Cisco ルータを使用したパケットフラッドの識別とトレース

目次

概要

Denial of Service（DoS; サービス拒絶）攻撃は、インターネットで一般的な攻撃です。 このような攻撃に対応するために使用する最初のステップは、攻撃の種類を正確に見分けることです。 一般的に使用される DoS 攻撃の多くは、高帯域幅のパケット フラッドや、その他の反復的なパケット ストリームによるものです。

DoS 攻撃ストリームのパケットの多くは、Cisco IOS® ソフトウェアのアクセス リスト エントリと一致する場合、分離できます。 これは、攻撃をフィルタリングする場合に有用です。 これは、不明な攻撃を識別する場合や、スプーフィングされたパケット ストリームを実際の送信元までトレースする場合にも有効です。

同様の目的のために、Cisco ルータのデバッグ ロギングや IP アカウンティングなどの機能が役立つ場合もあります（特に新しいまたはまれな攻撃に対して）。 しかし、Cisco IOS ソフトウェアの最近のバージョンでは、一般的な攻撃の識別とトレースには、主にアクセス リストとアクセス リスト ロギングが役立ちます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

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。

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。

最も一般的な DoS 攻撃

DoS 攻撃にはさまざまなタイプがあります。 ソフトウェアのバグを利用して比較的わずかなトラフィックでシステムをシャット ダウンする攻撃は無視するとしても、ネットワークを横断して送信できる IP パケットが、すべてフラッディング DoS 攻撃の実行に使用され得る事実に変わりはありません。 攻撃を受けた場合は、発生している現象が通常のカテゴリには含まれない現象である可能性を、常に疑う必要があります。

その一方で、多くの攻撃は似たようなものであるのも事実です。 攻撃者は、一般的な手法を選択するものです。これは、こうした手法が特に効果的であったり、トレースが特に困難であったり、ツールが入手できたりするためです。 多くの DoS 攻撃者は自分でツールを作成するだけのスキルまたは動機がないため、インターネットにあるプログラムを使用します。 こうしたツールには流行があります。

この稿が書かれている 1999 年 7 月の時点では、シスコへの問い合せのほとんどは「smurf」攻撃に関するものです。 この攻撃の被害者には次の2つがあります: 1 つは「最終的なターゲット」で、もう 1 つは「リフレクタ」です。 この攻撃では、リフレクタ サブネットのブロードキャスト アドレスに ICMP エコー要求 (「ping」) が大量に流されます。 これらのパケットの送信元アドレスは、最終的なターゲットのアドレスに偽装されています。 攻撃者から送信されるパケットごとに、リフレクタ サブネットの多くのホストが応答します。 それによって最終的なターゲットがフラッディングし、両方の被害者の帯域幅が消費されます。

「fraggle」と呼ばれる類似の攻撃では、同様にダイレクト ブロードキャストが使用されますが、ICMP エコー要求の代わりに UDPエコー要求が使用されます。 通常 fraggle は smurf に比べて増幅要素が小さく、それほど一般的ではありません。

smurf 攻撃は、通常はネットワーク リンクが過負荷になることによって発見されます。 これらの攻撃とその防御方法の詳細については、「Denial of Service 攻撃の情報ページ」を参照してください 。

