CHAPTER 4

設定用テンプレートの設計と展開

テンプレートを使用してデバイスのパラメータと設定を定義し、後から、デバイス タイプに基づいて指定されたデバイス数にそのテンプレートを展開できます。テンプレートは、新規サービスや新規サイトを実装するときの生産性を高めます。多数のデバイス間の設定変更は、時間を要する冗長な作業になる場合がありますが、テンプレートを利用して必要な設定を適用し、デバイス間の整合性を保つことにより、時間を節約できます。

表 4-1 に、テンプレートを作成し、展開するためのプロセスの説明を示します。

表 4-1　設定テンプレートを使用するためのプロセス

作業	その他の情報
1. テンプレートを作成します。	[Design] メニューで、作成するテンプレートのタイプを選択します。
2. テンプレートをパブリッシュします。	テンプレートを作成した後で、[Publish] アイコンをクリックしてテンプレートをパブリッシュし、展開できるようにします。
3. テンプレートを展開します。	[Deploy] メニューで、展開するテンプレートを選択します。
4. テンプレートの展開ステータスを確認します。	テンプレートの展開ステータスを確認するには、[Tools] > [Task Manager] > [Jobs Dashboard] を選択します。

この章の内容は、次のとおりです。

ブランチの設計および展開用テンプレートについて

同様のデバイスおよび設定のセットを使用するサイト、オフィス、またはブランチがある場合は、設定テンプレートを使用して、ブランチ内の 1 つまたは複数のデバイスに適用できる汎用設定を作成できます。また、新規のブランチがあり、そのブランチ内のデバイスに共通の設定をすばやく正確に適用する場合も、設定テンプレートを使用できます。

ブランチの展開とは

ブランチの展開とは、ブランチ ルータ用の最低限の設定を作成することです。Prime AM を利用すると、次の機能を含む一連の必須機能を作成できます。

- イーサネット インターフェイス用の機能テンプレート
- ルーティング設定用の機能テンプレート
- 必要な追加機能用の CLI テンプレート

作成するすべてのテンプレートは、ブランチ ルータに必要な個々の機能テンプレートをすべて集約する 1 つの*複合テンプレート*に追加できます。ブランチの展開操作を行うときや、他のブランチで設定を複製するために、この複合テンプレートを使用できます。

ブランチに同種のデバイスのセットが存在する場合は、「ゴールデン」設定を含む複合テンプレートを展開して、展開作業を簡略化し、デバイス構成の一貫性を保つことができます。また、複合テンプレートを使用して既存のデバイス構成と比較することにより、不一致があるかどうかを確認できます。

関連トピック

- 「ブランチ展開用の設定テンプレートの作成」（P.4-2）
- 「ブランチ展開用の複合テンプレートの作成と展開」（P.4-4）

ブランチ展開用の設定テンプレートの作成

ここでは、ブランチの展開でよく使用される設定テンプレートの作成および展開方法について説明します。

- イーサネット インターフェイスの設定テンプレートの作成
- EIGRP ルーティング設定テンプレートの作成
- RIP ルーティング設定テンプレートの作成
- CLI 設定テンプレートの作成

イーサネット インターフェイスの設定テンプレートの作成

多くのブランチ展開には、イーサネット インターフェイスの設定テンプレートが必要であり、この設定テンプレートをブランチ展開用の複合テンプレートに組み込みます。

イーサネット インターフェイスの設定テンプレートを作成するには、次の手順を実行します。

ステップ 1　[Design] > [Configuration Templates] を選択します。

ステップ 2　[Features and Technologies] フォルダの下の [Interfaces] を展開し、[Ethernet Interfaces] をクリックします。

ステップ 3　基本的なテンプレート情報を入力します。

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

ステップ 5　[Template Detail] の下の [Ethernet Interfaces] テーブルで [Add Row] をクリックします。

ステップ 6　デバイスで設定されているイーサネット インターフェイスのフィールドに入力します。（たとえば、[Interface] フィールドに「GigabitEthernet0/1」と入力する場合には、GigabitEthernet0/1 インターフェイスがデバイスに物理的に存在している必要があります）。

ステップ 7　[IP Address] フィールドに、192.168.1.1 255.255.255.0 のように、有効な IP とマスクの設定を入力します。

ステップ 8　[Save] をクリックします。

ステップ 9　[Save as New Template] をクリックします。

EIGRP ルーティング設定テンプレートの作成

多くのブランチ展開には、EIGRP ルーティング設定テンプレートが必要であり、この設定テンプレートをブランチ展開用の複合テンプレートに組み込みます。

EIGRP ルーティング設定テンプレートを作成するには、次の手順を実行します。

ステップ 1　[Design] > [Templates] > [Configuration] を選択します。

ステップ 2　[Features and Technologies] フォルダの下の [Routing] を展開し、[EIGRP] をクリックします。

ステップ 3　基本的なテンプレート情報を入力します。

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

ステップ 5　[Template Detail] の下の [EIGRP Routes] テーブルで [Add Row] をクリックします。

ステップ 6　自律システム（AS）番号と、FastEthernet0/0 などのパッシブ インターフェイスを入力し、[Auto Summary] の値を選択します。

ステップ 7　[Save] をクリックします。

ステップ 8　[Save as New Template] をクリックします。

RIP ルーティング設定テンプレートの作成

多くのブランチ展開には、RIP ルーティング設定テンプレートが必要であり、この設定テンプレートをブランチ展開用の複合テンプレートに組み込みます。

RIP ルーティング設定テンプレートを作成するには、次の手順を実行します。

ステップ 1　[Design] > [Templates] > [Configuration] を選択します。

ステップ 2　[Features and Technologies] フォルダの下の [Routing] を展開し、[RIP] をクリックします。

ステップ 3　基本的なテンプレート情報を入力します。

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

ステップ 5　[Template Detail] の下の [Enable RIP] をクリックします。

ステップ 6　RIP バージョンを選択します。

ステップ 7　[Advanced Configuration] で、次の項目を選択します。

- [IP Network List] : 10.10.10.10 などのネットワーク IP アドレスを入力します。
- [Passive Interfaces] : **FastEthernet0/0** などのパッシブ インターフェイスを入力します。

