网络技术与信息安全

第9讲 防火墙日志分析

河南中医药大学信息技术学院

许成刚

一、认识防火墙日志

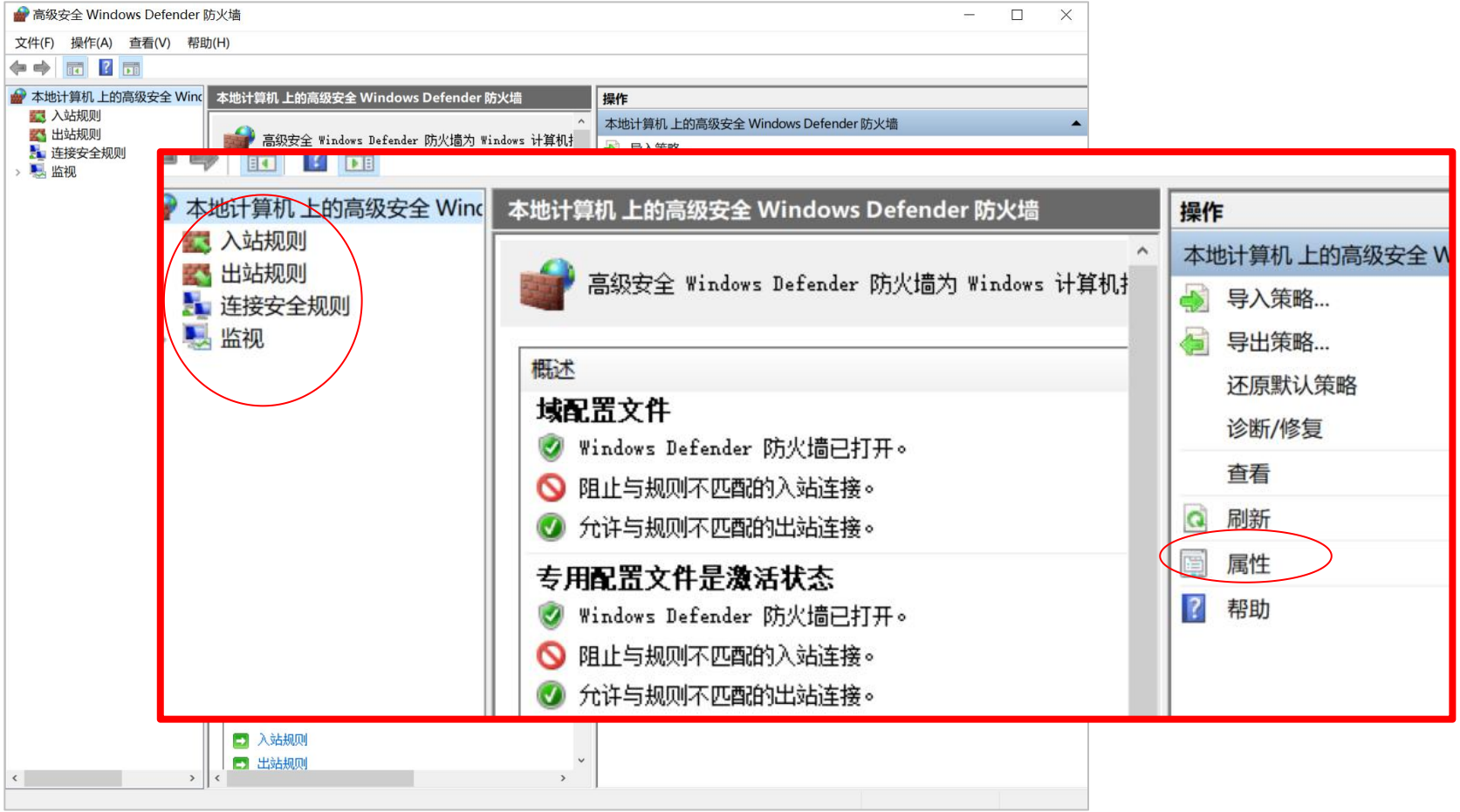
认识防火墙日志

什么是防火墙日志

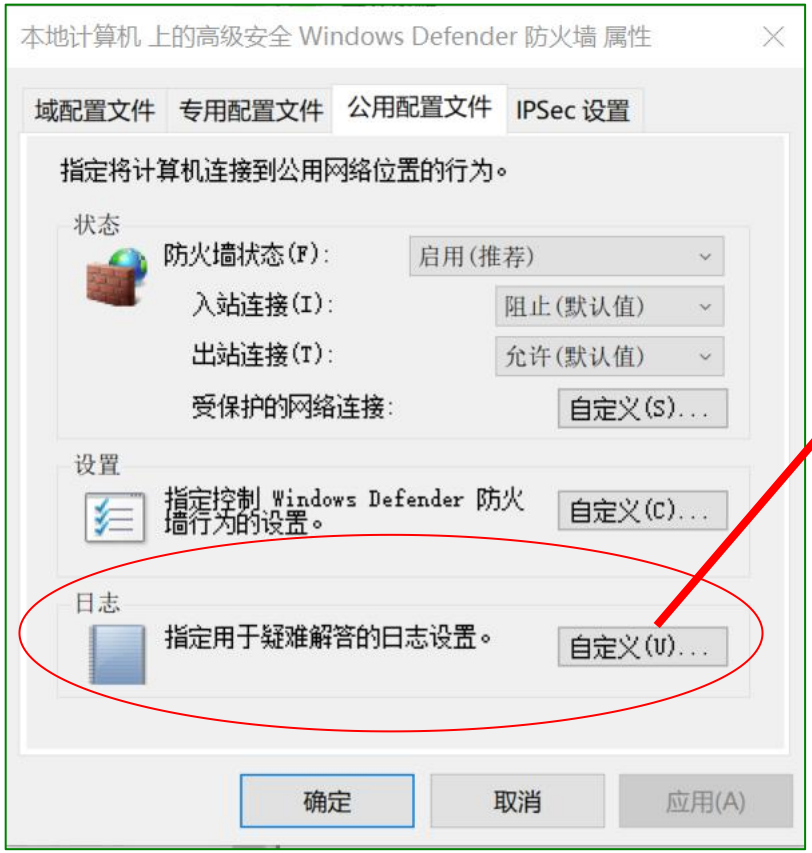
- 日志是FW在运行过程中输出的信息，通过查看日志，管理员可以实时了解网络中各种业务的运行状态，掌握FW上各个功能模块的运行情况；
- 由于网络中的数据流要经过防火墙，因此通过分析防火墙日志，可以发现用户的上网行为。

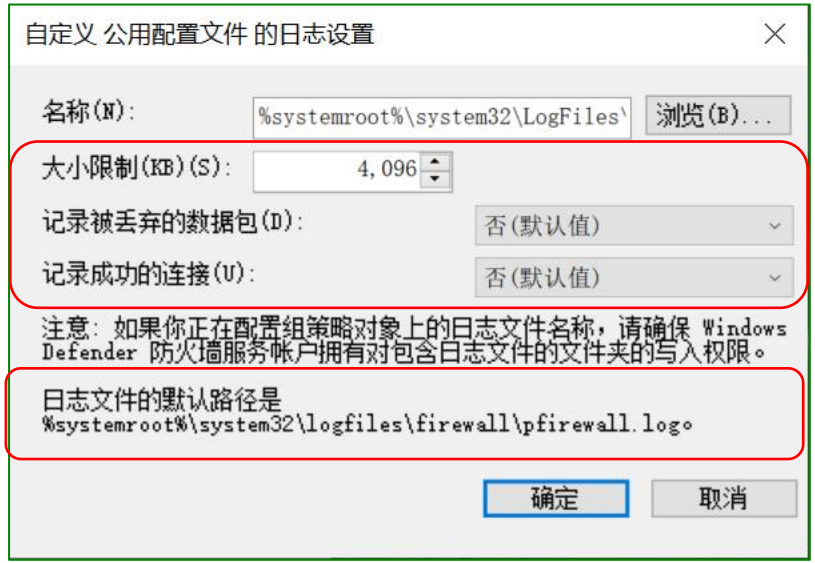
- 举例：Windows防火墙中的日志

举例：Windows防火墙的日志



举例：Windows防火墙的日志





认识防火墙日志

日志类型

FW支持的输出日志，常见的有：

- 安全事件日志
  - 记录所有与网络安全相关的信息，包括入侵检测、攻击行为等。管理员可通过安全日志查看网络上的安全事件，并及时采取相应的应对措施。
- 访问控制日志
  - 记录网络连接请求的允许或拒绝状态，包括源/目的IP、端口、协议等详细信息，用于验证防火墙规则有效性。
- 系统日志
  - 系统日志记录防火墙设备本身的运行状态和事件，包括硬件故障、软件异常等。管理员可通过系统日志监控设备的性能表现，及时发现和解决问题，确保设备稳定运行。

