTP サーバが変換される（DNS 修正を設定したスタティック NAT）」（P.6-40）
- 「マッピング インターフェイス上の IPv4 DNS サーバおよび FTP サーバ、実際のインターフェイス上の IPv6 ホスト（DNS64 修正を設定したスタティック NAT64）」（P.6-42）

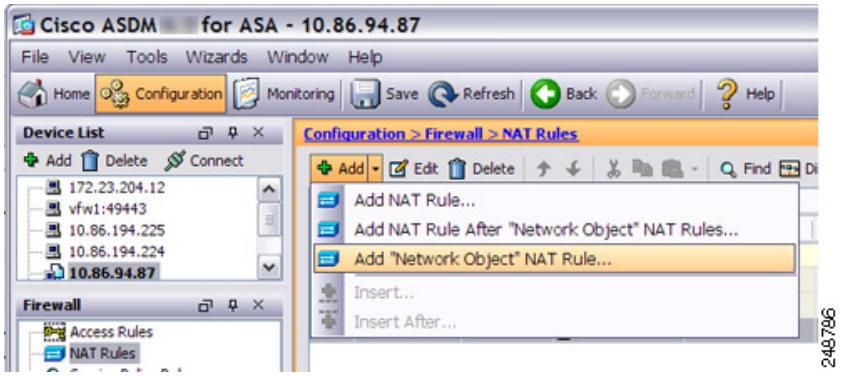
内部 Web サーバへのアクセスの提供（スタティック NAT）

次の例では、内部 Web サーバに対してスタティック NAT を実行します。実際のアドレスはプライベート ネットワーク上にあるので、パブリック アドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバへのトラフィックをホストが開始できるようにするために必要です （図 6-1 を参照）。

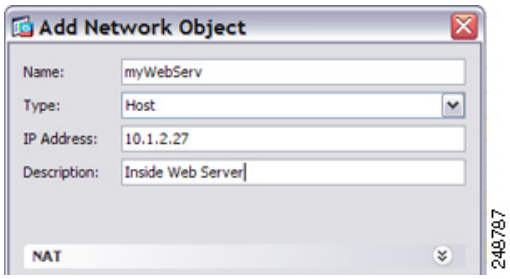
図 6-1　内部 Web サーバのスタティック NAT



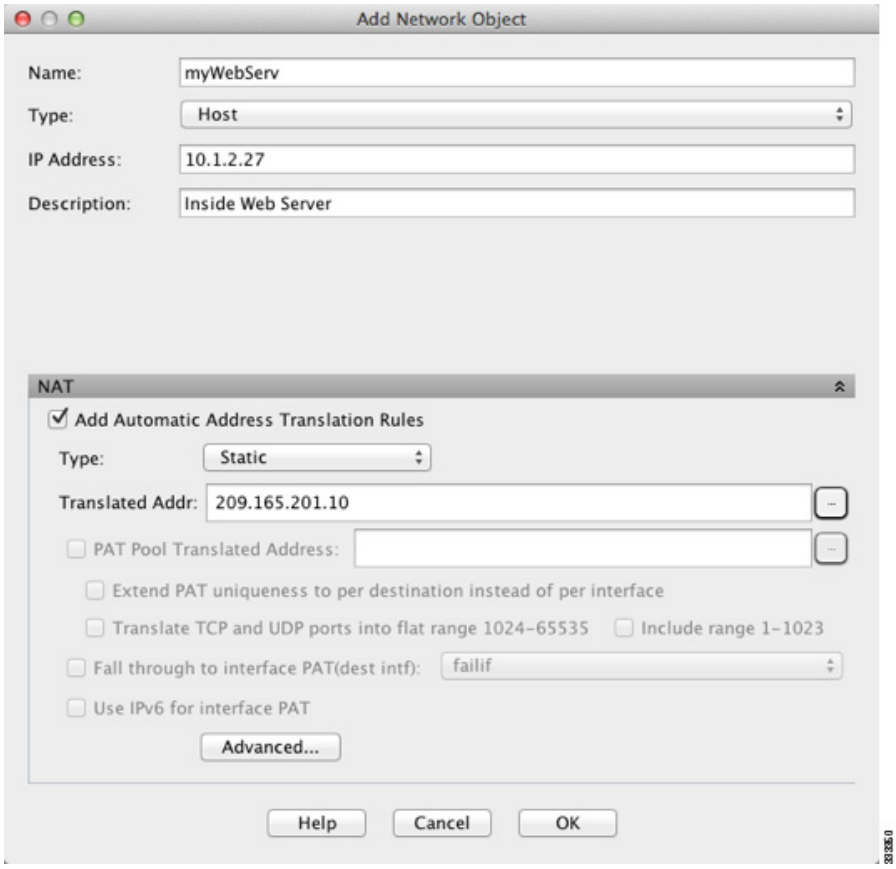
ステップ 1　内部 Web サーバのネットワーク オブジェクトを作成します。



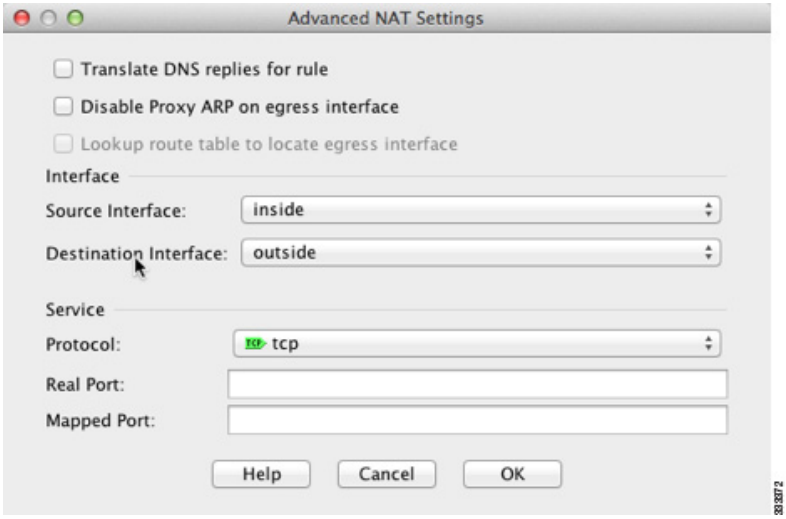
ステップ 2　Web サーバのアドレスを定義します。



ステップ 3　オブジェクトのスタティック NAT を設定します。



ステップ 4　[Advanced] をクリックして、実際のインターフェイスとマッピング インターフェイスを設定します。

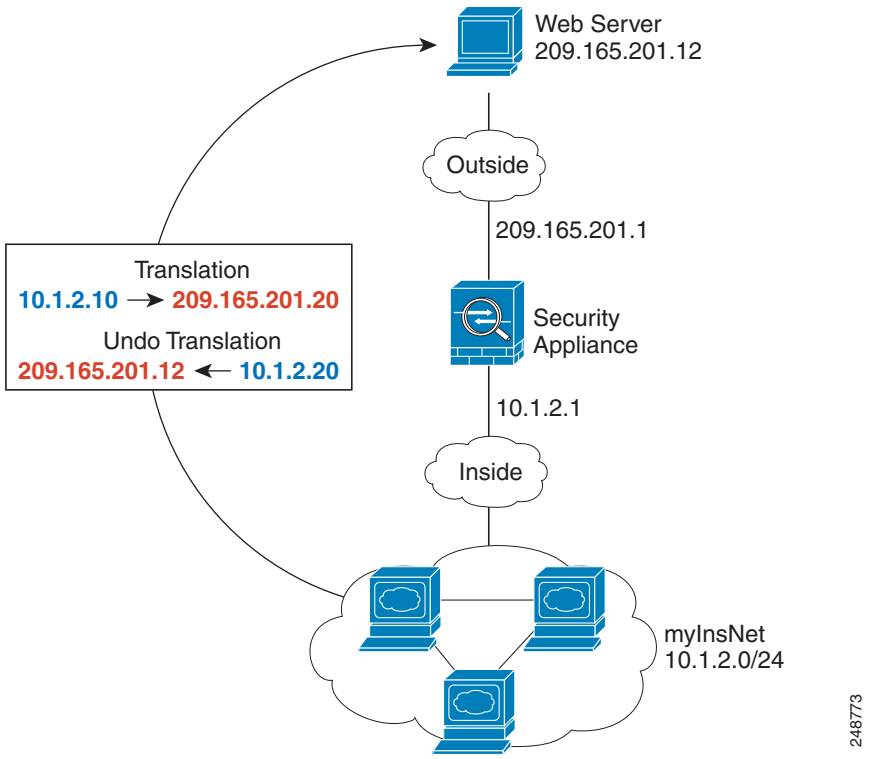


ステップ 5　[OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

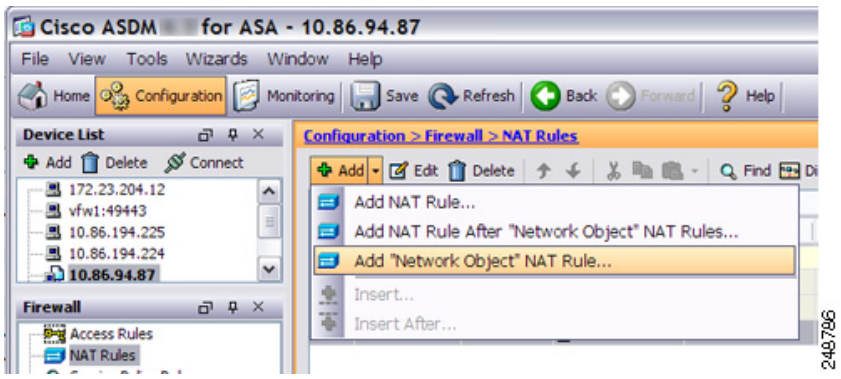
内部ホストの NAT（ダイナミック NAT）および外部 Web サーバの NAT（スタティック NAT）

次の例では、プライベート ネットワーク上の内部ユーザが外部にアクセスする場合、このユーザにダイナミック NAT を設定します。また、内部ユーザが外部 Web サーバに接続する場合、この Web サーバのアドレスが内部ネットワークに存在するように見えるアドレスに変換されます （図 6-2 を参照）。

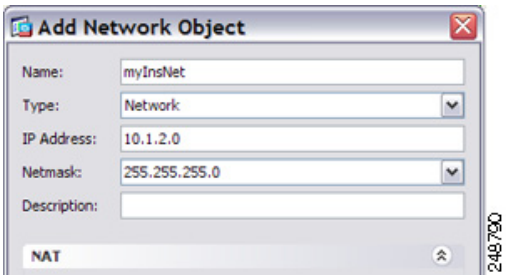
図 6-2　内部のダイナミック NAT、外部 Web サーバのスタティック NAT



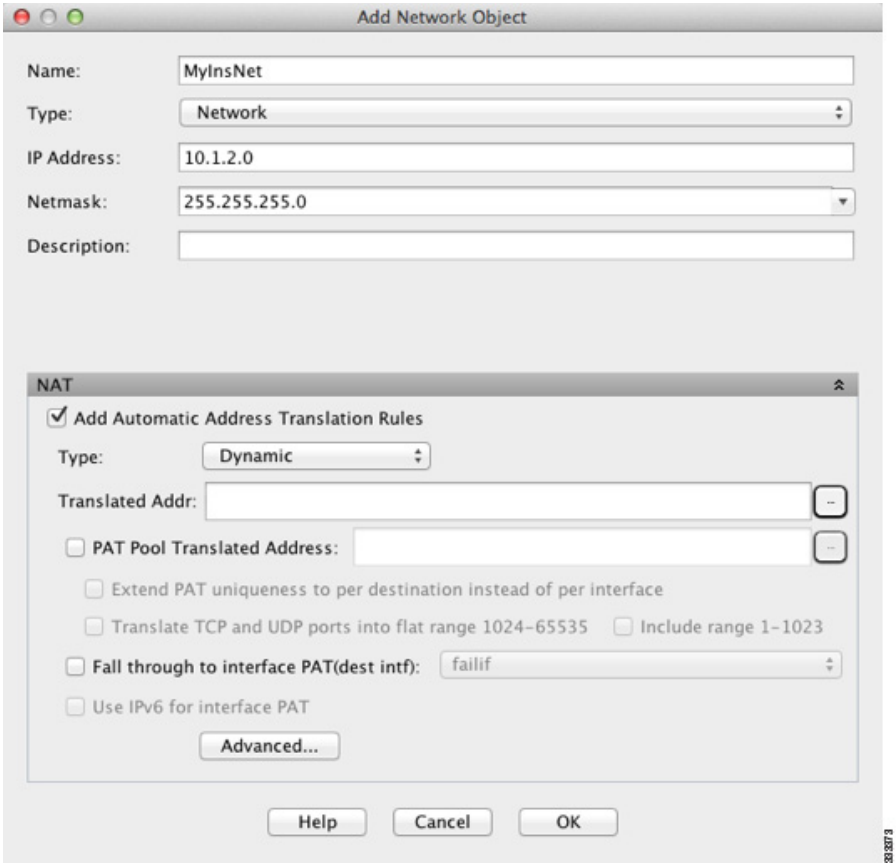
ステップ 1　内部ネットワークのネットワーク オブジェクトを作成します。



ステップ 2　内部ネットワークのアドレスを定義します。

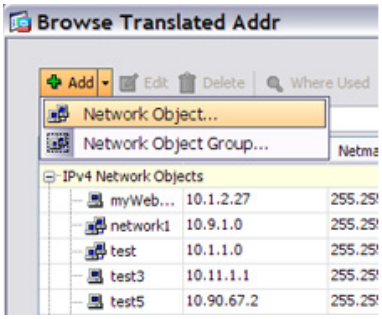


ステップ 3　内部ネットワークのダイナミック NAT をイネーブルにします。

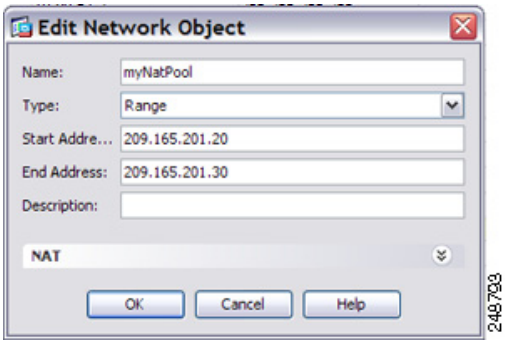


ステップ 4　[Translated Addr] フィールドで、内部アドレスの変換先となるダイナミック NAT プールを表す新しいネットワーク オブジェクトを追加するには、参照ボタンをクリックします。

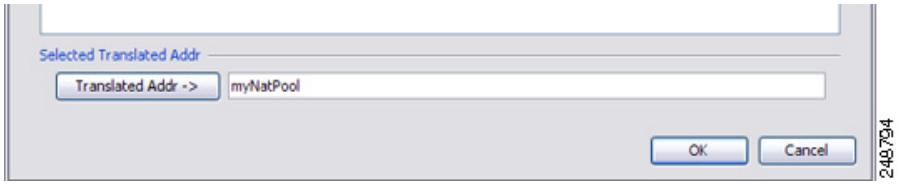
a.　新しいネットワーク オブジェクトを追加します。



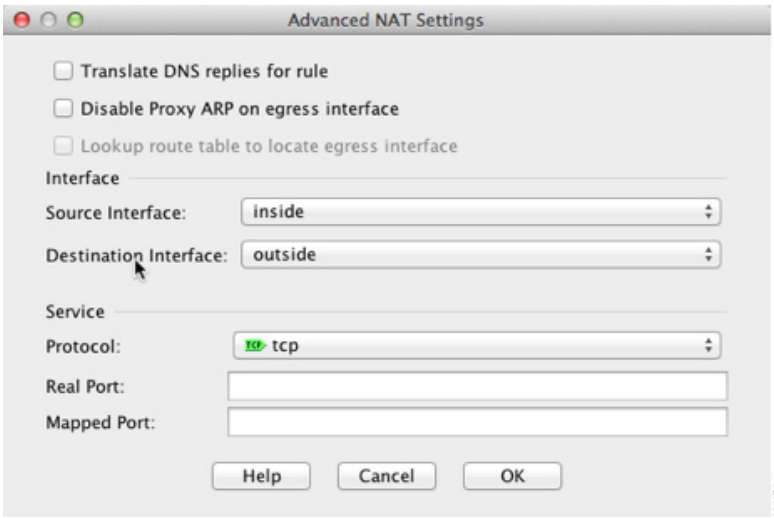
b. NAT プールのアドレスを定義して、[OK] をクリックします。



c. 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

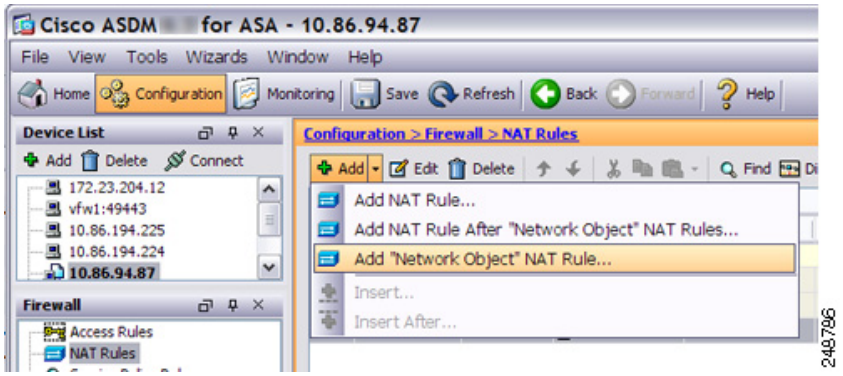


ステップ 5　[Advanced] をクリックして、実際のインターフェイスとマッピング インターフェイスを設定します。

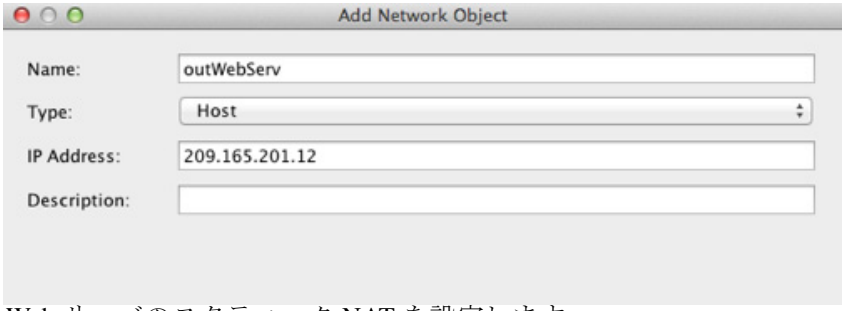


ステップ 6　[OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックして [NAT Rules] テーブルに戻ります。

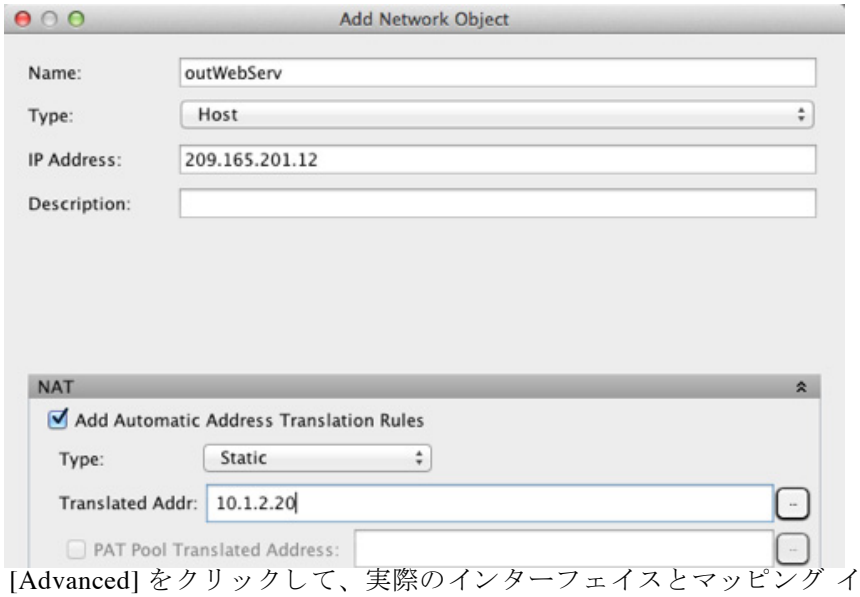
ステップ 7　外部 Web サーバのネットワーク オブジェクトを作成します。



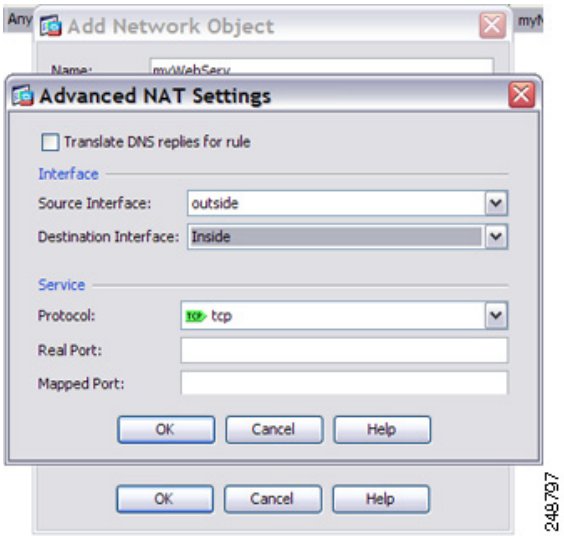
ステップ 8　Web サーバのアドレスを定義します。



ステップ 9　Web サーバのスタティック NAT を設定します。



ステップ 10　[Advanced] をクリックして、実際のインターフェイスとマッピング インターフェイスを設定します。

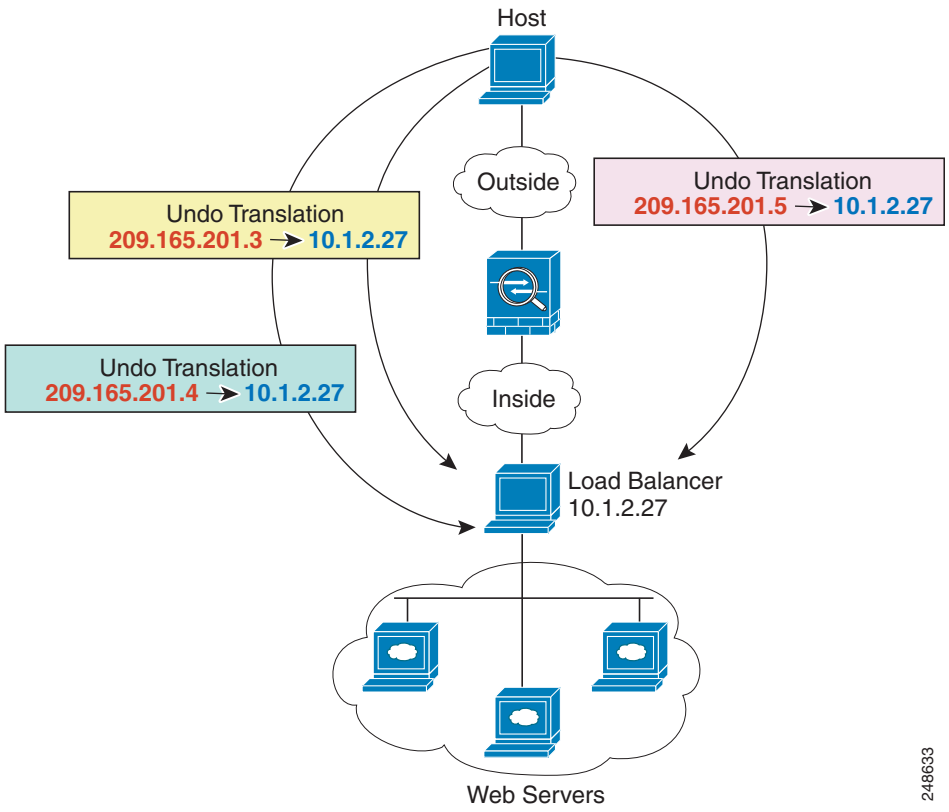


ステップ 11　[OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

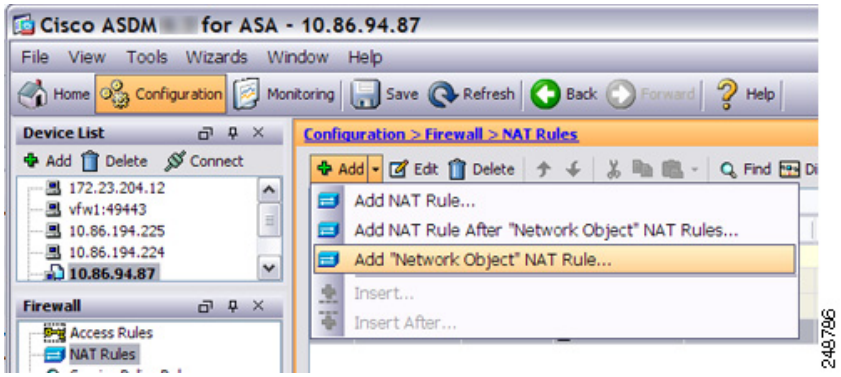
複数のマッピング アドレス（スタティック NAT、1 対多）を持つ内部ロード バランサ

次の例では、複数の IP アドレスに変換される内部ロード バランサを示しています。外部ホストがマッピング IP アドレスの 1 つにアクセスする場合、1 つのロード バランサのアドレスには変換されません。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします（図 6-3 を参照）。

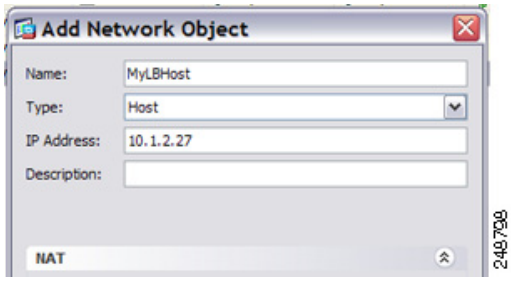
図 6-3　内部ロード バランサのスタティック NAT（1 対多）



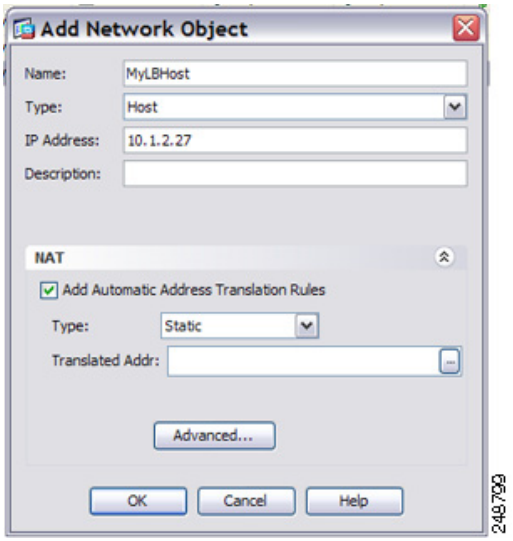
ステップ 1　ロード バランサのネットワーク オブジェクトを作成します。



ステップ 2　ロード バランサのアドレスを定義します。

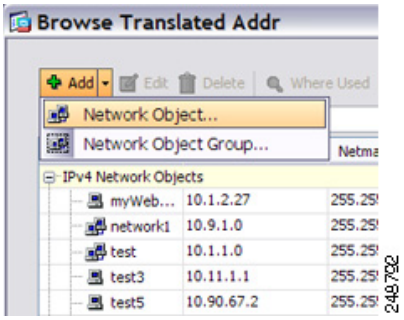


ステップ 3　ロード バランサのスタティック NAT を設定します。

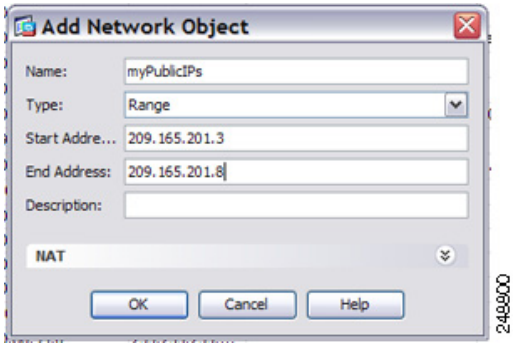


ステップ 4　[Translated Addr] フィールドで、ロード バランサ アドレスの変換先となるスタティック NAT アドレス グループを表す新しいネットワーク オブジェクトを追加するには、参照ボタンをクリックします。

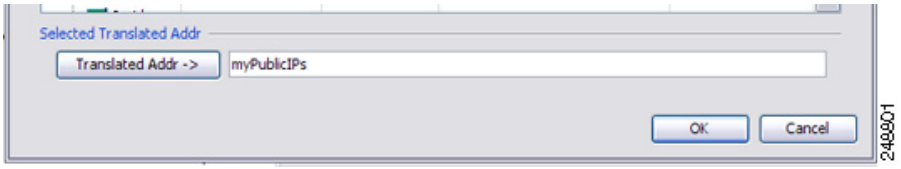
a.　新しいネットワーク オブジェクトを追加します。



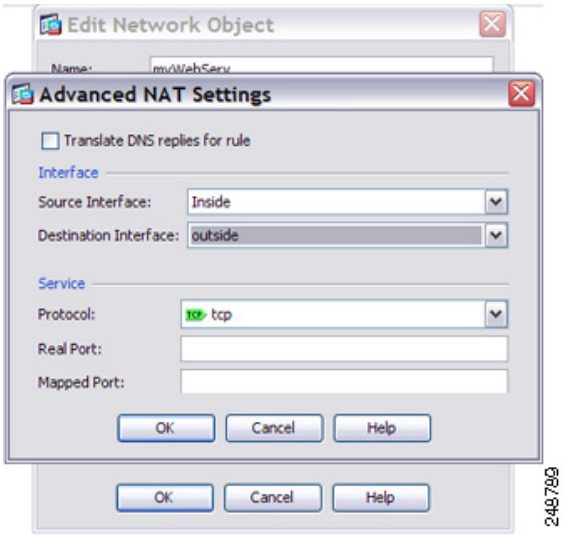
b.　スタティック NAT アドレス グループを定義し、[OK] をクリックします。



c. 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。



ステップ 5　[Advanced] をクリックして、実際のインターフェイスとマッピング インターフェイスを設定します。

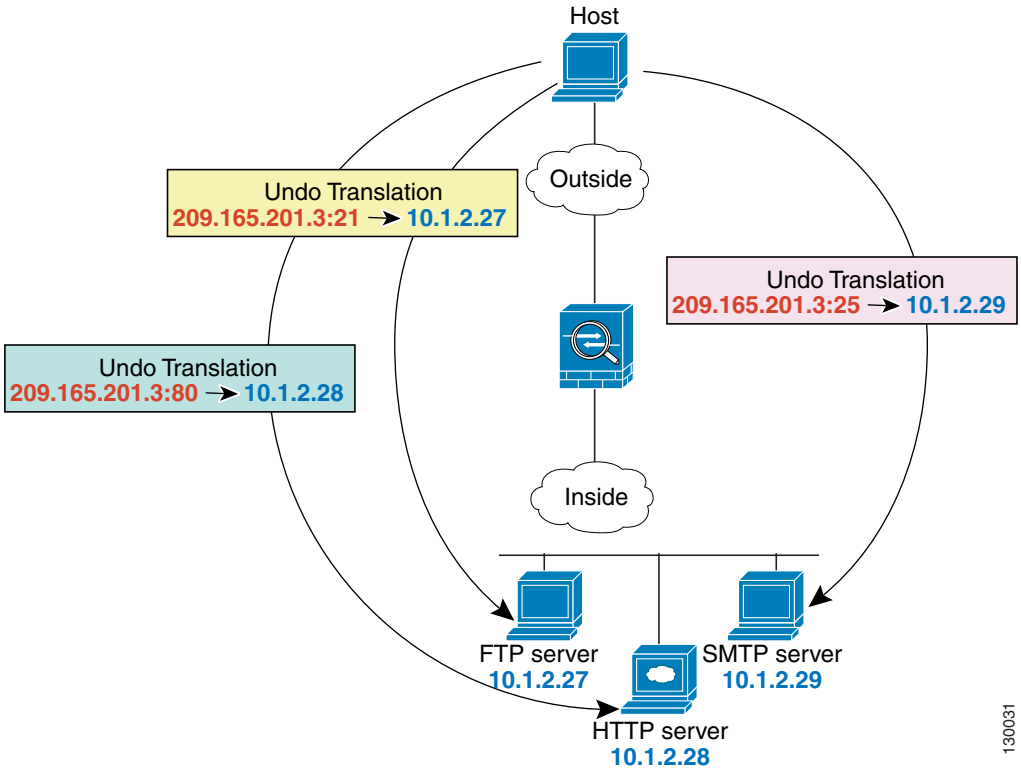


ステップ 6　[OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

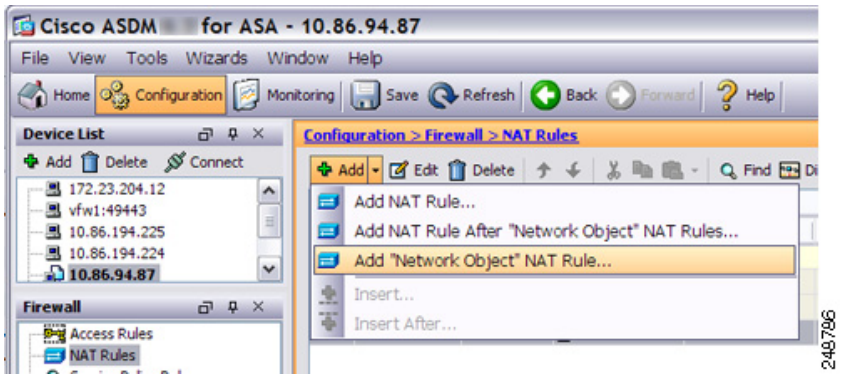
FTP、HTTP、および SMTP のための単一アドレス（ポート変換を設定したスタティック NAT）

次のポート変換を設定したスタティック NAT の例では、リモート ユーザは単一のアドレスで FTP、HTTP、および SMTP にアクセスできるようになります。これらのサーバは実際には、それぞれ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定したスタティック NAT ルールを指定すると、使用するマッピング IP アドレスは同じで、それぞれ別のポートを使用することができます。（図 6-4 を参照）。

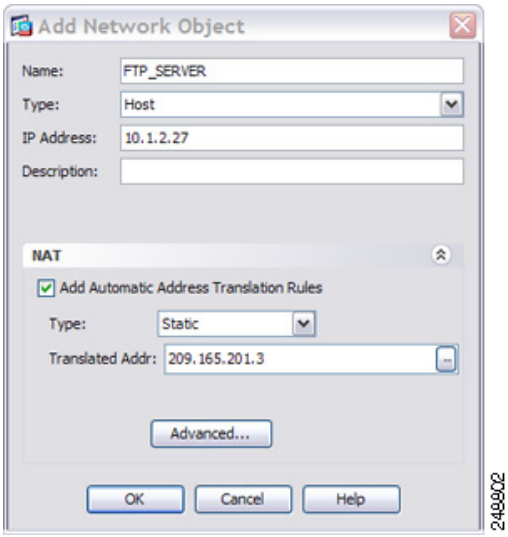
図 6-4　　ポート変換を設定したスタティック NAT



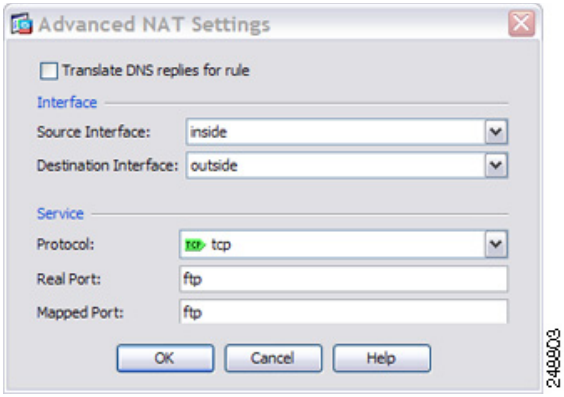
ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。



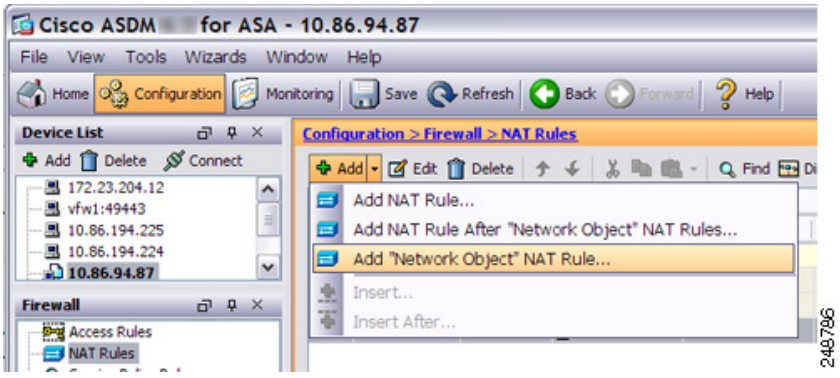
ステップ 2　FTP サーバのアドレスを定義し、アイデンティティ ポート変換を設定したスタティック NAT を FTP サーバに設定します。



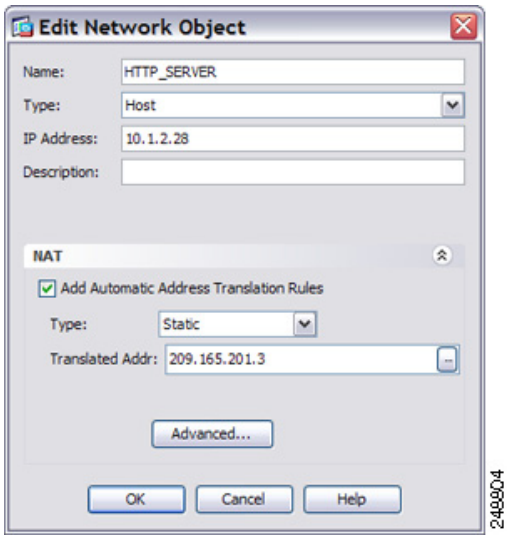
ステップ 3　[Advanced] をクリックし、FTP の実際のインターフェイスおよびマッピング インターフェイスとポート変換を設定します。



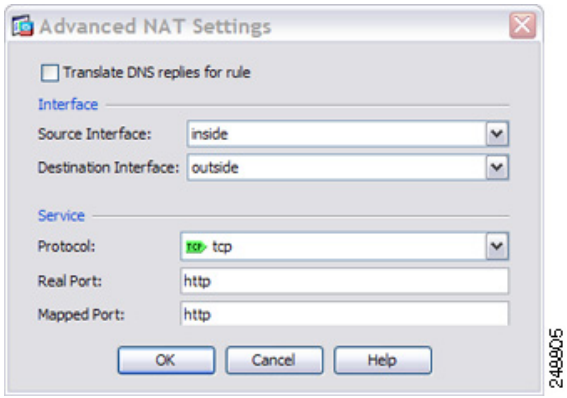
ステップ 4　HTTP サーバ アドレスのネットワーク オブジェクトを作成します。



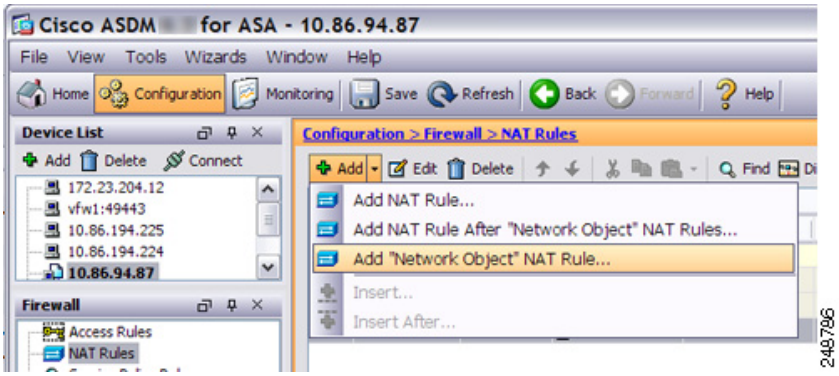
ステップ 5　HTTP サーバのアドレスを定義し、アイデンティティ ポート変換を設定したスタティック NAT を HTTP サーバに設定します。



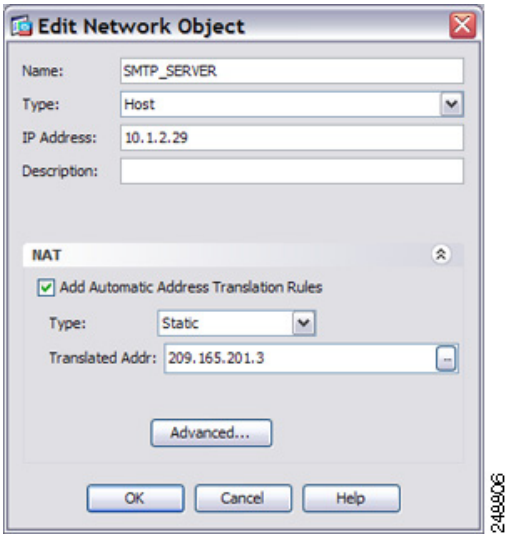
ステップ 6　[Advanced] をクリックし、HTTP の実際のインターフェイスおよびマッピング インターフェイスとポート変換を設定します。



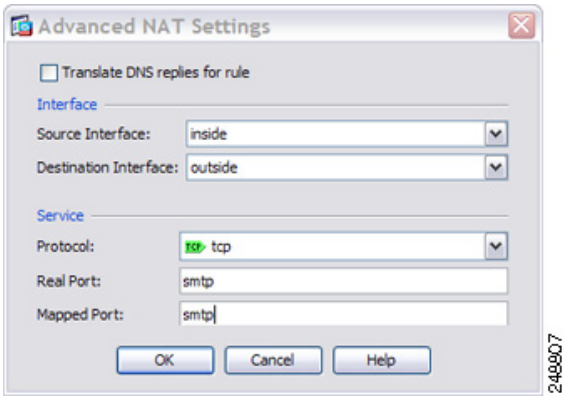
ステップ 7　SMTP サーバ アドレスのネットワーク オブジェクトを作成します。



ステップ 8　SMTP サーバのアドレスを定義し、アイデンティティ ポート変換を設定したスタティック NAT を SMTP サーバに設定します。



ステップ 9　[Advanced] をクリックし、SMTP の実際のインターフェイスおよびマッピング インターフェイスとポート変換を設定します。



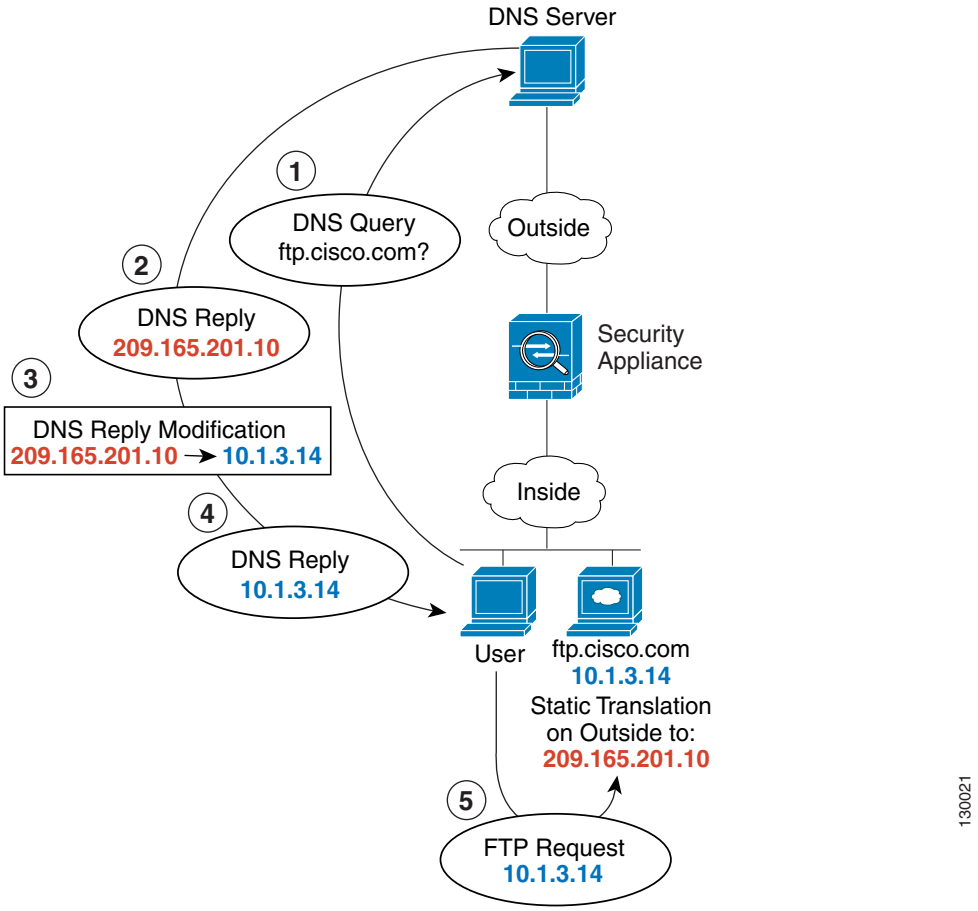
ステップ 10　[OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

マッピング インターフェイス上の DNS サーバ、実際のインターフェイス上の Web サーバ（DNS 修正を設定したスタティック NAT）

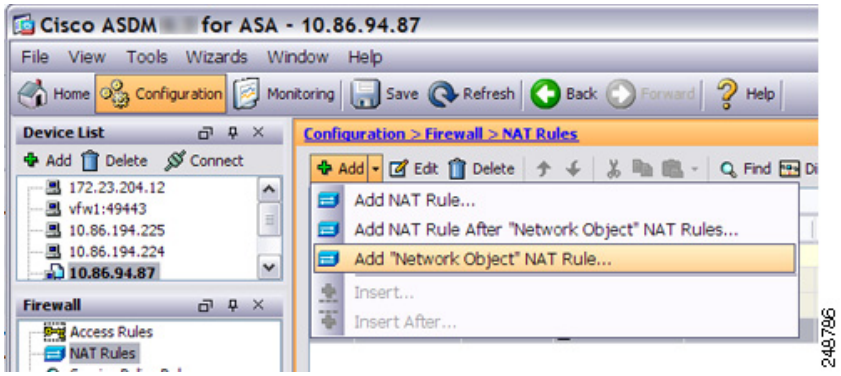
たとえば、DNS サーバが外部インターフェイスからアクセス可能であるとします。ftp.cisco.com というサーバが内部インターフェイス上にあります。ftp.cisco.com の実際のアドレス（10.1.3.14）を、外部ネットワーク上で可視のマッピング アドレス（209.165.201.10）にスタティックに変換するように、ASA を設定します（図 6-5 を参照）。この場合、このスタティック ルールで DNS 応答修正をイネーブルにする必要があります。これにより、実際のアドレスを使用して ftp.cisco.com にアクセスすることを許可されている内部ユーザは、マッピング アドレスではなく実際のアドレスを DNS サーバから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバは応答でマッピング アドレス（209.165.201.10）を示します。ASA は、内部サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正をイネーブルにしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックを送信することを試みます。

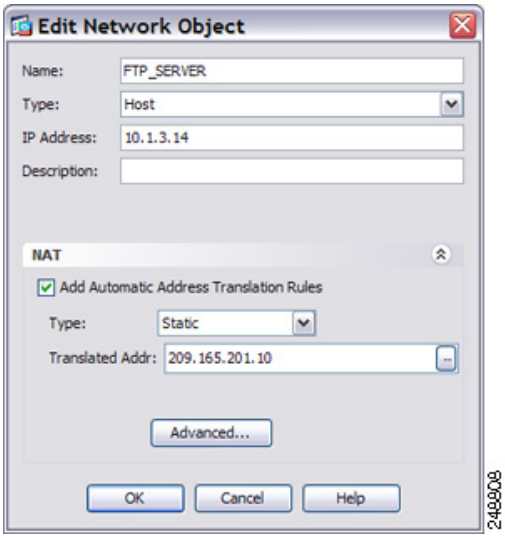
図 6-5　DNS 応答修正



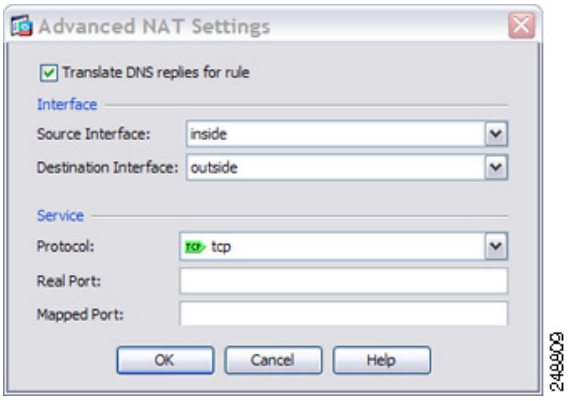
ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。



ステップ 2　FTP サーバのアドレスを定義し、DNS 修正を設定したスタティック NAT を設定します。



ステップ 3　実際のインターフェイスとマッピング インターフェイスおよび DNS 修正を設定するには、[Advanced] をクリックします。

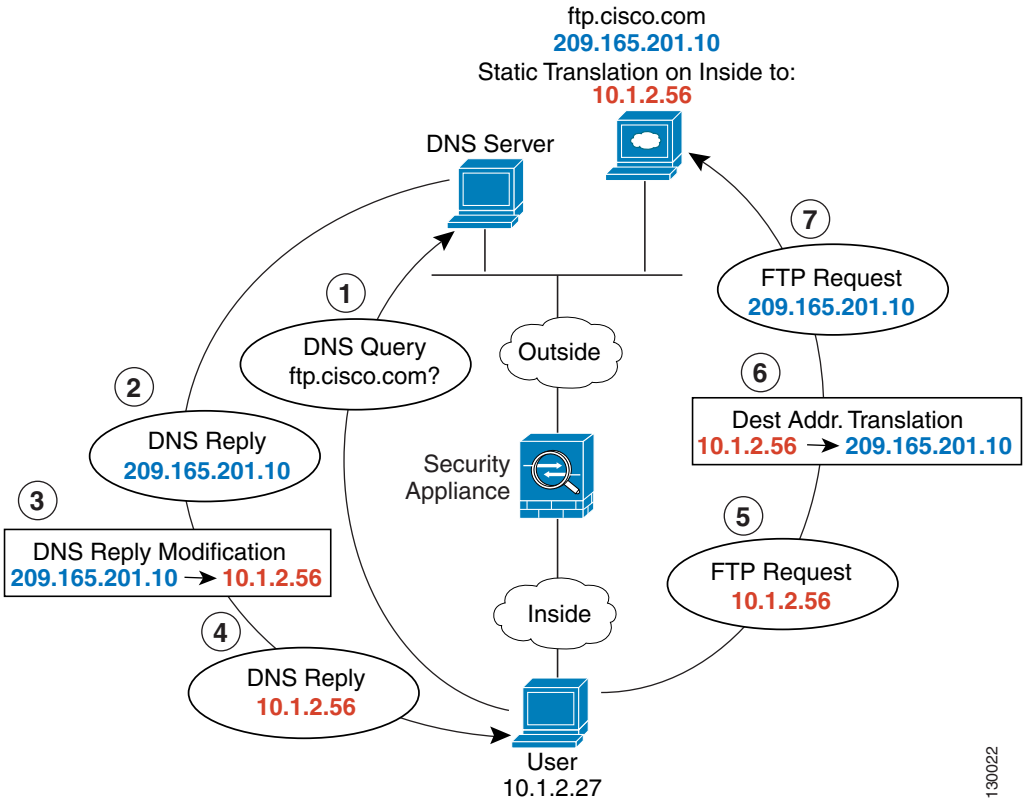


ステップ 4　[OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

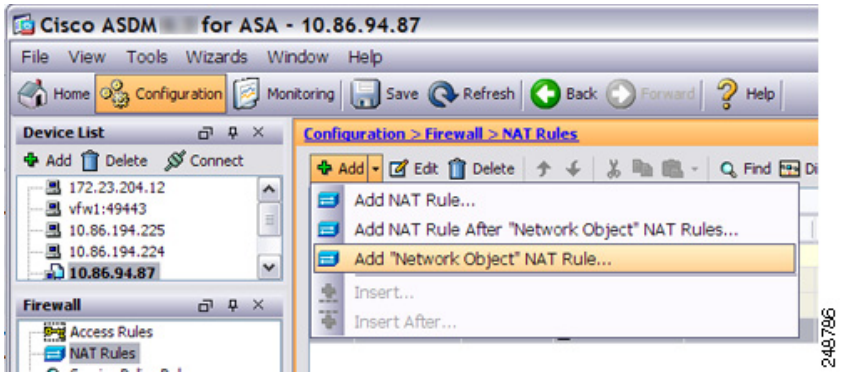
マッピング インターフェイス上の DNS サーバおよび FTP サーバ、FTP サーバが変換される（DNS 修正を設定したスタティック NAT）

図 6-6 に、外部の FTP サーバと DNS サーバを示します。ASA には、外部サーバ用のスタティック変換があります。この場合に、内部ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答として実際のアドレス 209.165.201.10 を返します。ftp.cisco.com のマッピング アドレス（10.1.2.56）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。

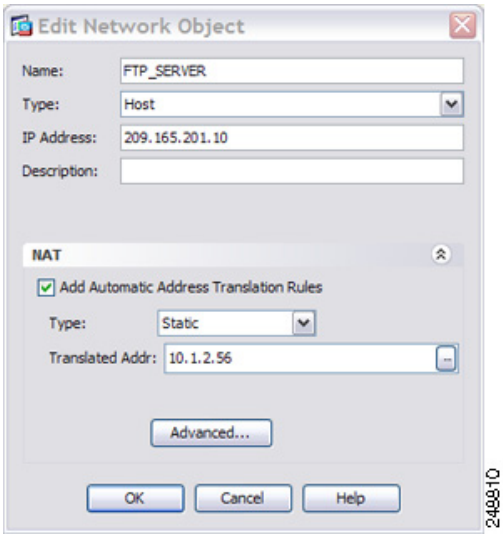
図 6-6　外部 NAT を使用する DNS 応答修正



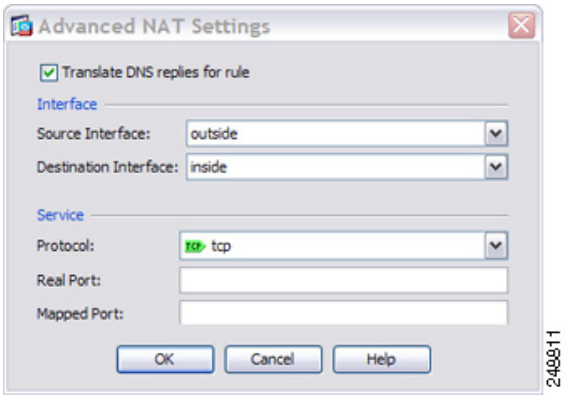
ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。



ステップ 2　FTP サーバのアドレスを定義し、DNS 修正を設定したスタティック NAT を設定します。



ステップ 3　実際のインターフェイスとマッピング インターフェイスおよび DNS 修正を設定するには、[Advanced] をクリックします。

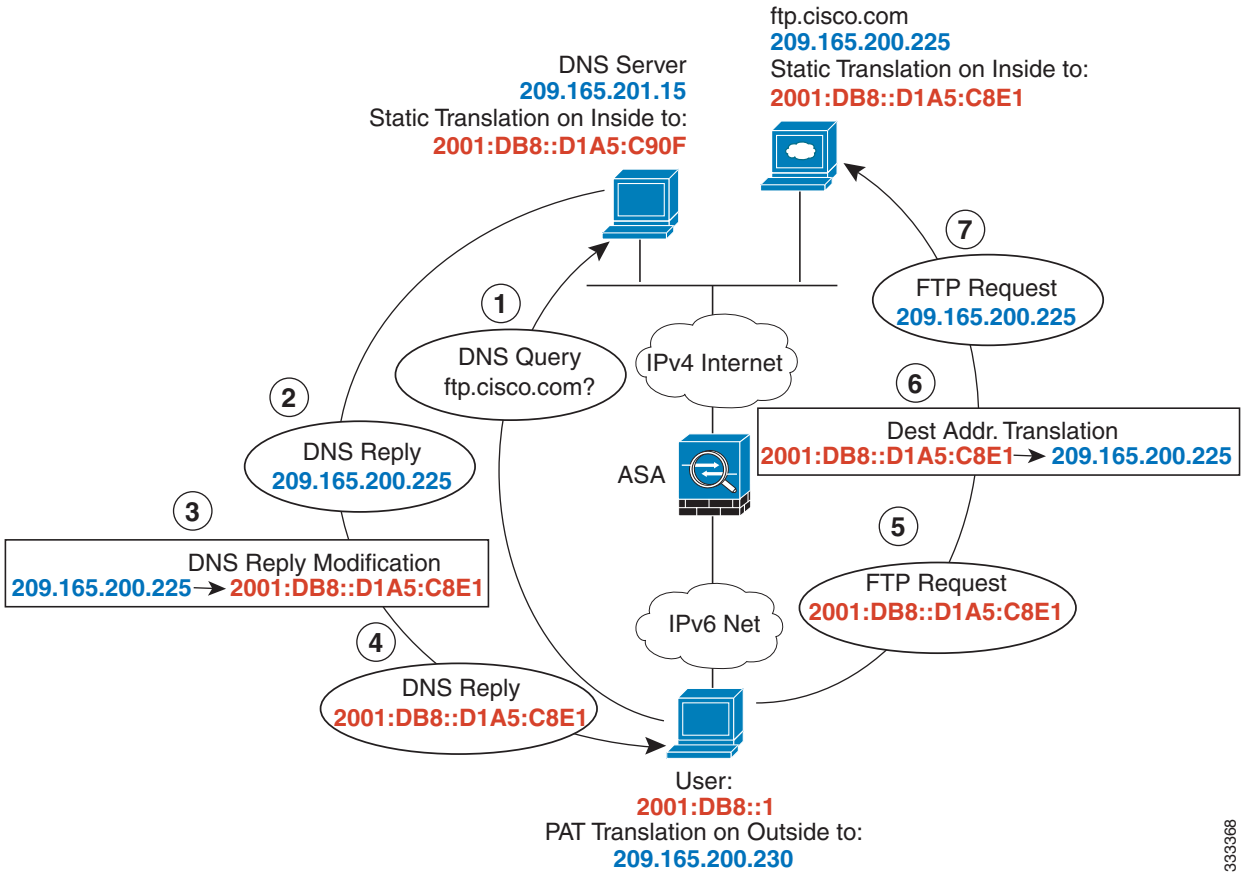


ステップ 4　[OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

マッピング インターフェイス上の IPv4 DNS サーバおよび FTP サーバ、実際のインターフェイス上の IPv6 ホスト（DNS64 修正を設定したスタティック NAT64）

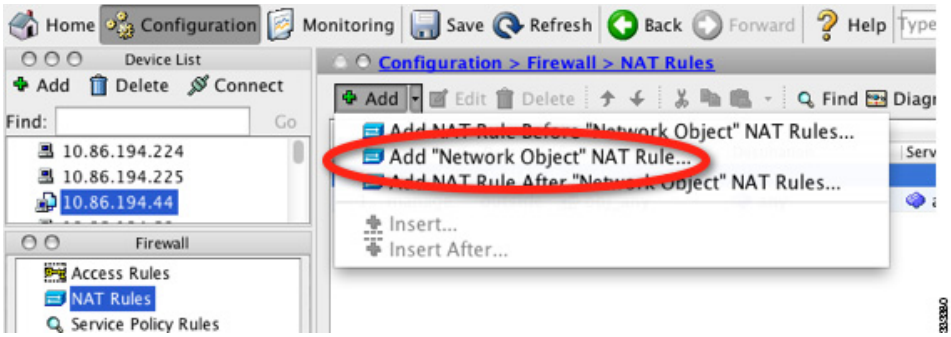
図 6-6 に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。ASA には、外部サーバ用のスタティック変換があります。この場合に、内部 IPv6 ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答として実際のアドレス 209.165.200.225 を返します。ftp.cisco.com のマッピング アドレス（2001:DB8::D1A5:C8E1）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。この例には、DNS サーバのスタティック NAT 変換、および内部 IPv6 ホストの PAT ルールも含まれています。

図 6-7　　外部 NAT を使用する DNS 応答修正

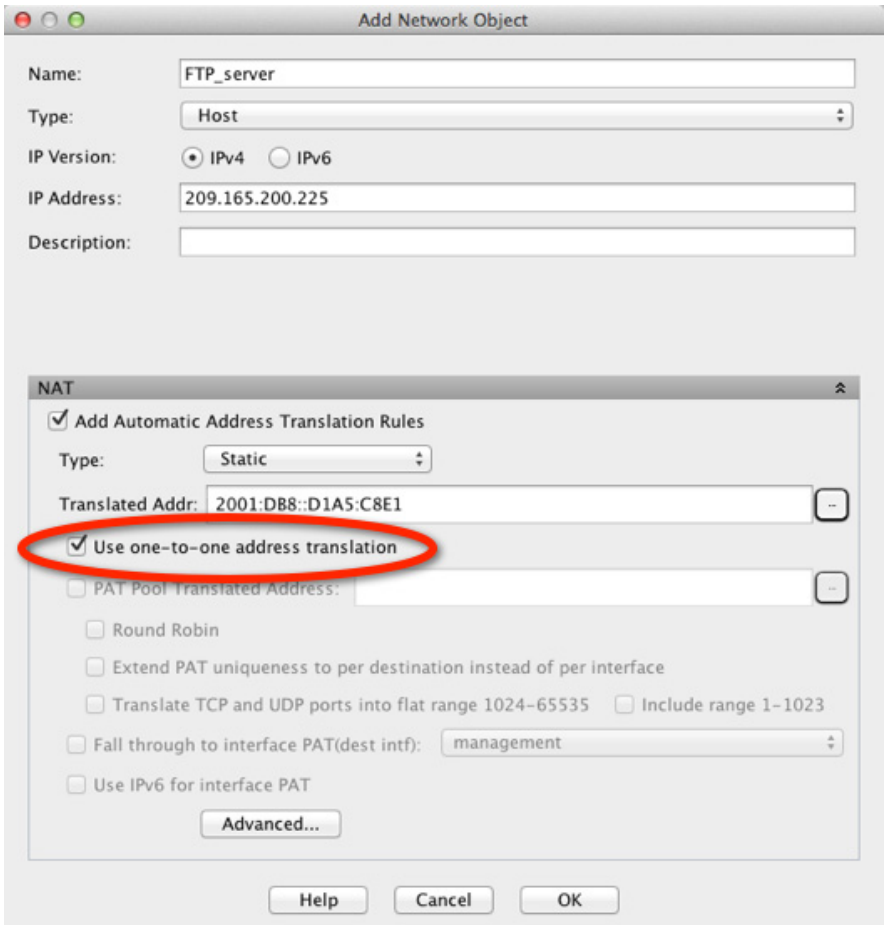


ステップ 1　FTP サーバのための、DNS 修正を設定したスタティック NAT を設定します。

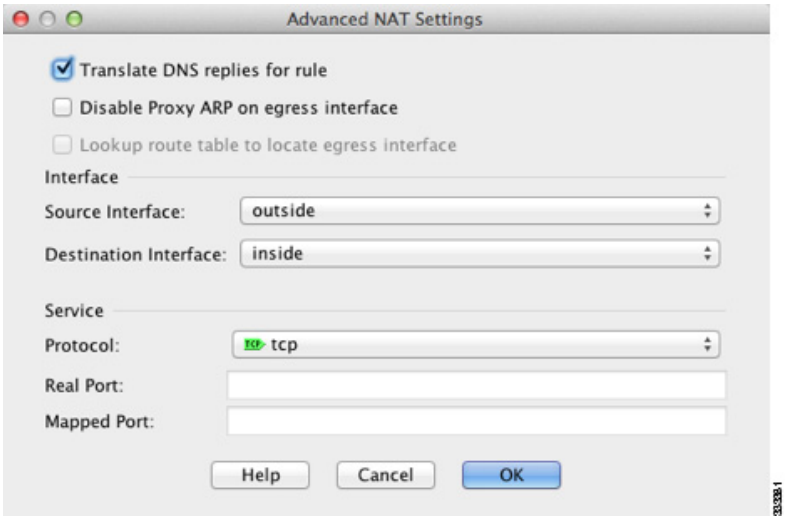
a.　FTP サーバ アドレスのためのネットワーク オブジェクトを作成します。



b. FTP サーバのアドレスを定義し、DNS 修正を設定したスタティック NAT を設定します。これは 1 対 1 変換であるため、NAT46 に対して one-to-one 方式を設定します。



c. 実際のインターフェイスとマッピング インターフェイスおよび DNS 修正を設定するには、[Advanced] をクリックします。

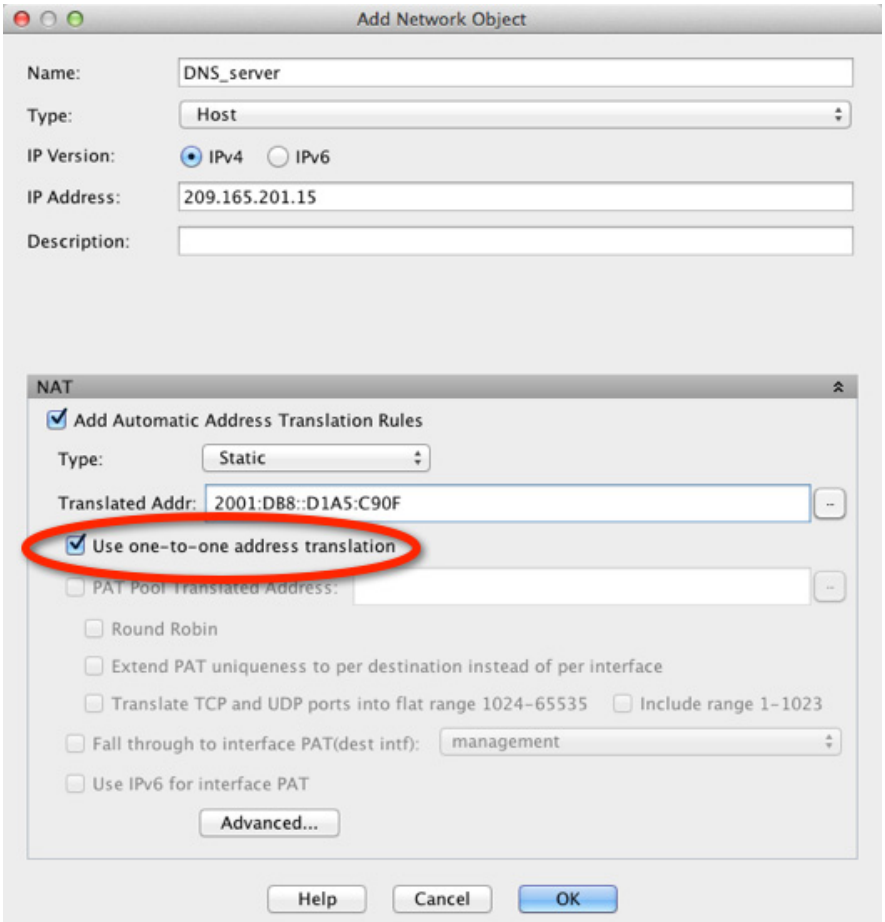


d. [OK] をクリックして [Edit Network Object] ダイアログボックスに戻ります。

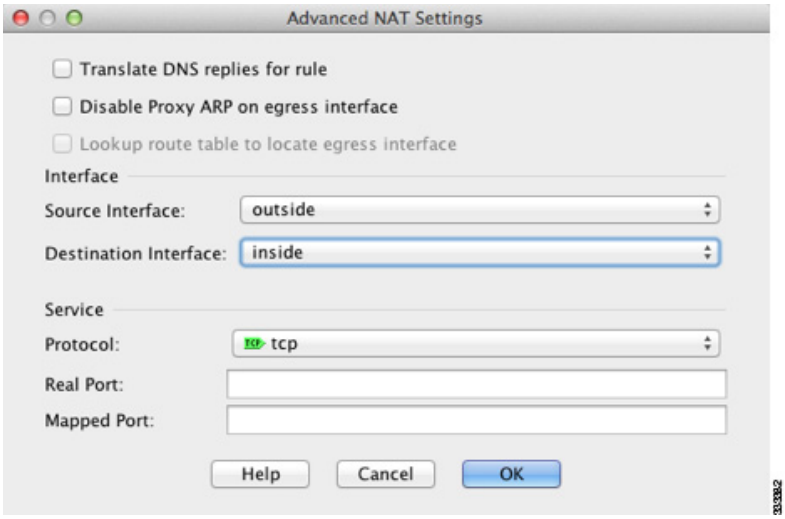
ステップ 2　DNS サーバの NAT を設定します。

a. DNS サーバ アドレスのためのネットワーク オブジェクトを作成します。

b. DNS サーバのアドレスを定義し、one-to-one 方式を使用してスタティック NAT を設定します。

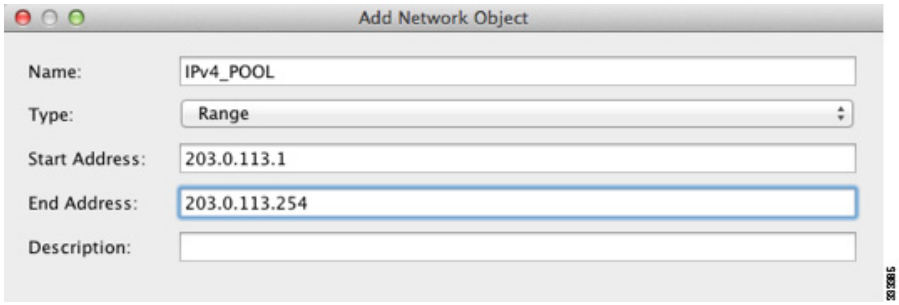


c. 実際のインターフェイスとマッピング インターフェイスを設定するには、[Advanced] をクリックします。



d. [OK] をクリックして [Edit Network Object] ダイアログボックスに戻ります。

ステップ 3　内部 IPv6 ネットワークを変換するための IPv4 PAT プールを設定します。

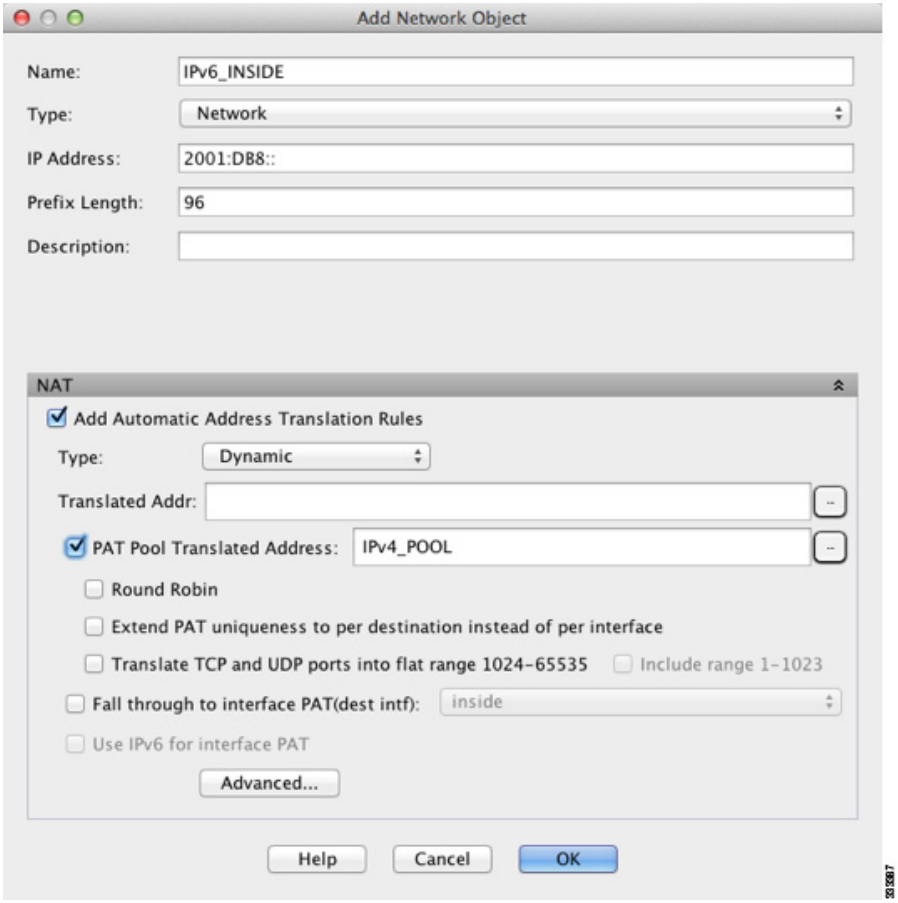


[NAT] で、[Add Automatic Address Translation Rules] チェックボックスをオフにします。

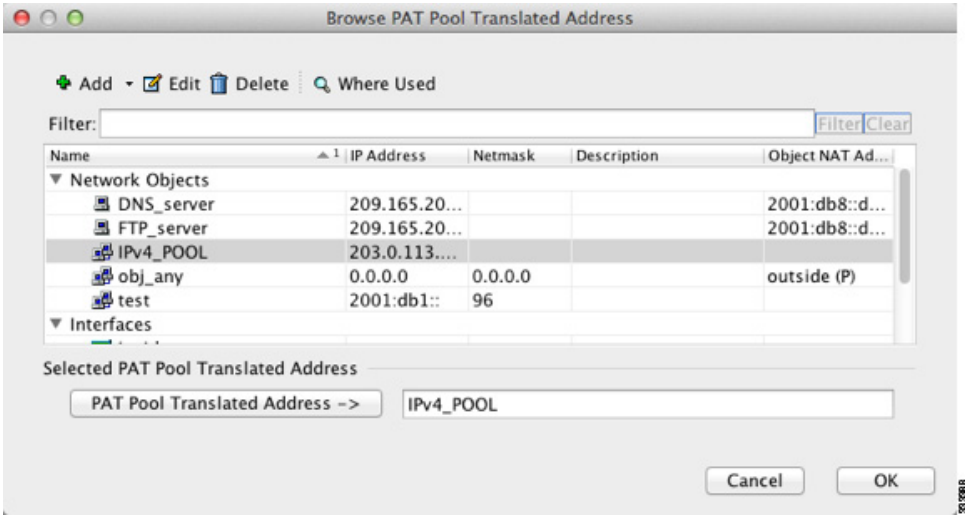
ステップ 4　内部 IPv6 ネットワークのための PAT を設定します。

a. 内部 IPv6 ネットワークのためのネットワーク オブジェクトを作成します。

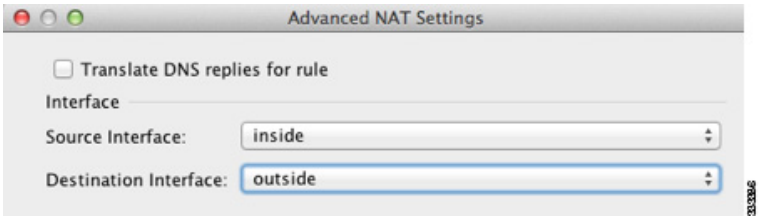
b. IPv6 ネットワーク アドレスを定義し、PAT プールを使用するダイナミック NAT を設定します。



c. [PAT Pool Translated Address] フィールドの横にある、[...] ボタンをクリックし、以前に作成した PAT プールを選択して、[OK] をクリックします。



d. 実際のインターフェイスとマッピング インターフェイスを設定するには、[Advanced] をクリックします。



e. [OK] をクリックして [Edit Network Object] ダイアログボックスに戻ります。

ステップ 5　[OK] をクリックし、さらに [Apply] をクリックします。

ネットワーク オブジェクト NAT の機能履歴

表 6-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 6-1　　ネットワーク オブジェクト NAT の機能履歴

機能名	プラットフォーム リリース	機能情報
ネットワーク オブジェクト NAT	8.3(1)	ネットワーク オブジェクトの IP アドレスの NAT を設定します。 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [NAT Rules] [Configuration] > [Firewall] > [Objects] > [Network Objects/Groups]
アイデンティティ NAT の設定が可能なプロキシ ARP およびルート ルックアップ	8.4(2)/8.5(1)	アイデンティティ NAT の以前のリリースでは、プロキシ ARP はディセーブルにされ、出力インターフェイスの決定には常にルート ルックアップが使用されていました。これらを設定することはできませんでした。8.4(2) 以降、アイデンティティ NAT のデフォルト動作は他のスタティック NAT コンフィギュレーションの動作に一致するように変更されました。これにより、デフォルトでプロキシ ARP はイネーブルにされ、NAT コンフィギュレーションにより出力インターフェイスが決定されるようになりました（指定されている場合）。これらの設定をそのまま残すこともできますし、個別にイネーブルまたはディセーブルにすることもできます。通常のスタティック NAT のプロキシ ARP をディセーブルにすることもできるようになっています。 8.3(1)、8.3(2)、8.4(1) から 8.4(2) にアップグレードすると、既存機能を保持するため、すべてのアイデンティティ NAT コンフィギュレーションに **no-proxy-arp** キーワードと **route-lookup** キーワードが含まれるようになっています。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object] > [Advanced NAT Settings]。

表 6-1　ネットワーク オブジェクト NAT の機能履歴（続き）

機能名	プラットフォーム リリース	機能情報
PAT プールおよびラウンド ロビン アドレス割り当て	8.4(2)/8.5(1)	1 つのアドレスの代わりに、PAT アドレスのプールを指定できるようになりました。また、オプションで、PAT アドレスのすべてのポートを使用してからプール内の次のアドレスを使用するのではなく、PAT アドレスのラウンドロビン割り当てをイネーブルにすることもできます。これらの機能は、1 つの PAT アドレスで多数の接続を行っている場合にそれが DoS 攻撃の対象となることを防止するのに役立ちます。またこの機能により、多数の PAT アドレスを簡単に設定できます。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object]。
ラウンドロビン PAT プール割り当てで、既存のホストの同じ IP アドレスを使用する	8.4(3)	ラウンドロビン割り当てで PAT プールを使用するときに、ホストに既存の接続がある場合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT IP アドレスが使用されます。 変更された画面はありません。 *この機能は、8.5(1) または 8.6(1) では使用できません。*
PAT プールの PAT ポートのフラットな範囲	8.4(3)	使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用*できない* 場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートには、小さい PAT プールのみがあります。 下位ポート範囲を使用するトラフィックが数多くある場合は、PAT プールを使用するときに、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。1024 ～ 65535 または 1 ～ 65535 です。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object]。 *この機能は、8.5(1) または 8.6(1) では使用できません。*
PAT プールの拡張 PAT	8.4(3)	各 PAT IP アドレスでは、最大 65535 個のポートを使用できます。65535 個のポートで変換が不十分な場合は、PAT プールに対して拡張 PAT をイネーブルにすることができます。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、*サービス*ごとに 65535 個のポートが使用されます。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object]。 *この機能は、8.5(1) または 8.6(1) では使用できません。*

表 6-1　ネットワーク オブジェクト NAT の機能履歴（続き）

機能名	プラットフォーム リリース	機能情報
VPN ピアのローカル IP アドレスを変換してピアの実際の IP アドレスに戻す自動 NAT ルール	8.4(3)	まれに、内部ネットワークで、割り当てられたローカル IP アドレスではなく、VPN ピアの実際の IP アドレスを使用する場合があります。VPN では通常、内部ネットワークにアクセスするために、割り当てられたローカル IP アドレスがピアに指定されます。ただし、内部サーバおよびネットワーク セキュリティがピアの実際の IP アドレスに基づく場合などに、ローカル IP アドレスを変換してピアの実際のパブリック IP アドレスに戻す場合があります。 この機能は、トンネル グループごとに 1 つのインターフェイスでイネーブルにすることができます。VPN セッションが確立または切断されると、オブジェクト NAT ルールが動的に追加および削除されます。ルールは **show nat** コマンドを使用して表示できます。 **（注）** ルーティングの問題のため、この機能が必要でない場合は、この機能の使用は推奨しません。ご使用のネットワークとの機能の互換性を確認するには、Cisco TAC にお問い合わせください。次の制限事項を確認してください。 • Cisco IPsec および AnyConnect クライアントのみがサポートされます。 • NAT ポリシーおよび VPN ポリシーが適用されるように、パブリック IP アドレスへのリターン トラフィックは ASA にルーティングされる必要があります。 • ロードバランシングはサポートされません（ルーティングの問題のため）。 • ローミング（パブリック IP 変更）はサポートされません。 ASDM ではこのコマンドはサポートされません。コマンドライン ツールを使用してコマンドを入力してください。
IPv6 用の NAT のサポート	9.0(1)	NAT が IPv6 トラフィックをサポートするようになり、IPv4 と IPv6 の間の変換もサポートされます。IPv4 と IPv6 の間の変換は、トランスペアレント モードではサポートされません。 次の画面が変更されました。[Configuration] > [Firewall] > [Objects] > [Network Objects/Group]。
逆引き DNS ルックアップ用の NAT のサポート	9.0(1)	NAT ルールがイネーブルにされた DNS インスペクションを使用する IPv4 NAT、IPv6 NAT、および NAT64 を使用する場合、NAT は逆引き DNS ルックアップ用の DNS PTR レコードの変換をサポートするようになりました。

表 6-1　ネットワーク オブジェクト NAT の機能履歴（続き）

機能名	プラットフォーム リリース	機能情報
Per-Session PAT	9.0(1)	Per-session PAT 機能によって PAT のスケーラビリティが向上し、クラスタリングの場合に各メンバ ユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、マスター ユニットに転送してマスター ユニットを所有者とする必要があります。Per-Session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンド ノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。「ヒットエンドラン」トラフィック、たとえば HTTP や HTTPS の場合は、Per-Session 機能によって、1 アドレスでサポートされる接続率が大幅に増加することがあります。Per-session 機能を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。Per-session 機能を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/平均ライフタイムです。 デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-session PAT xlate を使用します。Multi-Session PAT を必要とするトラフィック、たとえば H.323、SIP、Skinny に対して Per-session PAT をディセーブルにするには、Per-session 拒否ルールを作成します。 次の画面が導入されました。[Configuration] > [Firewall] > [Advanced] > [Per-Session NAT Rules]。

Twice NAT（ASA 8.3 以降）

Twice NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。この章では、Twice NAT を設定する方法について説明します。

- 「Twice NAT に関する情報」（P.7-1）
- 「Twice NAT のライセンス要件」（P.7-2）
- 「Twice NAT の前提条件」（P.7-2）
- 「ガイドラインと制限事項」（P.7-2）
- 「デフォルト設定」（P.7-4）
- 「Twice NAT の設定」（P.7-4）
- 「Twice NAT のモニタリング」（P.7-31）
- 「Twice NAT の設定例」（P.7-32）
- 「Twice NAT の機能履歴」（P.7-50）

（注） NAT の機能の詳細については、第 5 章「ネットワーク アドレス変換（NAT）（ASA 8.3 以降）」を参照してください。

Twice NAT に関する情報

Twice NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、たとえば送信元アドレスが宛先 X に向かう場合は A に変換され、宛先 Y に向かう場合は B に変換されるように指定できます。

（注） スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。たとえば、ポート アドレス変換を使用するスタティック NAT を設定し、送信元アドレスを Telnet サーバとして指定する場合に、Telnet サーバに向かうすべてのトラフィックのポートを 2323 から 23 に変換するには、このコマンドで、変換する*送信元*ポート（実際：23、マッピング：2323）を指定する必要があります。Telnet サーバ アドレスを送信元アドレスとして指定しているため、その送信元ポートを指定します。

宛先アドレスはオプションです。宛先アドレスを指定する場合、宛先アドレスを自身にマッピングするか（アイデンティティ NAT）、別のアドレスにマッピングできます。宛先マッピングは、常にスタティック マッピングです。

Twice NAT では、ポート変換を設定したスタティック NAT のサービス オブジェクトも使用できます。ネットワーク オブジェクト NAT は、インライン定義だけを受け入れます。

Twice NAT とネットワーク オブジェクト NAT の違いの詳細については、「NAT の実装方法」（P.5-15）を参照してください。

Twice NAT ルールは、NAT ルール テーブルのセクション 1 に追加されます。指定した場合には、セクション 3 に追加されます。NAT の順序付けの詳細については、「NAT ルールの順序」（P.5-20）を参照してください。

Twice NAT のライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

Twice NAT の前提条件

- 実際のアドレスとマッピング アドレスの両方について、ネットワーク オブジェクトまたはネットワーク オブジェクト グループを設定します。ネットワーク オブジェクト グループは、非連続的な IP アドレスの範囲または複数のホストやサブネットで構成されるマッピング アドレスを作成する場合に特に便利です。ネットワーク オブジェクトまたはグループを作成するには、『一般的な操作のコンフィギュレーション ガイド』を参照してください。
- ポート変換を設定したスタティック NAT の場合、TCP または UDP サービス オブジェクトを設定します。サービス オブジェクトを作成するには、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

オブジェクトおよびグループに関する特定のガイドラインについては、設定する NAT タイプの設定の項を参照してください。「ガイドラインと制限事項」（P.7-2）も参照してください。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

- ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

- トランスペアレント モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定する必要があります。--Any-- は使用できません。
- トランスペアレント モードでは、インターフェイス PAT を設定できません。トランスペアレント モードのインターフェイスには、IP アドレスが設定されていないためです。管理 IP アドレスもマッピング アドレスとして使用できません。
- トランスペアレント モードでは、IPv4 ネットワークと IPv6 ネットワークとの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。

IPv6 のガイドライン

- IPv6 をサポートします。
- ルーテッド モードの場合は、IPv4 と IPv6 との間の変換もできます。
- トランスペアレント モードの場合は、IPv4 ネットワークと IPv6 ネットワークとの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。
- トランスペアレント モードの場合は、PAT プールは IPv6 に対してはサポートされません。
- スタティック NAT の場合は、/64 までの IPv6 サブネットを指定できます。これよりも大きいサブネットはサポートされません。
- FTP を NAT46 とともに使用する場合は、IPv4 FTP クライアントが IPv6 FTP サーバに接続するときに、クライアントは拡張パッシブ モード（EPSV）または拡張ポート モード（EPRT）を使用する必要があります。PASV コマンドおよび PORT コマンドは IPv6 ではサポートされません。

その他のガイドライン

- 送信元 IP アドレスがサブネット（またはセカンダリ接続を使用するその他のアプリケーション）の場合、FTP 宛先ポート変換を設定できません。FTP データ チャネルの確立に失敗します。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待機せずに新しい NAT 情報を使用する必要がある場合は、**clear xlate** コマンドを使用して変換テーブルを消去できます。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

（注） ダイナミック NAT または PAT ルールを削除し、次に削除したルールに含まれるアドレスと重複するマッピング アドレスを含む新しいルールを追加すると、新しいルールは、削除されたルールに関連付けられたすべての接続がタイムアウトするか、**clear xlate** コマンドを使用してクリアされるまで使用されません。この予防手段のおかげで、同じアドレスが複数のホストに割り当てられないようにできます。

- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。
- NAT ルールで **any** キーワードを使用する場合、「any」トラフィック（IPv4 と IPv6）は、ルールによって異なります。ASA がパケットに対して NAT を実行する前に、パケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件では、ASA は、NAT ルールの **any** の値を決定できます。たとえば、「any」から IPv6 サーバへのルールを設定しており、このサーバが IPv4 アドレスからマッピングされている場合、**any** は「任意の IPv6 トラフィック」を意味します。「any」から「any」へのルールを設定しており、送信元をインターフェイス IPv4 アドレスにマッピングする場合、マッピングされたインターフェイス アドレスによって宛先も IPv4 であることが示されるため、**any** は「任意の IPv4 トラフィック」を意味します。

- NAT で使用されるオブジェクトおよびオブジェクト グループを未定義にすることはできません。IP アドレスを含める必要があります。
- 同じオブジェクトを複数のルールで使用できます。
- マッピング IP アドレス プールは、次のアドレスを含むことができません。
  - マッピング インターフェイスの IP アドレス。ルールに --Any-- インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT（ルーテッド モードのみ）の場合、IP アドレスの代わりにインターフェイス名を使用します。
  - （トランスペアレント モード）管理 IP アドレス。
  - （ダイナミック NAT）VPN がイネーブルの場合は、スタンバイ インターフェイスの IP アドレス。
  - 既存の VPN プールのアドレス。
- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- NAT のトランザクション コミット モデルを使用することで、システムのパフォーマンスと信頼性を高めることができます。詳細については、『一般的な操作のコンフィギュレーション ガイド』の基本設定の章を参照してください。このオプションは、[Configurations] > [Device Management] > [Advanced] > [Rule Engine] にあります。

デフォルト設定

- デフォルトでは、NAT テーブルのセクション 1 の最後にルールが追加されます。
- （ルーテッド モード）デフォルトの実際のインターフェイスおよびマッピング インターフェイスは Any で、すべてのインターフェイスにルールが適用されます。
- （8.3(1)、8.3(2)、8.4(1)）アイデンティティ NAT のデフォルト動作で、プロキシ ARP はディセーブルにされます。これは設定できません。（8.4(2) 以降）アイデンティティ NAT のデフォルト動作で、プロキシ ARP はイネーブルにされ、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP をディセーブルにできます。
- オプションのインターフェイスを指定する場合、ASA によって NAT コンフィギュレーションが使用されて、出力インターフェイスが決定されます。（8.3(1) ～ 8.4(1)）唯一の例外はアイデンティティ NAT です。アイデンティティ NAT では、NAT コンフィギュレーションに関係なく、常にルート ルックアップが使用されます。（8.4(2) 以降）アイデンティティ NAT の場合、デフォルト動作は NAT コンフィギュレーションの使用ですが、代わりにルート ルックアップを常に使用するオプションがあります。

Twice NAT の設定

この項では、Twice NAT の設定方法について説明します。

- 「ダイナミック NAT または PAT プールを使用したダイナミック PAT の設定」（P.7-5）
- 「ダイナミック PAT（隠蔽）の設定」（P.7-13）
- 「スタティック NAT またはポート変換を設定したスタティック NAT の設定」（P.7-19）
- 「アイデンティティ NAT の設定」（P.7-25）
- 「Per-Session PAT ルールの設定」（P.7-31）

ダイナミック NAT または PAT プールを使用したダイナミック PAT の設定

この項では、ダイナミック NAT または PAT プールを使用するダイナミック PAT の Twice NAT を設定する方法について説明します。詳細については、「ダイナミック NAT」（P.5-8）または「ダイナミック PAT」（P.5-10）を参照してください。

ガイドライン

PAT プールの場合：

- 使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用 *できない* 場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。（8.4(3) 以降、8.5(1) または 8.6(1) を除く）下位ポート範囲を使用するトラフィックが数多くある場合は、PAT プールに対して、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。1024 ～ 65535 または 1 ～ 65535 です。
- （8.4(3) 以降、8.5(1) または 8.6(1) を除く）2 つの個別のルールで同じ PAT プール オブジェクトを使用する場合は、各ルールに対して同じオプションを指定します。たとえば、1 つのルールで拡張 PAT およびフラットな範囲が指定される場合は、もう一方のルールでも拡張 PAT およびフラットな範囲が指定される必要があります。

PAT プールの拡張 PAT の場合（8.4(3) 以降、8.5(1) または 8.6(1) を除く）：

- 多くのアプリケーション インスペクションでは、拡張 PAT はサポートされていません。サポート対象外のインスペクションの完全な一覧については、第 8 章「アプリケーション レイヤ プロトコル インスペクションの準備」の「デフォルト インスペクションと NAT に関する制限事項」（P.8-6）を参照してください。
- ダイナミック PAT ルールに対して拡張 PAT をイネーブルにする場合は、PAT プール内のアドレスを、ポート変換ルールを設定した別のスタティック NAT の PAT アドレスとしても使用することはできません。たとえば、PAT プールに 10.1.1.1 が含まれている場合、PAT アドレスとして 10.1.1.1 を使用する、ポート変換ルールを設定したスタティック NAT は作成できません。
- NAT プールは固有の宛先ごとに作成されるため、拡張 PAT は大量のメモリを消費する場合があり、メモリを使い尽くしてしまう可能性があります。これにより、接続数を減らしたとしても、すぐにメモリが枯渇してしまう場合があります。
- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。
- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。

PAT プールのラウンドロビンの場合：

- （8.4(3) 以降、8.5(1) または 8.6(1) を除く）ホストに既存の接続がある場合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT IP アドレスが使用されます。**注**：この「粘着性」は、フェールオーバーが発生すると失われます。ASA がフェールオーバーすると、ホストからの後続の接続では最初の IP アドレスが使用されない場合があります。

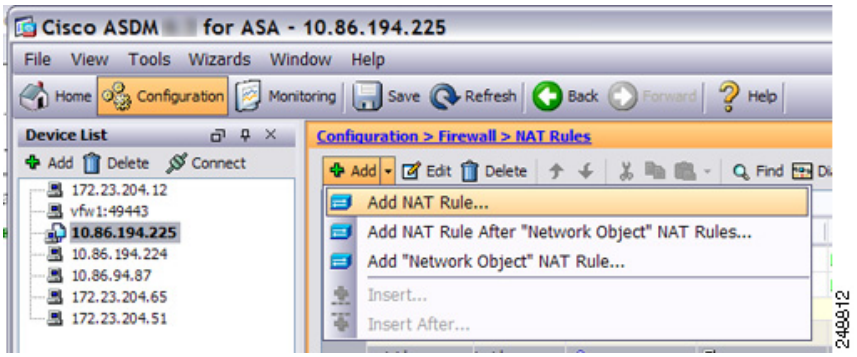
- （8.4(2)、8.5(1)、および 8.6(1)）ホストに既存の接続がある場合、そのホストからの後続の接続では、ラウンドロビン割り当てのため、接続ごとに*別の* PAT アドレスが使用される可能性があります。この場合、ホストについて情報を交換する 2 つの Web サイト（e- コマース サイトと支払サイトなど）にアクセスするときに問題が発生する可能性があります。これらのサイトが、1 つのホストとして扱うべきものを 2 つの異なる IP アドレスと見なした場合、トランザクションは失敗することがあります。
- ラウンドロビンでは、特に拡張 PAT と組み合わせた場合に、大量のメモリが消費されます。NAT プールはマッピングされるプロトコル/IP アドレス/ポート範囲ごとに作成されるため、ラウンドロビンでは数多くの同時 NAT プールが作成され、メモリが使用されます。拡張 PAT では、さらに多くの同時 NAT プールが作成されます。

手順の詳細

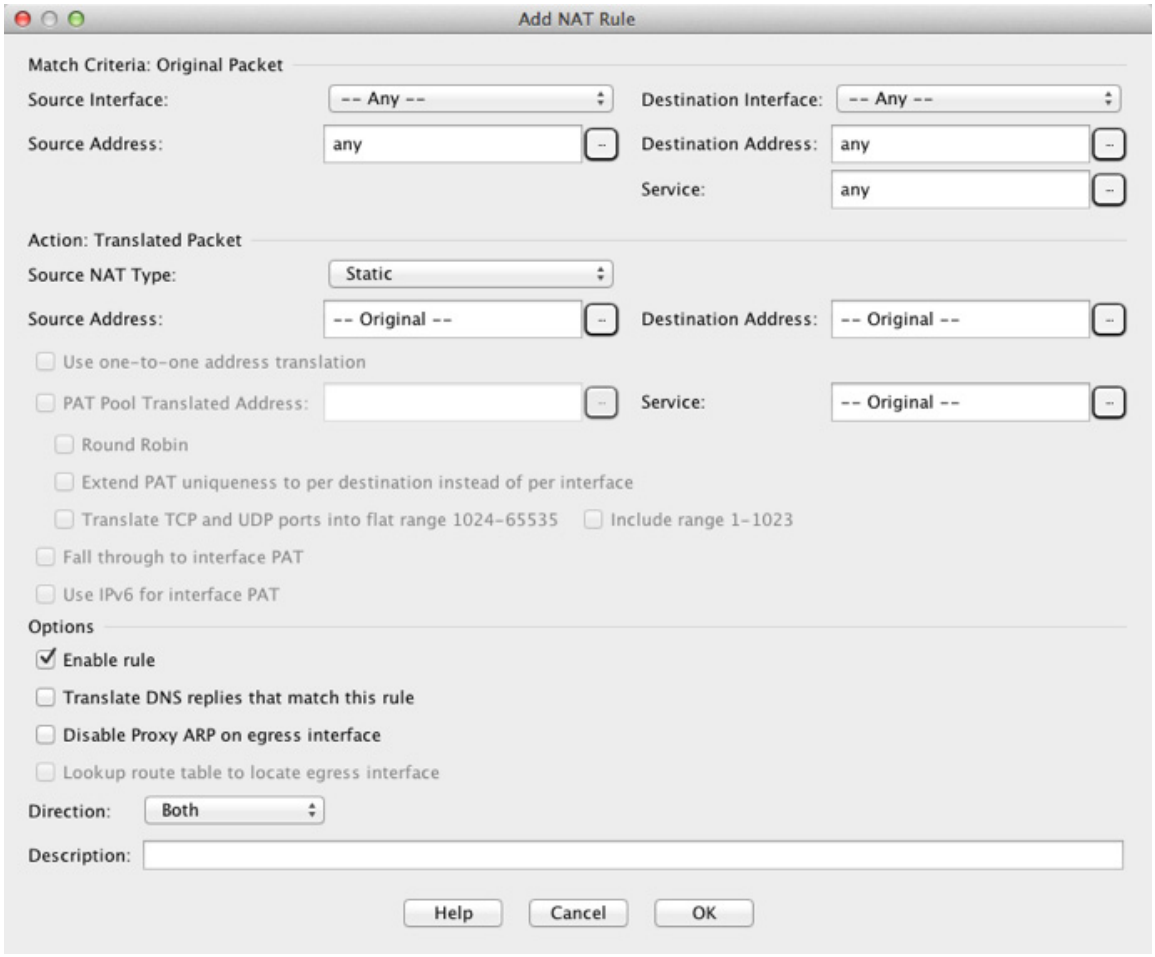
ダイナミック NAT を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] を選択して、[Add] をクリックします。

このルールをセクション 3（ネットワーク オブジェクト ルールの後）に追加する場合は、[Add] の横にある下矢印をクリックし、[Add NAT Rule After Network Object NAT Rules] を選択します。



[Add NAT Rule] ダイアログボックスが表示されます。

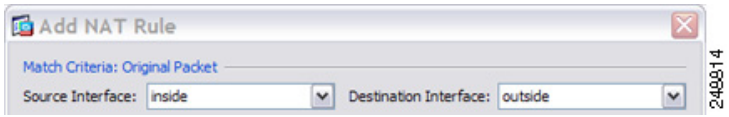


ステップ 2　送信元インターフェイスおよび宛先インターフェイスを設定します。

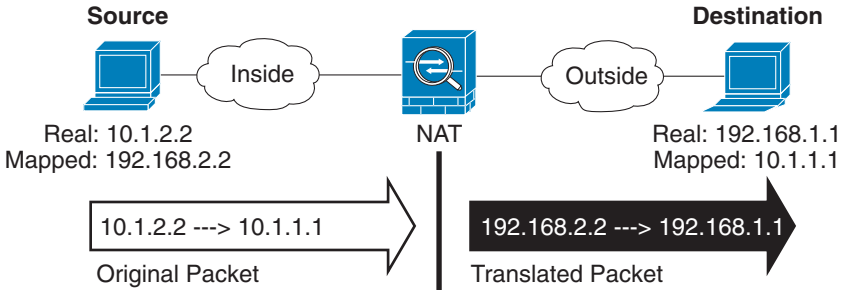
ルーテッド モードのデフォルトでは、どちらのインターフェイスも --Any-- に設定されています。トランスペアレント ファイアウォール モードでは、特定のインターフェイスを設定する必要があります。

a. [Match Criteria: Original Packet] > [Source Interface] ドロップダウン リストから、送信元インターフェイスを選択します。

