CHAPTER 3

異常ベースの検出

ここでは、Cisco SCE プラットフォームを使用した異常ベースの検出について説明します。

概要

最も包括的な脅威検出モジュールは異常検出モジュールです。これは、システムが認識しているすべての IP アドレスとの間で、成功した接続（TCP の場合は正常に確立された接続、それ以外は双方向接続）のレートと、失敗した接続（単方向接続、「不審」接続とも呼ばれる）のレートをモニタします。次の条件のいずれかに合致すると、異常ベースの検出がトリガーされます。

- 合計接続レートが定義済みしきい値を超える

  または、
- 不審接続レートが定義済みしきい値を超え、さらに不審接続とそれ以外の接続の比率が定義済みしきい値を超える

比率メトリックは強力な悪質アクティビティ インジケータであり、信頼できる悪質アクティビティ識別子としてレート修飾子とともに動作します。

異常検出は、以降で説明するように、異常の方向性に基づいて 3 つのカテゴリに分けられます。3 通りの方式で使用されている概念は同一ですが、異常についてモニタされるエンドポイントのロールが異なります。

スキャン / スイープ / 攻撃は、悪質アクティビティのカテゴリの 1 つで、IP アドレスからの接続レートの異常検出に基づいています（モジュールは、関連する宛先 IP アドレスを無視します）。異常は、上記で指定した条件に基づいて検出され、次のいずれかを示します。

- 攻撃 — ホストが別のホストの攻撃に関与しています。
- スイープ — ホストが脆弱なホストを検索するためにネットワークをスイープしています（これは、ネットワーク ワームに対抗する通常のアクティビティです）。
- スキャン — ホストが別のホストのポートをスキャンし、どのサービスが使用され、どのポートが潜在的に脆弱であるかを検出しています。

DoS 攻撃は、1 組のホスト間の接続レートの異常（一方のホストが他方を攻撃している）に基づいて検出されます。単一の攻撃または大規模な DDoS 攻撃の一部である可能性があります。

DDoS 攻撃は、1 つの IP アドレスへの接続レートの異常に基づいて検出されます（モジュールは、関連する送信元 IP アドレスを無視します）。この異常は、その IP アドレスが攻撃を受けていることを示しています。攻撃は、単一 IP アドレス（DoS）または複数の IP アドレス（DDoS）によって行われる可能性があります。

複数のタイプの異常に備え、それぞれに対して検出しきい値と対処方法を柔軟に定義できます。

- 異常検出（サブスクライバ / ネットワーク）
- プロトコル（TCP/UDP/ICMP/ その他）
- TCP/UDP のポートの一意性 — 異常しきい値を単一ポートに適用するか、ポートの集合に適用するかを指定します。

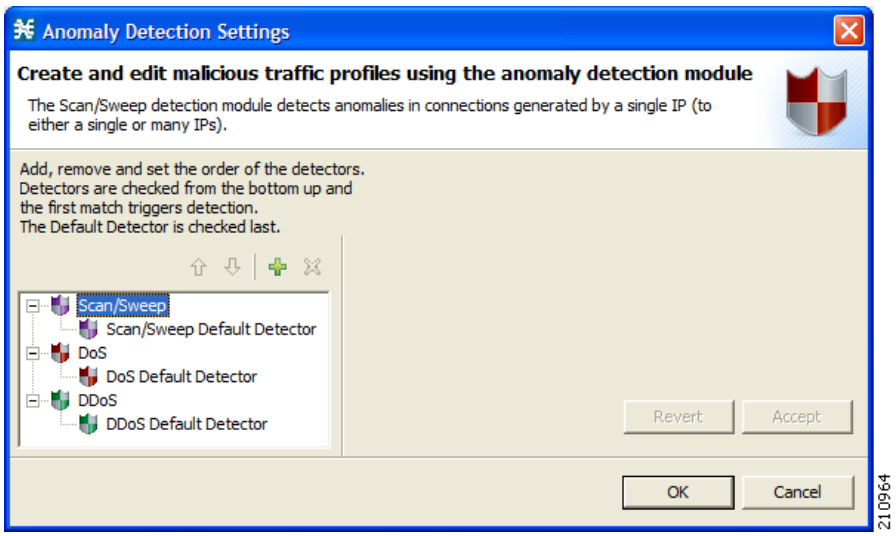
レポータ内の悪質トラフィック レポート ファミリには、悪質なアクティビティのさまざまな側面をモニタできるレポートが含まれています。

異常検出の設定

異常検出の設定画面には、各種ディテクタの「ツリー」が表示されます。ツリーは、3 つの異常カテゴリから構成されます。

設定の観点から、スキャン / スイープ、DoS、DDoS の 3 つのカテゴリに分類されています。

図 3-1　異常検出の設定



異常検出の設定の一般的な概念

- ディテクタの構造（p.3-3）
- 検出しきい値の設定（p.3-4）
- 対処方法の設定（p.3-5）
- デフォルトのディテクタ（p.3-6）
- 追加のディテクタ（p.3-6）

ディテクタの構造

以下で、異常検出で使用される用語について説明します。広範囲にわたり「関連（している）」という言い方が使われていますが、意味は、各異常のセマンティックによって異なり、各異常カテゴリ（スキャン / スイープ / 攻撃、DoS、DDoS）固有の説明に中で解説されています。

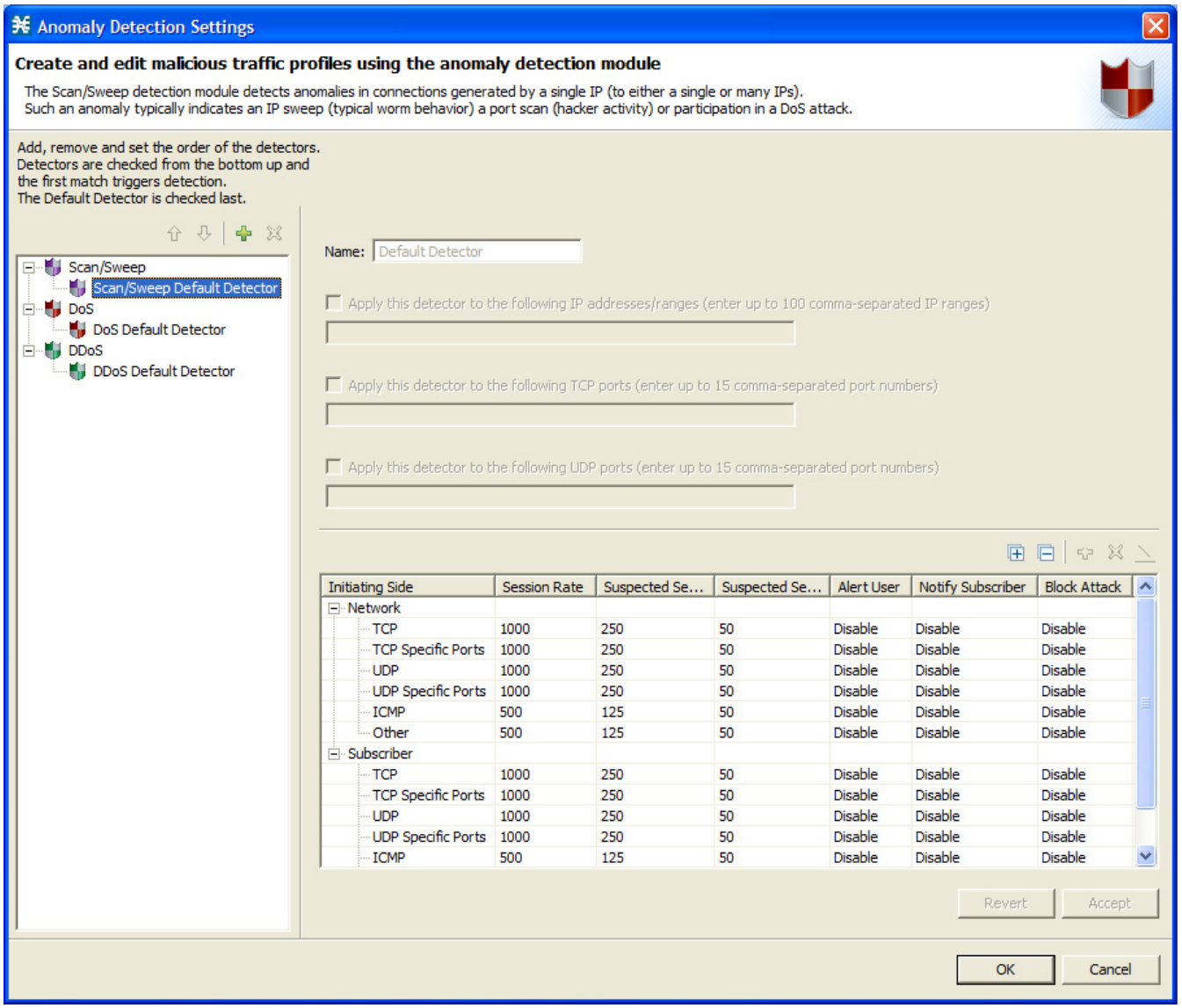
ディテクタ階層の第 1 レベルには、サブスクライバとネットワークの 2 つのサブカテゴリがあります。サブスクライバ サブカテゴリは、サブスクライバ ポート上の IP アドレス関連の悪質トラフィックを示します。ネットワーク サブカテゴリは、ネットワーク ポート上の IP アドレス関連の悪質トラフィックを示します。

