CHAPTER 42

ルータ情報の表示

Cisco Configuration Professional（Cisco CP）を監視モードで使用すると、ルータ、ルータ インターフェイス、ファイアウォール、およびアクティブな VPN 接続についての情報の最新スナップショットを表示できます。また、ルータ イベント ログ内のメッセージも表示できます。

（注） ［監視］ウィンドウは、ダイナミックに最新情報で更新されるわけではありません。このウィンドウを開いた後に変更された情報を表示するには、［更新］をクリックする必要があります。

監視モードでは、ルータのログが検査され、Cisco IOS **show** コマンドの結果が参照されます。監視モードの機能のうち、ファイアウォール統計情報などのログ エントリに基づく機能を使用するには、ロギングが有効になっている必要があります。Cisco CP ではロギングがデフォルトで有効になっています。ただし、この設定は、［追加タスク］>［ルータ プロパティ］>［ロギング］を選択して表示されるウィンドウで変更することができます。また、ログ イベントを生成するには、個別のルールの設定作業が必要な場合もあります。詳細については、ヘルプ トピック「ファイアウォール上のアクティビティを表示する方法」を参照してください。

目的	手順
ルータ インターフェイスについての情報を表示する。	ツールバーで［監視］をクリックし、左側のフレームで［インターフェイス ステータス］をクリックする。情報を表示するインターフェイスを［インターフェイスの選択］フィールドから選択し、表示する情報を［Available Items］（選択可能な項目）グループで選択する。次に、［詳細の表示］をクリックする。
CPU またはメモリの使用状況を示すグラフを表示する。	ツールバーで［監視］をクリックする。［概要］ページに CPU およびメモリの使用状況のグラフが表示される。
ファイアウォールについての情報を表示する。	ツールバーで［監視］をクリックし、左側のフレームで［ファイアウォール ステータス］をクリックする。
VPN 接続についての情報を表示する。	ツールバーで［監視］をクリックし、左側のフレームで［VPN ステータス］をクリックする。［IPSec トンネル］、［DMVPN トンネル］、［Easy VPN サーバ］、または［IKE SA］のタブを選択する。
ルータ イベント ログ内のメッセージを表示する。	ツールバーで［監視］をクリックし、左側のフレームで［ロギング］をクリックする。

概要

監視モードの［概要］画面には、ルータのアクティビティと統計情報の概要が表示されます。この画面は、監視モードの他の画面の情報を要約する役割を果たします。この画面には、このヘルプ トピックで説明する情報が表示されます。

（注） ［概要］画面にヘルプ　トピックで説明されている機能情報が表示されない場合は、Cisco IOS イメージでこの機能をサポートしていません。たとえば、セキュリティ機能をサポートしていない Cisco IOS イメージをルータで実行している場合、［ファイアウォール ステータス］セクションおよび［VPN ステータス］セクションは、この画面に表示されません。

ワイヤレス アプリケーションの起動ボタン

ルータに無線インターフェイスが備わっている場合は、このボタンをクリックして無線インターフェイスを監視および設定できます。［監視の概要］ウィンドウには無線インターフェイスのインターフェイス ステータス情報が表示されますが、インターフェイス ステータスのモニタウィンドウにこのインターフェイスのリストは表示されません。

ルータに無線インターフェイスが備わっていない場合、このボタンは表示されません。

更新ボタン

ルータから最新の情報を取得し、画面に表示されている統計情報を更新します。

リソース ステータス

ルータのハードウェアの基本的な情報が表示されます。次のフィールドがあります。

CPU の使用状況

CPU の使用率が表示されます。

メモリの使用状況

RAM の使用率が表示されます。

フラッシュの使用状況

ルータにインストールされているフラッシュの合計容量に占める使用可能フラッシュの容量の割合が表示されます。

インターフェイス ステータス

ルータにインストールされているインターフェイスの基本的な情報とステータスが表示されます。

（注）　Cisco CP でサポートされているタイプのインターフェイスのみが、ここでの統計の対象になります。サポートされていないインターフェイスは対象になりません。

稼働インターフェイスの合計数

ルータ上の有効な（稼働中の）インターフェイスの合計数。

停止インターフェイスの合計数

ルータ上の無効な（停止中の）インターフェイスの合計数。

インターフェイス

インターフェイス名。

IP

インターフェイスの IP アドレス。

ステータス

インターフェイスのステータス（[稼働] または [停止]）。

帯域幅の使用状況

インターフェイスの帯域幅の使用率。

説明

インターフェイスの説明を参照できる場合はその説明。Cisco CP によって $FW_OUTSIDE$ や ETH_LAN などの説明が追加される場合があります。

ファイアウォール ステータス グループ

ルータのリソースの基本的な情報が表示されます。次のフィールドがあります。

拒否した試行回数

Telnet、HTTP、ping などのプロトコルを利用して行われた接続試行をファイアウォールで拒否したときに生成されたログ メッセージの数が表示されます。接続試行を拒否した場合にログ エントリが生成されるようにするには、接続試行を拒否するアクセス ルールを、ログ エントリを作成するように設定する必要があります。

ファイアウォール ログ

有効になっている場合、ファイアウォール ログのエントリの数が表示されます。

QoS

関連付けられた QoS ポリシーがあるインターフェイスの数。

VPN ステータス グループ

ルータのリソースの基本的な情報が表示されます。次のフィールドがあります。

接続中の IKE SA の数

現在設定済みかつ動作中の IKE セキュリティ アソシエーション（SA）接続の数が表示されます。

接続中の IPSec トンネルの数

現在設定済みかつ動作中の IPSec 仮想プライベート ネットワーク（VPN）接続の数が表示されます。

DMVPN クライアントの数

ルータが DMVPN ハブとして設定されている場合、DMVPN クライアントの数が表示されます。

アクティブな VPN クライアントの数

ルータが Easy VPN サーバとして設定されている場合、Easy VPN リモート クライアントの数がこのフィールドに表示されます。

NAC ステータス グループ

ルータ上のネットワーク アドミッション コントロール（NAC）ステータスの基本的なスナップショットが表示されます。

NAC の有効なインターフェイス フィールド数

NAC が有効なルータ インターフェイスの数。

検証されたホスト フィールド数

アドミッション コントロール プロセスによって検証されたポスチャ エージェントを持つホストの数。

ログ グループ

ルータのリソースの基本的な情報が表示されます。次のフィールドがあります。

ログ エントリの合計数

ルータのログに現在保存されているエントリの合計数。

高い重大度

保存されているログ エントリのうち、重大度レベルが 2 以下のものの数。これらのメッセージには直ちに対処する必要があります。重大度の高いメッセージがない場合、このリストは空になります。

警告

保存されているログ エントリのうち、重大度レベルが 3 または 4 のものの数。これらのメッセージは、ネットワークの問題を示していることがあります。ただし、直ちに対処する必要はありません。

情報

保存されているログ エントリのうち、重大度レベルが 6 以上のものの数。これらの情報メッセージは、正常なネットワーク イベントを通知するものです。

インターフェイス ステータス

［インターフェイス ステータス］画面には、ルータ上のさまざまなインターフェイスの現在のステータスが表示されます。また、選択したインターフェイスを経由して転送されたパケット、バイト、またはデータ エラーの数も表示されます。この画面に表示される統計情報は、ルータの再起動、カウンタのリセット、または選択したインターフェイスのリセットが最後に行われてからの累計です。

監視インターフェイス / 監視の終了ボタン

このボタンをクリックすると、選択したインターフェイスの監視を開始または終了できます。ボタンのラベルは、Cisco CP がインターフェイスを監視しているかどうかで変わります。

