CHAPTER 5

リモート アクセス VPN サービスのモニタリング

Remote Access Service（RAS; リモート アクセス サービス）VPN は、モバイル ユーザや在宅勤務者などのリモート ユーザへの接続の安全性を保護します。RAS VPN のモニタリングは、クラスタ、コンセントレータ、およびユーザ セッション パフォーマンスの最も重要なすべての指標を、ひと目でわかるように提示します。

Performance Monitor により、RAS VPN の問題が存在しているか、どこに問題があるかを、すばやく判断することができます。この情報を利用し、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。

オプションとして、一度に 1 人の RAS ユーザをログアウトできます。

ヒント RAS 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、RAS VPN のモニタリング機能について説明します。

RAS 仮想クラスタについて

（注）

- Performance Monitor およびマニュアルにおける *ロード バランシング サービス*は、コンテンツ スイッチング サービス モジュールの Web サーバ ロードバランシング機能だけを表しています。Performance Monitor は、仮想クラスタ内で組み合わせたコンセントレータまたはアプリケーションのロード バランシングはモニタしません。
- PIX OS および Easy VPN は RAS VPN の使用をサポートしていますが、これらの 2 つのテクノロジーは、両方とも仮想クラスタの使用をサポートしていません。

RAS VPN では、リモート ユーザが、ダイヤルアップ、ISDN、DSL、ケーブル、その他のテクノロジーによって接続し、共有しているパブリック インフラストラクチャを介してプライベート ネットワークに参加することができます。

Performance Monitor は、複数の種類の異なるデバイスで生じた RAS VPN サービスをモニタしますが、Cisco VPN 3000 シリーズ コンセントレータおよび ASA 5520 または 5550 アプライアンスに対しては特別な考慮が必要です。これらのものはロードバランシングに対して単独で、または*仮想クラスタ*内で組み合わせてモニタすることが可能なためです。仮想クラスタでは、コンセントレータのコレクション、またはアプライアンスのコレクションを 1 つのエンティティとして機能させることができます。

クラスタは、1 つの IP アドレスによって外部のクライアント スペースに認識されます。仮想 IP アドレスはルーティング可能なアドレス、つまり他のデバイスがパケットを送信できる有効なアドレスにする必要があります。そうしないと、受信パケットがクラスタに到達できません。

この仮想 IP アドレスは、VPN クラスタ内の特定のデバイスには関連付けられません。これは、*仮想クラスタ マスター*によってサービスされます。仮想クラスタ マスタ コンセントレータは、特定のクラスタ内のすべてのセカンダリ コンセントレータまたはアプライアンスからのロード情報を保持しています。各セカンダリ コンセントレータは、KeepAlive 負荷情報をマスターに送信します。

- VPN 3000 シリーズには、6 つの異なったコンセントレータ モデルがあります。これらのモデルの使用および機能については、http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/index.html を参照してください。モニタしているコンセントレータが正常に機能しているかどうかを判断するうえで役に立ちます。
- ASA 5520 および 5550 アプライアンスの使用および機能については、http://www.cisco.com/en/US/products/ps6120/index.html を参照してください。

Easy VPN について

Cisco Easy VPN は、いくつかの種類のシスコ デバイスに対するソフトウェアの機能で、リモート オフィスおよびテレワーカーに対する VPN の展開を簡潔にするものです。Easy VPN では、多数のデバイスにおける VPN 管理が一元化されるため、VPN 展開の複雑さが軽減します。Easy VPN の実装では、サポートされているデバイス内で Cisco Easy VPN Server と Cisco Easy VPN Remote 機能の両方を使用する必要があります。

Easy VPN を使用すると、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はリモート VPN クライアントのように機能します。したがって、これらのデバイスは Easy VPN サーバからセキュリティ ポリシーを受け取ることが可能になり、これにより組織内の遠隔地における VPN 構成の要件が最小になります。

また、Cisco Easy VPN Server に対応しているデバイスは、自身の PC 上で Cisco VPN クライアント ソフトウェアを実行しているモバイル リモート ワーカーによって開始された VPN トンネルを終了することができます。

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 の詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/secursw/ps5299/index.html

（注）

- Easy VPN は RAS クラスタの使用をサポートしていません。
- Performance Monitor は Easy VPN セッションのユーザ名を表示しません。また、ユーザ名を特別な Easy VPN セッションに関連付けません。
- Performance Monitor の User Session Report 機能は、Easy VPN をサポートしていません。