认识防火墙日志

日志类型

FW支持的输出日志，常见的有：

- 用户行为日志
  - 记录网络用户的行为活动，包括登录、访问网站、下载文件等。管理员可通过用户行为日志监控用户的上网行为。
- 流量（会话）日志
  - 统计网络流量数据，包括带宽使用、会话持续时间、数据传输量等，用于网络性能优化。

    报文经过FW处理后将会在FW上建立会话。FW支持会话信息的输出，管理员可以根据实际需要，选择在会话老化后输出、新建会话时输出、或者定期输出会话信息。

认识防火墙日志

日志格式

FW支持的日志格式如下：

Syslog格式

- 系统日志协议（syslog),用来记录设备的日志，标准化网络设备与日志服务器通信的消息格式。
- 网络中的路由器、交换机、防火墙、Unix/Linux 服务器等众多设备都支持它，更容易管理这些设备生成的日志。
- 会话日志、丢包日志、业务日志以及系统日志以Syslog格式输出时，日志的信息以文本格式呈现。

认识防火墙日志

日志格式

二进制格式

- 会话日志以二进制格式输出时，占用的网络资源较少，但不能在FW上直接查看，需要输出到日志服务器查看。

Netflow格式

- 对于会话日志，FW还支持以Netflow格式输出到日志服务器进行查看，便于管理员分析网络中的IP报文流信息。

Dataflow格式

- 业务日志以Dataflow格式输出，在日志服务器上查看。

认识防火墙日志

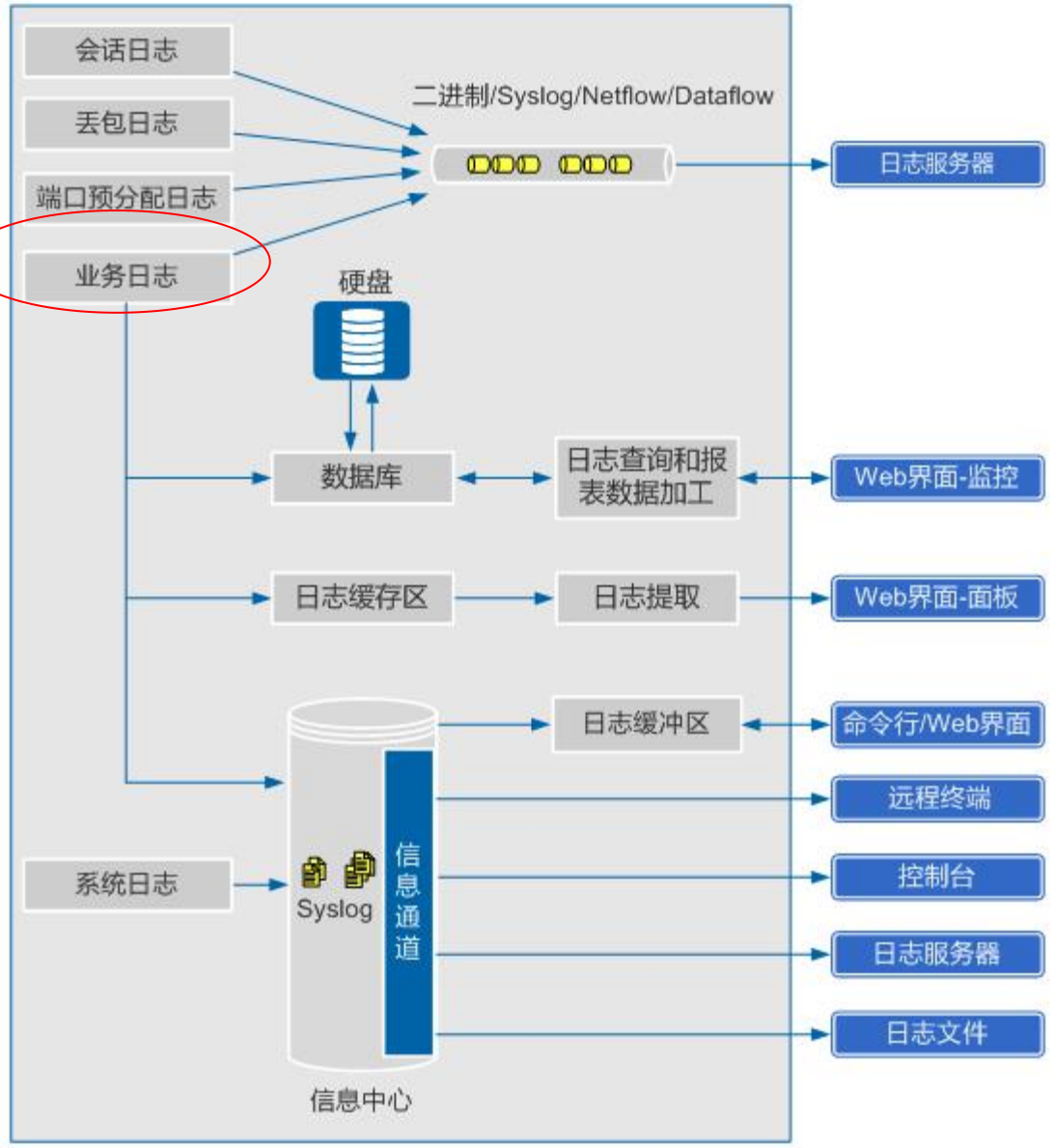
日志输出的方式

- 在防火墙上，不同类型的日志，其输出方式也有区别。例如：
  - 对于会话日志、丢包日志和端口预分配日志，防火墙通过单独的通道，直接输出到日志服务器，供管理员进行查看和分析。
  - 对于业务日志，可以通过单独的通道，直接输出到日志服务器，供管理员进行查看和分析；可以输出到内存数据库中，然后经过日志查询模块统计加工后，以日志和报表的形式显示在Web界面上；可以输出到日志缓存区中，然后显示在Web界面的“面板”上；还可以通过信息中心输出。
  - 对于系统日志，防火墙通过信息中心输出。信息中心是防火墙上系统软件模块的信息枢纽，可以将系统日志向日志服务器、日志缓冲区、控制台（Console用户界面）、终端（VTY用户界面）、日志文件等方向输出。管理员可以在防火墙上查看系统日志，也可以在日志服务器上查看系统日志。

日志的输出方式

例如业务日志：

1. 可以通过单独的通道，直接输出到日志服务器；
2. 可以输出到内存数据库，然后经过日志查询模块统计加工后，以日志和报表的形式显示在Web界面上；
3. 可以输出到日志缓存区中，然后显示在Web界面的“面板”上；
4. 可以通过信息中心输出



二、日志服务器的应用

日志服务器的应用

日志服务器（Syslog 服务器）的作用

- 日志服务器是集中接收、存储、解析防火墙 / 交换机 / 路由器等网络设备 syslog 日志的服务器。
- 防火墙本地存储空间有限，日志会循环覆盖，把防火墙日志外发到日志服务器，实现长期保存、审计、检索、告警、等保（网络安全等级保护）合规。具体如下：
  - 长期存储：不受防火墙本地磁盘限制，日志不会被循环覆盖；
  - 集中审计：多台防火墙、交换机日志统一在一处查询；
  - 故障排查：统一检索五元组，查哪些流量被 deny；
  - 安全分析：检测扫描、暴力破解，安全事件溯源；
  - 等保合规：满足日志留存 6 个月的审计要求。