接続のテスト ボタン

選択した接続をテストする場合にクリックします。ダイアログ ボックスが表示され、この接続を使用して ping を実行するリモート ホストを指定できます。ping を実行すると、このダイアログ ボックスにテスト結果（合格または不合格）が表示されます。テストが失敗した場合は、考えられる原因と問題の解決手順が表示されます。

インターフェイス リスト

統計情報を表示するインターフェイスをこのリストから選択します。このリストには、IP アドレスとサブネット マスク、およびインターフェイスがあるスロットとポートが表示されます。Cisco CP の説明やユーザの説明が入力されていれば、その説明も表示されます。

監視するグラフ タイプの選択グループ

ここに表示されているチェック ボックスが示しているのは、選択したインターフェイスのデータ項目のうち、Cisco CP を使用して統計情報を表示できる項目です。次のデータ項目があります。

- ［入力されたパケット］— 選択したインターフェイスの受信パケット数。
- ［出力されたパケット］— 選択したインターフェイスの送信パケット数。

- ［帯域幅の使用状況］— インターフェイスによる帯域幅の使用率。割合（%）で表示されます。帯域幅の割合の計算方法は次のとおりです。

  帯域幅の割合 =(Kbps/bw) * 100

  この式の各値は次のとおりです。

  ビット数 / 秒 = ((入力数の変化 + 出力数の変化) * 8) / ポーリング間隔

  Kbps= 1 秒あたりのビット数 /1024

  bw= インターフェイスの帯域幅の容量

  入力バイトと出力バイトの差は、2 回目の表示間隔の後でのみ計算されるので、帯域幅の割合のグラフには、2 回目の表示間隔以降の帯域幅の使用状況が正しく表示されます。ポーリング間隔と表示間隔については、このトピックの「表示間隔」のセクションを参照してください。
- ［入力されたバイト］— 選択したインターフェイスの受信バイト数。
- ［出力されたバイト］— 選択したインターフェイスの送信バイト数。
- ［入力エラー］— 選択したインターフェイスでデータ受信時に発生したエラーの数。
- ［出力エラー］— 選択したインターフェイスでデータ送信時に発生したエラーの数。
- ［パケット フロー］— 選択したインターフェイスのフロー内にあるパケットの数。このデータ項目は、選択したインターフェイスが［設定］>［インターフェイスと接続］>［編集］>［アプリケーション サービス］で設定されている場合にのみ表示されます。
- ［バイト フロー］— 選択したインターフェイスのフローのバイト数。このデータ項目は、選択したインターフェイスが［設定］>［インターフェイスと接続］>［編集］>［アプリケーション サービス］で設定されている場合にのみ表示されます。
- ［合計フロー］— 選択したインターフェイスの送信元および宛先からのフローの合計数。このデータ項目は、選択したインターフェイスが［設定］>［インターフェイスと接続］>［編集］>［アプリケーション サービス］で設定されている場合にのみ表示されます。

（注） ルータの Cisco IOS イメージが Netflow をサポートしていない場合、フロー カウンタは使用できません。

上記の項目の統計情報を表示するには、次の手順に従ってください。

ステップ 1　統計情報を表示する項目のチェック ボックスを選択します。

ステップ 2　［監視インターフェイス］をクリックすると、選択したすべてのデータ項目の統計情報が表示されます。

インターフェイス ステータス エリア

表示間隔

このプルダウン フィールドでは、各項目のデータの表示量と、データの更新頻度の両方を選択します。次のオプションがあります。

（注）　リストに表示されるポーリング頻度はおよその値です。実際の頻度とは多少異なることがあります。

- 10 秒ごとのリアルタイム データ。このオプションを選択すると、ルータに対するポーリングが最大 2 時間継続され、約 120 個のデータ ポイントが取得されます。
- 過去 10 分間のデータを 10 秒ごとにポーリング
- 過去 60 分間のデータを 1 分ごとにポーリング
- 過去 12 時間のデータを 10 分ごとにポーリング

（注）　最後から 3 番目までのオプションを選択すると、最大 60 個のデータ ポイントが取得されます。60 個のデータ ポイントが取得された後も Cisco CP によるデータのポーリングは継続され、最も古いデータ ポイントが最も新しいデータ ポイントで置き換えられます。

テーブルの表示 / テーブルの非表示

このボタンをクリックすると、パフォーマンス グラフの表示と非表示を切り替えることができます。

リセット ボタン

このボタンをクリックすると、インターフェイスの統計情報の集計をゼロにリセットできます。

グラフ エリア

このエリアには、指定したデータのグラフと単純な数値が表示されます。

（注） 最後から 3 番目までのオプションを選択すると、最大 30 個のデータ ポイントが取得されます。30 個のデータ ポイントが取得された後も Cisco CP によるデータのポーリングは継続され、最も古いデータ ポイントが最も新しいデータ ポイントで置き換えられます。

ファイアウォール ステータス

このウィンドウには、ルータに設定されているファイアウォールに関する次の統計情報が表示されます。

- ［検査用に設定されたインターフェイスの数］— トラフィックをファイアウォールで検査するように設定したルータのインターフェイスの数。
- ［TCP パケット カウントの数］— 検査用に設定されたインターフェイス経由で送信された TCP パケットの合計数。
- ［UDP パケット カウントの数］— 検査用に設定されたインターフェイス経由で送信された UDP パケットの合計数。
- ［アクティブな接続の総数］— 現在のセッションの数。

また、［ファイアウォール ステータス］ウィンドウには、次のカラムを持つ表にアクティブなファイアウォール セッションも表示されます。

- ［送信元 IP アドレス］— パケットの発信元ホストの IP アドレス。
- ［宛先 IP アドレス］— パケットの宛先ホストの IP アドレス。
- ［プロトコル］— 検査するネットワーク プロトコル。
- ［マッチ カウント］— ファイアウォールの条件に一致するパケットの数。

更新ボタン

このボタンをクリックすると、表内のファイアウォール セッションが更新され、ルータから取得した最新のデータが表示されます。

ゾーンベース ポリシー ファイアウォールのステータス

ゾーンベース ポリシー ファイアウォール機能をサポートする Cisco IOS イメージがルータで実行されている場合は、ルータに設定された各ゾーン ペアに対し、ファイアウォールのアクティビティのステータスを表示できます。

ファイアウォール ポリシー リスト エリア

ここには、各ゾーン ペアのポリシー名、送信元ゾーン、および宛先ゾーンが表示されます。次の表は、2 つのゾーン ペアのデータ例を示します。

ゾーン ペア名	ポリシー名	送信元ゾーン	宛先ゾーン
wan-dmz-in	pmap-wan	zone-wan	zone-dmz
wan-dmz-out	pmap-dmz	zone-dmz	zone-wan

この例では、DMZ へのインバウンド トラフィック、および DMZ からのアウトバウンド トラフィックに対してそれぞれゾーン ペアが設定されています。

ファイアウォールの統計情報を表示するゾーン ペアを選択してください。

表示間隔

データの収集方法を指定するオプションとして、以下のいずれかを選択します。

- 10 秒ごとのリアルタイム データ — データは 10 秒ごとに報告されます。[廃棄パケット] および [許可パケット] グラフでは、水平軸上の 1 目盛りは 10 秒を表します。
- 過去 60 分間のデータを 1 分ごとにポーリング — データは 1 分ごとに報告されます。[廃棄パケット] および [許可パケット] グラフでは、水平軸上の 1 目盛りは 1 分を表します。
- 過去 12 時間のデータを 12 分ごとにポーリング — データは 12 分ごとに報告されます。[廃棄パケット] および [許可パケット] グラフでは、水平軸上の 12 目盛りは 12 分を表します。

