Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスによるビジネス アプリケーションの保護

Cisco ASA 5500 適応型セキュリティ アプライアンスによるアプリケーション セキュリティの新たな段階

ネットワーク セキュリティの脅威は、ますますアプリケーション レイヤを対象とするようになってきています。ネットワーク管理者やセキュリティ管理者は、ビジネスの生産性を向上させるために新しいサービスを展開する一方で、それらのサービスを攻撃から保護するために、困難な妥協をしなければならないことがあります。Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスを利用すると、新しいアプリケーションの迅速で、堅牢で、セキュアな導入が可能になるため、このような妥協を繰り返す必要がなくなります。

概要

ネットワーク化されたアプリケーションは、ビジネス インフラストラクチャの重要な要素になっています。従来のセキュリティ ソリューションには、これらのアプリケーションを攻撃から保護するために必要な、幅広いアプリケーションのサポート、詳細な検査、統合ネットワーク サービス、およびパフォーマンス レベルが不足しています。Cisco® ASA 5500 シリーズを利用して、新たな妥協のないアプリケーション セキュリティを実現すると、現在および将来の脅威からネットワーク化されたアプリケーションを保護するという困難な課題に対処できます。

課題

インターネットの爆発的な成長によって、ビジネス プロセスのネットワーク化が急速に進んでいます。ネットワーク化されたアプリケーションは、これらのビジネス プロセスのバックボーンになっています。Web ブラウジング、E メール通信、および IP テレフォニーなどのアプリケーションは、ビジネス インフラストラクチャの重要な要素です。メッセージングおよびプレゼンス アプリケーション（インスタント メッセージングなど）は、社員間だけでなくパートナーやカスタマーとの重要なビジネス コミュニケーション ツールと見なされるようになりつつあります。ネットワーク化されたアプリケーションは、高性能ネットワークの普及とともに、ビジネスの生産性向上に大きく貢献しています。

企業のネットワーク依存度が高まるにつれて、これらのアプリケーションの可用性と完全性はビジネスを行う上で不可欠なものになっています。しかし、従来のセキュリティ技術を回避できるようにするツールの登場によって、アプリケーションが不正利用される可能性が高まっていることから、ネットワーク化されたアプリケーションの可用性を確保するためのセキュリティ ポリシーを実施することが困難になっています。実際に、ピアツーピアのファイル共有ネットワークなどのアプリケーションでは、アプリケーション自体にその種のツールが内蔵されていることがあります。「ポートホッピング」やトンネリングなどのアプリケーション動作を使用すると、Web ブラウジング（ポート 80）などで使用するファイアウォールのオープン ポートをインテリジェントに検索し、見つけ出したオープン ポートを使用してアプリケーション自身をトンネリングさせることができます。従来のセキュリティ デバイスで、ネットワーク セグメンテーション ポリシーや アクセプタブル ユース ポリシー（AUP）を実施するのはほぼ不可能です。このようにアプリケーション利用が十分に管理できないと、社員の生産性悪化やネットワーク リソースの浪費を招く可能性があります。また、法規制上の問題につながる場合もあります。

さらに、アプリケーション レイヤを対象とする攻撃の件数も増えています。これらの攻撃はネットワーク化されたアプリケーションによって実現されるはずの生産性向上を低下させる恐れがあります。これは、アプリケーションの可用性と完全性が攻撃によって悪影響を受けるためです。IP テレフォニーや Web 対応アプリケーションの場合、アプリケーションレイヤに対する攻撃の防御はそれほど必要とされていませんでした。しかし、従来のセキュリティ デバイスにはアプリケーション レイヤを保護する機能がほとんどなく、数少ない保護機能も現在および将来発生する脅威に対応できるものではありません。

また、従来のソリューションには、最新のネットワークで使用するために重要となるネットワーク サービスやパフォーマンス プロファイルが不足しています。ビジネスクリティカルなトラフィック（IP テレフォニーなど）には高い可用性が不可欠で、ネットワーク内をトール品質サービスを使用して伝送する必要があります。セキュリティ サービスがネットワーク上のサービス配信に悪影響を与えることは許されません。

このような困難な状況で、セキュリティ管理者やネットワーク管理者は、アプリケーションの提供またはアプリケーションの保護のいずれかを犠牲にしなければならない難しい立場にあります。そのため、このような妥協を繰り返すことなく、今日のクリティカルなビジネス アプリケーションのセキュリティを実現する新たなソリューションが必要とされています。

