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ておくと、それをデバイス タイプに基づいて、指定した数のデバイスにあとから展開できます。新しいサービスまたは新しいサイトを実装する場合、テンプレートによって生産性が高まります。多数のデバイスにわたって設定を変更するには、時間と手間がかかることがあります。テンプレートで必要な設定を適用し、デバイス間で一貫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て展開するプロセスを示します。

表 4-1　コンフィギュレーション テンプレート使用のプロセス

タスク	追加情報
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. テンプレートを公開します。	テンプレートを作成したら、[Publish] アイコンをクリックしてテンプレートを公開し、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のステータスを確認します。	[Tools] > [Task Manager] > [Jobs Dashboard] を選択して、テンプレートの展開のステータスを確認します。

この章は、次の項で構成されています。

ブランチの設計および展開用のテンプレートについて

類似したデバイスと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、コンフィギュレーション テンプレートを使用して、ブランチ内の 1 台以上のデバイスに適用できる汎用設定を作成できます。新しいブランチがあり、ブランチ内のデバイスで共通の設定を迅速かつ正確にセットアップする場合にも、コンフィギュレーション テンプレートを使用できます。

ブランチの展開とは

ブランチの展開では、ブランチ ルータに対して最低限の設定を作成します。Prime NCS（WAN）では、次のような必要な機能のセットを作成できます。

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

次に、作成したすべてのテンプレートは、単一の*複合テンプレート*に追加できます。これは、ブランチ ルータに必要なすべての個々の機能テンプレートを集約したものです。また、この複合テンプレートを使用して、ブランチ展開処理を実行し、他のブランチで設定を複製することができます。

ブランチ内に類似したデバイスのセットがある場合は、「ゴールデン」設定を含む複合テンプレートを展開して、展開を簡単にし、デバイス設定間の一貫性を保つことができます。複合テンプレートを使用して、既存のデバイス設定と比較して不一致があるかどうかを調べることもできます。

関連項目

- 「ブランチでの展開のためのコンフィギュレーション テンプレートの作成」（P.4-2）
- 「ブランチでの展開のための複合テンプレートの作成と展開」（P.4-4）

ブランチでの展開のためのコンフィギュレーション テンプレートの作成

ここでは、ブランチでの展開で一般に使用される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 コンフィギュレーション テンプレートの作成
- EIGRP ルーティング コンフィギュレーション テンプレートの作成
- RIP ルーティング コンフィギュレーション テンプレートの作成
- CLI コンフィギュレーション テンプレートの作成

イーサネット インターフェイス コンフィギュレーション テンプレートの作成

多くのブランチでの展開では、イーサネット インターフェイス コンフィギュレーション テンプレートが必要です。このテンプレートは、ブランチでの展開のために、複合テンプレートに含めます。

イーサネット インターフェイス コンフィギュレーション 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 フォルダで、[Interfaces] を展開してから、[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] で、[Ethernet Interfaces] テーブルの [Add Row] をクリックします。

ステップ 6　デバイスで設定するイーサネット 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、GigabitEthernet0/1 インターフェイスは、そのデバイスに物理的に存在する必要があります）。

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

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 コンフィギュレーション テンプレートの作成

多くのブランチでの展開では、EIGRP ルーティング コンフィギュレーション テンプレートが必要です。このテンプレートは、ブランチでの展開のために、複合テンプレートに含めます。

EIGRP ルーティング コンフィギュレーション 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 フォルダで、[Routing] を展開してから、[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] で、EIGRP Routes テーブルの [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 コンフィギュレーション テンプレートの作成

多くのブランチでの展開では、RIP ルーティング コンフィギュレーション テンプレートが必要です。このテンプレートは、ブランチでの展開のために、複合テンプレートに含めます。

RIP ルーティング コンフィギュレーション 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 フォルダで、[Routing] を展開してから、[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] で、[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 コンフィギュレーション テンプレートの作成

多くのブランチでの展開では、CLI コンフィギュレーション テンプレートが必要です。このテンプレートは、ブランチでの展開のために、複合テンプレートに含めます。

CLI コンフィギュレーション 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 フォルダで、[CLI Template] を展開してから、[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] タブをクリックしてから、次のテキストを入力します。

```
banner motd #Welcome to Prime NCS#
```

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。

ブランチでの展開のための複合テンプレートの作成と展開

デバイスに対して一括して適用する既存の機能テンプレートまたは CLI テンプレートのコレクションがある場合は、複合テンプレートを作成します。複合テンプレートに含まれるテンプレートが、デバイスに適用される順序を指定してください。

