



CHAPTER 6

サイト間 VPN サービスのモニタリング

サイト間 VPN のモニタリングでは、デバイスおよびトンネルのパフォーマンスの最も重要なすべての指標が、一目でわかるように示されます。Performance Monitor では、サイト間の問題が存在しているか、どこに問題があるかを、すぐに判断することもできます。この情報を利用して、ネットワーク管理ツールを使用して、ネットワークおよびユーザの問題を軽減したり、なくしたりすることが可能です。

サイト間 VPN では、次の間の接続が可能です。

- 組織の本社、遠隔オフィス、および支社。
- 組織のイントラネットおよび信頼できるパートナー、仕入先、顧客、または持ち株会社。

Performance Monitor は、次の場所でサイト間 VPN サービスをモニタします。

- Cisco IOS VPN ルータ。
- サポートされている 1 つ以上のサービス モジュールがインストールされた Cisco Catalyst 6500 シリーズ スイッチ。
- Cisco VPN 3000 シリーズ コンセントレータ。
- 適応型セキュリティ アプライアンス。
- PIX Security Appliances (PIX ファイアウォールとも呼ばれる)。



(注)

Performance Monitor では、ある Easy VPN サーバで、サイト間 VPN またはリモートアクセス VPN のいずれかで、サポートされているルータ、アプライアンス、ファイアウォール、およびコンセントレータが VPN ヘッドエンド デバイスのように機能することが可能であっても、すべての Easy VPN セッションが RAS VPN セッションのように示されます。「[Easy VPN について](#)」(P.5-2) を参照してください。



ヒント

サイト間 VPN サービスの一般的な問題をトラブルシューティングするには、付録のトラブルシューティングを参照してください。

ここでは、サイト間 VPN のモニタリング機能について説明します。

- 「[DMVPN について](#)」(P.6-2)
- 「[サイト間デバイスの操作](#)」(P.6-3)
- 「[サイト間デバイスの詳細の操作](#)」(P.6-6)
- 「[サイト間トンネルの操作](#)」(P.6-9)

DMVPN について

Cisco IOS ルータの Dynamic Multipoint VPN (DMVPN; ダイナミック マルチポイント VPN) 機能は、GRE トンネル、IPSec 暗号化、および Next Hop Resolution Protocol (NHRP) を組み合わせて、大規模および小規模の IPsec VPN を作成するための簡潔で拡張性のある方法を提供します。NHRP では、ハブがすべてのスポークに関するパブリック IP アドレスのデータベースを保持しています。DMVPN ネットワークのスポークは、ブートセッション中に自身のパブリック IP アドレスをハブに登録します。ソース スポークはハブ上の NHRP データベースに問い合わせ、宛先スポークのパブリック IP アドレスを取得します。マルチポイント GRE トンネル インターフェイスでは、単一の GRE トンネルが複数の IPSec トンネルをサポートできます。これにより、複雑さが軽減します。

DMVPN は、ハブツースポーク、およびスポークツースポークの 2 つのコンフィギュレーションをサポートしています。

- ハブツースポーク展開の利点には、次のものがあります。
 - ハブ アンド スポークに対して設定が簡潔で小さくなる。
 - VPN に新しいスポークを追加するためのゼロタッチ プロビジョニング。
 - 動的にアドレス指定されたスポークのサポート。
 - ハブツースポークからのマルチキャスト トラフィックのサポート。
- スポークツースポーク展開の利点には、ハブ アンド スポーク展開のすべての利点が含まれ、さらに次の利点もあります。
 - ダイナミック スポークツースポーク トンネルの方向付け。
 - 仮想フル メッシュへの、小さいスポークによる参加のサポート。

また、Performance Monitor では、第 3 のオプションとしてスポークツースポークを選択できます。スポークツースポークは、実際にはユーザが展開できる設定ではありません。Performance Monitor の便利な点は、スポークを選択し、それに関連するハブを簡単に識別できることです。

