CHAPTER 6

ネットワークの運用とモニタリング

Prime NCS（WAN）の [Operate] タブには、ネットワークを毎日モニタリングしたり、ネットワーク デバイスのインベントリと設定管理に関連した日常的な操作または随時操作の実行に役立つツールが用意されています。[Operate] タブには、毎日のモニタリング、トラブルシューティング、保守、および操作に必要なダッシュボード、Device Work Center、およびツールが含まれています。

ダッシュレットとダッシュボードのモニタリング

Prime NCS（WAN）は、モニタリング データをダッシュボードおよびダッシュレットに自動的に表示します。次のいずれかのダッシュボードを [Operate] > [Monitoring Dashboard] で選択して、要約情報を表示できます。

- [Overview]：デバイス数、CPU 使用率およびメモリ使用率の上位 5 デバイスなど、ネットワークに関する概要情報が表示されます。[Overview] ダッシュボードからデバイスまたはインターフェイスのアラーム数をクリックすると、詳細なダッシュボードとアラームとイベントが表示され、問題のトラブルシューティングと切り分けに役立ちます。
- [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、アラームとイベントの要約が表示されます。このダッシュボード内の項目をクリックすると、アラームまたはイベントの詳細が表示され、問題のトラブルシューティングを行うことができます。
- [Performance]：CPU とメモリの使用率情報が表示されます。
- [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 ヘルスの要約が表示されます。[Detailed Dashboards] を使用すると、ネットワーク内の輻輳を表示して、サイト、デバイス、およびインターフェイスの詳細情報を収集できます。たとえば、特定のサイトの [Detailed Dashboards] を表示して、アラームが最も多いデバイスや、サイトのデバイスの到達可能性ステータスなどを知ることができます。

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のようにして変更できます。

表 6-1 に、Prime NCS（WAN）ダッシュボードのモニタリング情報をどこで取得できるかを示します。

表 6-1　モニタリング データの取得

表示するモニタリング データ	選択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]
デバイスの到達可能性ステータス	[Operate] > [Monitoring Dashboard] > [Overview]

表 6-1　モニタリング データの取得（続き）

表示するモニタリング データ	選択するダッシュボード
イベント情報	[Operate] > [Monitoring Dashboard] > [Incidents]
インターフェイス ステータス、可用性、および使用率情報	[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 送信元情報	[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] を選択すると、ジョブのステータスが表示され、次のことができます。

- 実行中と完了済みのすべてのジョブ、および対応するジョブ詳細を表示する
- ジョブをフィルタリングし、関心がある特定のジョブだけを表示する
- 送信した最新のジョブの詳細を表示する
- ジョブの実行結果を表示する
- ジョブの削除、編集、実行、取り消し、一時停止、および再開など、ジョブを変更する

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取得できます。ジョブを展開して詳細を表示したら、[History] タブをクリックし、カーソルを [Status] フィールドの上に置きます。結果ウィンドウに、ジョブの失敗原因の判別に役立つトラブルシューティング情報が表示されます。

モニタリングの設定

Prime NCS（WAN）でネットワーク内のデバイスとインターフェイスをモニタリングする方法を定義できます。

[Auto Monitoring] オプションを有効にすると、Prime NCS（WAN）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リングすることができます。デフォルトでは、Prime NCS（WAN）はネットワーク内のすべてのデバイスに対して 15 分ごとにポーリングを行い、デバイス ヘルス データを収集します。大部分のユーザは [Auto Monitoring] を有効にしています。

ネットワークまたは Prime NCS（WAN）の展開が非常に大規模な場合は、過度のポーリング トラフィックを避けるために、[Auto Monitoring] を有効にしないでおくこともできます。その場合は [Auto Monitoring] を無効のままとし、ビジネス上重要なデバイスだけを含んだ 1 つ以上のデバイス グループを作成します。また、それらのデバイスに適したポーリング頻度を指定した、デフォルトのデバイス ヘルス モニタリング テンプレートのバージョン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 テンプレートを展開する場合、それとビジネス上重要なデバイス グループだけに適用するよう指定できます。

また、Cisco IOS Netflow と Cisco Prime Assurance に対して、重複排除を有効にすることもできます（可能な場合）。NetFlow を送信する複数のルータとスイッチがあり、その送信先に、Cisco Prime Assurance サーバだけでなく、Cisco Prime Assurance がデータを取り出す複数の NAM が設定されて

いる場合、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。重複排除を有効にすると、Cisco Prime Assurance が同じメトリックを複数回カウントしないようにすることができます。

ステップ 1　[Administration] > [System] を選択してから、[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。

- Prime NCS（WAN）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リングするには [Auto monitoring]。
- Prime NCS（WAN）で冗長なデータを排除するには [Enable deduplication]。

Device Work Center とは

[Operate] > [Device Work Center] から、デバイス インベントリとデバイス コンフィギュレーション情報を表示できます。Device Work Center には、表 6-2 に示すように、上部に一般的な管理機能、下部に設定機能が表示されます。

表 6-2　Device Work Center タスク

タスク	説明	[Operate] > [Device Work Center] での位置
デバイスの管理	デバイスの追加、編集、一括インポート、および削除を実行し、デバイスから強制的にデータを収集します。	Device Work Center の上部に各ボタン。
基本的なデバイス情報と収集ステータスの表示	基本的なデバイス情報（到達可能性ステータス、IP アドレス、デバイス タイプなと）、および収集ステータス情報が表示されます。	Device Work Center の上部に表示。 [Collection Status] セルの上にカーソルを合わせてアイコンをクリックすると、インベントリ収集に関連するエラーが表示されます。
デバイス グループの管理	デフォルトでは、Prime NCS（WAN）が動的デバイス グループを作成して、デバイスを適切な Device Type フォルダに割り当てます。新しいデバイス グループを作成でき、User Defined フォルダに格納されます。	Device Work Center の左ペインに表示。 デバイス グループの作成と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 プロファイルを設定後、サイトにデバイスを追加できます。 **（注）**　1 つのデバイスは 1 つのサイトだけに属することができます。	Device Work Center の上部にある [Add to Site] ボタン。 サイトへのデバイスの追加の詳細については、サイト プロファイルの作成を参照してください。

表 6-2　Device Work Center タスク（続き）

タスク	説明	[Operate] > [Device Work Center] での位置
デバイス詳細の表示	メモリ、ポート、環境、およびインターフェイス情報などのデバイス詳細が表示されます。	Device Work Center でデバイスを選択し、画面下部にある [Device Details] タブをクリックします。
	デバイスの情報、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、およびインターフェイスが表示されます。詳細については、360 度ビュー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、表示されるアイコンをクリックします。
コンフィギュレーション テンプレートの作成と展開	選択したデバイス用のコンフィギュレーション テンプレートを作成し、展開することができます。また、デバイスに展開する 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 コンフィギュレーションの表示	アーカイブしたコンフィギュレーションを表示し、コンフィギュレーションのロールバックをスケジュールし、アーカイブ収集をスケジュールします。	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に関する詳細、デバイスに推奨されるソフトウェア イメージ、およびデバイスの最新のソフトウェア イメージ動作が表示されます。	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

選択したデバイスの機能設定を作成または変更することができます。詳細については、次の項を参照してください。

- 「Application Visibility」（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 のコンポーネント」（P.6-27）
- 「ゾーンの概要」（P.6-36）

Application Visibility

Application Visibility（AV）機能は、インターネットへ送信されるトラフィックのモニタリングに役立ちます。AV を設定するには、次の作業が必要です。