ステップ 8　[Save] をクリックします。

ステップ 9　[Save as New Template] をクリックします。

CLI 設定テンプレートの作成

多くのブランチ展開には、CLI 設定テンプレートが必要であり、この設定テンプレートをブランチ展開用の複合テンプレートに組み込みます。

CLI 設定テンプレートを作成するには、次の手順を実行します。

ステップ 1　[Design] > [Templates] > [Configuration] を選択します。

ステップ 2　[Features and Technologies] フォルダの下の [CLI Templates] を展開し、[CLI] をクリックします。

ステップ 3　基本的なテンプレート情報を入力します。

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

ステップ 5　[Template Detail] で [CLI Content] タブをクリックし、次のテキストを入力します。

```
banner motd #Welcome to Prime AM#
```

ステップ 6　[Save] をクリックします。

ステップ 7　[Save as New Template] をクリックします。

ブランチ展開用の複合テンプレートの作成と展開

デバイスにまとめて適用したい既存の機能または CLI テンプレートの集合がある場合は、複合テンプレートを作成します。複合テンプレートに包含されたテンプレートをデバイスに適用する順番を指定します。

ブランチで複製された同種のデバイスが複数存在する場合は、「マスター」複合テンプレートを作成し、ブランチ内のすべてのデバイスに展開できます。このマスター複合テンプレートは、後で新規のブランチを作成するときにも使用できます。

ステップ 1　[Design] > [Templates] > [Configuration] を選択し、[Composite Template] をクリックします。

ステップ 2　複合テンプレートのパラメータを入力します。

ステップ 3　[Validation Criteria] ドロップダウン リストから、複合テンプレートに包含されたすべてのテンプレートを適用するデバイスを選択します。たとえば、複合テンプレート内のあるテンプレートを Cisco 7200 シリーズ ルータに適用し、別のテンプレートをすべてのルータに適用する場合は、[Device Type] ドロップダウン メニューで [Cisco 7200 Series routers] を選択します。

（注）　デバイス タイプがグレー表示されている場合、そのデバイス タイプにはテンプレートを適用できません。

ステップ 4　[Template Details] で、複合テンプレートに組み込むテンプレートを選択します。

ステップ 5　矢印を使用して、デバイスに展開する順番で複合内にテンプレートを配置します。たとえば、ACL を作成してインターフェイスに関連付けるには、最初に ACL テンプレート、次にインターフェイス テンプレートの順番で配置します。

ステップ 6　[Save as New Template] をクリックします。

ステップ 7　[My Templates] フォルダに移動し、保存したテンプレートを選択します。

ステップ 8　[Publish] アイコンをクリックしてテンプレートをパブリッシュし、展開できるようにします。

ステップ 9　[Go to Deployment] アイコンをクリックし、[Deploy] > [Configuration Tasks] ページに移動します。

ステップ 10　パブリッシュしたテンプレートで、[Deploy] をクリックします。

ステップ 11　テンプレート展開オプションの指定の説明に従って、展開オプションを指定します。

ステップ 12　[OK] をクリックします。

ステップ 13　[Tools] > [Task Manager] > [Jobs Dashboard] を選択して、テンプレートの展開ステータスを確認します。

設定テンプレートの作成

Prime AM は、次のタイプの設定テンプレートを提供します。

- CLI テンプレート：独自のパラメータに基づいて作成されたユーザ定義のテンプレート。CLI テンプレートでは、設定内の要素を選択できます。Prime AM には、実際の値および論理ステートメントに置き換わる変数が用意されています。また、Cisco Prime LAN 管理システムからテンプレートをインポートできます。CLI テンプレートの作成と展開を参照してください。
- 機能およびテクノロジー テンプレート：デバイスの設定内で機能またはテクノロジーに固有の設定。機能およびテクノロジー テンプレートの作成と展開を参照してください。
- 複合テンプレート：1 つのテンプレートにグループ化される 2 つ以上の機能テンプレートまたは CLI テンプレート。複合テンプレート内のテンプレートをデバイスに展開する順番を指定します。ブランチ展開用の複合テンプレートの作成と展開を参照してください。

（注）　デバイスに展開する前に、すべてのテンプレートをパブリッシュする必要があります。

テンプレートを使用してデバイスのパラメータと設定を定義し、後から、デバイス タイプに基づいて指定されたデバイス数にそのテンプレートを展開できます。多数のデバイス間の設定変更は、時間を要する冗長な作業になる場合がありますが、テンプレートを利用して必要な設定を適用し、デバイス間の整合性を保つことにより、時間を節約できます。

デフォルト設定テンプレート

Prime AM には、デフォルト設定テンプレートが搭載されており、[Design] > [Configuration Templates] > [My Templates] > [OOTB] で見つけることができます。これらのテンプレートについては、表 4-2 を参照してください。

表 4-2　Prime AM 提供の設定テンプレート

使用する設定テンプレート	使用目的
Medianet – PerfMon	Medianet に対するパフォーマンス モニタリングを設定します。
PA with WAAS	Cisco Performance Agent[1] および Wide Area Application Services（WAAS）を設定します。
PA without WAAS	Cisco Performance Agent を WAAS なしで設定します。
Collecting Traffic Statistics	ネットワーク トラフィック統計情報を収集します。

1. Cisco Performance Agent は、Cisco IOS ソフトウェアのライセンス付き機能です。この機能は、総合的なアプリケーション パフォーマンスおよびネットワーク使用のデータを提供し、ネットワーク管理者がユーザ エクスペリエンスを正確に評価し、ネットワーク リソースの使用を最適化するのに役立ちます。

