CHAPTER 6

ネットワークの運用とモニタリング

Prime AM の [Operate] タブには、ネットワークを毎日モニタするのに役立つツールが用意されています。また、これらのツールは、ネットワーク デバイス インベントリおよび設定管理に関連したその他の日常的または特別な操作を実行する際にも利用できます。[Operate] タブには、ダッシュボードとデバイス ワーク センターが含まれ、日々のモニタリング、トラブルシューティング、メンテナンス、運用に必要なツールも含まれています。

ダッシュレットとダッシュボードのモニタリング

Prime AM では、モニタリング データがダッシュボードとダッシュレットに自動的に表示されます。[Operate] > [Monitoring Dashboard] で次のいずれかのダッシュボードを選択して、概要情報を表示できます。

- [Overview] : デバイス数などのネットワークに関する概要情報、および CPU 使用率とメモリ使用率のそれぞれ上位 5 台のデバイスを表示します。この概要ダッシュボードから、デバイスまたはインターフェイス アラーム数をクリックして、詳細なダッシュボードを表示したり、問題のトラブルシューティングや切り分けに役立つアラームおよびイベントを表示したりできます。
- [Incidents] : ネットワーク全体、特定のサイト、または特定のデバイスについて、アラームおよびイベントの概要を表示します。ダッシュボード内の項目をクリックすることにより、アラームまたはイベントの詳細を表示し、問題をトラブルシューティングできます。
- [Performance] : CPU 使用率およびメモリ使用率の情報を表示します。
- [Detail Dashboards] : サイト、デバイス、またはインターフェイスについて、ネットワーク ヘルスの概要を表示します。この詳細ダッシュボードでは、ネットワークの輻輳を確認したり、サイト、デバイス、インターフェイスの詳細な情報を集めたりすることができます。たとえば、特定のサイトの詳細ダッシュボードを表示して、どのデバイスでアラームが頻発しているか、そのサイトのデバイス到達可能性ステータスなどを調べることができます。

ダッシュボードに表示される情報は、ダッシュボードの共通タスクの説明に従って変更できます。

表 6-1 に、各種モニタリング情報を表示する際に使用する Prime AM ダッシュボードを示します。

表 6-1　モニタリング データの表示

表示するモニタリング データ	使用するダッシュボード
アラーム情報	[Operate] > [Monitoring Dashboard] > [Incidents]
CPU 使用率	[Operate] > [Monitoring Dashboard] > [Performance]
詳細なデバイス情報	[Operate] > [Monitoring Dashboard] > [Detail Dashboards]
詳細なインターフェイス情報	[Operate] > [Monitoring Dashboard] > [Detail Dashboards]

表 6-1　モニタリング データの表示 （続き）

表示するモニタリング データ	使用するダッシュボード
デバイス到達可能性ステータス	[Operate] > [Monitoring Dashboard] > [Overview]
イベント情報	[Operate] > [Monitoring Dashboard] > [Incidents]
インターフェイスのステータス、可用性、および使用率の情報	[Operate] > [Monitoring Dashboard] > [Performance]
ライセンス情報	[Operate] > [Monitoring Dashboard] > [Overview]
メモリ使用率	[Operate] > [Monitoring Dashboard] > [Performance]
サイト情報	[Operate] > [Monitoring Dashboard] > [Detail Dashboards]
syslog 送信側情報	[Operate] > [Monitoring Dashboard] > [Incidents]
使用率統計情報	[Operate] > [Monitoring Dashboard] > [Overview]

ジョブのモニタリング

[Tools] > [Task Manager] > [Jobs Dashboard] を選択して、ジョブのステータスを表示したり、次の作業を実行したりします。

- 実行中および完了したすべてのジョブと、それらのジョブの詳細を表示する
- ジョブをフィルタリングして、興味のある特定のジョブを表示する
- 最後に送信されたジョブの詳細を表示する
- ジョブの実行結果を表示する
- ジョブを変更する（ジョブの削除、編集、実行、取り消し、一時停止、再開など）

ジョブが失敗した場合は、[Jobs Dashboard] からトラブルシューティング情報を得られます。ジョブを展開してその詳細を表示してから、[History] タブをクリックし、カーソルを [Status] フィールド内に置きます。結果ウィンドウに、ジョブの失敗原因の特定に役立つトラブルシューティング情報が表示されます。

モニタリング設定の設定

Prime AM によるネットワーク内のデバイスとインターフェイスのモニタ方法を定義できます。

[Auto Monitoring] オプションをイネーブルにすることにより、Prime AM で、すべてのネットワーク デバイスの可用性、CPU、メモリ、および温度を自動的にモニタできます。デフォルトでは、Prime AM は、ネットワーク内のすべてのデバイスを 15 分ごとにポーリングしてデバイスヘルス データを取得します。ほとんどのユーザは、[Auto Monitoring] をイネーブルにします。

ネットワークの規模または Prime AM の導入規模が非常に大きい場合は、ポーリング トラフィックが過大になるのを防ぐために、[Auto Monitoring] をイネーブルにしないこともできます。この場合、[Auto Monitoring] をディセーブルのままにし、ビジネスに不可欠なデバイスのみで構成される 1 つ以上のデバイス グループを作成できます。また、これらのデバイスに対して適切なポーリング頻度を設定したデフォルト デバイス ヘルス モニタリング テンプレートを作成することもできます。デフォルトまたはカスタム デバイス ヘルス モニタリング テンプレートを導入する場合、そのテンプレートを、ビジネスに不可欠なデバイス グループに対してのみ適用することもできます。

必要ならば、Cisco IOS Netflow と Cisco Prime Assurance に対して重複排除をイネーブルにすることもできます。NetFlow を Cisco Prime Assurance サーバに送信するルータとスイッチが複数存在し、Cisco Prime Assurance がデータを取得する NAM が複数存在する場合、Cisco Prime Assurance は、同じトラフィック統計情報を複数回受信する可能性があります。Cisco Prime Assurance が同じメトリックを重複してカウントすることがないように、重複排除をイネーブルにできます。

ステップ 1　[Administration] > [System] を選択し、[Monitoring Settings] を選択します。

ステップ 2　次のオプションをオンにします。

- [Auto monitoring]。Prime AM ですべてのデバイスとインターフェイスを自動的にモニタします。
- [Enable deduplication]。Prime AM で重複データを排除します。

デバイス ワーク センターとは

[Operate] > [Device Work Center] から、デバイス インベントリとデバイス構成情報を表示できます。デバイス ワーク センターでは、表 6-2 に説明されているように、上部には一般的な管理機能が、下部には設定機能が用意されています。

表 6-2　デバイス ワーク センターの作業

作業	説明	[Operate] > [Device Work Center] 内の場所
デバイスの管理	デバイスの追加、編集、バルク インポート、および削除を実行したり、デバイスからデータを強制的に収集したりします。	[Device Work Center] の上部に配置されたボタン。
基本的なデバイス情報と収集ステータスの表示	到達可能性ステータス、IP アドレス、デバイス タイプなどの基本的なデバイス情報と、収集ステータス情報を表示します。	[Device Work Center] の上部に表示されます。 [Collection Status] セルにカーソルを置き、アイコンをクリックして、インベントリ収集に関連したエラーを表示します。
デバイス グループの管理	デフォルトでは、Prime AM によってダイナミック デバイス グループが作成され、デバイスは適切な [Device Type] フォルダに割り当てられます。ユーザは、[User Defined] フォルダに表示される新しいデバイス グループを作成できます。	[Device Work Center] の左ペインに表示されます。 デバイス グループの作成および使用の詳細については、デバイス グループの使用を参照してください。
サイトへのデバイスの追加	サイト プロファイルをセットアップした後、サイトにデバイスを追加できます。 **（注）**　各デバイスは、1 つのサイトにのみ属することができます。	[Device Work Center] の上部に配置された [Add to Site] ボタン。 デバイスをサイトに追加する方法の詳細については、サイト プロファイルの作成を参照してください。
デバイスの詳細情報の表示	メモリ、ポート、環境、インターフェイスなど、デバイスの詳細情報を表示します。	[Device Work Center] でデバイスを選択し、画面の下部にある [Device Details] タブをクリックします。
	デバイスの情報とステータス、および関連するモジュール、アラーム、ネイバー、インターフェイスを表示します。詳細については、[360º View] の使用を参照してください。	デバイスの IP アドレスの上にカーソルを置き、表示されたアイコンをクリックします。

表 6-2　デバイス ワーク センターの作業 （続き）

作業	説明	[Operate] > [Device Work Center] 内の場所
設定テンプレートの作成と導入	選択したデバイスに対して設定テンプレートを作成し、導入できます。また、デバイスに導入される CLI をプレビューすることもできます。	[Device Work Center] の下部にある [Configuration] タブをクリックします。
デバイス構成の表示	アーカイブされた設定を表示したり、設定のロールバックをスケジュールしたり、アーカイブの収集をスケジュールしたりします。	[Device Work Center] の下部にある [Configuration Archive] タブをクリックします。
ソフトウェア イメージの表示	選択したデバイス上のイメージ、そのデバイスの推奨ソフトウェア イメージ、およびデバイスに対する最新のソフトウェア イメージ操作について詳細情報を表示します。	[Device Work Center] の下部にある [Image] タブをクリックします。

デバイス上の機能の設定

選択したデバイスに対して機能設定を作成または変更できます。詳細については、次の項を参照してください。

- 「アプリケーションの可視化」（P.6-4）
- 「NAT の概要」（P.6-7）
- 「ダイナミック マルチポイント VPN」（P.6-15）
- 「GETVPN」（P.6-21）
- 「VPN コンポーネント」（P.6-26）
- 「ゾーンの概要」（P.6-36）

アプリケーションの可視化

アプリケーションの可視化（AV）機能は、インターネットに向けて送信されるトラフィックをモニタする際に役立ちます。AV を設定するには、次の作業を実行する必要があります。

- AV 設定を作成する
- インターフェイス上で AV ポリシーを割り当てる
- AV 詳細オプションを変更する

（注）　アプリケーションの可視化機能は、IOS バージョン 3.5 以降の ASR デバイス上でサポートされています。この機能は ISR デバイス上ではサポートされません。「EMS_」で始まるオブジェクトまたはエンティティに対して CLI インターフェイス経由で変更を行うことはサポートされていません。そのような変更を行うと、予期せぬ動作が発生する可能性があります。

AV の設定

アプリケーションの可視化設定機能は、トランザクション レコードと使用状況レコードの NetFlow メッセージを送信するために、デバイス内で必要な要素を作成します。AV を設定するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Application Visibility] > [Configuration] を選択します。[AV Configuration] ページが表示されます。

ステップ 5　[AV Configuration] ページから、プライマリ CM IP アドレス、セカンダリ CM IP アドレス、VPN ルーティングおよび転送（VRF）、および送信元 IP アドレスを設定します。

ステップ 6　AV の詳細パラメータを設定します。AV の詳細パラメータの詳細については、「AV 詳細オプションの変更」（P.6-6）を参照してください。

表 6-3 に、[AV Configuration] ページ上の要素を示します。

表 6-3　[Application Visibility] ページ

要素	説明
Primary CM IP	プライマリ CM の IP アドレスを入力します。
Secondary CM IP	（オプション）セカンダリ CM の IP アドレスを入力します。
VRF	プライマリ CM IP、セカンダリ CM IP、および送信元 IP 用の VRF。グローバル VRF がデフォルトの VRF です。
Source IP Address	インターフェイス用の IP アドレスを指定します。CM に向けて FNF メッセージを送信する際の送信元として使用されます。

ステップ 7　[Save] または [Apply] をクリックして、変更をサーバに保存します。

インターフェイスの管理

既存の AV ポリシーを編集するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Application Visibility] > [Interfaces] を選択します。

ステップ 5　[Interface] ページで、AV レコードをイネーブルまたはディセーブルにするインターフェイスを 1 つ以上選択します。インターフェイス上で AV をイネーブルにするには、[Enable] を選択し、コレクタに送信するレコードを選択します。

a. 使用状況レコード（UR）：使用状況レコードは、特定のインターフェイス上で動作している各種アプリケーションのレコードです。オペレータは、使用状況レコードを使用して、各種アプリケーションの帯域幅の使用状況をモニタできます。使用状況レコードにより、一定期間のアプリケーションの使用量、ピークと平均の使用量、および特定のアプリケーション タイプの使用量を表示できます。使用状況レコードでは、インターフェイスのカテゴリ情報が定期的に集約されます。（たとえば、ピアツーピア トラフィックや電子メールの使用状況に関する情報がエクスポートされます）。

b. トランザクション レコード（TR）：トランザクションとは、エンドポイント間の一連の論理的なやり取りです。通常、1 つのフロー内には 1 つのトランザクションが存在します。トランザクション レコードでは、トランザクション レベルでトラフィックがモニタされます。これらのレコードにより、トラフィック フローが詳細に分析されます。トランザクション レコードは、ネットワーク側インターフェイスの入力方向と出力方向に向かいます。これらのトランザクション レコードにより、システムは、それぞれの一方向フローをキャプチャできます。

ステップ 6　[OK] をクリックして、変更をデバイスに導入します。

AV 詳細オプションの変更

アプリケーションの可視化詳細オプションを変更するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Application Visibility] > [Configuration] を選択します。[AV Configuration] ページが表示されます。

ステップ 5　[AV Configuration] ページで、AV 設定の新しい値を設定します。

ステップ 6　タイトル領域をクリックして、[Advanced Options] と [Record Advanced Options] を表示します。値をカスタマイズするには、個別の属性チェックボックスをオンにし、新しい値を設定します。システムのデフォルト値を使用するには、個別の属性のチェックボックスをオフにします。

