



CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの設定

この章は、次の項で構成されています。

- [CloudSec を使用したセキュアな VXLAN EVPN マルチサイトについて \(1 ページ\)](#)
- [CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの注意事項と制約事項 \(2 ページ\)](#)
- [CloudSec の MLAG ボーダー ゲートウェイのサポート \(4 ページ\)](#)
- [MLAG 拡張 \(6 ページ\)](#)
- [CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの設定 \(7 ページ\)](#)
- [CloudSec を使用したセキュアな VXLAN EVPN マルチサイト \(15 ページ\)](#)
- [CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの統計情報の表示 \(20 ページ\)](#)
- [CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの設定例 \(21 ページ\)](#)
- [VIP を使用するマルチサイトから PIP を使用するマルチサイトへの移行 \(22 ページ\)](#)
- [既存の vPC BGW の移行 \(23 ページ\)](#)

CloudSec を使用したセキュアな VXLAN EVPN マルチサイトについて

CloudSec を使用したセキュアな VXLAN EVPN マルチサイトは、VXLAN ベースのマルチサイトファブリックのデータセキュリティとデータ整合性を保証します。この機能は、UDP パケットの IEEE MACsec の暗号化メカニズムを使用して、許可された VXLAN EVPN エンドポイント間にセキュアなトンネルを提供します。

CloudSec セッションは、2つの異なるサイトのボーダー ゲートウェイ (BGW) 間の DCI を介したポイントツーポイントです。サイト間のすべての通信は、VIP の代わりにマルチサイト PIP を使用します。移行情報の詳細については、[VIP を使用するマルチサイトから PIP を使用するマルチサイトへの移行 \(22 ページ\)](#) を参照してください。

CloudSec を使用したセキュア VXLAN EVPN マルチサイトが、ピアごとに有効になっていることを確認します。CloudSec をサポートしないピアは、CloudSec をサポートするピアと動作できますが、トラフィックは暗号化されません。CloudSec 非対応サイトから CloudSec 対応サイトへの移行中のみ、暗号化されていないトラフィックを許可することをお勧めします。

CloudSec キー交換では BGP が使用され、MACsec では MACsec Key Agreement (MKA) が使用されます。CloudSec コントロールプレーンは、BGP IPv4 アドレス ファミリをキー情報の交換に使用します。CloudSec キーは、アンダーレイ BGP セッションを使用する BGP IPv4 ルートのトンネルカプセル化 (トンネルタイプ 18) 属性の一部として伝送されます。

キー ライフタイムおよびヒットレス キー ロールオーバー

CloudSec キー チェーンには、キー ID とオプションのライフタイムが設定された複数の事前共有キー (PSK) を含めることができます。事前共有キーは、トラフィックの暗号化と整合性検証のためにさらにキーを取得するために使用されるシードキーです。事前共有キーのリストは、異なるライフタイムを持つキーチェーンで設定できます。

キーのライフタイムには、キーが期限切れになる時刻が指定されます。ライフタイムが設定されている場合、ライフタイムの期限が切れた後に、MKA はキー チェーン内の次に設定された事前共有キーにロールオーバーします。キーのタイムゾーンは、ローカルまたは UTC を指定できます。デフォルトの時間帯は UTC です。ライフタイム設定が存在しない場合は、無期限のデフォルト ライフタイムが使用されます。

CloudSec キー チェーンを設定するには、[CloudSec キーチェーンとキーの設定 \(10 ページ\)](#) を参照してください。

最初のキーのライフタイムが期限切れになると、リスト内の次のキーに自動的にロールオーバーします。同一のキーがリンクの両側で同時に設定されている場合、キーのロールオーバーはヒットレスになります。つまり、キーはトラフィックを中断せずにロールオーバーされます。つまり、トラフィックが中断されることなくキーがロールオーバーされます。キーのライフタイムは、ヒットレス キー ロールオーバーを実現するためにオーバーラップする必要があります。

CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの注意事項と制約事項

CloudSec を使用したセキュアな VXLAN EVPN マルチサイトには、次の注意事項と制約事項があります。

- Cisco NX-OS リリース 10.2(2)F 以降、vPC ボード ゲートウェイのマルチシャーシリンク アグリゲーション グループ (MLAG) のサポートは、Cisco Nexus 9300-FX2、-FX3、および N9K-C9332D-GX2B スイッチでサポートされます。
- Cisco NX-OS リリース 10.2(3) 以降、vPC ボード ゲートウェイの MLAG サポートは、Cisco Nexus 9364D-GX2A および 9348D-GX2A プラットフォーム スイッチでサポートされます。

- MLAG Cloudsec をサポートするには、MCT/vPC ピア リンク ポートが CloudSec に対応している必要があります。ポートのサブセットのみが CloudSec/MACsec をサポートするため、これは N9K-C9332D-GX2B スイッチに必要です。一方、Cisco Nexus 9300-FX2/FX3 ファミリ スイッチでは、すべてのポートが CloudSec に対応しています。
- CloudSec を使用しているセキュアな VXLAN EVPN マルチサイトは、Cisco NX-OS リリース 9.3(5) 以降 Cisco Nexus 9300-FX2 プラットフォーム スイッチでサポートされます。
- CloudSec を使用しているセキュアな VXLAN EVPN マルチサイトは、Cisco NX-OS リリース 10.1(1) 以降から Cisco Nexus 9300-FX3 プラットフォーム スイッチでサポートされます。
- CloudSec を使用しているセキュアな VXLAN EVPN マルチサイトは、Cisco NX-OS リリース 10.2(1q)F 以降から Cisco Nexus 9300-GX2 プラットフォーム スイッチでサポートされます。
- Cisco Nexus NX-OS リリース 10.1(3) 以降、CloudSec を使用したセキュア VXLAN EVPN マルチサイトは、Cisco Nexus 9300-GX2A プラットフォーム スイッチでのみサポートされます。
- L3 インターフェイスおよび L3 ポートチャネルは DCI リンクとしてサポートされます。
- スイッチ宛ての CloudSec トラフィックは、DCI アップリンクを介してスイッチに入る必要があります。
- CloudSec を使用したセキュアな VXLAN EVPN マルチサイトは、ルートサーバ経由で接続されているサイト、またはフル メッシュ（ルート サーバなし）を使用して接続されているサイトでサポートされます。ルート サーバを介して接続されているサイトの場合は、サーバを Cisco NX-OS リリース 9.3(5) 以降のリリースにアップグレードし、[CloudSec VXLAN EVPN トンネル暗号化の有効化（7 ページ）](#) の手順に従います。
- Cisco NX-OS リリース 10.2(1q)F 以降、VXLAN トンネル暗号化は Cisco Nexus N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.2(3) 以降、VXLAN トンネル暗号化は Cisco Nexus 9364D-GX2A、および 9348D-GX2A プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.1(1) 以降、VXLAN トンネル暗号化機能は Cisco Nexus 9300-FX3 プラットフォーム スイッチでサポートされます。
- ICV は、Cisco NX-OS リリース 9.3(7) ではデフォルトで無効になっています。以前のリリース（Cisco NX-OS リリース 9.3(6)）のノードと cloudsec トンネルセッションを形成する場合は、ノードで ICV を無効にする必要があります。
- CloudSec を使用して、同じサイト上のすべての BGW をセキュア VXLAN EVPN マルチサイト用に設定する必要があります。
- DCI リンクで CloudSec を使用するセキュア VXLAN EVPN マルチサイトと、内部ファブリックで MACsec を共存させることができます。ただし、同じポートまたはポートグループ（MAC ID）で同時に有効にすることはできません。