- AV 設定の作成
- インターフェイスへの AV ポリシーの割り当て
- AV 詳細オプションの変更

（注）　Application Visibility 機能は、IOS バージョン 3.5 以降の ASR デバイスでサポートされています。この機能は ISR デバイスではサポートされていません。「EMS_」で始まるオブジェクト/エンティティに対する CLI インターフェイスからの変更はサポートされず、予期しない動作となることがあります。

AV の設定

Application Visibility 設定機能は、トランザクション レコードおよび使用状況レコード用の NetFlow メッセージを送信するために必要な要素をデバイス内に作成します。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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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 ルーティングと転送（VRF）、および送信元 IP アドレスを設定します。

ステップ 6　詳細 AV パラメータを設定します。詳細 AV 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] ページの要素のリストを示します。

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	（任意）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 の VRF。デフォルトの VRF は [Global VRF] です。
Source IP Address	CM への FNF メッセージの転送元として使用されるインターフェイスの IP アドレスを指定します。

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。

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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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 レコードを有効または無効にする 1 つ以上のインターフェイスを選択します。インターフェイス上で AV を有効にするには、[Enable] を選択してから、コレクタの送信先に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実行されるさまざまなタイプの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、さまざまなアプリケーションの帯域幅使用状況をモニタリングできます。使用状況レコードでは、特定の期間におけるアプリケーション使用状況、ピークと平均の使用状況、および特定のアプリケーション タイプの使用状況を示すことができます。使用状況レコードは、そのインターフェイスのカテゴリ情報の定期的な集約を行います。（たとえば、ピアツーピア トラフィックまたは電子メール使用状況のエクスポート情報など）。

b. トランザクション レコード（TR）：トランザクションとは、エンドポイント間での一連の論理的な交換のことです。通常、1 つのフローには 1 つのトランザクションがあります。トランザクション レコードは、トランザクション レベルでトラフィックをモニタリングします。これらのレコードにより、トラフィック フローの詳細な分析ができます。トランザクション レコードは、ネットワーク側のインターフェイスの入力および出力方向に送られます。これらのトランザクション レコードを使用して、システムはそれぞれの単方向フローを 1 回だけキャプチャできます。

ステップ 6　[OK] をクリックして、デバイスに加えた変更を展開します。

AV 詳細オプションの変更

Application Visibility 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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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、特定の属性のチェックボックスをオンにして新しい値を設定します。システム デフォルト値を使用するには、そ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] ページの要素のリストを示します。

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	（任意）セカンダリ CM の IP アドレスを入力します。

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

要素	説明
VRF	プライマリ CM IP、セカンダリ CM IP、および送信元 IP の VRF。デフォルトの VRF は [Global VRF] です。
Source IP Address	CM への FNF メッセージの転送元として使用されるインターフェイスの IP アドレスを指定します。
Advance Options	
DSCP Value	（任意）エクスポータの DSCP Service Code Point 値を設定するには、[DSCP Value] チェックボックスをオンにします。範囲は 0 ～ 63 です。
TTL	（任意）エクスポータの TTL またはホップ限界を設定するには、[TTL] チェックボックスをオンにします。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 キャッシュ内のフロー エントリの最大数を設定します。
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 キャッシュ内のフロー エントリの最大数を設定します。
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	許容される最大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（通常はファイアウォール）がプライベート 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）にパブリック アドレスを割り当てるプロセスのことです。NAT は、経済性とセキュリティの両方の目的で、組織または会社で使用されるパブリック IP アドレスの数を制限するために役立ちます。

組織が NAT 機能を使用すると、既存のネットワークを持っていてインターネットにアクセスする必要がある場合に、IP アドレスが枯渇する問題を解決できます。組織の IP ネットワークで NAT を使用することにより、外部のネットワークに異なる 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、グローバルなルーティングが可能なアドレスを持たない組織でも、そのアドレスをグローバルにルーティング可能なアドレス空間に変換して、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、Classless Inter Domain Routing（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します。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、Internet Control Message Protocol（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（通常、2 つのネットワークどうしを接続）で動作し、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（内部ローカル）アドレスをパブリック（内部グローバル）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 でマッピングできます。
- 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 を設定する手順は、次のとおりです。

1. NAT プール（ダイナミック NAT に必要）の作成
2. ACL の設定
3. NAT44 ルールの作成
4. インターフェイスへのルールの割り当て
5. NAT の最大変換の設定（任意）

（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 プラットフォームでサポートされています。「EMS_」で始まるオブジェクト/エンティティに対する CLI インターフェイスからの変更はサポートされず、予期しない動作となることがあります。

IP プール

IP プールは、ダイナミック NAT で使用する IP の範囲を表すデバイス オブジェクトです。NAT の IP プール機能を使用すると、ダイナミック NAT で使用できる新しいプールの作成、既存のプールの変更、デバイスからのプールの削除ができます。

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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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] または [IP Range + Prefix] ボタンをクリックし、[Name]、[IP Address/Range]、[Prefix Length]、および [Description] に入力します。

ステップ 6　コンフィギュレーションを保存するには、[OK] をクリックします。

表 6-5 に [IP Pools] ページの要素のリストを示します。

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、この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（.）で区切った 4 つの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	（任意）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 データベースに展開します。

ステップ 8　既存の IP プールを編集するには、[NAT IP Pools] ページで次のようにします。

a.　選択した IP プールの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.　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かれます。プール名を除く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 プールを選択してから、[Delete] ボタンをクリックします。

ステップ 11　警告メッセージに対して [Ok] をクリックし、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 機能を使用すると、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

この項では、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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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] の左パネルから、[NAT] > [NAT44] を選択します。

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

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

表 6-6 に [Static Rule] ページの要素のリストを示します。

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だけ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（.）で区切った 4 つの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] を定義した場合、[Destination A] はデフォルトで [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（.）で区切った 4 つの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] を定義した場合、[Source A] はデフォルトで [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。

表 6-6　[Static Rule] ページ（続き）

要素	説明
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（.）で区切った 4 つの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] を定義した場合、[Destination B] はデフォルトで [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（.）で区切った 4 つの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] を定義した場合、[Source A] および [Source B] はデフォルトで [Any] になります。
Options	スタティック タイプの詳細オプションが表示されます。次を設定します。 • 埋め込み IP アドレス（ペイロードなし）を無視するには、[Ignore Embedded IP address] チェックボックスをオンにします。 • ポート変換を有効にするには、[Enable Port Translation] チェックボックスをオンにしてから、次のものを定義します。 – TCP または UDP – 元のポート – ポート変換

表 6-7 に [Dynamic NAT] ページの要素のリストを示します。

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だけ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] を定義した場合、[Destination A] はデフォルトで [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] を定義した場合、[Source A] はデフォルトで [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] を定義した場合、[Destination B] はデフォルトで [Any] になります。

表 6-7　[Dynamic NAT] ページ（続き）

要素	説明
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] を定義した場合、[Source A] および [Source B] はデフォルトで [Any] になります。
Options	ダイナミック タイプの詳細オプションが表示されます。 • 埋め込み IP アドレス（ペイロードなし）を無視するには、[Ignore Embedded IP address] チェックボックスをオンにします。 • ポート変換を有効にするには、[Enable Port Translation] チェックボックスをオンにしてから、次のものを定義します。 – 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 デバイスでのみサポートされます。

表 6-8 に [Dynamic PAT] ページの要素のリストを示します。

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ウ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	未定義。
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	未定義。
Options	ダイナミック PAT 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。選択肢は [Yes] または [No] です。 （注）　このオプションは、ISR デバイスでのみサポートされます。

