网 络 工 程
本 科 实 验 报 告

实验名称： 防火墙 ACL 配置

学 员 姓 名	程景愉	学 号	202302723005
培 养 类 型	无军籍	年 级	2023
专 业	网络工程	所 属 学 院	计算机学院
指 导 教 员	张军	职 称	工程师
实 验 室	306-707	实 验 时 间	2025.09.28

国防科技大学教育训练部制

《本科实验报告》填写说明

实验报告内容编排应符合以下要求：

（1）采用 A4（21cm×29.7cm）白色复印纸，单面黑字。上下左右各侧的页边距均为 3cm；缺省文档网格：字号为小 4 号，中文为宋体，英文和阿拉伯数字为 Times New Roman，每页 30 行，每行 36 字；页脚距边界为 2.5cm，页码置于页脚、居中，采用小 5 号阿拉伯数字从 1 开始连续编排，封面不编页码。

（2）报告正文最多可设四级标题，字体均为黑体，第一级标题字号为 4 号，其余各级标题为小 4 号；标题序号第一级用“一、”、“二、”……，第二级用“（一）”、“（二）”……，第三级用“1.”、“2.”……，第四级用“（1）”、“（2）”……，分别按序连续编排。

（3）正文插图、表格中的文字字号均为 5 号。

目录

图目录

1 实验目的

本实验旨在通过配置 ACL，实现对网络流量的精确识别和控制，提高网络的安全性和稳定性。通过配置防火墙，实现对内外网络的访问控制，保护内部网络免受外部威胁。

2 实验原理

2.1 ACL

2.1.1 ACL 概述

访问控制列表 ACL（Access Control List）是由一条或多条规则组成的集合。所谓规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源地址、目的地址、端口号等。ACL 本质上是一种报文过滤器，规则是过滤器的滤芯。设备基于这些规则进行报文匹配，可以过滤出特定的报文，并根据应用 ACL 的业务模块的处理策略来允许或阻止该报文通过。

2.1.2 ACL 的作用

ACL 作为一个过滤器，设备通过应用 ACL 来阻止和允许特定流量的流入和流出，如果没有它，任何流量都会自由流入和流出，使得网络容易受到攻击。

如 Figure 1 所示，为保证财务数据安全，企业在路由设备上应用 ACL 可以阻止内网内部研发部门主机对财务服务器的访问，同时允许总裁办公室访问财务服务器。为了保护企业内网的安全，在路由设备上应用 ACL 可以封堵网络病毒常用的端口，防止 Internet 上的恶意流量入侵。

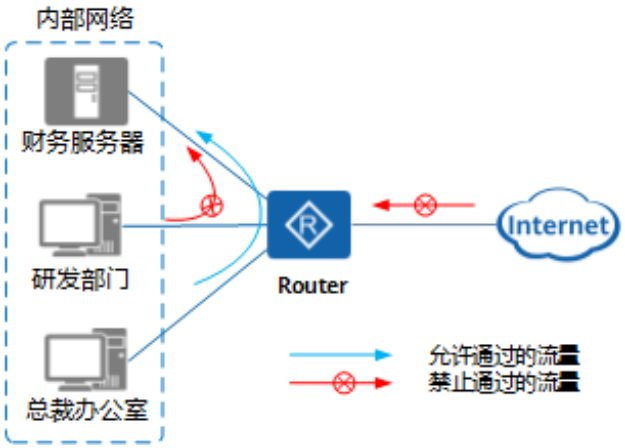

Figure 1: ACL 应用示例

2.1.3 ACL 的功能

借助 ACL，可以实现以下功能：

- 提供安全访问：企业重要服务器资源被随意访问，企业机密信息容易泄露，造成安全隐患。使用 ACL 可以指定用户访问特定的服务器、网络与服务，从而避免随意访问的情况。
- 防止网络攻击：Internet 病毒肆意侵略企业内网，内网环境的安全性堪忧。使用 ACL 可以封堵高危端口，从而达成为外网流量的阻塞。
- 提高网络带宽利用率：网络带宽被各类业务随意挤占，服务质量要求最高的语音、视频业务的带宽得不到保障，造成用户体验差。使用 ACL 实现对网络流量的精确识别和控制，限制部分网络流量从而保障主要业务的质量。

2.1.4 ACL 的组成

ACL 的每一条规则都会允许或者阻止特定的流量，在定义一条合理的 ACL 规则之前，需要了解其基本组成。

- ACL 标识：使用数字或者名称来标识 ACL。
  - 使用数字标识 ACL：不同的类型的 ACL 使用不同的数字进行标识。关于每类 ACL 编号的详细介绍，请参见 ACL 的分类。
  - 使用名称标识 ACL：可以使用字符来标识 ACL，就像用域名代替 IP 地址一样，更加方便记忆。
- 规则：即描述匹配条件的判断语句。
  - 规则编号：用于标识 ACL 规则，所有规则均按照规则编号从小到大进行排序。
    - 动作：包括 permit/deny 两种动作，表示设备对所匹配的数据包接受或者丢弃。
    - 匹配项：ACL 定义了极其丰富的匹配项。包括生效时间段、IP 协议（ICMP、TCP、UDP 等）、源/目的地址以及相应的端口号（21、23、80 等）。

2.1.5 ACL 的分类

随着 ACL 技术的发展，其种类越来越丰富，根据其不同的规则和使用场景，常用的可分为以下几类:

1. 基本 ACL：基本 ACL 规则只包含源 IP 地址，对设备的 CPU 消耗较少，可用于简单的部署，但是使用场景有限，不能提供强大的安全保障。
2. 高级 ACL：相较于基本 ACL，高级 ACL 提供更高的扩展性，可以对流量进行更精细的匹配。通过配置高级 ACL，可以阻止特定主机或者整个网段的源或者目标。除此之外，还可以使用协议信息（IP、ICMP、TCP、UDP）去过滤相应的流量。
3. 二层 ACL：在公司的内部网络中，想对特定的终端进行访问权限控制，这时就需要二层 ACL。使用二层 ACL，可以根据源 MAC 地址、目的 MAC 地址、802.1p 优先级、二层协议类型等二层信息对流量进行管控。
4. 用户 ACL:由于企业内部同部门的工作人员的终端不在同一个网段难以管理,需要将其纳入一个用户组,并对其用户组进行访问权限管理,这时候就需要用户 ACL。用户 ACL 在高级 ACL 的基础上增加了用户组的配置项，可以实现对不同用户组的流量管控。
5. 时间 ACL：在某些特定的时间段内，对特定的流量进行管控，这时就需要时间 ACL。时间 ACL 在高级 ACL 的基础上增加了时间段的配置项，可以实现对不同时间段的流量管控。

2.1.6 ACL 的使用步骤

ACL 的使用分为两个步骤。

1. 设置相应的 ACL 规则：为 ACL 设置相关规则的时候，需要了解入口流量与出口流量，如 Figure 2 所示：入口流量指的是进入设备（以路由器为例）接口的流量（无论来源是外部 Internet 还是内部网络），同理，出口流量指的是从设备接口流出的流量。

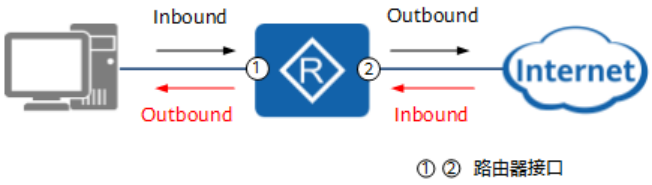

Figure 2: 入口流量与出口流量

当外部 Internet 访问内部网络时，通过路由器接口 2 的入口流量，其源 IP 地址为外部的公网 IP；而当内部网络需要访问外部网络时，通过路由器的接口 1 的入口流量，其源 IP 地址则为内网的 IP。

2. 应用 ACL 规则：规则设置完成后，需要将 ACL 应用在设备的接口上才能正常工作。因为所有的路由和转发决策都是由设备的硬件做出的，所以 ACL 语句可以更快地执行。

2.1.7 ACL 的匹配机制

设备使用 ACL 的匹配机制如 Figure 3 所示。

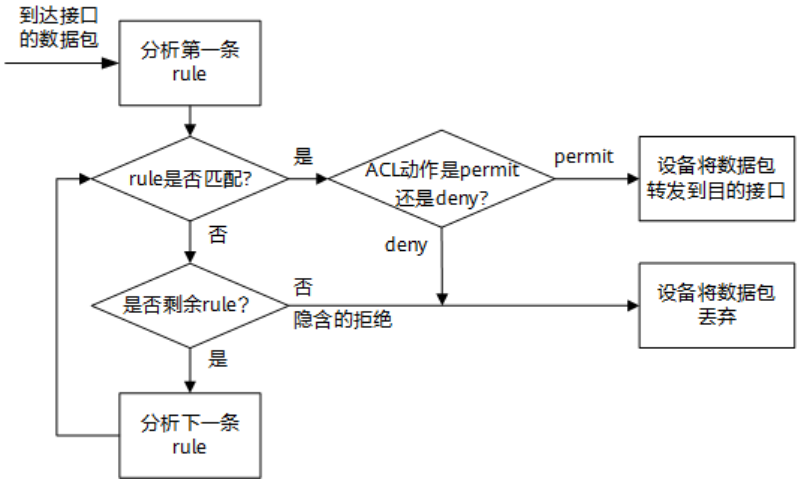

Figure 3: ACL 的匹配机制

ACL 规则的匹配遵循”一旦命中即停止匹配”的机制。当 ACL 处理数据包时，一旦数据包与某条 ACL 规则匹配，就会停止匹配，设备根据该条匹配的语句内容决定允许或者拒绝该数据包。如果数据包内容与 ACL 语句不匹配，那么将依次使用 ACL 列表中的下一条语句去匹配数据包直到列表的末尾。一般在 ACL 的列表末尾会有一条隐式的拒绝所有的语句，所以数据包与所有的规则都不匹配的情况下会被直接拒绝。此时设备不会将此数据包流入或流出接口，而是直接将其丢弃。

2.1.8 ACL 的应用场景

ACL 的应用场景包括以下几个方面：

1. 在 NAT 中使用 ACL：通过 NAT 的端口映射可使得外网访问内部网络。考虑到内部的网络安全，不可能允许所有的外部用户访问内部网络，这时可以设置 ACL 规则并应用在企业路由器上，使得特定的外网用户可以访问内部网络。