これらのサブカテゴリを基にして、オペレータはサブスクライバ側またはネットワーク側のどちらかの異常に対処できます。

各サブカテゴリは、さらに次の 6 つのサブカテゴリに細分化されます。

- TCP — 任意の TCP 宛先ポート上のホスト関連の接続レートの異常を示します。すべての TCP ポート上の接続の集約レートは、このルールのマッチング対象となります。
- TCP 固有 — 特定の TCP 宛先ポート上のホスト関連の接続レートの異常を示します。たとえば、ポート 80 の特定ホストに関連する接続レートはこのルールのマッチング対象であり、同様に、TCP ポート 23、25、110（および任意の指定された TCP ポート）ごとのホスト関連の接続レートもマッチング対象となります。
- UDP — 任意の UDP 宛先ポート上のホスト関連の接続レートの異常を示します。すべての UDP ポート上の接続の集約レートは、このルールのマッチング対象となります。
- UDP 固有 — 特定の UDP 宛先ポート上のホスト関連の接続レートの異常を示します。たとえば、ポート 53 のホストに関連する接続レートはこのルールのマッチング対象となり、同様に、各 UDP ポート上でホストによって生成された接続レートもマッチング対象になります。
- ICMP — ICMP を使用するホストに関連する接続レートの異常を示します。
- その他 — TCP/UDP/ICMP 以外のプロトコルを使用するホストに関連する接続レートの異常を示します。

図 3-2　ディテクタの構造



検出しきい値の設定

特定の検出パラメータと関連する対処方法の設定は、サブカテゴリごとに実行されます。

各異常カテゴリで設定可能な検出パラメータは、次のとおりです。

- セッション レート — セッション レートしきい値（IP アドレスごとのセッション数 / 秒）を示します。このしきい値を超えると、このタイプの異常がトリガーされます。

  たとえば、TCP 異常のセッション レートとして値 1000 を設定すると、（任意のポート上で）ホストから 1000 TCP セッション / 秒のレートが検出された場合に、異常がトリガーされます。

- 不審セッション レート — 不審セッション レートしきい値（不審セッション数 / 秒）を示します。このしきい値を超えると、異常回線項目がトリガーされます。

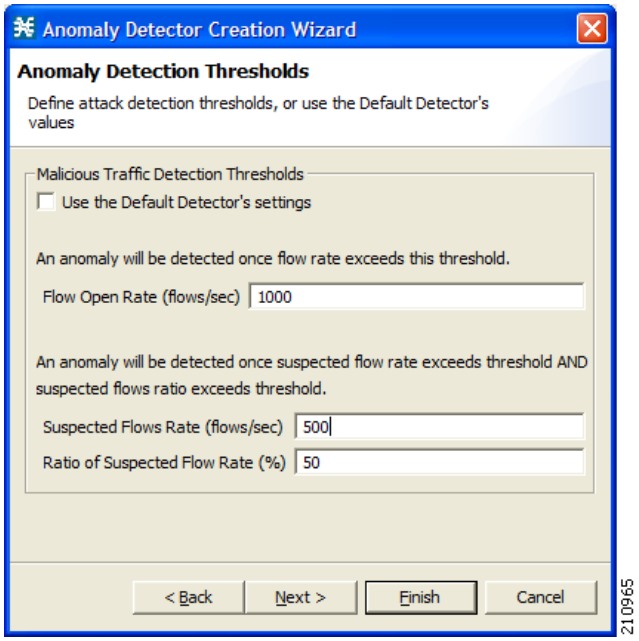
  不審セッションは、適切に確立されなかった TCP セッション、または他のプロトコル（UDP/ICMP/ その他）の単方向セッションです。

このパラメータは、不審セッション比率と組み合せて、トラフィック異常のインジケータとして使用されます。セッションレートが比較的高い場合、つまり通常見られないほど大きい数値の場合は、悪質なアクティビティを示しています。

たとえば、TCP 異常の不審セッション数 / 秒として値 1000 を設定すると、（任意のポート上で）ホストから 1000 TCP 不審セッション / 秒が検出され、さらに不審接続比率が定義済みしきい値を超えた場合に、異常がトリガーされます。

- 不審セッション比率 — 不審セッション レートと合計セッション レートの比率。比率が高い場合は、大量の「不審」セッションを示しており、悪質なアクティビティが発生している可能性があります。

図 3-3　検出しきい値の設定



対処方法の設定

各異常サブカテゴリには、検出時の対処方法を定義するオプションも含まれています。

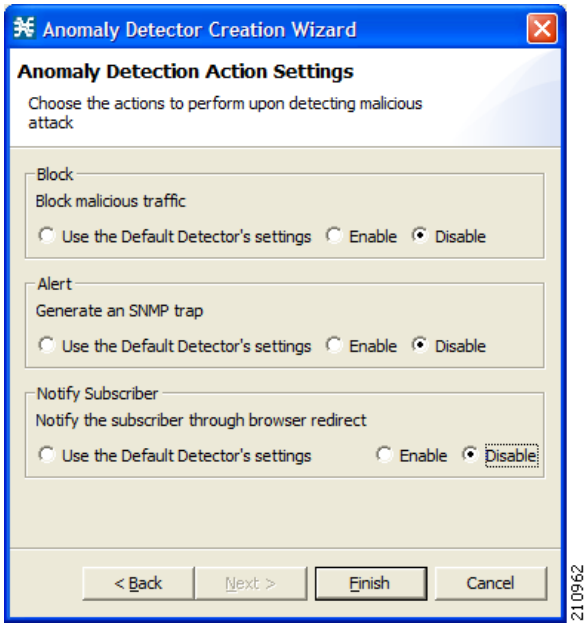
異常サブカテゴリごとに、デバイス上のログ ファイルへのロギング、および SCE Raw Data Record（RDR）を使用した Collection Manager Database へのロギングを設定することはできません。悪質トラフィックの RDR を有効化または無効化するには、Configuration メニューから RDR 設定値を選択します。

独立しているが相互に排他的でない 3 つの対処方法があります。これらは項目ごとに設定できます。

- ユーザ アラート — 該当する攻撃の開始と終了を示す SNMP トラップを生成します（詳細については Pcube 専用 MIB を参照してください）。
- サブスクライバ通知 — サブスクライバのブラウジング セッションをキャプティブ ポータルにリダイレクトし、悪質なアクティビティについてサブスクライバに通知します。サブスクライバ通知を設定するには、Configuration メニューから Subscriber Notifications を選択し、さらに Network Attack Notification を選択します。サブスクライバ通知オプションの詳細については、『*Cisco Service Control Application for Broadband User Guide*』を参照してください。

- ブロック　— 関連セッションをブロックします。ブロックは、異常をトリガーした悪質トラフィックの仕様に基づいて実行されます。たとえば、検出された異常がサブスクライバ側からのポートを限定しない TCP スキャンである場合は、そのサブスクライバ側から開始されたすべての TCP セッションがブロックされます。ブロックは、異常が見られなくなるまで持続します（異常がなくなったかどうかを確認するため、ブロックは断続的に解除されます）。異常に対してサブスクライバ通知を有効にした場合、ブラウジングに関連するポート（デフォルトでは、TCP ポート 80）にはブロックが適用されない点に注意してください。

図 3-4　異常検出の対処方法の設定



デフォルトのディテクタ

悪質トラフィックの各カテゴリに削除できないデフォルトのディテクタがあります。デフォルトのディテクタのしきい値と対処方法には、工場出荷時にデフォルト値が設定されています。

