ASA 8.2：通过ASA防火墙的数据包流

目录

简介

本文档介绍通过思科自适应安全设备(ASA)防火墙的数据包流。它显示处理内部数据包的Cisco ASA过程。它还讨论数据包可能被丢弃的不同可能性以及数据包向前推进的不同情况。

先决条件

要求

思科建议您了解Cisco 5500系列ASA。

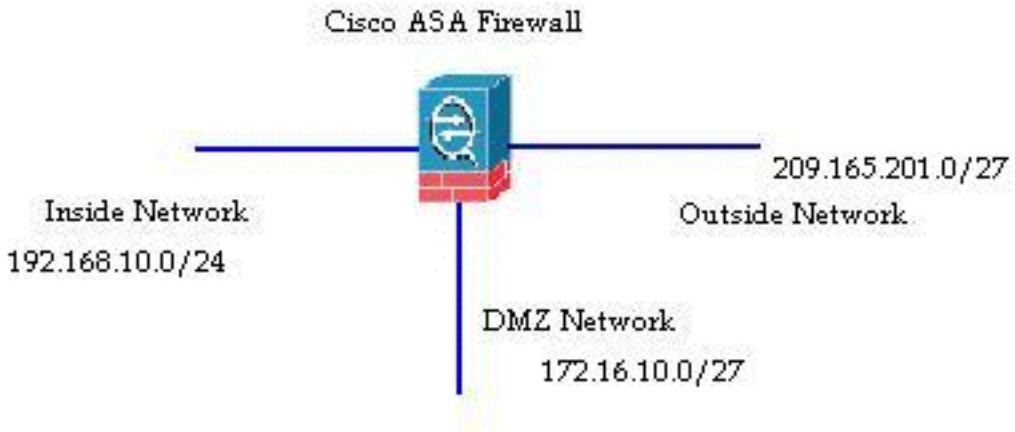
使用的组件

本文档中的信息基于运行软件版本8.2的Cisco ASA 5500系列ASA。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

接收数据包的接口称为**入口**接口，数据包通过的接口称为**出口**接口。当您参考通过任何设备的数据包流时，如果从这两个接口来看，任务会轻松简化。以下是一个示例场景：



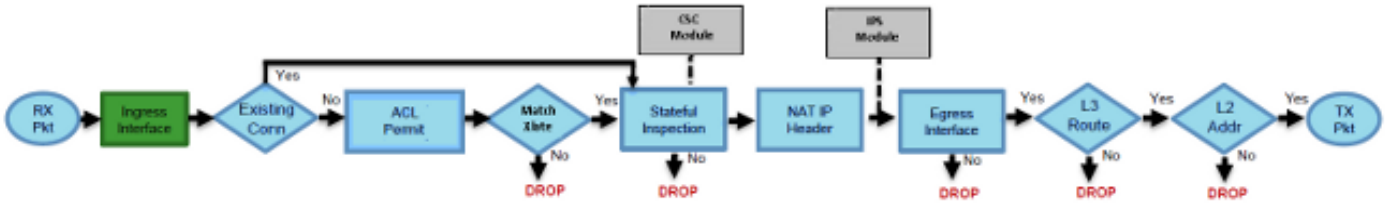
当内部用户(192.168.10.5)尝试访问非军事区(DMZ)网络(172.16.10.5)中的Web服务器时，数据包流如下所示：

- 源地址 — 192.168.10.5
- 源端口 — 22966
- 目的地址 — 172.16.10.5
- 目标端口 — 8080
- 入口接口 — 内部
- 出口接口 — DMZ
- 使用的协议 — TCP（传输控制协议）

在您按照此处所述确定数据包流的详细信息后，很容易将问题隔离到此特定连接条目。

Cisco ASA数据包处理算法

下面是Cisco ASA如何处理其接收的数据包的图：



下面是具体步骤：

1. 数据包在入口接口到达。
2. 一旦数据包到达接口的内部缓冲区，接口的输入计数器将递增1。
3. Cisco ASA首先查看其内部连接表详细信息，以验证这是否是当前连接。如果数据包流与当前连接匹配，则会绕过访问控制列表(ACL)检查，并将数据包转发。如果数据包流与当前连接不匹配，则检验TCP状态。如果是SYN数据包或UDP（用户数据报协议）数据包，则连接计数器递增1，然后发送数据包进行ACL检查。如果它不是SYN数据包，则丢弃该数据包并记录事件。
4. 数据包根据接口ACL进行处理。它按ACL条目的顺序进行检验，如果它与任何ACL条目匹配，它将向前移动。否则，数据包将被丢弃并记录信息。当数据包与ACL条目匹配时，ACL命中计数将递增1。

5. 数据包已验证转换规则。如果数据包通过此检查，则会为此流创建连接条目，数据包将向前移动。否则，数据包将被丢弃并记录信息。
6. 数据包接受检查检查。此检查验证此特定数据包流是否符合协议。Cisco ASA具有内置检测引擎，根据其预定义的应用级功能集检查每个连接。如果通过检查，则向前推进。否则，数据包将被丢弃并记录信息。如果涉及内容安全(CSC)模块，将实施其他安全检查。
7. 根据网络地址转换/端口地址转换(NAT/PAT)规则转换IP报头信息，并相应地更新校验和。当涉及AIP模块时，数据包将转发到高级检测和防御安全服务模块(AIP-SSM)以进行IPS相关安全检查。
8. 根据转换规则，数据包被转发到出口接口。如果转换规则中未指定出口接口，则根据全局路由查找确定目标接口。
9. 在出口接口上，执行接口路由查找。请记住，出口接口由具有优先级的转换规则决定。
10. 找到第3层路由并确定下一跳后，将执行第2层解析。MAC报头的第2层重写在此阶段发生。
11. 数据包在线路上传输，接口计数器在出口接口上增加。

NAT解释

有关NAT操作顺序的详细信息，请参阅以下文档：

- Cisco ASA软件版本8.2及更低版本
- Cisco ASA软件版本8.3及更高版本

显示命令

以下是一些有用的命令，可帮助跟踪流程不同阶段的数据包流详细信息：

```
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 消息

系统日志消息提供有关数据包处理的有用信息。以下是供您参考的一些系统日志消息示例：

- 没有连接条目时的系统日志消息：
  `%ASA-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name`
- ACL拒绝数据包时的系统日志消息：
  `%ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port by access_group acl_ID`
- 找不到转换规则时的系统日志消息：
  `%ASA-3-305005: No translation group found for protocol src interface_name: source_address/source_port dst interface_name:dest_address/dest_port`
- 安全检查拒绝数据包时的系统日志消息：

```
%ASA-4-405104: H225 message received from outside_address/outside_port to
inside_address/inside_port before SETUP
```

- 没有路由信息时的系统日志消息：

```
%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
```

有关Cisco ASA生成的所有系统日志消息的完整列表以及简要说明，请参阅Cisco ASA系列系统日志消息。

相关信息

- Cisco ASA 支持页
- Cisco ASA 5500系列命令参考，8.2
- Cisco ASA 5500系列配置指南，8.3
- 技术支持和文档 - Cisco Systems