Performance Monitor では、[Tunnels] ページに DMVPN の使用が表示されます。ここでは、表示されたすべての結果は、[Select Tunnel Type] リストから選択した内容によって制約されています。「[サイト間デバイス トンネル テーブルの表示](#)」(P.6-9) を参照してください。



(注)

次のすべてを実行した場合、DMVPN スポークツースポーク トンネルに関する大量の E メールを受信する可能性があります。

- スポーク間セッションをサポートするフル メッシュ トポロジを使用するように、DMVPN を設定する。
- サイト間 VPN トンネル ダウン イベントのしきい値を設定する。
- これらのイベントの自動 E メール通知をスケジューリングする。

サイト間トンネルはダイナミックで、多数のトンネル ダウン イベントが含まれる設計により、存続期間が短くなります。この大量の E メールの問題が発生する場合は、Eメールの通知をディセーブルにするか、ハブだけをモニタするように Performance Monitor を設定することを推奨します。

DMVPN と Easy VPN の比較

次の表は、DMVPN と Easy VPN の主な違いについてまとめています。Easy VPN の詳細、および Performance Monitor で Easy VPN がどのように表示されるかについては、「[Easy VPN について](#)」(P.5-2) を参照してください。

表 6-1 DMVPN と Easy VPN の比較

サービス/機能名	DMVPN	Easy VPN
マルチキャスト トラフィックのサポート	あり。	—
スポークツースポーク通信	あり。	—
GRE/Quality of Service のサポート	あり。	—
ルーティング プロトコルのサポート	あり。	—
証明書のサポート	あり。	—
ステートフル フェールオーバー	回復用のルーティング プロトコルによって異なる。	あり。
ハブごとのスケラビリティ	ルーティング プロトコルのため、DMVPN ハブは、1 つのハブでサポートするスポークが少ない。	1 つのハブで多数のスポークをサポートする。
すべてのスポークで同一設定	—	あり。
クロスプラットフォームのサポート	—	あり。
ソフトウェアまたはハードウェア クライアントのサポート	ハードウェア クライアントのみ。	あり。
ハブへのトンネルが常時稼動	あり。	不要。

サイト間デバイスの操作

ここでは、サイト間 VPN サービスを提供する個々のデバイスおよびモジュールのステータスを、どのようにモニタするかについて説明します。

- 「[サイト間デバイスの使用とアクティビティのモニタリング](#)」 (P.6-3)
- 「[サイト間デバイス障害のモニタリング](#)」 (P.6-5)
- 「[サイト間デバイス暗号化アクティビティのモニタリング](#)」 (P.6-5)

サイト間デバイスの使用とアクティビティのモニタリング

ネットワーク内で検証済みのサイト間デバイスまたはサービス モジュールの使用、およびアクティビティ統計情報のテーブルを表示および作業できます。すべてのデバイスを表示することも、特定のグループ内のデバイスを表示することもできます。この概要を使用すると、次のことができます。

- デバイスの使用状況とアクティビティ、デバイス障害、およびデバイスの暗号化アクティビティの説明を分離します。
- サイト間 VPN サービスを提供するデバイスまたはモジュールの状態を要約したチャートおよびグラフを表示します。

サイト間デバイス テーブルを表示するには、[Monitor] > [Site-to-Site VPN] > [Devices] を選択します。このテーブルのカラムの説明については、[表 6-2](#) を参照してください。

このテーブルを使用すると、たとえば次のことができます。

■ サイト間デバイスの操作

- ユーザ定義の 1 つのデバイス グループのデバイスのみを表示するか、またはすべてのデバイスを表示する。[Select Group] リストからグループ名を選択します。リフレッシュされたページには、指定されたグループのデバイスのみが表示されます。デフォルトでは、すべてのデバイスが表示されます。モニタしているデバイスの中には、ユーザ定義のデバイス グループに属していないものがあります。
- イベント ブラウザを開いて、特定のデバイスまたはサービス モジュールに関する重大なエラー (P1 または P2) のみを表示する。デバイスの [Alert] カラムでアラート アイコンをクリックします。



