ASA/PIX 7.x 以降： ネットワーク攻撃の緩和策

目次

概要

このドキュメントでは、Cisco セキュリティ アプライアンス（ASA/PIX）を使用して、Denial-of-Services（DoS; サービス拒絶）などのさまざまなネットワーク攻撃を緩和する方法を説明しています。

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

このドキュメントの情報は、ソフトウェア バージョン 7.0 以降が稼働する Cisco 5500 シリーズ Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

このドキュメントは、ソフトウェア バージョン 7.0 以降が稼働する Cisco 500 シリーズ PIX にも適用できます。

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。

SYN 攻撃に対する防御

ASA/PIX 上では、Transmission Control Protocol（TCP; 伝送制御プロトコル）synchronize/start（SYN）攻撃をどのような方法で緩和できるのでしょうか。

TCP SYN 攻撃

TCP SYN 攻撃は、完全に処理することが不可能な大量の接続を送信元が送りつける、DoS 攻撃（サービス拒絶攻撃）の一種です。 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。

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 パケットを受信し、synchronize acknowledge（SYN ACK）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 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。

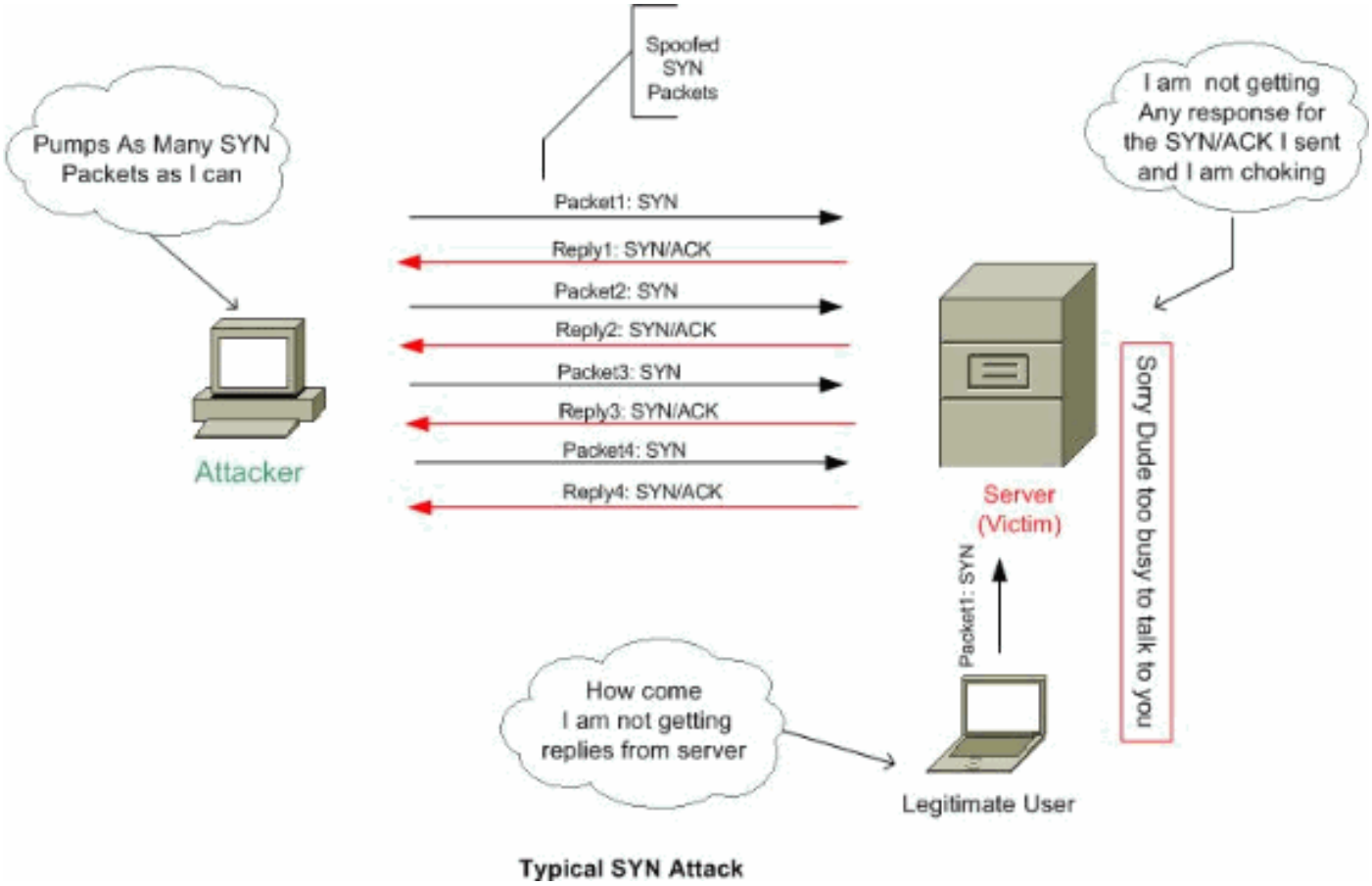
SYN ACK に対する ACK を待機している間、宛先ホスト上の有限サイズの接続キューは、完了を待機している接続の追跡管理を続けます。 ACK は SYN ACK の数ミリ秒後に到達すると想定されており、通常、このキューはすぐに空になります。

