CHAPTER 2

機能の概要

ここでは、SCE プラットフォームのサービス セキュリティ機能の概要を説明します。

機能の概要

Cisco SCE プラットフォームは、脅威を検出するために 3 通りのアプローチを使用します。

- 異常検出 — ホスト IP アドレス同士の接続速度（成功した場合も失敗した場合も）をモニタします。通常の接続レートを超過したかどうか、および成功した接続と失敗した接続の比率に基づいて、悪質なアクティビティを検出します。異常検出機能により、次のカテゴリのアクティビティであることがわかります。
  - スキャン / スイープ / 攻撃 — ホストが異常な接続速度を生成している兆候に基づきます。
  - DoS/DDoS — ホストが異常な接続速度のターゲットとなっている兆候に基づきます。
  - DoS — 1 組のホストが異常な接続速度をもたらすアクティビティに関与し、一方が生成し、もう一方がターゲットとなっている兆候に基づきます。
- 異常検出メカニズムは、ゼロデイ攻撃の解消において効果的です。つまり、それらの具体的な性質や L7 シグニチャに関する予備知識は必要なく、むしろそれらのネットワーク アクティビティの特性に基づいて、出現した時点で脅威を解消できます。

  詳細については、「異常ベースの検出」（p.3-1）を参照してください。
- 大量メール送信アクティビティ検出 — 個々のサブスクライバの SMTP セッション レートのモニタリングに基づきます。SCE プラットフォームのサブスクライバ認識機能を使用し、サブスクライバ認識モードまたは匿名サブスクライバ モードで動作できます。SMTP は、E メールの送信に使用されるプロトコルです。個々のサブスクライバから開始されたセッションのレートが過剰な場合、通常は、E メール送信に関わる悪質アクティビティを示しています。このようなアクティビティには、メールベースのウイルス、またはスパムゾンビ アクティビティがあります。
- シグニチャ ベースの検出 — SCE プラットフォームのステートフル L7 機能を使用して、他のメカニズムでは検出が難しい悪質なアクティビティを検出します。ユーザはこのような脅威に対して独立してシグニチャを設定できるため、脅威を解消する際のターンアラウンド時間を短縮できます（この機能の詳細は、このマニュアルでは取り上げていません）。

3 つのどの検出アプローチを用いても、オペレータはそれぞれのビジネス ニーズに応じて、数通りの方法で対処策を講じることができます。

モニタ — これらの各方式によって検出された悪質なアクティビティについてネットワークを検査します。検査は、検出された悪質なアクティビティについて収集された情報に基づくレポートを使用するか、または、異常検出モジュールを使用して悪質アクティビティを検出できる SNMP トラップを使用して、実行されます。

ブロック — SCE プラットフォームによって検出された悪質なアクティビティを自動的にブロックし、ネットワークに脅威が広まって悪影響が出るのを防ぎます。

通知 ― サブスクライバの Web 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の被害が発生していることを通知します。

オペレータは、高度な柔軟性を使用して、それぞれ固有のニーズに基づいて検出方式と対処方法を調整できます。SCA BB Security Dashboard は、セキュリティ機能を設定およびモニタするためのフロント エンドを備えた簡易な GUI アプリケーションです。

図 2-1　SCA BB Security Dashboard