(注) 重大なエラーがないデバイスまたはモジュールでは、[Alert] カラムが空になっています。

- 1 つのデバイスまたはサービス モジュールの全体の状態を要約するチャートとグラフを表示する。[Device] カラムで DNS 名または IP アドレスをクリックします。
- 1 つのデバイスまたはサービス モジュールに対するスループット グラフを表示する。[Throughput (Kbps)] カラムでハイパーリンクされているエントリをクリックします。
- 1 つのデバイスまたはサービス モジュールに対して、ドロップしたパケットのグラフを表示する。[Packet Drop %] カラムでハイパーリンクされているエントリをクリックします。

表 6-2 [Site-to-Site Devices] テーブル

エレメント	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラート アイコンが表示されます。このアイコンをクリックしてイベント ブラウザを開いて、重大なサイト間 VPN エラーのみがフィルタされた内容を表示します。「 インターフェイスのアイコンについて 」(P.3-5) を参照してください。 イベント ブラウザ要素のリファレンス情報については、「 イベント ブラウザ ウィンドウ 」(P.3-15) を参照してください。 (注) イベントをクリアした後、1 分経過するか、ページがリフレッシュされるかのいずれか早い方まで、アラート アイコンはデバイス モニタリング ページに表示され続けます。
[Device] カラム	デバイスの IP アドレスまたは DNS 名が表示されます。
[Model] カラム	シスコ デバイスのモデル名が表示されます。
[CPU Usage %] カラム	CPU の全能力に対する使用の平均パーセントが表示されます。
[Memory Usage %] カラム	前回のポーリング サイクル以降に使用したプロセッサの合計メモリ容量に対する、使用の平均パーセンテージが表示されます。
[Throughput (Bps)] カラム	前回のポーリング サイクル以降の、パブリック インターフェイスを介した受信および送信オクテットの合計 (バイト) が表示されます。
[No.Tunnels] カラム	前回のポーリング サイクル以降の、アクティブなトンネルと非アクティブなトンネルを組み合わせた数が表示されます。
[Packets In] カラム	前回のポーリング サイクル以降に、アクティブなフェーズ 1 (IKE) およびフェーズ 2 (IPSec) のトンネルを介して受信したパケット数が表示されます。
[Packets Out] カラム	前回のポーリング サイクル以降に、アクティブなフェーズ 1 (IKE) およびフェーズ 2 (IPSec) のトンネルを介して送信したパケット数が表示されます。
[Packet Drop %] カラム	前回のポーリング サイクル以降に、フェーズ 1 (IKE) トンネルおよびフェーズ 2 (IPSec) トンネルでドロップしたパケットの数を、すべての受信および送信パケットの割合 (パーセンテージ) として表示します。
[Last Updated] カラム	Performance Monitor がデバイスを最後にポーリングした日付と時間が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」 (P.3-9)
- 「テーブルの一般エレメント」 (P.3-8)

サイト間デバイス障害のモニタリング

検証済みのサイト間デバイスおよびサービス モジュールの操作における障害が記載されているテーブルを表示し、作業するには、[Monitor] > [Site-to-Site VPN] > [Devices] > [Failures] を選択します。

[Site-to-Site Failures] ページ上のすべての測定値は、デルタとして計算されます。カラムについては、表 6-3 を参照してください。

障害テーブルの 1 つのデバイスまたはサービス モジュールの全体の状態を要約するチャートとグラフを表示するには、[Device] カラムで対象の DNS 名または IP アドレスをクリックします。

表 6-3 [Site-to-Site Device Failures]