追加のディテクタ

悪質トラフィックの各カテゴリ（スキャン / スイープ、DoS、DDoS）で、デフォルト ディテクタの下に追加のディテクタを定義できます。3 つのカテゴリの合計で最大 100 ディテクタまで追加可能です。

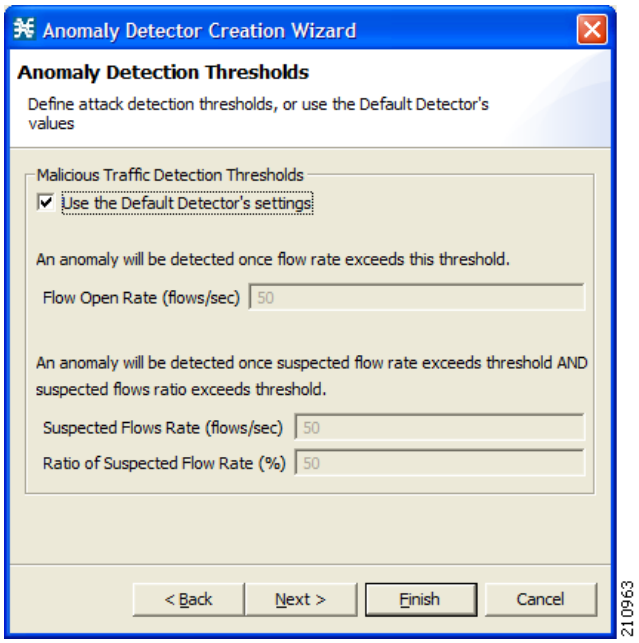
ディテクタは、IP アドレス リスト、UDP ポート リスト、TCP ポート リスト、または 3 つの組み合せに適用されます。ディテクタにはそれぞれ、このリストに合致する異常に適用される異なるしきい値または異なる対処方法、もしくはその両方を含める必要があります。

例として、特定のポートではなく 1 つの IP アドレスに対応する DDoS ディテクタを定義したり、特定のポートの攻撃をモニタする別のディテクタ（DNS ディテクタ、SMTP ディテクタなど）を定義したりできます。また、別の例として、特定のワームを対象とし、特定のポート リストを含むディテクタを定義することもできます。

追加のディテクタを作成し、複数の異常サブカテゴリに適用することができます。たとえば、特定の IP リストに対応する DDoS ディテクタを作成し、それをサブスクライバ側からの特定のポート攻撃のみに適用することができます。新しいディテクタは、DDoS の「潜在する」サブカテゴリをすべてカバーする必要はありません。

新しい異常サブカテゴリを作成した場合は、実行する対処方法を定義する必要がありますが、カスタム検出しきい値を使用することもできれば、デフォルト ディテクタの検出しきい値を継承することもできます。

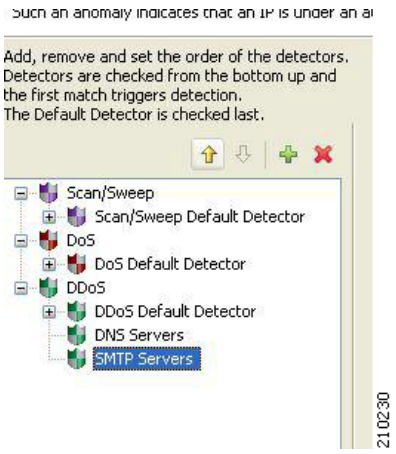
図 3-5　異常ディテクタ ウィザード



異常は、1 つディテクタによってのみトリガーされます。検出は、リストの下から上へ順次実行され、IP/ ポート リストの仕様とともに異常しきい値に最初に「合致」したディテクタによって実行する対処方法が決まります。

ユーザは、異常ツリー ウィンドウ内で上矢印および下矢印を使用して、各カテゴリ内のディテクタを必要な順番に並び替える必要があります。

図 3-6　異常ツリー ウィンドウ



スキャン / スイープ ディテクタ

スキャン / スイープ ディテクタは、ホストによって生成された接続の異常を検出します。概要の項で説明したとおり、これらの異常には、合計接続レート、不審接続レート、および不審接続比率があります。

ホストによって生成された不審接続の比率が高い（最小レートを超える）場合は、通常、ネットワークをスイープして脆弱なホストを検出することで繁殖を試みるワームの存在を示しています。脆弱性を持つ特定のポートで異常が検出された場合、ワームの存在はさらに明確となります。この場合、通常は、TCP/UDP 固有の異常がトリガーされます。

さらに、このカテゴリには、ホストによって実行されたポート スキャンと攻撃も含まれます。ポート スキャンは、通常、不審接続比率が高くなるという特徴を備えています。一方、ホスト攻撃は、通常接続または不審接続のどちらかになります。どちらのタイプの悪質トラフィックも、非ポート固有の異常ディテクタで検出できます。

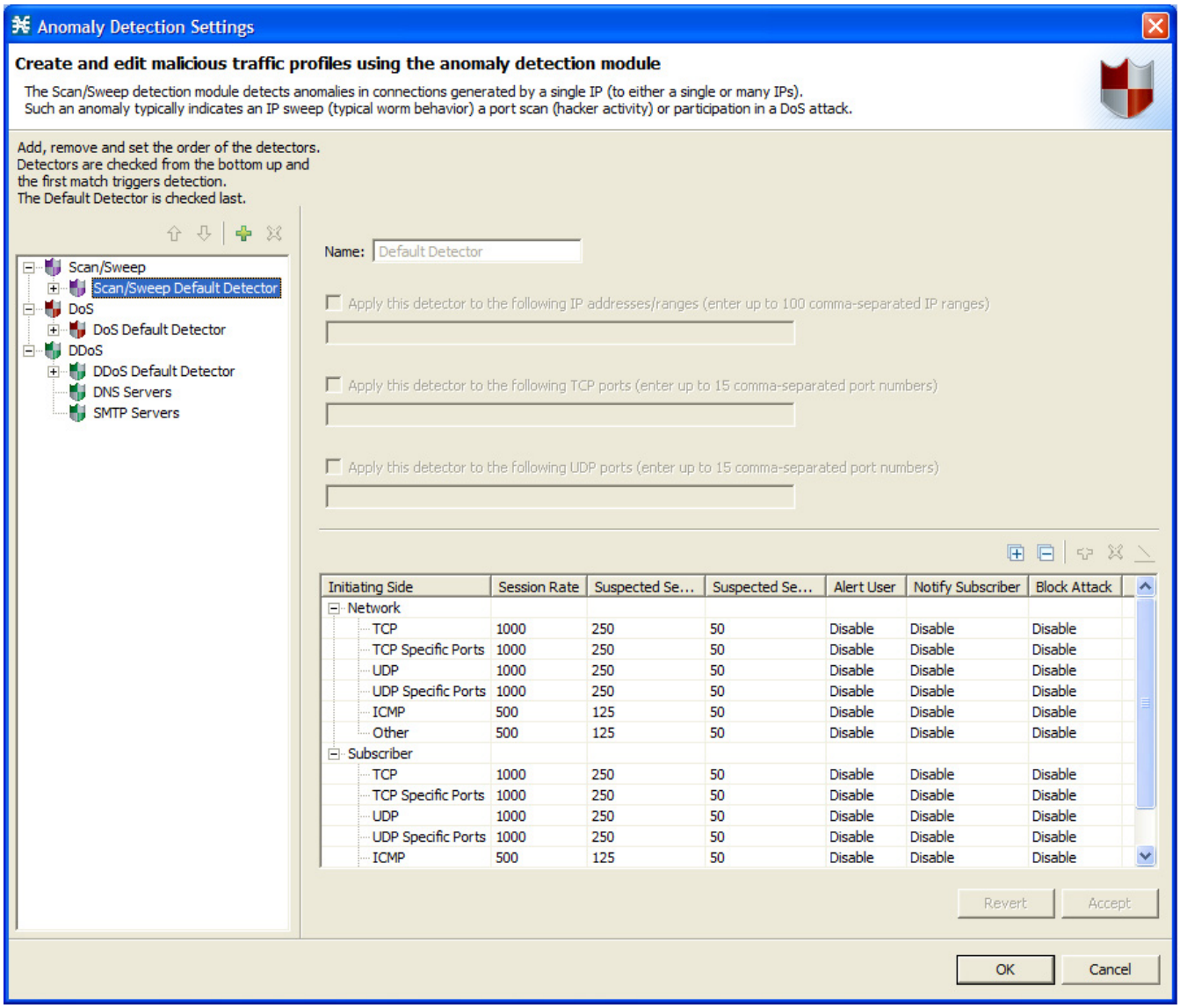
ディテクタ階層の第 1 レベルには、サブスクライバとネットワークの 2 つのサブカテゴリがあります。サブスクライバ サブカテゴリは、サブスクライバ ポート側にある IP アドレスから検出されたスキャン、スイープ、および攻撃を示します。ネットワーク サブカテゴリは、ネットワーク ポート側にある IP アドレスから検出されたスキャン、スイープ、および攻撃を示します。

