ASA 8.2 ：信息包流经ASA防火墙

Contents

Introduction

本文描述信息包流经Cisco可适应的安全工具(ASA)防火墙。它显示Cisco ASA程序处理内部信息包。它也讨论信息包可能被丢弃和不同的情况的不同的可能性信息包向前的地方进步。

Prerequisites

Requirements

Cisco建议您有Cisco 5500系列ASA知识。

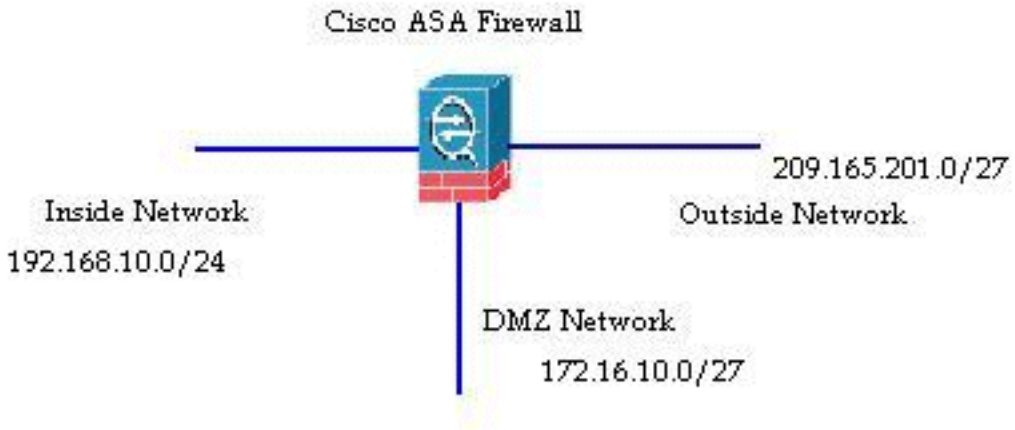
Components Used

本文的信息根据运行软件版本8.2的Cisco ASA 5500系列ASA。

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

背景信息

收到信息包的接口称为信息包退出称为输出接口的入口接口和接口。当您是指信息包时请流经所有设备，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，信息包流如下所示:

- 源地址- 192.168.10.5
- 源端口- 22966
- 目的地地址- 172.16.10.5
- 目的地端口- 8080
- 入口接口-里面
- 输出接口- DMZ
- 使用的协议- TCP (传输控制协议)

在您确定信息包流的详细资料如所描述这里后，查出问题到此特定连接项是容易的。

Cisco ASA信息包进程算法

这是图表Cisco ASA如何处理收到的信息包：

这详细是各自的步骤：

1. 信息包被到达在入口接口。
2. 一旦信息包到达接口的内部缓存，接口的输入计数器由一个增加。
3. Cisco ASA首先查看其内部连接表详细资料为了验证这是否是当前连接。如果信息包流匹配当前连接，则访问控制表(ACL)检查被绕过，并且信息包被移动今后。如果信息包流不匹配当前连接，则TCP状态被验证。如果它是同步信息包或UDP (用户数据协议)信息包，则连接计数器由一个增加，并且信息包为ACL检查被发送。如果它不是同步信息包，信息包被丢弃，并且事件被记录。
4. 信息包根据接口ACL被处理。被验证顺序按ACL条目的顺序，并且，如果匹配其中任一ACL条目，前进。否则，信息包被丢弃，并且信息被记录。当信息包匹配ACL条目时， ACL命中计数由一个增加。

5. 信息包为翻译规则被验证。如果信息包穿过此检查，则连接项为此流被创建，并且信息包前进。否则，信息包被丢弃，并且信息被记录。
6. 信息包对检查检查被服从。此检查验证此特定信息包流是否是与协议一致。Cisco 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。如果它通过了检查，前进。否则，信息包被丢弃，并且信息被记录。另外的安全性检查将是被实施的，如果内容安全(CSC)模块是包含的。
7. IP头信息根据网络地址转换端口地址转换(NAT/PAT)规则被转换，并且相应地更新校验和。信息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. 信息包转发到根据翻译规则的输出接口。如果输出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. 在输出接口，接口路由查找执行。切记，输出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，并且下一跳被识别，请分层堆积解决方法执行的2。MAC报头的第2层重写在此阶段发生。
11. 信息包在电线传输，并且接口计数器在输出接口增加。

NAT的解释

欲了解更详细的信息请参见这些文件大约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

这是在进程中帮助跟踪信息包流详细资料在不同的阶段的一些有用的命令：

```
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
```

系统消息

系统消息提供关于信息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，当信息包由ACL丢弃：
  ```
  %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，当信息包由安全检查丢弃：

```
%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
```

关于Cisco ASA生成的所有系统消息一张完全列表与简要说明一起，请参见Cisco ASA系列系统消息。

Related Information

- 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
- Technical Support & Documentation - Cisco Systems