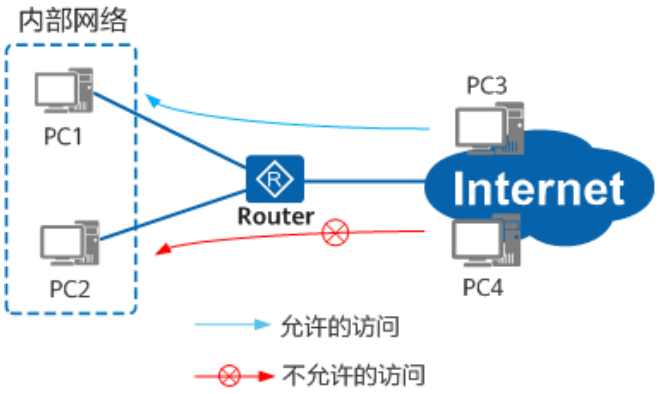

Figure 4: 在 NAT 中使用 ACL

如 Figure 4 所示，当公网主机想建立与内网主机的通信时，其发向内部网络主机的流量经过 NAT 设备时，设备利用 ACL 对流量进行过滤，阻断了 PC4 对 PC2 的访问，同时允许 PC3 对 PC1 的访问。

2. 在防火墙中使用 ACL：防火墙用在内外网络边缘处，防止外部网络对内部网络的入侵，也可以用来保护网络内部大型服务器和重要的资源（如数据）。由于 ACL 直接在设备的转发硬件中配置，在防火墙中配置 ACL 在保护网络安全的同时不会影响服务器的性能。

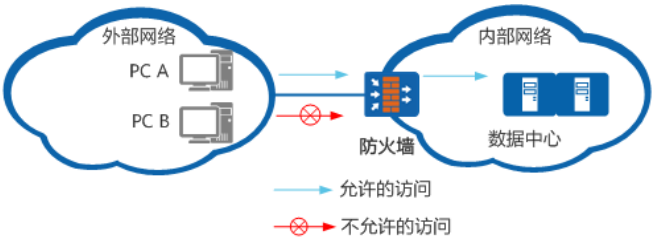

Figure 5: 在防火墙中使用 ACL

如 Figure 5 所示，在防火墙上配置 ACL 只允许外部特定主机 PC A 访问内部网络中的数据中心，并禁止其他外部主机的访问。

3. 在 QoS 中使用 ACL 限制用户互访：ACL 应用在 QoS 的流策略中，可以实现不同网段用户之间访问权限的限制，从而避免用户之间随意访问形成安全隐患。

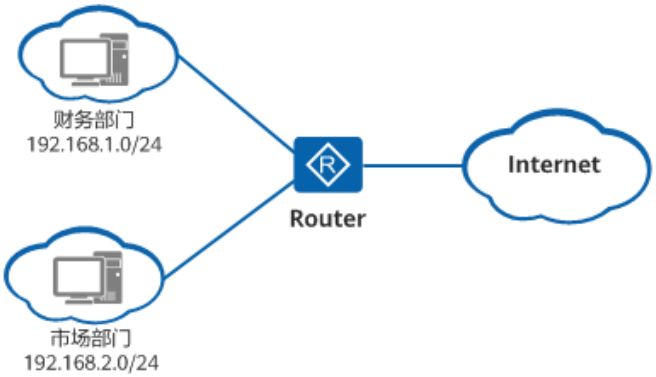

Figure 6: 使用 ACL 限制不同网段用户的互访

如 Figure 6 所示，某公司为财务部和市场部规划了两个网段的 IP 地址。为了避免两个部门之间相互访问造成公司机密的泄露，可以在两个部门连接 Router 的接口的入方向上应用绑定了 ACL 的流策略，从而禁止两个部门的互访。

2.2 防火墙

2.2.1 防火墙基本原理

防火墙是一种网络安全设备，用于监控和控制进出网络的流量，基于预定义的安全规则来允许或阻止数据包的传输。它通常部署在网络边界，用于保护内部网络免受外部威胁。

2.2.2 接口工作模式

防火墙的接口可以工作在以下三种模式之一：

1. 路由模式：当防火墙位于内部网络和外部网络之间时，可同时为设备与内部网络、外部网络相连的接口分别配置不同网段的 IP 地址。报文在三层区域的接口间进行转发时，根据报文的 IP 地址来查找路由表。此时设备表现为一个路由器。
2. 透明模式：接口无 IP 地址。在网络中像连接交换机一样连接防火墙。此时无需修改任何已有的 IP 配置，防火墙就像一个交换机一样工作，内部网络和外部网络必须处于同一个子网。报文在防火墙当中不仅进行二层的交换，还会对报文进行高层分析处理。
3. 混合模式：如果防火墙既存在工作在路由模式的接口（有的接口具有 IP 地址），又存在工作在透明模式的接口（有的接口无 IP 地址），则防火墙工作在混合模式下。这种工作模式基本上是透明模式和路由模式的混合，目前只用于透明模式下提供双机热备的特殊应用中，别的环境下不建议使用。

2.2.3 安全区域

安全区域（简称区域）是一个或多个接口的集合。区域是防火墙功能实现的基础，当数据报文在不同的区域之间传递时，将会触发安全策略进行检查。默认区域包括：

1. Untrust：外网，不安全网络，安全级别是 5。
2. DMZ：停火区，安全级别是 50。
3. Trust：内网，安全网络，安全级别是 85。
4. Local：管理接口、运行动态路由协议，安全级别是 100。

安全级别越大，安全级别越高，不同安全域的级别不能相同。

2.2.4 安全策略

安全策略是防火墙的核心功能，用于控制不同区域之间的流量通信。默认情况下，所有区域间不能通信。安全策略的匹配条件和动作包括：

1. 策略匹配条件：源安全域，目的安全域，源地址，目的地址，用户，服务，应用，时间段。
2. 策略动作：允许，禁止。
3. 内容安全（可选，策略动作为允许的时候执行）：反病毒，攻击防御，URL 过滤，文件过滤，内容过滤，应用行为控制，邮件过滤。