これらのサブカテゴリを基にして、オペレータはサブスクライバ側またはネットワーク側のいずれかから発生したスキャン / スイープ / 攻撃といった異常に対処できます。

各サブカテゴリは、さらに次の 6 つのサブカテゴリに細分化されます。

- TCP — すべての TCP 宛先ポート上でホストが生成した集約接続レートの異常を示します。たとえば、ポート 23、25、80、110、およびその他の任意の TCP ポートに対してホストが生成した集約接続レートは、このルールのマッチング対象となります。
- TCP 固有 — 特定の TCP 宛先ポートに対してホストが生成した接続レートの異常を示します。たとえば、ポート 80 に対してホストが生成した接続レートはこのルールのマッチング対象となり、同様に、その他の個々の TCP ポートに対してホストが生成した接続レートもマッチング対象になります。
- UDP — すべての UDP 宛先ポートに対してホストが生成した集約接続レートの異常を示します。たとえば、ポート 53、445、およびその他の任意の UDP ポートに対してホストが生成した集約接続レートは、このルールのマッチング対象となります。
- UDP 固有 — 特定の UDP 宛先ポートに対してホストが生成した接続レートの異常を示します。たとえば、ポート 53 に対してホストが生成した接続レートはこのルールのマッチング対象となり、同様に、その他の個々の UDP ポートに対してホストが生成した接続レートもマッチング対象になります。
- ICMP — ICMP を使用するホストによって生成された接続レートの異常を示します。
- その他 — TCP/UDP/ICMP 以外のプロトコルを使用するホストによって生成された接続レートの異常を示します。

図 3-7　スキャン / スイープ デフォルト ディテクタ



DDoS ディテクタ

DDoS ディテクタは、ホストが宛先となっている接続の異常を検出します。概要の項で説明したとおり、これらの異常には、合計接続レート、不審接続レート、および不審接続比率があります。

IP アドレスへの接続レートが高い場合は、その IP アドレスが攻撃を受けていることを示しています。

さらに、不審セッション レートが高く、加えて不審セッション比率が高い場合は、その IP アドレスが攻撃を受けていることをより明確に示しています。

DDoS ディテクタ モジュールは、DoS 攻撃と DDoS 攻撃を検出します。ただし、モジュールは接続の生成に関連した IP アドレスを追跡しないため、DoS 攻撃と DDoS 攻撃は区別しません。

ディテクタ階層の第 1 レベルには、サブスクライバとネットワークの 2 つのサブカテゴリがあります。サブスクライバ サブカテゴリは、サブスクライバ ポート側にある IP アドレスで検出された攻撃を示します。ネットワーク サブカテゴリは、ネットワーク ポート側にある IP アドレスで検出された攻撃を示します。

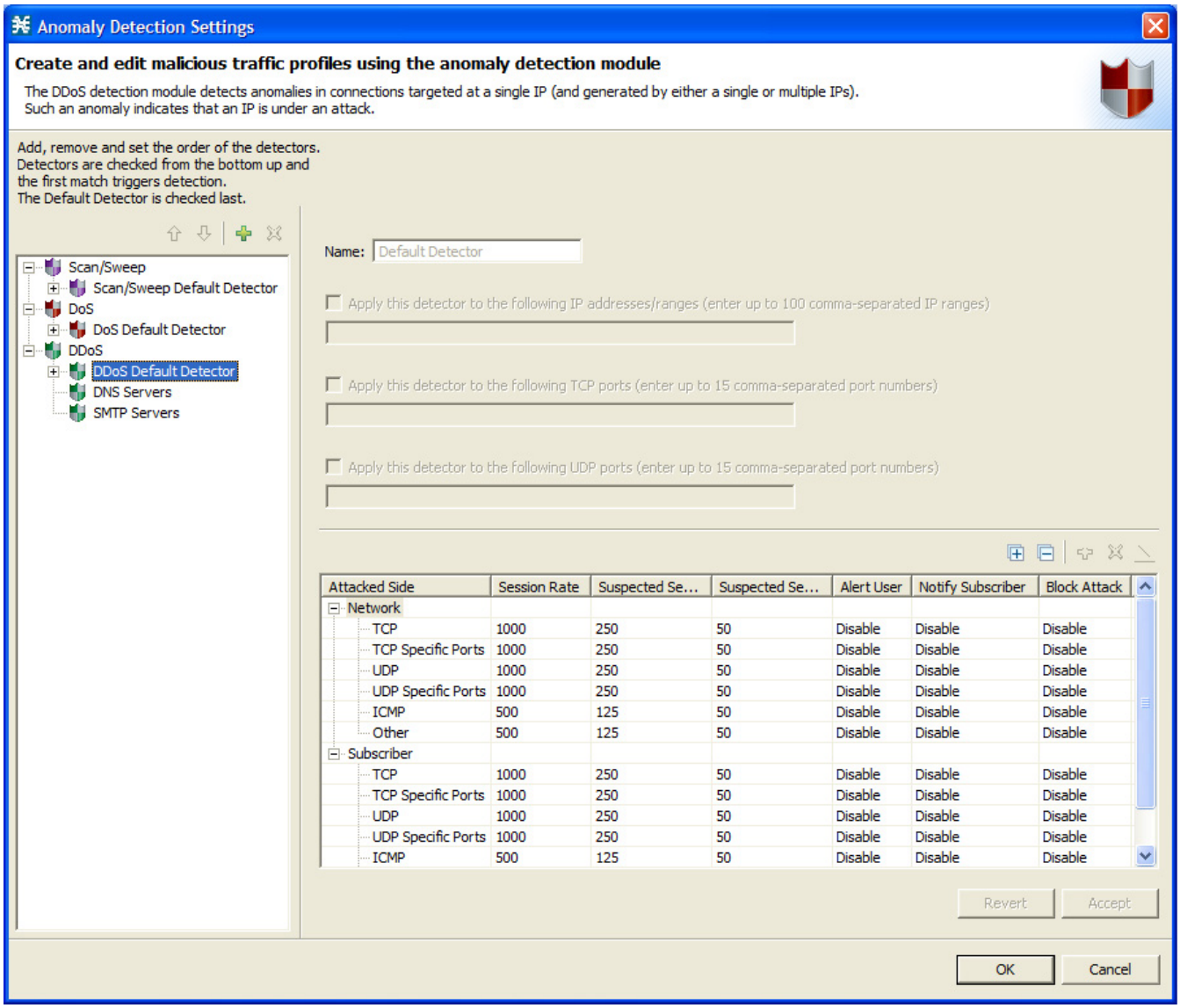
これらのサブカテゴリを基にして、オペレータはサブスクライバ側またはネットワーク側へ向かう異常に対処できます。

オペレータは、疑わしい攻撃からサブスクライバを保護することを検討する一方、ネットワーク側のアクティビティについてはこれを配慮しない場合があります。これは、攻撃を受けているとして誤って検出されたサブスクライバの正規のアクティビティには、攻撃の影響がないからです。

各サブカテゴリは、さらに次の 6 つのサブカテゴリに細分化されます。

- TCP — すべての TCP 宛先ポート上のホストに対する集約接続レートの異常を示します。たとえば、ポート 23、25、80、110、および任意の TCP ポートに対する集約接続レートは、このルールのマッチング対象となります。
- TCP 固有 — 特定の TCP 宛先ポート上のホストに対する接続レートの異常を示します。たとえば、ポート 80 上のホストに対する接続レートはこのルールのマッチング対象となり、同様に、その他の個々の TCP ポート上のホストに対する接続レートもマッチング対象になります。
- UDP — すべての UDP 宛先ポート上のホストに対する接続レートの異常を示します。たとえば、ポート 53、445、および任意の UDP ポートに対する集約接続レートは、このルールのマッチング対象となります。
- UDP 固有 — 特定の UDP 宛先ポート上のホストに対する接続レートの異常を示します。たとえば、ポート 53 上のホストに対する接続レートはこのルールのマッチング対象となり、同様に、その他の個々の UDP ポート上のホストに対する接続レートもマッチング対象になります。
- ICMP — ICMP を使用するホストに対する接続レートの異常を示します。
- その他 — TCP/UDP/ICMP 以外のプロトコルを使用するホストに対する接続レートの異常を示します。