RAS クラスタ テーブルの操作

Performance Monitor では、すべてのリモート アクセス クラスタの概要を表示できます。この概要を使用して、ユーザ データとコンセントレータ データを分離し、有効なクラスタ統計情報のサブセットを表示します。

ヒント　Performance Monitor は、1 日に 1 回、クラスタ メンバシップのレコードを自動的に更新します。クラスタ内で VPN コンセントレータを追加または削除した場合、またはクラスタ間でコンセントレータを移動した場合は、[Devices] > [Importing Devices] を選択し、[Revalidate] をクリックする必要があります。このようにしないと、次の自動更新まで、対象のクラスタについて誤った情報が表示されます。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Clusters] を選択します。テーブルのカラムの説明については、表 5-1 を参照してください。

Performance Monitor は、VPN コンセントレータのヘルスとパフォーマンスの測定値を平均して、ネットワーク内のクラスタについて表示する概要レベルの統計情報を作成します。

ステップ 2　次のいずれかを実行して、リストを調整したり、さらに詳細な情報を取得することができます。

- リスト内でデバイスを見つけるには、[Find Device] フィールドでデバイスの IP アドレスまたは DNS 名を入力し、[Find] をクリックします。デバイスが見つかると、[Remote Access Device Graphs] ページに、指定されたコンセントレータの情報が表示されます。グラフの種類については、「RAS デバイスの詳細グラフの表示」（P.5-5）を参照してください。
- RAS クラスタのドロップしたパケットのグラフを表示するには、[Packet Drop %] カラムの対象エントリをクリックします。
- RAS クラスタのスループット グラフを表示するには、[Throughput (kbps)] カラムの対象エントリをクリックします。
- RAS クラスタの帯域幅使用率のグラフを表示するには、[Bandwidth Usage %] カラムの対象エントリをクリックします。

参考

表 5-1　[Remote Access Clusters] ページ

エレメント	説明
[Cluster] カラム	仮想クラスタ マスターの DNS 名が表示されます。
[Devices] カラム	クラスタ内のデバイスの合計数が表示されます。

表 5-1　[Remote Access Clusters] ページ（続き）

エレメント	説明
[Master Device] カラム	指定したクラスタ上のマスター デバイスの IP アドレスが表示されます。 仮想クラスタ マスター コンセントレータは、クラスタ内のすべてのセカンダリ コンセントレータのロード情報を保持しています。各セカンダリは、KeepAlive メッセージ交換のロード情報をマスターへ送信します。
[# of Users] カラム	すべての RAS デバイス上のアクティブ セッションについて、集約した合計数が表示されます。 （注）　いずれかのユーザが RAS ユーザからログアウトすると、次に表示がリフレッシュしたときに、この値が異なる場合があります。
[Load Variance] カラム	最も高負荷のデバイスと、最も低負荷のデバイス間の差異を測定して計算されたスキューを示します。 デバイスの負荷は、現在のアクティブなセッションの数を、設定した最大許容接続数で除算した割合（パーセンテージ）として計算されます。
[Packet Drop %] カラム	IPSec 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計算結果を、すべての RAS デバイス上の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。 新しいブラウザを開いて、グラフとして選択した内容を表示するには、[Packets 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。
[Throughput (kbps)] カラム	すべての RAS デバイス上のパブリック インターフェイス間の送信および受信オクテットの合計が表示されます。 新しいブラウザを開いてグラフとして選択した内容を表示するには、[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。
[Bandwidth Usage %] カラム	すべての RAS デバイスで使用されている帯域幅を、すべての RAS デバイスで使用できる帯域幅で除算した平均（パーセンテージ）が表示されます。 新しいブラウザを開いてグラフとして選択した内容を表示するには、[Bandwidth Usage %] 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。
[Inbound Connection Failure %] カラム	すべての受信接続の試行において、受信のフェーズ 1（IKE）およびフェーズ 2（IPSec）接続の中で、リモートで開始されて失敗したものの平均（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）

RAS デバイスの操作

検証済みの VPN コンセントレータのステータスを説明している情報を分離してモニタする方法については、次のトピックを参照してください。

- 「RAS デバイスの詳細グラフの表示」（P.5-5）
- 「RAS デバイスの使用状況とアクティビティのモニタリング」（P.5-6）
- 「RAS デバイス障害のモニタリング」（P.5-8）
- 「RAS デバイスの暗号化アクティビティのモニタリング」（P.5-9）