ステップ 7　[Save] または [Apply] をクリックして、変更をサーバに保存します。

表 6-4 に、[AV Configuration] ページ上の要素を示します。

表 6-4　[Application Visibility] ページ

要素	説明
Primary CM IP	プライマリ CM の IP アドレスを入力します。
Secondary CM IP	（オプション）セカンダリ CM の IP アドレスを入力します。
VRF	プライマリ CM IP、セカンダリ CM IP、および送信元 IP 用の VRF。グローバル VRF がデフォルトの VRF です。

表 6-4　[Application Visibility] ページ （続き）

要素	説明
Source IP Address	インターフェイス用の IP アドレスを指定します。CM に向けて FNF メッセージを送信する際の送信元として使用されます。
Advance Options	
DSCP Value	（オプション）DSCP 値のチェックボックスをオンにして、エクスポータの DSCP サービス コード ポイント値を設定します。範囲は 0 ～ 63 です。
TTL	（オプション）[TTL] チェックボックスをオンにして、エクスポータの TTL またはホップ リミットを設定します。範囲は 1 ～ 255 です。
FNF Template Timeout	
Template Data Timeout	テンプレート データ タイムアウト値を秒単位で設定します。
Option Interface Timeout	オプション インターフェイス タイムアウト値を秒単位で設定します。
Attributes Table Timeout	属性テーブル タイムアウト値を秒単位で設定します。
Attributes Sampler Timeout	属性サンプラ タイムアウト値を秒単位で設定します。
Option Application Timeout	アプリケーション タイムアウトを秒単位で設定します。
VRF Table Timeout	VRF テーブル ID タイムアウト値を秒単位で設定します。
NetFlow Usage Records	
NetFlow Cache Size	フロー キャッシュ内の最大フロー エントリ数を設定します。
NetFlow Exporting Interval	キャッシュ フロー タイムアウトを指定します。
NetFlow Sampled Transaction Records	
NetFlow Cache Size	フロー キャッシュ内の最大フロー エントリ数を設定します。
Transaction Sampling	キャッシュ フロー タイムアウトを指定します。
NBAR Flow Table Size	最大許容セッション数を定義します。

NAT の概要

ネットワーク アドレス変換（NAT）とは、ネットワーク デバイス（一般にファイアウォール）がパブリック アドレスをプライベート ネットワーク内のコンピュータ（またはコンピュータのグループ）に割り当てるプロセスです。NAT は、経済上およびセキュリティ上の両方の理由から、組織または企業で使用されるパブリック IP アドレスの数を制限する際に役立ちます。

NAT 機能では、すでにネットワークを保有している組織がインターネットへのアクセスが必要になった際に、IP アドレスの枯渇問題を解決することができます。NAT により、組織の IP ネットワークは、外部ネットワークとは異なる IP アドレス空間を使用できます。したがって、NAT を使用すると、グローバルにルーティングできるアドレスを持たない組織でも、保有するアドレスをグローバルにルーティングできるアドレス空間に変換することにより、インターネットに接続できるようになります。また、サービス プロバイダーの変更や、クラスレス ドメイン間ルーティング（CIDR）ブロックへの自発的な再番号割り当てを行う組織は、NAT を使用して、より適切に番号を割り当て直せるようになります。NAT は RFC 1631 で規定されています。

NAT が設定されたルータには、少なくとも内部ネットワークに対して 1 つ、外部ネットワークに対して 1 つのインターフェイスがあります。標準的な環境では、NAT はサブ ドメインとバックボーンの間の出口ルータに設定されます。パケットがドメインから出て行くとき、NAT はローカルで意味のある

送信元アドレスをグローバルで一意のアドレスに変換します。パケットがドメインに入ってくるときは、NAT はグローバルで一意の宛先アドレスをローカル アドレスに変換します。出力点が複数存在する場合、個々の NAT は同一の変換テーブルを持っていなければなりません。アドレスが足りなくなって、パケットにアドレスを割り当てられなくなった場合、NAT はそのパケットをドロップし、インターネット制御メッセージ プロトコル（ICMP）ホスト到達不能パケットを送信します。

NAT の詳細については、
http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/xe-3s/iadnat-addr-consv.html
を参照してください。

NAT のタイプ

NAT はルータ上で動作し（一般に 2 つのネットワークだけを相互接続している）、パケットが別のネットワークに転送される前に、内部ネットワークのプライベート（ローカル内）アドレスをパブリック（グローバル内）アドレスに変換します。この機能により、ネットワーク全体を表す 1 つのアドレスのみを外部にアドバタイズするように NAT を設定できるようになります。これにより、内部ネットワークを外部から効果的に隠すことができるため、セキュリティがさらに強化されます。

NAT には次のタイプがあります。

- スタティック アドレス変換（SAT）：ローカル アドレスとグローバル アドレスを 1 対 1 マッピングします。
- ダイナミック アドレス変換：未登録の IP アドレスを、登録済み IP アドレスのプールから取得した登録済み IP アドレスにマップします。
- オーバーロード：複数の未登録 IP アドレスを、複数の異なるポートを使用して、1 つの登録済み IP アドレスにマップ（多対 1）するダイナミック NAT の一形式。この方法は、ポート アドレス変換（PAT）とも呼ばれます。PAT（NAT オーバーロード）を使用することにより、使用できる正規のグローバル IP アドレスが 1 つのみでも、数千のユーザをインターネットに接続することができます。

IP アドレス節約のために NAT を設定する方法

NAT を設定するには、次の手順を実行します。

1. NAT プールを作成します（ダイナミック NAT の場合に必要）
2. ACL を設定します
3. NAT44 ルールを作成します
4. インターフェイス上でルールを割り当てます
5. NAT 変換の最大数をセットアップします（オプション）

（注）　NAT 機能は、IOS バージョン 3.5 以降の ASR プラットフォーム上でサポートされています。NAT 機能は、IOS バージョン 12.4(24)T 以降の ISR プラットフォーム上でサポートされています。「EMS_」で始まるオブジェクトまたはエンティティに対して CLI インターフェイス経由で変更を行うことはサポートされていません。そのような変更を行うと、予期せぬ動作が発生する可能性があります。

IP プール

IP プールとは、ダイナミック NAT で使用される IP 範囲を表すデバイス オブジェクトです。NAT IP プール機能では、ダイナミック NAT で使用可能な新しいプールを作成したり、既存のプールを変更したり、デバイスからプールを削除したりできます。

IP プールの作成、編集、および削除

IP プールを作成、編集、および削除するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[NAT] > [IP Pools] を選択します。[NAT Pools] ページが表示されます。

ステップ 5　このページから、[Add IP Pool] > [IP+Prefix] ボタンまたは [IP Range + Prefix] ボタンをクリックし、名前、IP アドレス / 範囲、プレフィックス長、および説明を入力します。

ステップ 6　[Ok] をクリックして、設定を保存します。

表 6-5 に、[IP Pools] ページ上の要素を示します。

表 6-5　[IP Pools] ページ

要素	説明
Name	IP プールの名前を入力します。プールの作成後に名前を変更することはできません。
IP Address/Range	有効な IPv4 アドレスを入力します。有効な IPv4 アドレスは、ピリオド「.」で区切られた 4 オクテットで構成されます。
Prefix length	プレフィックス長を入力します。
Description	（オプション）ゾーンの説明を入力します。

ステップ 7　[Apply] ボタンをクリックして、プールをサーバ データベースに導入します。

ステップ 8　既存の IP プールを編集するには、NAT の [IP Pools] ページで次の作業を実行します。

a.　選択した IP プール パラメータ行をクリックし、そのパラメータを編集します。または

b.　IP プールを選択し、[Edit] ボタンをクリックします。選択した IP プール エンティティが編集用に開きます。プール名を除いたすべてのパラメータを編集できます。

ステップ 9　[Save] または [Apply] をクリックして、変更をサーバに保存します。

ステップ 10　既存の IP プールを削除するには、IP プールを選択し、[Delete] ボタンをクリックします。

ステップ 11　警告メッセージ上の [Ok] をクリックして、IP プールを削除します。選択した IP プールが削除されます。

NAT44

NAT44 機能では、NAT44 ルールを作成、削除、および変更できます。

NAT44 ルールの作成、編集、および削除

ここでは、NAT44 ルールの作成方法について説明します。

NAT ルールには、次の 3 つのタイプがあります。

- スタティック
- ダイナミック
- ダイナミック PAT

NAT44 ルールを作成するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　左の [Feature Selector] パネルから、[NAT] > [NAT44] を選択します。

ステップ 5　[NAT 44 Rule] ページから、[Add NAT Rule] ボタン上の下矢印アイコンをクリックします。

- [Static] をクリックしてスタティック ルールを作成します。このページ上の要素については、表 6-6 を参照してください。
- [Dynamic] をクリックして、ダイナミック NAT ルールを作成します。このページ上の要素については、表 6-7 を参照してください。
- [Dynamic PAT] をクリックして、ダイナミック PAT ルールを作成します。このページ上の要素については、表 6-8 を参照してください。

表 6-6 に、[Static Rule] ページ上の要素を示します。

表 6-6　[Static Rule] ページ

要素	説明
Direction	方向が表示されます。このリリースでは、インバウンドからアウトバウンドへの方向のみがサポートされています。
VRF	NAT 変換プロセスが実行される VRF が表示されます。デフォルト値はデフォルト VRF です。
Source A	有効な IPv4 アドレスを入力します。有効な IPv4 アドレスは、ピリオド「.」で区切られた 4 オクテットで構成されます。 • [Source A] を定義した場合は、[Source B] も定義する必要があります。 • [Source A] を定義すると、[Destination A] がデフォルトで [Any] になります。
Destination A	有効な IPv4 アドレスを入力します。有効な IPv4 アドレスは、ピリオド「.」で区切られた 4 オクテットで構成されます。 • [Destination A] を定義した場合は、[Destination B] も定義する必要があります。 • [Destination A] を定義すると、[Source A] がデフォルトで [Any] になります。
Translation	スタティック変換タイプが表示されます。
Source B	有効な IPv4 アドレスを入力します。有効な IPv4 アドレスは、ピリオド「.」で区切られた 4 オクテットで構成されます。 • [Source B] を定義した場合は、[Source A] も定義する必要があります。 • [Source B] を定義すると、[Destination B] がデフォルトで [Any] になります。
Destination B	有効な IPv4 アドレスを入力します。有効な IPv4 アドレスは、ピリオド「.」で区切られた 4 オクテットで構成されます。 • [Destination B] を定義した場合は、[Destination A] も定義する必要があります。 • [Destination B] を定義すると、[Source A] と [Source B] がデフォルトで [Any] になります。
Options	スタティック タイプ用の詳細オプションが表示されます。次を設定します。 • 埋め込まれている IP アドレスを無視するには（ペイロードなし）、[Ignore Embedded IP address] チェックボックスをオンにします。 • ポート変換をイネーブルにするには、[Enable Port Translation] チェックボックスをオンにし、次を定義します。 – TCP または UDP – 元のポート – ポート変換

表 6-7 に、[Dynamic NAT] ページ上の要素を示します。

表 6-7　[Dynamic NAT] ページ

要素	説明
Direction	方向が表示されます。このリリースでは、インバウンドからアウトバウンドへの方向のみがサポートされています。
VRF	NAT 変換プロセスが実行される VRF が表示されます。デフォルト値はデフォルト VRF です。
Source A	リストから ACL 名を選択します。 • [Source A] を定義した場合は、[Source B] も定義する必要があります。 • [Source A] を定義すると、[Destination A] がデフォルトで [Any] になります。
Destination A	リストから ACL 名を選択します。 • [Destination A] を定義した場合は、[Destination B] も定義する必要があります。 • [Destination A] を定義すると、[Source A] がデフォルトで [Any] になります。
Translation	ダイナミック NAT 変換タイプが表示されます。
Source B	ドロップダウン リストから NAT プールを選択します。 [Source B] を定義した場合は、[Source A] も定義する必要があります。 [Source B] を定義すると、[Destination B] がデフォルトで [Any] になります。
Destination B	ドロップダウン リストから NAT プールを選択します。 • [Destination B] を定義した場合は、[Destination A] も定義する必要があります。 • [Destination B] を定義すると、[Source A] と [Source B] がデフォルトで [Any] になります。
Options	ダイナミック タイプ用の詳細オプションが表示されます。 • 埋め込まれている IP アドレスを無視するには（ペイロードなし）、[Ignore Embedded IP address] チェックボックスをオンにします。 • ポート変換をイネーブルにするには、[Enable Port Translation] チェックボックスをオンにし、次を定義します。 – TCP または UDP – 元のポート – ポート変換 （注）　このオプションは、ISR デバイス上でのみサポートされます。

表 6-8 に、[Dynamic PAT] ページ上の要素を示します。

表 6-8　[Dynamic PAT] ページ

要素	説明
Direction	方向が表示されます。このリリースでは、インバウンドからアウトバンドへの方向がサポートされています。
VRF	NAT 変換プロセスが実行される VRF が表示されます。デフォルト値はデフォルト VRF です。
Source A	リストから ACL 名を選択します。
Destination A	定義されません。

表 6-8　[Dynamic PAT] ページ （続き）

要素	説明
Translation	ダイナミック PAT 変換タイプが表示されます。
Source B	リストから IP プール名を選択します。
Destination B	定義されません。
Options	ダイナミック PAT 用の詳細オプションが表示されます。[Ignores embedded IP Addresses (no-Payload)] オプションを選択します。[Yes] または [No] を選択できます。 （注）　このオプションは、ISR デバイス上でのみサポートされます。