図 3-8　DDoS デフォルト ディテクタ



DoS ディテクタ

DDoS ディテクタは、1 組のホスト間の接続における異常を検出します。概要の項で説明したとおり、これらの異常には、合計接続レート、不審接続レート、および不審接続比率があります。

1 組のホスト間の接続レートが高い場合は、送信元ホストが宛先ホストを攻撃していることを示している場合があります。

さらに、不審セッション レートが高く、加えて不審接続比率が高い場合は、一方のホストが他方を攻撃していることをより明確に示しています。

このモジュールは、1 組のホスト間の接続レートをモニタします。モニタ対象には、DoS 攻撃と DDoS 攻撃が含まれます。ただし、複数のホストが宛先ホストを攻撃している場合があり、このモジュールはそのような状態を明示的に検出しないため、DoS 攻撃と DDoS 攻撃は区別されません。

ディテクタ階層の第 1 レベルには、サブスクライバとネットワークの 2 つのサブカテゴリがあります。サブスクライバ サブカテゴリは、サブスクライバ ポート側にある IP アドレスから検出された攻撃を示します。ネットワーク サブカテゴリは、ネットワーク ポート側にある IP アドレスから検出された攻撃を示します。

これらのサブカテゴリを基にして、オペレータはサブスクライバ側またはネットワーク側から到達する異常に対処できます。

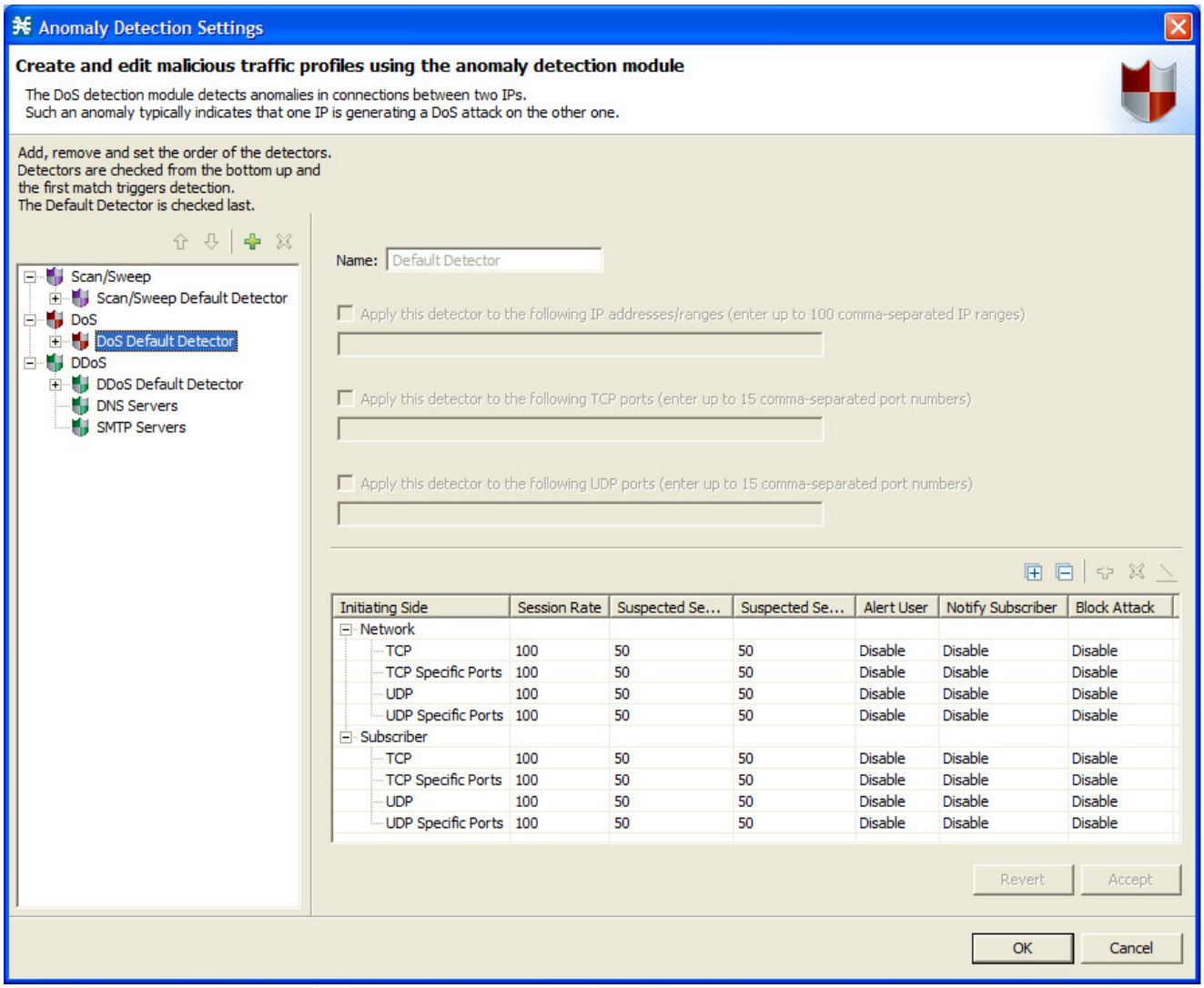
オペレータは、疑わしい攻撃からサブスクライバを保護することを検討する一方、ネットワーク側のアクティビティについてはこれを配慮しない場合があります。これは、攻撃を受けているとして誤って検出されたサブスクライバの正規のアクティビティには、攻撃の影響がないからです。

各サブカテゴリは、さらに次の 4 つのサブカテゴリに細分化されます。

- TCP — すべての TCP 宛先ポート上の 1 組のホスト間の集約接続レートの異常を示します。ポート 23、25、80、110、およびその他のすべての TCP ポート上の 1 組のホスト間の集約接続レートは、このルールのマッチング対象となります。
- TCP 固有 — 特定の TCP 宛先ポート上の 1 組のホスト間の接続レートの異常を示します。たとえば、ポート 80 上の 1 組のホスト間の接続レートはこのルールのマッチング対象となり、同様に、その他の個々の TCP ポート上の 1 組のホスト間の接続レートもマッチング対象になります。
- UDP — すべての UDP 宛先ポート上の 1 組のホスト間の集約接続レートの異常を示します。ポート 53、445、およびその他のすべての UDP ポート上の 1 組のホスト間の集約接続レートは、このルールのマッチング対象となります。
- UDP 固有 — 特定の UDP 宛先ポート上の 1 組のホスト間の接続レートの異常を示します。たとえば、ポート 53 上の 1 組のホスト間の接続レートはこのルールのマッチング対象となり、同様に、その他の個々の UDP ポート上の 1 組のホスト間の接続レートもマッチング対象になります。

DoS 検出には、ICMP カテゴリおよびその他のカテゴリはありません。これは、該当するプロトコルを使用する 1 組のホスト間の接続を相互に区別できないからです。

図 3-9　DoS デフォルト ディテクタ



悪質トラフィックのモニタリング

スキャン / スイープおよび DDoS モジュールを使用して検出されたトラフィック異常に関する情報は、SCE Raw Data Record（RDR）を介して送信され、Collection Manager Database に格納されます。この情報を使用して、ネットワーク動向の把握、新しい脅威の検出、および悪質なホストまたはサブスクライバの追跡を実行できます。

異常検出は、セッション レートしきい値の違反に基づいているため、実際にデータベースに格納されている情報は、検出しきい値のセットによって異なります。

たとえば、しきい値が 100 セッション / 秒に設定されたシステムについて生成されたスキャン / スイープ レポートと、しきい値が 1000 セッション / 秒に設定されたシステムについて生成されたレポートとの間では顕著な違い（イベント数がかなり異なる）が見られることがあります（トラフィック パターンは両方のシステムで同一であることが前提）。

悪質トラフィックを扱っているレポートは多数あります。

包括的な「傾向」を示すレポート：

- Top Scanned or Attacked ports
- Global Scan or Attack Rate
- Global DoS Rate
- Infected Sbscribers
- DoS Attacked Subscribers

