网络运维管理

第08讲 用户行为管理

河南中医药大学信息技术学院

《网络运维管理》课程教学组

用户行为管理

- 用户与认证
- 日志管理

用户行为管理

一、用户与认证

用户与认证

- 关于“用户”
  - 用户指的是访问网络资源的主体，表示“谁”在进行访问，是网络访问行为的重要标识。FW上的用户包括上网用户和接入用户两种形式：
  - 上网用户
    - 内部网络中访问网络资源的主体，如园区网的内部员工。上网用户可以直接通过FW访问网络资源。
  - 接入用户
    - 外部网络中访问网络资源的主体，如企业的分支机构员工和出差员工。接入用户需要先通过SSL VPN、L2TP VPN或IPSec VPN方式接入到FW，然后才能访问企业总部的网络资源。

用户与认证

- 关于“认证”

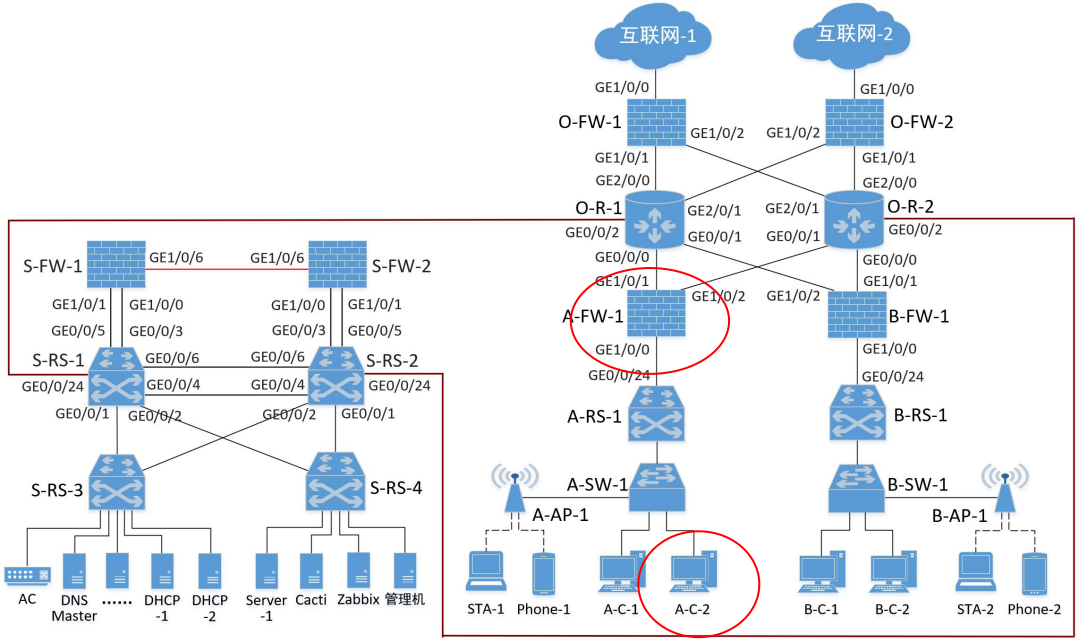
  FW通过认证来验证访问者的身份，FW对访问者进行认证的方式包括：

  - 本地认证
  - 服务器认证
  - 单点登录

用户与认证

本地认证

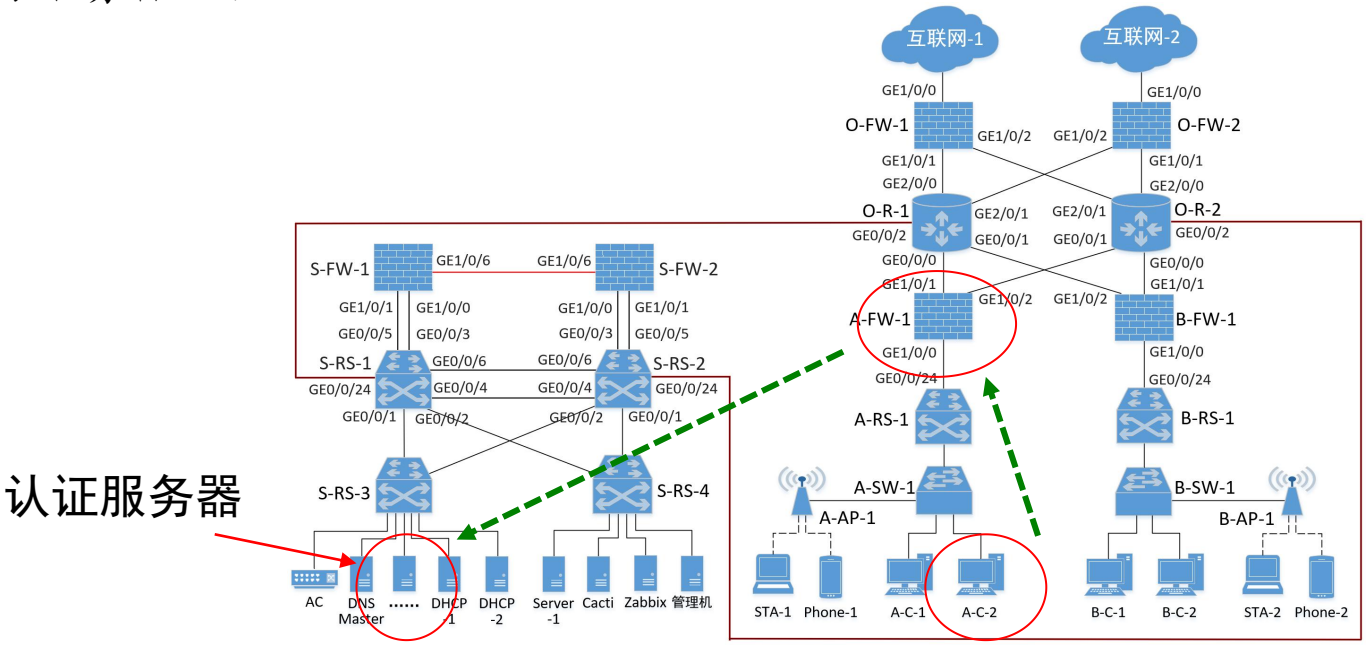
- 接入用户将标识其身份的用户名和密码发送给FW，FW上存储了密码，验证过程在FW上进行，该方式称为本地认证。