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。

TCP SYN 攻撃についての詳細は、『TCP SYN フラッディング攻撃に対する防御』を参照してください。



Typical SYN Attack

緩和策

このセクションでは、TCP と User Datagram Protocol (UDP; ユーザ データグラム プロトコル) の最大接続数、最大初期接続数、接続タイムアウトを設定することで SYN 攻撃を緩和する方法と、TCP シーケンスのランダム化をディセーブルにする方法を説明しています。

初期接続の制限に達すると、SYN+ACK を使用してサーバに送信された各 SYN パケットがセキュリティ アプライアンスによって応答されますが、SYN パケットは内部サーバへは受け渡されません。 外部デバイスによって ACK パケットが応答されると、セキュリティ アプライアンスではこれが有効な要求である (さらに潜在的な SYN 攻撃の一部ではない) と認識されます。 次に、セキュリティ アプライアンスではサーバとの接続が確立され、各接続がまとめられます。 セキュリティ アプライアンスでサーバから戻される ACK が受信されない場合、初期接続は積極的にタイムアウトにされます。

各 TCP 接続には、2 つの Initial Sequence Number (ISN; 初期シーケンス番号) が存在します。 そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。 セキュリティ アプライアンスによって、着信と発信の両方向で通過する TCP SYN の ISN がランダム化されます。

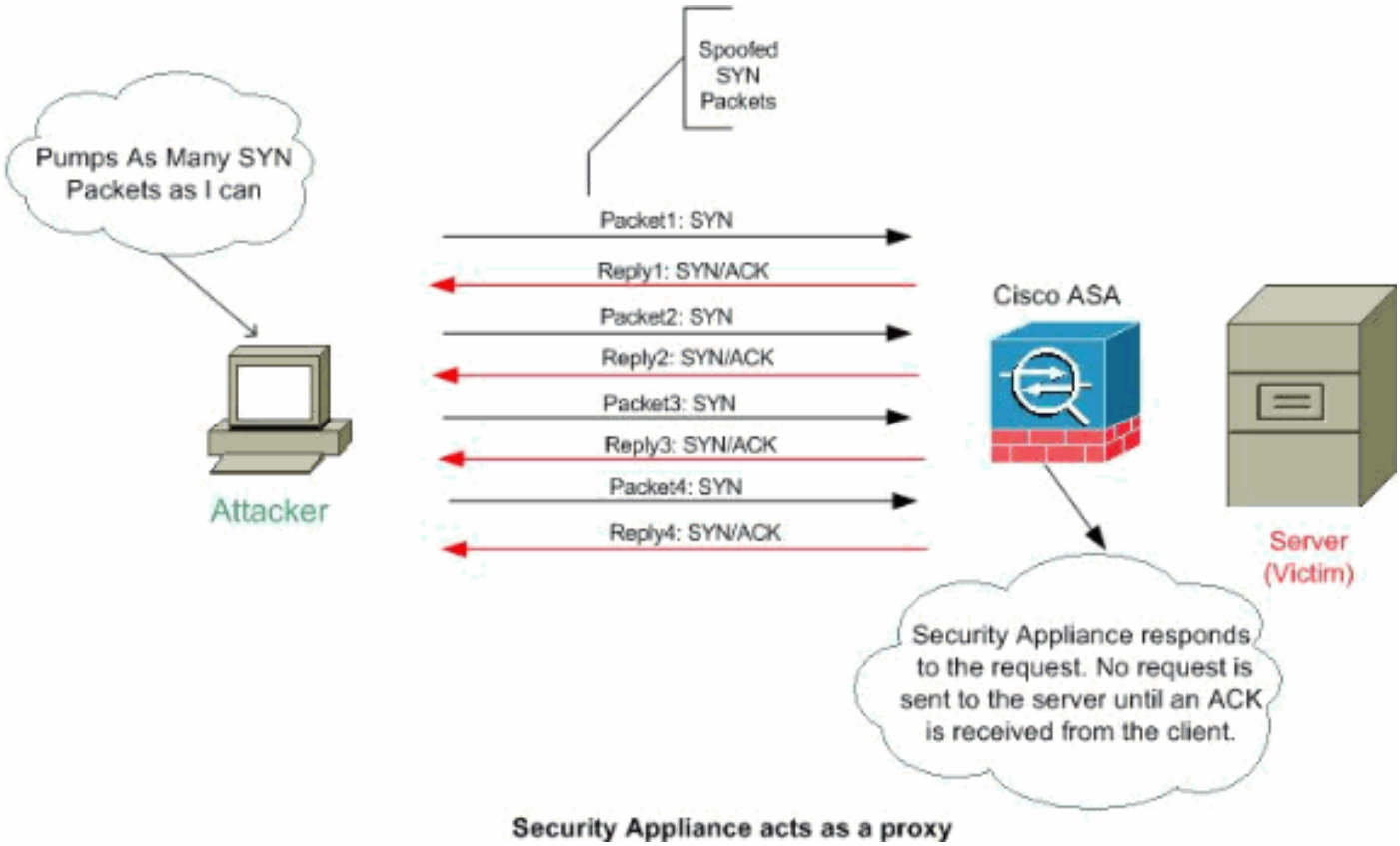
保護されたホストの ISN のランダム化によって、攻撃者が新規の接続の次の ISN を予測することが防止され、新規のセッションに対する潜在的な乗っ取りが防止されます。

TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにすることができます。 次に、例を示します。

- 別のインライン ファイアウォールでも初期シーケンス番号のランダム化が行われている場合、この処理によるトラフィックへの影響がなくても、両方のファイアウォールによってこの処理が実行される必要はありません。