個別のサブスクライバまたはホストのレポート

- Top Scanning or Aattacking hosts
- Top Scanning or Attacking Subscribers
- Top Attacked hosts
- Top Attacked Subscribers

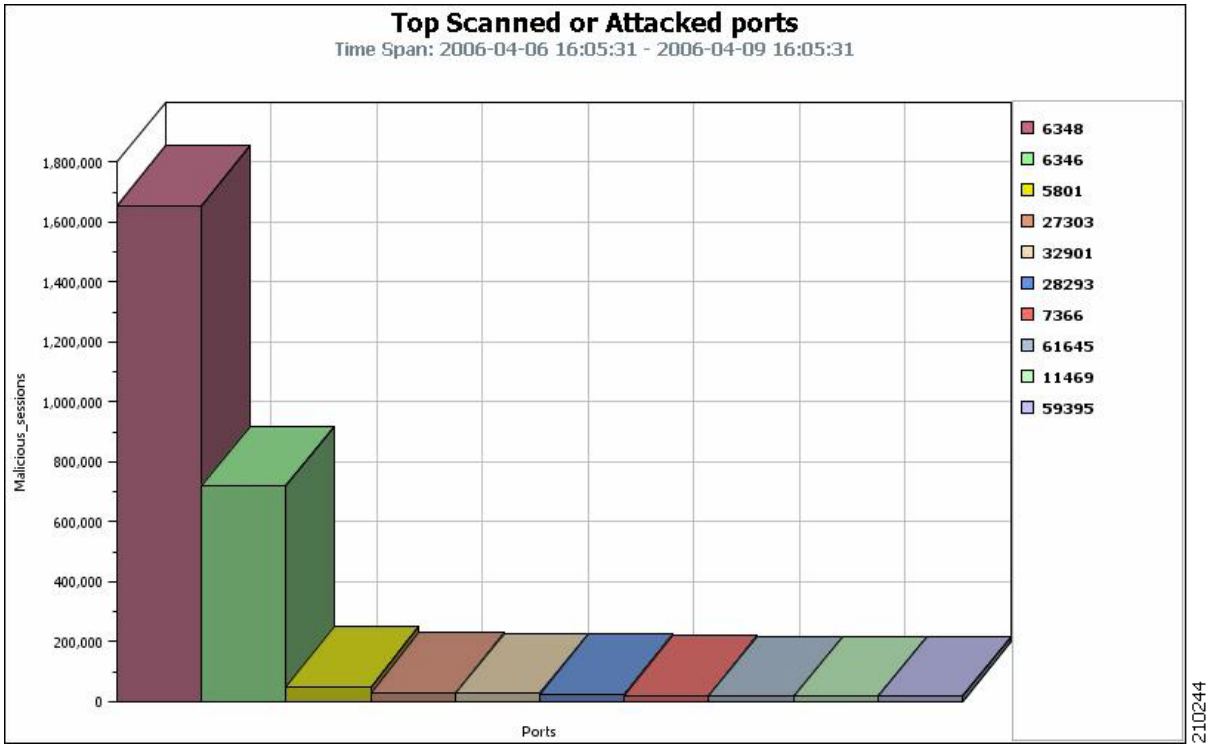
Top Scanned or Attacked Ports

Top Scanned or Attacked ports レポートは、SCE プラットフォームによって特定のポート上で検出されるスイープ / 攻撃アクティビティに関するレコードに基づいています。

レポートは、該当するアクティビティが検出されたポートのうち、アクティビティ量の多い上位のポートを示します。これは、ワーム、ボット、およびハッカーの検索対象となっている現在の「脆弱」なポートを示す良いインジケータとなります。

新しいネットワーク ワームが侵入すると、通常、特定ポートのスイープ量が増加するという特徴が見られます。このレポートを使用してネットワークを継続してモニタすることにより、オペレータはポート上の悪質なアクティビティの量の増加に基づいて、新しいネットワーク脅威の発生を検出できます。

図 3-10　Top Scanned or Attacked Ports レポート



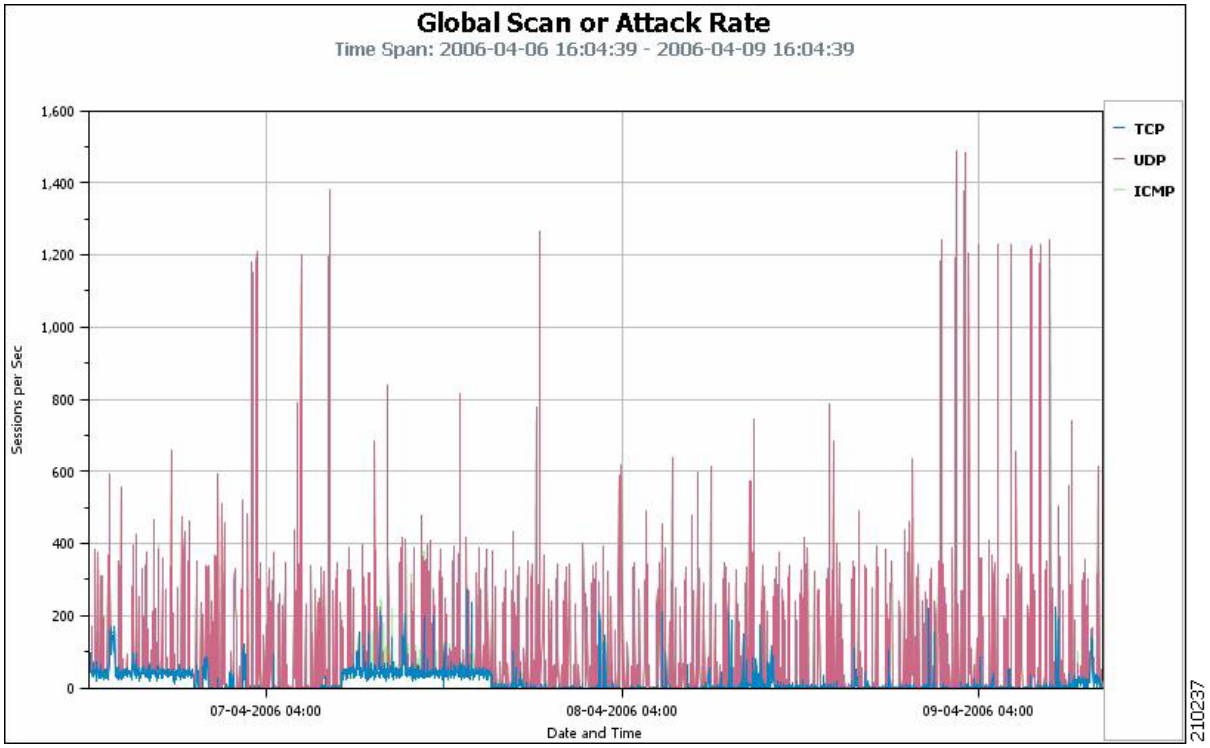
Global Scan/Attack Rate

Global Scan or Attack Rate レポートは、SCE プラットフォームによって検出されるスイープ / 攻撃アクティビティに関するレコードに基づいており、特定のポートに限定されません。

レポートは、経時的にグローバル スキャン / 攻撃レートをプロトコル別に分類して示します。レポートは、スキャンの方向がサブスクライバからか、またはネットワークからかによってフィルタできます。