ステップ 6　次の項目をクリックします。

- [Save]。デバイスに対する変更を保存して導入します。
- [Cancel]。保存せずに終了します。

ステップ 7　既存の NAT44 ルールを編集するには、[NAT44] ページで次の作業を実行します。

a. 選択した NAT44 ルール パラメータ行をクリックし、そのパラメータを編集します。または

b. NAT44 ルールを選択し、[Edit] ボタンをクリックします。選択した NAT44 ルール エンティティが編集用に開きます。プール名を除いたすべてのパラメータを編集できます。

ステップ 8　作成ルールに従って、送信元と宛先を変更できます。また、オプションの選択も、作成ルールに従って変更できます。

ステップ 9　[Save] または [Apply] をクリックして、変更をサーバに保存します。

ステップ 10　既存の NAT44 ルールを削除するには、ルールを選択し、[Delete] ボタンをクリックします。

ステップ 11　警告メッセージ上の [Ok] をクリックして、ルールを削除します。選択した NAT44 ルールが削除されます。

インターフェイスの管理

仮想インターフェイスは、特定の目的のため、または特定ユーザに共通の設定のための汎用設定情報に、ルータ依存の情報を加えて設定された論理インターフェイスです。

インターフェイスの設定

インターフェイスを特定のアソシエーションに割り当てるには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　左の [Feature Selector] パネルから、[NAT] > [Interfaces] を選択します。

ステップ 5　[Interface] ページで、変更するインターフェイスを選択し、VRF を入力し、ドロップダウン リストからアソシエーションを選択します。

表 6-9 に、[Interfaces] ページ上の要素を示します。

表 6-9　[Interfaces] ページ

要素	説明
Interface Name	インターフェイスの名前が表示されます。
VRF	インターフェイスが属している VRF の名前が表示されます。
Status	インターフェイスのステータスが表示されます。
Association	ドロップダウン リストからアソシエーションを選択します。オプションには、[Inside]、[Outside]、および [None] があります。

ステップ 6　次の項目をクリックします。

- [Save] または [Apply]。変更をサーバに保存します。
- [Cancel]。保存せずに終了します。

NAT MAX 変換の管理

NAT 変換のレート制限機能によって、ルータ上で同時に処理される NAT の数を制限できます。さらに、NAT MAX 機能により、NAT アドレスの使用をより詳細に制御できます。NAT 変換のレート制限機能を使用して、ウイルスやワーム、サービス拒否攻撃の影響を制限することができます。

NAT 最大変換数の制限機能では、グローバル変換の属性値を再設定できます。

NAT MAX 変換の設定

MAX 変換を設定するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　左の [Feature Selector] パネルから、[NAT] > [Max. Translation] を選択します。

ステップ 5　表 6-10 の説明に従ってパラメータ値を再設定します。

表 6-10 に、[MAX Translation] ページ上の要素を示します。

表 6-10　[MAX Translation] ページ

要素	説明
Maximum number of global translation entries	許容される NAT エントリの最大数を設定します。NAT エントリの許容数の上限は、2147483647 です。通常の NAT レート制限の範囲は 100 ～ 300 エントリです。
Maximum number of translations over all hosts	すべてのホストで許容される NAT エントリの最大数を設定します。NAT エントリの許容数の上限は、2147483647 です。通常の NAT レート制限の範囲は 100 ～ 300 エントリです。

表 6-10　[MAX Translation] ページ （続き）

要素	説明
Maximum number of translations over all VRF	すべての VRF で許容される NAT エントリの最大数を設定します。許容される NAT エントリの最大数は 2147483647 ですが、通常の NAT レート制限の範囲は 100 ～ 300 エントリです。
Maximum number of translations for ACL	指定された ACL で許容される NAT エントリの最大数を設定します。NAT エントリの許容数の上限は、214748364 です。通常の NAT レート制限の範囲は 100 ～ 300 エントリです。
Maximum number of translations for VRF	指定された VRF（複数可）で許容される NAT エントリの最大数を設定します。NAT エントリの許容数の上限は、2147483647 です。通常の NAT レート制限の範囲は 100 ～ 300 エントリです。
Maximum number of translations for host	指定されたホスト（複数可）で許容される NAT エントリの最大数を設定します。NAT エントリの許容数の上限は、214748364 です。通常の NAT レート制限の範囲は 100 ～ 300 エントリです。

ステップ 6　次の項目をクリックします。

- [Save] または [Apply]。変更をサーバに保存します。
- [Cancel]。保存せずに終了します。

ダイナミック マルチポイント VPN

DMVPN 機能では、総称ルーティング カプセル化（GRE）トンネル、IP セキュリティ（IPSec）暗号化、および Next Hop Resolution Protocol（NHRP）を組み合わせることにより、大小さまざまな規模の IPSec VPN に対応できます。

標準的な VPN 接続は、ポイントツーポイントの IPSec トンネルで 2 台のルータを接続します。DMVPN では、GRE over IPSec トンネルを使用して、中央ハブが他のリモート ルータ（スポークと呼びます）どうしを接続するネットワークを構築できます。IPSec トラフィックは、このハブを経由してネットワーク内のスポークにルーティングされます。

DMVPN の詳細については、『*Dynamic Multipoint IPsec VPNs (Using Multipoint GRE/NHRP to Scale IPsec VPNs)*』を参照してください（CCO ログイン ID が必要です）。

DMVPN の設定

Cisco Network Control System により、ルータを DMVPN ハブまたは DMVPN スポークとして設定できます。ルータは次の方法で設定できます。

ハブ

- 「ハブ アンド スポーク トポロジの設定」（P.6-18）

スポーク

- 「フルメッシュ トポロジの設定」（P.6-19）

DMVPN トンネルの作成

DMVPN トンネルを作成するには、次のパラメータを設定する必要があります。

- デバイス ロールとトポロジ タイプ
- マルチポイント GRE インターフェイス情報
- NHRP パラメータとトンネル パラメータ
- ネクスト ハブ サーバ（NHS）サーバ（オプション）

DMVPN トンネルを作成するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Security] > [DMVPN] を選択し、[Add] ボタンをクリックして DMVPN を作成します。

ステップ 5　[Device Role and Topology Type] セクションで、トポロジとデバイス ロールを選択します。オプションには、[Hub and Spoke Network]、[Full Mesh]、[Spoke]、および [Hub] があります。

ステップ 6　[Multipoint GRE Interface Information] セクションで、インターネットに接続する WAN 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。

ステップ 7　トンネル インターフェイスの IP アドレス、およびサブネット マスクを入力します。

ステップ 8　[NHRP and Tunnel Parameters] セクションで、ネットワーク ID、ホールド タイム、NHRP 認証文字列、トンネル キー、帯域幅、MTU、トンネル スループット遅延、および TCP 最大セグメント サイズの情報を入力します。

ステップ 9　[Encryption policy] フィールドで、プラス（+）のアンカー ボタンをクリックして、トランスフォーム セット プロファイルを追加します。

ステップ 10　[Transform Set Profile] ダイアログボックスで、名前を入力し、ドロップダウン リストからセキュリティ プロトコルとセキュリティ アルゴリズムの受け入れ可能な組み合わせを選択して、トランスフォーム セットを設定します。[IP Compression] をイネーブルにして、トランスフォーム セットの IP 圧縮をイネーブルにします。トランスフォーム セットのモードを選択します。[Tunnel] モードまたは [Transport] モードを選択できます。

ステップ 11　[NHS Server Information] セクションで、ハブとトンネルの物理インターフェイス用の IP アドレスと、フォールバック タイムを入力します。デバイスがクラスタをサポートする場合は、ネクスト ホップ サーバ情報を追加します（クラスタ ID、最大接続、ハブ IP アドレス、プライオリティなど）。

（注）　NHS サーバ情報は、スポーク設定の場合にのみ必要です。

ステップ 12　[Routing Information] セクションで、ルーティング情報を選択します。オプションには、[EIGR]、[RIPV2]、および [Other] があります。

（注）　ルーティング情報は、ハブ設定の場合にのみ必要です。

ステップ 13　ドロップダウン リストから既存の EIGRP 番号を選択します。あるいは、EIGRP 番号を入力します。他のプロトコルを設定するには、[Other] オプションを使用します。

表 6-11 に、[Dynamic Multipoint VPN] ページ上の要素を示します。

表 6-11　[DMVPN] ページ

要素	フィールドの説明
[Device Role and Topology] タブ	
[Hub and Spoke] オプション ボタン	[Hub and Spoke] オプション ボタンをオンにして、ハブ アンド スポーク トポロジを設定します。このトポロジでは、スポーク間のトラフィックがハブ ルータ経由でルーティングされます。
[Fully Mesh] オプション ボタン	[Fully Mesh] オプション ボタンをオンにして、フルメッシュ ネットワーク トポロジを設定します。このトポロジでは、スポークが別のスポーク デバイスに対してダイナミック トンネルを作成または確立し、作成したトンネルを使用してトラフィックを送信します。
[Spoke] オプション ボタン	[Spoke] オプション ボタンをオンにして、ルータをトポロジ内のスポークとして設定します。
[Hub] オプション ボタン	[Hub] オプション ボタンをオンにして、ルータをトポロジ内のハブとして設定します。
Multipoint GRE Interface Information	
WAN Interface	インターネットに接続する WAN 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。
Interface IP address	トンネル インターフェイスの IP アドレスを入力します。
Subnet mask	サブネット マスクを入力します。
NHRP and Tunnel Parameters	
Network ID	NHRP ネットワーク ID を入力します。このネットワーク ID は、非ブロードキャスト マルチアクセス（NBMA）ネットワークからのグローバルに固有な 32 ビットのネットワーク識別子です。範囲は 1 ～ 4294967295 です。
Hold Time	Next Hop Resolution Protocol（NHRP）NBMA アドレスが有効としてアドバタイズされる秒数を入力します。デフォルト値は 7200 秒です。
Tunnel Key	トンネル キーを入力します。トンネル キーは、特定のトンネル インターフェイスのキー ID をイネーブルにするために使用されます。値の範囲は 0 ～ 4294967295 です。
Bandwidth	意図される帯域幅をキロバイト/秒（kbps）の単位で入力します。
MTU	特定のインターフェイス上で送信される IP パケットの MTU サイズを入力します。イーサネットとシリアル インターフェイスの場合のデフォルト値は 1500 です。デフォルト値は、メディア タイプによって異なります。
Tunnel Throughput Delay	インターフェイスの遅延値を 10 マイクロ秒単位で設定します。トンネル スループット遅延は、特定のインターフェイスの遅延値を設定するために使用されます。
TCP Maximum segment Size	TCP 最大セグメント サイズをバイト単位で入力します。
IPsec Information	
Encryption policy	暗号化ポリシーを入力します。[Add] ボタンをクリックして、トランスフォーム セット プロファイルを追加します。
Transform Set Profile	
Integrity Algorithm	整合性アルゴリズムを入力します。このアルゴリズムは、ペイロードの整合性をチェックするために使用されます。
Encryption Algorithm	暗号化アルゴリズムを入力します。ペイロードの暗号化に使用されるアルゴリズムです。
Mode	モードを入力します。トラフィックを転送するモードを示します。
IP Compression	[IP Compression] チェックボックスをオンにして、ペイロードを圧縮します。
NHS Server	
Hub Physical Interface	ハブの物理インターフェイスの IP アドレスを入力します。

表 6-11　[DMVPN] ページ （続き）

要素	フィールドの説明
Hub Tunnel Interlace	ハブのトンネル インターフェイスの IP アドレスを入力します。
Routing Information	
EIGRP	[EIGRP routing information] チェックボックスをオンにします。
RIPV2	[RIPV2 routing information] チェックボックスをオンにします。
Other	[Other] チェックボックスをオンにして、他のルーティング プロトコルを選択します。
AS Number	ドロップダウン リストから既存の EIGRP 番号を選択します

ステップ 14　[Save] をクリックして、単一の NHS サーバ エントリの詳細情報とサーバのプライオリティを保存し、サーバのグループ全体を保存し、NHS クラスタ情報を保存します。NHS クラスタ情報を保存すると、NHS サーバが編集不可のフィールドに自動入力されます。

ステップ 15　設定をデバイスに保存するには、[OK] をクリックします。

ステップ 16　行った変更をルータに送信せずにすべて取り消すには、[Cancel] をクリックします。

ハブ アンド スポーク トポロジの設定

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Security] > [DMVPN] を選択し、[Add] ボタンをクリックして DMVPN トンネルを作成します。

ステップ 5　[Device Type and Topology] セクションで、トポロジとしてハブ アンド スポークを選択し、デバイス ロールとしてハブまたはスポークを選択します。

ステップ 6　ドロップダウン リストから WAN インターフェイスを選択し、トンネル インターフェイスのマルチポイント GRE IP アドレスとサブネット マスクを設定します。

ステップ 7　NHRP とトンネル インターフェイスのパラメータを設定します（IP アドレス、NHRP パラメータとマップ、MTU 値、トンネルの送信元、トンネル モード、トンネル キーなど）。

ステップ 8　デバイス間のデータ フローを保護するためのトランスフォームセットを作成します。トランスフォームには、最大で認証ヘッダー（AH）、カプセル化セキュリティ ペイロード（ESP）暗号化、ESP 認証、および圧縮の 4 つを指定できます。これらのトランスフォームにより、IPSec セキュリティ プロトコルとアルゴリズムが決まります。