- セキュリティ アプライアンスを経由する external BGP（eBGP; 外部 BGP）マルチホップを使用し、eBGP ピアで MD5 が使用されている場合、ランダム化によって MD5 チェックサムが分割されます。
- セキュリティ アプライアンスで接続のシーケンス番号のランダム化が実行されないことが要件となる Wide Area Application Services（WAAS）デバイスを使用します。

注: NAT 設定では、最大接続数、最大初期接続数、および TCP シーケンスのランダム化を設定することもできます。 両方の方式を使用してこれらの設定を同じトラフィックに設定する場合、セキュリティ アプライアンスでは低い制限が使用されます。 TCP シーケンスのランダム化については、どちらかの方式を使用してディセーブルになっている場合、セキュリティ アプライアンスでは TCP シーケンスのランダム化がディセーブルにされます。



Security Appliance acts as a proxy

接続の制限を設定するには、次の手順を実行します。

1. トラフィックを識別するには、『モジュラ ポリシー フレームワークの使用』に従って **class-map** コマンドを使用し、クラス マップを追加します。
2. クラス マップ トラフィックで適用される処理を設定する**ポリシー マップ**を追加したり編集したりするには、次のコマンドを入力します。`hostname(config)#`**`policy-map name`**
3. 処理を割り当てる（手順 1 からの）クラス マップを識別するには、次のコマンドを入力します。`hostname(config-pmap)#`**`class class_map_name`**
4. 最大接続数（TCP と UDP の両方）、最大初期接続数、per-client-embryonic-max、per-client-max を設定したり、TCP シーケンスのランダム化をディセーブルにするかどうかを設定したりするには、次のコマンドを入力します。`hostname(config-pmap-c)#`**`set connection`** `{[`**`conn-max`** `number] [`**`embryonic-conn-max`** `number] [`**`per-client-embryonic-max`** `number] [`**`per-client-max`** `number][`**`random-sequence-number`** `{`**`enable`** `|` **`disable`**`}}` この場合、数は 0 ~ 65535 の整数です。 デフォルトは 0 であり、これは接続数に制限がないことを意味しています。このコマンドすべてを 1 行で入力することも（順番は任意）、各アトリビュートを個別のコマンドとして入力することもできます。 実行コンフィギュレーションでは、コマンドは 1 行にまとめられます。

5. 接続、初期接続（ハーフオープン）、およびハーフクローズの接続にタイムアウトを設定するには、次のコマンドを入力します。`hostname(config-pmap-c)#set connection {[embryonic hh[:mm[:ss]]] [half-closed hh[:mm[:ss]]] [tcp hh[:mm[:ss]]]}` **embryonic** hh[: mm[: ss] は 0:0:5 ~ 1192:59:59 の時間です。 デフォルトは 0:0:30 です。 また、この値を 0 に設定することもでき、これは接続にタイムアウトが発生しないことを意味しています。**half-closed** hh[: mm[: ss] および **tcp** hh[: mm[: ss] の値は 0:0:5 ~ 1192:59:59 の時間です。 **half-closed** のデフォルトは 0:10:0 で、**tcp** のデフォルトは 1:0:0 です。 また、これらの値を 0 に設定することもでき、これは接続にタイムアウトが発生しないことを意味しています。このコマンドすべてを 1 行で入力することも（順番は任意）、各アトリビュートを個別のコマンドとして入力することもできます。 実行コンフィギュレーションでは、コマンドは 1 行にまとめられます。**初期（ハーフオープン）接続**：初期接続とは、発信元と宛先の間で必要なハンドシェイクが完了していない TCP 接続です。**ハーフクローズ接続**：ハーフクローズ接続とは、FIN を送信することで一方向でのみ接続が閉じられている場合です。 ただし、ピアによって TCP セッションは維持されたままです。**Per-client-embryonic-max**：クライアントごとに許可された同時初期接続の最大数であり、0 ~ 65535 です。 デフォルトは 0 であり、無制限の接続数が許可されます。**Per-client-max**：クライアントごとに許可された同時接続の最大数であり、0 ~ 65535 です。 デフォルトは 0 であり、無制限の接続数が許可されます。
6. 1 つ以上のインターフェイスでポリシー マップをアクティブにするには、次のコマンドを発行します。`hostname(config)#service-policy policymap_name {global | interface interface_name}` この場合、**global** ではすべてのインターフェイスにポリシー マップが適用され、**interface** では 1 つのインターフェイスにポリシーが適用されます。 許可されるグローバル ポリシーは 1 つだけです。 インターフェイスでは、そのインターフェイスへサービス ポリシーを適用することで、グローバル ポリシーを上書きできます。 各インターフェイスに適用できるポリシー マップは 1 つだけです。

例：

```
ciscoasa(config)#class-map tcp_syn ciscoasa(config-cmap)#match port tcp eq 80 ciscoasa(config-cmap)#exit ciscoasa(config)#policy-map tcpmap ciscoasa(config-pmap)#class tcp_syn ciscoasa(config-pmap-c)#set connection conn-max 100 ciscoasa(config-pmap-c)#set connection embryonic-conn-max 200 ciscoasa(config-pmap-c)#set connection per-client-embryonic-max 10 ciscoasa(config-pmap-c)#set connection per-client-max 5 ciscoasa(config-pmap-c)#set connection random-sequence-number enable ciscoasa(config-pmap-c)#set connection timeout embryonic 0:0:45 ciscoasa(config-pmap-c)#set connection timeout half-closed 0:25:0 ciscoasa(config-pmap-c)#set connection timeout tcp 2:0:0 ciscoasa(config-pmap-c)#exit ciscoasa(config-pmap)#exit ciscoasa(config)#service-policy tcpmap global
```