ブランチ全体に複製される複数の類似したデバイスがある場合は、ブランチ内のすべてのデバイスに対して「マスター」複合テンプレートを作成し、展開できます。このマスター複合テンプレートは、新しいブランチを作成するときに後で使用することもできます。

ステップ 1　[Design] > [Templates] > [Configuration] を選択してから、[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含まれる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に、Cisco 7200 シリーズ ルータに適用するテンプレートと、すべてのルータに適用する別のテンプレートがある場合は、[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 タイプがグレイ アウトされている場合、テンプレートをそのデバイス タイプに適用できません。

ステップ 4　[Template Details] で、複合テンプレートに含めるテンプレートを選択します。

ステップ 5　矢印を使用し、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序に配置します。たとえば、ACL を作成し、インターフェイスに関連付けるには、インターフェイス テンプレートの前に ACL テンプレートを配置します。

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、展開できるようにテンプレートを公開します。

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　公開したテンプレートで、[Deploy] をクリックします。

ステップ 11　テンプレートの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、テンプレート展開のステータスを確認します。

コンフィギュレーション テンプレートの作成

Prime NCS（WAN）には、次のタイプのコンフィギュレーション テンプレートがあります。

- CLI テンプレート：独自のパラメータに基づいて作成されるユーザ定義テンプレート。CLI テンプレートを使用すると、コンフィギュレーションの要素を選択できます。Prime NCS（WAN）には、実際の値や論理ステートメントと置き換える変数が用意されています。Cisco Prime LAN Management System からテンプレートをインポートすることもできます。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：デバイスの機能またはテクノロジーに固有な設定。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：2 つ以上の機能テンプレートまたは CLI テンプレートを 1 つのテンプレートにグループ化したもの。複合テンプレートに含まれるテンプレートが、デバイスに展開される順序を指定してください。ブランチでの展開のため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）　すべてのテンプレートは、デバイスに展開する前に*公開*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ておくと、それをデバイス タイプに基づいて、指定した数のデバイスにあとから展開できます。多数のデバイスにわたって設定を変更するには、時間と手間がかかることがあります。テンプレートで必要な設定を適用し、デバイス間で一貫性を保つことにより、時間を節約できます。

デフォルト コンフィギュレーション テンプレート

Prime NCS（WAN）には、デフォルトのコンフィギュレーション テンプレートが付属し、[Design] > [Configuration Templates] > [My Templates] > [OOTB] にあります。これらのテンプレートについて、表 4-2 で説明します。

表 4-2　Prime NCS（WAN）に付属するコンフィギュレーション テンプレート

テンプレート名	目的
Medianet – PerfMon	Medianet のパフォーマンス モニタリングを設定します。
PA with WAAS	Cisco Performance Agent[1] と Wide Area Application Services（WAAS）を設定します。
PA without WAAS	WAAS なしで Cisco Performance Agent を設定します。
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 Software のライセンス機能です。包括的なアプリケーション パフォーマンスとネットワークの使用に関するデータを提供します。このデータは、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ために役立ちます。

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 ユーザが実行する必要がある高度な機能です。CLI テンプレートを作成するには、次の条件を満たしている必要があります。

- CLI の専門知識を持ち、CLI をよく理解し、Apache VTL で CLI を記述できる。Apache Velocity Template Language（Apache VTL）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 を適用可能なデバイスについて理解している。
- Prime NCS（WAN）でサポートされるデータ型を理解している。
- テンプレート内の設定を理解し、手動でラベルを付けることができる。

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の説明に従って、前提条件を満たしていることを確認します。

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**を展開してから、[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リストされます。

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

これにより、テンプレートの展開時に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から、[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、Apache VTL を使用してコードを入力する必要があります。

ステップ 8　テンプレートで使用されてい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）をクリックします。次に、変数を変更するには、[Manage Variables] 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。

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　左上隅の [Publish] アイコンをクリックしてから、[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　公開したテンプレートで、[Deploy] をクリックします。

ステップ 14　テンプレートの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 テンプレートのデータベース変数について

デバイスが検出され、Prime NCS（WAN）に追加されたときに、インベントリ収集中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、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 CLI テンプレートを作成し、展開する場合は、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、*$interfaceNameList* は、データベースから値が取得されるデータベース変数タイプです。*$interfaceNameList* のデフォルト値は、`Inventory::EthernetProtocolEndpoint.IntfName` です。

データベースからの値を *interfaceNameList* に登録するには、以下の説明に従ってクエリー文字列をキャプチャするためのプロパティ ファイルを作成し、/opt/CSCOlumos/conf/ifm/template/InventoryTagsInTemplate フォルダに保存する必要があります。