ネットワーク ワームが発生すると、通常、スキャン アクティビティの急増が見られます。このレポートはその検出に役立ちます。

図 3-11　Global Scan or Attack Rate レポート

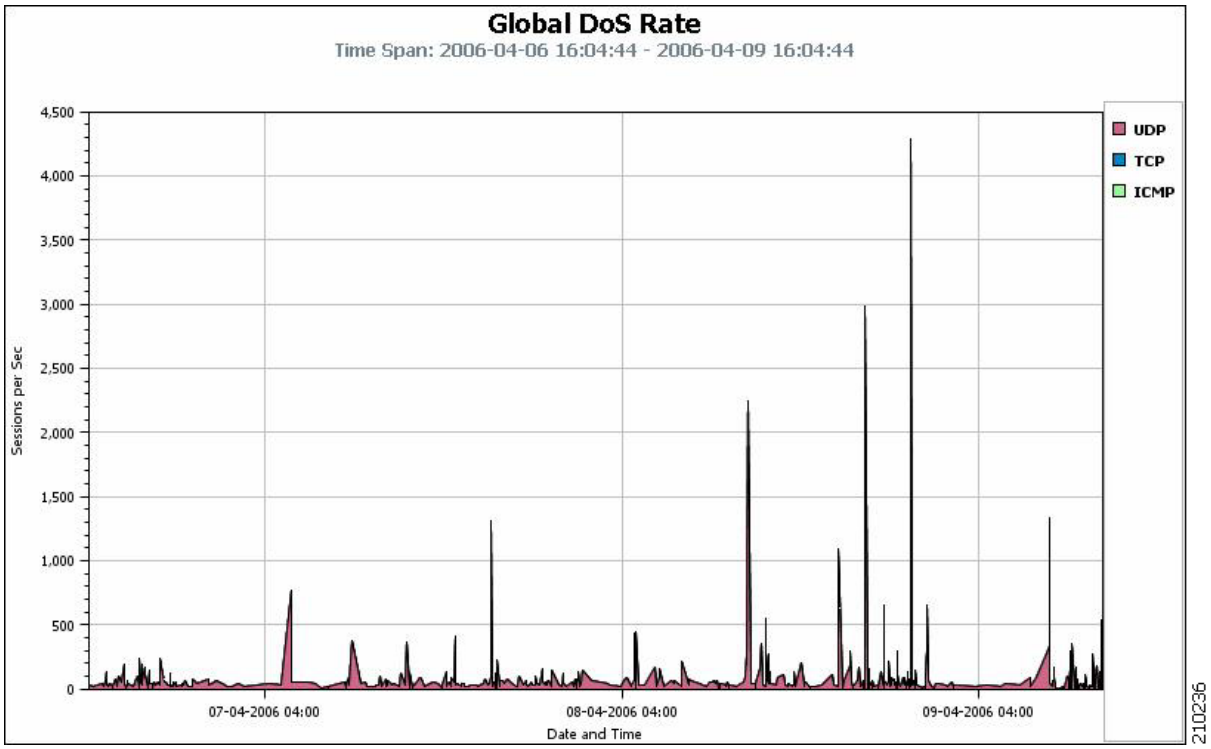


Global DoS Rate

Global DoS Rate レポートは、SCE プラットフォームによって検出される DDoS アクティビティに関するレコードに基づいており、特定のポートに限定されません。

このレポートは、経時的にグローバル DoS レートをプロトコル別に分類して示します。レポートは、攻撃の方向がサブスクライバへ向かっているか、またはネットワークに向かっているかによってフィルタできます。

図 3-12　Global DoS Rate レポート



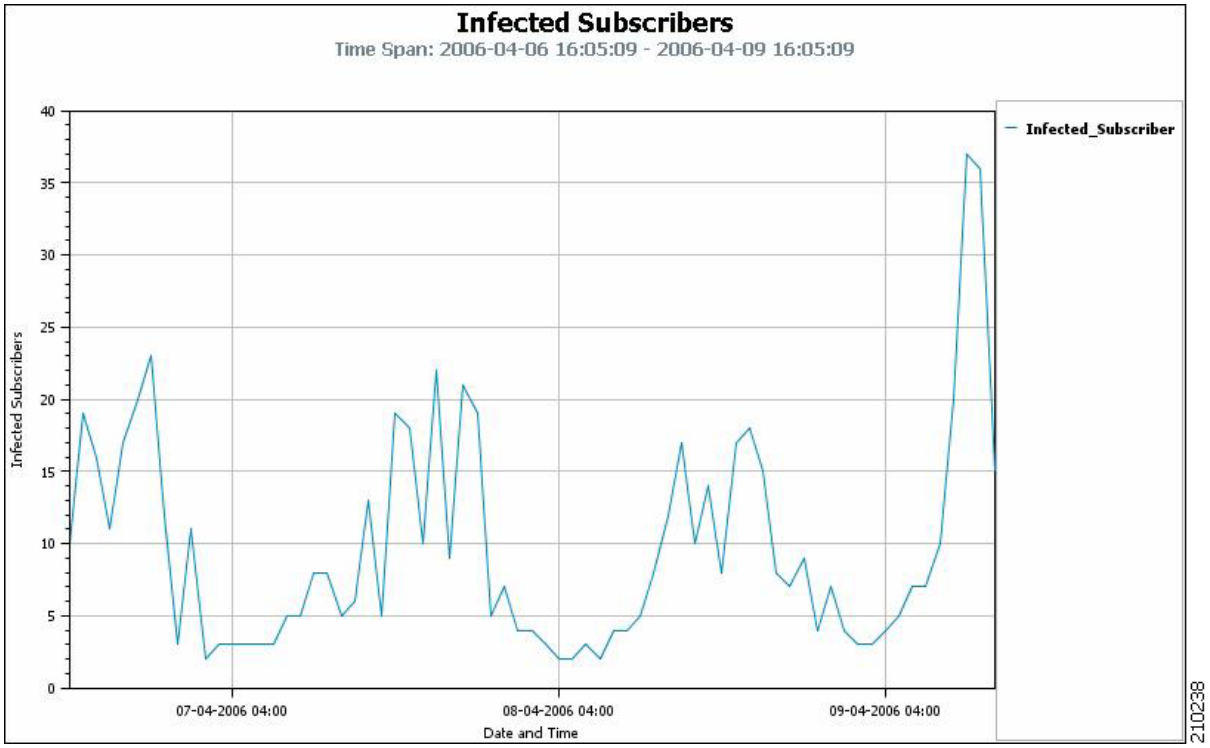
Infected Subscribers

Infected Subscribers レポートは、SCE プラットフォームによって検出されるスキャン / 攻撃アクティビティに関するレコードに基づいており、特定のポートに限定されません。

レポートは、時間（1 時間単位）の経過とともに感染したサブスクライバの数を見積もります。この数は、対象の時間枠内に悪質トラフィックを生成したと見なされたサブスクライバの数を表します。「感染」は、サブスクライバ ホスト上の悪質エージェントによってトラフィックが生成されることが前提となっています。

新しいワームが侵入すると、通常、感染したサブスクライバ数の急増がトリガーされます。そのため、このレポートは、このアクティビティをモニタリングする適した方式として使用できます。

図 3-13　Infected Subscribers レポート

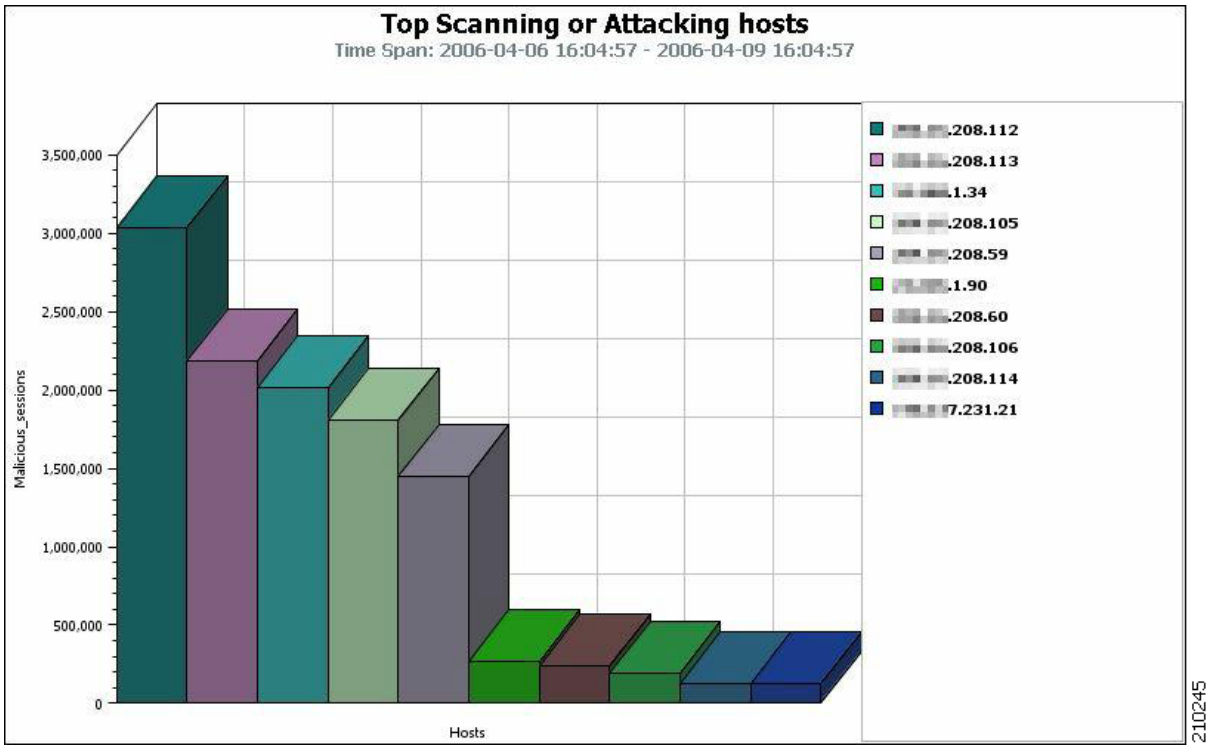


Top Scanning or Attacking Hosts

Top Scanning or Attacking hosts レポートは、SCE プラットフォームによって検出されるスキャン / 攻撃アクティビティに関するレコードに基づいており、特定のポートに限定されません。