注: 特定のホストのハーフオープン セッションの合計数を確認するには、このコマンドを使用します。

```
ASA-5510-8x# show local-host all Interface dmz: 0 active, 0 maximum active, 0 denied Interface management: 0 active, 0 maximum active, 0 denied Interface xx: 0 active, 0 maximum active, 0 denied Interface inside: 7 active, 18 maximum active, 0 denied local host: <10.78.167.69>, TCP flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark = unlimited UDP flow count/limit = 0/unlimited
```

注: 行 TCP embryonic count to host は、ハーフオープン セッションの数を表示します。

IP スプーフィング攻撃に対する防御

PIX/ASA では IP スプーフィング攻撃をブロックできるのでしょうか。

IP スプーフィング

アクセスを可能にするために、侵入者はスプーフィングされた送信元 IP アドレスを使用してパケットを作成します。 これによって、IP アドレスに基づく認証が使用されるアプリケーションが悪用され、不正なユーザと対象のシステムでの潜在的なルート（root）アクセスへとつながります。 rsh や rlogin などのサービスが例として挙げられます。

フィルタリング ルータ ファイアウォールによって、送信元アドレスがローカル ドメイン内ではない着信パケットがフィルタリングされるように設定されていない場合、これらのフィルタリング ルータ ファイアウォールを介してパケットをルーティングすることが可能です。 応答パケットが攻撃者に到達できない場合であっても、説明された攻撃が可能であることに注意することが重要です。

潜在的に脆弱な構成例の一部を次に示します。

- プロキシ アプリケーションによって認証に送信元 IP アドレスが使用されるプロキシ ファイアウォール
- 複数の内部インターフェイスがサポートされる外部ネットワークへのルータ
- 内部ネットワークでサブネット化がサポートされる 2 つのインターフェイスが含まれたルータ

緩和策

Unicast Reverse Path Forwarding（uRPF）では、ルーティング テーブルに従ってすべてのパケットに正しい発信元インターフェイスに一致する送信元 IP アドレスが含まれていることを確認することで、（実際の発信元を不明瞭にするために、パケットによって誤った送信元 IP アドレスが使用される）IP スプーフィングに対する防御が行われます。

通常、セキュリティ アプライアンスでは、パケットの転送先を判断する際に宛先アドレスが参照されるだけです。 ユニキャスト RPF では、セキュリティ アプライアンスに対して、送信元アドレスも参照するように指示が行われます。 これが、**Reverse Path Forwarding（RPF）**と呼ばれる理由です。 セキュリティ アプライアンスの通過を許可するトラフィックについては、セキュリティ アプライアンス ルーティング テーブル内に送信元アドレスへ戻るルートが含まれている必要があります。 RFC 2267 を参照してください。 詳しい情報が掲載されています

注: : `-- %PIX-1-106021:` リバース パス チェックが有効になっていると、Deny protocol reverse path check from src_addr to dest_addr on interface int_name ログ メッセージが表示される場合があります。 この問題を解決するには、**no ip verify reverse-path interface (interface name)** コマンドでリバース パス チェックを無効にします。

`no ip verify reverse-path interface (interface name)`

Outside トラフィックの場合、たとえば、セキュリティ アプライアンスではユニキャスト RPF の保護に対応するためにデフォルト ルートを使用することができます。 Outside インターフェイスからトラフィックが着信し、送信元アドレスがルーティング テーブルで認識されない場合、セキュリティ アプライアンスではデフォルト ルートが使用され、送信元インターフェイスとして Outside インターフェイスが正しく識別されます。

ルーティング テーブルで認識されていても、Inside インターフェイスと関連付けられているアドレスから Outside インターフェイスにトラフィックが着信する場合、セキュリティ アプライアンスによってパケットが廃棄されます。 同様に、不明な送信元アドレスから Inside インターフェイスにトラフィックが着信すると、一致するルート（デフォルト ルート）には Outside インターフェイスが示されるため、セキュリティ アプライアンスによってパケットが廃棄されます。