- 「RAS デバイスの暗号化アクセラレータ カード データの表示」（P.5-10）
- 「リモート アクセス インターフェイス テーブルの表示」（P.5-11）

RAS デバイスの詳細グラフの表示

ネットワーク内で検証済みの VPN 3000 シリーズ コンセントレータの情報を分離し、そのヘルスとパフォーマンスを示す詳細グラフを表示することができます。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Device Details] を選択します。

デフォルトでは、[Remote Access Device Graphs] ページに、IP アドレスとして最も小さい数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 5-2 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。

RAS グラフの種類

表 5-2　RAS グラフの種類

グラフの種類	説明
[Bandwidth Utilization]	パブリック インターフェイスで使用されているデバイスの帯域幅容量の割合（パーセンテージ）を示します。 • 縦軸は、特定のポーリング サイクル内で使用されている帯域幅容量の平均（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。
[CPU Usage]	使用されたデバイスの CPU 能力の割合を示します。 • 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。
[Inbound Connect Failures]	長期にわたる受信接続失敗のトレンドを示します。 • 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。

表 5-2　RAS グラフの種類（続き）

グラフの種類	説明
[Throughput vs. Session]	一定期間のスループットの傾向を VPN セッション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。 • 2 種類の情報を表示するため、2 つの縦軸を使用します。 – 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バイト単位で示します。 – 右の（青色の）縦軸は、特定のポーリング サイクル内の平均セッション数を示します。 • 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。
[IKE Phase 1 Connection Failures]	フェーズ 1（IKE）接続で失敗した割合（パーセンテージ）を示します。 • 縦軸は、特定のポーリング サイクル内で失敗した接続の平均（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。
[IPSec Phase 2 Connection Failures]	フェーズ 2（IPSec）接続で失敗した割合（パーセンテージ）を示します。 • 縦軸は、特定のポーリング サイクル内で失敗した接続の平均（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。

RAS デバイスの使用状況とアクティビティのモニタリング

Performance Monitor では、ネットワーク内のクラスタで RAS VPN サービスを提供している検証済みのすべての Cisco VPN 3000 シリーズ コンセントレータについて、概要を参照できます。この概要を使用すると、次のことができます。

- VPN コンセントレータの使用およびアクティビティ、コンセントレータの障害、およびコンセントレータの暗号化アクティビティを表しているデータを分離します。
- VPN コンセントレータの状態を要約しているテーブルおよびグラフを表示します。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Devices] を選択します。テーブルのカラムの説明については、表 5-3 を参照してください。

[Remote Access Devices] ページに、コンセントレータの使用およびアクティビティの統計情報のテーブルが表示されます。この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（あるポーリング サイクルから次のサイクルまでの差の範囲を示します）。ただし、現在のユーザ数は整数です。

（注）　いずれかのユーザが RAS ユーザからログアウトすると、次に表示がリフレッシュされたときに、現在のユーザ数の整数値が異なる場合があります。

ステップ 2　次のいずれかを実行して、リストを調整したり、さらに詳細な情報を取得することができます。

- 特定のクラスタ内でこれらのデバイスだけをリストに表示するには、[Select Cluster] リストでクラスタを選択します。Easy VPN は、RAS クラスタの使用をサポートしていないことに注意してください。
- 特定のコンセントレータについて詳細グラフを表示するには、[Device] カラムで IP アドレスまたは DNS 名をクリックします。

- コンセントレータのドロップしたパケットのグラフを表示するには、[Packet Drop %] カラムの対象エントリをクリックします。
- コンセントレータのスループット グラフを表示するには、[Throughput (kbps)] カラムの対象エントリをクリックします。
- コンセントレータの帯域幅使用のグラフを表示するには、[Bandwidth Usage %] カラムの対象エントリをクリックします。

参考

表 5-3　[Remote Access Devices]