2.2.5 安全策略工作流程

安全策略的工作流程如下:

1. 对收到的流量进行检测，检测出流量的属性，包括：源安全区域、目的安全区域、源地址/地区、目的地址/地区、用户、服务（源端口、目的端口、协议类型）、应用和时间段。
2. 如果所有条件（流量属性）都匹配，则此流量成功匹配安全策略。如果其中有一个条件不匹配，则继续匹配下一条安全策略。以此类推，如果所有安全策略都不匹配，则防火墙会执行缺省安全策略的动作（默认为禁止）。
3. 如果流量成功匹配一条安全策略，防火墙会执行此安全策略的动作。如果动作为禁止，则防火墙会阻断此流量。如果动作为允许，则防火墙会判断安全策略是否引用了安全配置文件。如果引用了安全配置文件，则继续进行步骤 4 的处理；如果没有引用安全配置文件，则允许此流量通过。

3 实验环境

3.1 实验背景

本实验基于华为 USG6303E-AC 防火墙，通过配置 ACL 实现以下需求:

1. Trust 区域在工作时间（周一到周五 09:00-21:00）禁止访问 untrust 区域的娱乐类应用。
2. 允许 trust 区域访问 untrust 区域的其余流量。
3. 允许任意区域访问 DMZ 区域的 http、https、ftp 服务（使用服务组）。

配置步骤包括:

1. 给接口设置 IP 地址。
2. 将接口加入区域。
3. 定义时间段对象、服务对象。
4. 设置安全策略。

3.2 实验设备

设备名称	设备型号	设备数量
防火墙	华为 USG6303E-AC	1
PC	联想启天 M410 Windows 10	3

另有网线若干。

4 实验步骤及结果

4.1 实验拓扑

按实验背景，绘制拓扑图如下:

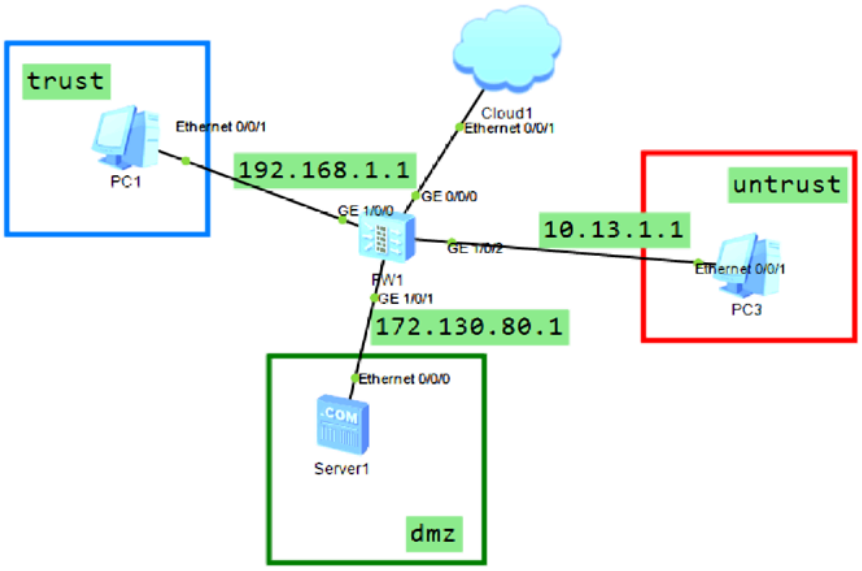

Figure 7: 实验拓扑图

4.2 按照拓扑图接线

按照拓扑图接线。

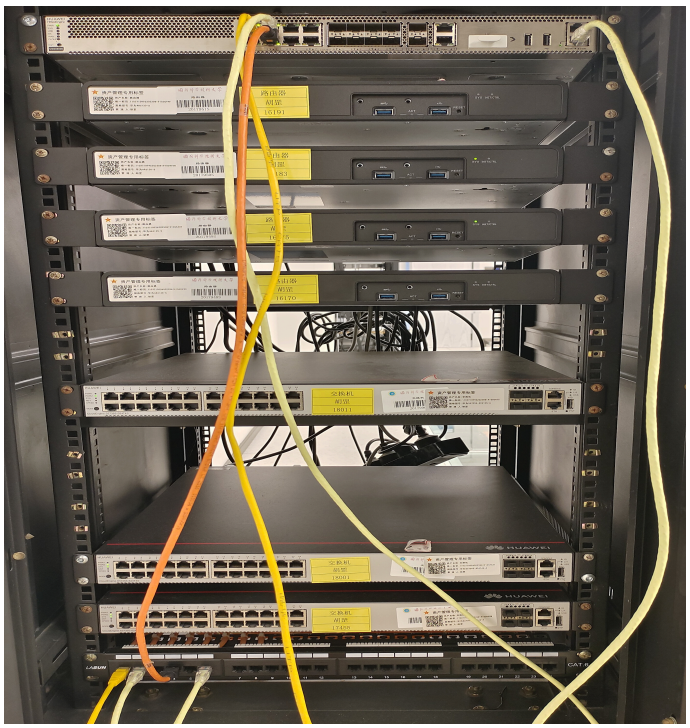

Figure 8: 机柜接线图

4.3 配置基本网络

4.3.1 配置 PC

- 配置 PC1 的 IP 地址为 192.168.1.1/24，网关为 192.168.1.2；

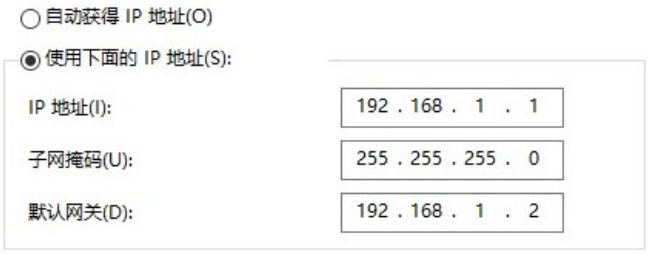

Figure 9: 配置 PC1 的 IP 地址

- 配置 PC2（Server）的 IP 地址为 `172.130.80.1/24`，网关为 `172.130.80.2`；

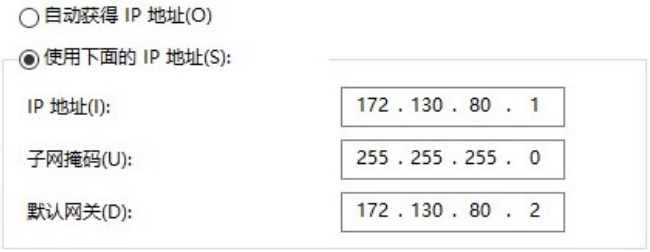

Figure 10: 配置 PC2 的 IP 地址

- 配置 PC3 的 IP 地址为 `10.13.1.1/24`，网关为 `10.13.1.2`；

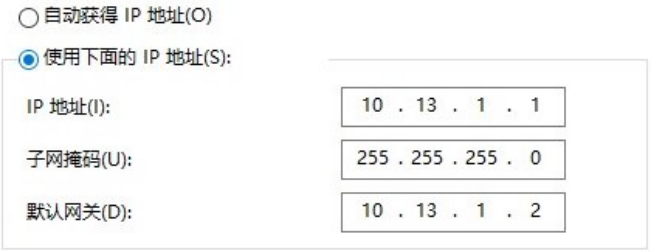

Figure 11: 配置 PC3 的 IP 地址

- 配置管理 PC 的 IP 地址为 `192.168.0.2/24`，网关为 `192.168.0.1`。

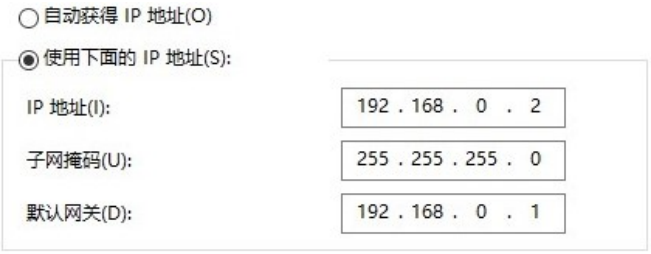

Figure 12: 配置管理 PC 的 IP 地址

这样配置之后，PC1、PC2、PC3 分别属于 `trust`、`dmz`、`untrust` 区域；管理 PC 用于通过 MGMT 网口管理防火墙。

4.4 配置防火墙

4.4.1 配置防火墙接口

通过“网络”-“接口”配置防火墙的接口 IP 地址和区域信息总览：