エレメント	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラートアイコンが表示されます。このアイコンをクリックしてイベント ブラウザを開いて、重大なサイト間 VPN エラーのみがフィルタされた内容を表示します。「 インターフェイスのアイコンについて 」(P.3-5) を参照してください。 イベント ブラウザ要素のリファレンス情報については、「 イベント ブラウザ ウィンドウ 」(P.3-15) を参照してください。
[Device] カラム	デバイスの DNS 名または IP アドレスが表示されます。
[Inbound Connection Failure %] カラム	受信のフェーズ 1 (IKE) およびフェーズ 2 (IPSec) の接続において、リモートで開始され、失敗したものを、すべての接続の試行 (受信および送信) の割合 (パーセンテージ) として表示します。
[Outbound Connection Failure %] カラム	送信のフェーズ 1 (IKE) およびフェーズ 2 (IPSec) の接続において、ローカルで開始され、失敗したものを、すべての送信接続の試行の割合 (パーセンテージ) として表示します。
[Replay] カラム	現在のトンネル、および前のフェーズ 2 (IPSec) トンネルのすべてにおいて (アンチリプレイ処理のために) ドロップした受信パケットの合計数が表示されます。
[Connection Failure %] カラム	すべての交換において、受信および送信の接続失敗の合計が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」 (P.3-9)
- 「テーブルの一般エレメント」 (P.3-8)

サイト間デバイス暗号化アクティビティのモニタリング

検証済みのサイト間デバイスの暗号化アクティビティに関するテーブルを表示し、作業するには、[Monitor] > [Site-to-Site VPN] > [Devices] > [Cryptos] を選択します。

[Site-to-Site Cryptos] ページには、VPN ルータおよび IPSec VPN サービス モジュールの暗号化および復号化アクティビティが示されます。[Site-to-Site Cryptos] ページ上のすべての測定値は、デルタとして計算されます。カラムについては、表 6-4 を参照してください。

暗号化アクティビティ テーブルの 1 つのデバイスまたはサービス モジュールの全体の状態を要約するチャートとグラフを表示するには、[Device] カラムで対象の DNS 名または IP アドレスをクリックします。

表 6-4 [Site-to-Site Cryptos] ページ

エレメント	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラートアイコンが表示されます。このアイコンをクリックしてイベントブラウザを開いて、重大なサイト間 VPN エラーのみがフィルタされた内容を表示します。「 インターフェイスのアイコンについて 」(P.3-5) を参照してください。 イベント ブラウザ要素のリファレンス情報については、「 イベントブラウザ ウィンドウ 」(P.3-15) を参照してください。
[Device] カラム	デバイスの DNS 名または IP アドレスが表示されます。
[Packet In] カラム	すべての SEP カードでの、受信パケットの集約数が表示されます。
[Packet Out] カラム	すべての SEP カードでの、送信パケットの集約数が表示されます。
[Packet Drop %] カラム	現在および以前のアクティブなフェーズ 1 (IKE) およびフェーズ 2 (IPSec) のトンネルでの、最終的に失敗した送信の暗号化の合計数の計算結果が表示されます。
[Encrypt Failure %] カラム	アクティブなフェーズ 2 (IPSec) の全トンネルで、最終的に失敗した送信の暗号化の割合 (パーセンテージ) が表示されます。
[Decrypt Failure %] カラム	アクティブなフェーズ 2 (IPSec) の全トンネルで、最終的に失敗した受信の復号化の割合 (パーセンテージ) が表示されます。

関連トピック

- 「[Performance Monitor テーブルのオプション タスク](#)」(P.3-9)
- 「[テーブルの一般エレメント](#)」(P.3-8)

サイト間デバイスの詳細の操作

Performance Monitor では、必要なサイト間 VPN のデバイス情報の詳細を表示および作業できます。追加情報については、次のトピックを参照してください。