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。アイコンをクリックすると、イベント ブラウザが開き、重大な RAS エラーだけが表示されるようにフィルタ処理された画面が表示されます。「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。 新しいブラウザを開いて、グラフとして選択した内容を表示するには、[Device] 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。
[Cluster] カラム	仮想クラスタ マスターの 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と番号が表示されます。
[# Of Users] カラム	アクティブ セッションの数が表示されます。 **（注）** いずれかのユーザが RAS ユーザからログアウトすると、次に表示がリフレッシュしたときに、この値が異なる場合があります。
[Packet Drop %] カラム	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計算結果を、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。 新しいブラウザを開いて、グラフとして選択した内容を表示するには、[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。
[Packets In] カラム	受信パケットの数が表示されます。
[Packets Out] カラム	送信パケットの数が表示されます。
[Throughput (kbps)] カラム	指定した RAS デバイス上のパブリック インターフェイスを介した送信および受信の合計オクテットが表示されます。 新しいブラウザを開いて、グラフとして選択した内容を表示するには、[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。
[Bandwidth Usage %] カラム	指定した RAS デバイスで使用されている帯域幅を、そのデバイスで使用できる帯域幅で除算した割合（パーセンテージ）が表示されます。 新しいブラウザを開いて、グラフとして選択した内容を表示するには、[Bandwidth Usage] 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。
[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）

RAS デバイス障害のモニタリング

検証済みの VPN コンセントレータの操作における障害が記載されているテーブルを表示および操作できます。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Devices] > [Failures] を選択します。テーブルのカラムの説明については、表 5-4 を参照してください。

[Remote Access 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。

ステップ 2　リストを絞り込んで、より詳細な情報を表示することができます。

- 特定のクラスタ内でこれらのデバイスだけをリストに表示するには、[Select Cluster] リストでクラスタを選択します。Easy VPN は、RAS クラスタの使用をサポートしていないことに注意してください。
- 特定の VPN コンセントレータについて詳細な統計情報を表示するには、[Device] カラムで IP アドレスまたは DNS 名をクリックします。「RAS デバイスの操作」（P.5-4）を参照してください。

参考

表 5-4　[Remote Access 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。アイコンをクリックすると、イベント ブラウザが開き、重大な RAS エラーだけが表示されるようにフィルタ処理された画面が表示されます。「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。 選択したデバイスのパフォーマンスのサマリー グラフを表示するには、[Device] カラムでいずれかのエントリをクリックします。
[Inbound Connect Failure %] カラム	リモートで開始され、フェーズ 1（IKE）またはフェーズ 2（IPSec）で失敗したすべての受信接続試行の割合（パーセンテージ）が表示されます。
[IKE Phase 1 Failure %] カラム	ローカルに開始され、有効化することに失敗したフェーズ 1（IKE）トンネルの割合（パーセンテージ）が表示されます。
[IPSec Phase 2 Failure %] カラム	フェーズ 2（IPSec）で受け取った交換で、無効なために拒否された割合（パーセンテージ）が表示されます。
[Replays] 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。

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）

RAS デバイスの暗号化アクティビティのモニタリング

検証済みの VPN コンセントレータについて、暗号化アクティビティ データの概要テーブルを表示および操作できます。

（注）　表示される結果には、VPN 3005 コンセントレータまたは VPN 3015 コンセントレータは含まれていません。これらのデバイスは、Scalable Encryption Processor（SEP）カードの代わりにソフトウェアの暗号化を使用します。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Devices] > [Cryptos] を選択します。テーブルのカラムの説明については、表 5-5 を参照してください。

[Remote Access Cryptos] ページ上のすべての測定値は、SEP カード数の整数値を除いて、デルタとして計算されます。

ステップ 2　リストを絞り込んで、より詳細な情報を表示することができます。

- 特定のクラスタ内でこれらのデバイスだけをリストに表示するには、[Select Cluster] リストでクラスタを選択します。Easy VPN は、RAS クラスタの使用をサポートしていないことに注意してください。
- 特定の VPN コンセントレータについて詳細な統計情報を表示するには、[Device] カラムで IP アドレスまたは DNS 名をクリックします。「RAS デバイスの操作」（P.5-4）を参照してください。

参考

表 5-5　[Remote Access Device Cryptos]

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。アイコンをクリックすると、イベント ブラウザが開き、重大な RAS エラーだけが表示されるようにフィルタ処理された画面が表示されます。「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 IP アドレスまたは DNS 名が表示されます。 選択したデバイスのパフォーマンス グラフを表示するには、[Device] カラムでいずれかのエントリをクリックします。
[No.Cards] カラム	モニタ対象のデバイスにインストールされている SEP カードの合計数が表示されます。
[Encryption Failure %] カラム	すべての SEP カードにおいて、現在アクティブなフェーズ 2（IPSec）の全トンネルで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。