CLI テンプレートを作成するための前提条件

CLI テンプレートの作成は、エキスパート ユーザを対象とした高度な機能です。CLI テンプレートを作成する前に、次のことを確認してください。

- CLI の専門知識を持ち、理解していること。また、Apache VTL で CLI を作成できること。Apache Velocity テンプレート言語の詳細については、http://velocity.apache.org を参照してください。
- 作成する CLI を適用できるデバイスを把握していること。
- Prime AM でサポートされているデータ タイプを把握していること。
- テンプレート内の設定について理解し、手動で分類できること。

CLI テンプレートの作成と展開

CLI テンプレートを作成する前に、CLI テンプレートを作成するための前提条件で述べた前提条件を満たしていることを確認してください。

ステップ 1　[Design] > [Configuration Templates] を選択します。

ステップ 2　[CLI Template] フォルダを展開し、[CLI] をクリックします。

ステップ 3　基本的なテンプレート情報を入力します。

ステップ 4　[Validation Criteria] ドロップダウン リストから、この CLI テンプレートを適用できるデバイス タイプを選択します。

[Device Type] フィールドには、製品タイプ、製品ファミリ、およびモデル番号が表示されます。

ステップ 5　[Template Detail] の下の [Manage Variables] をクリックします。

これにより、テンプレートを展開するときの値を定義する変数を指定できます。

ステップ 6　[Add Row] をクリックし、新しい変数のパラメータを入力して、[Save] をクリックします。

ステップ 7　CLI 情報を入力します。

（注）　[CLI] フィールドには、Apache VTL を使用したコードを入力する必要があります。

ステップ 8　テンプレートに使用されるすべての変数のリストを表示するには、[Form View]（これは読み取り専用ビューです）をクリックしてから [Manage Variables] をクリックして変数を変更します。

ステップ 9　[Save As New Template] をクリックします。

ステップ 10　[My Templates] フォルダに移動し、保存したテンプレートを選択します。

ステップ 11　右上にある [Publish] アイコンをクリックして、[OK] をクリックします。

ステップ 12　[Go to Deployment] アイコンをクリックし、[Deploy] > [Configuration tasks] ページに移動します。

ステップ 13　パブリッシュしたテンプレートで、[Deploy] をクリックします。

ステップ 14　テンプレート展開オプションの指定の説明に従って、展開オプションを指定します。

ステップ 15　[OK] をクリックします。

CLI テンプレート内のデータベース変数について

デバイスが検出され、Prime AM に追加された場合、インベントリ収集時に集められたデータベース値を使用して、CLI テンプレートを作成できます。たとえば、CLI テンプレートを作成し、展開して、ブランチ内のすべてのインターフェイスをシャットダウンするには、次のコマンドを含む CLI テンプレートを作成できます。

```
#foreach ($interfaceName in $interfaceNameList)
interface $interfaceName \n
shutdown
#end
```

ここで、*$interfaceNameList* は、値が取得されるデータベースのデータベース変数タイプです。*$interfaceNameList* のデフォルト値は、`Inventory::EthernetProtocolEndpoint.IntfName` です。

interfaceNameList にデータベースの値を入力するには、以下の説明のとおりにプロパティ ファイルを作成してクエリー文字列をキャプチャし、/opt/CSCOlumos/conf/ifm/template/InventoryTagsInTemplate フォルダに保存する必要があります。

サンプル プロパティ ファイル

ファイル名：interface.properties

```
# for interface name tag->Name
EthernetProtocolEndpoint.IntfName=select u.name from EthernetProtocolEndpoint u where
u.owningEntityId =
# say for other attributes of EthernetProtocolEndpoint Model, should we define tags
# any good generic way of accepting tags -attr+its mapped query ?
```

CLI テンプレートとプロパティ ファイルを作成し、CLI テンプレートを展開すると、デバイスに次の CLI が設定されます。この出力は、デバイスに 2 つのインターフェイス（Gigabitethernet0/1 および Gigabitethernet0/0）が搭載されていることを前提としています。

```
interface GigabitEthernet0/0
shutdown
interface GigabitEthernet0/1
shutdown
```

（注）　*InterfaceNameList* は、Prime AM のデフォルトのデータベース変数です。

プロパティ ファイルに指定された Enterprise JavaBeans Query Language（EJB QL）が文字列のリストを返すことを確認してください。指定されている要素が 1 つであれば、EJB QL は、1 つの要素を含むリストを返します。

テンプレート展開オプションの指定

テンプレートをパブリッシュした後で、そのテンプレートを 1 つまたは多数のデバイスに展開する場合は、デバイス、値、およびスケジュール情報を指定して展開を調整します。表 4-3 に、展開オプションの説明を示します。

表 4-3　[Deploy] > [Configuration Task] オプション

オプション	説明
Device Selection	テンプレートを展開するデバイスのリストを表示します。
Value Assignment	設定テンプレートに以前に定義された値とは異なる変数を指定できます。名前をクリックすると、以前に定義された変数が表示されます。値を変更するには、変更する変数をクリックし、新しい値を入力して、[Apply] をクリックします。 （注）　変更した値は、展開する特定の設定にのみ適用されます。今後の展開 すべての設定テンプレートを変更するには、[Design] > [Configuration Templates] を選択して、テンプレートを変更します。
Schedule	意味のある展開ジョブ名を作成して、そのジョブを今すぐ実行するか、将来的に実行するかを指定できます。
Summary	展開オプションの選択肢がまとめられます。

機能およびテクノロジー テンプレートの作成

機能およびテクノロジー テンプレートは、デバイス構成に基づいたテンプレートです。機能およびテクノロジー テンプレートでは、デバイスの設定にある特定の機能またはテクノロジーに焦点を絞っています。デバイスを Prime AM に追加すると、Prime AM は追加されたモデルのデバイス構成を収集します。

（注）　Prime AM は、あらゆるデバイス タイプの設定可能オプションをすべてサポートしているわけではありません。設定する特定の機能またはパラメータ用の機能およびテクノロジー テンプレートが Prime AM に存在しない場合は、CLI テンプレートの作成と展開の説明に従って CLI テンプレートを作成してください。