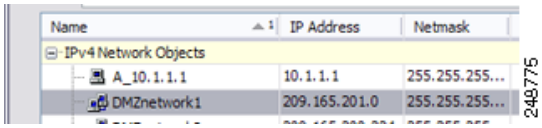
b. [Match Criteria: Original Packet] > [Destination Interface] ドロップダウン リストから、宛先インターフェイスを選択します。



ステップ 3　元のパケットのアドレスが IPv4 であるか IPv6 であるか、つまり、パケットのアドレスが送信元インターフェイス上のネットワーク（*実際の送信元アドレス*と *マッピング宛先アドレス*）に表示されるかどうかを識別します。元のパケットと変換されたパケットの例については、次の図を参照してください。



a. [Match Criteria: Original Packet] > [Source Address] の場合、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Original Source Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。デフォルトは **any** です。

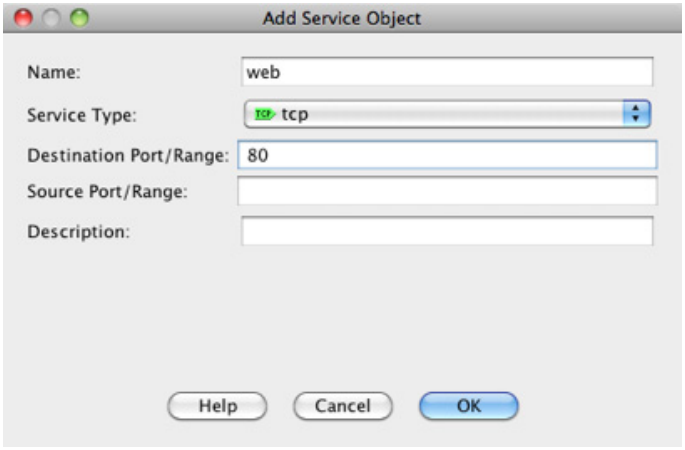


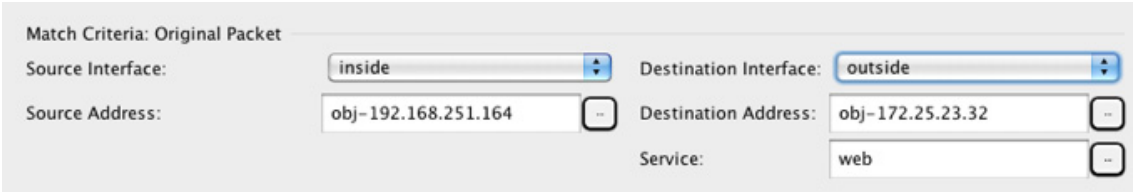
b. （オプション）[Match Criteria: Original Packet] > [Destination Address] の場合、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Original Destination Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。

Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、単にアイデンティティ NAT を使用できます。宛先アドレスを使用せずに Twice NAT を設定して、実際のアドレスに対するネットワーク オブジェクト グループの使用または手動でのルールの順序付けを含む、Twice NAT の他の特質の一部を活用することができます。詳細については、「ネットワーク オブジェクト NATと Twice NAT の主な違い」（P.5-15）を参照してください。

ステップ 4　（オプション）元のパケット ポート（*マッピング宛先ポート*）を識別します。[Match Criteria: Original Packet] > [Service] の場合、参照ボタンをクリックして既存の TCP または UDP サービス オブジェクトを選択するか、[Browse Original Service] ダイアログボックスから新しいオブジェクトを作成します。

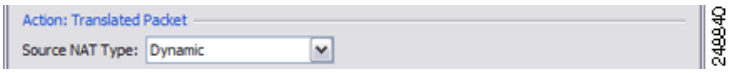
ダイナミック NAT では、ポート変換はサポートされません。しかし、宛先変換は常にスタティックなので、宛先ポートに対してポート変換を実行できます。サービス オブジェクトには送信元ポートと宛先ポートの両方を含めることができますが、この場合は、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。「not equal（等しくない）」（**!=**）演算子はサポートされていません。



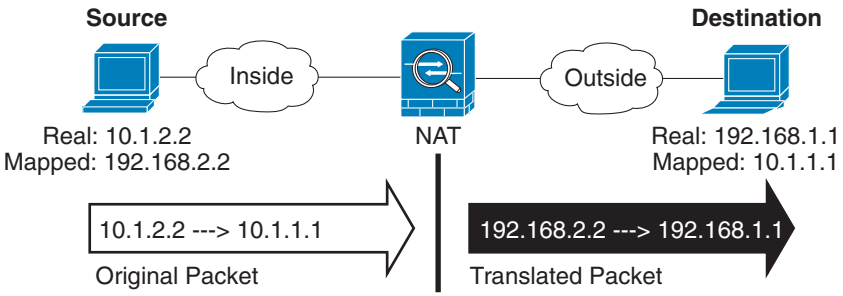


ステップ 5　[Match Criteria: Translated Packet] > [Source NAT Type] ドロップダウン リストから、[Dynamic] を選択します。

この設定は送信元アドレスにのみ適用されます。宛先の変換は常にスタティックになります。



ステップ 6　変換済みパケットのアドレスが IPv4 であるか IPv6 であるか、つまり、パケットのアドレスが宛先インターフェイス上のネットワーク（*マッピング送信元アドレス*と*実際の宛先アドレス*）に表示されるかどうかを識別します。必要に応じて、IPv4 と IPv6 の間で変換できます。元のパケットと変換されたパケットの例については、次の図を参照してください。



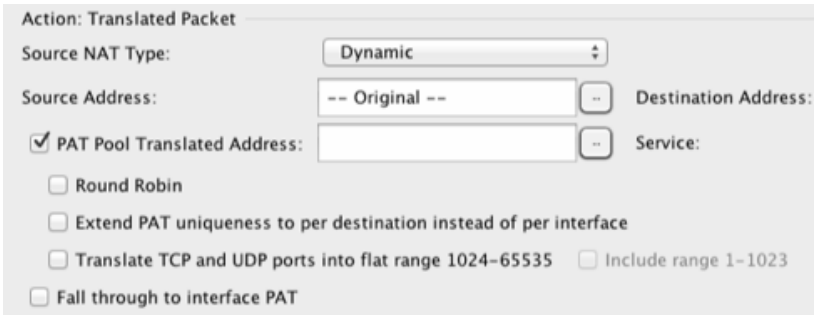
a.　ダイナミック NAT または PAT プールを使用するダイナミック PAT を実行できます。

- ダイナミック NAT：[Match Criteria: Translated Packet] > [Source Address] の場合、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Translated Source Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。

ダイナミック NAT では、通常、大きい送信元アドレスのグループが小さいグループにマッピングされます。

（注） オブジェクトまたはグループは、サブネットを含むことはできません。

- PAT プールを使用したダイナミック PAT : PAT プールを設定するには、[PAT Pool Translated Address] チェックボックスをオンにしてから、参照ボタンをクリックして、既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Translated PAT Pool Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。**注**：[Source Address] フィールドは空のままにしておきます。



（注） オブジェクトまたはグループは、サブネットを含むことはできません。

（オプション）PAT プールの場合は、次のオプションを設定します。

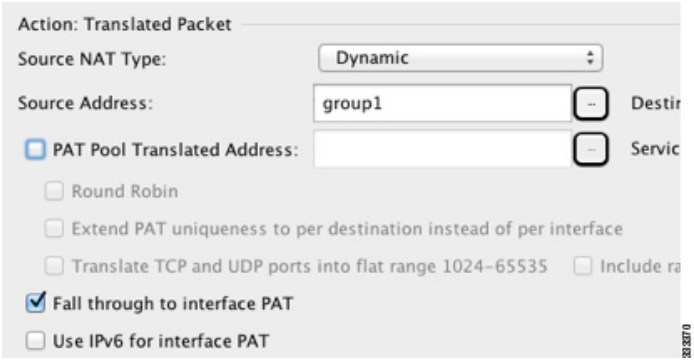
– ラウンドロビン方式でアドレス/ポートを割り当てるには、[Round Robin] チェックボックスをオンにします。ラウンドロビンを使用しない場合、デフォルトでは、次の PAT アドレスが使用される前に PAT アドレスのすべてのポートが割り当てられます。ラウンドロビン方式では、最初のアドレスに戻って再び使用される前に、2 番目のアドレス、またその次と、プール内の各 PAT アドレスからアドレス/ポートが割り当てられます。

– （8.4(3) 以降、8.5(1) または 8.6(1) を除く）拡張 PAT を使用するには、[Extend PAT uniqueness to per destination instead of per interface] チェックボックスをオンにします。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、*サービス*ごとに 65535 個のポートが使用されます。通常は、PAT 変換を作成するときに宛先ポートとアドレスは考慮されないため、PAT アドレスごとに 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。

– （8.4(3) 以降、8.5(1) または 8.6(1) を除く）ポートの割り当て時に 1 つのフラットな範囲として 1024 ～ 65535 のポート範囲を使用するには、[Translate TCP or UDP ports into flat range (1024-65535)] チェックボックスをオンにします。変換のマッピング ポート番号を選択するときに、ASA によって、使用可能な場合は実際の送信元ポート番号が使用されます。ただし、このオプションを設定しないと、実際のポートが使用 *できない* 場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の全範囲を使用するには、[Include range 1 to 1023] チェックボックスもオンにします。

b. （任意、ルーテッド モードのみ）他のマッピングされた送信元アドレスがすでに割り当てられている場合に、インターフェイス IP アドレスをバックアップの手段として使用するには、[Fall through to interface PAT] チェックボックスをオンにします。IPv6 インターフェイス アドレスを使用するには、[Use IPv6 for interface PAT] チェックボックスもオンにします。

宛先インターフェイス IP アドレスが使用されます。このオプションは、特定の [Destination Interface] を設定する場合にだけ使用できます。

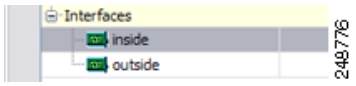


c. [Match Criteria: Translated Packet] > [Destination Address] の場合、参照ボタンをクリックして既存のネットワーク オブジェクト、グループ、またはインターフェイスを選択するか、[Browse Translated Destination Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。

宛先アドレスのアイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。

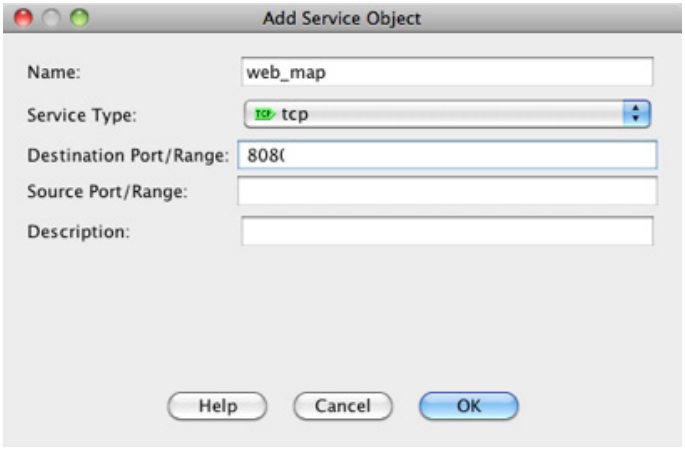
宛先アドレスを変換する場合、スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、「スタティック NAT」（P.5-3）を参照してください。拒否されるマッピング IP アドレスについては、「ガイドラインと制限事項」（P.7-2）を参照してください。

ポート変換を設定したスタティック インターフェイス NAT に限り、[Browse] ダイアログボックスからインターフェイスを選択します。サービス変換も必ず設定します（ステップ 7 を参照）。このオプションでは、ステップ 2 で [Source Interface] に特定のインターフェイスを設定する必要があります。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.5-6）を参照してください。

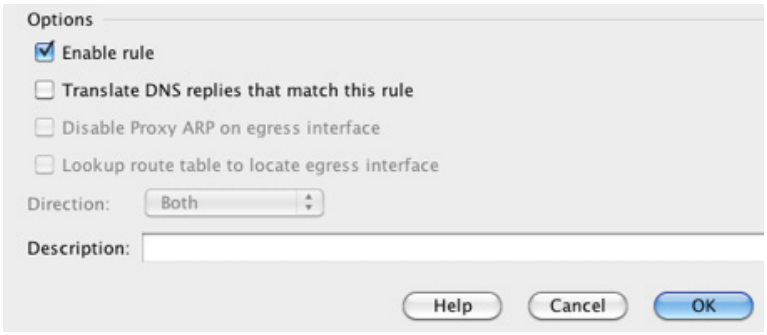


ステップ 7　（オプション）変換されたパケット ポート（*実際の宛先ポート*）を識別します。[Match Criteria: Translated Packet] > [Service] の場合、参照ボタンをクリックして既存の TCP または UDP サービス オブジェクトを選択するか、[Browse Translated Service] ダイアログボックスから新しいオブジェクトを作成します。

ダイナミック NAT では、ポート変換はサポートされません。しかし、宛先変換は常にスタティックなので、宛先ポートに対してポート変換を実行できます。サービス オブジェクトには送信元ポートと宛先ポートの両方を含めることができますが、この場合は、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。「not equal（等しくない）」（**!=**）演算子はサポートされていません。



ステップ 8　（オプション）[Options] 領域で NAT オプションを設定します。



a. [Enable rule]：この NAT ルールをイネーブルにします。このルールはデフォルトでイネーブルになっています。

b. （送信元専用ルールの場合）[Translate DNS replies that match this rule]：DNS 応答内の DNS A レコードを書き換えます。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。宛先アドレスを設定する場合、DNS 修正は設定できません。詳細については、「DNS および NAT」（P.5-32）を参照してください。

c. [Description]：ルールに関する説明を 200 文字以内で追加します。

ステップ 9　[OK] をクリックします。

ダイナミック PAT（隠蔽）の設定

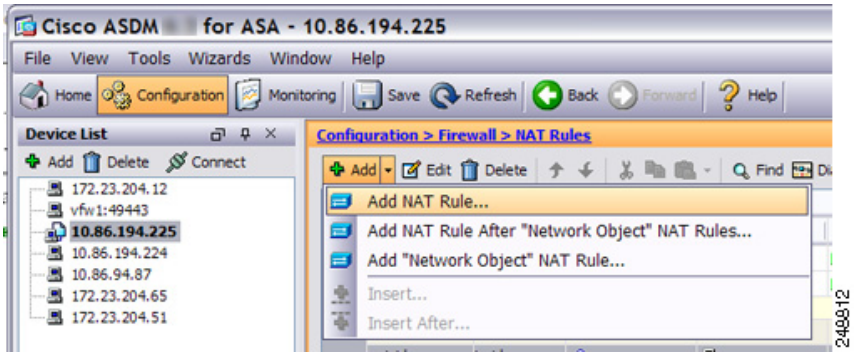
この項では、ダイナミック PAT（隠蔽）の Twice NAT の設定方法について説明します。PAT プールを使用するダイナミック PAT については、この項ではなく、「ダイナミック NAT または PAT プールを使用したダイナミック PAT の設定」（P.7-5）を参照してください。詳細については、「ダイナミック PAT」（P.5-10）を参照してください。

手順の詳細

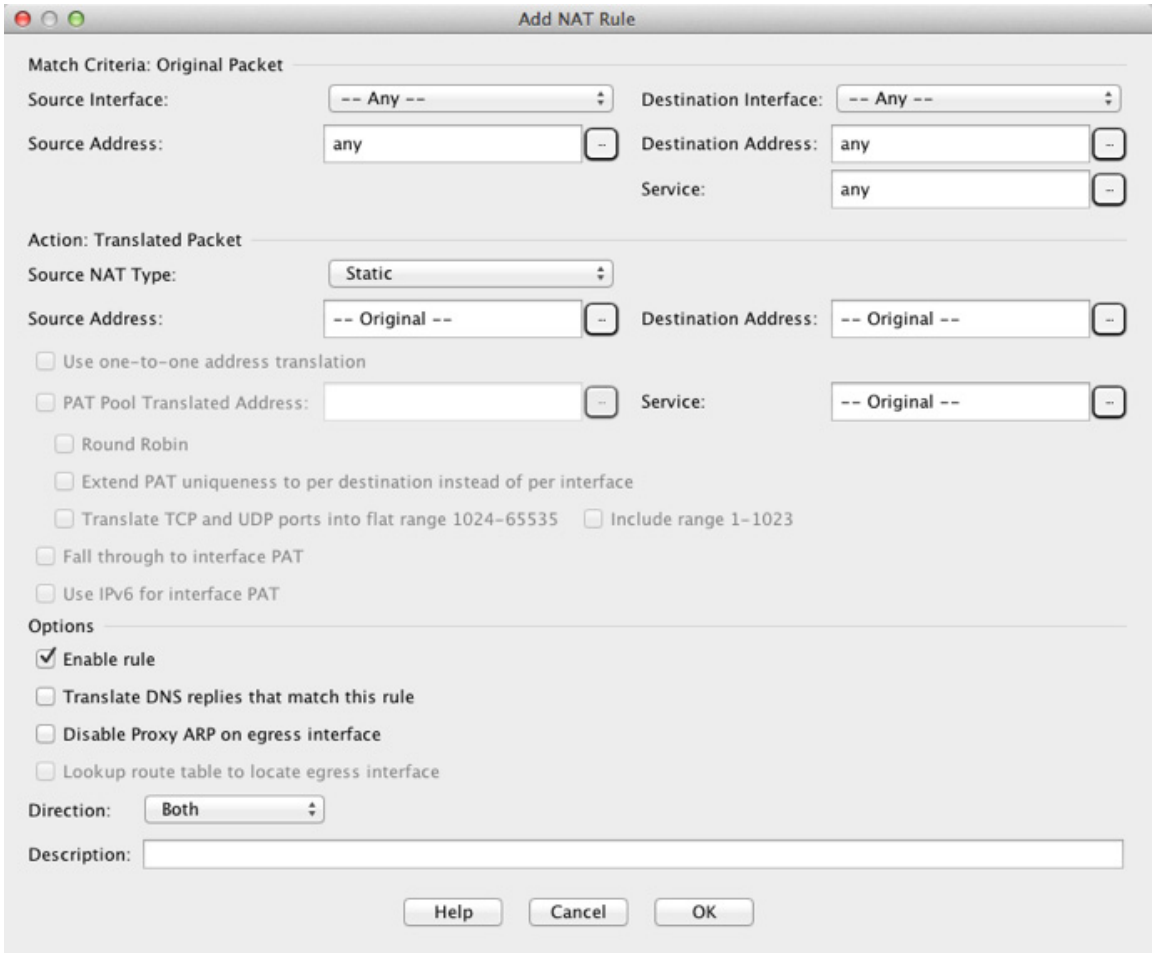
ダイナミック PAT を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] を選択して、[Add] をクリックします。

このルールをセクション 3（ネットワーク オブジェクト ルールの後）に追加する場合は、[Add] の横にある下矢印をクリックし、[Add NAT Rule After Network Object NAT Rules] を選択します。



[Add NAT Rule] ダイアログボックスが表示されます。

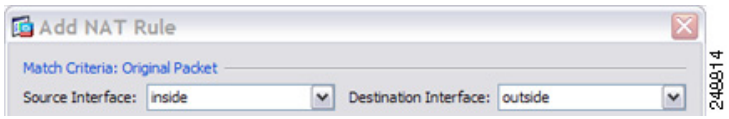


ステップ 2　送信元インターフェイスおよび宛先インターフェイスを設定します。

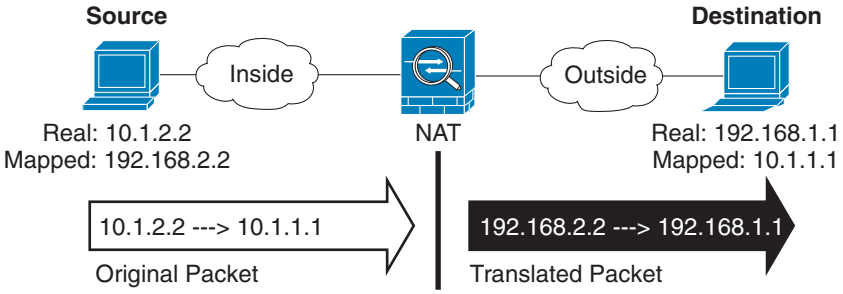
ルーテッド モードのデフォルトでは、どちらのインターフェイスも --Any-- に設定されています。トランスペアレント ファイアウォール モードでは、特定のインターフェイスを設定する必要があります。

a. [Match Criteria: Original Packet] > [Source Interface] ドロップダウン リストから、送信元インターフェイスを選択します。

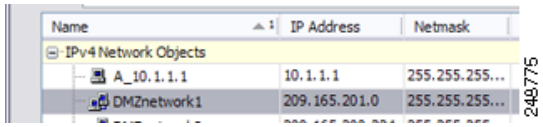
b. [Match Criteria: Original Packet] > [Destination Interface] ドロップダウン リストから、宛先インターフェイスを選択します。



ステップ 3　元のパケットのアドレスが IPv4 であるか IPv6 であるか、つまり、パケットのアドレスが送信元インターフェイス上のネットワーク（*実際の送信元アドレス*と *マッピング宛先アドレス*）に表示されるかどうかを識別します。元のパケットと変換されたパケットの例については、次の図を参照してください。



a. [Match Criteria: Original Packet] > [Source Address] の場合、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Original Source Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。デフォルトは **any** です。

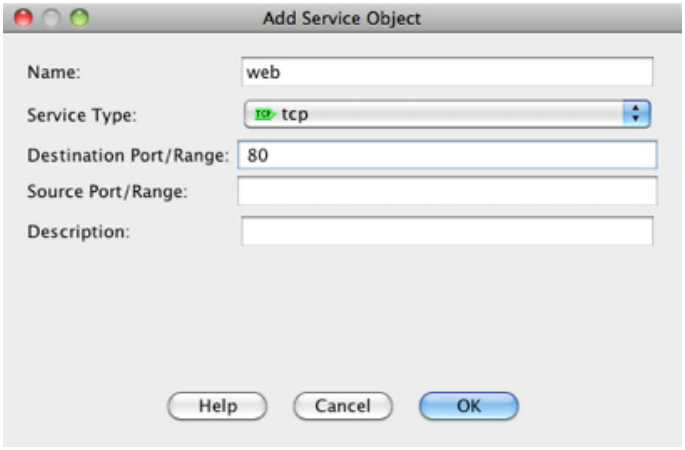


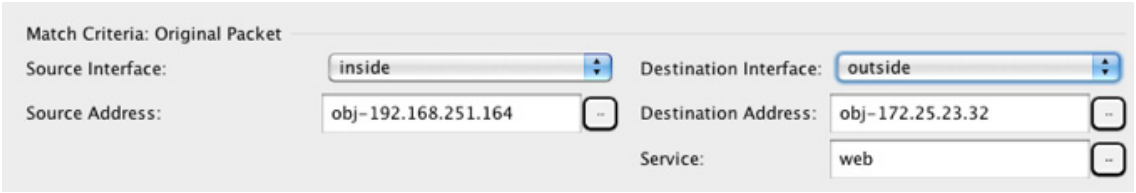
b. （オプション）[Match Criteria: Original Packet] > [Destination Address] の場合、参照ボタン をクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Original Destination Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。

Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、単にアイデンティティ NAT を使用できます。宛先アドレスを使用せずに Twice NAT を設定して、実際のアドレスに対するネットワーク オブジェクト グループの使用または手動でのルールの順序付けを含む、Twice NAT の他の特質の一部を活用することができます。詳細については、「ネットワーク オブジェクト NAT と Twice NAT の主な違い」（P.5-15）を参照してください。

ステップ 4　（オプション）元のパケット ポート（*マッピング宛先ポート*）を識別します。[Match Criteria: Original Packet] > [Service] の場合、参照ボタンをクリックして既存の TCP または UDP サービス オブジェクトを選択するか、[Browse Original Service] ダイアログボックスから新しいオブジェクトを作成します。

ダイナミック PAT では、追加のポート変換はサポートされません。しかし、宛先変換は常にスタティックなので、宛先ポートに対してポート変換を実行できます。サービス オブジェクトには送信元ポートと宛先ポートの両方を含めることができますが、この場合は、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。「not equal（等しくない）」（**!=**）演算子はサポートされていません。

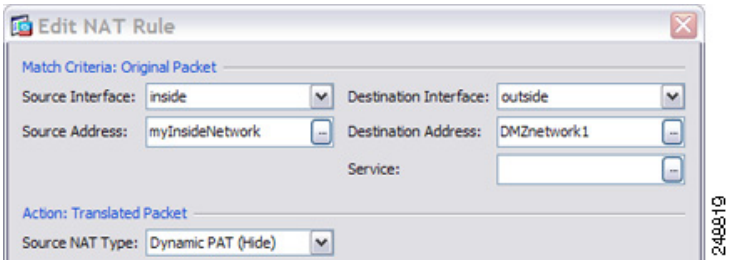




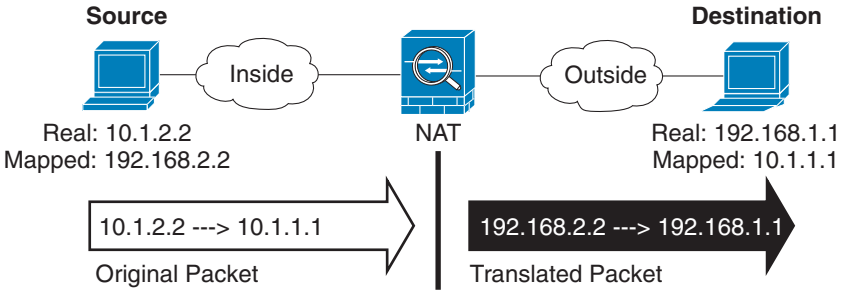
ステップ 5　[Match Criteria: Translated Packet] > [Source NAT Type] ドロップダウン リストから、[Dynamic PAT (Hide)] を選択します。

この設定は送信元アドレスにのみ適用されます。宛先の変換は常にスタティックになります。

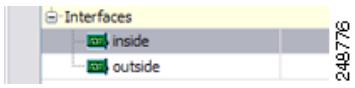
（注）　PAT プールを使用するダイナミック PAT を設定するには、[Dynamic PAT (Hide)] の代わりに [Dynamic] を選択します。「ダイナミック NAT または PAT プールを使用したダイナミック PAT の設定」（P.7-5）を参照してください。



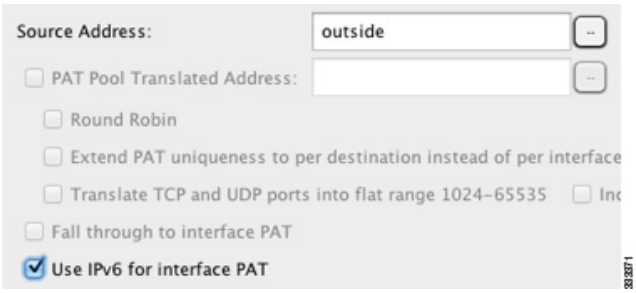
ステップ 6　変換済みパケットのアドレスが IPv4 であるか IPv6 であるか、つまり、パケットのアドレスが宛先インターフェイス上のネットワーク（*マッピング送信元アドレス*と*実際の宛先アドレス*）に表示されるかどうかを識別します。必要に応じて、IPv4 と IPv6 の間で変換できます。元のパケットと変換されたパケットの例については、次の図を参照してください。



a. [Match Criteria: Translated Packet] > [Source Address] の場合、参照ボタンをクリックして既存のネットワーク オブジェクトまたはインターフェイスを選択するか、[Browse Translated Source Address] ダイアログボックスから新しいオブジェクトを作成します。



インターフェイスの IPv6 アドレスを使用するには、[Use IPv6 for interface PAT] チェックボックスをオンにします。



b. [Match Criteria: Translated Packet] > [Destination Address] の場合、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Translated Destination Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。

宛先アドレスのアイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。

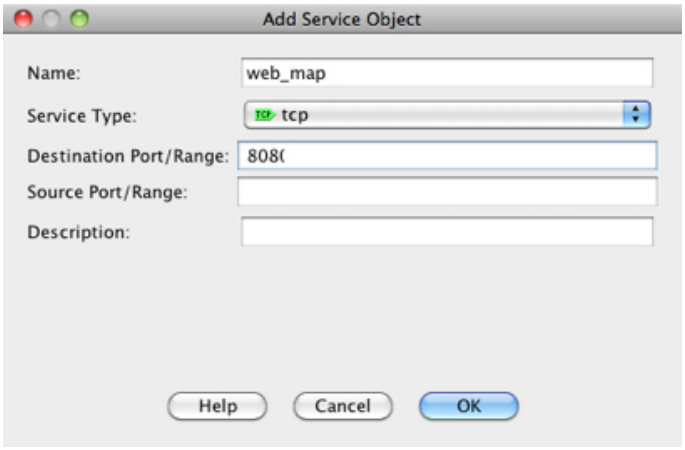
宛先アドレスを変換する場合、スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、「スタティック NAT」（P.5-3）を参照してください。拒否されるマッピング IP アドレスについては、「ガイドラインと制限事項」（P.7-2）を参照してください。

ポート変換を設定したスタティック インターフェイス NAT に限り、[Browse] ダイアログボックスからインターフェイスを選択します。サービス変換も必ず設定します（ステップ 7 を参照）。このオプションでは、ステップ 2 で [Source Interface] に特定のインターフェイスを設定する必要があります。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.5-6）を参照してください。

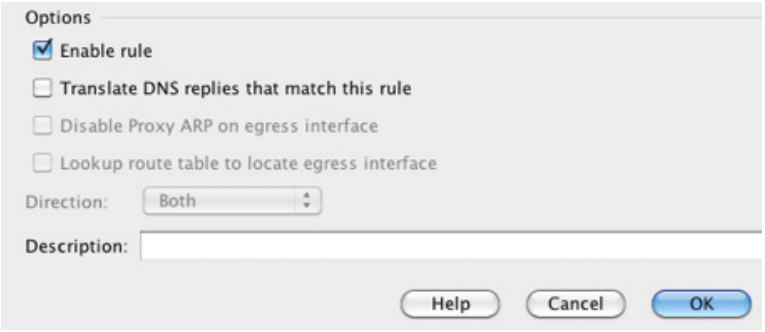
ステップ 7　（オプション）変換されたパケット ポート（*実際の宛先ポート*）を識別します。[Match Criteria: Translated Packet] > [Service] の場合、参照ボタンをクリックして [Browse Translated Service] ダイアログボックスから既存の TCP または UDP サービス オブジェクトを選択します。

[Browse Translated Service] ダイアログボックスから新しいサービス オブジェクトを作成して、このオブジェクトをマッピング宛先ポートとして使用することもできます。

ダイナミック PAT では、追加のポート変換はサポートされません。しかし、宛先変換は常にスタティックなので、宛先ポートに対してポート変換を実行できます。サービス オブジェクトには送信元ポートと宛先ポートの両方を含めることができますが、この場合は、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。「not equal（等しくない）」（**!=**）演算子はサポートされていません。



ステップ 8　（オプション）[Options] 領域で NAT オプションを設定します。



a. [Enable rule]：この NAT ルールをイネーブルにします。このルールはデフォルトでイネーブルになっています。

b. （送信元専用ルールの場合）[Translate DNS replies that match this rule]：DNS 応答内の DNS A レコードを書き換えます。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。宛先アドレスを設定する場合、DNS 修正は設定できません。詳細については、「DNS および NAT」（P.5-32）を参照してください。

c. [Description]：ルールに関する説明を 200 文字以内で追加します。

ステップ 9　[OK] をクリックします。

スタティック NAT またはポート変換を設定したスタティック NAT の設定

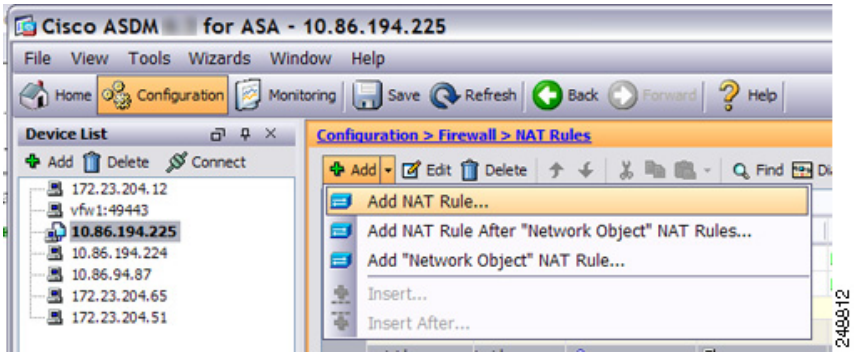
この項では、Twice NAT を使用してスタティック NAT ルールを設定する方法について説明します。スタティック NAT の詳細については、「スタティック NAT」（P.5-3）を参照してください。

手順の詳細

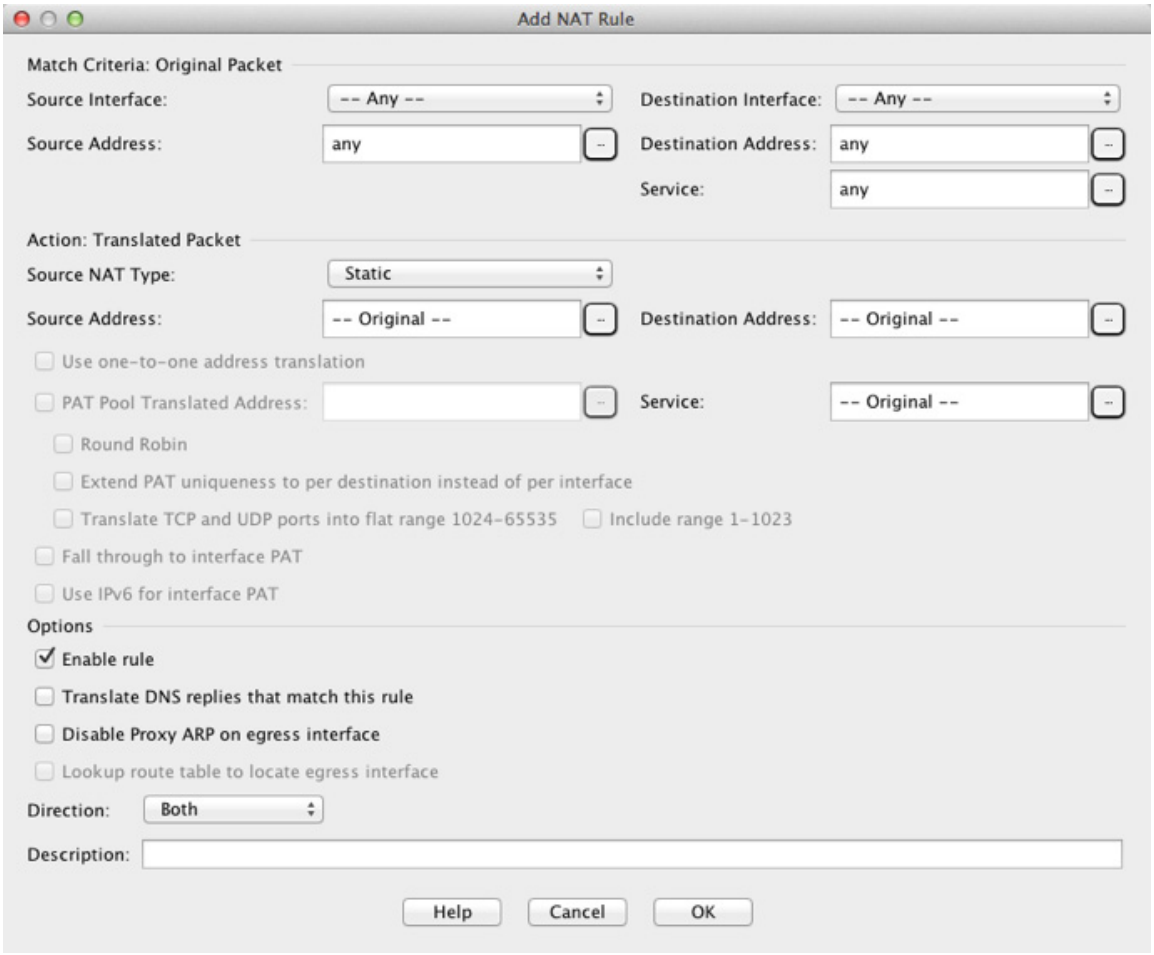
スタティック NAT を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] を選択して、[Add] をクリックします。

このルールをセクション 3（ネットワーク オブジェクト ルールの後）に追加する場合は、[Add] の横にある下矢印をクリックし、[Add NAT Rule After Network Object NAT Rules] を選択します。



[Add NAT Rule] ダイアログボックスが表示されます。

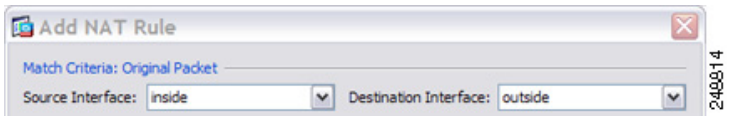


ステップ 2　送信元インターフェイスおよび宛先インターフェイスを設定します。

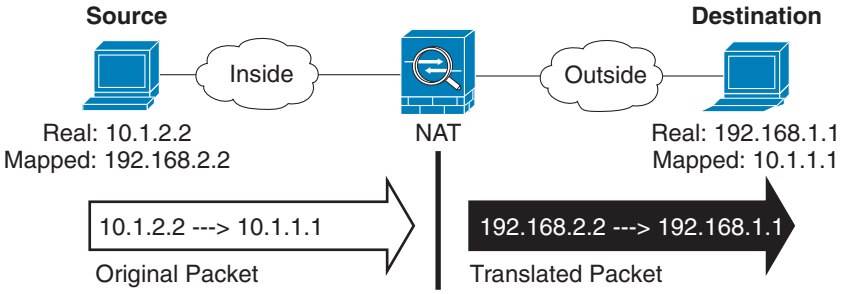
ルーテッド モードのデフォルトでは、どちらのインターフェイスも --Any-- に設定されています。トランスペアレント ファイアウォール モードでは、特定のインターフェイスを設定する必要があります。

a. [Match Criteria: Original Packet] > [Source Interface] ドロップダウン リストから、送信元インターフェイスを選択します。

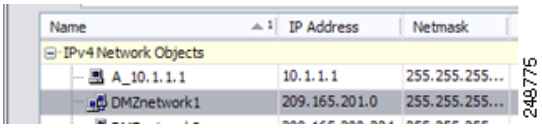
b. [Match Criteria: Original Packet] > [Destination Interface] ドロップダウン リストから、宛先インターフェイスを選択します。



ステップ 3　元のパケットのアドレスが IPv4 であるか IPv6 であるか、つまり、パケットのアドレスが送信元インターフェイス上のネットワーク（*実際の送信元アドレス*と *マッピング宛先アドレス*）に表示されるかどうかを識別します。元のパケットと変換されたパケットの例については、次の図を参照してください。



a. [Match Criteria: Original Packet] > [Source Address] の場合、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Original Source Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。デフォルトは **any** ですが、アイデンティティ NAT を除いてはこのオプションを使用しないでください。詳細については、「アイデンティティ NAT の設定」（P.7-25）を参照してください。

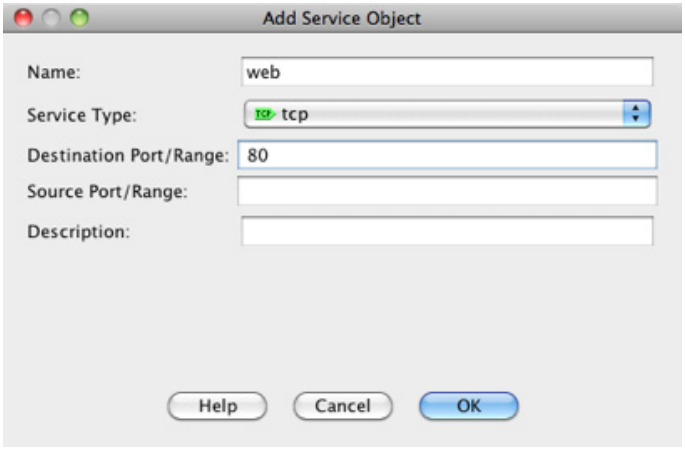


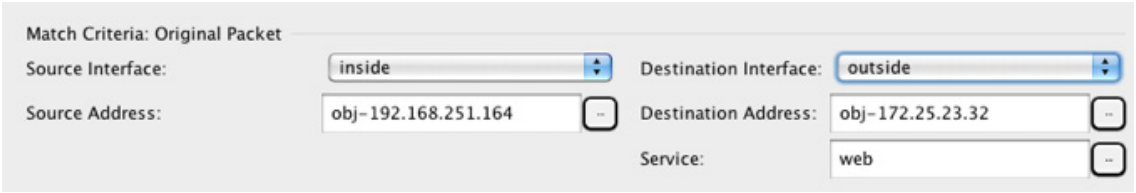
b. （オプション）[Match Criteria: Original Packet] > [Destination Address] の場合、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Original Destination Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。

Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、単にアイデンティティ NAT を使用できます。宛先アドレスを使用せずに Twice NAT を設定して、実際のアドレスに対するネットワーク オブジェクト グループの使用または手動でのルールの順序付けを含む、Twice NAT の他の特質の一部を活用することができます。詳細については、「ネットワーク オブジェクト NAT と Twice NAT の主な違い」（P.5-15）を参照してください。

ステップ 4　（オプション）元のパケットの送信元ポートまたは宛先ポート（*実際の送信元ポート*または*マッピング宛先ポート*）を識別します。[Match Criteria: Original Packet] > [Service] の場合、参照ボタンをクリックして既存の TCP または UDP サービス オブジェクトを選択するか、[Browse Original Service] ダイアログボックスから新しいオブジェクトを作成します。

サービス オブジェクトは、送信元ポートと宛先ポートの両方を含むことができます。実際のサービス オブジェクトとマッピング サービス オブジェクトの両方に、送信元ポート *または*宛先ポートの*いずれか*を指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバなど）に送信元ポートおよび宛先ポートの*両方*を指定する必要がありますが、固定の送信元ポートはめったに使用されません。オブジェクトで送信元ポートと宛先ポートの両方を指定することはほとんどありませんが、この場合には、元のパケットのサービス オブジェクトに実際の送信元ポート/マッピングされた宛先ポートが含まれます。変換されたパケットのサービス オブジェクトには、マッピングされた送信元ポート/実際の宛先ポートが含まれます。NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。「not equal（等しくない）」（**!=**）演算子はサポートされていません。

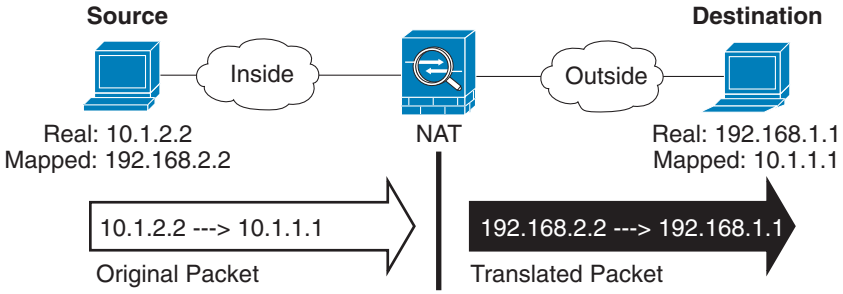




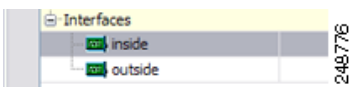
ステップ 5　[Match Criteria: Translated Packet] > [Source NAT Type] ドロップダウン リストから、[Static] を選択します。[Static] がデフォルトの設定です。

この設定は送信元アドレスにのみ適用されます。宛先の変換は常にスタティックになります。

ステップ 6　変換済みパケットのアドレスが IPv4 であるか IPv6 であるか、つまり、パケットのアドレスが宛先インターフェイス上のネットワーク（*マッピング送信元アドレス*と*実際の宛先アドレス*）に表示されるかどうかを識別します。必要に応じて、IPv4 と IPv6 の間で変換できます。元のパケットと変換されたパケットの例については、次の図を参照してください。

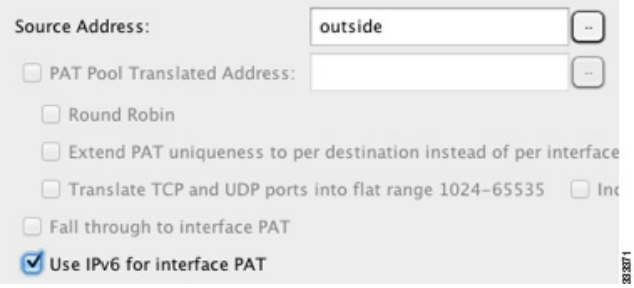


a. [Match Criteria: Translated Packet] > [Source Address] の場合、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Translated Source Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。



スタティック NAT のマッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。

ポート変換が設定されたスタティック インターフェイス NAT では、マッピング アドレスのネットワーク オブジェクト/グループではなく、インターフェイスを指定できます。インターフェイスの IPv6 アドレスを使用するには、[Use IPv6 for interface PAT] チェックボックスをオンにします。



詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.5-6）を参照してください。拒否されるマッピング IP アドレスについては、「ガイドラインと制限事項」（P.7-2）を参照してください。

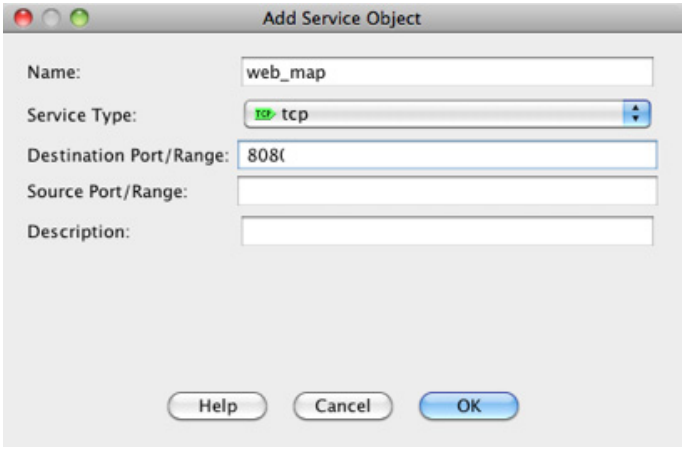
b. [Match Criteria: Translated Packet] > [Destination Address] の場合、参照ボタンをクリックして既存のネットワーク オブジェクト、グループ、またはインターフェイスを選択するか、[Browse Translated Destination Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。

スタティック NAT のマッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。

ポート変換が設定されたスタティック インターフェイス NAT では、マッピング アドレスのネットワーク オブジェクト/グループではなく、インターフェイスを指定できます。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.5-6）を参照してください。拒否されるマッピング IP アドレスについては、「ガイドラインと制限事項」（P.7-2）を参照してください。

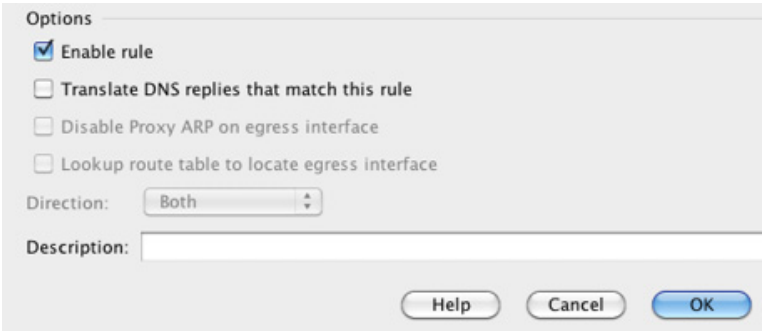
ステップ 7　（オプション）変換されたパケットの送信元ポートまたは宛先ポート（*マッピング送信元ポート***または***実際の宛先ポート*）を識別します。[Match Criteria: Translated Packet] > [Service] の場合、参照ボタンをクリックして既存の TCP または UDP サービス オブジェクトを選択するか、[Browse Translated Service] ダイアログボックスから新しいオブジェクトを作成します。

サービス オブジェクトは、送信元ポートと宛先ポートの両方を含むことができます。実際のサービス オブジェクトとマッピング サービス オブジェクトの両方に、送信元ポート *または*宛先ポートの *いずれか*を指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバなど）に送信元ポートおよび宛先ポートの *両方*を指定する必要がありますが、固定の送信元ポートはめったに使用されません。オブジェクトで送信元ポートと宛先ポートの両方を指定することはほとんどありませんが、この場合には、元のパケットのサービス オブジェクトに実際の送信元ポート/マッピングされた宛先ポートが含まれます。変換されたパケットのサービス オブジェクトには、マッピングされた送信元ポート/実際の宛先ポートが含まれます。NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。「not equal（等しくない）」（**!=**）演算子はサポートされていません。



ステップ 8　（オプション）NAT46 の場合、[Use one-to-one address translation] チェックボックスをオンにします。NAT46 の場合、最初の IPv4 アドレスを最初の IPv6 アドレス、2 番目の IPv4 アドレスを 2 番目の IPv6 アドレス、以下同様に 1 対 1 で順に変換するように指定します。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このキーワードを使用する必要があります。

ステップ 9　（オプション）[Options] 領域で NAT オプションを設定します。



a. [Enable rule]：この NAT ルールをイネーブルにします。このルールはデフォルトでイネーブルになっています。

b. （送信元専用ルールの場合）[Translate DNS replies that match this rule]：DNS 応答内の DNS A レコードを書き換えます。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。宛先アドレスを設定する場合、DNS 修正は設定できません。詳細については、「DNS および NAT」（P.5-32）を参照してください。

c. [Disable Proxy ARP on egress interface]：マッピング IP アドレスへの着信パケットのプロキシ ARP をディセーブルにします。詳細については、「マッピング アドレスとルーティング」（P.5-22）を参照してください。

d. [Direction]：ルールを単方向にするには、[Unidirectional] を選択します。デフォルトは [Both] です。ルールを単方向にすると、トラフィックが実際のアドレスへの接続を開始するのを回避できます。

e. [Description]：ルールに関する説明を 200 文字以内で追加します。

ステップ 10　[OK] をクリックします。

アイデンティティ NAT の設定

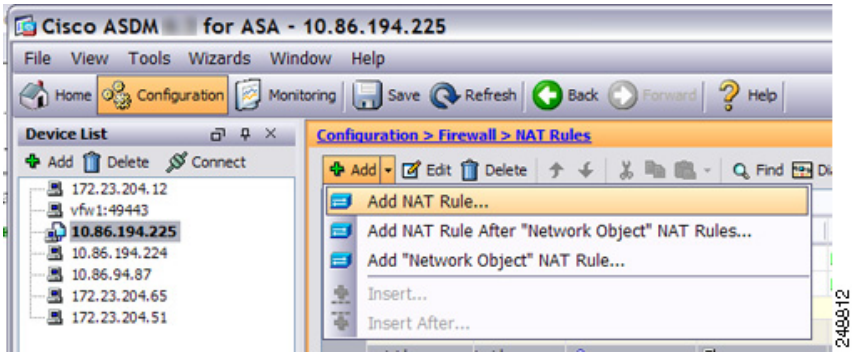
この項では、Twice NAT を使用してアイデンティティ NAT ルールを設定する方法について説明します。アイデンティティ NAT の詳細については、「アイデンティティ NAT」（P.5-12）を参照してください。

手順の詳細

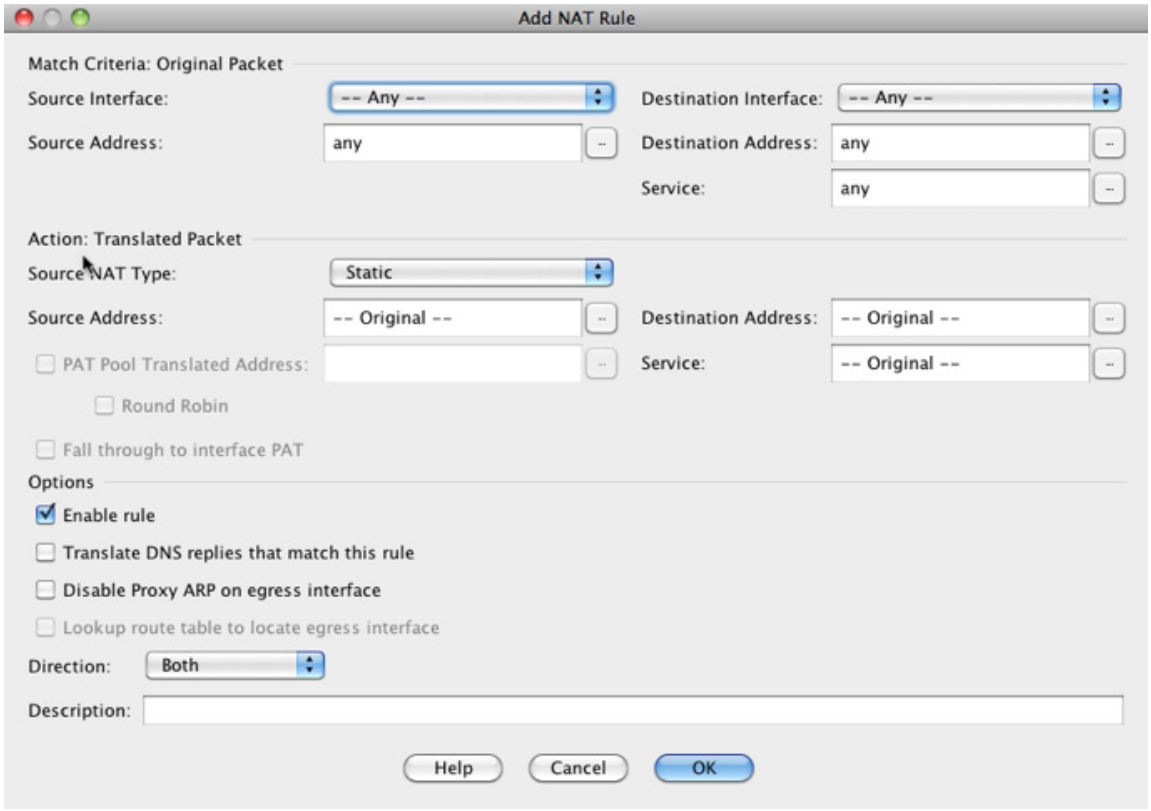
アイデンティティ NAT を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] を選択して、[Add] をクリックします。

このルールをセクション 3（ネットワーク オブジェクト ルールの後）に追加する場合は、[Add] の横にある下矢印をクリックし、[Add NAT Rule After Network Object NAT Rules] を選択します。



[Add NAT Rule] ダイアログボックスが表示されます。

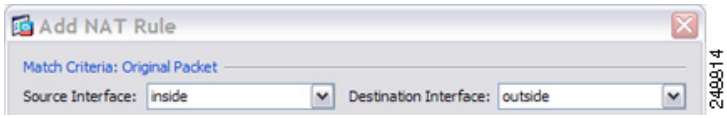


ステップ 2　送信元インターフェイスおよび宛先インターフェイスを設定します。

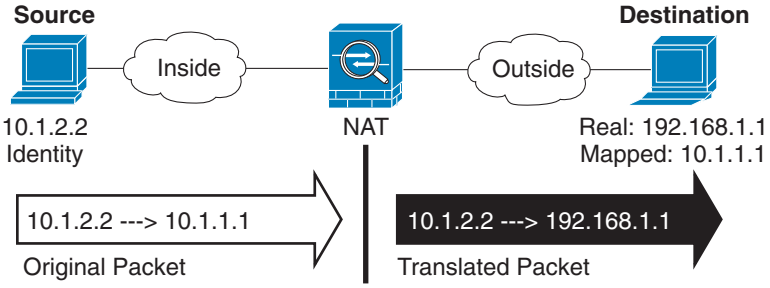
ルーテッド モードのデフォルトでは、どちらのインターフェイスも --Any-- に設定されています。トランスペアレント ファイアウォール モードでは、特定のインターフェイスを設定する必要があります。

a. [Match Criteria: Original Packet] > [Source Interface] ドロップダウン リストから、送信元インターフェイスを選択します。

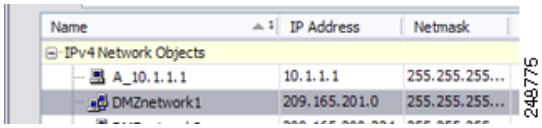
b. [Match Criteria: Original Packet] > [Destination Interface] ドロップダウン リストから、宛先インターフェイスを選択します。



ステップ 3　元のパケットのアドレスが IPv4 であるか IPv6 であるか、つまり、パケットのアドレスが送信元インターフェイス上のネットワーク（*実際の送信元アドレス*と *マッピング宛先アドレス*）に表示されるかどうかを識別します。元のパケットと変換されたパケットの例については、次の図を参照してください。ここでは、内部ホストでアイデンティティ NAT を実行しますが、外部ホストを変換します。



a. [Match Criteria: Original Packet] > [Source Address] の場合、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Original Source Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。デフォルトは **any** です。このオプションは、マッピング アドレスも **any** に設定する場合にのみ使用します。

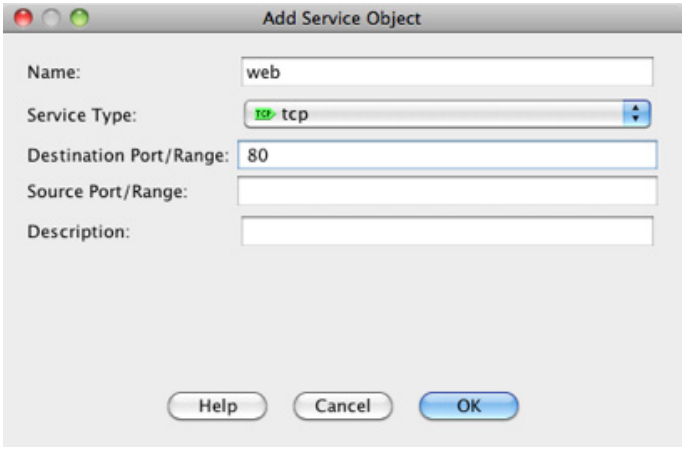


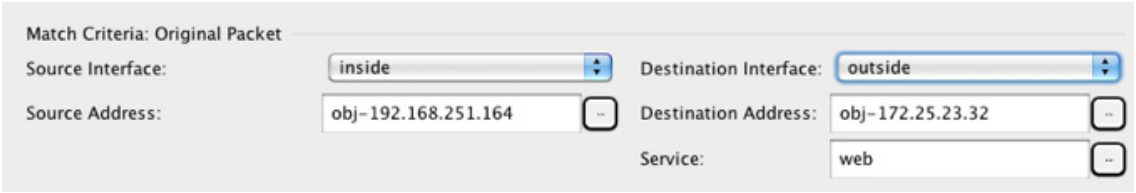
b. （オプション）[Match Criteria: Original Packet] > [Destination Address] の場合、参照ボタン をクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Original Destination Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。

Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、単にアイデンティティ NAT を使用できます。宛先アドレスを使用せずに Twice NAT を設定して、実際のアドレスに対するネットワーク オブジェクト グループの使用または手動でのルールの順序付けを含む、Twice NAT の他の特質の一部を活用することができます。詳細については、「ネットワーク オブジェクト NAT と Twice NAT の主な違い」（P.5-15）を参照してください。

ステップ 4　（オプション）元のパケットの送信元ポートまたは宛先ポート（*実際の送信元ポート*または*マッピング宛先ポート*）を識別します。[Match Criteria: Original Packet] > [Service] の場合、参照ボタンをクリックして既存の TCP または UDP サービス オブジェクトを選択するか、[Browse Original Service] ダイアログボックスから新しいオブジェクトを作成します。

サービス オブジェクトは、送信元ポートと宛先ポートの両方を含むことができます。両方のサービス オブジェクトに、送信元ポート*または*宛先ポートの*いずれか*を指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバなど）に送信元ポートおよび宛先ポートの*両方*を指定する必要がありますが、固定の送信元ポートはめったに使用されません。オブジェクトで送信元ポートと宛先ポートの両方を指定することはほとんどありませんが、この場合には、元のパケットのサービス オブジェクトに実際の送信元ポート/マッピングされた宛先ポートが含まれます。変換されたパケットのサービス オブジェクトには、マッピングされた送信元ポート/実際の宛先ポートが含まれます。NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。「not equal（等しくない）」（**!=**）演算子はサポートされていません。

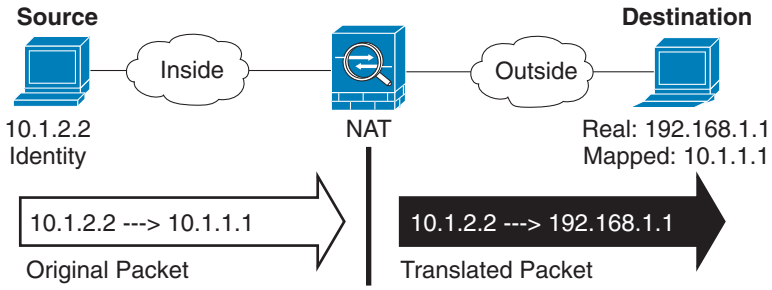




ステップ 5　[Match Criteria: Translated Packet] > [Source NAT Type] ドロップダウン リストから、[Static] を選択します。[Static] がデフォルトの設定です。

この設定は送信元アドレスにのみ適用されます。宛先の変換は常にスタティックになります。

ステップ 6　変換されたパケット アドレスを識別します。つまり、宛先インターフェイス ネットワークに表示されるパケット アドレス（*マッピング送信元アドレス*と*実際の宛先アドレス*）です。元のパケットと変換されたパケットの例については、次の図を参照してください。ここでは、内部ホストでアイデンティティ NAT を実行しますが、外部ホストを変換します。



a. [Match Criteria: Translated Packet] > [Source Address] の場合、参照ボタンをクリックして [Browse Translated Source Address] ダイアログボックスから実際の送信元アドレスに選択したものと同じネットワーク オブジェクトまたはグループを選択します。実際のアドレスに **any** を指定した場合は **any** を使用します。

b. [Match Criteria: Translated Packet] > [Destination Address] の場合、参照ボタンをクリックして既存のネットワーク オブジェクト、グループ、またはインターフェイスを選択するか、[Browse Translated Destination Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。

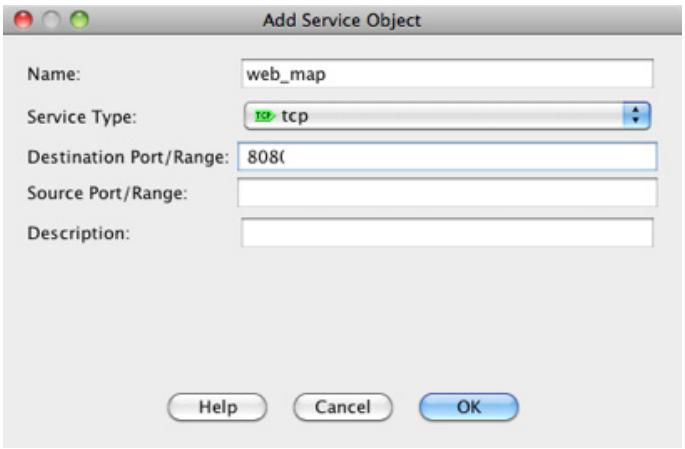
宛先アドレスのアイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。

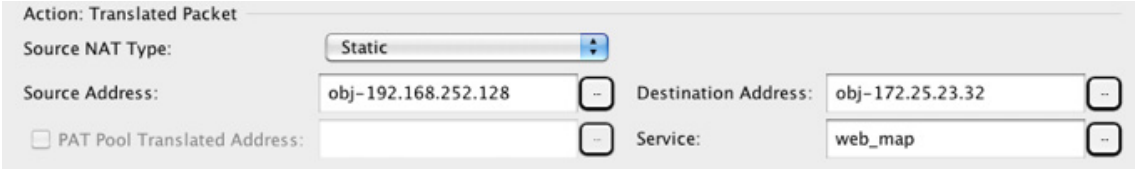
宛先アドレスを変換する場合、スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、「スタティック NAT」（P.5-3）を参照してください。拒否されるマッピング IP アドレスについては、「ガイドラインと制限事項」（P.7-2）を参照してください。

ポート変換を設定したスタティック インターフェイス NAT に限り、インターフェイスを選択します。インターフェイスを指定する場合は、必ずサービス変換も設定します。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.5-6）を参照してください。

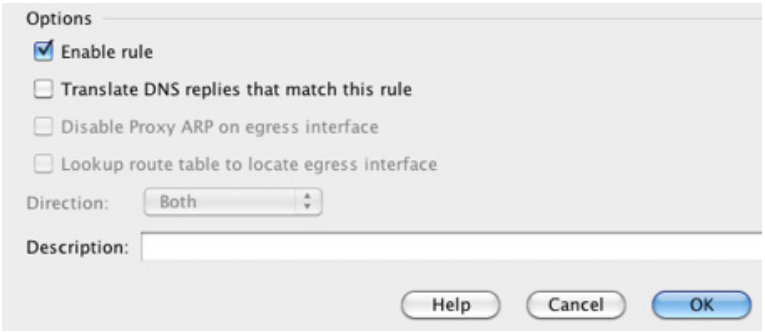
ステップ 7　（オプション）変換されたパケットの送信元ポートまたは宛先ポート（*マッピング送信元ポート*または*実際の宛先ポート*）を識別します。[Match Criteria: Translated Packet] > [Service] の場合、参照ボタンをクリックして既存の TCP または UDP サービス オブジェクトを選択するか、[Browse Translated Service] ダイアログボックスから新しいオブジェクトを作成します。

サービス オブジェクトは、送信元ポートと宛先ポートの両方を含むことができます。両方のサービス オブジェクトに、送信元ポート *または*宛先ポートの*いずれか*を指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバなど）に送信元ポートおよび宛先ポートの*両方*を指定する必要がありますが、固定の送信元ポートはめったに使用されません。オブジェクトで送信元ポートと宛先ポートの両方を指定することはほとんどありませんが、この場合には、元のパケットのサービス オブジェクトに実際の送信元ポート/マッピングされた宛先ポートが含まれます。変換されたパケットのサービス オブジェクトには、マッピングされた送信元ポート/実際の宛先ポートが含まれます。NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。「not equal（等しくない）」（**!=**）演算子はサポートされていません。





ステップ 8　（オプション）[Options] 領域で NAT オプションを設定します。



a. [Enable rule]：この NAT ルールをイネーブルにします。このルールはデフォルトでイネーブルになっています。

b. [Disable Proxy ARP on egress interface]：マッピング IP アドレスへの着信パケットのプロキシ ARP をディセーブルにします。詳細については、「マッピング アドレスとルーティング」（P.5-22）を参照してください。

c. （ルーテッド モード、インターフェイスを指定）[Lookup route table to locate egress interface]：NAT コマンドに指定したインターフェイスを使用する代わりに、ルート ルックアップを使用して出力インターフェイスを決定します。詳細については、「出力インターフェイスの決定」（P.5-25）を参照してください。

d. [Direction]：ルールを単方向にするには、[Unidirectional] を選択します。デフォルトは [Both] です。ルールを単方向にすると、トラフィックが実際のアドレスへの接続を開始するのを回避できます。この設定は、テストのために使用する場合があります。

e. [Description]：ルールに関する説明を 200 文字以内で追加します。

（注）　宛先アドレスを設定しない場合でも [Translate DNS replies that match this rule] チェックボックスを使用できますが、アドレスをそれ自身に変換しているので DNS 応答に修正が必要ないため、このオプションはアイデンティティ NAT には適用されません。詳細については、「DNS および NAT」（P.5-32）を参照してください。

ステップ 9　[OK] をクリックします。

Per-Session PAT ルールの設定

デフォルトでは、すべての TCP PAT トラフィックおよびすべての UDP DNS トラフィックが Per-Session PAT を使用します。トラフィックに Multi-Session PAT を使用するには、Per-Session PAT ルールを設定します。許可ルールで Per-Session PAT を使用し、拒否ルールで Multi-Session PAT を使用します。Per-Session PAT と Multi-Session PAT の詳細については、「Per-Session PAT と Multi-Session PAT（バージョン 9.0(1) 以降）」（P.5-11）を参照してください。

手順の詳細

Per-Session PAT ルールを設定するには、「Per-Session PAT ルールの設定」（P.6-20）を参照してください。

Twice NAT のモニタリング

[Monitoring] > [Properties] > [Connection Graphs] > [Xlates] ペインでは、アクティブなネットワーク アドレス変換をグラフィック形式で表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs]：グラフ化できるコンポーネントを一覧表示します。
  - [Xlate Utilization]：ASA の NAT の使用状況を表示します。
- [Graph Window Title]：グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add]：[Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove]：[Selected Graphs] リストから選択したエントリを削除するには、このフィールドをクリックします。
- [Show Graphs]：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

[Monitoring] > [Properties] > [Connection Graphs] > [Perfmon] ペインでは、パフォーマンス情報をグラフィック形式で表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs]：グラフ化できるコンポーネントを一覧表示します。
  - [AAA Perfmon]：ASA の AAA パフォーマンス情報を表示します。
  - [Inspection Perfmon]：ASA の検査パフォーマンス情報を表示します。
  - [Web Perfmon]：URL アクセスおよび URL サーバ要求などの ASA の Web パフォーマンス情報を表示します。
  - [Connections Perfmon]：ASA の接続パフォーマンス情報を表示します。
  - [Xlate Perfmon]：ASA の NAT パフォーマンス情報を表示します。

- [Graph Window Title]：グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add]：[Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove]：[Selected Graphs] リストから選択した統計タイプを削除するには、このフィールドをクリックします。
- [Show Graphs]：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

Twice NAT の設定例

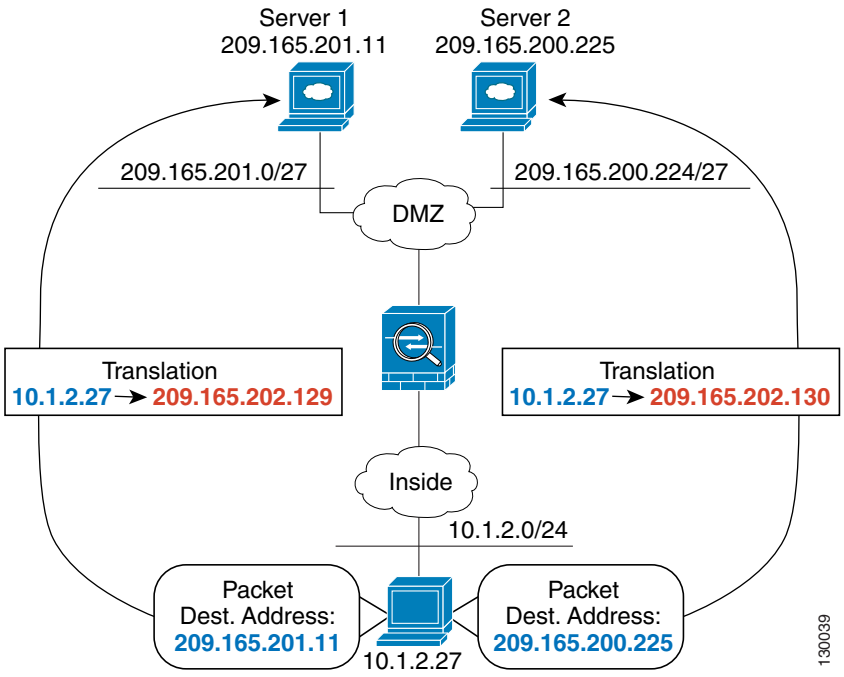
ここでは、次の設定例を示します。

- 「宛先に応じて異なる変換（ダイナミック PAT）」（P.7-32）
- 「宛先アドレスおよびポートに応じて異なる変換（ダイナミック PAT）」（P.7-41）

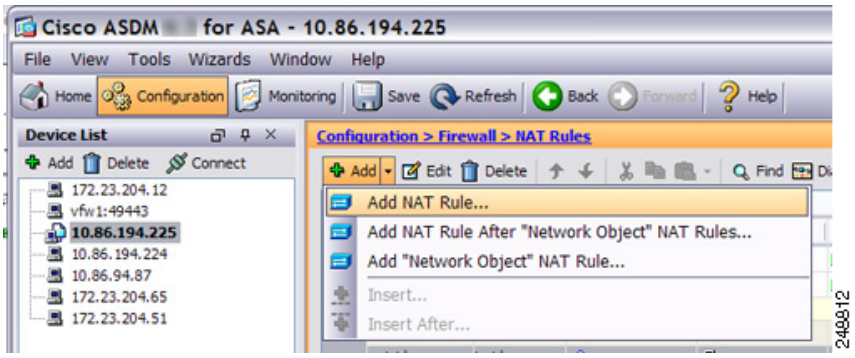
宛先に応じて異なる変換（ダイナミック PAT）

図 7-1 に、2 台の異なるサーバにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129:ポートに変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

図 7-1　異なる宛先アドレスを使用する Twice NAT

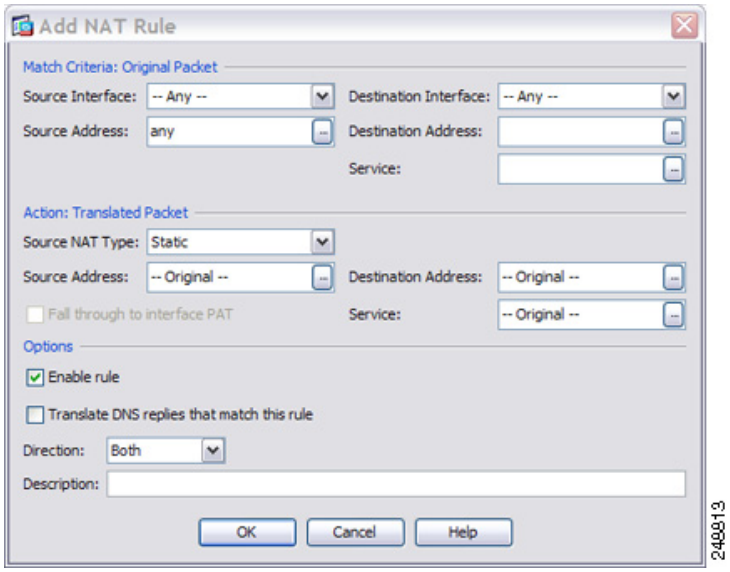


ステップ 1　内部ネットワークから DMZ ネットワーク 1 へのトラフィックの NAT ルールを追加します。

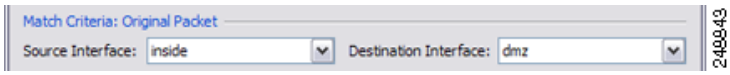


デフォルトでは、セクション 1 の最後に NAT ルールが追加されます。NAT ルールをセクション 3（ネットワーク オブジェクト NAT ルールの後）に追加する場合は、[Add NAT Rule After Network Object NAT Rules] を選択します。

[Add NAT Rule] ダイアログボックスが表示されます。

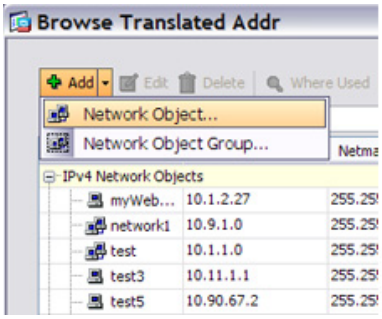


ステップ 2　送信元インターフェイスおよび宛先インターフェイスを設定します。

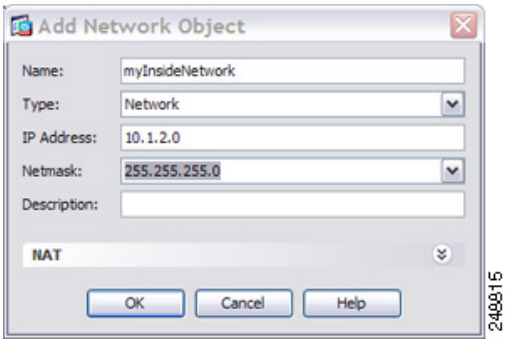


ステップ 3　[Original Source Address] の場合、参照ボタンをクリックして、[Browse Original Source Address] ダイアログボックスで内部ネットワークの新しいネットワーク オブジェクトを追加します。

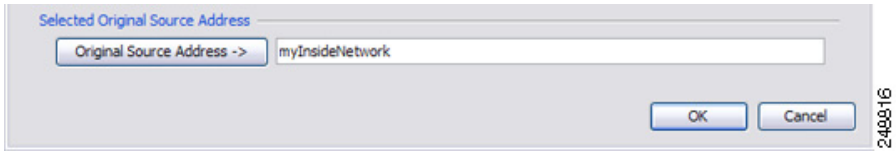
a.　新しいネットワーク オブジェクトを追加します。



b. 内部ネットワーク アドレスを定義し、[OK] をクリックします。

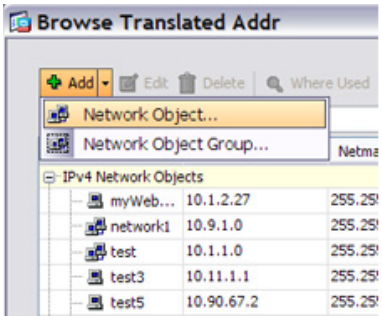


c. 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

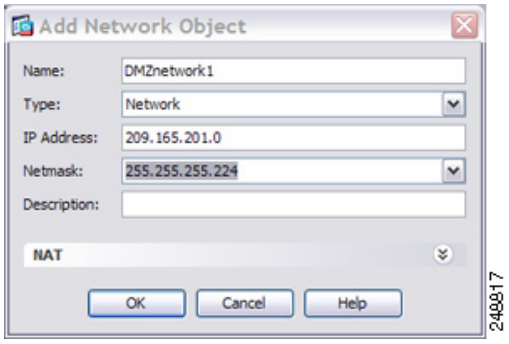


ステップ 4　[Original Destination Address] の場合、参照ボタンをクリックして、[Browse Original Destination Address] ダイアログボックスで DMZ ネットワーク 1 の新しいネットワーク オブジェクトを追加します。

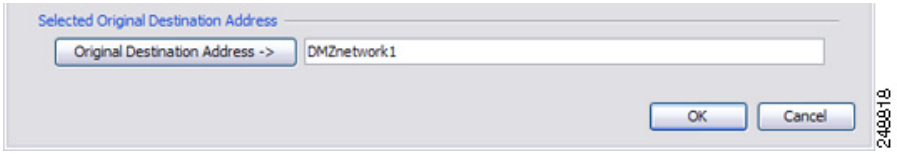
a. 新しいネットワーク オブジェクトを追加します。



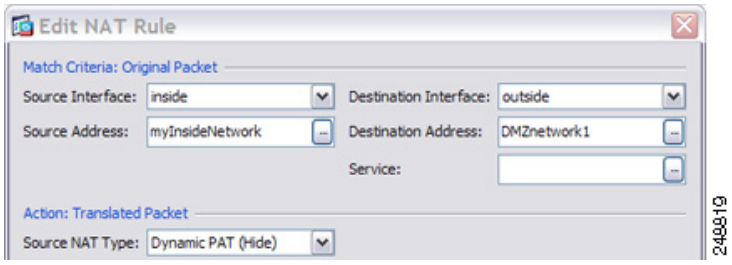
b. DMZ ネットワーク 1 のアドレスを定義し、[OK] をクリックします。



c. 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

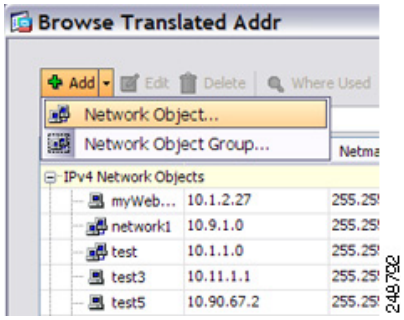


ステップ 5　NAT タイプを [Dynamic PAT (Hide)] に設定します。

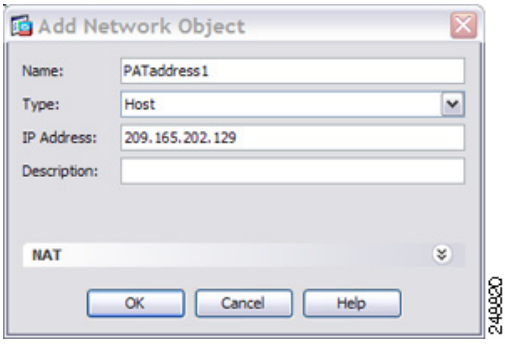


ステップ 6　[Translated Source Address] の場合、参照ボタンをクリックして、[Browse Translated Source Address] ダイアログボックスで PAT アドレスの新しいネットワーク オブジェクトを追加します。

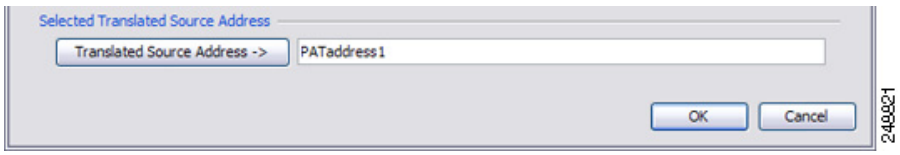
a. 新しいネットワーク オブジェクトを追加します。



b. PAT アドレスを定義し、[OK] をクリックします。

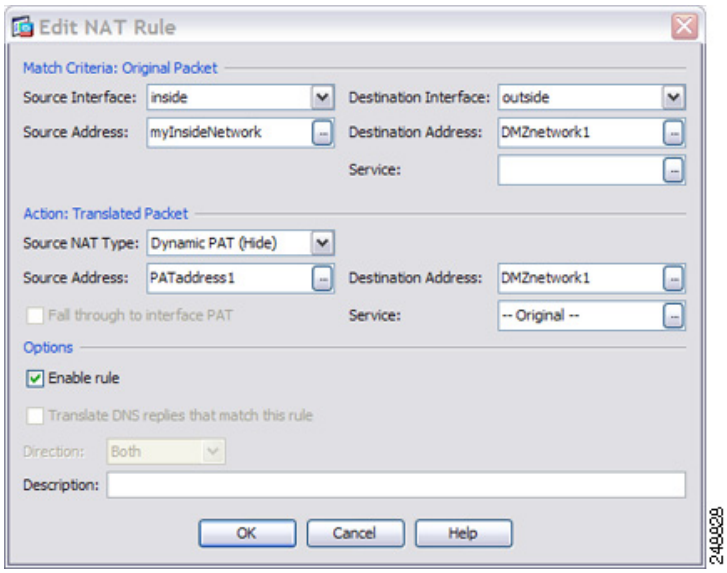


c. 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。



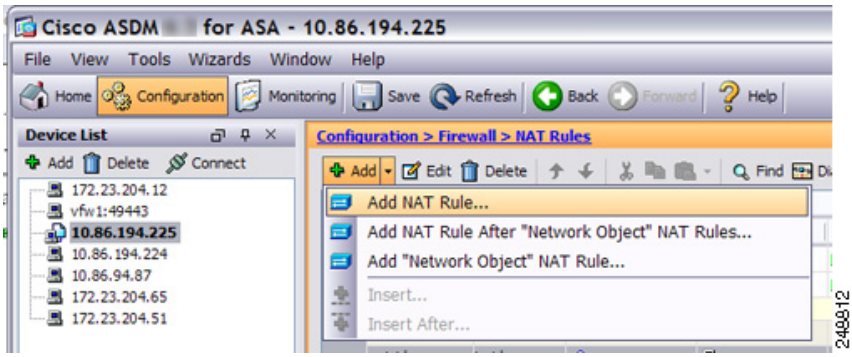
ステップ 7　[Translated Destination Address] の場合、元の宛先アドレスの名前を入力するか（DMZnetwork1）、または参照ボタンをクリックして選択します。

宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。



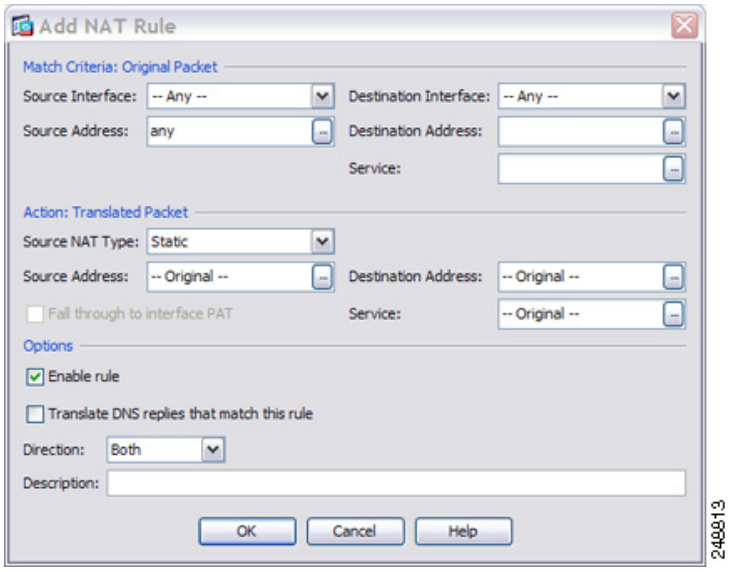
ステップ 8　[OK] をクリックして NAT テーブルにルールを追加します。

ステップ 9　内部ネットワークから DMZ ネットワーク 2 へのトラフィックの NAT ルールを追加します。

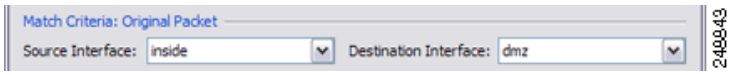


デフォルトでは、セクション 1 の最後に NAT ルールが追加されます。NAT ルールをセクション 3（ネットワーク オブジェクト NAT ルールの後）に追加する場合は、[Add NAT Rule After Network Object NAT Rules] を選択します。

[Add NAT Rule] ダイアログボックスが表示されます。



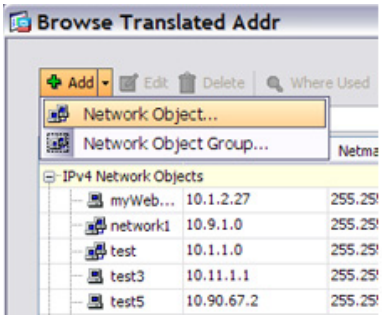
ステップ 10　送信元インターフェイスおよび宛先インターフェイスを設定します。



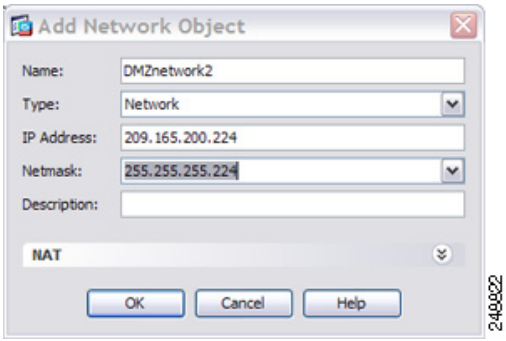
ステップ 11　[Original Source Address] の場合、内部ネットワーク オブジェクトの名前を入力するか（myInsideNetwork）、または参照ボタンをクリックして選択します。

ステップ 12　[Original Destination Address] の場合、参照ボタンをクリックして、[Browse Original Destination Address] ダイアログボックスで DMZ ネットワーク 2 の新しいネットワーク オブジェクトを追加します。

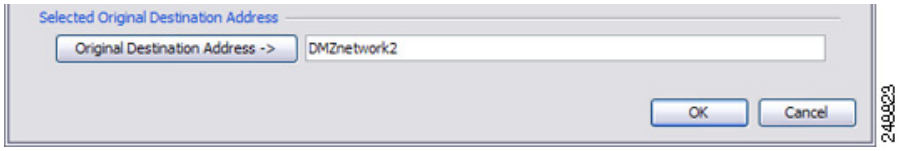
a. 新しいネットワーク オブジェクトを追加します。



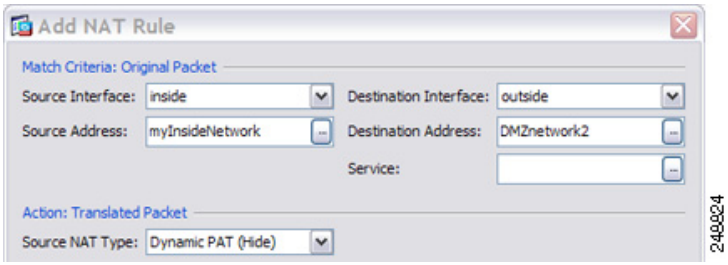
b. DMZ ネットワーク 2 のアドレスを定義し、[OK] をクリックします。



c. 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

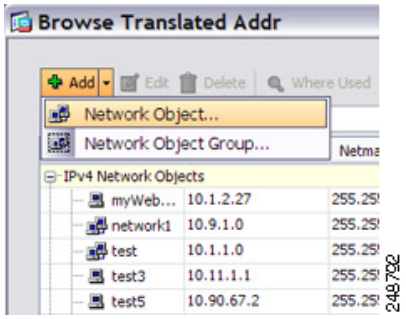


ステップ 13　NAT タイプを [Dynamic PAT (Hide)] に設定します。

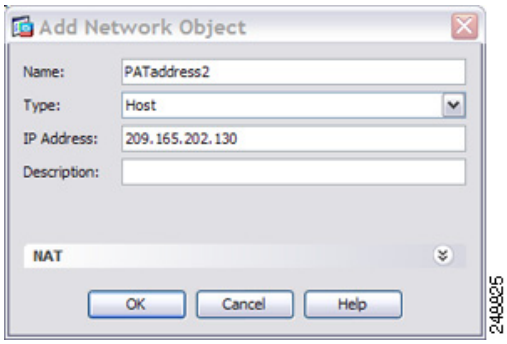


ステップ 14　[Translated Source Address] の場合、参照ボタンをクリックして、[Browse Translated Source Address] ダイアログボックスで PAT アドレスの新しいネットワーク オブジェクトを追加します。

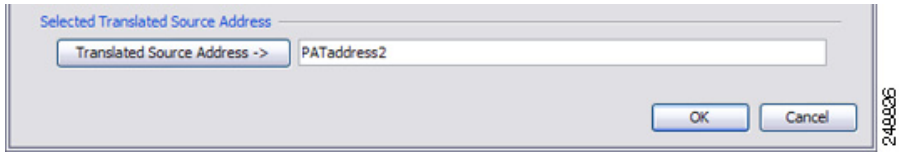
a. 新しいネットワーク オブジェクトを追加します。



b. PAT アドレスを定義し、[OK] をクリックします。

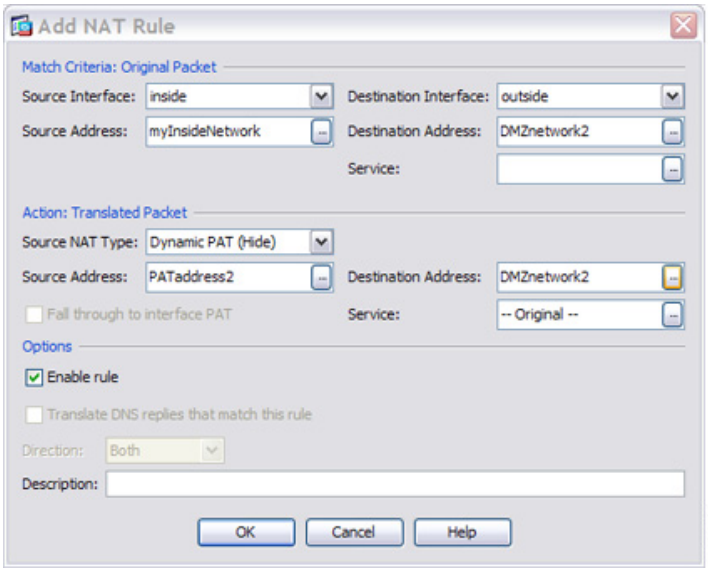


c. 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。



ステップ 15　[Translated Destination Address] の場合、元の宛先アドレスの名前を入力するか（DMZnetwork2）、または参照ボタンをクリックして選択します。

宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。



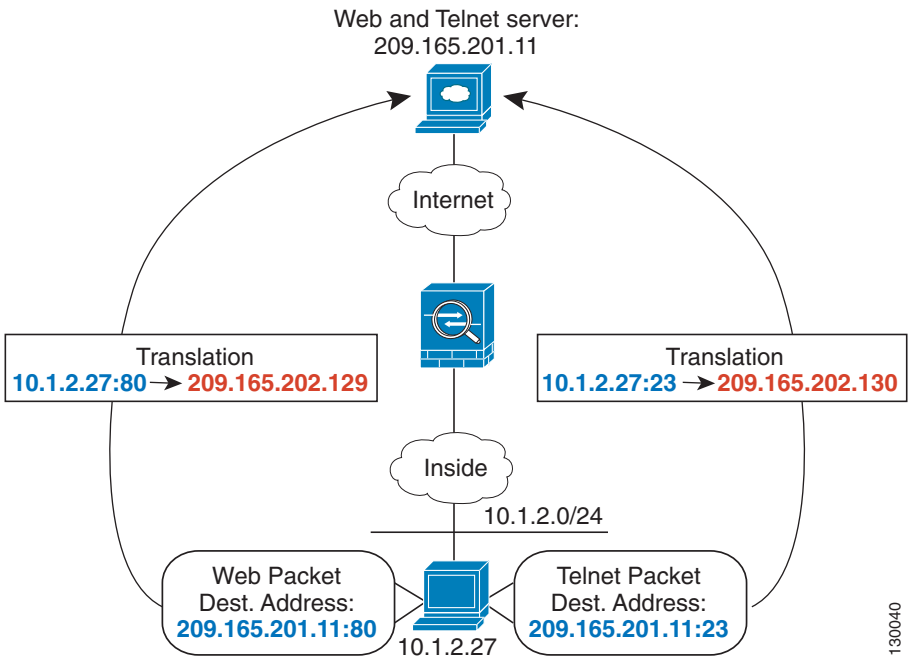
ステップ 16　[OK] をクリックして NAT テーブルにルールを追加します。

ステップ 17　[Apply] をクリックします。

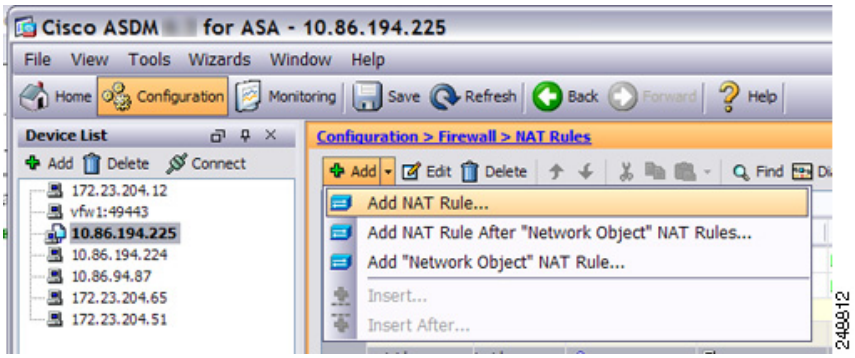
宛先アドレスおよびポートに応じて異なる変換（ダイナミック PAT）

図 7-2 に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Telnet サービスを求めてサーバにアクセスすると、実際のアドレスは 209.165.202.129:*port* に変換されます。ホストが Web サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130:*port* に変換されます。

図 7-2　異なる宛先ポートを使用する Twice NAT

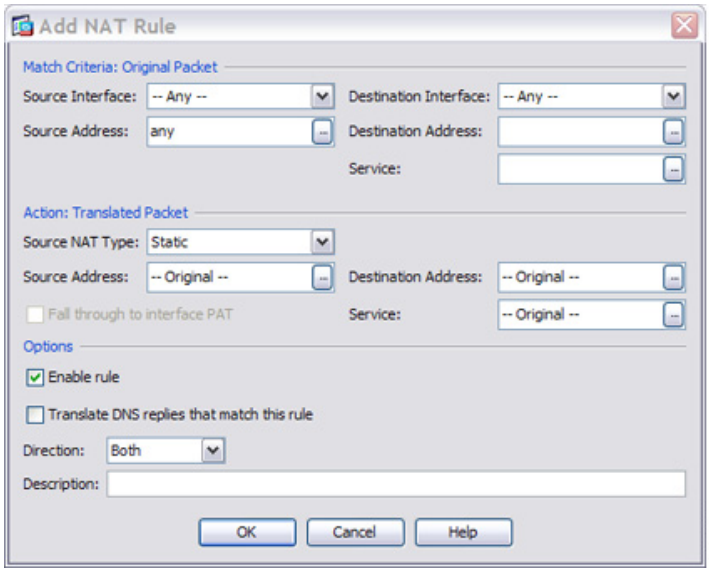


ステップ 1　内部ネットワークから Telnet サーバへのトラフィックの NAT ルールを追加します。

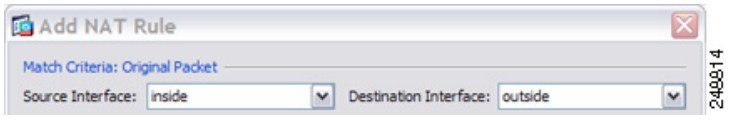


デフォルトでは、セクション 1 の最後に NAT ルールが追加されます。NAT ルールをセクション 3（ネットワーク オブジェクト NAT ルールの後）に追加する場合は、[Add NAT Rule After Network Object NAT Rules] を選択します。

[Add NAT Rule] ダイアログボックスが表示されます。

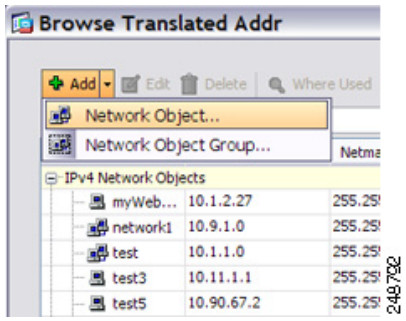


ステップ 2　送信元インターフェイスおよび宛先インターフェイスを設定します。

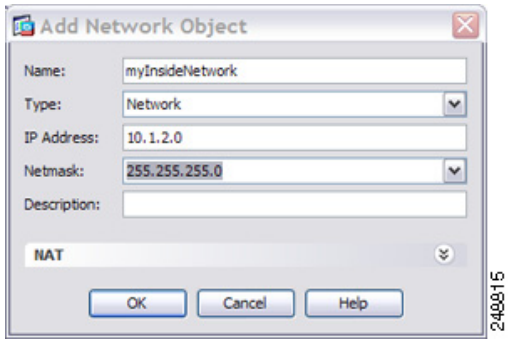


ステップ 3　[Original Source Address] の場合、参照ボタンをクリックして、[Browse Original Source Address] ダイアログボックスで内部ネットワークの新しいネットワーク オブジェクトを追加します。