表 5-5　[Remote Access Device Cryptos]（続き）

エレメント	説明
[Decryption Failure %] カラム	すべての SEP カードにおいて、現在アクティブなフェーズ 2（IPSec）の全トンネルで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。
[Packet Drop %] カラム	すべての SEP カードにおいて、フェーズ 1（IKE）およびフェーズ 2（IPSec）の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）が表示されます。
[Encrypted Packets] カラム	すべての SEP カードにおいて、暗号化された送信パケットの集約数が表示されます。
[Decrypted Packets] カラム	すべての SEP カードにおいて、復号化された受信パケットの集約数が表示されます。
[Throughput (Kbps)] カラム	すべての SEP カードにおいて、送信（暗号化）および受信（復号化）されたオクテットの集約数（Kbps）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）

RAS デバイスの暗号化アクセラレータ カード データの表示

検証済みの VPN コンセントレータについて、暗号化アクセラレータ カード データのテーブルを表示および操作できます。

（注）　表示される結果には、VPN 3005 コンセントレータまたは VPN 3015 コンセントレータは含まれていません。これらのデバイスは、SEP カードの代わりにソフトウェアの暗号化を使用します。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Device Details] > [Crypto Status] を選択します。テーブルのカラムの説明については、表 5-6 を参照してください。

[Remote Access 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。

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。

参考

表 5-6　[Remote Access Cryptos]

エレメント	説明
[Slot] カラム	SEP カードがインストールされている VPN コンセントレータ内のスロットの数を識別します。
[Status] カラム	SEP カードの機能状態を表すメッセージが表示されます。
[Packets In] カラム	SEP カードの復号化された受信パケットの数が表示されます。
[Packets Out] カラム	SEP カードの暗号化された送信パケットの数が表示されます。

表 5-6　[Remote Access Cryptos]（続き）

エレメント	説明
[Packet Drop %] カラム	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、復号化された受信パケットおよび暗号化された送信パケットの割合（パーセンテージ）として表示します。
[Throughput (Kbps)] カラム	SEP カードにおいて、一定期間に暗号化された送信オクテットおよび復号化された受信オクテットの合計数が表示されます。

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）

リモート アクセス インターフェイス テーブルの表示

検証済みの VPN コンセントレータについて、インターフェイス ステータス データのテーブルを表示および操作できます。

手順

ステップ 1　[Monitor] > [Remote Access 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 5-7 を参照してください。

[Remote Access Interfaces] ページには、*パブリック インターフェイス*および*プライベート インターフェイス*の情報が表示されます。パブリック（外部）インターフェイスは、パブリック IP アドレスを使用して、外部ネットワークに接続します。プライベート（内部）インターフェイスは、プライベート IP アドレスを使用し、外部ネットワークからは見えません。

[Remote Access 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。

参考

表 5-7　[Remote Access Interfaces] ページ

エレメント	説明
[Description] カラム	物理インターフェイスの具体的な説明（DEC 21143A PCI Fast Ethernet など）が示されます。
[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。
[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（CSMACD; 搬送波感知多重アクセス/衝突検出）に適用される、100 Mb/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。
[Access] カラム	[Public] または [Private] のいずれかが表示されます。
[Admin Status] カラム	[Up] または [Down] が表示されます。
[Oper Status] カラム	[Up] または [Down] が表示されます。
[Speed (Kbps)] カラム	インターフェイスの速度（Kbps）が表示されます。

表 5-7　[Remote Access Interfaces] ページ（続き）

エレメント	説明
[Packets In] カラム	前回のポーリング サイクル以降の受信パケットの合計数が表示されます。
[Packets Out] カラム	前回のポーリング サイクル以降の送信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割合（パーセンテージ）が表示されます。
[Throughput (Kbps)] カラム	インターフェイスにおいて、一定期間に暗号化された送信オクテットおよび復号化された受信オクテットの合計数が表示されます。

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）

RAS ユーザの操作

ここでは、RAS ユーザをモニタする次の機能について説明します。

- 「RAS ユーザの詳細の表示」（P.5-12）
- 「RAS デバイスの上位 10 ユーザの識別」（P.5-13）
- 「RAS クラスタの上位 10 ユーザの識別」（P.5-15）