プロパティ ファイルの例

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、デバイスで次の 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 と Gigabitethernet0/0）があることを仮定しています。

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

```
shutdown
```

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

プロパティ ファイルで指定した Enterprise JavaBeans Query Language（EJB QL）が文字列のリストを返すか、（単一の要素を指定した場合は）1 つの要素を含むリストを返すことを確認します。

テンプレートの展開オプションの指定

テンプレートを公開し、1 つ以上のデバイスにそのテンプレートを展開する場合は、デバイス、値、およびスケジュール情報を指定して、展開を調整できます。表 4-3 で、展開オプションについて説明します。

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

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	コンフィギュレーション テンプレートで事前に定義された変数以外の変数を指定できます。名前をクリックすると、事前に定義された変数が表示されます。いずれかの値を変更するには、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）　変更は、展開するその設定だけに適用されます。今後の *すべての*展開に対してコンフィギュレーション 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	わかりやすい展開ジョブ名を付けてから、ただちにジョブを実行するか、後で実行するかを指定できます。
Summary	ユーザが選択した展開オプションを要約します。

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、デバイスの設定に基づくテンプレートです。機能およびテクノロジー テンプレートでは、デバイスの設定に関して特定の機能またはテクノロジーに重点を置きます。Prime NCS（WAN）にデバイスを追加したときに、Prime NCS（WAN）によって、追加したモデルのデバイス設定が収集されます。

（注）　Prime NCS（WAN）で、すべてのデバイス タイプに対するすべての設定オプションがサポートされ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に対して、Prime NCS（WAN）に機能およびテクノロジー テンプレートがない場合は、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ます。

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 テンプレートは、設定に対する変更の展開を容易にするために作成します。たとえば、SNMP の機能およびテクノロジー テンプレートを作成してから、指定したデバイスにすばやく展開できます。複合テンプレートに 1 つ以上の機能およびテクノロジー テンプレートを追加することもできます。この操作を行った場合、SNMP テンプレートを更新したときに、その SNMP テンプレートが含まれる複合テンプレートには、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リストされます。

（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している場合は、[Device Type] フィールドには、該当するデバイス タイプだけがリストされ、選択を変更することはできません。

ステップ 5　[Template Detail] で、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、展開できるようにテンプレートを公開します。

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　公開したテンプレートで、[Deploy] をクリックします。

ステップ 11　テンプレートの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。

スタティック 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、スタティック ルートを設定できます。大規模ネットワークまたは複雑なネットワークでは、スタティック ルートが輻輳することがあります。スタティック ルーティング テンプレートを作成することにより、ネットワークを変更するたびに、手動で変更を加える必要がなくなります。

スタティック ルーティング テンプレートを作成し、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から、[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] で、[Add Row] をクリックしてから、各フィールドに入力します。

（注）　[Permanent Route] で、次のいずれかを選択します。

- 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であっても、ルーティング テーブルからルートを削除しないことを指定するには、[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は、ルーティング テーブルからルートを削除することを指定するには、[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、展開できるようにテンプレートを公開します。

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　公開したテンプレートで、[Deploy] をクリックします。

ステップ 10　テンプレートの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

アクセス リストを設定するためのテンプレートを作成し、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、Security サブフォルダを展開してから、[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] で、[Add Row] をクリックしてから、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推奨します。
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、展開できるようにテンプレートを公開します。

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　公開したテンプレートで、[Deploy] をクリックします。

ステップ 10　テンプレートの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 コンフィギュレーション テンプレートの作成

次の機能用のセキュリティ コンフィギュレーション テンプレートを作成できます。

- Dynamic Multipoint 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、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リシーを入力します。

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、IKE 認証タイプを選択します。

デフォルトの事前共有キーを選択する場合は、秘密キーを提供し、再確認する必要があります。認証タイプとして [Digital Certificate] を選択する場合は、ルータには、そのルータ自体を認証するために認証局によって発行されたデジタル証明書が必要です。

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、[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、そのパラメータを編集します。

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、トランスフォーム セット プロファイルを追加します。

ステップ 10　[Transform Set Profile] ダイアログボックスで、名前を入力し、ドロップダウン リストからセキュリティ プロトコルと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。

ステップ 11　IP 圧縮を有効にし、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、[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、そのパラメータを編集します。

ステップ 13　[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。

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] で、[Extended Interior Gateway Routing Protocol (EIGRP)] または [Routing Information Protocol Version 2 (RIPv2)] を選択します。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。

