改訂：2025 年 7 月 8 日

SD-Routing デバイス用 Cisco DMVPN の設定（リリース 17.15.x）

新機能と変更された機能

現在のリリースで利用可能な機能を以下の表に示します。

Cisco IOS XE リリース	機能名	説明	サポートされるプラットフォーム
Cisco IOS XE 17.15.1a	Cisco DMVPN	この機能により、Cisco Catalyst SD-WAN Manager のフィーチャパーセルを使用して、DMVPN ソリューションで SD-Routing デバイスを設定できるようになります。	• Cisco Catalyst 8000v vEdge ソフトウェア • Cisco Catalyst 8500 シリーズ エッジ プラットフォーム • Cisco Catalyst 8300 シリーズ エッジ プラットフォーム

Cisco DMVPN について

Cisco DMVPN（ダイナミックマルチポイント VPN）は、すべてのデバイスを静的に設定することなく、複数のサイトで VPN ネットワークを構築するためのルーティング技術です。この技術では、トンネリングプロトコルと暗号化されたセキュリティ対策を使用して、サイト間に仮想接続（トンネル）を作成します。これらのトンネルは必要に応じて動的に作成されるため、効率的でコスト効果も高くなります。

Cisco DMVPN のコンポーネント

Cisco DMVPN は次に示す 4 つの主要なコンポーネントで構成されています。

コンポーネント	目的
マルチポイント GRE（mGRE）	mGRE は、GRE のカプセル化を利用してマルチポイント仮想プライベートネットワーク（VPN）を作成するためのトンネリングメカニズムです。 さまざまな送信元からのデータパケットをカプセル化してから単一のトンネルに送ることで拡張性が向上し、VPN 管理が簡素化されます。

コンポーネント	目的
Next Hop Resolution Protocol（NHRP）	Next Hop Resolution Protocol（NHRP）は、ネクストホップクライアント（NHC）をネクストホップサーバー（NHS）に動的に登録するための解決プロトコルです。ダイナミックマルチポイント仮想プライベートネットワーク（DMVPN）設計では、NHCはスポークルータで、NHSはハブルータです。すべてのクライアントが登録されると、スポークルータは同じノンブロードキャスト マルチプル アクセス（NBMA）ネットワーク内の他のスポークルータを検出できるようになります。 NHRP により、企業は中央ハブを経由せずにネクストホップサーバーとネクストホップクライアントが相互に直接通信する方法を提供でき、潜在的なボトルネックを回避できます。
IPSec 暗号化	IPSec はデバイス間の接続を保護するためのプロトコルグループです。IPSec は、パブリックネットワーク経由で送信されるデータの安全性を維持するのに役立ちます。 多くの場合、IPSec はVPN を設定するために使用されます。パケットの送信元を認証するとともに、IPパケットを暗号化する機能を備えています。
BGP、EIGRP、OSPFなどのルーティングプロトコル	• **BGP**：ボーダーゲートウェイプロトコル（BGP）は、インターネットでのデータ送信の最適なネットワークルートを決定する一連のルールです。 BGPをルーティングプロトコルとして使用すると、DMVPNスポークとハブの間でルーティング情報を動的に交換できるため、ハブアンドスポークトポロジでの最適なルーティングが実現します。 • **EIGRP**：Enhanced Interior Gateway Routing Protocol（EIGRP）は、パケットを配信するための2つのレイヤ3デバイス間のベストパスを見つけるために使用されるダイナミック ルーティング プロトコルです。 このアルゴリズムは、ルート計算中のどの時点でもループが発生しないようにし、トポロジ変更に関与するすべてのデバイスを同期できるようにします。トポロジ変更の影響を受けないデバイスは、再計算に含まれません。 • **OSPF**：OSPFは、直接接続されたリンクに関する情報を自律システムネットワーク内のすべてのルータに送信するリンクステート ルーティング プロトコルです。 このプロトコルはネットワーク全体のトポロジ情報を保持しており、各宛先への最短パスを計算するために、この情報が自律システムのエリア内にあるすべてのルータと共有されます。