RAS ユーザの詳細の表示

現在の 1 人の RAS VPN ユーザに関して、最新の詳しい接続情報を分離および表示できます。オプションで、検索したユーザをログアウトすることができます。

（注） 対象の RAS VPN コンセントレータに多数のアクティブ セッションがある場合、ユーザ セッションの検索時間が 1 分を超えることがあります。

ヒント 次の内容について、レポートを表示することもできます。

- 選択した傾向タイプに従った、指定した期間における RAS VPN ユーザの上位 10 人のランク。「RAS VPN の上位 10 ユーザ レポートの表示」（P.10-8）を参照してください。
- 指定した期間における、1 人以上の RAS VPN ユーザの VPN セッションの説明。「RAS VPN ユーザ セッション レポートの表示」（P.10-9）を参照してください。

始める前に

ユーザのログアウト機能は、次の場合だけ有効です。

- 自分の CiscoWorks ユーザ ロールが System Administrator または Network Administrator の場合。「ユーザの権限について」（P.3-2）を参照してください。

- 対象の VPN コンセントレータで VPN 3000 Concentrator Series Manager がイネーブルになっており、Performance Monitor が対象のコンセントレータについて、正しい認証クレデンシャルのレコードを持っている場合。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [User Lookup] を選択します。

ステップ 2　次のユーザの詳細情報を入力します。

- [Find User]：ユーザの IP アドレスまたはユーザ名を入力します。
- [Search In]：必要な場合は、1 つのデバイスまたは 1 つのクラスタのいずれかに制限して検索し、その名前または IP アドレスを選択することで検索の対象を特定できます。特定のデバイスまたはクラスタに関する検索を制限しない場合は、[Devices All] を選択します。

ステップ 3　[Go] をクリックします。ユーザが見つかった場合は、次のユーザ セッションの詳細が表示されます。

- [User Name]：ユーザのログイン名。
- [Group Name]：ユーザが属しているユーザ グループ。
- [Cluster Name]：VPN コンセントレータがクラスタ メンバの場合、名前または IP アドレスによってクラスタを識別します。
- [Device Name]：名前または IP アドレスによって VPN コンセントレータを識別します。
- [Client IP Address]：ユーザの IP アドレス。
- [Protocol]：ユーザの接続プロトコル（IPSec over UDP など）。
- [Throughput (Kbps)]：ユーザの平均スループット / 秒。
- [Connection Duration]：日、時間、分、および秒で測定されます。
- [Octet In]：トンネルの開始以降の受信オクテットの合計数。
- [Octet Out]：トンネルの開始以降の送信オクテットの合計数。

ステップ 4　（任意）ユーザ セッションを終了するには、[Logout] をクリックします。

ログアウトが正常に終了すると、指定したユーザがログアウトされ、そのユーザの IP アドレスは、アクティブな RAS セッションを表すテーブルに表示されなくなります。「The user <username> was logged out successfully」というシステム メッセ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）

RAS デバイスの上位 10 ユーザの識別

Performance Monitor は、検証済みのすべての VPN コンセントレータに接続した、または 1 つのクラスタ内で検証済みのコンセントレータに接続されている上位 10 人のユーザをランキングすることができます。ランキングの値はスループット、接続期間、または 1 ユーザあたりのトラフィック数によって判断されます。

（注）　Performance Monitor は、各 VPN コンセントレータの上位 10 人のユーザをランキングします。次に、全体の上位 10 人のユーザを算出するときに、それらの 10 人のみを対象として互いにランクを決めます。あるコンセントレータに対して上位 10 人に入らないユーザは、（個別のコンセントレータについて 1 位のユーザが持っているスループットまたは帯域幅の要件が、除外されるユーザよりも低い場合でも）全体のランキングから除外されます。したがって、上位 10 人のランキングはおよそのランキングです。

始める前に

ユーザのログアウト機能は、次の場合だけ有効です。

- 自分の CiscoWorks ユーザ ロールが System Administrator または Network Administrator の場合。「ユーザの権限について」（P.3-2）を参照してください。
- 対象の VPN コンセントレータで VPN 3000 Concentrator Series Manager がイネーブルになっており、Performance Monitor が対象のコンセントレータについて、正しい認証クレデンシャルのレコードを持っている場合。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Device Details] > [Top 10 Device Users] を選択します。

[Top 10 Device Users] ページ上のすべての測定値は、デルタではなく整数です。テーブルのカラムについては、表 5-8 を参照してください。

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。

ステップ 3　上位ユーザを算出するランキング基準を、[Compute Using] リストから選択します。次のオプションがあります。

- [Throughput] : kbps 単位で測定されたスループットに従ってユーザをランキングします。
- [Connect Duration] : 現在のセッションの期間（日、時間、分、および秒）に従ってユーザをランキングします。
- [Total Traffic] : 受信および送信パケットの合計に従ってユーザをランキングします。