日志服务器的应用

使用日志服务器的基本流程

- 防火墙（Syslog 客户端）→网络→日志服务器（Syslog 服务端）

1. 防火墙生成流量、NAT、IPS、系统日志；
2. 按照 RFC3164/RFC5424/CEF 格式，通过 UDP/TCP 发送给日志服务器IP；
3. 日志服务器接收，保存到文件 / 数据库；
4. 支持检索、过滤、报表、告警。

日志服务器的应用

日志服务器与防火墙的通信

- 为了保证防火墙与日志服务器之间的正常通信，需要在防火墙上设置日志服务器信息，即配置防火墙与日志服务器通信时使用的参数。如果网络中存在多台日志服务器，则可以在防火墙上设置多个日志主机，实现日志主机的容灾备份功能。
- 防火墙和日志服务器对接，不同格式的日志都有固定的UDP端口号

日志格式	默认情况下日志服务器的接收端口
二进制格式	9002
Dataflow格式	9903
Netflow格式	9996
Syslog格式	514

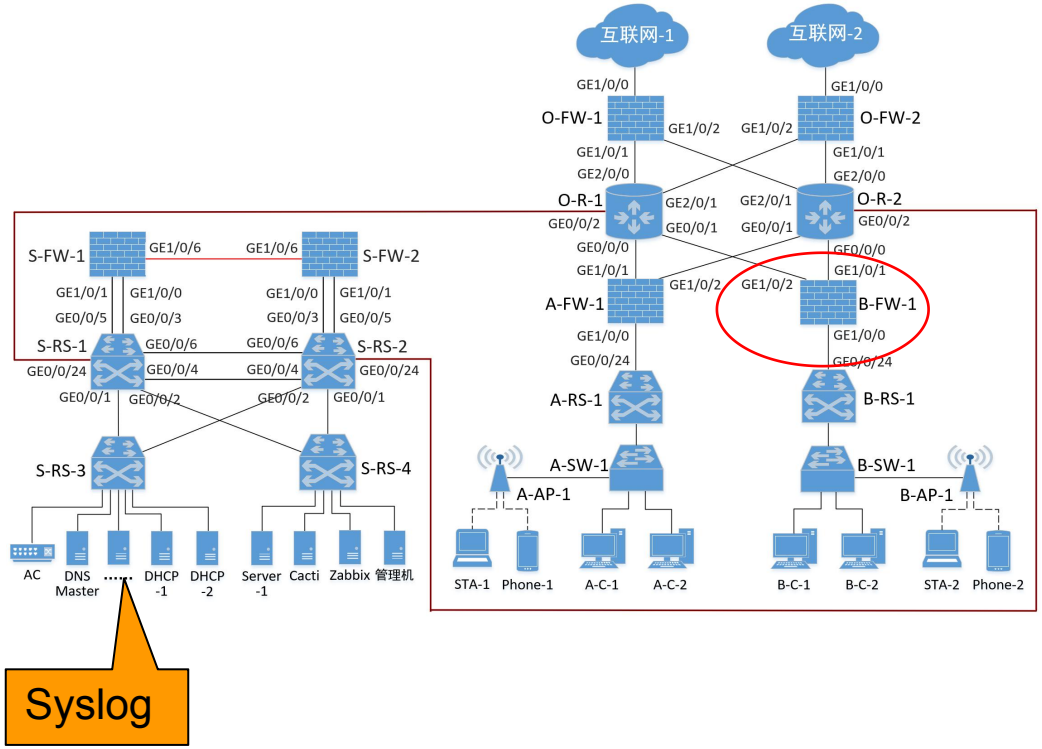
【案例】

Syslog日志服务器的部署应用

【案例】日志服务器的部署应用

- 要点：

1. Syslog日志服务器的安装与配置；
2. 在防火墙上配置日志服务器信息并进行日志收集；
3. 查看防火墙日志



【案例】日志服务器的部署应用

要点1：安装配置Syslog服务器

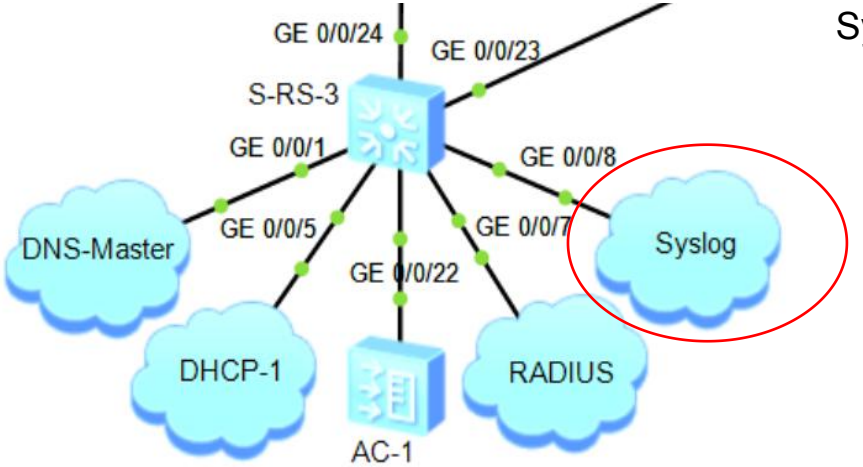
① 在VirtualBox中创建Centos虚拟机。

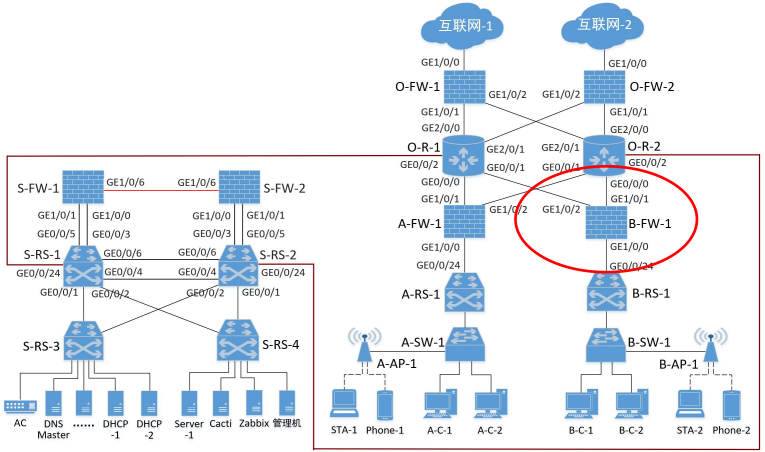
② 配置Syslog日志服务器。

启用UDP和TCP传输

定义Syslog日志模板及日志存放位置

③ 接入eNSP网络





Syslog

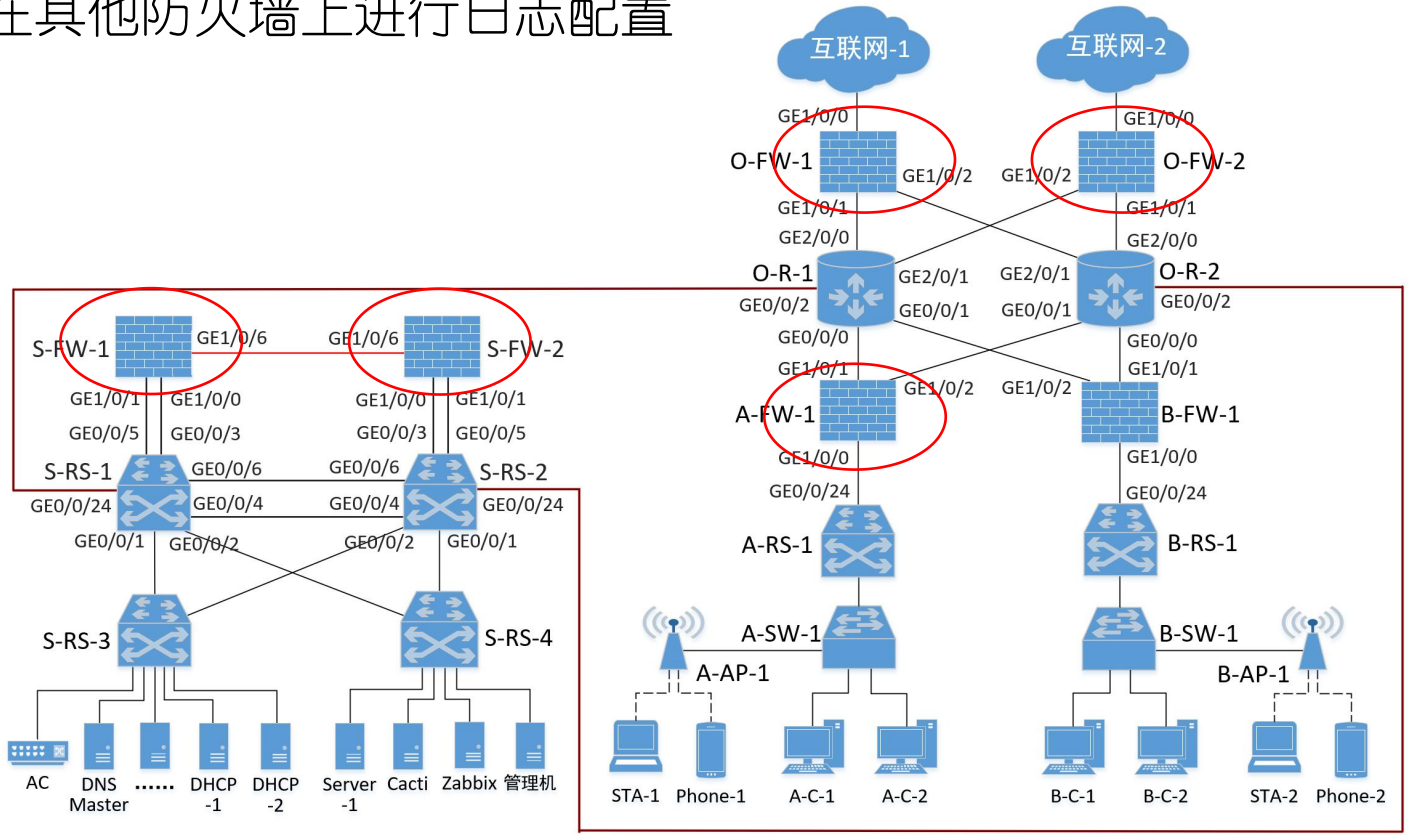
【案例】日志服务器的部署应用

- 要点2：配置防火墙A-FW-1使用日志服务器记录日志
  - 在防火墙A-FW-1上添加日志服务器信息
  - 在安全策略列表中启用日志
  - 开启防火墙日志中心