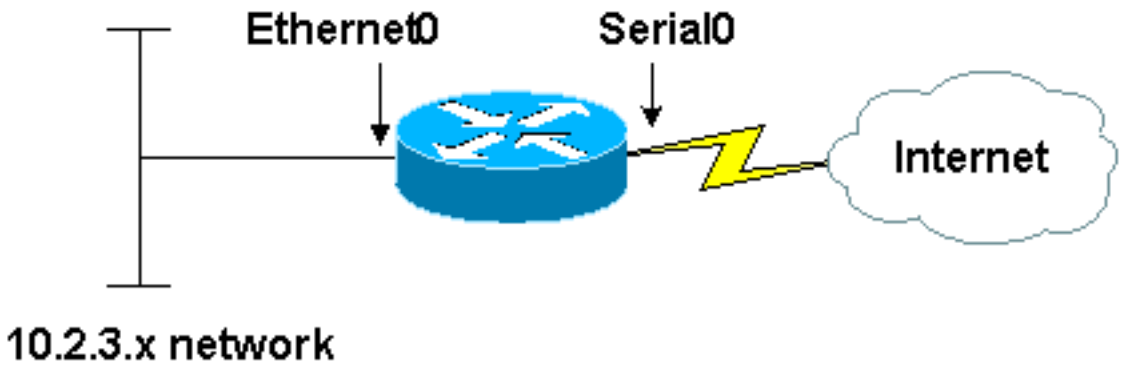
もう 1 つの一般的な攻撃として、SYN フラッドがあります。この攻撃は、ターゲット マシンを TCP 接続要求で氾濫させます。 接続要求パケットの送信元アドレスと送信元 TCP ポートはランダム化されます。 これは、完了しない多数の接続の状態情報を、ターゲット ホストに維持させることを目的としています。

SYN フラッド攻撃は、通常はターゲット ホスト（一般的に HTTP または SMTP サーバ）の極端な速度低下、クラッシュ、または停止によって明らかになります。 また、ターゲット ホストから戻るトラフィックがルータの問題を引き起こす可能性もあります。 それはこのリターン トラフィックが元のパケットのランダム化された送信元アドレスに戻ったときに、「実際の」IP トラフィックのローカル プロパティがないことから、ルート キャッシュがオーバーフローする可能性があるためです。 Cisco ルータでは、この問題はしばしばメモリ不足のルータで発生します。

シスコに報告されるフラッディング DoS 攻撃の大部分は、smurf と SYN フラッド攻撃で説明がつきます。これらの攻撃をすばやく認識することは、非常に重要です。 どちらの攻撃も（ping フラッドのようないくつかの「第 2 層」攻撃を含めて）、Cisco アクセス リストを使用して容易に認識できます。

DoS 識別アクセス リスト

2 つのインターフェイスを持つルータを考えてください。 Ethernet 0 は商用 ISP または小規模 ISP で内部 LAN に接続されています。 Serial 0 は ISP 経由でインターネット接続を提供します。 Serial 0 の入力パケット レートはフル リンク帯域幅に固定されてしまっており、LAN 上のホストでは速度低下、クラッシュ、停止、またはその他の DoS 攻撃の兆候が現れています。 ルータが接続されている小規模サイトにはネットワーク アナライザがなく、このサイトの人々は、アナライザ トレースが入手できた場合でもそれを読んだ経験がほとんどないか、まったくありません。



ここで、次の出力が示すアクセス リストを適用すると仮定します。

```
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

このリストではトラフィックがフィルタ アウトされず、 エントリはすべて許可されます。 しかし、このリストではパケットがカテゴリに分かれており、攻撃が次に挙げる 3 つのタイプのいずれであるかを診断することができます。 3 つのタイプは smurf 攻撃、SYN フラッド攻撃、fraggle 攻撃です。

smurf 攻撃の最終的なターゲット

show access-list コマンドを発行すると、次のような出力が表示されます。

```
Extended IP access list 169
    permit icmp any any echo (2 matches)
    permit icmp any any echo-reply (21374 matches)
    permit udp any any eq echo
    permit udp any eq echo any
    permit tcp any any established (150 matches)
    permit tcp any any (15 matches)
    permit ip any any (45 matches)
```

シリアル インターフェイスに着信するトラフィックのほとんどは、ICMP エコー応答パケットで構成されています。 これはおそらく smurf 攻撃のサインです。このサイトは、リフレクタではなく最終的なターゲットになっています。 次の出力に示すようにアクセス リストを変更すると、攻撃に関する詳細な情報を収集できます。

