ASA 8.2 ：数据包流经ASA防火墙

目录

简介

本文描述数据包流经思科可适应安全工具(ASA)防火墙。它显示思科ASA步骤处理内部数据包。它也讨论数据包可能丢弃和不同的情况的不同的可能性数据包向前的地方进步。

先决条件

要求

Cisco建议您有Cisco 5500系列ASA知识。

使用的组件

本文档中的信息根据运行软件版本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

收到数据包的接口呼叫数据包退出呼叫**出口接口的入口接口**和接口。当您参考数据包请流经所有设备，任务容易地简化，如果查看它根据这两个接口。这是示例情景：

当一个内部的用户(192.168.10.5)尝试访问在非敏感区域(DMZ)网络(172.16.10.5)的一Web服务器，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
- 目的地端口- 8080
- 入口接口-里面
- 出口接口- DMZ
- 使用的协议- TCP (传输控制协议)

在您确定数据包流的详细信息如描述此处后，查出对此特定连接项的问题是容易的。

思科ASA数据包进程算法

这是图表思科ASA如何处理收到的数据包：

这详细是各自的步骤：

1. 数据包被到达在入口接口。
2. 一旦数据包到达接口的内部缓冲器，接口的输入计数器由一个增加。
3. 如果这是当前连接，思科ASA首先查看其内部连接表详细信息为了验证。如果数据包流匹配当前连接，则访问控制表(ACL)检查绕过，并且数据包移动的向前。如果数据包流不匹配当前连接，则TCP状态验证。如果它是SYN数据包或UDP (用户数据报协议)数据包，则连接计数器由一个增加，并且数据包为ACL检查发送。如果它不是SYN数据包，数据包丢弃，并且事件被记录。
4. 数据包根据接口ACL处理。它验证顺序按ACL条目的顺序，并且，如果匹配其中任一ACL条目，移动向前。否则，数据包丢弃，并且信息被记录。当数据包匹配ACL条目时， ACL命中数计数由一个增加。
5. 数据包为翻译规则验证。如果数据包穿过此检查，则连接项为此流创建，并且数据包移动向前。否则，数据包丢弃，并且信息被记录。
6. 数据包对检查检查被服从。此检查验证此特定数据包流是否是与协议一致。思科ASA有根据其预定义的套应用程序级功能检查每连接的一内置的检测引擎。如果它通过检查，移动的向前。否则，数据包丢弃，并且信息被记录。附加安全性安全性检查将实现，如果内容安全(CSC)模块是包含的。
7. IP报头信息根据网络地址地址转换端口地址转换(NAT/PAT)规则翻译，并且校验和相应地更新。数据包转发到先进的检查和预防安全服务模块(AIP-SSM) IPS涉及的安全性检查的，当AIP模块是包含的时。
8. 数据包转发对根据翻译规则的出口接口。如果出口接口在转换规则没有指定，则目的地接口根据全局路由查找决定。
9. 在出口接口，接口路由查找执行。切记，出口接口取决于采取优先级的转换规则。
10. 一旦找到了第3层路由，并且下一跳识别， Layer2解决方法执行。MAC报头的Layer2重写在此阶段发生。
11. 数据包在电线传送，并且接口计数器在出口接口增加。

NAT的说明

欲了解更详细的信息参考这些文档大约NAT操作：

- Cisco ASA软件版本8.2和前
- Cisco ASA软件版本8.3及以后

显示命令

这是一些有用的命令数据包流选派在进程的不同的阶段的帮助跟踪：

```
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

系统消息提供关于数据包处理的有用的信息。这是一些示例系统消息供您的参考：

- 系统消息，当没有连接项：
  `%ASA-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name`
- 系统消息，当数据包由ACL拒绝：
  `%ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port by access_group acl_ID`
- 系统消息，当没有找到的转换规则：
  `%ASA-3-305005: No translation group found for protocol src interface_name: source_address/source_port dst interface_name:dest_address/dest_port`
- 系统消息，当数据包由安全检查拒绝：
  `%ASA-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP`
- 系统消息，当没有路由信息：
  `%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`

对于思科ASA生成的所有系统消息完整列表与简要说明一起，参考思科ASA系列系统消息。

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