ユニキャスト RPF は次のように実装されています。

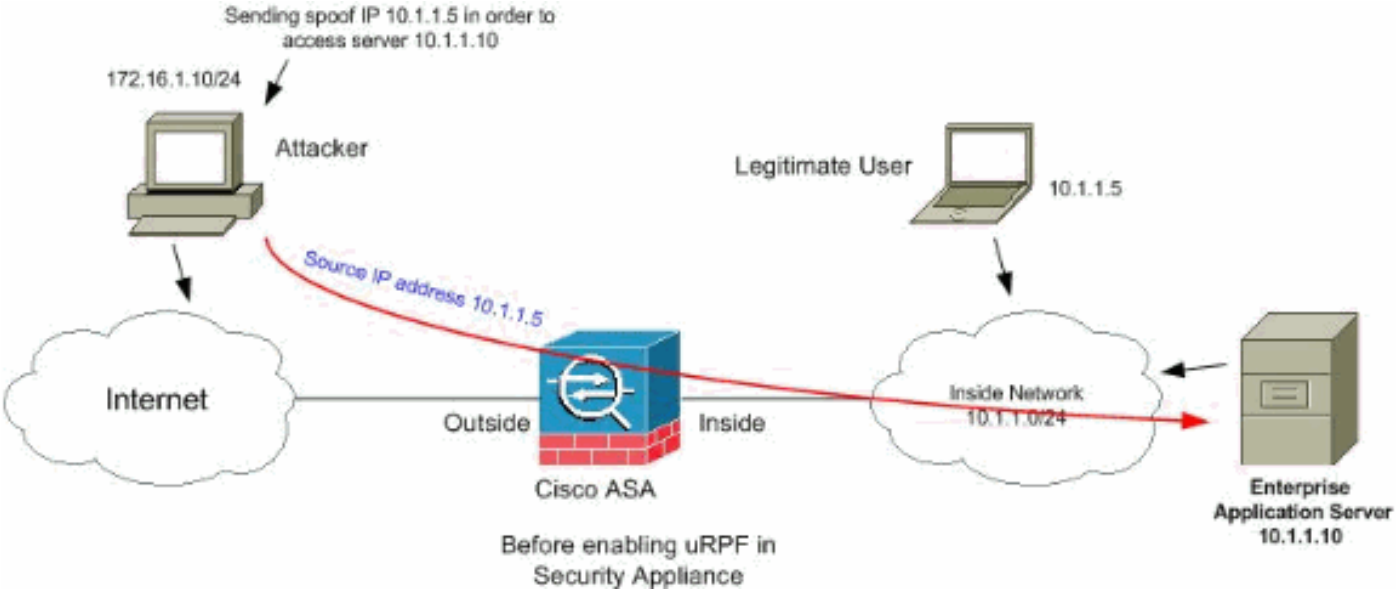
- ICMP パケットにはセッションが含まれていないため、各パケットがチェックされます。
- UDP と TCP にはセッションが含まれているため、初期パケットには逆ルートのルックアップが必要です。 セッション中に着信する後続のパケットは、セッションの一部として維持されている既存の状態を使用してチェックされます。 先頭以外のパケットは、先頭のパケットによって使用される同じインターフェイスに着信したことを確認するためにチェックされます。

ユニキャスト RPF をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)#ip verify reverse-path interface interface_name
```

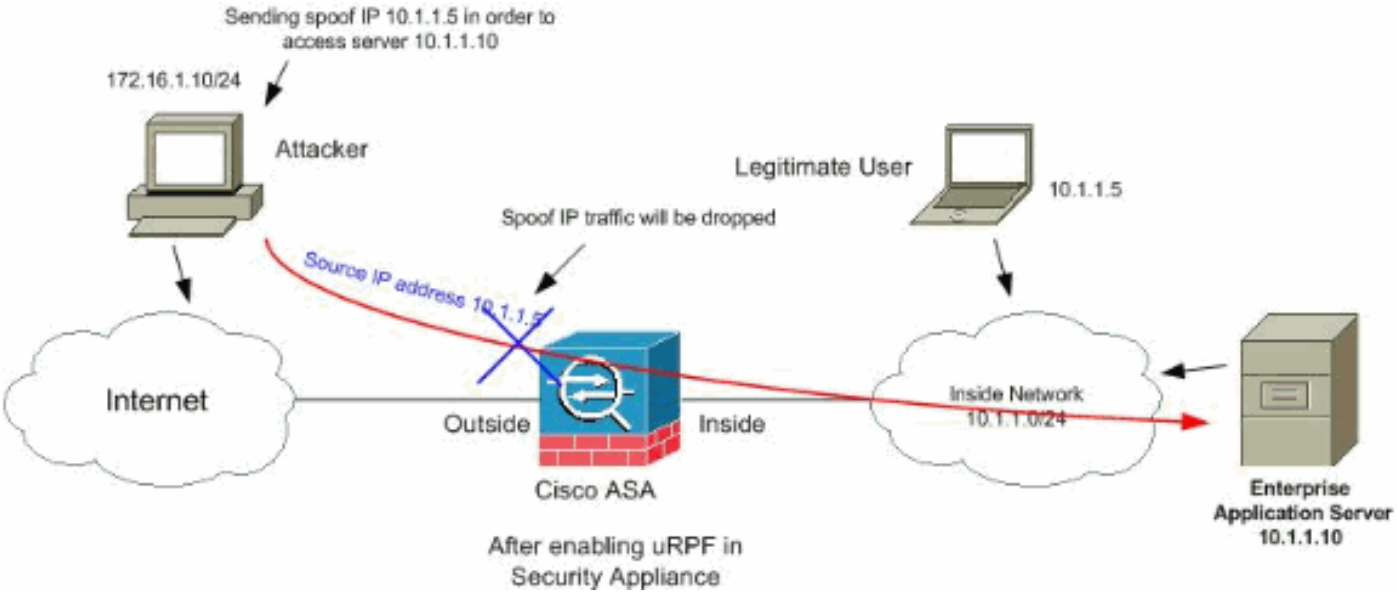
例：

次の図に示すように、攻撃者の PC では、偽造された送信元 IP アドレス 10.1.1.5/24 が含まれたパケットを送信することで、アプリケーション サーバ 10.1.1.10 に要求が発信され、サーバではこの要求への応答として、実際の IP アドレス 10.1.1.5/24 にパケットが送信されます。 このタイプの不正パケットによって、Inside ネットワーク内のアプリケーション サーバと正当なユーザの両方が攻撃されます。



ユニキャスト RPF では、送信元アドレスのスプーフィングに基づいた攻撃を防止することができます。 次に示すように、ASA の Outside インターフェイスで uRPF を設定する必要があります。