レポートは、指定した期間の TopN のスキャニング ホストまたは攻撃ホストを示し、サブスクライバまたはネットワーク別、およびプロトコル別にフィルタできます。

図 3-14　Top Scanning or Attacking Hosts レポート



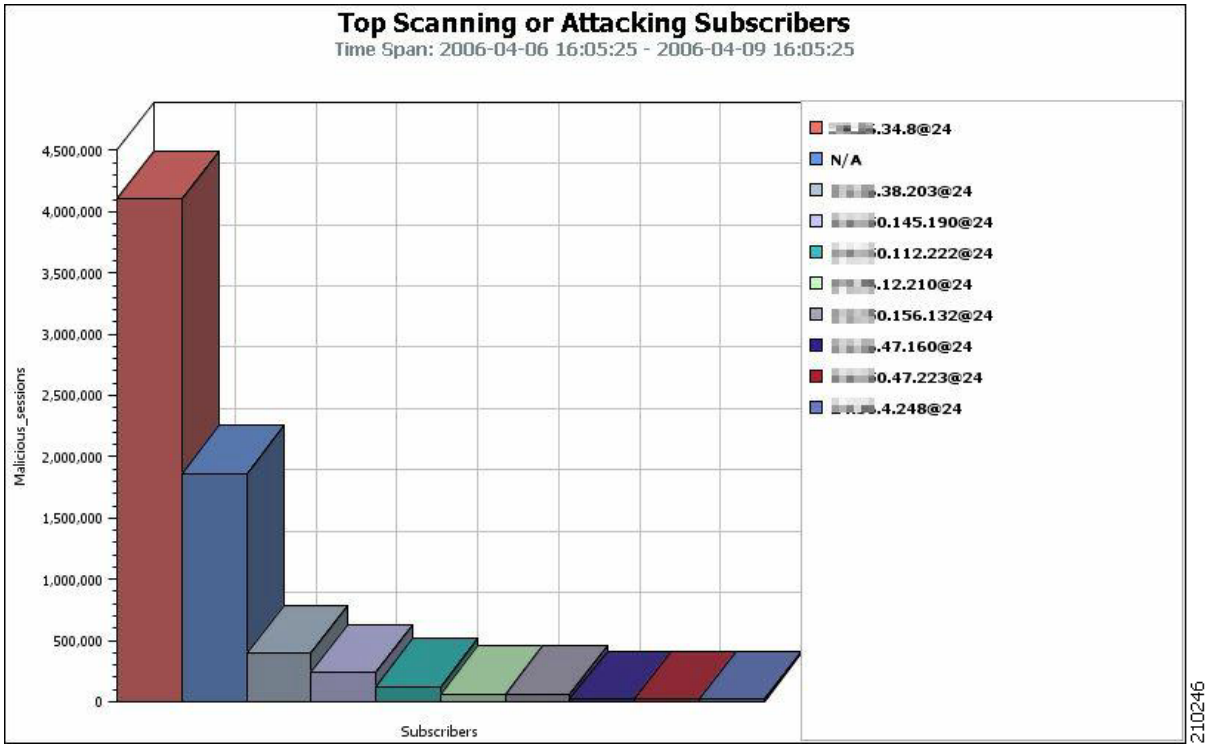
Top Scanning/Attacking Subscrivers

Top Scanning or Attacking Subscribers レポートは、SCE プラットフォームによって検出されるスキャン / 攻撃アクティビティに関するレコードに基づいており、特定のポートに限定されません。

このレポートは、指定された期間の TopN のスキャニング サブスクライバまたは攻撃サブスクライバを示し、プロトコル別にフィルタできます。

一般に、このようなレポートに示される N/A サブスクライバは、「名前付き」サブスクライバに帰属せず、通常は送信元 IP アドレスのスプーフィングに起因するスキャン / 攻撃トラフィックの合計です。

図 3-15　Top Scanning or Attacking Subscribers レポート

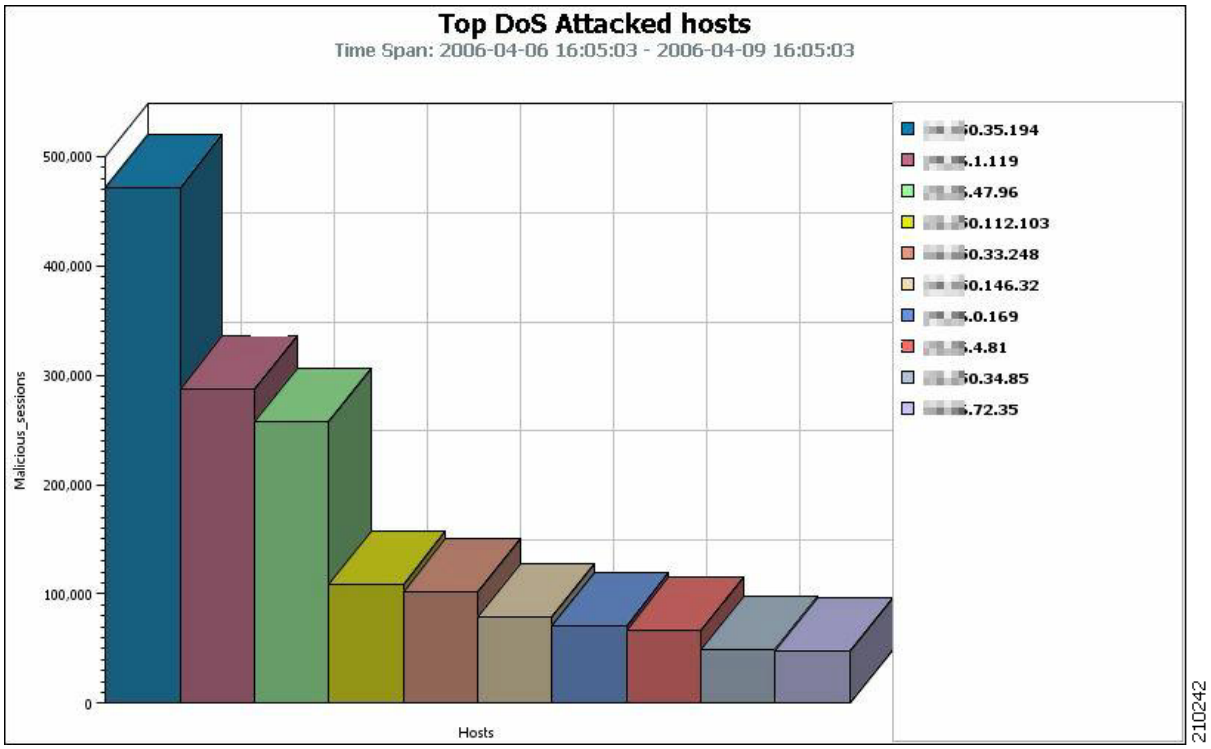


Top DoS Attacked Hosts

Top DoS Attacked hosts レポートは、SCE プラットフォームによって検出される DDoS アクティビティに関するレコードに基づいており、特定のポートに限定されません。

このレポートは、指定した期間の TopN の攻撃されたホストを示し、サブスクライバまたはネットワーク別、およびプロトコル別にフィルタできます。

図 3-16　Top DoS Attacked Hosts レポート



Top DoS Attacked Subscribers

Top DoS Attacked Subscribers レポートは、SCE プラットフォームによって検出される DDoS アクティビティに関するレコードに基づいており、特定のポートに限定されません。

このレポートは、時間（1 時間単位）の経過に伴い攻撃されたサブスクライバの数を示します。この数は、対象の時間枠内に攻撃を受けたと見なされたサブスクライバの数を表します。レポートは、プロトコル別にフィルタすることもできます。

図 3-17　Top DoS Attacked Subscribers レポート