- CloudSec ピアを使用するセキュアな VXLAN EVPN マルチサイトは、それらの間のセキュアなトラフィックを復号化するために同じキーチェーン設定を持つ必要があります。
- Cisco Nexus 9300-FX2 ファミリースイッチのセキュリティキー配布の BGP IPv4 アップデートでは、最大 60 のピアがサポートされます。
- Cisco NX-OS リリース 10.2(3) 以降、セキュリティキー配布の BGP IPv4 アップデートは Cisco Nexus 9300-FX3 プラットフォームスイッチでサポートされます。
- アクティブタイマーが設定されたすべてのキーが期限切れになったときにセッションを維持するには、キーチェーンごとにライフタイムなしで1つのキーだけを設定します。ベストプラクティスとして、キーごとにライフタイムを設定することを推奨します。
- CloudSec キーは、アンダーレイ BGP セッションを使用する BGP IPv4 ルートでトンネルカプセル化属性を使用して BGW間で交換されます。

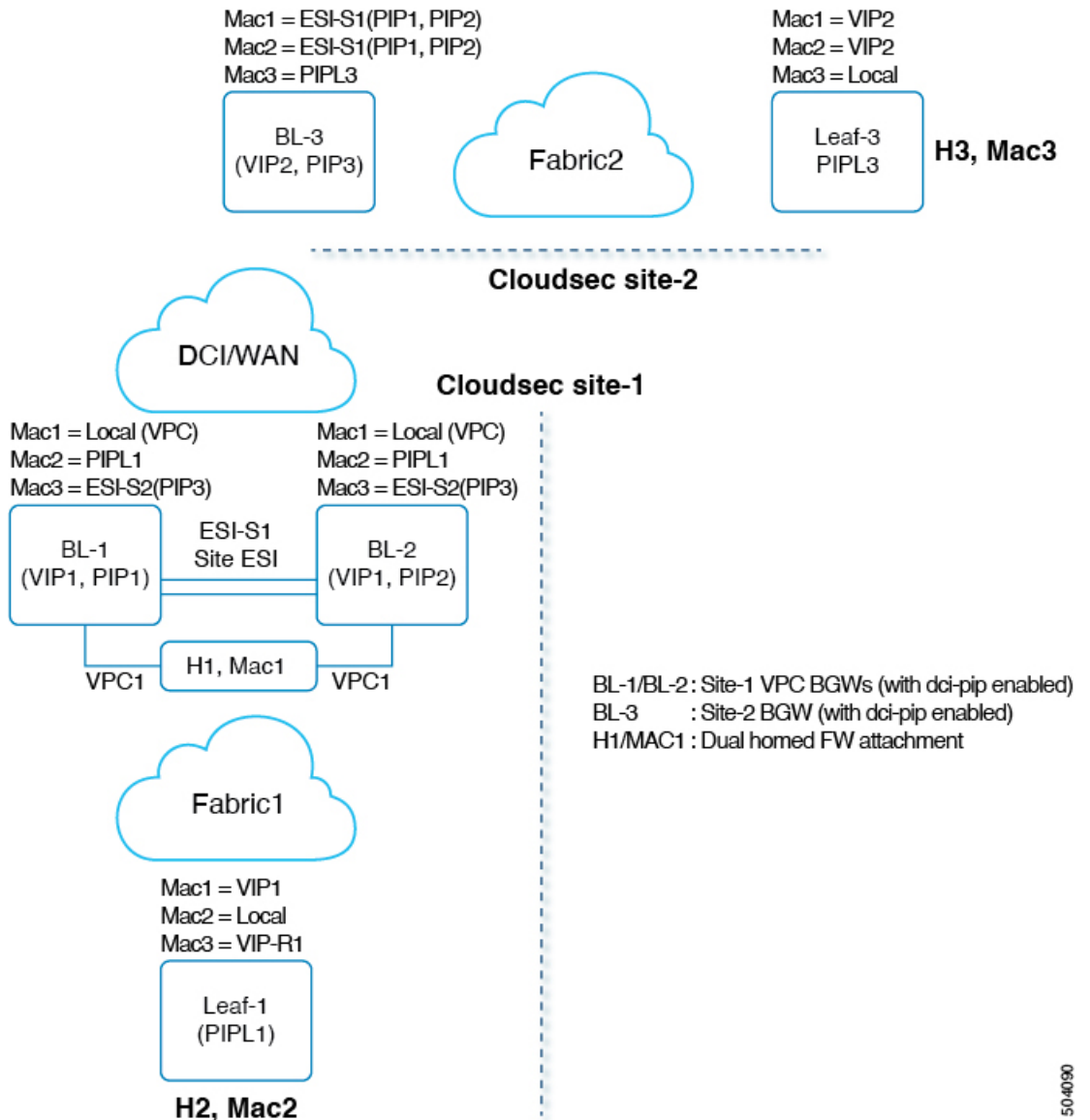
この属性が中間ノードによって伝播されない場合は、CloudSec エンドポイントノード、つまり BGW間で直接 BGP IPv4 ユニキャストセッションを設定する必要があります。

