Cisco IOS IPS データシート

このデータシートでは、Cisco IOS® Intrusion Prevention System（IPS; 侵入防御システム）の概要を示します。

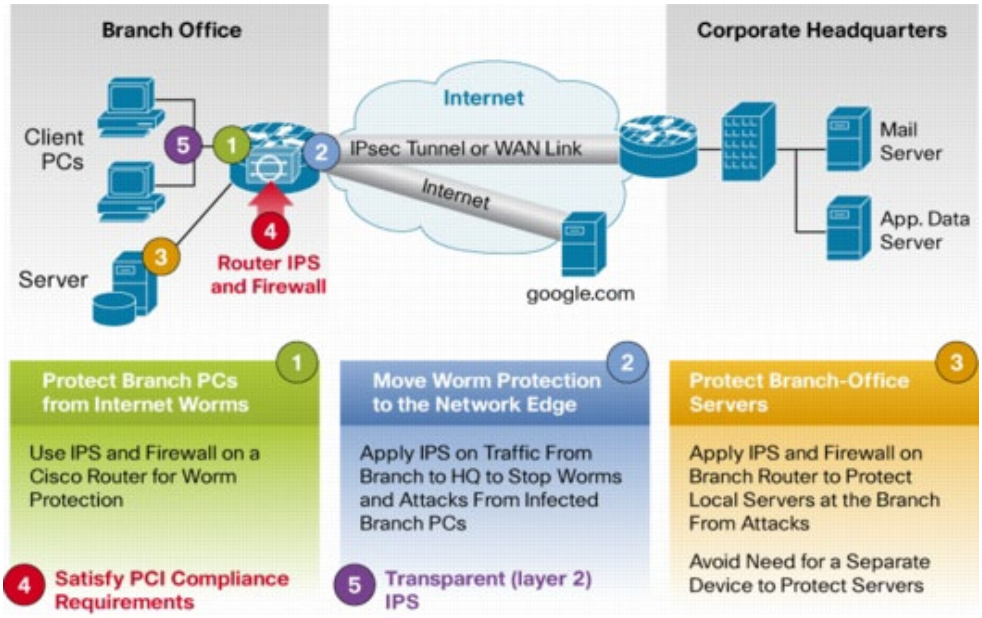
製品概要

今日のビジネス環境では、ネットワークへの侵入者および攻撃者は、ネットワークの外側だけではなく、内側にも存在する場合があります。攻撃者は、分散型サービス拒絶（DDoS）攻撃をしかけたり、インターネット接続に対して攻撃を行ったり、ネットワークやホストの脆弱性を悪用したりします。また、インターネットのワームやウイルスは、数分のうちに世界中に広がる可能性を秘めています。ほとんどの場合、人による対応を待っている余裕はありません。ネットワーク自体がインテリジェンス性を備え、このような攻撃、脅威、エクスプロイト、ワーム、およびウイルスを瞬時に認識して軽減する必要があります。

Cisco IOS IPS は、Cisco IOS ソフトウェアによって広範囲のネットワーク攻撃を効果的に軽減する、インライン型のディープ パケット インスペクション ベースのソリューションです。データセンターや企業の本社でトラフィックを検査することによって攻撃を防御するのは一般的な手法ですが、ネットワーク レベルの防御機能を広く分散配置して、ブランチや在宅勤務者のオフィスのエントリ ポイント付近で悪意のあるトラフィックを阻止することも重要です。

Cisco IOS IPS：主な使用方法および利点

IPS を使用してヘッドエンドまたは中央拠点でトラフィックを検査して攻撃を防御するのは一般的な手法ですが、可能な限りネットワークのエントリ ポイント付近で悪意のあるトラフィックを確実に阻止するために、ブランチ オフィスや在宅勤務者のオフィス、パートナーまたはサービス プロバイダーが管理するカスタマー ネットワークを保護することも重要です。IOS IPS は、5 つの方法でネットワークを保護します。