在防火墙A-FW-1上添加日志服务器信息

【案例】日志服务器的部署应用

- 要点3：在其他防火墙上进行日志配置

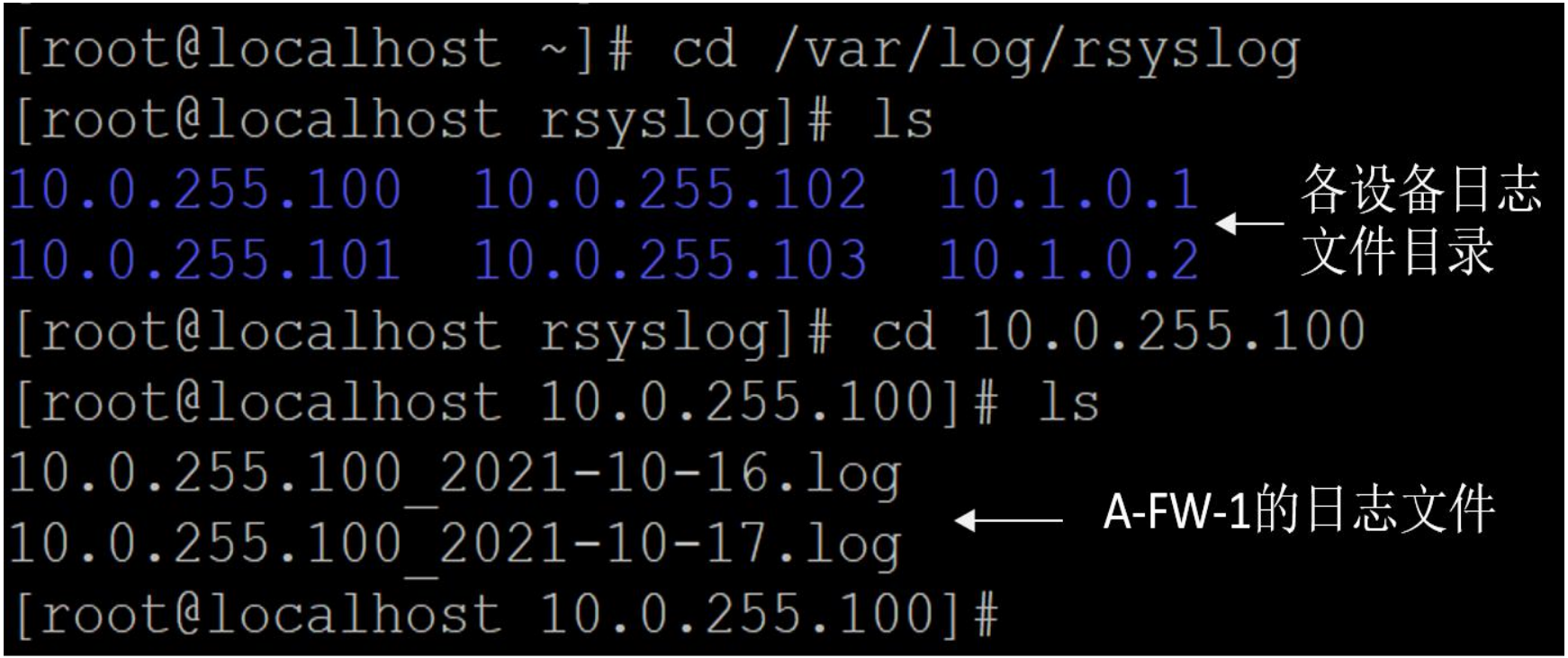


【案例】日志服务器的部署应用

- 要点4：在日志服务器上查看日志文件
  - 根据前面的设置，我们把各个防火墙的日志以设备为单位放在了日志服务器Syslog的/var/log/rsyslog目录下。
  - 进入/var/log/rsyslog目录，可以看到6个子目录，分别用A-FW-1、B-FW-1等六个防火墙的管理IP地址命名（每个设备的日志文件放在独立的目录中）。
  - 进入10.0.255.100目录，可以看到防火墙A-FW-1的日志文件，文件名分别为10.0.255.100_2021-10-16.log和10.0.255.100_2021-10-17.log，表示分别存放A-FW-1在2021年10月16日和17日的日志记录
  - 具体见下页

【案例】日志服务器的部署应用

- 要点4：在日志服务器上查看日志文件



【案例】日志服务器的部署应用

- 要点5：查看日志文件的内容

命令：

```
# vi /var/log/rsyslog/10.0.255.100/10.0.255.100_2021-10-17.log
```

//日志文件中包含大量日志记录信息，本记录与用户test123登录失败有关

Oct 17 08:23:51 A-FW-1 %%01CM/5/USER_ACCESSRESULT(s)[294]: [USER_INFO_AUTHENTICATION]DEVICEMAC:00-e0-fc-07-72-96;DEVICENAME:A-FW-1;USER:test123;MAC:ff-ff-ff-ff-ff-ff;IPADDRESS:192.168.64.200;TIME:1634459031;ZONE:UTC+0800;DAYLIGHT:false;ERRCODE:133;RESULT:Authentication fail;AUTHENPLACE:Local;CIB ID:641;ACCESS TYPE:None;