ステップ 9　使用されるルーティング プロトコルを設定します。このページ上の要素については、表 6-11 を参照してください。

ステップ 10　設定をデバイスに保存するには、[Save] をクリックします。

ステップ 11　変更をデバイスに適用せずに [Create DMVPN Tunnel] ページを閉じるには、[Cancel] をクリックします。

フルメッシュ トポロジの設定

ダイナミック スポークツースポーク オプションでは、DMVPN フルメッシュ トポロジを設定できます。このトポロジでは、ルータをスポークとして設定でき、ネットワーク内の他のスポークに対して直接 IPSec トンネルを確立できます。

ハブ アンド スポーク トポロジを設定するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Security] > [DMVPN] をクリックし、[Add] ボタンをクリックしてフルメッシュ トポロジの DMVPN トンネルを作成します。

ステップ 5　[Create DMVPN Tunnel] 設定ページから、[Full Mesh] オプション ボタンを選択して、ネットワーク タイプをフル メッシュ トポロジに設定します。

ステップ 6　ハブ アンド スポーク トポロジの設定のステップ 6 ～ステップ 8 を実行します。このページ上の要素については、表 6-11 を参照してください。

ステップ 7　フルメッシュ スポーク トポロジの場合、[NHS Server Information] セクションで、ネクスト ホップ サーバ情報を追加します（ハブの物理インターフェイスの IP アドレスやハブのトンネル インターフェイスの IP アドレスなど）。

ステップ 8　設定をデバイスに保存するには、[Save] をクリックします。

ステップ 9　変更をデバイスに適用せずに [Create DMVPN Tunnel] ページを閉じるには、[Cancel] をクリックします。

クラスタの設定

クラスタを設定するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Security] > [DMVPN] をクリックし、[Add] ボタンをクリックして DMVPN トンネルを作成します。

ステップ 5　[Create DMVPN Tunnel] 設定ページから、[Spoke] オプション ボタンを選択して、デバイス ロールをスポークに設定します。

ステップ 6　ハブ アンド スポーク トポロジの設定のステップ 6 ～ステップ 8 を実行します。このページ上の要素については、表 6-11 を参照してください。

（注）　このデバイスは、15.1(2)T 以降の IOS バージョンを実行している必要があります。

ステップ 7　[Add Row] ボタンをクリックしてクラスタ関連の情報を設定し、クラスタ ID と最大接続の値を追加します。

ステップ 8　[Expand Row] ボタン（オプション ボタンの隣）をクリックし、[Add Row] ボタンをクリックして NHS サーバ情報を追加します。

ステップ 9　NHS サーバ、GRE トンネル IP アドレス、およびこの NHS サーバのプライオリティを入力します。[Save] ボタンをクリックして、NHS サーバ エントリの設定を保存します。

ステップ 10　[Save] ボタンをクリックして、NHS サーバ グループ情報を保存します。

ステップ 11　[Save] ボタンをもう一度クリックして、クラスタ設定の NHS グループ情報を保存します。NHS サーバ IP アドレスがテーブルに自動的に入力されます。

DMVPN の編集

既存の DMVPN トンネルを編集するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Security] > [DMVPN] を選択します。使用可能なトンネルが表示されます。

ステップ 5　トンネルを選択し、[Edit] ボタンをクリックします。[Edit DMVPN Tunnel] ページが表示されます。

ステップ 6　[Edit DMVPN Tunnel] ページから、DMVPN パラメータを編集できます。

[Edit DMVPN Tunnel] ページ上の要素については、表 6-11 を参照してください。

ステップ 7　編集した DMVPN トンネル設定をデバイスに送信するには、[Ok] をクリックします。

ステップ 8　設定をデバイスに適用せずに [Edit DMVPN Tunnel] ページを閉じるには、[Cancel] をクリックします。

DMVPN の削除

既存の DMVPN トンネルを削除するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　DMVPN トンネルを削除するデバイスをリストから選択します。デバイスが追加されていない場合は、[Add] ボタンをクリックしてデバイスを追加します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。左側に [Feature Selector] パネルが表示されます。

ステップ 4　左の [Feature Selector] パネルから、[Security] > [DMVPN] を選択します。使用可能なトンネルが表示されます。

ステップ 5　トンネルを選択し、[Delete] ボタンをクリックします。

選択したトンネルを削除するには、警告メッセージ上の [Yes] をクリックします。[Edit DMVPN Tunnel] ページ上の要素については、表 6-11 を参照してください。

ステップ 6　選択したトンネルを削除しない場合は、警告メッセージ上の [No] をクリックします。

ステップ 7　行った変更をルータに送信せずにすべて取り消すには、[Cancel] をクリックします。

GETVPN

Group Encrypted Transport VPN（GETVPN）の導入には、3 つの主要コンポーネントとして、キー サーバ（KS）、グループ メンバー（GM）、およびグループ ドメイン オブ インタープリテーション（GDOI）プロトコルが使用されます。GM はトラフィックの暗号化または復号化を実行し、KS は暗号キーをすべてのグループ メンバーに配布します。KS は、所定の有効期間に対してデータ暗号キーを 1 つだけ決定します。すべての GM が同じキーを使用するため、どの GM でも、他の GM で暗号化されたトラフィックを復号化できます。GDOI プロトコルは、グループ キーとグループ セキュリティ アソシエーション（SA）管理のために、GM と KS の間で使用されます。GETVPN の導入には、少なくとも 1 台の KS が必要です。

従来型の IPSec 暗号化ソリューションとは異なり、GETVPN ではグループ SA という概念が使用されます。GETVPN グループ内のすべてのメンバーは、共通の暗号化ポリシーと共有 SA を使用して互いに通信できます。したがって、GM 間の IPSec をピアツーピアでネゴシエートする必要はなく、その結果、GM ルータに対するリソース負荷が軽減されます。

グループ メンバー

GM は、キー サーバに登録して、グループ内のデータ トラフィックを暗号化するのに必要な IPSec SA を取得します。GM は、グループ識別番号を KS に渡して、このグループの個別のポリシーとキーを取得します。これらのキーは、現在の IPSec SA が期限切れになる前に、KS によって定期的に更新されます。その結果、トラフィックのロスがなくなります。

キー サーバ

KS は、セキュリティ ポリシーのメンテナンス、GM の認証、およびトラフィックの暗号化用のセッション キーの提供を担当します。KS は、個々の GM を登録時に認証します。登録成功後、GM は、グループ SA に参加できるようになります。

GM はいつでも登録可能で、最新のポリシーおよびキーを受信できます。GM が KS に登録するとき、KS は GM のグループ識別番号を確認します。この識別番号が有効で、なおかつ GM から有効なインターネット キー交換（IKE）クレデンシャルが提供されると、KS は、SA ポリシーとキーをそのグループ メンバーに送信します。

GM が KS から受信するキーには、キー暗号キー（KEK）とトラフィック暗号キー（TEK）の 2 種類があります。TEK は、同じグループ内のグループ メンバーがデータの暗号化に使用する IPSec SA の一部になります。KEK は、KS と GM の間のキー再生成メッセージを保護するために使用されます。

KS は、近々 IPSec SA の期限が切れる場合や、KS でセキュリティ ポリシーが変更された場合に、キー再生成メッセージを送信します。キー再生成時には、マルチキャスト転送またはユニキャスト転送を使用してキーを配布できます。マルチキャスト方式の方が、キーを各グループ メンバーに個別に送信する必要がないので、よりスケーラブルです。マルチキャスト キー再生成方式では、ユニキャストの場合とは異なり、KS が、キー再生成の受信成功についての確認応答を GM から受け取ることはありません。ユニキャスト キー再生成方式では、キー再生成に対する確認応答が特定の GM から 3 回連続してなければ、KS はその GM をデータベースから削除します。

GDOI プロトコルは、グループ キーとグループ SA 管理に使用されます。GDOI では、GM と KS を認証するために、Internet Security Association Key Management Protocol（ISAKMP）が使用されます。GETVPN には、RSA シグニチャ（証明書）や事前共有キーなどの標準的な ISAKMP 認証方式をすべて使用できます。

GETVPN の詳細については、http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/deployment_guide_c07_554713.html を参照してください。

GETVPN の設定

Cisco Network Control System により、GETVPN を設定できます。GETVPN を設定するには、次を設定する必要があります。

- グループ メンバー
- キー サーバ

GETVPN グループ メンバーの作成

[Add GroupMember] 設定ページを使用して、GETVPN グループ メンバーを設定します。

GETVPN グループ メンバーを作成するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを追加し、デバイスを設定します。画面の下部にデバイスの詳細が表示されます。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Security] > [GETVPN-GroupMember] をクリックし、[Add] ボタンをクリックして GET VPN グループ メンバーを作成します。

ステップ 5　[Add GroupMember] ダイアログボックスで、[General] タブを選択し、グループ名とグループ アイデンティティを入力します。ドロップダウン リストから登録インターフェイスを選択します。

ステップ 6　プライマリ キー サーバとセカンダリ キー サーバの IP アドレスを入力します。[Add Row] ボタンまたは [Delete] ボタンをクリックして、セカンダリ キー サーバの IP アドレスを追加または削除します。[Row] または [Field] をクリックして、セカンダリ キー サーバの IP アドレスを編集します。

ステップ 7　次の項目をクリックします。

- [Save]。設定を保存します。
- [Cancel]。変更を保存せずに終了します。

ステップ 8　[Add Group Member] ダイアログボックスで、[Advanced] タブを選択し、ドロップダウン リストからローカル例外 ACL とフェール クローズ ACL を選択します。

ステップ 9　[Enable Passive SA] チェックボックスをオンにして、パッシブ SA をイネーブルにします。このオプションを使用して、このグループ メンバーに対してパッシブ SA モードを有効にします。

表 6-12 に、[GETVPN GroupMember] ページ上の要素を示します。

表 6-12　[GETVPN Group Member] ページ

要素	フィールドの説明
General	

表 6-12　[GETVPN Group Member] ページ （続き）

要素	フィールドの説明
Group Name	GETVPN グループの名前を入力します。
Group Identity	GETVPN グループの一意のアイデンティティを入力します。これには、番号または IP アドレスを使用できます。範囲は 0 ～ 2147483647 です。
Registration Interface	クリプト マップを関連付ける必要のある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。
Primary Key Server	クライアントが接続するプライマリ キー サーバの IP アドレスを指定します。プライマリ キー サーバは、グループ ポリシーの作成、およびすべてのグループ メンバーへのそれらの配布を担当し、セカンダリ キー サーバと定期的に同期します。プライオリティの最も高いサーバが、プライマリ キー サーバとして選択されます。
Secondary Key Server	グループ メンバーがプライマリ キー サーバの登録失敗時にフォール バックするセカンダリ キー サーバの IP アドレスを指定します。グループ メンバーは、すべてのセカンダリ キー サーバのリストから使用可能な任意のキー サーバに登録するように設定できます。グループ メンバーの設定に応じて、登録の順序が決定されます。最初に定義されたキー サーバに対して接続が試みられ、その後、定義された順番でキー サーバへの接続が試みられます。
Add Row	[Add Row] ボタンをクリックして、セカンダリ キー サーバを追加します。
Delete	[Delete] ボタンをクリックして、セカンダリ キー サーバを削除します。
[Advanced] タブ	
Local Exception ACL	暗号化から除外されるトラフィックを示す ACL を選択します。
Fail Close ACL	グループ メンバーがキー サーバに登録されるまでの間、クリア テキストで送信されるトラフィックを示す ACL を選択します。フェール クローズ機能が設定されると、グループ メンバーを通過するすべてのトラフィックは、そのグループ メンバーが正常に登録されるまでドロップされます。グループ メンバーが正常に登録され、SA がダウンロードされると、この機能は自動的に無効になります。
Enable Passive SA	このオプションを使用して、グループ メンバーに対してパッシブ SA モードを有効にします。パッシブ SA モードは、キー サーバ上の受信専用 SA オプションを無効にし、すべての発信トラフィックを暗号化します。

ステップ 10　次の項目をクリックします。

- [Ok]。テーブルにグループ メンバーを追加します。コマンドを表示するには、[CLI] プレビューをクリックします。スケジュールの導入後、設定がデバイス上で適用されます。
- [Cancel]。行った変更をルータに送信せずにすべて取り消します。
- [Close]。ページを閉じます。

GETVPN キー サーバの作成

[Add KeyServer] 設定ページを使用して、GETVPN キー サーバを設定します。

GETVPN キー サーバを作成するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを追加し、デバイスを設定します。画面の下部にデバイスの詳細が表示されます。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　左の [Feature Selector] パネルから、[Security] > [GETVPN-KeyServer] をクリックし、[Add] ボタンをクリックして GETVPN キー サーバを作成します。

ステップ 5　[Add Key Server] ダイアログボックスで、[General] タブを選択し、このキー サーバのグループ名、グループ アイデンティティ、WAN IP アドレス、およびプライオリティを入力します。

ステップ 6　協調キー サーバの IP アドレスを入力します。[Add Row] ボタンまたは [Delete] ボタンをクリックして、協調キー サーバの IP アドレスを追加または削除します。[Row] または [Field] をクリックし、IP アドレスを編集します。

ステップ 7　[Add KeyServer] ダイアログボックスで、[Rekey] タブを選択し、ドロップダウン リストから配布方式を選択します。マルチキャスト IP アドレス、KEK ライフタイム、TEK ライフタイム、キーの再送信、キー再生成の暗号化用の RSA キー、キー再生成の暗号化方式などの情報を入力します。

ステップ 8　[Add KeyServer] ダイアログボックスで、[GETVPN Traffic] タブを選択し、暗号化されるトラフィック、暗号化ポリシー、およびアンチ リプレイを入力します。