```
interface serial 0
no ip access-group 169 in

no access-list 169
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply log-input
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

ここでは、疑わしいトラフィックに一致するアクセス リスト エントリに log-input キーワードを追加しました（11.2 より前の Cisco IOS ソフトウェア リリースでは、このキーワードがありません。 代わりに「log」キーワードを使用します）。 これにより、このリスト エントリに一致するパケットに関する情報がルータにログされます。 logging buffered が設定された場合、show log コマンドによって次のメッセージが得られます（レートの制約のため、メッセージの表示に時間がかかる場合があります）。 メッセージは次の出力のように表示されます。

```
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.72
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.154
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.59
```

```
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.82
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.56
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.84
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.33
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
```

エコー応答パケットの送信元アドレスは、アドレス プレフィクス 192.168.212.0/24、192.168.45.0/24、および 172.16.132.0/24 でクラスタ化されます（192.168.x.x および 172.16.x.x ネットワークのプライベート アドレスはインターネット上にはありません。これはラボ用の例示です）。これは典型的な smurf 攻撃です。送信元アドレスは smurf リフレクタのアドレスです。適切なインターネット「whois」データベースでこれらのアドレス ブロックのオーナーを参照することにより、これらのネットワークの管理者を見つけ、攻撃への対処への協力を求めることができます。

ここでは、これらのリフレクタは smurf 攻撃の被害者であり、攻撃者ではない点を忘れないことが重要です。攻撃者が DoS フラッドの IP パケットで自分自身の送信元アドレスを使用することは非常にまれであり、smurf 攻撃を成功させるためには、そのようなことはあり得ないことです。フラッド パケット内のどのアドレスも、完全に偽装されているか、または何らかの被害者のアドレスと考える必要があります。smurf 攻撃の最終的なターゲットにとって最も生産的なアプローチは、リフレクタに連絡を取り、ネットワークを再設定して攻撃を遮断するよう依頼するか、攻撃的なストリームのトレースへの協力を依頼することです。

smurf 攻撃の最終的なターゲットの被害は、インターネットからの着信リンクの過負荷が原因であることが多いため、通常はリフレクタに連絡する以外の対応はありません。パケットがターゲットの管理下にあるすべてのマシンに到達するまでに、ほとんどの部分がすでに被害を受けています。

急場をしのぐための対応策の 1 つとしては、上流のネットワーク プロバイダーに、すべての ICMP エコー応答、または特定のリフレクタからのすべての ICMP エコー応答を、フィルタ アウトするように依頼する方法があります。このタイプのフィルタを設定したままにすることは推奨されません。一時的なフィルタの場合も、フィルタにかけるのはエコー応答のみで、すべての ICMP パケットではないことが必要です。その他に、アップストリームのプロバイダーが QoS およびレート制限機能を使用して、エコー応答で利用可能な帯域幅を制限することが可能です。適切な帯域幅の制限は、無期限に維持しておくことができます。どちらのアプローチも、アップストリームのプロバイダーの機器に必要な容量があることが前提になりますが、その容量が得られない場合があります。

smurf 攻撃のリフレクタ

着信トラフィックがエコー応答ではなくエコー要求から構成されている場合（すなわち、2 番目ではなく最初のアクセス リスト エントリで通常よりも多くの一致がカウントされている場合）は、ネットワークが smurf 攻撃のリフレクタとして使用されているか、または単純な ping フラッドが発生している可能性があります。どらちのケースでも、攻撃が成功していた場合は、シリアル