Cisco DMVPN の展開シナリオ

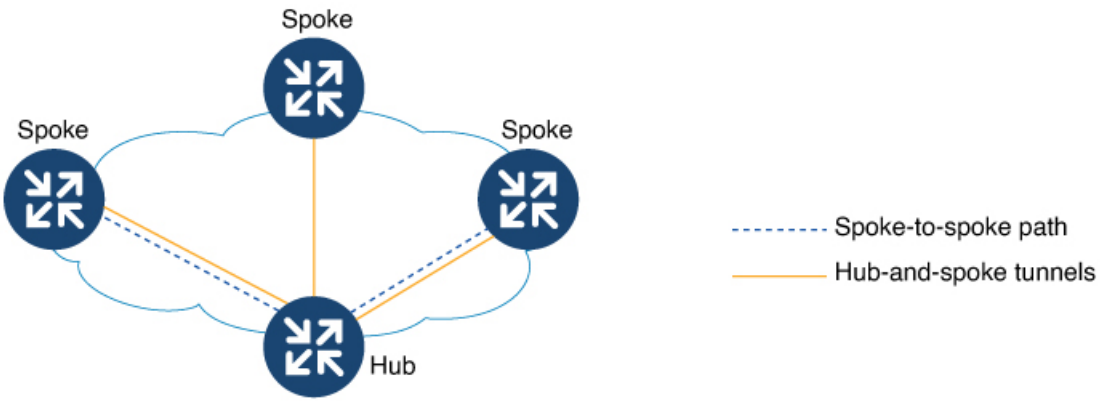
Cisco DMVPN は、次の 2 つの方法で展開できます。

ハブアンドスポーク導入モデル

この従来のトポロジでは、中央デバイス（ハブ）が複数の他のデバイス（スポーク）に接続されます。主要なエンタープライズリソースは大規模なセントラルサイトに配置され、いくつかの小規模サイトや分散拠点が VPN を介してセントラルサイトに直接接続されます。任意のリモートサイトから別のリモートサイトへのトラフィックは、このハブを通過します。

このモデルは低帯域幅を必要とするサイトに最適です。

図 *1 :* ハブアンドスポークモデルで展開される *DMVPN* ソリューション

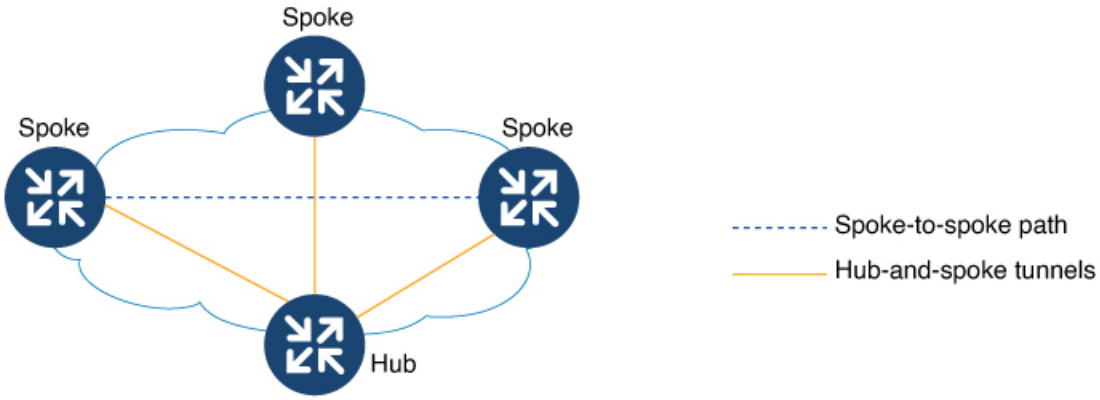


スポークツースポーク導入モデル

Cisco DMVPN を使用すると、完全メッシュ VPN を作成できます。ここでは、従来のハブアンドスポーク接続がスポーク間に動的に直接作成された IPSec トンネルによって補われます。直接のスポークツースポークトンネルでは、リモートサイト間のトラフィックがハブを通過する必要はありません。

これにより、追加の遅延がなくなり、WAN 帯域幅を節約できます。この導入モデルは、高帯域幅を必要とするサイトに最適です。

図 *2 :* スポークツースポークモデルで展開される *DMVPN* ソリューション



フィーチャパーセルを使用した Cisco DMVPN の設定

ここでは、Cisco Catalyst SD-WAN Manager のフィーチャパーセルを使用して、SD-Routing デバイスに Cisco DMVPN を設定する方法について詳しく説明します。

フィーチャパーセルを使用して DMVPN トンネルを作成するためのさまざまな手順の概要を次の表に示します。

DMVPN トンネルの設定手順	**詳細情報の参照先**
サービスプロファイルでの VRF の設定	VRF の設定
DMVPN トンネルの設定	トンネルの基本属性の設定 オーバーレイとアンダーレイの設定 NHRP の設定 BFD の設定 詳細なパラメータの設定