監視ポリシー

クリックすると、選択したポリシーに対するファイアウォール データが収集されます。

監視の終了

クリックすると、ファイアウォール データの収集が停止します。

統計エリア

このエリアには、選択したゾーン ペアのファイアウォール統計情報が表示されます。左側のツリーでノードをクリックすると、このエリアの表示内容を制御できます。以下に、各ノードをクリックした場合の表示内容について説明します。

アクティブ セッション

クリックすると、選択したゾーン ペアで検査されるトラフィックのタイプ、送信元 IP アドレス、および宛先 IP アドレスが表示されます。

廃棄パケット

クリックすると、選択したゾーン ペアについて、［表示間隔］リストで選択した時間間隔で廃棄されたパケットの累積数を示すグラフが表示されます。廃棄するように設定したトラフィックに関するデータが収集され、レイヤ 4 ポリシー マップに記録されます。

許可パケット

クリックすると、選択したゾーン ペアについて、［表示間隔］リストで選択した時間間隔で許可されたパケットの累積数を示すグラフが表示されます。通過アクションを設定したトラフィックに関するデータが収集され、レイヤ 4 ポリシー マップに記録されます。

VPN ステータス

このウィンドウには、ルータで使用できる VPN 接続のツリーが表示されます。VPN 接続ツリーで、次の VPN カテゴリのいずれかを選択できます。

- IPSec トンネル
- DMVPN トンネル
- Easy VPN サーバ
- IKE SA
- SSL VPN コンポーネント

アクティブな VPN カテゴリの統計情報を表示するには、VPN 接続ツリーから選択します。

IPSec トンネル

このグループには、ルータに設定されている各 IPSec VPN の統計情報が表示されます。表の行は、それぞれ 1 つの IPSec VPN を表しています。表のカラムと、各カラムに表示される情報は次のとおりです。

- ［インターフェイス］カラム

  IPSec トンネルがアクティブになっている、ルータ上の WAN インターフェイス。
- ［ローカル IP］カラム

  ローカル IPSec インターフェイスの IP アドレス。
- ［リモート IP］カラム

  リモート IPSec インターフェイスの IP アドレス。
- ［ピア］カラム

  リモート ピアの IP アドレス。
- トンネル ステータス

  IPSec トンネルの現在のステータス。値は次のとおりです。
  - ［稼働］— トンネルはアクティブです。
  - ［停止］— エラーまたはハードウェア障害のため、トンネルは非アクティブです。

- ［カプセル化パケット］カラム
  IPSec VPN 接続上でカプセル化されたパケットの数。
- ［非カプセル化パケット］カラム
  IPSec VPN 接続上で非カプセル化されたパケットの数。
- ［送信エラー パケット］カラム
  パケット送信時に発生したエラーの数。
- ［受信エラー パケット］カラム
  パケット受信時に発生したエラーの数。
- ［暗号化されたパケット］カラム
  接続上で暗号化されたパケットの数。
- ［解読されたパケット］カラム
  接続上で解読されたパケットの数。

トンネルの監視ボタン

［IPSec トンネル］表で選択した IPSec トンネルを監視する場合にクリックします。「IPSec トンネルの監視」を参照してください。

トンネルのテスト ... ボタン

選択した VPN トンネルをテストする場合にクリックします。テストの結果は、別のウィンドウに表示されます。

更新ボタン

このボタンをクリックすると、［IPSec トンネル］表が更新され、ルータから取得した最新のデータが表示されます。

IPSec トンネルの監視

IPSec トンネルを監視するには、次の手順に従ってください。

ステップ 1　［IPSec トンネル］表で監視するトンネルを選択します。

ステップ 2　［監視する項目の選択］にある該当のチェック ボックスを選択して、監視する情報のタイプを選択します。

ステップ 3　［表示間隔］ドロップダウン リストを使用して、リアルタイム グラフを表示する間隔を選択します。

DMVPN トンネル

このグループには、ダイナミック マルチポイント VPN（DMVPN）トンネルに関する以下の統計情報が表示されます。各行は、それぞれ 1 つの VPN トンネルを表しています。

- ［リモート サブネット］カラム

  トンネルが接続するサブネットのネットワーク アドレス。
- ［リモート トンネル IP］カラム

  リモート トンネルの IP アドレス。これは、リモート デバイスによってトンネルに割り当てられたプライベート IP アドレスです。
- ［リモート ルータのパブリック インターフェイスの IP］カラム

  リモート ルータのパブリック（外部）インターフェイスの IP アドレス。
- ステータス カラム

  DMVPN トンネルのステータス。
- ［有効期限］カラム

  トンネルの登録が期限切れになり DMVPN トンネルがシャットダウンされる日時。

トンネルの監視ボタン

［DMVPN トンネル］表で選択した DMVPN トンネルを監視する場合にクリックします。「DMVPN トンネルの監視」を参照してください。

更新ボタン

このボタンをクリックすると、［DMVPN トンネル］表が更新され、ルータから取得した最新のデータが表示されます。

リセット ボタン

トンネル リストの統計情報カウンタをリセットする場合にクリックします。カプセル化パケットと非カプセル化パケットの数、送信エラーと受信エラーの数、および暗号化されたパケットと解読されたパケットの数がゼロに設定されます。

DMVPN トンネルの監視

DMVPN トンネルを監視するには、次の手順に従ってください。

ステップ 1　［DMVPN トンネル］表で監視するトンネルを選択します。

ステップ 2　［監視する項目の選択］にある該当のチェック ボックスを選択して、監視する情報のタイプを選択します。

ステップ 3　［表示間隔］ドロップダウン リストを使用して、リアルタイム グラフを表示する間隔を選択します。

Easy VPN サーバ

このグループには、各 Easy VPN サーバ グループの次の情報が表示されます。

- サーバ クライアントの合計数（右上隅に表示されます）
- グループ名
- クライアント接続の数

グループ詳細ボタン

［グループ詳細］ボタンをクリックすると、選択したグループの次の情報が表示されます。

- グループ名
- キー
- プール名
- DNS サーバ
- WINS サーバ
- ドメイン名
- ACL
- バックアップ サーバ
- ファイアウォールの R-U-There
- ローカル LAN を含む
- グループ ロック
- パスワードの保存
- このグループでの最大許容接続数
- ユーザあたりの最大ログイン数

このグループ内のクライアント接続

このエリアには、選択したグループの次の情報が表示されます。

- パブリック IP アドレス
- 割り当てられた IP アドレス
- 暗号化されたパケット
- 解読されたパケット
- 廃棄されたアウトバウンド パケット
- 廃棄されたインバウンド パケット
- ステータス

更新ボタン

このボタンをクリックすると、ルータから取得した最新データが表示されます。

切断ボタン

- 表の行を選択してから［切断］をクリックすると、クライアントとの接続が廃棄されます。

IKE SA

このグループには、ルータに設定されているアクティブな IKE セキュリティ アソシエーションに関する以下の統計情報が表示されます。

- ［送信元 IP］カラム

  IKE SA を開始したピアの IP アドレス。
- ［宛先 IP］カラム

  リモート IKE ピアの IP アドレス。
- ［状態］カラム

  IKE ネゴシエーションの現在の状態が表示されます。次の状態があります。
  - ［MM_NO_STATE］— Internet Security Association and Key Management Protocol（ISAKMP）SA は作成されましたが、それ以外にはまだ何も行われていません。
  - ［MM_SA_SETUP］— ピア間で ISAKMP SA のパラメータについての合意が行われました。
  - ［MM_KEY_EXCH］— ピア間で Diffie-Hellman パブリック キーが交換され、共有秘密キーが生成されました。ISAKMP SA はまだ認証されていません。
  - ［MM_KEY_AUTH］— ISAKMP SA が認証されました。ルータがこの交換プロセスの開始側である場合、状態は直ちに QM_IDLE に移行し、クイック モードでの交換プロセスが開始されます。
  - ［AG_NO_STATE］— ISAKMP SA は作成されましたが、それ以外にはまだ何も行われていません。
  - ［AG_INIT_EXCH］— ピア間で最初の交換プロセスがアグレッシブ モードで行われましたが、SA は認証されていません。