回線の着信側だけでなく発信側でも攻撃が発生していることが疑われます。 実際、増幅要素のために、発信側では着信側よりもさらに過大な負荷が発生していると考えられます。

smurf 攻撃と単なる ping フラッドを見分けるには、次の方法があります。

- smurf 攻撃のパケットは、ユニキャスト アドレスではなくダイレクト ブロードキャスト アドレスに送信されます。これに対して通常の ping フラッドは、ほぼ 100 % ユニキャストを使用します。 **log-input** キーワードを使用するアドレスは、該当するアクセス リスト エントリで確認できます。
- smurf リフレクタとして使用されている場合は、システムのイーサネット側の **show interface** 表示に異常な数の出力ブロードキャストが現れます。また、通常は **show ip traffic** 表示に異常な数の送信ブロードキャストが現れます。 通常の ping フラッドでは、バックグラウンド ブロードキャスト トラフィックは増加しません。
- smurf リフレクタとして使用されている場合は、インターネットからの着信トラフィックよりもインターネットへの発信トラフィックの方が多くなります。 一般的に、シリアル インターフェイスでは入力パケットよりも出力パケットの方が多くなります。 入力インターフェイスが攻撃ストリームで完全に充溢しても、応答ストリームは攻撃ストリームよりも大きく、パケット ドロップがカウントされます。

smurf リフレクタには、smurf 攻撃の最終的なターゲットよりも多くの選択肢があります。 リフレクタが攻撃を排除する場合は、通常 **no ip directed-broadcast** (または同等の非 IOS コマンド) が役に立ちます。 これらのコマンドは、アクティブな攻撃がない場合でもすべての設定に属します。 Cisco 機器が smurf 攻撃に使用されることを防止する方法については、「Cisco ルータにおけるセキュリティの向上」を参照してください。 smurf 攻撃に関する全般的な情報と Cisco 以外の機器の保護については、「DoS 攻撃に関する情報」ページを参照してください 。

smurf リフレクタは最終的なターゲットよりも攻撃者に 1 段階近いため、攻撃をよりトレースしやすい位置にいます。 攻撃をトレースする場合は、関係する ISP と協力する必要があります。 トレースを完了した後に何らかの措置を講じる場合は、適切な捜査機関と連携する必要があります。 攻撃のトレースを試みる場合は、できるだけ早い段階で捜査機関の協力を要請してください。 フラッディング攻撃に関する技術情報については、「トレース」のセクションを参照してください。

fraggle

fraggle 攻撃は、攻撃ストリームに ICMP エコー要求ではなく UDP エコー要求が使用される点を除いては、smurf に類似しています。 fraggle 攻撃は、アクセス リストの 3 行目および 4 行目から識別されます。 被害に対する適切な対応方法はほぼ同じですが、ほとんどのネットワークでは UDP エコー サービスの重要度は ICMP エコーよりも低くなっています。 したがってそれらを完全に無効にしても、マイナスの影響はあまりありません。

