CHAPTER 7

ファイアウォール サービスのモニタリング

Performance Monitor は、Cisco 適応型セキュリティ アプライアンス、Cisco Secure PIX Firewall デバイス、および Cisco Catalyst 6500 スイッチのファイアウォール サービス モジュール（FWSM）で提供されるファイアウォール サービスの状態を判別します。

ここでは、ファイアウォール モニタリング機能について説明します。

ヒント ファイアウォールの一般的な問題のトラブルシューティングについては、付録の「トラブルシューティング」を参照してください。

ファイアウォール デバイス テーブルの操作

Performance Monitor では、すべての有効なファイアウォール デバイス、モジュール、およびセキュリティ コンテキストが表形式で示され、ひと目で概要を確認できます。このテーブルを使用して、ステータス、使用状況、およびエラーの説明を分離できます。

手順

ステップ 1 [Monitor] > [Firewall] > [Devices] を選択します。テーブルのカラムの説明については、表 7-1 を参照してください。

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。

- 単一デバイスの仮想コンテキストだけを表示するようにリストを制限するには、[Select Admin Context] リストからデバイスの管理コンテキストを選択します。デフォルト設定では、すべてが表示されます（すべての仮想コンテキストを含む、すべてのファイアウォールがリストされます）。
- イベント ブラウザを開いて、重大なファイアウォール エラーだけを表示するには、[Alert] カラムにアラート アイコンが表示されたときに、このアイコンをクリックします。
- 単一のデバイス、モジュール、またはコンテキストの状態を要約するグラフを表示するには、デバイス、モジュール、またはコンテキストの IP アドレスまたは DNS 名が [Device] カラムに表示されたときに、これをクリックします。

参考

表 7-1　[Firewall Devices] ページ

要素	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、重大なファイアウォール 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.3-14）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	関連するファイアウォールの DNS 名または IP アドレスが表示されます。 **（注）**　ルータは、少なくとも 1 つのインターフェイスがインスペクション ポリシーを使用して設定されている場合だけ、[Firewall Devices] ページに表示されます。
[Model] カラム	関連するアプライアンス、デバイス、またはサービス モジュールのハードウェア モデルを示しています。
[Version] カラム	関連するファイアウォールにインストールされている Cisco Firewall ソフトウェア リリース バージョンを示します。
[Memory Usage %] カラム	関連するファイアウォールが使用しているメモリのバイトの割合が表示されます。
[CPU Usage %] カラム	現在使用されている CPU 能力の割合が表示されます。これは、最近 5 秒間の平均です。
[No.Connections] カラム	関連するファイアウォールでアクティブな接続の合計数が表示されます。
[Xlates] カラム	関連するファイアウォールでアクティブな変換の数が表示されます。
[Packet Rate In] カラム	すべてのインターフェイスにわたる、受信パケットの現在のレートの合計が表示されます。
[Packet Rate Out] カラム	すべてのインターフェイスにわたる、送信パケットの現在のレートの合計が表示されます。
[No.Errors] カラム	前回のポーリング サイクル以降に発生した受信パケット エラーの数が、すべてのファイアウォール インターフェイスで集約されて表示されます。
[Throughput (Kbps)] カラム	前回のポーリング サイクル以降の関連するファイアウォールの 1 秒あたりの平均スループット速度が、すべてのインターフェイスで集約されて表示されます。
[Last Updated] カラム	表示された値がポーリングまたはトラップによって提供された時間が表示されます。

関連項目

- 「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）

ファイアウォール デバイスの詳細の操作

ここでは、単一のファイアウォール デバイスまたはモジュール用のモニタリング機能について説明します。

- 「デバイスまたはモジュールの詳細グラフの表示と意味」（P.7-3）

- 「デバイスまたはモジュール インターフェイス テーブルの表示」（P.7-4）
- 「デバイスまたはモジュール ブロック テーブルの表示」（P.7-5）
- 「デバイスまたはモジュール接続テーブルの表示」（P.7-5）

デバイスまたはモジュールの詳細グラフの表示と意味

1 つの検証済みファイアウォール デバイスまたはモジュールの CPU 使用状況、メモリ使用状況、インターフェイス エラー、スループット、および接続を示すグラフを表示および操作できます。

ステップ 1　[Select Monitor] > [Firewall] > [Device Details] を選択します。

デフォルトでは、Performance Monitor は、IP アドレスとして最も低い番号を使用するデバイスまたはモジュールのヘルスとパフォーマンスを示すグラフを表示します。グラフの説明については、表 7-2 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 番めの 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。