主な利点

- オペレーティング システムおよびアプリケーションの脆弱性を悪用する多数の攻撃、エクスプロイト、ワーム、およびウイルスから、広範に分散配置した保護システムを通じてネットワーク全体を保護します。
- ブランチ オフィスや在宅勤務者のオフィス、および中堅・中小企業ネットワークで、スタンドアロン型の IPS デバイスを配置する必要がなくなります。
- 独自のリスク評価ベースのシグニチャ イベント アクション プロセッサにより、IPS のポリシーをきわめて簡単に管理できます。
- ワームと攻撃のシグニチャ セットおよびイベント アクションをカスタマイズできます。
- 任意の組み合わせのルータ LAN と WAN インターフェイスを通過する双方向のトラフィックに対して、インライン型のインスペクションを実行できます。
- Cisco IOS® Firewall、コントロールプレーン ポリシング、およびその他の Cisco IOS ソフトウェア セキュリティ機能と連携して、ルータおよびルータの背後にあるネットワークを保護できます。
- Cisco IPS アプライアンスと同じシグニチャ データベースの攻撃シグニチャを約 2,400個サポートできます。

表 1 最新 IOS リリースで提供される Cisco IOS IPS 機能

機能	利点
VRF 対応（仮想 IPS）- 12.4(20)T 以降の IOS T トレイン リリースで使用可能	企業は、特定の仮想ネットワーク セグメント（VRF）だけに IPS を適用したり、各 VRF に異なるインスペクション ルールを適用したりできます。また、VRF ID により各仮想セグメント内で生成された IPS アラームやイベントを識別することができます。
Microsoft SMB/MSRPC プロトコルの脆弱性に対するシグニチャ、および NDA に基づくベンダー提供シグニチャのサポート	Microsoft およびその他の多数の新しい脆弱性（一部は公開前）に対して効率的な保護を提供できます。
シグニチャの重大度、信頼性、およびターゲット値評価に基づく IPS アラームのリスク評価値	低/高リスク評価によりイベントをフィルタリングまたは区別することで、IPS イベントをより正確かつ効率的に監視できます。
Signature Event Action Processor（SEAP）のサポート	イベントのリスク評価の計算値に基づいて、シグニチャ イベント アクションを迅速かつ自動的に調整できます。
ローカル TFTP または HTTP(S) サーバによるシグニチャの自動アップデート	最小限のユーザ操作で、最新の脅威を防御できます。
IDCONF（XML）シグニチャ プロビジョニング メカニズム	Cisco Security Manager 3.1 および Cisco Router and Security Device Manager（SDM）2.4 により、HTTPS を使って安全なプロビジョニングを実行できます。
Cisco IOS CLI による個別およびカテゴリベースのシグニチャのプロビジョニング	カスタム スクリプトを使用して、シグニチャのより詳細なカスタマイズと調整ができます。
最新の Cisco® IPS アプライアンスおよびモジュールと同じシグニチャ形式とデータベースの使用	Cisco IPS アプライアンスと Cisco IOS® IPS 間で、共通の展開および攻撃シグニチャ定義を使用できます。

プラットフォームのサポート

Cisco IOS IPS は、Advanced Security、Advanced Enterprise、および Advanced IP Services ソフトウェア フィーチャ セットに含まれており、表 2 のルータでサポートされます。ベースの ISR セキュリティ ルータ バンドルには、対応するソフトウェア イメージと共に、IPS 機能およびその他の脅威防御機能をサポートするのに十分なメモリとストレージが含まれています。

表 2 利用環境

製品ファミリ	サポートされるプラットフォーム
800	871、876、877、878、881、887、888

製品ファミリ	サポートされるプラットフォーム
1800	1801、1802、1803、1811、1812、1841、1861
2800	2801、2811、2821、2851
3800	3825、3845
7200	7204VXR、7206VXR
7301	7301

Basic および Advanced シグニチャ カテゴリ

Cisco IOS ソフトウェア リリース 12.4(11)T 以降の T トレイン リリースでは、2 つのシグニチャ カテゴリ（Basic または Advanced）のどちらかを選択することによって、IOS IPS のシグニチャ プロビジョニングを実行できます。個々のシグニチャを選択し、CLI（コマンドライン インターフェイス）を使用してパラメータを調整することもできます。CLI で簡単にスクリプトを作成し、多数のルータ用のシグニチャ設定を管理できます。

IOS Basic および Advanced シグニチャ カテゴリは、あらかじめ選択されたシグニチャのセットで、ほとんどの IOS IPS ユーザが最初に使用するうえで十分なシグニチャが含まれています。セキュリティ上の脅威の検出を目的とした、ワーム、ウイルス、IM、またはピアツーピアに関する最新の信頼性の高い（誤検出の少ない）ブロッキング シグニチャが含まれているので、展開とシグニチャ管理が簡単になります。Cisco IOS IPS では、これらの 2 つのカテゴリに含まれていないシグニチャを選択して、調整することもできます。