- ［AG_AUTH］— ISAKMP SA が認証されました。ルータがこの交換プロセスの開始側である場合、状態は直ちに QM_IDLE に移行し、クイックモードでの交換プロセスが開始されます。
- ［QM_IDLE］— ISAKMP SA はアイドル状態です。ピアでの認証は取り消されず、後続のクイック モードでの交換プロセスで使用できます。

- ［更新］ボタン — このボタンをクリックすると［IKE SA］表が更新され、ルータから取得した最新データが表示されます。
- ［クリア］ボタン — 表の行を選択してから［クリア］をクリックすると、その行に対応する IKE SA 接続をクリアできます。

SSL VPN コンポーネント

監視ウィンドウで［VPN ステータス］ボタンをクリックすると、ルータで SSL VPN アクティビティの監視が開始されます。このウィンドウには、ルータ上で設定されたすべての SSL VPN コンテキストに対して収集されたデータが表示されます。

デフォルトでは、このデータは 10 秒ごとに更新されます。データの表示から更新までが 10 秒間では短すぎる場合は、［1 分ごとのリアルタイム データ］の自動更新の間隔を選択できます。

SSL VPN ツリーでコンテキストを選択し、そのコンテキストのデータとそのコンテキストに設定されたユーザのデータを表示します。

システム リソース

SSL VPN トラフィックがすべてのコンテキストで使用している CPU とメモリ リソースの割合が、このエリアに表示されます。

接続ユーザ数

このグラフには、アクティブ ユーザの数が時間の経過に従って表示されます。監視が開始されてからの最大アクティブ ユーザ数は、グラフ エリアの上部に表示されます。監視の開始時刻はグラフの左下隅に表示され、現在の時刻はグラフ下の中央に表示されます。

タブ付きエリア

ウィンドウのこのエリアには、収集された統計情報が一連のタブに見やすく表示されます。

下の任意のリンクをクリックすると、タブに表示されるデータの説明に移動できます。

ユーザ セッション

URL の細分化

ポート転送

CIFS

フル トンネル

（注）　ポート転送やフル トンネルなどの機能がルータに設定されていない場合は、その機能のタブにはデータが表示されません。

統計情報の中には、ルータが監視データを更新するたびに新たに収集されるものがあります。アクティブ ユーザの統計情報の最大数などのその他の統計情報は、更新時に収集されますが、監視が開始されたときに収集された同じデータと比較されます。［VPN ステータス］ボタンをクリックすると、SSL VPN を含むすべての VPN アクティビティの監視が開始されます。

SSL VPN コンテキスト

このウィンドウには、［SSL VPN コンポーネント］ウィンドウと同じタイプの情報が表示されますが、選択したコンテキストに対して収集したデータのみが表示されます。表示される情報の説明については、「SSL VPN コンポーネント」を参照してください。

ユーザ セッション

このタブには、SSL VPN ユーザ セッションに関する次の情報が表示されます。

- ［アクティブなユーザ セッション］— すべてのトラフィック タイプについて、監視データの更新以降アクティブになっている SSL VPN ユーザ セッションの数。
- ［最大ユーザ セッション］— 監視の開始以降アクティブになっている SSL VPN ユーザ セッションの最大数。
- ［アクティブなユーザ TCP 接続］— 監視データの更新以降アクティブになっている TCP ベースの SSL VPN ユーザ セッションの数。
- ［セッション割り当てエラー］— 監視の開始以降に発生したセッション割り当てエラーの数。
- ［VPN セッション タイムアウト］— 監視の開始以降に発生した VPN セッション タイムアウトの数。
- ［ユーザがクリアした VPN セッション］— 監視の開始以降、ユーザがクリアした VPN セッションの数。
- ［AAA の保留中の要求］— 監視データの更新以降、保留になっている AAA 要求の数。
- ［ピーク時］— 監視の開始以降に記録された最も長いユーザ セッション。
- ［終了したユーザ セッション］— 監視の開始以降に終了したユーザ セッションの数。
- ［認証エラー］— 監視の開始以降、認証に失敗したセッションの数。
- ［VPN アイドル タイムアウト］— 監視の開始以降に発生した VPN アイドル タイムアウトの数。
- ［超過したコンテキスト ユーザ数の制限］— 監視の開始以降、コンテキスト セッションの制限に達した後でユーザがセッションの開始を試行した回数。
- ［超過した合計ユーザ数の制限］— 監視の開始以降、セッション合計の制限に達した後でユーザがセッションの開始を試行した回数。

URL の細分化

このタブには、URL の細分化アクティビティに関するデータが表示されます。詳細については、下記のリンクからアクセスできるコマンド リファレンスを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

ポート転送

このタブには、ポート転送アクティビティに関して収集されたデータが表示されます。詳細については、下記のリンクでコマンド リファレンスを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

CIFS

このタブには、CIFS の要求、応答、および接続に関して収集されたデータが表示されます。詳細については、下記のリンクからアクセスできるコマンド リファレンスを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

フル トンネル

このタブには、企業イントラネット上の SSL VPN クライアントとサーバ間のフル トンネル接続に関する情報が表示されます。

- ［アクティブなトンネル接続］— データが最後に更新されて以降アクティブなフル トンネル接続の数。データは 10 秒ごと、または毎分更新できます。
- ［ピーク時のアクティブな接続］— 監視の開始以降、最も長く継続したフル トンネル接続。
- ［アクティブなトンネル接続の最大数］— 監視の開始以降アクティブなフル トンネル接続の最高数。

- ［失敗したトンネル接続の試行回数］— 監視の開始以降、フル トンネル接続の試行が失敗した回数。
- ［成功したトンネル接続の試行回数］— 監視の開始以降、フル トンネル接続が正常に確立した回数。

サーバ：

- ［サーバに送信された IP パケット］— ルータが企業のイントラネットのフル トンネル クライアントからサーバへ転送した IP パケットの数。
- ［サーバに送信された IP トラフィック（バイト単位）］— 企業のイントラネットのフル トンネル クライアントからサーバへ転送された IP トラフィックの量（バイト単位）。
- ［サーバから受信した IP パケット］— ルータがクライアントへのフル トンネル接続でサーバから受信した IP パケットの数。
- ［サーバから受信した IP トラフィック（バイト単位）］— クライアントへのフル トンネル接続で企業のイントラネットのサーバから受信された IP トラフィックの量（バイト単位）。

ユーザ リスト

このウィンドウには、［SSL VPN コンポーネント］ツリーで選択されたコンテキストのユーザ情報が表示されます。コンテキストには複数のグループ ポリシーを、それぞれ独自の URL リストとサーバ リストを使用して設定できるので、この画面には個々のユーザが各自の SSL VPN 接続を使用する方法について貴重な情報が表示されます。