表 6-13 に、[GETVPN KeyServer] ページ上の要素を示します。

表 6-13　[GETVPN Key Server] ページ

要素	フィールドの説明
General	
Group Name	GETVPN グループの名前を入力します。
Group Identity	GETVPN グループの一意のアイデンティティを入力します。これには、番号または IP アドレスを使用できます。範囲は 0 ～ 2147483647 です。
WAN IP Address	WAN IP アドレスを入力します。このキー サーバが関連付けられるインターフェイスの IP アドレスになります。
Co-operative Key Server	グループ メンバーがプライマリ キー サーバの登録失敗時にフォール バックする協調キー サーバの IP アドレスを指定します。グループ メンバーは、すべてのセカンダリ キー サーバのリストから使用可能な任意のキー サーバに登録するように設定できます。グループ メンバーの設定に応じて、登録の順序が決定されます。最初に定義されたキー サーバに対して接続が試みられ、その後、定義された順番でキー サーバへの接続が試みられます。
Add Row	[Add Row] ボタンをクリックして、協調キー サーバを追加します。
Delete Row	[Delete Row] ボタンをクリックして、協調キー サーバを削除します。
Rekey	
Distribution Method	ドロップダウン リストから配布方式を選択します。配布方式は、キー再生成情報をキー サーバからグループ メンバーに送信するために使用されます。[Unicast] または [Multicast] を選択できます。
Multicast IP Address	配信方式にマルチキャストを選択した場合、キー再生成を送信する必要のあるマルチキャスト アドレスを指定します。
KEK Lifetime	KEK ライフタイムを秒単位で入力します。範囲は 120 ～ 86400 です。
TEK Lifetime	TEK ライフタイムを秒単位で入力します。範囲は 120 ～ 86400 です。
Retransmit Key	キー再生成の再送信を行う頻度と期間を秒単位で入力します。
RSA Key for Rekey Encryption	キー再生成の情報を暗号化するために使用される RSA キーの詳細情報を入力します。

表 6-13　[GETVPN Key Server] ページ （続き）

要素	フィールドの説明
Rekey Encryption Method	ドロップダウン リストから暗号化アルゴリズムを選択します。この暗号化アルゴリズムは、キーを暗号化するために使用されます。 • [AES-128] : 128 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES-192] : 192 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES-256] : 256 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [DES] : 56 ビット キーを使用するデータ暗号規格に従って暗号化を実行します。 • [3DES] : 56 ビット キーを使用して暗号化を 3 回実行します。3DES は DES よりも強力なセキュリティを確保しますが、暗号化と復号化に多くの処理を必要とします。AES に比べるとセキュリティは低くなります。このオプションを使用するには 3DES のライセンスが必要です。
GETVPN Traffic	
Traffic to Encrypt	ドロップダウン リストから、暗号化が必要な参加者間のトラフィックを示す ACL を選択します。このアクセス リストにより、暗号化されるトラフィックが決定されます。「permit」行に一致するトラフィックのみが暗号化されます。 **（注）** 暗号セッションがアップ状態でなくても常に許可される一部のトラフィックは暗号化しないでください。
Encryption Policy	ドロップダウン リストから、トラフィックの暗号化に使用されるトランスフォーム セットを選択します。ピア間のトラフィックを暗号化するために使用されるトランスフォーム セットをテーブルから追加します。
Anti Replay	時間ベースまたはカウンタベースのアンチ リプレイ オプションを選択します。

ステップ 9　次の項目をクリックします。

- [Ok]。テーブルにグループ メンバーを追加します。コマンドを表示するには、[CLI] プレビューをクリックします。スケジュールの導入後、設定がデバイス上で適用されます。
- [Cancel]。行った変更をルータに送信せずにすべて取り消します。

ステップ 10　[Close] をクリックしてページを閉じます。

GET VPN グループ メンバーまたはキー サーバの編集

既存の GETVPN グループ メンバーまたは GETVPN キー サーバを編集するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを追加し、デバイスを設定します。画面の下部にデバイスの詳細が表示されます。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Security] > [GETVPN-Group Member] または [GETVPN-KeyServer] を選択します。[GETVPN-GroupMember] または [GETVPN-KeyServer] サマリー ページが表示されます。

ステップ 5　GETVPN サマリー ページから、グループ名を選択し、[Edit] をクリックします。[Edit GETVPN-GroupMember] または [Edit GETVPN-Keyserver] ページが表示されます。

ステップ 6　[Edit GETVPN-GroupMember] または [Edit GETVPN-KeyServer] ページから、GETVPN パラメータを編集できます。

[GETVPN-GroupMember] または [GETVPN-Keyserver] ページ上の要素については、表 6-12 と表 6-13 を参照してください。

ステップ 7　次の項目をクリックします。

- [Ok]。設定を保存します。
- [Cancel]。行った変更をルータに送信せずにすべて取り消します。

ステップ 8　[Close] をクリックしてページを閉じます。

GETVPN グループ メンバーまたはキー サーバの削除

既存の GETVPN グループ メンバーまたは GETVPN キー サーバを削除するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを追加し、デバイスを設定します。画面の下部にデバイスの詳細が表示されます。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] ペインから、[Security] > [GETVPN-Group Member] または [GETVPN-KeyServer] を選択します。[GETVPN-GroupMember] または [GETVPN-KeyServer] サマリー ページが表示されます。

ステップ 5　GETVPN サマリー ページから、グループ名を選択し、[Delete] をクリックします。[GETVPN-GroupMember] または [GETVPN-KeyServer] ページ上の要素については、表 6-12 と表 6-13 を参照してください。

ステップ 6　次の項目をクリックします。

- [Ok]。設定を保存します。
- [Cancel]。行った変更をルータに送信せずにすべて取り消します。

ステップ 7　[Close] をクリックしてページを閉じます。

VPN コンポーネント

主要な VPN コンポーネントは次のとおりです。

- 「IKE ポリシー」（P.6-27）
- 「IKE 設定」（P.6-29）
- 「IPsec プロファイル」（P.6-30）

- 「事前共有キー」（P.6-32）
- 「RSA キー」（P.6-32）
- 「トランスフォーム セット」（P.6-34）

IKE ポリシー

インターネット キー交換（IKE）は、安全で認証された通信を手配するための標準方式です。IKE は、ネットワーク上の 2 つのホスト間にセッション キー（および関連する暗号化とネットワーキング設定）を確立します。IKE ポリシーは、認証中にピアのアイデンティティを保護します。

IKE ネゴシエーションは保護される必要があります。そのため、各 IKE ネゴシエーションは、それぞれのピアが共通（共有）の IKE ポリシーに合意してから開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。2 つのピアがポリシーに合意した後、そのポリシーのセキュリティ パラメータは、各ピアに確立されたセキュリティ アソシエーションによって識別されます。これらのセキュリティ アソシエーションは、ネゴシエーション中の後続のすべての IKE トラフィックに適用されます。

IKE ネゴシエーションが開始されると、IKE は、両ピア上で同一の IKE ポリシーを検索します。ネゴシエーションを開始したピアがすべてのポリシーをリモート ピアに送信し、リモート ピアの方では一致するポリシーを探そうとします。リモート ピアは、相手側ピアから受信したすべてのポリシーと自身の最優先ポリシーを比較することにより、一致しているポリシーを検索します。一致するポリシーが見つかるまで、リモート ピアはプライオリティが高い順に各ポリシーをチェックします。2 つのピアのポリシーが一致するのは、2 つのピアが同じ暗号化、ハッシュ、認証、Diffie-Hellman（D-H）パラメータの各値を持ち、リモート ピアのポリシーに指定されているライフタイムが、比較しているポリシーのライフタイム以下の場合です。ライフタイムが等しくない場合は、短い方の（リモート ピアのポリシーの）ライフタイムが使用されます。

IKE ポリシーの作成、編集、および削除

IKE ポリシー機能では、IKE ポリシーを作成、編集、および削除できます。

IKE ポリシーを作成、編集、または削除するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択してから、デバイスを選択するか、[Add] をクリックして新しいデバイスを追加し、デバイスを設定します。画面の下部にデバイスの詳細が表示されます。

ステップ 2　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 3　[Feature Selector] パネルから、[Security] > [VPN Components] > [IKE Policies] をクリックし、[Add Row] ボタンをクリックして IKE ポリシーを作成します。

ステップ 4　[IKE Policies] ページで、プライオリティ、認証、D-H グループ、暗号化、ハッシュ、およびライフタイムを入力します。

ステップ 5　IKE ポリシー パラメータを編集するには、[Field] をクリックし、その IKE ポリシーのパラメータを編集します。

ステップ 6　IKE ポリシーを削除するには、リストから IKE ポリシーを選択し、[Delete] ボタンをクリックします。

表 6-14 に、[IKE Policies] ページ上の要素を示します。

表 6-14　[IKE Policies] ページ

要素	説明
IKE Policies	

表 6-14　[IKE Policies] ページ （続き）

要素	説明
Priority	IKE プロポーザルのプライオリティ値を入力します。このプライオリティ値によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエートする 2 つのピアを比較することで、IKE プロポーザルの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、デバイスは、次に低いプライオリティ番号を持つポリシーで定義されているパラメータの使用を試行します。 範囲は 1 ～ 10000 です。値が小さいほど、プライオリティが高くなります。
Authentication	ドロップダウン リストから事前共有キーまたは RSA シグニチャを選択します。 • [Pre-SHARE] : 事前共有キーを使用して認証が実施されます。 • [RSA_SIG] : デジタル署名を使用して認証が実施されます。
Encryption	ドロップダウン リストから暗号化アルゴリズムを選択します。 • [AES-128] : 128 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES-192] : 192 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES-256] : 256 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [DES] : 56 ビット キーを使用するデータ暗号規格に従って暗号化を実行します。 • [3DES] : 56 ビット キーを使用して暗号化を 3 回実行します。3DES は DES よりも強力なセキュリティを確保しますが、暗号化と復号化に多くの処理を必要とします。AES に比べるとセキュリティは低くなります。このオプションを使用するには 3DES のライセンスが必要です。
Diffie-Hellman Group	ドロップダウン リストから D-H グループ アルゴリズムを選択します。 Diffie-Hellman グループは、2 つの IPsec ピア間で共有秘密を利用する際に、相手への共有秘密の送信をなくすために使用されます。係数が大きいほど、セキュリティが高くなりますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。オプションは次のとおりです。 • [1] : Diffie-Hellman グループ 1（768 ビット係数）。 • [2] : Diffie-Hellman グループ 2（1024 ビット係数）。 • [5] : Diffie-Hellman グループ 5（1536 ビット係数。128 ビット キーの保護に推奨される）。
Hash	ドロップダウン リストから、IKE プロポーザルで使用されるハッシュ アルゴリズムを選択します。このハッシュ アルゴリズムによって、メッセージの整合性の確保に使用されるメッセージ ダイジェストが作成されます。次のオプションがあります。 • [SHA (Secure Hash Algorithm)] : 160 ビットのダイジェストを生成します。SHA には、ブルートフォース アタックに対して、MD5 よりも高い耐性が備えられています。 • [MD5 (Message Digest 5)] : 128 ビットのダイジェストを生成します。MD5 では、処理時間が SHA よりも少なくなります。

表 6-14　[IKE Policies] ページ （続き）

要素	説明
Lifetime	セキュリティ アソシエーション（SA）のライフタイム（秒単位）。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエートを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。 範囲は 60 ～ 86400 秒です。デフォルト値は、86400 です。

ステップ 7　次の項目をクリックします。

- [Save]。設定を保存します。
- [Cancel]。変更を保存せずに終了します。
- もう一度 [Save]。CLI コマンドを生成します。

IKE 設定

IKE 設定機能では、ピア ルータに対して IKE をグローバルにイネーブルにできます。

IKE 設定の作成

IKE ポリシーをイネーブルにし、IKE にアグレッシブ モードを設定するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択してから、デバイスを選択するか、[Add] をクリックして新しいデバイスを追加し、デバイスを設定します。画面の下部にデバイスの詳細が表示されます。

ステップ 2　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 3　[Feature Selector] パネルから、[Security] > [VPN Components] > [IKE Settings] をクリックします。

ステップ 4　[Enable IKE] チェックボックスと [Enable Aggressive Mode] チェックボックスをオンにして、IKE ポリシーとアグレッシブ モードをイネーブルにします。

ステップ 5　ドロップダウン リストから IKE アイデンティティを選択します。

ステップ 6　デッド ピア検知キープアライブとデッド ピア検知リトライを秒単位で入力します。

表 6-15 に、[IKE Settings] ページ上の要素を示します。

表 6-15　[IKE Settings] ページ

要素	説明
IKE Settings	

表 6-15　[IKE Settings] ページ （続き）

要素	説明
Enable IKE	[Enable IKE] チェックボックスをオンにして、IKE をグローバルにイネーブルにします。デフォルトでは、IKE はイネーブルです。個々のインターフェイスに対して IKE をイネーブルにする必要はありません。ルータにあるすべてのインターフェイスに対して IKE をグローバルにイネーブルにできます。 IP セキュリティ（IPSec）の実装に IKE を使用しない場合は、すべての IPSec ピアに対して IKE をディセーブルにできます。1 台のピアに対して IKE をディセーブルにする場合は、すべての IPSec ピアに対して IKE をディセーブルにする必要があります。
Enable Aggressive Mode	[Enable Aggressive Mode] チェックボックスをオンにして、Internet Security Association and Key Management Protocol（ISAKMP）アグレッシブ モードをイネーブルにします。アグレッシブ モードをディセーブルにすると、デバイスに対するすべてのアグレッシブ モード要求とデバイスによって行われるすべてのアグレッシブ モード要求がブロックされます。
IKE Identity	ドロップダウン リストから ISAKMP アイデンティティを選択します。オプションには、[IP address]、[Distinguished Name]、および [HostName] があります。事前共有キーまたは RSA シグニチャ認証を指定する場合は、ISAKMP アイデンティティを必ず設定します。原則として、各ピアのアイデンティティはすべて同じ方法で（IP アドレスまたはホスト名で）設定する必要があります。 • [IP Address] : ISAKMP アイデンティティを、IKE ネゴシエーション時のリモート ピアとの通信に使用されるインターフェイスの IP アドレスに設定します。 • [Distinguished Name] : ISAKMP アイデンティティを、ルータ証明書の識別名（DN）に設定します。 • [Host Name] : ISAKMP アイデンティティを、ドメイン名が連結されたホスト名に設定します（myhost.example.com など）。
Dead Peer Detection Keepalive	ゲートウェイがピアに DPD メッセージを送信できるようにします。DPD は、ルータがインターネット キー交換（IKE）ピアの稼動状況を照会できるようにするキープアライブ方式です。 DPD メッセージの送信間隔の秒数を [DPD Keepalive] フィールドに指定します。範囲は 10 ～ 3600 秒です。
Dead Peer Detection Retry	DPD メッセージが失敗したときに再試行するまでの秒数を [DPD Retry] に指定します。範囲は 2 ～ 60 秒です。