- CloudSec を使用したセキュアな VXLAN EVPN マルチサイトは、次をサポートします。
 - ボーダー ゲートウェイ上の直接接続された L2 ホスト
 - DCI インターフェイスの IP アンナナバード設定
 - マルチキャストアンダーレイ
 - OAM パストレース
 - TRM
 - ボーダー ゲートウェイの VIP 専用モデル
 - ダウンストリーム VNI を使用した VXLAN EVPN
- Cisco NX-OS リリース 10.3(1) 以降、DSVNI を使用する MLAG cloudsec は Cisco Nexus 9000 シリーズスイッチでサポートされます。
- CloudSec が有効になっている場合、非中断の ISSU はサポートされません。

Cloudsec の MLAG ボーダー ゲートウェイのサポート

次のトポロジは、Cloudsec のマルチシャーシリンクアグリゲーション (MLAG) ボーダーゲートウェイ (BGW) のサポートを示しています。

図 1: Cloudsec の MLAG BGW サポート



50-4090

MLAG は、BGW へのデュアルホーム接続/接続です。BGW は冗長性のための単一の VXLAN エンドポイントとして仮想的に機能し、両方のスイッチは共通のエミュレート/仮想 IP アドレス (VIP) を共有することによってアクティブモードで機能します。DCI 上の VXLAN カプセル化は、BGW VTEP のプライマリ IP アドレスに基づいています。

上記のトポロジでは、ホスト H1/MAC1 は、Cloudsec 対応の vPC BGW BL-1/BL-2 にデュアルホーム接続されています。H1 は、ファブリックへの vPC BGW (VIP1) のセカンダリ ループバック IP アドレスで引き続きアドバタイズされます。ただし DCI に対しては、BL-1/BL-2 の両方が PIP としてネクストホップを使用して H1 をアドバタイズし、サイト ESI もタイプ 2 NLRI に追加されます。

エニーキャストおよび vPC BGW の Cloudsec 機能の場合、dci-advertise-pip はタイプ 2/タイプ 5 ルートが DCI にアドバタイズされる方法に関して、BGP 手順を変更するように構成されています。サイト内部ネットワークから受信したすべてのタイプ 2/タイプ 5 ルートは、vPC BGW の PIP としてネクスト ホップを使用して DCI にアドバタイズされます。

両方の vPC BGW は、それぞれのプライマリ IP アドレスを使用してルートをアドバタイズします。Site-ESI 属性が Type-2 NLRI に追加されます。vPC BGW 上のすべてのデュアル接続ホストは、PIP としてネクストホップでアドバタイズされ、サイト ESI 属性は DCI を介して接続されます。すべての孤立ホストは、DCI への PIP としてネクストホップでアドバタイズされ、サイト ESI 属性は付加されません。

vPC BGW がピア vPC BGW の PIP アドレスを学習し、DCI 側でアドバタイズする場合、両方の vPC BGW からの BGP パス属性は同じになります。したがって、DCI 中間ノードは PIP アドレスを所有していない vPC BGW からのパスを選択することになる可能性があります。このシナリオでは、リモート サイトからの暗号化されたトラフィックに MCT リンクが使用されます。vPC BGW BGP は、次の場合にピア vPC BGW の PIP アドレスを学習します。

- iBGP は vPC BGW 間で構成されます。
- BGP は、ファブリック側のアンダーレイ ルーティング プロトコルとして使用されます。
- アンダーレイ ルーティング プロトコルとして使用される IGP、および IGP ルートが BGP に再配布されます。

vPC BGW が BGP でピア vPC BGW の PIP アドレスを学習する場合、アウトバウンドルート マップを構成して、BGW のパスを最適なパスにする必要があります。

リモートサイト BGW では、直接接続された L3 ホストは両方の vPC BGW から学習されます。通常直接接続された BGW からのパスは、AS パスが低いため優先されます。L3 ホストまたは L3 ネットワークが vPC ペア BGW に二重接続されている場合、ローカルパスは両方の vPC ペアで選択されます。

MLAG 拡張

従来、単一のループバック インターフェイスは NVE 送信元 インターフェイスとして設定され、vPC コンプレックスの PIP と VIP の両方が構成されています。CloudSec が有効になっている vPC BGW では、MLAG 展開でのコンバージェンスを向上させるために、NVE の下で送信元とエニーキャスト IP アドレスに個別のループバック インターフェイスを使用することをお勧めします。送信元インターフェイスに構成されている IP アドレスは vPC ノードの PIP であり、エニーキャストインターフェイスに構成されている IP アドレスはその vPC コンプレックスの VIP です。NVE エニーキャストインターフェイスも構成されている場合、NVE ソースインターフェイスで設定されたセカンダリ IP は効果がないことに注意してください。

個別のループバックを使用すると、DCI 側を宛先とするデュアル接続タイプ 2/5 トラフィックのコンバージェンスが改善されます。

ユーザーがエニーキャスト インターフェイスを指定したい場合、ユーザーは既存の送信元 インターフェイスを構成解除し、送信元 インターフェイスとエニーキャスト インターフェイス

の両方で再構成する必要があります。これにより、一時的なトラフィック損失が発生します。すべてのグリーンフィールド展開では、指定されたコンバージェンスの問題を回避するために、送信元インターフェイスとエニーキャストインターフェイスの両方を設定することをお勧めします。

エンドユーザインターフェイス

ユーザーは、vPCBGWのNVE送信元インターフェイスとともにエニーキャストインターフェイスを指定する必要があります。現在のVxLANv6展開では、送信元インターフェイスとエニーキャストインターフェイスの両方を指定するプロビジョニングがすでに存在しています。VxLANv4のMLAGコンバージェンスを改善するには、エニーキャストオプションが必須です。

設定例：

```
Interface nve <number>
    source-interface <interface> [anycast <anycast-intf>]
```

iBGP セッションの要件

アンダーレイ IPv4/IPv6 ユニキャスト iBGP セッションは、vPC BGW ピア ノード間で構成する必要があります。これは、vPC BGW での DCI 分離中のキー伝播に対応するためです。

CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの設定

CloudSec を使用してセキュアな VXLAN EVPN マルチサイトを設定するには、次の手順に従います。

- [CloudSec VXLAN EVPN トンネル暗号化の有効化 \(7 ページ\)](#)
- [CloudSec キーチェーンとキーの設定 \(10 ページ\)](#)
- [CloudSec ポリシーの設定 \(12 ページ\)](#)
- [CloudSec ピアの設定 \(13 ページ\)](#)
- [DCI アップリンクで CloudSec を使用したセキュアな VXLAN EVPN マルチサイトを有効にする \(14 ページ\)](#)