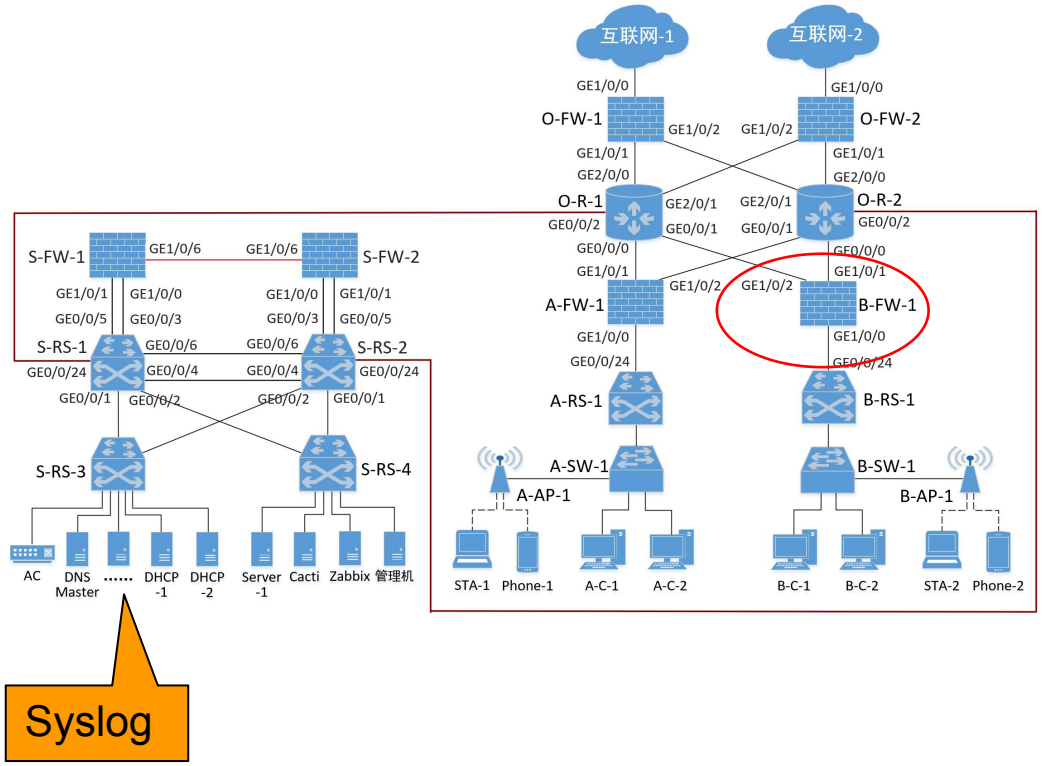
【内容字段含义见下页】

日志内容	说明
Oct 17 08:23:51	日志产生时间，格林尼治时间
A-FW-1	指产生日志的设备
CM/5/USER_ACCESSRESULT	日志消息中的标记。含义：用户上线
USER_INFO_AUTHENTICATION	用户认证信息
DEVICEMAC:00-e0-fc-07-72-96	产生日志的设备的MAC地址，即A-FW-1的MAC地址
DEVICENAME:A-FW-1	产生日志的设备名称：A-FW-1
USER:test123	认证用户名。注意test123是错误的用户名
MAC:ff-ff-ff-ff-ff-ff	认证用户MAC地址
IPADDRESS:192.168.64.200	认证用户的IP地址：192.168.64.200 （即实体主机A）
TIME:1634459031	上线时间
ZONE:UTC+0800	时区，东八区，在原时间上+8小时
DAYLIGHT:false	是否夏令时（否）
ERRCODE:133	错误码是133
RESULT:Authentication fail	结果：认证失败
AUTHENPLACE:Local	认证位置：本地（A-FW-1采用本地认证）
CIB ID:641	CIB编号：641
ACCESS TYPE:None	接入类型：如果用户上线不成功，则接入类型记录为None

三、防火墙日志分析

日志分析——分析用户上网行为

- 【实验案例】分析用户上网行为
- 要点：
  1. 完成Tableau软件的安装；
  2. 实现使用Tableau分析防火墙日志及用户上网行为



日志分析——分析用户上网行为

- 要点1：在本地实体主机上安装Tableau软件

日志分析——分析用户上网行为

- 要点2：筛选（清洗）防火墙日志
  - 在使用Tableau进行数据分析时，首先需要根据分析目标对采集到的数据进行清洗。
  - 为了突出重点并减少清洗数据的成本，此处首先对防火墙A-FW-1的日志进行配置：一是在日志文件中只保存会话日志；二是会话日志格式模板中只显示设备名称、源IP、目的IP、发送报文数量、接收报文数量、协议字段的内容。

【模版设置见下页】

设置日志模版，筛选（清洗）防火墙日志

新建Syslog日志模板

名称 Mytemplate *

配置模式 表达式 列表

IPv4会话日志

关联自定义日志字段

字段	名称	操作
$ipversion	ip-version	
$protocol	protocol	
$srcip	source-ip	
$srcport	source-port	
$dstip	destination-ip	
$dstport	destination-port	
$srcnatip	source-nat-ip	
$srcnatport	source-nat-port	
$dstnatip	destination-nat-ip	
$dstnatport	destination-nat-…	

日志格式

$hostname $srcip $dstip $sendpackets $rcvpackets $protocol *

配置举例：

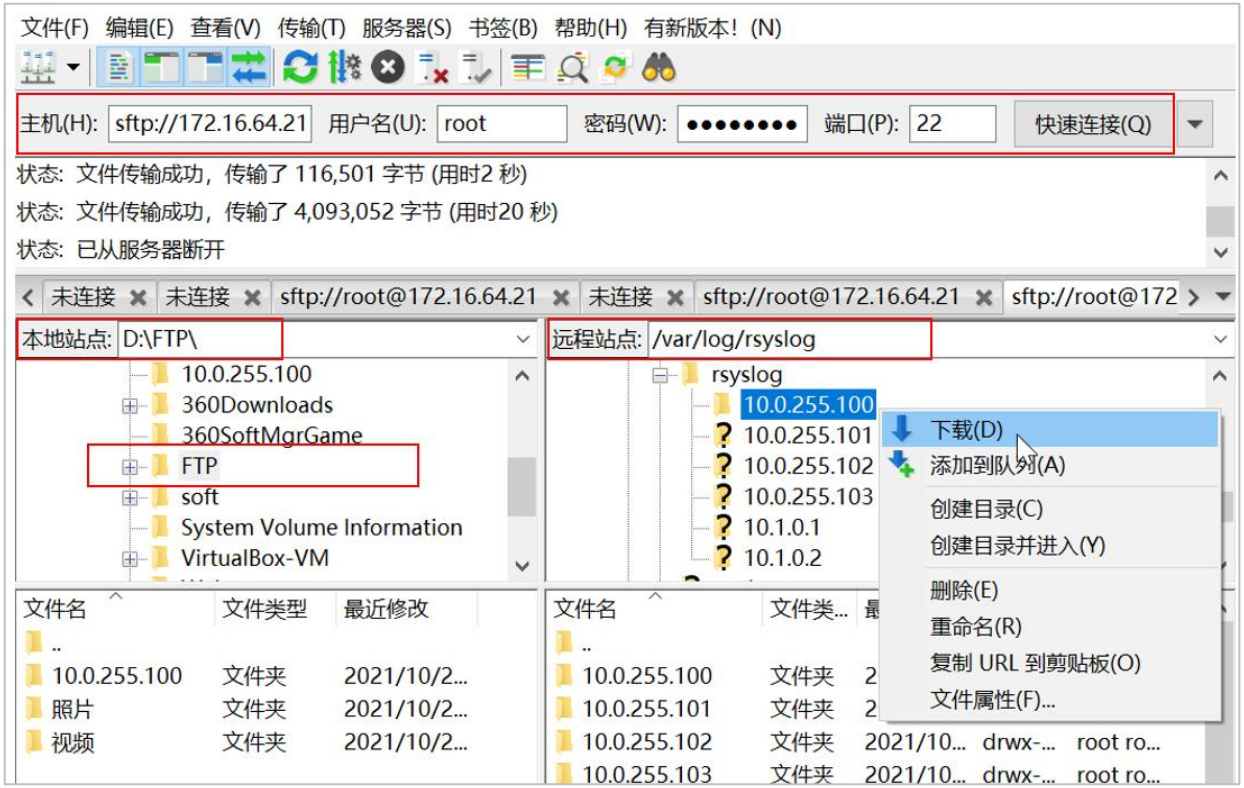
$protocol $srcip:$srcport -> $dstip:$dstport BeginTime :$begintime EndTime: $endtime SendPkts=$sendpackets, SendBytes=$sendbytes, RcvPkts=$rcvpackets, RcvBytes=$rcvbytes