用户与认证

服务器认证

- 接入用户将标识其身份的用户名和密码发送给FW，FW上没有存储密码，FW将用户名和密码发送至第三方认证服务器，验证过程在认证服务器上进行，该方式称为服务器认证。



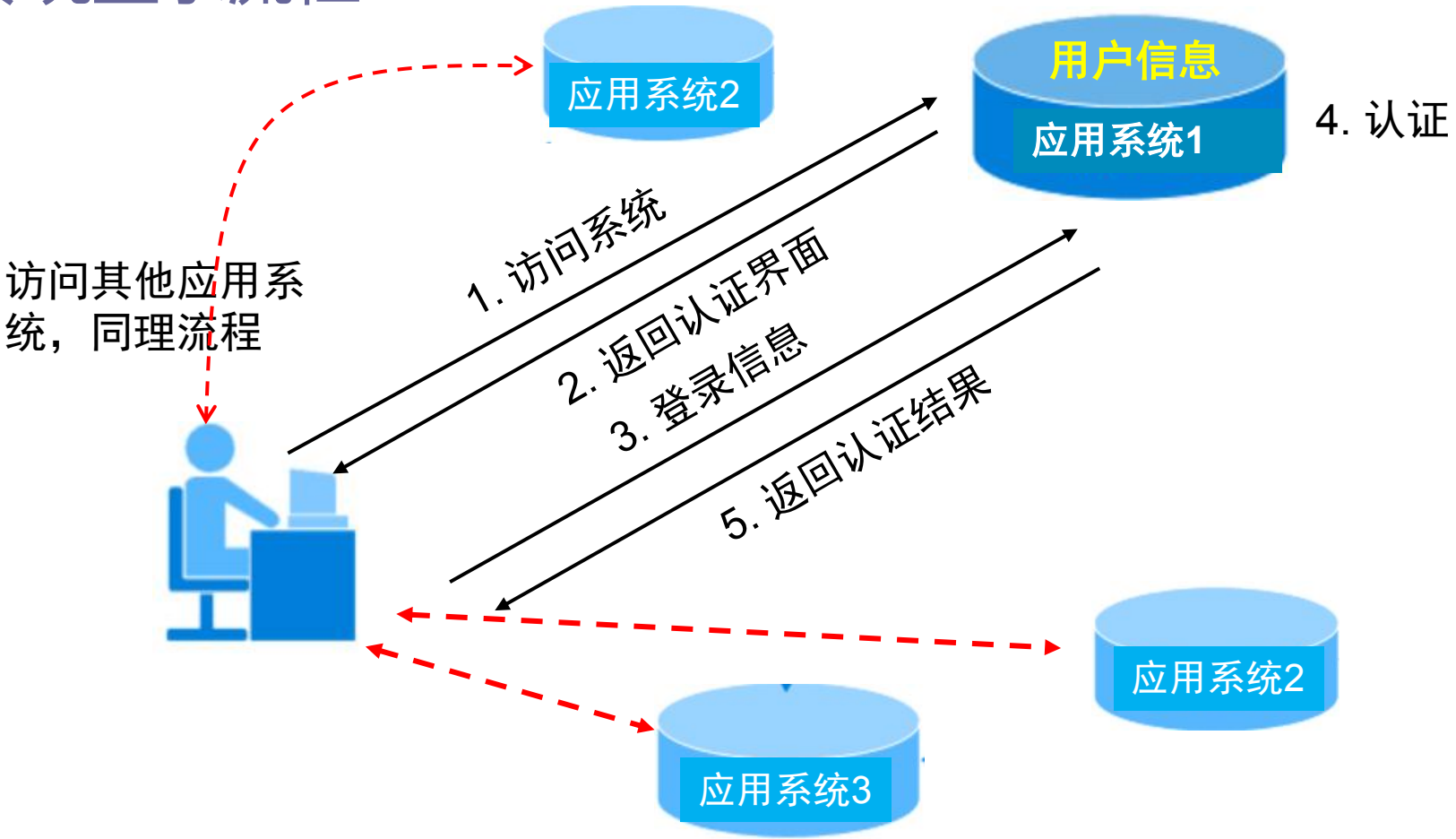
用户与认证

- 单点登录
  - 在企业内部多个应用系统（如财务、学生、教务、人事等等）的场景下，用户只需登录一次，就可访问多个系统
  - 访问者将标识其身份的用户名和密码发送给第三方认证服务器，认证通过后，第三方认证服务器将访问者的身份信息发送给FW。FW只记录访问者的身份信息不参与认证过程，该方式称为单点登录（Single Sign-On）。