SYN フラッド

アクセス リストの 5 行目と 6 行目が次のようになりました。

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
```

これらのうち最初の行では、TCP パケットを ACK ビット セットと照合します。 ここでは、TCP SYN ではないパケットの照合が目的です。 したがって 2 番目の行では、TCP SYN であるパケットのみを照合します。 SYN フラッドは、これらのリスト エントリのカウンタから簡単に識別されます。 正常なトラフィックでは、非 SYN TCP パケットは、SYN よりも少なくとも 2 倍、通常は 4 倍または 5 倍多くなります。 SYN フラッドでは、SYN の数が 非 SYN TCP パケットの数

を何度も超えるのが特徴です。

攻撃以外の条件でこのような現象が発生するのは、大量の正常な接続要求による過負荷の場合に限られます。 一般的に、このような過負荷は突然発生し、真の SYN フラッドほど多くの SYN パケットを伴いません。 また多くの場合 SYN フラッドには、完全に無効な発信元アドレスを持つパケットが含まれています。 **log-input** キーワードを使用することにより、接続要求がこのようなアドレスから送信されているかどうかを確認できます。

SYN フラッドに似た攻撃に、「プロセス テーブル攻撃」と呼ばれる攻撃があります。 プロセス テーブル攻撃では、TCP 接続の完了後に、それ以上プロトコル トラフィックがない状態でタイムアウトまで放置されます。これに対して SYN フラッドでは、最初の接続要求のみが送信されます。 プロセス テーブル攻撃では TCP の最初のハンドシェイクが完了する必要があるため、一般的に攻撃者がアクセス (通常は不正アクセス) 可能な実際のマシンの IP アドレスを使用して実行する必要があります。 したがってプロセス テーブル攻撃は、パケット ロギングを使用することで SYN フラッドと簡単に識別できます。 プロセス テーブル攻撃の SYN は、すべて 1 つまたは少数のアドレス、あるいは多くても 1 つまたは少数のサブネットから送信されます。

SYN フラッドの被害者が取ることができる対応は非常に限られています。 一般に攻撃を受けるシステムは重要なサービスであるため、システムへのアクセスをブロックすることは攻撃者の思うつぼです。 シスコ製品を含む多くのルータやファイアウォール製品には、SYN フラッドの影響を軽減するために使用できる機能があります。 ただし、これらの機能の効果は環境によって異なります。 詳細については、Cisco IOS ファイアウォール機能セットおよび Cisco IOS TCP の代行受信機能のマニュアル、『Cisco ルータにおけるセキュリティの向上』を参照してください。

SYN フラッドのトレースは可能ですが、トレースのプロセスでは、攻撃者から被害者までの経路における各 ISP の協力が必要です。 SYN フラッドのトレースを試みる場合は、早い段階で捜査機関に連絡し、アップストリーム サービス プロバイダーの協力を仰いでください。 シスコの機器を使用したトレースの詳細については、このドキュメントの「トレース」のセクションを参照してください。

その他の攻撃

攻撃を受けていると考えられ、かつ送信元および宛先の IP アドレス、プロトコル番号、およびポート番号を使用してその攻撃を識別できる場合は、アクセス リストを使用して仮説を検証することができます。 疑わしいトラフィックに一致するアクセス リスト エントリを作成し、適切なインターフェイスに適用し、一致カウンタを検討するか、トラフィックをログしてください。

ロギングおよびカウンタに関する注意

アクセス リスト エントリのカウンタは、そのエントリに対するすべての一致をカウントします。あるアクセス リストを 2 つのインターフェイスに適用した場合、表示されるカウントは 2 つの合計になります。

アクセス リスト ロギングでは、あるエントリに一致するすべてのパケットが表示されるわけではありません。 ロギングは、CPU への過負荷を避けるためにレートが制限されます。 ロギングで表示されるのは十分に代表的と呼べるサンプルですが、完全なパケット トレースではありません。 表示されないパケットがあることに注意してください。