シグニチャ カテゴリは、シスコのシグニチャ アップデート パッケージに含まれる重要な要素です。このパッケージは、http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup で提供されています。これらのシグニチャ アップデート パッケージは、過去のすべての Cisco IPS シグニチャ アップデートを累積したもので、ルータの CLI、Cisco Configuration Professional（CCP）、または Cisco Security Manager（CSM）を使用して、ローカル PC またはサーバからルータにダウンロードできます。

IOS メインラインおよび 12.4(11)T より前の T トレイン リリースで Cisco IOS IPS を使用することは推奨されません。これらのリリースでは、IOS IPS 機能で使用するシグニチャ形式でシグニチャ アップデートが提供されていません。

Signature Micro Engine

Cisco IOS IPS は、Signature Micro Engine（SME）を使用して、一連の攻撃シグニチャを（ルータのメモリに）ロードし、スキャンします。各エンジンは、レイヤ 4 または 7 プロトコルと、プロトコルのフィールドおよび引数を検査するようにカスタマイズされています。プロトコルのデータを搬送する各パケット内で、許容される範囲の値または許容される値の組み合わせを持つ正当なパラメータ セットが検索されます。また、並列シグニチャ スキャニング技法を使用して常に SME 内で複数のパターンをスキャンすることにより、プロトコルに固有の悪質なアクティビティを検出します。

攻撃の軽減

Cisco IOS IPS は、最新の IOS IPS シグニチャ リストにある約 2,400 の攻撃、エクスプロイト、ワーム、およびウイルスからネットワークを保護します。Cisco IOS IPS では、Microsoft Windows OS およびアプリケーションの脆弱性の悪用をはじめ、ANTS、Bagle、MyDoom、Netsky、Agobot、Minmai、Klez、Sober、Zotob、Norvag、Phatbot、MyTob、GaoBot、Blaster、W2K RPC DoS、ZAFI.D、Slapper、Apache/mod_ssl、Slammer、GaoBot、Blaster、Nachi、Ping Tunnel といったウイルスやワームなど、多数の攻撃を検出して、阻止できます。

検出されたシグニチャに対するアクション

攻撃と一致するトラフィックを検出するために選択した個々のシグニチャまたはシグニチャ カテゴリには、検出された場合の対応として、以下の 5 つのアクションを任意に組み合わせて設定できます。

1. syslog メッセージによってアラームを送信するか、Secure Device Event Exchange（SDEE）形式でアラームを記録する
2. 悪質なパケットを破棄する
3. セッションを中断させるために、接続の両端に TCP-Reset パケットを送信する
4. 攻撃者（送信元アドレス）からのすべてのパケットを一時的に拒否する
5. 攻撃者（送信元アドレス）からの同じ TCP セッション（接続）に属す以降のパケットを拒否する

設定およびシグニチャのプロビジョニング

Cisco IOS 12.4(11)T2 以降のリリースを実行している単一ルータ上では、ルータの CLI または Cisco Configuration Professional（CCP）バージョン 1.1 以上を使用して、IOS IPS の設定および IPS シグニチャのより詳細なプロビジョニングと調整を行うことができます。また、Cisco Security Manager（CSM）バージョン 3.1 以上を使用すると、Cisco IOS 12.4(11)T2 以降のリリースを実行している複数のルータの IPS のポリシーおよびシグニチャ セットを管理できます。IOS メインライン リリースまたは 12.4(11)T2 より前の IOS リリースで IOS IPS を使用することは推奨されません。

イベント監視

Cisco IOS IPS では、攻撃シグニチャを検出した場合、syslog メッセージを送信するか、SDEE 形式でアラームを記録できます。単一ルータによって生成されたイベントは、CCP を使用して監視できます。また、5 台までのルータによって生成された IPS イベントは、Cisco IPS Manager Express（IME）を使用して監視できます。6 台以上のルータからのイベントを監視する場合には、syslog および SDEE をサポートしている任意の互換性のある監視アプリケーションやデバイスを使用することもできますが、ネットワーク全域での監視と IPS アラームの相関処理を行うために、Cisco Security Monitoring, Analysis, and Response System（MARS）アプライアンスを使用することを強く推奨します。

関連情報

Cisco IOS IPS の詳細については、http://www.cisco.com/jp/go/iosips/ を参照してください。

シスコシステムズ合同会社
〒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
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

お問い合せ先

09.10