ステップ 6　次のいずれかをクリックします。

- 変更をデバイスに保存して展開するには [Save]。
- 保存しないで終了するには [Cancel]。

ステップ 7　既存の NAT44 ルールを編集するには、[NAT44] ページで次のようにします。

a. 選択した NAT44 ルールのパラメータ行をクリックし、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かれます。プール名を除く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、発信元と送信先を変更できます。また、[Options] 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、ルールを選択してから、[Delete] ボタンをクリックします。

ステップ 11　警告メッセージに対して [Ok] をクリックし、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、特定の目的または特定ユーザに共通の設定のための汎用設定情報とルータ依存情報を使用し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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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] の左パネルから、[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 の中でドロップダウン リストからアソシエーションを選択します。

表 6-9 に [Interfaces] ページの要素のリストを示します。

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する VRF の名前が表示されます。
Status	インターフェイスの状態が表示されます。
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。選択できる項目は、[Inside]、[Outside]、および [None] です。

ステップ 6　次のいずれかをクリックします。

- 変更をサーバに保存するには [Save] または [Apply]。
- 保存しないで終了するには [Cancel]。

NAT MAX 変換の管理

レート制限 NAT 変換機能によって、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 機能では、ユーザによる NAT アドレスの使用を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、サービス拒絶攻撃の影響を制限することができます。

NAT 最大変換機能を使用すると、グローバル変換の属性値をリセットできます。

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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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] の左パネルから、[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をリセットします。

表 6-10 に [MAX Translation] ページの要素のリストを示します。

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。許容される NAT エントリの最大数は 2147483647 です。一般的な 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	すべてのホストからの許容される 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。一般的な NAT レート制限の範囲は、100 ～ 300 エントリです。
Maximum number of translations over all VRF	すべての VRF からの許容される 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 からの許容される 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 214748364 です。一般的な 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（1 つまたは複数）からの許容される 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。一般的な 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（1 つまたは複数）からの許容される 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 214748364 です。一般的な NAT レート制限の範囲は、100 ～ 300 エントリです。

ステップ 6　次のいずれかをクリックします。

- 変更をサーバに保存するには [Save] または [Apply]。
- 保存しないで終了するには [Cancel]。

ダイナミック マルチポイント VPN

DMVPN 機能により、総称ルーティング カプセル化（GRE）トンネル、IP Security（IPSec）暗号化、および Next Hop Resolution Protocol（NHRP）を組み合わせて、IPSec VPN にスケーラビリティを向上できます。

一般的な VPN 接続は、2 台のルータを接続するポイントツーポイント IPSec トンネルです。DMVPN を使用すると、中央ハブから IPSec トンネルで GRE を使用して、他のリモート ルータ（スポークと呼ばれる）が接続されたネットワークを作成できます。IPSec トラフィックは、そのハブを通じ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 では、ルータを DMVPN ハブまたは DMVPN スポークとして設定できます。ルータは次のように設定できます。

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 およびトンネル パラメータ
- Next Hub Server（NHS）サーバ（任意）

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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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。オプションは [Spoke]、[Hub]、および [Dynamic Connection between Spokes] です。

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 アドレスとサブネット マスクを入力します。

ステップ 8　[NHRP and Tunnel Parameters] セクションで、[Network ID]、[Hold Time]、[NHRP Authentication String]、[Tunnel Key]、[Bandwidth]、[MTU]、[Tunnel Throughput Delay]、および [TCP Maximum Segment Size] の各情報を入力します。

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、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 [Name] に入力し、ドロップダウン リストからセキュリティ プロトコルとアルゴリズムの許容される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] を有効にして、トランスフォーム セットの IP 圧縮を有効にします。トランスフォーム セットのモードを選択します。オプションは [Tunnel] モードまたは [Transport] モードです。

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の IP アドレス、および [Fallback Time] を入力します。デバイスがクラスタをサポートしている場合は、[Cluster ID]、[Max Connection]、[Hub IP address]、および [Priority] などのネクスト ホップ サーバ情報を追加します。

（注）　NHS サーバ情報は、スポークの設定だけに必要です。[Use Cluster for NHS] チェックボックスをオンにした場合は、[Cluster ID]、[Max Connection]、および [Next Hub Server] などの情報を追加します。NHS クラスタ設定があるテンプレートは、Cisco IOS Software バージョン 15.1(2)T 以降を実行しているデバイスだけに適用されます。

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

（注）　このルーティング情報は、ハブ設定だけに必要です。

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。または、EIGRP 番号を入力します。その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] ページの要素のリストを示します。

表 6-11　[DMVPN] ページ

要素	フィールドの説明
[Device Role and Topology] タブ	
[Spoke] オプション ボタン	トポロジ内のスポークとしてルータを設定するには、[Spoke] オプション ボタンをオンにします。
[Hub] オプション ボタン	トポロジ内のハブとしてルータを設定するには、[Hub] オプション ボタンをオンにします。
Dynamic Connection between Spokes	スポーク間のダイナミック接続を設定するには、[Create Dynamic Connection between spokes] チェックボックスをオンにします。
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 のネットワーク 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、グローバルに一意の 32 ビット ネットワーク ID です。範囲は 1 ～ 4294967295 です。
Hold Time	Next Hop Resolution Protocol（NHRP）の NBMA アドレスが有効なもの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 インターフェイスに対してキー ID を有効にするために使用されます。値の範囲は 0 ～ 4294967295 です。
Bandwidth	意図する帯域幅を 1 秒あたりのキロバイト数（kbps）単位で入力します。
MTU	特定のインターフェイスで送信される 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 インターフェイスに対するデフォルト値は 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。トンネルの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。トランスフォーム セット プロファイルを追加するには、[Add] ボタンをクリックします。
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。ペイロードを暗号化するため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ためのモードを指定します。
IP Compression	ペイロードを圧縮するには、[IP Compression] チェックボックスをオンにします。
NHS Server	

表 6-11　[DMVPN] ページ（続き）

要素	フィールドの説明
Use Cluster For NHS	[Use Cluster For NHS] チェックボックスをオンにして、[Cluster ID]、[Max Connections]、[Hub's Physical IP Address]、[Hub Tunnel IP]、および [Priority] などの情報を追加します。
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。
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	その他のルーティング プロトコルを選択するには、[Other] チェックボックスをオンにします。
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 エントリの詳細とそのサーバのプライオリティを保存し、サーバ 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、編集できないフィールドに NHS サーバが自動的に入力されます。

ステップ 15　[OK] をクリックして、コンフィギュレーションをデバイスに保存します。

ステップ 16　加えた変更をルータへ送信せずに、すべての変更を取り消すには、[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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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 [Hub and Spoke] を選択し、デバイス ロールとして [Hub] または [Spoke] のいずれかを選択します。

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後、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 およびトンネル インターフェイスのパラメータ、たとえば、IP アドレス、NHRP パラメータおよびマップ、MTU 値、トンネルの送信元、トンネル モード、トンネル キーなどを設定します。

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。1 つの認証ヘッダー（AH）、1 つのカプセル化セキュリティ ペイロード（ESP）暗号化、1 つの ESP 認証、および 1 つの圧縮という、最大 4 つのトランスフォームを指定できます。これらのトランスフォームは、IPSec セキュリティのプロトコルとアルゴリズムを定義します。

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

ステップ 10　[Save] をクリックして、コンフィギュレーションをデバイスに保存します。

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 オプションを使用すると、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、ネットワーク内の他のスポークに直接 IPSec トンネルを確立できるスポークとして、ルータを設定できます。

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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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 トポロジを持つ 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 トポロジとして設定します。

