ASA 8.2：ASA ファイアウォールを通過するパケット フロー

内容

概要

このドキュメントでは、Cisco 適応型セキュリティ アプライアンス（ASA）ファイアウォールを通過するパケット フローについて説明します。ここには、内部パケットを処理する Cisco ASA のプロシージャが示されています。また、パケットがドロップされるさまざまな可能性と、パケット処理のさまざまな状況についても説明します。

前提条件

要件

Cisco 5500 シリーズ ASA に関する基本的な知識があることが推奨されます。

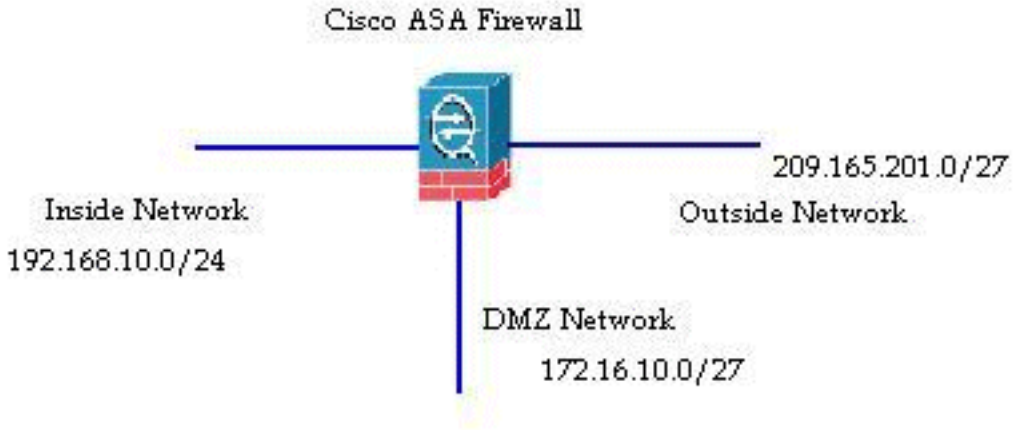
使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 8.2 を実行している Cisco ASA 5500 シリーズ ASA に基づきます。

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

パケットを受信するインターフェイスは**入力**インターフェイスと呼ばれ、送信パケットが通過するインターフェイスは**出力**インターフェイスと呼ばれます。デバイスからパケット フローを参照する場合、これら 2 つのインターフェイスの観点から検討するとタスクを簡単に単純化できます。次に例を示します。



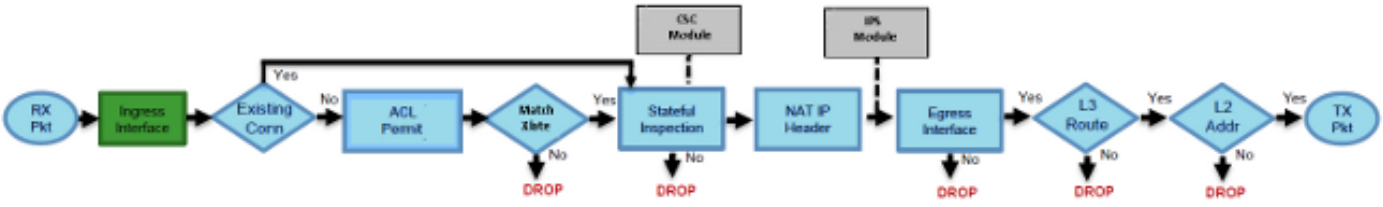
内部ユーザ（192.168.10.5）が緩衝地帯（DMZ）のネットワーク（172.16.10.5）内の Web サーバにアクセスしようとした場合、パケット フローは次のようになります。

- 送信元アドレス：192.168.10.5
- 送信元ポート：22966
- 宛先アドレス：172.16.10.5
- 宛先ポート：8080
- 入力インターフェイス：内部
- 出力インターフェイス：DMZ
- 使用プロトコル：TCP（Transmission Control Protocol）