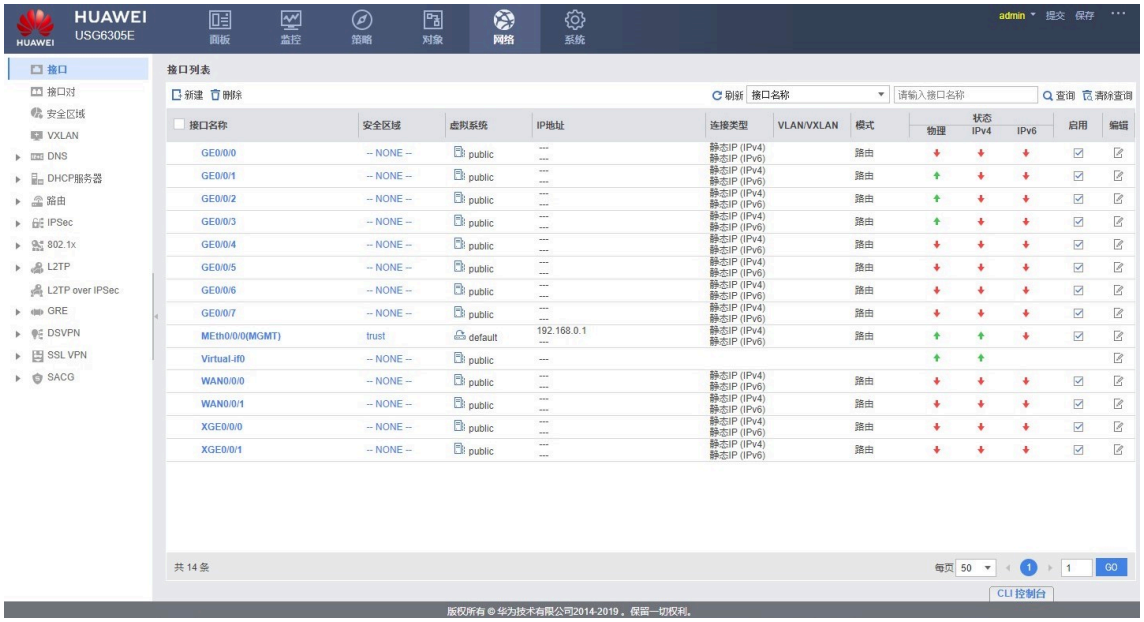

Figure 13: 配置防火墙接口前

- 配置防火墙的 GE0/0/1 接口 IP 地址为 `192.168.1.2/24`，区域为 `trust`；

Figure 14: 配置防火墙的 GE0/0/1 接口

- 配置防火墙的 GE0/0/2 接口 IP 地址为 `172.130.80.2/24`，区域为 `dmz`；

Figure 15: 配置防火墙的 GE0/0/2 接口

- 配置防火墙的 GE0/0/3 接口 IP 地址为 `10.13.1.2/24`，区域为 `untrust`。

Figure 16: 配置防火墙的 GE0/0/3 接口

查看配置结果：

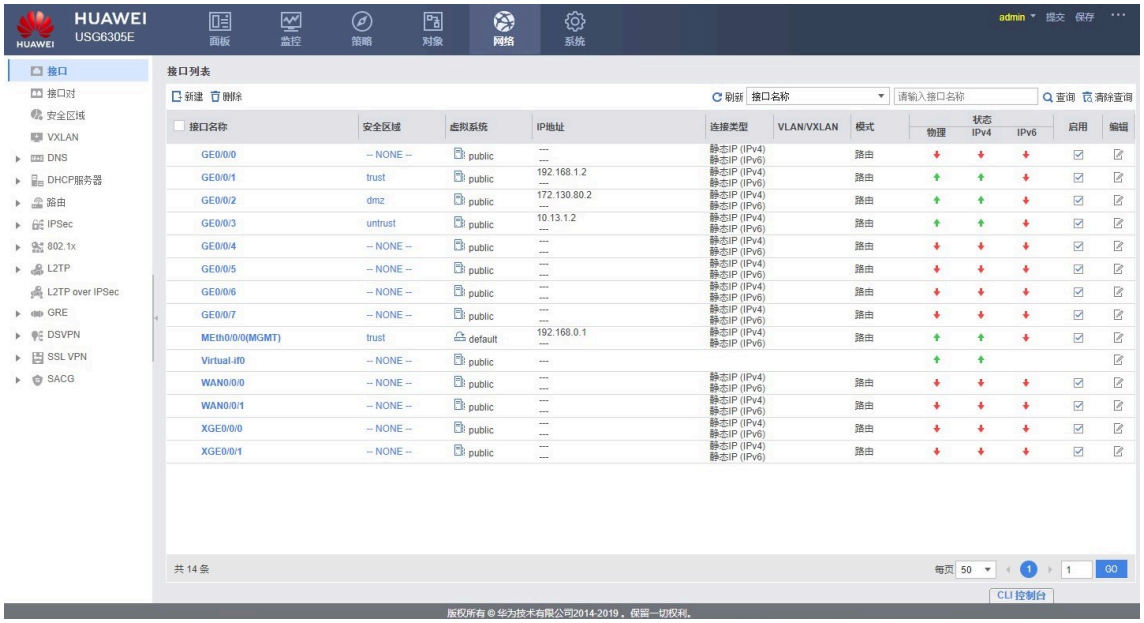

Figure 17: 配置防火墙接口后

4.4.2 配置安全策略

通过“策略”-“安全策略”配置安全策略：

- 配置 trust 区域到 untrust 区域的安全策略，在工作时间禁止访问 untrust 区域：

Figure 18: 配置 trust 区域在工作时间禁止访问 untrust 区域

- 配置 trust 区域到 untrust 区域的安全策略，允许访问其余流量：

Figure 19: 配置 trust 到 untrust 的安全策略

- 创建包含 http、https、ftp 服务的服务组：

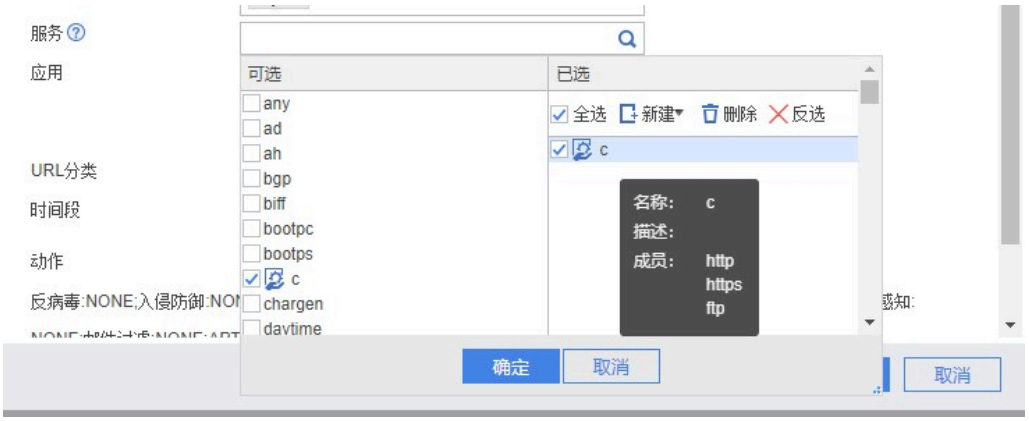

Figure 20: 创建服务组

- 使用创建的服务组配置 trust 区域到 dmz 区域的安全策略：

Figure 21: 配置 trust 到 dmz 的安全策略