ステップ 6　ハブ アンド スポーク トポロジの設定の項のステップ 6 からステップ 8 を繰り返します。このページの要素については、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 トポロジでは、[NHS Server Information] セクションで、次のハブのサーバ情報、たとえば、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 アドレスなどを追加します。

ステップ 8　[Save] をクリックして、コンフィギュレーションをデバイスに保存します。

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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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 ロールをスポークとして設定します。

ステップ 6　ハブ アンド スポーク トポロジの設定の項のステップ 6 からステップ 8 を繰り返します。このページの要素については、表 6-11 を参照してください。

（注）　デバイスで IOS のバージョン 15.1(2)T 以降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情報を設定し、[Cluster-ID] と [Maximum Connection] の値を追加します。

ステップ 8　[Expand Row] ボタン（オプション ボタンの横）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　再び [Save] ボタンをクリックして、クラスタ設定の含まれた NHS グループ情報を保存します。これにより、テーブルに NHS サーバ IP アドレスが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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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] ページが開きます。

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　[Ok] をクリックして、編集した DMVPN トンネル設定をデバイスに送信します。

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　デバイスを選択後、[Configuration] をクリックします。[Feature Selector] の左パネルが表示されます。

ステップ 4　[Feature Selector] の左パネルから、[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。

警告メッセージに対して [Yes] をクリックし、選択したトンネルを削除します。[Edit DMVPN Tunnel] ページの要素については、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、警告メッセージに対して [No] をクリックします。

ステップ 7　加えた変更をルータへ送信せずに、すべての変更を取り消すには、[Cancel] をクリックします。

GETVPN

Group Encrypted Transport VPN（GETVPN）展開には、キー サーバ（KS）、グループ メンバ（GM）、およびドメイン オブ インタープリテーション（GDOI）プロトコルという、3 つの主要コンポーネントがあります。GM はトラフィックを暗号化/復号化し、KS はすべてのグループ メンバに暗号キーを配布します。KS は、ある一定期間の 1 つだけのデータ暗号化キーを決定します。すべての GM が同じキーを使用するため、すべての GM は他のすべての GM によって暗号化されたトラフィックを復号化することができます。GDOI プロトコルは、GM と KS の間でグループ キーおよびグループのセキュリティ アソシエーション（SA）管理に使用されます。GETVPN 展開には、最小 1 つの KS が必要です。

従来の IPSec 暗号化ソリューションとは異なり、GETVPN ではグループ SA の概念が使用されます。GETVPN グループ内のすべてのメンバは、共通の暗号化ポリシーと共有 SA を使用して互いに通信することができます。したがって、GM 間でピアツーピア ベースの IPSec のネゴシエーションを行う必要はなく、これによって GM ルータにかかるリソースの負荷が軽減されます。

グループ メンバ

GM は、グループ内のデータ トラフィックを暗号化するために必要な IPSec SA を取得するために、キー サーバに登録します。GM はグループ識別番号を KS に提供して、それぞれのグループのポリシーとキーを取得します。これらのキーは、トラフィックのロスがないよう、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。

キー サーバ

KS は、セキュリティ ポリシーを保守し、GM を認証し、トラフィック暗号化用のセッション キーを提供する処理を担当します。KS は、個々の GM を登録時に認証します。GM は登録が成功した場合のみ、グループ SA に参加できます。

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 に登録するときに、KS は GM のグループ識別番号を検証します。この識別番号が有効で、GM が有効なインターネット キー エクスチェンジ（IKE）クレデンシャルを提供した場合、KS は SA ポリシーとキーをグループ メンバに送信します。

GM が KS から受け取るキーには、キー暗号化キー（KEK）とトラフィック暗号キー（TEK）という 2 つのタイプがあります。TEK は、同じグループ内のグループ メンバ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 の間でキーの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、キーの再生成メッセージを送信します。キーは、キーの再生成時にマルチキャストかユニキャストのいずれかのトランスポートを使用して配布できます。マルチキャスト方式は、それぞれのグループ メンバに個別にキーを送信する必要がないため、拡張性に優れています。ユニキャストの場合と異なり、

KS は GM から、マルチキャストのキー再生成方式で再生成されたキーの受け取りが成功したことについて、確認応答を受け取りません。ユニキャストのキー再生成方式では、KS は GM から 3 回連続してキーの再生成の確認応答がなかった場合、その特定の 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 の管理に使用されます。GDOI では、GM と KS の認証に Internet Security Association Key Management Protocol（ISAKMP）が使用されます。GETVPN には、RSA 署名（証明書）や事前共有キーなど、標準的なすべての ISAKMP 認証スキームを使用できます。

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 を使用すると、GETVPN を設定できます。GETVPN を設定するには、次のものを設定する必要があります。

- グループ メンバ
- キー サーバ

GETVPN グループ メンバの作成

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

GETVPN グループ メンバを作成するには、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てから、デバイスを設定します。デバイスの詳細が画面の下部に表示されます。

ステップ 3　デバイスを選択後、[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 GETVPN グループ メンバを作成します。

ステップ 5　[Add GroupMember] ダイアログボックスで [General] タブを選択し、[Group Name] および [Group Identity] を入力します。ドロップダウン リストから [Registration Interface] 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　次のいずれかをクリックします。

- コンフィギュレーションを保存するには [Save]。
- 変更内容を保存しないで終了するには [Cancel]。

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 [Local Exception ACL] および [Fail Close ACL] を選択します。

ステップ 9　[Add Group Member] ダイアログボックスで [Migration] タブを選択し、[Enable Passive SA] チェックボックスをオンにして Passive SA を有効にします。このグループ メンバでパッシブ SA モードをオンにするには、このオプションを使用します。

表 6-12 に [GETVPN GroupMember] ページの要素のリストを示します。

表 6-12　[GETVPN Group Member] ページ

要素	フィールドの説明
General	
Group Name	GETVPN グループの名前を入力します。
Group Identity	GETVPN グループの一意の識別情報を入力します。これには、番号か IP アドレスを指定できます。範囲は 0 ～ 2147483647 です。
Registration Interface	クリプト マップを関連付ける必要が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	クライアントを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 ポリシーを作成してすべてのグループ メンバに配布する処理、およびセカンダリ キー サーバと定期的に同期する処理を担当します。プライオリティが最も高いサーバが、プライマリ キー サーバとして選択されます。
Secondary Key Server	プライマリ キー サーバの登録に失敗した場合に、グループ メンバが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。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グループ メンバを設定できます。グループ メンバの設定によって、登録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	セカンダリ キー サーバを追加するには、[Add Row] ボタンをクリックします。
Delete	セカンダリ キー サーバを削除するには、[Delete] ボタンをクリックします。
[Advanced] タブ	
Local Exception ACL	暗号化から除外する必要があるトラフィックの ACL を選択します。
Fail Close ACL	グループ メンバがキー サーバに登録されるまで、クリア テキストで送信する必要があるトラフィックの ACL を選択します。フェール クローズ機能を設定した場合、グループ メンバを通過するすべてのトラフィックは、グループ メンバが正常に登録されるまでドロップされます。グループ メンバが正常に登録され、SA がダウンロードされた後、この機能は自動的にオフになります。
[Migration] タブ	
Enable Passive SA	グループ メンバでパッシブ SA モードをオンにするには、このオプションを使用します。パッシブ SA モードでは、キー サーバの受信専用 SA オプションが上書きされ、すべての発信トラフィックが暗号化されます。