機能およびテクノロジー テンプレートの作成と展開

機能およびテクノロジー テンプレートを作成すると、設定変更の展開を簡略化できます。たとえば、SNMP 機能およびテクノロジー テンプレートを作成し、そのテンプレートを指定のデバイスにすばやく展開できます。また、1 つまたは複数の機能およびテクノロジー テンプレートを複合テンプレートに追加できます。その場合、SNMP テンプレートを更新すると、その SNMP テンプレートを包含する複合テンプレートに最新の変更が自動的に適用されます。

ステップ 1　[Design] > [Configuration Templates] を選択します。

ステップ 2　[Features and Technologies] フォルダを展開し、適切なサブフォルダを選択してから、作成するテンプレート タイプを選択します。

ステップ 3　基本的なテンプレート情報を入力します。

ステップ 4　[Validation Criteria] ドロップダウン リストから、この機能テンプレートを適用できるデバイス タイプを選択します。[Device Type] フィールドには、製品タイプ、製品ファミリ、およびモデル番号が表示されます。

（注）　特定のデバイス タイプだけに適用する機能テンプレートを作成する場合、[Device Type] フィールドには適用可能なデバイス タイプだけが表示され、この選択肢を変更することはできません。

ステップ 5　[Template Detail] の下に CLI 情報を入力します。

ステップ 6　[Save As New Template] をクリックします。

ステップ 7　[My Templates] フォルダに移動し、保存したテンプレートを選択します。

ステップ 8　[Publish] アイコンをクリックしてテンプレートをパブリッシュし、展開できるようにします。

ステップ 9　[Go to Deployment] アイコンをクリックし、[Deploy] > [Configuration Tasks] ページに移動します。

ステップ 10　パブリッシュしたテンプレートで、[Deploy] をクリックします。

ステップ 11　テンプレート展開オプションの指定の説明に従って、展開オプションを指定します。

ステップ 12　[OK] をクリックします。

静的ルーティング テンプレートの作成と展開

テンプレートを使用して、静的ルートを設定できます。大規模で複雑なネットワークでは、静的ルートに過剰な負荷がかかる場合があります。静的ルーティング テンプレートを作成することにより、ネットワークに変更があるたびに手動で変更せずに済みます。

静的ルーティング テンプレートを作成および展開するには、次の手順を実行します。

ステップ 1　[Design] > [Configuration Templates] を選択します。

ステップ 2　[Features and Technologies] フォルダを展開し、[Routing] サブフォルダを展開して、[Static] をクリックします。

ステップ 3　基本的なテンプレート情報を入力します。

ステップ 4　[Template Detail] の下の [Add Row] をクリックして、フィールドに入力します。

（注）　[Permanent Route] の値は次のように選択してください。

- ネクストホップ インターフェイスがシャットダウンした場合またはネクストホップ IP アドレスが到達不能な場合であっても、ルートがルーティング テーブルから削除されないように指定するには、[True] を選択します。
- ネクストホップ インターフェイスがシャットダウンした場合またはネクストホップ IP アドレスが到達不能な場合に、ルートがルーティング テーブルから削除されるように指定するには、[False] を選択します。

ステップ 5　[Save As New Template] をクリックします。

ステップ 6　[My Templates] フォルダに移動し、保存したテンプレートを選択します。

ステップ 7　[Publish] アイコンをクリックしてテンプレートをパブリッシュし、展開できるようにします。

ステップ 8　[Go to Deployment] アイコンをクリックし、[Deploy] > [Configuration Tasks] ページに移動します。

ステップ 9　パブリッシュしたテンプレートで、[Deploy] をクリックします。

ステップ 10　テンプレート展開オプションの指定の説明に従って、展開オプションを指定します。

ステップ 11　[OK] をクリックします。

ACL テンプレートの作成と展開

テンプレートを作成および展開してアクセス リストを設定するには、次の手順を実行します。

ステップ 1　[Design] > [Configuration Templates] を選択します。

ステップ 2　[Features and Technologies] フォルダを展開し、[Security] サブフォルダを展開して、[ACL] をクリックします。

ステップ 3　基本的なテンプレート情報を入力します。

ステップ 4　[Template Detail] の下の [Add Row] をクリックして、表 4-4 で説明するフィールドに入力します。

表 4-4　ACL テンプレートの詳細

フィールド	説明
Name/Number	ACL の名前または番号。
Applied To	ACL を適用するルータのインターフェイスを入力します。ACL は、トラフィックの送信元に最も近いインターフェイスに適用することをお勧めします。
Type	次のどちらかを選択します。 [Standard]：標準 IP ACL は、送信元 IP アドレスに基づいてトラフィックを制御します。 [Extended]：拡張 IP ACL は、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、および宛先ポートに基づいてトラフィックを識別します。
Description	ACL の説明。

ステップ 5　[Save As New Template] をクリックします。

ステップ 6　[My Templates] フォルダに移動し、保存したテンプレートを選択します。

ステップ 7　[Publish] アイコンをクリックしてテンプレートをパブリッシュし、展開できるようにします。

ステップ 8　[Go to Deployment] アイコンをクリックし、[Deploy] > [Configuration Tasks] ページに移動します。

ステップ 9　パブリッシュしたテンプレートで、[Deploy] をクリックします。

ステップ 10　テンプレート展開オプションの指定の説明に従って、展開オプションを指定します。

ステップ 11　[OK] をクリックします。

セキュリティ設定テンプレートの作成

次の機能用のセキュリティ設定テンプレートを作成できます。

- ダイナミック マルチポイント VPN（DMVPN）
- Group Encrypted Transport VPN（GETVPN）

DMVPN テンプレートの作成

DMVPN テンプレートを作成するには、次の手順を実行します。

ステップ 1　[Design] > [Configuration] > [Features and Technologies] > [Security] > [DMVPN] を選択します。