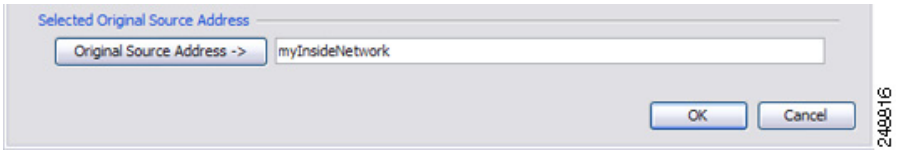
a.　新しいネットワーク オブジェクトを追加します。



b.　内部ネットワーク アドレスを定義し、[OK] をクリックします。

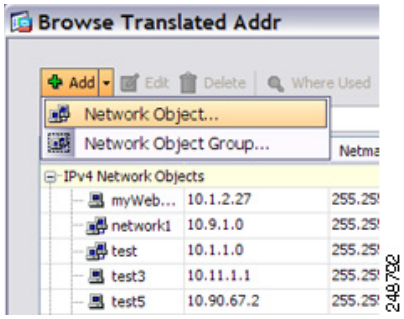


c. 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

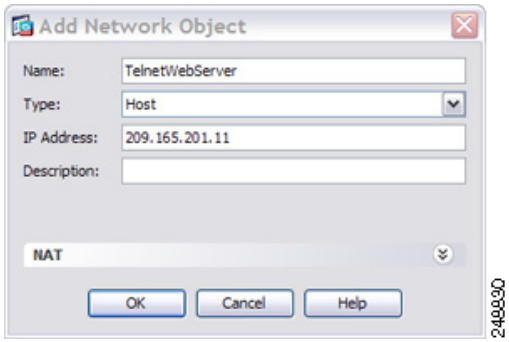


ステップ 4　[Original Destination Address] の場合、参照ボタンをクリックして、[Browse Original Destination Address] ダイアログボックスで Telnet/Web サーバの新しいネットワーク オブジェクトを追加します。

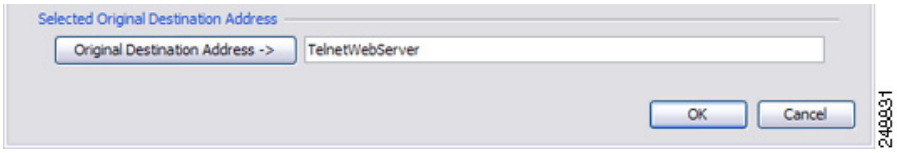
a. 新しいネットワーク オブジェクトを追加します。



b. サーバ アドレスを定義し、[OK] をクリックします。

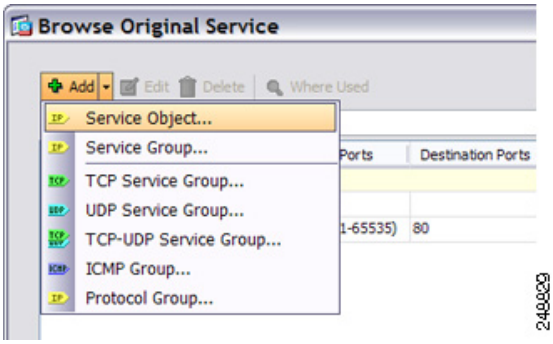


c. 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

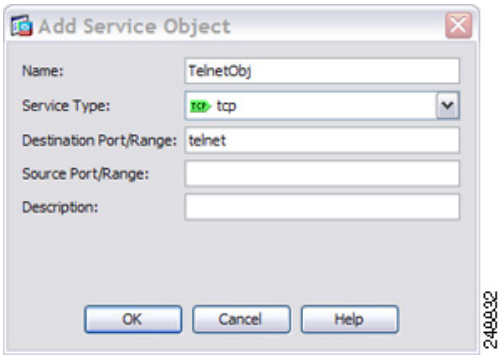


ステップ 5　[Original Service] の場合、参照ボタンをクリックして、[Browse Original Service] ダイアログボックスで Telnet の新しいサービス オブジェクトを追加します。

a. 新しいサービス オブジェクトを追加します。

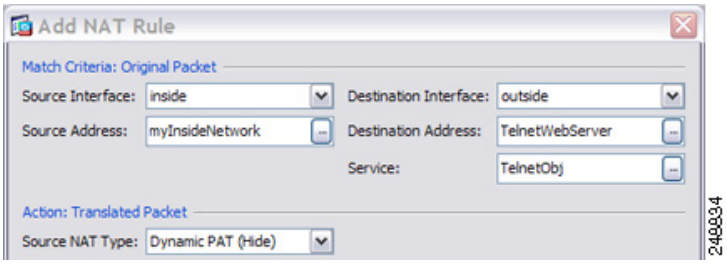


b. プロトコルとポートを定義し、[OK] をクリックします。



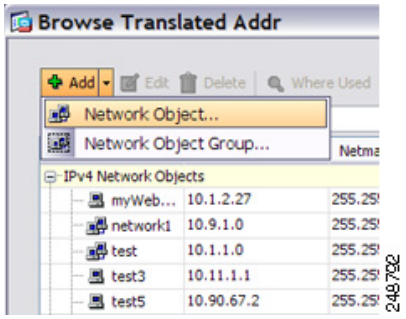
c. 新しいサービス オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

ステップ 6　NAT タイプを [Dynamic PAT (Hide)] に設定します。

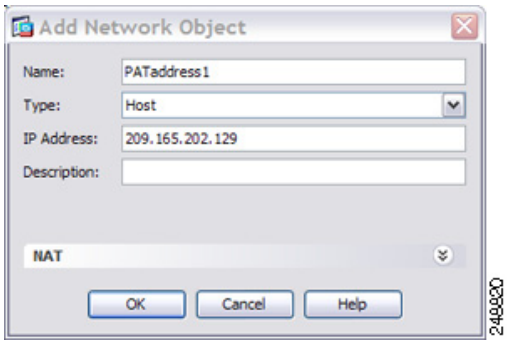


ステップ 7　[Translated Source Address] の場合、参照ボタンをクリックして、[Browse Translated Source Address] ダイアログボックスで PAT アドレスの新しいネットワーク オブジェクトを追加します。

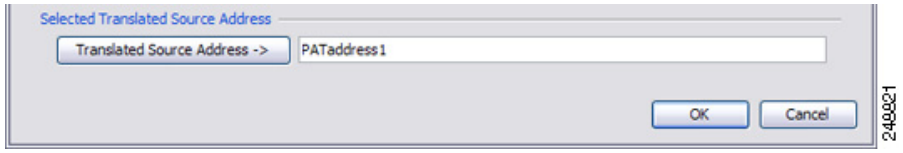
a. 新しいネットワーク オブジェクトを追加します。



b. PAT アドレスを定義し、[OK] をクリックします。

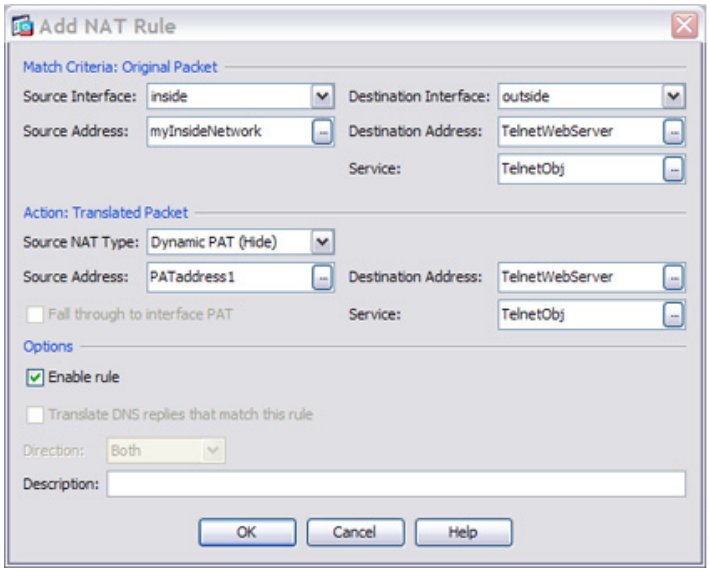


c. 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。



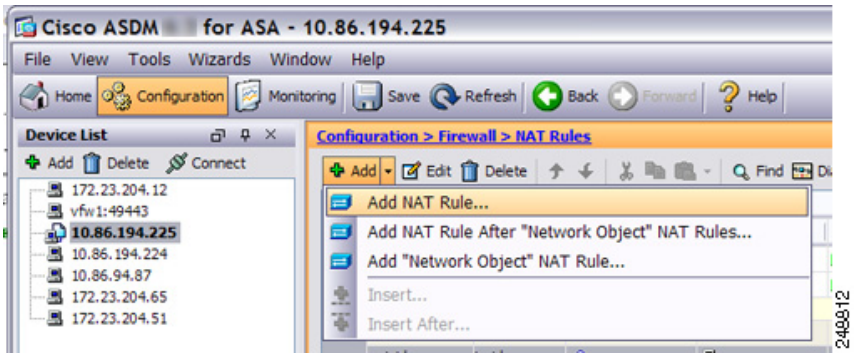
ステップ 8　[Translated Destination Address] の場合、元の宛先アドレスの名前を入力するか（TelnetWebServer）、または参照ボタンをクリックして選択します。

宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。



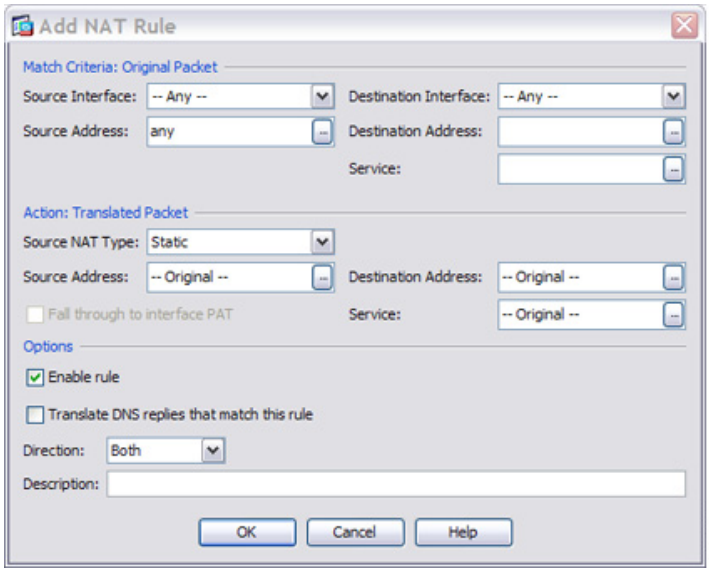
ステップ 9　[OK] をクリックして NAT テーブルにルールを追加します。

ステップ 10　内部ネットワークから Web サーバへのトラフィックの NAT ルールを追加します。

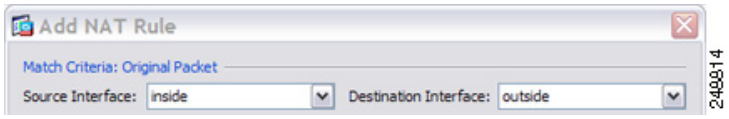


デフォルトでは、セクション 1 の最後に NAT ルールが追加されます。NAT ルールをセクション 3（ネットワーク オブジェクト NAT ルールの後）に追加する場合は、[Add NAT Rule After Network Object NAT Rules] を選択します。

[Add NAT Rule] ダイアログボックスが表示されます。



ステップ 11　実際のインターフェイスおよびマッピング インターフェイスを設定します。

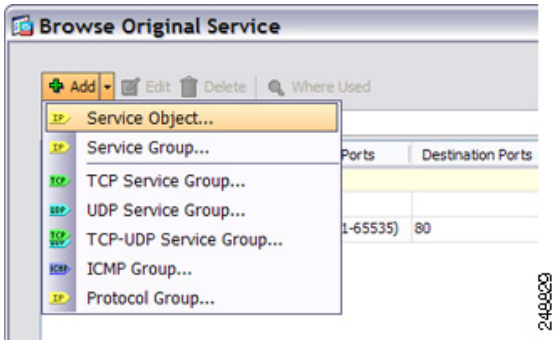


ステップ 12　[Original Source Address] の場合、内部ネットワーク オブジェクトの名前を入力するか（myInsideNetwork）、または参照ボタンをクリックして選択します。

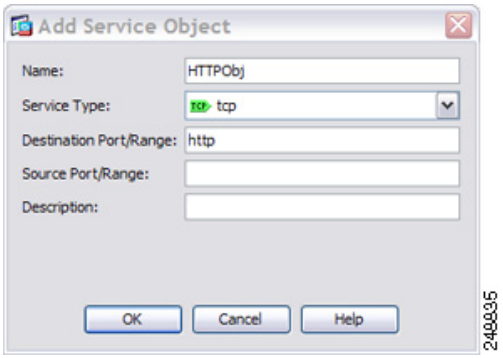
ステップ 13　[Original Destination Address] の場合、Telnet/Web サーバのネットワーク オブジェクトの名前を入力するか（TelnetWebServer）、または参照ボタンをクリックして選択します。

ステップ 14　[Original Service] の場合、参照ボタンをクリックして、[Browse Original Service] ダイアログ ボックスで HTTP の新しいサービス オブジェクトを追加します。

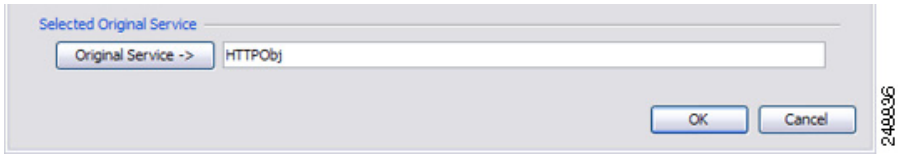
a.　新しいサービス オブジェクトを追加します。



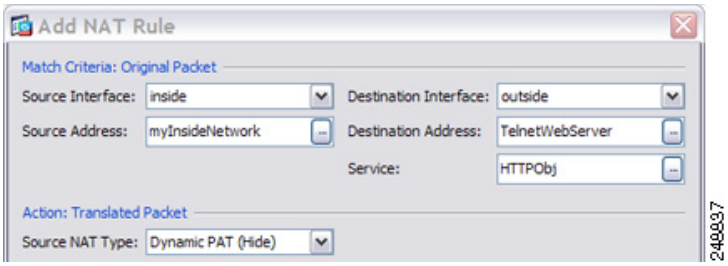
b.　プロトコルとポートを定義し、[OK] をクリックします。



c. 新しいサービス オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

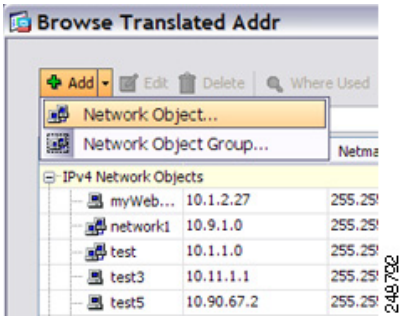


ステップ 15　NAT タイプを [Dynamic PAT (Hide)] に設定します。

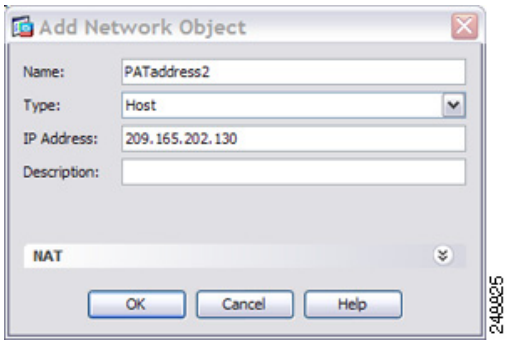


ステップ 16　[Translated Source Address] の場合、参照ボタンをクリックして、[Browse Translated Source Address] ダイアログボックスで PAT アドレスの新しいネットワーク オブジェクトを追加します。

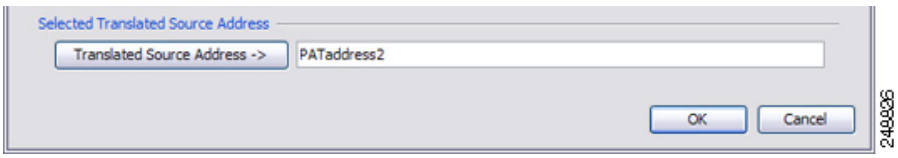
a. 新しいネットワーク オブジェクトを追加します。



b. PAT アドレスを定義し、[OK] をクリックします。

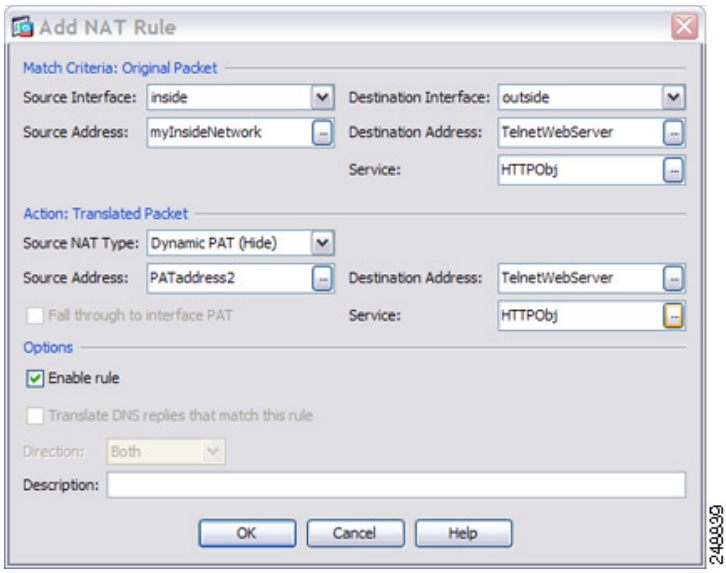


c. 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。



ステップ 17　[Translated Destination Address] の場合、元の宛先アドレスの名前を入力するか（TelnetWebServer）、または参照ボタンをクリックして選択します。

宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。



ステップ 18　[OK] をクリックして NAT テーブルにルールを追加します。

ステップ 19　[Apply] をクリックします。

Twice NAT の機能履歴

表 7-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 7-1　Twice NAT の機能履歴

機能名	プラットフォーム リリース	機能情報
Twice NAT	8.3(1)	Twice NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules]。
アイデンティティ NAT の設定が可能なプロキシ ARP およびルート ルックアップ	8.4(2)/8.5(1)	アイデンティティ NAT の以前のリリースでは、プロキシ ARP はディセーブルにされ、出力インターフェイスの決定には常にルート ルックアップが使用されていました。これらを設定することはできませんでした。8.4(2) 以降、アイデンティティ NAT のデフォルト動作は他のスタティック NAT コンフィギュレーションの動作に一致するように変更されました。これにより、デフォルトでプロキシ ARP はイネーブルにされ、NAT コンフィギュレーションにより出力インターフェイスが決定されるようになりました（指定されている場合）。これらの設定をそのまま残すこともできますし、個別にイネーブルまたはディセーブルにすることもできます。通常のスタティック NAT のプロキシ ARP をディセーブルにすることもできるようになっています。 8.3 よりも前の設定の場合、8.4(2) 以降への NAT 免除ルール（**nat 0 access-list** コマンド）の移行には、プロキシ ARP をディセーブルにするキーワード **no-proxy-arp** およびルート ルックアップを使用するキーワード **route-lookup** があります。8.3(2) および 8.4(1) への移行に使用された **unidirectional** キーワードは、移行に使用されなくなりました。8.3(1)、8.3(2)、8.4(1) から 8.4(2) にアップグレードすると、既存機能を保持するため、すべてのアイデンティティ NAT コンフィギュレーションに **no-proxy-arp** キーワードと **route-lookup** キーワードが含まれるようになっています。**unidirectional** キーワードは削除されました。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit NAT Rule]
PAT プールおよびラウンドロビン アドレス割り当て	8.4(2)/8.5(1)	1 つのアドレスの代わりに、PAT アドレスのプールを指定できるようになりました。また、オプションで、PAT アドレスのすべてのポートを使用してからプール内の次のアドレスを使用するのではなく、PAT アドレスのラウンドロビン割り当てをイネーブルにすることもできます。これらの機能は、1 つの PAT アドレスで多数の接続を行っている場合にそれが DoS 攻撃の対象となることを防止するのに役立ちます。またこの機能により、多数の PAT アドレスを簡単に設定できます。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules] > [Add NAT Rule]/[Edit NAT Rule]。

表 7-1　Twice NAT の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
ラウンドロビン PAT プール割り当てで、既存のホストの同じ IP アドレスを使用する	8.4(3)	ラウンドロビン割り当てで PAT プールを使用するときに、ホストに既存の接続がある場合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT IP アドレスが使用されます。 変更された画面はありません。 *この機能は、8.5(1) または 8.6(1) では使用できません。*
PAT プールの PAT ポートのフラットな範囲	8.4(3)	使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用 *できない* 場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートには、小さい PAT プールのみがあります。 下位ポート範囲を使用するトラフィックが数多くある場合は、PAT プールを使用するときに、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。1024 ～ 65535 または 1 ～ 65535 です。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules] > [Add NAT Rule]/[Edit NAT Rule]。 *この機能は、8.5(1) または 8.6(1) では使用できません。*
PAT プールの拡張 PAT	8.4(3)	各 PAT IP アドレスでは、最大 65535 個のポートを使用できます。65535 個のポートで変換が不十分な場合は、PAT プールに対して拡張 PAT をイネーブルにすることができます。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、*サービス*ごとに 65535 個のポートが使用されます。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules] > [Add NAT Rule]/[Edit NAT Rule]。 *この機能は、8.5(1) または 8.6(1) では使用できません。*

表 7-1　Twice NAT の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
VPN ピアのローカル IP アドレスを変換してピアの実際の IP アドレスに戻す自動 NAT ルール	8.4(3)	まれに、内部ネットワークで、割り当てられたローカル IP アドレスではなく、VPN ピアの実際の IP アドレスを使用する場合があります。VPN では通常、内部ネットワークにアクセスするために、割り当てられたローカル IP アドレスがピアに指定されます。ただし、内部サーバおよびネットワーク セキュリティがピアの実際の IP アドレスに基づく場合などに、ローカル IP アドレスを変換してピアの実際のパブリック IP アドレスに戻す場合があります。 この機能は、トンネル グループごとに 1 つのインターフェイスでイネーブルにすることができます。VPN セッションが確立または切断されると、オブジェクト NAT ルールが動的に追加および削除されます。ルールは **show nat** コマンドを使用して表示できます。 **（注）** ルーティングの問題のため、この機能が必要でない場合は、この機能の使用は推奨しません。ご使用のネットワークとの機能の互換性を確認するには、Cisco TAC にお問い合わせください。次の制限事項を確認してください。 • Cisco IPsec および AnyConnect クライアントのみがサポートされます。 • NAT ポリシーおよび VPN ポリシーが適用されるように、パブリック IP アドレスへのリターン トラフィックは ASA にルーティングされる必要があります。 • ロードバランシングはサポートされません（ルーティングの問題のため）。 • ローミング（パブリック IP 変更）はサポートされません。 ASDM ではこのコマンドはサポートされません。コマンドライン ツールを使用してコマンドを入力してください。
IPv6 用の NAT のサポート	9.0(1)	NAT が IPv6 トラフィックをサポートするようになり、IPv4 と IPv6 の間の変換もサポートされます。IPv4 と IPv6 の間の変換は、トランスペアレント モードではサポートされません。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules]。
逆引き DNS ルックアップ用の NAT のサポート	9.0(1)	NAT ルールがイネーブルにされた DNS インスペクションを使用する IPv4 NAT、IPv6 NAT、および NAT64 を使用する場合、NAT は逆引き DNS ルックアップ用の DNS PTR レコードの変換をサポートするようになりました。

表 7-1　Twice NAT の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
Per-Session PAT	9.0(1)	Per-session PAT 機能によって PAT のスケーラビリティが向上し、クラスタリングの場合に各メンバ ユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、マスター ユニットに転送してマスター ユニットを所有者とする必要があります。Per-Session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンド ノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。「ヒットエンドラン」トラフィック、たとえば HTTP や HTTPS の場合は、Per-Session 機能によって、1 アドレスでサポートされる接続率が大幅に増加することがあります。Per-session 機能を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。Per-session 機能を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/平均ライフタイムです。 デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-session PAT xlate を使用します。Multi-Session PAT を必要とするトラフィック、たとえば H.323、SIP、Skinny に対して Per-session PAT をディセーブルにするには、Per-session 拒否ルールを作成します。 次の画面が導入されました。[Configuration] > [Firewall] > [Advanced] > [Per-Session NAT Rules]。
NAT ルール エンジンのトランザクション コミット モデル	9.3(1)	イネーブルの場合、NAT ルールの更新はルール コンパイルの完了後に適用され、ルール照合のパフォーマンスに影響を及ぼすことはありません。 [Configuration] > [Device Management] > [Advanced] > [Rule Engine] 画面に NAT が追加されました。

PART 3

アプリケーション インスペクション

アプリケーション レイヤ プロトコル インスペクションの準備

次のトピックで、アプリケーション レイヤ プロトコル インスペクションを設定する方法について説明します。

- 「アプリケーション レイヤ プロトコル インスペクション」（P.8-1）
- 「アプリケーション インスペクションのガイドライン」（P.8-5）
- 「アプリケーション インスペクションのデフォルト」（P.8-6）
- 「アプリケーション レイヤ プロトコル インスペクションの設定」（P.8-10）
- 「正規表現の設定」（P.8-13）
- 「アプリケーション インスペクションの履歴」（P.8-17）

アプリケーション レイヤ プロトコル インスペクション

インスペクション エンジンは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルでは、高速パスでパケットを渡すのではなく、ASA で詳細なパケット インスペクションを行う必要があります（高速パスの詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください）。そのため、インスペクション エンジンがスループット全体に影響を与えることがあります。ASA では、デフォルトでいくつかの一般的なインスペクション エンジンがイネーブルになっていますが、ネットワークによっては他のインスペクション エンジンをイネーブルにしなければならない場合があります。

次のトピックで、アプリケーション インスペクションについて詳しく説明します。

- 「インスペクション エンジンの動作」（P.8-1）
- 「アプリケーション プロトコル インスペクションを使用するタイミング」（P.8-3）
- 「インスペクション ポリシー マップ」（P.8-3）

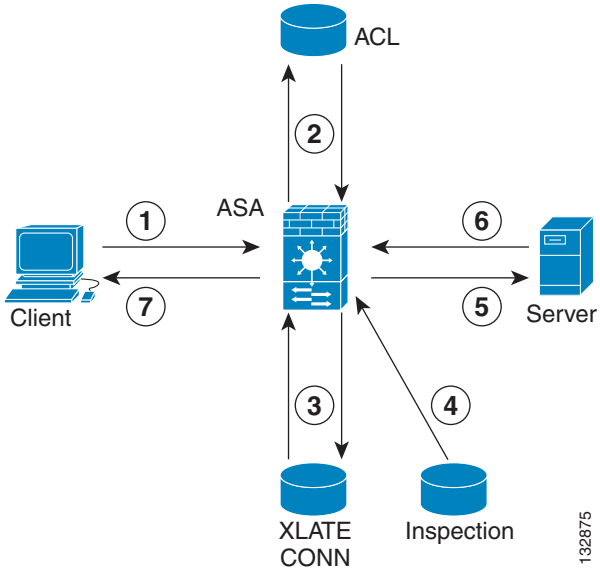
インスペクション エンジンの動作

次の図に示すように、ASA は基本動作を行うために 3 つのデータベースを使用します。

- ACL：特定のネットワーク、ホスト、およびサービス（TCP/UDP ポート番号）に基づく接続の認証と許可のために使用されます。

- インスペクション：事前定義済みの一連のスタティックなアプリケーションレベルのインスペクション機能を含みます。
- 接続（XLATE および CONN テーブル）：確立済みの各接続についての状態および他の情報を保持します。この情報は、確立済みのセッション内でトラフィックを効率的に転送するため、適応型セキュリティ アルゴリズムおよびカットスルー プロキシによって使用されます。

図 8-1　　インスペクション エンジンの動作



この図では、動作順に番号が付けられています。

1. TCP SYN パケットが ASA に到着して、新しい接続を確立します。
2. ASA は ACL データベースをチェックして、接続が許可されるかどうかを判定します。
3. ASA は接続データベース（XLATE および CONN テーブル）に新しいエントリを作成します。
4. ASA はインスペクション データベースをチェックして、接続にアプリケーションレベルのインスペクションが必要かどうかを判定します。
5. アプリケーション インスペクション エンジンがパケットに必要な処理を完了した後、ASA はパケットを宛先システムに転送します。
6. 宛先システムは初期要求に応答します。
7. ASA は応答パケットを受信し、接続データベースで接続を検索して、確立済みのセッションに属しているのでパケットを転送します。

ASA のデフォルト コンフィギュレーションには、サポートされるプロトコルを特定の TCP または UDP ポート番号と関連付けて、必要とされる特殊な処理を識別する、一連のアプリケーション インスペクション エントリが含まれます。

アプリケーション プロトコル インスペクションを使用するタイミング

ユーザが接続を確立すると、ASA は ACL と照合してパケットをチェックし、アドレス変換を作成し、高速パスでのセッション用にエントリを作成して、後続のパケットが時間のかかるチェックをバイパスできるようにします。ただし、高速パスは予測可能なポート番号に基づいており、パケット内部のアドレス変換を実行しません。

多くのプロトコルは、セカンダリの TCP ポートまたは UDP ポートを開きます。既知のポートで初期セッションが使用され、動的に割り当てられたポート番号がネゴシエートされます。

パケットに IP アドレスを埋め込むアプリケーションもあります。この IP アドレスは送信元アドレスと一致する必要があり、通常、ASA を通過するときに変換されます。

これらのアプリケーションを使用する場合は、アプリケーション インスペクションをイネーブルにする必要があります。

IP アドレスを埋め込むサービスに対してアプリケーション インスペクションをイネーブルにすると、ASA は埋め込まれたアドレスを変換し、チェックサムや変換の影響を受けたその他のフィールドを更新します。

ダイナミックに割り当てられたポートを使用するサービスに対してアプリケーション インスペクションをイネーブルにすると、ASA はセッションをモニタしてダイナミックに割り当てられたポートを特定し、所定のセッションの間、それらのポートでのデータ交換を許可します。

インスペクション ポリシー マップ

*インスペクション ポリシー マップ*を使用して、多くのアプリケーション インスペクションで実行される特別なアクションを設定できます。これらのマップはオプションです。インスペクション ポリシー マップをサポートするプロトコルに関しては、マップを設定しなくてもインスペクションをイネーブルにできます。デフォルトのインスペクション アクション以外のことが必要な場合にのみ、これらのマップが必要になります。

インスペクション ポリシー マップをサポートするアプリケーションのリストについては、「アプリケーション レイヤ プロトコル インスペクションの設定」（P.8-10）を参照してください。

インスペクション ポリシー マップは、次に示す要素の 1 つ以上で構成されています。インスペクション ポリシー マップで使用可能な実際のオプションは、アプリケーションに応じて決まります。

- トラフィック一致基準：アプリケーション トラフィックをそのアプリケーションに固有の基準（URL 文字列など）と照合し、その後アクションをイネーブルにできます。

  一部のトラフィック一致基準では、正規表現を使用してパケット内部のテキストを照合します。ポリシー マップを設定する前に、正規表現クラス マップ内で、正規表現を単独またはグループで作成およびテストしておいてください。

- インスペクション クラス マップ：一部のインスペクション ポリシー マップでは、インスペクション クラス マップを使用して複数のトラフィック一致基準を含めることができます。その後、インスペクション ポリシー マップ内でインスペクション クラス マップを指定し、そのクラス全体でアクションをイネーブルにします。クラス マップを作成することと、インスペクション ポリシー マップ内で直接トラフィック照合を定義することの違いは、より複雑な一致基準を作成できる点と、クラス マップを再使用できる点です。ただし、異なる一致基準に対して異なるアクションを設定することはできません。

- パラメータ：パラメータは、インスペクション エンジンの動作に影響します。

次のトピックで、詳細に説明します。

- 「使用中のインスペクション ポリシー マップの交換」（P.8-4）
- 「複数のトラフィック クラスの処理方法」（P.8-4）

使用中のインスペクション ポリシー マップの交換

サービス ポリシーですでに使用しているインスペクション ポリシー マップを交換する必要がある場合、次の方法を使用してください。

- すべてのインスペクション ポリシー マップ：使用中のインスペクション ポリシー マップを別のマップ名と交換する場合は、そのマップを削除して変更を適用し、新しいインスペクション ポリシー マップをサービス ポリシーに追加する必要があります。
- HTTP インスペクション ポリシー マップ：使用中の HTTP インスペクション ポリシー マップを変更する場合、変更を有効にするにはインスペクション ポリシー マップ アクションを削除し、再適用する必要があります。たとえば、「http-map」インスペクション ポリシー マップを変更する場合、そのインスペクション ポリシー マップを削除して変更を適用し、サービス ポリシーに再度追加する必要があります。

複数のトラフィック クラスの処理方法

インスペクション ポリシー マップには、複数のインスペクション クラス マップや直接照合を指定できます。

1 つのパケットが複数の異なる照合と一致する場合、ASA がアクションを適用する順序は、インスペクション ポリシー マップにアクションが追加された順序ではなく、ASA の内部ルールによって決まります。内部ルールは、アプリケーションのタイプとパケット解析の論理的進捗によって決まり、ユーザが設定することはできません。HTTP トラフィックの場合、Request Method フィールドの解析が Header Host Length フィールドの解析よりも先に行われ、Request Method フィールドに対するアクションは Header Host Length フィールドに対するアクションより先に行われます。

アクションがパケットをドロップすると、インスペクション ポリシー マップではそれ以降のアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合、それ以降の一致基準との照合は行われません。最初のアクションがパケットのログへの記録である場合、接続のリセットなどの 2 番目のアクションは実行されます。

パケットが、同じ複数の一致基準と照合される場合は、ポリシー マップ内のそれらのコマンドの順序に従って照合されます。

クラス マップは、そのクラス マップ内で重要度が最低の照合オプション（重要度は、内部ルールに基づきます）に基づいて、別のクラス マップまたは直接照合のと同じタイプであると判断されます。クラス マップに、別のクラス マップと同じタイプの重要度が最低の照合オプションがある場合、それらのクラス マップはポリシー マップに追加された順序で照合されます。クラス マップごとに最低重要度の照合が異なる場合は、最高重要度の照合オプションを持つクラス マップが最初に照合されます。

アプリケーション インスペクションのガイドライン

フェールオーバーのガイドライン

インスペクションが必要なマルチメディア セッションのステート情報は、ステートフル フェールオーバーのステート リンク経由では渡されません。ステート リンク経由で複製される GTP および SIP は例外です。

IPv6 のガイドライン

IPv6 は次のインスペクションでサポートされています。

- DNS
- FTP
- HTTP
- ICMP
- SCCP（Skinny）
- SIP
- SMTP
- IPSec パススルー
- IPv6

NAT64 は次のインスペクションでサポートされています。

- DNS
- FTP
- HTTP
- ICMP

その他のガイドラインと制限事項

- 一部のインスペクション エンジンは、PAT、NAT、外部 NAT、または同一セキュリティ インターフェイス間の NAT をサポートしません。NAT サポートの詳細については、「デフォルト インスペクションと NAT に関する制限事項」（P.8-6）を参照してください。
- すべてのアプリケーション インスペクションについて、ASA はアクティブな同時データ接続の数を 200 接続に制限します。たとえば、FTP クライアントが複数のセカンダリ接続を開く場合、FTP インスペクション エンジンはアクティブな接続を 200 だけ許可して 201 番目の接続からはドロップし、適応型セキュリティ アプライアンスはシステム エラー メッセージを生成します。
- 検査対象のプロトコルは高度な TCP ステート トラッキングの対象となり、これらの接続の TCP ステートは自動的には複製されません。スタンバイ装置への接続は複製されますが、TCP ステートを再確立するベスト エフォート型の試行が行われます。
- ASA（インターフェイス）に送信される TCP/UDP トラフィックはデフォルトで検査されます。ただし、インターフェイスに送信される ICMP トラフィックは、ICMP インスペクションをイネーブルにした場合でも検査されません。したがって、ASA がバックアップ デフォルト ルートを介して到達できる送信元からエコー要求が送信された場合など、特定の状況下では、インターフェイスへの ping（エコー要求）が失敗する可能性があります。

アプリケーション インスペクションのデフォルト

次のトピックで、アプリケーション インスペクションのデフォルトの動作について説明します。

- 「デフォルト インスペクションと NAT に関する制限事項」（P.8-6）
- 「デフォルトのインスペクション ポリシー マップ」（P.8-10）

デフォルト インスペクションと NAT に関する制限事項

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーがコンフィギュレーションに含まれ、すべてのインスペクションがすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。デフォルト アプリケーション インスペクション トラフィックには、各プロトコルのデフォルト ポートへのトラフィックが含まれます。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する（標準以外のポートにインスペクションを適用する場合や、デフォルトでイネーブルになっていないインスペクションを追加する場合など）には、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用する必要があります。

次の表に、サポートされているすべてのインスペクション、デフォルトのクラス マップで使用されるデフォルト ポート、およびデフォルトでオンになっているインスペクション エンジン（太字）を示します。この表には、NAT に関する制限事項も含まれています。この表の見方は次のとおりです。

- デフォルト ポートに対してデフォルトでイネーブルになっているインスペクション エンジンは太字で表記されています。
- ASA は、これらの指定された標準に準拠していますが、検査対象のパケットには準拠を強制しません。たとえば、各 FTP コマンドは特定の順序である必要がありますが、ASA によってその順序を強制されることはありません。

表 8-1　サポートされているアプリケーション インスペクション エンジン

アプリケーション	デフォルト ポート	NAT に関する制限事項	Standards	注
CTIQBE	TCP/2748	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	—	—
DCERPC	TCP/135	NAT64 なし。	—	—
DNS over UDP	UDP/53	NAT サポートは、WINS 経由の名前解決では使用できません。	RFC 1123	—
FTP	TCP/21	（クラスタリング）スタティック PAT はサポートされません。	RFC 959	—
GTP	UDP/3386 UDP/2123	拡張 PAT はサポートされません。 NAT なし。	—	特別なライセンスが必要です。

表 8-1　サポートされているアプリケーション インスペクション エンジン （続き）

アプリケーション	デフォルト ポート	NAT に関する制限事項	Standards	注
H.323 H.225 および **RAS**	TCP/1720 UDP/1718 UDP (RAS) 1718-1719	ダイナミック NAT または PAT はサポートされません。 スタティック PAT は機能しない可能性があります。 （クラスタリング）スタティック PAT はサポートされません。 拡張 PAT はサポートされません。 Per-Session PAT はサポートされません。 同一セキュリティのインターフェイス上の NAT はサポートされません。 NAT64 なし。	ITU-T H.323、H.245、H225.0、Q.931、Q.932	—
HTTP	TCP/80	—	RFC 2616	ActiveX と Java を除去する場合の MTU 制限に注意してください。MTU が小さすぎて Java タグまたは ActiveX タグを 1 つのパケットに納められない場合は、除去の処理は行われません。
ICMP	—	—	—	ASA インターフェイスに送信される ICMP トラフィックは検査されません。
ICMP ERROR	—	—	—	—
ILS（LDAP）	TCP/389	拡張 PAT はサポートされません。 NAT64 なし。	—	—
インスタント メッセージング（IM）	クライアントにより異なる	拡張 PAT はサポートされません。 NAT64 なし。	RFC 3860	—
IP オプション	—	NAT64 なし。	RFC 791、RFC 2113	—
IPsec パススルー	UDP/500	PAT はサポートされません。 NAT64 なし。	—	—
IPv6	—	NAT64 なし。	RFC 2460	—
MGCP	UDP/2427、2727	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	RFC 2705bis-05	—
MMP	TCP 5443	拡張 PAT はサポートされません。 NAT64 なし。	—	—

表 8-1　サポートされているアプリケーション インスペクション エンジン （続き）

アプリケーション	デフォルト ポート	NAT に関する制限事項	Standards	注
NetBIOS Name Server over IP	UDP/137、138（送信元ポート）	拡張 PAT はサポートされません。 NAT64 なし。	—	NetBIOS は、NBNS UDP ポート 137 および NBDS UDP ポート 138 に対してパケットの NAT 処理を実行することでサポートされます。
PPTP	TCP/1723	NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	RFC 2637	—
RADIUS アカウンティング	1646	NAT64 なし。	RFC 2865	—
RSH	TCP/514	PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	Berkeley UNIX	—
RTSP	TCP/554	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	RFC 2326、2327、1889	HTTP クローキングは処理しません。
ScanSafe（クラウド Web セキュリティ）	TCP/80 TCP/413	—	—	これらのポートは、ScanSafe インスペクションの default-inspection-traffic クラスには含まれません。
SIP	TCP/5060 UDP/5060	同一セキュリティのインターフェイス上の NAT はサポートされません。 拡張 PAT はサポートされません。 Per-Session PAT はサポートされません。 NAT64 または NAT46 はなし。 （クラスタリング）スタティック PAT はサポートされません。	RFC 2543	一定の条件下で、Cisco IP Phone 設定をアップロード済みの TFTP は処理しません。

表 8-1　サポートされているアプリケーション インスペクション エンジン （続き）

アプリケーション	デフォルト ポート	NAT に関する制限事項	Standards	注
SKINNY（SCCP）	TCP/2000	同一セキュリティのインターフェイス上の NAT はサポートされません。 拡張 PAT はサポートされません。 Per-Session PAT はサポートされません。 NAT64、NAT46、または NAT66 はなし。 （クラスタリング）スタティック PAT はサポートされません。	—	一定の条件下で、Cisco IP Phone 設定をアップロード済みの TFTP は処理しません。
SMTP および **ESMTP**	TCP/25	NAT64 なし。	RFC 821、1123	—
SNMP	UDP/161、162	NAT および PAT はサポートされません。	RFC 1155、1157、1212、1213、1215	v.2 RFC 1902 ～ 1908、v.3 RFC 2570 ～ 2580
SQL*Net	TCP/1521	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	—	v.1 および v.2
Sun RPC over UDP および TCP	UDP/111	拡張 PAT はサポートされません。 NAT64 なし。	—	デフォルトのルールには UDP ポート 111 が含まれています。TCP ポート 111 の Sun RPC インスペクションをイネーブルにする場合は、TCP ポート 111 を照合する新しいルールを作成し、Sun RPC インスペクションを実行する必要があります。
TFTP	UDP/69	NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	RFC 1350	ペイロード IP アドレスは変換されません。
WAAS	TCP/1- 65535	拡張 PAT はサポートされません。 NAT64 なし。	—	—
XDMCP	UDP/177	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	—	—

デフォルトのインスペクション ポリシー マップ

一部のインスペクション タイプは、非表示のデフォルト ポリシー マップを使用します。たとえば、マップを指定しないで ESMTP インスペクションをイネーブルにした場合、_default_esmtp_map が使用されます。

デフォルトのインスペクションは、各インスペクション タイプについて説明しているセクションで説明されています。これらのデフォルト マップは、[show running-config all policy-map] コマンドを使用して表示できます。[Tools] > [Command Line Interface] を使用します。

DNS インスペクションは、明示的に設定されたデフォルト マップ preset_dns_map を使用する唯一のインスペクションです。

アプリケーション レイヤ プロトコル インスペクションの設定

サービス ポリシーにアプリケーション インスペクションを設定します。サービス ポリシーでは、一貫性と柔軟性を備えた方法で ASA 機能を設定できます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。アプリケーションによっては、インスペクションをイネーブルにすると特別なアクションを実行できるものがあります。サービス ポリシーに関する一般的な情報については、第 1 章「サービス ポリシー」を参照してください。

一部のアプリケーションでは、デフォルトでインスペクションがイネーブルになっています。詳細については、「デフォルト インスペクションと NAT に関する制限事項」（P.8-6）を参照してください。この項を参照してインスペクション ポリシーを変更してください。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] の順に選択します。

ステップ 2　「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従ってサービス ポリシー ルールを追加または編集し、[Rule Action] ページに進みます。

標準以外のポートを照合する場合は、非標準ポート用の新しいルールを作成します。各インスペクション エンジンの標準ポートについては、「デフォルト インスペクションと NAT に関する制限事項」（P.8-6）を参照してください。

必要に応じて同じサービス ポリシー内に複数のルールを組み合わせることができるため、照合するトラフィックに応じたルールを作成できます。ただし、トラフィックがインスペクション アクションを含むルールと一致し、その後同様にインスペクション アクションを含む別のルールとも一致した場合、最初に一致したルールだけが使用されます。

RADIUS アカウンティング インスペクションを実装している場合、「管理トラフィックのサービス ポリシー ルールの追加」（P.1-14）に従って管理サービス ポリシー ルールを作成します。

ステップ 3　ルールのアクションで、[Protocol Inspection] タブをクリックします。

ステップ 4　（使用中のポリシーを変更）異なるインスペクション ポリシー マップを使用するために使用中のポリシーを編集する場合は、インスペクションをディセーブルにし、新しいインスペクション ポリシー マップ名で再度イネーブルにします。

a. プロトコルのチェックボックスをオフにします。

b. [OK] をクリックします。

c. [Apply] をクリックします。

d. この手順を繰り返して [Protocol Inspections] タブに戻ります。

ステップ 5　適用したいインスペクション タイプを選択します。

デフォルトのインスペクション トラフィック クラスに対してのみ、複数のオプションを選択できます。

一部のインスペクション エンジンでは、トラフィックにインスペクションを適用するときの追加パラメータを制御できます。インスペクション ポリシー マップを設定するには、インスペクション タイプの [Configure] をクリックします。既存のマップを選択することも、新しいマップを作成することもできます。[Configuration] > [Firewall] > [Objects] > [Inspect Maps] リストから、インスペクション ポリシー マップを事前に定義できます。

次の表に、検査可能なプロトコル、インスペクション ポリシー マップまたはインスペクション クラス マップを使用できるかどうか、さらにインスペクションに関する詳細情報へのポインタを示します。

表 8-2　インスペクション プロトコル

プロトコル	インスペクション ポリシー マップのサポート	インスペクション クラス マップのサポート	注意
CTIQBE	No	No	「CTIQBE インスペクション」（P.10-1）を参照してください。
クラウド Web セキュリティ	Yes	Yes	ScanSafe（クラウド Web セキュリティ）をイネーブルにしたい場合、この手順ではなく、次のトピック、「クラウド Web セキュリティにトラフィックを送信するサービス ポリシーの方法」（P.16-10）で説明している手順を使用してください。前述の手順では、ポリシー インスペクション マップの設定方法を含む、完全なポリシー設定について説明しています。
DCERPC	Yes	No	「DCERPC インスペクション」（P.12-1）を参照してください。
DNS	Yes	Yes	「DNS インスペクション」（P.9-1）を参照してください。
ESMTP	Yes	No	「SMTP および拡張 SMTP 検査」（P.9-34）を参照してください。
FTP	Yes	Yes	「FTP インスペクション」（P.9-8）を参照してください。
GTP	Yes	No	「GTP インスペクション」（P.12-4）を参照してください。
H.323 H.225	Yes	Yes	「H.323 インスペクション」（P.10-2）を参照してください。
H.323 RAS	Yes	Yes	「H.323 インスペクション」（P.10-2）を参照してください。
HTTP	Yes	Yes	「HTTP インスペクション」（P.9-14）を参照してください。

表 8-2　インスペクション プロトコル （続き）

プロトコル	インスペクション ポリシー マップのサポート	インスペクション クラス マップのサポート	注意
ICMP	No	No	「ICMP インスペクション」（P.9-20）を参照してください。
ICMP Error	No	No	「ICMP エラー インスペクション」（P.9-20）を参照してください。
ILS	No	No	「ILS インスペクション」（P.11-1）を参照してください。
IM	Yes	Yes	「インスタント メッセージ インスペクション」（P.9-21）を参照してください。
IP-Options	Yes	No	「IP オプション インスペクション」（P.9-24）を参照してください。
IPSec パススルー	Yes	No	「IPsec パススルー インスペクション」（P.9-27）を参照してください。
IPv6	Yes	No	「IPv6 インスペクション」（P.9-30）を参照してください。
MGCP	Yes	No	「MGCP インスペクション」（P.10-9）を参照してください。
NetBIOS	Yes	No	「NETBIOS インスペクション」（P.9-32）を参照してください。
PPTP	No	No	「PPTP インスペクション」（P.9-34）を参照してください。
RADIUS アカウンティング	Yes	No	「RADIUS アカウンティング インスペクション」（P.12-9）を参照してください。 RADIUS アカウンティング インスペクションは管理サービス ポリシーでのみ使用可能です。このインスペクションを実装するには、ポリシー マップを選択する必要があります。
RSH	No	No	「RSH インスペクション」（P.12-12）を参照してください。
RTSP	Yes	No	「RTSP インスペクション」（P.10-13）を参照してください。
SCCP（Skinny）		No	「Skinny（SCCP）インスペクション」（P.10-25）を参照してください。
SIP	Yes	Yes	「SIP インスペクション」（P.10-17）を参照してください。
SNMP	Yes	No	「SNMP インスペクション」（P.12-12）を参照してください。
SQLNET	No	No	「SQL*Net インスペクション」（P.11-2）を参照してください。

表 8-2　インスペクション プロトコル （続き）

プロトコル	インスペクション ポリシー マップのサポート	インスペクション クラス マップのサポート	注意
SUNRPC	No	No	「Sun RPC インスペクション」（P.11-3）を参照してください。 デフォルトのクラス マップには UDP ポート 111 が含まれています。TCP ポート 111 の Sun RPC インスペクションをイネーブルにするには、TCP ポート 111 を照合する新しいクラス マップを作成し、クラスをポリシーに追加してから、そのクラスに **inspect sunrpc** コマンドを適用する必要があります。
TFTP	No	No	「TFTP インスペクション」（P.9-39）を参照してください。
WAAS	No	No	TCP オプション 33 解析をイネーブルにします。Cisco Wide Area Application Services 製品を導入するときに使用します。
XDMCP	No	No	「XDMCP インスペクション」（P.12-13）を参照してください。

ステップ 6　必要に応じて、他の [Rule Actions] タブを使用し、このルールに対して他の機能を設定できます。

ステップ 7　[OK] をクリックします（またはウィザードで [Finish] をクリックします）。

正規表現の設定

正規表現は、テキスト文字列のパターン照合を定義します。一部のプロトコル インスペクション マップでは、正規表現を使用して、URL や特定のヘッダー フィールドのコンテンツなどの文字列に基づいてパケットを照合できます。

- 「正規表現の作成」（P.8-13）
- 「正規表現クラス マップの作成」（P.8-17）

正規表現の作成

正規表現は、ストリングそのものとしてテキスト ストリングと文字どおりに照合することも、*メタ文字*を使用してテキスト ストリングの複数のバリアントと照合することもできます。正規表現を使用して特定のアプリケーション トラフィックの内容と照合できます。たとえば、HTTP パケット内部の URL 文字列と照合できます。

はじめる前に

正規表現をパケットと照合する場合のパフォーマンスへの影響については、コマンド リファレンスの **regex** コマンドを参照してください。一般的に、長い入力文字列と照合したり、多くの正規表現と照合しようとすると、システム パフォーマンスが低下します。

（注） 最適化のために、ASA では、難読化解除された URL が検索されます。難読化解除では、複数のスラッシュ（//）が単一のスラッシュに圧縮されます。通常、「http://」のようなダブル スラッシュが使用される文字列では、代わりに「http:/」を検索してください。

次の表に、特別な意味を持つメタ文字を示します。

表 8-3　　正規表現のメタ文字

文字	説明	注意
.	ドット	任意の単一文字と一致します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
(*exp*)	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、**d(ola)g** は dog および dag に一致しますが、**dolag** は do および ag に一致します。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、**doglcat** は、dog または cat に一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。たとえば、**lo?se** は、lse または lose に一致します。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示す修飾子。たとえば、**lo*se** は、lse、lose、loose などに一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示す修飾子。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
{*x*} または {*x*,}	最小繰り返し限定作用素	少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
[*abc*]	文字クラス	カッコ内の任意の文字と一致します。たとえば、**[abc]** は、a、b、または c に一致します。
[^*abc*]	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、**[^abc]** は、a、b、c 以外の任意の文字に一致します。**[^A-Z]** は、大文字のアルファベット文字以外の任意の単一の文字に一致します。
[*a-c*]	文字範囲クラス	範囲内の任意の文字と一致します。**[a-z]** は、任意の小文字のアルファベット文字に一致します。文字と範囲を組み合わせて使用することもできます。**[abcq-z]** および **[a-cq-z]** は、a、b、c、q、r、s、t、u、v、w、x、y、z に一致します。 ダッシュ（-）文字は、角カッコ内の最初の文字または最後の文字である場合にのみリテラルとなります（**[abc-]** や **[-abc]**）。

表 8-3　正規表現のメタ文字 （続き）

文字	説明	注意
「」	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、**" test"** は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
****	エスケープ文字	メタ文字とともに使用すると、リテラル文字と一致します。たとえば、**\[** は左角カッコに一致します。
char	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	タブ	タブ 0x09 と一致します。
\f	改ページ	フォーム フィード 0x0c と一致します。
\x*NN*	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
NNN	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 040 はスペースを表します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Regular Expressions] を選択します。

ステップ 2　[Regular Expressions] 領域で、次のいずれかを実行します。

- [Add] を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存のオブジェクトを選択し、[Edit] をクリックします。

ステップ 3　[Value] フィールドに正規表現を入力するか、[Build] をクリックしてヘルプを利用しながら表現を作成します。

正規表現の長さは 100 文字までに制限されています。

[Build] をクリックした場合、次のプロセスを使用して表現を作成します。

a. [Build Snippet] 領域で、次のオプションを使用して表現のコンポーネントを作成します。作成中の表現を表示するには、この項の終わりにある [Snippet Preview] 領域を確認してください。

- [Starts at the beginning of the line (^)]：部分式は行頭から開始し、開始場所はメタ文字のカレット（^）で示します。このオプションを使用して作成した部分式は、正規表現の先頭に挿入してください。
- [Specify Character String]：単語やフレーズなどの特定の文字列を照合しようとしている場合、その文字列を入力します。

  テキスト文字列の中に文字どおりに使用したいメタ文字がある場合、[Escape Special Characters] を選択し、そのメタ文字の前にエスケープ文字のバックスラッシュ（\）を追加します。たとえば、「example.com」と入力すると、このオプションによって「example\.com」に変換されます。

大文字および小文字を照合したい場合は、[Ignore Case] を選択します。たとえば、「cats」は「[cC][aA][tT][sS]」に変換されます。

- [Specify Character]：特定のフレーズではなく、特定タイプの文字や文字の組み合わせを照合しようとしている場合は、このオプションを選択し、次のオプションを使用して文字を特定します。

  [Negate the character]：識別した文字を照合の対象外に指定します。

  [Any character (.)]：すべての文字と一致させる、メタ文字のピリオド（.）を挿入します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。

  [Character set]：文字セットを挿入します。テキストをこのセットに含まれるすべての文字と照合します。たとえば、[0-9A-Za-z] の場合、部分式は 0 ～ 9 の数字と A ～ Z の大文字および小文字と照合します。[\n\f\r\t] セットは、改行、改ページ、復帰、タブと一致します。

  [Special character]：エスケープが必要な文字（\、?、*、+、|、.、[、(、^ など）を挿入します。エスケープ文字はバックスラッシュ（\）で、このオプションを選択すると自動的に入力されます。

  [Whitespace character]：空白スペースには \n（改行）、\f（改ページ）、\r（復帰）、\t（タブ）があります。

  [Three digit octal number]：8 進数を使用する ASCII 文字（3 桁まで）と一致します。たとえば、\040 はスペースを意味します。バックスラッシュ（\）は自動的に入力されます。

  [Two digit hexadecimal number]：16 進数を使用する ASCII 文字（厳密に 2 桁）と一致します。バックスラッシュ（\）は自動的に入力されます。

  [Specified character]：任意の 1 文字を入力します。

b. 次のいずれかのボタンを使用して、正規表現ボックスに部分式を追加します。正規表現ボックスに直接入力できることにも注意してください。

- [Append Snippet]：部分式を正規表現の最後に追加します。
- [Append Snippet as Alternate]：部分式をパイプ記号（|）で区切って、正規表現の最後に追加します。区切られた表現の一方と照合します。たとえば、**dog|cat** は、dog または cat に一致します。
- [Insert Snippet at Cursor]：部分式をカーソル位置に挿入します。

c. 表現が完了するまで、部分式を追加するプロセスを繰り返します。

d. （オプション）[Selection Occurrences] では、表現またはその一部を、一致すると考えられるテキストとどれくらいの頻度で照合する必要があるかを選択します。[Regular Expression] フィールドでテキストを選択し、次のいずれかのオプションをクリックしてから [Apply to Selection] をクリックします。たとえば、正規表現が「test me」であり、「me」を選択して [One or more times] を適用する場合、正規表現は「test (me)+」に変更されます。

- [Zero or one times (?)]：直前の表現が 0 または 1 個存在します。たとえば、**lo?se** は、lse または lose に一致します。
- [One or more times (+)]：直前の表現が少なくとも 1 個存在します。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
- [Any number of times (*)]：直前の表現が 0、1、または任意の個数あります。たとえば、**lo*se** は、lse、lose、loose などに一致します。
- [At least]：少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
- [Exactly]：*x* 回だけ繰り返します。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。

e. 表現が意図したテキストに一致することを検証するには、[Test] をクリックします。テストが失敗した場合は、[Test] ダイアログボックスで編集を試みるか、表現ビルダーに戻ることができます。テキスト ダイアログの表現を編集し、[OK] をクリックすると、編集内容が保存され、表現ビルダーに反映されます。

f. [OK] をクリックします。

正規表現クラス マップの作成

正規表現クラス マップは、1 つ以上の正規表現を特定します。正規表現クラス マップは、正規表現オブジェクトを集めているにすぎません。多くの場合、正規表現オブジェクトの代わりに正規表現クラス マップを使用できます。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Regular Expressions] を選択します。

ステップ 2　[Regular Expressions Classes] 領域で、次のいずれかを実行します。

- [Add] を選択して、新しいクラス マップを追加します。名前を入力し、任意で説明を入力します。
- 既存のクラス マップを選択し、[Edit] をクリックします。

ステップ 3　マップに含めたい表現を選択し、[Add] をクリックします。不要なものを削除します。

ステップ 4　[OK] をクリックします。

アプリケーション インスペクションの履歴

機能名	リリース	説明
インスペクション ポリシー マップ	7.2(1)	インスペクション ポリシー マップが導入されました。**class-map type inspect** コマンドが導入されました。
正規表現およびポリシー マップ	7.2(1)	インスペクション ポリシー マップで使用される正規表現およびポリシー マップが導入されました。**class-map type regex** コマンド、**regex** コマンド、および**match regex** コマンドが導入されました。
インスペクション ポリシー マップの match any	8.0(2)	インスペクション ポリシー マップで使用される **match any** キーワードが導入されました。トラフィックを 1 つ以上の基準に照合してクラス マップに一致させることができます。以前は、**match all** だけが使用可能でした。

基本インターネット プロトコルのインスペクション

ここでは、基本インターネット プロトコルのアプリケーション インスペクションについて説明します。特定のプロトコルにインスペクションを使用する必要がある理由、およびインスペクション適用の方法全体については、「アプリケーション レイヤ プロトコル インスペクションの準備」（P.8-1）を参照してください。

- 「DNS インスペクション」（P.9-1）
- 「FTP インスペクション」（P.9-8）
- 「HTTP インスペクション」（P.9-14）
- 「ICMP インスペクション」（P.9-20）
- 「ICMP エラー インスペクション」（P.9-20）
- 「インスタント メッセージ インスペクション」（P.9-21）
- 「IP オプション インスペクション」（P.9-24）
- 「IPsec パススルー インスペクション」（P.9-27）
- 「IPv6 インスペクション」（P.9-30）
- 「NETBIOS インスペクション」（P.9-32）
- 「PPTP インスペクション」（P.9-34）
- 「SMTP および拡張 SMTP 検査」（P.9-34）
- 「TFTP インスペクション」（P.9-39）

DNS インスペクション

ここでは、DNS アプリケーション インスペクションについて説明します。

- 「DNS インスペクションのアクション」（P.9-2）
- 「DNS インスペクションのデフォルト」（P.9-2）
- 「DNS インスペクションの設定」（P.9-2）
- 「DNS インスペクションのモニタリング」（P.9-7）

DNS インスペクションのアクション

DNS インスペクションはデフォルトではイネーブルです。DNS インスペクションをカスタマイズして多くのタスクを実行できます。

- DNS レコードを NAT の設定に基づいて変換します。詳細については、「DNS および NAT」（P.5-32）を参照してください。
- メッセージの長さ、ドメイン名の長さ、ラベルの長さを適用します。
- DNS メッセージに圧縮ポインタが出現した場合、ポインタが参照するドメイン名の整合性を確認します。
- 圧縮ポインタのループが終了するかどうかを確認します。
- DNS のヘッダー、タイプ、クラス、その他に基づいてパケットを検査します。

DNS インスペクションのデフォルト

DNS インスペクションは、preset_dns_map インスペクション クラス マップを使用して、デフォルトでイネーブルになります。

- 最大 DNS メッセージ長は、512 バイトです。
- 最大クライアント DNS メッセージ長は、リソース レコードに一致するように自動的に設定されます。
- DNS ガードはイネーブルになり、ASA によって DNS 応答が転送されるとすぐに、ASA は DNS クエリーに関連付けられている DNS セッションを切断します。ASA はまた、メッセージ交換をモニタして DNS 応答の ID が DNS クエリーの ID と一致することを確認します。
- NAT の設定に基づく DNS レコードの変換はイネーブルです。
- プロトコルの強制はイネーブルであり、DNS メッセージ形式チェックが行われます。ドメイン名の長さが 255 文字以下、ラベルの長さが 63 文字、圧縮、ループ ポインタのチェックなどです。

DNS インスペクションの設定

DNS インスペクションはデフォルトではイネーブルです。デフォルト以外の処理が必要な場合にのみ設定する必要があります。DNS インスペクションをカスタマイズする場合は、次のプロセスを使用します。

手順

ステップ 1　「DNS インスペクション クラス マップの設定」（P.9-3）

ステップ 2　「DNS インスペクション ポリシー マップの設定」（P.9-4）

ステップ 3　「DNS インスペクション サービス ポリシーの設定」（P.9-6）

DNS インスペクション クラス マップの設定

オプションとして、DNS インスペクション クラス マップを作成し、DNS インスペクションのトラフィック クラスを定義できます。他のオプションとしては、DNS インスペクション ポリシー マップでトラフィック クラスを直接定義することもできます。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な一致基準を作成でき、クラス マップを再利用できるという点です。

ヒント　以下で説明する手順に加えて、インスペクション マップまたはサービス ポリシーの作成中にもクラス マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Class Maps] > [DNS] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいクラス マップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　照合オプションとして [Match All] または [Match Any] を選択します。

[Match All] がデフォルトです。トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。[Match Any] は、少なくとも 1 つの基準に一致したトラフィックがクラス マップに一致することを意味します。

ステップ 5　一致テーブルでエントリを追加または編集して、一致基準を設定します。対象トラフィックを定義するために必要な数のエントリを追加します。

a. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

b. 一致基準を選択し、その値を定義します。

- [Header Flag]：フラグが等しい必要があるか、または指定された値を含む必要があるかを選択した後、ヘッダー フラグ名を選択するか、またはヘッダーの 16 進値（0x0 ～ 0xfff）を入力します。複数のヘッダー値を選択する場合、「等しい」はすべてのフラグがパケットに存在する必要があることを示し、「含む」はいずれか 1 つのフラグでもパケットに存在すればよいことを示します。ヘッダー フラグ名は、**AA**（権限応答）、**QR**（クエリー）、**RA**（使用できる再帰）、**RD**（必要な再帰）、**TC**（切り捨て）です。
- [Type]：パケットの DNS タイプ フィールドの名前または値です。フィールド名は、**A**（IPv4 アドレス）、**AXFR**（フル ゾーン転送）、**CNAME**（正規の名前）、**IXFR**（増分ゾーン転送）、**NS**（権限ネーム サーバ）、**SOA**（権限ゾーンの開始）、**TSIG**（トランザクション署名）です。値は、DNS タイプ フィールドの 0 ～ 65535 の任意の数字です。特定の値または値の範囲を入力します。

- [Class]：パケットの DNS クラス フィールドの名前または値です。使用可能な唯一のフィールド名は Internet です。値は、DNS クラス フィールドの 0 ～ 65535 の任意の数字です。特定の値または値の範囲を入力します。
- [Question]：DNS メッセージの質問部分です。
- [Resource Record]：DNS のリソース レコードです。追加、応答、権限の各リソース レコード セクションと照合するかどうかを選択します。

c. [OK] をクリックします。

ステップ 6　[DNS Traffic Class Map] ダイアログ ボックスの [OK] をクリックします。

DNS インスペクション ポリシー マップでクラス マップを使用できるようになります。

DNS インスペクション ポリシー マップの設定

デフォルトのインスペクション動作がネットワークにとって十分でない場合、DNS インスペクション ポリシー マップを作成して DNS インスペクション アクションをカスタマイズできます。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にもインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [DNS] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[DNS Inspect Map] ダイアログ ボックスの [Security Level] ビューで、目的の設定に最も一致するレベルを選択します。デフォルトのレベルは [Low] です。

プリセット レベルの 1 つが要件と一致する場合は、これで完了です。[OK] をクリックし、残りの手順をスキップして、DNS インスペクションのサービス ポリシー ルールでマップを使用します。

設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、手順を続けます。

ステップ 5　[Protocol Conformance] タブをクリックし、必要なオプションを選択します。

- [Enable DNS guard function]：DNS ガードを使用します。ASA によって DNS 応答が転送されるとすぐに、ASA は DNS クエリーに関連付けられている DNS セッションを切断します。ASA はまた、メッセージ交換をモニタして DNS 応答の ID が DNS クエリーの ID と一致することを確認します。

- [Enable NAT re-write function]：DNS レコードを NAT の設定に基づいて変換します。
- [Enable protocol enforcement]：DNS メッセージ形式のチェックをイネーブルにします。ドメイン名の長さが 255 文字以下、ラベルの長さが 63 文字、圧縮、ループ ポインタのチェックなどを行います。
- [Randomize the DNS identifier for DNS query]。
- [Enforce TSIG resource record to be present in DNS message]：準拠していないパケットをドロップまたはロギングできます。必要であれば、ドロップされたパケットをロギングできます。

ステップ 6　[Filtering] タブをクリックし、必要なオプションを選択します。

- [Global Settings]：クライアントまたはサーバのどちらからのパケットであるかに関係なく、指定した最大長を超えるパケットをドロップするかどうかを選択します（512 ～ 65535 バイト）。
- [Server Settings]：[Drop packets that exceed specified maximum length] および [Drop packets sent to server that exceed length indicated by the RR]：サーバ DNS メッセージの最大長を設定するか（512 ～ 65535 バイト）、またはリソース レコードでの値に設定します。両方の設定をイネーブルにすると、小さい方の値が使用されます。
- [Client Settings]:[Drop packets that exceed specified maximum length] および [Drop packets sent to server that exceed length indicated by the RR]：クライアント DNS メッセージの最大長を設定するか（512 ～ 65535 バイト）、またはリソース レコードでの値に設定します。両方の設定をイネーブルにすると、小さい方の値が使用されます。

ステップ 7　[Mismatch Rate] タブをクリックして、DNS ID 不一致レートが指定した、しきい値を超えた場合のロギングをイネーブルにするかどうかを選択します。たとえば、しきい値を 3 秒あたり 30 個の不一致に設定できます。

ステップ 8　[Inspections] タブをクリックして、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

トラフィック一致基準は、DNS クラス マップをベースにするか、インスペクション マップで一致を直接設定するか、またはこの両方によって定義できます。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b. 基準を直接定義する場合は [Single Match] を選択し、基準を定義する DNS クラス マップを選択する場合は [Multiple Match] を選択します（「DNS インスペクション クラス マップの設定」（P.9-3）を参照）。

c. 基準をここで定義した場合は、基準の一致タイプとして [Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。次に、基準を以下のように設定します。

- [Header Flag]：フラグが等しい必要があるか、または指定された値を含む必要があるかを選択した後、ヘッダー フラグ名を選択するか、またはヘッダーの 16 進値（0x0 ～ 0xfff）を入力します。複数のヘッダー値を選択する場合、「等しい」はすべてのフラグがパケットに存在する必要があることを示し、「含む」はいずれか 1 つのフラグでもパケットに存在すればよいことを示します。ヘッダー フラグ名は、**AA**（権限応答）、**QR**（クエリー）、**RA**（使用できる再帰）、**RD**（必要な再帰）、**TC**（切り捨て）です。

- [Type]：パケットの DNS タイプ フィールドの名前または値です。フィールド名は、**A**（IPv4 アドレス）、**AXFR**（フル ゾーン転送）、**CNAME**（正規の名前）、**IXFR**（増分ゾーン転送）、**NS**（権限ネーム サーバ）、**SOA**（権限ゾーンの開始）、**TSIG**（トランザクション署名）です。値は、DNS タイプ フィールドの 0 ～ 65535 の任意の数字です。特定の値または値の範囲を入力します。
- [Class]：パケットの DNS クラス フィールドの名前または値です。使用可能な唯一のフィールド名は Internet です。値は、DNS クラス フィールドの 0 ～ 65535 の任意の数字です。特定の値または値の範囲を入力します。
- [Question]：DNS メッセージの質問部分です。
- [Resource Record]：DNS のリソース レコードです。追加、応答、権限の各リソース レコード セクションと照合するかどうかを選択します。

d. 一致したトラフィックに対して実行する主要なアクションを選択します。パケットのドロップ、接続の切断、マスク（ヘッダー フラグ一致の場合のみ）、何もしない、のいずれかです。

e. ロギングをイネーブルまたはディセーブルのどちらにするかを選択します。TSIG を強制する場合は、ロギングをディセーブルにする必要があります。

f. TSIG リソース レコードの存在を強制するかどうかを選択します。パケットのドロップ、パケットのロギング、またはパケットのドロップとロギングが可能です。通常、TSIG を強制するには [Primary Action] で [None] を選択し、[Log] で [Disable] を選択する必要があります。ただし、ヘッダー フラグ一致の場合は、マスクのプライマリ アクションとともに TSIG を適用できます。

g. [OK] をクリックしてインスペクションを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 9　[DNS Inspect Map] ダイアログ ボックスの [OK] をクリックします。

DNS インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

DNS インスペクション サービス ポリシーの設定

ASA のデフォルトの設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの DNS インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- DNS インスペクション ルールがある場合、または DNS インスペクションを追加しているルールがある場合は、それを選択して、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別の DNS インスペクション ポリシー マップを使用する場合は、DNS インスペクションをディセーブルにしてから、新しい DNS インスペクション ポリシー マップ名で再度イネーブルにする必要があります。

a. [DNS] チェックボックスの選択を解除します。

b. [OK] をクリックします。

c. [Apply] をクリックします。

d. この手順を繰り返して [Protocol Inspections] タブに戻ります。

ステップ 4　[DNS] を選択します

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した DNS インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「DNS インスペクション ポリシー マップの設定」（P.9-4）を参照してください。

b. ボットネット トラフィック フィルタを使用している場合は、[Enable DNS snooping] を選択します。DNS スヌーピングは、外部 DNS 要求が送信されるインターフェイスでだけイネーブルにすることを推奨します。すべての UDP DNS トラフィック（内部 DNS サーバへの送信トラフィックを含む）に対して DNS スヌーピングをイネーブルにすると、ASA で不要な負荷が発生します。暗号化された SIP トラフィックを検査する場合は、[Enable encrypted traffic inspection] を選択し、TLS プロキシを選択します（必要な場合は [Manage] をクリックして作成します）。たとえば、DNS サーバが外部インターフェイスに存在する場合は、外部インターフェイスのすべての UDP DNS トラフィックに対して DNS インスペクションとスヌーピングをイネーブルにする必要があります。

c. [Select DNS Inspect Map] ダイアログ ボックスの [OK] をクリックします。

ステップ 6　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

DNS インスペクションのモニタリング

現在の DNS 接続に関する情報を表示するには、[Tools] > [Command Line Interface] で次のコマンドを入力するか、または [Monitoring] > [Properties] > [Connections] を使用します。

```
hostname# show conn
```

DNS サーバを使用する接続の場合、show conn コマンドの出力で、接続の送信元ポートが DNS サーバの IP アドレスに置き換えられることがあります。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元/宛先 IP アドレス、送信元/宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つだけ作成されます。DNS ID は app_id で追跡され、各 app_id のアイドル タイマーは独立して実行されます。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答がセキュリティ アプライアンスを通過できるのは、限られた期間内だけであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力した場合、新しい DNS セッションによってリセットされている DNS 接続のアイドル タイマーが表示されます。これは共有 DNS 接続の性質によるものであり、仕様です。

DNS アプリケーション インスペクションの統計情報を表示するには、**show service-policy** コマンドを入力します。次に、**show service-policy** コマンドの出力例を示します。

```
hostname# show service-policy
Interface outside:
Service-policy: sample_policy
    Class-map: dns_port
      Inspect: dns maximum-length 1500, packet 0, drop 0, reset-drop 0
```

FTP インスペクション

ここでは、FTP インスペクション エンジンについて説明します。

- 「FTP インスペクションの概要」（P.9-8）
- 「厳密な FTP」（P.9-8）
- 「FTP インスペクションの設定」（P.9-9）
- 「FTP インスペクションの確認とモニタリング」（P.9-14）

FTP インスペクションの概要

FTP アプリケーション インスペクションは、FTP セッションを検査し、次の 4 つのタスクを実行します。

- ダイナミックな二次的データ接続の準備
- FTP コマンド応答シーケンスの追跡
- 監査証跡の生成
- 埋め込み IP アドレスの変換

FTP アプリケーション インスペクションによって、FTP データ転送用にセカンダリ チャネルが用意されます。これらのチャネルのポートは、PORT コマンドまたは PASV コマンドを使用してネゴシエートされます。セカンダリ チャネルは、ファイル アップロード、ファイル ダウンロード、またはディレクトリ リスト イベントへの応答で割り当てられます。

（注）　**no inspect ftp** コマンドを使用して、FTP インスペクション エンジンをディセーブルにすると、アウトバウンド ユーザはパッシブ モードだけで接続を開始でき、インバウンド FTP はすべてディセーブルになります。

厳密な FTP

厳密な FTP を使用すると、Web ブラウザが FTP 要求内の埋め込みコマンドを送信できなくなるため、保護されたネットワークのセキュリティが強化されます。厳密な FTP をイネーブルにするには、[Configuration] > [Firewall] > [Service Policy Rules] > [Edit Service Policy Rule] > [Rule Actions] > [Protocol Inspection] タブで、FTP の横にある [Configure] ボタンをクリックします。

厳密な FTP を使用するときは、オプションで FTP インスペクション ポリシー マップを指定して、ASA を通過することが許可されない FTP コマンドを指定できます。

インターフェイスに対して **strict** オプションをオンにすると、FTP インスペクションによって次の動作が適用されます。

- FTP コマンドが確認応答されてからでないと、ASA は新しいコマンドを許可しません。
- ASA は、埋め込みコマンドを送信する接続をドロップします。
- 227 コマンドと PORT コマンドが、エラー文字列に表示されないように確認されます。

注意　**strict** オプションを使用すると、FTP RFC に厳密に準拠していない FTP クライアントは失敗することがあります。

strict オプションがイネーブルの場合、各 FTP コマンドと応答シーケンスが追跡され、次の異常なアクティビティがないか確認されます。

- 切り捨てされたコマンド : PORT コマンドおよび PASV 応答コマンドのカンマの数が 5 であるかどうかが確認されます。カンマの数が 5 でない場合は、PORT コマンドが切り捨てられていると見なされ、TCP 接続は閉じられます。
- 不正なコマンド：FTP コマンドが、RFC の要求どおりに <CR><LF> 文字で終了しているかどうか確認されます。終了していない場合は、接続が閉じられます。
- RETR コマンドと STOR コマンドのサイズ：これらが、固定の定数と比較チェックされます。サイズが定数より大きい場合は、エラー メッセージがロギングされ、接続が閉じられます。
- コマンド スプーフィング : PORT コマンドは、常にクライアントから送信されます。PORT コマンドがサーバから送信される場合、TCP 接続は拒否されます。
- 応答スプーフィング：PASV 応答コマンド（227）は、常にサーバから送信されます。PASV 応答コマンドがクライアントから送信される場合、TCP 接続は拒否されます。これにより、ユーザが「227 xxxxx a1, a2, a3, a4, p1, p2」を実行する場合のセキュリティ ホールが予防できます。
- TCP ストリーム編集：ASA は、TCP ストリーム編集を検出した場合に接続が閉じられます。
- 無効ポート ネゴシエーション：ネゴシエートされたダイナミック ポート値が、1024 未満であるかどうかが調べられます。1 ～ 1024 の範囲のポート番号は、予約済み接続用に指定されているため、ネゴシエートされたポートがこの範囲内であった場合、TCP 接続は解放されます。
- コマンド パイプライン：PORT コマンドと PASV 応答コマンド内のポート番号の後に続く文字数が、定数の 8 と比べられます。8 より大きい場合は、TCP 接続が閉じられます。
- ASA は、SYST コマンドに対する FTP サーバ応答を X の連続に置き換えることで、FTP クライアントがサーバのシステム タイプを取得できないようにします。このデフォルトの動作を無効にするには、FTP マップで、**no mask-syst-reply** コマンドを使用します。

FTP インスペクションの設定

FTP インスペクションは、デフォルトでイネーブルになっています。デフォルト以外の処理が必要な場合にのみ設定する必要があります。FTP インスペクションをカスタマイズする場合は、次のプロセスを使用します。

手順

ステップ 1　「FTP インスペクション クラス マップの設定」（P.9-10）

ステップ 2　「FTP インスペクション ポリシー マップの設定」（P.9-11）

ステップ 3　「FTP インスペクション サービス ポリシーの設定」（P.9-13）

FTP インスペクション クラス マップの設定

オプションとして、FTP インスペクション クラス マップを作成し、FTP インスペクションのトラフィック クラスを定義できます。他のオプションとしては、FTP インスペクション ポリシー マップでトラフィック クラスを直接定義することもできます。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な一致基準を作成でき、クラス マップを再利用できるという点です。

ヒント　以下で説明する手順に加えて、インスペクション マップまたはサービス ポリシーの作成中にもクラス マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Class Maps] > [FTP] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいクラス マップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　照合オプションとして [Match All] または [Match Any] を選択します。

[Match All] がデフォルトです。トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。[Match Any] は、少なくとも 1 つの基準に一致したトラフィックがクラス マップに一致することを意味します。

ステップ 5　一致テーブルでエントリを追加または編集して、一致基準を設定します。対象トラフィックを定義するために必要な数のエントリを追加します。

a. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

b. 一致基準を選択し、その値を定義します。

- [File Name]：選択した正規表現または正規表現クラスに対して転送されるファイルの名前と照合します。

- [File Type]：選択した正規表現または正規表現クラスに対して転送されるファイルの MIME またはメディア タイプと照合します。
- [Server]：選択した正規表現または正規表現クラスに対する FTP サーバの名前と照合します。
- [User]：選択した正規表現または正規表現クラスに対するログイン ユーザの名前と照合します。
- [Request Command]：パケットで使用される FTP コマンドです。以下の任意の組み合わせです。

  APPE：ファイルに追加します。

  CDUP：現在の作業ディレクトリの親ディレクトリに移動します。

  DELE：サーバのファイルを削除します。

  GET：サーバからファイルを取得します。

  HELP：ヘルプ情報を提供します。

  MKD：サーバにディレクトリを作成します。

  PUT：ファイルをサーバに送信します。

  MKD：サーバのディレクトリを削除します。

  RNFR：「変更元」ファイル名を指定します。

  RNTO：「変更先」ファイル名を指定します。

  SITE：サーバ固有のコマンドの指定に使用されます。通常、これはリモート管理に使用されます。

  STOU：一意のファイル名を使用してファイルを保存します。

c. [OK] をクリックします。

ステップ 6　[FTP Traffic Class Map] ダイアログ ボックスの [OK] をクリックします。

FTP インスペクション ポリシー マップでクラス マップを使用できるようになります。

FTP インスペクション ポリシー マップの設定

厳密な FTP インスペクションには、セキュリティと制御を向上させるためのコマンド フィルタリングとセキュリティ チェック機能が用意されています。プロトコルとの適合性のインスペクションには、パケットの長さのチェック、デリミタとパケットの形式のチェック、コマンドのターミネータのチェック、およびコマンドの検証が含まれます。

また、ユーザの値に基づいて FTP 接続をブロックできるので、FTP サイトにダウンロード用のファイルを置き、アクセスを特定のユーザだけに制限できます。ファイルのタイプ、サーバ名、および他の属性に基づいて、FTP 接続をブロックできます。インスペクション時に FTP 接続が拒否されると、システム メッセージのログが作成されます。

FTP インスペクションで FTP サーバがそのシステム タイプを FTP クライアントに公開することを許可し、許可する FTP コマンドを制限する場合、FTP インスペクション ポリシー マップを作成および設定します。作成したマップは、FTP インスペクションをイネーブルにすると適用できます。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にもインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [FTP] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[FTP Inspect Map] ダイアログ ボックスの [Security Level] ビューで、目的の設定に最も一致するレベルを選択します。デフォルトのレベルは [High] です。

プリセット レベルの 1 つが要件と一致する場合は、これで完了です。[OK] をクリックし、残りの手順をスキップして、FTP インスペクションのサービス ポリシー ルールでマップを使用します。

設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、手順を続けます。

ヒント　[File Type Filtering] ボタンはファイル メディアまたは MIME タイプのインスペクションを設定するためのショートカットです。これについては後で説明します。

ステップ 5　[Parameters] タブをクリックし、サーバからの接続時バナーをマスクするかどうか、または SYST コマンドへの応答をマスクするかどうかを選択します。

これらの項目をマスクすることによって、クライアントは攻撃を利する可能性のあるサーバ情報の検出を防ぐことができます。

ステップ 6　[Inspections] タブをクリックして、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

トラフィック一致基準は、FTP クラス マップをベースにするか、インスペクション マップで一致を直接設定するか、またはこの両方によって定義できます。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b. 基準を直接定義する場合は [Single Match] を選択し、基準を定義する FTP クラス マップを選択する場合は [Multiple Match] を選択します（「FTP インスペクション クラス マップの設定」（P.9-10）を参照）。

c. 基準をここで定義した場合は、基準の一致タイプとして [Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。次に、「FTP インスペクション クラス マップの設定」（P.9-10）の説明に従って基準を設定します。

d. ロギングをイネーブルまたはディセーブルのどちらにするかを選択します。アクションは常に接続をリセットします。パケットをドロップして接続を閉じ、サーバまたはクライアントに TCP リセットを送信します。

e. [OK] をクリックしてインスペクションを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 7　[FTP Inspect Map] ダイアログ ボックスの [OK] をクリックします。

FTP インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

FTP インスペクション サービス ポリシーの設定

ASA のデフォルトの設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの FTP インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- FTP インスペクション ルールがある場合、または FTP インスペクションを追加しているルールがある場合は、それを選択して、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別の FTP インスペクション ポリシー マップを使用する場合は、FTP インスペクションをディセーブルにしてから、新しい FTP インスペクション ポリシー マップ名で再度イネーブルにする必要があります。

a. [FTP] チェックボックスの選択を解除します。

b. [OK] をクリックします。

c. [Apply] をクリックします。

d. この手順を繰り返して [Protocol Inspections] タブに戻ります。

ステップ 4　[FTP] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. [Use Strict FTP] を選択します。

b. デフォルト マップを使用するか、またはユーザが設定した FTP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「FTP インスペクション ポリシー マップの設定」（P.9-11）を参照してください。

c. [Select FTP Inspect Map] ダイアログ ボックスの [OK] をクリックします。

ステップ 6　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

FTP インスペクションの確認とモニタリング

FTP アプリケーション インスペクションでは、次のログ メッセージが生成されます。

- 取得またはアップロードされたファイルごとに監査レコード 303002 が生成されます。
- FTP コマンドが RETR または STOR であるかがチェックされ、取得コマンドおよび保存コマンドがログに記録されます。
- IP アドレスを提供するテーブルを検索してユーザ名が取得されます。
- ユーザ名、接続元の IP アドレス、接続先の IP アドレス、NAT アドレス、およびファイル操作がログに記録されます。
- メモリ不足によって動的なセカンダリ チャネルの準備に失敗した場合は、監査レコード 201005 が生成されます。

NAT と連携することにより、FTP アプリケーション インスペクションでは、アプリケーション ペイロード内の IP アドレスが変換されます。これは、RFC 959 に詳細に記述されています。

HTTP インスペクション

ここでは、HTTP インスペクション エンジンについて説明します。

- 「HTTP インスペクションの概要」（P.9-14）
- 「HTTP インスペクションの設定」（P.9-15）

HTTP インスペクションの概要

ヒント　アプリケーションおよび URL のフィルタリングを実行するサービス モジュールをインストールできます。これには、ASA CX や ASA FirePOWER などの HTTP インスペクションが含まれます。ASA 上で実行される HTTP インスペクションは、これらのモジュールと互換性がありません。HTTP インスペクション ポリシー マップを使用して ASA 上で手作業による設定を試みるより、専用のモジュールを使用してアプリケーション フィルタリングを設定する方がはるかに簡単であることに注意してください。

HTTP インスペクション エンジンを使用して、HTTP トラフィックに関係する特定の攻撃やその他の脅威から保護します。

HTTP アプリケーション インスペクションで HTTP のヘッダーと本文をスキャンし、さまざまなデータ チェックができます。これらのチェックで、HTTP 構築、コンテンツ タイプ、トンネル プロトコル、メッセージ プロトコルなどがセキュリティ アプライアンスを通過することを防止します。

拡張 HTTP インスペクション機能はアプリケーション ファイアウォールとも呼ばれ、HTTP インスペクション ポリシー マップを設定するときに使用できます。これによって、攻撃者がネットワーク セキュリティ ポリシーに従わない HTTP メッセージを使用できないようにします。

HTTP アプリケーション インスペクションでトンネル アプリケーションと ASCII 以外の文字を含む HTTP 要求や応答をブロックして、悪意のあるコンテンツが Web サーバに到達することを防ぎます。HTTP 要求や応答ヘッダーのさまざまな要素のサイズ制限、URL のブロッキング、HTTP サーバ ヘッダー タイプのスプーフィングもサポートされています。

拡張 HTTP インスペクションは、すべての HTTP メッセージについて次の点を確認します。

- RFC 2616 への準拠
- RFC で定義された方式だけを使用していること
- 追加の基準への準拠

HTTP インスペクションの設定

HTTP インスペクションはデフォルトではイネーブルになりません。ASA CX や ASA FirePOWER などの HTTP インスペクションおよびアプリケーション フィルタリングに専用のモジュールを使用していない場合、以下の方法を使用して、ASA に HTTP インスペクションを手動で設定できます。

ヒント　サービス モジュールと ASA の両方で HTTP インスペクションを設定しないでください。インスペクションの互換性はありません。

手順

ステップ 1　「HTTP インスペクション クラス マップの設定」（P.9-15）
ステップ 2　「HTTP インスペクション ポリシー マップの設定」（P.9-18）
ステップ 3　「HTTP インスペクション サービス ポリシーの設定」（P.9-19）

HTTP インスペクション クラス マップの設定

オプションとして、HTTP インスペクション クラス マップを作成し、HTTP インスペクションのトラフィック クラスを定義できます。他のオプションとしては、HTTP インスペクション ポリシー マップでトラフィック クラスを直接定義することもできます。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な一致基準を作成でき、クラス マップを再利用できるという点です。

ヒント　以下で説明する手順に加えて、インスペクション マップまたはサービス ポリシーの作成中にもクラス マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Class Maps] > [HTTP] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいクラス マップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　照合オプションとして [Match All] または [Match Any] を選択します。

[Match All] がデフォルトです。トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。[Match Any] は、少なくとも 1 つの基準に一致したトラフィックがクラス マップに一致することを意味します。

ステップ 5　一致テーブルでエントリを追加または編集して、一致基準を設定します。対象トラフィックを定義するために必要な数のエントリを追加します。

a. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

b. 一致基準を選択し、その値を定義します。

- [Request/Response Content Type Mismatch]：応答のコンテンツ タイプが要求の accept フィールドの MIME タイプの 1 つと一致しないパケットを照合します。
- [Request Arguments]：要求の引数を、選択した正規表現または正規表現クラスと照合します。
- [Request Body Length]：要求の本文が指定したバイト数より大きいパケットを照合します。
- [Request Body]：要求の本文を、選択した正規表現または正規表現クラスと照合します。
- [Request Header Field Count]：要求のヘッダー フィールドの数が指定した数より多いパケットを照合します。フィールドのヘッダー タイプを正規表現または定義済みのタイプと照合できます。定義済みのタイプは次のとおりです。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。
- [Request Header Field Length] : 要求のヘッダー フィールドの長さが指定したバイト数より大きいパケットを照合します。フィールドのヘッダー タイプを正規表現または定義済みのタイプと照合できます。定義済みのタイプは、上の [Request Header Field Count] に対する一覧と同じです。
- [Request Header Field]：要求の選択したヘッダー フィールドの内容を、選択した正規表現または正規表現クラスと照合します。事前定義されたヘッダー タイプを指定するか、または正規表現を使用してヘッダーを選択できます。
- [Request Header Count]：要求のヘッダーの数が指定した数より多いパケットを照合します。
- [Request Header Length]：要求のヘッダーの長さが指定したバイト数より大きいパケットを照合します。

- [Request Header Non-ASCII]：要求のヘッダーに ASCII 以外の文字が含まれるパケットを照合します。
- [Request Method]：要求メソッドが定義済みのタイプまたは選択した正規表現もしくは正規表現クラスと一致するパケットを照合します。定義済みのタイプは次のとおりです。bcopy、bdelete、bmove、bpropfind、bproppatch、connect、copy、delete、edit、get、getattribute、getattributenames、getproperties、head、index、lock、mkcol、mkdir、move、notify、options、poll、post、propfind、proppatch、put、revadd、revlabel、revlog、revnum、save、search、setattribute、startrev、stoprev、subscribe、trace、unedit、unlock、unsubscribe。
- [Request URI Length]：要求の URI の長さが指定したバイト数より大きいパケットを照合します。
- [Request URI]：要求の URI の内容を、選択した正規表現または正規表現クラスと照合します。
- [Request Body]：要求の本文を、選択した正規表現または正規表現クラスあるいは ActiveX または Java アプレットの内容と照合します。
- [Response Body Length]：応答の本文の長さが指定したバイト数より大きいパケットを照合します。
- [Response Header Field Count]：応答のヘッダー フィールドの数が指定した数より多いパケットを照合します。フィールドのヘッダー タイプを正規表現または定義済みのタイプと照合できます。定義済みのタイプは次のとおりです。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。
- [Response Header Field Length]：応答のヘッダー フィールドの長さが指定したバイト数より大きいパケットを照合します。フィールドのヘッダー タイプを正規表現または定義済みのタイプと照合できます。定義済みのタイプは、上の [Response Header Field Count] に対する一覧と同じです。
- [Response Header Field]：応答の選択したヘッダー フィールドの内容を、選択した正規表現または正規表現クラスと照合します。事前定義されたヘッダー タイプを指定するか、または正規表現を使用してヘッダーを選択できます。
- [Response Header Count]：応答のヘッダーの数が指定した数より多いパケットを照合します。
- [Response Header Length]：応答のヘッダーの長さが指定したバイト数より大きいパケットを照合します。
- [Response Header Non-ASCII] : 応答のヘッダーに ASCII 以外の文字が含まれるパケットを照合します。
- [Response Status Line]：応答のステータス行の内容を、選択した正規表現または正規表現クラスと照合します。

c. [OK] をクリックします。

ステップ 6　[HTTP Traffic Class Map] ダイアログ ボックスの [OK] をクリックします。

HTTP インスペクション ポリシー マップでクラス マップを使用できるようになります。

HTTP インスペクション ポリシー マップの設定

メッセージがパラメータに違反したときのアクションを指定するには、HTTP インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、HTTP インスペクションをイネーブルにすると適用できます。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にもインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [HTTP] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[HTTP Inspect Map] ダイアログ ボックスの [Security Level] ビューで、必要なコンフィギュレーションと最もよく一致するレベルを選択します。デフォルトのレベルは [Low] です。

プリセット レベルの 1 つが要件と一致する場合は、これで完了です。[OK] をクリックし、残りの手順をスキップして、HTTP インスペクションのサービス ポリシー ルールでマップを使用します。

設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、手順を続けます。

ヒント　[URI Filtering] ボタンは要求 URI のインスペクションを設定するためのショートカットです。これについては後で説明します。

ステップ 5　[Parameters] タブをクリックし、必要なオプションを設定します。

- [Body Match Maximum] : HTTP メッセージの本文照合時に検索される、最大文字数です。デフォルトは 200 バイトです。大きな値を指定すると、パフォーマンスに大きな影響を与えます。
- [Check for protocol violations] : パケットが HTTP プロトコルに準拠しているかどうかを確認します。違反している場合、接続のドロップ、リセット、またはログへの記録を行うことができます。ドロップまたはリセットする場合は、ロギングをイネーブルにすることもできます。
- [Spoof server string] : サーバ HTTP ヘッダーの値を指定した文字列に置き換えます。最大 82 文字です。

ステップ 6　[Inspections] タブをクリックして、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

トラフィック一致基準は、HTTP クラス マップをベースにするか、インスペクション マップで一致を直接設定するか、またはこの両方によって定義できます。

a. 次のいずれかを実行します。
   - [Add] をクリックして、新しい基準を追加します。
   - 既存の基準を選択し、[Edit] をクリックします。

b. 基準を直接定義する場合は [Single Match] を選択し、基準を定義する HTTP クラス マップを選択する場合は [Multiple Match] を選択します（「HTTP インスペクション クラス マップの設定」（P.9-15）を参照）。

c. 基準をここで定義した場合は、基準の一致タイプとして [Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。次に、「HTTP インスペクション クラス マップの設定」（P.9-15）の説明に従って基準を設定します。

d. 接続のドロップ、リセット、またはログへの記録を行うかどうかを選択します。接続のドロップまたはリセットの場合は、ロギングをイネーブルまたはディセーブルにできます。

e. [OK] をクリックしてインスペクションを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 7　[HTTP Inspect Map] ダイアログ ボックスの [OK] をクリックします。

HTTP インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

HTTP インスペクション サービス ポリシーの設定

HTTP インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの HTTP ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで HTTP インスペクションを追加できます。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- HTTP インスペクション ルールがある場合、または HTTP インスペクションを追加しているルールがある場合は、それを選択して、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別の HTTP インスペクション ポリシー マップを使用する場合は、HTTP インスペクションをディセーブルにしてから、新しい HTTP インスペクション ポリシー マップ名で再度イネーブルにする必要があります。

a. [HTTP] チェックボックスの選択を解除します。

b. [OK] をクリックします。

c. [Apply] をクリックします。

d. この手順を繰り返して [Protocol Inspections] タブに戻ります。

ステップ 4　[HTTP] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した HTTP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「HTTP インスペクション ポリシー マップの設定」（P.9-18）を参照してください。

b. [Select HTTP Inspect Map] ダイアログ ボックスの [OK] をクリックします。

ステップ 6　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

ICMP インスペクション

ICMP インスペクション エンジンを使用すると、ICMP トラフィックが「セッション」を持つようになるため、TCP トラフィックや UDP トラフィックのように検査することが可能になります。ICMP インスペクション エンジンを使用しない場合は、ACL で ICMP によるASAの通過を禁止することを推奨します。ステートフル インスペクションを実行しないと、ICMP がネットワーク攻撃に利用される可能性があります。ICMP インスペクション エンジンは、要求ごとに応答が 1 つだけであること、シーケンス番号が正しいことを確認します。

ただし、ASA インターフェイスに送られる ICMP トラフィックは、ICMP インスペクションをイネーブルにした場合でも、検査されません。したがって、ASA がバックアップ デフォルト ルートを介して到達できる送信元からエコー要求が送信された場合など、特定の状況下では、インターフェイスへの ping（エコー要求）が失敗する可能性があります。

ICMP インスペクションをイネーブルにする方法については、「アプリケーション レイヤ プロトコル インスペクションの設定」（P.8-10）を参照してください。

ICMP エラー インスペクション

ICMP エラー インスペクションをイネーブルにすると、ASA は NAT の設定に基づいて、ICMP エラー メッセージを送信する中間ホップ用の変換セッションを作成します。ASAは、変換後の IP アドレスでパケットを上書きします。

ディセーブルの場合、ASAは、ICMP エラー メッセージを生成する中間ノード用の変換セッションを作成しません。内部ホストとASAの間にある中間ノードによって生成された ICMP エラー メッセージは、NAT リソースをそれ以上消費することなく、外部ホストに到達します。外部ホストが traceroute コマンドを使用してASAの内部にある宛先までのホップをトレースする場合、これは適切ではありません。ASAが中間ホップを変換しない場合、すべての中間ホップは、マッピングされた宛先 IP アドレスとともに表示されます。

ICMP ペイロードがスキャンされて、元のパケットから 5 つのタプルが取得されます。取得した 5 つのタプルを使用してルックアップを実行し、クライアントの元のアドレスを判別します。ICMP エラー インスペクション エンジンは、ICMP パケットに対して次の変更を加えます。

- IP ヘッダー内のマッピング IP を実際の IP（宛先アドレス）に変更し、IP チェックサムを修正する。
- ICMP パケットに変更を加えたため、ICMP ヘッダー内の ICMP チェックサムを修正する。
- ペイロードに次の変更を加える。
  - 元のパケットのマッピング IP を実際の IP に変更する。
  - 元のパケットのマッピング ポートを実際のポートに変更する。
  - 元のパケットの IP チェックサムを再計算する。

ICMP エラー インスペクションをイネーブルにする方法については、「アプリケーション レイヤ プロトコル インスペクションの設定」（P.8-10）を参照してください。

インスタント メッセージ インスペクション

インスタント メッセージ（IM）インスペクション エンジンを使用すると、IM のネットワーク使用を制御し、機密情報の漏洩、ワームの送信、および企業ネットワークへのその他の脅威を停止できます。

IM インスペクションはデフォルトではイネーブルになりません。IM インスペクションが必要な場合は設定する必要があります。

手順

ステップ 1　「インスタント メッセージ インスペクション ポリシー マップの設定」（P.9-21）

ステップ 2　「IM インスペクション サービス ポリシーの設定」（P.9-23）

インスタント メッセージ インスペクション ポリシー マップの設定

メッセージがパラメータに違反したときのアクションを指定するには、IM インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、IM インスペクションをイネーブルにすると適用できます。