CloudSec VXLAN EVPN トンネル暗号化の有効化

CloudSec VXLAN EVPN トンネル暗号化を有効にするには、次の手順を実行します。

始める前に

IPv4 ユニキャストアドレスファミリーで BGP ピアを設定します。IPv4 プレフィックスが CloudSec キーを伝送するトンネル コミュニティ属性とともに伝播されていることを確認します。

VXLAN EVPN マルチサイトを設定し、次のコマンドを使用して、CloudSec VXLAN EVPN トンネル暗号化のピア IP アドレスをアドバタイズします。

```
evpn multisite border-gateway ms-id
dci-advertise-pip
```



注意 **dci-advertise-pip** なしで VXLAN EVPN マルチサイトを設定すると、ボーダー ゲートウェイを VIP 専用モードに戻します。これは CloudSec VXLAN EVPN トンネル暗号化ではサポートされません。

ルート サーバを介して接続されているサイトには、次の 2 つのオプションがあります。

- デュアル RD を有効にする：このデフォルトの動作により、メモリが限られたリーフデバイスを処理するために、以前のリリースと同じメモリスケールが維持されます。すべての同一サイト BGW は、リモート BGW に EVPN ルートをアドバタイズする間、再発信ルートに同じ RD 値を使用します。
- デュアル RD の無効化：リーフデバイスのメモリ制限がない場合は、BGW で **no dual rd** コマンドを設定できます。EVPN ルートをリモート BGW にアドバタイズする間、同じ BGW で再発信されたルートに異なる RD 値が使用されます。

BGW でデュアル RD が有効になっているかどうかに応じて、次のいずれかの操作を実行します。

- デュアル RD が BGW で設定されている場合は、次の手順を実行します。

1. BGW に BGP 追加パスを適用します。

```
router bgp as-num
  address-family l2vpn evpn
    maximum-paths number
  additional-paths send
  additional-paths receive
```

2. BGW で各 L3VNI VRF のマルチパスを設定します。

```
vrf evpn-tenant-00001
  address-family ipv4 unicast
    maximum-paths 64
  address-family ipv6 unicast
    maximum-paths 64
```

3. ルート サーバに BGP 追加パスを適用します。

```
router bgp as-num
  address-family l2vpn evpn
    retain route-target all
  additional-paths send
  additional-paths receive
  additional-paths selection route-map name

route-map name permit 10
  set path-selection all advertise
```


- **no dual rd** が BGW で設定されている場合、またはフル メッシュが設定されている場合は、次の手順を実行します。

1. BGW でアドレス ファミリと最大パスを設定します。

```
router bgp as-num
  address-family l2vpn evpn
    maximum-paths number
```

2. BGW で各 L3VNI VRF のマルチパスを設定します。

```
vrf evpn-tenant-00001
  address-family ipv4 unicast
    maximum-paths 64
  address-family ipv6 unicast
    maximum-paths 64
```



(注) BGP 追加パスは、ルート サーバでは必要ありません。

手順の概要

1. **configure terminal**
2. **[no] feature tunnel-encryption**
3. **[no] tunnel-encryption source-interface loopback number**
4. **tunnel-encryption icv**
5. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	[no] feature tunnel-encryption 例 : <pre>switch(config)# feature tunnel-encryption</pre>	CloudSec VXLAN EVPN トンネル暗号化を有効にします。
ステップ 3	[no] tunnel-encryption source-interface loopback number 例 : <pre>switch(config)# tunnel-encryption source-interface loopback 2</pre>	トンネルの送信元をループバック インターフェイスとして BGP ループバックを指定します。設定された送信元 インターフェイスの IP アドレスは、CloudSec VXLAN EVPN トンネル暗号化キー ルートを通知するためのプレフィックスとして使用されます。

	コマンドまたはアクション	目的
		<p>(注) NVE 送信元インターフェイスではなく、BGP ループバック インターフェイスを入力します。</p> <p>(注) MTU の変更は、インターフェイスのトンネル暗号化設定の前に行う必要があります。これにより、CRC ドロップエラーが回避されます。</p>
ステップ 4	tunnel-encryption icv 例： <pre>switch(config)# tunnel-encryption icv</pre>	Integrity Check Value (ICV) を有効にします。ICV は、ポートに到着するフレームの整合性チェックを行います。生成された ICV がフレーム内の ICV と同じであれば、そのフレームは受け入れられ、同じでなければ破棄されます。これは、Cisco NX-OS リリース 9.3(7) 以降、サポートされます。
ステップ 5	(任意) copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次のタスク

[CloudSec キーチェーンとキーの設定。](#)

CloudSec キーチェーンとキーの設定

デバイスに CloudSec キーチェーンとキーを作成できます。

始める前に

CloudSec を使用したセキュア VXLAN EVPN マルチサイトが有効になっていることを確認します。

手順の概要

1. **configure terminal**
2. **[no] key chain name tunnel-encryption**
3. **[no] key key-id**
4. **[no] key-octet-string octet-string cryptographic-algorithm {AES_128_CMAC | AES_256_CMAC}**
5. **[no] send-lifetime start-time duration duration**
6. (任意) **show key chain name**
7. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[no] key chain name tunnel-encryption 例： switch(config)# key chain kcl tunnel-encryption switch(config-tunnelencryptkeychain)#	CloudSec キーチェーンを作成して CloudSec キーのセットを保持し、トンネル暗号化キーチェーン設定モードを開始します。
ステップ 3	[no] key key-id 例： switch(config-tunnelencryptkeychain)# key 2000 switch(config-tunnelencryptkeychain-tunnelencryptkey)#	CloudSec キーを作成し、トンネル暗号キー設定モードを開始します。範囲は 1~32 オクテットで、最大サイズは 64 です。 (注) キーの文字数は偶数でなければなりません。
ステップ 4	[no] key-octet-string octet-string cryptographic-algorithm {AES_128_CMAC AES_256_CMAC} 例： switch(config-tunnelencryptkeychain-tunnelencryptkey)# key-octet-string abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789 cryptographic-algorithm AES_256_CMAC	そのキーの octet ストリングを設定します。octet-string 引数には、最大 64 文字の 16 進数文字を含めることができます。octet キーは内部でエンコードされるため、クリア テキストのキーは show running-config tunnel-encryption コマンドの出力に表示されません。
ステップ 5	[no] send-lifetime start-time duration duration 例： switch(config-tunnelencryptkeychain-tunnelencryptkey)# send-lifetime 00:00:00 May 06 2020 duration 100000	キーの送信ライフタイムを設定します。デフォルトでは、デバイスは開始時間を UTC として扱います。 <i>start-time</i> 引数は、キーがアクティブになる日時です。 <i>duration</i> 引数はライフタイムの長さ (秒) です。範囲は 1800~2147483646 秒 (約68年) です。
ステップ 6	(任意) show key chain name 例： switch(config-tunnelencryptkeychain-tunnelencryptkey)# show key chain kcl	キーチェーンの設定を表示します。
ステップ 7	(任意) copy running-config startup-config 例： switch(config-tunnelencryptkeychain-tunnelencryptkey)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次のタスク