[Dynamic Multipoint VPN Configuration Template] ページが開きます。

ステップ 2　[Template Basic] セクションの適切なフィールドに、名前と説明を入力します。

ステップ 3　[Validation Criteria] ドロップダウン リストから、デバイス タイプを選択して OS バージョンを入力します。

ステップ 4　[Template Detail] セクションで、IKE 認証および暗号化ポロシーを入力します。

ステップ 5　[IKE Authentication Type] フィールドで、プラス（+）のアンカー ボタンをクリックして、IKE 認証タイプを選択します。

デフォルトの [Pre-Shared key] を選択する場合は、秘密キーを入力して再確認する必要があります。認証タイプとして [Digital Certificate] を選択した場合には、ルータに、ルータ自体を認証するためのデジタル証明書が認証局から発行されている必要があります。

ステップ 6　[IKE Authentication Policy] セクションで、[Add Row] ボタンをクリックして IKE ポリシーを追加します。

ステップ 7　プライオリティを入力し、ドロップダウン リストから [Authentication]、[Diffie-Hellman (D-H) Group]、[Encryption]、[Hash]、および [Lifetime] を選択します。

IKE ポリシーを削除するには、ポリシーを選択して [Delete] をクリックします。

IKE ポリシーのパラメータを編集するには、行またはフィールドをクリックし、パラメータを編集します。

ステップ 8　[Save] をクリックして、設定を保存します。

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 ボックスに名前を入力し、ドロップダウン リストから許容可能なセキュリティ プロトコルとアルゴリズムの組み合わせを選択して、トランスフォーム セットを設定します。

ステップ 11　IP 圧縮をイネーブルにして、トランスフォーム セットのモードを選択します。

ステップ 12　トランスフォーム セットを削除するには、トランスフォーム セットを選択して [Delete] をクリックします。トランスフォーム セットのパラメータを編集するには、行またはフィールドをクリックし、パラメータを編集します。

ステップ 13　[Save] をクリックして、設定を保存します。

ステップ 14　[Topology and Routing Information] セクションで、トポロジとデバイス ロールを選択します。[Routing Protocol] には、[Extended Interior Gateway Routing Protocol (EIGRP)] または [Routing Information Protocol Version 2 (RIPv2)] を選択します。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。

（注）　デバイス ロールとして [Hub] を選択すると、ルーティング情報がディセーブルになります。

ステップ 15　[NHRP and Tunnel Parameters] セクションに、必要な情報を入力します。

ステップ 16　[NHS Server Information] セクションには、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 アドレスなどのネクスト ハブ サーバの情報を追加します。

（注）　[Cluster Support] 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 クラスタ設定が定義されたテンプレートは、Cisco IOS ソフトウェア バージョン 15.1(2)T 以降を実行するデバイスにのみ適用されます。

ステップ 17　[Save As New Template] をクリックします。

新規の複合テンプレートが [My Templates] フォルダに表示されます。

（注）　テンプレートを作成した後は、展開できるようにそのテンプレートをパブリッシュします。

[Dynamic Multipoint VPN Template] ページの要素のリストと説明については、表 4-5 を参照してください。

表 4-5　[Dynamic Multipoint VPN Template] ページ

要素	フィールドの説明
[Template Basic] タブ	
Name	DMVPN テンプレートの名前を入力します。
Description	（オプション）DMVPN テンプレートの説明を入力します。
[Validation Criteria] タブ	
Device Type	ドロップダウン リストからデバイス タイプを選択します。
OS Version	デバイスの OS バージョンを入力します。
IPSec の情報	

表 4-5　[Dynamic Multipoint VPN Template] ページ （続き）

要素	フィールドの説明
Authentication Type	[Preshared Keys] または [Digital Certificates] オプション ボタンをクリックします。 • [Preshared Keys] : 秘密キーを 2 つのピア間で共有したり、認証段階で IKE に使用したりすることが可能になります。 • [Digital Certificates] : IKE キー管理メッセージを署名および暗号化するために、RSA キー ペアが使用される認証方式。証明書によって、2 つのピア間の通信の否認防止が提供されます。つまり、実際に通信が行われたことを証明できます。
Priority	IKE プロポーザルのプライオリティ値。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。 有効値の範囲は 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。このフィールドをブランクのままにすると、Security Manager によって、まだ割り当てられていない最も小さい値が割り当てられます。値は 1 から始まり、次は 5 となり、その後は 5 ずつ増加します。
Authenticate	ドロップダウン リストから、認証タイプを選択します。
Diffie-Hellman Group	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取得するために使用する Diffie-Hellman グループ。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が、グループ 14 の方がより強力）。AES 暗号化を使用する場合は、このグループ（またはそれ以上）を使用します。ASA では、最上のグループとしてこのグループがサポートされます。
Encryption policy	ドロップダウン リストから暗号化ポリシーを選択します。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。フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA の確立に使用される暗号化アルゴリズム： [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。

表 4-5　[Dynamic Multipoint VPN Template] ページ （続き）

要素	フィールドの説明
Hash	IKE プロポーザルで使用されるハッシュ アルゴリズム。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。オプションは次のとおりです。 • [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。
Lifetime	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。 60 ～ 2147483647 秒の値を指定できます。デフォルトは 86400 です。
トランスフォーム セット	
Name	トランスフォーム セット名を入力します。トランスフォーム セットは、トンネル上のトラフィックを暗号化します。
ESP Encryption Algorithm	ペイロードの暗号化に使用されるアルゴリズム。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。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	ペイロードの整合性チェックに使用されるアルゴリズム。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。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 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	ペイロードを圧縮する IP 圧縮をイネーブルにします。Lempel-Ziv-Stac（LZS）アルゴリズムを使用した IP 圧縮。
Mode	トラフィックを転送するモードを選択します。
デバイス ロールおよびトポロジ	
[Hub and Spoke] オプション ボタン	ハブ アンド スポーク トポロジを設定するには、[Hub and Spoke] オプション ボタンを選択します。このトポロジでは、スポーク間のトラフィックがハブ ルータを介してルーティングされます。