オプションとして、IM インスペクション クラス マップを作成し、IM インスペクションのトラフィック クラスを定義できます。他のオプションとしては、IM インスペクション ポリシー マップでトラフィック クラスを直接定義することもできます。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な一致基準を作成でき、クラス マップを再利用できるという点です。この手順ではインスペクション マップについて説明しますが、トラフィック照合のアクションを指定しないことを除き、クラス マップは基本的に同じです。[Configuration] > [Firewall] > [Objects] > [Class Maps] > [Instant Messaging (IM)] の順に選択することによって、IM クラス マップを設定できます。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にもインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [Instant Messaging (IM)] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

トラフィック一致基準は、IM クラス マップをベースにするか、インスペクション マップで一致を直接設定するか、またはこの両方によって定義できます。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b. 基準を直接定義する場合は [Single Match] を選択し、基準を定義する HTTP クラス マップを選択する場合は [Multiple Match] を選択します。[Manage] をクリックして、新しいクラス マップを作成します。

c. 基準をここで定義した場合は、基準の一致タイプとして [Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。次に、基準を設定します。

- [Protocol]：特定の IM プロトコル（Yahoo Messenger や MSN Messenger など）のトラフィックを照合します。
- [Service]：特定の IM サービス（チャット、ファイル転送、Web カメラ、音声チャット、会議、ゲームなど）を照合します。
- [Version]：IM メッセージのバージョンを、選択した正規表現または正規表現クラスと照合します。
- [Client Login Name]：選択した正規表現または正規表現クラスと IM メッセージの送信元クライアントのログイン名を照合します。
- [Client Peer Login Name]：選択した正規表現または正規表現クラスと IM メッセージの宛先ピアのログイン名を照合します。
- [Source IP Address]：送信元の IP アドレスおよびマスクを照合します。
- [Destination IP Address]：宛先の IP アドレスおよびマスクを照合します。
- [Filename]：IM メッセージのファイル名を、選択した正規表現または正規表現クラスと照合します。

d. 接続のドロップ、リセット、またはログへの記録を行うかどうかを選択します。接続のドロップまたはリセットの場合は、ロギングをイネーブルまたはディセーブルにできます。

e. [OK] をクリックしてインスペクションを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 5　[IM Inspect Map] ダイアログ ボックスの [OK] をクリックします。

IM インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

IM インスペクション サービス ポリシーの設定

IM インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの IM ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで IM インスペクションを追加できます。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- IM インスペクション ルールがある場合、または IM インスペクションを追加しているルールがある場合は、それを選択して、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別の IM インスペクション ポリシー マップを使用する場合は、IM インスペクションをディセーブルにしてから、新しい IM インスペクション ポリシー マップ名で再度イネーブルにする必要があります。

a.　[IM] チェックボックスの選択を解除します。

b.　[OK] をクリックします。

c.　[Apply] をクリックします。

d.　この手順を繰り返して [Protocol Inspections] タブに戻ります。

ステップ 4　[IM] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a.　デフォルト マップを使用するか、設定した IM インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「インスタント メッセージ インスペクション ポリシー マップの設定」（P.9-21）を参照してください。

b.　[Select IM Inspect Map] ダイアログ ボックスの [OK] をクリックします。

ステップ 6　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

IP オプション インスペクション

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASAを通過できるかを制御できます。このインスペクションを設定することで、パケットの転送許可や、指定した IP オプションのクリアがASAに指示され、パケットの転送が可能になります。

ここでは、IP オプション インスペクション エンジンについて説明します。

- 「IP オプション インスペクションの概要」（P.9-24）
- 「IP オプション インスペクションのデフォルト」（P.9-25）
- 「IP オプション インスペクションの設定」（P.9-25）
- 「IP オプション インスペクションのモニタリング」（P.9-27）

IP オプション インスペクションの概要

各 IP パケットには、Options フィールドのある IP ヘッダーが含まれています。Options フィールドは、通常は IP オプションと呼ばれ、制御機能を提供します。特定の状況で必要になりますが、一般的な通信では必要ありません。具体的には、IP オプションにはタイムスタンプ、セキュリティ、および特殊なルーティングの規定が含まれています。IP オプションの使用は任意であり、このフィールドにはオプションを 0 個、1 個、またはそれ以上含めることができます。

IP オプションおよび関連する RFC の参照のリストについては、IANA のページ（http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml）を参照してください。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASAを通過できるかを制御できます。このインスペクションを設定することで、パケットの転送許可や、指定した IP オプションのクリアがASAに指示され、パケットの転送が可能になります。

オプションをクリアしたときの結果

IP オプション インスペクション ポリシー マップを設定する場合、各オプション タイプを許可またはクリアするかどうかを指定できます。オプション タイプを指定しないと、そのオプションを含むパケットはドロップされます。

オプションを単に許可すると、そのオプションを含むパケットは未変更で渡されます。

IP ヘッダーからオプションをクリアするように指定すると、IP ヘッダーは次のように変更されます。

- オプションがヘッダーから除去されます。
- Options フィールドは、32 ビット境界で終了するようにパディングされます。
- パケット内のインターネット ヘッダー長（IHL）が変更されます。
- パケット全体の長さが変更されます。
- チェックサムが再計算されます。

インスペクションでサポートされる IP オプション

IP オプション インスペクションでは、パケット内の次の IP オプションをチェックできます。IP ヘッダーにこれら以外のオプションがさらに含まれている場合、これらのオプションを許可するように ASA が設定されているかどうかに関係なく、ASA はそのパケットをドロップします。

- End of Options List（EOOL）または IP Option 0：このオプションにはゼロ バイトが 1 つだけ含まれており、オプションのリストの終わりを示すために、すべてのオプションの末尾に表示されます。これは、ヘッダー長に基づくヘッダーの末尾とは一致しない場合があります。
- No Operation（NOP）または IP Option 1：IP ヘッダーの Options フィールドには、オプションを 0 個、1 個、またはそれ以上含めることができ、これがフィールド変数全体の長さになります。ただし、IP ヘッダーは 32 ビットの倍数である必要があります。すべてのオプションのビット数が 32 ビットの倍数でない場合、NOP オプションは、オプションを 32 ビット境界上に揃えるために、「内部パディング」として使用されます。
- Router Alert（RTRALT）または IP Option 20：このオプションは、中継ルータに対し、パケットの宛先がそのルータでない場合でも、パケットのコンテンツを検査するよう通知します。このインスペクションは、RSVP を実装している場合に役に立ちます。同様のプロトコルは、パケットの配信パス上にあるルータでの比較的複雑な処理を必要とします。Router Alert オプションが含まれた RSVP パケットをドロップすると、VoIP の実装で問題が生じることがあります。

IP オプション インスペクションのデフォルト

IP オプション インスペクションは、_default_ip_options_map インスペクション ポリシー マップを使用して、デフォルトでイネーブルになります。

- Router Alert オプションは許可されます。
- その他のオプションを含むパケットはドロップされます。これには、サポートされていないオプションを含むパケットが含まれます。

IP オプション インスペクションの設定

IP オプション インスペクションはデフォルトでイネーブルになっています。デフォルト マップで許可されているもの以外の追加オプションが必要な場合にのみ、設定する必要があります。

手順

ステップ 1　「IP オプション インスペクション ポリシー マップの設定」（P.9-25）

ステップ 2　「IP オプション インスペクション サービス ポリシーの設定」（P.9-26）

IP オプション インスペクション ポリシー マップの設定

デフォルト以外の IP オプション インスペクションを実行する場合は、IP オプション インスペクション ポリシー マップを作成して、サポートされる各オプション タイプの処理方法を指定します。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にもインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [IP Options] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　許可するオプションを選択します。各オプション タイプの説明については、「インスペクションでサポートされる IP オプション」（P.9-24）を参照してください。

選択していないオプションを含むパケットはドロップされます。

ステップ 5　許可する各オプションについて、パケットを許可する前にオプションをクリアするかどうかを選択します。

オプションをクリアすると、インスペクションはパケットを送信する前にパケット ヘッダーからオプションを除去します。

ステップ 6　**[OK]** をクリックします。

これで、このインスペクション マップを IP オプション インスペクションのサービス ポリシーで使用できるようになります。

IP オプション インスペクション サービス ポリシーの設定

ASA のデフォルトのコンフィギュレーションには、すべてのインターフェイスにグローバルに適用される IP オプション インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- IP オプション インスペクション ルールがある場合、または IP オプション インスペクションを追加しているルールがある場合は、それを選択して、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別の IP オプション インスペクション ポリシー マップを使用する場合は、IP オプション インスペクションをディセーブルにしてから、新しい IP オプション インスペクション ポリシー マップ名で再度イネーブルにする必要があります。

a. [IP Options] チェックボックスをオフにします。

b. [OK] をクリックします。

c. [Apply] をクリックします。

d. この手順を繰り返して [Protocol Inspections] タブに戻ります。

ステップ 4　[IP Options] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した IP オプション インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「IP オプション インスペクション ポリシー マップの設定」（P.9-25）を参照してください。

b. [Select IP Options Inspect Map] ダイアログ ボックスの [OK] をクリックします。

ステップ 6　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

IP オプション インスペクションのモニタリング

以下の方法を使用して IP オプション インスペクションの結果をモニタリングできます。

- インスペクションによってパケットがドロップされるたびに、syslog 106012 が発行されます。メッセージではドロップの原因になったオプションが示されます。
- **show service-policy inspect ip-options** コマンドを使用して、各オプションの統計情報を表示します。

IPsec パススルー インスペクション

ここでは、IPsec パススルー インスペクション エンジンについて説明します。

- 「IPsec パススルー インスペクションの概要」（P.9-27）
- 「IPsec パススルー インスペクションの設定」（P.9-28）

IPsec パススルー インスペクションの概要

Internet Protocol Security（IPsec）は、データ ストリームの各 IP パケットを認証および暗号化することによって、IP 通信をセキュリティで保護するためのプロトコル スイートです。IPsec には、セッションの開始時、およびセッション中に使用される暗号キーのネゴシエーションの開始時に、エージェント間の相互認証を確立するためのプロトコルも含まれています。IPsec を使用して、ホスト（コンピュータ ユーザまたはサーバなど）のペア間、セキュリティ ゲートウェイ（ルータやファイアウォールなど）のペア間、またはセキュリティ ゲートウェイとホスト間のデータ フローを保護できます。

IPsec パススルー アプリケーション インスペクションは、IKE UDP ポート 500 接続に関連付けられた ESP（IP プロトコル 50）および AH（IP プロトコル 51）トラフィックを簡単に横断できます。このインスペクションは、冗長な ACL コンフィギュレーションを回避して ESP および AH トラフィックを許可し、タイムアウトと最大接続数を使用してセキュリティも確保します。

ESP または AH トラフィックの制限を指定するには、IPsec パススルーのポリシー マップを設定します。クライアントあたりの最大接続数と、アイドル タイムアウトを設定できます。

NAT および非 NAT トラフィックは許可されます。ただし、PAT はサポートされません。

IPsec パススルー インスペクションの設定

IPsec パススルー インスペクションはデフォルトではイネーブルになりません。IPsec パススルー インスペクションが必要な場合は設定する必要があります。

手順

ステップ 1　「IPsec パススルー インスペクション ポリシー マップの設定」（P.9-28）

ステップ 2　「IPsec パススルー インスペクション サービス ポリシーの設定」（P.9-29）

IPsec パススルー インスペクション ポリシー マップの設定

IPsec パススルー マップでは、IPsec パススルー アプリケーション インスペクションのデフォルト設定値を変更できます。IPsec パススルー マップを使用すると、アクセス リストを使用しなくても、特定のフローを許可できます。

コンフィギュレーションに含まれるデフォルト マップ _default_ipsec_passthru_map では、ESP 接続に対するクライアントごとの最大数は制限なしに設定され、ESP アイドル タイムアウトは 10 分に設定されます。異なる値が必要な場合、または AH 値を設定する必要がある場合にのみ、インスペクション ポリシー マップを設定する必要があります。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にもインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [IPsec Pass Through] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[IPsec Pass Through Inspect Map] ダイアログ ボックスの [Security Level] ビューで、必要なコンフィギュレーションと最もよく一致するレベルを選択します。

プリセット レベルの 1 つが要件と一致する場合は、これで完了です。[OK] をクリックし、残りの手順はスキップして、IPsec パススルー インスペクションのサービス ポリシー ルールでマップを使用します。

設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、手順を続けます。

ステップ 5　ESP および AH トンネルを許可するかどうかを選択します。

プロトコルごとに、各クライアントに許可される最大接続数およびアイドル タイムアウトも設定できます。

ステップ 6　[OK] をクリックします。

これで、このインスペクション マップを IPsec パススルー インスペクション サービス ポリシーで使用できるようになります。

IPsec パススルー インスペクション サービス ポリシーの設定

IPsec パススルー インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの IPsec ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで IPsec インスペクションを追加できます。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- IPsec パススルー インスペクション ルールがある場合、または IPsec パススルー インスペクションを追加しているルールがある場合は、それを選択して、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別のインスペクション ポリシー マップを使用する場合は、IPsec パススルー インスペクションをディセーブルにしてから、新しいインスペクション ポリシー マップ名で再度イネーブルにする必要があります。

a. [IPsec Pass Through] チェックボックスをオフにします。

b. [OK] をクリックします。

c. [Apply] をクリックします。

d. この手順を繰り返して [Protocol Inspections] タブに戻ります。

ステップ 4　[IPsec Pass Through] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した IPsec パススルー インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「IPsec パススルー インスペクション ポリシー マップの設定」（P.9-28）を参照してください。

b. [Select IPsec Pass Through Inspect Map] ダイアログ ボックスの [OK] をクリックします。

ステップ 6　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

IPv6 インスペクション

IPv6 インスペクションを使用すると、拡張ヘッダーに基づいて IPv6 トラフィックを選択的にログに記録したりドロップしたりできます。さらに、IPv6 インスペクションでは、IPv6 パケット内の拡張ヘッダーのタイプと順序が RFC 2460 に準拠しているかどうかも確認できます。

- 「IPv6 インスペクションのデフォルト」（P.9-30）
- 「IPv6 インスペクションの設定」（P.9-30）

IPv6 インスペクションのデフォルト

IPv6 インスペクションをイネーブルにし、インスペクション ポリシー マップを指定しないと、デフォルトの IPv6 インスペクション ポリシー マップが使用され、次のアクションが実行されます。

- 既知の IPv6 拡張ヘッダーのみを許可します。準拠しないパケットはドロップされ、ログに記録されます。
- RFC 2460 仕様で定義されている IPv6 拡張ヘッダーの順序を適用します。準拠しないパケットはドロップされ、ログに記録されます。
- ルーティング タイプ ヘッダーを含むパケットをドロップします。

IPv6 インスペクションの設定

IPv6 インスペクションはデフォルトではイネーブルになりません。IPv6 インスペクションが必要な場合は設定する必要があります。

手順

ステップ 1　「IPv6 インスペクション ポリシー マップの設定」（P.9-30）

ステップ 2　「IPv6 インスペクション サービス ポリシーの設定」（P.9-31）

IPv6 インスペクション ポリシー マップの設定

ドロップまたはロギングする拡張ヘッダーを指定するには、またはパケットの検証をディセーブルにするには、サービス ポリシーで使用される IPv6 インスペクション ポリシー マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [IPv6] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[Enforcement] タブをクリックし、既知の IPv6 拡張ヘッダーだけを許可するかどうか、または RFC 2460 で定義されている IPv6 拡張ヘッダーの順序を適用するかどうかを選択します。準拠しないパケットはドロップされ、ログに記録されます。

ステップ 5　（オプション）[Header Matches] タブをクリックし、IPv6 メッセージのヘッダーに基づいてドロップまたはログに記録するトラフィックを指定します。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b. 一致する IPv6 拡張ヘッダーを選択します。

- 認証（AH）認証ヘッダー。
- 宛先オプション ヘッダー。
- カプセル化セキュリティ ペイロード（ESP）ヘッダー。
- フラグメント ヘッダー。
- ホップバイホップ オプション ヘッダー。
- [Routing header]：1 つのヘッダー タイプ番号または番号の範囲を指定します。
- [Header Count]：パケットをドロップまたはログに記録しないで許可する拡張ヘッダーの最大数を指定します。
- [Routing header address count]：パケットをドロップまたはログに記録しないで許可するタイプ 0 ルーティング ヘッダー内のアドレスの最大数を指定します。

c. パケットをドロップするか、ログに記録するかを選択します。パケットをドロップする場合は、ロギングをイネーブルにすることもできます。

d. [OK] をクリックしてインスペクションを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 6　[IPv6 Inspect Map] ダイアログ ボックスの [OK] をクリックします。

これで、このインスペクション マップを IPv6 インスペクション サービス ポリシーで使用できるようになります。

IPv6 インスペクション サービス ポリシーの設定

IPv6 インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。デフォルトのグローバル インスペクション ポリシーを編集して IPv6 インスペクションを追加できます。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。

- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- IPv6 インスペクション ルールがある場合、または IPv6 インスペクションを追加しているルールがある場合は、それを選択して、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別の IPv6 インスペクション ポリシー マップを使用する場合は、IPv6 インスペクションをディセーブルにしてから、新しい IPv6 インスペクション ポリシー マップ名で再度イネーブルにする必要があります。

a. [IPv6] チェックボックスをオフにします。

b. [OK] をクリックします。

c. [Apply] をクリックします。

d. この手順を繰り返して [Protocol Inspections] タブに戻ります。

ステップ 4　[IPv6] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した IPv6 インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「IPv6 インスペクション ポリシー マップの設定」（P.9-30）を参照してください。

b. [Select IPv6 Inspect Map] ダイアログ ボックスの [OK] をクリックします。

ステップ 6　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

NETBIOS インスペクション

NETBIOS インスペクションはデフォルトでイネーブルになっています。NetBIOS インスペクション エンジンは、ASAの NAT コンフィギュレーションに基づいて、NetBIOS ネーム サービス（NBNS）パケット内の IP アドレスを変換します。必要に応じて、NetBIOS プロトコル違反をドロップまたはログに記録するポリシー マップを作成できます。

手順

ステップ 1　「インスペクション制御を追加するための NetBIOS インスペクション ポリシー マップの設定」（P.9-33）

ステップ 2　「NetBIOS インスペクション サービス ポリシーの設定」（P.9-33）

インスペクション制御を追加するための NetBIOS インスペクション ポリシー マップの設定

プロトコル違反のアクションを指定するには、NetBIOS インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、NETBIOS インスペクションをイネーブルにすると適用できます。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [NetBIOS] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[Check for Protocol Violations] を選択します。このオプションを選択しない場合、マップを作成する理由はありません。

ステップ 5　実行するアクションは、パケットのドロップまたはログ記録から選択します。パケットをドロップする場合は、ロギングをイネーブルにすることもできます。

ステップ 6　**[OK]** をクリックします。

NetBIOS インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

NetBIOS インスペクション サービス ポリシーの設定

NetBIOS アプリケーション インスペクションでは、NetBIOS ネーム サービス パケットおよび NetBIOS データグラム サービス パケットに埋め込まれている IP アドレスで NAT を実行します。また、プロトコル準拠チェックを行って、さまざまなフィールドの数や長さの整合性を確認します。

ASA のデフォルトの設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの NetBIOS インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- NetBIOS インスペクション ルールがある場合、または NetBIOS インスペクションを追加しているルールがある場合は、それを選択して、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　[NetBIOS] を選択します。

ステップ 4　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、デフォルト マップを使用するか、またはユーザが設定した NetBIOS インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「インスペクション制御を追加するための NetBIOS インスペクション ポリシー マップの設定」（P.9-33）を参照してください。

ステップ 5　[Select NetBIOS Inspect Map] ダイアログ ボックスの [OK] をクリックします。

ステップ 6　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

PPTP インスペクション

PPTP は、PPP トラフィックのトンネリングに使用されるプロトコルです。PPTP セッションは、1 つの TCP チャネルと通常 2 つの PPTP GRE トンネルで構成されます。TCP チャネルは、PPTP GRE トンネルのネゴシエートと管理に使用される制御チャネルです。GRE トンネルは、2 つのホスト間の PPP セッションを伝送します。

PPTP アプリケーション インスペクションは、イネーブルになると、PPTP プロトコル パケットを検査し、PPTP トラフィックを許可するために必要な GRE 接続と xlate をダイナミックに作成します。

具体的には、ASAは、PPTP のバージョン通知と発信コールの要求/応答シーケンスを検査します。RFC 2637 で定義されている PPTP バージョン 1 だけが検査されます。どちらかの側から通知されたバージョンがバージョン 1 でない場合、TCP 制御チャネルでのそれ以降のインスペクションはディセーブルになります。また、発信コールの要求と応答のシーケンスは追跡されます。接続と xlate は、後続のセカンダリ GRE データ トラフィックを許可するために、必要に応じてダイナミックに割り当てられます。

PPTP インスペクション エンジンは、PPTP トラフィックを PAT で変換できるように、イネーブルにする必要があります。また、PAT は、PPTP TCP 制御チャネルで修正バージョンの GRE（RFC 2637）がネゴシエートされた場合に限り、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE（RFC 1701、RFC 1702）には実行されません。

PPTP インスペクションをイネーブルにする方法については、「アプリケーション レイヤ プロトコル インスペクションの設定」（P.8-10）を参照してください。

SMTP および拡張 SMTP 検査

ESMTP インスペクションは、スパム、フィッシング、不正な形式のメッセージによる攻撃、バッファ オーバーフロー /アンダーフロー攻撃を検出します。また、アプリケーション セキュリティとプロトコル準拠により、正常な ESMTP メッセージだけを通し、各種の攻撃の検出や送受信者およびメール中継のブロックも行います。

ここでは、ESMTP インスペクション エンジンについて説明します。

- 「SMTP および拡張 SMTP（ESMTP）のインスペクションの概要」（P.9-35）
- 「ESMTP インスペクションのデフォルト」（P.9-36）
- 「ESMTP インスペクションの設定」（P.9-36）

SMTP および拡張 SMTP（ESMTP）のインスペクションの概要

ESMTP アプリケーション インスペクションを使用すると、ASAを通過できる SMTP コマンドの種類を制限し、モニタ機能を追加することによって、SMTP ベースの攻撃からより強固に保護できます。

ESMTP は SMTP プロトコルの拡張で、ほとんどの観点で SMTP に似ています。便宜上、このマニュアルでは、SMTP という用語を SMTP と ESMTP の両方に使用します。拡張 SMTP に対するアプリケーション インスペクション処理は、SMTP アプリケーション インスペクションに似ており、SMTP セッションのサポートが含まれています。拡張 SMTP セッションで使用するほとんどのコマンドは、SMTP セッションで使用するコマンドと同じですが、ESMTP セッションの方が大幅に高速で、配信ステータス通知など信頼性およびセキュリティに関するオプションが増えています。

拡張 SMTP アプリケーション インスペクションでは、AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS、および VRFY を含む拡張 SMTP コマンドに対するサポートが追加されています。ASAは、7 つの RFC 821 コマンド（DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET）をサポートするとともに、合計 15 の SMTP コマンドをサポートします。

その他の拡張 SMTP コマンド（ATRN、ONEX、VERB、CHUNKING など）、およびプライベート拡張はサポートされません。サポートされないコマンドは、内部サーバにより拒否される X に変換されます。この結果は、「500 Command unknown: 'XXX'」のようなメッセージで表示されます。不完全なコマンドは、廃棄されます。

ESMTP インスペクション エンジンは、文字「2」、「0」、「0」を除くサーバの SMTP バナーの文字をアスタリスクに変更します。復帰（CR）、および改行（LF）は無視されます。

SMTP インスペクションをイネーブルにする場合、次のルールに従わないと、対話型の SMTP に使用する Telnet セッションが停止することがあります。SMTP コマンドの長さは 4 文字以上にする必要があります。復帰と改行で終了する必要があります。次の応答を発行する前に現在の応答を待機する必要があります。

SMTP サーバは、数値の応答コード、およびオプションの可読文字列でクライアント要求に応答します。SMTP アプリケーション インスペクションは、ユーザが使用できるコマンドとサーバが返送するメッセージを制御し、その数を減らします。SMTP インスペクションは、次の 3 つの主要なタスクを実行します。

- SMTP 要求を 7 つの基本 SMTP コマンドと 8 つの拡張コマンドに制限します。
- SMTP コマンド応答シーケンスをモニタします。
- 監査証跡の生成：メール アドレス内に埋め込まれている無効な文字が置き換えられたときに、監査レコード 108002 を生成します。詳細については、RFC 821 を参照してください。

SMTP インスペクションでは、次の異常な署名がないかどうか、コマンドと応答のシーケンスをモニタします。

- 切り捨てられたコマンド
- 不正なコマンド終端（<CR><LR> で終了していない）
- MAIL コマンドと RCPT コマンドでは、メールの送信者と受信者が指定されます。異常な文字がないか、メール アドレスがスキャンされます。縦棒（|）は削除され（ブランクに変更されます）、「<」および「>」はメール アドレスを定義する場合にのみ許可されます（「>」より前に「<」がある必要があります）。
- SMTP サーバによる不意の移行
- 未知のコマンドに対しては、ASA はパケット内のすべての文字を X に変更します。この場合、サーバがクライアントに対してエラー コードを生成します。パケット内が変更されるため、TCP チェックサムの再計算または調整が必要になります。

- TCP ストリーム編集
- コマンド パイプライン

ESMTP インスペクションのデフォルト

ESMTP インスペクションは、_default_esmtp_map インスペクション ポリシー マップを使用して、デフォルトでイネーブルになります。

- サーバ バナーはマスクされます。
- 暗号化されたトラフィックが検査されます。
- 送信側と受信側のアドレスの特殊文字は認識されず、アクションは実行されません。
- コマンド行の長さが 512 より大きい接続は、ドロップされてログに記録されます。
- 受信者が 100 より多い接続は、ドロップされてログに記録されます。
- 本文の長さが 998 バイトより大きいメッセージはログに記録されます。
- ヘッダー行の長さが 998 より大きい接続は、ドロップされてログに記録されます。
- MIME ファイル名が 255 文字より長いメッセージは、ドロップされてログに記録されます。
- 「others」に一致する EHLO 応答パラメータはマスクされます。

ESMTP インスペクションの設定

ESMTP インスペクションはデフォルトでイネーブルになっています。デフォルト インスペクション マップとは異なるプロセスが必要な場合にのみ、設定する必要があります。

手順

ステップ 1　「ESMTP インスペクション ポリシー マップの設定」（P.9-36）

ステップ 2　「ESMTP インスペクション サービス ポリシーの設定」（P.9-38）

ESMTP インスペクション ポリシー マップの設定

メッセージがパラメータに違反したときのアクションを指定するには、ESMTP インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、ESMTP インスペクションをイネーブルにすると適用できます。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [ESMTP] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。

- 内容を表示するマップを選択します。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[ESMTP Inspect Map] ダイアログ ボックスの [Security Level] ビューで、必要なコンフィギュレーションと最もよく一致するレベルを選択します。

プリセット レベルの 1 つが要件と一致する場合は、これで完了です。[OK] をクリックし、残りの手順をスキップして、ESMTP インスペクションのサービス ポリシー ルールでマップを使用します。

設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、手順を続けます。

ヒント　[MIME File Type Filtering] ボタンはファイル タイプのインスペクションを設定するためのショートカットです。これについては後で説明します。

ステップ 5　[Parameters] タブをクリックし、必要なオプションを設定します。

- [Mask Server Banner]：ESMTP サーバからのバナーをマスクするかどうか。
- [Encrypted Packet Inspection]：インスペクションなしで ESMTP over TLS（暗号化された接続）を許可するかどうか。必要に応じて、暗号化された接続をログに記録できます。

ステップ 6　[Filtering] タブをクリックし、必要なオプションを設定します。

- [Configure mail relay]：メール中継のドメイン名を指定します。接続をドロップし、必要に応じてログに記録できます。または、ログへの記録だけを行うこともできます。
- [Check for special characters]：電子メールの送信者または受信者アドレスに特殊文字パイプ(|)、バック クォート、NUL が含まれるメッセージに対して実行するアクションを指定します。接続をドロップし、必要に応じてログに記録できます。または、ログへの記録だけを行うこともできます。

ステップ 7　[Inspections] タブをクリックして、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。次に、基準を設定します。

- [Body Length]：ESMTP 本文メッセージの長さが指定したバイト数より大きいメッセージと一致します。
- [Body Line Length]：ESMTP 本文メッセージの行の長さが指定したバイト数より大きいメッセージと一致します。
- [Commands]：メッセージ内のコマンド動詞と一致します。次のコマンドの 1 つ以上を指定できます。auth、data、ehlo、etrn、helo、help、mail、noop、quit、rcpt、rset、saml、soml、vrfy。
- [Command Recipient Count]：受信者の数が指定した値より大きいメッセージと一致します。
- [Command Line Length]：コマンド動詞の行の長さが指定したバイト数より大きいメッセージと一致します。

- [EHLO Reply Parameters]：ESMTP EHLO 応答パラメータと一致します。次のパラメータの 1 つ以上を指定できます。8bitmime、auth、binaryname、checkpoint、dsn、etrn、others、pipelining、size、vrfy。
- [Header Length]：ESMTP ヘッダーの長さが指定したバイト数より大きいメッセージと一致します。
- [Header Line Length]：ESMTP ヘッダーの行の長さが指定したバイト数より大きいメッセージと一致します。
- [Header To: Fields Count]：ヘッダーの To フィールドの数が指定した値より大きいメッセージと一致します。
- [Invalid Recipients Count]：無効な受信者の数が指定した値より大きいメッセージと一致します。
- [MIME File Type] : MIME またはメディア ファイル タイプを、指定した正規表現または正規表現クラスと照合します。
- [MIME Filename Length]：ファイル名が指定したバイト数より大きいメッセージと一致します。
- [MIME Encoding] : MIME エンコーディング タイプと一致します。次のタイプの 1 以上を指定できます。7bit、8bit、base64、binary、others、quoted-printable。
- [Sender Address]：送信者の電子メール アドレスを、指定した正規表現または正規表現クラスと照合します。
- [Sender Address Length]：送信者のアドレスが指定したバイト数より大きいメッセージと一致します。

c. 接続のドロップ、リセット、またはログへの記録を行うかどうかを選択します。接続のドロップまたはリセットの場合は、ロギングをイネーブルまたはディセーブルにできます。コマンドおよび EHLO 応答パラメータの一致の場合、コマンドをマスクすることもできます。コマンドの一致の場合、1 秒間のパケット数制限を適用することもできます。

d. [OK] をクリックしてインスペクションを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 8　[ESMTP Inspect Map] ダイアログ ボックスの [OK] をクリックします。

ESMTP インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

ESMTP インスペクション サービス ポリシーの設定

ASA のデフォルトのコンフィギュレーションには、すべてのインターフェイスにグローバルに適用される ESMTP インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。

- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- ESMTP インスペクション ルールがある場合、または ESMTP インスペクションを追加しているルールがある場合は、それを選択して、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別のインスペクション ポリシー マップを使用する場合は、ESMTP インスペクションをディセーブルにしてから、新しいインスペクション ポリシー マップ名で再度イネーブルにする必要があります。

a. [ESMTP] チェックボックスをオフにします。
b. **[OK]** をクリックします。
c. [Apply] をクリックします。
d. この手順を繰り返して [Protocol Inspections] タブに戻ります。

ステップ 4　[ESMTP] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した ESMTP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「ESMTP インスペクション ポリシー マップの設定」（P.9-36）を参照してください。
b. [Select ESMTP Inspect Map] ダイアログ ボックスの [OK] をクリックします。

ステップ 6　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

TFTP インスペクション

TFTP インスペクションはデフォルトでイネーブルになっています。

TFTP は、RFC 1350 に記述されているように、TFTP サーバとクライアントの間のファイルの読み書きを行うための簡易プロトコルです。

ASAは、TFTP トラフィックを検査し、必要に応じてダイナミックに接続と変換を作成し、TFTP クライアントとサーバの間のファイル転送を許可します。具体的には、インスペクション エンジンは TFTP 読み取り要求（RRQ）、書き込み要求（WRQ）、およびエラー通知（ERROR）を検査します。

有効な読み取り要求（RRQ）または書き込み要求（WRQ）を受信すると、必要に応じて、ダイナミックなセカンダリ チャネルと PAT 変換が割り当てられます。このセカンダリ チャネルは、これ以降 TFTP によってファイル転送またはエラー通知用に使用されます。

TFTP サーバだけがセカンダリ チャネル経由のトラフィックを開始できます。また、TFTP クライアントとサーバの間に存在できる不完全なセカンダリ チャネルは 1 つまでです。サーバからのエラー通知があると、セカンダリ チャネルは閉じます。

TFTP トラフィックのリダイレクトにスタティック PAT が使用されている場合は、TFTP インスペクションをイネーブルにする必要があります。

TFTP インスペクションをイネーブルにする方法については、「アプリケーション レイヤ プロトコル インスペクションの設定」（P.8-10）を参照してください。

CHAPTER 10

音声とビデオのプロトコルのインスペクション

ここでは、音声およびビデオ プロトコルのアプリケーション インスペクションについて説明します。特定のプロトコルにインスペクションを使用する理由に関する基本情報については、「アプリケーション レイヤ プロトコル インスペクションの準備」（P.8-1）を参照してください。

- 「CTIQBE インスペクション」（P.10-1）
- 「H.323 インスペクション」（P.10-2）
- 「MGCP インスペクション」（P.10-9）
- 「RTSP インスペクション」（P.10-13）
- 「SIP インスペクション」（P.10-17）
- 「Skinny（SCCP）インスペクション」（P.10-25）
- 「音声とビデオのプロトコル インスペクションの履歴」（P.10-29）

CTIQBE インスペクション

CTIQBE プロトコル インスペクションは、NAT、PAT、および双方向 NAT をサポートします。これによって、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが Cisco CallManager と連動し、ASA を越えてコール セットアップを行えるようになります。

TAPI と JTAPI は、多くの Cisco VoIP アプリケーションで使用されます。CTIQBE は、Cisco TSP が Cisco CallManager と通信するために使用されます。

CTIQBE インスペクションをイネーブルにする方法については、「アプリケーション レイヤ プロトコル インスペクションの設定」（P.8-10）を参照してください。

- 「CTIQBE インスペクションの制限事項」（P.10-1）

CTIQBE インスペクションの制限事項

CTIQBE アプリケーション インスペクションの使用時に適用される制限を次にまとめます。

- CTIQBE アプリケーション インスペクションは、**alias** コマンドを使用するコンフィギュレーションをサポートしません。
- CTIQBE コールのステートフル フェールオーバーはサポートされていません。

- CTIQBE インスペクションをデバッグする 、メッセージの送信が遅れて、リアルタイム環境のパフォーマンスに影響を与える可能性があります。このデバッグまたはログをイネーブルにし、ASA を介して Cisco IP SoftPhone でコール セットアップを完了できない場合は、Cisco IP SoftPhone の動作するシステムで Cisco TSP 設定のタイムアウト値を増やしてください。

次に、CTIQBE アプリケーション インスペクションを特定の事例で使用する際に、特別に注意が必要な事項をまとめます。

- 2 つの Cisco IP SoftPhone が異なる Cisco CallManager に登録されていて、各 CallManager が ASA の異なるインターフェイスに接続されている場合、これら 2 つの電話間のコールは失敗します。
- Cisco IP SoftPhone と比較して Cisco CallManager の方が高セキュリティ インターフェイス上に配置されている状態で、NAT または外部 NAT が Cisco CallManager IP アドレスに必要な場合、マッピングはスタティックである必要があります。Cisco IP SoftPhone では Cisco CallManager IP アドレスを PC 上の Cisco TSP コンフィギュレーションで明示的に指定することが必要なためです。
- PAT または外部 PAT の使用時に Cisco CallManager IP アドレスを変換する場合、Cisco IP SoftPhone を正常に登録させるには、TCP ポート 2748 を PAT（インターフェイス）アドレスと同じポートにスタティックにマッピングする必要があります。CTIQBE 受信ポート（TCP 2748）は固定されていて、Cisco CallManager、Cisco IP SoftPhone、Cisco TSP のいずれにおいてもユーザによる設定はできません。

H.323 インスペクション

ここでは、H.323 アプリケーション インスペクションについて説明します。

- 「H.323 インスペクションの概要」（P.10-2）
- 「H.323 の動作」（P.10-3）
- 「H.245 メッセージでの H.239 サポート」（P.10-4）
- 「H.323 インスペクションの制限事項」（P.10-4）
- 「H.323 インスペクションの設定」（P.10-5）
- 「H.323 および H.225 タイムアウト値の設定」（P.10-9）

H.323 インスペクションの概要

H.323 インスペクションは、Cisco CallManager や VocalTec Gatekeeper など、H.323 準拠のアプリケーションをサポートします。H.323 は、国際電気通信連合によって定義されている、LAN を介したマルチメディア会議用のプロトコル群です。ASA は、H.323 v3 機能の同一コール シグナリング チャネルでの複数コールを含めて、H.323 を Version 6 までサポートします。

H.323 インスペクションをイネーブルにした場合、ASA は、H.323 Version 3 で導入された機能である同一コール シグナリング チャネルでの複数コールをサポートします。この機能によってセットアップ時間が短縮され、ASA でのポート使用が減少します。

H.323 インスペクションの 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化形式で符号化されているため、ASA では ASN.1 デコーダを使用して H.323 メッセージを復号化します。
- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。RAS を使用すると、H.225 接続もダイナミックに割り当てることができます。

H.323 の動作

H.323 のプロトコルのコレクションは、合計で最大 2 つの TCP 接続と 4 ～ 8 つの UDP 接続を使用できます。FastConnect は 1 つの TCP 接続だけを使用し、RAS は登録、アドミッション、およびステータス用に 1 つの UDP 接続を使用します。

H.323 クライアントは、最初に TCP ポート 1720 を使用して、H.323 サーバへの TCP 接続を確立し、Q.931 コール セットアップを要求します。H.323 端末は、コール セットアップ プロセスの一部として、H.245 TCP 接続に使用するため、クライアントに 1 つのポート番号を供給します。H.323 ゲートキーパーが使用されている環境では、初期パケットは UDP を使用して送信されます。

H.323 インスペクションは、Q.931 TCP 接続をモニタして、H.245 ポート番号を決定します。H.323 端末が、FastConnect を使用していない場合は、ASA が H.225 メッセージのインスペクションに基づいて、H.245 接続をダイナミックに割り当てます。

（注） RAS を使用すると、H.225 接続もダイナミックに割り当てることができます。

各 H.245 メッセージ内で、H.323 エンドポイントが、後続の UDP データ ストリームに使用するポート番号を交換します。H.323 インスペクションは、H.245 メッセージを調査して、ポート番号を識別し、メディア交換用の接続をダイナミックに作成します。RTP はネゴシエートされたポート番号を使用し、RTCP はその次に高いポート番号を使用します。

H.323 制御チャネルは、H.225、H.245、および H.323 RAS を処理します。H.323 インスペクションでは、次のポートが使用されます。

- 1718：ゲートキーパー検出 UDP ポート
- 1719：RAS UDP ポート
- 1720：TCP 制御ポート

RAS シグナリング用に予約済み H.323 ポート 1719 のトラフィックを許可する必要があります。さらに、H.225 コール シグナリング用に、予約済み H.323 ポート 1720 のトラフィックを許可する必要があります。ただし、H.245 シグナリング ポートは、H.225 シグナリングのエンドポイント間でネゴシエートされます。H.323 ゲートキーパーの使用時、ASA は、ACF メッセージと RCF メッセージのインスペクションに基づいて H.225 接続を開きます。

H.225 メッセージを検査した後、ASA は H.245 チャネルを開き、H.245 チャネルで送信されるトラフィックも検査します。ASA を通過するすべての H.245 メッセージは、H.245 アプリケーション インスペクションを受けます。このインスペクションでは、埋め込み IP アドレスが変換され、H.245 メッセージでネゴシエートされたメディア チャネルが開かれます。

H.323 ITU 規準では、メッセージ長を定義する TPKT ヘッダーが最初に送信されてから、H.225 と H.245 が信頼できる接続上を送信されることが要求されています。TPKT ヘッダーは、必ずしも H.225 メッセージや H.245 メッセージと同一の TCP パケットで送信される必要はないため、ASA は、メッセージを正しく処理して復号化するために TPKT 長を記憶しておく必要があります。ASA は、次のメッセージに備えて、TPKT 長が含まれるレコードを接続ごとに保持します。

ASA でメッセージ内の IP アドレスに NAT を行う必要がある場合、チェックサム、UUIE 長、および TPKT（H.225 メッセージが入っている TCP パケットに含まれている場合）は変更されます。TPKT が別の TCP パケットで送信される場合、ASA がその TPKT へのプロキシ ACK を実行し、新しい TPKT を新しい長さで H.245 メッセージに追加します。

（注） ASA は、TPKT に対する ACK の代理処理では TCP オプションをサポートしていません。

H.323 インスペクションを受けるパケットが通る各 UDP 接続は、H.323 接続としてマークされ、[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインで設定された H.323 タイムアウト値でタイムアウトします。

（注）　ゲートキーパーがネットワーク内にある場合は、H.323 エンドポイント間のコール セットアップをイネーブルにできます。ASA には、RegistrationRequest/RegistrationConfirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開くオプションが含まれています。これらの RRQ/RCF メッセージはゲートキーパーとの間で送受信されるので、発信側エンドポイントの IP アドレスは不明で、ASA は発信元 IP アドレス/ポート 0/0 を通じてピンホールを開きます。デフォルトでは、このオプションは無効になっています。

H.245 メッセージでの H.239 サポート

ASA は、2 つの H.323 エンドポイントの間に存在します。2 つの H.323 エンドポイントが、スプレッドシート データなどのデータ プレゼンテーションを送受信できるようにテレプレゼンテーション セッションをセットアップするとき、ASA はエンドポイント間で H.239 ネゴシエーションが成功することを保証します。

H.239 は、H.300 シリーズ エンドポイントが 1 回のコールで追加ビデオ チャネルを開くことができる機能を提供する規格です。コールで、エンドポイント（ビデオ電話など）はビデオ用チャネルとデータ プレゼンテーション用チャネルを送信します。H.239 ネゴシエーションは H.245 チャネルで発生します。

ASA が追加メディア チャネル用とメディア制御チャネル用のピンホールを開きます。エンドポイントは、オープン論理チャネル メッセージ（OLC）を使用して新しいチャネルの作成を通知します。メッセージ拡張は H.245 バージョン 13 の一部です。

テレプレゼンテーション セッションの復号化と符号化は、デフォルトでイネーブルにされています。H.239 の符号化と復号化は ASN.1 コーダによって実行されます。

H.323 インスペクションの制限事項

H.323 インスペクションは、Cisco Unified Communications Manager（CUCM）7.0 でテストおよびサポートされています。CUCM 8.0 以上ではサポートされていません。H.323 インスペクションは、他のリリースおよび製品と連携できる場合があります。

H.323 アプリケーション インスペクションの使用に関して、次の既知の問題および制限があります。

- 完全にサポートされているのは、スタティック NAT だけです。スタティック PAT は、H.323 メッセージのオプション フィールドに埋め込まれた IP アドレスを正しく変換できないことがあります。この問題が発生した場合は、H.323 でスタティック PAT を使用しないでください。
- ダイナミック NAT または PAT ではサポートされません。
- 拡張 PAT ではサポートされません。
- 同じセキュリティ レベルのインターフェイス間の NAT ではサポートされません。
- 外部 NAT ではサポートされません。
- NAT64 ではサポートされません。

- NetMeeting クライアントが H.323 ゲートキーパーに登録し、同じく H.323 ゲートキーパーに登録されている H.323 ゲートウェイを呼び出そうとすると、接続は確立されますが、どちらの方向でも音声が聞こえません。この問題は、ASA の問題ではありません。
- ネットワーク スタティック アドレスを設定した場合、このネットワーク スタティック アドレスが第三者のネットマスクおよびアドレスと同じであると、すべてのアウトバウンド H.323 接続が失敗します。

H.323 インスペクションの設定

H.323 インスペクションは RAS、H.225、H.245 をサポートし、埋め込まれた IP アドレスとポートをすべて変換する機能を備えています。ステートのトラッキングとフィルタリングを実行し、インスペクション機能のアクティベーションをカスケードできます。H.323 インスペクションは、電話番号のフィルタリング、T.120 のダイナミック制御、H.245 のトンネル機能制御、HSI グループ、プロトコルのステート トラッキング、H.323 通話時間制限の適用、音声/ビデオ制御をサポートします。

H.323 インスペクションはデフォルトではイネーブルです。デフォルト以外の処理が必要な場合にのみ設定する必要があります。H.323 インスペクションをカスタマイズする場合は、次の手順に従います。

手順

ステップ 1　「H.323 インスペクション クラス マップの設定」（P.10-5）
ステップ 2　「H.323 インスペクション ポリシー マップの設定」（P.10-6）
ステップ 3　「H.323 インスペクションのサービス ポリシーの設定」（P.10-8）

H.323 インスペクション クラス マップの設定

オプションで H.323 インスペクションのクラス マップを作成し、H.323 インスペクションのトラフィック クラスを定義できます。もう 1 つのオプションでは、H.323 インスペクションのポリシー マップで直接トラフィック クラスを定義します。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な一致基準を作成でき、クラス マップを再利用できるという点です。

ヒント　以下で説明する手順に加えて、インスペクション マップまたはサービス ポリシーの作成中にもクラス マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Class Maps] > [H.323] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいクラス マップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　照合オプションとして [Match All] または [Match Any] を選択します。

[Match All] がデフォルトです。トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。[Match Any] は、少なくとも 1 つの基準に一致したトラフィックがクラス マップに一致することを意味します。

ステップ 5　一致テーブルでエントリを追加または編集して、一致基準を設定します。対象トラフィックを定義するために必要な数のエントリを追加します。

a. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）を選択します。

b. 一致基準を選択し、その値を定義します。

- [Called Party]：選択した正規表現または正規表現クラスに対して H.323 の着信側を照合します。
- [Calling Party]：選択した正規表現または正規表現クラスに対して H.323 の発信側を照合します。
- [Media Type]：メディア タイプ（音声、ビデオ、またはデータ）と照合します。

c. [OK] をクリックします。

ステップ 6　[H.323 Traffic Class Map] ダイアログ ボックスで [OK] をクリックします。

これで、H.323 インスペクション ポリシー マップでクラス マップを使用できるようになります。

H.323 インスペクション ポリシー マップの設定

ネットワークに対してデフォルトのインスペクション動作が十分でない場合は、H.323 インスペクション ポリシー マップを作成して H.323 インスペクションのアクションをカスタマイズできます。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にもインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [H.323] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。

- 内容を表示するマップを選択します。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[H.323 Inspect Map] ダイアログボックスの [Security Level] ビューで、目的の設定に最も一致するレベルを選択します。デフォルトのレベルは [Low] です。

プリセット レベルの 1 つが要件と一致する場合は、これで完了です。[OK] をクリックし、残りの手順はスキップして、H.323 インスペクションのサービス ポリシー ルールでマップを使用します。

ヒント　[Phone Number Filtering] ボタンは、着信側または発信側のインスペクションを設定するためのショートカットです。これについては、後で説明します。

ステップ 5　設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、次の操作を実行します。

a. [State Checking] タブをクリックし、RAS および H.225 メッセージの状態遷移のチェックをイネーブルにするかどうか選択します。

また、RCF メッセージをチェックして、RRQ メッセージ内の通話信号アドレスのピンホールを開くこともできます。これにより、ゲートキーパーがネットワーク内にある場合に H.323 エンドポイント間のコール セットアップがイネーブルになります。RegistrationRequest/RegistrationConfirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開くには、このオプションを使用します。これらの RRQ/RCF メッセージはゲートキーパーとの間で送受信されるので、発信側エンドポイントの IP アドレスは不明で、ASA は発信元 IP アドレス/ポート 0/0 を通じてピンホールを開きます。デフォルトでは、このオプションは無効になっています。

b. [Call Attributes] タブをクリックし、コールの制限時間（最大値は 1193 時間）を適用するかどうか、またはコールのセットアップ中に発信側番号と着信側番号のプレゼンスを強制するかどうかを選択します。

c. [Tunneling and Protocol Conformance] タブをクリックし、H.245 トンネリングをチェックするかどうかを選択します。接続をドロップするか、ロギングすることができます。

ピンホールに流れる RTP パケットがプロトコルに準拠していることをチェックするかどうかを選択することもできます。また、準拠をチェックする場合は、シグナリング交換に基づいてペイロードを音声またはビデオに限定するかどうかを選択できます。

ステップ 6　必要に応じて、[HSI Group Parameters] タブをクリックし、HSI グループを定義します。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しいグループを追加します。
- 既存のグループを選択し、[Edit] をクリックします。

b. グループ ID（0 ～ 2147483647）と HSI の IP アドレスを指定します。

c. HSI グループにエンドポイントを追加するには、IP アドレスを入力し、エンドポイントが ASA に接続するときに使用するインターフェイスを選択して、[Add>>] をクリックします。不要になったエンドポイントを削除します。グループあたり最大 10 個のエンドポイントを設定できます。

d. [OK] をクリックして、グループを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 7　[Inspections] タブをクリックして、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

トラフィック一致基準は、H.323 クラス マップをベースにするか、インスペクション マップで一致を直接設定するか、またはこの両方によって定義できます。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b. 基準を直接定義する場合は [Single Match] を選択し、基準を定義する H.323 クラス マップを選択する場合は [Multiple Match] を選択します（「H.323 インスペクション クラス マップの設定」（P.10-5）を参照）。

c. 基準をここで定義した場合は、基準の一致タイプとして [Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。次に、基準を以下のように設定します。

- [Called Party]：選択した正規表現または正規表現クラスに対して H.323 の着信側を照合します。
- [Calling Party]：選択した正規表現または正規表現クラスに対して H.323 の発信側を照合します。
- [Media Type]：メディア タイプ（音声、ビデオ、またはデータ）と照合します。

d. トラフィックの照合で実行するアクションを選択します。発信側または着信側を照合する場合は、パケットをドロップするか、接続をドロップするか、接続をリセットできます。メディア タイプの照合の場合、アクションは常にパケットのドロップです。このアクションではロギングをイネーブルにすることができます。

e. [OK] をクリックしてインスペクションを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 8　[H.323 Inspect Map] ダイアログ ボックスで [OK] をクリックします。

これで、このインスペクション マップを H.323 インスペクションのサービス ポリシーで使用できるようになります。

H.323 インスペクションのサービス ポリシーの設定

デフォルトの ASA 設定には、すべてのインターフェイスでグローバルに適用されるデフォルト ポートでの H.323、H.255、および RAS のインスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。

- H.323 インスペクション ルール、つまり H.323 インスペクションを追加しているルールがある場合は、そのルールを選択し、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　[H.323 H.255] および [H.323 RAS] を選択します。

ステップ 4　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、デフォルト マップを使用するか、設定した H.323 インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「H.323 インスペクション ポリシー マップの設定」（P.10-6）を参照してください。

マップをポリシーに割り当てるには、[Select H.323 Inspect Map] ダイアログ ボックスで [OK] をクリックします。

ステップ 5　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

H.323 および H.225 タイムアウト値の設定

[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ページで H.323/H.255 グローバル タイムアウト値を設定できます。H.255 シグナリング接続を閉じるまでの非アクティビティ間隔（デフォルトは 1 時間）または H.323 制御接続を閉じるまでの非アクティブ間隔（デフォルトは 5 分）を設定できます。

MGCP インスペクション

ここでは、MGCP アプリケーション インスペクションについて説明します。

- 「MGCP インスペクションの概要」（P.10-9）
- 「MGCP インスペクションの設定」（P.10-11）
- 「MGCP タイムアウト値の設定」（P.10-12）

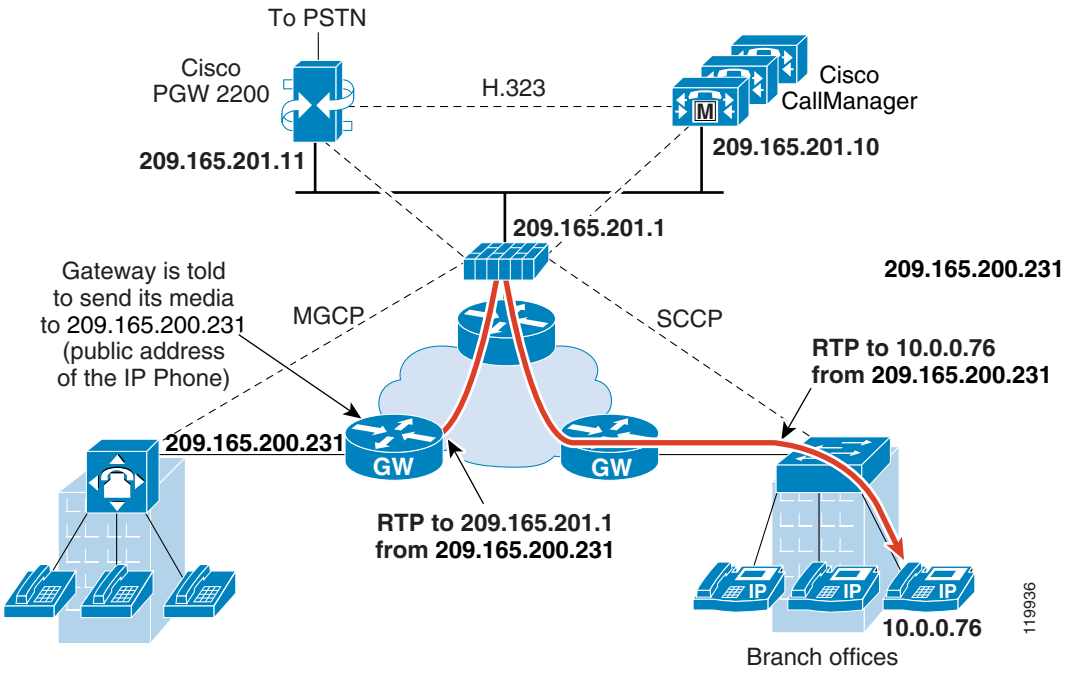
MGCP インスペクションの概要

MGCP は、メディア ゲートウェイ コントローラまたはコール エージェントと呼ばれる外部のコール制御要素からメディア ゲートウェイを制御するために使用するマスター /スレーブ プロトコルです。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。NAT および PAT を MGCP とともに使用すると、限られた外部（グローバル）アドレスのセットで、内部ネットワークの多数のデバイスをサポートできます。メディア ゲートウェイの例は次のとおりです。

- トランキング ゲートウェイ。電話ネットワークと Voice over IP ネットワークとの間のインターフェイスです。このようなゲートウェイは通常、大量のデジタル回線を管理します。
- 住宅用ゲートウェイ。従来のアナログ（RJ11）インターフェイスを Voice over IP ネットワークに提供します。住宅用ゲートウェイの例としては、ケーブル モデムやケーブル セットトップ ボックス、xDSL デバイス、ブロードバンド ワイヤレス デバイスなどがあります。
- ビジネス ゲートウェイ。従来のデジタル PBX（構内交換機）インターフェイスまたは統合 soft PBX インターフェイスを Voice over IP ネットワークに提供します。

MGCP メッセージは UDP を介して送信されます。応答はコマンドの送信元アドレス（IP アドレスと UDP ポート番号）に返送されますが、コマンド送信先と同じアドレスからの応答は到達しない場合があります。これは、複数のコール エージェントがフェールオーバー コンフィギュレーションで使用されているときに、コマンドを受信したコール エージェントが制御をバックアップ コール エージェントに引き渡し、バックアップ コール エージェントが応答を送信する場合に起こる可能性があります。次の図は、NAT と MGCP を使用する方法を示しています。

図 10-1　NAT と MGCP の使用



MGCP エンドポイントは、物理または仮想のデータ送信元および宛先です。メディア ゲートウェイには、他のマルチメディア エンドポイントとのメディア セッションを確立して制御するために、コール エージェントが接続を作成、変更、および削除できるエンドポイントが含まれています。また、コール エージェントは、特定のイベントを検出してシグナルを生成するようにエンドポイントに指示できます。エンドポイントは、サービス状態の変化を自動的にコール エージェントに伝達します。

- 通常、ゲートウェイは UDP ポート 2427 をリッスンしてコール エージェントからのコマンドを受信します。
- コール エージェントがゲートウェイからのコマンドを受信するポート。通常、コール エージェントは UDP ポート 2727 をリッスンしてゲートウェイからコマンドを受信します。

（注）　MGCP インスペクションでは、MGCP シグナリングと RTP データで異なる IP アドレスを使用することはサポートされていません。一般的かつ推奨される方法は、ループバック IP アドレスや仮想 IP アドレスなどの復元力のある IP アドレスから RTP データを送信することです。ただし、ASA は、MGCP シグナリングと同じアドレスから RTP データを受信する必要があります。

MGCP インスペクションの設定

MGCP インスペクションをイネーブルにするには、次のプロセスを使用します。

手順

ステップ 1　「インスペクション制御を追加するための MGCP インスペクション ポリシー マップの設定」（P.10-11）

ステップ 2　「MGCP インスペクションのサービス ポリシーの設定」（P.10-12）

インスペクション制御を追加するための MGCP インスペクション ポリシー マップの設定

ASA がピンホールを開く必要のあるコール エージェントとゲートウェイがネットワークに複数ある場合、MGCP マップを作成します。作成した MGCP マップは、MGCP インスペクションをイネーブルにすると適用できます。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [MGCP] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　（オプション）[Command Queue] タブをクリックし、MGCP コマンド キューで使用できるコマンドの最大数を指定します。デフォルトは 200 で、使用できる範囲は 1 ～ 2147483647 です。

ステップ 5　[Gateways and Call Agents] タブをクリックし、マップのゲートウェイとコール エージェントのグループを設定します。

a. [Add] をクリックして新しいグループを作成するか、グループを選択して [Edit] をクリックします。

b. コール エージェント グループの**グループ ID** を入力します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。0 ～ 2147483647 の範囲の値を指定できます。

c. 関連付けられているコール エージェントによって制御されるメディア ゲートウェイの IP アドレスをグループに追加するには、それらの IP アドレスを [Gateway to Be Added] に入力し、[Add>>] をクリックします。使用しなくなったゲートウェイを削除します。

メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（UDP 2727）に送信します。

d. MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを追加するには、それらの IP アドレスを [Call Agent to Be Added] に入力し、[Add>>] をクリックします。不要になったエージェントを削除します。

通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（UDP 2427）に送信します。

e. [MGCP Group] ダイアログ ボックスで [OK] をクリックします。必要に応じてプロセスを繰り返し、その他のグループを追加します。

ステップ 6　[MGCP Inspect Map] ダイアログ ボックスで [OK] をクリックします。

これで、このインスペクション マップを MGCP インスペクションのサービス ポリシーで使用できるようになります。

MGCP インスペクションのサービス ポリシーの設定

MGCP インスペクションは、デフォルトのインスペクション ポリシーでイネーブルになっていないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトのインスペクション クラスにはデフォルトの MGCP ポートが含まれるため、デフォルトのグローバル インスペクション ポリシーを編集して MGCP インスペクションを追加するだけで済みます。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- MGCP インスペクション ルール、つまり RTSP インスペクションを追加しているルールがある場合は、そのルールを選択し、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　[MGCP] を選択します。

ステップ 4　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、デフォルト マップを使用するか、設定した MGCP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「インスペクション制御を追加するための MGCP インスペクション ポリシー マップの設定」（P.10-11）を参照してください。

ポリシー マップを割り当てるには、[Select MGCP Inspect Map] ダイアログボックスで [OK] をクリックします。

ステップ 5　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

MGCP タイムアウト値の設定

[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ページで複数の MGCP グローバル タイムアウト値を設定できます。MGCP メディア接続を閉じるまでの非アクティブ間隔を設定できます（デフォルトは 5 分）。PAT xlate のタイムアウトも設定できます（30 秒）。

RTSP インスペクション

ここでは、RTSP アプリケーション インスペクションについて説明します。

- 「RTSP インスペクションの概要」（P.10-13）
- 「RealPlayer 設定要件」（P.10-13）
- 「RSTP インスペクションの制限事項」（P.10-14）
- 「RTSP インスペクションの設定」（P.10-14）

RTSP インスペクションの概要

RTSP インスペクション エンジンを使用することにより、ASA は RTSP パケットを通過させることができます。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV の各接続で使用されます。

（注）　Cisco IP/TV の場合、RTSP TCP ポート 554 および 8554 を使用します。

RTSP アプリケーションは、制御チャネルとしての TCP（例外的に UDP）とともに予約済みポート 554 を使用します。ASA は、RFC 2326 に準拠して、TCP だけをサポートします。この TCP 制御チャネルは、クライアント上で設定されているトランスポート モードに応じて、音声/ビデオ トラフィックの送信に使用されるデータ チャネルのネゴシエーションに使用されます。

サポートされている RDT トランスポートは、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、x-pn-tng/udp です。

ASA は、ステータス コード 200 の SETUP 応答メッセージを解析します。SETUP 応答メッセージが、インバウンド方向に移動している場合、サーバは ASA との相対位置関係で外部に存在することになるため、サーバから着信する接続に対してダイナミック チャネルを開くことが必要になります。この応答メッセージがアウトバウンド方向である場合、ASA は、ダイナミック チャネルを開く必要はありません。

RFC 2326 では、クライアント ポートとサーバ ポートが、SETUP 応答メッセージ内に含まれていることは必要でないため、ASA では、状態を維持し、SETUP メッセージ内のクライアント ポートを記憶します。QuickTime が、SETUP メッセージ内にクライアント ポートを設定すると、サーバは、サーバ ポートだけで応答します。

RTSP インスペクションは、PAT またはデュアル NAT をサポートしていません。また、ASA は、RTSP メッセージが HTTP メッセージ内に隠される HTTP クローキングを認識できません。

RealPlayer 設定要件

RealPlayer を使用するときは、転送モードを正しく設定することが重要です。ASA では、サーバからクライアントに、またはその逆に **access-list** コマンドを追加します。RealPlayer の場合、[Options] > [Preferences] > [Transport] > [RTSP] [Settings] をクリックして転送モードを変更します。

RealPlayer で TCP モードを使用する場合は、[Use TCP to Connect to Server] チェックボックスおよび [Attempt to use TCP for all content] チェックボックスをオンにします。ASA で、インスペクション エンジンを設定する必要はありません。

RealPlayer で UDP モードを使用する場合、[Use TCP to Connect to Server] および [Attempt to use UDP for static content] チェック ボックスをオンにします。マルチキャストでの使用ができないライブ コンテンツについては、ASA で、**inspect rtsp** *port* コマンドを追加します。

RSTP インスペクションの制限事項

RSTP インスペクションには次の制限が適用されます。

- ASA は、マルチキャスト RTSP または UDP による RTSP メッセージをサポートしません。
- ASA には、RTSP メッセージが HTTP メッセージ内に隠されている HTTP クローキングを認識する機能はありません。
- 埋め込み IP アドレスが HTTP メッセージまたは RTSP メッセージの一部として SDP ファイル内に含まれているため、ASA は、RTSP メッセージに NAT を実行できません。パケットはフラグメント化できますが、ASA ではフラグメント化されたパケットに対して NAT を実行することはできません。
- Cisco IP/TV では、メッセージの SDP 部分に対して ASA が実行する変換の数は、Content Manager にあるプログラム リストの数に比例します（各プログラム リストには、少なくとも 6 個の埋め込み IP アドレスを含めることができます）。
- Apple QuickTime 4 または RealPlayer 用の NAT を設定できます。Cisco IP/TV は、ビューアと Content Manager が外部ネットワークにあり、サーバが内部ネットワークにあるときにだけ NAT を使用できます。

RTSP インスペクションの設定

RTSP インスペクションはデフォルトでイネーブルになっています。デフォルト以外の処理が必要な場合にのみ設定する必要があります。RTSP インスペクションをカスタマイズする場合は、次の手順に従います。

手順

ステップ 1　「RTSP インスペクションのクラス マップの設定」（P.10-14）

ステップ 2　「RTSP インスペクションのポリシー マップの設定」（P.10-15）

ステップ 3　「RTSP インスペクションのサービス ポリシーの設定」（P.10-17）

RTSP インスペクションのクラス マップの設定

オプションで RTSP インスペクションのクラス マップを作成し、RTSP インスペクションのトラフィック クラスを定義できます。もう 1 つのオプションでは、RTSP インスペクションのポリシー マップで直接トラフィック クラスを定義します。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な一致基準を作成でき、クラス マップを再利用できるという点です。

ヒント　以下で説明する手順に加えて、インスペクション マップまたはサービス ポリシーの作成中にもクラス マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Class Maps] > [RTSP] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいクラス マップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　照合オプションとして [Match All] または [Match Any] を選択します。

[Match All] がデフォルトです。トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。[Match Any] は、少なくとも 1 つの基準に一致したトラフィックがクラス マップに一致することを意味します。

ステップ 5　一致テーブルでエントリを追加または編集して、一致基準を設定します。対象トラフィックを定義するために必要な数のエントリを追加します。

a. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

b. 一致基準を選択し、その値を定義します。

- [URL Filter]：選択した正規表現または正規表現クラスに対して URL を照合します。
- [Request Method]：announce、describe、get_parameter、options、pause、play、record、redirect、setup、set_parameters、teardown のいずれかの要求方式と照合します。

c. [OK] をクリックします。

ステップ 6　[RTSP Traffic Class Map] ダイアログボックスで [OK] をクリックします。

これで、RTSP インスペクション ポリシー マップでクラス マップを使用できるようになります。

RTSP インスペクションのポリシー マップの設定

ネットワークに対してデフォルトのインスペクション動作が十分でない場合は、RTSP インスペクション ポリシー マップを作成して RTSP インスペクションのアクションをカスタマイズできます。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にもインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [RTSP] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを選択し、[Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[Parameters] タブをクリックし、必要なオプションを設定します。

- [Enforce Reserve Port Protection]：メディア ポート ネゴシエーション中の予約済みポートの使用を制限するかどうか。
- [Maximum URL Length]：メッセージで使用できる URL の最大長（0 ～ 6000）。

ステップ 5　[Inspections] タブをクリックして、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

トラフィック一致基準は、RTSP クラス マップをベースにするか、インスペクション マップで一致を直接設定するか、またはこの両方によって定義できます。

a. 次のいずれかを実行します。
   - [Add] をクリックして、新しい基準を追加します。
   - 既存の基準を選択し、[Edit] をクリックします。
b. 基準を直接定義する場合は [Single Match] を選択し、基準を定義する RTSP クラス マップを選択する場合は [Multiple Match] を選択します（「RTSP インスペクションのクラス マップの設定」（P.10-14）を参照）。
c. 基準をここで定義した場合は、基準の一致タイプとして [Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。次に、基準を以下のように設定します。
   - [URL Filter]：選択した正規表現または正規表現クラスに対して URL を照合します。
   - [Request Method]：announce、describe、get_parameter、options、pause、play、record、redirect、setup、set_parameters、teardown のいずれかの要求方式と照合します。
d. トラフィックの照合で実行するアクションを選択します。URL の照合の場合は、接続をドロップするかロギングし、ドロップした接続のロギングをイネーブルにすることができます。要求方式の照合の場合は、レート制限（パケット/秒）を適用できます。
e. [OK] をクリックしてインスペクションを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 6　[RTSP Inspect Map] ダイアログ ボックスで [OK] をクリックします。

これで、このインスペクション マップを RTSP インスペクションのサービス ポリシーで使用できるようになります。

RTSP インスペクションのサービス ポリシーの設定

デフォルトの ASA 設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの RTSP インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- RTSP インスペクション ルール、つまり RTSP インスペクションを追加しているルールがある場合は、そのルールを選択し、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　[RTSP] を選択します。

ステップ 4　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、デフォルト マップを使用するか、設定した RTSP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「RTSP インスペクションのポリシー マップの設定」（P.10-15）を参照してください。

ポリシー マップを割り当てるには、[Select RTSP Inspect Map] ダイアログ ボックスで [OK] をクリックします。

ステップ 5　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

SIP インスペクション

SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、およびインスタント メッセージングに広く使用されているプロトコルです。テキストベースの性質とその柔軟性により、SIP ネットワークは数多くのセキュリティ脅威にさらされます。

SIP アプリケーション インスペクションでは、メッセージ ヘッダーおよび本文のアドレス変換、ポートの動的なオープン、および基本的な健全性チェックが行われます。SIP メッセージの健全性を実現するアプリケーション セキュリティおよびプロトコルへの準拠と、SIP ベースの攻撃の検出もサポートされます。

SIP インスペクションはデフォルトでイネーブルになっています。これは、デフォルト以外の処理が必要な場合、または暗号化されたトラフィックのインスペクションをイネーブルにするために TLS プロキシを識別する場合にのみ設定する必要があります。ここでは、SIP インスペクションについてより詳細に説明します。

- 「SIP インスペクションの概要」（P.10-18）
- 「SIP インスペクションの制限事項」（P.10-18）
- 「SIP インスタント メッセージ」（P.10-19）

- 「デフォルトの SIP インスペクション」（P.10-20）
- 「SIP インスペクションの設定」（P.10-20）
- 「SIP タイムアウト値の設定」（P.10-25）

SIP インスペクションの概要

IETF で定義されている SIP により、特に 2 者間の音声会議などのコール処理セッション（「コール」）が使用可能になります。SIP は、コール シグナリング用の SDP で動作します。SDP は、メディア ストリーム用のポートを指定します。SIP を使用することにより、ASA は SIP VoIP ゲートウェイおよび VoIP プロキシ サーバをサポートできます。SIP と SDP の定義は、次の RFC に記載されています。

- SIP：Session Initiation Protocol、RFC 3261
- SDP：Session Description Protocol、RFC 2327

ASA 経由の SIP コールをサポートする場合は、シグナリング メッセージは予約済みの宛先ポート（UDP/TCP 5060）経由で送信され、メディア ストリームはダイナミックに割り当てられるため、メディア接続アドレスのシグナリング メッセージ、メディア ポート、およびメディアの初期接続を検査する必要があります。また、SIP は、IP パケットのユーザデータ部分に IP アドレスを埋め込みます。ASA がサポートする SIP 要求 URI の最大長は 255 であることに注意してください。

SIP インスペクションの制限事項

SIP インスペクションは、埋め込まれた IP アドレスに NAT を適用します。ただし、送信元と宛先両方のアドレスを変換するように NAT を設定している場合、外部アドレス（「trying」応答メッセージの SIP ヘッダー内の「from」）は書き換えられません。そのため、宛先アドレスの変換を回避するように SIP トラフィックを使用している場合は、オブジェクト NAT を使用する必要があります。

PAT を SIP で使用する場合、次の制限事項が適用されます。

- ASA で保護されているネットワークの SIP プロキシにリモート エンドポイントを登録しようとすると、次のような一定の条件下で登録が失敗します。
  - PAT がリモート エンドポイント用に設定されている。
  - SIP レジストラ サーバが外部ネットワークにある。
  - エンドポイントからプロキシ サーバに送信された REGISTER メッセージの接続先フィールドにポートが設定されていない。
- SDP 部分の所有者/作成者フィールド（o=）の IP アドレスが接続フィールド（c=）の IP アドレスと異なるパケットを SIP デバイスが送信すると、o= フィールドの IP アドレスが正しく変換されない場合があります。これは、o= フィールドでポート値を提供しない SIP プロトコルの制限によるものです。
- PAT を使用する場合は、ポートを持たない内部 IP アドレスを含む SIP ヘッダー フィールドは変換されない可能性があるため、内部 IP アドレスが外部に漏れます。この漏出を避けるには、PAT の代わりに NAT を設定します。

SIP インスタント メッセージ

インスタント メッセージとは、ほぼリアルタイムにユーザ間でメッセージを転送することです。SIP は、Windows Messenger RTC Client バージョン 4.7.0105 を使用する Windows XP のチャット機能のみをサポートします。次の RFC で定義されているように、MESSAGE/INFO 方式および 202 Accept 応答を使用して IM をサポートします。

- Session Initiation Protocol（SIP）Specific Event Notification、RFC 3265
- Session Initiation Protocol（SIP）Extension for Instant Messaging、RFC 3428

MESSAGE/INFO 要求は、登録または加入の後、任意の時点で着信する可能性があります。たとえば、2 人のユーザはいつでもオンラインになる可能性がありますが、何時間もチャットをすることはありません。そのため、SIP インスペクション エンジンは、設定されている SIP タイムアウト値に従ってタイムアウトするピンホールを開きます。この値は、登録継続時間よりも 5 分以上長く設定する必要があります。登録継続時間は Contact Expires 値で定義し、通常 30 分です。

MESSAGE/INFO 要求は、通常、ポート 5060 以外の動的に割り当てられたポートを使用して送信されるため、SIP インスペクション エンジンを通過する必要があります。

（注） チャット機能のみがサポートされています。ホワイトボード、ファイル転送、アプリケーション共有はサポートされていません。RTC Client 5.0 はサポートされていません。

SIP インスペクションは、テキストベースの SIP メッセージを変換し、メッセージの SDP 部分の内容長を再計算した後、パケット長とチェックサムを再計算します。また、エンドポイントが受信すべきアドレスまたはポートとして、SIP メッセージの SDP 部分に指定されたポートに対するメディア接続をダイナミックに開きます。

SIP インスペクションでは、SIP ペイロードから取得したインデックス CALL_ID/FROM/TO を持つデータベースが使用されます。これらのインデックスにより、コール、送信元、宛先が識別されます。このデータベースには、SDP のメディア情報フィールド内で見つかったメディア アドレスとメディア ポート、およびメディア タイプが格納されます。1 つのセッションに対して、複数のメディア アドレスとポートが存在することが可能です。ASA は、これらのメディア アドレス/ポートを使用して、2 つのエンドポイント間に RTP/RTCP 接続を開きます。

初期コール セットアップ（INVITE）メッセージでは、予約済みポート 5060 を使用する必要があります。ただし、後続のメッセージにはこのポート番号がない場合もあります。SIP インスペクション エンジンはシグナリング接続のピンホールを開き、それらの接続を SIP 接続としてマークします。これは、SIP アプリケーションに到達した変換対象のメッセージに対して行われます。

コールのセットアップ時に、SIP セッションは、着信側エンドポイントから応答メッセージでメディア アドレスとメディア ポートを受信し、着信側エンドポイントがどの RTP ポートで受信するかを知らされるまで「一時的な」状態にあります。1 分以内に、応答メッセージの受信に障害があった場合は、シグナリング接続は切断されます。

最終的なハンドシェイクが行われると、コール状態はアクティブに移行し、シグナリング接続は、BYE メッセージの受信まで継続されます。

内部エンドポイントが、外部エンドポイントに発呼した場合、メディア ホールが、外部インターフェイスに対して開き、内部エンドポイントから送信された INVITE メッセージで指定された内部エンドポイントのメディア アドレスとメディア ポートに、RTP/RTCP UDP パケットが流れることが許可されます。内部インターフェイスに対する要求外の RTP/RTCP UDP パケットは、ASA のコンフィギュレーションで特別に許可されない限り、ASA を通過できません。

デフォルトの SIP インスペクション

SIP インスペクションはデフォルトでイネーブルになっており、次を含むデフォルトのインスペクション ポリシー マップを使用します。

- SIP インスタント メッセージ（IM）の拡張機能：イネーブル
- SIP トラフィック以外の SIP ポート使用：許可
- サーバとエンドポイントの IP アドレスの非表示：ディセーブル
- ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル
- 1 以上の宛先ホップ カウントを保証：イネーブル
- RTP 準拠：適用強制しない
- SIP 準拠：ステート チェックとヘッダー検証を実行しない

また、暗号化されたトラフィックのインスペクションはイネーブルになっていません。暗号化されたトラフィックを検査するには、TLS プロキシを設定する必要があります。

SIP インスペクションの設定

SIP アプリケーション インスペクションでは、メッセージ ヘッダーおよび本文のアドレス変換、ポートの動的なオープン、および基本的な健全性チェックが行われます。SIP メッセージの健全性を実現するアプリケーション セキュリティおよびプロトコルへの準拠と、SIP ベースの攻撃の検出もサポートされます。

SIP インスペクションはデフォルトでイネーブルになっています。これは、デフォルト以外の処理が必要な場合、または暗号化されたトラフィックのインスペクションをイネーブルにするために TLS プロキシを識別する場合にのみ設定する必要があります。SIP インスペクションをカスタマイズする場合は、次の手順に従います。

手順

ステップ 1　「SIP インスペクションのクラス マップの設定」（P.10-20）

ステップ 2　「SIP インスペクション ポリシー マップの設定」（P.10-22）

ステップ 3　「SIP インスペクションのサービス ポリシーの設定」（P.10-24）

SIP インスペクションのクラス マップの設定

オプションで SIP インスペクションのクラス マップを作成し、SIP のトラフィック クラスを定義できます。もう 1 つのオプションでは、SIP インスペクションのポリシー マップで直接トラフィック クラスを定義します。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な一致基準を作成でき、クラス マップを再利用できるという点です。

ヒント　以下で説明する手順に加えて、インスペクション マップまたはサービス ポリシーの作成中にもクラス マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Class Maps] > [SIP] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいクラス マップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　照合オプションとして [Match All] または [Match Any] を選択します。

[Match All] がデフォルトです。トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。[Match Any] は、少なくとも 1 つの基準に一致したトラフィックがクラス マップに一致することを意味します。

ステップ 5　一致テーブルでエントリを追加または編集して、一致基準を設定します。対象トラフィックを定義するために必要な数のエントリを追加します。

a. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

b. 一致基準を選択し、その値を定義します。

- [Called Party]：選択した正規表現または正規表現クラスに対して、To ヘッダーで指定された着信側を照合します。
- [Calling Party]：選択した正規表現または正規表現クラスに対して、From ヘッダーで指定された発信側を照合します。
- [Content Length]：指定された長さ（0 ～ 65536 バイト）より長い SIP コンテンツ ヘッダーを照合します。
- [Content Type]：Content Type ヘッダー、つまり SDP タイプか、選択した正規表現または正規表現クラスと一致するタイプを照合します。
- [IM Subscriber]：選択した正規表現または正規表現クラスに対して SIP IM サブスクライバを照合します。
- [Message Path]：選択した正規表現または正規表現クラスに対して SIP Via ヘッダーを照合します。
- [Request Method]：ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update のいずれかの SIP 要求方式を照合します。
- [Third-Party Registration]：選択した正規表現または正規表現クラスに対してサードパーティ登録の要求者を照合します。
- [URI Length]：指定された長さ（0 ～ 65536 バイト）を超えている、選択したタイプ（SIP または TEL）の SIP ヘッダーの URI を照合します。

c. [OK] をクリックします。

ステップ 6　[SIP Traffic Class Map] ダイアログ ボックスで [OK] をクリックします。

これで、SIP インスペクション ポリシー マップでクラス マップを使用できるようになります。

SIP インスペクション ポリシー マップの設定

ネットワークに対してデフォルトのインスペクション動作が十分でない場合は、SIP インスペクション ポリシー マップを作成して SIP インスペクションのアクションをカスタマイズできます。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にもインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [SIP] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[SIP Inspect Map] ダイアログ ボックスの [Security Level] ビューで、目的の設定に最も一致するレベルを選択します。デフォルトのレベルは [Low] です。

プリセット レベルの 1 つが要件と一致する場合は、これで完了です。[OK] をクリックし、残りの手順はスキップして、SIP インスペクションのサービス ポリシー ルールでマップを使用します。

ステップ 5　設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、次の操作を実行します。

a. [Filtering] タブをクリックし、SIP インスタント メッセージング（IM）拡張機能をイネーブルにするかどうか、または SIP ポート上の SIP 以外のトラフィックを許可するかどうかを選択します。

b. [IP Address Privacy] タブをクリックし、サーバとエンドポイントの IP アドレスを非表示にするかどうかを選択します。

c. [Hop Count] タブをクリックし、宛先までのホップ数が 0 を超えていることを確認するかどうかを選択します。これにより、宛先に到達するまで 0 にすることができない Max-Forwards ヘッダーの値がチェックされます。また、不適合なトラフィックに対して実行するアクション（パケットのドロップ、接続のドロップ、リセット、またはログ）と、ロギングをイネーブルまたはディセーブルのどちらにするかを選択する必要もあります。

d. [RTP Conformance] タブをクリックし、ピンホールに流れる RTP パケットがプロトコルに準拠していることをチェックするかどうかを選択します。また、準拠をチェックする場合は、シグナリング交換に基づいてペイロードを音声またはビデオに限定するかどうかを選択できます。

e. [SIP Conformance] タブをクリックし、状態遷移チェックとヘッダー フィールドの厳格な検証をイネーブルにするかどうかを選択します。選択したオプションごとに、不適合なトラフィックに対して実行するアクション（パケットのドロップ、接続のドロップ、リセット、またはログ）と、ロギングをイネーブルまたはディセーブルのどちらにするかを選択します。

f. [Field Masking] タブをクリックし、Alert-Info および Call-Info ヘッダーの SIP 以外の URI を検査するかどうか、User-Agent および Server ヘッダーのサーバおよびエンドポイントのソフトウェア バージョンを検査するかどうかを選択します。選択したオプションごとに、実行するアクション（マスクまたはロギング）と、ロギングをインネーブルまたはディセーブルのどちらにするかを選択します。

ステップ 6　[Inspections] タブをクリックして、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

トラフィック一致基準は、SIP クラス マップをベースにするか、インスペクション マップで一致を直接設定するか、またはこの両方によって定義できます。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b. 基準を直接定義する場合は [Single Match] を選択し、基準を定義する SIP クラス マップを選択する場合は [Multiple Match] を選択します（「SIP インスペクションのクラス マップの設定」（P.10-20）を参照）。

c. 基準をここで定義した場合は、基準の一致タイプとして [Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。次に、基準を以下のように設定します。

- [Called Party]：選択した正規表現または正規表現クラスに対して、To ヘッダーで指定された着信側を照合します。
- [Calling Party]：選択した正規表現または正規表現クラスに対して、From ヘッダーで指定された発信側を照合します。
- [Content Length]：指定された長さ（0 ～ 65536 バイト）より長い SIP コンテンツ ヘッダーを照合します。
- [Content Type]：Content Type ヘッダー、つまり SDP タイプか、選択した正規表現または正規表現クラスと一致するタイプを照合します。
- [IM Subscriber]：選択した正規表現または正規表現クラスに対して SIP IM サブスクライバを照合します。
- [Message Path]：選択した正規表現または正規表現クラスに対して SIP Via ヘッダーを照合します。
- [Request Method]：ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update のいずれかの SIP 要求方式を照合します。
- [Third-Party Registration]：選択した正規表現または正規表現クラスに対してサードパーティ登録の要求者を照合します。
- [URI Length]：指定された長さ（0 ～ 65536 バイト）を超えている、選択したタイプ（SIP または TEL）の SIP ヘッダーの URI を照合します。

d. 一致するトラフィックに対して実行するアクション（パケットのドロップ、接続のドロップ、リセット、ログ）と、ログをイネーブルまたはディセーブルのどちらにするかを選択します。「invite」および「register」に一致する要求方式の場合は、レート制限（パケット/秒）も適用できます。

e. [OK] をクリックしてインスペクションを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 7　[SIP Inspect Map] ダイアログ ボックスで [OK] をクリックします。

これで、このインスペクション マップを SIP インスペクションのサービス ポリシーで使用できるようになります。

SIP インスペクションのサービス ポリシーの設定

デフォルトの ASA 設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの SIP インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- SIP インスペクション ルール、つまり SIP インスペクションを追加しているルールがある場合は、そのルールを選択し、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　[SIP] を選択します。

ステップ 4　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した SIP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「SIP インスペクション ポリシー マップの設定」（P.10-22）を参照してください。

b. 暗号化された SIP トラフィックを検査する場合は、[Enable encrypted traffic inspection] を選択し、TLS プロキシを選択します（必要な場合は [Manage] をクリックして作成します）。

電話プロキシまたは UC-IME プロキシを選択してこれらのプロキシに TLS プロキシを関連付けることはできますが、この設定は推奨されません。電話プロキシまたは UC-IME プロキシに一度に割り当てることができるのは、1 つの TLS プロキシのみです。電話プロキシまたは UC-IME プロキシ インスペクションに複数のサービス ポリシー ルールを設定し、異なる TLS プロキシをそれらのルールに割り当てようとすると、ASDM は、電話プロキシと UC-IME インスペクションに設定されているその他のすべてのサービス ポリシー ルールが、最後に選択された TLS プロキシを使用するように変更されるという警告を表示します。

UC-IME プロキシ コンフィギュレーションでは、2 つの TLS プロキシ（インバウンド トラフィック用とアウトバウンド トラフィック用）が必要です。TLS プロキシを UC-IME プロキシに直接関連付けるのではなく、電話プロキシの場合のように、TLS プロキシは SIP インスペクション ルールを介して UC-IME プロキシに間接的に関連付けられます。

c. [Select SIP Inspect Map] ダイアログ ボックスで [OK] をクリックします。

ステップ 5　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

SIP タイムアウト値の設定

メディア接続は、接続がアイドル状態になってから 2 分以内に切断されます。ただし、これは設定可能なタイムアウトであり、時間間隔は変更することが可能です。

[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ページで複数の SIP グローバル タイムアウト値を設定できます。

Skinny（SCCP）インスペクション

ここでは、SCCP アプリケーション インスペクションについて説明します。

- 「SCCP インスペクションの概要」（P.10-25）
- 「Cisco IP Phone のサポート」（P.10-26）
- 「SCCP インスペクションの制限事項」（P.10-26）
- 「デフォルトの SCCP インスペクション」（P.10-26）
- 「SCCP（Skinny）インスペクションの設定」（P.10-27）

SCCP インスペクションの概要

Skinny（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境でも使用できます。Cisco CallManager と併用すると、SCCP クライアントは、H.323 準拠端末と同時使用できます。

ASA は、SCCP に対して PAT と NAT をサポートします。IP 電話で使用できるグローバル IP アドレスよりも IP 電話が多い場合は、PAT が必要です。Skinny アプリケーション インスペクションは、SCCP シグナリング パケットの NAT と PAT をサポートすることで、すべての SCCP シグナリング パケットとメディア パケットが ASA を通過できるようにします。

Cisco CallManager と Cisco IP Phone 間の通常のトラフィックは SCCP を使用しており、特別な設定をしなくても SCCP インスペクションによって処理されます。ASA は、TFTP サーバの場所を Cisco IP Phone とその他の DHCP クライアントに送信することで、DHCP オプション 150 および 66 もサポートします。Cisco IP Phone では、デフォルト ルートを設定する DHCP オプション 3 を要求に含めることもできます。

（注）　ASA は、SCCP プロトコル バージョン 22 以前が稼働している Cisco IP Phone からのトラフィックのインスペクションをサポートします。

Cisco IP Phone のサポート

Cisco CallManager が Cisco IP Phone と比べて高セキュリティ インターフェイスにあるトポロジでは、NAT が Cisco CallManager の IP アドレスに必要な場合、マッピングは**スタティック**である必要があります。これは、Cisco IP Phone では Cisco CallManager の IP アドレスをコンフィギュレーションで明示的に指定する必要があるためです。スタティック アイデンティティ エントリを使用すると、高セキュリティ インターフェイス上にある Cisco CallManager が Cisco IP Phone からの登録を受け付けるようにできます。

Cisco IP Phone では、TFTP サーバにアクセスして、Cisco CallManager サーバに接続するために必要な設定情報をダウンロードする必要があります。

TFTP サーバと比較して Cisco IP Phone の方が低セキュリティ インターフェイス上にある場合は、ACL を使用して UDP ポート 69 の保護された TFTP サーバに接続する必要があります。TFTP サーバに対してはスタティック エントリが必要ですが、識別スタティック エントリにする必要はありません。NAT を使用する場合、識別スタティック エントリは同じ IP アドレスにマッピングされます。PAT を使用する場合は、同じ IP アドレスとポートにマッピングされます。

Cisco IP Phone が TFTP サーバおよび Cisco CallManager と比べて*高*セキュリティ インターフェイス上にある場合、Cisco IP Phone が接続を開始できるようにする際に、ACL やスタティック エントリは必要ありません。

SCCP インスペクションの制限事項

内部の Cisco CallManager のアドレスが NAT または PAT 用に別の IP アドレスかポートを設定している場合、ASA は現在のところ TFTP を経由して転送するファイルの内容に対して NAT または PAT をサポートしていないため、外部の Cisco IP Phone 用の登録は失敗します。ASA は TFTP メッセージの NAT をサポートし、TFTP ファイル用にピンホールを開きますが、ASA は電話の登録中に TFTP によって転送された Cisco IP Phone のコンフィギュレーション ファイルに埋め込まれた Cisco CallManager の IP アドレスとポートを変換することはできません。

（注） ASA では、コール セットアップ中であるコール以外の SCCP コールのステートフル フェールオーバーはサポートされていません。

デフォルトの SCCP インスペクション

SCCP インスペクションは以下のデフォルト値を使用してデフォルトでイネーブルになります。

- 登録：適用強制しない
- メッセージの最大 ID：0x181
- プレフィックスの長さの最小値：4
- メディア タイムアウト：00:05:00
- シグナリング タイムアウト：01:00:00
- RTP 準拠：適用強制しない

また、暗号化されたトラフィックのインスペクションはイネーブルになっていません。暗号化されたトラフィックを検査するには、TLS プロキシを設定する必要があります。

SCCP（Skinny）インスペクションの設定

SCCP（Skinny）アプリケーション インスペクションでは、パケット データ内に埋め込まれている IP アドレスとポート番号の変換、およびピンホールの動的なオープンを実行します。また、追加のプロトコル準拠チェックと基本的なステート トラッキングも行います。

SCCP インスペクションはデフォルトではイネーブルです。これは、デフォルト以外の処理が必要な場合、または暗号化されたトラフィックのインスペクションをイネーブルにするために TLS プロキシを識別する場合にのみ設定する必要があります。SCCP インスペクションをカスタマイズする場合は、次の手順に従います。

手順

ステップ 1　「インスペクション制御を追加するための Skinny（SCCP）インスペクション ポリシー マップの設定」（P.10-27）

ステップ 2　「SCCP インスペクションのサービス ポリシーの設定」（P.10-28）

インスペクション制御を追加するための Skinny（SCCP）インスペクション ポリシー マップの設定

メッセージがパラメータに違反したときのアクションを指定するには、SCCP インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、SCCP インスペクションをイネーブルにすると適用できます。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [SCCP (Skinny)] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[SCCP (Skinny) Inspect Map] ダイアログ ボックスの [Security Level] ビューで、目的の設定に最も一致するレベルを選択します。デフォルトのレベルは [Low] です。

プリセット レベルの 1 つが要件と一致する場合は、これで完了です。[OK] をクリックし、残りの手順をスキップして、SCCP インスペクションのサービス ポリシー ルールでマップを使用します。

ステップ 5　設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、次の操作を実行します。

a.　[Parameters] タブをクリックし、次のオプションから選択します。

- [Enforce endpoint registration]：コールを発信または着信する前に Skinny エンドポイントを登録するかどうか。
- [Maximum Message ID]：許可される最大の SCCP ステーション メッセージ ID。デフォルトの最大値は 0x181 です。16 進数値は 0x0 ～ 0xffff です。

- [SCCP Prefix Length]：最大および最小の SCCP プレフィックス長。デフォルトの最小値は 4 で、デフォルトの最大値はありません。
- [Timeouts]：メディアおよびシグナリング接続のタイムアウトを設定するかどうか、およびそれらのタイムアウト値。デフォルトはメディアの場合は 5 分、シグナリングの場合は 1 時間です。

b. [RTP Conformance] タブをクリックし、ピンホールに流れる RTP パケットがプロトコルに準拠していることをチェックするかどうかを選択します。また、準拠をチェックする場合は、シグナリング交換に基づいてペイロードを音声またはビデオに限定するかどうかを選択できます。

ステップ 6　（オプション）[Message ID Filtering] タブをクリックし、SCCP メッセージのステーション メッセージ ID フィールドに基づいてドロップするトラフィックを指定します。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）を選択します。

c. [Value] フィールドで、0x0 ～ 0xffff の 16 進数のステーション メッセージ ID の値に基づいてトラフィックを指定します。1 つのメッセージ ID の値を入力するか、ID の範囲の開始値と終了値を入力します。

d. ロギングをイネーブルまたはディセーブルのどちらにするかを選択します。デフォルトのアクションは、常にパケットのドロップです。

e. [OK] をクリックして、フィルタを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 7　[SCCP (Skinny) Inspect Map] ダイアログ ボックスで [OK] をクリックします。

これで、このインスペクション マップを SCCP インスペクションのサービス ポリシーで使用できるようになります。

SCCP インスペクションのサービス ポリシーの設定

デフォルトの ASA 設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの SCCP インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- SCCP インスペクション ルール、つまり SCCP インスペクションを追加しているルールがある場合は、そのルールを選択し、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　[SCCP （Skinny）] を選択します。

ステップ 4　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した SCCP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「インスペクション制御を追加するための Skinny（SCCP）インスペクション ポリシー マップの設定」（P.10-27）を参照してください。

b. 暗号化された SCCP トラフィックを検査する場合は、[Enable encrypted traffic inspection] を選択し、TLS プロキシを選択します（必要な場合は [Manage] をクリックして作成します）。

ASA に設定されている電話機プロキシを使用して Skinny アプリケーション トラフィックを検査することもできますが、この設定は推奨されません。

c. [Select SCCP Inspect Map] ダイアログ ボックスで [OK] をクリックします。

ステップ 5　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

音声とビデオのプロトコル インスペクションの履歴

機能名	リリース	機能情報
IPv6 に対する SIP、SCCP、および TLS プロキシのサポート	9.3(1)	SIP、SCCP、および TLS プロキシ（SIP または SCCP を使用）を使用している場合、IPv6 トラフィックを検査できるようになりました。 変更された ASDM 画面はありません。

データベースおよびディレクトリ プロトコルのインスペクション

ここでは、データベースおよびディレクトリ プロトコルのアプリケーション インスペクションについて説明します。特定のプロトコルにインスペクションを使用する必要がある理由、およびインスペクション適用の方法全体については、「アプリケーション レイヤ プロトコル インスペクションの準備」（P.8-1）を参照してください。

- 「ILS インスペクション」（P.11-1）
- 「SQL*Net インスペクション」（P.11-2）
- 「Sun RPC インスペクション」（P.11-3）

ILS インスペクション

ILS インスペクション エンジンは、LDAP を使用してディレクトリ情報を ILS サーバと交換する Microsoft NetMeeting、SiteServer、および Active Directory の各製品に対して NAT をサポートします。

ASA は ILS に対して NAT をサポートします。NAT は、ILS または SiteServer Directory のエンドポイントの登録および検索で使用されます。LDAP データベースには IP アドレスだけが保存されるため、PAT はサポートされません。

LDAP サーバが外部にある場合、内部ピアが外部 LDAP サーバに登録された状態でローカルに通信できるように、検索応答に対して NAT を行うことを検討してください。このような検索応答では、最初に xlate が検索され、次に DNAT エントリが検索されて正しいアドレスが取得されます。これらの検索が両方とも失敗した場合、アドレスは変更されません。NAT 0（NAT なし）を使用していて、DNAT の相互作用を想定していないサイトの場合は、パフォーマンスを向上させるためにインスペクション エンジンをオフにすることをお勧めします。

ILS サーバが ASA 境界の内部にある場合は、さらに設定が必要なことがあります。この場合、外部クライアントが指定されたポート（通常は TCP 389）の LDAP サーバにアクセスするためのホールが必要となります。

（注） ILS トラフィック（H225 コール シグナリング）はセカンダリ UDP チャネルだけで発生するため、TCP 接続は一定間隔の間に TCP アクティビティがなければ切断されます。デフォルトでは、この間隔は 60 分です。この値は、TCP **timeout** コマンドを使用して調整できます。ASDM では、[Configuration] > [Firewall] > [Advanced] > [Global Timeout] ペインにあります。

ILS/LDAP はクライアント/サーバ モデルに従っており、セッションは 1 つの TCP 接続で処理されます。クライアントのアクションに応じて、このようなセッションがいくつか作成されることがあります。

接続ネゴシエーション時間中、クライアントからサーバに BIND PDU が送信されます。サーバから成功を示す BIND RESPONSE を受信すると、ILS Directory に対する操作を実行するためのその他の操作メッセージ（ADD、DEL、SEARCH、MODIFY など）が交換される場合があります。ADD REQUEST PDU および SEARCH RESPONSE PDU には、NetMeeting セッションを確立するために H.323（SETUP および CONNECT メッセージ）によって使用される、NetMeeting ピアの IP アドレスが含まれている場合があります。Microsoft NetMeeting v2.X および v3.X は、ILS をサポートしています。

ILS インスペクションでは、次の操作が実行されます。

- BER 復号化機能を使用して LDAP REQUEST PDU/RESPONSE PDU を復号化する。
- LDAP パケットを解析する。
- IP アドレスを抽出する。
- 必要に応じて IP アドレスを変換する。
- BER 符号化機能を使用して、変換後のアドレスが含まれる PDU を符号化する。
- 新しく符号化された PDU を元の TCP パケットにコピーする。
- TCP チェックサムとシーケンス番号の増分を調整する。

ILS インスペクションには、次の制限事項があります。

- 照会要求や応答はサポートされません。
- 複数のディレクトリのユーザは統合されません。
- 複数のディレクトリに複数の ID を持っている単一のユーザは NAT には認識されません。

ILS インスペクションをイネーブルする方法については、「アプリケーション レイヤ プロトコル インスペクションの設定」（P.8-10）を参照してください。

SQL*Net インスペクション

SQL*Net インスペクションはデフォルトでイネーブルになっています。

SQL*Net プロトコルは、さまざまなパケット タイプで構成されています。ASA はこれらのパケットを処理して、ASA のどちらの側の Oracle アプリケーションにも一貫性のあるデータ ストリームが表示されるようにします。

SQL*Net のデフォルトのポート割り当ては 1521 です。これは、Oracle が SQL*Net 用に使用している値ですが、構造化照会言語（SQL）の IANA ポート割り当てとは一致しません。

（注）　SQL 制御 TCP ポート 1521 と同じポートで SQL データ転送が行われる場合は、SQL*Net のインスペクションをディセーブルにします。SQL*Net インスペクションがイネーブルになっていると、セキュリティ アプライアンスはプロキシとして機能し、クライアントのウィンドウ サイズを 65000 から約 16000 に減らすため、データ転送の問題が発生します。

ASA は、すべてのアドレスを変換し、パケットを調べて、SQL*Net バージョン 1 用に開くすべての埋め込みポートを見つけます。

SQL*Net バージョン 2 の場合、データ長ゼロの REDIRECT パケットの直後に続くすべての DATA パケットまたは REDIRECT パケットはフィックスアップされます。

フィックスアップが必要なパケットには、埋め込みホスト アドレスおよびポート アドレスが次の形式で含まれています。

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL*Net バージョン 2 の各 TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker）は、NAT 対象のアドレスがあるかどうかがスキャンされません。また、インスペクションがパケット内に埋め込まれたポートにダイナミック接続を開くこともありません。