```
ciscoasa(config)#ip verify reverse-path interface outside
```



syslog メッセージを使用したスプーフィングの識別

セキュリティ アプライアンスでは、次に示すような syslog エラー メッセージが継続して受信されます。 これは、スプーフィングされたパケットを使用した潜在的な攻撃か、非対称ルーティングが原因でトリガーが実行される場合がある潜在的な攻撃を示しています。

1. **%PIX|ASA-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name** **説明**これは接続に関連したメッセージです。 このメッセージは、Inside アドレスへの接続の試行が、指定されたトラフィック タイプに定義されたセキュリティ ポリシーによって拒否される場合に表示されます。 表示される *tcp_flags* 値は、接続が拒否されたときに存在していた TCP ヘッダー内のフラグに対応します。 たとえば、セキュリティ アプライアンス内で接続状態が存在しない TCP パケットが着信し、廃棄されています。 このパケット内の *tcp_flags* は FIN および ACK です。*tcp_flags* は次のとおりです。ACK： 確認応答の番号が受信されました。FIN： データが送信されました。PSH： レシーバはデータをアプリケーションに受け渡しました。RST： 接続がリセットされました。SYN： 接続を開始するために、シーケンス番号が同期されました。URG： 緊急ポインタが有効であると宣言されました。PIX/ASA 上でスタティック変換が失敗する原因はさまざまです。 ただし、一般的な原因は、Demilitarized Zone（DMZ; 非武装地帯）インターフェイスが Outside インターフェイスと同じセキュリティ レベル（0）で設定されている場合です。この問題を解決するには、すべてのインターフェイスに異なるセキュリティ レベルを割り当ててください。詳細については、『インターフェイス パラメータの設定』を参照してください。このエラー メッセージは、外部デバイスによって IDENT パケットが内部クライアントに送信され、PIX Firewall によって廃棄される場合にも表示されます。 詳細については、『IDENT プロトコルによって発生する PIX パフォーマンスの問題』を参照してください。
2. **%PIX|ASA-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}** **説明**これは接続に関連したメッセージです。 このメッセージは、**outbound deny** コマンドが原因で、指定された接続が失敗する場合に表示されます。 プロトコル変数は、ICMP、TCP、または UDP のいずれかの可能性があります。**推奨処置：** **show outbound** コマンドを使用して、発信リストをチェックします。
3. %PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst

interface_name: IP_address (type dec, code dec)**説明**セキュリティ アプライアンスによって着信 ICMP パケットのアクセスが拒否されました。 デフォルトでは、具体的に許可されていない限り、すべての ICMP パケットのアクセスが拒否されます。

4. %PIX|ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.**説明**このメッセージは、0.0.0.0 の宛先 IP アドレスとセキュリティ アプライアンス インターフェイスの宛先 MAC アドレスが設定されたセキュリティ アプライアンス インターフェイスにパケットが到着すると生成されます。 また、このメッセージは、無効な送信元アドレスが含まれたパケットがセキュリティ アプライアンスによって廃棄されると生成されます。送信元アドレスには次のいずれか、またはその他の無効なアドレスが含まれている場合があります。ループバック ネットワーク（127.0.0.0）ブロードキャスト（limited、net-directed、subnet-directed、および all-subnets-directed）宛先ホスト（land.c）スプーフィング パケット検出をさらに強化するためには、**icmp** コマンドを使用して、内部ネットワークに属する送信元アドレスを持つパケットを廃棄するようにセキュリティ アプライアンスを設定します これは、**access-list** コマンドが使用されなくなっており、このコマンドが正しく動作することが保証されなくなっていることが理由です。**推奨処置**： 外部ユーザが保護されているネットワークを危険にさらそうとしていないかどうかを判別します。 誤って設定されているクライアントがないかどうかを確認します。
5. %PIX|ASA-2-106017: Deny IP due to Land Attack from IP_address to IP_address**説明**セキュリティ アプライアンスによって、IP 宛先と同一の IP 送信元アドレスを持ち、送信元ポートと同一の宛先ポートを持つパケットが受信されました。 このメッセージは、システム攻撃を目的とした設計のスプーフィングされたパケットを示します。 この攻撃は、Land 攻撃と呼ばれます。**推奨処置**： このメッセージが引き続き表示される場合は、攻撃が進行中である可能性があります。 パケットでは、攻撃の起点を判断するのに十分な情報は提供されません。
6. %PIX|ASA-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name**説明**攻撃が進行中です。 着信接続で IP アドレスをスプーフィングしようとする試みが行われています。 逆ルート ルックアップとも呼ばれるユニキャスト RPF では、ルートによって表される送信元アドレスを持たないパケットが検出され、そのパケットがセキュリティ アプライアンスへの攻撃の一部であると想定されます。このメッセージは、**ip verify reverse-path** コマンドでユニキャスト RPF をイネーブルにしている場合に表示されます。 この機能は、インターフェイスに入力されるパケットに対して動作します。 Outside で設定されている場合、セキュリティ アプライアンスでは Outside から到達するパケットが確認されます。セキュリティ アプライアンスでは、送信元アドレスに基づいてルートが検索されます。 エントリが検出されず、ルートが定義されていない場合、システム ログ メッセージが表示され、接続は廃棄されます。ルートが存在する場合、セキュリティ アプライアンスによって対応するインターフェイスが確認されます。 パケットが別のインターフェイスに到着した場合、このパケットはスプーフィングであるか、または宛先までに複数のパスがある非対象ルーティング環境が存在しています。 セキュリティ アプライアンスでは、非対称ルーティングがサポートされません。セキュリティ アプライアンスが内部インターフェイスで設定されている場合、スタティック **route** コマンド文または RIP がチェックされます。 送信元アドレスが見つからない場合、内部ユーザがアドレスをスプーフィングしています。**推奨処置**： 攻撃が進行中であっても、この機能がイネーブルになっていれば、ユーザによる処置は不要です。 セキュリティ アプライアンスによって攻撃が撃退されます。**注: show asp drop** Accelerated Security PathASP; また、ASP 廃棄カウンタが最後にクリアされた時刻も示されています。 **ip verify reverse-path** がインターフェイス上で設定されている場合は、**show asp drop rpf-violated** コマンドを使用すると、セキュリティ アプライアンスがパケットを受信し、そのパケットの送信元 IP が、受信されたインターフェイスと同じインターフェイスではないことがルック