ステップ 7　次の項目をクリックします。

- [Save]。設定を保存します。
- [Refresh]。ページを更新します。

IPsec プロファイル

IPsec プロファイル（ISAKMP プロファイルとも呼ばれる）により、1 つ以上の IPSec トンネルと関連付けることが可能な一連の IKE パラメータを定義できます。IPsec プロファイルでは、アイデンティティ照合基準方式によって一意に識別される着信 IPSec 接続に対してパラメータが適用されます。これ

らの基準は、着信 IKE 接続によって提示される IKE アイデンティティに基づきます。このアイデンティティには、IP アドレス、完全修飾ドメイン名（FQDN）、およびグループ（バーチャル プライベート ネットワーク（VPN）リモート クライアント グルーピング）が含まれます。

IPsec プロファイルの作成、編集、および削除

IKE プロファイル機能では、IPSec プロファイルを作成、編集、および削除できます。

IPsec プロファイルを作成、編集、または削除するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択してから、デバイスを選択するか、[Add] をクリックして新しいデバイスを追加し、デバイスを設定します。画面の下部にデバイスの詳細が表示されます。

ステップ 2　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 3　[Feature Selector] パネルから、[Security] > [VPN Components] > [IPsec Profile] をクリックし、[Add Row] ボタンをクリックして IPsec プロファイルを作成します。

ステップ 4　[IPsec Profile] ページで、名前、説明、トランスフォーム セット、IPsec SA ライフタイムなどの情報を入力します。

ステップ 5　IPsec プロファイル パラメータを編集するには、[Field] をクリックし、その IPsec プロファイルのパラメータを編集します。

ステップ 6　IPsec プロファイルを削除するには、リストから IPsec プロファイルを選択し、[Delete] ボタンをクリックします。

表 6-16 に、[IPsec Profile] ページ上の要素を示します。

表 6-16　[IPSec Profile] ページ

要素	説明
Name	この IPsec プロファイルの名前を入力します。プロファイルを編集するときは、IPsec プロファイルの名前を編集することはできません。
Description	追加時または編集時に IPsec プロファイルの説明を追加します。
Transform Sets	リストからトランスフォーム セットを選択します。このルータに設定されているトランスフォーム セットが表示されます。 トランスフォーム セットは、特定のセキュリティ プロトコルとアルゴリズムを組み合わせたものです。IPSec セキュリティ アソシエーションのネゴシエーション中に、ピアは特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。トランスフォームには、特定のセキュリティ プロトコルとそれに対応するアルゴリズムが記述されています。
IPsec SA Lifetime	IPSec SA ライフタイムを入力します。設定された時間が経過すると、新しい SA が確立されます。秒単位の時間を入力します。範囲は 120 ～ 86400 です。

ステップ 7　次の項目をクリックします。

- [Save]。設定を保存します。
- [Cancel]。変更を保存せずに終了します。
- もう一度 [Save]。CLI コマンドを生成します。

事前共有キー

事前共有キー機能では、2 つのピア間で秘密キーを共有できます。この機能は、認証フェーズ中に IKE で使用されます。

事前共有キーの作成、編集、および削除

事前共有キーを作成、編集、または削除するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択してから、デバイスを選択するか、[Add] をクリックして新しいデバイスを追加し、デバイスを設定します。画面の下部にデバイスの詳細が表示されます。

ステップ 2　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 3　[Feature Selector] パネルから、[Security] > [VPN Components] > [Pre-Shared Keys] をクリックし、[Add Row] ボタンをクリックして事前共有キーを作成します。

ステップ 4　[Pre-Shared Keys] ページで、IP アドレス、ホスト名、サブネット マスク、および事前共有キーを入力します。

ステップ 5　事前共有キー パラメータを編集するには、[Field] をクリックし、その事前共有キーのパラメータを編集します。

ステップ 6　事前共有キーを削除するには、リストから事前共有キーを選択し、[Delete] ボタンをクリックします。

表 6-17 に、[Pre-Shared Keys] ページ上の要素を示します。

表 6-17　[Pre-Shared Keys] ページ

要素	説明
IP Address / Host Name	リモート ピアの IP アドレスまたはホスト名を入力します。
Subnet Mask	サブネット マスクを入力します。
Pre-shared Keys	事前共有キーを入力し、確認のためにその事前共有キーをもう一度入力します。

ステップ 7　次の項目をクリックします。

- [Save]。設定を保存します。
- [Cancel]。変更を保存せずに終了します。
- もう一度 [Save]。設定を保存し、CLI コマンドを生成します。

RSA キー

RSA キー ペアは、公開キーと秘密キーで構成されます。公開キー インフラストラクチャ（PKI）を設定する場合、証明書登録要求に公開キーを含める必要があります。証明書が付与された後、ピアが公開キーを使用して、ルータに送信されるデータを暗号化できるように、公開キーが証明書に組み込まれます。秘密キーはルータに保持され、ピアによって送信されたデータの復号化と、ピアとネゴシエーションするときの、トランザクションのデジタル署名に使用されます。

RSA キー ペアには、キーのモジュラス値が含まれています。モジュラス値に応じて、RSA キーのサイズが決まります。モジュラス値が大きいほど、RSA キーの安全性が高まります。ただし、モジュラス値が大きくなると、キーの生成にかかる時間が長くなり、キーのサイズが大きくなると暗号化処理および復号化処理にかかる時間が長くなります。

RSA キーの作成、インポート、エクスポート、および削除

RSA キーを作成、エクスポート、インポート、または削除するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択してから、デバイスを選択するか、[Add] をクリックして新しいデバイスを追加し、デバイスを設定します。画面の下部にデバイスの詳細が表示されます。

ステップ 2　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 3　[Feature Selector] パネルから、[Security] > [VPN Components] > [RSAKeys] をクリックし、[Add Row] ボタンをクリックして RSA キーを作成します。

ステップ 4　[Add RSA Keys] ダイアログボックスが表示されます。

ステップ 5　[Add RSA Keys] ダイアログボックスで、ラベル、モジュラス、およびタイプを入力します。

ステップ 6　[Make the Key exportable] チェックボックスをオンにして、RSA をエクスポート可能なキーとして生成します。

ステップ 7　次の項目をクリックします。

- [OK]。設定を保存します。
- [Cancel]。変更を保存せずに終了します。

ステップ 8　RSA キーをインポートするには、[Import] ボタンをクリックします。[Import RSA Key] ダイアログボックスが表示されます。

ステップ 9　[Import RSA Key] ダイアログボックスで、RSA キーのラベル、キー タイプ、およびキーを復号化するパスワードを入力します。キー タイプが汎用キー、シグニチャ、または暗号化の場合は、保存された公開キーと秘密キーのデータをコピー アンド ペーストします。用途キーをインポートするには、シグニチャ キーと暗号化キーの両方の公開キーと秘密キーのデータを入力します。

ステップ 10　次の項目をクリックします。

- [Import]。RSA キーをインポートします。
- [Close]。変更内容を保存せずに終了します。

ステップ 11　RSA キーをエクスポートするには、リストから RSA キーを選択し、[Export] ボタンをクリックします。[Export RSA Key Pair] ダイアログボックスが表示されます。

ステップ 12　[Export RSA Key Pair] ダイアログボックスで、RSA キーを暗号化するパスワードを入力し、ドロップダウン リストから暗号化アルゴリズムを選択します。

表 6-18 に、[RSA Keys] ページ上の要素を示します。

表 6-18　[RSA Keys] ページ

要素	説明
RSA Keys	
Label	キー ペアの名前を入力します。

表 6-18　[RSA Keys] ページ （続き）

要素	説明
Modulus	キーのモジュラス値を入力します。512 ～ 1024 のモジュラス値の場合、64 の倍数となる整数値を入力します。1024 よりも大きい値が必要な場合は、1536 または 2048 を入力できます。512 より大きい値を入力すると、キー生成に 1 分以上かかる場合があります。 モジュラス値に応じて、キーのサイズが決まります。モジュラス値が大きいほど、キーの安全性が高まります。ただし、モジュラス値が大きくなると、キーの生成にかかる時間が長くなり、キーのサイズが大きくなると暗号化処理および復号化処理にかかる時間が長くなります。
Type	生成される RSA キーのタイプを選択します。オプションには、[General Purpose]、[Usages Keys]、[Encryption Keys]、および [Signature Keys] があります。
Make Key Exportable	[Make the Key exportable] チェックボックスをオンにして、RSA キーをエクスポート可能なキーとして生成し、別の場所に保存します。
Import RSA Key	
Decryption Password	復号化パスワードを入力します。
Key Type	ドロップダウン リストから、インポートされるキーのタイプを選択します。オプションには、[General purpose]、[Usages keys]、[Encryption Keys]、および [Signature keys] があります。
PEM-formatted Public Key or Certificate	PEM 形式の公開キーまたは証明書を入力します。キーのエクスポート時に生成された公開キー データ。
PEM-formatted Encrypted Private Key	PEM 形式の暗号化された秘密キーを入力します。キーのエクスポート時に生成された秘密キー データ。
Export RSA Key	
Encryption Password	暗号化パスワードを入力してください。
Encryption Algorithm	暗号化アルゴリズムを選択します。

ステップ 13　次の項目をクリックします。

- [OK]。エクスポートされたキーを表示します。
- [Cancel]。変更を保存せずに終了します。

ステップ 14　RSA キーを削除するには、リストから RSA キーを選択し、[Delete] ボタンをクリックします。

トランスフォーム セット

トランスフォーム セットは、Upset で保護されたトラフィックに適用される、セキュリティ プロトコル、アルゴリズム、およびその他の設定の有効な組み合わせです。IPSec セキュリティ アソシエーションのネゴシエーション中に、両ピアは、特定のデータ フローを保護するときに特定のトランスフォーム セットを使用することに合意します。

トランスフォーム セットの作成、編集、および削除

トランスフォーム セットを作成、編集、または削除するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択してから、デバイスを選択するか、[Add] をクリックして新しいデバイスを追加し、デバイスを設定します。画面の下部にデバイスの詳細が表示されます。

ステップ 2　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 3　[Feature Selector] パネルから、[Security] > [VPN Components] > [Transform Sets] をクリックし、[Add Row] ボタンをクリックしてトランスフォーム セットを作成します。

ステップ 4　[Transform Sets] ページで、名前を入力し、セキュリティ プロトコルとアルゴリズムの受け入れ可能な組み合わせを選択して、トランスフォーム セットを設定します。トランスフォーム セットのモードを指定します。[Tunnel] モードまたは [Transport] モードを選択できます。

ステップ 5　トランスフォーム セット パラメータを編集するには、[Field] をクリックし、そのトランスフォーム セットのパラメータを編集します。

ステップ 6　トランスフォーム セットを削除するには、リストからトランスフォーム セットを選択し、[Delete] ボタンをクリックします。

表 6-19 に、[Transform Set] ページ上の要素を示します。

表 6-19　[Transform Set] ページ

要素	説明
Name	トランスフォーム セットの名前を入力します。
ESP Encryption Algorithm	ドロップダウン リストから ESP 暗号化アルゴリズムを選択します。このアルゴリズムは、ペイロードを暗号化するために使用されます。次のオプションがあります。 • 128 ビット高度暗号化規格（AES）暗号化アルゴリズムを使用する ESP。 • 192 ビット AES 暗号化アルゴリズムを使用する ESP。 • 256 ビット AES 暗号化アルゴリズムを使用する ESP • 168 ビット DES 暗号化アルゴリズム（3DES、トリプル DES とも呼ばれる）を使用する ESP。 • ヌル暗号化アルゴリズム。
ESP Integrity Algorithm	ドロップダウン リストから整合性アルゴリズムを選択します。このアルゴリズムは、ペイロードの整合性をチェックするために使用されます。次のオプションがあります。 • MD5（HMAC バリアント）認証アルゴリズムを使用する ESP。 • SHA（HMAC バリアント）認証アルゴリズムを使用する ESP
AH Integrity	ドロップダウン リストから AH 整合性を選択します。次のオプションがあります。 • MD5（Message Digest 5）（ハッシュに基づくメッセージ認証コード（HMAC）バリアント）認証アルゴリズムを使用する AH • SHA（セキュア ハッシュ アルゴリズム）（HMAC バリアント）認証アルゴリズムを使用する AH。
Compression	Lempel-Ziv-Stac（LZS）アルゴリズムを使用した IP 圧縮をイネーブルまたはディセーブルにします。