ユーザを選択して［切断］ボタンをクリックすると、このウィンドウで個々の SSL VPN 使用を制御できます。

ユーザ リスト エリア

このエリアには、このコンテキストに対して設定されたすべてのグループのアクティブなユーザがすべて表示されます。このエリアには、次の情報が表示されます。

- ［ユーザのログイン名］— AAA サーバで認証されたユーザ名。

- ［クライアントの IP アドレス］— このセッションでユーザに割り当てられた SSL VPN IP アドレス。この IP アドレスは、このコンテキストで設定されたアドレス プールから取得されます。
- ［コンテキスト］— このユーザのグループ ポリシーが設定されているコンテキスト下の SSL VPN コンテキスト。
- ［接続の数］— ユーザに対するアクティブな接続の数。たとえば、ユーザがメール サーバに接続していたり、ネットワーク上の別のサーバのファイルを参照している場合などです。
- 作成日 — セッションが作成された時間。
- ［最終使用日］— ユーザが任意のアクティブな接続でトラフィックを最後に送信した時刻。
- ［Cisco Secure Desktop］— True または False。Cisco Secure Desktop がユーザの PC にダウンロードされているかどうかを示します。
- ［グループ名］— ユーザを設定する際に使用するグループ ポリシーの名前。グループ ポリシーは、URL リスト、ユーザが利用できるサービス、サーバ名を解決する際に使用できる WINS サーバ、および企業のイントラネットでファイルを参照する際にユーザに表示されるサーバを指定します。
- ［URL リスト名］— ユーザのポータル ページに表示される URL リストの名前。URL リストは、ユーザが属するグループに対して設定されます。詳細については、「グループ ポリシー：クライアントレス タブ」を参照してください。
- ［アイドル タイムアウト］— ルータが切断するまでの、セッションがアイドル状態にある秒数。この値は、ユーザが属するグループに対して設定されます。詳細については、「グループ ポリシー：全般タブ」を参照してください。
- ［セッション タイムアウト］— セッションが、終了せずにアクティブ状態を維持できる最大秒数。この値は、ユーザが属するグループに対して設定されます。詳細については、「グループ ポリシー：全般タブ」を参照してください。
- ［ポート転送名］— この値は、ユーザが属するグループに対して設定されます。詳細については、「グループ ポリシー：シン クライアント タブ」を参照してください。
- ［NBNS リスト名］— この値は、ユーザが属するグループに対して設定されます。詳細については、「グループ ポリシー：クライアントレス タブ」を参照してください。

トラフィック ステータス

このウィンドウには、インターフェイスで監視できるトラフィック タイプのツリーが表示されます。トラフィック タイプを監視するには、そのトラフィック タイプを少なくとも 1 つのインターフェイスで有効にしておく必要があります。

次のトラフィック タイプのいずれかを［トラフィック ステータス］ツリーから選択できます。

- Netflow の上位トーカー
- QoS
- アプリケーション / プロトコル トラフィック

  このタイプは、Network-Based Application Recognition（NBAR）を使用してトラフィックを監視します。

Netflow の上位トーカー

［設定］>［インターフェイスと接続］>［インターフェイス / 接続の編集］の順にクリックして、Netflow 統計情報を少なくとも 1 つのインターフェイスで有効に設定してある場合は、Netflow 統計情報を参照できます。［トラフィック ステータス］ツリーから、［上位 N トラフィック フロー］>［上位プロトコル］または［上位 N トラフィック フロー］>［上位トーカー］（高トラフィック ソース）の順に選択します。

（注） ルータの Cisco IOS イメージが Netflow をサポートしていない場合は、［トラフィック ステータス］ツリーで Netflow の選択項目は使用できません。

上位プロトコル

このウィンドウでは、次のカラムを含む表が表示されます。

- ［プロトコル］— 検査するプロトコル。
- ［合計フロー］— そのプロトコルに関連付けられたフローの合計数。
- ［フロー / 秒］— そのプロトコルの 1 秒あたりのアクティブ フロー。
- ［パケット / フロー］— 1 フローごとに送信されるパケット数。

- ［バイト / パケット］— 送信されるパケットごとのバイト数。
- ［パケット / 秒］— 1 秒ごとに送信されるパケット数。

更新ボタン

フローに関する現在の情報でウィンドウを更新します。

上位トーカー

このウィンドウでは、次のカラムを含む表が表示されます。

- ［送信元 IP アドレス］— 上位トーカーの送信元 IP アドレス。

  送信元 IP アドレスを選択して、［送信元アドレスのフロー ステータス］で詳細な情報を確認します。
- ［パケット］— 送信元 IP アドレスから受信した合計パケット数。
- ［バイト］— 送信元 IP アドレスから受信した合計バイト数。
- ［フロー］— 送信元 IP アドレスに関連付けられたフローの数。

（注） ［設定］>［追加タスク］>［ルータ プロパティ］>［NetFlow］の順にクリックして、Netflow の上位トーカーを有効にしていない場合は、上位 10 のトーカーの統計情報が表示されます。

送信元アドレスのフロー ステータス

この表には、選択した送信元 IP アドレスに関連付けられたフローに関する次の情報が表示されます。

- ［宛先 IP アドレス］— 上位トーカーの宛先 IP アドレス。
- ［プロトコル］— 宛先 IP アドレスと交換されたパケットで使用されるプロトコル。
- ［パケット数］— 宛先 IP アドレスと交換されたパケットの数。

更新ボタン

フローに関する現在の情報でウィンドウを更新します。

QoS

［QoS ステータス］ウィンドウでは、QoS が設定されているインターフェイス上のトラフィックのパフォーマンスを監視できます（「QoS ポリシーとインターフェイスとの関連付け」参照）。また、QoS が設定されていないインターフェイスの帯域幅の利用状況や送信バイト数も監視できます。QoS インターフェイスのインバウンド トラフィックを監視する場合、統計情報はプロトコル レベルでのみ表示されます。QoS が設定されていないインターフェイスのプロトコル レベルの統計情報は、両方向のトラフィックについて収集されます。

このウィンドウでは、以下の統計情報を監視できます。

- Cisco CP が定義したトラフィック タイプの帯域幅利用状況
  - 各トラフィック タイプのクラスごとの帯域幅利用状況
  - 各クラスのプロトコルの帯域幅利用状況

  帯域幅の利用状況は Kbps 単位で表示されます。
- 各トラフィック タイプのインバウンド バイト数とアウトバウンド バイト数の合計
  - トラフィック タイプに定義されている各クラスのインバウンド バイト数とアウトバウンド バイト数
  - 各クラスのプロトコルごとのインバウンド バイト数とアウトバウンド バイト数

  値が 1,000,000 を超える場合、グラフでは、バイト数が 1,000,000 の倍数で表示されることがあります。また、値が 1,000,000,000 を超える場合は、バイト数が 1,000,000,000 の倍数で表示されることがあります。
- 各トラフィック タイプの廃棄パケットの統計情報

インターフェイス — IP/ マスク — スロット / ポート — 説明

このエリアには、QoS ポリシーが関連付けられているインターフェイス、その IP アドレスとサブネット マスク、スロット / ポート情報（ある場合）、および説明のリストが表示されます。

このリストから監視するインターフェイスを選択します。

表示間隔

統計情報を収集する間隔を次の中から選択します。

- ［今すぐ］—［監視の開始］をクリックすると統計情報が収集されます。
- ［1 分ごと］—［監視の開始］をクリックすると統計情報が収集され、1 分ごとに更新されます。
- ［5 分ごと］—［監視の開始］をクリックすると統計情報が収集され、5 分ごとに更新されます。
- ［1 時間ごと］—［監視の開始］をクリックすると統計情報が収集され、1 時間ごとに更新されます。