DMVPN トンネルの設定

このタスクでは、サービスプロファイルを使用して Catalyst SD-WAN Manager で DMVPN トンネルを設定する方法について詳しく説明します。

DMVPN トンネルを設定する前に、「サービスプロファイルでの VRF の設定」を行う必要があります。

ステップ 1 Cisco Catalyst SD-WAN Manager に移動します。**[Configuration]** > **[Configuration Groups]**を選択します。[Solution] で [SD Routing] を選択します。

ステップ 2 VRF の設定タスク内で作成したサービスプロファイルを選択します。VRF を選択し、[+] をクリックして [DMVPN Tunnel] を選択します。リストから既存の DMVPN トンネルを選択するか、新しい DMVPN トンネルを作成します。

ステップ 3 DMVPN トンネルの名前と説明を指定します。[Basic Configuration] タブで、次の項目を指定します。

- [Interface Name]：インターフェイス名を **dmvpn** <*number from 1-255*> の形式で指定します（例：*dmvpn1*）。インターフェイス名がSD-Routingデバイスで一意であることを確認することが重要です。
- [Shutdown]：（任意）DMVPNトンネルを有効にするには、トグルボタンをクリックします。デフォルトでは、DMVPN トンネルはシャットダウンされています。
- [Description]：（任意）インターフェイスの説明を指定します。
- [Tunnel Key]：トンネルキーを識別するための数値を0～4,294,967,295の範囲で指定します。トンネルキーは、複数のトンネルを介してさまざまなタイプのトラフィックをルーティングするためのパラメータとして使用することもできます。また、トンネルキーを使用して特定のルーティングポリシーを適用することもできます。


（注）

同一の DMVPN ネットワーク内に存在するハブおよびスポークに対しては、すべて同じキー値を設定する必要があります。

- [IPSec Profile]：（任意）DMVPN トンネルを暗号化する場合は、IPSec プロファイルを選択します。IPSec プロファイルの作成手順については、DMVPN トンネル内のデータ暗号化 （7 ページ）を参照してください。

ステップ 4 オーバーレイとアンダーレイの詳細を指定します。

DMVPNでは、オーバーレイトンネルとアンダーレイトンネルを介したIPv4およびIPv6のユニキャスト転送とマルチキャスト転送がサポートされています。

オーバーレイ

a) [IPv4 address]、[IPv4 Subnet Mask]：IPv4 アドレスおよびサブネットマスクを指定します。
b) [IPv6 Prefix]：IPv6 アドレスのプレフィックスを指定します。

アンダーレイ

アンダーレイトランスポートの場合は、**IPv4** または **IPv6** アドレスを選択します。

- [Tunnel Source]：トンネルインターフェイスの有効なインターフェイス名を指定します。
- [VRF]：ドロップダウンリストから、[Tunnel Source] インターフェイスに設定されている VRF を選択します。
- [Global VRF]：トンネルパケットを転送するためのグローバル VRF を選択します。

ステップ 5 NHRP の設定

DMVPN Role

a) [Hub]、[Spoke]、[Both]：ネットワークでの DMVPN ロール（ハブ、スポーク、または両方）を指定します。
b) [Network ID]：非ブロードキャスト マルチアクセス（NBMA）ネットワークでグローバルに一意の 32 ビットネットワーク識別子を指定します。範囲は 1 ～ 4294967295 です。
c) [Hold Time]：（任意）ポジティブな権威のある NHRP 応答で NBMA アドレスが有効としてアドバタイズされる時間（秒単位）。推奨値の範囲は、300 ～ 600 秒です。
d) [Authentication Key]：（任意）インターフェイスの認証文字列を指定します。


（注）

同一の DMVPN ネットワーク内に存在するハブおよびスポークに対しては、すべて同じ NHRP 認証文字列を設定する必要があります。

e) [Redirect]：（任意）[DMVPN Role] で [Hub] または [Both]を選択すると、このオプションが有効になります。リダイレクトを有効にすると、特定の宛先に到達するための効率的で短いパスがハブからスポークに伝えられます。これにより、デバイスは相互に直接通信できるため、中間ホップが必要ありません。

f) [Shortcut]：（任意）このオプションは [DMVPN Role] で [Spoke] を選択すると有効になります。ハブから発行されたリダイレクトメッセージをスポークで受け入れることができます。