[CloudSec ポリシーの設定。](#)

CloudSec ポリシーの設定

異なるパラメータを使用して複数の CloudSec ポリシーを作成できます。しかし、1つのインターフェイスでアクティブにできるポリシーは1つのみです。

始める前に

CloudSec を使用したセキュア VXLAN EVPN マルチサイトが有効になっていることを確認します。

手順の概要

1. **configure terminal**
2. (任意) **[no] tunnel-encryption must-secure-policy**
3. **[no] tunnel-encryption policy name**
4. (任意) **[no] cipher-suite name**
5. (任意) **[no] window-size number**
6. (任意) **[no] sak-rekey-time time**
7. (任意) **show tunnel-encryption policy**
8. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	(任意) [no] tunnel-encryption must-secure-policy 例 : <pre>switch(config)# tunnel-encryption must-secure-policy</pre>	暗号化されていないパケットがセッションの回線を介して送信されないようにします。CloudSec ヘッダーを伝送しないパケットはドロップされます。 このコマンドの no 形式は、暗号化されていないトラフィックを許可します。CloudSec 非対応サイトから CloudSec 対応サイトへの移行中にのみ、暗号化されていないトラフィックを許可することをお勧めします。デフォルトでは、CloudSec を使用するセキュアな VXLAN EVPN マルチサイトは「セキュア」モードで動作することが必要です。

	コマンドまたはアクション	目的
ステップ 3	[no] tunnel-encryption policy name 例： switch(config)# tunnel-encryption policy pl switch(config-tunenc-policy)#	CloudSec ポリシーを作成します。
ステップ 4	(任意) [no] cipher-suite name 例： switch(config-tunenc-policy)# cipher-suite GCM-AES-XPB-256	GCM-AES-XPB-128 または GCM-AES-XPB-256 のいずれかを設定します。デフォルト値は GCM-AES-XPB-256 です。
ステップ 5	(任意) [no] window-size number 例： switch(config-tunenc-policy)# window-size 134217728	インターフェイスが設定されたウィンドウサイズ未満の packets を受け入れないように、再生保護ウィンドウを設定します。範囲は 134217728～1073741823 IP packets です。デフォルト値は 268435456 です。
ステップ 6	(任意) [no] sak-rekey-time time 例： switch(config-tunenc-policy)# sak-rekey-time 1800	SAK キー再生成を強制する時間を秒単位で設定します。このコマンドを使用して、セッションキーを予測可能な時間間隔に変更できます。有効な範囲は 1800～2592000 秒です。デフォルト値はありません。すべてのピアに同じキー再作成値を使用することを推奨します。
ステップ 7	(任意) show tunnel-encryption policy 例： switch(config-tunenc-policy)# show tunnel-encryption policy	CloudSec ポリシー設定を表示します。
ステップ 8	(任意) copy running-config startup-config 例： switch(config-tunenc-policy)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次のタスク

[CloudSec ピアの設定](#)

CloudSec ピアの設定

CloudSec ピアを設定できます。

始める前に

CloudSec を使用したセキュアな VXLAN EVPN マルチサイト

手順の概要

1. **configure terminal**
2. **[no] tunnel-encryption peer-ip peer-ip-address**
3. **[no] keychain name policy name**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[no] tunnel-encryption peer-ip peer-ip-address 例： switch(config)# tunnel-encryption peer-ip 33.1.33.33	ピアの NVE 送信元インターフェイスの IP アドレスを指定します。
ステップ 3	[no] keychain name policy name 例： switch(config)# keychain kc1 policy p1	CloudSec ピアにポリシーをアタッチします。

次のタスク

[DCI アップリンクで CloudSec を使用したセキュアな VXLAN EVPN マルチサイトを有効にする](#)

DCI アップリンクで CloudSec を使用したセキュアな VXLAN EVPN マルチサイトを有効にする

すべての DCI アップリンクで CloudSec を使用してセキュアな VXLAN EVPN マルチサイトを有効にするには、次の手順に従います。



(注) この設定は、レイヤ 2 ポートには適用できません。



(注) ポートで CloudSec を有効にして、CloudSec を無効にするときにポートを初期化すると、システムはそのポートをシャットダウンします。ポートがすでに稼働している場合、ポートはシャットダウン後に自動的に稼働します。

始める前に

CloudSec を使用したセキュア VXLAN EVPN マルチサイトが有効になっていることを確認します。

手順の概要

1. **configure terminal**
2. **[no] interface ethernet port/slot**
3. **[no] tunnel-encryption**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[no] interface ethernet port/slot 例： switch(config)# interface ethernet 1/1 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 3	[no] tunnel-encryption 例： switch(config-if)# tunnel-encryption	指定したインターフェイスで CloudSec を使用してセキュアな VXLAN EVPN マルチサイトを有効にします。

CloudSec を使用したセキュアな VXLAN EVPN マルチサイト

CloudSec 設定情報を使用してセキュアな VXLAN EVPN マルチサイトを表示するには、以下のタスクのいずれかを実行します。

コマンド	目的
show tunnel-encryption info global	CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの設定情報を表示します。
show tunnel-encryption policy [policy-name]	特定の CloudSec ポリシーまたはすべての CloudSec ポリシーの設定を表示します。
show tunnel-encryption session [peer-ip peer-ip-address] [detail]	エンドポイント間のセッションがセキュアかどうかなど、CloudSec セッションに関する情報を表示します。