一部のソフトウェア バージョンでは、アクセス リスト ロギングが一部のスイッチング モードでしか動作しません。 アクセス リスト エントリで、多数の一致がカウントされても何もログされない場合は、ルート キャッシュをクリアして、パケットのプロセスを強制的に切り替えてみてください。 ただし、多数のインターフェイスがある負荷の高いルータでこれを行う場合は注意して

ください。 キャッシュが再構築される間に、多数のトラフィックが廃棄される可能性があります。 可能な限り Cisco Express Forwarding を使用してください。

アクセス リストとロギングはパフォーマンスに影響を与えますが、大きな影響ではありません。ルータの CPU 負荷がおよそ 80 % を超えている場合や、アクセス リストを非常に高速のインターフェイスに適用する場合は、注意が必要です。

トレース

DoS パケットの送信元アドレスはほとんどの場合、攻撃者自身とは無関係な値に設定されています。 そのため、攻撃者の識別には役立ちません。 攻撃の発信元を識別するために役立つ唯一の方法は、ネットワークをホップバイホップでトレースしていくことです。 このプロセスでは、ルータの再設定と ログ情報のチェックを行います。 攻撃者から被害者までのパスに沿ったすべてのネットワーク オペレータによる協力が必要です。 こうした協力を確保するためには、通常は捜査機関の関与が必要です。また、攻撃者に対して何らかの行動を起こすためにも、捜査機関の関与は必要です。

DoS フラッドのトレース プロセスは、比較的シンプルです。 まずフラッド トラフィックを転送していることがわかっているルータ（「A」と呼びます）から開始し、A がそのトラフィックを受信している元のルータ（「B」と呼びます）を識別します。 次に B にログインし、B がそのトラフィックを受信している元のルータ（「C」と呼びます）を見つけます。 最終的な送信元が発見されるまでこれを続けます。

この方法については、次のような複雑な要素があります。

- 「最終的な送信元」が、確かに攻撃者が構成したコンピュータであっても、実際には他の被害者によって所有され操作されているコンピュータである場合があります。 この場合、DoS フラッドのトレースは第 1 段階に過ぎません。
- 攻撃者はトレースされることを認識しているため、限られた時間のみ攻撃を続けます。 フラッドを実際にトレースできるだけの時間がない場合があります。
- 特に攻撃者が比較的高度な技術を持つ場合、複数の送信元から攻撃が来る場合があります。可能な限り多くの送信元の識別を試みることが重要です。
- コミュニケーションに問題があると、すばやいトレース プロセスが不可能になります。 関係するネットワーク オペレータによっては、十分な技術力を持つスタッフがいない場合がしばしばあります。
- 攻撃者が発見された場合でも、法的および政治的問題のために攻撃者に対する措置が困難になる場合があります。

DoS 攻撃をトレースしようとしてもほとんどが失敗してしまいます。 このため多くのネットワーク オペレータは、圧力を受けない限り攻撃のトレースを試みることさえしません。 「重大な」攻撃のみをトレースするネットワーク オペレータも多くありますが、何が「重大」かの定義はさまざまです。 捜査機関が関与した場合にのみトレースに協力するネットワーク オペレータもあります。

「log-input」によるトレース

Cisco ルータを通過する攻撃をトレースする場合、最も効果的な方法は攻撃トラフィックに一致するアクセス リスト エントリを構築し、**log-input** キーワードを指定し、攻撃ストリームが最終的なターゲットに送信される経路になっているインターフェイスの発信側に、そのアクセス リストを適用することです。 アクセス リストによって生成されたログ エントリは、トラフィックが通過するルータ インターフェイスを識別し、インターフェイスがマルチポイント接続の場合は、受

信デバイスのレイヤ 2 アドレスを割り当てます。 次にそのレイヤ 2 アドレスを使用して、チェーン内の次のルータを識別できます。これには、たとえば **show ip arp mac-address** コマンドを使用します。

SYN フラッド

SYN フラッドをトレースするために、次のようなアクセス リストを作成できます。

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any host victim-host log-input
access-list 169 permit ip any any
```