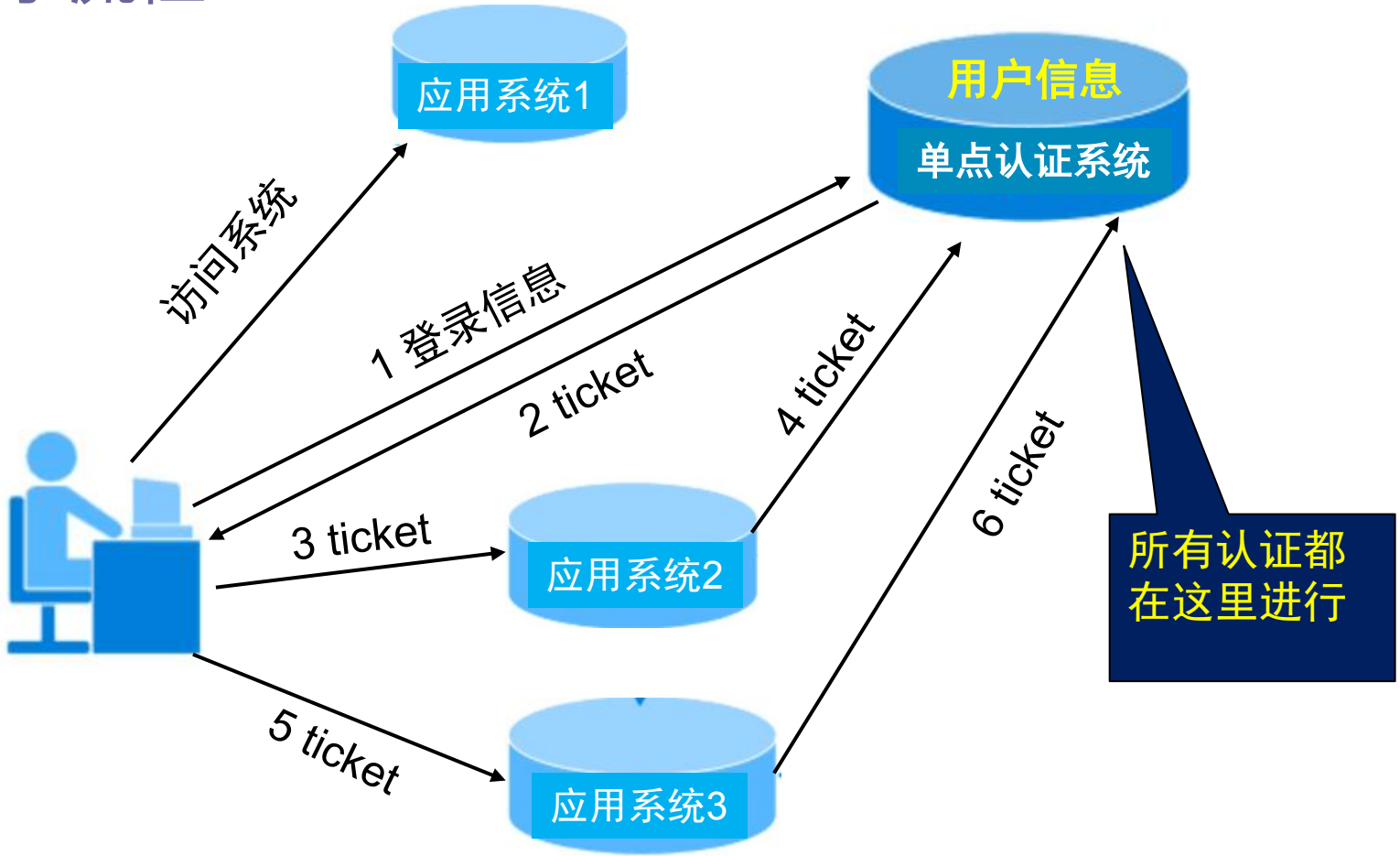
用户与认证

- 单点登录
  - 认证机制
    - 当用户第一次访问应用系统的时候，因为还没有登录，会被引导到认证系统中进行登录；
    - 根据用户提供的登录信息，认证系统进行身份校验，如果通过校验，应该返回给用户一个认证的凭据——ticket；
    - 用户再访问别的应用的时候，就会将这个ticket带上，作为自己认证的凭据，应用系统接受到请求之后会把ticket送到认证系统进行校验，检查ticket的合法性。如果通过校验，用户就可以在不用再次登录的情况下访问应用系统2和应用系统3了。
    - 图示见下页

传统登录流程


应用系统2
用户信息
应用系统1
4. 认证
访问其他应用系统，同理流程
1. 访问系统
2. 返回认证界面
3. 登录信息
5. 返回认证结果
应用系统2
应用系统3