ステップ 4　必要な場合は、ユーザを切断できます。対象の RAS VPN コンセントレータに多数のアクティブ セッションがある場合、ユーザ セッションを終了するための時間が 1 分を超えることがあります。

ユーザをログアウトするには、対象ユーザのオプション ボタンをクリックし、[Logout] をクリックします。ログアウトが正常に終了すると、対象ユーザがログアウトされ、そのユーザの IP アドレスは、アクティブな RAS セッションを表すテーブルに表示されなくなります。

参考

表 5-8　[Top 10 Device Users]

エレメント	説明
[User] カラム	現在のセッションに関連付けられているユーザ名が表示されます。 **（注）**　EzVPN セッションはこの機能をサポートしていません。
[Group] カラム	ユーザ名に関連付けられているユーザ グループ名が表示されます。 ユーザ セッションが Easy VPN サーバとして設定されているルータに関連付けられている場合は、そのグループ名がハイパーリンクされています。このような場合は、リンクをクリックして [Details of the Group Policy] ウィンドウを開きます。「グループ ポリシーの詳細」（P.5-17）を参照してください。
[Public IP Address] カラム	ユーザの IP アドレスが表示されます。
[Protocol] カラム	記載されている VPN セッションで使用中のプロトコルを識別します。
[Traffic In] カラム	受信パケットの合計数が表示されます。
[Traffic Out] カラム	送信パケットの合計数が表示されます。
[Total Traffic] カラム	受信オクテットと送信オクテットを組み合わせた数が表示されます。
[Connect Duration] カラム	ユーザが現在のセッションを確立してから経過した日数、時間、分、および秒が表示されます。
[Throughput (Kbps)] カラム	1 つのユーザ セッションあたりの一定期間の暗号化された送信オクテットおよび復号化された受信オクテットの合計数が表示されます。

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）

RAS クラスタの上位 10 ユーザの識別

1 つのクラスタに接続されているすべてのユーザをランキングすることも、すべてのクラスタ間で（Easy VPN ユーザを除く）ユーザをランキングすることもできます。Easy VPN は RAS クラスタの使用をサポートしていません。

Easy VPN ユーザを除いて、一度に 1 人のユーザをログアウトすることができます。

始める前に

ユーザのログアウト機能は、次の場合だけ有効です。

- 自分の CiscoWorks ユーザ ロールが System Administrator または Network Administrator の場合。「ユーザの権限について」（P.3-2）を参照してください。
- 対象の VPN コンセントレータで VPN 3000 Concentrator Series Manager がイネーブルになっており、Performance Monitor が対象のコンセントレータについて、正しい認証クレデンシャルのレコードを持っている場合。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Top 10 Cluster Users] を選択します。

[Top 10 Cluster Users] ページ上のすべての測定値は、デルタではなく整数です。

ステップ 2　表示するクラスタを、[Select Cluster] リストから選択します。レポートの対象を特定のクラスタに制限しない場合は、[All] を選択します。

ステップ 3　上位ユーザを算出するランキング基準を、[Compute Using] リストから選択します。次のオプションがあります。

- [Throughput] : kbps 単位で測定されたスループットに従ってユーザをランキングします。
- [Connect Duration] : 現在のセッションの期間（日、時間、分、および秒）に従ってユーザをランキングします。
- [Total Traffic] : 受信および送信パケットの合計に従ってユーザをランキングします。

ステップ 4　必要な場合は、ユーザを切断できます。対象の RAS VPN コンセントレータに多数のアクティブ セッションがある場合、ユーザ セッションを終了するための時間が 1 分を超えることがあります。

ユーザをログアウトするには、対象ユーザのオプション ボタンをクリックし、[Logout] をクリックします。ログアウトが正常に終了すると、対象ユーザがログアウトされ、そのユーザの IP アドレスは、アクティブな RAS セッションを表すテーブルに表示されなくなります。

参考

表 5-9　[Top 10 Cluster Users]