SQL*Net バージョン 2 の TNSFrame、Redirect パケット、および Data パケットは、ペイロードのデータ長がゼロの REDIRECT TNSFrame タイプの後に続く場合、開くポートおよび NAT 対象のアドレスがあるかどうかスキャンされます。データ長ゼロの Redirect メッセージが ASA を通過すると、後に続く Data メッセージまたは Redirect メッセージは変換対象でありポートはダイナミックに開かれると想定するフラグが、接続データ構造に設定されます。先行するパラグラフの TNS フレームのいずれかが Redirect メッセージの後に到着した場合、フラグはリセットされます。

SQL*Net インスペクション エンジンは、チェックサムを再計算し、IP および TCP の長さを変更し、新旧のメッセージの長さの差を使用してシーケンス番号と確認応答番号を再調整します。

SQL*Net バージョン 1 では、その他のすべての場合を想定しています。TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker、Redirect、Data）とすべてのパケットは、ポートおよびアドレスがあるかどうかスキャンされます。アドレスが変換され、ポート接続が開かれます。

SQL*Net インスペクションをイネーブルする方法については、「アプリケーション レイヤ プロトコル インスペクションの設定」（P.8-10）を参照してください。

Sun RPC インスペクション

この項では、Sun RPC アプリケーション インスペクションについて説明します。

- 「Sun RPC インスペクション」（P.11-3）
- 「許可された Sun RPC サービスの識別」（P.11-4）

Sun RPC インスペクション

Sun RPC インスペクション エンジンは、Sun RPC プロトコルのアプリケーション インスペクションをイネーブルまたはディセーブルにします。Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスはどのポート上でも実行できます。サーバ上の Sun RPC サービスにアクセスしようとするクライアントは、そのサービスが実行されているポートを知る必要があります。そのためには、予約済みポート 111 でポート マッパー プロセス（通常は rpcbind）に照会します。

クライアントがサービスの Sun RPC プログラム番号を送信すると、ポート マッパー プロセスはサービスのポート番号を応答します。クライアントは、ポート マッパー プロセスによって特定されたポートを指定して、Sun RPC クエリをサーバに送信します。サーバが応答すると、ASA はこのパケットを代行受信し、そのポートで TCP と UDP の両方の初期接続を開きます。

ヒント　Sun RPC インスペクションはデフォルトではイネーブルです。Sun RPC サーバ テーブルを管理するだけで、ファイアウォールの通過を許可されているサービスを識別できます。Sun RPC インスペクションをイネーブルする方法については、「アプリケーション レイヤ プロトコル インスペクションの設定」（P.8-10）を参照してください。

Sun RPC インスペクションには、次の制限事項が適用されます。

- Sun RPC ペイロード情報の NAT または PAT はサポートされていません。
- Sun RPC インスペクションはインバウンド ACL のみをサポートします。Sun RPC インスペクションはアウトバウンド ACL はサポートしません。これは、インスペクション エンジンでセカンダリ接続でなくダイナミック ACL が使用されるためです。ダイナミック ACL は常に入力方向に追加され、出力方向には追加されません。したがって、このインスペクション エンジンはアウトバウンド ACL をサポートしません。ASA に設定されているダイナミック ACL を表示するには、**show asp table classify domain permit** コマンドを使用します。

許可された Sun RPC サービスの識別

ファイアウォールの通過を許可する Sun RPC サーバおよびサービスを識別する必要があります。Sun RPC インスペクションでは、トラフィックを評価するときにこのテーブルを使用します。

手順

ステップ 1　[Configuration] > [Firewall] > [Advanced] > [SUNRPC Server] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして新しいサーバを追加します。
- サーバを選択し、[Edit] をクリックします。

ステップ 3　サービス プロパティを設定します。

- [Interface Name]：サーバへのトラフィックが伝送されるインターフェイス。
- [IP Address/Mask]：Sun RPC サーバのアドレス。
- [Service ID]：サーバのサービス タイプ。サービス タイプ（100003 など）を判定するには、Sun RPC サーバ マシンの UNIX または Linux コマンド ラインで、**sunrpcinfo** コマンドを使用します。
- [Protocol]：サービスがプロトコルとして使用する TCP または UDP。
- [Port/Port Range]：サービスで使用されているポートまたはポートの範囲。
- [Timeout]：接続のアイドル タイムアウト。

ステップ 4　[OK] をクリックします。

CHAPTER 12

管理アプリケーション プロトコルのインスペクション

ここでは、管理アプリケーション プロトコルのアプリケーション インスペクションについて説明します。特定のプロトコルにインスペクションを使用する必要がある理由、およびインスペクション適用の方法全体については、「アプリケーション レイヤ プロトコル インスペクションの準備」（P.8-1）を参照してください。

ASA では、デフォルトでいくつかの一般的なインスペクション エンジンがイネーブルになっていますが、ネットワークによっては他のインスペクション エンジンをイネーブルにしなければならない場合があります。

- 「DCERPC インスペクション」（P.12-1）
- 「GTP インスペクション」（P.12-4）
- 「RADIUS アカウンティング インスペクション」（P.12-9）
- 「RSH インスペクション」（P.12-12）
- 「SNMP インスペクション」（P.12-12）
- 「XDMCP インスペクション」（P.12-13）

DCERPC インスペクション

ここでは、DCERPC インスペクション エンジンについて説明します。

- 「DCERPC の概要」（P.12-1）
- 「DCERPC インスペクションの設定」（P.12-2）

DCERPC の概要

DCERPC は、Microsoft 社の分散クライアント/サーバ アプリケーションで広く使われているプロトコルです。このプロトコルによって、ソフトウェア クライアントがサーバにあるプログラムをリモートで実行できるようになります。

通常、このプロトコルの接続では、クライアントが予約済みポート番号で接続を受け入れるエンドポイント マッパーというサーバに、必要なサービスについてダイナミックに割り当てられるネットワーク情報を問い合わせます。次に、クライアントは、サービスを提供しているサーバのインスタンスへのセカンダリ接続をセットアップします。セキュリティ アプライアンスは、適切なポート番号とネットワーク アドレスへのセカンダリ接続を許可し、必要に応じて NAT を適用します。

DCERPC インスペクション マップは、EPM とウェルノウン TCP ポート 135 上のクライアントとの間のネイティブ TCP 通信を検査します。クライアント用に EPM のマッピングとルックアップがサポートされています。クライアントとサーバは、どのセキュリティ ゾーンにあってもかまいません。埋め込まれたサーバの IP アドレスとポート番号は、EPM からの応答メッセージで受け取ります。クライアントが EPM から返されたサーバのポートに対して複数の接続を試みる可能性があるので、ピンホールが複数使用でき、そのタイムアウトを設定できるようになっています。

（注）　DCERPC の検査は、ASA にピンホールを開くための EPM とクライアント間の通信だけがサポートされます。EPM を使用しない RPC 通信を使用するクライアントは、DCERPC インスペクションではサポートされません。

DCERPC インスペクションの設定

DCERPC インスペクションはデフォルトではイネーブルになっていません。DCERPC インスペクションが必要な場合は設定する必要があります。

手順

ステップ 1　「DCERPC インスペクション ポリシー マップの設定」（P.12-2）

ステップ 2　「DCERPC インスペクションのサービス ポリシーの設定」（P.12-3）

DCERPC インスペクション ポリシー マップの設定

DCERPC インスペクションの追加のパラメータを指定するには、DCERPC インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、DCERPC インスペクションをイネーブルにすると適用できます。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [DCERPC] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[DCERPC Inspect Map] ダイアログ ボックスの [Security Level] ビューで、目的の設定に最も一致するレベルを選択します。

プリセット レベルの 1 つが要件と一致する場合は、これで完了です。[OK] をクリックし、残りの手順をスキップして、DCERPC インスペクションのサービス ポリシー ルールでマップを使用します。

設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、手順を続けます。

ステップ 5　必要なオプションを設定します。

- [Pinhole Timeout]：ピンホール タイムアウトを設定します。クライアントが使用するサーバ情報は、複数の接続のエンドポイント マッパーから返される場合があるため、タイムアウト値はクライアントのアプリケーション環境を考慮して設定します。範囲は、0:0:1 ～ 1193:0:0 です。
- [Enforce endpoint-mapper service]：サービスのトラフィックだけが処理されるように、バインディング時にエンドポイント マッパー サービスを実行するかどうかを設定します。
- [Enable endpoint-mapper service lookup]：エンドポイント マッパー サービスのルックアップ操作をイネーブルにするかどうかを設定します。サービス ルックアップのタイムアウトも適用できます。タイムアウトを設定しない場合は、ピンホール タイムアウトが適用されます。

ステップ 6　[OK] をクリックします。

DCERPC インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

DCERPC インスペクションのサービス ポリシーの設定

DCERPC インスペクションは、デフォルトのインスペクション ポリシーでイネーブルになっていないため、このインスペクションが必要な場合はイネーブルにする必要があります。デフォルトのグローバル インスペクション ポリシーを編集するだけで、DCERPC インスペクションを追加できます。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- DCERPC インスペクション ルール、つまり DCERPC インスペクションを追加しているルールがある場合は、そのルールを選択し、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別のインスペクション ポリシー マップを使用する場合は、DCERPC インスペクションをディセーブルにしてから、新しいインスペクション ポリシー マップ名で再度イネーブルにする必要があります。

a. [DCERPC] チェックボックスをオフにします。

b. [OK] をクリックします。

c. [Apply] をクリックします。

d. この手順を繰り返して [Protocol Inspections] タブに戻ります。

ステップ 4　[DCERPC] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した DCERPC インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「DCERPC インスペクション ポリシー マップの設定」（P.12-2）を参照してください。

b. [Select DCERPC Inspect Map] ダイアログ ボックスで [OK] をクリックします。

ステップ 6　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

GTP インスペクション

ここでは、GTP インスペクション エンジンについて説明します。

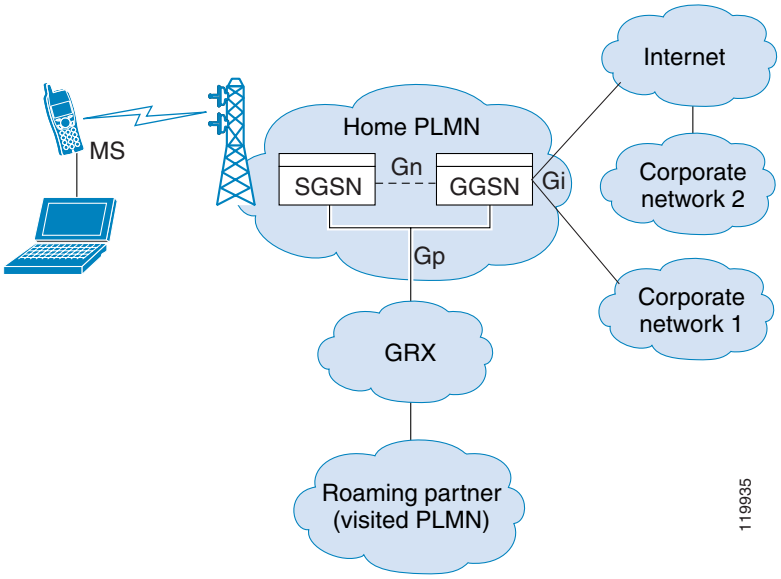
（注）　GTP インスペクションには、特別なライセンスが必要です。

- 「GTP インスペクションの概要」（P.12-4）
- 「GTP インスペクションのデフォルト」（P.12-5）
- 「GTP インスペクションの設定」（P.12-6）

GTP インスペクションの概要

GPRS は、モバイル ユーザに対して、GSM ネットワークと企業ネットワークまたはインターネットとの間で中断しない接続を提供します。GGSN は、GPRS 無線データ ネットワークと他のネットワークとの間のインターフェイスです。SGSN は、モビリティ、データ セッション管理、およびデータ圧縮を実行します。

図 12-1　GPRS トンネリング プロトコル



UMTS は、固定回線テレフォニー、モバイル、インターネット、コンピュータ テクノロジーの商用コンバージェンスです。UTRAN は、このシステムで無線ネットワークを実装するためのネットワーキング プロトコルです。GTP を使用すると、GGSN、SGSN、および UTRAN 間の UMTS/GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。

GTP には固有のセキュリティやユーザ データの暗号化は含まれていませんが、ASA で GTP を使用することによって、これらの危険性からネットワークを保護できます。

SGSN は、GTP を使用する GGSN に論理的に接続されます。GTP を使用すると、GSN 間の GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによって、SGSN は、トンネルの作成、変更、および削除を行い、モバイル ステーションに GPRS ネットワーク アクセスを提供できます。GTP は、トンネリング メカニズムを使用して、ユーザ データ パケットを伝送するためのサービスを提供します。

（注） GTP をフェールオーバーと同時に使用しているとき、GTP 接続が確立され、データがトンネルを超えて伝送される前にアクティブ装置に障害が発生した場合、GTP データ接続（「j」フラグが設定されています）は、スタンバイ装置に複製されません。これは、アクティブ装置が初期接続をスタンバイ装置に複製しないためです。

GTP インスペクションのデフォルト

GTP インスペクションはデフォルトではイネーブルになっていません。ただし、ユーザ自身のインスペクション マップを指定せずにイネーブルにすると、次の処理を行うデフォルト マップが使用されます。マップを設定する必要があるのは、異なる値が必要な場合のみです。

- エラーは許可されません。
- 要求の最大数は 200 です。
- トンネルの最大数は 500 です。
- GSN タイムアウトは 30 分です。

- PDP コンテキストのタイムアウトは 30 分です。
- 要求のタイムアウトは 1 分です。
- シグナリング タイムアウトは 30 分です。
- トンネリングのタイムアウトは 1 時間です。
- T3 応答のタイムアウトは 20 秒です。
- 未知のメッセージ ID はドロップされ、ログに記録されます。

GTP インスペクションの設定

GTP インスペクションはデフォルトではイネーブルになっていません。GTP インスペクションが必要な場合は設定する必要があります。

手順

ステップ 1　「GTP インスペクション ポリシー マップの設定」（P.12-6）

ステップ 2　「GTP インスペクションのサービス ポリシーの設定」（P.12-8）

ステップ 3　（オプション）過剰請求攻撃から保護するために RADIUS アカウンティング インスペクションを設定します。「RADIUS アカウンティング インスペクション」（P.12-9）を参照してください。

GTP インスペクション ポリシー マップの設定

GTP トラフィックに追加のパラメーターを適用する必要があり、デフォルト マップがニーズを満たさない場合は、GTP マップを作成して設定します。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックのいずれかを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [GTP] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。マップを編集するには、[Customize] をクリックします。残りの手順は、マップをカスタマイズするか追加することが前提になります。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[GTP Inspect Map] ダイアログ ボックスの [Security Level] ビューで、マップの現在の設定を確認します。

このビューはマップがデフォルト値を使用しているのか、またはカスタマイズされているのかを示します。設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、手順を続けます。

ヒント　[IMSI Prefix Filtering] ボタンは、IMSI プレフィックス フィルタリングを設定するためのショートカットです。これについては後で説明します。

ステップ 5　[Permit Parameters] タブをクリックして必要なオプションを設定します。

- [Permit Response]：ASA が GTP インスペクションを実行する場合、デフォルトで ASA は、GTP 要求で指定されていない GSN からの GTP 応答をドロップします。これは、GSN のプール間でロードバランシングを使用して、GPRS の効率とスケーラビリティを高めているときに発生します。

  GSN プーリングを設定してロード バランシングをサポートするには、GSN を指定するオブジェクト グループを作成し、これを「**From Object Group**」として選択します。同様に、SGSN のネットワーク オブジェクト グループを作成し、これを「**To Object Group**」として選択します。GSN 応答が、GTP 要求を送信した GSN と同じオブジェクト グループに属し、SGSN が、応答する GSN が GTP 応答の送信を許可されているオブジェクト グループに属している場合、ASA は応答を許可します。

  ネットワーク オブジェクト グループは、GSN または SGSN をホスト アドレスまたは GSN や SGSN を含むサブネットから識別できます。

- [Permit Errors]：無効なパケットやインスペクション時にエラーが見つかったパケットを、ドロップしないでASA から送信することを許可するかどうかを設定します。

ステップ 6　[General Parameters] タブをクリックし、必要なオプションを設定します。

- [Maximum Number of Requests]：応答待ちでキューに格納される GTP 要求の最大数を設定します。
- [Maximum Number of Tunnels]：許可されるトンネルの最大数を設定します。
- [Enforce Timeout] ：次の動作のアイドル タイムアウトを実行するかどうかを設定します。タイムアウトは hh: mm: ss 形式です。
  - [GSN]：GSN が削除されるまでの非アクティブ時間の最大値です。
  - [PDP-Context]：GTP セッションの PDP コンテキストを受け取るまでの非アクティブ時間の最大値です。
  - [Request]：GTP セッション時に GTP メッセージを受け取るまでの非アクティブ時間の最大値です。
  - [Signaling]：GTP シグナリングが削除されるまでの非アクティブ時間の最大値です。
  - [T3-Response timeout]：接続を削除するまでの、応答待ち時間の最大値です。
  - [Tunnel]：GTP トンネルの非アクティブ時間の最大値です。

ステップ 7　必要に応じて[IMSI Prefix Filtering]タブをクリックして、IMSI プレフィックス フィルタリングを設定します。

デフォルトでは、セキュリティ アプライアンスは、有効なモバイル カントリ コード（MCC）とモバイル ネットワーク コード（MNC）の組み合わせをチェックしません。IMSI プレフィックス フィルタリングを設定すると、受信パケットの IMSI の MCC と MNC が設定された MCC と MNC の組み合わせと比較され、一致しないものはドロップされます。

モバイル カントリ コードは 0 以外の 3 桁の数字です。1 桁または 2 桁の値にはプレフィックスとして 0 を追加します。モバイル ネットワーク コードは 2 桁または 3 桁の数字です。

許可されるすべての MCC と MNC の組み合わせを追加します。デフォルトでは、ASA は MNC と MCC の組み合わせが有効であるかどうかをチェックしないため、設定した組み合わせが有効であるかどうかを確認する必要があります。MCC および MNC コードの詳細については、ITU E.212 勧告『*Identification Plan for Land Mobile Stations*』を参照してください。

ステップ 8　[Inspections] タブをクリックして、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）を選択します。次に、基準を設定します。

- [Access Point Name]：アクセス ポイント名を、指定された正規表現または正規表現クラスに対して照合します。デフォルトでは、有効なアクセス ポイント名を持つすべてのメッセージが検査され、どの名前でも許可されます。
- [Message ID]：メッセージ ID（1 ～ 255）を照合します。1 つの値または値の範囲を指定できます。デフォルトでは、すべての有効なメッセージ ID が許可されます。
- [Message Length]：UDP ペイロードの長さが指定した最小値と最大値の間にあるメッセージを照合します。
- [Version]：GTP バージョン（0 ～ 255）を照合します。1 つの値または値の範囲を指定できます。GTP のバージョン 0 はポート 3386 を使用し、バージョン 1 はポート 2123 を使用します。デフォルトでは、すべての GTP バージョンが許可されます。

c. メッセージ ID の照合には、パケットをドロップするかパケット/秒のレート制限を適用するかのいずれかを選択します。他のすべての照合のアクションは、パケットをドロップします。すべての照合に対してロギングをイネーブルにするかどうかを選択できます。

d. [OK] をクリックしてインスペクションを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 9　[GTP Inspect Map] ダイアログ ボックスの [OK] をクリックします。

これで、このインスペクション マップを GTP インスペクション サービス ポリシーで使用できるようになります。

GTP インスペクションのサービス ポリシーの設定

GTP インスペクションは、デフォルトのインスペクション ポリシーでイネーブルになっていないため、このインスペクションが必要な場合はイネーブルにする必要があります。デフォルトのグローバル インスペクション ポリシーを編集するだけで、GTP インスペクションを追加できます。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- GTP インスペクション ルール、つまり GTP インスペクションを追加しているルールがある場合は、そのルールを選択し、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別のインスペクション ポリシー マップを使用する場合は、GTP インスペクションをディセーブルにしてから、新しいインスペクション ポリシー マップ名で再度イネーブルにする必要があります。

a. [GTP] チェックボックスをオフにします。

b. [OK] をクリックします。

c. [Apply] をクリックします。

d. この手順を繰り返して [Protocol Inspections] タブに戻ります。

ステップ 4　[GTP] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した GTP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「GTP インスペクション ポリシー マップの設定」（P.12-6）を参照してください。

b. [Select GTP Inspect Map] ダイアログ ボックスの [OK] をクリックします。

ステップ 6　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

RADIUS アカウンティング インスペクション

ここでは、RADIUS アカウンティング インスペクション エンジンについて説明します。

- 「RADIUS アカウンティング インスペクションの概要」（P.12-9）
- 「RADIUS アカウンティング インスペクションの設定」（P.12-10）

RADIUS アカウンティング インスペクションの概要

RADIUS アカウンティング インスペクションの目的は、RADIUS サーバを使用した GPRS ネットワークでの過剰請求攻撃を防ぐことです。RADIUS アカウンティング インスペクションを実行するのに GTP/GPRS ライセンスは必要ありませんが、GTP インスペクションを実行して GPRS セットアップを設定しない限り、意味がありません。

GPRS ネットワークにおける過剰請求攻撃によって、コンシューマに対して利用していないサービスの請求が行われます。この場合、悪意のある攻撃者は、サーバへの接続をセットアップし、SGSN から IP アドレスを取得します。攻撃者がコールを終了しても、攻撃者のサーバはパケットの送信を続けます。このパケットは GGSN によってドロップされますが、サーバからの接続はアクティブなままです。攻撃者に割り当てられていた IP アドレスが解放され、正規ユーザに再割り当てされるので、正規ユーザは、攻撃者が利用するサービスの分まで請求されることになります。

RADIUS アカウンティング インスペクションは、GGSN へのトラフィックが正規のものかどうかを確認することにより、このような攻撃を防ぎます。RADIUS アカウンティングの機能を正しく設定しておくと、ASA は、RADIUS アカウンティング要求の開始メッセージと終了メッセージに含まれる Framed IP 属性との照合結果に基づいて接続を切断します。終了メッセージの Framed IP 属性の IP アドレスが一致している場合、ASA は、一致する IP アドレスを持つ送信元との接続をすべて検索します。

ASA でメッセージを検証できるように、RADIUS サーバとの事前共有秘密キーを設定することもできます。共有秘密が設定されていない場合、ASA は、送信元 IP アドレスが RADIUS メッセージを送信できるよう設定されたいずれかの IP アドレスであるということだけをチェックします。

（注） GPRS をイネーブルにして RADIUS アカウンティング インスペクションを使用すると、ASA はアカウンティング要求の終了メッセージで 3GPP-Session-Stop-Indicator をチェックして、セカンダリ PDP コンテキストを正しく処理します。具体的には、ASA では、アカウンティング要求の終了メッセージがユーザ セッションおよび関連するすべての接続を終了する前に、メッセージに 3GPP-SGSN-Address 属性が含まれる必要があります。一部のサードパーティの GGSN は、この属性をデフォルトでは送信しない場合があります。

RADIUS アカウンティング インスペクションの設定

RADIUS アカウンティング インスペクションはデフォルトではイネーブルになっていません。RADIUS アカウンティング インスペクションが必要な場合は設定する必要があります。

手順

ステップ 1　「RADIUS アカウンティング インスペクション ポリシー マップの設定」（P.12-10）

ステップ 2　「RADIUS アカウンティング インスペクションのサービス ポリシーの設定」（P.12-11）

RADIUS アカウンティング インスペクション ポリシー マップの設定

RADIUS アカウンティング インスペクション ポリシー マップを作成して、インスペクションに必要な属性を設定する必要があります。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にもインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [RADIUS Accounting] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[Host Parameters] タブをクリックし、各 RADIUS サーバまたは GGSN の IP アドレスを追加します。

ASA がメッセージを検証できるように、任意で秘密キーを含めることができます。キーがない場合、IP アドレスだけがチェックされます。ASA は、これらのホストから RADIUS アカウンティング メッセージのコピーを受信します。

ステップ 5　[Other Parameters] タブをクリックし、必要なオプションを設定します。

- [Send responses to the originator of the RADIUS accounting message] : バナーを ESMTP サーバからマスクするかどうかを設定します。
- [Enforce user timeout] ：ユーザのアイドル タイムアウトを実行するかどうか、また、タイムアウト値を設定します。デフォルトは 1 時間です。
- [Enable detection of GPRS accounting] : GPRS 過剰請求保護を実行するかどうかを設定します。セカンダリ PDP コンテキストを適切に処理するため、ASA は、Accounting-Request の Stop および Disconnect メッセージの 3GPP VSA 26-10415 属性をチェックします。この属性が存在する場合、ASA は、設定したインターフェイスのユーザ IP アドレスに一致する送信元 IP を持つすべての接続を切断します。
- [Validate Attribute] ：Accounting-Request Start メッセージを受信する際、ユーザ アカウントのテーブルを作成する場合に使用する追加基準です。これらの属性は、ASA が接続を切断するかどうかを決定する場合に役立ちます。

  検証する追加属性を指定しない場合は、Framed IP アドレス属性の IP アドレスのみに基づいて決定されます。追加属性を設定し、ASA が現在追跡されているアドレスを含むが、その他の検証する属性が異なるアカウンティング開始メッセージを受信すると、古い属性を使用して開始するすべての接続は、IP アドレスが新しいユーザに再割り当てされたという前提で、切断されます。

  値の範囲は 1 ～ 191 で、このコマンドは複数回入力できます。属性番号および説明のリストについては、http://www.iana.org/assignments/radius-types を参照してください。

ステップ 6　[OK] をクリックします。

これで、RADIUS アカウンティング インスペクションのサービス ポリシーで、このインスペクション マップを使用できるようになります。

RADIUS アカウンティング インスペクションのサービス ポリシーの設定

RADIUS アカウンティング インスペクションは、デフォルトのインスペクション ポリシーでイネーブルになっていないため、このインスペクションが必要な場合はイネーブルにする必要があります。RADIUS アカウンティング インスペクションは ASA に送られるトラフィックのためのものですので、標準ルールではなく、管理インスペクション ルールとして設定する必要があります。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- 新しいルールを作成するには、[Add] > [Add Management Service Policy Rule] をクリックします。「管理トラフィックのサービス ポリシー ルールの追加」（P.1-14）に従って、ウィザードを使って [Rules Actions] ページに進みます。
- RADIUS アカウンティング インスペクション ルール、つまり RADIUS アカウンティング インスペクションを追加した管理ルールがある場合は、そのルールを選択して [Edit] をクリックし、[Rule Actions] タブをクリックします。

ステップ 2　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別のインスペクション ポリシー マップを使用する場合は、RADIUS アカウンティング インスペクションをディセーブルにしてから、新しいインスペクション ポリシー マップ名で再度イネーブルにする必要があります。

a. RADIUS アカウンティング マップに [None] を選択します。

b. [OK] をクリックします。

c. [Apply] をクリックします。

d. この手順を繰り返して [Protocol Inspections] タブに戻ります。

ステップ 3　目的の [RADIUS Accounting Map] を選択します。この時点でマップを作成できます。詳細については、「RADIUS アカウンティング インスペクション ポリシー マップの設定」（P.12-10）を参照してください。

ステップ 4　[OK] または [Finish] をクリックして、管理サービス ポリシー ルールを保存します。

RSH インスペクション

RSH インスペクションはデフォルトでイネーブルになっています。RSH プロトコルは、TCP ポート 514 で RSH クライアントから RSH サーバへの TCP 接続を使用します。クライアントとサーバは、クライアントが STDERR 出力ストリームを受信する TCP ポート番号をネゴシエートします。RSH インスペクションは、必要に応じて、ネゴシエートされたポート番号の NAT をサポートします。

RSH インスペクションのイネーブル化の詳細については、「アプリケーション レイヤ プロトコル インスペクションの設定」（P.8-10）を参照してください。

SNMP インスペクション

SNMP アプリケーション インスペクションでは、SNMP トラフィックを特定のバージョンの SNMP に制限できます。以前のバージョンの SNMP は安全性が低いため、セキュリティ ポリシーを使用して特定の SNMP バージョンを拒否する必要が生じる場合もあります。ASA は、SNMP バージョン 1、2、2c、または 3 を拒否できます。許可するバージョンは、SNMP マップを作成して制御します。

SNMP インスペクションは、デフォルトのインスペクション ポリシーでイネーブルになっていないため、このインスペクションが必要な場合はイネーブルにする必要があります。デフォルトのグローバル インスペクション ポリシーを編集するだけで、SNMP インスペクションを追加できます。インターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [SNMP] の順に選択し、次を実行します。

a. [Add] をクリックするか、マップを選択して [Edit] をクリックします。マップを追加する場合はマップ名を入力します。

b. 拒否する SNMP のバージョンを選択します。

c. [OK] をクリックします。

ステップ 2　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- SNMP インスペクション ルール、つまり SNMP インスペクションを追加しているルールがある場合は、そのルールを選択し、[Edit] をクリックします。

ステップ 3　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 4　（使用中のポリシーを変更する場合）使用中のポリシーを編集して別のインスペクション ポリシー マップを使用する場合は、SNMP インスペクションをディセーブルにしてから、新しいインスペクション ポリシー マップ名で再度イネーブルにする必要があります。

a. [SNMP] チェックボックスをオフにします。

b. [OK] をクリックします。

c. [Apply] をクリックします。

d. この手順を繰り返して [Protocol Inspections] タブに戻ります。

ステップ 5　[SNMP] を選択します。

ステップ 6　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップ（すべてのバージョンを許可します）を使用するか、または設定した SNMP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。

b. [SNMP Inspect Map] ダイアログ ボックスで [OK] をクリックします。

ステップ 7　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

XDMCP インスペクション

XDMCP インスペクションはデフォルトでイネーブルになっていますが、XDMCP インスペクション エンジンは、**established** コマンドが適切に構成されていないと使用できません。

XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションは確立時に TCP を使用します。

XWindows セッションを正常にネゴシエートして開始するために、ASAは、Xhosted コンピュータからの TCP 戻り接続を許可する必要があります。戻り接続を許可するには、ASAで **established** コマンドを使用します。XDMCP がディスプレイを送信するポートをネゴシエートすると、**established** コマンドが参照され、この戻り接続を許可すべきかどうかが確認されます。

XWindows セッション中、マネージャは予約済みポート 6000 l n 上でディスプレイ Xserver と通信します。次の端末設定を行うと、各ディスプレイは別々に Xserver と接続します。

```
setenv DISPLAY Xserver:n
```

n はディスプレイ番号です。

XDMCP が使用されている場合、ディスプレイは IP アドレスを使用してネゴシエートされます。IP アドレスは、ASAが必要に応じて NAT を行うことができます。XDCMP インスペクションでは、PAT はサポートされません。

XDMCP インスペクションのイネーブル化の詳細については、「アプリケーション レイヤ プロトコル インスペクションの設定」（P.8-10）を参照してください。

PART 4

接続設定と QoS

接続設定

この章では、ASA を経由する接続用、または、ASA を宛先とする管理接続用の接続を設定する方法について説明します。接続の設定には、次のものが含まれます。

- 最大接続数（TCP および UDP 接続、初期接続、クライアントあたりの接続）
- 接続タイムアウト
- デッド接続検出
- TCP シーケンスのランダム化
- TCP 正規化カスタマイゼーション
- TCP ステート バイパス
- グローバル タイムアウト
- 「接続の設定に関する情報」（P.13-1）
- 「接続設定のライセンス要件」（P.13-5）
- 「ガイドラインと制限事項」（P.13-5）
- 「デフォルト設定」（P.13-6）
- 「接続の設定」（P.13-6）
- 「接続設定の機能履歴」（P.13-12）

接続の設定に関する情報

この項では、接続の制限が必要になる理由を示します。

- 「TCP 代行受信および初期接続の制限」（P.13-2）
- 「クライアントレス SSL 互換での管理パケットの TCP 代行受信のディセーブル化」（P.13-2）
- 「デッド接続検出（DCD）」（P.13-2）
- 「TCP シーケンスのランダム化」（P.13-3）
- 「TCP の正規化」（P.13-3）
- 「TCP ステート バイパス」（P.13-3）

TCP 代行受信および初期接続の制限

初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA では、クライアントあたりの制限値と初期接続の制限を利用して TCP 代行受信を開始します。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。TCP 代行受信では、SYN クッキー アルゴリズムを使用して TCP SYN フラッディング攻撃を防ぎます。SYN フラッディング攻撃は、通常はスプーフィングされた IP アドレスから送信されてくる一連の SYN パケットで構成されています。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、接続要求に対してサービスを提供できなくなります。接続の初期接続しきい値を超えると、ASA はサーバのプロキシとして動作し、クライアント SYN 要求に対する SYN-ACK 応答を生成します。ASA がクライアントから ACK を受信すると、クライアントを認証し、サーバへの接続を許可できます。

（注）　TCP SYN クッキー保護を使用して SYN 攻撃からサーバを保護する場合、保護するサーバの TCP SYN バックログ キューより低い初期接続制限を設定する必要があります。これより高い初期接続制限を設定すると、有効なクライアントが、SYN 攻撃中にサーバにアクセスできなくなります。

TCP 代行受信に関する統計情報（攻撃を受けた上位 10 サーバなど）を表示する方法については、第 17 章「脅威検出」を参照してください。

クライアントレス SSL 互換での管理パケットの TCP 代行受信のディセーブル化

デフォルトでは、TCP 管理接続では TCP 代行受信が常にイネーブルになっています。TCP 代行受信をイネーブルにすると、3 ウェイ TCP 接続確立のハンドシェイク パケットが代行受信されるため、ASA ではクライアントレス SSL のパケットを処理できなくなります。クライアントレス SSL では、クライアントレス SSL 接続で selective-ack や他の TCP オプションを提供するために、3 ウェイ ハンドシェイク パケットを処理する機能が必要になります。管理トラフィックの TCP 代行受信をディセーブルにするには、初期接続制限を設定します。初期接続制限に達した後にだけ TCP 代行受信をイネーブルにできます。

デッド接続検出（DCD）

DCD では、デッド接続を検出して、トラフィックをまだ処理できる接続を期限切れにすることなく、そのデッド接続を期限切れにすることができます。DCD は、アイドル状態でも有効な接続を維持する場合に設定します。

DCD をイネーブルにすると、アイドル タイムアウト動作が変化します。アイドル タイムアウトになると、DCD プローブが 2 つのエンドホストそれぞれに送信され、接続の有効性が判断されます。設定された間隔でプローブが送信された後にエンドホストが応答を返さないと、その接続は解放され、リセット値が設定されていれば各エンドホストに送信されます。両方のエンドホストが応答して接続の有効性が確認されると、アクティビティ タイムアウトは現在時刻に更新され、それに応じてアイドル タイムアウトが再スケジュールされます。

DCD をイネーブルにすると、TCP ノーマライザでのアイドルタイムアウト処理の動作が変更されます。DCD プローブにより、**show conn** コマンドで表示される接続でのアイドル タイムアウトがリセットされます。タイムアウト コマンドで設定したタイムアウト値を超過していても、DCD プローブのために存続している接続を判別するため、**show service-policy** コマンドには、DCD からのアクティビティ数を示すカウンタが含まれています。

TCP シーケンスのランダム化

それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。ASA は、インバウンドとアウトバウンドの両方向で通過する TCP SNY の ISN をランダム化します。

保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

- 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
- ASA で eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
- ASA で接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

TCP の正規化

TCP 正規化機能は、検出時に ASA が対処できる異常なパケットを識別します。ASA は、パケットを許可、ドロップ、またはクリアできます。TCP 正規化は、攻撃から ASA を保護するのに役立ちます。TCP 正規化は常にイネーブルになっていますが、機能の一部の動作をカスタマイズできます。

TCP 正規化には、設定できないアクションと設定できるアクションが含まれます。通常、接続をドロップまたはクリアする設定できないアクションは、どのような場合でも不良なパケットに適用されます。設定できるアクション（「TCP マップを使用した TCP ノーマライザのカスタマイズ」（P.13-6）を参照）は、ネットワークのニーズに応じたカスタマイズが必要な場合があります。

TCP 正規化に関する次のガイドラインを参考にしてください。

- ノーマライザは、SYN フラッドからの保護は行いません。ASA には、他の方法による SYN フラッド保護機能が組み込まれています。
- ノーマライザは、ASA がフェールオーバーのためにルーズ モードになっていない限り、SYN パケットを最初のパケットと見なします。

TCP ステート バイパス

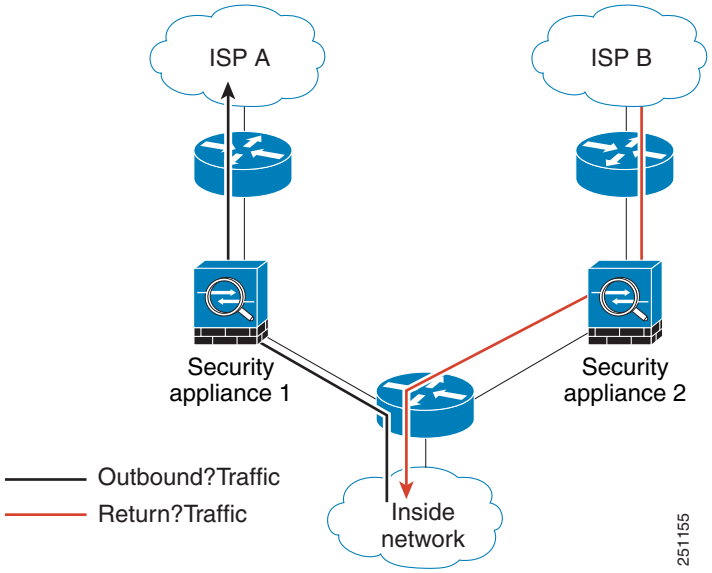
デフォルトでは、ASA を通過するトラフィックはすべて、アダプティブ セキュリティ アルゴリズムを使用して検査され、セキュリティ ポリシーに基づいて、通過を許可されるか、またはドロップされます。ASA では、各パケットの状態（新規接続であるか、または確立済み接続であるか）がチェックされ、そのパケットをセッション管理パス（新規接続の SYN パケット）、

ファスト パス（確立済みの接続）、またはコントロール プレーン パス（高度なインスペクション）に割り当てることによって、ファイアウォールのパフォーマンスが最大化されます。ステートフル ファイアウォールの詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

高速パスの既存の接続に一致する TCP パケットは、セキュリティ ポリシーのあらゆる面の再検査を受けることなく ASA を通過できます。この機能によってパフォーマンスは最大になります。ただし、SYN パケットを使用してファスト パスにセッションを確立する方法、およびファスト パスで行われるチェック（TCP シーケンス番号など）が、非対称ルーティング ソリューションの障害となる場合があります。これは、接続のアウトバウンド フローとインバウンド フローの両方が同じ ASA を通過する必要があるためです。

たとえば、ある新しい接続が ASA 1 に開始されるとします。SYN パケットはセッション管理パスを通過し、接続のエントリが高速パス テーブルに追加されます。この接続の後続のパケットが ASA 1 を通過する場合、パケットは高速パスのエントリと一致して、通過します。しかし、後続のパケットが ASA 2 に到着すると、SYN パケットがセッション管理パスを通過していないために、高速パスにはその接続のエントリがなく、パケットはドロップされます。図 13-1 は非対称ルーティングの例を示したもので、アウトバウンド トラフィックはインバウンド トラフィックとは異なる ASA を通過しています。

図 13-1　非対称ルーティング



アップストリーム ルータに設定された非対称ルーティングがあり、トラフィックが 2 つの ASA の間で切り替わる場合は、特定のトラフィックに対して TCP ステート バイパスを設定できます。TCP ステート バイパスは、高速パスでのセッションの確立方法を変更し、高速パスのインスペクションをディセーブルにします。この機能は、TCP トラフィックを UDP 接続と同じように処理します。指定されているネットワークに一致する非 SYN パケットが ASA に到着し、高速パスのエントリがない場合は、パケットはセッション管理パスを通過して、高速パスの接続を確立します。いったん高速パスに入ると、トラフィックは高速パスのインスペクションをバイパスします。

接続設定のライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

ガイドラインと制限事項

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド モードとトランスペアレント モードでサポートされます。

フェールオーバーのガイドライン

フェールオーバーはサポートされます。

TCP ステート バイパスでサポートされない機能

TCP ステート バイパスを使用するときは、次の機能はサポートされません。

- アプリケーション インスペクション: アプリケーション インスペクションではインバウンド トラフィックとアウトバウンド トラフィックの両方が同じ ASA を通過する必要があるので、アプリケーション インスペクションは TCP ステート バイパスではサポートされません。
- AAA 認証済みセッション：ユーザが 1 つの ASA で認証するとき、他の ASA を介して返されるトラフィックは、ユーザがその ASA で認証を受けていないので拒否されます。
- TCP 代行受信、最大初期接続制限、TCP シーケンス番号のランダム化：ASA は接続のステートを追跡しないので、これらの機能は適用されません。
- TCP 正規化：TCP ノーマライザはディセーブルになります。
- SSM および SSC 機能：TCP ステート バイパスおよび IPS や CSC などの SSM または SSC 上で実行するアプリケーションは使用できません。

TCP ステート バイパスの NAT のガイドライン

変換セッションは ASA ごとに個別に確立されるので、TCP ステート バイパス トラフィック用に両方の ASA でスタティック NAT を設定してください。ダイナミック NAT を使用すると、ASA 1 でのセッションに選択されるアドレスが、ASA 2 でのセッションに選択されるアドレスと異なります。

最大同時接続および初期接続のガイドライン

ASA モデル上の CPU コア数によっては、同時接続および初期接続の最大数が、各コアによる接続の管理方法が原因で、設定されている数を超える場合があります。最悪の場合、ASA は最大 *n*-1 の追加接続および初期接続を許可します。ここで、*n* はコアの数です。たとえば、モデルに 4 つのコアがあり、6 つの同時接続および 4 つの初期接続を設定した場合は、各タイプで 3 つの追加接続を使用できます。ご使用のモデルのコア数を確認するには、**show cpu core** コマンドを入力します。

デフォルト設定

TCP ステート バイパス
TCP ステート バイパスは、デフォルトでディセーブルになっています。

接続の設定

- 「TCP マップを使用した TCP ノーマライザのカスタマイズ」（P.13-6）
- 「接続の設定」（P.13-8）
- 「グローバル タイムアウトの設定」（P.13-10）

接続設定の構成のタスク フロー

ステップ 1　TCP 正規化カスタマイゼーションについては、「TCP マップを使用した TCP ノーマライザのカスタマイズ」（P.13-6）に従って TCP マップを作成します。

ステップ 2　グローバル タイムアウトを除くすべての接続設定については、第 1 章「サービス ポリシー」に従ってサービス ポリシーを設定します。

ステップ 3　「接続の設定」（P.13-8）に従って接続を設定します。

ステップ 4　「グローバル タイムアウトの設定」（P.13-10）に従ってグローバル タイムアウトを設定します。

TCP マップを使用した TCP ノーマライザのカスタマイズ

TCP ノーマライザをカスタマイズするには、まず、TCP マップを使用する設定を定義します。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Objects] > [TCP Maps] ペインを選択し、[Add] をクリックします。
[Add TCP Map] ダイアログボックスが表示されます。

ステップ 2　[TCP Map Name] フィールドで、名前を入力します。

ステップ 3　[Queue Limit] フィールドで、異常なパケットの最大数を 0 ～ 250 パケットの範囲で指定します。
[Queue Limit] では、バッファリングして TCP 接続用に配列できる異常パケットの最大数を設定します。デフォルト値の 0 は、この設定がディセーブルであり、トラフィックのタイプに応じたデフォルトのシステム キュー制限が使用されることを意味します。

- アプリケーション インスペクション、IPS、および TCP check-retransmission の接続のキュー制限は 3 パケットです。ASA が異なるウィンドウ サイズの TCP パケットを受信した場合は、アドバタイズされた設定と一致するようにキュー制限がダイナミックに変更されます。
- 他の TCP 接続の場合は、異常なパケットはそのまま通過します。

[Queue Limit] を 1 以上に設定すると、すべての TCP トラフィックに対して許可される異常なパケットの数がこの設定と一致します。たとえば、アプリケーション インスペクション、IPS、および TCP check-retransmission トラフィックの場合、[Queue Limit] 設定が優先されるため、TCP パケットからのアドバタイズされた設定はすべて無視されます。その他の TCP トラフィックについては、異常なパケットはバッファに格納されて、そのまま通過するのではなく、正しい順序に設定されます。

ステップ 4　[Timeout] フィールドで、異常なパケットがバッファに残存できる最大期間を 1 ～ 20 秒の間で設定します。

これらのパケットが配列されず、タイムアウト期間内に渡されなかった場合は、ドロップされます。デフォルトは 4 秒です。[Queue Limit] が 0 に設定されない場合は、すべてのトラフィックに関してタイムアウトを変更できません。[Timeout] が有効になるには、制限を 1 以上に設定する必要があります。

ステップ 5　[Reserved Bits] 領域で、[Clear and allow]、[Allow only]、または [Drop] をクリックします。

[Allow only] を指定すると、TCP ヘッダーに予約ビットのあるパケットだけが許可されます。

[Clear and allow] を指定すると、TCP ヘッダーの予約ビットをクリアしてパケットを許可します。

[Drop] を指定すると、TCP ヘッダーに予約ビットのあるパケットをドロップします。

ステップ 6　次のいずれかのオプションをオンにします。

- [Clear urgent flag]：ASA を通じて URG フラグをクリアします。URG フラグは、ストリーム中の他のデータよりもプライオリティの高い情報がこのパケットに含まれていることを示すために使用します。TCP RFC では、URG フラグの正確な解釈が明確にされていません。そのため、エンド システムは緊急オフセットをさまざまな方法で処理しており、これが攻撃に対する脆弱性になることがあります。
- [Drop Connection on Window Variation]：予想外のウィンドウ サイズの変更が発生した接続をドロップします。ウィンドウ サイズ メカニズムによって、TCP は大きなウィンドウをアドバタイズでき、続いて、過剰な量のデータを受け入れずに、はるかに小さなウィンドウをアドバタイズできます。TCP 仕様により、「ウィンドウの縮小」は極力避けることが推奨されています。この条件が検出された場合に、接続をドロップできます。
- [Drop packets that exceed maximum segment size]: ピアで設定した MSS を超過したパケットをドロップします。
- [Check if transmitted data is the same as original]：再送信データ チェックをイネーブルにします。
- [Drop packets which have past-window sequence]: ウィンドウ シーケンス番号を超えているパケット、つまり、TCP パケットのシーケンス番号が TCP 受信ウィンドウの右端よりも大きい場合に、パケットをドロップします。このオプションを選択しない場合、[Queue Limit] を 0（ディセーブル）に設定する必要があります。
- [Drop SYN Packets with data]：データのある SYN パケットをドロップします。
- [Enable TTL Evasion Protection]：ASA の TTL 回避保護をイネーブルにします。セキュリティ ポリシーを回避しようとする攻撃を防ぐ場合は、このオプションをイネーブルにしないでください。
- たとえば、攻撃者は TTL を非常に短くしてポリシーを通過するパケットを送信できます。TTL がゼロになると、ASA とエンドポイントの間のルータはパケットをドロップします。この時点で、攻撃者は TTL を長くした悪意のあるパケットを送信できます。このパケットは、ASA にとって再送信のように見えるため、通過します。一方、エンドポイント ホストにとっては、このパケットが攻撃者によって受信された最初のパケットになります。この場合、攻撃者はセキュリティによる攻撃の防止を受けず、攻撃に成功します。
- [Verify TCP Checksum]：チェックサム検証をイネーブルにします。
- [Drop SYNACK Packets with data]: データを含む TCP SYNACK パケットをドロップします。

- [Drop packets with invalid ACK]：無効な ACK を持つパケットをドロップします。次のような場合に無効な ACK が検出される可能性があります。
  - TCP 接続が SYN-ACK-received ステータスでは、受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号と同じでない場合、その ACK は無効です。
  - 受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号より大きい場合は常に、その ACK は無効です。

（注）　無効な ACK を含む TCP パケットは、WAAS 接続で自動的に許可されます。

ステップ 7　TCP オプションを設定するには、次のいずれかのオプションをオンにします。

- [Clear Selective Ack]：[selective-ack TCP] オプションを許可するかクリアするかを設定します。
- [Clear TCP Timestamp]：TCP タイムスタンプ オプションを許可するかクリアするかを設定します。
- [Clear Window Scale]：ウィンドウ スケール タイムスタンプ オプションを許可するかクリアするかを設定します。
- [Range]：有効な TCP オプションの範囲を設定します。正しい範囲は 6 ～ 7 と 9 ～ 255 です。下限境界値は上限境界値以下でなければなりません。範囲ごとに [Allow] または [Drop] を選択します。

ステップ 8　[OK] をクリックします。

接続の設定

接続を設定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] ペインで、第 1 章「サービス ポリシー」に従ってサービス ポリシーを設定します。

新しいサービス ポリシー ルールの一部として接続制限を設定できます。または、既存のサービス ポリシーを編集することもできます。

ステップ 2　[Rule Actions] ダイアログボックスで、[Connection Settings] タブをクリックします。

ステップ 3　最大接続数を設定するには、[Maximum Connections] 領域で次の値を設定します。

- [TCP & UDP Connections]：トラフィック クラスのすべてのクライアントで同時に接続される TCP および UDP 接続の最大数を 2000000 までの範囲で指定します。どちらのプロトコルともデフォルトは 0 で、接続可能な最大許容数に設定されています。
- [Embryonic Connections]：ホストごとの初期接続の最大数を 2000000 までの範囲で指定します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。

検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。

- [Per Client Connections] : 最大 2000000 クライアントごとに、同時 TCP および UDP 接続の最大数を指定します。クライアントあたりの最大接続数の接続をすでに開いているクライアントが新しい接続を試みると、ASA は、その接続を拒否してパケットをドロップします。
- [Per Client Embryonic Connections] : 最大 2000000 クライアントごとに同時 TCP 初期接続の最大数を指定します。クライアントあたりの最大初期接続数の接続を ASA からすでに開いているクライアントが新しい TCP 接続を要求すると、ASA は、その要求の処理を TCP 代行受信機能に代行させ、接続を阻止します。

ステップ 4　接続タイムアウトを設定するには、[TCP Timeout] 領域で次の値を設定します。

- [Connection Timeout] :（TCP だけでなく、*あらゆる*プロトコルの）接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトをディセーブルにするには、0:0:0 を入力します。この期間は 5 分以上にする必要があります。デフォルトは 1 時間です。
- [Send reset to TCP endpoints before timeout] : ASA が、接続スロットを解放する前に接続のエンドポイントに TCP リセット メッセージを送信するように指定します。
- [Embryonic Connection Timeout] : 初期接続（ハーフ オープン）接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトをディセーブルにするには、0:0:0 を入力します。デフォルトは 30 秒です。
- [Half Closed Connection Timeout] : ハーフ クローズ接続が閉じられるまで、0:5:0（9.1(1) 以前の場合）または 0:0:30（9.1(2) 以降の場合）と 1193:0:0 の間でアイドル タイムアウト期間を設定します。デフォルトは 0:10:0 です。ハーフクローズの接続は DCD の影響を受けません。また、ASA は、ハーフクローズ接続を切断するときにリセット パケットを送信しません。

ステップ 5　シーケンス番号のランダム化をディセーブルにするには、[Randomize Sequence Number] をオフにします。

別のインライン ファイアウォールで TCP イニシャル シーケンス番号のランダム化をイネーブルにしている場合は、そのランダム化をディセーブルにできます。2 つのファイアウォールで同じ動作を実行する必要はないからです。ただし、両方のファイアウォールで ISN ランダム化をイネーブルにしたままにしてもトラフィックには影響しません。

それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスでは、アウトバウンド方向に通過する TCP SYN の ISN をランダム化します。同一セキュリティ レベルの 2 つのインターフェイス間の接続の場合、ISN は双方向の SYN でランダム化されます。

保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

ステップ 6　TCP 正規化を設定するには、[Use TCP Map] をオンにします。ドロップダウン リストから既存の TCP マップを選択するか（選択可能な場合）、[New] をクリックして新しい TCP マップを追加します。

[Add TCP Map] ダイアログボックスが表示されます。「TCP マップを使用した TCP ノーマライザのカスタマイズ」（P.13-6）を参照してください。

ステップ 7　[OK] をクリックします。

ステップ 8　存続可能時間を設定するには、[Decrement time to live for a connection] をオンにします。

ステップ 9　TCP ステート バイパスをイネーブルにするには、[Advanced Options] 領域で、[TCP State Bypass] をオンにします。

ステップ 10　[OK] または [Finish] をクリックします。

グローバル タイムアウトの設定

[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインでは、ASA で使用するタイムアウトの期間を設定できます。すべての期間は、*hh*:*mm*:*ss* の形式で表示されます。さまざまなプロトコルの接続スロットと変換スロットのアイドル時間を設定します。指定したアイドル時間の間スロットが使用されなかった場合、リソースは空いているプールに戻されます。TCP 接続スロットは、通常の接続クローズ シーケンスの約 60 秒後に解放されます。

フィールド

[Authentication absolute] と [Authentication inactivity] を除くすべての場合において、チェックボックスをオフにすることはタイムアウト値を指定しないことを意味します。これら 2 つの場合にチェックボックスをオフにすることは、新しい接続ごとに再認証することを意味します。

- [Connection]：接続スロットが解放されるまでのアイドル時間を変更します。接続のタイムアウトをディセーブルにするには、0:0:0 を入力します。この期間は 5 分以上にする必要があります。デフォルトは 1 時間です。
- [Half-closed]：TCP ハーフクローズ接続がクローズするまでのアイドル時間を変更します。最小値は 5 分です。デフォルトは 10 分です。ハーフクローズ接続のタイムアウトをディセーブルにするには、0:0:0 と入力します。
- [UDP]：UDP プロトコル接続がクローズするまでのアイドル時間を変更します。この期間は 1 分以上にする必要があります。デフォルトは 2 分です。タイムアウトをディセーブルにするには、0:0:0 と入力します。
- [ICMP]：全般的な ICMP 状態がクローズするまでのアイドル時間を変更します。
- [H.323]：H.323 メディア接続がクローズするまでのアイドル時間を変更します。デフォルトは 5 分です。タイムアウトをディセーブルにするには、0:0:0 と入力します。
- [H.225]：H.225 シグナリング接続がクローズするまでのアイドル時間を変更します。H.225 のデフォルト タイムアウトは 1 時間（1:0:0）です。値を 0:0:0 にすると、この接続はクローズされません。すべての呼び出しがクリアされた後にこの接続をすぐにクローズするには、値を 1 秒（0:0:1）にすることを推奨します。
- [MGCP]：MGCP メディア ポートがクローズするまでのアイドル時間を表す MGCP のタイムアウト値を変更します。MGCP のデフォルト タイムアウトは 5 分（0:5:0）です。タイムアウトをディセーブルにするには、0:0:0 と入力します。
- [MGCP PAT]：MGCP PAT 変換が削除されるまでのアイドル時間を変更します。デフォルトは 5 分（0:5:0）です。最小時間は 30 秒です。デフォルト値に戻すには、チェックボックスをオフにします。
- [TCP Proxy Reassembly]：再構築のためバッファ内で待機しているパケットをドロップするまでのアイドル タイムアウトを 0:0:10 ～ 1193:0:0 の範囲で設定します。デフォルトは、1 分（0:1:0）です。
- [Floating Connection]：ネットワークへの複数のスタティック ルートが存在しており、それぞれメトリックが異なる場合、ASA は接続確立時点でメトリックが最良のルートを使用します。より適切なルートが使用可能になった場合は、このタイムアウトによって接続が閉じられるので、その適切なルートを使用して接続を再確立できます。デフォルトは 0 です（接続はタイムアウトしません）。この機能を活用するには、0:1:0 ～ 1193:0:0 の間の新しい値にタイムアウトを変更します。
- [SUNRPC]：SunRPC スロットが解放されるまでのアイドル時間を変更します。この期間は 1 分以上にする必要があります。デフォルトは 10 分です。タイムアウトをディセーブルにするには、0:0:0 と入力します。

- [SIP]：SIP シグナリング ポート接続がクローズするまでのアイドル時間を変更します。この期間は 5 分以上にする必要があります。デフォルトは 30 分です。
- [SIP Media]：SIP メディア ポート接続がクローズするまでのアイドル時間を変更します。この期間は 1 分以上にする必要があります。デフォルトは 2 分です。
- [SIP Provisional Media]：SIP 暫定メディア接続のタイムアウト値を 0:1:0 ～ 1193:0:0 の間で変更します。デフォルトは 2 分です。
- [SIP Invite]：PROVISIONAL 応答とメディア xlate のピンホールがクローズされるまでのアイドル時間を変更します。最小値は 0:1:0 で、最大値は 0:30:0 です。デフォルト値は 0:3:0 です。
- [SIP Disconnect]：CANCEL または BYE メッセージで 200 個の OK を受信しない場合に、SIP セッションを削除するまでのアイドル時間を変更します。最小値は 0:0:1 で、最大値は 0:10:0 です。デフォルト値は 0:2:0 です。
- [Authentication absolute]：認証キャッシュがタイムアウトになり、新しい接続を再認証する必要が生じるまでの期間を変更します。この期間は、変換スロット値よりも短い必要があります。システムは、新しい接続を開始して再びプロンプトが表示されるまで待機します。新しい接続のすべてでキャッシングと再認証をディセーブルにするには、0:0:0 と入力します。

（注）　接続でパッシブ FTP を使用する場合は、この値を 0:0:0 に設定しないでください。

（注）　[Authentication Absolute] = 0 の場合、HTTPS 認証は動作しない場合があります。HTTPS 認証後に、ブラウザが複数の TCP 接続を開始して Web ページをロードすると、最初の接続は通過しますが、その後の接続では認証が起動されます。このため、ユーザには、認証の成功後も常に認証ページが表示されます。これを回避するには、認証の絶対タイムアウトを 1 秒に設定します。この回避策を使用すると、認証されていないユーザが同じ送信元 IP アドレスからアクセスすれば 1 秒間だけファイアウォールを通過できるおそれがあります。

- [Authentication inactivity]：認証キャッシュがタイムアウトになり、ユーザが新しい接続を再認証する必要が生じるまでのアイドル時間を変更します。この期間は、変換スロット値よりも短い必要があります。
- [Translation Slot]：変換スロットが解放されるまでのアイドル時間を変更します。この期間は 1 分以上にする必要があります。デフォルトは 3 時間です。このタイムアウトをディセーブルにするには、0:0:0 を入力します。
- （8.4(3) 以降。8.5(1) および 8.6(1) は含まない）[PAT Translation Slot]：PAT 変換スロットが解放されるまでのアイドル時間（0:0:30 ～ 0:5:0 の間）を変更します。デフォルトは 30 秒です。前の接続がアップストリーム デバイスで引き続き開いている可能性があるため、開放された PAT ポートを使用する新しい接続をアップストリーム ルータが拒否する場合、このタイムアウトを増やすことができます。

接続設定の機能履歴

表 13-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 13-1　　接続設定の機能履歴

機能名	プラットフォーム リリース	機能情報
TCP ステート バイパス	8.2(1)	この機能が導入されました。**set connection advanced-options tcp-state-bypass** コマンドが導入されました。
すべてのプロトコルの接続タイムアウト	8.2(2)	アイドル タイムアウトは、TCP だけでなく、すべてのプロトコルに適用するように変更されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policies] > [Rule Actions] > [Connection Settings]。
バックアップ スタティック ルートを使用する接続のタイムアウト	8.2(5)/8.4(2)	同じネットワークへの複数のスタティック ルートが存在しており、それぞれメトリックが異なる場合は、ASA は接続確立時点でメトリックが最良のルートを使用します。より適切なルートが使用可能になった場合は、このタイムアウトによって接続が閉じられるので、その適切なルートを使用して接続を再確立できます。デフォルトは 0 です（接続はタイムアウトしません）。この機能を使用するには、タイムアウトを新しい値に変更します。 次の画面が変更されました。[Configuration] > [Firewall] > [Advanced] > [Global Timeouts]。
PAT xlate に対する設定可能なタイムアウト	8.4(3)	PAT xlate がタイムアウトし（デフォルトでは 30 秒後）、ASA が新しい変換用にポートを再使用すると、一部のアップストリーム ルータは、前の接続がアップストリーム デバイスで依然として開いている可能性があるため、この新しい接続を拒否する場合があります。PAT xlate のタイムアウトを、30 秒～5 分の範囲内の値に設定できるようになりました。 次の画面が変更されました。[Configuration] > [Firewall] > [Advanced] > [Global Timeouts]。 *この機能は、8.5(1) または 8.6(1) では使用できません。*
サービス ポリシー ルールの最大接続数の引き上げ	9.0(1)	サービス ポリシー ルールの最大接続数が 65535 から 2000000 に引き上げられました。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rules] > [Connection Settings]。
ハーフ クローズ タイムアウト最小値を 30 秒に削減	9.1(2)	グローバル タイムアウトおよび接続タイムアウトの両方のハーフ クローズド タイムアウトの最小値は、より優れた DoS 保護を提供するために 5 分から 30 秒に短縮されました。 次の画面が変更されました。 [Configuration] > [Firewall] > [Service Policy Rules] > [Connection Settings] [Configuration] > [Firewall] > [Advanced] > [Global Timeouts]。

CHAPTER 14

QoS

衛星接続を使用した長距離電話では、会話が、短い間ですが認識できる程度に割り込みされ、不定期に中断されることがあります。このような中断は、ネットワークで送信されるパケットが到着する間隔の時間で、遅延と呼ばれます。音声やビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。Quality of Service（QoS）機能を使用すると、重要なトラフィックのプライオリティを高くし、帯域幅の過剰な使用を防ぎ、ネットワーク ボトルネックを管理してパケットのドロップを防止できます。

（注） ASASM については、ASASM の代わりにスイッチで QoS を実行することを推奨します。スイッチの方が、この領域においては多機能です。一般的に、QoS は、ASA よりも広範な機能を持つ傾向がある、ネットワーク内のルータおよびスイッチで実行するのが最適です。

この章では、QoS ポリシーの適用方法について説明します。

- 「QoS について」（P.14-1）
- 「QoS のガイドライン」（P.14-3）
- 「QoS の設定」（P.14-4）
- 「QoS のモニタ」（P.14-8）
- 「QoS の履歴」（P.14-10）

QoS について

常に変化するネットワーク環境では、QoS は 1 回限りの構成ではなく、ネットワーク設計の継続的で不可欠な要素であることを考慮する必要があります。

この項では、ASA で使用できる QoS 機能について説明します。

- 「サポートされる QoS 機能」（P.14-2）
- 「トークン バケットとは」（P.14-2）
- 「ポリシング」（P.14-2）
- 「プライオリティ キューイング」（P.14-3）
- 「DSCP（DiffServ）の保存」（P.14-3）

サポートされる QoS 機能

ASA は、次の QoS の機能をサポートしています。

- ポリシング：分類されたフローがネットワーク帯域幅を大量に使用するのを防ぐため、クラスごとの最大使用帯域幅を制限できます。詳細については、「ポリシング」（P.14-2）を参照してください。
- プライオリティ キューイング：Voice over IP（VoIP）のような遅延を許されない重要なトラフィックについて、トラフィックを低遅延キューイング（LLQ）に指定することで、常に他のトラフィックより先に送信できます。「プライオリティ キューイング」（P.14-3）を参照してください。

トークン バケットとは

トークン バケットは、フロー内のデータを規制するデバイス（トラフィック ポリサーなど）の管理に使用されます。トークン バケット自体には、廃棄ポリシーまたはプライオリティ ポリシーはありません。むしろ、トークン バケットは、フローによって規制機能が過剰に働く場合に、トークンを廃棄し、送信キューの管理の問題はフローに任せます。

トークン バケットは、転送レートの正式な定義です。トークン バケットには、バースト サイズ、平均レート、時間間隔という 3 つのコンポーネントがあります。平均レートは通常 1 秒間のビット数で表されますが、次のような関係によって、任意の 2 つの値を 3 番目の値から求めることができます。

平均レート = バースト サイズ / 時間間隔

これらの用語の定義は次のとおりです。

- 平均レート：認定情報レート（CIR）とも呼ばれ、単位時間に送信または転送できるデータ量の平均値を指定します。
- バースト サイズ：認定バースト（Bc）サイズとも呼ばれ、スケジューリングに関する問題を発生させることなく単位時間内に送信できるトラフィックの量を、バーストあたりのバイト数で指定します
- 時間間隔：測定間隔とも呼ばれ、バーストごとの時間を秒単位で指定します。

トークン バケットのたとえで言えば、トークンは特定のレートでバケットに入れられます。バケット自体には指定された容量があります。バケットがいっぱいになると、新しく到着するトークンは廃棄されます。各トークンは、送信元が一定の数のビットをネットワークに送信するための権限です。パケットを送信するため、規制機能はパケット サイズに等しい数のトークンをバケットから削除する必要があります。

パケットを送信するための十分なトークンがバケットにない場合、パケットは、パケットが廃棄されるか、ダウン状態とマークされるまで待機します。バケットがすでにトークンで満たされている場合、着信トークンはオーバーフローし、以降のパケットには使用できません。したがって、いつでも、送信元がネットワークに送信できる最大のバーストは、バケットのサイズにほぼ比例します。

ポリシング

ポリシングは、設定した最大レート（ビット/秒単位）を超えるトラフィックが発生しないようにして、1 つのトラフィック クラスが全体のリソースを占有しないようにする方法です。トラフィックが最大レートを超えると、ASA は超過した分のトラフィックをドロップします。また、ポリシングでは、許可されるトラフィックの最大単一バーストも設定されます。

プライオリティ キューイング

LLQ プライオリティ キューイングを使用すると、特定のトラフィック フロー（音声やビデオのような遅延の影響を受けやすいトラフィックなど）をその他のトラフィックよりも優先できます。プライオリティ キューイングでは、インターフェイスで LLQ プライオリティ キューが使用されますが（「インターフェイスのプライオリティ キューの設定」（P.14-6）を参照してください）、他のトラフィックはすべて「ベスト エフォート」キューに入ります。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これは*テール ドロップ*と呼ばれます。キューがいっぱいになることを避けるには、キューのバッファ サイズを大きくします。送信キューに入れることのできるパケットの最大数も微調整できます。これらのオプションを使用して、プライオリティ キューイングの遅延と強固さを制御できます。LLQ キュー内のパケットは、常に、ベストエフォート キュー内のパケットよりも前に送信されます。

QoS 機能の相互作用のしくみ

ASA で必要な場合は、個々の QoS 機能を単独で設定できます。ただし、普通は、たとえば一部のトラフィックを優先させて、他のトラフィックによって帯域幅の問題が発生しないようにするために、複数の QoS 機能を ASA に設定します。次のことを設定できます。

プライオリティ キューイング（特定のトラフィックについて）+ ポリシング（その他のトラフィックについて）

同じトラフィックのセットに対して、プライオリティ キューイングとポリシングを両方設定することはできません。

DSCP（DiffServ）の保存

DSCP（DiffServ）のマーキングは、ASA を通過するすべてのトラフィックで維持されます。ASA は、分類されたトラフィックをローカルにマーク/再マークすることはありません。たとえば、すべてのパケットの緊急転送（EF）DSCP ビットをオフにして、「プライオリティ」処理として ASA にそれらのパケットを LLQ に入れさせる必要があるかどうかを決定できます。

QoS のガイドライン

コンテキスト モードのガイドライン

シングル コンテキスト モードでだけサポートされます。マルチ コンテキスト モードをサポートしません。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

IPv6 のガイドライン

IPv6 はサポートされません。

モデルのガイドライン

- （ASA 5512-X ～ ASA 5555-X）プライオリティ キューイングは、Management 0/0 インターフェイスでサポートされていません。
- （ASASM）ポリシングだけがサポートされます。

その他のガイドラインと制限事項

- QoS は単方向に適用されます。ポリシー マップを適用するインターフェイスに出入りする（QoS 機能によって異なります）トラフィックだけが影響を受けます。詳細については、「機能の方向」（P.1-4）を参照してください。
- プライオリティ トラフィックに対しては、**class-default** クラス マップは使用できません。
- プライオリティ キューイングの場合、プライオリティ キューは物理インターフェイス用に、または ASASM の場合には VLAN 用に設定する必要があります。
- ポリシングでは、to-the-box トラフィックはサポートされません。
- ポリシングでは、VPN トンネルとの間で送受信されるトラフィックはインターフェイスのポリシングをバイパスします。
- ポリシングでは、トンネル グループ クラス マップを照合する場合、出力ポリシングのみがサポートされます。

QoS の設定

ASA に QoS を実装するには、次の手順を使用します。

ステップ 1　「プライオリティ キューのプライオリティ キューおよび TX リング制限の決定」（P.14-4）
ステップ 2　「インターフェイスのプライオリティ キューの設定」（P.14-6）
ステップ 3　「プライオリティ キューイングとポリシング用のサービス ルールの設定」（P.14-7）

プライオリティ キューのプライオリティ キューおよび TX リング制限の決定

プライオリティ キューおよび TX リング制限を決定するには、次のワークシートを使用します。

- 「キュー制限のワークシート」（P.14-4）
- 「TX リング制限のワークシート」（P.14-5）

キュー制限のワークシート

次のワークシートは、プライオリティ キューのサイズを計算する方法を示しています。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます（*テール ドロップ*と呼ばれます）。キューがいっぱいになることを避けるには、「インターフェイスのプライオリティ キューの設定」（P.14-6）に従ってキューのバッファ サイズを調節します。

ワークシートに関するヒント:

- アウトバウンド帯域幅：たとえば、DSL のアップリンク速度は 768 Kbps などです。プロバイダーに確認してください。
- 平均パケット サイズ：この値は、コーデックまたはサンプリング サイズから決定します。たとえば、VoIP over VPN の場合は、160 バイトなどを使用します。使用するサイズがわからない場合は、256 バイトにすることをお勧めします。
- 遅延：遅延はアプリケーションによって決まります。たとえば、VoIP の場合の推奨される最大遅延は 200 ミリ秒です。使用する遅延がわからない場合は、500 ミリ秒にすることをお勧めします。

表 14-1　　キュー制限のワークシート

1	_____ *アウトバウンド帯域幅（Mbps または Kbps）*	Mbps **x 125** Kbps **x .125**	**=**	_____ *バイト数/ミリ秒* _____ *バイト数/ミリ秒*		
2	_____ *ステップ 1 からのバイト数/ミリ秒*	**÷**	_____ *平均パケット サイズ（バイト）*	**x**	_____ *遅延（ミリ秒）*	**=** _____ *キュー制限（パケット数）*

TX リング制限のワークシート

次のワークシートは、TX リング制限を計算する方法を示しています。この制限により、イーサネット送信ドライバが受け入れるパケットの最大数が決まります。この制限に達すると、ドライバはパケットをインターフェイスのキューに差し戻し、輻輳が解消されるまでパケットをバッファに格納できるようにします。この設定により、ハードウェアベースの送信リングがプライオリティの高いパケットに対して制限以上の余分な遅延を発生させないことが保証されます。

ワークシートに関するヒント:

- アウトバウンド帯域幅：たとえば、DSL のアップリンク速度は 768 Kbps などです。プロバイダーに確認してください。
- 最大パケット サイズ：通常、最大サイズは 1538 バイト、またはタグ付きイーサネットの場合は 1542 バイトです。ジャンボ フレームを許可する場合（プラットフォームでサポートされている場合）、パケット サイズはさらに大きくなる場合があります。
- 遅延：遅延はアプリケーションによって決まります。たとえば、VoIP のジッタを制御するには、20 ミリ秒を使用します。

表 14-2　TX リング制限のワークシート

1	_____ *アウトバウンド帯域幅（Mbps または Kbps）*	Mbps	x **125**	=	_____ *バイト数/ミリ秒*	
		Kbps	x **0.125**	=	_____ *バイト数/ミリ秒*	
2	_____ *ステップ 1 からのバイト数/ミリ秒*	÷	_____ *最大パケット サイズ（バイト）*	x _____ *遅延（ミリ秒）*	=	_____ *TX リング制限（パケット数）*

インターフェイスのプライオリティ キューの設定

物理インターフェイスでトラフィックに対するプライオリティ キューイングをイネーブルにする場合は、各インターフェイスでプライオリティ キューを作成する必要もあります。各物理インターフェイスは、プライオリティ トラフィック用と、他のすべてのトラフィック用に、2 つのキューを使用します。他のトラフィックについては、必要に応じてポリシングを設定できます。

はじめる前に

- （ASASM）ASASM では、プライオリティ キューイングはサポートされません。
- （ASA 5512-X ～ ASA 5555-X）プライオリティ キューイングは、Management 0/0 インターフェイスでサポートされていません。

手順

ステップ 1　[Configuration] > [Device Management] > [Advanced] > [Priority Queue] を選択して、[Add] をクリックします。

ステップ 2　次のオプションを設定します。

- **インターフェイス**：プライオリティキューをイネーブルにする物理インターフェイスの名前、または ASASM の場合は VLAN インターフェイス名。
- **キュー制限**：指定したインターフェイスが 500 ミリ秒の間隔で送信できる平均 256 バイトの パケット数。

  ネットワーク ノードに 500 ミリ秒よりも長く留まるパケットは、エンドツーエンド アプリケーションでタイムアウトをトリガーする可能性があります。そのようなパケットは、各ネットワーク ノードで破棄できます。

  キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます（*テール ドロップ*と呼ばれます）。キューがいっぱいになることを避けるため、このオプションを使用してキューのバッファ サイズを大きくできます。

  このオプションの範囲の上限値は実行時に動的に決まります。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。

キューの制限を指定すると、優先順位の高い低遅延のキューとベストエフォート キューの両方に影響が及びます。

- **伝送リング制限** ：プライオリティ キューの深さ。これは、指定したインターフェイスが 10 ミリ秒の間隔で送信できる最大 1550 バイトのパケット数です。

  この設定により、ハードウェア ベースの伝送リングが優先順位の高いパケットに課す余分な遅延が 10 ミリ秒を超えないことが保証されます。

  このオプションは、Ethernet 伝送ドライバに送ることができる低遅延または通常プライオリティのパケットの最大数を設定します。この最大数を超えると、Ethernet 伝送ドライバがインターフェイスのキューにパケットを押し戻し、輻輳が解消されるまでパケットをキューにバッファします。

  値の範囲の上限は、実行時にダイナミックに決定されます。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。

  伝送リング制限の制限値を指定すると、優先順位の高い低遅延のキューとベストエフォート キューの両方に影響が及びます。

ステップ 3　[OK] をクリックします。

ステップ 4　[Apply] をクリックします。

プライオリティ キューイングとポリシング用のサービス ルールの設定

同じポリシー マップ内の異なるクラス マップに対し、プライオリティ キューイングとポリシングを設定できます。有効な QoS 設定については、「QoS 機能の相互作用のしくみ」（P.14-3）を参照してください。

はじめる前に

- プライオリティ トラフィックに対しては、**class-default** クラス マップは使用できません。
- （ASASM）ASASM はポリシングだけをサポートします。
- ポリシングでは、to-the-box トラフィックはサポートされません。
- ポリシングでは、VPN トンネルとの間で送受信されるトラフィックはインターフェイスのポリシングをバイパスします。
- ポリシングでは、トンネル グループ クラス マップを照合する場合、出力ポリシングのみがサポートされます。
- プライオリティ トラフィックの場合は、遅延が問題になるトラフィックだけを指定します。
- ポリシング トラフィックの場合は、他のすべてのトラフィックをポリシングすることも、トラフィックを特定のタイプに制限することもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

新しいサービス ポリシー ルールの一部として QoS を設定できます。または、既存のサービス ポリシーを編集することもできます。

ステップ 2　ウィザードで [Rules] ページにウィザードに進み、途中でインターフェイス（またはグローバル）とトラフィック一致基準を選択します。

ポリシング トラフィックに関しては、優先していない全トラフィックをポリシングするように選択するか、トラフィックを一定の種類に制限できます。

ヒント　トラフィック照合に ACL を使用する場合、ポリシングは ACL で指定された方向にのみ適用されます。つまり、送信元から宛先に向かうトラフィックはポリシングされますが、宛先から送信元に向かうトラフィックはポリシングされません。

サービス ポリシー ルールの詳細については、第 1 章「サービス ポリシー」を参照してください。

ステップ 3　[Rule Actions] ダイアログボックスで、[QoS] タブをクリックします。

ステップ 4　[Enable priority for this flow] を選択します。

このサービス ポリシー ルールが個別のインターフェイス用の場合、ASDM は自動的にこのインターフェイス用のプライオリティ キューを作成します（[Configuration] > [Device Management] > [Advanced] > [Priority Queue]。詳細については、「インターフェイスのプライオリティ キューの設定」（P.14-6）を参照してください）。このルールがグローバル ポリシー用の場合は、サービス ポリシー ルールを設定する *前*に、1 つ以上のインターフェイスにプライオリティ キューを手動で追加する必要があります。

ステップ 5　指定したタイプのトラフィック ポリシングをイネーブルにするには、[Enable policing] を選択して、[Input policing] または [Output policing]（または両方の）チェックボックスをオンにします。トラフィック ポリシングのタイプごとに、次のオプションを設定します。

- [Committed Rate]：このトラフィック フローのレート制限。これは、8000 ～ 2000000000 の範囲の値で、許容最大速度（ビット/秒）を指定します。
- [Conform Action]：レートが適合バースト値未満の場合に実行するアクション。値は、transmit または drop です。
- [Exceed Action]：レートが適合レート値と適合バースト値の間になっている場合に、このアクションを実行します。値は、transmit または drop です。
- [Burst Rate]：1000 ～ 512000000 の範囲の値で、適合レート値までトラフィックを抑制するまでに、持続したバーストにおいて許可される最大瞬間バイト数を指定します。

ステップ 6　[Finish] をクリックします。

ステップ 7　[Apply] をクリックしてコンフィギュレーションをデバイスに送信します。

QoS のモニタ

ASDM の QoS をモニタするには、コマンドライン インターフェイス ツールでコマンドを入力します。

- 「QoS ポリシーの統計情報」（P.14-9）
- 「QoS プライオリティの統計情報」（P.14-9）
- 「QoS プライオリティ キューの統計情報」（P.14-9）

QoS ポリシーの統計情報

トラフィック ポリシングの QoS 統計情報を表示するには、**show service-policy police** コマンドを使用します。

```
hostname# show service-policy police

Global policy:
    Service-policy: global_fw_policy

Interface outside:
    Service-policy: qos
        Class-map: browse
            police Interface outside:
                cir 56000 bps, bc 10500 bytes
                conformed 10065 packets, 12621510 bytes; actions: transmit
                exceeded 499 packets, 625146 bytes; actions: drop
                conformed 5600 bps, exceed 5016 bps
        Class-map: cmap2
            police Interface outside:
                cir 200000 bps, bc 37500 bytes
                conformed 17179 packets, 20614800 bytes; actions: transmit
                exceeded 617 packets, 770718 bytes; actions: drop
                conformed 198785 bps, exceed 2303 bps
```

QoS プライオリティの統計情報

priority コマンドを実装するサービス ポリシーの統計情報を表示するには、**show service-policy priority** コマンドを使用します。

```
hostname# show service-policy priority
Global policy:
    Service-policy: global_fw_policy
Interface outside:
    Service-policy: qos
        Class-map: TG1-voice
            Priority:
                Interface outside: aggregate drop 0, aggregate transmit 9383
```

「aggregate drop」は、このインターフェイスでの合計ドロップ数を示しています。「aggregate transmit」は、このインターフェイスで送信されたパケットの合計数を示しています。

QoS プライオリティ キューの統計情報

インターフェイスのプライオリティ キュー統計情報を表示するには、**show priority-queue statistics** コマンドを使用します。ベスト エフォート（BE）キューと低遅延キュー（LLQ）の両方の統計情報が表示されます。次の例に、test という名前のインターフェイスに対する **show priority-queue statistics** コマンドの使用方法を示します。

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type         = BE
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
```

```
Current Q Length  = 0
Max Q Length      = 0

Queue Type        = LLQ
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
hostname#
```

この統計情報レポートの内容は次のとおりです。

- 「Packets Dropped」は、このキューでドロップされたパケットの合計数を示します。
- 「Packets Transmit」は、このキューで送信されたパケットの合計数を示します。
- 「Packets Enqueued」は、このキューでキューイングされたパケットの合計数を示します。
- 「Current Q Length」は、このキューの現在の深さを示します。
- 「Max Q Length」は、このキューで発生した最大の深さを示します。

QoS の履歴

機能名	プラットフォーム リリース	説明
プライオリティ キューイングとポリシング	7.0(1)	QoS プライオリティ キューイングとポリシングが導入されました。 次の画面が導入されました。 [Configuration] > [Device Management] > [Advanced] > [Priority Queue] [Configuration] > [Firewall] > [Service Policy Rules]
シェーピングおよび階層型プライオリティ キューイング	7.2(4)/8.0(4)	QoS シェーピングおよび階層型プライオリティ キューイングが導入されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rules]。
ASA 5585-X での 10 ギガビット イーサネットによる標準プライオリティ キューのサポート	8.2(3)/8.4(1)	ASA 5585-X の 10 ギガビット イーサネット インターフェイスでの標準プライオリティ キューのサポートが追加されました。

CHAPTER 15

接続のトラブルシューティングおよびリソース

この章では、ASA のトラブルシューティング方法について説明します。

- 「コンフィギュレーションのテスト」（P.15-1）
- 「パフォーマンスのモニタリング」（P.15-9）
- 「システム リソースのモニタリング」（P.15-10）
- 「接続のモニタリング」（P.15-12）
- 「プロセスごとの CPU 使用率のモニタリング」（P.15-13）

コンフィギュレーションのテスト

この項では、シングル モード ASA または各セキュリティ コンテキストの接続性のテスト方法、ASA インターフェイスを ping する方法、およびあるインターフェイスにあるホストが他のインターフェイスのホストに ping できるようにする方法について説明します。

- 「ASA のインターフェイスへの ping の実行」（P.15-1）
- 「ASA のコンフィギュレーションおよび動作の検証、および ping を使用したインターフェイスのテストの実行」（P.15-3）
- 「トレースルートによるパケット ルーティングの決定」（P.15-6）
- 「パケット トレーサによるパケットの追跡」（P.15-7）

ASA のインターフェイスへの ping の実行

ASA インターフェイスが起動して動作しているかどうか、および ASA と接続ルータが正しく動作しているかどうかをテストするには、ASA インターフェイスを ping します。

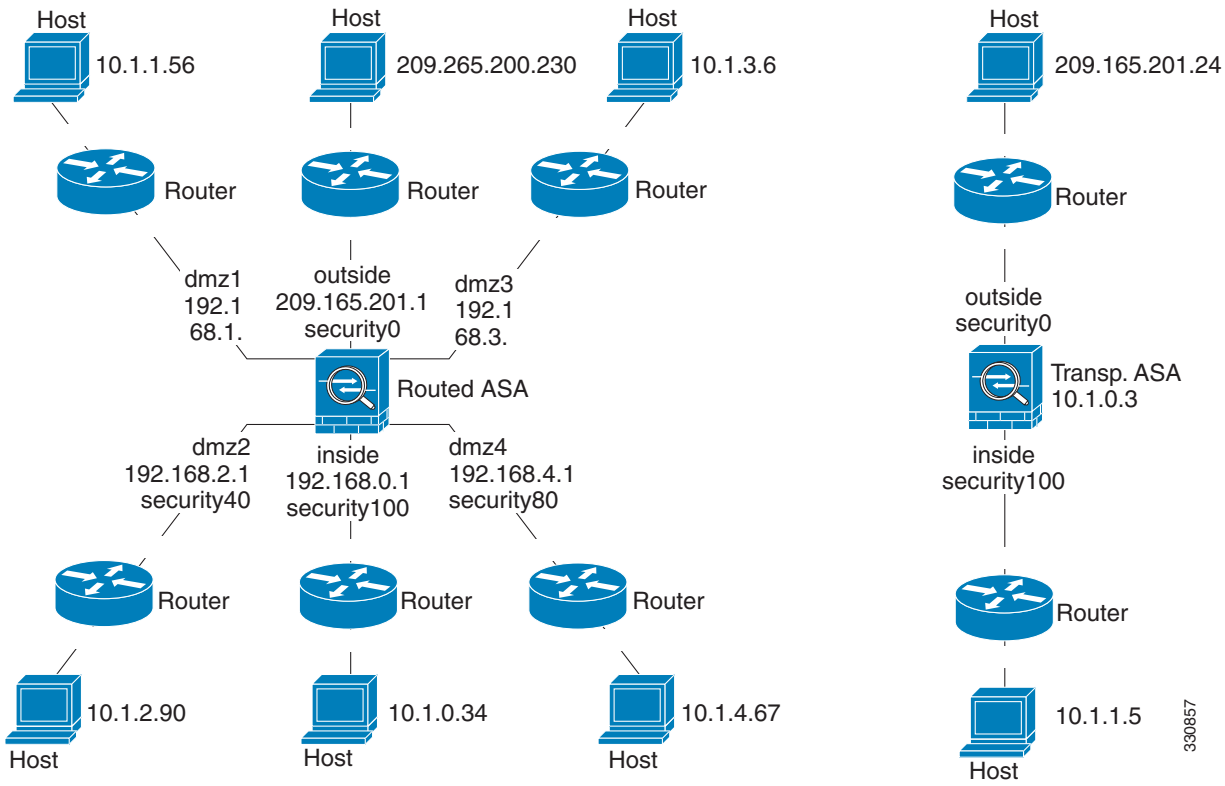
ASA インターフェイスを ping するには、次の手順を実行します。

ステップ 1 インターフェイス名、セキュリティ レベル、および IP アドレスを示すシングル モードの ASA またはセキュリティ コンテキストの図を作成します。

（注） この手順では IP アドレスを使用しますが、**ping** コマンドでは、DNS 名および **name** コマンドを使用してローカル IP アドレスに割り当てられた名前もサポートされます。

図には、直接接続されたすべてのルータ、および ASA を ping するルータの反対側にあるホストも含める必要があります。（図 15-1 を参照）。

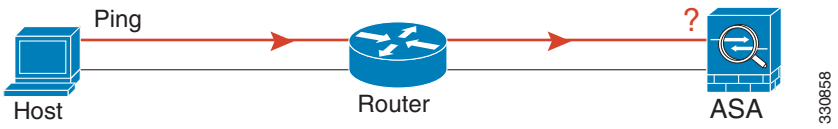
図 15-1　インターフェイス、ルータ、およびホストを含むネットワーク図



ステップ 2　直接接続されたルータから各 ASA インターフェイスを ping します。トランスペアレント モードでは、管理 IP アドレスを ping します。このテストは、ASA インターフェイスがアクティブであること、およびインターフェイス コンフィギュレーションが正しいことを確認します。

ASA インターフェイスがアクティブではない場合、インターフェイス コンフィギュレーションが正しくない場合、または ASA とルータの間でスイッチがダウンしている場合、ping は失敗する可能性があります（図 15-2 を参照）。この場合は、パケットが ASA に到達しないので、デバッグ メッセージや syslog メッセージは表示されません。

図 15-2　ASA のインターフェイスへの ping の失敗

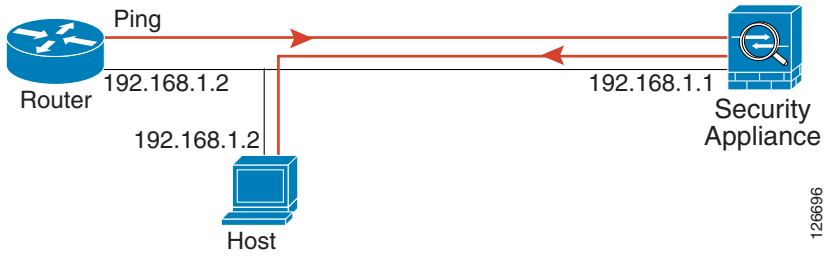


ping が ASA に到達し、応答があると、次のようなデバッグ メッセージが表示されます。