表 6-19　[Transform Set] ページ （続き）

要素	説明
Mode	ドロップダウン リストからモードを選択します。次のオプションがあります。 • [Transport] : データのみを暗号化します。トランスポート モードは、両方のエンドポイントで IPsec がサポートされている場合に使用されます。トランスポート モードは、認証ヘッダーまたはカプセル化されたセキュリティ ペイロードを元の IP ヘッダーの後に配置します。したがって、IP ペイロードのみが暗号化されます。この方法では、Quality-of-Service（QoS）制御などのネットワーク サービスを暗号化されたパケットに適用できます。 • [Tunnel] : データと IP ヘッダーを暗号化します。トンネル モードは、トランスポート モードよりも強固な保護を提供します。IP パケット全体が AH または ESP 内にカプセル化されるため、新しい IP ヘッダーが付加され、データグラム全体を暗号化できます。トンネル モードでは、ルータなどのネットワーク デバイスが、複数の VPN ユーザに対して IPsec プロキシの役割を果たすことができます。トンネル モードは、そのような設定で使用することが推奨されます。

ステップ 7　次の項目をクリックします。

- [Save]。設定を保存します。
- [Cancel]。変更を保存せずに終了します。
- もう一度 [Save]。設定変更を保存します。

ゾーンの概要

ゾーン ベースのファイアウォール（ZBFW）機能では、ゾーンと呼ばれるインターフェイス グループの間の Cisco IOS 単方向ファイアウォール ポリシーを簡単に管理できます。

ゾーンとは、同様の機能を果たすインターフェイスのグループです。たとえば、ルータで、ギガビット イーサネット インターフェイス 0/0/0 とギガビット イーサネット インターフェイス 0/0/1 をローカル LAN に接続できるとします。これら 2 つのインターフェイスは、内部ネットワークを表している点で同類です。したがって、ファイアウォール設定でゾーンとしてグループ化できます。

デフォルトでは、同じゾーン内のインターフェイス間のトラフィックはポリシーの制約を受けません。トラフィックは自由に通過します。ファイアウォール ゾーンはセキュリティ機能に使用されます。

セキュリティ ゾーン

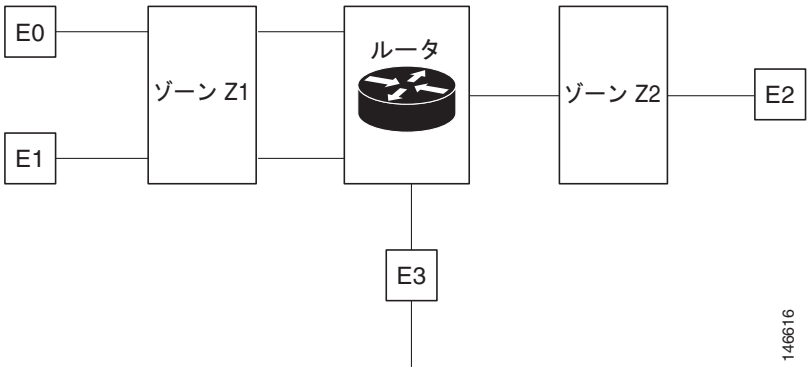
セキュリティ ゾーンとは、ポリシーを適用できるインターフェイスのグループです。インターフェイスをゾーンにグループ化するには、次の 2 つの手順を実行します。

- インターフェイスを付加できるようにゾーンを作成します。
- インターフェイスを特定のゾーンのメンバーとして設定します。

デフォルトでは、トラフィックは、同じゾーンのメンバーであるインターフェイス間を通ります。インターフェイスがセキュリティ ゾーンのメンバーである場合、そのインターフェイスを通るトラフィックはどちらの方向でもすべて（ルータ宛またはルータ発のトラフィックを除く）はドロップされます。ゾーンメンバー インターフェイスとの間の両方向のトラフィックを許可するには、そのゾーンのゾー

ン ペアの一部にして、そのゾーン ペアにポリシーを適用する必要があります。ポリシーで、inspect または pass アクションによってトラフィックが許可されると、トラフィックはインターフェイスを通過します。

図 6-1　セキュリティ ゾーンの図



- インターフェイス E0 と E1 はセキュリティ ゾーン Z1 のメンバーです。
- インターフェイス E2 は、セキュリティ ゾーン Z2 のメンバーです。
- インターフェイス E3 は、どのセキュリティ ゾーンのメンバーでもありません。

このシナリオでは、次の状況が存在します。

- インターフェイス E0 と E1 は同じセキュリティ ゾーン（Z1）のメンバーなので、2 つのインターフェイス間のトラフィックは自由に流れます。
- ポリシーが設定されていない場合、インターフェイス間（E0 と E2、E1 と E2、E3 と E1、E3 と E2 など）でトラフィックは流れません。
- ゾーン Z1 とゾーン Z2 の間のトラフィックを許可する明示的なポリシーが設定されると、E0 または E1 インターフェイスと E2 インターフェイスの間のみトラフィックは流れることができます。
- E3 はセキュリティ ゾーンに含まれていないため、E3 インターフェイスと E0/E1/E2 インターフェイスの間をトラフィックが流れることはできません。

詳細については、次の項を参照してください。

- 「アプリケーションの管理」（P.6-37）
- 「デフォルト パラメータの管理」（P.6-39）
- 「インターフェイスの管理」（P.6-39）
- 「ポリシー規則の管理」（P.6-40）
- 「サービスの管理」（P.6-44）
- 「セキュリティ ゾーンの作成」（P.6-45）

アプリケーションの管理

この機能では、伝送制御プロトコル（TCP）/ユーザ データグラム プロトコル（UDP）ポートをアプリケーションに割り当てまたは割り当て解除できます。

（注）　[Save] ボタンまたは [Delete] ボタンをクリックすると、変更がデバイスに導入されます。要求された操作の CLI を確認することはできません。また、保留中の変更のキューから操作要求を削除することもできません。オブジェクトを設定するために「EMS_」で始まる CLI で変更を行うことはサポートされていません。そのような変更を行うと、予期せぬ動作が発生する可能性があります。

アプリケーションの編集

TCP/UDP ポートをアプリケーションに割り当てまたは割り当て解除するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Zone Based Firewall] > [Applications] を選択します。[Applications] ページが表示されます。

ステップ 5　TCP/UDP ポートをアプリケーションに割り当てまたは割り当て解除するには、アプリケーションをクリックし、その TCP/UDP ポートの値を更新します。

a. カンマで区切られた 1 つ以上のポートを定義してポートを割り当てます（例：1234, 2222）。

b. ポート範囲を定義してポートを割り当てます（例：1111-1118）。ポートまたはポート範囲のグループも割り当てることができます。

c. 既存のポートの値を削除して、ポートを割り当て解除します。

表 6-20 に、[Applications] ページ上の要素を示します。

表 6-20　[Applications] ページ

要素	説明
Application Name	デバイスから取得されたアプリケーション名が表示されます。
TCP Ports	（オプション）特定のアプリケーションに割り当てられる TCP ポートの値
UDP Ports	（オプション）特定のアプリケーションに割り当てられる UDP ポートの値

ステップ 6　[Save] をクリックして、設定を保存します。

デフォルト パラメータの管理

デフォルト パラメータ マップを変更するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Zone Based Firewall] > [Default Parameters Map] を選択します。

ステップ 5　[Default Parameters Map] ページから、パラメータ マップの値を変更します。

（注）　デフォルト パラメータは ISR デバイス上でのみ変更できます。

ステップ 6　[Save] をクリックして、設定を保存します。

インターフェイスの管理

仮想インターフェイスは、特定の目的のための、または特定のユーザに共通の汎用設定情報で設定された論理インターフェイスです。ゾーン メンバー情報が RADIUS サーバから取得され、ダイナミックに作成されたインターフェイスがそのゾーンのメンバーになります。

インターフェイスの設定

インターフェイスをゾーンに割り当てたり、インターフェイスを特定のゾーンから割り当て解除したりするには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Zone Based Firewall] > [Interfaces] を選択します。

ステップ 5　[Interface] ページで、変更するインターフェイスを選択し、下矢印アイコンをクリックします。[Zone] ダイアログボックスが表示されます。

ステップ 6　[Zone] ダイアログボックスで、インターフェイスの新しいセキュリティ ゾーンを選択します。選択したインターフェイスがゾーンにすでに割り当てられている場合、警告メッセージが表示されます。

ステップ 7　そのインターフェイスの割り当てを変更する場合は、警告メッセージ上の [Yes] をクリックします。

ステップ 8　インターフェイスを特定のゾーンから割り当て解除するには、インターフェイスを選択し、ゾーン情報を削除します。

表 6-21 に、[Interfaces] ページ上の要素を示します。

表 6-21　[Interface] ページ

要素	説明
Interface Name	インターフェイス名が表示されます。
Zone	インターフェイスが属しているセキュリティゾーンの名前。
VRF	インターフェイスが属している VRF の名前。

ステップ 9　次の項目をクリックします。

- [Save]。変更を保存して適用します。
- [Cancel]。保存せずに終了します。

ポリシー規則の管理

ポリシー規則セクションでは、新しいファイアウォール ポリシー規則を作成したり、既存のポリシー規則を変更したり、ポリシー規則を削除したり、ポリシー規則の順序を変更したりできます。ファイアウォール ポリシー規則を作成するとき、ポリシー テーブル内の位置は自分で定義します。

ポリシー規則の作成

ポリシー規則を作成するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Zone Based Firewall] > [Policy Rules] を選択します。[Firewall Rules] ページが表示されます。

ステップ 5　[Firewall Rules] ページから、[Add Rule] ボタンをクリックし、名前、送信元ゾーン、宛先ゾーン、送信元 IP アドレス、宛先 IP アドレス、サービス、アクションなどの情報を入力します。送信元ゾーンと宛先ゾーンは異なるものにする必要があります。規則を移動するには、[Add Rule] ボタン上の下矢印アイコンをクリックします。規則をリストの先頭やリストの最後に配置したり、リスト内の選択した規則の前または後に移動したりできます。

（注）　名前フィールドはオプションです。ファイアウォール規則の名前を入力しなければ、システムによってファイアウォール規則の名前が生成されます。*rule_<number>* または *EMS_rule_<number>* の形式でファイアウォール規則の名前を作成することはできません（*rule_1* など）。これらの形式は、システムで予約されています。

ステップ 6　送信元および宛先 IP アドレスを追加するには、[add] アイコンをクリックします。[Source/Destination IP address] ダイアログボックスが表示されます。

a. [Source/Destination IP address] ダイアログボックスから、[Any] チェックボックスをオンにして値を any に設定します。

a. 送信元/宛先 IP アドレスを入力します。

b. 新しい IP アドレスとサブネットを追加するには、[Add] ボタンをクリックします。

c. 既存の値を削除するには、[Delete] をクリックします。

d. [Ok] をクリックして、設定を保存します。

e. 行った変更をルータに送信せずにすべて取り消すには、[Cancel] をクリックします。

ステップ 7　[Service] の値を設定します。アプリケーションを追加または削除するには、下矢印アイコンをクリックします。[Firewall Service] ダイアログボックスが表示されます。

a. [Firewall Service] ダイアログボックスで、[Application] チェックボックスをオンにして、検査するアプリケーションを選択します。

b. ACL ベースのアプリケーションを選択するには、TCP または UDP または ICMP アプリケーションを選択します。

c. 前後に移動するには、ナビゲーション矢印ボタンを使用します。

d. 設定を保存するには、[plus +] ボタンをクリックします。

ステップ 8　適切なアクションを選択します。オプションには、[Drop]、[Drop and Log]、[Inspect]、[Pass]、および [Pass and Log] があります。

ステップ 9　検査のアクションを選択する場合は、[Advance options] 列にある [Configure] ボタンをクリックします。[Advanced Parameters Configuration] ダイアログボックスが表示されます。

ステップ 10　[Advanced Parameters Configuration] ダイアログボックスで、次を実行します。

a. デバイスのデフォルト値をカスタマイズするには、パラメータのチェックボックスをオンにし、新しい値を設定します。

b. デバイスのデフォルト値を適用するには、パラメータのチェックボックスをオフにします。

c. ファイアウォール規則のデフォルト パラメータを表示するには、「デフォルト パラメータの管理」（P.6-39）を参照してください。

d. [Advanced Options] アイコンの上にカーソルを置くと、設定済みのパラメータがクイック ビュー ウィンドウに表示されます。

表 6-22 に、[policy rule] ページ上の要素を示します。

表 6-22　[Policy Rule] ページ

要素	説明
Name	（オプション）ポリシー規則の名前を入力します。
Source Zone	送信元ゾーンの名前を入力します。送信元ゾーンは、トラフィックの発信元のゾーンの名前を指定します。

表 6-22　[Policy Rule] ページ （続き）

要素	説明
Destination Zone	宛先ゾーンの名前を入力します。宛先ゾーンは、トラフィックの行き先のルータの名前を指定します。
Source	検査対象データの送信元 IP アドレスを入力します。有効なパラメータは次のとおりです。 • Any • IP Address • Subnet
Destination	検査対象データの宛先 IP アドレスを入力します。有効なパラメータは次のとおりです。 • Any • IP Address • Subnet
Service	検査対象データのサービス。有効なパラメータは次のとおりです。 • L3/4 アプリケーション。「アプリケーションの管理」（P.6-37）を参照してください。 • サービス（「サービスの管理」（P.6-44）） • ACL ベースのアプリケーション：TCP、UDP、ICMP
Action	規則の条件が一致したときに実行するアクションを選択します。規則は次の場合に一致します。 • トラフィックの送信元 IP が送信元規則の条件と一致する。 • トラフィックの宛先 IP が宛先規則の条件と一致し、さらにトラフィックの検査対象サービスがサービス規則の条件と一致する。 次のアクション オプションがあります。 • Drop • Drop and Log • Inspect • Pass • Pass and Log
Advance Options	[Action] オプションを [Inspect] に設定するときに、ファイアウォール規則のパラメータマップ動作を設定するための設定パラメータを指定します。