日志效果：

udp 2.2.2.2:10043 -> 2.2.2.1:20000 BeginTime :2017-10-19T13:21:03+08:00 EndTime: 2017-10-19T13:21:45+08:00, SendPkts=1, SendBytes=114, RcvPkts=1, RcvBytes=56

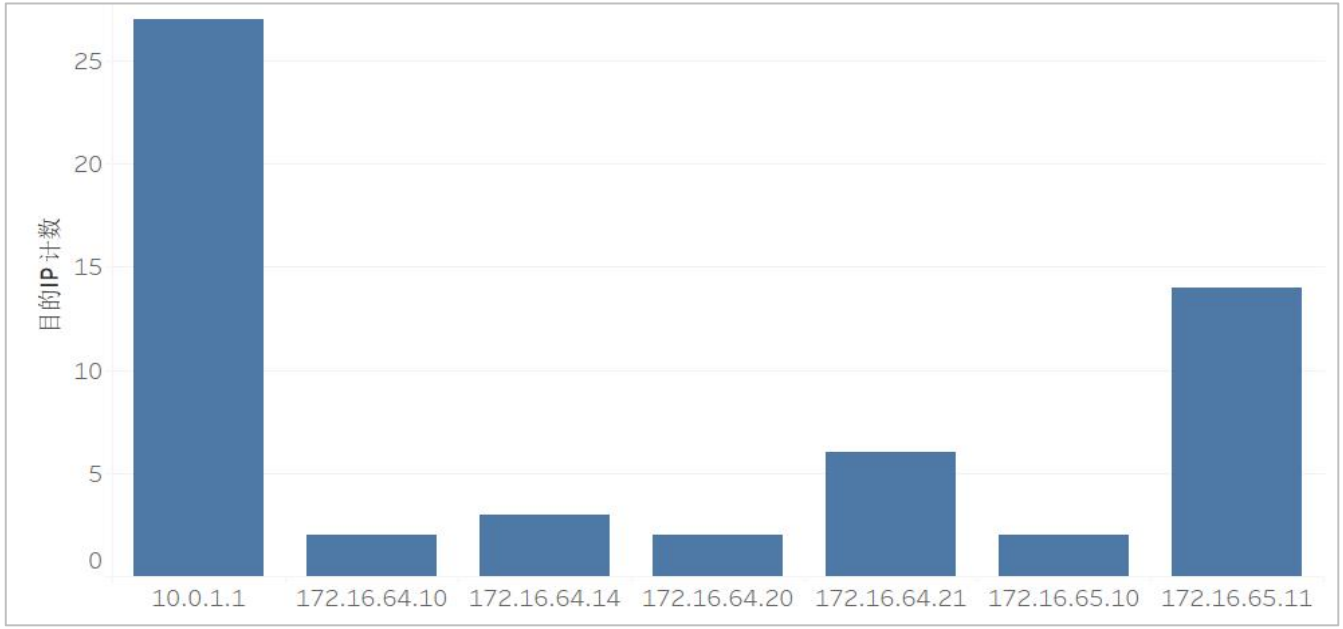
日志分析——分析用户上网行为

- 要点3：将防火墙A-FW-1的日志文件下载到本地主机
  - 在本地主机上安装FileZilla客户端软件，将防火墙日志文件下载到本地主机



日志分析——分析用户上网行为

- 要点4：使用Tableau软件分析防火墙日志（过程略）
  - 用户主机192.168.64.200访问各服务器的频次以柱状图的形式展示出来



往届学生

防火墙日志分析报告

【第1组】