单点登录流程


应用系统1
用户信息
单点认证系统
访问系统
1 登录信息
2 ticket
3 ticket
4 ticket
5 ticket
6 ticket
应用系统2
应用系统3
所有认证都
在这里进行

用户行为管理

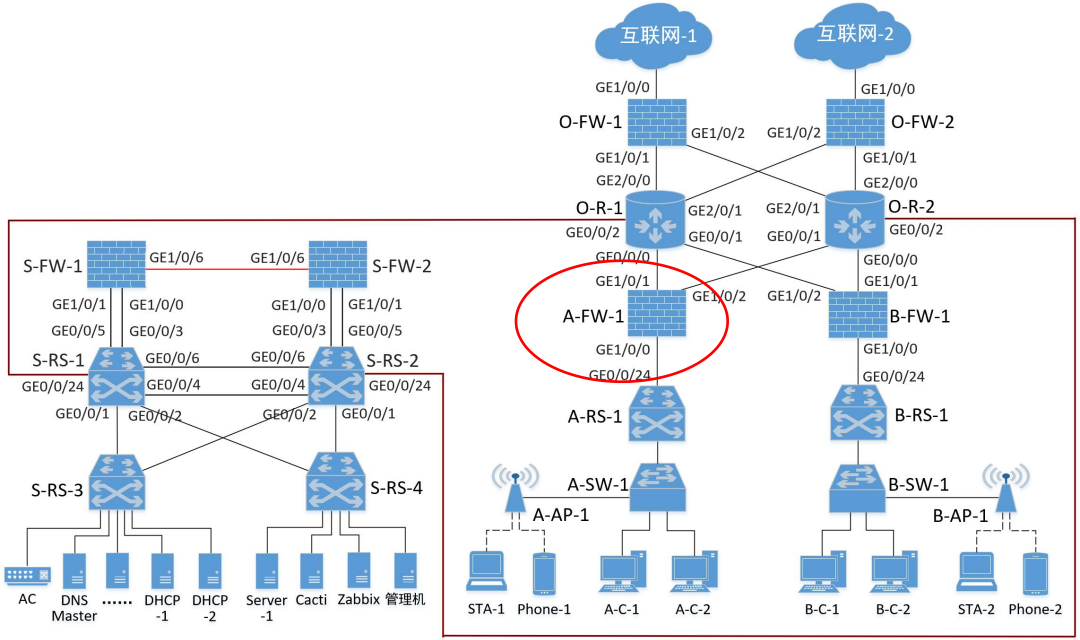
一、用户与认证

—— 本地认证

用户与认证 —— 本地认证

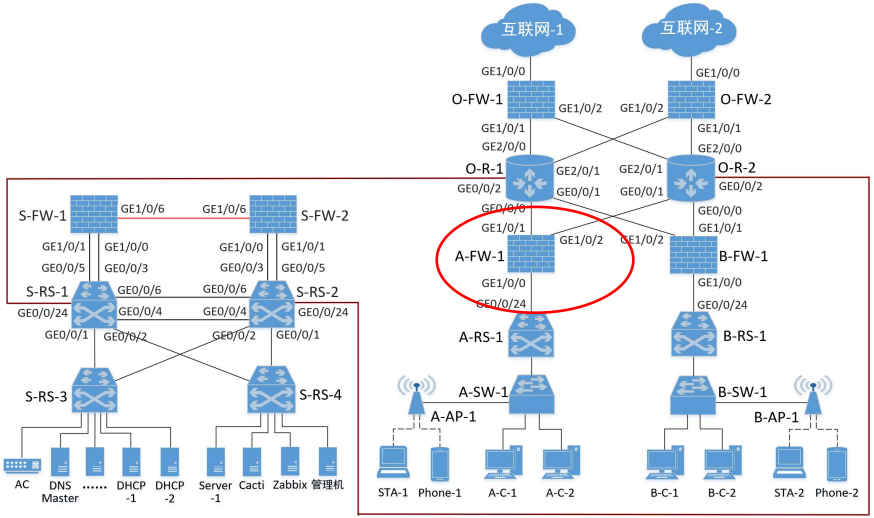
本地认证

- 管理机以Web方式登录A-FW-1
- 在防火墙上开启本地认证功能。
- 当用户区域A的用户访问网络资源时，若该访问需要通过防火墙（例如访问数据中心的Web服务器），则必须先在防火墙上进行认证，通过认证以后，才能进行后续访问。