- 「[サイト間デバイスの詳細グラフの表示と意味](#)」(P.6-6)
- 「[サイト間デバイス インターフェイス テーブルの表示](#)」(P.6-8)
- 「[サイト間デバイス トンネル テーブルの表示](#)」(P.6-9)

サイト間デバイスの詳細グラフの表示と意味

サイト間 VPN で、検証済みデバイスのステータスのグラフィカルな表示を示すことができます。

手順

ステップ 1 [Monitor] > [Site-to-Site VPN] > [Device Details] を選択します。

Performance Monitor では最初に、IP アドレスとして最小の数値を使用しているデバイスのヘルスとパフォーマンスを表すグラフが表示されます。グラフの説明については、[表 6-5](#) を参照してください。



- (注) 2つの縦 (Y) 軸を使用するグラフを解釈するときに、既知の問題が発生することがあります。最初の Y 軸は常にゼロで始まるのに対し、2番目の Y 軸は、指定された時間範囲の最も低い値がゼロよりも大きい場合でも、その値で始まります。そのため、2つの Y 軸を直接比較できないことがあります。

ステップ 2 [Select Device] リストから、グラフを表示するデバイスを選択します。

サイト間グラフの種類

表 6-5 サイト間デバイス グラフの種類

グラフの種類	説明
[CPU Usage]	<p>使用されているデバイスの CPU 能力の割合 (パーセンテージ) を示します。</p> <ul style="list-style-type: none"> 縦軸は、特定のポーリング サイクル内で使用されている CPU 能力の平均 (パーセンテージ) を示します。 横軸は、ポーリング サイクルの時刻を示します。
[Memory Usage]	<p>使用されているデバイスのメモリ容量の割合 (パーセンテージ) を示します。</p> <ul style="list-style-type: none"> 縦軸は、特定のポーリング サイクル内で使用されているメモリ容量の平均 (パーセンテージ) を示します。 横軸は、ポーリング サイクルの時刻を示します。
[Packet Drops]	<p>サイト間 VPN トンネルでドロップしたパケットの割合 (パーセンテージ) を示します。</p> <ul style="list-style-type: none"> 縦軸は、特定のポーリング サイクル内でドロップしたパケットの平均 (パーセンテージ) を示します。 横軸は、ポーリング サイクルの時刻を示します。
[Throughput vs. No. Tunnels]	<p>長期間のスループットの傾向を使用中のトンネル数の傾向と比較するうえで有用な折れ線グラフが表示されます。</p> <ul style="list-style-type: none"> 2種類の情報を表示するため、2つの縦軸を使用します。 <ul style="list-style-type: none"> 左の (オレンジの) 縦軸は、特定のポーリング サイクル内の平均スループットを 1 秒あたりのバイト単位で表します。 右の (青色の) 縦軸は、特定のポーリング サイクル内の平均トンネル数を表します。 横軸は、Performance Monitor がそれぞれの縦軸のトレンドを計算した時刻を示します。
[Inbound Connection Failures]	<p>長期にわたる受信接続失敗のトレンドを示します。</p> <ul style="list-style-type: none"> 縦軸は、特定のポーリング サイクル内での失敗の平均数を表します。 横軸は、ポーリング サイクルの時刻を示します。
[Outbound Connection Failures]	<p>長期にわたる送信接続失敗のトレンドを示します。</p> <ul style="list-style-type: none"> 縦軸は、特定のポーリング サイクル内での失敗の平均数を表します。 横軸は、ポーリング サイクルの時刻を示します。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」 (P.3-9)
- 「テーブルの一般エレメント」 (P.3-8)

サイト間デバイス インターフェイス テーブルの表示

サイト間デバイス インターフェイスのパフォーマンスおよびアクティビティ統計情報のテーブルを、表示および作業できます。

手順

ステップ 1 [Monitor] > [Site-to-Site VPN] > [Device Details] > [Interfaces] を選択します。テーブルのカラムの説明については、表 6-6 を参照してください。