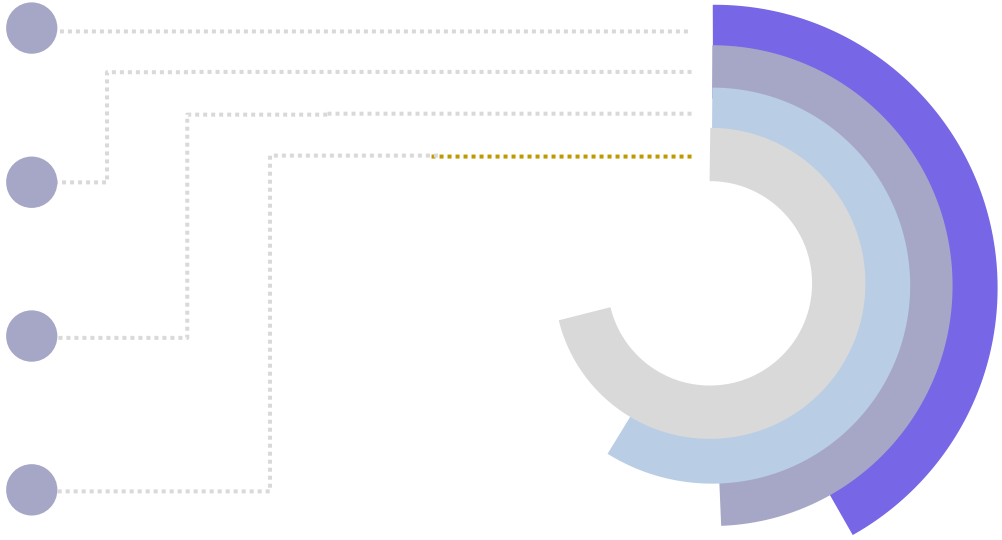
分析内容设计

用户活跃度分析

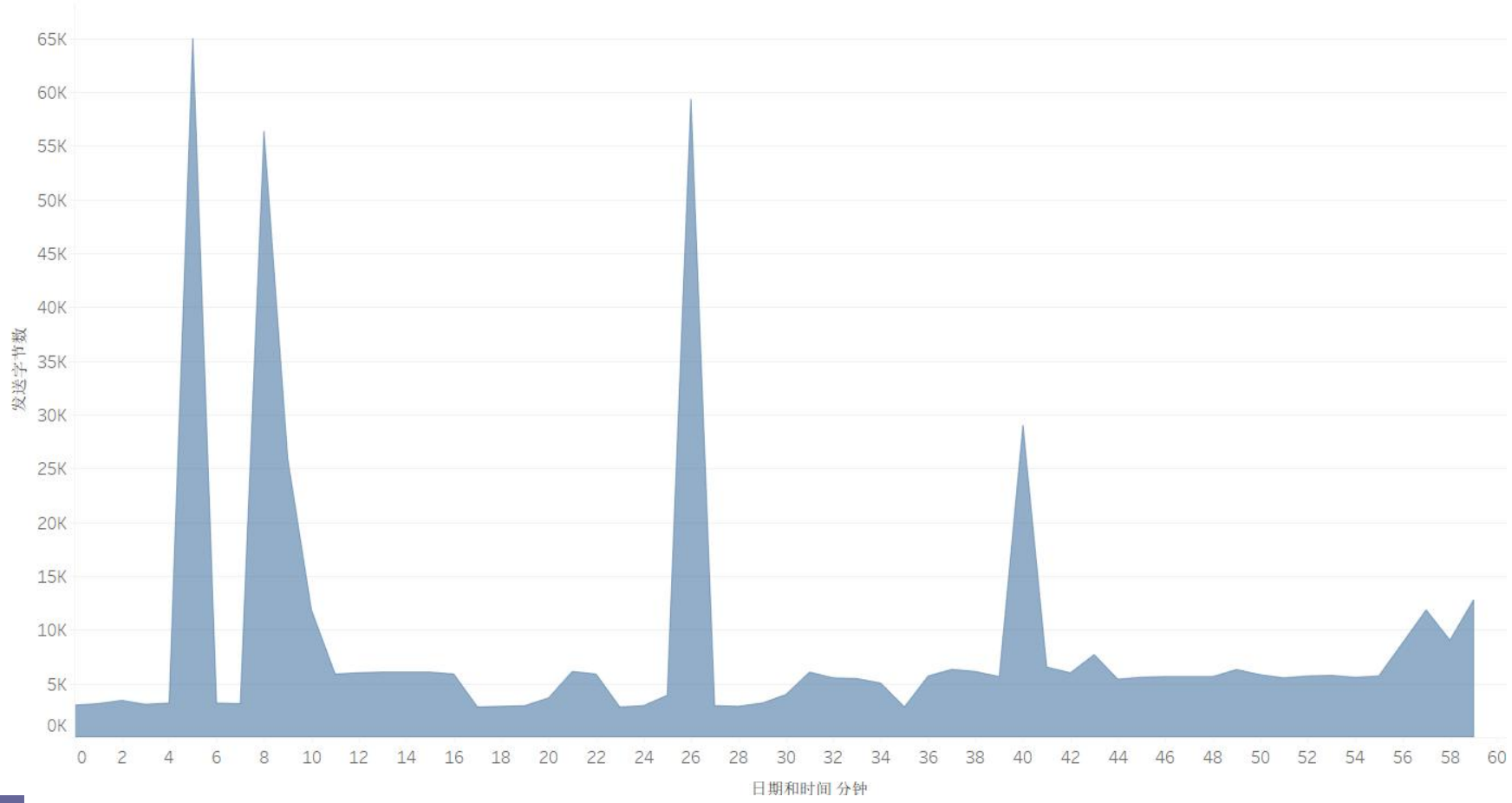
目的IP分析

协议组分析

被拒主机排行分析

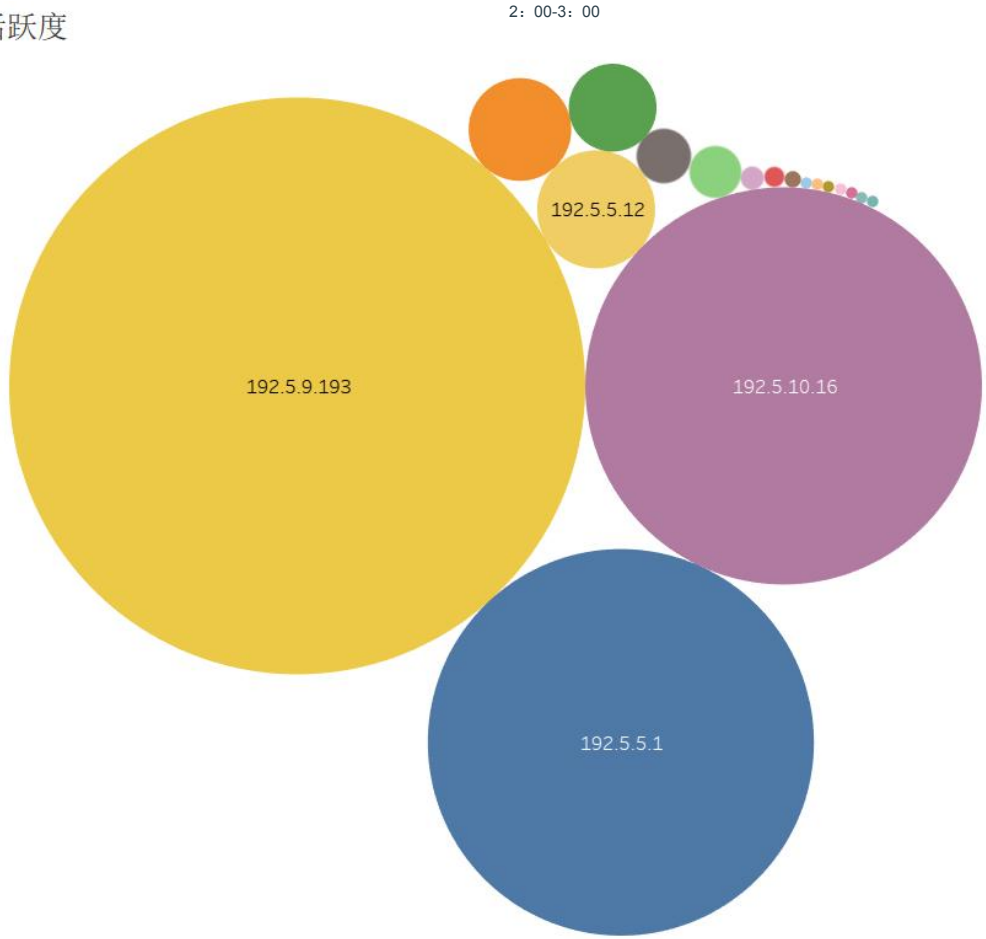


夜间2：00-3：00的流量报表



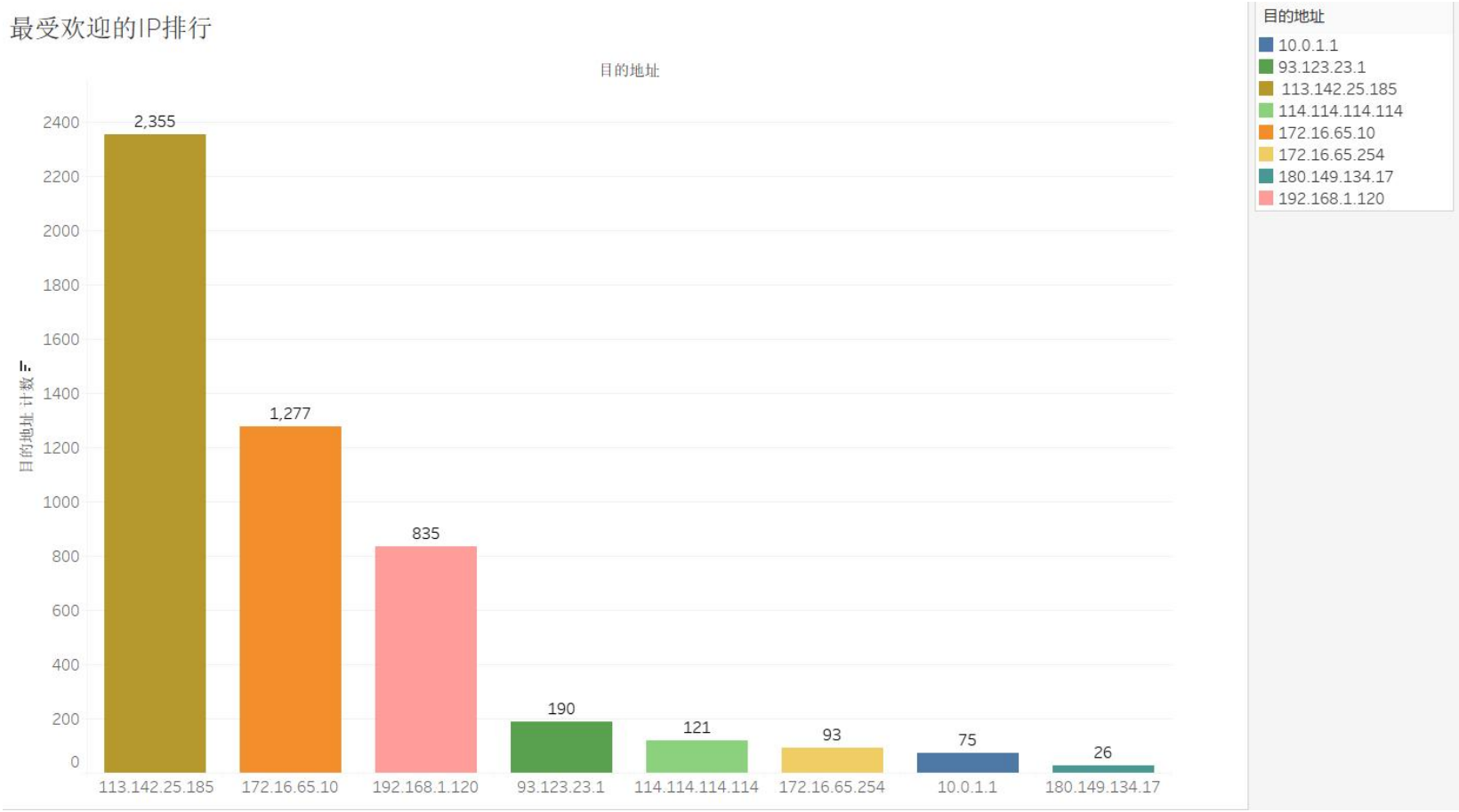
用户活跃度分析

夜间2点-3点用户活跃度



目的IP分析

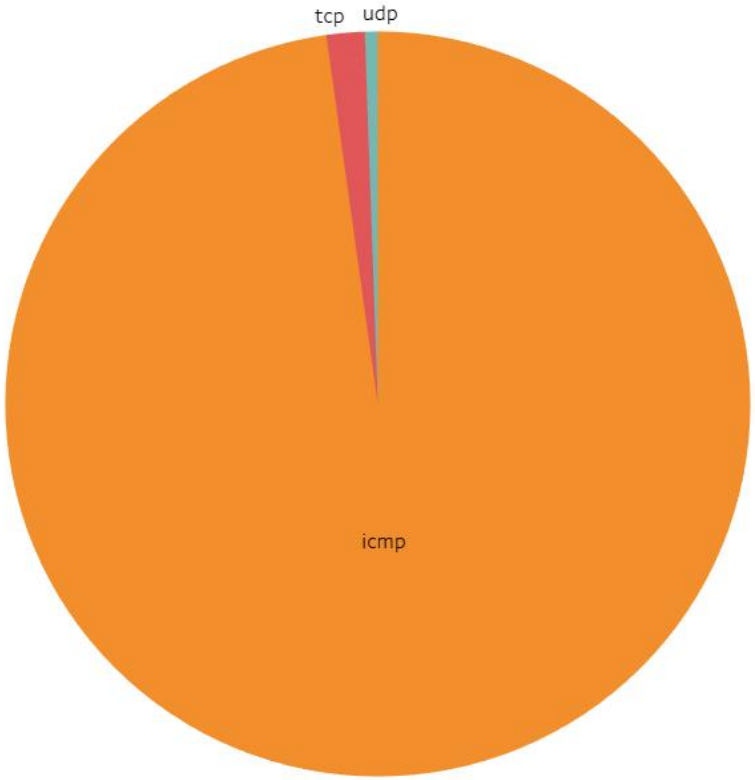
2：00-3：00

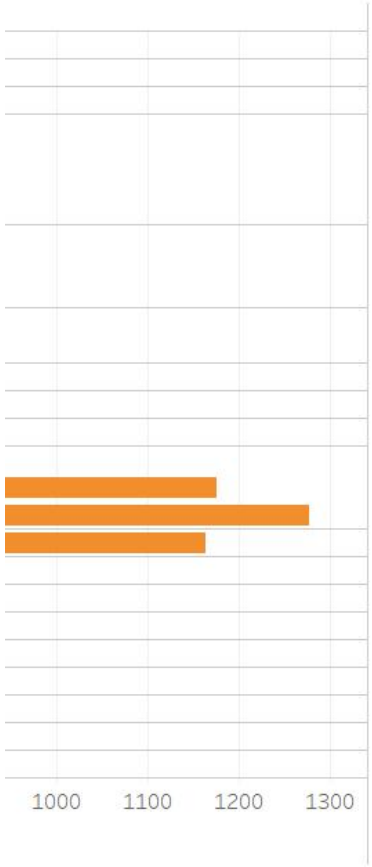


协议组分析

2：00-3：00

协议	源地址	目的
icmp	10.0.1.2	93.1
	10.0.4.5	192.
	172.16.65.10	192.
	192.5.5.1	93.1