ここで説明するようにパケット フローの詳細を特定すると、問題をこの特定の接続エントリに簡単に隔離できます。

Cisco ASA パケット処理アルゴリズム

次の図に、Cisco ASA が受信パケットをどのように処理するかを示します。



次に、個々の手順の詳細を示します。

1. パケットが入力インターフェイスに到達します。
2. パケットがインターフェイスの内部バッファに到達すると、インターフェイスの入力カウン

タが 1 増加します。
3. Cisco ASA はまず、内部接続テーブルの詳細を検討し、これが現在の接続であるかどうかを確認します。パケット フローが現在の接続と一致している場合はアクセス コントロール リスト（ACL）の確認がバイパスされ、パケットは先に進みます。パケット フローが現在の接続に一致していない場合は、TCP の状態が確認されます。SYN パケットまたは UDP（User Datagram Protocol）の場合は、接続カウンタが 1 増え、パケットは ACL の確認のために送信されます。SYN パケットでない場合、パケットはドロップされ、イベントが記録されます。
4. パケットは、インターフェイス ACL に基づいて処理されます。検証は、ACL エントリの順に行われ、ACL エントリのいずれかに一致する場合、転送されます。それ以外の場合、パケットはドロップされて情報がログに記録されます。パケットが ACL エントリに一致すると、ACL ヒット カウントが 1 増えます。
5. パケットは、トランスレーション ルールで検証されます。この確認にパケットが合格した場合、このフローに接続エントリが作成され、パケットは先にし進みます。それ以外の場合、パケットはドロップされて情報がログに記録されます。
6. パケットのインスペクション チェックが行われます。このインスペクション チェックでは、特定のパケット フローがプロトコルに準拠しているかどうかが検証されます。Cisco ASA には組み込み型のインスペクション エンジンがあり、事前に定義された一連のアプリケーション レベルの機能に従って、各接続を検査します。パケットは、このインスペクション チェックに合格すると、転送されます。それ以外の場合、パケットはドロップされて情報がログに記録されます。コンテンツ セキュリティ（CSC）モジュールが含まれている場合は、追加のセキュリティ チェックが実行されます。
7. IP ヘッダー情報はネットワークアドレス変換/ポート アドレス変換（NAT/PAT）ルールに従って変換され、それに応じてチェックサムが更新されます。AIP モジュールが含まれている場合は、パケットは Advanced Inspection and Prevention Security Services Module（AIP-SSM）に転送され、IPS 関連のセキュリティ チェックが行われます。
8. パケットは、トランスレーション ルールに基づいて出力インターフェイスに転送されます。変換ルールに出力インターフェイスが指定されていない場合、グローバル ルート ルックアップに基づいて宛先インターフェイスが決定されます。
9. 出力インターフェイスで、インターフェイス ルート ルックアップが実行されます。出力インターフェイスは、変換ルールが優先されて決定されることを覚えておいてください。
10. レイヤ 3 ルートが見つかり、ネクスト ホップが識別されると、レイヤ 2 解決が実行されます。MAC ヘッダーのレイヤ 2 の書き換えは、この段階で行われます。
11. パケットがネットワークに送信され、インターフェイス カウンタが出力インターフェイスで増分します。

NAT の説明

NAT 操作の順序の詳細については、次のドキュメントを参照してください。

- Cisco ASA ソフトウェア バージョン 8.2 以前
- Cisco ASA ソフトウェア バージョン 8.3 以降

show コマンド

次に、このプロセス内のさまざまな段階でのパケット フローの詳細の追跡に役立つ、便利なコマンドを示します。

```
show interface
show conn
show access-list
show xlate
show service-policy inspect
show run static
show run nat
show run global
show nat
show route
show arp
```

syslog メッセージ

syslog メッセージは、パケット処理に役に立つ情報を提供します。次に、参照用の syslog メッセージの例を示します。

- 接続エントリがない場合の syslog メッセージ：
  ```
  %ASA-6-106015: Deny TCP (no connection) from IP_address/port to
  IP_address/port flags tcp_flags on interface interface_name
  ```
- パケットが ACL によって拒否された場合の syslog メッセージ：
  ```
  %ASA-4-106023: Deny protocol src [interface_name:source_address/source_port]
  dst interface_name:dest_address/dest_port by access_group acl_ID
  ```
- 変換ルールが見つからなかった場合の syslog メッセージ：
  ```
  %ASA-3-305005: No translation group found for protocol src interface_name:
  source_address/source_port dst interface_name:dest_address/dest_port
  ```
- パケットがセキュリティ インスペクションにより拒否された場合の syslog メッセージ：
  ```
  %ASA-4-405104: H225 message received from outside_address/outside_port to
  inside_address/inside_port before SETUP
  ```
- ルート情報がない場合の syslog メッセージ：
  ```
  %ASA-6-110003: Routing failed to locate next-hop for protocol from src
  interface:src IP/src port to dest interface:dest IP/dest port
  ```

Cisco ASA が生成するすべての syslog メッセージのリストと簡単な説明は、「Cisco ASA シリーズ Syslog メッセージ」を参照してください。

関連情報

- Cisco ASA に関するサポート ページ
- Cisco ASA 5500 シリーズ コマンド リファレンス 8.2
- Cisco ASA 5500 シリーズ設定ガイド 8.3
- テクニカル サポートとドキュメント – Cisco Systems