コマンド	目的
show running-config tunnel-encryption	CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの実行中の設定を表示します。
show bgp ipv4 unicast ip-address	BGP ルートのトンネル暗号化情報を表示します。
show bgp l2vpn evpn	レイヤ 2 VPN EVPN アドレス ファミリとルーティング テーブル情報を表示します。
show ip route ip-address vrf vrf	VRF ルートを表示します。
show l2route evpn mac evi evi	レイヤ 2 ルート情報を表示します。
show nve interface interface detail	NVE インターフェイスの詳細を表示します。
show running-config rpm	実行中の設定でキー テキストを表示します。 (注) key-chain tunnelencrypt-psk no-show コマンドを実行する前にコマンドを入力すると、キーテキストは実行中の設定で非表示になります (アスタリスク付き)。 reload ascii コマンドを入力すると、キーテキストは実行中の設定から省略されます。

次の例では、CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの設定情報を表示します。

```
switch# show tunnel-encryption info global
Global Policy Mode: Must-Secure
SCI list: 0000.0000.0001.0002 0000.0000.0001.0004
No. of Active Peers      : 1
```

次に、設定されているすべての CloudSec ポリシーを表示する例を示します。出力には、各ポリシーの暗号、ウィンドウ サイズ、および SAK 再試行時間が表示されます。

```
switch# show tunnel-encryption policy
Tunnel-Encryption Policy  Cipher          Window         SAK Rekey time
-----
cloudsec                  GCM-AES-XPN-256  134217728     1800
p1                        GCM-AES-XPN-256  1073741823
system-default-tunenc-policy GCM-AES-XPN-256  268435456
```

次の例では、CloudSec セッションに関する情報を表示します。出力には、ピアの IP アドレスとポリシー、使用可能なキーチェーン、およびセッションがセキュアかどうかを示されます。

```
switch# show tunnel-encryption session
Tunnel-Encryption Peer Policy Keychain RxStatus TxStatus
-----
33.1.33.33         p1          kc1       Secure (AN: 0) Secure (AN: 2)
```



```

33.2.33.33      p1      kc1      Secure (AN: 0)  Secure (AN: 2)
33.3.33.33      p1      kc1      Secure (AN: 0)  Secure (AN: 2)
44.1.44.44      p1      kc1      Secure (AN: 0)  Secure (AN: 0)
44.2.44.44      p1      kc1      Secure (AN: 0)  Secure (AN: 0)

```

次に、BGP ルートのトンネル暗号化情報の例を示します。

```

switch# show bgp ipv4 unicast 199.199.199.199 □ Source-loopback configured on peer BGW
for CloudSec
BGP routing table information for VRF default, address family IPv4 Unicast
BGP routing table entry for 199.199.199.199/32, version 109
Paths: (1 available, best #1)
Flags: (0x8008001a) (high32 0x000200) on xmit-list, is in urib, is best urib route, is
in HW
Multipath: eBGP

  Advertised path-id 1
  Path type: external, path is valid, is best path, no labeled nexthop, in rib
  AS-Path: 1000 200 , path sourced external to AS
    89.89.89.89 (metric 0) from 89.89.89.89 (89.89.89.89)
      Origin IGP, MED not set, localpref 100, weight 0
      Tunnel Encapsulation attribute: Length 120

  Path-id 1 advertised to peers:
    2.2.2.2

```

次の例は、MAC が仮想 ESI に接続されているかどうかを示しています。

```

switch(config)# show bgp l2vpn evpn 0012.0100.000a
BGP routing table information for VRF default, address family L2VPN EVPN
Route Distinguisher: 110.110.110.110:32876
BGP routing table entry for [2]:[0]:[0]:[48]:[0012.0100.000a]:[0]:[0.0.0.0]/216, version
13198
Paths: (1 available, best #1)
Flags: (0x000202) (high32 00000000) on xmit-list, is not in l2rib/evpn, is not in HW
Multipath: eBGP

  Advertised path-id 1
  Path type: external, path is valid, is best path, no labeled nexthop
    Imported to 1 destination(s)
    Imported paths list: l2-10109
  AS-Path: 1000 200 , path sourced external to AS
    10.10.10.10 (metric 0) from 89.89.89.89 (89.89.89.89)
      Origin IGP, MED not set, localpref 100, weight 0
      Received label 10109
      Extcommunity: RT:100:10109 ENCAP:8
      ESI: 0300.0000.0000.0200.0309

  Path-id 1 not advertised to any peer

Route Distinguisher: 199.199.199.199:32876
BGP routing table entry for [2]:[0]:[0]:[48]:[0012.0100.000a]:[0]:[0.0.0.0]/216, version
24823
Paths: (1 available, best #1)
Flags: (0x000202) (high32 00000000) on xmit-list, is not in l2rib/evpn, is not in HW
Multipath: eBGP

  Advertised path-id 1
  Path type: external, path is valid, is best path, no labeled nexthop
    Imported to 1 destination(s)
    Imported paths list: l2-10109
  AS-Path: 1000 200 , path sourced external to AS
    9.9.9.9 (metric 0) from 89.89.89.89 (89.89.89.89)

```

```

Origin IGP, MED not set, localpref 100, weight 0
Received label 10109
Extcommunity: RT:100:10109 ENCAP:8
ESI: 0300.0000.0000.0200.0309

```

```
Path-id 1 not advertised to any peer
```

次に、リモートサイトから受信した EVPN タイプ 5 ルート用に作成された ECMP の例を示します。

```

switch(config)# show ip route 205.205.205.9 vrf vrf903
IP Route Table for VRF "vrf903"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

205.205.205.9/32, ubest/mbest: 2/0
  *via 9.9.9.9%default, [20/0], 11:06:32, bgp-100, external, tag 1000, segid: 900003
  tunnelid: 0x9090909 encap: VXLAN

  *via 10.10.10.10%default, [20/0], 3d05h, bgp-100, external, tag 1000, segid: 900003
  tunnelid: 0xa0a0a0a encap: VXLAN