これにより、ターゲット ホスト宛ての SYN が、正当な SYN を含めてすべてログされます。 攻撃者への実際の経路として最も可能性が高い経路を識別するには、ログ エントリを詳細に検査します。 一般的に、最も多くの一致パケットを送信しているのがフラッドの送信元です。 発信元の IP アドレス自体は何も意味しません。 ここでは送信元インターフェイスと送信元 MAC アドレスを探します。 フラッディング パケットが無効な送信元アドレスを持つことがあるため、正当なパケットとフラッディング パケットを区別することが可能です。 送信元アドレスが不正なパケットはすべて、フラッドの一部である可能性があります。

フラッディングは複数の送信元から行われる場合がありますが、SYN フラッドに関しては比較的まれです。

smurf 攻撃

smurf 攻撃ストリームをトレースするには、次のようなアクセス リストを使用します。

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any host victim-host log-input
access-list 169 permit ip any any
```

最初のエントリはリフレクタ アドレス宛てのパケットを排除しない点に注意してください。 これは、ほとんどの smurf 攻撃は複数のリフレクタ ネットワークを使用するためです。 最終的なターゲットと連絡が取れない場合は、リフレクタ アドレスをすべて知ることができない場合があります。 トレースが攻撃の送信元に近づくと、より多くの宛先にエコー要求が送信されることを確認できます。 これはよい兆候です。

ただし、大量の ICMP トラフィックを扱う場合は、簡単に読めないほどの大量のロギング情報が生成される可能性があります。 この場合は、宛先アドレスを、使用されていることが判明しているリフレクタのうちの 1 つに絞ることもできます。 その他に、255.255.255.0 のネットマスクは、インターネット内で非常に一般的であるという事実を利用したエントリを使用する方法もあります。 攻撃者が smurf リフレクタを発見する方法上の理由で、smurf 攻撃に実際に使用されるリフレクタ アドレスは、非常に高い確率でこのマスクに一致します。 .0 または .255 で終わるホスト アドレスは、インターネット内では非常にまれです。 したがって次の出力のように、smurf 攻撃のストリームに対して比較的に特定の認識エンジンを構築できます。

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any host victim-host log-input
access-list 169 permit ip any any
```

このリストでは、ログから多数の「ノイズ」パケットを排除できる一方、攻撃者に近づくにつれてさらに多くの攻撃ストリームを発見できる可能性があります。

「log-input」によらないトレース

log-input キーワードが存在するのは、Cisco IOS ソフトウェア バージョン 11.2 以降と、サービ

スプロバイダー市場向けに特別に作成された 11.1 ベースのソフトウェアです。 古いソフトウェアでは、このキーワードがサポートされません。 古いソフトウェアを持つルータを使用している場合は、次の 3 つのオプションがあります。

- ロギングを含まないが、疑わしいトラフィックに一致するエントリを含むアクセス リストを作成します。 各インターフェイスの*入力側*にこのリストを適用し、カウンタを調べます。 一致率の高いインターフェイスを探します。 この方法はパフォーマンス オーバーヘッドが非常に小さく、発信元インターフェイスを識別するために優れています。 この方法の最大の欠点は、リンク層送信元アドレスが得られないことです。したがって、この方法はポイントツーポイント回線に最も役立ちます。
- **log-input** ではなく、**log** キーワードを含むアクセス リスト エントリを作成します。 再び、各インターフェイスの着信側にこのリストを適用します。 この方法でも発信元 MAC アドレスは提供されませんが、IP データを表示するために役立つ可能性があります。 たとえば、あるパケット ストリームが実際に攻撃の一部であるかどうかを確認できます。 パフォーマンスへの影響は中 ~ 高で、新しいソフトウェアのほうが古いソフトウェアよりもパフォーマンスが高くなります。
- **debug ip packet detail** コマンドを使用して、パケットに関する情報を収集します。 この方法では MAC アドレスが得られますが、パフォーマンスに大きな影響が発生する可能性があります。 この方法を誤って使用すると、容易にルータが使用不可能になります。 この方法を使用する場合は、ルータが攻撃トラフィックをファースト、自律、または最適のいずれかのモードでスイッチングしていることを確認してください。 アクセス リストを使用して、デバッグをほんとうに必要な情報のみに制限します。 ローカル ログ バッファにデバッグ情報をログしますが、Telnet セッションとコンソールに対してはデバッグ情報のロギングをオフにします。 可能であれば、必要に応じて電源のオン→オフができるように、ルータに物理的に近い位置に人を配置します。**debug ip packet** コマンドでは、ファースト スイッチングされたパケットに関する情報は表示されないことに注意してください。 この情報の取得には、**clear ip cache** コマンドを実行する必要があります。 **clear** コマンドでは、デバッグ出力の 1 つまたは 2 つのパケットが得られます。

関連情報

- Kerberos
- テクニカルサポートとドキュメント - Cisco Systems