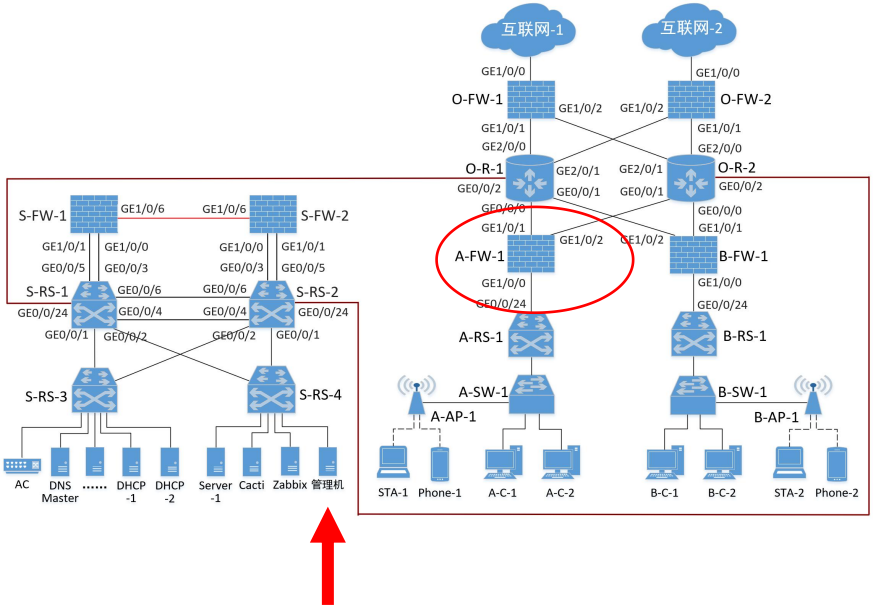
用户与认证 —— 本地认证

- 步骤1：Web登录A-FW-1防火墙
  - 要点：
    - 在防火墙上创建用于Web登录的用户和密码。
    - 通过管理机的浏览器登录防火墙。



用户与认证 —— 本地认证

- 步骤1：Web登录A-FW-1防火墙
  - 讨论1：
    - 管理机部署在哪？
    - 管理机与防火墙之间如何路由可达？
    - 实验中，管理机如何设置？（本地实体机的配置）



用户与认证 —— 本地认证

- 步骤1：Web登录A-FW-1防火墙
  - 讨论2：

```
[A-FW-1]aaa
[A-FW-1-aaa]manager-user user_web
[A-FW-1-aaa-manager-user-user_web]password
Enter Password:  （此处输入密码abcd@1234）
Confirm Password:  （再次输入密码）
[A-FW-1-aaa-manager-user-user_web]service-type web
[A-FW-1-aaa-manager-user-user_web]level 15
[A-FW-1-aaa-manager-user-user_web]quit
```

命令分析：

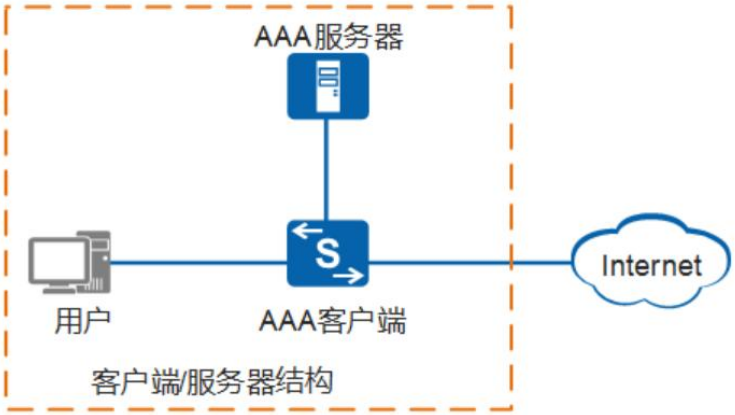
//进入AAA视图，创建用于Web登录的用户和密码（用户名user_web，密码abcd@1234）

用户与认证 —— 本地认证

- 步骤1：Web登录A-FW-1防火墙
  - 讨论3：关于AAA
  - AAA简介
    - AAA是Authentication（认证）、Authorization（授权）和Accounting（计费）的简称，提供了在NAS（Network Access Server，网络接入服务器）设备上配置访问控制的管理框架。
  - AAA作为网络安全的一种管理机制，以模块化的方式提供以下服务：
    - 认证：确认访问网络的用户的身份，判断访问者是否为合法的网络用户。
    - 授权：对不同用户赋予不同的权限，限制用户可以使用的服务。
    - 计费：记录用户使用网络服务过程中的所有操作，包括使用的服务类型、起始时间、数据流量等，用于收集和记录用户对网络资源的使用情况，并可以实现针对时间、流量的计费需求，也对网络起到监视作用。

用户与认证 —— 本地认证

- 步骤1：Web登录A-FW-1防火墙
  - 讨论3：关于AAA
  - AAA基本架构：AAA采用客户端/服务器结构，AAA客户端运行在接入设备上，通常被称为NAS（Network Access Server）设备，负责验证用户身份与管理用户接入；AAA服务器是认证服务器、授权服务器和计费服务器的统称，负责集中管理用户信息。



用户与认证 —— 本地认证

- 步骤1：Web登录A-FW-1防火墙
  - 讨论4：AAA视图
    - 华为网络设备（路由器、交换机、防火墙等）中，都设置有AAA视图模式。
    - 执行AAA命令后，用户能够从系统视图进入到AAA视图，从而进行有关用户接入方面的安全配置，例如：创建用户、设定用户级别、配置认证方案、配置授权方案、配置域等。