		114.
		180.
		192.
	192.5.5.10	93.1
		113
		192.
	192.5.5.12	172.
		192.
	192.5.5.44	113
	192.5.5.90	113
	192.5.5.200	113
	192.5.9.193	10.0
		113
		172.
	192.5.10.16	113
	192.168.1.120	192.
	192.168.43.102	192.
tcp	10.0.5.253	10.0
	192.5.5.200	10.0
udp	192.5.5.126	192.
	192.5.9.254	10.1
	192.5.10.254	10.1
	192.168.43.100	192.

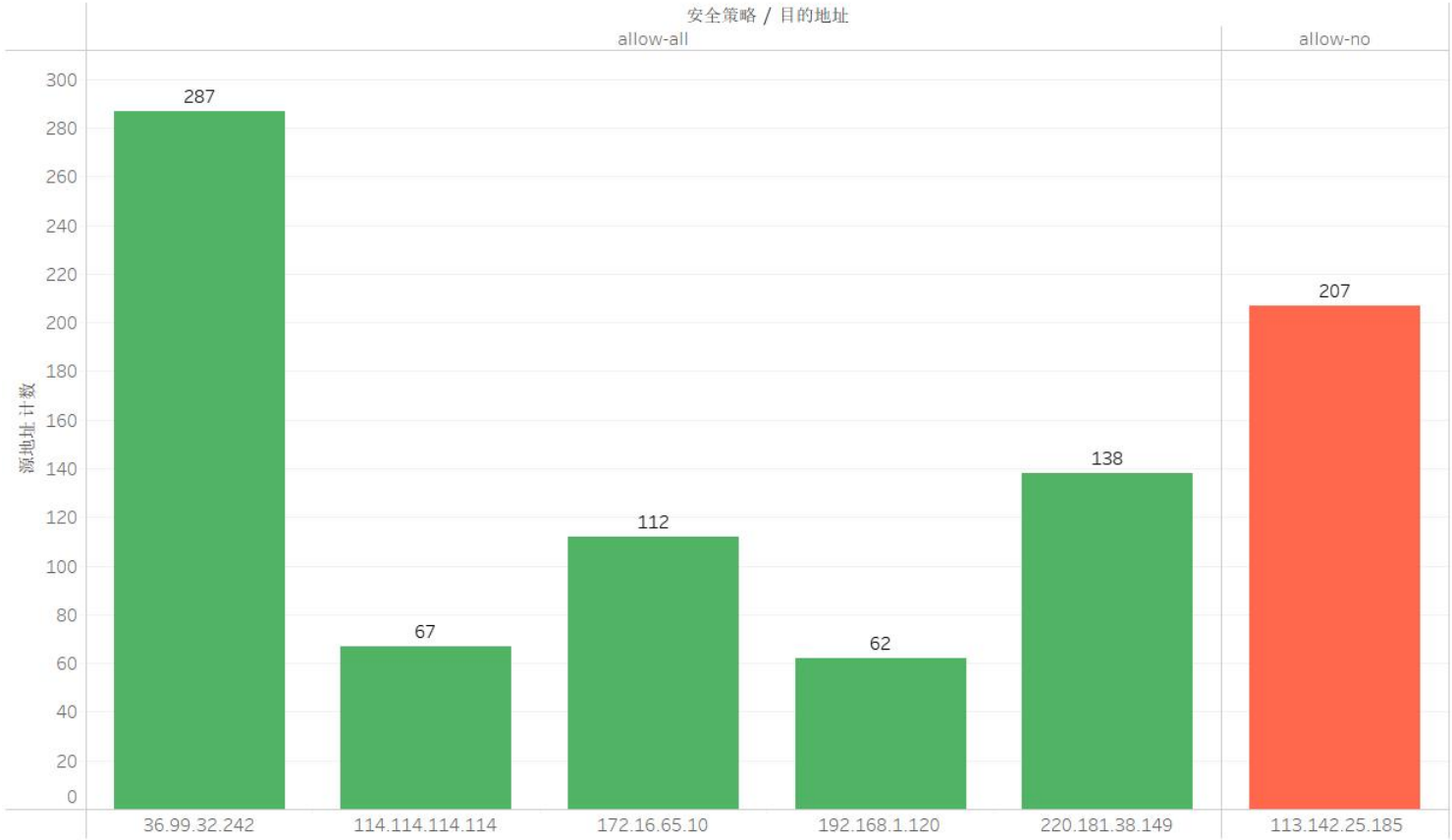




被拒绝访问的IP

16：20-15：00

安全报表



第9讲　防火墙日志分析

（完）