アップによって示されたときにカウンタが増分されます。ciscoasa#**show asp drop frame rpf-violated** Reverse-path verify failed 2 **注: 推奨事項：** このシステム メッセージに表示された送信元 IP に基づいてトラフィックの発信元をトレースし、スプーフィングされたトラフィックが送信されている理由を調査します。**注: システム ログ メッセージ：** 106021

7. `%PIX|ASA-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name`**説明**接続と一致するパケットが、その接続が開始されたインターフェイスとは異なるインターフェイスに到着します。たとえば、ユーザが Inside インターフェイスで接続を開始しても、境界インターフェイスに到着する同じ接続がセキュリティ アプライアンスで検出される場合、セキュリティ アプライアンスには宛先への複数のパスが存在することになります。 これは非対称ルーティングと呼ばれ、セキュリティ アプライアンスではサポートされていません。攻撃者は、セキュリティ アプライアンスに侵入する方法として、ある接続から別の接続にパケットを付加しようと試みることもあります。 どちらの場合も、セキュリティ アプライアンスによってこのメッセージが表示され、接続は廃棄されます。**推奨処置：** このメッセージは、**ip verify reverse-path** コマンドが設定されていない場合に表示されます。 ルーティングが非対称でないことを確認します。
8. `%PIX|ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_ID`**説明**IP パケットが ACL によって拒否されました。 このメッセージは、ACL の**ログ** オプションをイネーブルにしていなくても表示されます。**推奨処置：** 同じ送信元アドレスからのメッセージが引き続き表示される場合は、フットプリンティングまたはポート スキャンが行われようとしていることをメッセージが示している可能性もあります。 リモート ホストの管理者に連絡してください。
9. `%PIX|ASA-3-210011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name.`
10. `%ASA-4-419002: Received duplicate TCP SYN from in_interface:src_address/src_port to out_interface:dest_address/dest_port with different initial sequence number.`**説明**このシステム ログ メッセージは、ファイアウォール デバイスを経由する新たな接続の確立によって、設定された最大接続数制限の少なくとも 1 つを超える結果となることを示しています。 このシステム ログ メッセージは、スタティック コマンドを使用して設定された接続数制限と Cisco のモジュラ ポリシー フレームワークを使用して設定された接続数制限の両方に適用されます。 既存のいずれかの接続が切断されることで、現在の接続カウントが設定された最大数を下回るようになるまで、ファイアウォール デバイスを経由した新しい接続は許可されません。*cnt* : 現在の接続数 *limit* ：設定されている接続の制限*dir* — : トラフィックの方向（着信または発信）*sip* ：送信元 IP アドレス*sport* ：送信元ポート*dip* ：宛先 IP アドレス*dport* : 宛先ポート *iif_name* : トラフィック ユニットが受信されるインターフェイスの名前（プライマリまたはセカンダリ）。**推奨処置：** 妥当な理由により接続数制限が設定されているため、このシステム ログ メッセージは潜在的な DoS 攻撃を示している可能性があり、その場合はトラフィックの発信元はスプーフィングされた IP アドレスである可能性が高くなります。 送信元 IP アドレスが完全にランダムではない場合、アクセス リストを使用して発信元を識別し、それをブロックすることが有効である場合があります。 その他の場合は、スニファ トレースを取得してトラフィックの発信元を分析することが、正規のトラフィックから不要なトラフィックを切り分けるのに有効です。

ASA 8.x の基本的な脅威検出機能

Cisco セキュリティ アプライアンス ASA/PIX では、ソフトウェア バージョン 8.0 以降で脅威検出と呼ばれる機能がサポートされています。 基本的な脅威検出機能を使用して、セキュリティ ア

プライアンスでは、下記の原因で廃棄されたパケットのレートとセキュリティ イベントが監視されます。

- アクセス リストによる拒否
- 不良なパケット形式（invalid-ip-header や invalid-tcp-hdr-length など）
- 超過した接続数制限（システム全体のリソース制限と設定による制限の両方）
- 検出された DoS 攻撃（無効な SPI、ステートフル ファイアウォール チェックの障害）
- 基本ファイアウォール検査の不合格（このオプションは、ここに列挙されているファイアウォール関連のパケット ドロップすべてを含む総合レートです。 インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません）
- 検出された疑わしい ICMP パケット
- アプリケーション検査に失敗したパケット
- インターフェイス過負荷
- スキャン攻撃の検出（このオプションはスキャン攻撃をモニタします。 たとえば、最初の TCP パケットが SYN パケットでない、または 3 ウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニタします。 完全なスキャニング攻撃検出（詳細は、『スキャニング脅威検出の設定』を参照）では、たとえば、このスキャニング攻撃レート情報が取得され、ホストを攻撃者として分類し自動的に遮断するなどの方法で対処します。）
- 検出された TCP SYN 攻撃や検出されたデータなし UDP セッション攻撃などの不完全なセッション検出

セキュリティ アプライアンスによって脅威が検出されると、システム ログ メッセージが即座に送信されます（「730100」）。

基本的な脅威検出では、廃棄や潜在的な脅威が存在する場合にのみパフォーマンスへの影響があります。 このシナリオであっても、パフォーマンスへの影響はそれほど大きいものではありません。

セキュリティ アプライアンスへのログイン時に潜在的な攻撃を識別するには、**show threat-detection rate** コマンドを使用します。