ソリューション：Cisco ASA 5500 シリーズのアプリケーション セキュリティ

今日発生しているセキュリティ上の脅威に対処するには、新たな手法によるセキュリティ対策が必要です。包括的なアプリケーション セキュリティを実現するには、ネットワーク上のすべてのアプリケーションに個別に対処するのではなく、ネットワーク上のアプリケーションを認識するアプリケーション アウェアな機能が必要です。各アプリケーションには、共通のサービスに加えて、アプリケーション固有の検査サービスが必要です。これらのアプリケーション検査サービスは、今日のネットワークに求められる厳しいパフォーマンス要件やサービス要件に対応しなければなりません。アプリケーション セキュリティ ポリシーの柔軟な展開と実施を可能にするには、これらの要件をすべて明確で包括的なアーキテクチャに結合する必要があります。Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは、アプリケーション セキュリティに対してこのような新しい手法を実現するように設計されており、クリティカルなビジネス アプリケーションの可用性と完全性を保護することができます。

CISCO ASA 5500 シリーズのアプリケーション セキュリティ インスペクション エンジン

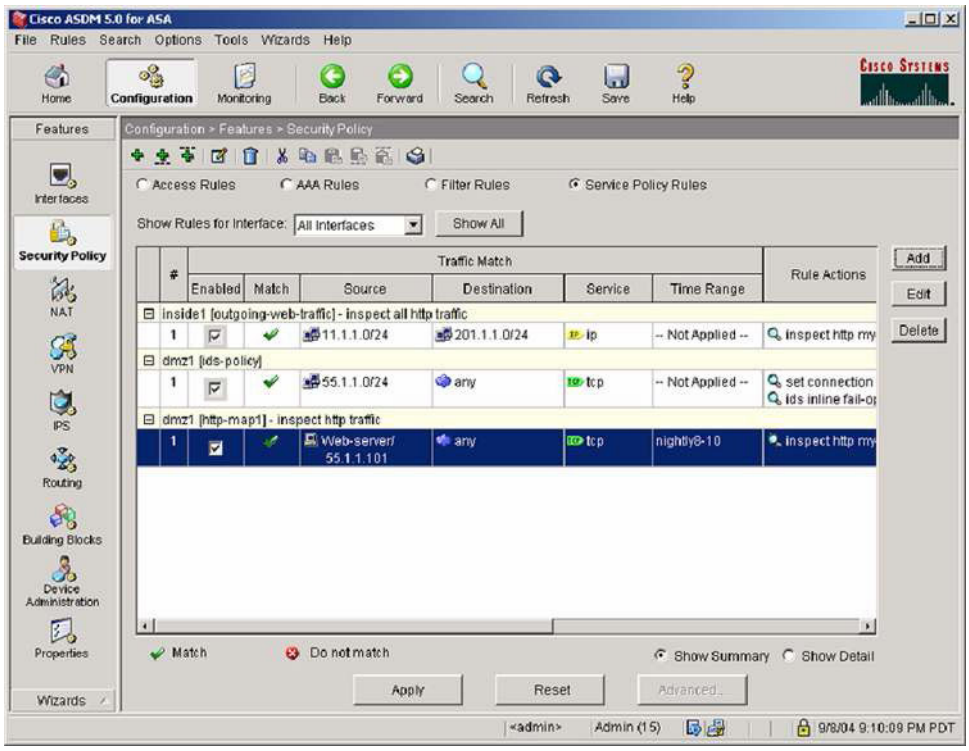
- Web ブラウジング（HTTP）
- E メール（SMTP/eSMTP）
- エンタープライズ IP テレフォニー（SIP、H.323、SCCP）
- プロバイダーの音声サービス（MGCP、GTP）
- ファイル転送（FTP）
- トンネリング アプリケーション（ピアツーピアまたはインスタント メッセージング）
- Domain Name System（DNS）
- その他多数

Cisco ASA 5500 シリーズは、Adaptive Identification and Mitigation（AIM）アーキテクチャを通じて、ネットワークに対する優れた防御とポリシー制御を実現します。Cisco ASA 5500 シリーズは、主要なすべてのネットワーク プロトコルに対応したアプリケーション セキュリティ インスペクション エンジンを備えているため、包括的なアプリケーション セキュリティ ポリシーの導入が可能になります。各インスペクション エンジンはアプリケーション フローを監視するため、各プロトコルに応じてプロトコル異常の検出と防御を行うことができます。たとえば、Web インスペクション エンジンを利用すると、管理者はHTTP に関する RFC やその他の基準にトラフィックを適合させることによって、ポート 80 を使用するトラフィックが有効な Web トラフィックであることを保証することができます。これには、2 つの大きな利点があります。第 1 に、インスペクション エンジンは、ポート 80 を利用したトンネリングによってセ