NHRP Summary Map

[IPv4 NHRP Summary Map]、[IPv6 NHRP Summary Map]：スポークツースポーク NHRP サマリーマップは、NHRP 解決応答で RIB の IP アドレスネットワークとサブネットマスクを使用せず、設定済みの IP アドレスネットワークとサブネットマスクを使用します。この機能は、ネットワーク上の NHRP 解決トラフィックを削減するのに役立ちます。

NBMA サマリーマップ


（注）

NBMA サマリーマップの詳細は、[DMVPN Role] で [Spoke] または [Both] を選択した場合にのみ指定する必要があります。

[IPv4 NHS NBMA Summary Map]、[IPv6 NHS NBMA Summary Map]：スポーク（NHC）でハブ（NHS）の非ブロードキャストマルチプルアクセスネットワーク（NBMA）アドレスに完全修飾ドメイン名（FQDN）を設定することができます。これにより、スポークはFQDNを使用してハブのIPアドレスをダイナミックに特定することができます。

- [NHS Address]：スポークの IP アドレスを指定します。この IP アドレスは、ハブの IPv4 オーバーレイで指定したトンネルインターフェイスの IP アドレスと一致している必要があります。
- [NBMA Address]：ハブのトンネル送信元インターフェイスのアドレスを指定します。
- [Multicast]：マルチキャストトラフィックを有効にするには、このトグルボタンを選択します。

ステップ 6 BFD の設定

トグル ボタンを選択して BFD を有効にします。BFD を有効にすると、障害検出通知が迅速に制御プロトコルに送信され、ネットワーク全体のコンバージェンス時間が短縮されることで、高速ピア障害検出が実現します。

- [Transmit Interval (Milliseconds)]：（任意）シングルホップ BFD の制御パケットを送信する最小間隔。
- [Minimum Receive Interval (Milliseconds)]：（任意）BFD 制御パケットを受信する最小間隔。
- [Multiplier]：（任意）この倍率によって、セッションダウンが宣言される前に失われた可能性のある連続パケットの最小数が指定されます。

ステップ 7 詳細なパラメータの設定

a) [IPv4 MTU]、[IPv6 MTU]：（任意）すべてのインターフェイスで送受信されるフレームのデフォルト最大伝送単位（MTU）のサイズを指定します。デフォルト値は 1400 バイトです。

b) [IPv4 TCP MSS]、[IPv6 TCP MSS]：（任意）すべての TCP 接続の最大セグメントサイズを指定します。デフォルト値は 1360 秒です。

c) [Throughput Delay]：（任意）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。デフォルト値は 1000 秒です。

d) [Bandwidth]：（任意）目的の帯域幅をキロバイト/秒（kbps）で指定します。デフォルト値は 1400 Kbps です。

機能プロファイルで使用する各パラメータの詳細については、『Security and VPN Configuration Guide』[英語] を参照してください。

article_task_postreq

DMVPN トンネルを設定した後に、設定グループと SD-Routing デバイスの関連付けおよび展開 （10 ページ）。

DMVPN トンネル内のデータ暗号化

（注）

データに IPSec 暗号化を追加すると、トンネル内のデータがネットワークを通過するときにデータを保護できます。Cisco DMVPN で使用される IPSec 暗号化は IKEv2 に基づいています。IKEv1 を使用した IPSec の設定はサポートされていません。

この設定は、オプションです。

IPSec 暗号化の [IKEv2 Authentication Type] で [Enterprise CA] を設定する前に、**[System Profile]** > **[Certificate]**の [SCEP enrollment] でトラストポイントを設定していることを確認します。

ステップ 1 Cisco Catalyst SD-WAN Manager に移動します。**[Configuration]** > **[Configuration Groups]**を選択します。[Solution] で [SD Routing] を選択します。

ステップ 2 既存の**サービスプロファイル**を選択するか、新しいプロファイルを作成します。

ステップ 3 既存の DMVPN トンネルを選択します。[+] 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プロファイルを識別するための名前と説明を指定します。詳細を入力して、プロファイルを設定します。

認証

a) [Local Identity]：通信を確立するために宛先ピアとの交換で送信するローカル IKE ID を指定します。

b) [Remote Identity]：通信を確立するために宛先ピアと交換するリモートIKE IDを指定します。複数のリモート ID を設定できます。各種 ID タイプは次のとおりです。