```
ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
```

ping 応答がルータに戻されない場合は、スイッチ ループまたは冗長 IP アドレスが存在する可能性があります（図 15-3 を参照）。

図 15-3　IP アドレッシングの問題による ping の失敗



ステップ 3　リモート ホストから各 ASA インターフェイスを ping します。トランスペアレント モードでは、管理 IP アドレスを ping します。このテストは、直接接続されたルータがホストと ASA の間でパケットをルーティングできるかどうか、および ASA がパケットを正確にルーティングしてホストに戻せるかどうかを確認します。

中間ルータを通ってホストに戻るルートが ASA にない場合、ping は失敗する可能性があります（図 15-4 を参照）。この場合は、デバッグ メッセージは ping が成功したことを示しますが、ルーティングの失敗を示す syslog メッセージ 110001 が表示されます。

図 15-4　ASA の戻りルート未設定による ping の失敗

ASA のコンフィギュレーションおよび動作の検証、および ping を使用したインターフェイスのテストの実行

ping ツールは、ASA および関係する通信リンクのコンフィギュレーションおよび動作を検証する場合、また他のネットワーク デバイスをテストする場合に便利です。

- 「ping に関する情報」（P.15-3）
- 「ASA インターフェイスからの ping の送信」（P.15-4）
- 「ASA インターフェイスへの ping の送信」（P.15-4）
- 「ASA のインターフェイスを通過する ping」（P.15-5）
- 「ping ツールのトラブルシューティング」（P.15-5）
- 「ping ツールの使い方」（P.15-5）

ping に関する情報

ping が IP アドレスに送信されると、応答が返されます。このプロセスを使用して、ネットワーク デバイスは、相互に検出、識別、およびテストすることができます。

ping ツールでは、ICMP（RFC 777 および RFC 792 に記載）を使用して、2 つのネットワーク デバイス間でのエコー要求とエコー応答のトランザクションを定義します。エコー要求パケットは、ネットワーク デバイスの IP アドレスへ送信されます。受信側のデバイスは送信元と宛先のアドレスを逆にしてから、そのパケットをエコー応答として送り返します。

管理者は、次の方法で ASDM の ping インタラクティブ診断ツールを使用できます。

- 2 つのインターフェイス間のループバック テスト：同じ ASA で一方のインターフェイスから相手側のインターフェイスに ping を外部ループバック テストとして起動すると、双方のインターフェイスの基本的な「アップ」ステータスおよび動作を検証できます。
- ASA への ping 送信：ping ツールにより、別の ASA のインターフェイスに ping を送信し、そのインターフェイスがアップしていて応答することを確認できます。
- ASA を通過する ping 送信：ping ツールの送信 ping パケットがデバイスに到達する途中で、中間の ASA を通過する場合があります。エコー パケットは、返されるときにそのインターフェイスを両方とも通過します。この手順によって、中間にある装置のインターフェイス、動作、応答時間についての基本的なテストができます。
- ネットワーク デバイスの疑わしい動作をテストするための ping 送信：正常に機能していないと思われるネットワーク デバイスに対して、ASA のインターフェイスから ping を送信できます。インターフェイスが正しく設定されているにもかかわらずエコーを受信しない場合は、デバイスに問題があると考えられます。
- 中間の通信状態をテストする場合の ping 送信：正常に機能し、エコー要求を返すことがわかっているネットワーク デバイスに対して、ASA のインターフェイスから ping を送信できます。エコーを受信した場合、中間にあるデバイスがすべて正常に動作し、物理的に正しく接続されていることが確認されたことになります。

ASA インターフェイスからの ping の送信

インターフェイスの基本的なテストを行う場合は、正常に機能し、中間通信パスを経由して応答を返すことがわかっているネットワーク デバイスに対して、ASA のインターフェイスから ping 送信を開始できます。基本的なテストの場合は、次の手順を必ず実行してください。

- 「既知の正常な」デバイスが、ASA のインターフェイスから送信された ping を受信することを確認します。ping を受信しない場合は、送信ハードウェアまたはインターフェイスのコンフィギュレーションに問題がある可能性があります。
- ASA のインターフェイスが正しく設定されているにもかかわらず、「既知の正常な」デバイスからエコー応答を受信しない場合は、インターフェイス ハードウェアの受信機能に問題があると考えられます。「既知の正常な」受信機能を持つ別のインターフェイスで、同じ「既知の正常な」デバイスに対して ping を送信してエコーを受信できる場合、最初のインターフェイスのハードウェアの受信機能に問題があると確認されたことになります。

ASA インターフェイスへの ping の送信

ASA のインターフェイスに ping を送信しようとする場合は、[Tools] > [Ping] の順に選択して、そのインターフェイスで ping 応答（ICMP エコー応答）がイネーブルになっていることを確認してください。ping 機能がディセーブルになっていると、ASA は他のデバイスやソフトウェア アプリケーションから検出されず、ASDM の ping ツールに応答しません。

ASA のインターフェイスを通過する ping

「既知の正常な」送信元からの他のタイプのネットワーク トラフィックが ASA を通過していることを確認するには、[Monitoring] > [Interfaces] > [Interface Graphs] または SNMP 管理ステーションを選択します。

内部ホストから外部ホストへの ping の送信をイネーブルにするには、ICMP インスペクションを設定します。[Configuration] > [Firewall] > [Service Policies] を選択します。

ping ツールのトラブルシューティング

ping を送信してエコーを受信しない場合は、ASA のコンフィギュレーションまたは動作にエラーがあることも原因として考えられます。必ずしも ping を送信した IP アドレスから応答がないことが原因であるとは限りません。ping ツールを使用して、ASA のインターフェイスから、インターフェイスに、またはインターフェイスを通過させて ping を送信する前に、次の基本的な確認を行ってください。

- インターフェイスが設定されていることを確認します。[Configuration] > [Device Setup] > [Interfaces] を選択します。
- スイッチやルータなど通信パスの中間デバイスで、他のタイプのネットワーク トラフィックが正常に配信されていることを確認します。
- 「既知の正常な」送信元からの他のタイプのトラフィックが通過することを確認します。[Monitoring] > [Interfaces] > [Interface Graphs] を選択します。

ping ツールの使い方

ping ツールを使用するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Ping] の順に選択します。

[Ping] ダイアログボックスが表示されます。

ステップ 2　[IP Address] フィールドに、ICMP エコー要求パケットの宛先 IP アドレスを入力します。

ping は、IPv6 アドレスもサポートします。

（注）　[Configuration] > [Firewall] > [Objects] > [Objects/Groups Names] ペインでホスト名が割り当てられている場合は、IP アドレスの代わりにホスト名を使用できます。

ステップ 3　（オプション）ドロップダウン リストから、エコー要求パケットを送信する ASA のインターフェイスを選択します。指定しない場合、ASA はルーティング テーブルを調べ、宛先アドレスを見つけて必要なインターフェイスを使用します。

ステップ 4　[Ping] をクリックして、指定したインターフェイスまたはデフォルトのインターフェイスから、指定した IP アドレスに ICMP エコー要求パケットを送信し、応答タイマーを開始します。

応答は [Ping Output] 領域に表示されます。IP アドレスへの ping は 3 回送信され、結果は次のフィールドに表示されます。

- ping が送信されたデバイスの IP アドレスまたはデバイス名（設定されている場合）。デバイス名が割り当てられている場合、結果が応答なしの場合でもそのデバイス名が表示される場合があります。

- ping が送信されると、指定した最大値つまりタイムアウト値でミリ秒タイマーが作動します。このタイマーは、異なるルートやアクティビティ レベルの相対応答時間をテストするのに便利です。
- ping の実行結果の例：

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ping が失敗した場合、実行結果は次のようになります。

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

ステップ 5　新しい IP アドレスを入力するには、[Clear Screen] をクリックして、[Ping output] 領域から前の応答を削除します。

トレースルートによるパケット ルーティングの決定

Traceroute ツールにより、パケットが宛先に到着するまでのルートを判断できます。このツールは、送信される各プローブの結果を出力します。出力の各行が 1 つの TTL 値に対応します（昇順）。次の表に、このツールによって出力される記号の一覧を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
nn msec	各ノードで、指定した数のプローブのラウンドトリップにかかる時間（ミリ秒）。
!N.	ICMP ネットワークに到達できません。
!H	ICMP ホストに到達できません。
!P	ICMP に到達できません。
!A	ICMP が設定によって禁止されています。
?	ICMP の原因不明のエラーが発生しました。

Traceroute ツールを使用するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Traceroute] の順に選択します。

[Traceroute] ダイアログボックスが表示されます。

ステップ 2　ルートをトレースするホスト名または IP アドレスを入力します。ホスト名が指定されている場合は、[Configuration] > [Firewall] > [Objects] > [Service Objects/Groups] の順に選択して名前を定義するか、またはこのツールをイネーブルにするように DNS サーバを設定して、ホスト名を IP アドレスに解決します。

ステップ 3　応答を待機しているときの接続タイムアウト時間を秒単位で入力します。デフォルトは 3 秒です。

ステップ 4　UDP プローブ メッセージで使用される宛先ポートを入力します。デフォルトは 33434 です。

ステップ 5　各 TTL レベルで送信されるプローブ数を入力します。デフォルトは 3 です。

ステップ 6　最初のプローブの最小および最大 TTL 値を指定します。デフォルトの最小値は 1 です。値を大きくすると、始めに表示される既知のホップが少なくなります。デフォルトの最大値は 30 です。トレースルートは、パケットが宛先に到達するか、または最大値に達すると終了します。

ステップ 7　[Specify source interface or IP address] チェックボックスをオンにします。ドロップダウン リストから、パケット トレースの送信元インターフェイスまたは IP アドレスを選択します。この IP アドレスはいずれかのインターフェイスの IP アドレスにする必要があります。トランスペアレント モードの場合は、ASA の管理 IP アドレスにする必要があります。

ステップ 8　名前解決が設定されている場合、使用されたホップ名を出力結果に表示するには、[Reverse Resolve] チェックボックスをオンにします。出力結果に IP アドレスを表示するには、このチェックボックスをオフにします。

ステップ 9　UDP プローブ パケットの代わりに ICMP プローブ パケットを使用するよう指定するには、[Use ICMP] チェックボックスをオンにします。

ステップ 10　[Trace Route] をクリックしてトレースルートを開始します。

[Traceroute Output] 領域に、トレースルートの結果についての詳細なメッセージが表示されます。

ステップ 11　[Clear Output] をクリックして新しいトレースルートを開始します。

パケット トレーサによるパケットの追跡

パケット トレーサ ツールは、パケット スニフィングとネットワーク障害箇所特定のためのパケット追跡を実現するとともに、パケットに関する詳細情報と ASA によるパケットの処理方法を示します。コンフィギュレーション コマンドがパケット ドロップの原因ではない場合は、パケット トレーサ ツールを実行すると、その原因に関する情報が読みやすい形式で表示されます。

パケット トレーサ ツールでは次のことができます。

- ASA を通過するパケットの寿命をトレースして、パケットが正しく動作しているかどうかを確認する。
- ネットワーク内にドロップするすべてのパケットをデバッグする。
- コンフィギュレーションが意図したとおりに機能しているかを確認する。
- パケットに適用可能なすべてのルール、およびルールが追加される原因となった CLI コマンドを表示する。
- データ パス内でのパケット変化を時系列で表示する。
- データ パスにトレーサ パケットを挿入する。
- ユーザ アイデンティティおよび FQDN に基づいて IPv4 アドレスまたは IPv6 アドレスを検索する。
- 特定のセッションが許可または拒否された原因をデバッグする。
- どのセキュリティ グループ タグ（SGT）の値が使用されているか（つまり、パケットの SGT、IP-SGT Manager、またはインターフェイスに対して設定されている **policy static sgt** コマンドのいずれから取得したものか）を特定する。
- 適用されているセキュリティ グループ ベースのセキュリティ ポリシーを特定する。

パケット トレーサを使用するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Packet Tracer] の順に選択します。

[Cisco ASDM Packet Tracer] ダイアログボックスが表示されます。

ステップ 2　ドロップダウン リストからパケット トレースの送信元インターフェイスを選択します。

ステップ 3　パケット トレースのプロトコル タイプを指定します。指定できるプロトコル タイプは、ICMP、IP、TCP、および UDP です。

ステップ 4　[SGT number] チェックボックスをオンにします。Cisco TrustSec ソリューションに統合されたときに ASA から送信されるセキュリティ グループ タグのパケット トレースをイネーブルにするには、セキュリティ グループ タグ番号を入力します。有効なセキュリティ グループ タグ番号の範囲は 0 ～ 65533 です。

ステップ 5　[Source] ドロップダウン リストで、次のいずれかのオプションを選択します。

- IP Address
- User
- FQDN
- Security Tag
- Security Name

Cisco TrustSec ソリューションに統合されたときに、ASA から送信されたパケットをトレースする場合は [Security Tag] または [Security Name] オプションを選択します。セキュリティ名は Cisco ISE 上で作成され、セキュリティ グループに対応するわかりやすい名前が付けられます。

セキュリティ ポリシーがそのセキュリティ タグまたはセキュリティ名付きで ASA に設定されると、ASA はそのポリシーを実行します （セキュリティ タグまたはセキュリティ名を含む ASA にセキュリティ ポリシーを作成できます。セキュリティ グループの名前に基づいてポリシーを実行するには、ASA はセキュリティ名をセキュリティ タグにマッピングするためにセキュリティ グループ テーブルが必要です)。

ASA を Cisco TrustSec ソリューションに統合するための設定に関する詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

ステップ 6　ユーザが [Source] ドロップダウン リストで選択したオプションに基づいて、トレースする項目に対応するテキストを入力します。たとえば、[Source IP Address] フィールドに、パケット トレースの送信元 IP アドレスを入力します。

ステップ 7　TCP および UDP の場合のみ、ドロップダウン リストから、パケット トレースの送信元ポートを選択します。

ステップ 8　[Destination] ドロップダウン リストで、次のいずれかのオプションを選択します。

- IP Address
- FQDN
- Security Tag
- Security Name

ステップ 9　[Destination] ドロップダウン リストで選択したオプションに基づいて、トレースする項目に対応するテキストを入力します。たとえば、[Destination IP Address] フィールドに、パケット トレースの送信元 IP アドレスを入力します。

ステップ 10　TCP および UDP の場合のみ、ドロップダウン リストから、パケット トレースの宛先ポートを選択します。

ステップ 11　ICMP の場合のみ、[Type] ドロップダウン リストから、パケット トレースのタイプを選択します。次に、該当するフィールドにトレース コードとトレース ID を入力します。

ステップ 12　IP の場合のみ、[Protocol] フィールドにプロトコル番号を入力します。有効値の範囲は 0 ～ 255 です。

ステップ 13　[Start] をクリックして、パケットをトレースします。

[Information Display Area] に、パケット トレースの結果に関する詳細情報が表示されます。

（注）　パケット トレースをグラフィカルに表現するには、[Show animation] チェックボックスをオンにします。

ステップ 14　[Clear] をクリックして新しいパケット トレースを開始します。

パフォーマンスのモニタリング

ASA のパフォーマンス情報をグラフ形式または表形式で表示するには、次の手順を実行します。

ステップ 1　ASDM メイン ウィンドウで、[Monitoring] > [Properties] > [Connection] > [Graphs] > [Perfmon] の順に選択します。

ステップ 2　[Available Graphs] リストからエントリを 1 つ以上選択し、[Add] をクリックして、それらのエントリを [Selected Graphs] リストに移動します。エントリを [Selected Graphs] リストから削除するには、[Remove] をクリックします。使用可能なオプションは次のとおりです。

- [AAA Perfmon]：ASA の AAA パフォーマンス情報を表示します。
- [Inspection Perfmon]：ASA の検査パフォーマンス情報を表示します。
- [Web Perfmon]：URL アクセスおよび URL サーバ要求などの ASA の Web パフォーマンス情報を表示します。
- [Connections Perfmon]：ASA の接続パフォーマンス情報を表示します。
- [Xlate Perfmon]：ASA の NAT パフォーマンス情報を表示します。

1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

ステップ 3　既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、[Graph Window Title] フィールドに新しいウィンドウ タイトルを入力します。

ステップ 4　[Show Graphs] をクリックして、新しいグラフ ウィンドウまたは更新したグラフ ウィンドウにパフォーマンス統計情報を表示します。

ステップ 5　[Table] タブをクリックして、同じパフォーマンス統計情報を表形式で表示します。

ステップ 6　いずれかのタブ上の [View] ドロップダウン リストから、情報を更新して表示する期間を [Real-time, data every 10 sec]、[Last 10 minutes, data every 10 sec]、[Last 60 minutes, data every 1 min]、[Last 12 hours, data every 12 minutes]、または [Last 5 days, data every two hours] から選択します。

ステップ 7　（オプション）[Export] をクリックして、[Export Graph Data] ダイアログボックスを表示します。エクスポートするよう選択されたパフォーマンス統計情報は、すでにオンになっています。

ステップ 8　（オプション）[Export] を再度クリックして、[Save] ダイアログボックスを表示します。

ステップ 9　（オプション）[Save] をクリックして、パフォーマンス統計情報をローカル ドライブ上のテキスト ファイル（.txt）に保存し、後で参照できるようにします。

ステップ 10　（オプション）[Print] をクリックして、[Print Graph] ダイアログボックスを表示します。

ステップ 11　（オプション）ドロップダウン リストからグラフまたはテーブル名を選択し、[Print] をクリックして、[Print] ダイアログボックスを表示します。

ステップ 12　（オプション）[OK] をクリックして、選択したパフォーマンス統計情報を印刷します。

システム リソースのモニタリング

- 「ブロック」（P.15-10）
- 「CPU」（P.15-11）
- 「メモリ」（P.15-11）

ブロック

空きメモリ ブロックおよび使用中のメモリ ブロックを表示するには、次の手順を実行します。

ステップ 1　ASDM メイン ウィンドウで、[Monitoring] > [Properties] > [System Resources Graphs] > [Blocks] の順に選択します。

ステップ 2　[Available Graphs] リストからエントリを 1 つ以上選択し、[Add] をクリックして、それらのエントリを [Selected Graphs] リストに移動します。エントリを [Selected Graphs] リストから削除するには、[Remove] をクリックします。使用可能なオプションは次のとおりです。

- [Blocks Used]：ASA で使用中のメモリ ブロックを表示します。
- [Blocks Free]：ASA の空きメモリ ブロックを表示します。

1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

ステップ 3　既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、[Graph Window Title] フィールドに新しいウィンドウ タイトルを入力します。

ステップ 4　[Show Graphs] をクリックして、新しいグラフ ウィンドウまたは更新したグラフ ウィンドウにシステム リソース統計情報を表示します。

ステップ 5　[Table] タブをクリックして、同じパフォーマンス統計情報を表形式で表示します。

ステップ 6　いずれかのタブ上の [View] ドロップダウン リストから、情報を更新して表示する期間を [Real-time, data every 10 sec]、[Last 10 minutes, data every 10 sec]、[Last 60 minutes, data every 1 min]、[Last 12 hours, data every 12 minutes]、または [Last 5 days, data every two hours] から選択します。

ステップ 7　（オプション）[Export] をクリックして、[Export Graph Data] ダイアログボックスを表示します。エクスポートするよう選択されたメモリ ブロック統計情報は、すでにオンになっています。

ステップ 8　（オプション）[Export] を再度クリックして、[Save] ダイアログボックスを表示します。

ステップ 9　（オプション）[Save] をクリックして、メモリ ブロック統計情報をローカル ドライブ上のテキスト ファイル（.txt）に保存し、後で参照できるようにします。

ステップ 10　（オプション）[Print] をクリックして、[Print Graph] ダイアログボックスを表示します。

ステップ 11　（オプション）ドロップダウン リストからグラフまたはテーブル名を選択し、[Print] をクリックして、[Print] ダイアログボックスを表示します。

ステップ 12　（オプション）[OK] をクリックして、選択したメモリ ブロック統計情報を印刷します。

CPU

CPU 使用率を表示するには、次の手順を実行します。

ステップ 1　ASDM メイン ウィンドウで、[Monitoring] > [Properties] > [System Resources Graphs] > [CPU] の順に選択します。

ステップ 2　[Available Graphs] リストからエントリを 1 つ以上選択し、[Add] をクリックして、それらのエントリを [Selected Graphs] リストに移動します。エントリを [Selected Graphs] リストから削除するには、[Remove] をクリックします。

1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

ステップ 3　既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、[Graph Window Title] フィールドに新しいウィンドウ タイトルを入力します。

ステップ 4　[Show Graphs] をクリックして、新しいグラフ ウィンドウまたは更新したグラフ ウィンドウにシステム リソース統計情報を表示します。

ステップ 5　[Table] タブをクリックして、同じパフォーマンス統計情報を表形式で表示します。

ステップ 6　いずれかのタブ上の [View] ドロップダウン リストから、情報を更新して表示する期間を [Real-time, data every 10 sec]、[Last 10 minutes, data every 10 sec]、[Last 60 minutes, data every 1 min]、[Last 12 hours, data every 12 minutes]、または [Last 5 days, data every two hours] から選択します。

ステップ 7　（オプション）[Export] をクリックして、[Export Graph Data] ダイアログボックスを表示します。エクスポートするよう選択された CPU 使用率統計情報は、すでにオンになっています。

ステップ 8　（オプション）[Export] を再度クリックして、[Save] ダイアログボックスを表示します。

ステップ 9　（オプション）[Save] をクリックして、CPU 使用率統計情報をローカル ドライブ上のテキスト ファイル（.txt）に保存し、後で参照できるようにします。

ステップ 10　（オプション）[Print] をクリックして、[Print Graph] ダイアログボックスを表示します。

ステップ 11　（オプション）ドロップダウン リストからグラフまたはテーブル名を選択し、[Print] をクリックして、[Print] ダイアログボックスを表示します。

ステップ 12　（オプション）[OK] をクリックして、選択した CPU 使用率統計情報を印刷します。

メモリ

メモリ使用率を表示するには、次の手順を実行します。

ステップ 1　ASDM メイン ウィンドウで、[Monitoring] > [Properties] > [System Resources Graphs] > [Blocks] の順に選択します。

ステップ 2　[Available Graphs] リストからエントリを 1 つ以上選択し、[Add] をクリックして、それらのエントリを [Selected Graphs] リストに移動します。エントリを [Selected Graphs] リストから削除するには、[Remove] をクリックします。使用可能なオプションは次のとおりです。

- [Free Memory]：ASA の空きメモリを表示します。
- [Used Memory]：ASA の使用中のメモリを表示します。

1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

ステップ 3　既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、[Graph Window Title] フィールドに新しいウィンドウ タイトルを入力します。

ステップ 4　[Show Graphs] をクリックして、新しいグラフ ウィンドウまたは更新したグラフ ウィンドウにシステム リソース統計情報を表示します。

ステップ 5　[Table] タブをクリックして、同じパフォーマンス統計情報を表形式で表示します。

ステップ 6　いずれかのタブ上の [View] ドロップダウン リストから、情報を更新して表示する期間を [Real-time, data every 10 sec]、[Last 10 minutes, data every 10 sec]、[Last 60 minutes, data every 1 min]、[Last 12 hours, data every 12 minutes]、または [Last 5 days, data every two hours] から選択します。

ステップ 7　（オプション）[Export] をクリックして、[Export Graph Data] ダイアログボックスを表示します。エクスポートするよう選択されたメモリ使用率統計情報は、すでにオンになっています。

ステップ 8　（オプション）[Export] を再度クリックして、[Save] ダイアログボックスを表示します。

ステップ 9　（オプション）[Save] をクリックして、メモリ使用率統計情報をローカル ドライブ上のテキスト ファイル（.txt）に保存し、後で参照できるようにします。

ステップ 10　（オプション）[Print] をクリックして、[Print Graph] ダイアログボックスを表示します。

ステップ 11　（オプション）ドロップダウン リストからグラフまたはテーブル名を選択し、[Print] をクリックして、[Print] ダイアログボックスを表示します。

ステップ 12　（オプション）[OK] をクリックして、選択したメモリ使用率統計情報を印刷します。

接続のモニタリング

現在の接続を表形式で表示するには、ASDM メイン ウィンドウで、[Monitoring] > [Properties] > [Connections] の順に選択します。各接続は、次のパラメータにより識別されます。

- プロトコル
- 送信元：
  - セキュリティ ID
  - セキュリティ名
  - IP アドレス
  - ポート
- 宛先：
  - セキュリティ ID
  - セキュリティ名

  - IP アドレス
  - ポート
- 最後にパケットが送信または受信されてからのアイドル時間
- その接続で送信および受信されたトラフィックの量

プロセスごとの CPU 使用率のモニタリング

CPU で実行されているプロセスをモニタできます。特定のプロセスで使用される CPU の使用率に関する情報を取得できます。CPU 使用率の統計情報は降順で並べられ、使用率の最も高いプロセスが先頭に表示されます。また、プロセスごとの CPU に対する負荷に関する情報（記録時間の 5 秒前、1 分前、および 5 分前の情報）も含まれています。この情報は 5 秒おきに自動的に更新され、リアルタイムの統計情報が表示されます。ASDM では、30 秒おきに更新されます。

CPU 使用率をプロセスごとに表示するには、次の手順を実行します。

ステップ 1　ASDM メイン ウィンドウで、[Monitoring] > [Properties] > [Per-Process CPU Usage] の順に選択します。

ステップ 2　画面の自動リフレッシュを停止するには、[Stop auto-refresh] をクリックします。

ステップ 3　画面上の情報をローカルのテキスト ファイルに保存するには、[Save log to local file] をクリックします。

[Save] ダイアログボックスが表示されます。

ステップ 4　テキスト ファイルの名前を入力し、[Save] をクリックします。

CPU 使用率の範囲に応じてプロセスを色分けするには、[Configure CPU usage] をクリックします。

[Color Settings] ダイアログボックスが表示されます。

ステップ 5　範囲のオプション（49% 以下、50 ～ 79%、および 80% 以上）の中からいずれかを選択します。

ステップ 6　前景または背景のセルをクリックして [Pick a Color] ダイアログボックスを表示し、指定した範囲の前景色および背景色を選択します。

ステップ 7　[Swatches]、[HSB]、または [RGB] のいずれかのタブをクリックして、カラー パレットを選択します。完了したら、[OK] をクリックします。

ステップ 8　[OK] をクリックすると、色分けされたエントリが表示されます。

ステップ 9　[Refresh] をクリックすると、いつでも手動でデータをリフレッシュできます。

PART 5

高度なネットワーク保護

CHAPTER 16

ASA および Cisco クラウド Web セキュリティ

Cisco クラウド Web セキュリティ では、Software as a Service（SaaS）による Web セキュリティおよび Web フィルタリング サービスが提供されます。ネットワークでASAを使用している企業は、追加ハードウェアをインストールせずに クラウド Web セキュリティ サービスを使用できます。

ASA でクラウド Web セキュリティがイネーブルになっている場合、ASA は、選択された HTTP および HTTPS トラフィックを クラウド Web セキュリティ プロキシ サーバに透過的にリダイレクトします。クラウド Web セキュリティ プロキシ サーバは、コンテンツをスキャンし、Cisco ScanCenter で設定されたポリシーに基づいてトラフィックに関する警告を許可、ブロック、または送信して、許容範囲での使用を促進し、マルウェアからユーザを保護します。

ASA は、任意でアイデンティティ ファイアウォール（IDFW）および AAA ルールによりユーザを認証および識別できます。ASA は、ユーザ クレデンシャル（ユーザ名またはユーザ グループ、あるいはその両方を含む）を暗号化して、クラウド Web セキュリティにリダイレクトするトラフィックに含めます。クラウド Web セキュリティ サービスは、このユーザ クレデンシャルを使用して、ポリシーとトラフィックを照合します。また、ユーザベースのレポーティングでもこのクレデンシャルを使用します。ASA は、ユーザ認証を行わずに（オプションの）デフォルトのユーザ名またはグループ、あるいはその両方を指定できます。ただし、クラウド Web セキュリティ サービスがポリシーを適用するために、ユーザ名とグループは必要ありません。

サービス ポリシー ルールを作成するときに、クラウド Web セキュリティに送信するトラフィックをカスタマイズできます。また、サービス ポリシー ルールに一致する Web トラフィックのサブセットが最初に要求された Web サーバに代わりに直接移動し、クラウド Web セキュリティ にスキャンされないように、「ホワイトリスト」を設定できます。

プライマリおよびバックアップ クラウド Web セキュリティ プロキシ サーバを設定できます。ASA は各サーバを定期的にポーリングして、可用性を確認します。

（注） この機能は「ScanSafe」とも呼ばれるため、一部のコマンドには ScanSafe 名が表示されます。

- 「Cisco クラウド Web セキュリティについて」（P.16-2）
- 「Cisco クラウド Web セキュリティのライセンス要件」（P.16-7）
- 「クラウド Web セキュリティの前提条件」（P.16-7）
- 「ガイドラインと制限事項」（P.16-8）
- 「デフォルト設定」（P.16-9）
- 「Cisco クラウド Web セキュリティ の設定」（P.16-9）
- 「クラウド Web セキュリティのモニタ」（P.16-27）
- 「関連資料」（P.16-28）
- 「Cisco クラウド Web セキュリティの機能の履歴」（P.16-28）

Cisco クラウド Web セキュリティについて

- 「クラウド Web セキュリティへの Web トラフィックのリダイレクト」（P.16-2）
- 「ユーザ認証およびクラウド Web セキュリティ」（P.16-2）
- 「認証キー」（P.16-3）
- 「ScanCenter ポリシー」（P.16-4）
- 「クラウド Web セキュリティのアクション」（P.16-5）
- 「ホワイトリストを使用したスキャンのバイパス」（P.16-6）
- 「IPv4 および IPv6 のサポート」（P.16-6）
- 「プライマリ プロキシ サーバからバックアップ プロキシ サーバへのフェールオーバー」（P.16-7）

クラウド Web セキュリティへの Web トラフィックのリダイレクト

エンド ユーザが HTTP または HTTPS 要求を送信すると、ASA はその要求を受信し、オプションでユーザやグループの情報を取得します。トラフィックがクラウド Web セキュリティの ASA サービス ポリシー ルールと一致した場合、ASA は要求をクラウド Web セキュリティ プロキシ サーバにリダイレクトします。ASA は、プロキシ サーバへの接続のリダイレクトによって、エンド ユーザとクラウド Web セキュリティ プロキシ サーバの間の仲介役として機能します。ASA は、クライアント要求の宛先 IP アドレスおよびポートを変更し、クラウド Web セキュリティに固有の HTTP ヘッダーを追加して、クラウド Web セキュリティ プロキシ サーバに変更された要求を送信します。クラウド Web セキュリティ HTTP ヘッダーには、ユーザ名、ユーザ グループなど、さまざまな種類の情報が含まれています（使用可能な場合）。

ユーザ認証およびクラウド Web セキュリティ

ユーザ アイデンティティは、クラウド Web セキュリティでポリシーを適用するために使用できます。また、ユーザ アイデンティティは、クラウド Web セキュリティ レポーティングにも役立ちます。クラウド Web セキュリティを使用するには、ユーザ アイデンティティは必要はありません。クラウド Web セキュリティ ポリシーのトラフィックを識別する他の方法があります。

ASA は、ユーザのアイデンティティを決定したり、デフォルト アイデンティティを提供したりする次の方式をサポートします。

- AAA ルール：ASA が AAA ルールを使用してユーザ認証を実行すると、ユーザ名が AAA サーバまたはローカル データベースから取得されます。AAA ルールによるアイデンティティには、グループ情報が含まれていません。設定されている場合は、デフォルトのグループが使用されます。AAA ルールの設定については、従来の機能ガイドを参照してください。
- IDFW：ASA が Active Directory（AD）で IDFW を使用すると、アクセス ルールなどの機能またはサービス ポリシーで ACL を使用するか、ユーザ アイデンティティ モニタを設定してユーザ アイデンティティ情報を直接ダウンロードして、ユーザやグループをアクティブ化したときに、AD エージェントからユーザ名およびグループが取得されます。

  IDFW の設定方法については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。
- デフォルトのユーザ名とグループ：ASA は、ユーザ認証を使用せずに、クラウド Web セキュリティ サービス ポリシー ルールと一致するすべてのユーザのオプションのデフォルトのユーザ名やグループを使用します。

認証キー

各 ASA は、クラウド Web セキュリティから取得した認証キーを使用する必要があります。認証キーを使用して、クラウド Web セキュリティは、Web 要求に関連付けられた会社を識別し、ASA が有効なカスタマーに関連付けられていることを確認できます。

ASA では、2 つの認証キー（企業キーおよびグループ キー）のいずれか 1 つを使用できます。

- 「企業認証キー」（P.16-3）
- 「グループ認証キー」（P.16-3）

企業認証キー

企業認証キーは、企業内の複数の ASA で使用できます。このキーは、単に ASA のクラウド Web セキュリティ サービスをイネーブルにします。管理者は ScanCenter（https://scancenter.scansafe.com/portal/admin/login.jsp）でこのキーを生成します。後で使用するためにこのキーを電子メールで送信できます。ScanCenter では、後でこのキーを検索できません。ScanCenter には、最後の 4 桁だけが表示されます。詳細については、クラウド Web セキュリティのマニュアルを参照してください。マニュアルは、http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html から入手できます。

グループ認証キー

グループ認証キーは 2 つの機能を実行する各 ASA に固有の特別なキーです。

- 1 つの ASA のクラウド Web セキュリティ サービスをイネーブルにします。
- ASA からのすべてのトラフィックが識別されるため、ASA ごとに ScanCenter ポリシーを作成できます。

ポリシーにグループ認証キーを使用する方法については、「ScanCenter ポリシー」（P.16-4）を参照してください。

管理者は ScanCenter（https://scancenter.scansafe.com/portal/admin/login.jsp）でこのキーを生成します。後で使用するためにこのキーを電子メールで送信できます。ScanCenter では、後でこのキーを検索できません。ScanCenter には、最後の 4 桁だけが表示されます。詳細については、クラウド Web セキュリティのマニュアルを参照してください。マニュアルは、http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html から入手できます。

ScanCenter ポリシー

ScanCenter では、トラフィックは、ルールに一致するまで順にルールに照合されます。その後、クラウド Web セキュリティがルールの設定済みのアクションを適用します。ユーザ トラフィックはグループの関連付け（*ディレクトリ グループ*または*カスタム グループ*）に基づいて ScanCenter ポリシー ルールと照合できます。

- 「ディレクトリ グループ」（P.16-4）
- 「カスタム グループ」（P.16-4）
- 「グループおよび認証キーの相互運用の仕組み」（P.16-5）

ディレクトリ グループ

ディレクトリ グループはトラフィックが属するグループを定義します。グループが存在する場合、グループは、クライアント要求の HTTP ヘッダーに含まれています。ASA は、IDFW を設定すると HTTP ヘッダーにグループを含めます。IDFW を使用しない場合は、クラウド Web セキュリティ インスペクションの ASA ルールに一致するトラフィックのデフォルト グループを設定できます。

ディレクトリ グループを設定する場合、グループ名を正確に入力する必要があります。

- IDFW グループ名は次の形式で送信されます。

  domain-name\group-name

  ASA が IDFW グループ名を学習すると、ASA での形式は *domain-name\\group-name* となります。ただし、一般的な ScanCenter 表記に準拠させるため、ASA はバックスラッシュ（\）を 1 つだけ使用するように名前を変更します。

- デフォルト グループ名は次の形式で送信されます。

  [*domain*\]*group-name*

  ASA では、オプションのドメイン名を 2 つのバックスラッシュ（\\）が続くように設定する必要があります。ただし、一般的な ScanCenter 表記に準拠させるため、ASA はバックスラッシュ（\）を 1 つだけ使用するように名前を変更します。たとえば、「Cisco\\Boulder1」と指定すると、ASA は、グループ名をクラウド Web セキュリティに送信するときに、バックスラッシュ（\）を 1 つのみ使用する「Cisco\Boulder1」に変更します。

カスタム グループ

カスタム グループは、次の 1 つ以上の基準を使用して定義されます。

- ScanCenter グループ認証キー：カスタム グループのグループ認証キーを生成できます。その後、ASA を設定するときにこのグループ キーを識別すると、ASA からのすべてのトラフィックがグループ キーでタグ付けされます。

- 送信元 IP アドレス：カスタム グループの送信元 IP アドレスを特定できます。ASA サービス ポリシーが送信元 IP アドレスに基づくため、代わりに ASA で IP アドレスベースのポリシーを設定することもできます。
- ユーザ名：カスタム グループのユーザ名を識別できます。
  - IDFW ユーザ名は次の形式で送信されます。

    *domain-name**username*
  - RADIUS または TACACS+ を使用する場合、AAA ユーザ名は次の形式で送信されます。

    LOCAL*username*
  - LDAP を使用する場合、AAA ユーザ名は次の形式で送信されます。

    *domain-name**username*
  - デフォルトのユーザ名は、次の形式で送信されます。

    [*domain-name*\]*username*

    たとえば「ゲスト」としてデフォルトのユーザ名を設定する場合、ASA は「ゲスト」を送信します。「Cisco \ゲスト」としてデフォルトのユーザ名を設定する場合は、ASA は「Cisco \ゲスト」を送信します。

グループおよび認証キーの相互運用の仕組み

カスタム group+group キーが提供する ASA ごとのポリシーが必要ない場合は、企業キーを使用します。すべてのカスタム グループがグループ キーに関連付けられているわけではありません。キーを使用しないカスタム グループを使用して、IP アドレスまたはユーザ名を識別できます。また、キーを使用しないカスタム グループは、ディレクトリ グループを使用するルールとともにポリシー内で使用できます。

ASA ごとのポリシーが必要であり、グループ キーを使用している場合でも、ディレクトリ グループおよびキーを使用しないカスタム グループによって提供される照合機能を使用できます。この場合、グループ メンバーシップ、IP アドレス、またはユーザ名に基づいていくつかの例外を除いて ASA ベースのポリシーが必要になる場合があります。たとえば、すべての ASA 間で America\Management グループのユーザを除外する場合は、次の手順を実行します。

1. America\Management 用のディレクトリ グループを追加します。
2. このグループに対する免除ルールを追加します。
3. 免除ルールの後に各カスタム group+group キーのルールを追加して、ASA ごとのポリシーを適用します。
4. America\Management のユーザからのトラフィックは免除ルールに一致し、その他すべてのトラフィックは発信元の ASA のルールに一致します。

キー、グループ、およびポリシー ルールの組み合わせが可能です。

クラウド Web セキュリティのアクション

設定されたポリシーの適用後、クラウド Web セキュリティは、ユーザ要求をブロック、許可、またはユーザ要求に関する警告を送信します。

- 許可：クラウド Web セキュリティは、クライアント要求を許可する場合、最初の要求先サーバにアクセスし、データを取得します。サーバ応答が ASA に転送され、ここからユーザに転送されます。

- ブロック：クラウド Web セキュリティは、クライアント要求をブロックする場合、アクセスがブロックされたことをユーザに通知します。HTTP 302「Moved Temporarily」応答が、クライアント アプリケーションを クラウド Web セキュリティ プロキシ サーバでホストされている Web ページに送信され、ブロック エラー メッセージが表示されます。ASA はクライアントに 302 応答を転送します。
- 警告：サイトにアクセプタブル ユース ポリシー違反があることをクラウド Web セキュリティ プロキシ サーバが決定すると、サイトに関する警告ページが表示されます。警告を挿入し、接続要求をドロップすることも、警告をクリックし、要求されたサイトに進むこともできます。

ASA がプライマリまたはバックアップ クラウド Web セキュリティ プロキシ サーバに到達できない場合の、ASA による Web トラフィックの処理方法を選択できます。これにより、すべての Web トラフィックがブロックされたり、許可されたりする可能性があります。デフォルトでは、Web トラフィックをブロックします。

ホワイトリストを使用したスキャンのバイパス

AAA ルールまたは IDFW を使用する場合、その他の場合にはサービス ポリシー ルールに一致する特定のユーザまたはグループからの Web トラフィックがスキャンのためクラウド Web セキュリティ プロキシ サーバにリダイレクトされないように ASA を設定できます。クラウド Web セキュリティ スキャンをバイパスすると、ASA はプロキシ サーバに接続せず、最初に要求された Web サーバからコンテンツを直接取得します。Web サーバから応答を受け取ると、データをクライアントに送信します。このプロセスはトラフィックの「ホワイトリスト」といいます。

ACL を使用してクラウド Web セキュリティに送信するトラフィックのクラスを設定すると、ユーザまたはグループに基づいてトラフィックを免除する同じ結果を得ることができますが、ホワイトリストを使用した方がより簡単です。ホワイトリスト機能は、ユーザおよびグループだけに基づき、IP アドレスには基づかないことに注意してください。

IPv4 および IPv6 のサポート

クラウド Web セキュリティは、現在 IPv4 アドレスだけをサポートしています。IPv6 を内部的に使用する場合は、クラウド Web セキュリティに送信する必要がある IPv6 フローに対して NAT 64 を実行する必要があります。

次の表に、クラウド Web セキュリティ リダイレクションでサポートされるクラス マップ トラフィックを示します。

クラス マップ トラフィック	クラウド Web セキュリティ インスペクション
IPv4 から IPv4	サポートあり
IPv6 から IPv4（NAT64 を使用）	サポートあり
IPv4 から IPv6	未サポート
IPv6 から IPv6	未サポート

プライマリ プロキシ サーバからバックアップ プロキシ サーバへのフェールオーバー

Cisco クラウド Web セキュリティ サービスに登録すると、プライマリ クラウド Web セキュリティ プロキシ サーバとバックアップ プロキシ サーバが割り当てられます。

クライアントがプライマリ サーバに到達できない場合、ASA は可用性を判定するためにタワーのポーリングを開始します。（クライアントのアクティビティが存在しない場合、ASA は 15 秒ごとにポーリングします）。設定された回数だけ再試行してもプロキシ サーバが使用できない場合（デフォルトは 5 回。この設定は設定可能）、サーバは到達不能として宣言され、バックアップ プロキシ サーバがアクティブになります。

クライアントまたは ASA が、再試行回数に到達する前に少なくとも 2 回連続してサーバに到達できる場合、ポーリングは停止し、タワーはアクセス可能であると判定されます。

バックアップ サーバへのフェールオーバー後、ASA はプライマリ サーバをポーリングし続けます。プライマリ サーバが到達可能になると、ASA はプライマリ サーバの使用に戻ります。

Cisco クラウド Web セキュリティのライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	ASA とクラウド Web セキュリティ サーバ間のトラフィックを暗号化する高度暗号化（3DES/AES）ライセンス。

クラウド Web セキュリティ側では、Cisco クラウド Web セキュリティ ライセンスを購入し、ASA が処理するユーザの数を特定する必要があります。その後、ScanCenter にログインし、認証キーを生成します。

クラウド Web セキュリティの前提条件

（オプション）ユーザ認証の前提条件

クラウド Web セキュリティにユーザ アイデンティティ情報を送信するには、ASA で次のいずれかを設定します。

- AAA ルール（ユーザ名のみ）：従来の機能ガイドを参照してください。
- IDFW （ユーザ名およびグループ）：『一般的な操作のコンフィギュレーション ガイド』を参照してください。

（オプション）完全修飾ドメイン名の前提条件

サービス ポリシー ルールまたはクラウド Web セキュリティ サーバに対して ACL で FQDN を使用する場合は、『一般的な操作のコンフィギュレーション ガイド』に従って ASA の DNS サーバを設定する必要があります。

ガイドラインと制限事項

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

マルチ コンテキスト モードでは、サーバ設定はシステム内だけで使用でき、サービス ポリシー ルールの設定はセキュリティ コンテキスト内だけで使用できます。

各コンテキストには、必要に応じて独自の認証キーを設定できます。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

IPv6 のガイドライン

IPv6 はサポートされません。「IPv4 および IPv6 のサポート」（P.16-6）を参照してください。

その他のガイドライン

- クラウド Web セキュリティは、ASA クラスタリングではサポートされません。
- クライアントレス SSL VPN はクラウド Web セキュリティではサポートされません。クラウド Web セキュリティの ASA サービス ポリシーからクライアントレス SSL VPN トラフィックを免除してください。
- クラウド Web セキュリティ プロキシ サーバへのインターフェイスがダウンすると、**show scansafe server** コマンドは、約 15 ～ 25 分間、両方のサーバを示します。この状態が発生する原因は、ポーリング メカニズムがアクティブな接続に基づいていること、また、そのインターフェイスがダウンしており、ゼロ接続を示し、ポーリング時間が最も長い方法が使用されることなどです。
- クラウド Web セキュリティは、ASA CX モジュールではサポートされません。同じトラフィックに対して ASA CX アクションおよびクラウド Web セキュリティ インスペクションの両方を設定した場合、ASA は ASA CX アクションのみを実行します。
- クラウド Web セキュリティ インスペクションは同じトラフィックの HTTP インスペクションと互換性があります。HTTP インスペクションは、デフォルト グローバル ポリシーの一部としてデフォルトでイネーブルになっています。
- クラウド Web セキュリティは、別の接続に対して同じ送信元ポートおよび IP アドレスを使用できる可能性がある拡張 PAT またはアプリケーションではサポートされません。たとえば、2 つの異なる接続（別個のサーバへの接続）が拡張 PAT を使用する場合、これらの接続は別個の宛先によって区別されているため、ASA は、両方の接続変換に同じ送信元 IP および送信元ポートを再利用する可能性があります。ASA がこれらの接続をクラウド Web セキュリティ サーバにリダイレクトすると、宛先がクラウド Web セキュリティ サーバの IP アドレスおよびポート（デフォルトは 8080）に置き換えられます。その結果、接続は両方とも、同じフロー（同じ送信元 IP/ポートおよび宛先 IP/ポート）に属しているように見え、リターン トラフィックが適切に変換解除されません。
- この Default Inspection Traffic トラフィック クラスには、クラウド Web セキュリティ インスペクションのデフォルト ポートは含まれません（80 および 443）。

デフォルト設定

デフォルトでは、Cisco クラウド Web セキュリティはイネーブルになりません。

Cisco クラウド Web セキュリティ の設定

- 「クラウド Web セキュリティ プロキシ サーバとの通信の設定」（P.16-9）
- 「（マルチ コンテキスト モード）セキュリティ コンテキストごとのクラウド Web セキュリティの許可」（P.16-10）
- 「クラウド Web セキュリティにトラフィックを送信するサービス ポリシーの方法」（P.16-10）
- 「（オプション）ホワイトリストに記載されたトラフィックの設定　」（P.16-24）
- 「クラウド Web セキュリティ ポリシーの設定」（P.16-27）

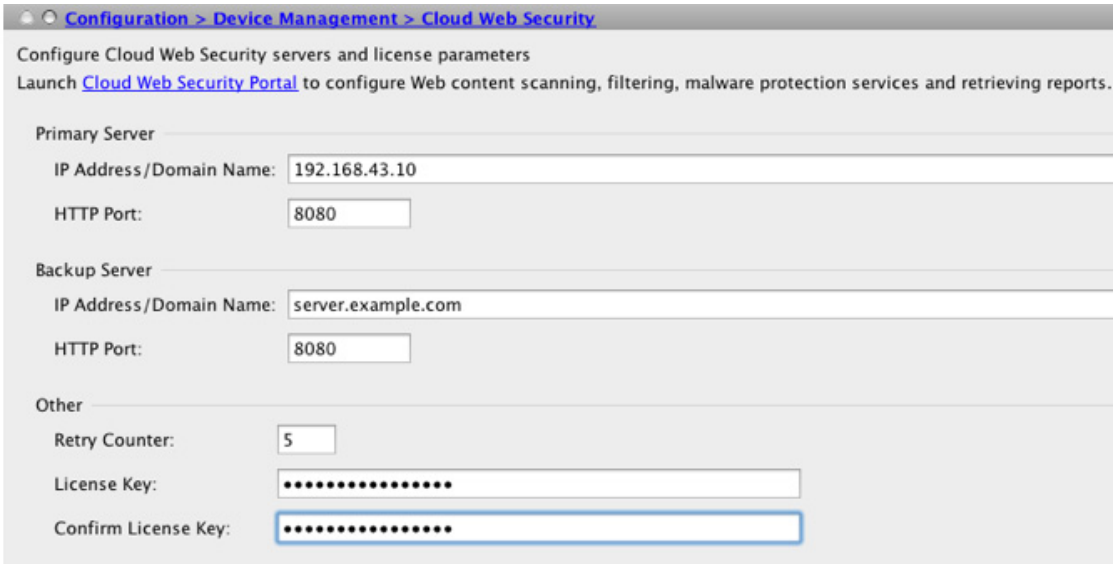
クラウド Web セキュリティ プロキシ サーバとの通信の設定

ガイドライン

公開キーは ASA ソフトウェアに組み込まれているため、設定する必要がありません。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Cloud Web Security] を選択します。



ステップ 2　[Primary Server] 領域で、次の情報を入力します。

- [IP Address/Domain Name]：プライマリ サーバの IPv4 アドレスまたは FQDN を入力します。

- [HTTP Port]：プライマリ サーバの HTTP ポート（トラフィックをリダイレクトする必要があるポート）を入力します。デフォルトでは、ポートは 8080 です。リダイレクトするポートを変更しない限り、この値を変更しないでください。

ステップ 3　[Backup Server] 領域で、次の情報を入力します。

- [IP Address/Domain Name] : バックアップ サーバの IPv4 アドレスまたは FQDN を入力します。
- [HTTP Port]：バックアップ サーバの HTTP ポート（トラフィックをリダイレクトする必要があるポート）を入力します。デフォルトでは、ポートは 8080 です。有効な値は 1 ～ 65535 です。

ステップ 4　[Other] 領域で、次の情報を入力します。

- [Retry Counter]：サーバが到達不能であると判定する前に、クラウド Web セキュリティ プロキシ サーバに対するポーリングに連続して失敗した回数を示す値を入力します。ポーリングは、30 秒ごとに実行されます。有効な値は 2 ～ 100 で、デフォルトは 5 です。
- [License Key]：要求の送信元の組織を示すために、ASA が クラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。認証キーは 16 バイトの 16 進数です。「認証キー」（P.16-3）を参照してください。
- [Confirm License Key]：認証キーを確認します。

ステップ 5　[Apply] をクリックします。

（マルチ コンテキスト モード）セキュリティ コンテキストごとのクラウド Web セキュリティの許可

マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可する必要があります。詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

（注）　管理コンテキストおよび特定のコンテキスト両方の Scansafe タワーに対応するルートを設定する必要があります。これは Scansafe タワーがアクティブ/アクティブ フェールオーバーのシナリオで到達不能にならないことを保障します。

クラウド Web セキュリティにトラフィックを送信するサービス ポリシーの方法

サービス ポリシーは、複数のサービス ポリシー ルールで構成され、グローバルに適用されるか、またはインターフェイスごとに適用されます。各サービス ポリシー ルールでは、クラウド Web セキュリティへのトラフィックを送信するか（Match）、またはクラウド Web セキュリティからのトラフィックを除外するか（Do Not Match）のいずれかを指定できます。インターネット宛に送信されるトラフィックのルールを作成します。これらのルールの順序は重要です。ASA がパケットを転送するか除外するかを判断する場合、ASA は、ルールがリストされている順序で、各ルールによってパケットをテストします。いずれかのルールに合致した場合、それ以降のルールはチェックされません。たとえば、すべてのトラフィックが明示的に一

致するルールをポリシーの冒頭に作成した場合、残りのステートメントは一切チェックされません。ポリシーの追加後、必要に応じてルールの順序を変更できます。

サービス ポリシー ルールの詳細については、第 1 章「サービス ポリシー」を参照してください。

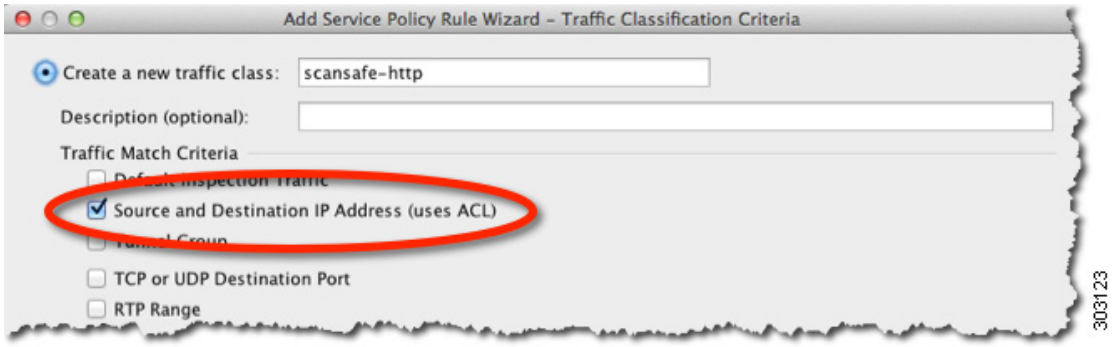
前提条件

（オプション）ホワイトリストを使用して一部のトラフィックをクラウド Web セキュリティへの送信から免除する必要がある場合は、サービス ポリシー ルールでホワイトリストを参照できるように、最初に「（オプション）ホワイトリストに記載されたトラフィックの設定 」（P.16-24）に従ってホワイトリストを作成します。

手順の詳細

ステップ 1　サービス ポリシー ルールを追加するには、[Configuration] > [Firewall] > [Service Policy Rules] を選択し、[Add] > [Service Policy Rule] をクリックします。

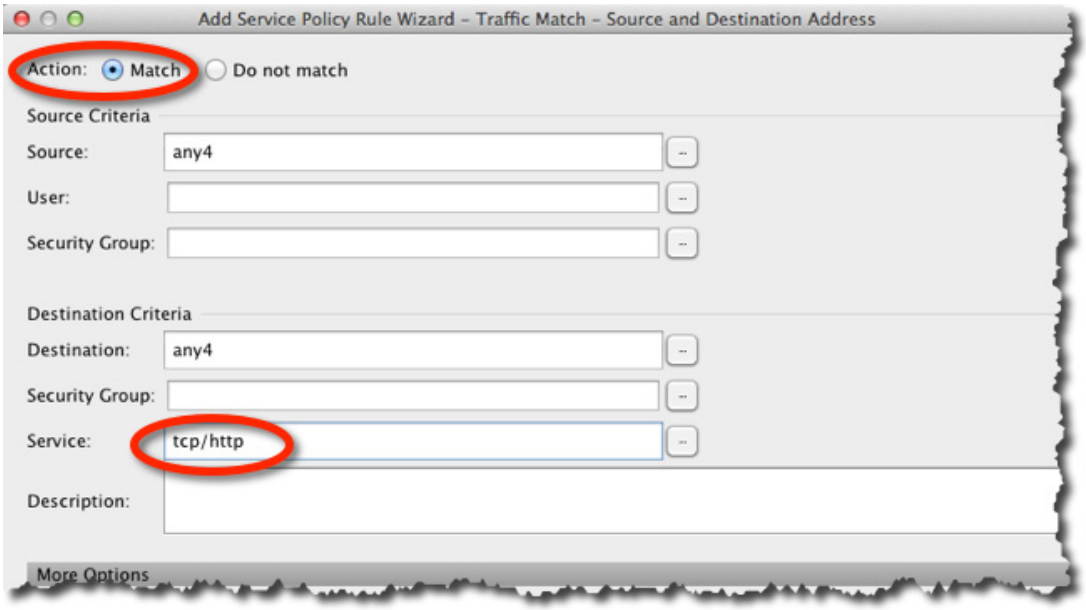
ステップ 2　[Service Policy] ダイアログボックスで、新しいサービス ポリシーの一部としてクラウド Web セキュリティを設定するか、または、既存のサービス ポリシーを編集できます。[Next] をクリックします。



ステップ 3　[Traffic Classification Criteria] ダイアログボックスで、トラフィック クラスに名前を付け（またはデフォルト名を受け入れて）、[Create a new traffic class] オプションを選択したままにし、[Source and Destination IP address (Uses ACL)] をクリックして、[Next] をクリックします。

このタイプの新しいトラフィック クラスを作成する場合は、最初にアクセス コントロール エントリ（ACE）を 1 つだけ指定できます。ルールを追加した後は、同じインターフェイスまたはグローバル ポリシーに新しいルールを追加し、それから [Traffic Classification] ダイアログボックスで [Add rule to existing traffic class] を指定することによって、ACE を追加できます。

[Traffic Match - Source and Destination] ダイアログボックスが表示されます。



a. [Match] または [Do Not Match] をクリックします。

[Match] は送信元および宛先に一致するトラフィックがクラウド Web セキュリティに送信されるように指定します。[Do Not Match] は一致したトラフィックをクラウド Web セキュリティから除外します。他のトラフィックに一致する、または一致しないように指定する追加のルールを後で追加できます。

ルールを作成する場合は、インターネット宛ての適切なトラフィックに一致し、他の内部ネットワーク宛てのトラフィックには一致しないようにする方法を考慮します。たとえば、宛先が DMZ の内部サーバである場合に内部トラフィックがクラウド Web セキュリティに送信されないようにするには、DMZ へのトラフィックを免除する ACL に拒否 ACE を追加します。

b. [Source Criteria] 領域で、送信元 IP アドレスまたはネットワーク オブジェクト、オプションの IDFW ユーザ名またはグループ、および任意の TrustSec セキュリティ グループを入力または参照します。

c. [Destination Criteria] 領域で、宛先 IP アドレスまたはネットワーク オブジェクトおよび任意の TrustSec セキュリティ グループを入力または参照します。

FQDN ネットワーク オブジェクトは、特定のサーバへのトラフィックへの一致または除外に役立つ場合があります。

d. [Service] フィールドに、「http」または「https」を入力し、[Next] をクリックします。

（注） クラウド Web セキュリティは HTTP および HTTPS トラフィックだけで動作します。各トラフィックのタイプは、ASA によって個別に処理されます。このため、HTTP-only ルールおよび HTTPS-only ルールを作成する必要があります。

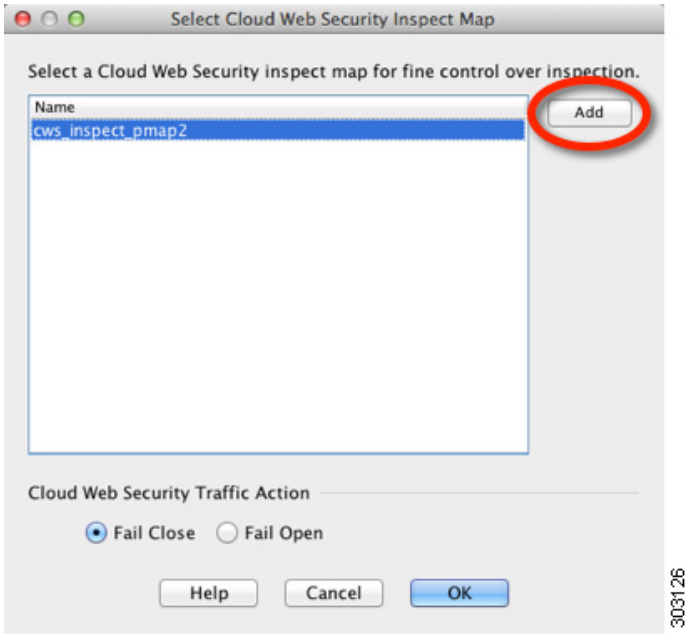
[Rule Actions] ダイアログボックスが表示されます。

ステップ 4　[Protocol Inspection] タブで、[Cloud Web Security] チェックボックスをオンにします。

ステップ 5　[Configure] をクリックし、トラフィック アクション（フェール オープンまたはフェール クローズ）を設定して、インスペクション ポリシー マップを追加します。

インスペクション ポリシー マップでは、ルールに不可欠なパラメータを設定し、任意で選択ホワイト リストを識別します。クラウド Web セキュリティに送信するトラフィックのクラスごとにインスペクション ポリシー マップが必要です。[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [Cloud Web Security] ペインで、インスペクション ポリシー マップを事前に設定することもできます。

[Select Cloud Web Security Inspect Map] ダイアログボックスが表示されます。

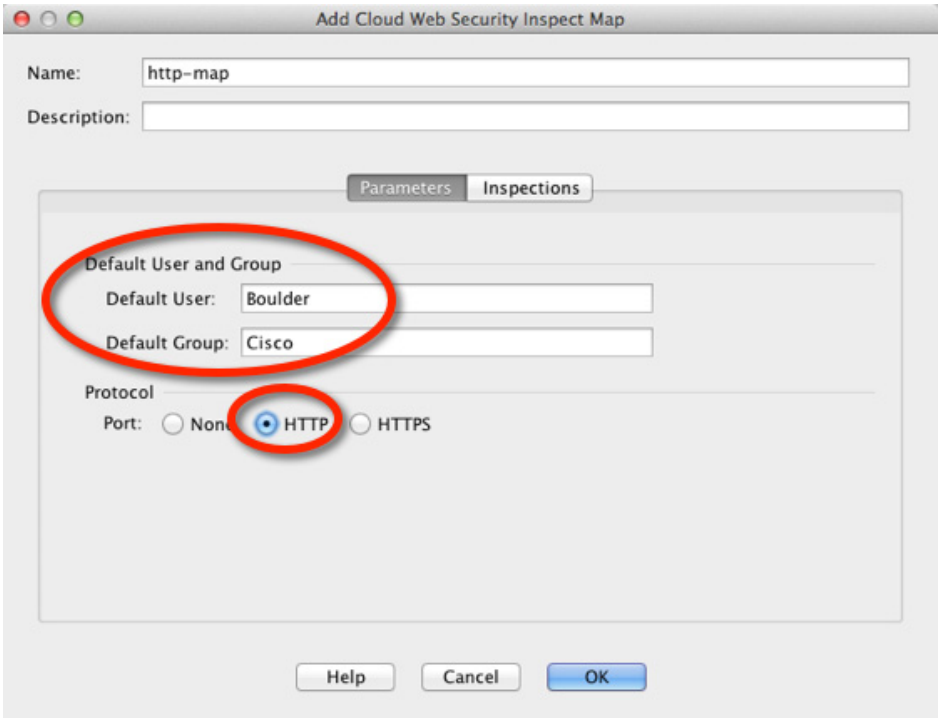


a. [Cloud Web Security Traffic Action] で、次のいずれかを選択します。
   - [Fail Close]：クラウド Web セキュリティ サーバを使用できない場合、すべてのトラフィックをドロップします。
   - [Fail Open]：クラウド Web セキュリティ サーバを使用できない場合、ASA を通過するトラフィックを許可します。

b. 既存のインスペクション ポリシー マップを選択するか、[Add] ボタンを使用して追加します。

c. [Add] をクリックして、新しいインスペクション ポリシー マップを追加します。

[Add Cloud Web Security Inspect Map] ダイアログボックスが表示されます。



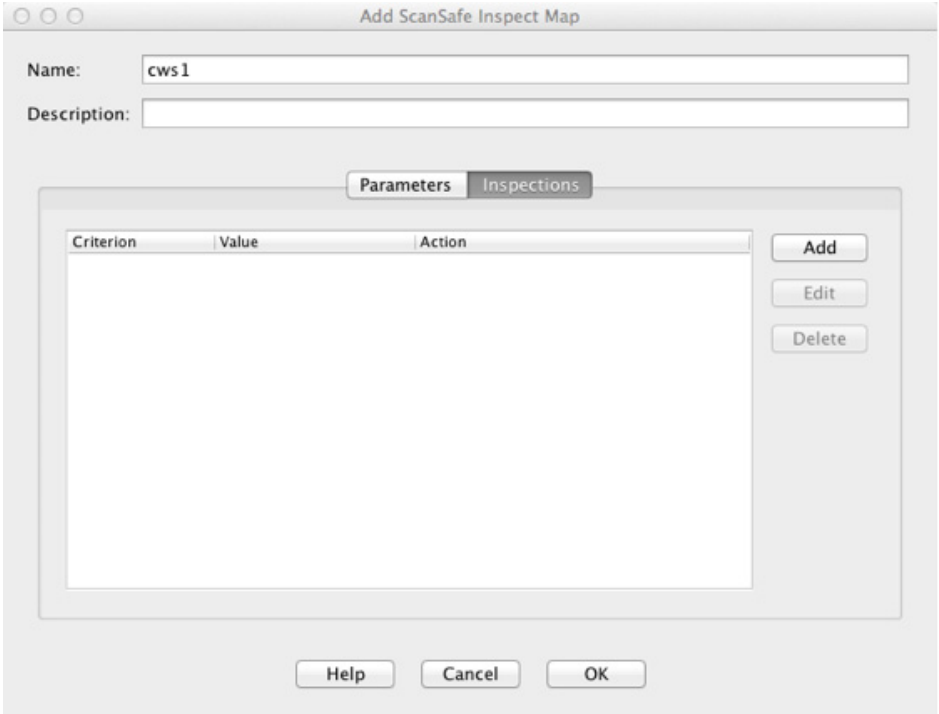
d. [Name] フィールドに、インスペクション ポリシー マップの名前を最大 40 文字までの長さで指定します。

e. （オプション）説明を入力します。

f. （オプション）[Parameters] タブで、[Default User] および [Default Group] を指定します。ASA が ASA に着信するユーザの ID を判定できない場合、デフォルト ユーザおよびグループが適用されます。

g. [Protocol] には、ステップ 3dで設定したサービスに一致する [HTTP] または [HTTPS] をクリックします。クラウド Web セキュリティは、各タイプのトラフィックを別々に処理します。

h. （オプション）ホワイト リストを識別するには、[Inspections] タブをクリックします。



- 「（オプション）ホワイトリストに記載されたトラフィックの設定　」（P.16-24）で作成したインスペクション クラス マップを選択するには、[Add] をクリックします。

  [Add Cloud Web Security Match Criterion] ダイアログボックスが表示されます。
- [Cloud Web Security Traffic Class] ドロップダウン メニューから、インスペクション クラス マップを選択します。

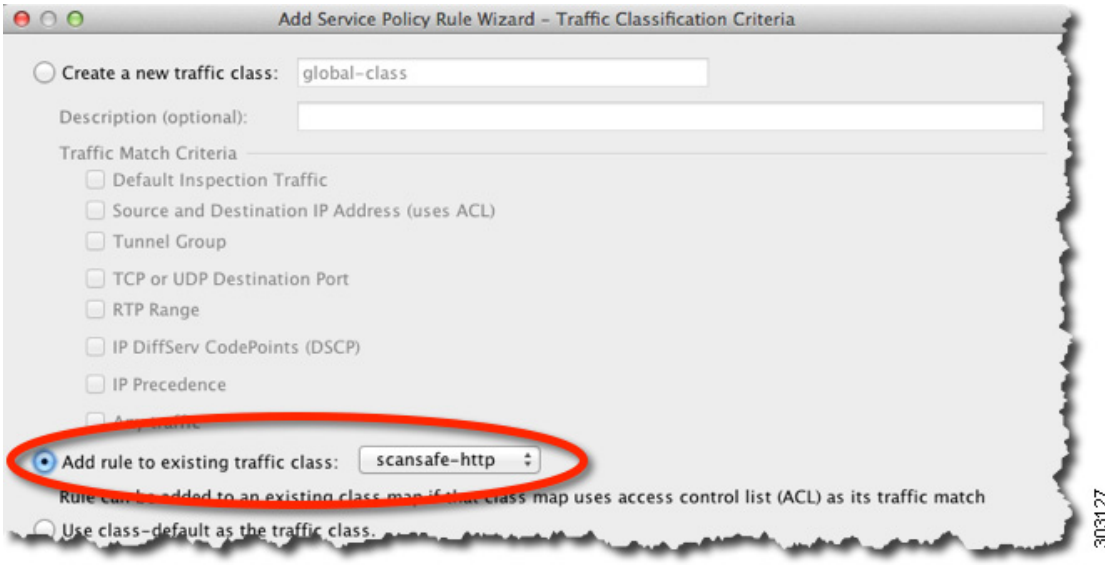
  クラス マップを追加または編集するには、[Manage] をクリックします。
- [Action] では、[Whitelist] をクリックします。
- ポリシー マップにホワイト リストを追加するには、[OK] をクリックします。
- [OK] をクリックします。

ステップ 6　[Finish] をクリックします。ルールは、サービス ポリシー ルール テーブルに追加されます。

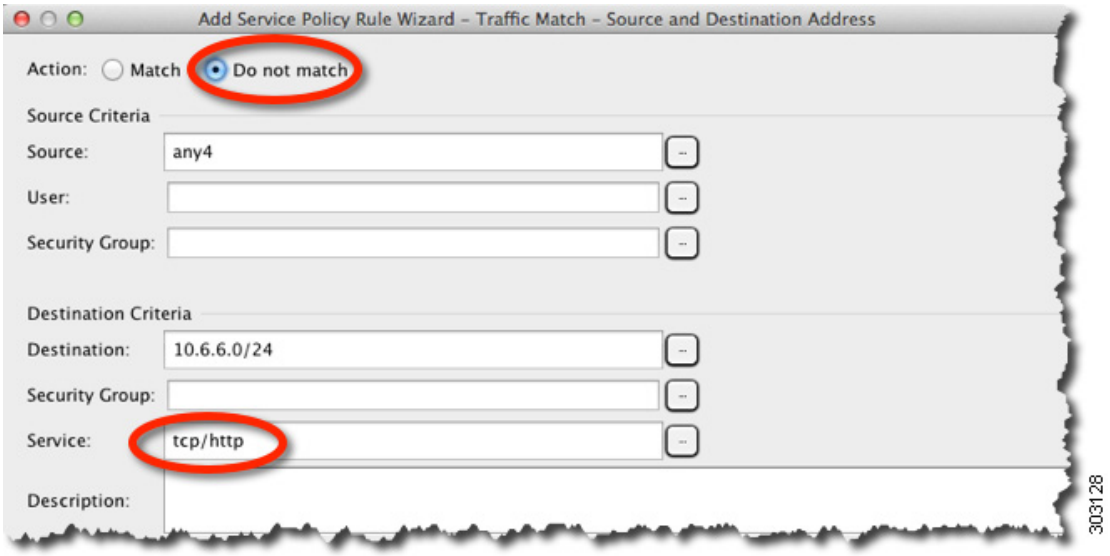
ステップ 7　追加のトラフィックを一致または除外するために、このトラフィック クラスに追加のサブルール（ACE）を追加するには、次の手順を実行します。

a. [Configuration] > [Firewall] > [Service Policy Rules] を選択し、[Add] > [Service Policy Rule] をクリックします。

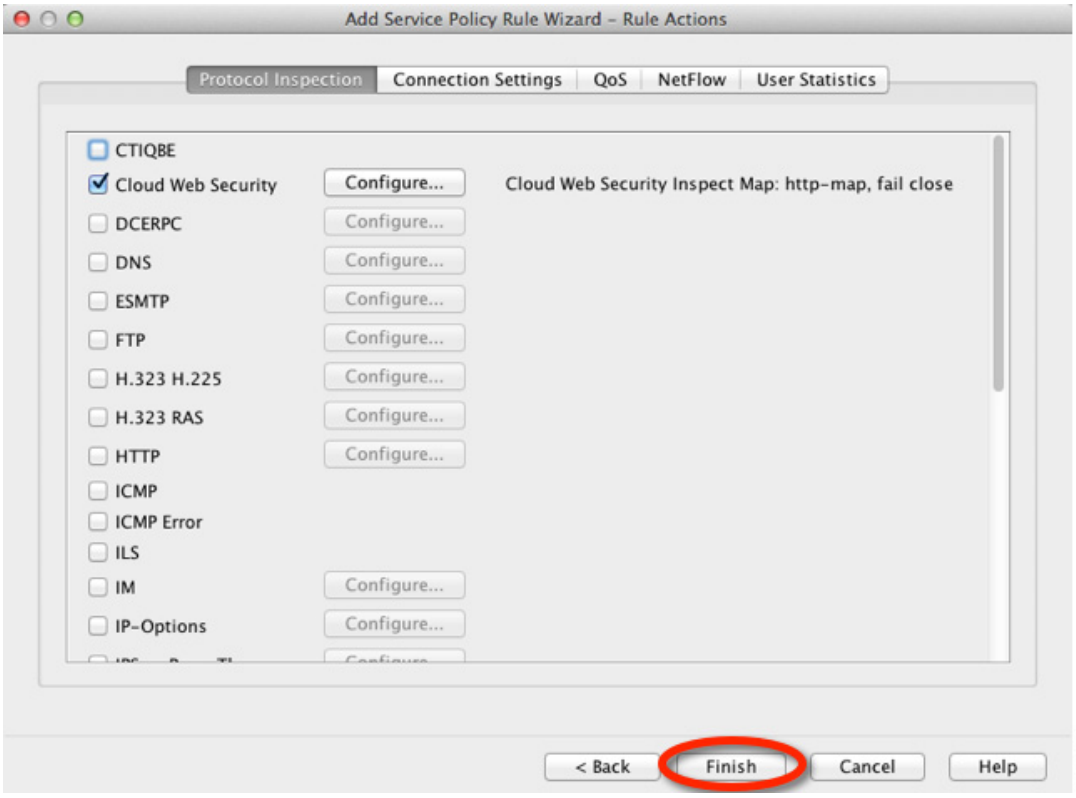
b. ステップ 2 で、同じサービス ポリシーを選択します。[Next] をクリックします。



c. [Traffic Classification Criteria] ダイアログボックスで、[Add Rule to Existing Traffic Class] を選択し、ステップ 3 で作成した名前を選択します。[Next] をクリックします。



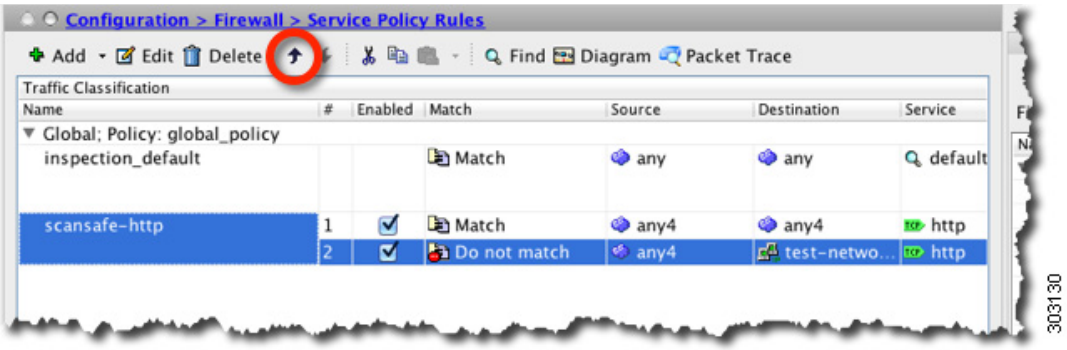
d. [Traffic Match - Source and Destination] ダイアログ ボックスで、[Match] を選択して追加トラフィックのインスペクションを追加するか、[Do Not Match] を選択してクラウド Web セキュリティ インスペクションからトラフィックを除外します。必ずこのクラス（HTTP または HTTPS）の前のルールに一致するようにサービスを設定してください。クラウド Web セキュリティの同じトラフィック クラスに HTTP と HTTPS を混在させることはできません。[Next] をクリックします。

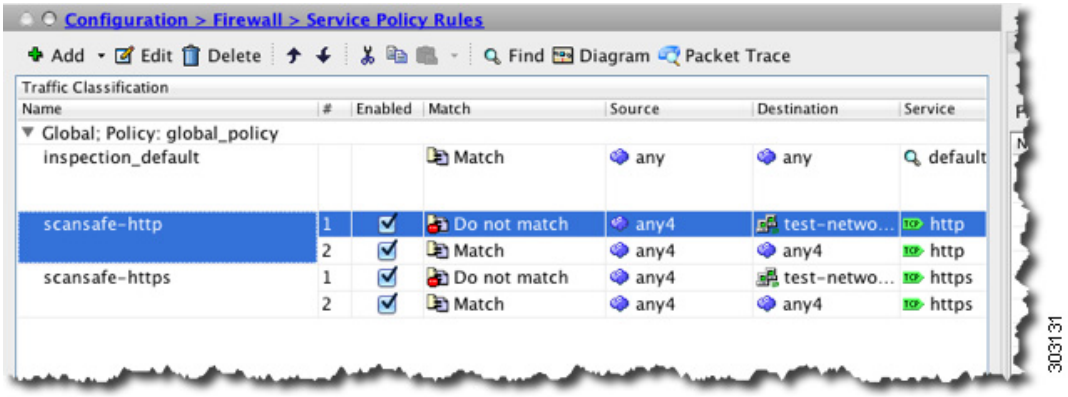


e. [Rule Actions] ダイアログボックスでは、一切変更を加えずに [Finish] をクリックします。このトラフィック クラスでは、複数の ACE を追加した場合でも、1 セットのルールのアクションを使用できるので、すでに指定されているアクションは継承されます。

ステップ 8　HTTPS トラフィックなど、追加のトラフィック クラスを作成するには、この手順全体を繰り返します。ルールおよびサブルールを必要な数だけ作成できます。

ステップ 9　[Service Policy Rules] ペインでクラウド Web セキュリティのルールとサブルールの順序を調整します。ACE の順序の変更方法については、「サービス ポリシー ルールの順序の管理」（P.1-16）を参照してください。



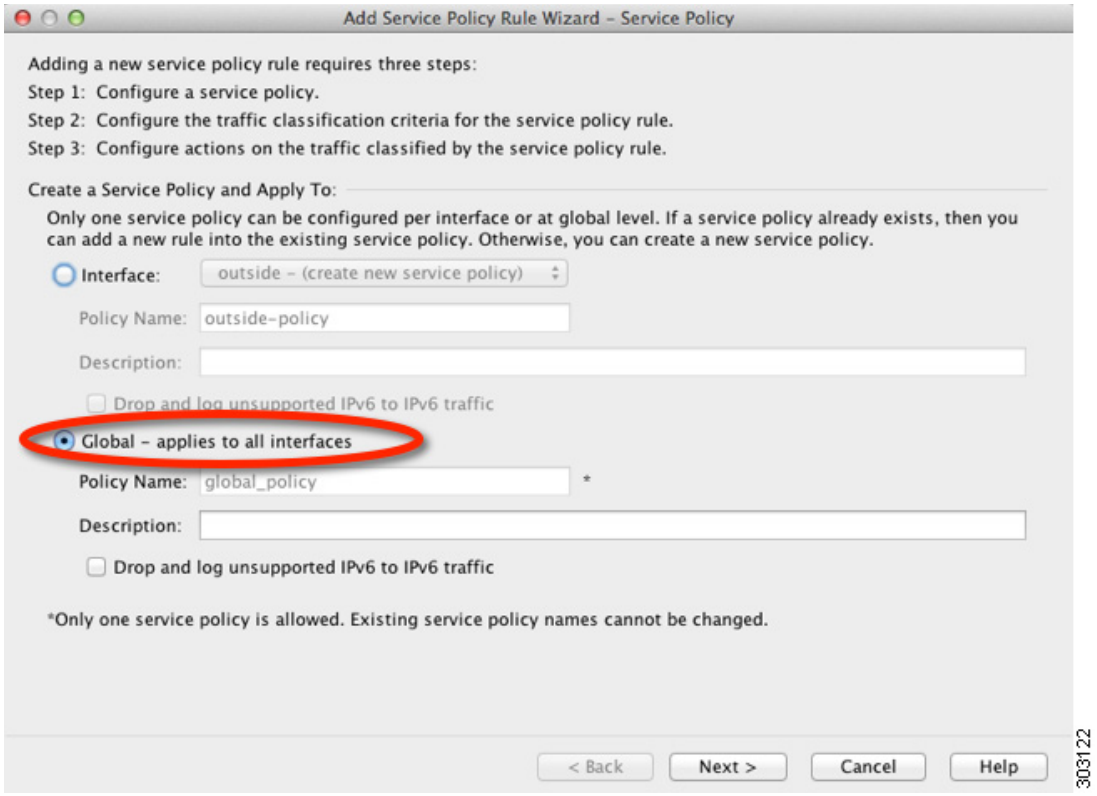


ステップ 10　[Apply] をクリックします。

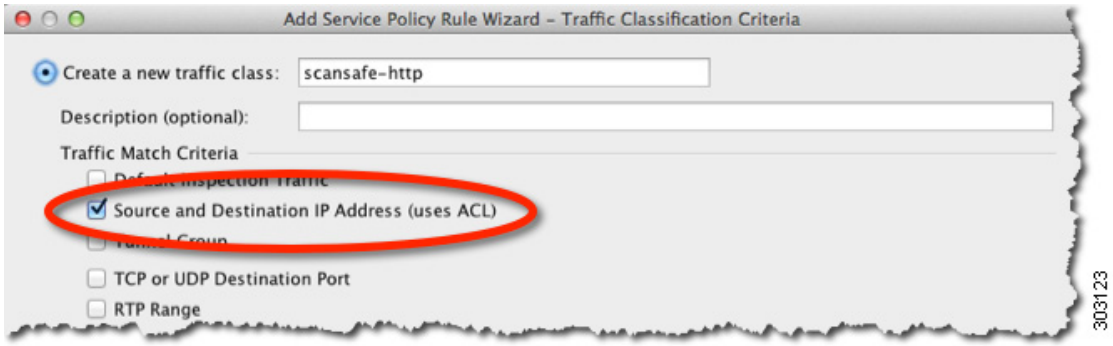
例

次の例は、10.6.6.0/24（test_network）に送信されるすべての IPv4 HTTP および HTTPS トラフィックを除外し、他のすべての HTTP および HTTPS トラフィックをクラウド Web セキュリティに送信し、このサービス ポリシー ルールを、既存のグローバル ポリシーの一部としてすべてのインターフェイスに適用します。クラウド Web セキュリティ サーバが到達不能の場合、ASA は一致するすべてのトラフィックをドロップします（フェール クローズ）。ユーザがユーザ ID 情報を持たない場合、デフォルトのユーザ Boulder とグループ Cisco が使用されます。

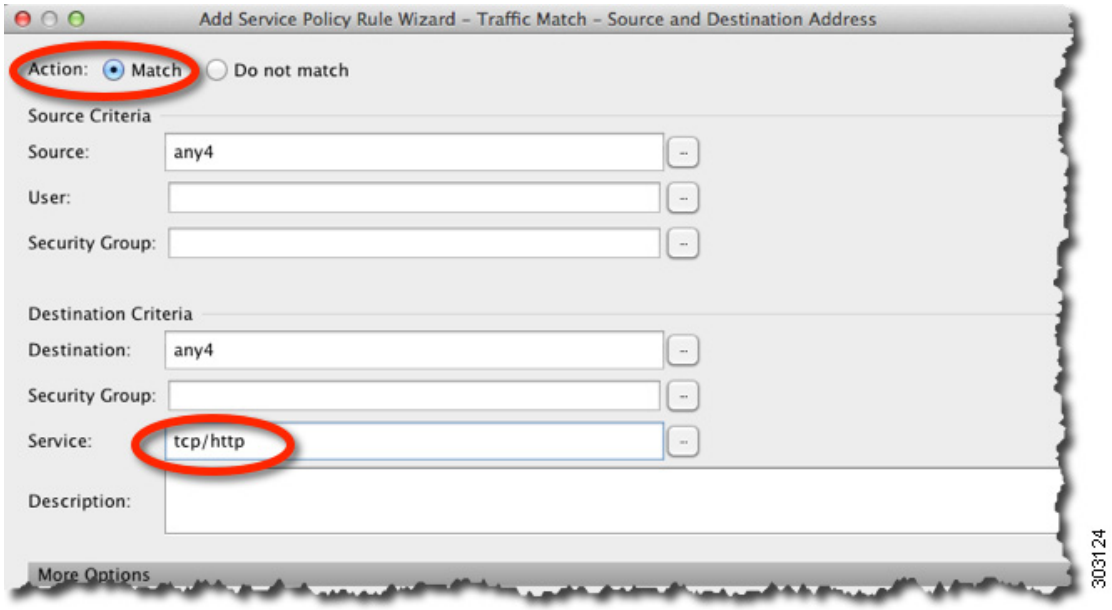
ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] を選択し、[Add] > [Service Policy Rule] をクリックします。デフォルトの global_policy にこのルールを追加します。



ステップ 2　「scansafe-http」と呼ばれる新しいトラフィック クラスを追加し、一致するトラフィックに ACL を指定します。

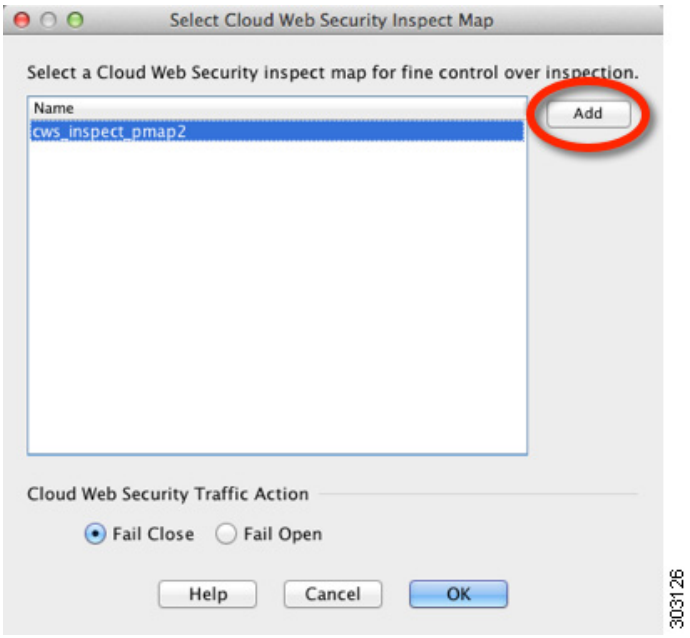


ステップ 3　[Match] を選択し、送信元と宛先に **any4** を指定します。サービスに **tcp/http** を指定します。

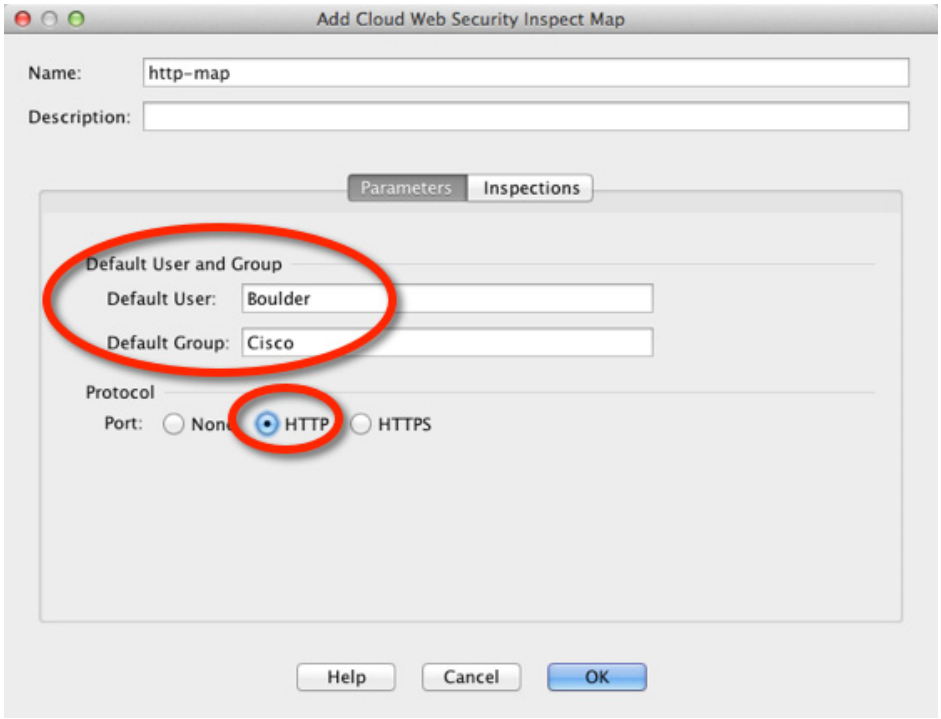


ステップ 4　[Cloud Web Security] をオンにして、[Configure] をクリックします。

ステップ 5　デフォルトの [Fail Close] アクションを受け入れ、[Add] をクリックします。

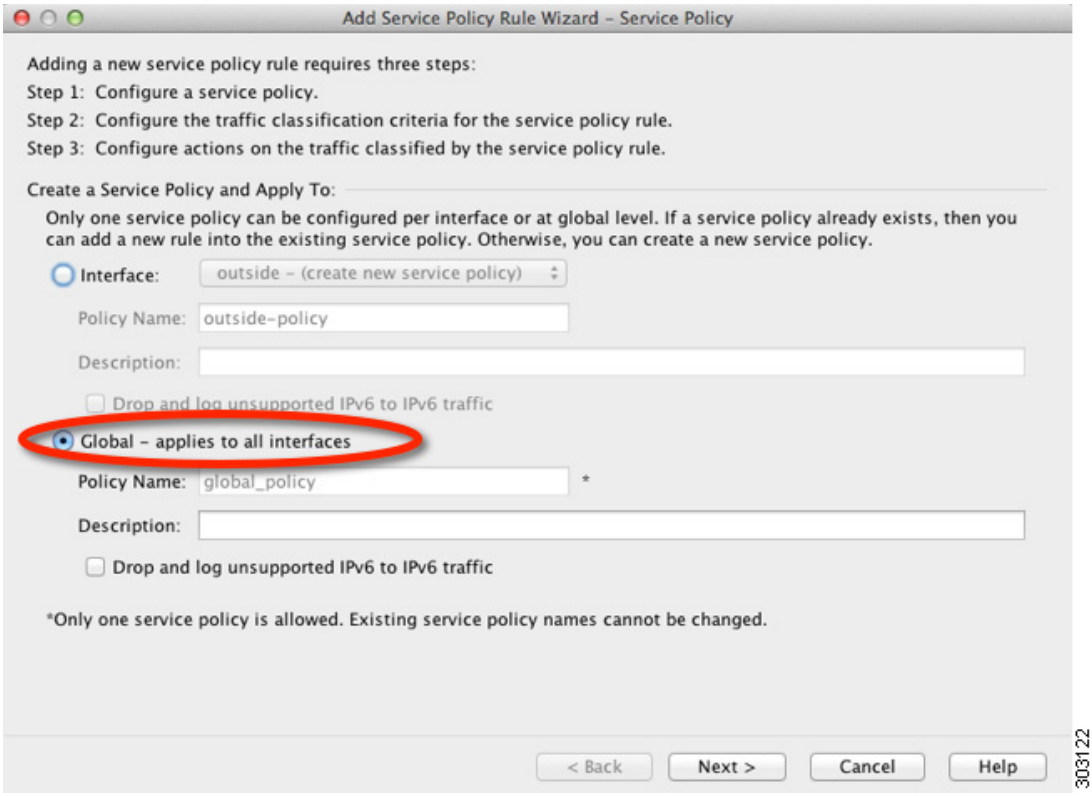


ステップ 6　インスペクション ポリシー マップに「http-map」という名前を付け、[Default User] に [Boulder]、[Default Group] に [Cisco] を設定します。[HTTP] を選択します。

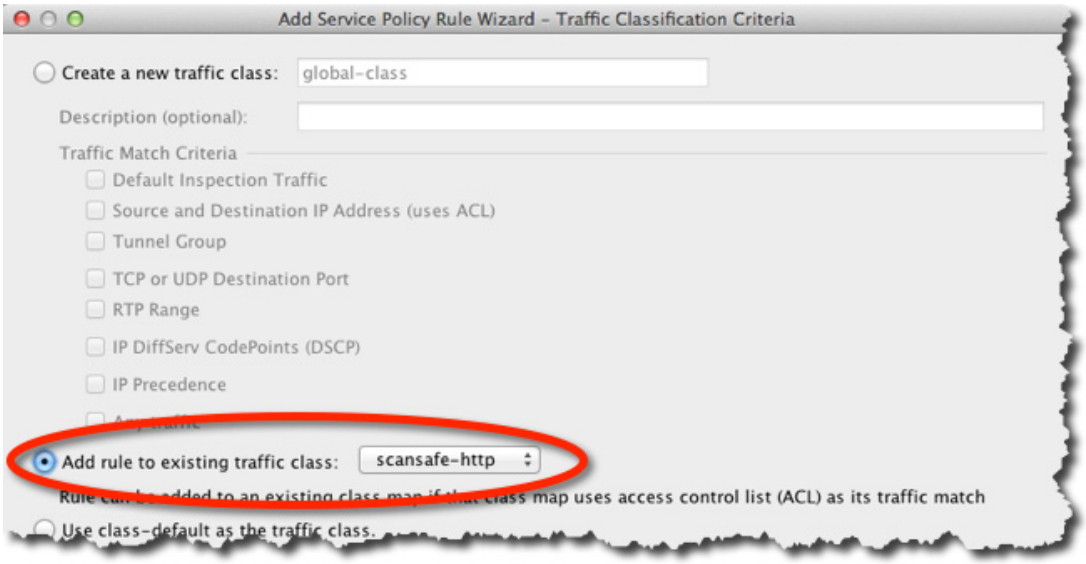


ステップ 7　[OK]、[OK] とクリックし、[Finish] をクリックします。ルールは、サービス ポリシー ルール テーブルに追加されます。

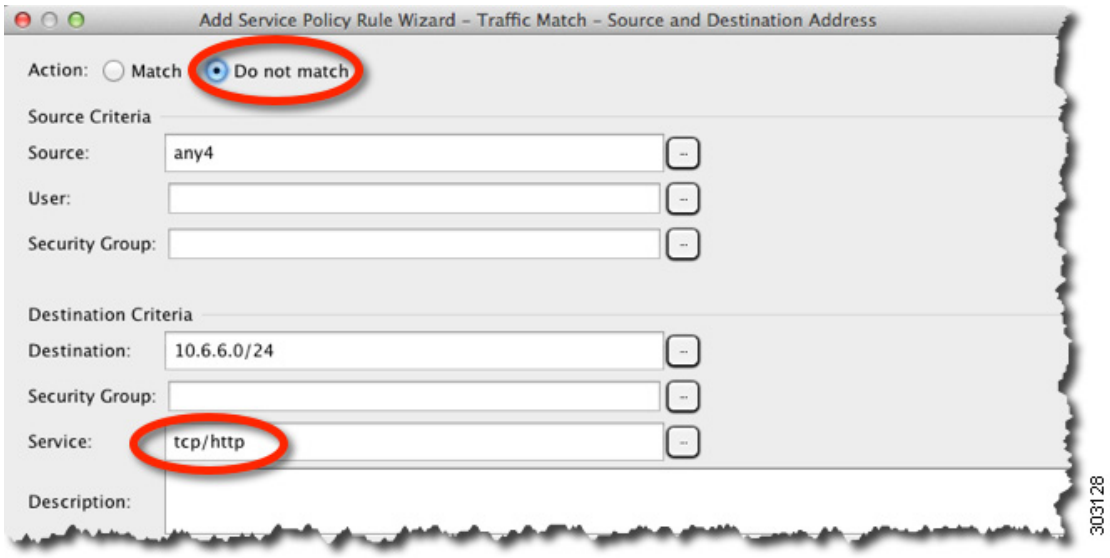
ステップ 8　[Configuration] > [Firewall] > [Service Policy Rules] を選択し、[Add] > [Service Policy Rule] をクリックします。デフォルトの global_policy に新しいルールを追加します。



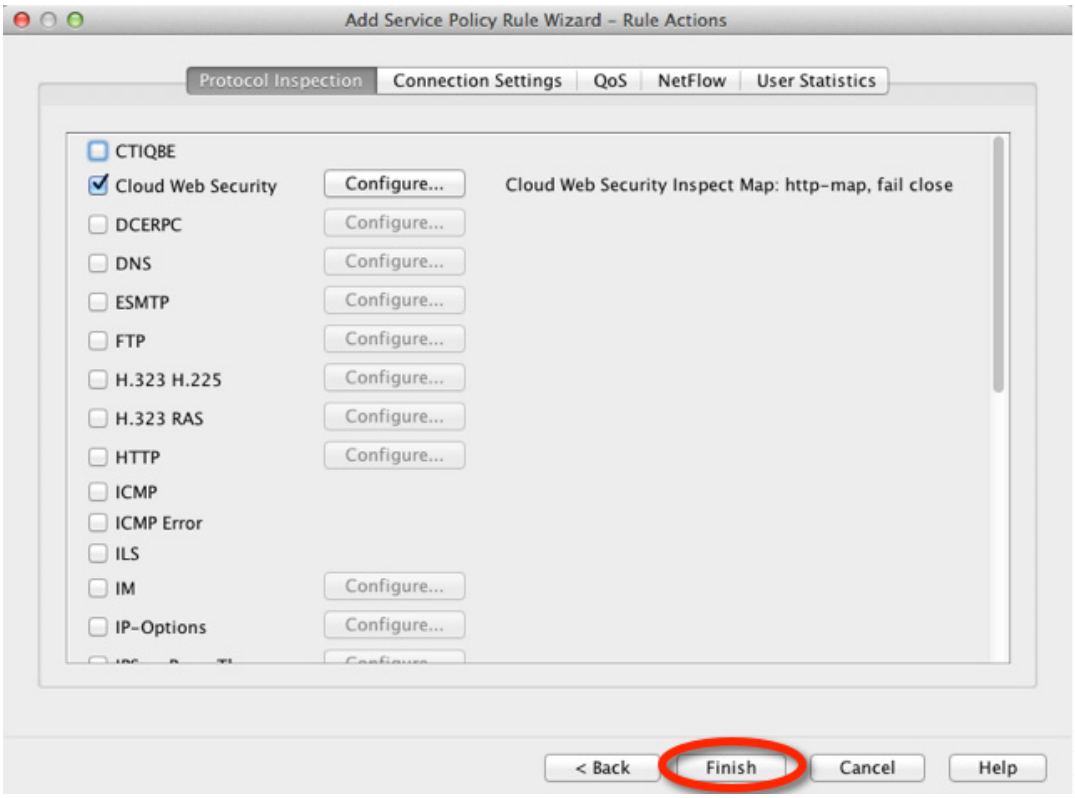
ステップ 9　[Add rule to existing traffic class] をクリックし、[scansafe-http] を選択します。



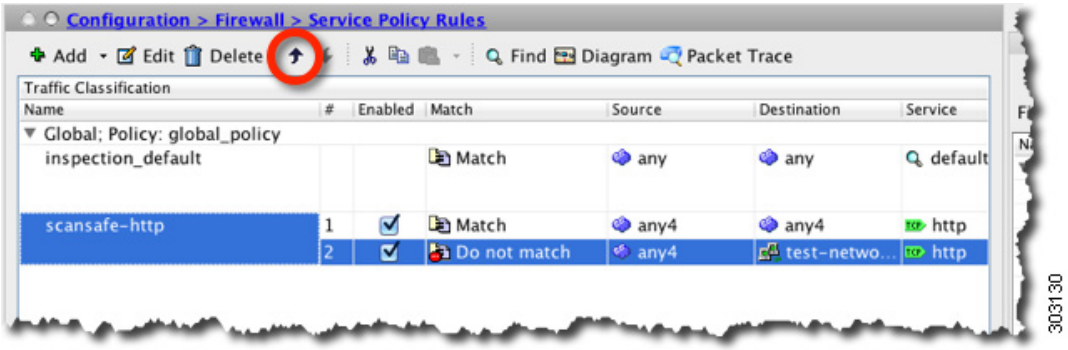
ステップ 10　[Do not match] を選択し、送信元として [any4]、宛先として [10.6.6.0/24] を設定します。[Service] を [tcp/http] に設定します。



ステップ 11　[Finish] をクリックします。

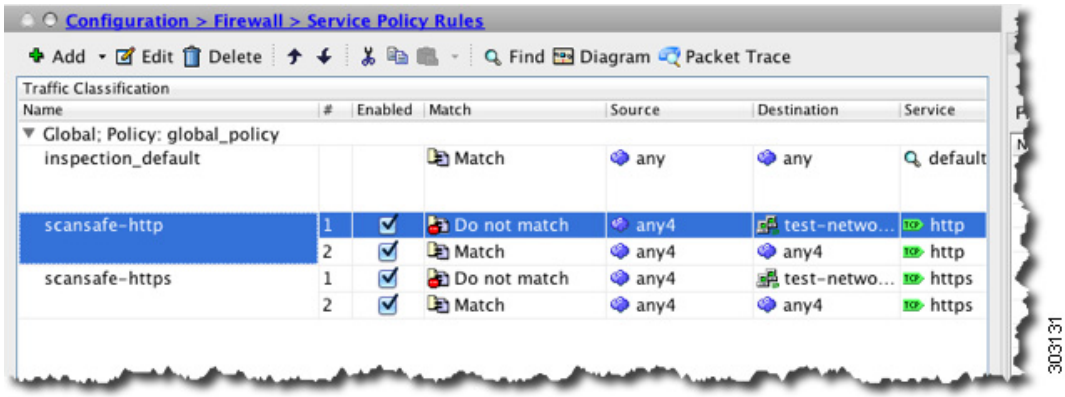


ステップ 12　[Do not match] ルールが [Match] ルールの上に来るようにルールの順序を変更します。



ユーザ トラフィックは、これらのルールと順番に比較されます。この [Match] ルールはリストの最初にあるので、test_network へのトラフィックを含むすべてトラフィックがそのルールにのみ一致し、[Do not match] ルールがヒットすることはありません。[Do not match] ルールを [Match] ルールの上に移動すると、test_network へのトラフィックは [Do not match] に一致し、他のすべてのトラフィックは [Match] ルールに一致します。

ステップ 13　次のように変更して上記の手順を繰り返します。「scansafe-https」と呼ばれる新しいトラフィック クラスを追加し、インスペクション ポリシー マップに [HTTPS] を選択します。



ステップ 14　[Apply] をクリックします。

（オプション）ホワイトリストに記載されたトラフィックの設定

ユーザ認証を使用する場合は、ユーザ名やグループ名に基づいて一部のトラフィックをクラウド Web セキュリティによるフィルタリングから免除できます。クラウド Web セキュリティ サービス ポリシー ルールを設定する場合は、ホワイトリスト インスペクション クラス マップを参照できます。IDFW および AAA のユーザ クレデンシャルをこの機能とともに使用できます。

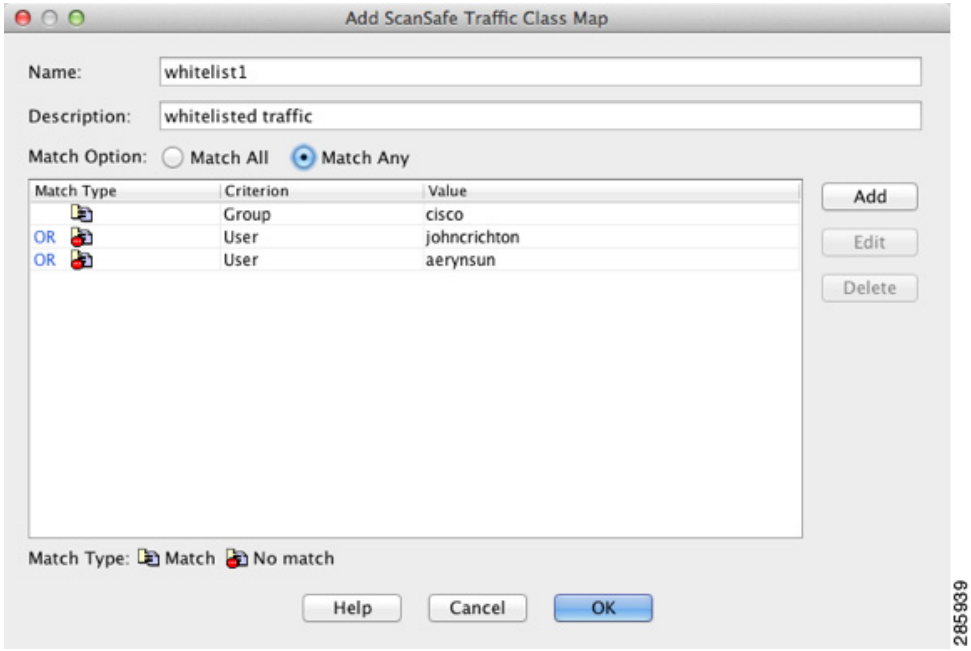
サービス ポリシー ルールを設定すると、ユーザまたはグループに基づいてトラフィックを免除する同じ結果を得ることができますが、ホワイトリストを使用した方がより簡単です。ホワイトリスト機能は、ユーザおよびグループだけに基づき、IP アドレスには基づかないことに注意してください。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Class Maps] > [Cloud Web Security] を選択します。

ステップ 2　[Add] をクリックして、新しいクラス マップを作成します。

[Add Cloud Web Security Traffic Class Map] 画面が表示されます。



ステップ 3　[Name] フィールドに、新しいクラス マップの名前を入力します（40 文字以下）。

ステップ 4　[Description] フィールドに、クラス マップの説明を入力します（200 文字以下）。

ステップ 5　[Match Option] には、[Add] をクリックして定義した基準を選択します。

- [Match All]：トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。
- [Match Any]：トラフィックが少なくとも基準の 1 つに一致したらクラス マップと一致することを指定します。

ステップ 6　[Add] をクリックします。

[Add Cloud Web Security Match Criterion] ウィンドウが表示されます。

ステップ 7　[Match Type] を選択します。

- [Match]：ホワイト リストに任意のユーザ/グループを指定します。
- [No Match]：ホワイト リストに必要と*しない*ユーザ/グループを指定します。たとえば、ホワイト リストにグループ「cisco」を指定しているが、ユーザ「johncrichton」および「aerynsun」からのトラフィックはスキャンしたい場合、これらのユーザに [No Match] を指定することができます。

ステップ 8　[Match Criterion] を選択します。

- [User]：ユーザを指定します。
- [Group]：グループを指定します。
- [User and Group]：ユーザおよびグループを指定します。

ステップ 9　[OK] をクリックします。

ステップ 10　必要に応じてさらに一致基準を追加します。

ステップ 11　クラス マップを追加するには、[OK] をクリックします。

ステップ 12　[Apply] をクリックします。

ステップ 13　「クラウド Web セキュリティにトラフィックを送信するサービス ポリシーの方法」（P.16-10）に従って、クラウド Web セキュリティ ポリシーにホワイト リストを使用します。

（オプション）ユーザ アイデンティティ モニタを設定します

IDFW を使用する場合、ASA は、アクティブな ACL に含まれるユーザおよびグループの AD サーバからのユーザ アイデンティティ情報のみをダウンロードします。ACL は、アクセス ルール、AAA ルール、サービス ポリシー ルール、またはアクティブと見なされるその他の機能で使用する必要があります。クラウド Web セキュリティでは、そのポリシーがユーザ アイデンティティに基づくことができるため、すべてのユーザに対する完全な IDFW カバレッジを取得するには、アクティブな ACL の一部ではないグループをダウンロードする必要があります。たとえば、ユーザおよびグループとともに ACL を使用するクラウド Web セキュリティ サービス ポリシー ルールを設定して、関連グループをアクティブ化できますが、これは必須ではありません。IP アドレスのみに基づく ACL を使用できます。ユーザ アイデンティティ モニタ機能を使用すると、AD エージェントからグループ情報を直接ダウンロードできます。

制限事項

ASA は、ユーザ アイデンティティ モニタ用に設定されたグループ、アクティブな ACL によってモニタされているグループも含めて 512 以下のグループモニタできます。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Identity Options] を選択し、[Cloud Web Security Configuration] セクションにスクロールします。

ステップ 2　[Add] をクリックします。

[Add Monitor User] ダイアログボックスが表示されます。

ステップ 3　ドメインを追加するには、[Manage] をクリックして、[Add] をクリックします。ASA であらかじめ定義したドメインのグループのみモニタできます。

[Configure Identity Domains] ダイアログボックスが表示されます。ドメインを追加する方法の詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

ステップ 4　ドメインの追加が終了したら、[OK] をクリックします。

ステップ 5　グループ名を入力するか、またはドメインごとに AD エージェントのグループを検索できます。

- グループ名を直接入力するには、一番下のフィールドに次の形式で名前を入力し、[OK] をクリックします。

  *domain-name**group*

- AD エージェントのグループを検索するには、次の手順を実行します。

a.　[Domain] ドロップダウン リストからドメインを選択します。

b. [Find] フィールドで、グループ名に対応するテキスト文字列を入力し、[Find] をクリックします。

ASA は、指定したドメインの AD エージェントから名前をダウンロードします。

c. モニタする名前をダブルクリックすると、一番下のフィールドに追加されます。

d. [OK] をクリックします。

追加グループに対して手順を繰り返します。

ステップ 6　モニタするグループを追加したら、[Apply] をクリックします。

クラウド Web セキュリティ ポリシーの設定

ASA サービス ポリシー ルールを設定した後は、ScanCenter ポータルを起動して、Web コンテンツ スキャン、フィルタリング、マルウェア保護サービスおよびレポートを設定します。

手順の詳細

https://scancenter.scansafe.com/portal/admin/login.jsp に移動します。

詳細については、『Cisco ScanSafe Cloud Web Security Configuration Guides』を参照してください。

http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html

クラウド Web セキュリティのモニタ

コマンド	目的
[Monitoring] > [Properties] > [Cloud Web Security]	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。 合計と現在の HTTP 接続を表示します。マルチ コンテキスト モードでは、統計情報はコンテキスト内にのみ表示されます。
次の URL を参照してください。 http://Whoami.scansafe.net	トラフィックがクラウド Web セキュリティ サーバに移動するかどうかを確認するには、クライアントからこの Web サイトにアクセスします。

関連資料

関連資料	URL
『Cisco ScanSafe Cloud Web Security Configuration Guides』	http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html

Cisco クラウド Web セキュリティの機能の履歴

表 16-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 16-1　クラウド Web セキュリティ の機能の履歴

機能名	プラットフォーム リリース	機能情報
クラウド Web セキュリティ	9.0(1)	この機能が導入されました。 Cisco クラウド Web セキュリティ は、Web トラフィックに対するコンテンツ スキャンおよびその他のマルウェア保護サービスを提供します。また、ユーザ アイデンティティに基づいて Web トラフィックのリダイレクトと報告を行うこともできます。 次の画面が導入または変更されました。 [Configuration] > [Device Management] > [Cloud Web Security] [Configuration] > [Firewall] > [Objects] > [Class Maps] > [Cloud Web Security] [Configuration] > [Firewall] > [Objects] > [Class Maps] > [Cloud Web Security] > [Add/Edit] [Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [Cloud Web Security] [Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [Cloud Web Security] > [Add/Edit] [Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [Cloud Web Security] > [Add/Edit] > [Manage Cloud Web Security Class Maps] [Configuration] > [Firewall] > [Identity Options] [Configuration] > [Firewall] > [Service Policy Rules] [Monitoring] > [Properties] > [Cloud Web Security]

脅威検出

この章では、脅威検出の統計情報およびスキャン脅威検出を設定する方法について説明します。

- 「脅威の検出」（P.17-1）
- 「脅威検出のガイドライン」（P.17-3）
- 「脅威検出のデフォルト」（P.17-4）
- 「脅威検出の設定」（P.17-4）
- 「脅威検出のモニタリング」（P.17-7）
- 「脅威検出の履歴」（P.17-8）

脅威の検出

ASA の脅威検出は、攻撃に対して最前線で防御する機能です。脅威検出は、パケット ドロップの統計を分析し、トラフィック パターンに基づいた「トップ」レポートを蓄積することで、デバイスのレイヤ 3 と 4 にトラフィックのベースラインを作成します。一方、IPS または次世代 IPS サービスを提供するモジュールは、ASA が許可したトラフィックの攻撃ベクトルをレイヤ 7 まで識別して軽減させますが、すでに ASA がドロップしたトラフィックは認識できません。そのため、脅威検出と IPS を一緒に使用することで、より総合的な脅威に対する防御を可能にします。

脅威検出は次の要素から構成されています。

- さまざまな脅威を収集する複数レベルの統計情報

  脅威検出統計情報は、ASA に対する脅威の管理に役立ちます。たとえば、スキャン脅威検出をイネーブルにすると、統計情報を見ることで脅威を分析できます。次の 2 種類の脅威検出統計情報を設定できます。

  - 基本脅威検出統計情報：システムに対する攻撃アクティビティについての全体的な情報を含みます。基本脅威検出統計情報はデフォルトでイネーブルになっており、パフォーマンスに対する影響はありません。
  - 拡張脅威検出統計情報：オブジェクト レベルでアクティビティを追跡するので、ASA は個別のホスト、ポート、プロトコル、または ACL についてのアクティビティを報告できます。拡張脅威検出統計情報は、収集される統計情報によってはパフォーマンスに大きく影響するので、デフォルトでは ACL の統計情報だけがイネーブルになっています。

- ホストがスキャンを実行する時期を決定するスキャン脅威検出機能 オプションとして、スキャン脅威であることが特定されたホストを排除できます。

基本脅威検出統計情報

ASA は、基本脅威検出統計情報を使用して、次の理由でドロップしたパケットおよびセキュリティ イベントの割合をモニタします。

- ACL による拒否。
- 不正なパケット形式（invalid-ip-header や invalid-tcp-hdr-length など）。
- 接続制限の超過（システム全体のリソース制限とコンフィギュレーションで設定されている制限の両方）。
- DoS 攻撃の検出（無効な SPI、ステートフル ファイアウォール検査の不合格など）。
- 基本ファイアウォール検査に不合格。このオプションは、このリストのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません。
- 疑わしい ICMP パケットの検出。
- アプリケーション インスペクションに不合格のパケット。
- インターフェイスの過負荷。
- スキャン攻撃の検出。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニタします。フル スキャン脅威検出では、このスキャン攻撃レート情報を収集し、ホストを攻撃者として分類して自動的に排除することによって対処します。
- 不完全セッションの検出（TCP SYN 攻撃の検出やデータなし UDP セッション攻撃の検出など）。

ASA は、脅威を検出するとただちにシステム ログ メッセージ（733100）を送信します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト レート間隔は、平均レート間隔の 1/30 または 10 秒のうち、どちらか大きいほうです。ASA は、受信するイベントごとに平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、ASA は、バースト期間におけるレート タイプごとに最大 1 つのメッセージの割合で 2 つの別々のシステム メッセージを送信します。

基本脅威検出は、ドロップや潜在的な脅威があった場合に限りパフォーマンスに影響を与えます。この状況でも、パフォーマンスへの影響は大きくありません。

拡張脅威検出統計情報

拡張脅威検出統計情報は、ホスト、ポート、プロトコル、ACL などの個別のオブジェクトについて、許可されたトラフィック レートとドロップされたトラフィック レートの両方を表示します。

注意　拡張統計情報をイネーブルにすると、イネーブルにする統計情報のタイプに応じて、ASA のパフォーマンスが影響を受けます。ホスト統計情報をイネーブルにすることは、パフォーマンスに大幅に影響を与えます。トラフィックの負荷が高い場合、このタイプの統計情報は一時的にイネーブルにすることを検討できます。一方、ポート統計情報は大きな影響を与えません。

スキャン脅威検出

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、ASA の脅威検出スキャンでは、広範なデータベースが保持され、これに含まれるホスト統計情報をスキャン アクティビティに関する分析に使用できます。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

スキャン脅威レートを超過すると、ASA は syslog メッセージ（733101）を送信し、必要に応じて攻撃者を排除します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト イベント レートは、平均レート間隔の 1/30 または 10 秒のうち、どちらか大きいほうです。スキャン攻撃の一部と見なされるイベントが検出されるたびに、ASA は平均レート制限とバースト レート制限をチェックします。ホストから送信されるトラフィックがどちらかのレートを超えると、そのホストは攻撃者と見なされます。ホストが受信したトラフィックがどちらかのレートを超えると、そのホストはターゲットと見なされます。

次の表に、スキャン脅威検出のデフォルトのレート制限を示します。

表 17-1　スキャン脅威検出のデフォルトのレート制限

平均レート	バースト レート
直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
直前の 3600 秒間で 5 ドロップ/秒。	直近の 120 秒間で 10 ドロップ/秒。

注意　スキャン脅威検出機能は、ホストおよびサブネットベースのデータ構造を作成し情報を収集する間、ASA のパフォーマンスとメモリに大きく影響することがあります。

脅威検出のガイドライン

セキュリティ コンテキストのガイドライン

拡張脅威統計情報を除き、脅威検出はシングル モードのみでサポートされます。マルチ モードでは、TCP 代行受信の統計情報が唯一サポートされている統計情報です。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

モニタ対象トラフィックのタイプ

- through-the-box トラフィックだけがモニタされます。to-the-box トラフィックは、脅威検出に含まれません。
- ACL によって拒否されたトラフィックは、スキャン脅威検出をトリガーしません。ASA から許可され、フローを作成したトラフィックだけがスキャン脅威検出の影響を受けます。

脅威検出のデフォルト

基本脅威検出統計情報は、デフォルトでイネーブルになっています。

次の表に、デフォルト設定を示します。これらのデフォルト設定すべてを表示するには、**show running-config all threat-detection** コマンドを [Tools] > [Command Line Interface] で使用します。

拡張統計情報では、ACL の統計情報はデフォルトでイネーブルになっています。

表 17-2　基本脅威検出のデフォルト設定

	トリガー設定	
パケット ドロップの理由	**平均レート**	**バースト レート**
• DoS 攻撃の検出 • 不正なパケット形式 • 接続制限の超過 • 疑わしい ICMP パケットの検出	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 400 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 120 秒間で 320 ドロップ/秒。
スキャン攻撃の検出	直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
	直前の 3600 秒間で 4 ドロップ/秒。	直近の 120 秒間で 8 ドロップ/秒。
不完全セッションの検出（TCP SYN 攻撃の検出やデータなし UDP セッション攻撃の検出など）（複合）	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 200 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 120 秒間で 160 ドロップ/秒。
ACL による拒否	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 800 ドロップ/秒。
	直前の 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 640 ドロップ/秒。
• 基本ファイアウォール検査に不合格 • アプリケーション インスペクションに不合格のパケット	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 1600 ドロップ/秒。
	直前の 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 1280 ドロップ/秒。
インターフェイスの過負荷	直前の 600 秒間で 2000 ドロップ/秒。	直近の 20 秒間で 8000 ドロップ/秒。
	直前の 3600 秒間で 1600 ドロップ/秒。	直近の 120 秒間で 6400 ドロップ/秒。

脅威検出の設定

基本脅威検出統計情報はデフォルトでイネーブルになっており、ユーザが必要とする唯一の脅威検出サービスである場合があります。さらに脅威検出サービスを実装する場合は、次の手順を使用します。

手順

ステップ 1　「基本脅威検出統計情報の設定」（P.17-5）

基本脅威検出統計情報には、DoS 攻撃（サービス拒絶攻撃）などの攻撃に関連している可能性があるアクティビティが含まれます。

ステップ 2　「拡張脅威検出統計情報の設定」（P.17-5）

ステップ 3　「スキャン脅威検出の設定」（P.17-6）

基本脅威検出統計情報の設定

基本脅威検出統計情報は、デフォルトでイネーブルになっています。ディセーブルにすることも、一度ディセーブルにした後で再度イネーブルにすることもできます。

手順

ステップ 1　[Configuration] > [Firewall] > [Threat Detection] ペインを選択します。

ステップ 2　必要に応じて、[Enable Basic Threat Detection] を選択または選択解除します。

ステップ 3　[Apply] をクリックします。

拡張脅威検出統計情報の設定

広範な統計情報を収集するように ASA を設定することができます。デフォルトでは、ACL の統計情報はイネーブルになっています。他の統計情報をイネーブルにするには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Firewall] > [Threat Detection] を選択します。

ステップ 2　[Scanning Threat Statistics] 領域で、次のオプションのいずれかを選択します。

- [Enable All Statistics]
- [Disable All Statistics]
- [Enable Only Following Statistics]

ステップ 3　[Enable Only Following Statistics] を選択した場合は、次のオプションから 1 つ以上を選択します。

- [Hosts]：ホスト統計情報をイネーブルにします。ホストがアクティブで、スキャン脅威ホスト データベース内に存在する限り、ホスト統計情報は累積されます。ホストは、非アクティブになってから 10 分後にデータベースから削除されます（統計情報もクリアされます）。
- [Access Rules]（デフォルトでイネーブル）：アクセス ルールの統計情報をイネーブルにします。
- [Port]：TCP/UDP ポートの統計情報をイネーブルにします。
- [Protocol]：TCP/UDP 以外の IP プロトコルの統計情報をイネーブルにします。

- [TCP-Intercept]：TCP 代行受信によって代行受信された攻撃の統計情報をイネーブルにします（TCP 代行受信をイネーブルにする方法については「接続の設定」（P.13-8）を参照してください）。

ステップ 4　ホスト、ポート、およびプロトコルの統計情報については、収集するレート間隔の数を変更できます。[Rate Intervals] 領域で、統計タイプのそれぞれに対して [1 hour]、[1 and 8 hours]、または [1, 8 and 24 hours] を選択します。デフォルトの間隔は [1 hour] で、メモリ使用量が低く抑えられます。

ステップ 5　TCP 代行受信の統計情報については、次のオプションを [TCP Intercept Threat Detection] 領域で設定できます。

- [Monitoring Window Size]：履歴モニタリングの時間枠のサイズを 1 ～ 1440 分の範囲内で設定します。デフォルトは 30 分です。ASA はレート間隔の間に攻撃の数を 30 回サンプリングするので、デフォルトの 30 分間隔では、60 秒ごとに統計情報が収集されます。
- [Burst Threshold Rate]：syslog メッセージ生成のしきい値を 25 ～ 2147483647 の範囲内で設定します。デフォルトは 1 秒間に 400 です。バースト レートがこれを超えると、syslog メッセージ 733104 が生成されます。
- [Average Threshold Rate]：syslog メッセージ生成の平均レートのしきい値を 25 ～ 2147483647 の範囲内で設定します。デフォルトは 1 秒間に 200 回です。平均レートがこれを超えると、syslog メッセージ 733105 が生成されます。

デフォルト値を復元するには、[Set Default] ボタンをクリックします。

ステップ 6　[Apply] をクリックします。

スキャン脅威検出の設定

攻撃者を識別し、必要に応じて排除するように、スキャン脅威検出を設定できます。

手順

ステップ 1　[Configuration] > [Firewall] > [Threat Detection] を選択します。

ステップ 2　[Enable Scanning Threat Detection] を選択します。

ステップ 3　（オプション）ASA がホストを攻撃者と識別した場合に自動的にホスト接続を終了させるには、[Shun Hosts detected by scanning threat] を選択し、必要に応じて次のオプションを入力します。

- ホスト IP アドレスを排除対象から除外するには、[Networks excluded from shun] フィールドにアドレスまたはネットワーク オブジェクト名を入力します。複数のアドレスまたはサブネットは、カンマで区切って入力できます。IP アドレス オブジェクトのリストからネットワークを選択するには、[...] ボタンをクリックします。
- （オプション）攻撃ホストの排除期間を設定するには、[Set Shun Duration] を選択し、10 ～ 2592000 秒の間の値を入力します。デフォルトの期間は 3600 秒（1 時間）です。デフォルト値を復元するには、[Set Default] をクリックします。

ステップ 4　[Apply] をクリックします。

脅威検出のモニタリング

次のトピックでは、脅威検出のモニタ方法とトラフィック統計情報の表示方法を説明します。

- 「基本脅威検出統計情報のモニタリング」（P.17-7）
- 「拡張脅威検出統計情報のモニタリング」（P.17-7）

基本脅威検出統計情報のモニタリング

基本脅威検出統計情報を表示するには、[Home] > [Firewall Dashboard] > [Traffic Overview] を選択します。

拡張脅威検出統計情報のモニタリング

次のダッシュボードを使用して拡張脅威統計情報をモニタできます。

- [Home] > [Firewall Dashboard] > [Top 10 Access Rules] : ほとんどのヒットのアクセス ルールを表示します。許可および拒否はこのグラフでは区別されません。拒否されたトラフィックは、[Traffic Overview] > [Dropped Packets Rate] グラフで追跡できます。
- [Home] > [Firewall Dashboard] > [Top Usage Statistics] : [Top 10 Sources] および [Top 10 Destinations] タブに、ホストの統計情報が表示されます。脅威検出アルゴリズムに起因して、フェールオーバー リンクとステート リンクの組み合わせとして使用されるインターフェイスは上位 10 個のホストに表示されることがあります。これは予期された動作であり、表示される IP アドレスは無視できます。

  [Top 10 Services] タブには、ポートとプロトコルの両方の統計情報が表示され（表示するには、両方がイネーブルに設定されている必要があります）、TCP/UDP ポートと IP プロトコル タイプを組み合わせた統計情報が表示されます。TCP（プロトコル 6）と UDP（プロトコル 17）は、IP プロトコルの表示には含まれていませんが、TCP ポートと UDP ポートはポートの表示に含まれています。これらのタイプ（ポートまたはプロトコル）の 1 つの統計情報だけをイネーブルにすると、イネーブルにされた統計情報だけが表示されます。
- [Home] > [Firewall Dashboard] > [Top Ten Protected Servers under SYN Attack] : TCP 代行受信の統計情報を表示します。履歴サンプリング データを表示するには、[Detail] ボタンをクリックします。ASA はレート間隔の間に攻撃の数を 30 回サンプリングするので、デフォルトの 30 分間隔では、60 秒ごとに統計情報が収集されます。

脅威検出の履歴

機能名	プラットフォーム リリース	説明
基本および拡張脅威検出統計情報、スキャン脅威検出	8.0(2)	基本および拡張脅威検出統計情報、スキャン脅威検出が導入されました。 次の画面が導入されました。[Configuration] > [Firewall] > [Threat Detection]、[Home] > [Firewall Dashboard] > [Traffic Overview]、[Home] > [Firewall Dashboard] > [Top 10 Access Rules]、[Home] > [Firewall Dashboard] > [Top Usage Status]、[Home] > [Firewall Dashboard] > [Top 10 Protected Servers Under SYN Attack]。
排除期間	8.0(4)/8.1(2)	排除期間を設定できるようになりました。 次の画面が変更されました。[Configuration] > [Firewall] > [Threat Detection]。
TCP 代行受信の統計情報	8.0(4)/8.1(2)	TCP 代行受信の統計情報が導入されました。 次の画面が導入または変更されました。[Configuration] > [Firewall] > [Threat Detection]、[Home] > [Firewall Dashboard] > [Top 10 Protected Servers Under SYN Attack]。
ホスト統計情報レート間隔のカスタマイズ	8.1(2)	統計情報が収集されるレート間隔の数をカスタマイズできるようになりました。デフォルトのレート数は、3 から 1 に変更されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Threat Detection]。
バースト レート間隔が平均レートの 1/30 に変更されました。	8.2(1)	以前のリリースでは、平均レートの 1/60 でした。メモリを最大限に使用するため、サンプリング間隔が平均レートの間に 30 回に減らされました。
ポートおよびプロトコル統計情報レート間隔のカスタマイズ	8.3(1)	統計情報が収集されるレート間隔の数をカスタマイズできるようになりました。デフォルトのレート数は、3 から 1 に変更されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Threat Detection]。
メモリ使用率の向上	8.3(1)	脅威検出のメモリ使用率が向上しました。

PART 6

ASA モジュール

ASA FirePOWER（SFR）モジュール

この章では、ASA で実行される ASA FirePOWER モジュールを設定する方法について説明します。

- 「ASA FirePOWER モジュール」（P.18-1）
- 「ASA FirePOWER モジュールのライセンス要件」（P.18-5）
- 「ASA FirePOWER のガイドライン」（P.18-6）
- 「ASA FirePOWER のデフォルト」（P.18-7）
- 「ASA FirePOWER モジュールの設定」（P.18-7）
- 「ASA FirePOWER モジュールの管理」（P.18-19）
- 「ASA FirePOWER モジュールのモニタリング」（P.18-24）
- 「ASA FirePOWER モジュールの履歴」（P.18-26）

ASA FirePOWER モジュール

ASA FirePOWER モジュールは、次世代 IPS（NGIPS）、Application Visibility and Control（AVC）、URL フィルタリング、高度なマルウェア対策（AMP）などの次世代ファイアウォール サービスを提供します。このモジュールは、シングルまたはマルチ コンテキスト モードとルーテッドまたはトランスペアレント モードで使用できます。

このモジュールは ASA SFR とも呼ばれます。

このモジュールには、初期設定およびトラブルシューティングのための基本的なコマンド ライン インターフェイス（CLI）が用意されていますが、デバイスのセキュリティ ポリシーは、独立したアプリケーションである FireSIGHT 管理センター を使用して設定できます。このアプリケーションは、独立した FireSIGHT 管理センター アプライアンスで、または VMware サーバ上で実行される仮想アプライアンスとしてホストできます （FireSIGHT 管理センター は防御センターとも呼ばれます）。

- 「ASA FirePOWER モジュールを ASA と連携させる方法」（P.18-2）
- 「ASA FirePOWER 管理アクセス」（P.18-4）
- 「ASA の機能との互換性」（P.18-5）

ASA FirePOWER モジュールを ASA と連携させる方法

ASA FirePOWER モジュールは、ASA とは別のアプリケーションを実行します。このモジュールは、ハードウェア モジュール（ASA 5585-X 上）か、ソフトウェア モジュール（5512-X ～ 5555-X）です。ハードウェア モジュールには、独立した管理およびコンソール ポートと、モジュール自体ではなく ASA によって直接使用される追加のデータ インターフェイスがあります。

デバイスは、パッシブ（「モニタ専用」）展開またはインライン展開のいずれかで設定できます。

- パッシブ展開では、トラフィックのコピーがデバイスに送信されますが、ASA には返されません。パッシブ モードでは、デバイスがトラフィックに対して実行したであろう処理を表示し、ネットワークに影響を与えずにトラフィックの内容を評価することができます。
- インライン展開では、実際のトラフィックがデバイスに送信され、デバイスのポリシーがトラフィックに対する処理に影響します。不要なトラフィックがドロップされ、ポリシーによって適用されるその他のアクションが実行された後、トラフィックはさらなる処理と最終的な送信のために ASA に返されます。

次の各項では、これらのモードについて詳しく説明します。

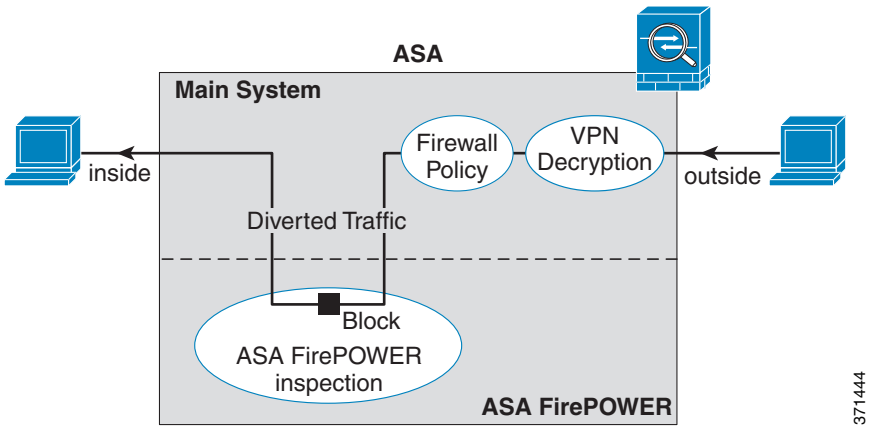
ASA FirePOWER インライン モード

インライン モードでは、トラフィックはファイアウォール検査を通過してから ASA FirePOWER モジュールへ転送されます。ASA で ASA FirePOWER インスペクションのトラフィックを識別する場合、トラフィックは次のように ASA およびモジュールを通過します。

1. トラフィックは ASA に入ります。
2. 着信 VPN トラフィックが復号化されます。
3. ファイアウォール ポリシーが適用されます。
4. トラフィックが ASA FirePOWER モジュールに送信されます。
5. ASA FirePOWER モジュールは、セキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
6. 有効なトラフィックが ASA に返送されます。ASA FirePOWER モジュールは、セキュリティ ポリシーに従ってトラフィックをブロックすることがあり、ブロックされたトラフィックは渡されません。
7. 発信 VPN トラフィックが暗号化されます。
8. トラフィックが ASA から出ます。

次の図に、ASA FirePOWER モジュールをインライン モードで使用する場合のトラフィック フローを示します。この例では、特定のアプリケーションに対して許可されていないトラフィックがモジュールによってブロックされます。それ以外のトラフィックは、ASA を通って転送されます。

図 18-1　　ASA での ASA FirePOWER モジュールのトラフィック フロー



（注） 2 つの ASA インターフェイス上でホスト間が接続されており、ASA FirePOWER のサービス ポリシーがインターフェイスの一方のみについて設定されている場合は、これらのホスト間のすべてのトラフィックが ASA FirePOWER モジュールに送信されます。これには、ASA FirePOWER インターフェイス以外からのトラフィックも含まれます（この機能は双方向であるため）。

ASA FirePOWER パッシブ（モニタ専用）モード

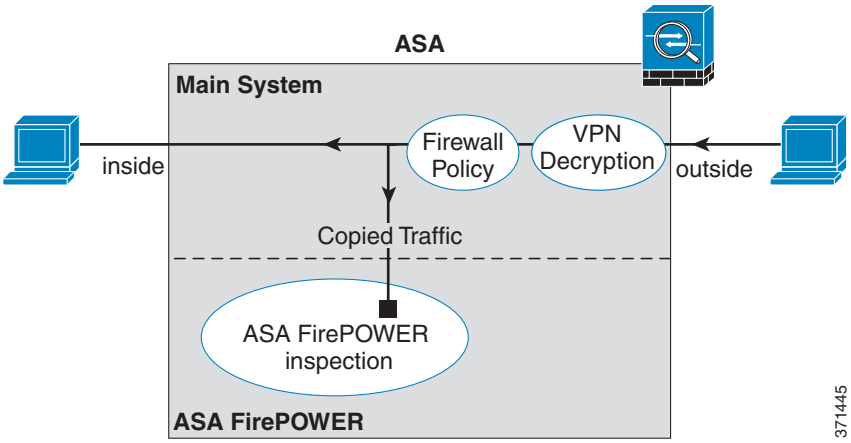
モニタ専用モードのトラフィック フローは、インライン モードのトラフィック フローと同じです。唯一の違いは、ASA FirePOWER モジュールが ASA に戻るトラフィックを通過させないことです。代わりに、モジュールはトラフィックにセキュリティ ポリシーを適用し、インライン モードで動作していた場合には実行したであろう処理をユーザに通知します。たとえば、トラフィックはイベントで「ドロップされていたはず」とマークされる場合があります。この情報をトラフィック分析に使用し、インライン モードが望ましいかどうかを判断するのに役立てることができます。

パッシブ モードを設定するには、モジュールへトラフィックをリダイレクトするサービス ポリシーに monitor-only という指示を追加します。

（注） ASA 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。マルチ コンテキスト モードでは、あるコンテキストについてモニタ専用モードを設定し、それ以外のコンテキストについて通常のインライン モードを設定することはできません。

次の図に、パッシブ 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。

図 18-2　ASA FirePOWER パッシブ（モニタ専用）モード



ASA FirePOWER 管理アクセス

ASA FirePOWER モジュールの管理には、初期設定（およびそれ以降のトラブルシューティング）およびポリシー管理という 2 つの異なる段階があります。

- 「初期設定」（P.18-4）
- 「ポリシー設定および管理」（P.18-5）

初期設定

初期設定では、ASA FirePOWER モジュールの CLI を使用する必要があります。デフォルトの管理アドレスの詳細については、「ASA FirePOWER のデフォルト」（P.18-7）を参照してください。

CLI にアクセスするには、次の方法を使用します。

- ASA 5585-X
  - ASA FirePOWER コンソール ポート：モジュールのコンソール ポートは、独立した外部コンソール ポートです。
  - ASA FirePOWER Management 1/0 インターフェイス（SSH を使用）：デフォルトの IP アドレスに接続することも、ASDM を使用して管理 IP アドレスを変更してから SSH を使用して接続することもできます。モジュールの管理インターフェイスは、独立した外部ギガビット イーサネット インターフェイスです。

（注）　**session** コマンドを使用し、ASA バックプレーンを介して ASA FirePOWER ハードウェア モジュール CLI にアクセスすることはできません。

- ASA 5512-X ～ ASA 5555-X
  - バックプレーンを経由した ASA セッション：ASA に CLI アクセスが可能な場合は、モジュールにセッション接続し、そのモジュール CLI にアクセスできます。

– ASA FirePOWER Management 0/0 インターフェイス（SSH を使用）：デフォルトの IP アドレスに接続することも、ASDM を使用して管理 IP アドレスを変更してから SSH を使用して接続することもできます。これらのモデルは、ASA FirePOWER モジュールをソフトウェア モジュールとして実行します。ASA FirePOWER160管理インターフェイスは、Management 0/0 インターフェイスを ASA と共有します。ASA と ASA FirePOWER モジュールのそれぞれに、別の MAC アドレスと IP アドレスがサポートされます。ASA FirePOWER IP アドレスの設定は、ASA FirePOWER オペレーティング システム内で（CLI または ASDM を使用して）実行する必要があります。ただし、物理特性（インターフェイスのイネーブル化など）は、ASA 上で設定されます。ASA インターフェイス コンフィギュレーションを削除して（特にインターフェイス名）、このインターフェイスを ASA FirePOWER 専用インターフェイスとすることができます。このインターフェイスは管理専用です。

ポリシー設定および管理

初期設定を実行した後で、FireSIGHT 管理センター を使用して ASA FirePOWER セキュリティ ポリシーを設定します。次に、ASDM または Cisco Security Manager を使用して、ASA FirePOWER モジュールにトラフィックを送信するための ASA ポリシーを設定します。

ASA の機能との互換性

ASA には、多数の高度なアプリケーション インスペクション機能があり、HTTP インスペクションもその一つです。ただし、ASA FirePOWER モジュールには ASA よりも高度な HTTP インスペクション機能があり、その他のアプリケーションについても機能が追加されています。たとえば、アプリケーション使用状況のモニタリングと制御です。

ASA FirePOWER モジュールの機能を最大限に活用するには、ASA FirePOWER モジュールに送信するトラフィックに関する次のガイドラインを参照してください。

- HTTP トラフィックに対して ASA インスペクションを設定しないでください。
- クラウド Web セキュリティ（ScanSafe）インスペクションを設定しないでください。同じトラフィックに対して ASA FirePOWER インスペクションおよびクラウド Web セキュリティ インスペクションの両方を設定した場合、ASA は ASA FirePOWER インスペクションのみを実行します。
- ASA 上の他のアプリケーション インスペクションは ASA FirePOWER モジュールと互換性があり、これにはデフォルト インスペクションも含まれます。
- Mobile User Security（MUS）サーバをイネーブルにしないでください。これは、ASA FirePOWER モジュールとの間に互換性がありません。
- フェールオーバーをイネーブルにしている場合、ASA がフェールオーバーすると、既存の ASA FirePOWER フローは新しい ASA に転送されます。新しい ASA の ASA FirePOWER モジュールがその時点からトラフィックのインスペクションを開始します。古いインスペクションの状態は転送されません。

ASA FirePOWER モジュールのライセンス要件

ASA FirePOWER モジュールと FireSIGHT 管理センター には、追加のライセンスが必要です。これらのライセンスは、ASA のコンテキストではなく、モジュール自体にインストールする必要があります。ASA 自体には、追加ライセンスは必要ありません。

詳細については、『*FireSIGHT System User Guide*』の「Licensing」の章または FireSIGHT 管理センター のオンライン ヘルプを参照してください。

ASA FirePOWER のガイドライン

フェールオーバーのガイドライン

フェールオーバーを直接サポートしていません。ASA がフェールオーバーすると、既存の ASA FirePOWER フローは新しい ASA に転送されます。新しい ASA の ASA FirePOWER モジュールがその時点からトラフィックのインスペクションを開始します。古いインスペクションの状態は転送されません。

フェールオーバーの動作の一貫性を確保するために、高可用性 ASA ペアの ASA FirePOWER モジュールで一貫性のあるポリシーを維持する必要があります（FireSIGHT 管理センター を使用）。

ASA クラスタリングのガイドライン

このモジュールは、クラスタリングは直接サポートしていませんが、クラスタで使用できます。FireSIGHT 管理センター を使用して、クラスタの ASA FirePOWER モジュールで一貫性のあるポリシーを維持する必要があります。クラスタ内のデバイスに異なる ASA インターフェイスベースのゾーン定義を使用しないでください。

モデルのガイドライン

- ASA 5585-X（ハードウェア モジュールとして）および 5512-X ～ ASA 5555-X（ソフトウェア モジュールとして）でサポートされています。詳細については、『*Cisco ASA Compatibility Matrix*』を参照してください。

  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

- 5512-X ～ ASA 5555-X の場合は、シスコのソリッド ステート ドライブ（SSD）を実装する必要があります。詳細については、ASA 5500-X のハードウェア ガイドを参照してください。

その他のガイドラインと制限事項

- 「ASA の機能との互換性」（P.18-5）を参照してください。
- ハードウェア モジュールにインストールされているソフトウェアのタイプの変更はできません。つまり、購入した ASA FirePOWER モジュールに、後で別のソフトウェアをインストールすることはできません。
- ASA 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。マルチ コンテキスト モードでは、あるコンテキストについてモニタ専用モードを設定し、それ以外のコンテキストについて通常のインライン モードを設定することはできません。

ASA FirePOWER のデフォルト

次の表に、ASA FirePOWER モジュールのデフォルト設定を示します。

表 18-1　ASA FirePOWER のデフォルトのネットワーク パラメータ

パラメータ	デフォルト
管理 IP アドレス	• システム ソフトウェア イメージ：192.168.45.45/24 • ブート イメージ： – ASA 5585-X：Management 1/0 192.168.8.8/24 – ASA 5512-X ～ ASA 5555-X：Management 0/0 192.168.1.2/24
ゲートウェイ	• システム ソフトウェア イメージ：なし • ブート イメージ： – ASA 5585-X：192.168.8.1/24 – ASA 5512-X ～ ASA 5555-X：192.168.1.1/24
SSH またはセッションのユーザ名	admin
パスワード	• システム ソフトウェア イメージ：**Sourcefire** • ブート イメージ：**Admin123**

ASA FirePOWER モジュールの設定

ASA FirePOWER モジュールの設定は、トラフィックを ASA FirePOWER モジュールに送信するための ASA FirePOWER モジュールでの ASA FirePOWER セキュリティ ポリシーの設定、およびその後の ASA の設定を含むプロセスです。ASA FirePOWER モジュールを設定するには、次の手順に従います。

ステップ 1　「ASA FirePOWER 管理インターフェイスの接続」（P.18-8）ケーブルで ASA FirePOWER 管理インターフェイスに（任意でコンソール インターフェイスにも）接続します。

ステップ 2　「（ASA 5512-X ～ 5555-X）ソフトウェア モジュールのインストールまたはイメージの再作成」（P.18-11）

ステップ 3　「ASA FirePOWER 管理 IP アドレスの変更」（P.18-15）（必要な場合）。これは最初の SSH アクセスに必要になる場合があります。

ステップ 4　「ASA FirePOWER CLI での基本的な ASA FirePOWER 設定値の設定」（P.18-15）これは ASA FirePOWER モジュールで行います。

ステップ 5　「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.18-16）これはデバイスを管理する FireSIGHT 管理センター を指定します。

ステップ 6　「ASA FirePOWER モジュールでのセキュリティ ポリシーの設定」（P.18-18）

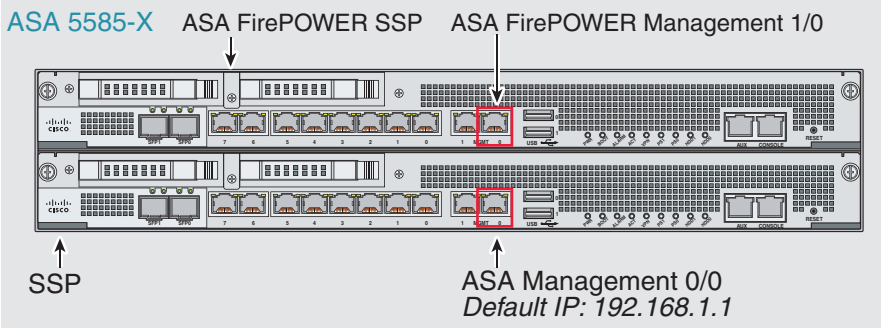
ステップ 7　「ASA FirePOWER モジュールへのトラフィックのリダイレクト」（P.18-18）

ASA FirePOWER 管理インターフェイスの接続

ASA FirePOWER モジュールへの管理アクセスを提供する以外に、ASA FirePOWER 管理インターフェイスは、HTTP プロキシ サーバまたは DNS サーバおよびインターネットへのアクセスを必要とします。これは、シグネチャの更新などのためです。この項では、推奨されるネットワーク コンフィギュレーションを示します。実際のネットワークでは、異なる可能性があります。

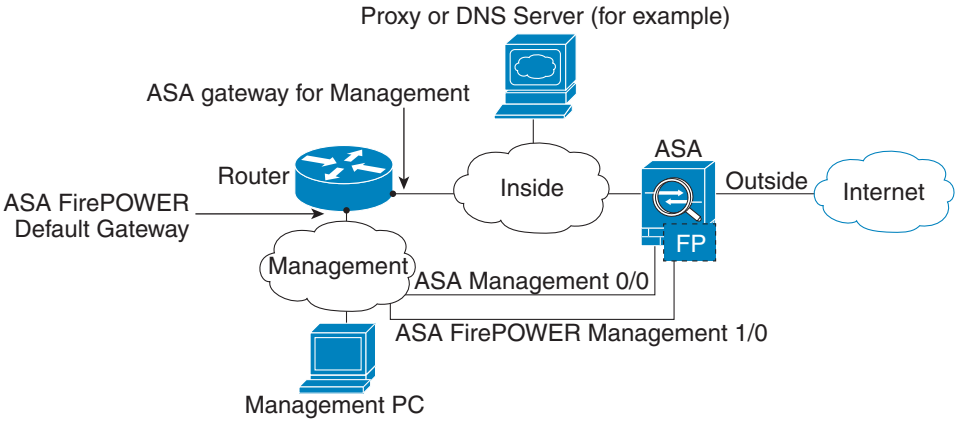
ASA 5585-X（ハードウェア モジュール）

ASA FirePOWER モジュールには、ASA とは別の管理およびコンソール インターフェイスが含まれます。初期設定の場合、デフォルト IP アドレスを使用して ASA FirePOWER Management 1/0 インターフェイスに SSH で接続できます。デフォルト IP アドレスを使用できない場合は、コンソール ポートを使用するか、ASDM を使用して SSH を使用できるように管理 IP アドレスを変更します （「ASA FirePOWER 管理 IP アドレスの変更」（P.18-15）を参照）。



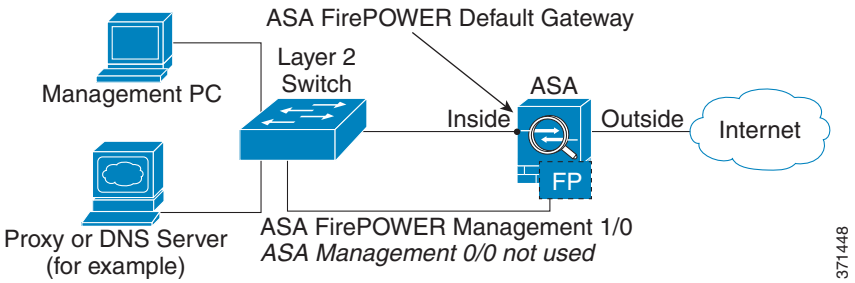
内部ルータがある場合

内部ルータがある場合は、管理ネットワーク（これには ASA Management 0/0 インターフェイスおよび ASA FirePOWER Management 1/0 インターフェイスの両方を含めることができます）と ASA 内部ネットワークとの間でルーティングできます（インターネット アクセス用）。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



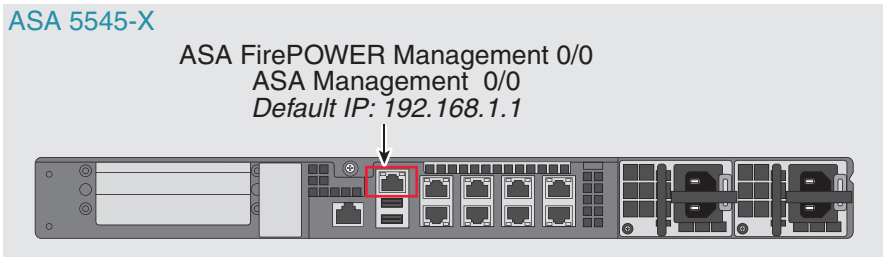
内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません（仮に持つとすれば、内部ルータがネットワーク間のルーティングを行う必要があります）。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA FirePOWER モジュールは ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に ASA FirePOWER Management 1/0 アドレスを設定できます。



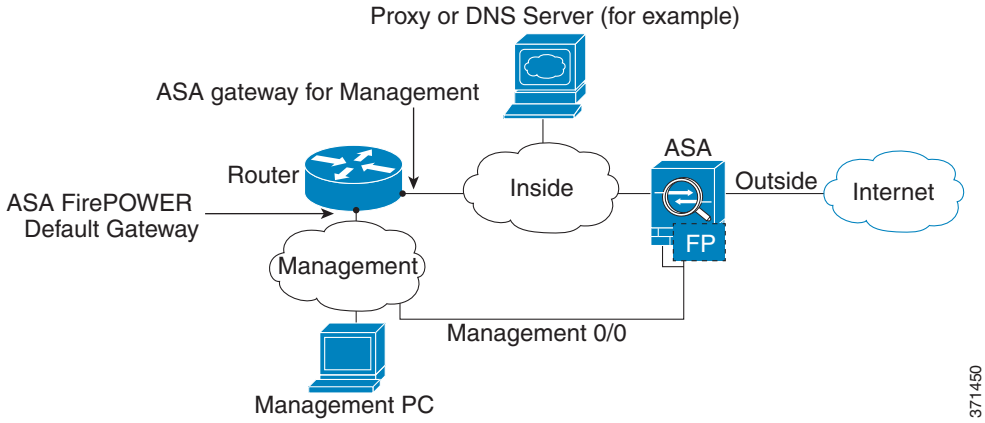
ASA 5512-X ～ ASA 5555-X（ソフトウェア モジュール）

これらのモデルは、ASA FirePOWER モジュールをソフトウェア モジュールとして実行し、ASA FirePOWER 管理インターフェイスは Management 0/0 インターフェイスを ASA と共有します。初期設定の場合、デフォルト IP アドレスを使用して ASA FirePOWER に SSH で接続できます。デフォルト IP アドレスを使用できない場合は、バックプレーンを経由して ASA FirePOWER にセッション接続するか、ASDM を使用して SSH を使用できるように管理 IP アドレスを変更します。



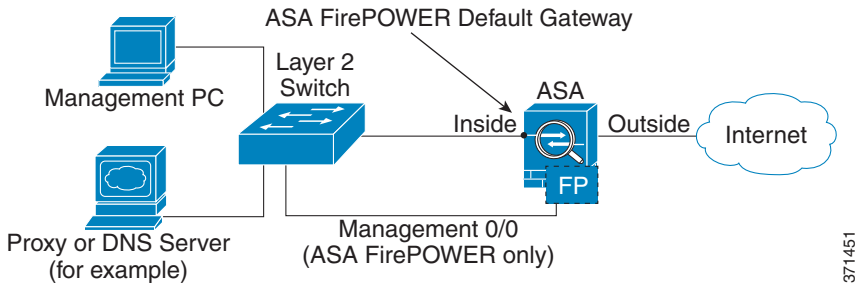
内部ルータがある場合

内部ルータがある場合、Management 0/0 ネットワーク間でルーティングできます。これには、ASA および ASA FirePOWER の両方の管理 IP アドレス、およびインターネット アクセス用の内部ネットワークが含まれます。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA で設定された名前を Management 0/0 インターフェイスから削除した場合も、そのインターフェイスの ASA FirePOWER IP アドレスを設定できます。ASA FirePOWER モジュールは実質的に ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に ASA FirePOWER 管理アドレスを設定できます。



（注）　Management 0/0 に対して ASA で設定された名前を削除する必要があります。この名前が ASA 上で設定されている場合は、ASA FirePOWER のアドレスは ASA と同じネットワーク上にあることが必要になり、その結果、他の ASA インターフェイス上ですでに設定されたネットワークが除外されます。名前が設定されていない場合は、ASA FirePOWER のアドレスが存在するのはどのネットワークでも、たとえば、ASA 内部ネットワークでもかまいません。

（ASA 5512-X ～ 5555-X）ソフトウェア モジュールのインストールまたはイメージの再作成

ASA FirePOWER モジュールとともに ASA を購入した場合、モジュール ソフトウェアおよび必要なソリッド ステート ドライブ（SSD）は事前にインストールされており、すぐに設定できます。既存の ASA に ASA FirePOWER ソフトウェア モジュールを追加する場合、または SSD を交換する必要がある場合は、この手順に従って ASA FirePOWER ブート ソフトウェアをインストールし、SSD を分割して、システム ソフトウェアをインストールする必要があります。

モジュールのイメージを再作成する手順は、最初に ASA FirePOWER モジュールをアンインストールする必要があることを除いてこれと同じです。システムのイメージの再作成は、SSD を交換する場合に行います。

物理的に SSD を取り付ける方法の詳細については、『ASA Hardware Guide』を参照してください。

はじめる前に

- フラッシュ（disk0）の空き領域には、少なくとも、ブート ソフトウェアのサイズに 3 GB を加えた大きさが必要です。
- マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。
- 実行している可能性があるその他のソフトウェア モジュールをシャットダウンする必要があります。デバイスでは、一度に 1 つのソフトウェア モジュールを実行できます。これは ASA CLI から実行する必要があります。たとえば、次のコマンドは IPS モジュール ソフトウェアをシャット ダウンしアンインストールしてから、ASA をリロードします。CX モジュールを削除するコマンドは、**ips** の代わりに **cxsc** キーワードを使用することを除いてこのコマンドと同じです。

