# ASA 8.2:通過ASA防火牆的資料包流

## 目錄



## 簡介

本檔案介紹通過思科調適型安全裝置(ASA)防火牆的封包流量。它顯示了用於處理內部資料包的Cisco ASA過程。它也討論了丟包的不同可能性以及資料包向前發展的不同情況。

## 必要條件

### 需求

思科建議您瞭解Cisco 5500系列ASA。

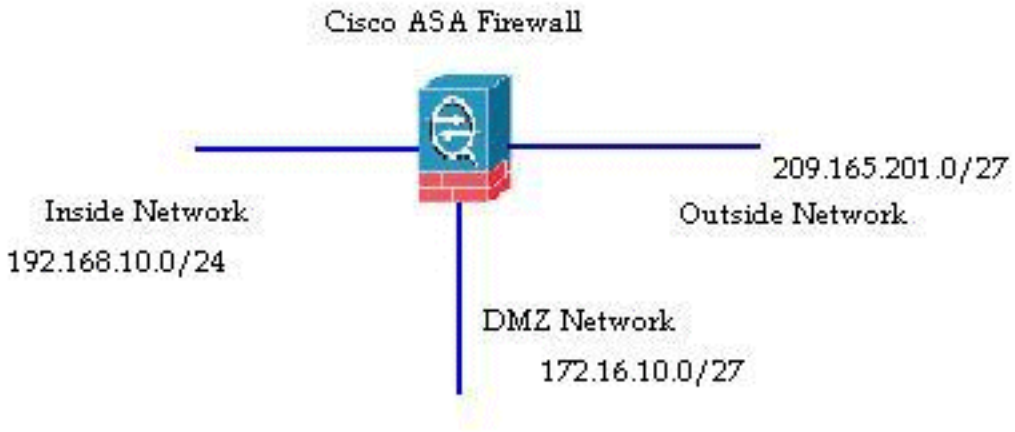
### 採用元件

本文檔中的資訊基於運行軟體版本8.2的Cisco ASA 5500系列ASA。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 背景資訊

接收封包的介面稱為**ingress**介面，而封包退出所在的介面稱為**egress**介面。當您參考通過任何裝置的資料包流時，如果您從這兩個介面的角度看它，任務會很容易簡化。以下是一個範例情境：




當內部使用者(192.168.10.5)嘗試訪問非軍事區(DMZ)網路(172.16.10.5)中的Web伺服器時，資料包流如下所示：

- 源地址 — 192.168.10.5
- 來源連線埠 — 22966
- 目的地址 — 172.16.10.5
- 目的地連線埠 — 8080
- 輸入介面 — 內部
- 輸出介面 — DMZ
- 使用的通訊協定 — TCP（傳輸控制通訊協定）

確定資料包流的詳細資訊後（如這裡所述），很容易將問題隔離到此特定連線條目。

## Cisco ASA封包處理演演算法

以下是Cisco ASA如何處理其接收的資料包的圖表：


以下是詳細的具體步驟：

1. 封包會在輸入介面到達。
2. 一旦封包到達介面的內部緩衝區，介面的輸入計數器就會增加1。
3. Cisco ASA首先檢視其內部連線表詳細資訊，以驗證此連線是否為當前連線。如果封包流與當前連線相符，則會繞過存取控制清單(ACL)檢查，並將封包轉送。如果資料包流與當前連線不匹配，則會驗證TCP狀態。如果是SYN封包或UDP（使用者資料包通訊協定）封包，則連線計數器會遞增1，且封包會傳送以進行ACL檢查。如果不是SYN資料包，則丟棄該資料包並記錄事件。
4. 封包的處理方式為依照介面ACL。系統會按ACL專案的順序進行驗證，如果它與任何ACL專案匹配，則會向前移動。否則封包會被捨棄，資訊會記錄下來。當封包與ACL專案相符時，ACL命中數會遞增1。

5. 驗證資料包的轉換規則。如果資料包通過此檢查，則會為此流建立連線條目，然後資料包向前移動。否則封包會被捨棄，資訊會記錄下來。
6. 資料包將接受檢查檢查。此檢查驗證此特定資料包流是否符合協定。Cisco ASA具有內建檢測引擎，可根據其預定義的一組應用級功能檢查每個連線。如果通過檢查，則向前移動。否則封包會被捨棄，資訊會記錄下來。如果涉及內容安全(CSC)模組，則會實施其他安全檢查。
7. 根據網路地址轉換/埠地址轉換(NAT/PAT)規則轉換IP報頭資訊，並相應地更新校驗和。涉及AIP模組時，資料包會被轉發到高級檢測和防禦安全服務模組(AIP-SSM)，以進行IPS相關的安全檢查。
8. 根據轉譯規則將封包轉送到輸出介面。如果在轉換規則中未指定輸出介面，則根據全域性路由查詢確定目標介面。
9. 在輸出介面上執行介面路由查詢。請記住，輸出介面由具有優先順序的轉換規則決定。
10. 一旦找到第3層路由並確定下一跳，就會執行第2層解析。MAC報頭的第2層重寫在此階段進行。
11. 封包通過線路傳輸，而介面計數器在輸出介面上增加。

## NAT說明

有關NAT操作順序的詳細資訊，請參閱以下文檔：

- Cisco ASA軟體8.2及更低版本
- Cisco ASA軟體版本8.3及更高版本

## 顯示命令

以下是一些有用的命令，可幫助跟蹤此過程中不同階段的資料包流詳細資訊：

```
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
```

## 系統日誌消息

系統日誌消息提供有關資料包處理的有用資訊。以下是一些供您參考的系統日誌消息示例：

- 沒有連線條目時的系統日誌消息：
  `%ASA-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name`
- ACL拒絕資料包時的系統日誌消息：
  `%ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port by access_group acl_ID`
- 未找到轉換規則時的系統日誌消息：
  `%ASA-3-305005: No translation group found for protocol src interface_name: source_address/source_port dst interface_name:dest_address/dest_port`

- 安全檢查拒絕資料包時的系統日誌消息：
  ```
  %ASA-4-405104: H225 message received from outside_address/outside_port to
  inside_address/inside_port before SETUP
  ```
- 沒有路由資訊時的系統日誌消息：
  ```
  %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
  ```

有關Cisco ASA生成的所有系統日誌消息的完整清單以及簡要說明，請參閱Cisco ASA系列系統日誌消息。

# 相關資訊

- Cisco ASA支援頁面
- Cisco ASA 5500系列命令參考，8.2
- Cisco ASA 5500系列配置指南8.3
- 技術支援與文件 - Cisco Systems