

概要

Cisco Catalyst 4500 シリーズは、豊富な統合セキュリティ機能を備え、重要なネットワーク インフラストラクチャをプロアクティブに防御します。Network Admission Control (NAC) 機能、コントロールプレーン ポリシング、および 802.1X ベースのユーザ Authentication, Authorization, and Accounting (AAA; 認証、許可、アカウントिंग) などの充実した機能群によって、ネットワーク セキュリティのリスクが低減します。セキュリティ ポリシーはワイヤレフトで動作する専用の Access Control List (ACL; アクセス制御リスト) で厳格に実施され、増え続けるウイルスやセキュリティ攻撃を寄せつけません。Cisco Catalyst 4500 シリーズでは、使いやすく強力なツールを提供して、エンドユーザやホストの設定に変更を加えることなく、追跡不能な man-in-the-middle 攻撃、コントロールプレーン リソースの消耗、IP スプーフィング、およびフラッド攻撃を効果的に防御します。セキュア リモート アクセス、ファイル転送、およびネットワーク管理は、それぞれ Secure Shell (SSH Version 1 および Version 2) プロトコル、SCP、および SNMPv3 を使用して実行されます。

レイヤ 2 のセキュリティの重要性

オープン キャンパス ネットワークでは、どのようなユーザでも任意のイーサネット ポートにアクセスすることができ、場合によっては不正に侵入する可能性もあるため、ネットワークのセキュリティを保証できません。OSI モデルは異なる通信レイヤが互いを認識することなく機能するように構築されています。そのため、レイヤ 2 のセキュリティは重要です。あるレイヤが不正侵入されると、セキュリティは脅かされますが、他のレイヤには影響が及びません。通信は以前と同様に進行するため、アプリケーション層の情報に危険にさらされていても、ユーザがそれに気付くことはありません。

2004 年の FBI/CSI のリスク評価では、次のことが明らかにされました。

- 企業ネットワークの全ポート中、99% がオープンである。
- 通常どのノート型パソコンからでもネットワークに接続し、ネットワークへのアクセス権を取得することができる。
- 調査対象企業が報告した損害総額は、1 億 4100 万米ドル以上である。
- 回答者の 59% が、考えられる要因として、不満を持った従業員によるインサイダー攻撃を挙げている。

この調査では、内部と外部のいずれの侵入についても報告しない企業が多数あることがわかりました。マイナスイメージの評判が広がり、事業に悪影響を与える恐れがあるためです。

企業のワイヤリング クラウドゼットに多くみられるレイヤ 2 スイッチング環境は、セキュリティ攻撃の格好のターゲットです。レイヤ 2 ドメインにおける代表的なセキュリティ攻撃のうち最も検出されにくいものの 1 つが、パスワードなどの機密情報収集を目的に、ネットワークを使用不能にしたり、ネットワーク ユーザを脅かしたりする攻撃です。このような攻撃では、スイッチの MAC アドレス学習機能、Address Resolution Protocol (ARP; アドレス解決プロトコル [RFC 826]) によるエンドステーションの MAC アドレス解決、Dynamic Host Control Protocol (DHCP; 動的ホスト制御プロトコル) サーバによる IP アドレス割り当てといった、通常のプロトコル処理が悪用されます。

代表的なレイヤ 2 のセキュリティ攻撃

残念ながら、インターネットではメニュー操作式のハッカー ツールがたやすく入手できるため、セキュリティ攻撃を仕掛けるのに高度なスキルは必要ありません。損害をもたらす可能性のある代表的な攻撃には、次のものがあります。

1. MAC アドレス フラッド攻撃
2. DHCP サーバスプーフィング
3. gratuitous ARP を使用した [man-in-the-middle] 攻撃
4. IP ホスト スプーフィング

認証とセキュリティ機能 (IEEE 802.1X や ACL など) は組織の攻撃防御ポリシーの一部として不可欠ですが、それらを使用しても、上述したレイヤ 2 のセキュリティ攻撃は防止できないことを理解することが重要です。認証済みのユーザが悪意を持っていた場合、これらの攻撃はすべて簡単に実行されてしまいます。

Cisco Catalyst 4500 シリーズの Cisco Catalyst 統合セキュリティ機能

Cisco® Catalyst® 4500 シリーズ スイッチの統合セキュリティ機能は、こうした代表的なレイヤ 2 のセキュリティ攻撃を防御するのに役立ちます。以下では、それぞれの脅威や攻撃防止に使用されるセキュリティ機能について概説します。

1. 攻撃：MAC アドレス フラッド攻撃

MAC アドレスはホスト デバイスの物理アドレスです。スイッチの通常の動作では、すべての着信パケットについて送信元のアドレスとポートがアドレス テーブルに登録されます。フレームの宛先が未知の MAC アドレスである場合は、VLAN 内のすべてのポートから送信されます。これがスイッチまたはブリッジにおけるレイヤ 2 のフォワーディング、フィルタリング、および学習メカニズムの機能です。スイッチには学習できる MAC アドレス数に対応した専用のメモリ空間が備わっています。この攻撃は、スイッチが本来備えている MAC アドレス学習機能とフォワーディング機能を悪用して、テーブルのフラッド攻撃やオーバーフローを引き起こそうとします。