監視の開始

QoS 統計情報の監視を開始する場合にクリックします。

監視に関する QoS パラメータの選択

監視するトラフィックの方向と統計情報のタイプを選択します。

方向

［入力］または［出力］をクリックします。

統計情報

次のいずれかを選択します。

- 帯域幅
- バイト
- 廃棄パケット

すべてのトラフィック — リアルタイム — ビジネスクリティカル — 通常

Cisco CP では、選択した統計情報のタイプに基づいて、すべてのトラフィック クラスの統計情報が棒グラフで表示されます。十分な統計情報が存在しないトラフィック タイプについては、棒グラフではなく、メッセージが表示されます。

QoS ポリシーとインターフェイスとの関連付け

ステップ 1　［インターフェイスと接続］>［インターフェイス / 接続の編集］の順にクリックします。

ステップ 2　［インターフェイス リスト］から、QoS ポリシーと関連付けるインターフェイスを選択します。

ステップ 3　［編集］ボタンをクリックします。

ステップ 4　［アプリケーション サービス］タブをクリックします。

ステップ 5　［インバウンド］ドロップダウン リストで QoS ポリシーを選択し、インターフェイスのインバウンド トラフィックに関連付けます。

ステップ 6　［アウトウンド］ドロップダウン リストで QoS ポリシーを選択し、インターフェイスのアウトバウンド トラフィックに関連付けます。

アプリケーション / プロトコル トラフィック

このウィンドウでは、プロトコルおよびアプリケーション検出機能である Network-Based Application Recognition（NBAR）を使用して、アプリケーションおよびプロトコル トラフィックを監視できます。NBAR を使用してパケットを分類し、特定のインターフェイスを介したネットワーク トラフィックをさらに効率的に処理できるようにします。

（注）　ルータの Cisco IOS イメージが NBAR をサポートしていない場合、このステータス ウィンドウは使用できません。

NBAR の有効化

特定のインターフェイスに対する NBAR のステータスを表示するには、まずそのインターフェイスで NBAR を有効化する必要があります。NBAR を有効化するには、次の手順に従ってください。

ステップ 1　［インターフェイスと接続］>［インターフェイス / 接続の編集］の順にクリックします。

ステップ 2　［インターフェイス リスト］から NBAR を有効化するインターフェイスを選択します。

ステップ 3　［編集］ボタンをクリックします。

ステップ 4　［アプリケーション サービス］タブをクリックします。

ステップ 5　［NBAR］チェック ボックスを選択します。

NBAR ステータス

NBAR ステータス テーブルには、［インターフェイスの選択］ドロップダウン リストから選択したインターフェイスに対する次の統計情報が表示されます。

- ［入力パケット カウント］— 選択したインターフェイスに受信と表示されたプロトコルのパケット数。
- ［出力パケット カウント］— 選択したインターフェイスから送信と表示されたプロトコルのパケット数。
- ［ビット レート（bps）］— インターフェイスを通過するトラフィックの速度（1 秒あたりのビット数）。

NAC ステータス

NAC がルータ上に設定されている場合は、NAC が設定されているルータ、インターフェイス上の NAC セッション、および選択されたインターフェイス上の NAC 統計情報に関するスナップショット情報を、Cisco CP によって表示できます。

このウィンドウの先頭の行には、アクティブな NAC セッションの数、初期化中の NAC セッションの数、およびすべてのアクティブで初期化中の NAC セッションをクリアできるボタンが表示されます。

ウィンドウには、関連付けられた NAC ポリシーがあるインターフェイスが表示されます。

```
FastEthernet0/0    10.10.15.1/255.255.255.0   0
```

インターフェイス エントリをクリックすると、そのインターフェイスのサブネットのホストにインストールされているポスチャ エージェントから返される情報が表示されます。インターフェイス情報の例は次のとおりです。

```
10.10.10.5     Remote EAP Policy     Infected       12
```

10.10.10.1 は、ホストの IP アドレスです。Remote EAP Policy は、有効な認証ポリシーのタイプです。ホストの現在のポスチャは Infected で、ホストがアドミッション コントロール プロセスを完了してから 12 分経っています。

（注） 選択されたサブネットのホストからポスチャ情報が返されない場合は、ウィンドウのこのエリアには何も表示されません。

認証タイプは次のとおりです。

- **Local Exception Policy —** ルータ上に設定された例外ポリシーを使用してホストを検証します。
- **Remote EAP Policy —** ポスチャがホストによって返され、ACS サーバによって割り当てられた例外ポリシーが使用されます。

- **Remote Generic Access Policy —** ホストにはポスチャ エージェントがインストールされておらず、ACS サーバによってエージェントレス ホスト ポリシーが割り当てられます。

ホストのポスチャ エージェントからは、次のポスチャ トークンが返される場合があります。

- **Healthy —** ホストは既知のウィルスに感染しておらず、最新のウィルス定義ファイルがインストールされています。
- **Checkup —** ポスチャ エージェントは、最新のウィルス定義ファイルがインストールされているかどうかを確認しています。
- **Quarantine —** ホストには、最新のウィルス定義ファイルがインストールされていません。ユーザは、最新のウィルス定義ファイルをダウンロードする手順を含む、指定された修復サイトに移動します。
- **Infected —** ホストは既知のウィルスに感染しています。ユーザは、ウィルス定義ファイルの更新情報を取得する修復サイトに移動します。
- **Unknown —** ホストのポスチャが不明です。

ロギング

Cisco CP には、次のログが用意されています。

- シスログ（Syslog）— ルータのログ。
- ファイアウォール ログ — ルータにファイアウォールが設定されている場合、このログにはそのファイアウォールによって生成されたエントリが記録されます。
- アプリケーション セキュリティ ログ — ルータにアプリケーション ファイアウォールが設定されている場合、このログにはそのファイアウォールによって生成されたエントリが記録されます。
- SDEE メッセージ ログ — ルータに SDEE が設定されている場合、このログには SDEE メッセージが記録されます。

ログを開くには、そのログ名が記載されたタブをクリックします。

シスログ（Syslog）

ルータには、重大度別に分類したイベントのログが格納されます。これは、UNIX のシスログ（syslog）サービスのログと同様です。

（注） ログ メッセージがシスログ（syslog）サーバに転送されていても、表示されるのはルータのログです。

ロギング バッファ

ロギング バッファとシスログ（syslog）ロギングが有効になっているかどうかが表示されます。両方が有効な場合には「有効」というテキストが表示されます。ロギング バッファが有効な場合、ログ メッセージの保持のため一定量のメモリが確保されます。このフィールドの設定は、ルータがリブートされると保持されません。これらのフィールドの設定がデフォルト設定の場合、ロギング バッファ用に 4,096 バイトのメモリが使用されます。

ロギング ホスト

ログ メッセージが転送されているシスログ（syslog）ホストの IP アドレスが表示されます。このフィールドは読み取り専用です。シスログ（syslog）ホストの IP アドレスを設定するには、［追加タスク］>［ルータ プロパティ］>［ロギング］を選択して表示されるウィンドウを使用します。

ロギング レベル（バッファ）

ルータ上のバッファに対して設定されているロギング レベルが表示されます。

ログ内のメッセージ数

ルータのログに保存されているメッセージの合計数が表示されます。

表示するロギング レベルの選択

このフィールドでは、ログ内のメッセージのうちどの重大度レベルのものを表示するかを選択します。このフィールドの設定を変更すると、ログ メッセージのリストが更新されます。