```

次の例は、リモートサイトから受信した MAC に ESI ベースの MAC マルチパスが設定されているかどうかを示しています。

```

switch(config)# show l2route evpn mac evi 109 mac 0012.0100.000a detail

Flags -(Rmac):Router MAC (Stt):Static (L):Local (R):Remote (V):vPC link
(Dup):Duplicate (Spl):Split (Rcv):Recv (AD):Auto-Delete (D):Del Pending
(S):Stale (C):Clear, (Ps):Peer Sync (O):Re-Originated (Nho):NH-Override
(Pf):Permanently-Frozen, (Orp): Orphan

Topology Mac Address      Prod   Flags  Seq No Next-Hops
-----
109      0012.0100.000a BGP    SplRcv 0          9.9.9.9 (Label: 10109)
                                     10.10.10.10 (Label: 10109)

Route Resolution Type: ESI
Forwarding State: Resolved (PL)
Resultant PL: 9.9.9.9, 10.10.10.10
Sent To: L2FM
ESI : 0300.0000.0000.0200.0309
Encap: 1

```

次の例は、PIP を使用した VXLAN EVPN マルチサイトが設定されていることを示しています。

```

switch(config)# show nve interface nvel detail
Interface: nvel, State: Up, encapsulation: VXLAN
VPC Capability: VPC-VIP-Only [not-notified]
Local Router MAC: 700f.6a15.c791
Host Learning Mode: Control-Plane
Source-Interface: loopback0 (primary: 14.14.14.14, secondary: 0.0.0.0)
Source Interface State: Up
Virtual RMAC Advertisement: No
NVE Flags:
Interface Handle: 0x49000001
Source Interface hold-down-time: 180
Source Interface hold-up-time: 30
Remaining hold-down time: 0 seconds
Virtual Router MAC: N/A

```

```

Virtual Router MAC Re-origination: 0200.2e2e.2e2e
Interface state: nve-intf-add-complete
Multisite delay-restore time: 180 seconds
Multisite delay-restore time left: 0 seconds
Multisite dci-advertise-pip configured: True
Multisite bgw-if: loopback1 (ip: 46.46.46.46, admin: Up, oper: Up)
Multisite bgw-if oper down reason:

```

次の例は、実行中の設定のキーテキストを示しています。**key-chain tunnelencrypt-psk no-show** コマンドを入力すると、キーテキストは非表示になります。

```

switch# show running-config rpm

!Command: show running-config rpm
!Running configuration last done at: Mon Jun 15 14:41:40 2020
!Time: Mon Jun 15 15:10:27 2020

version 9.3(5) Bios:version 05.40
key chain inter tunnel-encryption
  key 3301
    key-octet-string 7
      075f79696a58405441412e2a577f0f077d6461003652302552040a0b76015a504e370c
      7972700604755f0e22230c03254323277d2f5359741a6b5d3a5744315f2f cryptographic-algorithm
      AES_256_CMAC
key chain kcl tunnel-encryption
  key 3537
    key-octet-string 7
      072c746f172c3d274e33592e22727e7409106d003725325758037800777556213d4e0c7c00770576772
      d08515e0804553124577f5a522e046d6a5f485c35425f59 cryptographic-algorithm AES_256_CMAC
      send-lifetime local 09:09:40 Apr 15 2020 duration 1800
  key 2001
    key-octet-string 7
      075f79696a58405441412e2a577f0f077d6461003652302552040a0b76015a504e370c7972700604755
      f0e22230c03254323277d2f5359741a6b5d3a5744315f2f cryptographic-algorithm AES_256_CMAC
  key 2065
    key-octet-string 7
      0729791f6f5e3d213347292d517308730c156c7737223554270f787c07722a513e450a0a0703070c062
      e0256210d0e204120510d29222a051f1e594c2135375359 cryptographic-algorithm AES_256_CMAC
  key 2129
    key-octet-string 7
      075c796f6f2a4c2642302f5c56790e767063657a4b564f2156777c0a020228564a32780e0472007005530
      c5e560f04204056577f2a222d056d1f5c4c533241525d cryptographic-algorithm AES_256_CMAC
  key 2193
    key-octet-string 7
      07577014195b402336345a5f260f797d7d6264044b50415755047a7976755a574d350b7e720a0202715d7
      a50530d715346205d0c2d525c001f6b5b385046365a29 cryptographic-algorithm AES_256_CMAC

switch# configure terminal
switch(config)# key-chain tunnelencrypt-psk no-show
switch(config)# show running-config rpm

!Command: show running-config rpm
!Running configuration last done at: Mon Jun 15 15:10:44 2020
!Time: Mon Jun 15 15:10:47 2020

version 9.3(5) Bios:version 05.40
key-chain tunnelencrypt-psk no-show
key chain inter tunnel-encryption
  key 3301
    key-octet-string 7 ***** cryptographic-algorithm AES_256_CMAC
key chain kcl tunnel-encryption
  key 3537

```

```

key-octet-string 7 ***** cryptographic-algorithm AES_256_CMAC
send-lifetime local 09:09:40 Apr 15 2020 duration 1800
key 2001
key-octet-string 7 ***** cryptographic-algorithm AES_256_CMAC
key 2065
key-octet-string 7 ***** cryptographic-algorithm AES_256_CMAC
key 2129
key-octet-string 7 ***** cryptographic-algorithm AES_256_CMAC
key 2193
key-octet-string 7 ***** cryptographic-algorithm AES_256_CMAC

```

CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの統計情報の表示

次のコマンドを使用して、CloudSec 統計情報を使用してセキュア VXLAN EVPN マルチサイトを表示またはクリアできます。

コマンド	目的
show tunnel-encryption statistics [peer-ip peer-ip-address]	CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの統計情報を表示します。
clear tunnel-encryption statistics [peer-ip peer-ip-address]	CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの統計情報をクリアします。

次の例は CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの統計情報の例を示します。

```

switch# show tunnel-encryption statistics
Peer 16.16.16.16 SecY Statistics:

```

```

SAK Rx Statistics for AN [0]:
Unchecked Pkts: 0
Delayed Pkts: 0
Late Pkts: 0
OK Pkts: 8170598
Invalid Pkts: 0
Not Valid Pkts: 0
Not-Using-SA Pkts: 0
Unused-SA Pkts: 0
Decrypted In-Pkts: 8170598
Decrypted In-Octets: 4137958460 bytes
Validated In-Octets: 0 bytes

```

```

SAK Rx Statistics for AN [3]:
Unchecked Pkts: 0
Delayed Pkts: 0
Late Pkts: 0
OK Pkts: 0
Invalid Pkts: 0
Not Valid Pkts: 0
Not-Using-SA Pkts: 0
Unused-SA Pkts: 0
Decrypted In-Pkts: 0