ステップ 11　[Save] をクリックして、規則をデバイスに適用します。

ポリシー規則の編集

既存のポリシー規則を編集するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Zone Based Firewall] > [Policy Rules] を選択します。

ステップ 5　[Firewall Rules] ページで、次のいずれかを実行します。

a. 規則パラメータの行をクリックし、パラメータを編集します。または

b. チェックボックスをオンにして規則を選択し、[Edit] ボタンをクリックします。選択した規則エンティティが編集用に開きます。

ステップ 6　[Save] をクリックして、デバイス内の変更を適用します。

ポリシー規則の削除

既存のポリシー規則を削除するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Zone Based Firewall] > [Policy Rules] を選択します。

ステップ 5　[Firewall Rules] ページで、チェックボックスをオンにして規則を選択し、[Delete] ボタンをクリックします。

ステップ 6　警告メッセージ上の [Ok] をクリックして、ポリシー規則を削除します。選択したポリシー規則がデバイスから削除されます。

ファイアウォール規則の順序の変更

クラスデフォルトの規則は常にリストの最後になり、それらの位置は固定されています。通常の規則をクラスデフォルトの規則の下に移動することはできません。

ポリシー規則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　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Zone Based Firewall] > [Policy Rules] を選択します。

ステップ 5　[Firewall Rules] ページで、規則を特定の行に移動するには、規則を新しい位置にドラッグ アンド ドロップします。

サービスの管理

この機能では、サービス要素を作成、更新、または削除できます。TCP/UDP ポートをアプリケーションに割り当てまたは割り当て解除できます。

サービスの作成

サービスを作成するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Zone Based Firewall] > [Services] を選択します。[Service] ページが表示されます。

ステップ 5　[Service] ページで、[Add Service] ボタンをクリックして、新しいサービスを作成します。

ステップ 6　[Service] ページで、サービス名を入力します。

ステップ 7　アプリケーションを割り当てるには、下矢印アイコンをクリックします。[Applications Object Selector] ダイアログボックスが表示されます。

a. [Applications] ダイアログボックスで、[Applications] チェックボックスをオンにして、リストからアプリケーションを選択します（複数選択可）。

b. [OK] をクリックして変更を確定するか、[Cancel] をクリックして変更を取り消します。

表 6-23 に、[Service] ページ上の要素を示します。

表 6-23　[Service] ページ

要素	説明
Service Name	サービス名を入力します。サービスの作成後に名前を変更することはできません。また、アプリケーションのないサービスを作成することはできません。
Application	このサービスにグループ化されているアプリケーションのリストが表示されます。

ステップ 8　[Save] をクリックして、変更をデバイスに適用します。

サービスの編集

既存のサービスを編集するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Zone Based Firewall] > [Services] を選択します。

ステップ 5　[Service] ページで、次を実行します。

a. サービス パラメータの行をクリックし、パラメータを編集します。または

b. サービスを選択し、[Edit] ボタンをクリックします。選択したサービス エンティティが編集用に開きます。新しいアプリケーションを追加したり、すでに選択されているアプリケーションを削除したりできます。

c. 選択したリストからアプリケーションを削除するには、アプリケーション名の上にカーソルを置き、[X] アイコンをクリックします。

ステップ 6　[Save] をクリックして、設定を保存します。

サービスの削除

既存のサービスを削除するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Zone Based Firewall] > [Services] を選択します。

ステップ 5　[Service] ページから、サービスを選択し、[Delete] ボタンをクリックします。

ステップ 6　警告メッセージ上の [Ok] をクリックして、サービスを削除します。選択したサービスが削除されます。

セキュリティ ゾーンの作成

セキュリティ ゾーンを作成するには、次の手順を実行します。

（注）　ゾーン ベースのファイアウォール機能は、IOS バージョン 3.5 以降の ASR プラットフォーム上でサポートされています。ゾーン ベースのファイアウォール機能は、IOS リリース 12.4(24)T 以降の ISR プラットフォーム上でサポートされています。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Zone Based Firewall] > [Zones] を選択し、[Add Zone] ボタンをクリックしてセキュリティ ゾーンを作成します。

ステップ 5　[security zone] ページで、ゾーン名を入力します。

ステップ 6　ゾーンの VRF を選択します。

a. VRF の選択は、セキュリティ ゾーンに割り当て可能なインターフェイスに影響を与えます

b. デフォルトの VRF オプションを選択した場合、セキュリティ ゾーンは、他に関係している VRF のないインターフェイスに対してのみ割り当てできます。

ステップ 7　インターフェイスをセキュリティ ゾーンに割り当てるには、下矢印アイコンをクリックします。[Interface Object Selector] ダイアログボックスが表示されます。

a. [Interface selector] ダイアログボックスで、[Interface] チェックボックスをオンにして、リストからインターフェイスを選択します（複数選択可）。

b. [Ok] をクリックして、設定を保存します。

c. 行った変更をルータに送信せずにすべて取り消すには、[Cancel] をクリックします。

ステップ 8　[Advance options] 列で、[Configure] ボタンをクリックします。[Advanced Parameters Configuration] ダイアログボックスが表示されます。

ステップ 9　[Advanced Parameters Configuration] ダイアログボックスで、次を実行します。

a. アラートを設定するには、[Alert] チェックボックスをオンにし、[On] オプション ボタンをクリックします。

b. 最大検出を設定するには、[Maximum Detection] チェックボックスをオンにします。

c. TCP フラッディング レートを設定するには、[TCP SYN-Flood Rate per Destination] チェックボックスをオンにします。

d. FW ドロップ脅威検出レート、FW 検査脅威検出レート、および FW SYN 攻撃脅威検出レートを設定するには、[Basic Threat Detection Parameters] チェックボックスをオンにし、[On] オプション ボタンをクリックします。

ステップ 10　次の項目をクリックします。

- [Ok]。設定を保存します。
- [Cancel]。保存せずに終了します。

ステップ 11　既存のセキュリティ ゾーン パラメータを編集するには、ゾーンを選択し、[Advance options] 列の [Configure] ボタンをクリックします。[Advanced Parameters Configuration] ダイアログボックスが表示されます。

ステップ 12　[Advanced Parameters Configuration] ダイアログボックスで、値を編集し、[Save] をクリックして変更を保存します。[Advanced Options] アイコンの上にカーソルを置くと、設定済みのパラメータがクイック ビュー ウィンドウに表示されます。

（注）　デフォルトでは、詳細設定パラメータはディセーブルになっています。

表 6-24 に、[Security Zone] ページ上の要素を示します。

表 6-24　[Security Zone] ページ

要素	説明
Zone Name	ゾーン名を入力します。
VRF	ゾーンの VRF を選択します。
Interface	セキュリティ ゾーンに割り当てられているインターフェイスのリストが表示されます。インターフェイスが 3 つ以上ある場合は、マウスをアイコンの上に置くと、完全なリストが表示されます。
Advance Options	[Alert]、[Maximum Detection]、[TCP Synchronize-Flood Rate Per Destination]、[Basic Threat Detection] などの詳細パラメータを設定します。
Description	（オプション）ゾーンの説明を入力します。

ステップ 13　ゾーンの説明を入力します。

ステップ 14　次の項目をクリックします。

- [Save]。変更を保存します。
- [Cancel]。保存せずに終了します。

セキュリティ ゾーンの編集

既存のセキュリティ ゾーンを編集するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　左の [Feature Selector] パネルから、[Zone Based Firewall] > [Zones] を選択します。

ステップ 5　[Security Zone] ページで、次のいずれかを実行します。

a.　ゾーン パラメータの行をクリックし、パラメータを編集します。または

b.　ゾーンを選択し、[Edit] ボタンをクリックします。選択したゾーン エンティティが編集用に開きます。

ステップ 6　[add] アイコンをクリックして、インターフェイスをゾーンに割り当てるか、既存のインターフェイスをゾーンから割り当て解除します。さらに、ゾーンの説明を変更することもできます。

ステップ 7　[Save] をクリックして、設定を保存します。

セキュリティ ゾーンの削除

既存のセキュリティ ゾーンを削除するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Zone Based Firewall] > [Zones] を選択します。

ステップ 5　[Security Zone] ページで、セキュリティ ゾーンを選択し、[Delete] ボタンをクリックします。

ステップ 6　警告メッセージ上の [Ok] をクリックして、セキュリティ ゾーンを削除します。選択したゾーンが削除されます。

デフォルトゾーンの設定

デフォルト ゾーンを設定するには、次の手順を実行します。

（注）　デフォルトゾーン機能は、ASR プラットフォーム上でのみサポートされます。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成し、デバイスを設定します。

ステップ 3　デバイスを選択した後、[Configuration] をクリックします。[Feature Selector] パネルが表示されます。

ステップ 4　[Feature Selector] パネルから、[Zone Based Firewall] > [Zones] を選択します。

ステップ 5　[Security Zone] ページで、[Default Zone] ボタンをクリックして、デバイス内のデフォルト セキュリティ ゾーンをイネーブルまたはディセーブルにします。デバイスは、どのゾーンにも関係していないインターフェイスをすべてホストします。

ステップ 6　[OK] をクリックして、設定を保存します。

レポートを使用したモニタリング

Prime AM レポートは、問題のトラブルシューティングはもとより、システムとネットワークの状態のモニタリングにも役立ちます。レポートは、すぐに実行することも、指定した時刻に実行するようにスケジュールすることもできます。一度定義しておけば、今後の診断用に保存したり、定期的に実行してレポートを作成するようにスケジュールしたりできます。

レポートは CSV 形式または PDF 形式のいずれかに保存して、後からダウンロードできるよう Prime AM 上のファイルに保存することも、指定の電子メール アドレス宛に送信することもできます。

[Tools] > [Reports] > [Report Launch Pad] を選択して、使用可能なレポートのリストを表示します。

ヒント　レポート タイプの隣にある情報アイコンの上にカーソルを置いて、レポートの詳細情報を表示します。

新しいレポートの作成および実行

ステップ 1　[Tools] > [Reports] > [Report Launch Pad] を選択します。

ステップ 2　作成するレポートの隣にある [New] をクリックします。

ステップ 3　レポートの詳細情報を入力し、次をクリックします。

- [Save]：レポートをすぐには実行せずにこのレポート セットアップを保存します。レポートは、スケジュールされた時刻になると自動的に実行されます。
- [Save and Run]：このレポート セットアップを保存し、レポートをすぐに実行します。
- [Run]：レポート セットアップを保存せずにレポートを実行します。
- [Save and Export]：レポートを保存し、結果を CSV 形式または PDF 形式にエクスポートします。

- [Save and Email]：レポートを保存し、結果を電子メールで送信します。

スケジュールされているレポートの表示

現在スケジュールされているすべてのレポートを表示および管理するには、[Tools] > [Reports] > [Scheduled Run Results] を選択します。

保存されているレポート テンプレートの表示

必要なパラメータをすべて含むレポートが作成されている場合、そのレポート テンプレートを保存できます。

ステップ 1　[Tools] > [Reports] > [Saved Report Templates] を選択します。

ステップ 2　次のフィールドの中から選択して、どの保存されているレポート テンプレートを表示するか選択します。

- [Report Category]：ドロップダウン リストから該当するレポート カテゴリを選択します。あるいは [All] を選択します。
- [Report Type]：ドロップダウン リストから該当するレポート タイプを選択します。あるいは [All] を選択します。[Report Type] の選択項目は、選択したレポート カテゴリによって変化します。
- [Scheduled]：[All]、[Enabled]、[Disabled]、または [Expired] を選択して、保存されているレポート テンプレートのリストをスケジュール ステータスでフィルタリングします。

パケット キャプチャを使用したモニタリングとトラブルシューティング

Prime AM では、ネットワーク内のトラフィックのキャプチャを実行して、ネットワーク使用率のモニタリング、ネットワーク統計情報の収集、およびネットワーク問題の分析に役立てることができます。

ステップ 1　[Tools] > [Packet Capture] を選択し、[Create] をクリックします。

ステップ 2　必要なキャプチャ セッション パラメータを指定し、[Create] をクリックします。

サイトの接続に関する問題の診断

Prime AM ダッシュボードを使用してネットワークをモニタし、ネットワーク内の問題のあるデバイスを見つけてから、デバイス ワーク センターを使用してデバイス構成を変更できます。

ステップ 1　[Operate] > [Detailed Dashboards] を選択し、接続の問題が発生しているサイトを選択し、[Go] をクリックします。

ステップ 2　[Device Reachability Status] と [Top *N* Devices with Most Alarms] にレポートされたデータを表示して、問題の原因を突き止めます。

ステップ 3　アラームが頻発しているデバイスの名前をクリックします。これにより、そのデバイスの全体像が表示されます。

ステップ 4　[Alarm Browser] アイコンをクリックして、そのデバイスのアラームを表示します。アラームを展開して、アラームの詳細情報を表示します。

ステップ 5　デバイスの設定を既知の正常な設定と比較するには、[Operate] > [Device Work Center] を選択し、設定の変更が必要なデバイスを選択します。

ステップ 6　[Configuration Archive] タブをクリックし、矢印を展開して追加オプションを表示し、設定タイプおよび比較する設定を選択します。

ステップ 7　設定を変更またはロールバックします。詳細については、デバイス構成バージョンのロールバックを参照してください。