ログ

［表示するロギング レベルの選択］フィールドで指定した重大度レベルのメッセージがすべて表示されます。ログ イベントには次の情報が含まれています。

- ［重大度］カラム

  ログ イベントの重大度が表示されます。重大度は 1 ～ 7 の数値で表されます。数値が小さいほどイベントの重大度は高くなります。各重大度レベルの説明は次のとおりです。

  - 0 - 緊急

    システムが使用不可です。

  - 1 - アラート

    直ちに対処が必要です。

  - 2 - 重大

    重大な状態が発生しました。

- 3 - エラー
  エラー状態が発生しました。
- 4 - 警告
  警告対象の状態が発生しました。
- 5 - 通知
  特別な意味のある状態が発生しましたが、異常ではありません。
- 6 - 情報
  単なる情報メッセージです。
- 7 - デバッグ
  デバッグ用のメッセージです。

- ［時刻］カラム
  ログ イベントが発生した時刻が表示されます。
- ［説明］カラム
  ログ イベントの説明が表示されます。

更新ボタン

ログの最新の詳細情報と最新のログ エントリが反映されるようにウィンドウを更新します。

ログをクリアするボタン

ルータ上のログ バッファからすべてのメッセージが消去されます。

検索ボタン

［検索］ウィンドウを開きます。［検索］ウィンドウで、［検索］フィールドにテキストを入力して［検索］ボタンをクリックし、検索テキストを含むすべてのエントリを表示します。検索では、大文字と小文字が区別されません。

ファイアウォール ログ

このウィンドウの上部に表示されたログ エントリは、ファイアウォールにより生成されたログ メッセージに基づいています。ファイアウォールによってログ エントリが生成されるようにするには、アクセス ルールが呼び出されたときにログ メッセージが生成されるように、個々のアクセス ルールを設定する必要があります。ログ メッセージが生成されるようにアクセス ルールを設定する手順については、ヘルプ トピック「ファイアウォール上のアクティビティを表示する方法」を参照してください。

ファイアウォールのログ エントリが収集されるようにするには、ルータのロギングを設定する必要があります。[追加タスク] > [ルータ プロパティ] > [ロギング] を選択します。[編集] をクリックして、ロギングを設定します。ファイアウォールのロギング メッセージを取得するには、デバッグ（7）のロギング レベルを設定する必要があります。

ファイアウォール ログ

ファイアウォールによって拒否された接続試行のログを保持するようにルータを設定している場合は、ファイアウォール ログが表示されます。

ファイアウォールで拒否した試行回数

ファイアウォールで拒否した接続試行の回数が表示されます。

ファイアウォールで拒否した試行表

ファイアウォールで拒否した接続試行のリストが表示されます。この表には、次のカラムがあります。

- [時刻] カラム

  拒否した接続試行のそれぞれの発生時刻が表示されます。

- [説明] カラム

  拒否された試行について、ログ名、アクセス ルール名または番号、サービス、送信元アドレス、宛先アドレス、およびパケット数が表示されます。その例を次に示します。

```
%SEC-6-IPACCESSLOGDP: list 100 denied icmp 171.71.225.148->10.77.158.140 (0/0), 3 packets
```

更新ボタン

ルータに対してポーリングを行い、画面に表示されている情報を最新の情報で更新します。

検索ボタン

［検索］ウィンドウを開きます。［検索］メニューから検索のタイプを選択し、［検索］フィールドに適切なテキストを入力し、［検索］ボタンをクリックして一致するログ エントリを表示します。

検索のタイプは、次のとおりです。

- ［送信元 IP アドレス］— 攻撃元の IP アドレス。
  IP アドレスの一部を入力するだけでもかまいません。
- ［送信先 IP アドレス］— 攻撃先の IP アドレス。
  IP アドレスの一部を入力するだけでもかまいません。
- ［プロトコル］— 攻撃で使用されたネットワーク プロトコル。
- ［テキスト］— ログ エントリ内で検出される任意のテキスト。

検索では、大文字と小文字が*区別されません*。

上位攻撃の表示

［表示］ドロップダウン メニューから次の方法のいずれかを選択して、上位攻撃に関する情報を表示します。

- ［上位攻撃ポート］— 送信先ポートによる上位攻撃。
- ［上位攻撃者］— 攻撃者の IP アドレスによる上位攻撃。

［表示］ドロップダウン メニューの下にある上位攻撃の表には、上位攻撃エントリが表示されます。［表示］ドロップダウン メニューから［上位攻撃ポート］を選択した場合、上位攻撃の表には次のカラムを持つエントリが表示されます。

- ［ポート番号］— 送信先のポート。
- ［攻撃数］— 送信先ポートに対する攻撃の数。
- ［拒否されたパケット数］— 送信先ポートへのアクセスを拒否されたパケットの数。

- ［詳細の表示］— 選択したポートに対する攻撃の完全なログを表示するウィンドウを開くリンク。

［表示］ドロップダウン メニューから［上位攻撃者］を選択した場合、上位攻撃の表には次のカラムを持つエントリが表示されます。

- ［攻撃者の IP アドレス］— 攻撃が発信される IP アドレス。
- ［攻撃数］— その IP アドレスから送信される攻撃の数。
- ［拒否されたパケット数］— IP アドレスから発信され、アクセスを拒否されたパケットの数。
- ［詳細の表示］— 選択した IP アドレスから発信された攻撃の完全なログを表示するウィンドウを開くリンク。

「管理者以外のビュー」ユーザ アカウントでのファイアウォール監視

ファイアウォールを監視するには、ルータでバッファへのロギングが有効になっている必要があります。バッファへのロギングが有効になっていない場合は、管理者ビュー アカウントまたは非ビュー ベースの権限レベル 15 のユーザ アカウントを使用して Cisco CP にログインし、ロギングを設定します。

Cisco CP でロギングを設定するには、［追加タスク］>［ルータ プロパティ］>［ロギング］を選択します。

アプリケーション セキュリティ ログ

ロギングが有効になっており、指定したアプリケーションまたはプロトコルからのトラフィックをルータが受信したときに、アラームが生成されるように指定した場合、これらのアラームがこのウィンドウから表示可能なログに収集されます。

アプリケーション セキュリティのログ エントリが収集されるようにするには、ルータのロギングを設定する必要があります。［追加タスク］>［ルータ プロパティ］>［ロギング］を選択します。［編集］をクリックして、ロギングを設定します。ファイアウォールのロギング メッセージを取得するには、**情報（6）**以上のロギング レベルを設定する必要があります。すでに**デバッグ（7）**のロギングを設定している場合、ログにはアプリケーション セキュリティのログ メッセージが含まれます。

次はログ テキストの例です。

```
*Sep  8 12:23:49.914: %FW-6-DROP_PKT: Dropping im-yahoo pkt
128.107.252.142:1481 => 216.155.193.139:5050
*Sep  8 12:24:22.762: %FW-6-DROP_PKT: Dropping im-aol pkt
128.107.252.142:1505 => 205.188.153.121:5190
*Sep  8 12:26:02.090: %FW-6-DROP_PKT: Dropping im-msn pkt
128.107.252.142:1541 => 65.54.239.80:1863
*Sep  8 11:42:10.959: %APPFW-4-HTTP_PORT_MISUSE_IM: Sig:10006 HTTP
Instant Messenger detected - Reset - Yahoo Messenger from
10.10.10.2:1334 to 216.155.194.191:80
*Sep  8 12:27:54.610: %APPFW-4-HTTP_STRICT_PROTOCOL: Sig:15 HTTP
protocol violation detected - Reset -  HTTP Protocol not detected from
10.10.10.3:1583 to 66.218.75.184:80
*Sep  8 12:26:14.866: %FW-6-SESS_AUDIT_TRAIL_START: Start im-yahoo
session: initiator (10.10.10.3:1548) -- responder (66.163.172.82:5050)
*Sep  8 12:26:15.370: %FW-6-SESS_AUDIT_TRAIL: Stop im-yahoo session:
initiator (10.10.10.3:1548) sent 0 bytes -- responder
(66.163.172.82:5050) sent 0 bytes
*Sep  8 12:24:44.490: %FW-6-SESS_AUDIT_TRAIL: Stop im-msn session:
initiator (10.10.10.3:1299) sent 1543 bytes -- responder
(207.46.2.74:1863) sent 2577 bytes
*Sep  8  11:42:01.323: %APPFW-6-IM_MSN_SESSION: im-msn un-recognized
service session initiator 14.1.0.1:2000 sends 1364 bytes to responder
207.46.108.19:1863
*Sep  8  11:42:01.323: %APPFW-6-IM_AOL_SESSION: im-aol text-chat
service session initiator 14.1.0.1:2009 sends 100 bytes to responder
216.155.193.184:5050
```