```
hostname# sw-module module ips shutdown
hostname# sw-module module ips uninstall
hostname# reload
```

（注）　IPS または CX モジュールにトラフィックをリダイレクトするアクティブ サービス ポリシーがある場合、そのポリシーを削除する必要があります。たとえば、ポリシーがグローバル ポリシーの場合、**no service-policy** *ips_policy* **global** を使用します。ポリシーは、CLI または ASDM を使用して削除できます。

- モジュールのイメージを再作成する場合は、同じシャットダウン/アンインストール コマンドを使用して古いイメージを削除します。たとえば、**sw-module module sfr uninstall** を使用します。
- ASA FirePOWER のブート イメージとシステム ソフトウェア パッケージの両方を Cisco.com から取得します。

手順

ステップ 1　ブート イメージをデバイスにダウンロードします。システム ソフトウェアは転送しないでください。これは後で SSD にダウンロードされます。次の選択肢があります。

- ASDM：まず、ブート イメージをワークステーションにダウンロードするか、FTP、TFTP、HTTP、HTTPS、SMB、または SCP サーバに配置します。次に、ASDM で [Tools] > [File Management] の順に選択し、[Between Local PC and Flash] または [Between Remote Server and Flashnd] のいずれか該当する [File Transfer] コマンドを選択します。ブート ソフトウェアを ASA 上の disk0 に転送します。

- ASA CLI：まず、ブート イメージを TFTP、FTP、HTTP、または HTTPS サーバに配置し、**copy** コマンドを使用してそのブート イメージをフラッシュにダウンロードします。次の例では TFTP を使用しています。<TFTP Server> をお使いのサーバの IP アドレスまたはホスト名に置き換えてください。

```
ciscoasa# copy tftp://<TFTP SERVER>/asasfr-5500x-boot-5.3.1-58.img
disk0:/asasfr-5500x-boot-5.3.1-58.img
```

ステップ 2　ASA FirePOWER 管理インターフェイスからアクセス可能な HTTP、HTTPS、または FTP サーバに、Cisco.com から ASA FirePOWER システム ソフトウェアをダウンロードします。

ステップ 3　次のコマンドを入力して、ASA disk0 で ASA FirePOWER モジュール ブート イメージの場所を設定します。

```
hostname# sw-module module sfr recover configure image disk0:file_path
```

（注）「ERROR: Another service (cxsc) is running, only one service is allowed to run at any time」のようなメッセージが表示される場合は、すでに別のソフトウェア モジュールが設定されています。このソフトウェア モジュールをシャットダウンして削除し、上述した前提条件の項の説明に従って新しいモジュールをインストールする必要があります。

例：

```
hostname# sw-module module sfr recover configure image
disk0:asasfr-5500x-boot-5.3.1-58.img
```

ステップ 4　次のコマンドを入力して、ASA FirePOWER ブート イメージをロードします。

```
hostname# sw-module module sfr recover boot
```

ステップ 5　ASA FirePOWER モジュールが起動するまで約 5 ～ 15 分待ってから、現在実行中の ASA FirePOWER ブート イメージへのコンソール セッションを開きます。ログイン プロンプトを表示するには、セッションを開いた後に Enter を押さなければならない場合があります。デフォルトのユーザ名は **admin** で、デフォルトのパスワードは **Admin123** です。

```
hostname# session sfr console
Opening console session with module sfr.
Connected to module sfr.Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

ヒント　モジュールのブートが完了していない場合は、**session** コマンドが失敗し、ttyS1 経由で接続できないことに関するメッセージが表示されます。しばらく待ってから再試行してください。

ステップ 6　システム ソフトウェア パッケージをインストールできるように、**setup** コマンドを使用してシステムを設定します。

```
asasfr-boot> setup

        Welcome to SFR Setup
          [hit Ctrl-C to abort]
      Default values are inside []
```

次の項目を指定するように求められます。重要な設定項目は、管理アドレスとゲートウェイ、および DNS 情報です。

- ホスト名：65 文字までの英数字で、スペースは使用できません。ハイフンを使用できます。
- ネットワーク アドレス：スタティック IPv4 または IPv6 アドレスを設定するか、または DHCP（IPv4 の場合）または IPv6 ステートレス自動設定を使用することができます。
- DNS 情報：少なくとも 1 つの DNS サーバを指定する必要があります。ドメイン名と検索ドメインを設定することもできます。
- NTP 情報：システム時刻を設定するために、NTP をイネーブルにして NTP サーバを設定することができます。

ステップ 7　**system install** コマンドを使用してシステム ソフトウェア イメージをインストールします。

system install [**noconfirm**] *url*

確認メッセージを表示しないようにするには、**noconfirm** オプションを指定します。HTTP、HTTPS、または FTP URL を使用します。ユーザ名とパスワードが必要な場合は、それらを指定するように求められます。

インストールが完了すると、システムが再起動します。アプリケーション コンポーネントのインストールと ASA FirePOWER サービスの起動には 10 分以上かかります（**show module sfr** の出力で、すべてのプロセスが Up であると表示される必要があります）。

次に例を示します。

```
asasfr-boot> system install http://asasfr-sys-5.3.1-44.pkg
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA-FirePOWER 5.3.1-44 System Install
        Requires reboot:                Yes

Do you want to continue with upgrade? [y]: y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade.Press 'Enter' to reboot the system.
(Enter を押します)
Broadcast message from root (ttyS1) (Mon Feb 17 19:28:38 2014):

The system is going down for reboot NOW!
Console session with module sfr terminated.
```

ステップ 8　ASA FirePOWER モジュールへのセッションを開きます。フル機能のモジュールにログインしているため、別のログイン プロンプトが表示されます。

```
asa3# session sfr
Opening command session with module sfr.
Connected to module sfr.Escape character sequence is 'CTRL-^X'.

Sourcefire ASA5555 v5.3.1 (build 44)
Sourcefire3D login:
```

ステップ 9　ユーザ名 **admin** およびパスワード **Sourcefire** を使用してログインします。

ステップ 10　プロンプトに従ってシステム設定を完了します。

まず、エンド ユーザ ライセンス契約（EULA）を読み、これに同意する必要があります。次に、プロンプトに従って管理者パスワードを変更し、管理アドレスと DNS 設定を設定します。IPv4 と IPv6 の両方の管理アドレスを設定できます。次に例を示します。

```
System initialization in progress.Please stand by.
You must change the password for 'admin' to continue.
Enter new password: < 新しいパスワード >
Confirm new password: < パスワードの再入力 >
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.86.118.3
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
10.120.10.14
Enter a comma-separated list of search domains or 'none' [example.net]: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
（システムが自動的に再設定されるまで待機します）

This sensor must be managed by a Defense Center.A unique alphanumeric
registration key is always required.In most cases, to register a sensor
to a Defense Center, you must provide the hostname or the IP address along
with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Defense Center are separated by a NAT device,
you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.
```

ステップ 11　**configure manager add** コマンドを使用して、このデバイスを管理する FireSIGHT 管理センター アプライアンスを指定します。

登録キーを決めます。このキーは、デバイスをインベントリに追加するときに FireSIGHT 管理センター で使用します。次に、簡単な例を示します。NAT 境界がある場合は、コマンドが異なります。「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.18-16）を参照してください。

```
> configure manager add 10.89.133.202 123456
Manager successfully configured.
```

ステップ 12　上で入力したホスト名またはアドレスを使用し、ブラウザで HTTPS 接続を使用して FireSIGHT 管理センター にログインします。たとえば、https://DC.example.com などです。

[Device Management]（[Devices] > [Device Management]）ページでデバイスを追加します。詳細については、オンライン ヘルプまたは『*FireSIGHT System User Guide*』の「Managing Devices」の章を参照してください。

ヒント　また、FireSIGHT 管理センター で NTP と時刻設定も設定します。時刻同期設定は、[System] > [Local] > [System Policy] ページからローカル ポリシーを編集する場合に使用します。

ASA FirePOWER 管理 IP アドレスの変更

デフォルトの管理 IP アドレスを使用できない場合、ASA から管理 IP アドレスを設定できます。管理 IP アドレスを設定した後は、追加設定を実行するために SSH を使用して ASA FirePOWER モジュールにアクセスできます。

システムの初期設定時に「ASA FirePOWER CLI での基本的な ASA FirePOWER 設定値の設定」（P.18-15）の説明に従って ASA FirePOWER CLI で管理アドレスをすでに設定している場合は、ASA CLI または ASDM で管理アドレスを設定する必要はありません。

（注） ソフトウェア モジュールの場合、ASA FirePOWER CLI にアクセスして、ASA CLI からのセッション接続によって設定を実行できます。その後、設定の一環として ASA FirePOWER 管理 IP アドレスを設定できます。ハードウェア モジュールの場合は、コンソール ポートを使用して初期設定を完了できます。

ASA で管理 IP アドレスを変更するには、次のいずれかを実行します。マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

- CLI で次のコマンドを使用して、ASA FirePOWER 管理 IP アドレス、マスク、およびゲートウェイを設定します。ハードウェア モジュールの場合は **1**、ソフトウェア モジュールの場合は **sfr** を使用します。

  session {1 | sfr} do setup host ip *ip_address/mask,gateway_ip*

  たとえば、**session 1 do setup host ip 10.1.1.2/24,10.1.1.1** と指定します。

- ASDM では、[Wizards] > [Startup Wizard] の順に選択し、ウィザードで [ASA FirePOWER Basic Configuration] に進みます。このページでは、IP アドレス、マスク、およびデフォルト ゲートウェイを設定できます。

ASA FirePOWER CLI での基本的な ASA FirePOWER 設定値の設定

セキュリティ ポリシーを設定する前に、基本的なネットワーク設定およびその他のパラメータを ASA FirePOWER モジュール上で設定する必要があります。この手順では、完全なシステム ソフトウェア（ブート イメージだけでなく）がインストールされていること（直接インストールしたか、ハードウェア モジュールにインストール済みであること）を前提としています。

ヒント この手順では、初期設定を実行していることも前提としています。初期設定時に、これらの設定を行うように求められます。これらの設定を後で変更する必要がある場合は、各種の **configure network** コマンドを使用して個々の設定を変更します。**configure network** コマンドの詳細については、**?** コマンドを使用してヘルプを表示し、『*FireSIGHT System User Guide*』または FireSIGHT 管理センター のオンライン ヘルプを参照してください。

手順

ステップ 1　次のどちらかを実行します。

- （すべてのモデル）SSH を使用して ASA FirePOWER 管理 IP アドレスに接続します。
- （ASA 5512-X ～ ASA 5555-X）ASA CLI からモジュールへのセッションを開きます（ASA CLI へのアクセスについては、『一般的な操作のコンフィギュレーション ガイド』の「Getting Started」の章を参照してください）。マルチ コンテキスト モードでは、システム実行スペースからセッションを開きます。

```
hostname# session sfr
```

ステップ 2　ユーザ名 **admin** およびパスワード **Sourcefire** を使用してログインします。

ステップ 3　プロンプトに従ってシステム設定を完了します。

まず、エンド ユーザ ライセンス契約（EULA）を読み、これに同意する必要があります。次に、プロンプトに従って管理者パスワードを変更し、管理アドレスと DNS 設定を設定します。IPv4 と IPv6 の両方の管理アドレスを設定できます。センサーは FireSIGHT 管理センター で管理する必要があるというメッセージが表示されたら、設定は完了です。

次に例を示します。

```
System initialization in progress.Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <新しいパスワード>
Confirm new password: <パスワードの再入力>
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.86.118.3
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
10.120.10.14
Enter a comma-separated list of search domains or 'none' [example.net]: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
(システムが自動的に再設定されるまで待機します)

This sensor must be managed by a Defense Center.A unique alphanumeric
registration key is always required.In most cases, to register a sensor
to a Defense Center, you must provide the hostname or the IP address along
with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Defense Center are separated by a NAT device,
you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.
```

ステップ 4　ここで、「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.18-16）の説明に従って、このデバイスを管理する FireSIGHT 管理センター を指定する必要があります。

FireSIGHT 管理センター への ASA FirePOWER の追加

モジュールにポリシーを設定するためのアプリケーションである FireSIGHT 管理センター に、ASA FirePOWER モジュールを登録する必要があります。FireSIGHT 管理センター は防御センターとも呼ばれます

デバイスを登録するには、**configure manager add** コマンドを使用します。FireSIGHT 管理センター にデバイスを登録するには、一意の英数字の登録キーが常に必要です。これはユーザが指定する簡単なキーで、ライセンス キーと同じではありません。

ほとんどの場合、FireSIGHT 管理センター のホスト名または IP アドレスを登録キーと一緒に指定する必要があります。次に例を示します。

```
configure manager add DC.example.com my_reg_key
```

ただし、デバイスと FireSIGHT 管理センター が NAT デバイスによって分離されている場合、一意の NAT ID を登録キーと一緒に入力し、ホスト名の代わりに DONTRESOLVE を指定します。次に例を示します。

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

手順

ステップ 1　次のどちらかを実行します。

- （すべてのモデル）SSH を使用して ASA FirePOWER 管理 IP アドレスに接続します。
- （ASA 5512-X ～ ASA 5555-X）ASA CLI からモジュールへのセッションを開きます（ASA CLI へのアクセスについては、『一般的な操作のコンフィギュレーション ガイド』の「Getting Started」の章を参照してください）。マルチ コンテキスト モードでは、システム実行スペースからセッションを開きます。

  ```
  hostname# session sfr
  ```

ステップ 2　ユーザ名 **admin** または CLI コンフィギュレーション（管理者）アクセス レベルを持つ別のユーザ名でログインします。

ステップ 3　プロンプトで、**configure manager add** コマンドを使用して FireSIGHT 管理センター にデバイスを登録します。このコマンドの構文は次のとおりです。

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

それぞれの説明は次のとおりです。

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} では、FireSIGHT 管理センターの完全修飾ホスト名または IP アドレスを指定します。FireSIGHT 管理センター のアドレスを直接指定できない場合は、DONTRESOLVE を使用します。
- *reg_key* は、FireSIGHT 管理センター にデバイスを登録するために必要な一意の英数字の登録キーです。
- *nat_id* は、FireSIGHT 管理センター とデバイス間の登録プロセス中に使用されるオプションの英数字の文字列です。これは、ホスト名が DONTRESOLVE に設定されている場合に必要です。

ステップ 4　上で入力したホスト名またはアドレスを使用し、ブラウザで HTTPS 接続を使用して FireSIGHT 管理センター にログインします。たとえば、https://DC.example.com などです。

[Device Management]（[Devices] > [Device Management]）ページでデバイスを追加します。詳細については、オンライン ヘルプまたは『*FireSIGHT System User Guide*』の「Managing Devices」の章を参照してください。

ASA FirePOWER モジュールでのセキュリティ ポリシーの設定

ASA FirePOWER モジュールにセキュリティ ポリシーを設定するには、FireSIGHT 管理センター を使用します。セキュリティ ポリシーは、次世代 IPS フィルタリングやアプリケーション フィルタリングなど、モジュールによって提供されるサービスを制御します。ASA FirePOWER CLI、ASA CLI、または ASDM を使用してポリシーを設定することはできません。

FireSIGHT 管理センター を開くには、Web ブラウザを使用して次の URL を開きます。

https://*DC_address*

DC_address は、「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.18-16）で定義したマネージャの DNS 名または IP アドレスです。たとえば、https://dc.example.com などです。

セキュリティ ポリシーの設定方法については、『*FireSIGHT System User Guide*（*FireSIGHT システム ユーザ ガイド*）』または FireSIGHT 管理センター のオンライン ヘルプを参照してください。

ヒント　FireSIGHT 管理センター は、ASDM の [ASA FirePOWER Status] ダッシュボードから開くこともできます。[Home] > [ASA FirePOWER Status] を選択して、ダッシュボードの下部にあるリンクをクリックします。

ASA FirePOWER モジュールへのトラフィックのリダイレクト

トラフィックを ASA FirePOWER モジュールへリダイレクトするには、特定のトラフィックを識別するサービス ポリシーを作成します。

デバイスは、パッシブ（「モニタ専用」）展開またはインライン展開のいずれかで設定できます。

- パッシブ展開では、トラフィックのコピーがデバイスに送信されますが、ASA には返されません。パッシブ モードでは、デバイスがトラフィックに対して実行したであろう処理を表示し、ネットワークに影響を与えずにトラフィックの内容を評価することができます。
- インライン展開では、実際のトラフィックがデバイスに送信され、デバイスのポリシーがトラフィックに対する処理に影響します。不要なトラフィックがドロップされ、ポリシーによって適用されるその他のアクションが実行された後、トラフィックはさらなる処理と最終的な送信のために ASA に返されます。

（注）　ASA 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。マルチ コンテキスト モードでは、あるコンテキストについてモニタ専用モードを設定し、それ以外のコンテキストについて通常のインライン モードを設定することはできません。

はじめる前に

- （ASA FirePOWER と交換した）IPS または CX モジュールにトラフィックをリダイレクトするアクティブ サービス ポリシーがある場合は、ASA FirePOWER サービス ポリシーを設定する前にそのポリシーを削除する必要があります。
- ASA および ASA FirePOWER には、必ず一貫性のあるポリシーを設定してください（FireSIGHT 管理センター を使用）。両方のポリシーに、トラフィックのパッシブ モードまたはインライン モードを反映させる必要があります。
- マルチコンテキスト モードでは、各セキュリティ コンテキストでこの手順を実行します。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] の順に選択します。

ステップ 2　[Add] > [Add Service Policy Rule] を選択します。[Add Service Policy Rule Wizard - Service Policy] ダイアログボックスが表示されます。

ステップ 3　必要に応じて [Service Policy] ダイアログボックスに入力します。これらの画面の詳細については、ASDM オンライン ヘルプを参照してください。

ステップ 4　[Next] をクリックします。[Add Service Policy Rule Wizard - Traffic Classification Criteria] ダイアログボックスが表示されます。

ステップ 5　必要に応じて [Traffic Classification Criteria] ダイアログボックスに入力します。これらの画面の詳細については、ASDM オンライン ヘルプを参照してください。

ステップ 6　[Next] をクリックして [Add Service Policy Rule Wizard - Rule Actions] ダイアログボックスを表示します。

ステップ 7　[ASA FirePOWER Inspection] タブをクリックします。

ステップ 8　[Enable ASA FirePOWER for this traffic flow] チェックボックスをオンにします。

ステップ 9　[ASA FirePOWER Card Fails] 領域で、次のいずれかをクリックします。

- [Permit traffic]：モジュールが使用できない場合、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 ASA を設定します。
- [Close traffic]：モジュールが使用できない場合、すべてのトラフィックをブロックするように ASA を設定します。

ステップ 10　（オプション）トラフィックの読み取り専用コピーをモジュールに送信するには、[Monitor-only] をオンにします（パッシブ モード）。このオプションを選択した場合、トラフィックはインライン モードで送信されます。詳細については、「ASA FirePOWER パッシブ（モニタ専用）モード」（P.18-3）を参照してください。

ステップ 11　[Finish]、[Apply] の順にクリックします。

この手順を繰り返して、追加のトラフィック フローを必要に応じて設定します。

ASA FirePOWER モジュールの管理

この項には、モジュールの管理に役立つ手順が含まれます。

- 「パスワードのリセット」（P.18-20）
- 「モジュールのリロードまたはリセット」（P.18-20）
- 「モジュールのシャットダウン」（P.18-20）
- 「（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュール イメージのアンインストール」（P.18-21）
- 「（ASA 5512-X ～ ASA 5555-X）ASA からモジュールへのセッション接続」（P.18-21）
- 「5585-X ASA FirePOWER ハードウェア モジュールのイメージの再作成」（P.18-22）
- 「システム ソフトウェアのアップグレード」（P.18-24）

パスワードのリセット

管理ユーザのパスワードを忘れた場合は、CLI 設定権限を持つ別のユーザがログインして、パスワードを変更できます。

必要な権限を持つ別のユーザが存在しない場合は、**session do** コマンドを使用して ASA から管理者パスワードをリセットできます。

ヒント　ASA の hw-module および sw-module コマンドの password-reset オプションは、ASA FirePOWER では機能しません。

ユーザ **admin** のモジュール パスワードをデフォルトの **Sourcefire** にリセットするには、次のコマンドを使用します。ハードウェア モジュールの場合は **1**、ソフトウェア モジュールの場合は **sfr** を使用します。マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

```
session {1 | sfr} do password-reset
```

たとえば、**session sfr do password-reset** を使用します。

モジュールのリロードまたはリセット

モジュールをリロード、またはリセットしてからリロードするには、ASA CLI で次のいずれかのコマンドを入力します。マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

- ハードウェア モジュール（ASA 5585-X）：

  ```
  hw-module module 1 {reload | reset}
  ```

- ソフトウェア モジュール（ASA 5512-X ～ ASA 5555-X）：

  ```
  sw-module module sfr {reload | reset}
  ```

モジュールのシャットダウン

モジュール ソフトウェアをシャットダウンするのは、コンフィギュレーション データを失うことなく安全にモジュールの電源をオフにできるように準備するためです。モジュールをグレースフル シャットダウンするには、ASA CLI で次のいずれかのコマンドを入力します。マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

（注）　ASA をリロードする場合は、モジュールは自動的にはシャットダウンされないので、ASA のリロード前にモジュールをシャットダウンすることを推奨します。

- ハードウェア モジュール（ASA 5585-X）：

  ```
  hw-module module 1 shutdown
  ```

- ソフトウェア モジュール（ASA 5512-X ～ ASA 5555-X）：

  ```
  sw-module module sfr shutdown
  ```

（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュール イメージのアンインストール

ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールできます。マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1　ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールします。

```
hostname# sw-module module sfr uninstall

Module sfr will be uninstalled.This will completely remove the disk image
associated with the sw-module including any configuration that existed within it.

Uninstall module sfr? [confirm]
```

ステップ 2　ASA をリロードします。新しいモジュールをインストールする前に、ASA をリロードする必要があります。

```
hostname# reload
```

（ASA 5512-X ～ ASA 5555-X）ASA からモジュールへのセッション接続

基本的なネットワーク設定を構成し、モジュールをトラブルシューティングするには、ASA FirePOWER CLI を使用します。

ASA FirePOWER ソフトウェア モジュール CLI に ASA からアクセスするには、ASA からセッションを開始します。モジュールへのセッションを開始することも（Telnet を使用）、仮想コンソール セッションを作成することもできます。コンソール セッションは、コントロール プレーンがダウンし、Telnet セッションを確立できない場合に便利です。マルチ コンテキスト モードでは、システム実行スペースからセッションを開きます。

Telnet またはコンソール セッションでは、ユーザ名とパスワードの入力を求められます。ASA FirePOWER に設定されている任意のユーザ名でログインできます。最初は、**admin** が唯一の設定済みユーザ名です（このユーザ名は常に使用可能です）。最初のデフォルトのユーザ名は、フル イメージの場合は **Sourcefire**、ブート イメージの場合は **Admin123** です。

- Telnet セッション：

  session sfr

  ASA FirePOWER CLI にいるときに ASA CLI に戻るには、モジュールからログアウトするコマンド（**logout** や **exit** など）を入力するか、**Ctrl+Shift+6、x** を押します。

- コンソール セッション：

  session sfr console

  コンソール セッションを終了する唯一の方法は、**Ctrl+Shift+6、x** を押すことです。モジュールからログアウトすると、モジュールのログイン プロンプトに戻ります。

（注）　**session sfr console** コマンドは、**Ctrl+Shift+6、x** がターミナル サーバのプロンプトに戻るエスケープ シーケンスであるターミナル サーバとともに使用しないでください。**Ctrl+Shift+6、x** は、ASA FirePOWER コンソールをエスケープして、ASA プロンプトに戻るためのシーケンスでもあります。したがって、この状況で、ASA FirePOWER コンソールを終了しようとすると、ターミナル サーバ プロンプトまで終了することになります。ASA にターミナル サーバを再接続すると、ASA FirePOWER コンソール セッションがまだアクティブなままであり、ASA プロンプトに戻ることができません。ASA プロンプトにコンソールを戻すには、直接シリアル接続を使用する必要があります。この状況が発生した場合は、console コマンドの代わりに**session sfr** コマンドを使用します。

5585-X ASA FirePOWER ハードウェア モジュールのイメージの再作成

何らかの理由で ASA FirePOWER ASA 5585-X アプライアンスのハードウェア モジュールのイメージを再作成する必要がある場合は、ブート イメージとシステム ソフトウェア パッケージの両方をこの順序でインストールする必要があります。システムが機能するには、両方のパッケージをインストールする必要があります。通常の状況では、アップグレード パッケージをインストールするために、システムのイメージを再作成する必要はありません。

ブート イメージをインストールするには、モジュールのコンソール ポートにログインして、ASA FirePOWER SSP の Management-0 ポートからイメージを TFTP ブートする必要があります。Management-0 ポートは SSP の最初のスロットにあるため、Management1/0 とも呼ばれますが、ROMmon では Management-0 または Management0/1 として認識されます。

TFTP ブートを行うには、次の手順を実行します。

- ソフトウェア イメージを、ASA FirePOWER の Management1/0 インターフェイスからアクセス可能な TFTP サーバに配置する。
- Management1/0 をネットワークに接続する。このインターフェイスを使用して、ブート イメージを TFTP ブートする必要があります。
- ROMmon 変数を設定する。ROMmon 変数を設定するには、Esc を押して自動ブート プロセスを中断します。

ブート イメージがインストールされたら、システム ソフトウェア パッケージをインストールします。ASA FirePOWER からアクセス可能な HTTP、HTTPS、または FTP サーバに、パッケージを配置する必要があります。

次の手順では、ブート イメージをインストールしてからシステム ソフトウェア パッケージをインストールする方法を説明します。

手順

ステップ 1　コンソール ポートに接続します。ASA 製品に付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナル エミュレータを用いて PC をコンソールに接続します。コンソール ケーブルの詳細については、ASA のハードウェア ガイドを参照してください。

ステップ 2　**system reboot** コマンドを入力してシステムをリロードします。

ステップ 3　プロンプトが表示されたら、Esc を押してブートから抜け出します。GRUB がシステムをブートするために起動するのが表示された場合は、待ちすぎです。

これにより、ROMmon プロンプトに切り替わります。

ステップ 4　ROMmon プロンプトで、**set** と入力して次のパラメータを設定します。

- ADDRESS：モジュールの管理 IP アドレス。
- SERVER：TFTP サーバの IP アドレス。
- GATEWAY：TFTP サーバのゲートウェイ アドレス。TFTP サーバが Management1/0 に直接接続されている場合は、TFTP サーバの IP アドレスを使用します。TFTP サーバおよび管理アドレスが同じサブネット上にある場合は、ゲートウェイを設定しないでください。設定すると、TFTP ブートが失敗します。
- IMAGE：TFTP サーバ上のブート イメージのパスとイメージ名。たとえば、TFTP サーバの /tftpboot/images/filename.img にファイルを置いた場合、IMAGE の値は images/filename.img となります。

次に例を示します。

```
ADDRESS=10.5.190.199
SERVER=10.5.11.170
GATEWAY=10.5.1.1
IMAGE=asasfr-boot-5.3.1-26-54.img
```

ステップ 5　**sync** と入力して設定を保存します。

ステップ 6　**tftp** と入力してダウンロードおよびブート プロセスを開始します。

進行状況を示す！マークが表示されます。数分後にブートが完了すると、ログイン プロンプトが表示されます。

ステップ 7　パスワード **Admin123** を使用して **admin** としてログインします。

ステップ 8　システム ソフトウェア パッケージをインストールできるように、**setup** コマンドを使用してシステムを設定します。

次の項目を指定するように求められます。重要な設定項目は、管理アドレスとゲートウェイ、および DNS 情報です。

- ホスト名：65 文字までの英数字で、スペースは使用できません。ハイフンを使用できます。
- ネットワーク アドレス：スタティック IPv4 または IPv6 アドレスを設定するか、または DHCP（IPv4 の場合）または IPv6 ステートレス自動設定を使用することができます。
- DNS 情報：少なくとも 1 つの DNS サーバを指定する必要があります。ドメイン名と検索ドメインを設定することもできます。
- NTP 情報：システム時刻を設定するために、NTP をイネーブルにして NTP サーバを設定することができます。

ステップ 9　**system install** コマンドを使用してシステム ソフトウェア イメージをインストールします。

system install [**noconfirm**] *url*

確認メッセージを表示しないようにするには、**noconfirm** オプションを指定します。

インストールが完了すると、システムが再起動します。アプリケーション コンポーネントのインストールと ASA FirePOWER サービスの起動には 10 分以上かかります

次に例を示します。

```
asasfr-boot> system install http://asasfr-sys-5.3.1-54.pkg
```

ステップ 10　ブートが完了したら、パスワード **Sourcefire** を使用して **admin** としてログインします。

プロンプトに従ってシステム設定を完了します。

まず、エンド ユーザ ライセンス契約（EULA）を読み、これに同意する必要があります。次に、プロンプトに従って管理者パスワードを変更し、管理アドレスと DNS 設定を設定します。IPv4 と IPv6 の両方の管理アドレスを設定できます。

ステップ 11　**configure manager add** コマンドを使用して、このデバイスを管理する FireSIGHT 管理センター アプライアンスを指定します。

登録キーを決めます。このキーは、デバイスをインベントリに追加するときに FireSIGHT 管理センター で使用します。次に、簡単な例を示します。NAT 境界がある場合は、コマンドが異なります。「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.18-16）を参照してください。

```
> configure manager add 10.89.133.202 123456
Manager successfully configured.
```

ステップ 12　上で入力したホスト名またはアドレスを使用し、ブラウザで HTTPS 接続を使用して FireSIGHT 管理センター にログインします。たとえば、https://DC.example.com などです。

[Device Management]（[Devices] > [Device Management]）ページでデバイスを追加します。詳細については、『*FireSIGHT System User Guide*』の「Managing Devices」の章、または FireSIGHT 管理センター のオンライン ヘルプを参照してください。

システム ソフトウェアのアップグレード

FireSIGHT 管理センター を使用して ASA FirePOWER モジュールにアップグレード イメージを適用します。アップグレードを適用する前に、ASA が新しいバージョンに最小限必要なリリースを実行していることを確認します。場合によっては、モジュールをアップグレードする前に ASA をアップグレードする必要があります。

アップグレードの適用の詳細については、『*FireSIGHT System User Guide*』または FireSIGHT 管理センター のオンライン ヘルプを参照してください。

ASA FirePOWER モジュールのモニタリング

次の各トピックでは、モジュールのモニタリングに関するガイダンスを示します。ASA FirePOWER 関連の syslog メッセージについては、『syslog メッセージ ガイド』を参照してください。ASA FirePOWER の syslog メッセージは、メッセージ番号 434001 から始まります。

モニタリング コマンドを使用するには、[Tools] > [Command Line Interface] を使用します。

- 「モジュール ステータスの表示」（P.18-24）
- 「モジュールの統計情報の表示」（P.18-25）
- 「モジュール接続のモニタリング」（P.18-25）

モジュール ステータスの表示

[Home] ページで [ASA FirePOWER Status] タブを選択すると、モジュールに関する情報が表示されます。これは、モデル、シリアル番号、ソフトウェア バージョンなどのモジュール情報と、アプリケーションの名前とステータス、データ プレーンのステータス、全体のステータスなどのモジュール ステータスが含まれます。モジュールが FireSIGHT 管理センター に登録されている場合は、リンクをクリックしてアプリケーションを開き、さらなる分析とモジュール設定を行うことができます。

モジュールの統計情報の表示

sfr コマンドを含む各サービス ポリシーの統計情報およびステータスを表示するには、show service-policy sfr コマンドを使用します。カウンタをクリアするには、**clear service-policy** を使用します。

次に、ASA FirePOWER サービス ポリシーと現在の統計情報およびモジュールのステータスを表示する例を示します。

```
ciscoasa# show service-policy sfr

Global policy:
Service-policy: global_policy
    Class-map: my-sfr-class
      SFR: card status Up, mode fail-close
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

次に、モニタ専用ポリシーを表示する例を示します。この場合、パケット入力カウンタは増加しますが、ASA に戻されるトラフィックはないので、パケット出力カウンタはゼロのままです。

```
hostname# show service-policy sfr
Global policy:
Service-policy: global_policy
    Class-map: bypass
      SFR: card status Up, mode fail-open, monitor-only
        packet input 2626422041, packet output 0, drop 0, reset-drop 0, proxied 0
```

モジュール接続のモニタリング

ASA FirePOWER モジュールを通過する接続を表示するには、次のいずれかのコマンドを入力します。

- **show asp table classify domain sfr**

  トラフィックを ASA FirePOWER モジュールに送信するために作成された NP ルールを表示します。

- **show asp drop**

  ドロップされたパケットを表示します。ドロップのタイプについて、以下で説明します。

- **show conn**

  「X - inspected by service module」フラグを表示することにより、接続がモジュールに転送されているかどうかを示します。

show asp drop コマンドには、ASA FirePOWER モジュールに関連する次のドロップの理由を含めることができます。

フレーム ドロップ：

- sfr-bad-tlv-received：これが発生するのは、ASA が FirePOWER から受信したパケットにポリシー ID TLV がないときです。非制御パケットのアクション フィールドで Standy/Active ビットが設定されていない場合は、この TLV が存在している必要があります。
- sfr-request：FirePOWER 上のポリシーが理由で、フレームをドロップするよう FirePOWER から要求されました。このポリシーによって、FirePOWER はアクションを Deny Source、Deny Destination、または Deny Pkt に設定します。フレームがドロップされるべきでなかった場合は、フローを拒否しているモジュールのポリシーを確認します。

- sfr-fail-close：パケットがドロップされたのは、カードが動作中ではなく、設定済みのポリシーが「fail-close」であったからです（対照的に、「fail-open」の場合は、カードがダウンしていてもパケットの通過が許可されます）。カードのステータスを確認し、サービスを再開するか、再起動します。
- sfr-fail：既存のフローに対する FirePOWER コンフィギュレーションが削除されており、FirePOWER で処理できないため、ドロップされます。これが発生することは、ほとんどありません。
- sfr-malformed-packet：FirePOWER からのパケットに無効なヘッダーが含まれます。たとえば、ヘッダー長が正しくない可能性があります。
- sfr-ha-request：セキュリティ アプライアンスが FirePOWER HA 要求パケットを受信したが処理できなかった場合、このカウンタが増加してパケットがドロップされます。
- sfr-invalid-encap：セキュリティ アプライアンスが無効なメッセージ ヘッダーを持つ FirePOWER パケットを受信すると、このカウンタが増加してパケットがドロップされます。
- sfr-bad-handle-received：FirePOWER モジュールからパケットで不正フロー ハンドルを受信したため、フローをドロップしました。FirePOWER フローのハンドルがフロー期間中に変更されると、このカウンタが増加し、フローとパケットが ASA でドロップされます。
- sfr-invalid-encap：セキュリティ アプライアンスがモニタ専用モードのときに FirePOWER パケットを受信すると、このカウンタが増加してパケットがドロップされます。

フロードロップ：

- sfr-request：フローを終了させることを FirePOWER が要求しました。アクション ビット 0 が設定されます。
- reset-by-sfr：フローの終了とリセットを FirePOWER が要求しました。アクション ビット 1 が設定されます。
- sfr-fail-close：フローが終了させられたのは、カードがダウン状態であり、設定済みのポリシーが「fail-close」であったからです。

ASA FirePOWER モジュールの履歴

機能名	プラットフォーム リリース	機能情報
ASA 5585-X（すべてのモデル）で適合する ASA FirePOWER SSP ハードウェア モジュールをサポート。 ASA 5512-X ～ ASA 5555-X で ASA FirePOWER ソフトウェア モジュールをサポート。	ASA 9.2(2.4) ASA FirePOWER 5.3.1	ASA FirePOWER モジュールは、次世代 IPS（NGIPS）、Application Visibility and Control（AVC）、URL フィルタリング、高度なマルウェア対策（AMP）などの次世代ファイアウォール サービスを提供します。このモジュールは、シングルまたはマルチ コンテキスト モードとルーテッドまたはトランスペアレント モードで使用できます。 次の画面が導入されました。 [Home] > [ASA FirePOWER Status] [Wizards] > [Startup Wizard] > [ASA FirePOWER Basic Configuration] [Configuration] > [Firewall > Service Policy Rules] > [Add Service Policy Rule] > [Rule Actions] > [ASA FirePOWER Inspection]

ASA CX モジュール

この章では、ASA で実行される ASA CX モジュールを設定する方法について説明します。

- 「ASA CX モジュール」（P.19-1）
- 「ASA CX モジュールのライセンス要件」（P.19-6）
- 「ASA CX の前提条件」（P.19-6）
- 「ASA CX のガイドライン」（P.19-6）
- 「ASA CX のデフォルト設定」（P.19-8）
- 「ASA CX モジュールの設定」（P.19-8）
- 「ASA CX モジュールの管理」（P.19-20）
- 「ASA CX モジュールのモニタリング」（P.19-22）
- 「認証プロキシでの問題のトラブルシューティング」（P.19-24）
- 「ASA CX モジュールの履歴」（P.19-26）

ASA CX モジュール

ASA CX モジュールを使用すると、特定の状況の完全なコンテキストに基づいてセキュリティを強制することができます。このコンテキストには、ユーザのアイデンティティ（誰が）、ユーザがアクセスを試みているアプリケーションまたは Web サイト（何を）、アクセス試行の発生元（どこで）、アクセス試行の時間（いつ）、およびアクセスに使用されているデバイスのプロパティ（どのように）が含まれます。ASA CX モジュールを使用すると、フローの完全なコンテキストを抽出して、細分化したポリシーを適用することができます。たとえば、Facebook へのアクセスは許可するが Facebook でのゲームへのアクセスは禁止する、あるいは企業の機密データベースへのアクセスを財務担当者に許可するが他の社員には禁止するといったことが可能です。

- 「ASA CX モジュールがどのように ASA と連携するか」（P.19-2）
- 「ASA CX の管理アクセス」（P.19-4）
- 「アクティブ認証用の認証プロキシ」（P.19-5）
- 「ASA の機能との互換性」（P.19-5）

ASA CX モジュールがどのように ASA と連携するか

ASA CX モジュールは、ASA とは別のアプリケーションを実行します。このモジュールは、ハードウェア モジュール（ASA 5585-X 上）か、ソフトウェア モジュール（5512-X ～ 5555-X）です。ハードウェア モジュールには、独立した管理およびコンソール ポートと、モジュール自体ではなく ASA によって直接使用される追加のデータ インターフェイスがあります。

ご使用のデバイスをデモンストレーション用に、通常のインライン モードまたはモニタ専用モードのいずれかに設定できます。

- インライン展開では、実際のトラフィックがデバイスに送信され、デバイスのポリシーがトラフィックに対する処理に影響します。不要なトラフィックがドロップされ、ポリシーによって適用されるその他のアクションが実行された後、トラフィックはさらなる処理と最終的な送信のために ASA に返されます。
- モニタ専用展開では、トラフィックのコピーがデバイスに送信されますが、ASA に戻されることはありません。モニタ専用モードでは、デバイスによるトラフィックへの処理をネットワークに影響を与えることなく確認できます。モニタ専用のサービス ポリシーまたはトラフィック転送インターフェイスを使用してこのモードを設定できます。モニタ専用モードに関するガイドラインと制限事項については、「ASA CX のガイドライン」（P.19-6）を参照してください。

次の各項では、これらのモードについて詳しく説明します。

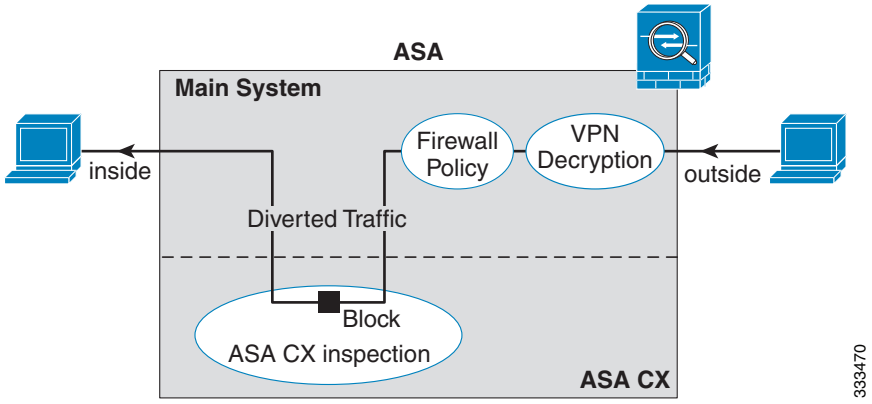
ASA CX の通常のインライン モード

通常のインライン モードでは、トラフィックは、ファイアウォール検査を通過してから ASA CX モジュールへ転送されます。ASA で ASA CX インスペクション対象として指定されたトラフィックは、次に示すように ASA および ASA CX モジュールを通過します。

1. トラフィックは ASA に入ります。
2. 着信 VPN トラフィックが復号化されます。
3. ファイアウォール ポリシーが適用されます。
4. トラフィックが ASA CX モジュールに送信されます。
5. ASA CX モジュールはセキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
6. 有効なトラフィックが ASA に返送されます。ASA CX モジュールは、セキュリティ ポリシーに従ってトラフィックをブロックすることがあり、ブロックされたトラフィックは渡されません。
7. 発信 VPN トラフィックが暗号化されます。
8. トラフィックが ASA から出ます。

次の図は、ASA CX モジュールを使用する場合のトラフィック フローを示します。この例では、特定のアプリケーションに対して許可されていないトラフィックを ASA CX モジュールが自動的にブロックします。それ以外のトラフィックは、ASA を通って転送されます。

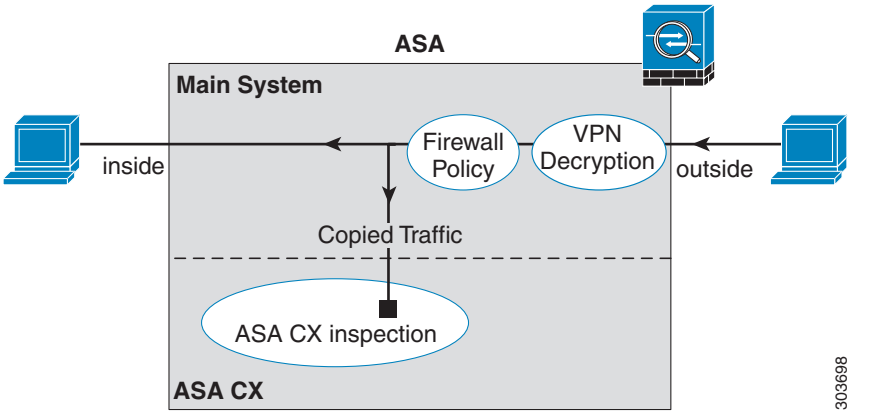
図 19-1　ASA での ASA CX モジュールのトラフィック フロー



モニタ専用モードでのサービス ポリシー

テストおよびデモンストレーション用に、ASA CX モジュールに読み取り専用トラフィックの重複ストリームを送信するように ASA を設定できるので、モジュールが ASA トラフィック フローに影響を与えることなく、どのようにトラフィックをインスペクションするかを確認できます。このモードでは、ASA CX モジュールが通常どおりトラフィックをインスペクションし、ポリシーを決定し、イベントを生成します。ただし、パケットが読み取り専用コピーであるため、モジュールのアクションは実際のトラフィックには影響しません。代わりに、モジュールはインスペクション後コピーをドロップします。次の図は、モニタ専用モードの ASA CX モジュールを示します。

図 19-2　ASA CX モニタ専用モード

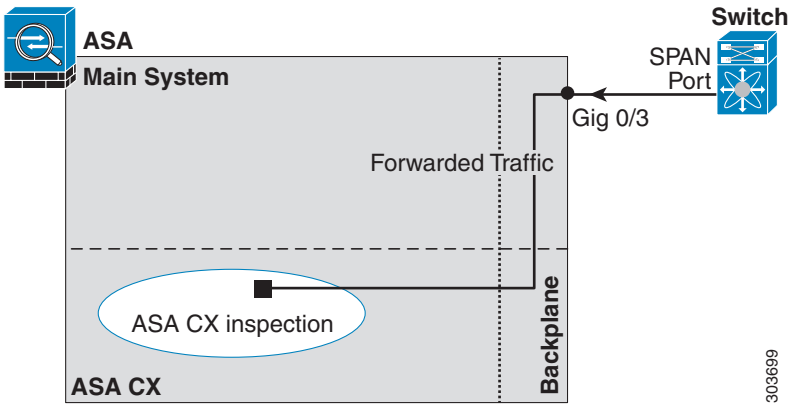


モニタ専用モードでのトラフィック転送インターフェイス

または、ASA インターフェイスを転送インターフェイスに設定し、ASA 処理を行わずに受信したすべてのトラフィックを直接 ASA CX モジュールに転送できます。テストおよびデモンストレーション用に、トラフィック転送では ASA 処理の余分な複雑性を取り除きます。トラフィック転送はモニタ専用モードでのみサポートされるので、ASA CX モジュールはインスペクション後トラフィックをドロップします。次の図は、トラフィック転送が設定されている

ASA GigabitEthernet 0/3 インターフェイスを示します。このインターフェイスは、ASA CX モジュールがすべてのネットワーク トラフィックをインスペクションできるように、スイッチの SPAN ポートに接続されます。

図 19-3　ASA CX トラフィック転送



ASA CX の管理アクセス

ASA CX モジュールの管理には、初期設定（およびそれ以降のトラブルシューティング）およびポリシー管理という 2 つの異なる段階があります。

- 「初期設定」（P.19-4）
- 「ポリシー設定および管理」（P.19-5）

初期設定

初期設定を行うには、ASA CX モジュールの CLI を使用して **setup** コマンドを実行し、その他の任意の設定値を設定する必要があります。

CLI にアクセスするには、次の方法を使用します。

- ASA 5585-X
  - ASA CX コンソール ポート：ASA CX コンソール ポートは、独立した外部コンソール ポートです。
  - ASA CX Management 1/0 インターフェイス（SSH を使用）：デフォルトの IP アドレス（192.168.8.8）に接続することも、ASDM を使用して管理 IP アドレスを変更してから SSH を使用して接続することもできます。ASA CX 管理インターフェイスは、独立した外部ギガビット イーサネット インターフェイスです。

（注）　**session** コマンドを使用して ASA バックプレーンを介して ASA CX ハードウェア モジュール CLI にアクセスすることはできません。

- ASA 5512-X ～ ASA 5555-X
  - バックプレーンを経由した ASA セッション：ASA に CLI アクセスが可能な場合は、モジュールにセッション接続し、そのモジュール CLI にアクセスできます。

– ASA CX Management 0/0 インターフェイス（SSH を使用）：デフォルトの IP アドレス（192.168.1.2）に接続することも、ASDM を使用して管理 IP アドレスを変更してから SSH を使用して接続することもできます。これらのモデルは、ASA CX モジュールをソフトウェア モジュールとして実行します。ASA CX 管理インターフェイスは、Management 0/0 インターフェイスを ASA と共有します。ASA と ASA CX モジュールのそれぞれに別の MAC アドレスと IP アドレスがサポートされます。ASA CX IP アドレスの設定は、ASA CX オペレーティング システム内で（CLI または ASDM を使用して）実行する必要があります。ただし、物理特性（インターフェイスのイネーブル化など）は、ASA 上で設定されます。ASA インターフェイス コンフィギュレーションを削除して（特にインターフェイス名）、このインターフェイスを ASA CX 専用インターフェイスとすることができます。このインターフェイスは管理専用です。

ポリシー設定および管理

初期設定を実行した後で、Cisco Prime Security Manager（PRSM）を使用して ASA CX ポリシーを設定します。PRSM は ASA CX 設定インターフェイスの名前であり、また ASA CX デバイスを設定する別の製品（Cisco Prime Security Manager）の名前でもあります。

その後、ASDM、ASA CLI、またはマルチ デバイス モードで PRISM を使用して、ASA CX モジュールにトラフィックを送信するように ASA ポリシーを設定します。

アクティブ認証用の認証プロキシ

アイデンティティ ポリシーを ASA CX に設定して、アクセス ポリシーで使用するユーザ アイデンティティ情報を収集できます。システムは、ユーザ アイデンティティをアクティブに（ユーザ名およびパスワードのクレデンシャルの入力を求めるプロンプトを表示する）またはパッシブに（AD エージェントまたは Cisco Context Directory Agent（CDA）が収集した情報を取得する）収集できます。

アクティブ認証を使用する場合は、認証プロキシとして動作するように ASA を設定する必要があります。ASA CX モジュールは認証要求を ASA インターフェイスの IP アドレス/プロキシ ポートにリダイレクトします。デフォルト ポートは 885 ですが、別のポートを設定することもできます。

アクティブ認証をイネーブルにするには、「ASA CX サービス ポリシーの作成」（P.19-17）で説明するように、トラフィックを ASA CX にリダイレクトするサービス ポリシーの一部として認証プロキシをイネーブルにします。

ASA の機能との互換性

ASA には、多数の高度なアプリケーション インスペクション機能があり、HTTP インスペクションもその一つです。ただし、ASA CX モジュールには ASA よりも高度な HTTP インスペクション機能があり、その他のアプリケーションについても機能が追加されています。たとえば、アプリケーション使用状況のモニタリングと制御です。

ASA CX モジュールの機能を最大限に活用するには、ASA CX モジュールに送信するトラフィックに関する次のガイドラインを参照してください。

- HTTP トラフィックに対して ASA インスペクションを設定しないでください。
- クラウド Web セキュリティ（ScanSafe）インスペクションを設定しないでください。同じトラフィックに対して ASA CX のアクションとクラウド Web セキュリティ インスペクションの両方が設定されている場合に、ASA が実行するのは ASA CX のアクションのみです。

- ASA 上の他のアプリケーション インスペクションは ASA CX モジュールと互換性があり、これにはデフォルト インスペクションも含まれます。
- Mobile User Security（MUS）サーバをイネーブルにしないでください。これは、ASA CX モジュールとの間に互換性がありません。
- ASA クラスタリングをイネーブルにしないでください。これは、ASA CX モジュールとの間に互換性がありません。

ASA CX モジュールのライセンス要件

ASA CX モジュールと PRSM には追加のライセンスが必要です。このライセンスは ASA のコンテキストではなく、モジュール自体にインストールする必要があります。ASA 自体には、追加ライセンスは必要ありません。詳細については、ASA CX のマニュアルを参照してください。

ASA CX の前提条件

PRSM を使用して ASA を設定するには、セキュアな通信を行うために ASA に証明書をインストールする必要があります。デフォルトでは、ASA は自己署名証明書を生成します。ただし、この証明書の発行者が不明であるため、ブラウザに証明書の検証を求めるプロンプトが表示されます。こうしたブラウザのプロンプトが表示されないようにするには、代わりに既知の認証局（CA）からの証明書をインストールします。CA からの証明書を要求する場合、証明書タイプがサーバ認証証明書とクライアント認証証明書の両方であることを確認します。詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

ASA CX のガイドライン

コンテキスト モードのガイドライン

ASA CX 9.1(3) から、マルチ コンテキスト モードがサポートされます。

ただし、（PRSM で設定されている）ASA CX モジュール自体はシングル コンテキスト モードのデバイスです。つまり、ASA から着信するコンテキスト固有のトラフィックは共通の ASA CX ポリシーと照合されます。したがって、複数のコンテキストで同じ IP アドレスを使用できず、各コンテキストに独自のネットワークを含める必要があります。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。トラフィック転送インターフェイスは、トランスペアレント モードでのみサポートされます。

フェールオーバーのガイドライン

フェールオーバーを直接にはサポートしていません。ASA がフェールオーバーしたときに、既存の ASA CX フローは新しい ASA に転送されますが、トラフィックは ASA CX によるインスペクションを受けることなく ASA の通過を許可されます。新しい ASA が受信した新しいフローだけが、ASA CX モジュールによる処理の対象となります。

ASA クラスタリングのガイドライン

クラスタリングはサポートされません。

IPv6 のガイドライン

- IPv6 をサポートします。
- （9.1(1) 以前）NAT 64 はサポートされません。9.1(2) 以降では、NAT 64 がサポートされます。

モデルのガイドライン

- ASA 5585-X および 5512-X ～ ASA 5555-X でのみサポートされています。詳細については、『*Cisco ASA Compatibility Matrix*』を参照してください。

  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

- 5512-X ～ ASA 5555-X の場合は、シスコのソリッド ステート ドライブ（SSD）を実装する必要があります。詳細については、ASA 5500-X のハードウェア ガイドを参照してください。

モニタ専用モードのガイドライン

モニタ専用モードは厳密にデモンストレーション用であり、モジュールの通常の動作モードではありません。

- ASA 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。マルチ コンテキスト モードでは、あるコンテキストについてモニタ専用モードを設定し、それ以外のコンテキストについて通常のインライン モードを設定することはできません。
- 次の機能は、モニタ専用モードではサポートされません。
  - 拒否ポリシー
  - アクティブ認証
  - 復号化ポリシー
- ASA CX は、モニタ専用モードでパケット バッファリングを実行せず、イベントはベストエフォート方式で生成されます。たとえば、長い URL がパケット境界にまたがっている一部のイベントは、バッファリングの欠如の影響を受ける可能性があります。
- ASA ポリシーと ASA CX の両方で必ずモードが一致するように設定する必要があります（両方ともモニタ専用モード、または両方とも通常のインライン モード）。

上記のほか、トラフィック転送インターフェイスには次のガイドラインがあります。

- ASA はトランスペアレント モードにする必要があります。
- 最大 4 つのインターフェイスを、トラフィック転送インターフェイスとして設定できます。その他の ASA インターフェイスは、通常どおり使用できます。
- トラフィック転送インターフェイスは、VLAN または BVI ではなく、物理インターフェイスである必要があります。また、物理インターフェイスには、それに関連付けられた VLAN を設定することはできません。
- トラフィック転送インターフェイスは、ASA トラフィックには使用できません。これらに名前を付けたり、フェールオーバーや管理専用を含む ASA 機能向けに設定できません。
- トラフィック転送インターフェイスとサービス ポリシーの両方を ASA CX トラフィック用に設定できません。

その他のガイドラインと制限事項

- 「ASA の機能との互換性」（P.19-5）を参照してください。
- ハードウェア モジュールにインストールされているソフトウェアのタイプの変更はできません。つまり、購入した ASA CX モジュールに、後で別のソフトウェアをインストールすることはできません。

ASA CX のデフォルト設定

次の表に、ASA CX モジュールのデフォルト設定を示します。

表 19-1　デフォルトのネットワーク パラメータ

パラメータ	デフォルト
管理 IP アドレス	ASA 5585-X：Management 1/0 192.168.8.8/24 ASA 5512-X ～ ASA 5555-X：Management 0/0 192.168.1.2/24
ゲートウェイ	ASA 5585-X：192.168.8.1/24 ASA 5512-X ～ ASA 5555-X：192.168.1.1/24
SSH またはセッションのユーザ名	admin
パスワード	Admin123

ASA CX モジュールの設定

ASA CX モジュールの設定プロセスでは、ASA CX セキュリティ ポリシーを ASA CX モジュール上で設定してから、トラフィックを ASA CX モジュールに送信するように ASA を設定します。ASA CX モジュールを設定するには、次の手順に従います。

ステップ 1　「ASA CX 管理インターフェイスの接続」（P.19-9）ケーブルで ASA CX 管理インターフェイスに接続します（任意でコンソール インターフェイスにも）。

ステップ 2　「（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールのインストールまたはイメージの再作成」（P.19-12）

ステップ 3　「（ASA 5585-X）ASA CX 管理 IP アドレスの変更」（P.19-14）（必要な場合）。これは最初の SSH アクセスに必要になる場合があります。

ステップ 4　「基本的な ASA CX 設定値の設定」（P.19-15）この設定は ASA CX モジュールで行います。

ステップ 5　「ASA CX モジュールでのセキュリティ ポリシーの設定」（P.19-16）

ステップ 6　（オプション）「認証プロキシ ポートの設定」（P.19-17）

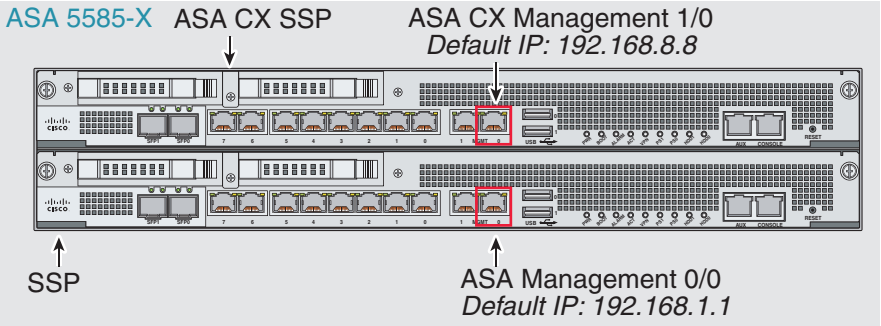
ステップ 7　「ASA CX モジュールへのトラフィックのリダイレクト」（P.19-17）

ASA CX 管理インターフェイスの接続

ASA CX モジュールへの管理アクセスを提供する以外に、ASA CX 管理インターフェイスは、HTTP プロキシ サーバまたは DNS サーバおよびインターネットへのアクセスを必要とします。これは、シグニチャ アップデートなどのためです。この項では、推奨されるネットワーク コンフィギュレーションを示します。実際のネットワークでは、異なる可能性があります。

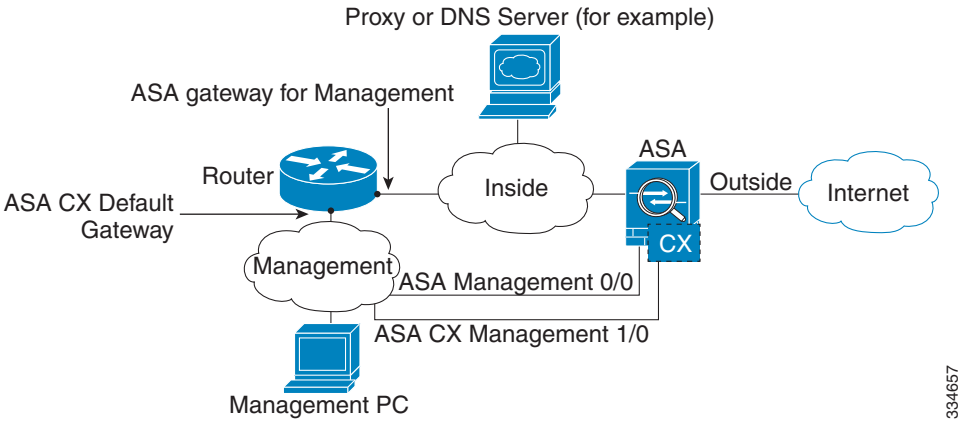
ASA 5585-X（ハードウェア モジュール）

ASA CX モジュールには、ASA とは別の管理およびコンソール インターフェイスが含まれます。初期設定を行うには、デフォルト IP アドレス（192.168.8.8/24）を使用して ASA CX Management 1/0 インターフェイスに SSH で接続できます。デフォルト IP アドレスを使用できない場合は、コンソール ポートを使用するか、ASDM を使用して SSH を使用できるように管理 IP アドレスを変更します。



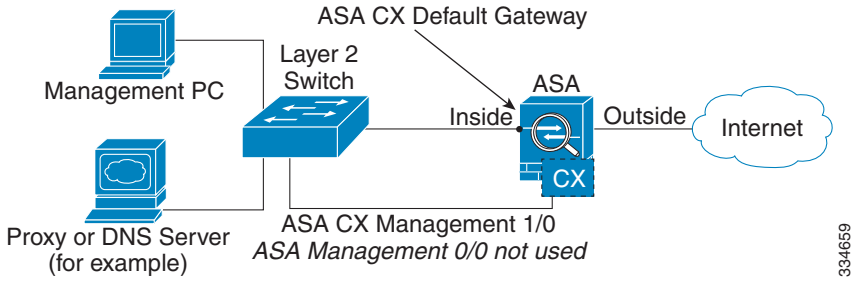
内部ルータがある場合

内部ルータがある場合は、管理ネットワーク（これには ASA Management 0/0 インターフェイスおよび ASA CX Management 1/0 インターフェイスの両方を含めることができます）と ASA 内部ネットワークとの間でルーティングできます（インターネット アクセス用）。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



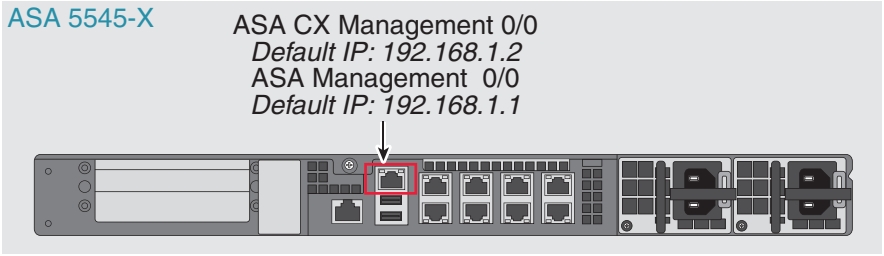
内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません（仮に持つとすれば、内部ルータがネットワーク間のルーティングを行う必要があります）。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA CX モジュールは ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に ASA CX Management 1/0 アドレスを設定できます。



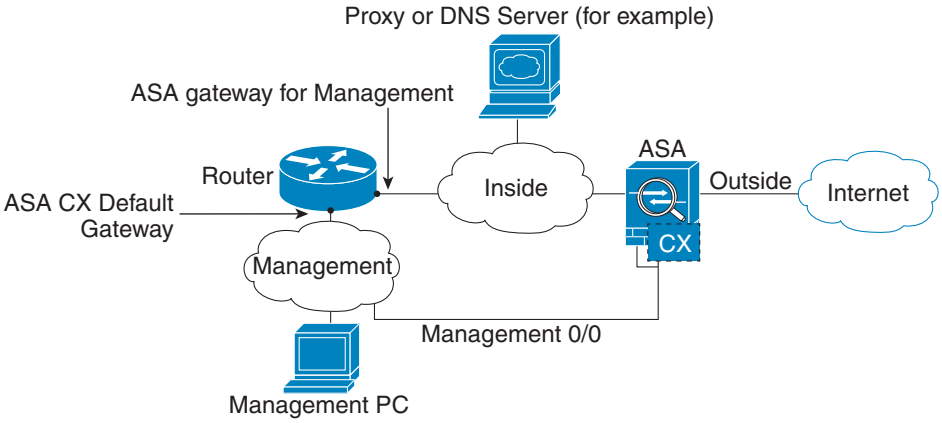
ASA 5512-X ～ ASA 5555-X（ソフトウェア モジュール）

これらのモデルは、ASA CX モジュールをソフトウェア モジュールとして実行し、ASA CX 管理インターフェイスは Management 0/0 インターフェイスを ASA と共有します。初期設定を行うには、SSH で ASA CX のデフォルト IP アドレス（192.168.1.2/24）に接続できます。デフォルト IP アドレスを使用できない場合は、バックプレーンを経由して ASA CX にセッション接続するか、ASDM を使用して SSH を使用できるように管理 IP アドレスを変更します。



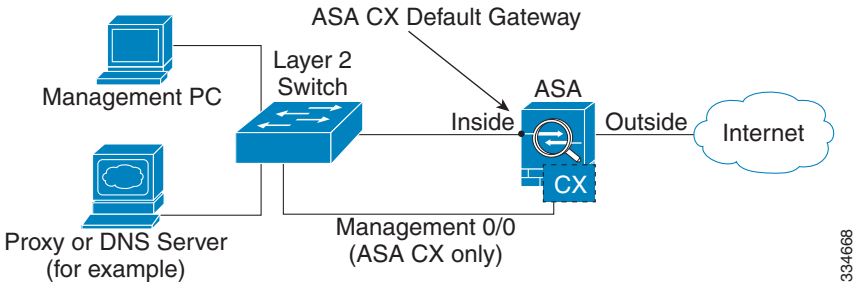
内部ルータがある場合

内部ルータがある場合、Management 0/0 ネットワーク間でルーティングできます。これには、ASA および ASA CX の両方の管理 IP アドレス、およびインターネット アクセス用の内部ネットワークが含まれます。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA 設定の名前を Management 0/0 インターフェイスから削除する場合、そのインターフェイスの ASA CX IP アドレスを引き続き設定できます。ASA CX モジュールは基本的には ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上にあるように ASA CX 管理アドレスを設定 できます。



（注） Management 0/0 に対して ASA が設定した名前を削除する必要があります。これが ASA で設定されている場合、ASA CX アドレスは、ASA と同じネットワーク上に存在する必要があり、これによって、その他の ASA インターフェイス上ですでに設定されたネットワークはすべて除外されます。名前が設定されていない場合、ASA CX は、任意のネットワーク上（たとえば、ASA 内部ネットワーク）に存在することができます。

（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールのインストールまたはイメージの再作成

ASA CX モジュールとともに ASA を購入した場合、モジュール ソフトウェアおよび必要なソリッド ステート ドライブ（SSD）は事前にインストールされており、すぐに使用できます。既存の ASA に ASA CX を追加する場合、または SSD を交換する必要がある場合は、この手順に従って ASA CX ブート ソフトウェアをインストールし、SSD を分割する必要があります。物理的に SSD を取り付けるには、『ASA Hardware Guide』を参照してください。

最初に ASA CX モジュールをアンインストールする必要がある点を除いて、モジュールのイメージの再作成はこれと同じ手順です。システムのイメージの再作成は、SSD を交換する場合に行います。

（注）　ASA 5585-X ハードウェア モジュールの場合、ASA CX モジュールからイメージをインストールまたはアップグレードする必要があります。詳細は、ASA CX モジュールのマニュアルを参照してください。

はじめる前に

- フラッシュ（disk0）の空き領域には、少なくとも、ブート ソフトウェアのサイズに 3 GB を加えた大きさが必要です。
- マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。
- 実行している可能性があるその他のソフトウェア モジュールをシャットダウンする必要があります。デバイスでは、一度に 1 つのソフトウェア モジュールを実行できます。これは ASA CLI から実行する必要があります。たとえば、次のコマンドは IPS ソフトウェア モジュールをシャットダウンしてアンインストールし、ASA をリロードします。