表 4-5　[Dynamic Multipoint VPN Template] ページ （続き）

要素	フィールドの説明
[Fully Mesh] オプション ボタン	フルメッシュ ネットワーク トポロジを設定するには、[Fully Mesh] オプション ボタンを選択します。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。
EIGRP	ルーティング情報を選択します。
RIPV2	ルーティング情報を選択します。
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。
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 アドレスを有効としてアドバタイズす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。範囲は 0 ～ 4294967295 です。
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 サイズを入力します。範囲は 500 ～ 1460 です。
Physical Interface	物理インターフェイスを入力します。
NHS Fallback Time	（オプション）NHS フォールバック時間を秒単位で入力します。範囲は 0 ～ 60 です。
NHS サーバ	
Cluster ID	1 つまたは複数のハブを持つグループを形成するためのクラスタ値を入力します。範囲は 0 ～ 10 です。
Max Connections	特定のグループ/クラスタでアクティブにできる最大接続数を入力します。
Priority	クラスタ内の特定のハブのプライオリティ。ハブ デバイスを使用するトンネルを形成するスポーク ルータのプライオリティに依存します。
Next Hop server	ネクストホップ サーバの IP アドレスを入力します。
Hub's Physical IP Address	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。

DMVPN テンプレートの展開

DMVPN テンプレートを展開するには、次の手順を実行します。

（注）　指定のテンプレートをデバイスに展開するには、まずパブリッシュする必要があります。

ステップ 1　[Deploy] > [Choose Configuration Tasks] > [My Templates] を選択します。

ステップ 2　[My Templates] ページで DMVPN テンプレートを選択し、[Tasked View] ボタンをクリックします。

ステップ 3　[Deploy Task] パッドから、[Run] をクリックします。

[Template Deployment] ページが開きます。

ステップ 4　デバイス選択セクションから、テンプレートを展開するデバイスのリストを選択します。

ステップ 5　[Value Assignment] セクションで、オプション ボタンをクリックしてデバイスを選択します。

ステップ 6　DMVPN については、[GRE IP] および [Subnet Mask] の値を変更できます。

ステップ 7　値を変更した場合は、[Apply] をクリックします。ページ上の要素については、表 4-5 を参照してください。

（注）　Cisco IOS ソフトウェア バージョン 15.1(2)T 以降のスポーク オプションを選択すると、NHS クラスタ設定セクションが表示されます。

ステップ 8　[Schedule] セクションで [Job Name] を入力し、次のいずれかのオプション ボタンをクリックします。

- [Run]：ジョブをただちに実行します。
- [Run at Schedule Time]：ジョブを実行する時間を指定します。

ステップ 9　[Summary] でエントリを確認してから、[OK] をクリックします。

GET VPN グループ メンバー テンプレートの作成

GETVPN グループ メンバー テンプレートを作成するには、次の手順を実行します。

ステップ 1　[Design] > [Configuration] > [Features and Technology] > [Security] > [GETVPN-GroupMember] を選択します。

[GETVPN-GroupMember Configuration Template] ページが表示されます。

ステップ 2　[Template Basic] セクションで、適切なフィールドに名前、説明、および作成者名を入力します。

ステップ 3　[Validation Criteria] ドロップダウン リストから、デバイス タイプを選択して OS バージョンを入力します。

ステップ 4　[Group Information] セクションで、グループ名とグループ ID を入力します。

ステップ 5　[IKE Authentication Policy +] ボタンをクリックして、IKE 認証情報を追加します。

ステップ 6　[IKE Authentication Policy] ダイアログ ボックスで、[Pre-Shared key] または [Digital Certificate] オプション ボタンをクリックします。

キー サーバは、デジタル証明書を使用して認証します。ルータには、ルータ自身を認証するためのデジタル証明書が認証局から発行されている必要があります。

ステップ 7　[IKE Policy] セクションで、[Add Row] をクリックして IKE ポリシーを追加し、[Save] をクリックします。[Row] または [Field] をクリックして、パラメータを編集します。リストから IKE ポリシーを選択し、[Delete] をクリックして IKE ポリシーを削除します。

ステップ 8　グループ メンバーの登録インターフェイスを入力します。

ステップ 9　[Traffic Detail] セクションで、[Local Exception ACL] および [Fail Close ACL] を入力します。

ステップ 10　[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。

ステップ 11　[Key Servers] セクションで、プライマリ キー サーバとセカンダリ キー サーバの IP アドレスまたはホスト名を入力します。

ステップ 12　[Add Row] または [Delete] をクリックして、セカンダリ キー サーバを追加または削除します。セカンダリ キー サーバを編集する場合は、[Row] または [Field] をクリックし、キー サーバの IP アドレスを編集します。

[GETVPN Group Member template] ページ上の要素のリストと説明については、表 4-6 を参照してください。

（注）　テンプレートを作成した後は、展開できるようにそのテンプレートをパブリッシュします。

ステップ 13　[Save As New Template] をクリックします。

作成したテンプレートは、[My Templates] の下に表示されます。

表 4-6　[GETVPN Group Member Template] ページ

要素	フィールドの説明
[Template Basic] タブ	
Name	GETVPN グループの名前を入力します。
Description	（オプション）GETVPN テンプレートの説明を入力します。
Author	（オプション）作成者名を入力します。
[Validation Criteria] タブ	
Device Type	ドロップダウン リストからデバイス タイプを選択します。
OS Version	デバイス タイプの OS バージョンを入力します。
テンプレートの詳細	
Group Name	GETVPN グループ メンバー テンプレートのグループ名を入力します。
Group ID	GETVPN グループ メンバーに固有のアイデンティティを入力します。この値は、数値または IP アドレスになります。範囲は 0 ～ 2147483647 です。
IKE 認証ポリシー	
Authorization Type	[Preshared Keys] または [Digital Certificates] オプション ボタンをクリックします。 • [Preshared Keys]：事前共有キーを使用すると、秘密キーを 2 つのピア間で共有したり、認証段階で IKE に使用したりできます。 • [Digital Certificates]：IKE キー管理メッセージを署名および暗号化するために、RSA キー ペアが使用される認証方式。証明書によって、2 つのピア間の通信の否認防止が提供されます。つまり、実際に通信が行われたことを証明できます。
Priority	IKE プロポーザルのプライオリティ値。このプライオリティ値によって、共通の 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。 有効値の範囲は 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。