ファイアウォールのグラフの種類

表 7-2　ファイアウォール デバイスのグラフの種類

グラフの種類	説明
CPU Usage	使用されたデバイスまたはモジュールの CPU 能力の割合を示します。 • 縦軸は、関連するポーリング サイクルで使用された CPU 能力の割合の平均を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
Memory Usage	使用されたデバイスまたはモジュールのメモリ容量の割合を示します。 • 縦軸は、関連するポーリング サイクルで使用されたメモリ容量の割合の平均を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
Throughput vs.Connection	長期にわたるスループットのトレンドと接続のトレンドを比較するのに役立つ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（オレンジ色の）縦軸は、関連するポーリング サイクルでの平均スループットをバイト単位で示します。 – 右の（青の）縦軸は、関連するポーリング サイクルでのファイアウォール接続数の平均を示します。 • 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。

表 7-2　ファイアウォール デバイスのグラフの種類（続き）

グラフの種類	説明
Interface Error	長期にわたるデバイスまたはモジュール インターフェイス エラーのトレンドを示します。 • 縦軸は、関連するポーリング サイクルで発生したエラーの平均数を示します。 • 横軸は、ポーリング サイクルの時刻を示します。

デバイスまたはモジュール インターフェイス テーブルの表示

1 つの検証済みのファイアウォール デバイスまたはモジュールのインターフェイス パフォーマンス統計情報テーブルを、表示および操作できます。

（注）　インスペクション ポリシーが設定されているルータのインターフェイスが、[Firewall Interfaces] ページに表示されます。ただし、PIX、ASA、および FWSM デバイスの場合は、すべてのインターフェイスが表示されます。

手順

ステップ 1　[Monitor] > [Firewall] > [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 7-3 を参照してください。

[Firewall Interfaces] ページのすべての測定値は、*デルタ*として計算されます。つまり、あるポーリング サイクルから次のポーリング サイクルまでの差の範囲を示します。

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

参考

表 7-3　[Firewall Interfaces] ページ

要素	説明
[Name] 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。
[Speed (Kbps)] カラム	関連するインターフェイスを通るトラフィック フローの平均速度（キロビット）が表示されます。
[Bytes In] カラム	前回のポーリング サイクル以降のインターフェイスでの受信バイトの合計数が表示されます。
[Bytes Out] カラム	前回のポーリング サイクル以降のインターフェイスでの送信バイトの合計数が表示されます。
[Packets In] カラム	前回のポーリング サイクル以降のインターフェイスで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 サイクル以降のインターフェイスでの送信パケットの合計数が表示されます。

表 7-3　[Firewall Interfaces] ページ（続き）

要素	説明
[Packet Errors] 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で発生したパケット エラーの合計数が表示されます。
[Bandwidth Utilization %] カラム	デバイス タイプごとに異なる値が表示されます。 • PIX：使用中の帯域幅容量の割合が表示されます。 • ファイアウォール サービス モジュール：「N/A」と表示されます。

関連項目

- 「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）

デバイスまたはモジュール ブロック テーブルの表示

ブロックとは、パケットを処理する内部バッファです。[Firewall Blocks] テーブルに表示される値は、1 つの検証済みのファイアウォール デバイスまたはモジュールのブロックの状態を示しています。ファイアウォール ブロック統計情報テーブルを表示および操作できます。

手順

ステップ 1　[Monitor] > [Firewall] > [Device Details] > [Blocks] を選択します。

デフォルトでは、[Firewall Blocks] ページには、IP アドレスとして最も低い番号を使用するデバイスまたはモジュールのブロック情報が表示されます。

ステップ 2　[Select Device] リストから、詳細を表示するデバイスを選択します。各カラムで、次の情報を示します。

- [Block Size]：ブロック サイズをバイト単位で表示します。
- [No.Available]：使用可能なブロックの数を表示します（関連するブロックのサイズ単位）。
- [No.In Use]：使用中のブロックの数を表示します（関連するブロックのサイズ単位）。

関連項目

- 「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）

デバイスまたはモジュール接続テーブルの表示

ファイアウォールは、接続要求の目的とプロトコルを調べてから、接続を許可または拒否します。1 つの検証済みのファイアウォール デバイスまたはモジュールの接続統計情報テーブルを、表示および操作できます。

手順

ステップ 1　[Monitor] > [Firewall] > [Device Details] > [Connections] を選択します。

各行には、記述されている値に関して 1 秒ごとに計算された変化のレートが表示されます（レートの種類は、測定値の各インスタンスで指定されます）。

Performance Monitor は、常に各値を再計算しているため、ある 1 秒間に関連する変化がなかった場合、行に値ゼロ（0）が表示されることがあります。

表示された値は累積値ではありません。値は、表示がリフレッシュされるときに増加したり減少したりすることがあります。

（注） 設定されていないファイアウォール機能については、常に値ゼロが表示されます。

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

関連項目

- 「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）