TCP SYN サービス拒絶攻撃から保護するための戦略の定義

内容

概要

Internet Service Provider (ISP; インターネット サービス プロバイダー) では、ネットワーク デバイスを対象としたサービス拒否攻撃が起こり得ます。

- **TCP SYN 攻撃**：送信者は、完了できない大量の接続を送信します。これにより接続キューが飽和して、正当な TCP ユーザへのサービスが行われなくなります。

この文書では、潜在的な TCP SYN 攻撃がどのように発生するかの技術的側面を説明し、Cisco IOS ソフトウェアを使用してこの攻撃を防御する推奨手法を説明します。

注：Cisco IOS 11.3ソフトウェアには、TCPサービス拒否攻撃を積極的に防止する機能があります。この機能は、文書「TCP インターセプトの設定 (サービス拒否攻撃の防御)」に説明されてます。

前提条件

要件

このドキュメントに関しては個別の前提条件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在的な影響について理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

問題の説明

TCP SYN 攻撃

通常の TCP 接続の開始時には、宛先ホストは発信元ホストから SYN（synchronize/start）パケットを受信し、SYN ACK（synchronize acknowledge）を返送します。 続いて、接続が確立される前に、宛先ホストは SYN ACK に対する ACK（acknowledge）を受け取る必要があります。これは、「TCP 3 ウェイ ハンドシェイク」と呼ばれます。

SYN ACK に対する ACK を待機している間、宛先ホスト上の有限サイズの接続キューは、完了を待機している接続の追跡管理を続けます。ACK は SYN ACK の数ミリ秒後に到達すると想定されており、通常、このキューはすぐに空になります。

TCP SYN 攻撃は、攻撃側発信元ホストに、標的ホストに向けてランダムな発信元アドレスを持つ TCP SYN パケットを生成させることで、この設計を不正に利用しています。標的の宛先ホストでは、このランダムな発信元アドレスに SYN ACK を返信し、接続キューにエントリを追加します。SYN ACK の宛先は不正なホストや存在しないホストなので、「3 ウェイ ハンドシェイク」の最後の部分が完了せず、タイマーが期限切れになるまで（一般的には約 1 分間）接続キューにエントリが残ってしまいます。ランダムな IP アドレスからの偽の TCP SYN パケットを高速に生成することにより、接続キューをいっぱいにして、正当なユーザへの TCP サービス（電子メール、ファイル転送、WWW など）を提供できなくすることが可能です。

発信元の IP アドレスは偽造されているので、攻撃の発信元を追跡する簡単な方法はありません。

この問題は外観上、電子メールを取得できない、WWW または FTP サービスへの接続を受け入れることができない、あるいは、ホスト上の大量の TCP 接続が SYN_RCVD 状態になる、といった症状となって現れます。

ネットワークデバイスへの不正侵入に対する防御

ファイアウォールを支えるデバイス

TCP SYN 攻撃の特徴は、ランダムな発信元 IP アドレスから SYN パケットが殺到することです。着信SYNパケットを停止するファイアウォールの背後にあるデバイスは、この攻撃モードからすでに保護されており、これ以上のアクションは必要ありません。ファイアウォールの例としては、Cisco Private Internet Exchange(PIX)ファイアウォールや、アクセスリストが設定されたCiscoルータなどがあります。Ciscoルータでアクセスリストを設定する方法の例については、ドキュメント『IPネットワークでのセキュリティの強化』を参照してください。

一般に利用可能なサービス(メールサーバ、パブリックWebサーバ) を提供するデバイス

アクセス リストを使用して、着信アクセスを選ばれた少数の IP アドレスに明示的に制限できるため、ファイアウォールの背後にあるデバイス上ではランダムな IP アドレスからの SYN 攻撃を防ぐことは比較的簡単です。しかし、インターネットにつながるパブリックWebサーバ、またはメールサーバの場合、どの着信IP送信元アドレスが友好的で、どれが非友好的なのかを判断することができません。そのため、ランダムな IP アドレスからの攻撃に対応する明解な防御策はありません。ホスト側で次の対策が選択できます。

- 接続キュー（SYN ACKキュー）のサイズを増やします。
- スリーウェイハンドシェイクのタイムアウトを減らす。
- ベンダーのソフトウェアパッチを使用して、問題を検出し、回避します（可能な場合）。

ホストのベンダーに連絡して、TCP SYN ACK 攻撃に対応するための特定のパッチをベンダーが作成しているかどうかを確認する必要があります。

注：攻撃者が自分のIPアドレスを変更する可能性があり、アドレスが正当なホストのものと同じか異なる可能性があるため、サーバでのIPアドレスのフィルタリングは無効です。

ネットワークがいつのまにか攻撃に加担している事態の防止

このサービス拒否攻撃の主なメカニズムは、ランダムな IP アドレスが送信元であるトラフィックを生成することであるため、インターネットが宛先であるトラフィックをフィルタリングすることをお勧めします。基本的に、「無効な送信元 IP アドレスを持つパケットがあればインターネットに入る前に廃棄する」と考えてください。この方法は自社のネットワークに対するサービス拒否攻撃は防止しませんが、攻撃を受けた側で、お客様のサイトを攻撃者の発信元としては除外するのに有効です。さらに、このクラスの攻撃の基盤としてネットワークの魅力を低下させます。

無効な IP アドレスの送信の禁止

お客様のネットワークをインターネットに接続するルータ上でパケットをフィルタリングすれば、有効な送信元 IP アドレスを持つパケットだけをお客様のネットワークからインターネットに送信できます。

たとえば、ネットワークがネットワーク172.16.0.0で構成されていて、ルータがシリアル0/1インターフェイスを使用してISPに接続している場合、次のようにアクセスリストを適用できます。

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 0/1
ip access-group 111 out
```

注：アクセスリストの最後の行は、無効な送信元アドレスを持つトラフィックがインターネットに着信しているかどうかを判別します。この行はそれほど重要ではありませんが、起こりうる攻撃の送信元を特定する際に役立ちます。

無効な IP アドレスの受信の禁止

エンドネットワークにサービスを提供するISPには、クライアントからの着信パケットの検証を

強く推奨します。これを行うには、境界ルータ上で着信パケットのフィルタリングを行います。

たとえば、クライアントが「serial 1/0」という名前のシリアルインターフェイスを介してルータに接続されている次のネットワーク番号を持っている場合、次のアクセスリストを作成できます。

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0.

access-list 111 permit ip 192.168.0.0 0.0.15.255 any
access-list 111 permit ip 172.18.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 1/0
ip access-group 111 in
```

注：アクセスリストの最後の行は、無効な送信元アドレスを持つトラフィックがインターネットに入っているかどうかを決定します。この行はそれほど重要ではありませんが、起こりうる攻撃の送信元を特定する際に役立ちます。

このトピックは、NANOG（North American Network Operator1s Group）のメーリング リストで一部詳細に議論されています。リストアーカイブは次の場所にあります。
http://www.merit.edu/mail.archives/nanog/index.html

TCP SYNサービス拒否攻撃およびIPスプーフィングの詳細については、次のドキュメントを参照してください。http://www.cert.org/advisories/CA-1996-21.html

http://www.cert.org/advisories/CA-1995-01.html

関連情報

- テクニカルサポート - Cisco Systems