表 4-6　[GETVPN Group Member Template] ページ （続き）

要素	フィールドの説明
Encryption	ドロップダウン ボックスから暗号化アルゴリズムを選択します。暗号化アルゴリズムは、フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA の確立に使用されます。 • [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。
Hash	IKE プロポーザルで使用されるハッシュ アルゴリズム。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。オプションは次のとおりです。 • [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。
Diffie-Hellman Group	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取得するために使用する Diffie-Hellman グループ。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が、グループ 14 の方がより強力）。AES 暗号化を使用する場合は、このグループ（またはそれ以上）を使用します。ASA では、最上のグループとしてこのグループがサポートされます。
Lifetime	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。 60 ～ 2147483647 秒の値を指定できます。デフォルトは 86400 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入力します。
トラフィックの詳細	
Local Exception ACL	暗号化から除外する必要のあるトラフィックに対する ACL を選択します。

表 4-6　[GETVPN Group Member Template] ページ （続き）

要素	フィールドの説明
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、クリア テキストで送信する必要のあるトラフィックに対する 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	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。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。
キー サーバ情報	
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 ポリシーを作成してすべてのグループ メンバーに配布する処理、およびセカンダリ キー サーバを定期的に同期する処理を担当します。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。1 つのグループ メンバーに最大 8 つのキー サーバを設定できます。

GET VPN キー サーバ テンプレートの作成

GETVPN キー サーバ テンプレートを使用して、テンプレートを作成します。

GETVPN キー サーバ テンプレートを作成するには、次の手順を実行します。

ステップ 1　[Design] > [Configuration] > [Features Technologies] > [Security] > [GETVPN-KeyServer] を選択します。

[GETVPN-KeyServer Configuration Template] ページが開きます。

ステップ 2　[Template Basic] セクションで、適切なフィールドに名前、説明、および作成者を入力します。

ステップ 3　[Validation Criteria] ドロップダウン リストから、デバイス タイプを選択して OS バージョンを入力します。

ステップ 4　[Group Information] セクションで、グループ名とグループ ID を入力します。

ステップ 5　[IKE Authentication Policy +] ボタンをクリックして、IKE 認証情報を追加します。[IKE Authentication Policy] ダイアログボックスが開きます。

ステップ 6　[Pre-Shared key] オプション ボタンまたは [Digital Certificate] オプション ボタンをクリックします。

ステップ 7　[IKE Authentication Policy] セクションで、[Add Row] をクリックして IKE ポリシーを追加します。

ステップ 8　[IKE Policy] セクションで、[Add Row] をクリックして IKE ポリシーを追加します。[Row] または [Field] をクリックして、パラメータを編集します。リストから IKE ポリシーを選択し、[Delete] をクリックして IKE ポリシーを削除します。

ステップ 9　デバイスの WAN IP アドレスを入力し、[Dead Peer Detection (DPD)] チェックボックスをオンにすることで、すべてのキー サーバで DPD をイネーブルにして、その他のキー サーバの状態を効果的に追跡できるようにします。

ステップ 10　[Key Server Profile] セクションで、[Rekey] タブを選択し、ドロップダウン リストから配布方法を選択します。[Rekey] セクションに必要な情報を入力します。

ステップ 11　キー再生成メッセージを暗号化するには、RSA キーを使用します。ドロップダウン リストから既存の RSA キーを選択するか、[+] ボタンをクリックして新規の RSA キーを作成します。

ステップ 12　RSA キーを生成するには、キーのラベルおよびモジュラスを指定します。証明書をエクスポートするには、[Exportable key] チェックボックスをオンにします。

ステップ 13　[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、暗号化ポリシー、およびアンチリプレイを入力します。

ステップ 14　ドロップダウン リストからキー再生成暗号化アルゴリズムを選択して、キー再生成を暗号化します。

ステップ 15　[Key Server Profile] ページで、[GETVPN Traffic] タブをクリックします。

ステップ 16　[GETVPN Traffic] ダイアログ ボックスで、暗号化するトラフィック、暗号化ポリシー、およびアンチリプレイを入力します。

ステップ 17　[Encryption Policy +] ボタンをクリックして、この暗号化ポリシーの一部とするトランスフォーム セットを追加します。

ステップ 18　すべてのグループ メンバーにクリア テキストでトラフィックを送信するには、[Migration] タブで、[Enable Receive Only SA Feature] チェックボックスをオンにします。この機能によって、到着する暗号化トラフィックを復号化できます。

（注）　テンプレートを作成した後は、展開できるようにそのテンプレートをパブリッシュします。

ステップ 19　[Save As New Template] をクリックします。

作成したテンプレートは、[My Templates] の下に表示されます。

[GETVPN Key Server template] ページの要素のリストと説明については、表 4-7 を参照してください。

表 4-7　[GETVPN Key Server Template] ページ

要素	説明
[Template Basic] タブ	
Name	GETVPN グループの名前を入力します。
Description	（オプション）GETVPN テンプレートの説明を入力します。
Author	（オプション）作成者名を入力します。
[Validation Criteria] タブ	
Device Type	ドロップダウン リストからデバイス タイプを選択します。
OS Version	OS バージョンを入力します。
テンプレートの詳細	
Group Name	テンプレートのグループ名を入力します。
Group ID	GETVPN グループに固有のアイデンティティを入力します。この値は、数値または IP アドレスになります。範囲は 0 ～ 2147483647 です。
WAN IP Address	WAN IP アドレスを入力します。
IKE 認証ポリシー	
Authorization type	[Pre-shared key] または [Digital Certificates] オプション ボタンをクリックします。これは、キー サーバとグループ メンバー間の初期の IKE 認可用です。