```

```
Decrypted In-Octets: 0 bytes
Validated In-Octets: 0 bytes

SAK Tx Statistics for AN [0]:
Encrypted Protected Pkts: 30868929
Too Long Pkts: 0
Untagged Pkts: 0
Encrypted Protected Out-Octets: 15758962530 bytes
```

CloudSec を使用したセキュアな VXLAN EVPN マルチサイトの設定例

次に、CloudSecを使用してセキュアVXLAN EVPNマルチサイトを設定する例を示します。

```
key chain kcl tunnel-encryption
key 2006
key-octet-string 7 075f79696a58405441412e2a577f0f077d6461003652302552040
a0b76015a504e370c7972700604755f0e22230c03254323277d2f5359741a6b5d3a5744315f2f
cryptographic-algorithm AES_256_CMAC

feature tunnel-encryption
tunnel-encryption source-interface loopback4
tunnel-encryption must-secure-policy

tunnel-encryption policy p1
  window-size 1073741823

tunnel-encryption peer-ip 11.1.11.11
  keychain kcl policy p1
tunnel-encryption peer-ip 11.2.11.11
  keychain kcl policy p1
tunnel-encryption peer-ip 44.1.44.44
  keychain kcl policy p1
tunnel-encryption peer-ip 44.2.44.44
  keychain kcl policy p1

interface Ethernet1/1
  tunnel-encryption

interface Ethernet1/7
  tunnel-encryption

interface Ethernet1/55
  tunnel-encryption

interface Ethernet1/59
  tunnel-encryption

evpn multisite border-gateway 111
dci-advertise-pip

router bgp 1000
router-id 12.12.12.12
no rd dual
address-family ipv4 unicast
  maximum-paths 10
address-family l2vpn evpn
  maximum-paths 10
```

VIP を使用するマルチサイトから PIP を使用するマルチサイトへの移行

```
vrf vxlan-900101
address-family ipv4 unicast
  maximum-paths 10
address-family ipv6 unicast
  maximum-paths 10
```

```
show tunnel-encryption session
Tunnel-Encryption Peer Policy Keychain RxStatus TxStatus
-----
11.1.11.11 p1 kc1 Secure (AN: 0) Secure (AN: 2)
11.2.11.11 p1 kc1 Secure (AN: 0) Secure (AN: 2)
44.1.44.44 p1 kc1 Secure (AN: 0) Secure (AN: 2)
44.2.44.44 p1 kc1 Secure (AN: 0) Secure (AN: 2)
```

次の例は、アウトバウンドルートマップを設定して、BGW のパスを最適なパスにする方法を示しています。この設定は、vPC BGW が BGP でピア vPC BGW の PIP アドレスを学習するときに行われます。

```
ip prefix-list pip_ip seq 5 permit 44.44.44.44/32 <<PIP2 address>>
route-map pip_ip permit 5
  match ip address prefix-list pip_ip
  set as-path prepend last-as 1
neighbor 45.10.45.10 <<R1 neighbor - Same route-map required for every DCI side underlay
BGP peer>>
  inherit peer EBGW-PEERS
  remote-as 12000
  address-family ipv4 unicast
  route-map pip_ip out
```

VIP を使用するマルチサイトから PIP を使用するマルチサイトへの移行

VIP を使用するマルチサイトから PIP を使用するマルチサイトにスムーズに移行するには、次の手順を実行します。移行は一度に 1 つのサイトで実行する必要があります。移行中のトラフィック損失は最小限に抑えることができます。

1. すべてのサイトのすべての BGW を Cisco NX-OS リリース 9.3(5) 以降のリリースにアップグレードします。
2. すべての BGW で BGP 最大パスを設定します。これは、ESI ベースの MAC マルチパスおよび BGP が EVPN タイプ 2 およびタイプ 5 ルートのすべてのネクストホップをダウンロードするために必要です。
3. 移行するサイトを 1 つずつ選択します。
4. 1 つの BGW を除き、同じサイトの BGW をシャットダウンします。NVE **shutdown** コマンドを使用して、BGW をシャットダウンできます。
5. トラフィックの損失を回避するには、アクティブな BGW で PIP を備えたマルチサイトを有効にする前に数分間待機します。これにより、同じサイトのシャットダウン BGW が EVPN ルートを取り消すことができるため、リモート BGW はアクティブ BGW だけにトラフィックを送信します。

6. **dci-advertise-pip** コマンドを設定して、アクティブな BGW で PIP を使用したマルチサイトを有効にします。

PIP 対応 BGW を備えたマルチサイトは、仮想 ESI の EVPN EAD-per-ES ルートをアドバタイズします。

PIP 対応 BGW を備えたマルチサイトは、仮想 ESI、ネクストホップを PIP アドレス、PIP インターフェイス MAC を RMAC（該当する場合）として DCI にアドバタイズします。ファブリックへの EVPN タイプ 2 およびタイプ 5 ルートのアドバタイズに関する変更はありません。

MAC ルートが ESI で受信されると、リモート BGW は ESI ベースの MAC マルチパスを実行します。

7. **dci-advertise-pip** コマンドを入力して、同じサイトの BGW を一度に 1 つずつ解除し、PIP でマルチサイトを有効にします。

ESI はすべての同じサイト BGW と同じであるため、リモート BGW は MAC ルートの ESI ベースの MAC マルチパスを実行します。

リモート BGW では、BGP はパスをマルチパスとして選択し、EVPN タイプ 5 ルートのすべてのネクストホップをダウンロードします。

既存の vPC BGW の移行

Cloudsec を使用できるように、既存の vPC BGW をスムーズに移行するには、次の手順に従います。移行は一度に 1 つのサイトで実行する必要があります。移行中のトラフィック損失は最小限に抑えることができます。

1. 両方の vPC BGW を、Cloudsec MLAG が更新された最新のイメージにアップグレードします。
2. vPC セカンダリのインターフェイス `nve1` をシャットダウンします。
3. vPC プライマリで **dci-advertise-pip** を有効にします。
4. インターフェイス `nve1` がまだ vPC セカンダリでシャットモードになっている状態で、vPC セカンダリで **dci-advertise-pip** を構成します。
5. vPC セカンダリのインターフェイス `nve1` のシャットダウンを解除します。

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。