この攻撃は、未知の MAC アドレスを使用してスイッチにフラッド攻撃を引き起こすことにより、ハードウェア本来の制限を悪用します。まずスイッチがその MAC アドレスを学習します。しかし、レイヤ 2 フォワーディング テーブルの限度を超えると、パケットが VLAN 内のすべてのポートにフラッド攻撃するため、ハッカーはスイッチド ネットワーク経由のネットワーク接続を傍受できるようになります。同時にネットワークのパフォーマンスは大幅に低下します。

防御策：ポート セキュリティ

ポート セキュリティは動的な機能で、同一の物理ポートにアクセスできるステーションの MAC アドレスを制限、識別するために使用します。スイッチがセキュア MAC アドレスをセキュア ポートに割り当てるように設定されている場合、あるいはスイッチが、それらのアドレスを動的に学習する場合、ポートは定義済みのアドレス グループに属さない送信元アドレスを持つパケットについてはフォワーディングを行いません。ポート セキュリティを使用し、スイッチポートで許可される MAC アドレスの数を制限することによって、MAC アドレス フラッド攻撃を効果的に封じることができま

2. 攻撃：DHCP サーバスプーフィングと [man-in-the-middle] 攻撃

ネットワーク攻撃者は多くの場合、不正な DHCP サーバを利用して IP ホストアドレスをばらまき、自分自身をデフォルト ゲートウェイに指定します。これにより、2 つのエンドポイント間を流れる正規のトラフィック フローのルート変更が可能になり、トラフィックは 2 つのエンドポイント間ですべて捕捉されます。そのためにこれは [man-in-the-middle] 攻撃と呼ばれています。

防御策：DHCP スヌーピング

DHCP スヌーピングとして知られるシスコの特許機能は、すべてのレイヤ 2 ポートで簡単に有効にできます。この機能では、DHCP 要求と DHCP 提供アドレスを送信できる正規の DHCP サーバに対して、信頼性のあるポートが定義されます。

VLAN 内のすべての DHCP メッセージを代行受信することにより、スイッチはユーザと正規の DHCP サーバとの間で小規模なセキュリティファイアウォールのように動作することができます。

3. 攻撃：ARP ベースの man-in-the-middle 攻撃

ARP の最も基本的な機能での使用法は、LAN セグメント上で 2 つのステーションの通信を可能にすることです。

攻撃者が偽造した送信元アドレスを持つ ARP パケットを送信すると、デフォルト ゲートウェイや他のホストはその偽造パケットを学習し、情報を自分の ARP テーブルに保存します。次に ARP によって、ターゲットのホスト内にこの悪意あるホストのエントリが作成されますが、その際に何らかの認証やフィルタリングが行われることはなく、ネットワークが脆弱化します。悪意あるホストは、2 つのエンドポイント間の通信をいずれのエンドポイントにも気付かれずに傍受できるようになります。攻撃者はパスワードやデータの収集、IP フォンの盗聴が可能になります。

防御策：ダイナミック ARP インспекション

この攻撃は、シスコのもう 1 つの特許セキュリティ機能である Dynamic ARP Inspection (DAI; ダイナミック ARP インспекション) によって簡単に防止できます。この機能を利用すると、アクセス スイッチが「有効な」ARP 要求および ARP 応答のみを中継するようにできます。DAI はスイッチ上ですべての ARP パケットを代行受信し、その ARP 情報を確認したうえで、スイッチの ARP キャッシュ更新や適切な宛先へのパケット フォワーディングを行います。

4. 攻撃：IP ホスト スプーフィング

IP アドレス スプーフィングを仕掛ける攻撃者は、手動でアドレスを変更するか、アドレス スプーフィング用に設計されたプログラムを実行することで、有効なアドレスになりすまします。インターネット ワームも、スプーフィング技術を利用して身元を偽る場合があります。

防御策：IP ソース ガード

IP ソース ガード機能を使用すると、攻撃者は有効なユーザの IP アドレスで偽装して攻撃を仕掛けることができなくなります。この機能は、有効な送信元アドレスを持つパケットのフォワーディングのみを許可します。

まとめ

モジュラ型スイッチである Cisco Catalyst 4500 シリーズは、豊富な専用ハードウェア リソースを備え、上述のレイヤ 2 セキュリティ機能やこの概要では説明していない他の多くのセキュリティ機能を実装しています。図 1 は、これらのレイヤ 2 セキュリティ機能を図式化したものです。

図 1 Cisco Catalyst 統合セキュリティ機能