IPv4

IPv6 prefix

FQDN

E メール

KeyID

[IKEv2 Authentication Type]：IKEv2 は、ピア VPN デバイス間にセキュアな VPN 通信チャネルを提供し、保護された方法で IPSec セキュリティ アソシエーション（SA）のネゴシエーションと認証を定義するトンネリングプロトコルです。

a) [Groups PSK]：デバイスに接続中のすべてのリモート アクセス クライアントに共通の事前共有キーを設定するには、このオプションを選択します。ドロップダウンリストから [Global] を選択し、認証キーとして使用するキーを指定します。

b) [Peer-peer PSK]：ネットワーク内のピアと共有する共通の事前共有キーを設定するには、このオプションを選択します。

   [Peer name]：ピア名を指定します。

   [Pre-shared Key]：キーを指定します。

   [Peer Address Type]：IPv4 アドレスまたは IPv6 プレフィックスを選択します。

c) [Enterprise CA]：内部ルート CA によって署名された証明書を取得するには、このオプションを選択します。

   [PKI Trustpoint Name]：ドロップダウンリストからトラストポイントを選択します。

   [Signature Type]：ドロップダウンリストから [Global] を選択します。認証の署名タイプを選択します。デフォルトの署名は RSA です。

IKEv2 設定

a) [DPD keepalive Interval]：IKE ピアのキープアライブ間隔を指定します。DPD は、IPSec ピアが存在し、利用可能な状態であるかを確認するためにデバイスによって使用される方法です。デフォルトは 10 秒です。

b) [DPD Retry Interval]：IKE ピアの再試行間隔を指定します。再試行間隔は、DPD の再試行メッセージに対してピアからの応答がない場合に DPD 再試行メッセージを送信する秒単位の間隔を示します。値の範囲は 2 ～ 60 秒です。デフォルトは 3 秒です。

c) [IKE SA Lifetime]： ネゴシエートされた IKE SA（セキュリティ アソシエーション）キーが有効である期間を指定します。デフォルトのライフタイムは 86400 秒です。

IPSec 設定

a) [Security Association (SA) Lifetime (Seconds)]：セキュリティ アソシエーションが期限切れになるまでのアクティブ期間を秒単位で指定します。

b) [Anti Replay Window Size]：パケットサイズを指定します。このオプションを設定すると、暗号化された各パケットに一意のシーケンス番号が割り当てられるため、暗号化パケットの重複を防止できます。

c) [Perfect Forward Secrecy (PFS)]：PFS を有効にするには、トグルボタンを使用します。PFS を有効にすると、同じキーが再度生成されないため、このオプションでは新しい Diffie-Hellman キー交換が強制的に行われます。PFS を使用すると、セキュリティがさらに向上します。1 つのキーが攻撃者によってクラックされた場合でも、侵害されるのはそのキーで送信されたデータだけになるためです。

d) [PFS Group]：Diffie-Hellman グループを指定します。インターネット キー エクスチェンジ（IKE）プロトコルでは、Diffie-Hellman を使用して、IKE および IPSec セキュリティ アソシエーション（SA）の両方に対応するキー情報が取得されます。

ステップ 5 [Save] をクリックします。

コマンドを使用した Cisco DMVPN の設定

機能プロファイルを使用して設定した機能のほかにも、Cisco SD-WAN Manager で IOS XE コマンドを使用して追加の機能を設定できます。

（注）

IOS XE CLI コマンドは、フィーチャパーセルを介して提供される設定と連携して動作します。ただし、**CLI アドオンプロファイル**や**CLI 設定グループ**を使用して設定されたコマンドは、対応するフィーチャパーセルによって指定された設定をオーバーライドします。

CLI アドオンプロファイルを使用した Cisco DMVPN の設定

- セットアップ時にプロビジョニングする機能について理解しておく必要があります。各種機能とその設定コマンドの詳細については、『Security and VPN Configuration Guide』[英語] を参照してください。
- 自律ルーティングデバイスを Cisco SD-WAN Manager にオンボードする必要があります。また、デバイスのステータスは [In Sync] である必要があります。**[Configuration]** > **[WAN Edges]**を選択して、デバイスのステータスを確認します。

ステップ 1 Cisco SD-WAN Manager に移動します。**[Configuration]** > **[Configuration Groups]**を選択します。[Solution] で [SD Routing] を選択します。

ステップ 2 既存の設定グループを選択するか、新しい設定グループを作成します。設定グループを選択してから [+ Add Profile] をクリックし、[CLI Add-on Profile] を追加します。