キュリティ ポリシーを回避しようとする HTTP 以外のアプリケーションを検出して防御します（Kazaa などのピアツーピア プログラムはこれに該当します）。第 2 に、インスペクション エンジンは、プロトコルのセマンティックスとベスト プラクティスを評価することによって、アプリケーション レイヤを対象とする既知および未知の攻撃を防御します。アプリケーション処理の脆弱性を狙うマルウェアは、標準規格に適合させることによって防御できます。

インスペクション エンジンを使用すると、セキュリティ管理者はプロトコルの適合性を確保するだけでなく、堅牢な制御機能を使用してアプリケーション内の個別機能の利用を制御することもできます。FTP インスペクション エンジンでは、ユーザがファイル サーバ上で実行可能なコマンドを管理者が制御することによって、ファイル サーバを保護します。たとえば、ユーザにファイルの取得を許可する一方で、ファイルの削除や不正なコンテンツが含まれる可能性のあるファイルのアップロードを禁止することができます。これらのサービスはすべて、シンプルで強力な Adaptive Security Device Manager（ASDM）GUI で設定できます。Cisco ASDM はウィザードと操作性に優れたインターフェイスを備えているため、堅牢なアプリケーション セキュリティ ポリシーを迅速に展開できます（図 1）。

図 1　Cisco ASDM バージョン 5.0



これらのインスペクション エンジンを実稼働ネットワーク環境で使用するには、今日のネットワークに求められる厳しいパフォーマンスやネットワーク サービス要件に対応しなければなりません。Cisco ASA 5500 シリーズは今日のネットワークに不可欠な高性能ニーズに対応しており、最大 450 Mbps の処理能力で保護サービスを並行処理できます。また、遅延の影響を受けやすい音声トラフィックの厳しいサービスレベル契約（SLA）にも、内蔵された QoS（Quality of Service）メカニズム（音声トラフィック専用の低遅延キューなど）を使用して容易に対処できます。さらに、アクティブ/アクティブ フェールオーバー サービスなどの高度なハイ アベイラビリティ機能を使用することで、セキュリティ インフラストラクチャの可用性も保護します。アクティブ/アクティブ フェールオーバー

サービスの場合、通常のネットワーク運用時には、フェールオーバーを構成する両方のデバイスでアプリケーション トラフィックを検査できるため、冗長投資をフルに活用することができます。

AIM アーキテクチャは、Cisco ASA 5500 シリーズで利用できるさまざまなアプリケーション セキュリティ インスペクション エンジンとネットワーク サービスを結びつけます。AIM アーキテクチャは、モジュール型のサービス処理とポリシー フレームワークを活用して、トラフィックフロー単位でのセキュリティ サービスやネットワーク サービスの利用を可能にします。AIM は効率的なトラフィック処理を行うことで、精度の高いポリシー制御と Anti-X 防御を実現します。また、効率性に優れた AIM アーキテクチャに加えて、ユーザによるインストールが可能な Security Services Module（SSM; セキュリティ サービス モジュール）を使用してソフトウェアとハードウェアを拡張できるため、プラットフォームを交換したり、パフォーマンスを犠牲にしたりすることなく、既存サービスの機能向上と新規サービスの導入を両立させることができます。Cisco ASA 5500 シリーズ アーキテクチャの基盤である AIM は、カスタマイズの容易なセキュリティ ポリシーと優れたサービス拡張性を兼ね備えているため、急速に進化する脅威にも対処できます。

まとめ

ネットワーク化されたアプリケーションは、ビジネスの生産性向上に大きく貢献しており、今後もさらなる発展が見込まれます。このようなメリットを実現するには、アプリケーションの可用性と完全性の保護が不可欠です。Cisco ASA 5500 シリーズを利用すると、従来のソリューションを脆弱化させることなく、包括的なアプリケーション セキュリティを実現できます。Cisco ASA 5500 シリーズは、柔軟性の高い高性能な AIM アーキテクチャを使用して、幅広いプロトコルのサポート、詳細なアプリケーションの制御、およびネットワーク サービスとの密接な統合を実現しています。このように柔軟性に優れた Cisco ASA 5500 シリーズを利用すると、今日のネットワークの保護だけでなく、将来のネットワークの保護にも柔軟に対応できます。

シスコシステムズ株式会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先（シスコ コンタクトセンター）
http://www.cisco.com/jp/go/contactcenter
0120-092-255（通話料無料）
電話受付時間：平日10:00～12:00、13:00～17:00

お問い合せ先

07.06