```
hostname# sw-module module ips shutdown
hostname# sw-module module ips uninstall
hostname# reload
```

（注）　IPS モジュールにトラフィックをリダイレクトするアクティブ サービス ポリシーがある場合、そのポリシーを削除する必要があります。たとえば、ポリシーがグローバル ポリシーの場合、**no service-policy** *ips_policy* **global** を使用します。ポリシーは、CLI または ASDM を使用して削除できます。

- モジュールのイメージを再作成する場合は、同じシャットダウン/アンインストール コマンドを使用して古いイメージを削除します。たとえば、**sw-module module cxsc uninstall** を使用します。
- Cisco.com（http://software.cisco.com/download/type.html?mdfid=284325223&flowid=34503）から、ASA CX のブート イメージおよびシステム ソフトウェア パッケージの両方を取得します。

手順

ステップ 1　ブート イメージをデバイスにダウンロードします。システム ソフトウェアは転送しないでください。これは後で SSD にダウンロードされます。次の選択肢があります。

- ASDM：まず、ブート イメージをワークステーションにダウンロードするか、FTP、TFTP、HTTP、HTTPS、SMB、または SCP サーバに配置します。次に、ASDM で [Tools] > [File Management] の順に選択し、[Between Local PC and Flash] または [Between Remote Server and Flashnd] のいずれか該当する [File Transfer] コマンドを選択します。ブート ソフトウェアを ASA 上の disk0 に転送します。
- ASA CLI：まず、ブート イメージを TFTP、FTP、HTTP、または HTTPS サーバに配置し、**copy** コマンドを使用してそのブート イメージをフラッシュにダウンロードします。次の例では TFTP を使用しています。<TFTP Server> をお使いのサーバの IP アドレスまたはホスト名に置き換えてください。

```
ciscoasa# copy tftp://<TFTP SERVER>/asacx-5500x-boot-9.3.1.1-112.img
disk0:/asacx-5500x-boot-9.3.1.1-112.img
```

ステップ 2　ASA CX 管理インターフェイスからアクセス可能な HTTP、HTTPS、または FTP サーバに、Cisco.com から ASA CX システム ソフトウェアをダウンロードします。

ステップ 3　次のコマンドを入力して、ASA disk0 で ASA CX モジュール ブート イメージの場所を設定します。

```
hostname# sw-module module cxsc recover configure image disk0:file_path
```

（注）　「ERROR: Another service (ips) is running, only one service is allowed to run at any time」のようなメッセージが表示される場合、別のソフトウェア モジュールがすでに設定されていることを意味します。このソフトウェア モジュールをシャットダウンして削除し、上述した前提条件の項の説明に従って新しいモジュールをインストールする必要があります。

例：

```
hostname# sw-module module cxsc recover configure image
disk0:asacx-5500x-boot-9.3.1.1-112.img
```

ステップ 4　次のコマンドを入力して、ASA CX ブート イメージをロードします。

```
hostname# sw-module module cxsc recover boot
```

ステップ 5　ASA CX モジュールが起動するまで約 5 分待ってから、現在実行中の ASA CX ブート イメージへのコンソール セッションを開きます。デフォルトのユーザ名は **admin** で、デフォルトのパスワードは **Admin123** です。

```
hostname# session cxsc console
Establishing console session with slot 1
Opening console session with module cxsc.
Connected to module cxsc.Escape character sequence is 'CTRL-SHIFT-6 then x'.
cxsc login: admin
Password: Admin123
```

ヒント　モジュールのブートが完了していない場合は、**session** コマンドが失敗し、ttyS1 経由で接続できないことに関するメッセージが表示されます。しばらく待ってから再試行してください。

ステップ 6　SSD を分割します。

```
asacx-boot> partition
....
Partition Successfully Completed
```

ステップ 7　「基本的な ASA CX 設定値の設定」（P.19-15）に従って、**setup** コマンドを使用して基本的なネットワーク設定を実行し（ASA CX CLI を終了しないでください）、この手順に戻ってソフトウェア イメージをインストールします。

ステップ 8　**system install** コマンドを使用してシステム ソフトウェア イメージをインストールします。

system install [**noconfirm**] *url*

確認メッセージを表示しないようにするには、**noconfirm** オプションを指定します。HTTP、HTTPS、または FTP URL を使用します。ユーザ名とパスワードが必要な場合は、それらを指定するように求められます。

インストールの完了時にシステムが再起動して、コンソール セッションが閉じられます。アプリケーション コンポーネントのインストールと ASA CX サービスの起動には 10 分以上かかります （**show module cxsc** の出力には、すべてのプロセスが Up と表示されます）。

次のコマンドは asacx-sys-9.3.1.1-112.pkg システム ソフトウェアをインストールします。

```
asacx-boot> system install https://upgrades.example.com/packages/asacx-sys-9.3.1.1-112.pkg

Username: buffy
Password: angelforever
Verifying
Downloading
Extracting
Package Detail
        Description:                 Cisco ASA CX 9.3.1.1-112 System Install
        Requires reboot:             Yes

Do you want to continue with upgrade?[n]: Y
Warning: Please do not interrupt the process or turn off the system.Doing so might leave
system in unusable state.
Upgrading
Stopping all the services ...
Starting upgrade process ...
Reboot is required to complete the upgrade.Press Enter to reboot the system.
```

（ASA 5585-X）ASA CX 管理 IP アドレスの変更

デフォルトの管理 IP アドレス（192.168.8.8）を使用できない場合は、管理 IP アドレスを ASA から設定できます。管理 IP アドレスを設定した後は、初期設定を実行するために SSH を使用して ASA CX モジュールにアクセスできます。

（注）　ソフトウェア モジュールの場合、ASA CX CLI にアクセスして、ASA CLI からのセッション接続によって設定を実行できます。その後、設定の一部として ASA CX 管理 IP アドレスを設定できます。「基本的な ASA CX 設定値の設定」（P.19-15）を参照してください。

ASA で管理 IP アドレスを変更するには、次のいずれかを実行します。マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

- CLI では、次のコマンドを使用して ASA CX の管理 IP アドレス、マスク、およびゲートウェイを設定します。

  session 1 do setup host ip *ip_address*/*mask*,*gateway_ip*

  たとえば、**session 1 do setup host ip 10.1.1.2/24,10.1.1.1** と指定します。
- （シングルコンテキスト モードのみ）ASDM では、[Wizards] > [Startup Wizard] を選択して、ウィザードの [ASA CX Basic Configuration] まで進めます。ここで IP アドレス、マスク、およびデフォルト ゲートウェイを設定できます。デフォルトが適していない場合は、他の認証プロキシ ポートを設定することもできます。

基本的な ASA CX 設定値の設定

セキュリティ ポリシーを設定する前に、基本的なネットワーク設定およびその他のパラメータを ASA CX モジュール上で設定する必要があります。ASA CX CLI は、これらの設定を行う唯一の方法です。

手順

ステップ 1　次のどちらかを実行します。

- （すべてのモデル）SSH を使用して ASA CX 管理 IP アドレスに接続します。
- （ASA 5512-X ～ ASA 5555-X）ASA CLI からモジュールへのコンソール セッションを開きます。マルチ コンテキスト モードでは、システム実行スペースからセッションを開きます。

  hostname# **session cxsc console**

ステップ 2　ユーザ名 **admin** およびパスワード **Admin123** を使用してログインします。この手順の中で、パスワードを変更します。

ステップ 3　次のコマンドを入力します。

asacx> **setup**

例：

```
asacx> setup
Welcome to Cisco Prime Security Manager Setup
[hit Ctrl-C to abort]
Default values are inside [ ]
```

セットアップ ウィザードでは入力が求められます。次の例は、ウィザードでの一般的な順序を示しています。プロンプトで N ではなく Y を入力した場合は、追加の設定を行うことができます。次に、IPv4 および IPv6 両方のスタティック アドレスの設定例を示します。IPv6 ステートレス自動設定を設定するには、スタティック IPv6 アドレスを設定するかどうかを尋ねるプロンプトで **N** と応答します。

```
Enter a hostname [asacx]: asa-cx-host
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n)[N]: N
Enter an IPv4 address [192.168.8.8]: 10.89.31.65
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 10.89.31.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: Y
Enter an IPv6 address: 2001:DB8:0:CD30::1234/64
Enter the gateway: 2001:DB8:0:CD30::1
Enter the primary DNS server IP address [ ]: 10.89.47.11
Do you want to configure Secondary DNS Server?(y/n) [N]: N
```

```
Do you want to configure Local Domain Name?(y/n) [N] Y
Enter the local domain name: example.com
Do you want to configure Search domains?(y/n) [N] Y
Enter the comma separated list for search domains: example.com
Do you want to enable the NTP service?(y/n) [N]: Y
Enter the NTP servers separated by commas: 1.ntp.example.com, 2.ntp.example.com
```

ステップ 4　最後のプロンプトが完了すると、設定のサマリーが示されます。サマリーに目を通して値が正しいことを確認し、変更した設定を適用するには **Y** を入力します。変更をキャンセルするには **N** を入力します。

例：

```
Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
Done.
Generating self-signed certificate, the web server will be restarted after that
...
Done.
Press ENTER to continue...
asacx>
```

（注）　ホスト名を変更した場合は、ログアウトして再びログインするまでプロンプトに新しい名前は表示されません。

ステップ 5　NTP を使用しない場合は、時刻を設定します。デフォルトのタイム ゾーンは UTC タイム ゾーンです。現在の設定を表示するには、**show time** コマンドを使用します。時間設定を変更するには、次のコマンドを使用できます。

```
asacx> config timezone
asacx> config time
```

ステップ 6　次のコマンドを入力して、admin のパスワードを変更します。

```
asacx> config passwd
```

例：

```
asacx> config passwd
The password must be at least 8 characters long and must contain
at least one uppercase letter (A-Z), at least one lowercase letter
(a-z) and at least one digit (0-9).
Enter password: Farscape1
Confirm password: Farscape1
SUCCESS: Password changed for user admin
```

ステップ 7　**exit** コマンドを入力してログアウトします。

ASA CX モジュールでのセキュリティ ポリシーの設定

ASA CX モジュールでセキュリティ ポリシーを設定するには PRSM を使用します。セキュリティ ポリシーは、モジュールが提供するサービスを制御します。ASA CX CLI、ASA CLI、または ASDM を使用してポリシーを設定することはできません。

PRSM は ASA CX 設定インターフェイスの名前であり、また ASA CX デバイスを設定する別の製品（Cisco Prime Security Manager）の名前でもあります。設定インターフェイスへのアクセス方法とその使用方法は同じです。PRSM を使用して ASA CX/PRSM セキュリティ ポリシーを設定する方法の詳細については、ASA CX ユーザ ガイドまたはオンライン ヘルプを参照してください。

PRSM を開くには、Web ブラウザを使用して次の URL を開きます。

https://*management_address*

management_address は ASA CX 管理インターフェイスまたは PRSM サーバの DNS 名または IP アドレスです。たとえば、https://asacx.example.com などです。

[Home] > [ASA CX Status] にこのアドレスへのショートカットがあります。[Connect to the ASA CX application] リンクをクリックして、モジュールを管理している ASA CX または PRSM サーバを開きます。

認証プロキシ ポートの設定

ASA CX ポリシーでアクティブ認証を使用する場合、ASA は、認証プロキシ ポートとしてポート 885 を使用します。885 が許可されない場合は別のポートを設定できますが、デフォルト以外のポートは 1024 より大きい必要があります。認証プロキシの詳細については、「アクティブ認証用の認証プロキシ」（P.19-5）を参照してください。

マルチコンテキスト モードでは、各セキュリティ コンテキスト内のポートを変更します。

認証プロキシ ポートを変更するには、[Configuration] > [Firewall] > [Advanced] > [ASA CX Auth Proxy] を選択します。このポートは、ASDM Startup Wizard の中で設定することもできます。

ASA CX モジュールへのトラフィックのリダイレクト

特定のトラフィックを識別するサービス ポリシーを作成して、ASA CX モジュールへのトラフィックをリダイレクトできます。デモンストレーション用でのみ、元のトラフィックが影響を受けることなく、ASA CX モジュールへのトラフィックのコピーを転送するサービス ポリシーに対するモニタ専用モードもイネーブルにできます。

デモンストレーション用のもう 1 つのオプションは、サービス ポリシーの代わりにトラフィック転送をモニタ専用モードで設定することです。トラフィック転送インターフェイスは、ASA をバイパスすることにより、すべてのトラフィックを ASA CX モジュールに直接送信します。

- 「ASA CX サービス ポリシーの作成」（P.19-17）
- 「トラフィック転送インターフェイスの設定（モニタ専用モード）」（P.19-19）

ASA CX サービス ポリシーの作成

特定のトラフィックを識別するサービス ポリシーを作成して、ASA CX モジュールへのトラフィックをリダイレクトします。

（注） ASA CX は双方向にリダイレクトを行います。したがって、1 つのインターフェイスにサービス ポリシーを設定し、そのインターフェイス上のホストとリダイレクションが設定されていないインターフェイス上のホストが接続されている場合、ASA CX ではないインターフェイスから発信されるトラフィックを含めたそれらのホスト間のすべてのトラフィックは ASA CX モジュールに送信されます。ただし、認証プロキシは入力トラフィックのみに適用されるため、ASA は、サービス ポリシーが適用されているインターフェイス上でのみ認証プロキシを実行します。

はじめる前に

- この手順を使用して ASA で認証プロキシをイネーブルにする場合は、必ず ASA CX モジュールで認証用のディレクトリ レルムも設定してください。詳細については、ASA CX ユーザ ガイドを参照してください。
- （ASA CX と交換した）IPS モジュールにトラフィックをリダイレクトするアクティブ サービス ポリシーがある場合は、ASA CX サービス ポリシーを設定する前にそのポリシーを削除する必要があります。
- ASA ポリシーと ASA CX の両方で必ずモードが一致するように設定する必要があります（両方ともモニタ専用モード、または両方とも通常のインライン モード）。
- マルチコンテキスト モードでは、各セキュリティ コンテキストでこの手順を実行します。
- PRSM をマルチ デバイス モードで使用するときは、以下で説明するようにトラフィックを ASA CX モジュールに送信するための ASA ポリシーの設定を、ASDM または ASA CLI を使用する代わりに PRSM の中で行うことができます。ただし、PRSM では、ASA サービス ポリシーを設定するときにいくつかの制限があります。詳細については、ASA CX のユーザ ガイドを参照してください。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] の順に選択します。

ステップ 2　[Add] > [Add Service Policy Rule] を選択します。[Add Service Policy Rule Wizard - Service Policy] ダイアログボックスが表示されます。

ステップ 3　必要に応じて [Service Policy] ダイアログボックスに入力します。これらの画面の詳細については、ASDM オンライン ヘルプを参照してください。

ステップ 4　[Next] をクリックします。[Add Service Policy Rule Wizard - Traffic Classification Criteria] ダイアログボックスが表示されます。

ステップ 5　必要に応じて [Traffic Classification Criteria] ダイアログボックスに入力します。これらの画面の詳細については、ASDM オンライン ヘルプを参照してください。

ステップ 6　[Next] をクリックして [Add Service Policy Rule Wizard - Rule Actions] ダイアログボックスを表示します。

ステップ 7　[ASA CX Inspection] タブをクリックします。

ステップ 8　[Enable ASA CX for this traffic flow] チェックボックスをオンにします。

ステップ 9　[ASA CX Card Fails] 領域で、次のいずれかを選択します。

- [Permit traffic]：モジュールが使用できない場合、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 ASA を設定します。
- [Close traffic]：モジュールが使用できない場合、すべてのトラフィックをブロックするように ASA を設定します。

ステップ 10　アクティブ認証に必要な認証プロキシをイネーブルにするには、[Enable Auth Proxy] チェックボックスをオンにします。このオプションは、モニタ専用モードでは使用できません。

ステップ 11　（オプション）デモンストレーション用にのみ、ASA CX モジュールへのトラフィックの読み取り専用コピーを送信するには、[Monitor-only] チェックボックスをオンにします。

（注）　すべてのクラスとポリシーは、モニタ専用モード、または通常のインライン モードのいずれか設定する必要があります。同じ ASA で両方のモードを混在させることはできません。

ステップ 12　[Finish]、[Apply] の順にクリックします。

この手順を繰り返して、追加のトラフィック フローを必要に応じて設定します。

トラフィック転送インターフェイスの設定（モニタ専用モード）

デモンストレーション用にのみ、すべてのトラフィックが ASA CX モジュールに直接転送されるトラフィック転送インターフェイスを設定できます。通常の ASA CX の動作については、「ASA CX サービス ポリシーの作成」（P.19-17）を参照してください。

詳細については、「モニタ専用モードでのトラフィック転送インターフェイス」（P.19-3）を参照してください。トラフィック転送インターフェイスに固有のガイドラインと制限事項については、「ASA CX のガイドライン」（P.19-6）も参照してください。

この機能を設定できるのは CLI だけです。[Tools] > [Command Line Interface] の順に選択し、[Multiple Line] オプション ボタンをクリックしてコマンドを入力します。コマンド ブロックが完了したら、[Send] をクリックします。

はじめる前に

- ASA ポリシーと ASA CX の両方で必ずモードが一致するように設定する必要があります（両方ともモニタ専用モード）。
- マルチコンテキスト モードでは、各セキュリティ コンテキストでこの手順を実行します。

手順

ステップ 1　トラフィック転送に使用する物理インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

interface *physical_interface*

例：

```
hostname(config)# interface gigabitethernet 0/5
```

ステップ 2　インターフェイスに設定された名前を削除します。このインターフェイスがいずれかの ASA 設定で使用されると、その設定は削除されます。指定したインターフェイス上でトラフィック転送を設定できません。

no nameif

ステップ 3　トラフィック転送をイネーブルにします。

traffic-forward cxsc monitor-only

ステップ 4　インターフェイスをイネーブルにします。

no shutdown

追加のインターフェイスについて、この手順を繰り返します。

例

次の例は、GigabitEthernet 0/5 のトラフィック転送インターフェイスを作成します。

```
interface gigabitethernet 0/5
  no nameif
  traffic-forward cxsc monitor-only
  no shutdown
```

ASA CX モジュールの管理

この項には、モジュールの管理に役立つ手順が含まれます。

- 「パスワードのリセット」（P.19-20）
- 「モジュールのリロードまたはリセット」（P.19-21）
- 「モジュールのシャットダウン」（P.19-21）
- 「（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュール イメージのアンインストール」（P.19-21）
- 「（ASA 5512-X ～ ASA 5555-X）ASA からモジュールへのセッション接続」（P.19-22）

パスワードのリセット

モジュールのパスワードをデフォルトにリセットできます。ユーザ **admin** のデフォルトのパスワードは **Admin123** です。パスワードをリセットした後は、モジュール アプリケーションを使用してパスワードを独自の値に変更する必要があります。

モジュールのパスワードをリセットすると、モジュールがリブートします。モジュールのリブート中は、サービスを使用できません。

モジュール パスワードをデフォルトにリセットするには、次のいずれかの方法を使用します。マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

- （CLI）ハードウェア モジュール（ASA 5585-X）の場合：

  ```
  hw-module module 1 password-reset
  ```

- （CLI）ソフトウェア モジュール（ASA 5512-X ～ ASA 5555-X）の場合：

  ```
  sw-module module cxsc password-reset
  ```

- （ASDM）[Tools] > [ASA CX Password Reset] の順に選択します。

（注） 新しいパスワードで ASDM に接続できない場合は、ASDM を再起動して再度ログインしてみます。新しいパスワードを定義したが、新しいパスワードと異なる既存のパスワードが ASDM にある場合は、[File] > [Clear ASDM Password Cache] を選択して、パスワード キャッシュを消去し、ASDM を再起動して再度ログインしてみます。

モジュールのリロードまたはリセット

モジュールをリロード、またはリセットしてからリロードするには、ASA CLI で次のいずれかのコマンドを入力します。マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

- ハードウェア モジュール（ASA 5585-X）：

  hw-module module 1 {**reload** | **reset**}

- ソフトウェア モジュール（ASA 5512-X ～ ASA 5555-X）：

  sw-module module cxsc {**reload** | **reset**}

モジュールのシャットダウン

モジュール ソフトウェアをシャットダウンするのは、コンフィギュレーション データを失うことなく安全にモジュールの電源をオフにできるように準備するためです。モジュールをグレースフル シャットダウンするには、ASA CLI で次のいずれかのコマンドを入力します。マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

（注） ASA をリロードする場合は、モジュールは自動的にはシャットダウンされないので、ASA のリロード前にモジュールをシャットダウンすることを推奨します。

- ハードウェア モジュール（ASA 5585-X）：

  hw-module module 1 shutdown

- ソフトウェア モジュール（ASA 5512-X ～ ASA 5555-X）：

  sw-module module cxsc shutdown

（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュール イメージのアンインストール

ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールできます。マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1　ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールします。

```
hostname# sw-module module cxsc uninstall

Module cxsc will be uninstalled.This will completely remove the disk image
associated with the sw-module including any configuration that existed within it.

Uninstall module cxsc?[confirm]
```

ステップ 2　ASA をリロードします。新しいモジュールをインストールする前に、ASA をリロードする必要があります。

```
hostname# reload
```

（ASA 5512-X ～ ASA 5555-X）ASA からモジュールへのセッション接続

ASA CX CLI を使用して、基本的なネットワーク設定を構成し、モジュールのトラブルシューティングを行います。

ASA から ASA CX ソフトウェア モジュール CLI にアクセスするには、ASA からセッション接続できます。モジュールへのセッションを開始することも（Telnet を使用）、仮想コンソール セッションを作成することもできます。コンソール セッションは、コントロール プレーンがダウンし、Telnet セッションを確立できない場合に便利です。マルチ コンテキスト モードでは、システム実行スペースからセッションを開きます。

Telnet またはコンソール セッションでは、ユーザ名とパスワードの入力を求められます。**admin** ユーザ名とパスワード（デフォルトは **Admin123**）を入力します。

- Telnet セッション：

  session cxsc

  ASA CX CLI で、終了して ASA CLI に戻るには、**exit** コマンドを使用するか Ctrl+Shift+6、x を押します。

- コンソール セッション：

  session cxsc console

  コンソール セッションを終了する唯一の方法は、Ctrl+Shift+6、x を押すことです。モジュールからログアウトすると、モジュールのログイン プロンプトに戻ります。

（注）　**session cxsc console** コマンドは、Ctrl+Shift+6、x がターミナル サーバのプロンプトに戻るエスケープ シーケンスであるターミナル サーバとともに使用しないでください。Ctrl+Shift+6、x は、ASA CX コンソールをエスケープし ASA プロンプトに戻るシーケンスでもあります。したがって、この状況で ASA CX を終了しようとすると、代わりにターミナル サーバ プロンプトに戻ります。ASA にターミナル サーバを再接続すると、ASA CX コンソール セッションがまだアクティブなままであり、ASA プロンプトに戻ることができません。ASA プロンプトにコンソールを戻すには、直接シリアル接続を使用する必要があります。この状況が発生した場合は、コンソール コマンドの代わりに **session cxsc** コマンドを使用します。

ASA CX モジュールのモニタリング

次の各トピックでは、モジュールのモニタリングに関するガイダンスを示します。ASA CX 関連の syslog メッセージについては、syslog メッセージ ガイドを参照してください。ASA CX の syslog メッセージは、メッセージ番号 429001 から始まります。

モニタリング コマンドを使用するには、[Tools] > [Command Line Interface] を使用します。

- 「モジュール ステータスの表示」（P.19-23）
- 「モジュールの統計情報の表示」（P.19-23）
- 「モジュール接続のモニタリング」（P.19-23）

モジュール ステータスの表示

ホーム ページから、[ASA CX Status] タブを選択してモジュールに関する情報を表示します。これは、モデル、シリアル番号、ソフトウェア バージョンなどのモジュール情報と、アプリケーションの名前とステータス、データ プレーンのステータス、全体のステータスなどのモジュール ステータスが含まれます。リンクをクリックしてアプリケーションを開き、分析とモジュール設定をさらに行うことができます。

モジュールの統計情報の表示

cxsc コマンドを含む各サービス ポリシーの統計情報およびステータスを表示するには、**show service-policy cxsc** コマンドを使用します。カウンタをクリアするには、**clear service-policy** を使用します。

次に示す **show service-policy** コマンドの出力例では、認証プロキシがディセーブルになっているときの、ASA CX ポリシーと現在の統計情報およびモジュールのステータスが表示されています。

```
hostname# show service-policy cxsc
Global policy:
Service-policy: global_policy
    Class-map: bypass
      CXSC: card status Up, mode fail-open, auth-proxy disabled
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

次に示す **show service-policy** コマンドの出力例では、認証プロキシがイネーブルになっているときの、ASA CX ポリシーと現在の統計情報およびモジュールのステータスが表示されています。この場合は、proxied カウンタもインクリメントされます。

```
hostname# show service-policy cxsc
Global policy:
Service-policy: pmap
    Class-map: class-default
      Default Queueing      Set connection policy: random-sequence-number disable
        drop 0
      CXSC: card status Up, mode fail-open, auth-proxy enabled
        packet input 7724, packet output 7701, drop 0, reset-drop 0, proxied 10
```

モジュール接続のモニタリング

ASA CX モジュールを通過する接続を表示するには、次のいずれかのコマンドを入力します。

- **show asp table classify domain cxsc**

  トラフィックを ASA CX モジュールに送信するために作成された NP ルールを表示します。

- **show asp table classify domain cxsc-auth-proxy**

  ASA CX モジュールの認証プロキシ用に作成された NP ルールを表示します。次に、コマンドの出力例を示します。ここでは、宛先「port=2000」は **cxsc auth-proxy port 2000** コマンドによって設定された認証プロキシ ポートであり、宛先「ip/id=192.168.0.100」は ASA インターフェイスの IP アドレスである 1 つのルールを示します。

  ```
  hostname# show asp table classify domain cxsc-auth-proxy
  Input Table
  in  id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
      hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
  ```

```
src ip/id=0.0.0.0, mask=0.0.0.0, port=0
dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
input_ifc=inside, output_ifc=identity
```

- **show asp drop**

  ドロップされたパケットを表示します。ドロップのタイプについて、以下で説明します。

- **show asp event dp-cp cxsc-msg**

  この出力には、dp-cp キューにある ASA CX モジュール メッセージの数が表示されます。ASA CX モジュールからの VPN クエリーのみが dp-cp に送信されます。

- **show conn**

  「X - inspected by service module」フラグを表示することにより、接続がモジュールに転送されているかどうかを示します。

show asp drop コマンドは、ASA CX モジュールに関連する次のドロップ理由を含めることができます。

フレーム ドロップ：

- cxsc-bad-tlv-received：これが発生するのは、ASA が CXSC から受信したパケットにポリシー ID TLV がないときです。非制御パケットのアクション フィールドで Standby Active ビットが設定されていない場合は、この TLV が存在している必要があります。
- cxsc-request：CXSC 上のポリシーが理由で、フレームをドロップするよう CXSC から要求されました。このポリシーによって、CXSC はアクションを Deny Source、Deny Destination、または Deny Pkt に設定します。
- cxsc-fail-close：パケットがドロップされたのは、カードが動作中ではなく、設定済みのポリシーが「fail-close」であったからです（対照的に、「fail-open」の場合は、カードがダウンしていてもパケットの通過が許可されます）。
- cxsc-fail：既存のフローに対する CXSC コンフィギュレーションが削除されており、CXSC で処理できないため、ドロップされます。これが発生することは、ほとんどありません。
- cxsc-malformed-packet：CXSC からのパケットに無効なヘッダーが含まれます。たとえば、ヘッダー長が正しくない可能性があります。

フロー ドロップ：

- cxsc-request：フローを終了させることを CXSC が要求しました。アクション ビット 0 が設定されます。
- reset-by-cxsc：フローの終了とリセットを CXSC が要求しました。アクション ビット 1 が設定されます。
- cxsc-fail-close：フローが終了させられたのは、カードがダウン状態であり、設定済みのポリシーが「fail-close」であったからです。

認証プロキシでの問題のトラブルシューティング

認証プロキシ機能を使用するときに問題が発生した場合は、次の手順に従って設定および接続のトラブルシューティングを行います。

（注）　2 つの ASA インターフェイス上でホスト間が接続されており、ASA CX のサービス ポリシーがインターフェイスの一方のみについて設定されている場合は、これらのホスト間のすべてのトラフィックが ASA CX モジュールに送信されます。これには、ASA CX インターフェイス以外からのトラフィックも含まれます（この機能は双方向です）。ただし、ASA が認証プロキシを実行するのは、サービス ポリシーが適用されているインターフェイス上のみです。これは、入力のみの機能であるからです。

手順

ステップ 1　コンフィギュレーションを確認します。

- ASA で、**show asp table classify domain cxsc-auth-proxy** コマンドの出力を調べて、ルールがインストールされていて正しいことを確認します。
- PRSM で、ディレクトリのレルムが作成されていて正しいクレデンシャルが指定されていることを確認するとともに、接続をテストして、認証サーバに到達可能であることを確認します。また、認証用のポリシー オブジェクトが設定されていることを確認します。

ステップ 2　**show service-policy cxsc** コマンドの出力を見て、プロキシされたパケットがあるかどうかを調べます。

ステップ 3　バックプレーンに対してパケット キャプチャを実行し（**capture** *name* **interface asa_dataplane**）、トラフィックが正しく設定されたポートにリダイレクトされているかどうかを確認します。**show running-config cxsc** コマンドまたは **show asp table classify domain cxsc-auth-proxy** コマンドを使用して設定されたポートを確認できます。

例

ポート 2000 が一貫して使用されていることの確認

1. 認証プロキシのポートを確認します。

```
hostname# show running-config cxsc
cxsc auth-proxy port 2000
```

2. 認証プロキシ ルールを確認します。

```
hostname# show asp table classify domain cxsc-auth-proxy

Input Table
in  id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=inside, output_ifc=identity
```

3. パケット キャプチャでは、リダイレクト要求が宛先ポート 2000 に送られる必要があります。

ASA CX モジュールの履歴

機能名	プラットフォーム リリース	説明
ASA CX SSP-10 および -20 に対する ASA 5585-X（SSP-10 および -20 搭載）のサポート	ASA 8.4(4.1) ASA CX 9.0(1)	ASA CX モジュールを使用すると、特定の状況の完全なコンテキストに基づいてセキュリティを強制することができます。このコンテキストには、ユーザのアイデンティティ（誰が）、ユーザがアクセスを試みているアプリケーションまたは Web サイト（何を）、アクセス試行の発生元（どこで）、アクセス試行の時間（いつ）、およびアクセスに使用されているデバイスのプロパティ（どのように）が含まれます。ASA CX モジュールを使用すると、フローの完全なコンテキストを抽出して、細分化したポリシーを適用することができます。たとえば、Facebook へのアクセスを許可するが Facebook でのゲームへのアクセスは禁止する、あるいは企業の機密データベースへのアクセスを財務担当者に許可するが他の社員には禁止するといったことが可能です。 次の画面が導入されました。 [Home] > [ASA CX Status] [Wizards] > [Startup Wizard] > [ASA CX Basic Configuration] [Configuration] > [Firewall > Service Policy Rules] > [Add Service Policy Rule] > [Rule Actions] > [ASA CX Inspection]
ASA CX SSP に対する ASA 5512-X ～ ASA 5555-X のサポート	ASA 9.1(1) ASA CX 9.1(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X に対する ASA CX SSP ソフトウェア モジュールのサポートが導入されました。 変更された画面はありません。
デモンストレーション用モニタ専用モード	ASA 9.1(2) ASA CX 9.1(2)	デモンストレーション目的でのみ、サービス ポリシー用のモニタリング専用モードをイネーブルにすることができ、元のトラフィックに影響を与えずに、トラフィックのコピーを ASA CX モジュールに転送することができます。 デモンストレーション用のもう 1 つのオプションは、サービス ポリシーの代わりにトラフィック転送をモニタ専用モードで設定することです。トラフィック転送インターフェイスは、ASA をバイパスすることにより、すべてのトラフィックを ASA CX モジュールに直接送信します。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rules] > [Add Service Policy Rule] > [Rule Actions] > [ASA CX Inspection]。 トラフィック転送機能は CLI のみでサポートされます。
ASA CX モジュールに対する NAT 64 のサポート	ASA 9.1(2) ASA CX 9.1(2)	ASA CX モジュールとともに NAT 64 を使用できるようになりました。 変更された画面はありません。
ASA CX SSP-40 および -60 に対する ASA 5585-X（SSP-40 および -60 搭載）のサポート	ASA 9.1(3) ASA CX 9.2(1)	ASA CX SSP-40 および -60 モジュールは、SSP-40 および -60 搭載の ASA 5585-X と一致するレベルで使用できます。 変更された画面はありません。

機能名	プラットフォーム リリース	説明
ASA CX モジュールに対するマルチ コンテキスト モードのサポート	ASA 9.1(3) ASA CX 9.2(1)	ASA でコンテキストごとに ASA CX サービス ポリシーを設定できるようになりました。 **（注）** コンテキストごとに ASA サービス ポリシーを設定できますが、（PRSM で設定されている）ASA CX モジュール自体はシングル コンテキスト モードのデバイスです。つまり、ASA から着信するコンテキスト固有のトラフィックは共通の ASA CX ポリシーと照合されます。 変更された画面はありません。
ASA CX バックプレーンでキャプチャされたパケットのフィルタリング	ASA 9.1(3) ASA CX 9.2(1)	**match** または **access-list** キーワードを **capture interface asa_dataplane** コマンドと共に使用して、ASA CX バックプレーンでキャプチャされたパケットをフィルタリングできるようになりました。 ASA CX モジュールに固有の制御トラフィックは、access-list または match フィルタリングの影響を受けません。ASA はすべての制御トラフィックをキャプチャします。 マルチ コンテキスト モードでは、コンテキストごとにパケット キャプチャを設定します。マルチ コンテキスト モードのすべての制御トラフィックが送信されるのはシステム実行スペースだけであることに注意してください。access-list または match を使用して制御トラフィックのフィルタリングを行うことができないため、これらのオプションはシステム実行スペースでは使用できません。 変更された ASDM 画面はありません。

ASA IPS モジュール

この章では、ASA IPS モジュールを設定する方法について説明します。ASA IPS モジュールは、ご使用の ASA モデルに応じて、ハードウェア モジュールである場合とソフトウェア モジュールである場合があります。ASA モデルごとにサポートされている ASA IPS モジュールのリストについては、次の URL にある『*Cisco ASA Compatibility Matrix*』を参照してください。

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

- 「ASA IPS モジュールに関する情報」（P.20-1）
- 「ASA IPS モジュールのライセンス要件」（P.20-5）
- 「ガイドラインと制限事項」（P.20-5）
- 「デフォルト設定」（P.20-6）
- 「ASA IPS モジュールの設定」（P.20-6）
- 「ASA IPS モジュールの管理」（P.20-19）
- 「ASA IPS モジュールのモニタリング」（P.20-23）
- 「ASA IPS モジュールの機能履歴」（P.20-23）

ASA IPS モジュールに関する情報

ASA IPS モジュールは、高度な IPS ソフトウェアを実行します。このソフトウェアによる、予防的なフル機能の侵入防御サービスは、ワームやネットワーク ウイルスなどの悪意のあるトラフィックがネットワークに影響を与える前に、これらを阻止します。

- 「ASA IPS モジュールがどのように ASA と連携するか」（P.20-1）
- 「動作モード」（P.20-2）
- 「仮想センサーの使用」（P.20-3）
- 「管理アクセスに関する情報」（P.20-4）

ASA IPS モジュールがどのように ASA と連携するか

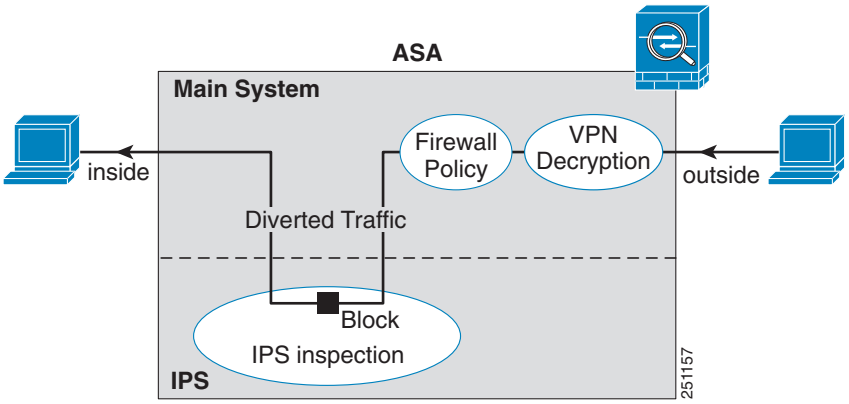
ASA IPS モジュールは、ASA とは別のアプリケーションを実行します。ASA IPS モジュールに外部管理インターフェイスが搭載されている場合は、ASA IPS モジュールに直接接続することができます。管理インターフェイスが搭載されていない場合は、ASA インターフェイスを介して ASA IPS モジュールに接続できます。ASA 5585-X 上の ASA IPS SSP にはデータ インターフェイスが含まれます。このインターフェイスによって、ASA のポート密度が増加します。ただし、ASA の全体的なスループットは増加しません。

トラフィックは、ファイアウォール検査を通過してから ASA IPS モジュールへ転送されます。ASA で IPS インスペクション対象として指定されたトラフィックは、次に示すように ASA および ASA IPS モジュールを通過します。**注**：この例は「インライン モード」の場合です。ASA がトラフィックのコピーを ASA IPS モジュールに送信するだけである「無差別モード」については、「動作モード」（P.20-2）を参照してください。

1. トラフィックは ASA に入ります。
2. 着信 VPN トラフィックが復号化されます。
3. ファイアウォール ポリシーが適用されます。
4. トラフィックが ASA IPS モジュールに送信されます。
5. ASA IPS モジュールはセキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
6. 有効なトラフィックが ASA に返送されます。ASA IPS モジュールは、セキュリティ ポリシーに従ってトラフィックをブロックすることがあり、ブロックされたトラフィックは渡されません。
7. 発信 VPN トラフィックが暗号化されます。
8. トラフィックが ASA から出ます。

図 20-1 は、ASA IPS モジュールをインライン モードで実行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、ASA IPS モジュールが攻撃と見なしたトラフィックは自動的にブロックされます。それ以外のトラフィックは、ASA を通って転送されます。

図 20-1　ASA での ASA IPS モジュールのトラフィック フロー：インライン モード



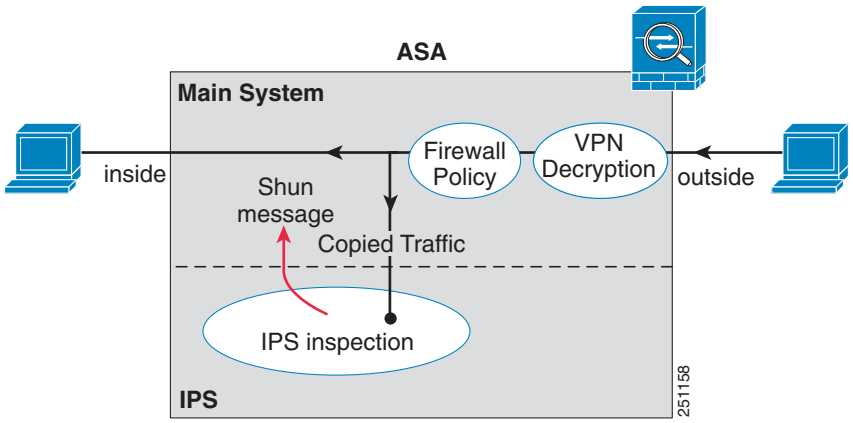
動作モード

次のいずれかのモードを使用して、トラフィックを ASA IPS モジュールに送信できます。

- インライン モード：このモードでは、ASA IPS モジュールはトラフィック フローの中に直接配置されます（図 20-1 を参照）。IPS インスペクション対象として指定されたトラフィックは、ASA IPS モジュールに渡されて検査を受けてからでなければ、ASA を通過することはできません。インスペクション対象と識別されたすべてのパケットは通過する前に分析されるため、このモードは最もセキュアです。また、ASA IPS モジュールはパケット単位でブロッキング 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ことがあります。

- 無差別モード：このモードでは、トラフィックの複製ストリームが ASA IPS モジュールに送信されます。このモードは安全性では劣りますが、トラフィックのスループットに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、無差別モードでは、ASA IPS モジュールがトラフィックをブロックできるのは、ASA にトラフィックの排除を指示するか、ASA 上の接続をリセットした場合だけです。また、ASA IPS モジュールがトラフィックを分析している間は、ASA IPS モジュールがそのトラフィックを排除できるようになる前に、少量のトラフィックが ASA を通過することがあります。図 20-2 は、無差別モードでの ASA IPS モジュールを示します。この例では、ASA IPS モジュールは脅威と見なしたトラフィックについての排除メッセージを ASA に送信します。

図 20-2　ASA での ASA IPS モジュールのトラフィック フロー：無差別モード



仮想センサーの使用

IPS ソフトウェアのバージョン 6.0 以降を実行している ASA IPS モジュールでは、複数の仮想センサーを実行できます。つまり、ASA IPS モジュールで複数のセキュリティ ポリシーを設定することができます。各 ASA セキュリティ コンテキストまたはシングル モードの ASA を 1 つまたは複数の仮想センサーに割り当てる、または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ることができます。仮想センターの詳細（サポートされている最大センサー数など）については、IPS のマニュアルを参照してください。

図 20-3 では、1 つのセキュリティ コンテキストと 1 つの仮想センター（インライン モード）がペアになり、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ます。

図 20-3　セキュリティ コンテキストと仮想センサー

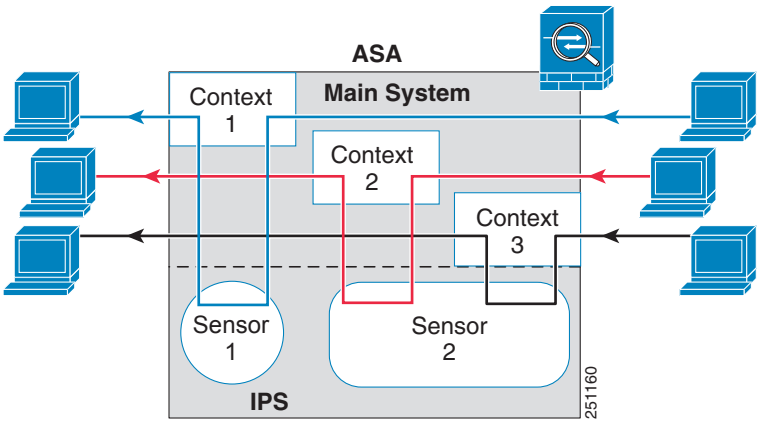
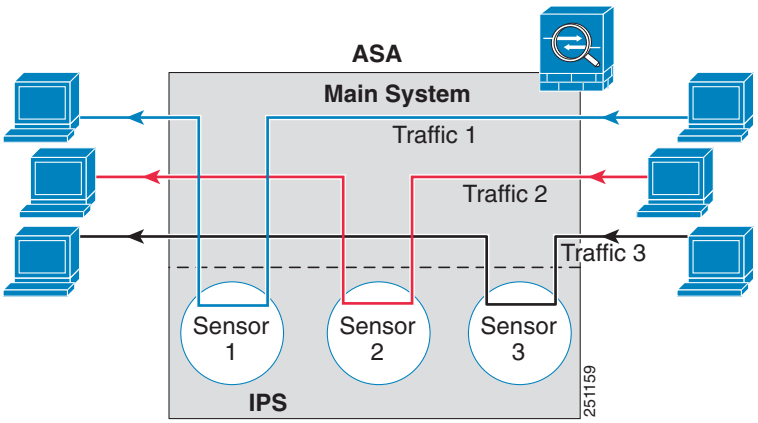


図 20-4 では、シングル モードの ASA が複数の仮想センサー（インライン モード）とペアになっています。定義されている各トラフィック フローは異なるセンサーに進みます。

図 20-4　複数の仮想センサーがあるシングル モードの ASA



管理アクセスに関する情報

次の方法を使用して、IPS アプリケーションを管理できます。

- ASA からモジュールへのセッション接続：ASA に CLI アクセスが可能な場合は、モジュールにセッション接続し、そのモジュール CLI にアクセスできます。「ASA からモジュールへのセッションの開始（必要な場合がある）」（P.20-10）を参照してください。
- ASDM または SSH を使用して IPS 管理インターフェイスに接続する：ASDM を ASA から起動すると、IPS アプリケーションを設定するために管理ステーションがモジュール管理インターフェイスに接続します。SSH の場合、モジュール管理インターフェイスでモジュール CLI に直接アクセスできます （Telnet アクセスでは、モジュール アプリケーションで追加の設定が必要になります）。モジュール管理インターフェイスは、syslog メッセージの送信や、シグニチャ データベースの更新などのモジュール アプリケーションの更新に使用できます。

管理インターフェイスについては、次の情報を参照してください。

- ASA 5585-X：IPS 管理インターフェイスは、独立した外部ギガビット イーサネット インターフェイスです。
- ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X：これらのモデルは、ASA IPS モジュールをソフトウェア モジュールとして実行します。IPS 管理インターフェイスは、Management 0/0 インターフェイスを ASA と共有します。ASA と ASA IPS モジュールのそれぞれに別の MAC アドレスと IP アドレスがサポートされます。IPS IP アドレスの設定は、IPS オペレーティング システム内で（CLI または ASDM を使用して）実行する必要があります。ただし、物理特性（インターフェイスのイネーブル化など）は、ASA 上で設定されます。ASA インターフェイス コンフィギュレーションを削除して（特にインターフェイス名）、このインターフェイスを IPS 専用インターフェイスとすることができます。このインターフェイスは管理専用です。

ASA IPS モジュールのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
ASA 5512-X、 ASA 5515-X、 ASA 5525-X、 ASA 5545-X、 ASA 5555-X	IPS モジュールのライセンス **（注）** IPS モジュール ライセンスがあると、ASA で IPS ソフトウェア モジュールを実行することができます。別の IPS シグニチャ サブスクリプションを購入する必要があります。フェールオーバー用に、各ユニットのサブスクリプションを購入します。IPS シグニチャのサポートを受けるには、IPS が事前インストールされた ASA を購入する必要があります（製品番号に「IPS」が含まれている必要があります）。結合されたフェールオーバー クラスタ ライセンスでは、非 IPS ユニットと IPS ユニットをペアにすることはできません。たとえば ASA 5515-X の IPS 版（製品番号 ASA5515-IPS-K9）を購入し、非 IPS 版（製品番号 ASA5515-K9）を使用してフェールオーバー ペアを作成しようとしている場合は、他のユニットから IPS モジュール ライセンスを継承した場合であっても、ASA5515-K9 ユニットの IPS シグニチャ アップデートを取得できません。
ASA 5585-X	基本ライセンス
他のすべてのモデル	サポートしない

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

モデルのガイドライン

- どのモデルがどのモジュールをサポートするかの詳細については、次の URL にある『*Cisco ASA Compatibility Matrix*』を参照してください。

  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

その他のガイドライン

- ASA と IPS モジュールの総スループットは、ASA 単独のスループットよりも低くなります。
  - ASA 5512-X ～ ASA 5555-X：http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/qa_c67-700608.html を参照
  - ASA 5585-X：http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/qa_c67-617018.html を参照
- モジュールにインストールされているソフトウェアのタイプの変更はできません。つまり、購入した ASA IPS モジュールに、後で別のソフトウェアをインストールすることはできません。

デフォルト設定

表 20-1 に、ASA IPS モジュールのデフォルト設定値を示します。

表 20-1　デフォルトのネットワーク パラメータ

パラメータ	デフォルト
管理 IP アドレス	192.168.1.2/24
ゲートウェイ	192.168.1.1/24（デフォルトの ASA 管理 IP アドレス）
ユーザ名	cisco
パスワード	cisco

（注）　ASA のデフォルトの管理 IP アドレスは 192.168.1.1/24 です。

ASA IPS モジュールの設定

この項では、ASA IPS モジュールを設定する方法について説明します。

- 「ASA IPS モジュールのタスク フロー」（P.20-7）
- 「ASA IPS 管理インターフェイスの接続」（P.20-7）
- 「ASA からモジュールへのセッションの開始（必要な場合がある）」（P.20-10）
- 「IPS モジュールの基本的なネットワーク設定値の設定」（P.20-13）
- 「（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールの起動」（P.20-11）
- 「ASA IPS モジュールでのセキュリティ ポリシーの設定」（P.20-14）
- 「セキュリティ コンテキストへの仮想センサーの割り当て」（P.20-16）
- 「ASA IPS モジュールへのトラフィックの誘導」（P.20-17）

ASA IPS モジュールのタスク フロー

ASA IPS モジュールの設定プロセスでは、IPS セキュリティ ポリシーを ASA IPS モジュール上で設定してから、トラフィックを ASA IPS モジュールに送信するように ASA を設定します。ASA IPS モジュールを設定するには、次の手順に従います。

ステップ 1　ASA IPS 管理インターフェイスにケーブル接続します。「ASA IPS 管理インターフェイスの接続」（P.20-7）を参照してください。

ステップ 2　モジュールへのセッションを開始します。バックプレーンを介して IPS CLI にアクセスします。ASDM ユーザの場合は、IPS ソフトウェアを実行していない場合、モジュールへのセッションを開始して IPS ソフトウェアを起動する必要がある場合があります。「ASA からモジュールへのセッションの開始（必要な場合がある）」（P.20-10）を参照してください。

ステップ 3　（ASA 5512-X ～ ASA 5555-X、必須の可能性があります）ソフトウェア モジュールをインストールします。「（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールの起動」（P.20-11）を参照してください。

ステップ 4　IPS モジュールの基本的なネットワーク設定を設定します。「IPS モジュールの基本的なネットワーク設定値の設定」（P.20-13）を参照してください。

ステップ 5　モジュール上で、インスペクションと保護のポリシーを設定します。このポリシーによって、トラフィックの検査方法と侵入検出時の処理が決まります。「ASA IPS モジュールでのセキュリティ ポリシーの設定」（P.20-14）を参照してください。

ステップ 6　（オプション）マルチ コンテキスト モードの ASA で、各コンテキストで使用可能な IPS 仮想センサーを指定します（仮想センサーが設定されている場合）。「セキュリティ コンテキストへの仮想センサーの割り当て」（P.20-16）を参照してください。

ステップ 7　ASA で、ASA IPS モジュールに誘導するトラフィックを指定します。「ASA IPS モジュールへのトラフィックの誘導」（P.20-17）を参照してください。

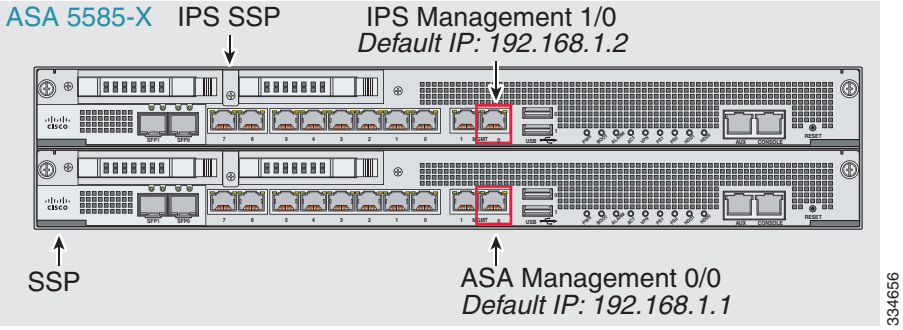
ASA IPS 管理インターフェイスの接続

IPS モジュールへの管理アクセスを提供する以外に、IPS 管理インターフェイスは、HTTP プロキシ サーバまたは DNS サーバおよびインターネットへのアクセスを必要とします。グローバル相関、シグニチャ アップデートおよびライセンス要求をダウンロードできるようにするためです。この項では、推奨されるネットワーク コンフィギュレーションを示します。実際のネットワークでは、異なる可能性があります。

- 「ASA 5585-X（ハードウェア モジュール）」（P.20-8）
- 「ASA 5512-X ～ ASA 5555-X（ソフトウェア モジュール）」（P.20-9）

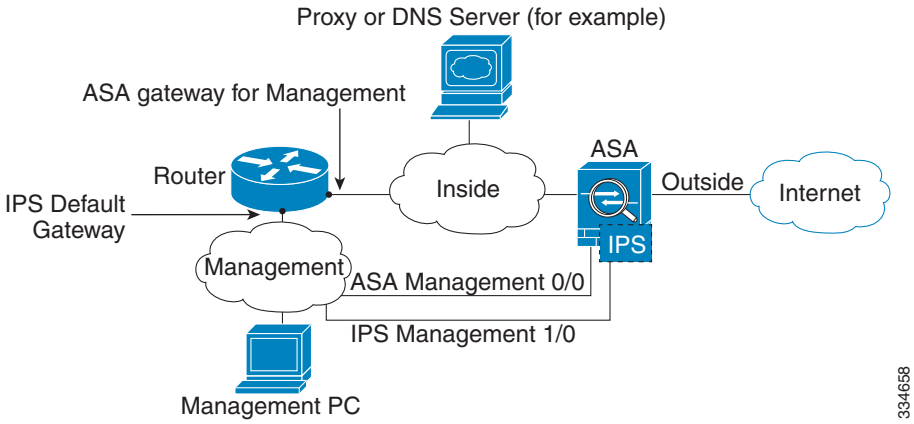
ASA 5585-X（ハードウェア モジュール）

IPS モジュールには、ASA とは別の管理インターフェイスが含まれます。



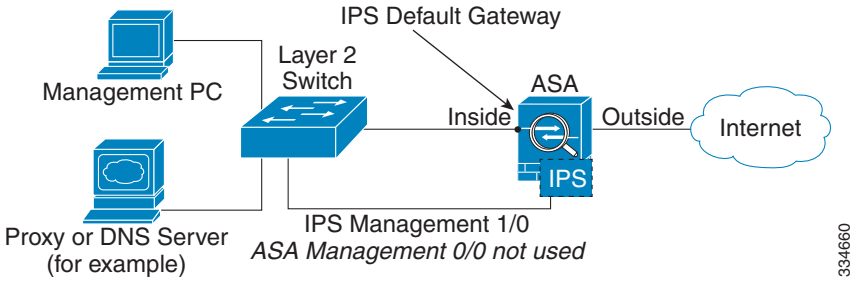
内部ルータがある場合

内部ルータがある場合は、管理ネットワーク（これには ASA Management 0/0 インターフェイスおよび IPS Management 1/0 インターフェイスの両方を含めることができます）と ASA 内部ネットワークとの間でルーティングできます。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



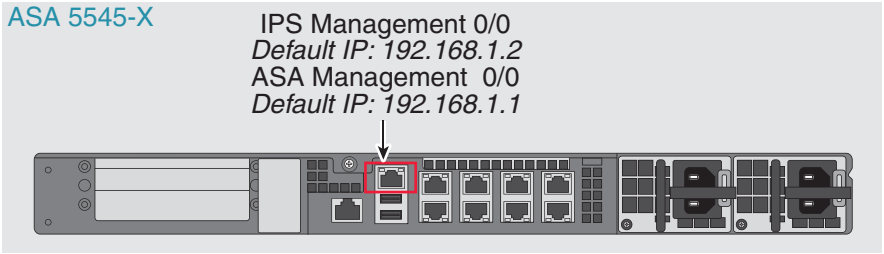
内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません（仮に持つとすれば、内部ルータがネットワーク間のルーティングを行う必要があります）。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。IPS モジュールは ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に IPS Management 1/0 アドレスを設定できます。



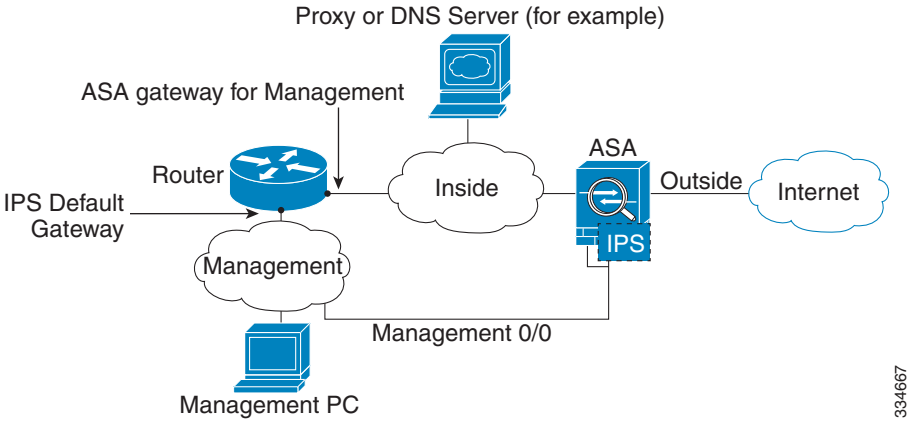
ASA 5512-X ～ ASA 5555-X（ソフトウェア モジュール）

これらのモデルは、IPS モジュールをソフトウェア モジュールとして実行し、IPS 管理インターフェイスは Management 0/0 インターフェイスを ASA と共有します。



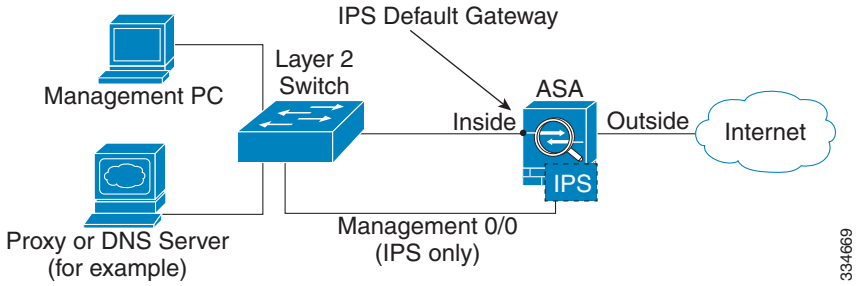
内部ルータがある場合

内部ルータがある場合は、Management 0/0 ネットワーク（これには ASA および IPS の両方の管理 IP アドレスが含まれます）と内部ネットワークとの間でルーティングできます。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA で設定された名前を Management 0/0 インターフェイスから削除した場合も、そのインターフェイスの IPS IP アドレスを設定できます。IPS モジュールは実質的に ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に IPS 管理アドレスを設定できます。



（注）　Management 0/0 に対して ASA で設定された名前を削除する必要があります。この名前が ASA 上で設定されている場合は、IPS のアドレスは ASA と同じネットワーク上にあることが必要になり、その結果、他の ASA インターフェイス上ですでに設定されたネットワークが除外されます。名前が設定されていない場合は、IPS のアドレスが存在するのはどのネットワークでも、たとえば、ASA 内部ネットワークでもかまいません。

次の作業

- 基本的なネットワーク設定を行います。「IPS モジュールの基本的なネットワーク設定値の設定」（P.20-13）を参照してください。

ASA からモジュールへのセッションの開始（必要な場合がある）

IPS モジュール CLI に ASA からアクセスするには、ASA からセッションを開始します。ソフトウェア モジュールの場合は、モジュールへのセッションを開始することも（Telnet を使用）、仮想コンソール セッションを作成することもできます。コンソール セッションは、コントロール プレーンがダウンし、Telnet セッションを確立できない場合に便利です。

マルチ コンテキスト モードを使用している場合は、CLI にアクセスする必要があり、CLI を使用している場合、またはトラブルシューティングには基本的なネットワーク設定を設定する必要があります。

手順の詳細

コマンド	目的

Telnet セッション。
ハードウェア モジュール（例：ASA 5585-X）の場合：
session 1
ソフトウェア モジュール（例：ASA 5545-X）の場合：
session ips
 	
例：
`hostname# session 1`
 	
`Opening command session with slot 1.`
`Connected to slot 1.Escape character sequence is 'CTRL-^X'.`
 	
`sensor login: cisco`
`Password: cisco`
	Telnet を使用してモジュールにアクセスします。ユーザ名とパスワードの入力を求められます。デフォルトのユーザ名は **cisco**、デフォルトのパスワードは **cisco** です。
	（注） 初めてモジュールにログインしたときに、デフォルトのパスワードの変更を要求するプロンプトが表示されます。パスワードは 8 文字以上で、辞書に載っていない単語にする必要があります。

コンソール セッション（ソフトウェア モジュールのみ）。
session ips console
 	
例：
`hostname# session ips console`
 	
`Establishing console session with slot 1`
`Opening console session with module ips.`
`Connected to module ips.Escape character sequence is 'CTRL-SHIFT-6 then x'.`
 	
`sensor login: cisco`
`Password: cisco`
	モジュール コンソールにアクセスします。ユーザ名とパスワードの入力を求められます。デフォルトのユーザ名は **cisco**、デフォルトのパスワードは **cisco** です。
	（注） このコマンドは、Ctrl+Shift+6、x がターミナル サーバのプロンプトに戻るエスケープ シーケンスであるターミナル サーバとともに使用しないでください。Ctrl+Shift+6、x は、IPS コンソールをエスケープし ASA プロンプトに戻るシーケンスでもあります。したがって、この状況で IPS を終了しようとすると、代わりにターミナル サーバ プロンプトに戻ります。ASA にターミナル サーバを再接続すると、IPS コンソール セッションがまだアクティブなままであり、ASA プロンプトに戻ることができません。ASA プロンプトにコンソールを戻すには、直接シリアル接続を使用する必要があります。
	
	代わりに **session ips** コマンドを使用します。

（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールの起動

ASA には一般的に、IPS モジュール ソフトウェアが付属しており、Disk0 に収録されています。このモジュールが実行されていない場合や、IPS モジュールを既存の ASA に追加する場合は、モジュール ソフトウェアを起動する必要があります。モジュールが実行中であるか不明な場合は、起動ウィザードの実行時に [IPS Basic Configuration] 画面が表示されません（「IPS モジュールの基本的なネットワーク設定値の設定」（P.20-13）を参照）。

手順の詳細

ステップ 1　次のどちらかを実行します。

- プリインストール済みの IPS を搭載する新しい ASA : フラッシュ メモリで IPS モジュール ソフトウェアのファイル名を表示するには、[Tools] > [File Management] を選択します。

  たとえば、IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip のようなファイル名を検索します。ファイル名をメモしておきます。このファイル名は、この手順で後ほど必要になります。

- 既存の ASA に新しい IPS をインストールする場合 : IPS ソフトウェアを Cisco.com からコンピュータにダウンロードします。Cisco.com のログインをお持ちの場合は、次の Web サイトからソフトウェアを入手できます。

  http://www.cisco.com/cisco/software/navigator.html?mdfid=282164240

  [Tools] > [File Management] を選択し、[File Transfer] > [Between Local PC and Flash] を選択して、新しいイメージを disk0 にアップロードします。ファイル名をメモしておきます。このファイル名は、この手順で後ほど必要になります。

ステップ 2　[Tools] > [Command Line Interface] を選択します。

ステップ 3　disk0 の IPS モジュール ソフトウェアの場所を設定するには、次のコマンドを入力し、[Send] をクリックします。

```
sw-module module ips recover configure image disk0:file_path
```

たとえば、この例のステップ 1 のファイル名を使用するには、次のとおりに入力します。

```
sw-module module ips recover configure image disk0:IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip
```

ステップ 4　IPS モジュール ソフトウェアをインストールし、ロードするには、次のコマンドを入力し、[Send] をクリックします。

```
sw-module module ips recover boot
```

ステップ 5　イメージ転送とモジュール再起動プロセスの進行状況を確認するには、次のコマンドを入力し、[Send] をクリックします。

```
show module ips details
```

出力の [Status] フィールドが、モジュールの動作ステータスを示します。モジュールの動作ステータスは、通常は「Up」と表示されます。ASA によってアプリケーション イメージがモジュールに転送されているときは、出力の [Status] フィールドには [Recover] と表示されます。ASA によるイメージの転送が完了してモジュールが再起動されると、新たに転送されたイメージが実行されます。

IPS モジュールの基本的なネットワーク設定値の設定

シングル コンテキスト モードでは、ASDM で起動ウィザードを使用して、基本的な IPS ネットワーク設定を行うことができます。これらの設定は、ASA コンフィギュレーションではなく、IPS コンフィギュレーションに保存されます。

マルチ コンテキスト モードでは、ASA からモジュールへのセッションを開始し、**setup** コマンドを使用して基本設定を行います。

（注）（ASA 5512-X ～ ASA 5555-X）[IPS Basic Configuration] 画面がウィザードに表示されない場合は、IPS モジュールが動作していません。「（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールの起動」（P.20-11）を参照し、モジュールをインストールした後でこの手順をもう一度実行してください。

手順の詳細：シングル モード

ステップ 1　[Wizards] > [Startup Wizard] を選択します。

ステップ 2　[IPS CX Basic Configuration] 画面が表示されるまで、[Next] をクリックして、初期画面から進みます。

ステップ 3　[Network Settings] 領域で、次の設定を行います。

- [IP Address]：管理 IP アドレス。デフォルトのアドレスは 192.168.1.2 です。
- [Subnet Mask]：管理 IP アドレスのサブネット マスク。
- [Gateway]：アップストリーム ルータの IP アドレス。ネクスト ホップ ルータの IP アドレス。ネットワークの要件については、「ASA IPS 管理インターフェイスの接続」（P.20-7）を参照してください。ASA の管理 IP アドレスのデフォルト設定は機能しません。
- [HTTP Proxy Server]：（オプション）HTTP プロキシ サーバのアドレス。インターネット経由でダウンロードする代わりに、グローバル相関の更新やその他の情報をダウンロードするためにプロキシ サーバを使用できます。
- [HTTP Proxy Port]：（オプション）HTTP プロキシ サーバのポート。
- [DNS Primary]：（オプション）プライマリ DNS サーバのアドレス。DNS サーバを使用している場合は、グローバル相関更新に正常に到達できる DNS サーバを少なくとも 1 つ設定する必要があります。

  グローバル相関が機能するには、DNS サーバまたは HTTP プロキシ サーバのいずれかが常に設定されている必要があります。DNS 解決は、グローバル相関更新サーバへのアクセスについてのみサポートされます。

ステップ 4　[Management Access List] 領域に、IPS 管理インターフェイスへのアクセスを許可するホストの IP アドレスとサブネット マスクを入力し、[Add] をクリックします。複数の IP アドレスを追加できます。

ステップ 5　[Cisco Account Password] 領域に、ユーザ名 **cisco** に対するパスワードを設定し、確認のためにもう一度入力します。ユーザ名 **cisco** とこのパスワードは、管理アクセス リストで指定されたホストからの Telnet セッションと ASDM（[Configuration] > [IPS]）から IPS モジュールへのアクセス時に使用されます。デフォルトのパスワードは、**cisco** です。

ステップ 6　IPS モジュールを SensorBase データ共有に参加させるために使用する [Network Participation] 領域で、[Full]、[Partial]、または [Off] をクリックします。

手順の詳細：CLI を使用するマルチ モード

	コマンド	目的
ステップ 1	「ASA からモジュールへのセッションの開始（必要な場合がある）」（P.20-10）に従って、IPS モジュールへのセッションを開始します。	
ステップ 2	**setup** **例：** `sensor# setup`	ASA IPS モジュールの初期設定用のセットアップ ユーティリティを実行します。基本設定を求めるプロンプトが表示されます。デフォルト ゲートウェイについては、アップストリーム ルータの IP アドレスを指定します。ネットワークの要件については、「ASA IPS 管理インターフェイスの接続」（P.20-7）を参照してください。ASA の管理 IP アドレスのデフォルト設定は機能しません。

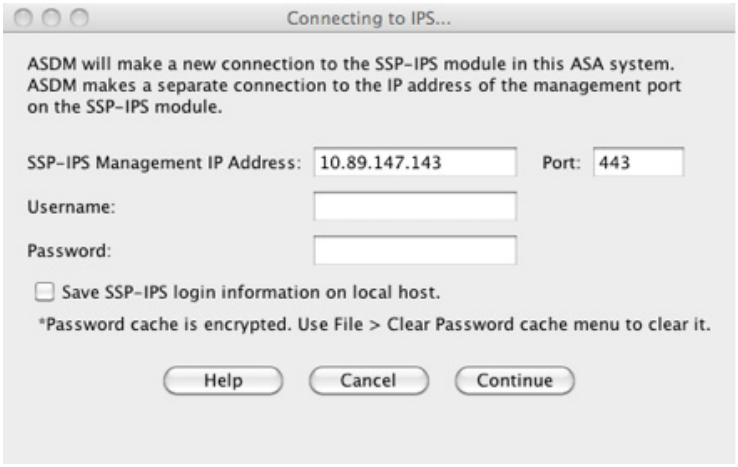
ASA IPS モジュールでのセキュリティ ポリシーの設定

この項では、ASA IPS モジュール アプリケーションを設定する方法について説明します。

手順の詳細

ステップ 1　*ASA* の管理 IP アドレスを使用して、ASDM に接続します。

ステップ 2　ASDM から IPS Device Manager（IDM）にアクセスするには、[Configuration] > [IPS] をクリックします。



ステップ 3　「IPS モジュールの基本的なネットワーク設定値の設定」（P.20-13）で設定した IP アドレス、ユーザ名、およびパスワードを、ポートとともに入力します。デフォルトの IP アドレスとポートは 192.168.1.2:443 です。デフォルトのユーザ名およびパスワードは、**cisco** と **cisco**.です。

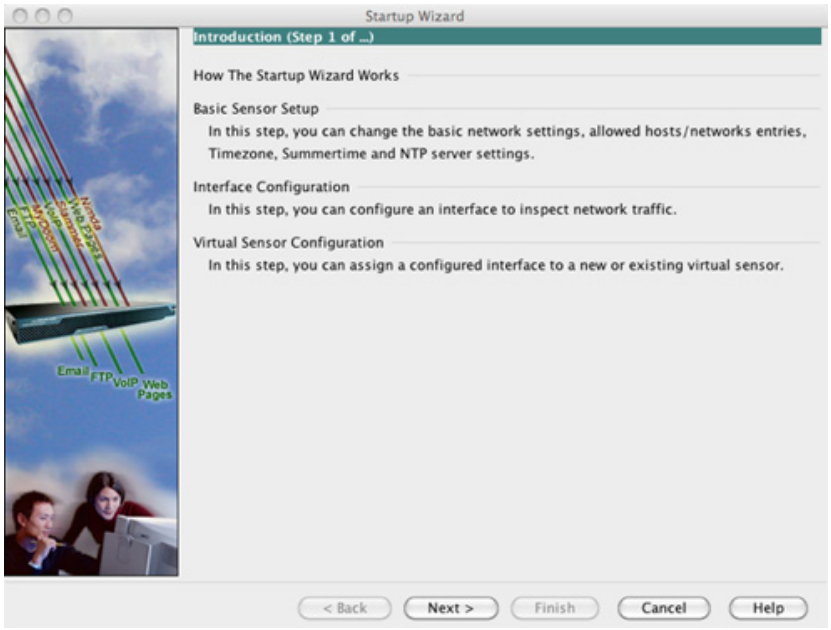
IDM にアクセスするためのパスワードがわからない場合は、ASDM を使用してパスワードをリセットできます。詳細については、「パスワードのリセット」（P.20-22）を参照してください。

ステップ 4　お使いのローカル PC にログイン情報を保存するには、[Save IPS login information on local host] チェックボックスをオンにします。

ステップ 5　[Continue] をクリックします。

[Startup Wizard] ペインが表示されます。

ステップ 6　[Launch Startup Wizard] をクリックします プロンプトに従って画面を完了します。詳細については、IDM オンライン ヘルプを参照してください。



仮想センサーを設定する場合は、センサーの 1 つをデフォルトとして指定します。ASA シリーズが、そのコンフィギュレーションで仮想センサー名を指定しない場合は、デフォルト センサーが使用されます。

次の作業

- マルチ コンテキスト モードの ASA の場合は、「セキュリティ コンテキストへの仮想センサーの割り当て」（P.20-16）を参照してください。
- シングル コンテキスト モードの ASA の場合は、「ASA IPS モジュールへのトラフィックの誘導」（P.20-17）を参照してください。

セキュリティ コンテキストへの仮想センサーの割り当て

ASA がマルチ コンテキスト モードにある場合、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ることができます。このようにすると、トラフィックを ASA IPS モジュールに送信するようにコンテキストを設定するときに、そのコンテキストに割り当てられているセンサーを指定できます。そのコンテキストに割り当てられていないセンサーを指定することはできません。コンテキストにセンサーを割り当てない場合は、ASA IPS モジュール上で設定されているデフォルト 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ためにマルチ コンテキスト モードを開始する必要はありません。シングル モードでトラフィック フローごとに異なるセンサーを使用できます。

前提条件

コンテキストの設定の詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

手順の詳細

ステップ 1　[ASDM Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

ステップ 2　[Context Management] > [Security Contexts] ペインで、設定するコンテキストを選択し、[Edit] をクリックします。

[Edit Context] ダイアログボックスが表示されます。コンテキストの設定の詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

ステップ 3　[IPS Sensor Allocation] 領域で、[Add] をクリックします。

[IPS Sensor Selection] ダイアログボックスが表示されます。

ステップ 4　[Sensor Name] ドロップダウン リストで、ASA IPS モジュールに設定されているものの中からセンサー名を選択します。

ステップ 5　（オプション）センサーにマッピング名を割り当てるには、[Mapped Sensor Name] フィールドに値を入力します。

このセンサー名は、コンテキスト内で実際のセンサー名の代わりに使用できます。マッピング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。セキュリティのために、コンテキストで使用されているセンサーをコンテキスト管理者に知らせない場合があります。または、コンテキスト コンフィギュレーションを一般化する場合もあります。たとえば、すべてのコンテキストで「sensor1」と「sensor2」という名前のセンサーが使用されるようにする場合に、コンテキスト A ではセンサー「highsec」と「lowsec」を sensor1 と sensor2 にマッピングし、コンテキスト B ではセンサー「medsec」と「lowsec」を sensor1 と sensor2 にマッピングします。

ステップ 6　[OK] をクリックして [Edit Context] ダイアログボックスに戻ります。

ステップ 7　（オプション）1 つのセンサーをこのコンテキストのデフォルト センサーとして設定するには、[Default Sensor] ドロップダウン リストからセンサー名を選択します。

コンテキスト コンフィギュレーション内に IPS を設定するときにセンサー名を指定しない場合、コンテキストはデフォルト センサーを使用します。コンテキストごとに設定できるデフォルト センサーは 1 つのみです。デフォルトとしてセンサーを指定せず、コンテキスト コンフィギュレーションにセンサー名が含まれていない場合、トラフィックは ASA IPS モジュールでデフォルト センサーを使用します。

ステップ 8　この手順をセキュリティ コンテキストごとに繰り返します。

ステップ 9　IPS セキュリティ ポリシーを設定するには各コンテキストに切り替えます（「ASA IPS モジュールへのトラフィックの誘導」（P.20-17）で説明されています）。

次の作業

IPS セキュリティ ポリシーを設定するには各コンテキストに切り替えます（「ASA IPS モジュールへのトラフィックの誘導」（P.20-17）で説明されています）。

ASA IPS モジュールへのトラフィックの誘導

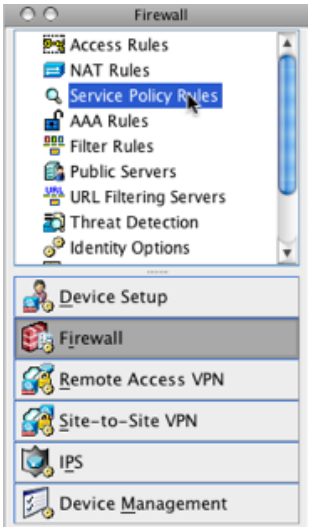
この項では、ASA から ASA IPS モジュールに誘導するトラフィックを指定します。

前提条件

マルチ コンテキスト モードでは、各コンテキスト実行スペースでこれらの手順を実行します。コンテキストに変更するには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] の順に選択します。



ステップ 2　[Add] > [Add Service Policy Rule] を選択します。[Add Service Policy Rule Wizard - Service Policy] ダイアログボックスが表示されます。

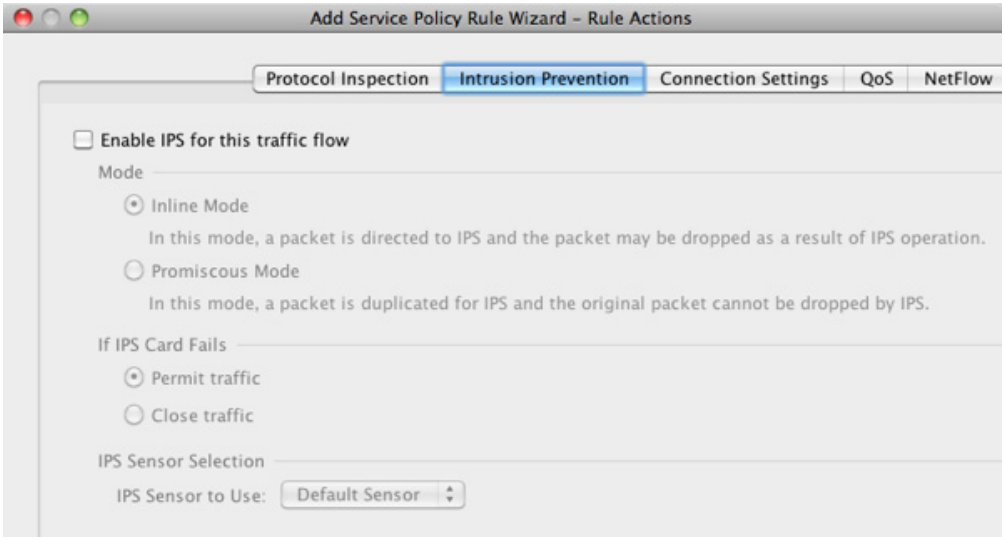
ステップ 3　必要に応じて [Service Policy] ダイアログボックスに入力します。これらの画面の詳細については、ASDM オンライン ヘルプを参照してください。

ステップ 4　[Next] をクリックします。[Add Service Policy Rule Wizard - Traffic Classification Criteria] ダイアログボックスが表示されます。

ステップ 5　必要に応じて [Traffic Classification Criteria] ダイアログボックスに入力します。これらの画面の詳細については、ASDM オンライン ヘルプを参照してください。

ステップ 6　[Next] をクリックして [Add Service Policy Rule Wizard - Rule Actions] ダイアログボックスを表示します。

ステップ 7　[Intrusion Prevention] タブをクリックします。



ステップ 8　[Enable IPS for this traffic flow] チェックボックスをオンにします。

ステップ 9　[Mode] 領域で、[Inline Mode] または [Promiscuous Mode] をクリックします。詳細については、「動作モード」（P.20-2）を参照してください。

ステップ 10　[If IPS Card Fails] 領域で、[Permit traffic] または [Close traffic] をクリックします。[Close traffic] オプションを選択すると、ASA は ASA IPS モジュールが使用不可の場合にすべてのトラフィックをブロックします。[Permit traffic] オプションを選択すると、ASA は ASA IPS モジュールが使用不可の場合に、すべてのトラフィックの通過を検査なしで許可します。[IPS Sensor Selection] 領域の詳細については、ASDM オンライン ヘルプを参照してください。

ステップ 11　（ASA 5512-X 以降）[IPS Sensor to use] ドロップダウン リストから、仮想センサー名を選択します。

仮想センサーを使用する場合は、このオプションを使用してセンサー名を指定できます。ASA 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を指定できます（「セキュリティ コンテキストへの仮想センサーの割り当て」（P.20-16）を参照）。センサー名を指定しないと、トラフィックはデフォルトの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のセンサーを指定できます。シングル モードの場合や、マルチ モードでデフォルト センサーが指定されていない場合は、ASA IPS モジュールで設定されているデフォルト センサーがトラフィックに使用されます。

ステップ 12　[OK]、続いて [Apply] をクリックします。

ステップ 13　この手順を繰り返して、追加のトラフィック フローを必要に応じて設定します。

ASA IPS モジュールの管理

この項には、モジュールのリカバリやトラブルシューティングに役立つ手順が含まれます。

- 「モジュール上でのイメージのインストールおよび起動」（P.20-19）
- 「モジュールのシャットダウン」（P.20-21）
- 「ソフトウェア モジュール イメージのアンインストール」（P.20-21）
- 「パスワードのリセット」（P.20-22）
- 「モジュールのリロードまたはリセット」（P.20-22）

モジュール上でのイメージのインストールおよび起動

モジュールに障害が発生して、モジュール アプリケーション イメージを実行できない場合は、TFTP サーバから（ハードウェア モジュールの場合）、またはローカル ディスク（ソフトウェア モジュールの場合）から、モジュール上に新しいイメージを再インストールできます。

（注）　モジュール ソフトウェア内部では、イメージをインストールするために **upgrade** コマンドを使用しないでください。

前提条件

- ハードウェア モジュール：指定する TFTP サーバが、最大 60 MB のファイルを転送できることを確認してください。

  （注）　ネットワークとイメージのサイズに応じて、このプロセスは完了までに約 15 分間かかることがあります。

- ソフトウェア モジュール：この手順を実行する前に、イメージを ASA 内部フラッシュ（disk0）にコピーします。

  （注）　IPS ソフトウェアを disk0 にダウンロードする前に、フラッシュ メモリの最低 50% が空いていることを確認します。IPS をインストールするときに、IPS のファイル システム用に内部フラッシュ メモリの 50% が予約されます。

手順の詳細

	コマンド	目的

ステップ 1	ハードウェア モジュール（例：ASA 5585-X）の場合：
	hw-module module 1 recover configure
	ソフトウェア モジュール（例：ASA 5545-X）の場合：
	sw-module module ips recover configure image disk0:*file_path*
	例：
	`hostname# hw-module module 1 recover configure`
	`Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg`
	`Port IP Address [127.0.0.2]: 10.1.2.10`
	`Port Mask [255.255.255.254]: 255.255.255.0`
	`Gateway IP Address [1.1.2.10]: 10.1.2.254`
	`VLAN ID [0]: 100`
		新しいイメージの場所を指定します。
		ハードウェア モジュールの場合：このコマンドを実行すると、TFTP サーバの URL、管理インターフェイスの IP アドレスとネットマスク、ゲートウェイ アドレスの入力を求めるプロンプトが表示されます。これらのネットワーク パラメータは ROMMON で設定されます。モジュール アプリケーション コンフィギュレーションで設定したネットワーク パラメータは ROMMON には使用できないため、ここで別個に設定する必要があります。
		ソフトウェア モジュールの場合：ローカル ディスク上のイメージの場所を指定します。
		リカバリ コンフィギュレーションを表示するには、**show module {1 | ips} recover** コマンドを使用します。
		マルチ コンテキスト モードでは、システム実行スペースでこのコマンドを入力します。

ステップ 2	ハードウェア モジュールの場合： **hw-module module 1 recover boot** ソフトウェア モジュールの場合： **sw-module module ips recover boot** **例：** `hostname# hw-module module 1 recover boot`	IPS モジュール ソフトウェアをインストールして起動します。
ステップ 3	ハードウェア モジュールの場合： **show module 1 details** ソフトウェア モジュールの場合： **show module ips details** **例：** `hostname# show module 1 details`	イメージ転送とモジュール再起動のプロセスの進捗を確認します。 出力の [Status] フィールドが、モジュールの動作ステータスを示します。モジュールの動作ステータスは、通常は「Up」と表示されます。ASA によってアプリケーション イメージがモジュールに転送されているときは、出力の [Status] フィールドには [Recover] と表示されます。ASA によるイメージの転送が完了してモジュールが再起動されると、新たに転送されたイメージが実行されます。

モジュールのシャットダウン

モジュール ソフトウェアをシャットダウンするのは、コンフィギュレーション データを失うことなく安全にモジュールの電源をオフにできるように準備するためです。**注**：ASA をリロードする場合は、モジュールは自動的にはシャットダウンされないので、ASA のリロード前にモジュールをシャットダウンすることを推奨します。モジュールをグレースフル シャットダウンするには、ASA CLI で次の手順を実行します。

手順の詳細

コマンド	目的
ハードウェア モジュール（例：ASA 5585-X）の場合： **hw-module module 1 shutdown** ソフトウェア モジュール（例：ASA 5545-X）の場合： **sw-module module ips shutdown** **例：** `hostname# hw-module module 1 shutdown`	モジュールをシャットダウンします。

ソフトウェア モジュール イメージのアンインストール

ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールするには、次の手順を実行します。

手順の詳細

	コマンド	目的

ステップ 1	**sw-module module ips uninstall**
	
	例：
	`hostname# sw-module module ips uninstall`
	`Module ips will be uninstalled.This will completely remove the`
	`disk image associated with the sw-module including any configuration`
	`that existed within it.`
	
	`Uninstall module <id>?[confirm]`
		ソフトウェア モジュール イメージおよび関連するコンフィギュレーションを永続的にアンインストールします。

ステップ 2	**reload** **例：** `hostname# reload`	ASA をリロードします。新しいモジュール タイプをインストールする前に、ASA をリロードする必要があります。

パスワードのリセット

モジュールのパスワードをデフォルトにリセットできます。ユーザ **cisco** のデフォルトのパスワードは **cisco** です。パスワードをリセットした後は、モジュール アプリケーションを使用してパスワードを独自の値に変更する必要があります。

モジュールのパスワードをリセットすると、モジュールがリブートします。モジュールのリブート中は、サービスを使用できません。

新しいパスワードで ASDM に接続できない場合は、ASDM を再起動して再度ログインしてみます。新しいパスワードを定義したが、新しいパスワードと異なる既存のパスワードが ASDM にある場合は、[File] > [Clear ASDM Password Cache] を選択して、パスワード キャッシュを消去し、ASDM を再起動して再度ログインしてみます。

モジュールのパスワードをデフォルトの「cisco」にリセットするには、次の手順を実行します。

手順の詳細

ステップ 1　ASDM メニューバーの [Tools] > [module Password Reset] を選択します。

[Password Reset] 確認ダイアログ ボックスが開きます。

ステップ 2　パスワードをデフォルトにリセットするには、[OK] をクリックします。

ダイアログボックスに、パスワードのリセットが正常に完了したか、失敗したかが表示されます。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。

モジュールのリロードまたはリセット

モジュールをリロードまたはリセットするには、ASA CLI で次のいずれかのコマンドを入力します。

手順の詳細

コマンド	目的
ハードウェア モジュール（例：ASA 5585-X）の場合： **hw-module module 1 reload** ソフトウェア モジュール（例：ASA 5545-X）の場合： **sw-module module ips reload** **例：** `hostname# hw-module module 1 reload`	モジュール ソフトウェアをリロードします。

コマンド	目的
ハードウェア モジュールの場合： **hw-module module 1 reset** ソフトウェア モジュールの場合： **sw-module module ips reset** **例：** `hostname# hw-module module 1 reset`	リセットを実行してから、モジュールをリロードします。

ASA IPS モジュールのモニタリング

『一般的な操作のコンフィギュレーション ガイド』の [Intrusion Prevention] タブを参照してください。

ASA IPS モジュールの機能履歴

表 20-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 20-2　ASA IPS モジュールの機能履歴

機能名	プラットフォーム リリース	機能情報
AIP SSM	7.0(1)	ASA 5510、5520、および 5540 対応の AIP SSM のサポートが導入されました。 次の画面が導入されました。[Configuration] > [Firewall] > [Service Policy Rules] > [Add/Edit Service Policy Rule] > [Intrusion Prevention]。
仮想センサー（ASA 5510 以降）	8.0(2)	仮想センサーのサポートが導入されました。仮想センサーを使用すると ASA IPS モジュール上で複数のセキュリティ ポリシーを設定できます。 次の画面が変更されました。[Context Management] > [Security Contexts] > [Edit Context]。
ASA 5505 用 AIP SSC	8.2(1)	ASA 5505 対応の AIP SSC のサポートが導入されました。 次の画面が導入されました。[Configuration] > [Device Setup] > [SSC Setup]。

表 20-2　ASA IPS モジュールの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
ASA 5585-X 対応の ASA IPS SSP-10、-20、-40、および -60 のサポート	8.2(5)/ 8.4(2)	ASA 5585-X 対応の ASA IPS SSP-10、-20、-40、および -60 のサポートが導入されました。ASA IPS SSP をインストールできるのは、SSP のレベルが一致する場合だけです（たとえば、SSP-10 と ASA IPS SSP-10）。 **（注）** ASA 5585-X はバージョン 8.3 ではサポートされていません。
SSP-40 および SSP-60 対応のデュアル SSP のサポート	8.4(2)	SSP-40 および SSP-60 の場合、同じシャーシでレベルが同じ 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-40 と SSP-60 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。 **（注）** 2 つの SSP をシャーシで使用する場合、VPN はサポートされません。しかし、VPN がディセーブルになっていないことに注意してください。 変更された画面はありません。
ASA 5512-X ～ ASA 5555-X に対する ASA IPS SSP のサポート	8.6(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X に対する ASA IPS SSP ソフトウェア モジュールのサポートが導入されました。 変更された画面はありません。