用户与认证 —— 本地认证

- 步骤1：Web登录A-FW-1防火墙
  - 讨论5：命令分析

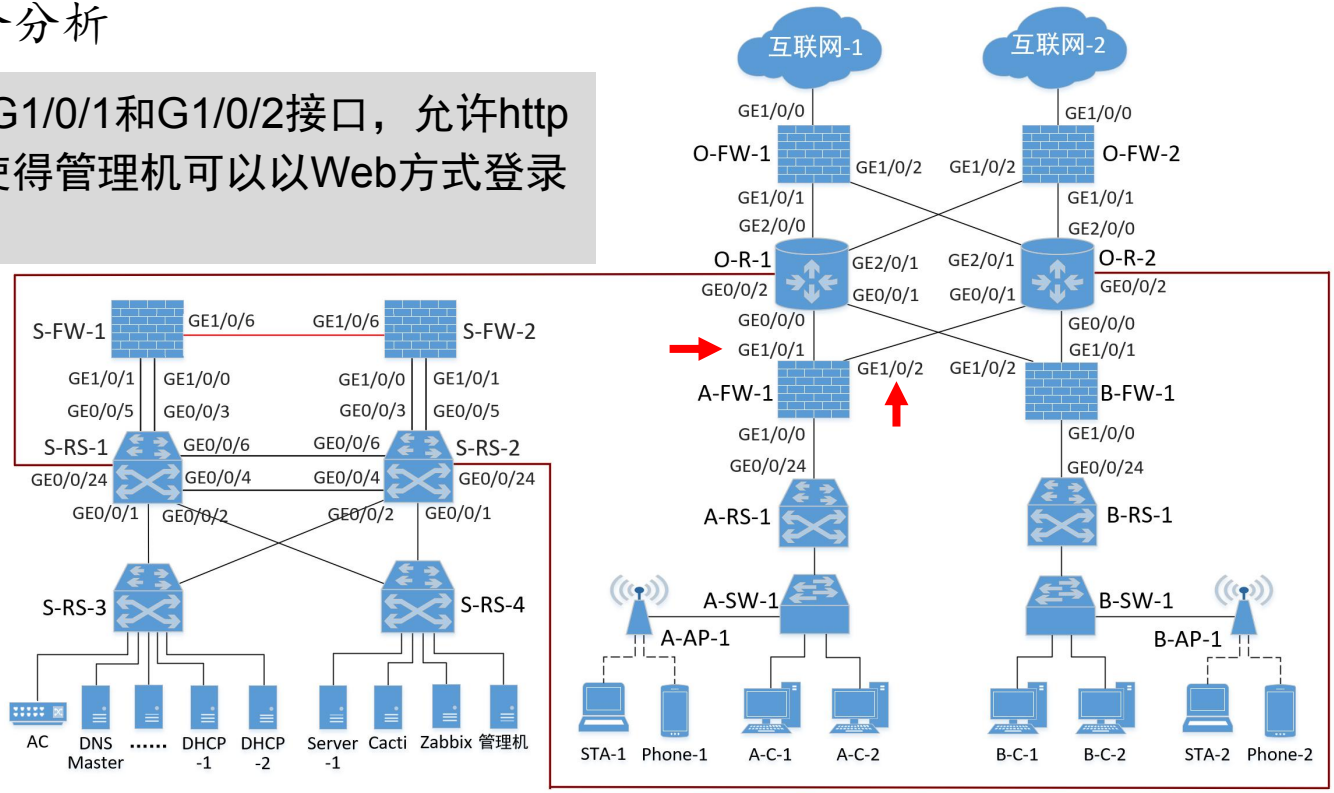
```
[A-FW-1]interface GigabitEthernet 1/0/1
[A-FW-1-GigabitEthernet1/0/1]service-manage http permit
[A-FW-1-GigabitEthernet1/0/1]service-manage https permit
[A-FW-1-GigabitEthernet1/0/1]quit
[A-FW-1]interface GigabitEthernet 1/0/2
[A-FW-1-GigabitEthernet1/0/2]service-manage http permit
[A-FW-1-GigabitEthernet1/0/2]service-manage https permit
[A-FW-1-GigabitEthernet1/0/2]quit

//为什么需要配置上述命令？
```

用户与认证 —— 本地认证

- 步骤1：Web登录A-FW-1防火墙
  - 讨论5：命令分析

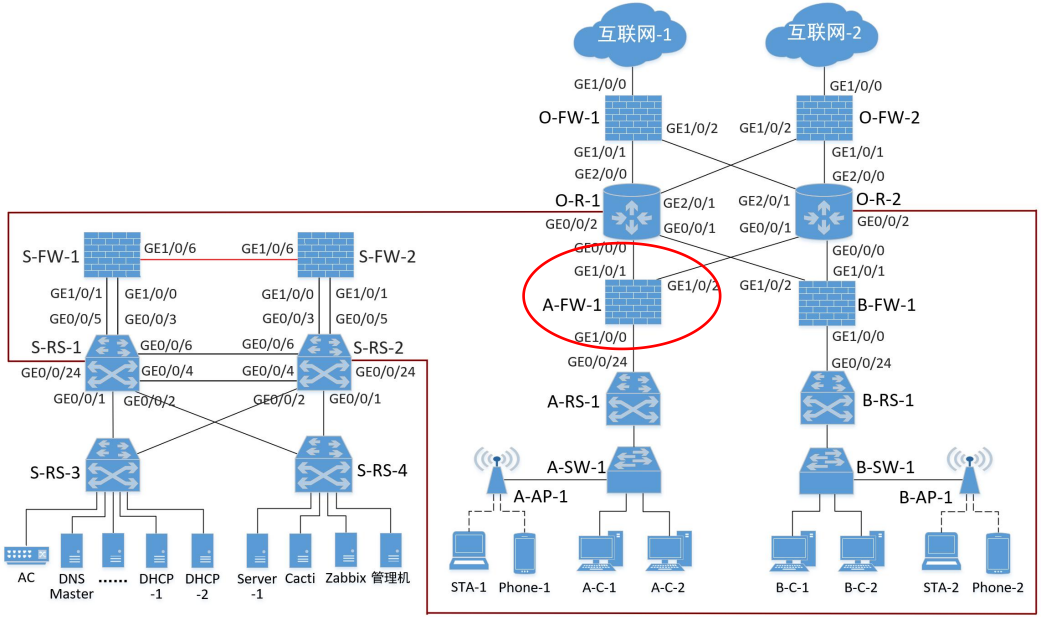
//配置防火墙的G1/0/1和G1/0/2接口，允许http和https操作，使得管理机可以以Web方式登录防火墙

