ASA 8.2：流经ASA防火墙的数据包

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[背景信息](#)
[Cisco ASA数据包处理算法](#)
[NAT说明](#)
[显示命令](#)
[Syslog 消息](#)
[相关信息](#)

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。它显示了处理内部数据包的Cisco ASA过程。本章还讨论数据包可能丢弃的不同可能性，以及数据包向前发展的不同情况。

先决条件

要求

Cisco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，数据包通过其出口的接口称为出口接口。当您提到通过任何设备的数据包流时，如果您从这两个接口的角度看它，任务会很容易简化。下面是一个示例场景：

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
- 目的端口 — 8080
- 入口接口 — 内部
- 出口接口 — DMZ
- 使用的协议 — TCP（传输控制协议）

确定数据包流的详细信息后（如此处所述），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

以下是Cisco ASA如何处理其接收的数据包的图表：

下面是各个步骤的详细信息：

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，以验证此连接是否为当前连接。如果数据包流与当前连接匹配，则绕过访问控制列表(ACL)检查并转发数据包。

   如果数据包流与当前连接不匹配，则会验证TCP状态。如果是SYN数据包或UDP（用户数据报协议）数据包，则连接计数递增1，并发送数据包进行ACL检查。如果不是SYN数据包，则丢弃该数据包并记录事件。
4. 根据接口ACL处理数据包。系统会按ACL条目的顺序进行检验，如果它与任何ACL条目匹配，则会向前移动。否则，数据包将被丢弃，信息将被记录。当数据包与ACL条目匹配时，ACL命中计数会递增1。
5. 验证数据包的转换规则。如果数据包通过此检查，则会为此流创建连接条目，然后数据包向前移动。否则，数据包将被丢弃，信息将被记录。
6. 数据包将接受检查检查。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，可根据其预定义的一组应用级功能检查每个连接。如果它通过了检查，则会向前移动。否则，数据包将被丢弃，信息将被记录。

   如果涉及内容安全(CSC)模块，则会实施其他安全检查。
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，数据包被转发到高级检测和防御安全服务模块(AIP-SSM)，以进行IPS相关的安全检查。
8. 根据转换规则将数据包转发到出口接口。如果在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. 一旦找到第3层路由并确定下一跳，即可执行第2层解析。MAC报头的第2层重写发生在此阶段。
11. 数据包通过线路传输，而出口接口的接口计数器会递增。

NAT说明

有关NAT操作顺序的详细信息，请参阅以下文档：

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

显示命令

以下是一些有用的命令，可帮助跟踪此过程中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。以下是一些供您参考的系统日志消息示例：

- 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
```

- 当数据包被ACL拒绝时显示系统日志消息：

```
%ASA-4-106023: Deny protocol src [interface_name:source_address/source_port]
 dst interface_name:dest_address/dest_port by access_group acl_ID
```

- 未找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
```

- 当数据包被安全检测拒绝时显示系统日志消息：

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

- 没有路由信息时显示系统日志消息：

```
%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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。