- 使用创建的服务组配置 untrust 区域到 dmz 区域的安全策略：

Figure 22: 配置 untrust 到 dmz 的安全策略

配置完成之后，查看总览：

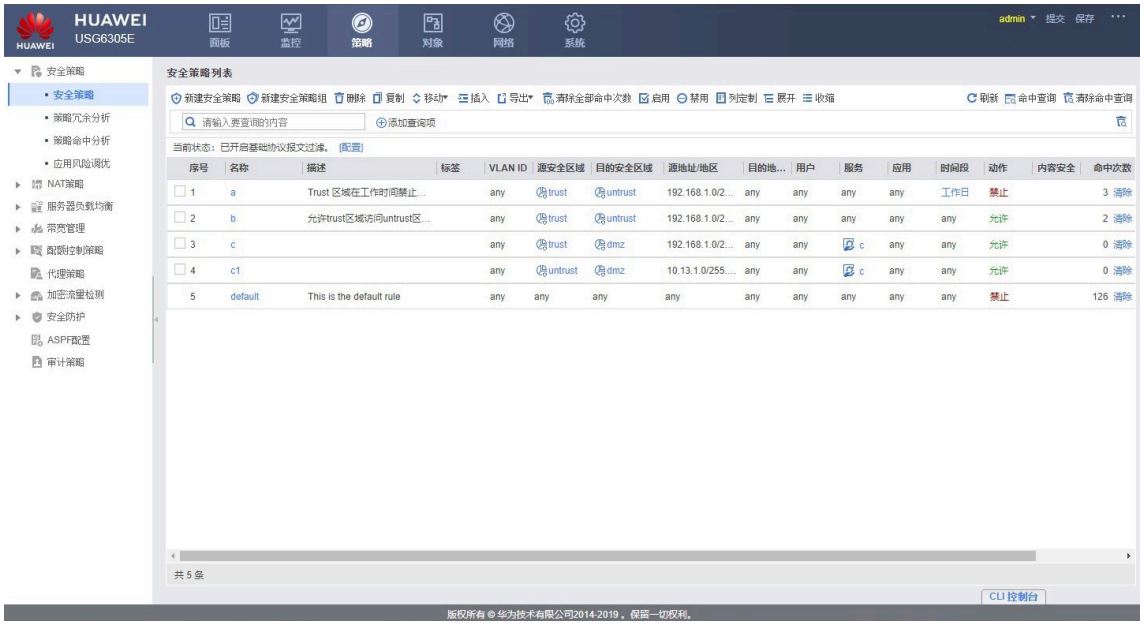

Figure 23: 安全策略总览

4.5 验证配置

在“系统”-“配置”-“时钟配置”中查看防火墙系统时间：

Figure 24: 修查看系统时间

时间为非工作时间（22 点），在 PC1 上 ping untrust 区域的 PC3，可以 ping 通。

修改系统时间为工作时间：

Figure 25: 修改系统时间

时间为工作时间（10 点），在 PC1 上 ping untrust 区域的 PC3，无法 ping 通。

下面是两次 ping 的结果，trust 区域电脑在不同时段内可或不可访问 untrust 区域：

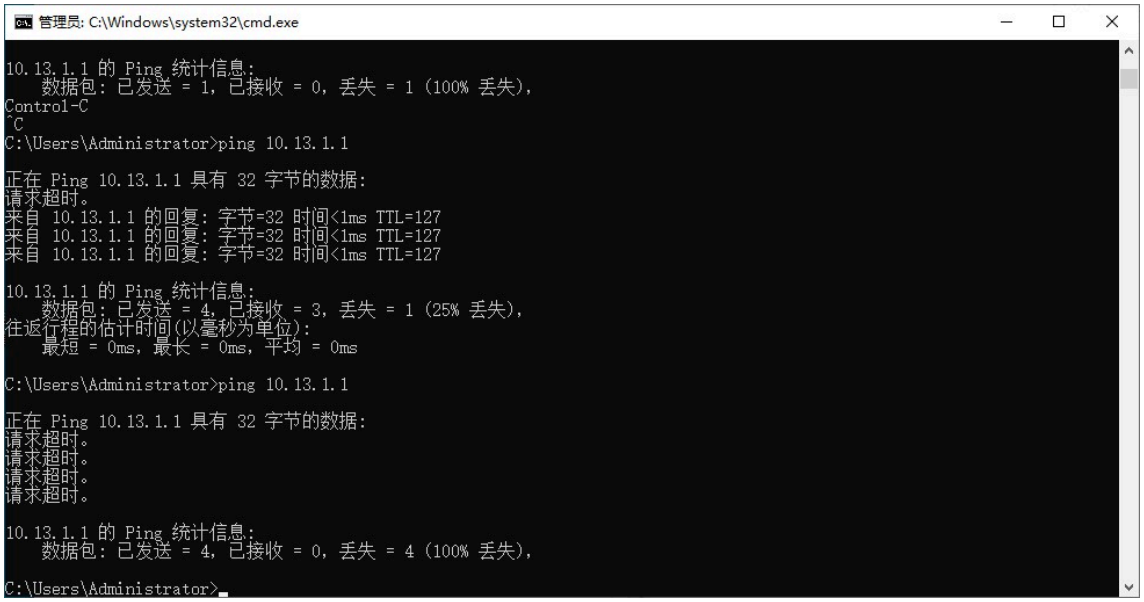

Figure 26: ping 结果

下面是防火墙上针对上述策略的命中次数变化，注意最右侧的命中次数变化，可以看到 ping 发出的 4 个请求被防火墙拦截：

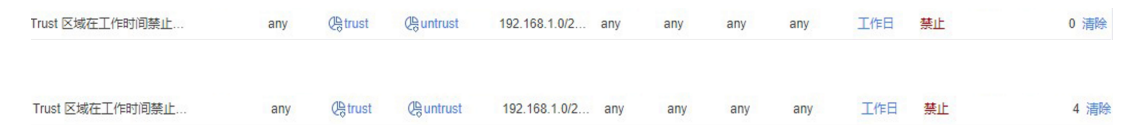

Figure 27: 防火墙命中次数变化

即策略配置无误。

5 实验总结

5.1 内容总结

本实验基于华为 USG6303E-AC 防火墩，通过配置 ACL 实现了以下需求：

1. Trust 区域在工作时间（周一到周五 09:00-21:00）禁止访问 untrust 区域。
2. 允许 trust 区域访问 untrust 区域的其余流量。
3. 允许任意区域访问 DMZ 区域的 http、https、ftp 服务（使用服务组）。