思考：防火墙的默认状况？



用户与认证 —— 本地认证

- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 要点：
    - 设置认证方式
    - 添加用户组和认证用户。



用户与认证 —— 本地认证

- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 讨论1：选择认证方式（选择“本地”）

防火墙开启了认证功能后，当用户区域主机想访问外部网络资源时，必须先登录防火墙的认证界面，输入相应的用户名和密码，通过认证后，才能正常访问外部网络资源。

用户与认证 —— 本地认证

- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 讨论2：认识NAC
  - NAC（Network Access Control）称为网络接入控制，通过对接入网络的客户端和用户的认证保证网络的安全。
  - **三种认证方式比较**
    - NAC包括三种认证方式：802.1X认证、MAC认证和Portal认证。由于三种认证方式认证原理不同，各自适合的场景也有所差异，实际应用中，可以根据场景部署某一种合适的认证方式，也可以部署几种认证方式组成的混合认证，混合认证的组合方式以设备实际支持为准。

用户与认证 —— 本地认证

- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 讨论2：认识NAC

表1　NAC的三种认证方式比较

对比项	802.1X认证	MAC认证	Portal认证
适合场景	新建网络、用户集中、信息安全要求严格的场景	打印机、传真机等哑终端接入认证的场景	用户分散、用户流动性大的场景
客户端需求	需要	不需要	不需要
优点	安全性高	无需安装客户端	部署灵活
缺点	部署不灵活	需登记MAC地址，管理复杂	安全性不高

用户与认证 —— 本地认证

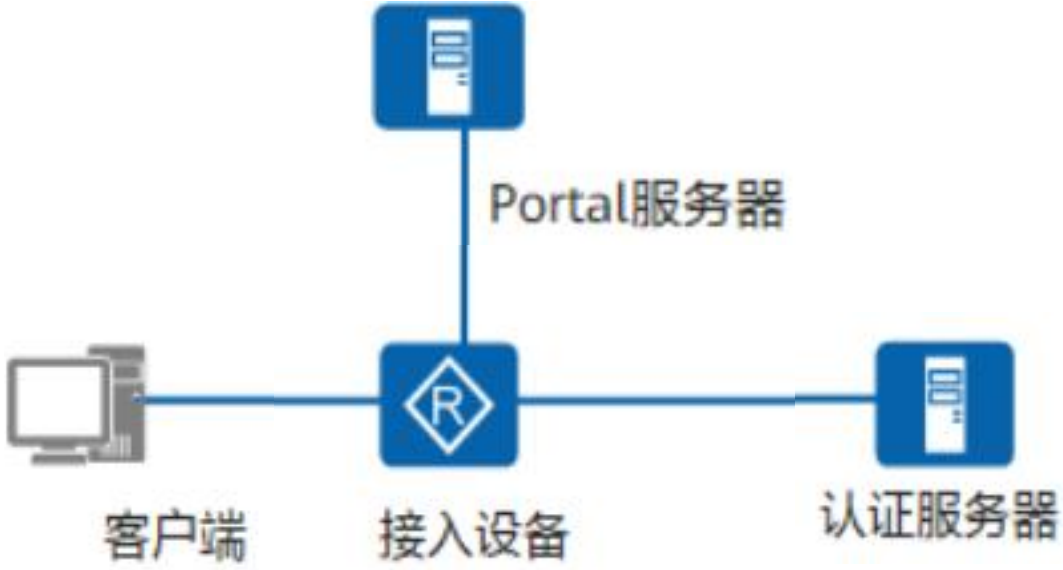
- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 讨论2：认识NAC
  - NAC与AAA
    - NAC与AAA互相配合，共同完成接入认证功能。
    - NAC：用于用户和接入设备之间的交互。NAC负责控制用户的接入方式，即用户采用802.1X，MAC或Portal中的哪一种方式接入，接入过程中的各类参数和定时器。确保合法用户和接入设备建立安全稳定的连接。
    - AAA：用于接入设备与认证服务器之间的交互。AAA服务器通过对接入用户进行认证、授权和计费实现对接入用户访问权限的控制。