表 4-7　[GETVPN Key Server Template] 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。このプライオリティ値によって、共通の 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。 有効値の範囲は 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。
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。暗号化アルゴリズムは、フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA の確立に使用されます。 • [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。
Hash	IKE プロポーザルで使用されるハッシュ アルゴリズム。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。オプションは次のとおりです。 • [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。
Diffie-Hellman Group	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取得するために使用する Diffie-Hellman グループ。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が、グループ 14 の方がより強力）。AES 暗号化を使用する場合は、このグループ（またはそれ以上）を使用します。ASA では、最上のグループとしてこのグループがサポートされます。
Lifetime	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。 60 ～ 86400 秒の値を指定できます。デフォルトは 86400 です。

表 4-7　[GETVPN Key Server Template] ページ （続き）

要素	説明
WAN IP Address	WAN IP アドレスを入力します。
Dead Peer Detection	キー サーバに対してデッド ピア検知をイネーブルにして状態を効果的に追跡できるようにするには、[Dead Peer Detection] チェックボックスをオンにします。
キー再生成	
Distribution Method	ドロップダウン リストから配布方法を選択します。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。オプションは [Unicast] または [Multicast] です。
Multicast IP Address	配布方法として [Multicast] 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頻度および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。
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が、キーの暗号化に使用されます。 • [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	（オプション）暗号化されるトラフィックに対応する ACL 名をドロップダウン 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）** 暗号化セッションが稼動していない場合でも、常に許可される必要のある特定のトラフィックを暗号化しないように気をつけてください。
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するトランスフォーム セットを選択します。テーブルから、ピア間でのトラフィックの暗号化に使用するトランスフォーム セットを追加します。 ドロップダウン リストから、トラフィックの暗号化用のトランスフォーム セットを選択します。テーブルから、ピア間のトラフィックの暗号化用に別のトランスフォーム セットを追加します。
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。
移行	

表 4-7　[GETVPN Key Server Template] ページ （続き）

要素	説明
Enable Receive Only SA feature	[Enabling Receive Only SA feature] チェックボックスをオンにすると、到着する暗号化トラフィックを復号化する機能を維持しながら、トラフィックをクリア テキストで送信できます。

GETVPN テンプレートの展開

この作業により、GETVPN グループ メンバーおよびキー サーバ テンプレートを展開できます。

（注）　テンプレートをデバイスに展開する前に、テンプレートをパブリッシュする必要があります。

GETVPN テンプレートを展開するには、次の手順を実行します。

ステップ 1　[Deploy] > [Choose Configuration Tasks] > [My Templates] を選択します。

ステップ 2　[My Templates] ページで GETVPN-GroupMember または KeyServer テンプレートを選択し、[Tasked View] ボタンをクリックします。

ステップ 3　[Deploy Task] パッドから、[Run] をクリックします。

[Template Deployment] ページが開きます。

ステップ 4　[Device Selection] セクションから、デバイスとロケーションを選択します。

ステップ 5　[Value Assignment] セクションで、オプション ボタンをクリックしてデバイスを選択します。

ステップ 6　GETVPN-GroupMember については、[Registration Interface]、[Enable Passive SA]、[Local Exception Policy ACL]、および [Fail Close ACL] の値を変更できます。

ステップ 7　GETVPN Key Server については、[Keyserver]、[WAN IP Address]、[ACL]、[Priority]、および [Cooperative servers] の値を変更できます。

ステップ 8　値を変更したら、[Apply] をクリックします。このページの要素については、表 4-6 および表 4-7 を参照してください。

ステップ 9　[Schedule] セクションをクリックし、[Job Name] を入力して、次のいずれかのオプション ボタンをクリックします。

- [Run]：ジョブをただちに実行します。
- [Run at Schedule Time]：ジョブを実行する時間を指定します。

ステップ 10　[Summary] でエントリを確認してから、[OK] をクリックします。

設定テンプレートのインポートと展開

設定テンプレートを新たに作成するほか、Cisco Prime LAN Management Solution（LMS）から設定をインポートできます。Cisco Prime LMS に「ゴールデン」テンプレートが存在する場合は、それらの設定を Prime AM にインポートして、ネットワーク内のデバイスに展開できる設定テンプレートとして保存できます。

設定をインポートするには、まず、Cisco Prime LMS から設定をエクスポートして保存する必要があります。

ステップ 1　[Design] > [Configuration Templates] を選択します。

ステップ 2　[CLI Template] フォルダを展開し、[CLI] テンプレートを選択します。

ステップ 3　[CLI template] ページの右上にある [Import] アイコンをクリックします。

ステップ 4　Cisco Prime LMS から以前にエクスポートした .xml コンフィギュレーション ファイルを参照し、[OK] をクリックします。

ステップ 5　[My Templates] フォルダに移動して、インポートした設定を選択します。

ステップ 6　設定の内容を表示するには、[CLI Content] タブをクリックします。

設定に定義されたパラメータを表示するには、[Form View] タブをクリックします。これらの値は読み取り専用です。

設定に定義された変数を変更するには、[Manage Variables] をクリックします。

ステップ 7　[Publish] アイコンをクリックしてテンプレートをパブリッシュし、展開できるようにします。

ステップ 8　[Go to Deployment] アイコンをクリックし、[Deploy] > [Configuration Tasks] ページに移動します。

ステップ 9　パブリッシュしたテンプレートで、[Deploy] をクリックします。

ステップ 10　テンプレート展開オプションの指定の説明に従って、展開オプションを指定します。

ステップ 11　[OK] をクリックします。

テンプレート展開のトラブルシューティング

テンプレートを展開できない最も一般的な理由は、次のとおりです。

- 1 つまたは複数のデバイスが到達不能：デバイスのクレデンシャルが適切であることを確認します。デバイスに PING を送信して、到達可能であることを確認します。（詳細については、[360º View] の使用を参照してください）。
- CLI に誤りがあったためにデバイスの CLI がエラーを戻した：テスト デバイスでコマンドを実行して、テンプレートに含まれている CLI コマンドに誤りがないことを確認します。