[Site-to-Site Interfaces] ページには、クリプト マップにバインドされている、または Internet Assigned Number Authority (IANA) インターフェイス タイプ 131 (トンネル) の一部になっているデバイス インターフェイスが示されます。

[Site-to-Site Interfaces] ページ上のすべての測定値は、デルタとして計算されます。

ステップ 2 [Select Device] リストから、表示するデバイスを選択します。

デフォルトでは、VPN インターフェイスのみがテーブルにリストされています。ただし、[Select Interfaces] リストから [All Interfaces] を選択して、デバイスに関するすべてのインターフェイスを表示することができます。

参考

表 6-6 [Site-to-Site Interfaces] ページ

エレメント	説明
[Descr] カラム	物理インターフェイスの特別な説明が示されます。例：DEC 21143A PCI Fast Ethernet。
[Address] カラム	インターフェイスの MAC アドレスが表示されます。
[Admin Status] カラム	[Up] または [Down] のいずれかが表示されます。
[Operation Status] カラム	[Up] または [Down] のいずれかが表示されます。
[Type] カラム	TCP/IP がバインドされているフレーム タイプが表示されます。たとえば、表示されたタイプ iso88023-csmacd は、Carrier Sense Multiple Access/Collision Detection (CSMA/CD; 搬送波感知多重アクセス/衝突検出) に適用される、100 MBits/s ファーストイーサネットのフレームタイプを示します。
[Speed (Kbps)] カラム	インターフェイスの速度 (Kbps) が表示されます。
[Packet In] カラム	前回のポーリング サイクル以降に、インターフェイス上で受信したパケットの合計数が表示されます。
[Packet Out] カラム	前回のポーリング サイクル以降に、インターフェイス上で送信したパケットの合計数が表示されます。
[Packet Drop %] カラム	前回のポーリング サイクル以降にドロップしたパケットの合計割合 (パーセンテージ) が表示されます。
[Throughput (Bps)] カラム	インターフェイスの平均スループット率 (バイト) が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」 (P.3-9)
- 「テーブルの一般エレメント」 (P.3-8)

サイト間トンネルの操作

ここでは、サイト間 VPN でのトンネルの操作方法について説明します。

- 「[サイト間デバイス トンネル テーブルの表示](#)」 (P.6-9)
- 「[サイト間 VPN トンネルの検索](#)」 (P.6-10)

サイト間デバイス トンネル テーブルの表示

検証済みのすべてのサイト間デバイスで、VPN トンネルのテーブルを表示し、それを使用して作業することも、1 つのデバイスについてトンネルを表示することもできます。

トンネルのリストを表示するには、[Monitor] > [Site-to-Site VPN] > [Device Details] > [Tunnels] を選択します。

デフォルトでは、[Tunnels] ページに、検証済みのすべてのサイト間デバイスのトンネルが表示されます。表示される値は、トンネルの開始以降に計算された整数です。

上記のテーブルのドロップダウン リストを使用してリストをフィルタできます。

- [Select Device]: デバイスの IP アドレスを選択して、そのデバイスの VPN トンネルに関する情報を表示します。
- [Select Tunnel Type]: 表示する DMVPN トンネルのタイプを選択するか、またはすべてのサイト間トンネルを表示するか、またはデバイスがどのハブを使用しているかを調べます。
 - [All]: 選択したデバイスに対するすべての DMVPN トンネルが表示されます。
 - [DMVPN Hub-Spoke]: 選択したデバイスに対する、ハブツースポークの DMVPN トンネルだけが表示されます。
 - [DMVPN Spoke-Hub]: このオプションでは、Performance Monitor で、どのハブが、[Select device] リストで選択したスポークに関連付けられているかを簡単に識別できて便利です。
 - [DMVPN Spoke-Spoke]: スポークツースポークの DMVPN トンネルだけが表示されます。これらのトンネルは動的で、多数のトンネルアップ イベントおよびトンネルダウン イベントを生成するライフタイムが非常に短いことがあります。