ステップ 3 新しいプロファイルを作成するには、[+ Create New] を選択します。名前と説明を指定します。既存の CLI アドオンプロファイルがある場合は、そのプロファイルを選択し、[Edit] をクリックします。

ステップ 4 [Config Preview] ペインで、機能を設定するために必要なコマンドを入力します。[Save]、[Done] の順にクリックします。

ステップ 5 設定グループと SD-Routing デバイスの関連付けおよび展開 （10 ページ）。[Next] をクリックします。

ステップ 6 [Summary] ウィンドウで [Preview CLI] を選択します。新旧の設定が表示されます。変更内容を確認します。設定グループに戻るには、[Cancel] をクリックします。

CLI 設定グループを使用した Cisco DMVPN の設定

- セットアップ時に対象とする機能について理解しておく必要があります。機能およびその設定コマンドの詳細については、https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-conn-dmvpn-dmvpn-0.html [英語] を参照してください。
- 自律ルーティングデバイスを Cisco SD-WAN Manager にオンボードする必要があります。また、デバイスのステータスは [In Sync] である必要があります。**[Configuration]** > **[WAN Edges]**を選択して、デバイスのステータスを確認します。

ステップ 1 Cisco Catalyst SD-WAN Manager に移動します。**[Configuration]** > **[Configuration Groups]**を選択します。[Solution] で [SD Routing] を選択します。

ステップ 2 リストから既存の CLI 設定グループを選択するか、[Create Configuration Group] を選択して新しい設定グループを作成します。

ステップ 3 名前と説明を指定します。[CLI Configuration Group] チェックボックスをオンにします。

ステップ 4 設定のロード元のデバイスを選択します。[Config Preview] ペインで設定内容を確認し、追加の機能を設定するために必要なコマンドを入力します。[Save]、[Done] の順にクリックします。

ステップ 5 設定グループと SD-Routing デバイスの関連付けおよび展開 （10 ページ）。[Next] をクリックします。

ステップ 6 [Summary] ウィンドウで [Preview CLI] を選択します。新旧の設定が表示されます。設定グループに戻るには、[Cancel] をクリックします。

設定グループと SD-Routing デバイスの関連付けおよび展開

このタスクでは、設定済みのプロファイルを設定グループに関連付けます。また、変更を 1 つ以上の SD-Routing デバイスにプロビジョニングします。

該当する設定グループが SD-Routing デバイスで作成されていることを確認してください。

ステップ 1 Cisco SD-WAN Manager で、前に作成した**設定グループ**を選択します。

ステップ 2 [+ Add] をクリックして、リストからデバイスを確認します。[Save] をクリックして、選択したデバイスに設定グループを割り当てます。

ステップ 3 設定変更をプロビジョニングするには、[Deploy] をクリックします。

a) 設定変更をプロビジョニングするデバイスを選択します。[Next] をクリックします。

b) デバイスごとに、IP アドレス、ホスト名を確認または更新します。これらのデバイスにアクセスするためのパスワードを指定します。[Next] をクリックします。

c) 設定の変更内容を確認する場合は、[Preview CLI] をクリックします。デバイスを選択して、設定変更を縦並びまたは横並びで表示します。削除された設定は赤色で強調表示され、新しい設定は緑色で強調表示されます。選択したデバイスのリストでデバイスを削除または追加するには、[Edit Device List] をクリックします。

d) [Deploy] をクリックして、デバイスに設定の変更をプロビジョニングします。

Cisco DMVPN のモニター

ここでは、コマンドを使用して Cisco DMVPN をモニターする方法について説明します。

コマンドを使用した Cisco DMVPN セッションのモニター

DMVPN トンネルをモニターし、セッション情報を表示するには、次のコマンドを使用します。これらのコマンドは、Cisco SD-WAN Manager の**[Tools]** > **[SSH terminal]**を使用して実行できます。

使用コマンド	目的
show dmvpn	DMVPN セッションの情報を表示します。
show dmvpn detail	各セッションの DMVPN 詳細情報（ネクストホップサーバー（NHS）および NHS ステータス、暗号セッション情報、ソケットの詳細など）を表示します。
show crypto session	アクティブな暗号セッションのステータス情報を表示します。
show ip nhrp traffic	NHRP トラフィックの統計情報を表示します。
show ip nhrp summary	すべてのオーバーレイエントリのマッピング情報を表示します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。