（注）　デバイス ロールとして [Hub] を選択した場合、ルーティング情報は無効になります。

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、ハブの物理インターフェイスの IP アドレス、ハブのトンネル インターフェイスの IP アドレスなど、次のハブのサーバ情報を追加します。

（注）　[Cluster Support] チェックボックスをオンにした場合は、[Cluster ID]、[Max Connection]、[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 17　[Save As New Template] をクリックします。

新しいテンプレートは、My Templates フォルダに表示されます。

ステップ 18　[Publish] アイコンをクリックして、展開できるようにテンプレートを公開します。

（注）　テンプレートの作成後に、展開に利用できるようにそのテンプレートを公開します。

[Dynamic Multipoint VPN Template] ページにある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	（任意）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 Information	

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] オプション ボタンまたは [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、認証フェーズ中に IKE で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。 有効な値の範囲は、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。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	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。 60 ～ 2147483647 秒の値を指定できます。デフォルトは 86400 です。
Transform Set	
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 セットによって、トンネル上のトラフィックが暗号化されます。
ESP Encryption Algorithm	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。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 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。
ESP Integrity Algorithm	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。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）（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	ペイロードを圧縮するために IP 圧縮を有効にします。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。
Device Role and Topology	
[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。

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

要素	フィールドの説明
[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。
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	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。
NHRP and Tunnel Parameters	
Network ID	NHRP ネットワーク ID を入力します。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 インターフェイスに対してキー ID を有効にするために使用されます。範囲は 0 ～ 4294967295 です。
NHRP Authentication String	認証文字列を入力します。
IP 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。
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	（任意）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 Server	
Cluster ID	1 つ以上のハブがあるグループを形成するために、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接続の最大数を入力します。
Priority	クラスタ内の特定のハブのプライオリティ。ハブ デバイスによって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）　デバイスに展開する前に、指定したテンプレートを公開する必要があります。

ステップ 1　[Deploy] > [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て [Tasked View] ボタンをクリックします。

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

[Template Deployment] ページが表示されます。

ステップ 4　デバイス選択セクションで、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 では、[GRE IP Address]、[Subnet Mask]、および [Tunnel Throughput Delay] 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。このページの要素については、表 4-5 を参照してください。

（注）　Cisco IOS Software バージョン 15.1(2)T 以降のスポーク オプションでは、[NHS cluster configuration] 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] に入力してから、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刻を指定します。

ステップ 9　[Summary] で入力した内容を確認し、[OK] をクリックします。

GET VPN グループ メンバ テンプレートの作成

GETVPN グループ メンバ 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 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、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 認証情報を追加するには、[IKE Authentication Policy +] ボタンをクリックします。

ステップ 6　[IKE Authentication Policy] ダイアログボックスで、[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。

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、そのルータ自体を認証するために認証局によって発行されたデジタル証明書が必要です。

ステップ 7　[IKE Policy] セクションで、[Add Row] をクリックして IKE ポリシーを追加してから、[Save] をクリックします。パラメータを編集するには、[Row] または [Field] をクリックします。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] をクリックします。

ステップ 8　グループ メンバに対する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] と [Fail Close ACL] に入力します。

ステップ 10　[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 アドレスとホスト名を入力します。

ステップ 11　セカンダリ キー サーバを追加または削除するには、[Add Row] または [Delete] をクリックします。セカンダリ キー サーバを編集する場合は、[Row] または [Field] をクリックして、キー サーバの IP アドレスを編集します。

ステップ 12　[Migration] セクションで、[Enable Passive SA] チェックボックスをオンにして、パッシブ 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。

[GETVPN Group Member template] ページにある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）　テンプレートの作成後に、展開に利用できるようにそのテンプレートを公開します。

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 に格納されます。

ステップ 14　[Publish] アイコンをクリックして、展開できるようにテンプレートを公開します。

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	（任意）GETVPN テンプレートの説明を入力します。
Author	（任意）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。
Template Detail	
Group Name	GETVPN グループ メンバ 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 メンバの一意の ID を入力します。数値または IP アドレスを指定できます。範囲は 0 ～ 2147483647 です。
IKE Authentication Policy	
Authorization Type	[Preshared Keys] オプション ボタンまたは [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、認証フェーズ中に IKE で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。 有効な値の範囲は、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。この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。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。
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。 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があるインターフェイスを入力します。
Traffic Details	
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。

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。
Key Server Information	
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。グループ メンバに対して最大 8 台のキー サーバを割り当てることができます。
Migration	
Enable Passive SA	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。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。

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、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 認証情報を追加するには、[IKE Authentication Policy +] ボタンをクリックします。[IKE Authentication Policy] ダイアログボックスが表示されます。

