# ASA 8.2： ASA ファイアウォールを通過するパケット フロー

## 目次



## 概要

この資料は a （ASA ）ファイアウォールによるパケットフローを Cisco 適応型セキュリティ アプライアンス（ASA ）ソフトウェア記述したものです。 それは内部パケットを処理するために Cisco ASA プロシージャを示します。 さらに、パケットがドロップされるさまざまな可能性やパケットが転送されるさまざまな状況について説明します。

## 前提条件

### 要件

Cisco は ASA の知識が Cisco 5500 シリーズあることを推奨します。

### 使用するコンポーネント

この文書に記載されている情報はソフトウェア バージョン 8.2 を実行する基づいた on Cisco ASA 5500 シリーズ ASA 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。

# 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。 あらゆるデバイスを通るパケットフローを参照するとき、タスクは容易にこれら二つのインターフェイスの点ではそれを検知 する場合簡約化されます。 次に例を示します。

内部ユーザ（192.168.10.5） 非武装地帯（DMZ アクセスする）試みネットワークの Webサーバに時（172.16.10.5）、このようにパケットフローな:

- 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
- 使用されるプロトコル- TCP （Transmission Control Protocol（TCP））

ここに記述されているようにパケットフローの詳細を判別した後、この特定の接続 エントリに問題を特定することは容易です。

## 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. パケットは入力 インターフェイスで達します。
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. 内部接続 表の Cisco ASA 最初に外観はこれが現在の接続であるかどうか確認するために詳述します。 パケットフローが現在の接続と一致する場合、Access Control List （ACL） チェックはバイパスされ、パケットは進められます。パケットフローが現在の接続を一致する場合、TCP 状態は確認されます。 それが Syn パケットまたは UDP （User Datagram Protocol（UDP））パケットである場合、Connection カウンターは 1 によって増分し、パケットは ACL チェックのために送信 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。 ACL ヒット カウントは 1 つによってパケットが ACL項目と一致するとき増分します。
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。 パケットがこのチェックを通る場合、接続 エントリはこのフローのために作成され、パケットは進みます。 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。 アプリケーション レベル 機能性のあらかじめ定義されたセットによって各接続を点検する Cisco ASA に組み込みインスペクション エンジンがあります。 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。追加 の セキュリティ チェックはコンテンツ セキュリティ（CSC）モジュールが複雑である場合設定されています。
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）ルールによって変換され、チェックサムはそれに応じてアップデートされます。 パケットは IPS 関連保安検査用の高度インスペクションおよび防止セキュリティ サービス モジュール（AIP-SSM）に AIP モジュールが複雑なとき転送されます。
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。 出力 インターフェイスが変換規則で規定 されない場合、デスティネーションインターフェイスはグローバル な ルート ルックアップに基づいて決定されます。
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判別されます優先順位を奪取 する 変換規則によって覚えていて下さい。
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 書き直しはこの段階で起こります。
11. パケットはネットワークで送信され、インターフェイス カウンタは出力 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 およびそれ以前
- Cisco ASA ソフトウェア バージョン 8.3 以降

## show コマンド

プロセスの異なるステージでパケットフロー 詳細のトラッキングを助けるいくつかの役に立つコマンドはここにあります:

```
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 によって拒否される場合の 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`

- 見つけられる変換規則ない場合の 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`

簡潔な説明と共に Cisco ASA によって生成されるすべての syslog メッセージの完全なリストに関しては Cisco ASA シリーズ Syslog メッセージを参照して下さい。

# 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