更新ボタン

ログの最新の詳細情報と最新のログ エントリが反映されるように画面を更新します。

検索ボタン

［検索］ウィンドウを開きます。［検索］ウィンドウで、［検索］フィールドにテキストを入力して［検索］ボタンをクリックし、検索テキストを含むすべてのエントリを表示します。検索では、大文字と小文字が*区別されません*。

SDEE メッセージ ログ

このウィンドウには、ルータが受信した SDEE メッセージのリストが表示されます。SDEE メッセージは、IPS 設定に変更があったときに生成されます。

SDEE メッセージ

表示する SDEE メッセージ タイプを選択します。

- ［すべて］― エラー、ステータス、アラートの各 SDEE メッセージが表示されます。
- ［エラー］－ SDEE エラー メッセージだけが表示されます。
- ［ステータス］－ SDEE ステータス メッセージだけが表示されます。
- ［アラート］－ SDEE アラート メッセージだけが表示されます。

更新ボタン

新しい SDEE メッセージがあるかどうかチェックする場合にクリックします。

検索ボタン

［検索］ウィンドウを開きます。［検索］メニューから検索のタイプを選択し、［検索］フィールドに適切なテキストを入力し、［検索］ボタンをクリックして一致するログ エントリを表示します。

検索のタイプは、次のとおりです。

- 送信元 IP アドレス
- 宛先 IP アドレス
- テキスト

検索では、大文字と小文字が*区別されません*。

時刻

メッセージを受信した時刻です。

タイプ

［エラー］、［ステータス］、および［アラート］があります。表示される SDEE メッセージについては、「SDEE メッセージ テキスト」を参照してください。

説明

該当する説明です。

IPS ステータス

このウィンドウは、IPS バージョン 4.x 以前をサポートする Cisco IOS イメージがルータで使用されている場合に表示されます。このウィンドウには、シグニチャのタイプ別に分類された IPS シグニチャ統計情報の表が表示されます。次の統計情報が表示されます。

- ［シグニチャ ID］— 数字で表されるシグニチャの ID。
- ［説明］— シグニチャの説明。
- ［リスク評価］— 0 ～ 100 の範囲の値であり、ネットワーク上の特定のイベントに関連付けられたリスクを数値的に表します。
- ［アクション］— パケットがシグニチャと一致した場合に実行されるアクション。
- ［送信元 IP アドレス］— パケットの発信元ホストの IP アドレス。
- ［宛先 IP アドレス］— パケットの宛先ホストの IP アドレス。
- ［ヒット］— 一致するパケットの数。
- ［ドロップ カウント］— 一致するパケットのうち破棄された数。

シグニチャを並べ替えるには、並べ替えるシグニチャの統計情報名が表示されたカラムの先頭をクリックします。

（注） シグニチャを並べ替えると、そのシグニチャはタイプ別に分類されなくなります。シグニチャをタイプ別に分類された状態に復元するには、［更新］ボタンをクリックします。

アクティブなシグニチャの総数

存在するシグニチャのうち、ルータでアクティブになっているシグニチャの総数を表示します。

非アクティブなシグニチャの総数

存在するシグニチャのうち、ルータで非アクティブになっているシグニチャの総数を表示します。

更新ボタン

最新のシグニチャ統計情報を確認して追加する場合にクリックします。

クリア ボタン

すべてのシグニチャ統計情報のカウンタを 0 に設定する場合にクリックします。

SDEE ログ

クリックすると、SDEE メッセージが表示されます。これらのメッセージは、[監視]>[ロギング]>[SDEE メッセージ ログ]を選択して表示することもできます。

IPS シグニチャ統計情報

このウィンドウは、ルータが IOS IPS 5.x 設定を使用している場合に表示されます。IOS IPS 設定で有効にしたシグニチャごとに統計情報が表示されます。ウィンドウ上部には、シグニチャ設定のスナップショットを示すシグニチャ合計が表示されます。以下の合計値が表示されます。

- シグニチャの合計数
- 有効にしたシグニチャの合計数
- リタイアにしたシグニチャの合計数
- コンパイルしたシグニチャの合計数

更新ボタンおよびクリアボタン

最新のシグニチャ統計情報を確認し、反映させるには、［更新］をクリックします。すべてのシグニチャ統計カウンタを 0 に設定するには［クリア］をクリックします。

SDEE ログ

クリックすると、SDEE メッセージが表示されます。これらのメッセージは、［監視］>［ロギング］>［SDEE メッセージ ログ］を選択して表示することもできます。

シグニチャ リスト エリア

すべてのシグニチャのシグニチャ ID、説明、ヒット数、および廃棄数が表示されます。シグニチャに一致するパケットが到達した場合は、その送信元 IP アドレスおよび宛先 IP アドレスも表示されます。

IPS Alert Statistics

［IPS Alert Statistics］ウィンドウには、見やすいように色分けしたアラート統計情報が表示されます。画面上部には、表示に使用される各色を説明する凡例が表示されます。

色	説明
赤	アラートを生成したイベントは、70 ～ 100 の高いリスク評価（RR）値を持ちます。
マゼンタ	アラートを生成したイベントは、40 ～ 69 の中程度のリスク評価（RR）値を持ちます。
青	アラートを生成したイベントは、0 ～ 39 の低いリスク評価（RR）値を持ちます。

カラムの見出しをクリックすると、このパラメータ値を基準に表示内容を並べ替えることができます。たとえば［シグニチャ ID］の見出しをクリックすると、シグニチャ ID を数値の昇順または降順で並べ替えることができます。次のリストは、各カラムの説明を示します。

- ［シグニチャ ID］— 数字で表されるシグニチャの ID。
- ［説明］— シグニチャの説明。
- ［リスク評価］— 0 ～ 100 の範囲の値であり、ネットワーク上の特定のイベントに関連付けられたリスクを数値的に表します
- ［イベント アクション］— シグニチャに一致するイベントが発生したときに IOS IPS が実行するアクション。
- ［送信元 IP アドレス］— パケットの発信元の IP アドレス。
- ［宛先 IP アドレス］— パケットの宛先の IP アドレス。悪意あるパケットの場合は、この宛先 IP アドレスはターゲットとみなされます。
- ［ヒット］— 一致するパケットの数。
- ［ドロップ カウント］— 一致するパケットのうち破棄された数。
- ［エンジン］— このシグニチャに関連付けられているシグニチャ エンジン。

802.1x 認証ステータス

インターフェイスの 802.1x 認証エリア

インターフェイス

802.1x 認証

再認証

802.1x クライアント エリア

クライアントの MAC アドレス

認証ステータス

インターフェイス