次の表に、トンネル テーブルのカラムを示します。

表 6-7 [Tunnels] ページ

エレメント	説明
[Local Endpoint] カラム	<p>トンネルが終了したローカル エンドポイント デバイスのインターフェイスの IP アドレスが表示されます。</p> <p>DMVPN トンネルの場合は、ハイパーリンクされている IP アドレスをクリックして、リモート IP アドレス、およびトンネルの期限が切れる予定の時刻を表示できます。</p> <p>(注) Performance Monitor の内部で、「ローカル」エンドポイント デバイスの ID が変化することがあります。これは、このようなデバイスの ID は常に、モニタしているデバイスに対して相対的に定義されるからです。</p>
[Remote Endpoint] カラム	<p>トンネルが終了したリモート エンドポイント デバイスのインターフェイスの IP アドレスが表示されます。</p> <p>(注) Performance Monitor の内部で、「リモート」エンドポイント デバイスの ID が変化することがあります。これは、このようなデバイスの ID は常に、モニタしているデバイスに対して相対的に定義されるからです。</p>

表 6-7 [Tunnels] ページ (続き)

エレメント	説明
[Local Subnet] カラム	次の 3 つのカラムの値は全体として、1 つのトンネルのアクセス リストを定義しています。
[Remote Subnet] カラム	<ul style="list-style-type: none"> • [Local Subnet] : ローカル エンドポイント デバイス上のトンネル サブネットおよびマスクが表示されます。 • [Remote Subnet] : リモート エンドポイント デバイス上のトンネル サブネットおよびマスクが表示されます。 • [Protocol] : トンネル プロトコルおよび使用したポート (TCP 80 など) が表示されます。
[Protocol] カラム	
[Status] カラム	
[Active Time] カラム	トンネルのライフタイムを時間、分、および秒単位で表示します。
[Auth Fail In] カラム	トンネルの開始以降の、受信パケットに対する認証失敗の数が表示されます。
[Auth Fail Out] カラム	トンネルの開始以降の、送信パケットに対する認証失敗の数が表示されます。
[Packets In] カラム	トンネル開始以降の受信パケットの数が表示されます。
[Packets Out] カラム	トンネル開始以降の送信パケットの数が表示されます。
[Packet Drop %] カラム	ドロップしたパケットが、トンネル開始以降の、受信および送信パケットのすべての割合 (パーセンテージ) として表示されます。
[Throughput (Bps)] カラム	トンネルの開始以降の、トンネルを介した受信および送信オクテットの合計 (バイト) が表示されます。
[Last Update] カラム	Performance Monitor がデバイスを最後にポーリングした日付と時間が表示されます。

関連トピック

- 「[Performance Monitor テーブルのオプション タスク](#)」 (P.3-9)
- 「[テーブルの一般エレメント](#)」 (P.3-8)

サイト間 VPN トンネルの検索

単一のトンネルを検索および分離し、プロパティを表示することができます。

手順

- ステップ 1** [Monitor] > [Site-to-Site VPN] > [Tunnel Lookup] を選択します。
[Site-to-Site Tunnel Lookup] ページが表示されます。
- ステップ 2** 1 つのトンネルを識別するには、次の値を入力します。
 - トンネルが終了した一方の終端の、エンドポイント デバイスのインターフェイスの IP アドレス。
 - 同じトンネルが終了した反対の終端の、エンドポイント デバイスのインターフェイスの IP アドレス。
- ステップ 3** [Go] をクリックします。トンネルが見つかると、そのトンネルの詳細がページに表示されます。カラムについては、「[サイト間デバイス トンネル テーブルの表示](#)」 (P.6-9) を参照してください。

関連トピック

- 「[Performance Monitor テーブルのオプション タスク](#)」 (P.3-9)
- 「[テーブルの一般エレメント](#)」 (P.3-8)