エレメント	説明
[User] カラム	現在のセッションに対して認証されているユーザ名が表示されます。
[Group] カラム	指名ユーザに関連付けられているユーザ グループ名のエントリが表示されます。 ユーザ セッションが Easy VPN サーバとして設定されているルータに関連付けられている場合は、そのグループ名がハイパーリンクされています。このような場合は、リンクをクリックして [Details of the Group Policy] ウィンドウを開きます。「グループ ポリシーの詳細」（P.5-17）を参照してください。 **（注）**　ユーザ セッションが、PIX ファイアウォールまたは VPN 3000 コンセントレータ上の Easy VPN サーバに関連付けられている場合は、グループ名はハイパーリンクされません。
[Public IP] カラム	ユーザのパブリック IP アドレスが表示されます。
[Protocol] カラム	この VPN セッションに対して、IPSec、L2TP、または PPTP のどのレイヤ 2 プロトコルが使用されているかを識別します。
[Traffic In] カラム	受信パケットの数が表示されます。
[Traffic Out] カラム	送信パケットの数が表示されます。
[Total Traffic] カラム	受信オクテットと送信オクテットを組み合わせた数が表示されます。
[Connect Duration] カラム	アクティブなセッションが開始されてから経過した秒数が表示されます。
[Throughput (kbps)] カラム	ユーザ セッションあたりに、受信オクテットに追加された送信オクテットの数が表示されます。

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）

グループ ポリシーの詳細

次の表は、セッションが、Easy VPN サーバとして設定されているルータに関連付けられている場合に、ユーザ セッションに割り当てられているグループ ポリシーのフィールドについて説明しています。このウィンドウを開く方法については、「RAS デバイスの上位 10 ユーザの識別」（P.5-13）または「RAS クラスタの上位 10 ユーザの識別」（P.5-15）を参照してください。

（注）　PIX Security Appliances からの Easy VPN セッションに対しては、同等の情報がありません。

表 5-10　[Details of the Group Policy] ウィンドウ

エレメント	説明
[Group Name] 行	対象のセッション内のユーザ名に関連付けられているユーザ グループ名が表示されます。
[Pool Name] 行	IP ローカル プール アドレスの名前が表示されます。この名前によって、内部 IP アドレスをクライアントへ割り当てるアドレス範囲を定義します。ユーザは少なくとも 1 つのプール名を定義する必要がありますが、各グループ ポリシーに対して別のプールを定義することもできます。この属性は必ず定義し、有効な IP ローカル プール アドレスを参照するようにします。そのようにしないと、クライアントの接続が失敗します。
[DNS Servers] 行	指定されたグループを使用しているすべての DNS サーバについて、IP アドレスのリストをカンマ区切り形式で表示します。
[WINS Servers] 行	指定されたグループを使用しているすべての WINS サーバについて、IP アドレスのリストをカンマ区切り形式で表示します。
[Domain Name] 行	グループが使用している、DNS 解決可能なドメイン名（cisco.com など）が表示されます。
[ACL] 行	どのトラフィックが暗号化されるかを定義する ACL の名前が表示されます。ACL 名は、対象グループに対してスプリットトンネリングが設定されている場合のみ表示されます。
[Backup Gateway] 行	プライマリ Easy VPN サーバへの接続が失敗した場合に、最初に試行するようルータで設定されているバックアップ ゲートウェイの IP アドレスまたはホスト名が表示されます。
[Firewall Are-U-There] 行	VPN セッションが Black Ice または Zone Alarm パーソナル ファイアウォールを通過することを示すように、クライアントがサーバ グループに対してシグナルを送信したかどうかを示します。
[Include-local-lan] 行	（スプリットトンネリングを使用せずに）クライアントおよびローカル ネットワークへの同時接続をサポートしているグループに対して、属性が設定されているかどうかを示します。これは「スタブ」ネットワークと呼ばれることもあり、デフォルトのルート 0.0.0.0/0 上ですべての非ローカル トラフィックを送信します。
[Group Lock] 行	preshred キー認証で IKE を使用する場合に、ユーザが Xauth ユーザ名（グループ名など）を提供できるよう、サーバ グループに対して属性が設定されているかどうかを示します。 （注）　シスコでは、証明書などの RSA シグニチャ認証メカニズムを使用するクライアントでは、Group-Lock 属性を使用しないことを推奨します。代わりに、このようなクライアントは User-VPN-Group 属性を使用してください。
[Save Password] 行	サーバ グループに対して、クライアント PC 上でユーザが XAuth 証明書をローカルに保存できるようにするオプションがイネーブルになっているかどうかを示します。