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。パラメータを編集するには、[Row] または [Field] をクリックします。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] をクリックします。

ステップ 9　他のキー サーバの状態を効果的に追跡するには、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して、すべてのキー サーバで DPD を有効にします。

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しい RSA キーを作成します。

ステップ 12　RSA キーを生成するには、キーのラベルとモジュラスを指定します。証明書をエクスポートする場合は、[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を暗号化するためのキー再生成暗号化アルゴリズムを選択します。

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　この暗号化ポリシーの一部であるトランスフォーム セットを追加するには、[Encryption Policy +] ボタンをクリックします。

ステップ 18　すべてのグループ メンバに対してクリア テキストでトラフィックを送信するには、[Migration] セクションで、[Enable Receive Only SA Feature] をオンにします。この機能によって、着信する暗号化トラフィックを復号化できます。

（注）　テンプレートの作成後に、展開に利用できるようにそのテンプレートを公開します。

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 に格納されます。

ステップ 20　[Publish] アイコンをクリックして、展開できるようにテンプレートを公開します。

[GETVPN Key Server template] ページにある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	（任意）GETVPN テンプレートの説明を入力します。
Author	（任意）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。
Template Detail	
Group Name	テンプレートのグループ名を入力します。
Group ID	GETVPN グループの一意の ID を入力します。数値または IP アドレスを指定できます。範囲は 0 ～ 2147483647 です。
WAN IP Address	WAN の IP アドレスを入力します。

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

要素	説明
IKE Authentication Policy	
Authorization type	[Pre-shared key] オプション ボタンまたは [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 メンバ間の初めの IKE 認証用です。
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。 有効な値の範囲は、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。この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。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。
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。

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

要素	説明
Lifetime	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。 60 ～ 86400 秒の値を指定できます。デフォルトは 86400 です。
WAN IP Address	WAN の IP アドレスを入力します。
Dead Peer Detection	キー サーバのデッド ピア検知を有効にして、その状態を効果的に追跡するには、[Dead Peer Detection] チェックボックスをオンにします。
[Accordian] ペイン	
[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 [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（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	キー再生成の再送信の頻度と時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	
Traffic to encrypt	（任意）暗号化す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。

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

要素	説明
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。 ドロップダウン リストから、トラフィックを暗号化するため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を暗号化するための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。
Migration	
Enable Receive Only SA feature	着信する暗号化トラフィックを復号化する機能を保持したまま、トラフィックをクリアテキストで送信するには、[Enabling Receive Only SA feature] チェックボックスをオンにします。

GETVPN テンプレートの展開

このタスクによって、GETVPN グループ メンバ テンプレートとキー サーバ テンプレートを展開できます。

（注）　デバイスにテンプレートを展開する前に、テンプレートを公開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] > [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] パッドで、[Deploy] をクリックします。

[Template Deployment] ページが表示されます。

ステップ 4　[Device Selection] セクションで、デバイスと場所を選択します。

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] に対して、[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] に対して、[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　値を変更した場合は、[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] に入力してから、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刻を指定します。

ステップ 10　[Summary] で入力した内容を確認し、[OK] をクリックします。

コンフィギュレーション テンプレートのインポートと展開

コンフィギュレーション テンプレートは新規作成するだけでなく、Cisco Prime LAN Management Solution（LMS）から設定をインポートすることもできます。Cisco Prime LMS に「ゴールデン」テンプレートがある場合は、Prime NCS（WAN）にこれらの設定をインポートし、ネットワーク内のデバイスに展開できるコンフィギュレーション テンプレートとして保存することができます。

設定をインポートするには、その前に Cisco Prime LMS から設定をエクスポートし、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 フォルダを展開してから、**CLI** テンプレートを選択します。

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

ステップ 4　Cisco Prime LMS から事前にエクスポートした設定 .xml ファイルを参照してから、[OK] をクリックします。

ステップ 5　My Templates フォルダに移動し、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。

設定で定義し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。

設定で定義したいずれかの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、展開できるようにテンプレートを公開します。

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　公開したテンプレートで、[Deploy] をクリックします。

ステップ 10　テンプレートの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

テンプレートが展開されない最も一般的な理由は次のとおりです。

- 1 台以上のデバイスに到達できない：デバイス クレデンシャルが正しいことを確認し、デバイスに対して ping を実行して、到達可能であることを確認します。（詳細については、360 度ビューの使用を参照してください）。
- CLI が正しくないために、デバイス CLI がエラーを返す：テスト デバイスでコマンドを実行することにより、テンプレートに含まれる CLI コマンドが正しいことを確認します。