```
ciscoasa#show threat-detection rate Average(eps) Current(eps) Trigger Total events 10-min ACL drop: 0 0 0 16 1-hour ACL drop: 0 0 0 112 1-hour SYN attck: 5 0 2 21438 10-min Scanning: 0 0 29 193 1-hour Scanning: 106 0 10 384776 1-hour Bad pkts: 76 0 2 274690 10-min Firewall: 0 0 3 22 1-hour Firewall: 76 0 2 274844 10-min DoS attck: 0 0 0 6 1-hour DoS attck: 0 0 0 42 10-min Interface: 0 0 0 204 1-hour Interface: 88 0 0 318225
```

設定部分についての詳細は、『ASA 8.0 コンフィギュレーション ガイド』の「基本的な脅威検出機能の設定」セクションを参照してください。

Syslog メッセージ 733100

エラー メッセージ:

```
%ASA-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt
```

システム ログ メッセージ内の指定されたオブジェクトが、指定されたバーストのしきい値レートまたは平均のしきい値レートを超えています。 このオブジェクトは、ホスト、TCP/UDP ポート、IP プロトコルの廃棄アクティビティ、または潜在的な攻撃によるさまざまな廃棄である可能性があります。 これは、システムが潜在的な攻撃にさらされていることを示しています。

注: 解決策が提供されるこれらのエラー メッセージは、ASA 8.0 以降にのみ適用されます。

1. Object：廃棄レート カウントの一般的な発生源または特定の発生源であり、その一部は次のとおりです。ファイアウォールBad pktsレート制限DoS attckACL dropConn limitICMP attkスキャニングSYN attckInspectInterface
2. rate_ID：超過されている設定済みのレート。 大部分のオブジェクトは、最大 3 つの異なるレートを異なる間隔で設定できます。
3. rate_val：特定のレート値。
4. total_cnt：オブジェクトが作成または消去された後の合計カウント。

次の 3 つの例は、これらの変数がどのように発生するのかを示しています。

- CPU またはバスの制限が原因のインターフェイス廃棄の場合：`%ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per second, max configured rate is 8000; Current average rate is 2030 per second, max configured rate is 2000; Cumulative total count is 3930654`
- 潜在的な攻撃が原因のスキャニング廃棄の場合：`ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per second_ max configured rate is 10; Current average rate is 245 per second_ max configured rate is 5; Cumulative total count is 147409 (35 instances received)`
- 潜在的な攻撃が原因の不良パケットの場合：`%ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per second, max configured rate is 400; Current average rate is 760 per second, max configured rate is 100; Cumulative total count is 1938933`

推奨処置：:

メッセージ内に表示されている指定済みオブジェクト タイプに従って、次の手順を実行します。

1. syslog メッセージ内のオブジェクトが次のいずれかの場合：ファイアウォールBad pktsレート制限DoS attackACL dropConn limitICMP attkスキャニングSYN attckInspectInterface稼働中の環境で廃棄レートが許容可能かどうかをチェックします。
2. **threat-detection rate xxx** コマンドを実行して、特定の廃棄のしきい値を適切な値に調整します（この場合、*xxx* は次のいずれかです）。acl-dropbad-packet-dropconn-limit-dropdos-dropfw-dropicmp-dropinspect-dropinterface-dropscanning-threatsyn-attack
3. syslog メッセージ内のオブジェクトが TCP または UDP ポート、IP プロトコル、またはホスト廃棄の場合、稼働中の環境で廃棄レートが許容可能かどうかをチェックします。
4. **threat-detection rate bad-packet-drop** コマンドを実行して、特定の廃棄のしきい値を適切な値に調整します。 詳細は、『ASA 8.0 コンフィギュレーション ガイド』の「基本的な脅威検出機能の設定」セクションを参照してください。

注: 廃棄レートの超過の警告を表示する必要がない場合、**no threat-detection basic-threat** コマンドを実行してこれをディセーブルにすることができます。

関連情報

- Cisco 5500 シリーズ適応型セキュリティ アプライアンス サポート ページ
- Cisco 500 シリーズ PIX に関するサポート ページ
- TCP SYN フラッディング攻撃に対する防御
- Cisco 適用緩和策速報： コンテント スイッチング モジュールにおけるサービス拒否の脆弱性の悪用に対する識別策と対応策

- Cisco 適用緩和策速報： Cisco PIX と ASA のアプライアンスおよびファイアウォール サービス モジュールにおける複数の脆弱性の悪用に対する識別と緩和
- IP スプーフィング
- テクニカルサポートとドキュメント - Cisco Systems