通过配置 ACL，实现了对不同区域之间的流量通信进行了控制，保障了网络的安全。

5.2 思考题

5.2.1 在某防火墙安全规则配置时，已经允许从主机 A 到主机 B 通过 ICMP 协议，但使用 ping 测试时发现从 A 到 B 还是不通，请问是什么原因?

这是一个非常常见的排错场景。ping 命令的成功依赖于一个双向的通信过程，而不仅仅是 A 到 B 的单向。

请求 (Request): 主机 A 发送一个 `ICMP Echo Request` 报文给主机 B。回复 (Reply): 主机 B 收到后，必须回复一个 `ICMP Echo Reply` 报文给主机 A。

我们在实验中配置的规则 `允许 A -> B` 只保证了第一步（请求）的成功。`ping` 仍然失败，最可能的原因是第二步（回复）的报文被阻断了。

以下是几个最可能的原因，按排查优先级排序：

1. 缺少返回策略 (最常见)： 防火墙是双向检查的。当主机 B 回复报文时，这个报文的流向是 `B -> A`。如果防火墙上没有配置“允许主机 B 到主机 A 的 ICMP 流量”的策略，这个回复报文就会被防火墙丢弃，主机 A 也就永远收不到回复，导致 `ping` 超时。 解决方法：(状态检测)：如果防火墙开启了状态检测（Stateful Inspection），它会自动“记住”A 发出的请求，并自动放行 B 的回复。需要检查防火墙是否为 ICMP 开启了状态检测。(静态 ACL)：如果防火墙是无状态的（或 ICMP 状态检测被关闭），必须额外添加一条反向规则，允许 `ICMP Echo Reply` 从 B 到 A。
2. 主机 B 的本地防火墙： 网络防火墙（如 FW1）可能放行了流量，但是主机 B 自己的防火墙（例如 Windows 防火墙或 Linux 的 iptables）默认配置为“禁止入站 ICMP 请求”。这是 Windows 操作系统出于安全考虑的默认设置。解决方法：登录主机 B，修改其本地防火墙设置，添加入站规则以允许 “文件和打印机共享(回显请求 - ICMPv4-In)”。
3. 路由问题： B 没有到 A 的路由：主机 B 可能不知道如何将回复报文“送回”给主机 A 所在的网段。需要检查主机 B 的路由表或其默认网关的路由表，确保有返回到主机 A 网段的路由。A 没有到 B 的路由：虽然的安全策略允许了，但主机 A 或其网关可能根本不知道如何将数据包路由到主机 B。
4. NAT (地址转换) 问题： 如果主机 A 在内网，主机 B 在外网，主机 A 访问 B 时源地址被 NAT 成了防火墙的公网地址。当 B 回复时，它会回复给防火墙的公网地址。需要检查防火墙上的 NAT 配置和会话表（`display firewall session table`），确认 ICMP 的 NAT 转换和会话是否都正常建立。

5.2.2 2）什么是 DMZ，设置 DMZ 有何意义?

- DMZ 是 “Demilitarized Zone” 的缩写，中文译为“隔离区”或“非军事区”。

在网络安全中，DMZ 是一个物理或逻辑上的子网络，它位于公司的内部私有网络 (Trust 区) 和外部公共网络 (Untrust 区 / Internet) 之间。它是一个缓冲区，一个“三不管”地带。

- 设置 DMZ 的核心意义是“隔离风险，保护内网”。

具体来说，公司里总有一些服务器是必须被外网（互联网）访问的，例如：公司官网的 Web 服务器 Email 服务器 (SMTP) DNS 服务器

这些服务器由于暴露在互联网上，是黑客攻击的主要目标。

1. 风险隔离： 我们不能把这些“高风险”的服务器直接放在内网（Trust 区）。如果 Web 服务器被黑客攻陷了，而它又在内网，那么黑客就能以此为跳板，直接攻击内网的员工电脑、财务数据、核心数据库等，后果不堪设想。
2. 保护内网 (核心)：通过将这些服务器放在 DMZ 区域，我们就建立了一道新的安全屏障。防火墙可以对这三个区域（Trust, Untrust, DMZ）实施精细的访问控制： 外网 (Untrust) -> DMZ：有限允许。只开放必须的端口（如 Web 服务的 80/443 端口）。 内网 (Trust) -> DMZ：有限允许。允许内网管理员去管理 DMZ 的服务器（如 SSH, RDP）。 DMZ ->

内网 (Trust)：绝对禁止。这是最关键的一条策略！禁止任何从 DMZ 发起的、指向内网的连接。

5.3 心得感悟

通过本次实验，我学会了如何配置 ACL，实现了对不同区域之间的流量通信进行了控制，保障了网络的安全。在实验过程中，我对防火墙的接口配置、安全策略配置有了更深入的了解，提高了自己的实际操作能力。

参考文献

[1] 华为. 什么是 ACL？如何使用 ACL?[EB/OL]. 中国: 华为, 2024. https://info.support.huawei.com/info-finder/encyclopedia/zh/ACL.html.