ステップ 10　次のいずれかをクリックします。

- テーブルにグループ メンバを追加するには [Ok]。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。スケジュール展開後、コンフィギュレーションがデバイスに適用されます。
- 加えた変更をルータへ送信せずに、すべての変更を取り消すには [Cancel]。
- ページを閉じるには [Close]。

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てから、デバイスを設定します。デバイスの詳細が画面の下部に表示されます。

ステップ 3　デバイスを選択後、[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] の左パネルから、[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 [Group Name]、[Group Identity]、[WAN IP address]、および [Priority] を入力します。

ステップ 6　[Co-operative Key Server] 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、共同キー 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。[Multicast IP Address]、[KEK Lifetime]、[TEK Lifetime]、[Retransmit Key]、[RSA Key for Rekey Encryption]、および [Rekey Encryption Method] 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、暗号化するトラフィック、[Encryption Policy]、および [Anti Replay] を入力します。

表 6-13 に [GETVPN KeyServer] ページの要素のリストを示します。

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 グループの一意の識別情報を入力します。これには、番号または IP アドレスを指定できます。範囲は 0 ～ 2147483647 です。
WAN IP Address	WAN IP アドレスを入力します。これは、このキー サーバに関連付けるインターフェイスの IP アドレスです。
Co-operative Key Server	プライマリ キー サーバの登録に失敗した場合に、グループ メンバがフォールバックする共同キー サーバの IP アドレスを指定します。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グループ メンバを設定できます。グループ メンバの設定によって、登録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	共同キー サーバを追加するには、[Add Row] ボタンをクリックします。
Delete Row	共同キー サーバを削除するには、[Delete Row] ボタンをクリックします。
Rekey	
[Distribution Method] オプション ボタン	配布方法を選択します。この配布方法は、キー サーバからグループ メンバにキー再生成情報を送信するために使用されます。オプションは、[Unicast] または [Multicast] です。
Multicast IP Address	配布方法としてマルチキャストを選択した場合は、キー再生成を送信する必要が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（秒）を入力します。範囲は 120 ～ 86400 です。
TEK Lifetime	TEK ライフタイム（秒）を入力します。範囲は 120 ～ 86400 です。
Retransmit Key	再生成されたキーの再送信の頻度と期間を秒単位で入力します。
RSA Key for Rekey Encryption	キー再生成情報を暗号化するために使用する RSA キーの詳細を入力します。
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	

表 6-13　[GETVPN Key Server] ページ（続き）

要素	フィールドの説明
Traffic to Encrypt	メンバ間で暗号化する必要があるトラフィックの ACL をドロップダウン リストから選択します。このアクセス リストでは、暗号化するトラフィックが定義されます。「permit」行と一致するトラフィックだけが、暗号化されます。 （注）　暗号化セッションが動作していない場合でも常に許可する必要がある特定のトラフィックは、暗号化しないでください。
Encryption Policy	トラフィックを暗号化するために使用するトランスフォーム セットをドロップダウン リストから選択します。ピア間のトラフィックを暗号化するために使用す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　次のいずれかをクリックします。

- テーブルにグループ メンバを追加するには [Ok]。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。スケジュール展開後、コンフィギュレーションがデバイスに適用されます。
- 加えた変更をルータへ送信せずに、すべての変更を取り消すには [Cancel]。

ステップ 10　[Close] をクリックして、ページを閉じます。

GETVPN グループ メンバまたはキー サーバの編集

既存の GETVPN グループ メンバまたは 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てから、デバイスを設定します。デバイスの詳細が画面の下部に表示されます。

ステップ 3　デバイスを選択後、[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] 要約ページが開きます。

ステップ 5　GETVPN の要約ページから、グループ名を選択して [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] ページの要素については、表 6-12 および表 6-13 を参照してください。

ステップ 7　次のいずれかをクリックします。

- コンフィギュレーションを保存するには [OK]。
- 加えた変更をルータへ送信せずに、すべての変更を取り消すには [Cancel]。

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 メンバまたはキー サーバの削除

既存の GETVPN グループ メンバまたは 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てから、デバイスを設定します。デバイスの詳細が画面の下部に表示されます。

ステップ 3　デバイスを選択後、[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] 要約ページが開きます。

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

ステップ 6　次のいずれかをクリックします。

- コンフィギュレーションを保存するには [OK]。
- 加えた変更をルータへ送信せずに、すべての変更を取り消すには [Cancel]。

ステップ 7　[Close] をクリックして、ページを閉じます。

VPN のコンポーネント

VPN のコンポーネントには、主に次のものが含まれています。

- 「IKE ポリシー」（P.6-27）
- 「IKE 設定」（P.6-30）
- 「IPsec プロファイル」（P.6-31）
- 「事前共有キー」（P.6-32）
- 「RSA キー」（P.6-33）
- 「トランスフォーム セット」（P.6-35）

IKE ポリシー

インターネット キー エクスチェンジ（IKE）は、セキュアな認証された通信を設定するための標準的な方式です。IKE では、ネットワークを介した 2 つのホストの間にセッション キー（およびそれに関連した暗号とネットワークの設定）が確立されます。IKE ポリシーは、認証のときにピアの識別情報を保護します。

IKE ネゴシエーションは保護される必要があります。このため、それぞれの IKE ネゴシエーションは、共通する（共有されている）IKE ポリシーについて合意しようとする各ピアによって開始されます。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ついて合意した後、そのポリシーのセキュリティ パラメータが、ピアごと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。それらのセキュリティ アソシエーションは、ネゴシエーションの間、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。ライフタイムが同一でない場合は、リモート ピアのポリシーのライフタイムよりも短い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 ポリシー機能を使用すると、IKE ポリシーの作成、編集、および削除ができます。

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] を選択後、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、そのデバイスを設定します。デバイスの詳細が画面の下部に表示されます。

ステップ 2　デバイスを選択後、[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 ポリシーの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] ページの要素のリストを示します。

表 6-14　[IKE Policies] ページ

要素	説明
IKE Policies	
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、ネゴシエーションする 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 署名を選択します。 • [Pre-SHARE]：事前共有キーを使用して認証が実行されます。 • [RSA_SIG]：デジタル署名を使用して認証が実行されます。

表 6-14　[IKE Policies] ページ（続き）

要素	説明
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 ピア間の共有秘密キーを互いに送信することなく実行するために使用されます。係数が大きいほどセキュリティが強化されますが、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。次のオプションがあります。 • [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	IKE プロポーザルで使用されるハッシュ アルゴリズムをドロップダウン リストから選択します。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、総当たり攻撃に対して、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。
Lifetime	セキュリティ アソシエーション（SA）のライフタイム（秒数）。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ション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　次のいずれかをクリックします。

- コンフィギュレーションを保存するには [Save]。
- 変更内容を保存しないで終了するには [Cancel]。
- CLI コマンドを生成するには、再び [Save]。

IKE 設定

IKE 設定機能を使用すると、ピア ルータに対して IKE をグローバルに有効にすることができます。

IKE 設定の作成

IKE ポリシーを有効にして、IKE をアグレッシブ モードに設定するには、次の手順を実行します。

ステップ 1　[Operate] > [Device Work Center] を選択後、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、そのデバイスを設定します。デバイスの詳細が画面の下部に表示されます。

ステップ 2　デバイスを選択後、[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　IKE ポリシーとアグレッシブ モードを有効にするには、[Enable IKE] および [Enable Aggressive Mode] チェックボックスをオンにします。

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

ステップ 6　[Dead Peer Detection Keepalive] および [Dead Peer Detection Retry] の時間を秒単位で入力します。

