



概要と目的

ここでは、Cisco SCE を使用したサービス セキュリティの概要を説明します。

概要と目的

近年、インターネットから生じるさまざまなタイプの攻撃や悪質なトラフィックからの保護の必要性に関心が集まっています。DoS 攻撃（サービス拒絶攻撃）や Distributed DoS 攻撃（DDoS; 分散型サービス拒否攻撃）、ワーム、ウイルス、悪質な HTTP コンテンツ、およびさまざまなタイプの侵入が猛威を増しつつあります。

SCE プラットフォームは、ステートフルでプログラム可能なインライン配置型のプラットフォームです。これらの特長によって、SCE プラットフォームは、サービス プロバイダーとその顧客のサイト上で悪質なトラフィックを検出し、その脅威を軽減することができます。

SCA BB には、異常検出、スパム / マスメーリング（大量メール送信）検出、およびシグニチャ検出から構成されたサービス セキュリティ機能が組み込まれています。この機能を使用して、SCE プラットフォームは、現在のネットワークに存在する多くの脅威を解消できます。

ただし、SCA BB ソリューションは、ネットワークの脅威に対して完璧なソリューションではありません。オペレータ ネットワーク内の悪質なアクティビティを監視したり、ネットワーク全体のパフォーマンスとユーザ エクスペリエンスを低下させることのある悪質アクティビティの大規模な拡大を軽減したりする上で、効果的なソリューションです。

このガイドには、構成とレポートについて詳細に説明している実用的なセクションが含まれています。それらは、サービス セキュリティの概念を明確にし、具体的に解説することを目的としています。関連する管理モジュールの操作の詳細については、SCA BB のユーザ ガイドを参照してください。