表 6-15 に [IKE Settings] ページの要素のリストを示します。

表 6-15　[IKE Settings] ページ

要素	説明
IKE Settings	
Enable IKE	IKE をグローバルに有効にするには、[Enable IKE] チェックボックスをオンにします。デフォルトで、IKE は有効になっています。インターフェイスごとに IKE を有効にする必要はなく、ルータ側ですべてのインターフェイスに対してグローバルに有効にすることができます。 IP Security（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 を無効にすることができます。あるピアに対して IKE を無効にする場合は、すべての IPSec ピアに対して IKE を無効にする必要があります。
Enable Aggressive Mode	Internet Security Association and Key Management Protocol（ISAKMP）アグレッシブ モードを有効にするには、[Enable Aggressive Mode] チェックボックスをオンにします。このアグレッシブ モードを無効にした場合、デバイスに対するすべてのアグレッシブ モード要求と、デバイスから出された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 identity] を選択します。オプションは、[IP address]、[Distinguished Name]、および [HostName] です。ISAKMP 識別情報は、事前共有キーまたは RSA 署名の認証を指定した場合は常に設定されます。原則として、ピアの識別情報はすべて同じ方法で（IP アドレスまたはホスト名のいずれかで）設定してください。 • [IP Address] : ISAKMP 識別情報を、IKE ネゴシエーションのときにリモート ピアと通信するために使用するインターフェイスの IP アドレスに設定します。 • [Distinguished Name] : ISAKMP 識別情報を、ルータ証明書の識別名（DN）に設定します。 • [Host Name] : ISAKMP 識別情報を、ドメイン名と連結されたホスト名（例：myhost.example.com）に設定します。

表 6-15　[IKE Settings] ページ（続き）

要素	説明
Dead Peer Detection Keepalive	ゲートウェイによるピアへの DPD メッセージの送信を有効にします。DPD は、ルータがインターネット キー エクスチェンジ（IKE）ピアの活性を照会するために使用できるキープアライブ スキームです。 DPD メッセージの間隔を、[DPD Keepalive] フィールドに秒数で指定します。範囲は 10 ～ 3600 秒です。
Dead Peer Detection Retry	DPD メッセージが失敗した場合の再試行の間隔を、[DPD Retry] に秒数で指定します。範囲は 2 ～ 60 秒です。

ステップ 7　次のいずれかをクリックします。

- コンフィギュレーションを保存するには [Save]。
- ページを更新するには [Refresh]。

IPsec プロファイル

IPsec プロファイルは ISAKMP プロファイルとも呼ばれ、これを使用すると、一連の IKE パラメータを定義して 1 つ以上の IPSec トンネルに関連付けることができます。IPsec プロファイルは、その一致識別基準の概念によって一意に識別された着信 IPSec 接続に、パラメータを適用します。これらの基準は、着信 IKE 接続によって提示された IKE 識別情報に基づいており、この識別情報には、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 グループ）が含まれます。

IPsec プロファイルの作成、編集、および削除

IKE プロファイル機能を使用すると、IPsec プロファイルの作成、編集、および削除ができます。

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] を選択後、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、そのデバイスを設定します。デバイスの詳細が画面の下部に表示されます。

ステップ 2　デバイスを選択後、[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、[Name]、[Description]、[Transform Set]、[IPsec SA Lifetime] などの情報を入力します。

ステップ 5　IPsec プロファイルの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] ページの要素のリストを示します。

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場合、IPsec プロファイルの名前を編集することはできません。
Description	追加または編集している 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。このルータ上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ます。
IPsec SA Lifetime	設定した期間が経過した後に新しい SA を確立するための、[IPSec SA Lifetime] を入力します。この時間は秒数で入力します。範囲は 120 ～ 86400 です。

ステップ 7　次のいずれかをクリックします。

- コンフィギュレーションを保存するには [Save]。
- 変更内容を保存しないで終了するには [Cancel]。
- CLI コマンドを生成するには、再び [Save]。

事前共有キー

事前共有キー機能を使用すると、2 つのピア間で秘密キーを共有できます。また、この機能は認証フェーズで IKE によって使用されます。

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] を選択後、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、そのデバイスを設定します。デバイスの詳細が画面の下部に表示されます。

ステップ 2　デバイスを選択後、[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 Address]、[Host Name]、[Subnet Mask]、および [Pre-Shared Keys] を入力します。

ステップ 5　事前共有キーの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] ページの要素のリストを示します。

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、そのキーを再入力して事前共有キーを確認します。

ステップ 7　次のいずれかをクリックします。

- コンフィギュレーションを保存するには [Save]。
- 変更内容を保存しないで終了するには [Cancel]。
- コンフィギュレーションを保存して CLI コマンドを生成するには、再び [Save]。

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] を選択後、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、そのデバイスを設定します。デバイスの詳細が画面の下部に表示されます。

ステップ 2　デバイスを選択後、[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、[Label]、[Modulus]、および [Type] を入力します。

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

ステップ 7　次のいずれかをクリックします。

- コンフィギュレーションを保存するには [OK]。
- 変更内容を保存しないで終了するには [Cancel]。

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ためのパスワードを入力します。キー タイプが汎用キー、署名、または暗号の場合は、保存された公開キーと秘密キーのデータをコピーして貼り付けます。用途キーをインポートするには、署名キーと暗号キーの両方の公開および秘密キー データを入力します。

ステップ 10　次のいずれかをクリックします。

- RSA キーをインポートするには [Import]。
- 変更内容を保存しないで終了するには [Close]。

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 キーを暗号化するための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] ページの要素のリストを示します。

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。
Modulus	キー モジュラス値を入力します。モジュラス値が 512 ～ 1024 の範囲内の場合は、64 の倍数（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 よりも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。モジュラスが大きいほどキーの安全性は高くなりますが、大きなモジュラスのキーは生成に要する時間が長くなり、大きなキーほど暗号化/復号化の処理にかかる時間が長くなります。
Type	生成する RSA キーのタイプを選択します。オプションは [General Purpose]、[Usages Keys]、[Encryption Keys]、および [Signature Keys] です。
Make Key Exportable	RSA キーをエクスポート可能なキーとして生成し、このキーを別の場所に保存するには、[Make the Key exportable] チェックボックスをオンにします。
Import RSA Key	
Decryption Password	復号化パスワードを入力します。
Key Type	インポートするキーのタイプをドロップダウン リストから選択します。オプションは [General purpose]、[Usages keys]、[Encryption Keys]、および [Signature keys] です。
PEM-formatted Public Key or Certificate	PEM-formatted 公開キーまたは証明書を入力します。キーをエクスポートする間に生成された公開キー データです。
PEM-formatted Encrypted Private Key	PEM-formatted 暗号秘密キーを入力します。キーをエクスポートする間に生成された秘密キー データです。
Export RSA Key	
Encryption Password	暗号化パスワードを入力します。
Encryption Algorithm	暗号化アルゴリズムを選択します。

ステップ 13　次のいずれかをクリックします。

- エクスポートされたキーを表示するには [OK]。
- 変更内容を保存しないで終了するには [Cancel]。

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同意します。

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] を選択後、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、そのデバイスを設定します。デバイスの詳細が画面の下部に表示されます。

ステップ 2　デバイスを選択後、[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、[Name] を入力し、トランスフォーム セットを設定するために有効なセキュリティ プロトコルとアルゴリズムの組み合わせを選択します。トランスフォーム セットのモードを指定します。オプションは [Tunnel] モードまたは [Transport] モードです。

ステップ 5　トランスフォーム セットの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] ページの要素のリストを示します。

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。ペイロードを暗号化するために使用するアルゴリズムです。次のオプションがあります。 • 128 ビット Advanced Encryption Standard（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。

表 6-19　[Transform Set] ページ（続き）

要素	説明
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。ペイロードの整合性をチェックするために使用するアルゴリズムです。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）（Hash-based Message Authentication Code（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 圧縮を有効または無効にします。
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] : データだけを暗号化します。トランスポート モードは、両方のエンドポイントが IPsec をサポートしている場合に使用されます。トランスポート モードでは、認証ヘッダーまたはカプセル化されたセキュリティ ペイロードが元の IP ヘッダーの後に置かれます。これにより、IP ペイロードだけが暗号化されます。この方式を使用すると、暗号化されたパケットに Quality of Service（QoS）制御などのネットワーク サービスを適用できます。 • [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 モードよりも強力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 モードを使用すると、ルータなどのネットワーク デバイスを複数の VPN ユーザ用の IPsec プロキシとして機能させることができます。トンネル モードは、そのような設定で使用してください。

ステップ 7　次のいずれかをクリックします。

- コンフィギュレーションを保存するには [Save]。
- 変更内容を保存しないで終了するには [Cancel]。
- コンフィギュレーションの変更を保存するには、再び [Save]。

ゾーンの概要

Zone Based Firewall（ZBFW）機能を使用すると、ゾーンと呼ばれるインターフェイス グループの間で 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。

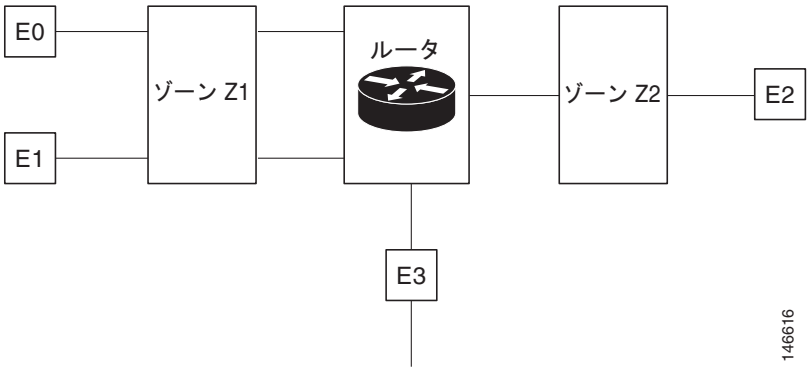
セキュリティ ゾーン

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 メンバのインターフェイスとの間で両方向のトラフィックを許可するには、そのゾーンをゾーン ペアに含めて、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場合、トラフィックはインターフェイスを通過できます。

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 ゾーンのメンバでもありません。

このシナリオでは、次のような状況になっています。

- インターフェイス E0 と E1 は同じセキュリティ ゾーン（Z1）のメンバなので、この 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（たとえば、E0 と E2 の間、E1 と E2 の間、E3 と E1 の間、および E3 と E2 の間）でトラフィックは流れません。
- E0 または E1 と E2 のインターフェイス間でトラフィックを流すことができるのは、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ている場合だけです。
- E3 は、どのセキュリティ ゾーンにも属していないため、E3 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まったくありません。

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.6-38）
- 「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.6-43）
- 「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

この機能を使用すると、Transmission Control Protocol（TCP）または User Datagram Protocol（UDP）ポートをアプリケーションに割り当てたり、割り当てを解除することができます。

（注）　[Save] または [Delete] ボタンをクリックすると、変更がデバイスに展開されます。要求された処理の CLI を調べることはできず、また、保留中の変更キューからの処理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 の内容を変更することはサポートされておらず、予期しない動作の原因になる場合があります。

アプリケーションの編集

アプリケーションに TCP/UDP ポートを割り当てるか、その割り当てを解除するには、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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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　アプリケーションに TCP/UDP ポートを割り当てるか、その割り当てを解除するには、アプリケーションをクリックし、その TCP/UDP ポート値を更新します。

a. 1 つ以上のポートをコンマで区切って定義することにより、ポートを割り当てます（例：1234, 2222 など）。

b. ポート範囲を定義することにより、ポートを割り当てます（例：1111-1118）。ポートのグループまたはポート範囲を割り当てることもできます。

c. 既存のポート値を削除することにより、ポートの割り当てを解除します。

表 6-20 に [Applications] ページの要素のリストを示します。

表 6-20　[Applications] ページ

要素	説明
Application Name	デバイスから実行されるアプリケーション名が表示されます。
TCP Ports	（任意）特定のアプリケーションに割り当てられた TCP ポートの値です。
UDP Ports	（任意）特定のアプリケーションに割り当てられた UDP ポートの値です。

ステップ 6　[Save] をクリックして、コンフィギュレーションを保存します。

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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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 マップ値を変更します。

（注）　デフォルト パラメータを変更できるのは ISR デバイスだけです。

ステップ 6　[Save] をクリックして、コンフィギュレーションを保存します。

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汎用設定情報を使用して設定された論理インターフェイス、または特定ユーザに共通の設定のために設定された論理インターフェイスです。ゾーン メンバ情報は、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になります。

インターフェイスの設定

ゾーンにインターフェイスを割り当てるか、特定のゾーンからインターフェイスの割り当てを解除するには、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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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すでにゾーンに割り当てられている場合は、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、警告メッセージに対して [Yes] をクリックします。

ステップ 8　特定のゾーンからインターフェイスの割り当てを解除するには、その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] ページの要素のリストを示します。

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する Security-Zone の名前です。
VRF	インターフェイスが属する VRF の名前です。

ステップ 9　次のいずれかをクリックします。

- 変更を保存して適用するには [Save]。
- 保存しないで終了するには [Cancel]。

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 ポリシー規則の作成、既存のポリシー規則の変更、ポリシー規則の削除、およびポリシー規則の順序の変更ができます。ファイアウォール ポリシー規則を作成する場合、ポリシー テーブル内の位置は任意に定義できます。

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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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] で [Add Rule] ボタンをクリックし、[Name]、[Source Zone]、[Destination Zone]、[Source] の IP アドレス、[Destination] の IP アドレス、[Service]、および [Action] などの情報を入力します。送信元ゾーンと宛先ゾーンは、異なるゾーンにする必要があります。規則を移動するには、[Add Rule] ボタンの下矢印アイコンをクリックします。規則をリストの一番上または一番下に配置したり、リスト内の選択した規則の前や後ろに移動することができます。

（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指定しなかった場合は、システムでファイアウォール規則の名前が生成されます。たとえば *rule_1* のように、*rule_<number>* または *EMS_rule_<number>* の形式を使用してファイアウォール規則名を作成することはできません。これらは、システムで予約済みの形式です。

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で、値を any に設定するには、[Any] チェックボックスをオンにします。

a. 送信元および宛先 IP アドレスを入力します。

b. 新しい IP アドレスおよび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. コンフィギュレーションを保存するには、[OK] をクリックします。

e. 加えた変更をルータへ送信せずに、すべての変更を取り消すには、[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、検査するアプリケーションを選択するには、[Application] チェックボックスをオンにします。

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

c. ナビゲーション用矢印ボタンを使用して、前後に移動します。

d. コンフィギュレーションを保存するには、プラス 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。オプションは [Drop]、[Drop and Log]、[Inspect]、[Pass]、および [Pass and Log] です。

ステップ 9　検査アクションを選択した場合は、[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 10　[Advanced Parameters Configuration] ダイアログボックスで、次のようにします。

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て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. カーソルを [Advanced Options] アイコンの上に置くと、設定された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] ページの要素のリストを示します。

表 6-22　[Policy Rule] ページ

要素	説明
Name	（任意）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、トラフィックの起点となるゾーンの名前を指定します。
Destination Zone	宛先ゾーンの名前を入力します。宛先ゾーンは、トラフィックの宛先となるルータの名前を指定します。
Source	検査対象のデータの送信元 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 アドレス • サブネット

表 6-22　[Policy Rule] ページ（続き）

要素	説明
Destination	検査対象のデータの宛先 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 アドレス • サブネット
Service	検査されるデータのサービスです。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.6-38）を参照 • サービス。「サービスの管理」（P.6-43） • ACL ベースのアプリケーション：TCP、UDP、ICMP
Action	規則条件に一致するものがあったときに、トラフィックに対して実行するアクションを選択します。次の場合に規則が一致します。 • トラフィックの送信元 IP が送信元規則条件と一致。 • トラフィックの宛先 IP が宛先規則条件と一致し、トラフィックの検査対象のサービスがサービス規則条件と一致。 アクションのオプションは次のとおりです。 • Drop • Drop and Log • Inspect • Pass • Pass and Log
Advance Options	[Action] オプションが [Inspect] に設定されているときに、ファイアウォール ルール パラメータマップ動作を設定するコンフィギュレーション 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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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、次のいずれかのオプションを選択します。

a.　規則のパラメータ行をクリックし、パラメータを編集します。または

b. 規則を選択するチェックボックスをオンにして、[Edit] ボタンをクリックします。選択された規則エンティティが編集用に開かれます。

ステップ 6　[Save] をクリックして、変更をデバイスに適用します。

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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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、規則を選択するチェックボックスをオンにして、[Delete] ボタンをクリックします。

ステップ 6　警告メッセージに対して [Ok] をクリックし、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。

ファイアウォールの規則の順序の変更

クラスのデフォルトの規則は、常にリストの一番下に表示され、その位置は固定されています。通常の規則をクラスのデフォルト規則よりも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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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、規則を特定の行まで移動するには、その規則を新しい位置までドラッグ アンド ドロップします。

サービスの管理

この機能を使用すると、サービス要素の作成、更新、または削除ができます。TCP/UDP ポートをアプリケーションに割り当てたり、その割り当てを解除することができます。

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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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、[Service Name] 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（複数を選択可能）。

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] ページの要素のリストを示します。

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、この名前を変更することはできません。また、アプリケーションを指定しないでサービスを作成することもできません。
Application	[Service] 内にグループとしてまとめられた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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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、次のようにします。

a. サービスのパラメータ行をクリックし、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かれます。新しいアプリケーションを追加したり、選択済みのアプリケーションを削除することができます。

c. 選択され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、コンフィギュレーションを保存します。

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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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、サービスを選択して [Delete] ボタンをクリックします。

ステップ 6　警告メッセージに対して [Ok] をクリックし、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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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、[Zone Name] 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 ゾーンに割り当てることができるインターフェイスに影響を及ぼします。

b.　ユーザがデフォルトの VRF オプションを選択した場合、セキュリティ ゾーンは他のどの VRF にも関連していないインターフェイスにのみ割り当てることができます。

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（複数を選択可能）。

b. コンフィギュレーションを保存するには、[OK] をクリックします。

c. 加えた変更をルータへ送信せずに、すべての変更を取り消すには、[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、次のようにします。

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

b. [Maximum Detection] チェックボックスをオンにし、最大検出数を設定します。

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

d. [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て 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します。

ステップ 10　次のいずれかをクリックします。

- コンフィギュレーションを保存するには [OK]。
- 保存しないで終了するには [Cancel]。

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 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。カーソルを [Advanced Options] アイコンの上に置くと、設定された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が無効になっています。

表 6-24 に、[Security Zone] ページの要素のリストを示します。

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。3 つ以上のインターフェイスが存在する場合は、アイコンの上にマウスを置くと、全リストを表示できます。
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できます。
Description	（任意）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　次のいずれかをクリックします。

- 変更を保存するには [Save]。

- 保存しないで終了するには [Cancel]。

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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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、次のいずれかのオプションを選択します。

a.　ゾーンのパラメータ行をクリックし、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かれます。

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、ゾーンから既存のインターフェイスの割り当てを解除します。ゾーンの [Description] 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、コンフィギュレーションを保存します。

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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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　警告メッセージに対して [Ok] をクリックし、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。

Default-Zone 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）　Default-Zone 機能は、ASR プラットフォームだけでサポートされます。

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てから、デバイスを設定します。

ステップ 3　デバイスを選択後、[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、デバイス内のデフォルト セキュリティ ゾーンを有効または無効にします。デバイスは、どのゾーンにも関連しないすべてのインターフェイスをホスティングします。

ステップ 6　コンフィギュレーションを保存するには、[OK] をクリックします。

モニタリングでのレポートの使用

Prime NCS（WAN）のレポート作成は、問題のトラブルシューティングにはもちろん、システムのモニタリングとネットワーク状態のモニタリングに役立ちます。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スケジュール設定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できるよう指定できます。

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 NCS（WAN）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。

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

ヒント　レポートの詳細を表示するには、そのレポート タイプの横にある情報アイコンの上にカーソルを置きます。

新しいレポートの作成と実行

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横にある [New] をクリックします。

ステップ 3　レポートの詳細を入力してから、次をクリックします。

- [Save]：レポートをすぐに実行するのでなく、このレポートの設定を保存する場合。レポートはスケジュールされた時刻に自動的に実行されます。
- [Save and Run]：このレポートの設定を保存し、すぐにレポートを実行する場合。
- [Run]：レポートの設定を保存しないでレポートを実行する場合。
- [Save and Export]：レポートを保存し、結果を CSV または PDF 形式でエクスポートする場合。
- [Save and Email]：レポートを保存し、結果を電子メールで送信する場合。

スケジュール設定されたレポートの表示

現在スケジュール設定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。

保存したレポート テンプレートの表示

必要なすべてのパラメータを含んだレポートの作成後、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　次のフィールドから選択することにより、保存したどのレポート テンプレートを表示するかを選択します。

- [Report Category]：ドロップダウン リストから該当するレポート カテゴリを選択するか、[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 タイプを選択するか、[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わります。
- [Scheduled]：[All]、[Enabled]、[Disabled]、[Expired] のいずれかを選択して、[Saved Report Templates] リストをスケジューリングのステータスによってフィルタリングします。

モニタリングおよびトラブルシューティングでのパケット キャプチャの使用

Prime NCS（WAN）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、ネットワーク使用状況のモニタリング、ネットワーク統計の収集、およびネットワークの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] を選択してから、[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 NCS（WAN）ダッシュボードを使用してネットワークをモニタリングし、ネットワーク内で問題のあるデバイスを特定した後、Device Work Center を使用してデバイスのコンフィギュレーションを変更することができます。

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

ステップ 2　[Device Reachability Status] と [Top *N* Devices with Most Alarms] に報告されたデータを表示して、問題の原因を判別します。

ステップ 3　最もアラームが多く表示され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 360 度ビューが起動されます。

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。アラームを展開すると、アラームの詳細が表示されます。

ステップ 5　デバイスのコンフィギュレーションを以前の正常だったコンフィギュレーションと比較するには、[Operate] > [Device Work Center] を選択し、コンフィギュレーションを変更する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ます。次に、コンフィギュレーションのタイプと、比較するコンフィギュレーションを選択します。

ステップ 7　コンフィギュレーションを変更するかロールバックします。詳細については、デバイス コンフィギュレーション バージョンのロールバックを参照してください。