用户与认证 —— 本地认证

- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 讨论3：认识Portal认证系统
    - Portal认证通常也称为Web认证，一般将Portal认证网站称为门户网站。用户上网时，必须在门户网站进行认证，如果未认证成功，仅可以访问特定的网络资源，认证成功后，才可以访问其他网络资源。
  - 优点
    - 一般情况下，客户端不需要安装额外的软件，直接在Web页面上认证，简单方便。
    - 部署位置灵活，可以在接入层或关键数据的入口作访问控制。
    - 用户管理灵活，可基于用户名与VLAN/IP地址/MAC地址的组合对用户进行认证。

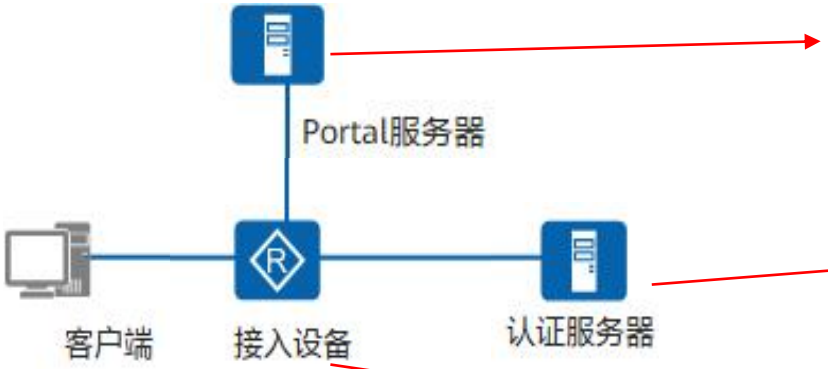
用户与认证 —— 本地认证

- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 讨论3：认识Portal认证系统
  - Portal认证系统主要包括四个基本要素：
    - 客户端
    - 接入设备
    - Portal服务器
    - 认证服务器



用户与认证 —— 本地认证

- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 讨论3：认识Portal认证系统



Portal服务器：接收客户端认证请求的服务器系统，提供免费门户服务和认证界面，与接入设备交互客户端的认证信息

认证服务器：与接入设备进行交互，完成对用户的认证、授权与计费。

接入设备：交换机、路由器等接入设备的统称，主要有三方面的作用：

① 在认证之前，将认证网段内用户的所有HTTP/HTTPS请求都重定向到Portal服务器。

② 在认证过程中，与Portal服务器、认证服务器交互，完成对用户身份认证、授权等功能。

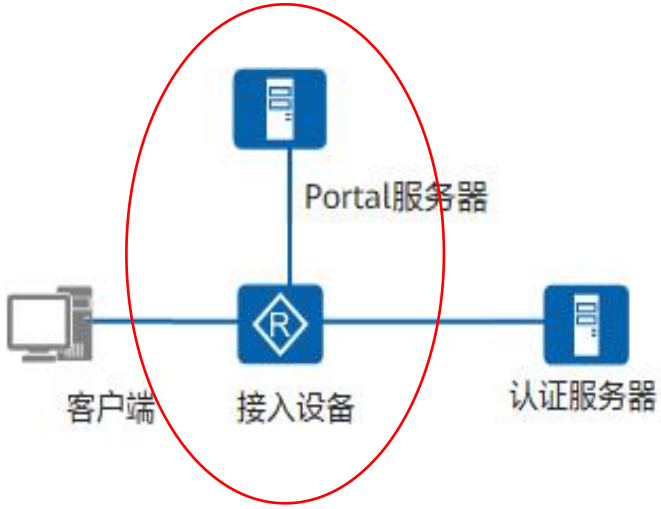
③ 在认证通过后，允许用户访问被管理员授权的网络资源。

用户与认证 —— 本地认证

- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 讨论3：认识Portal认证系统

说明：

- Portal服务器可以是接入设备之外的独立实体（外置Portal服务器），也可以是存在于接入设备之内的内嵌实体（内置Portal服务器）。



用户与认证 —— 本地认证

- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 讨论4：Portal认证方式
  - 按照网络中实施Portal认证的网络层次来分，Portal认证方式分为两种：二层认证方式和三层认证方式。
    - **二层认证方式：**当客户端与接入设备之间为二层网络时，即客户端与接入设备直连（或之间只有二层设备存在），接入设备可以学习到客户端的MAC地址，则接入设备可以利用IP地址和MAC地址来识别用户，此时可配置Portal认证为二层认证方式。
    - 二层认证流程简单，安全性高，但由于限制了用户只能与接入设备处于同一网段，所以组网灵活性不高。

用户与认证 —— 本地认证

- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 讨论4：Portal认证方式
  - 按照网络中实施Portal认证的网络层次来分，Portal认证方式分为两种：二层认证方式和三层认证方式。
    - **三层认证方式：**当客户端与接入设备之间包含三层网络时，即客户端与接入设备之间存在三层转发设备，接入设备不能获取到认证客户端的MAC地址，只能以IP地址作为用户的唯一标识，此时需要将Portal认证配置为三层认证方式。
    - 三层认证组网灵活，容易实现远程控制，但由于只能以IP地址作为用户的唯一标识，所以安全性不高

用户与认证 —— 本地认证

- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 讨论5：Portal认证触发方式

认证的第一件事情就是发起认证，有两种认证触发方式：

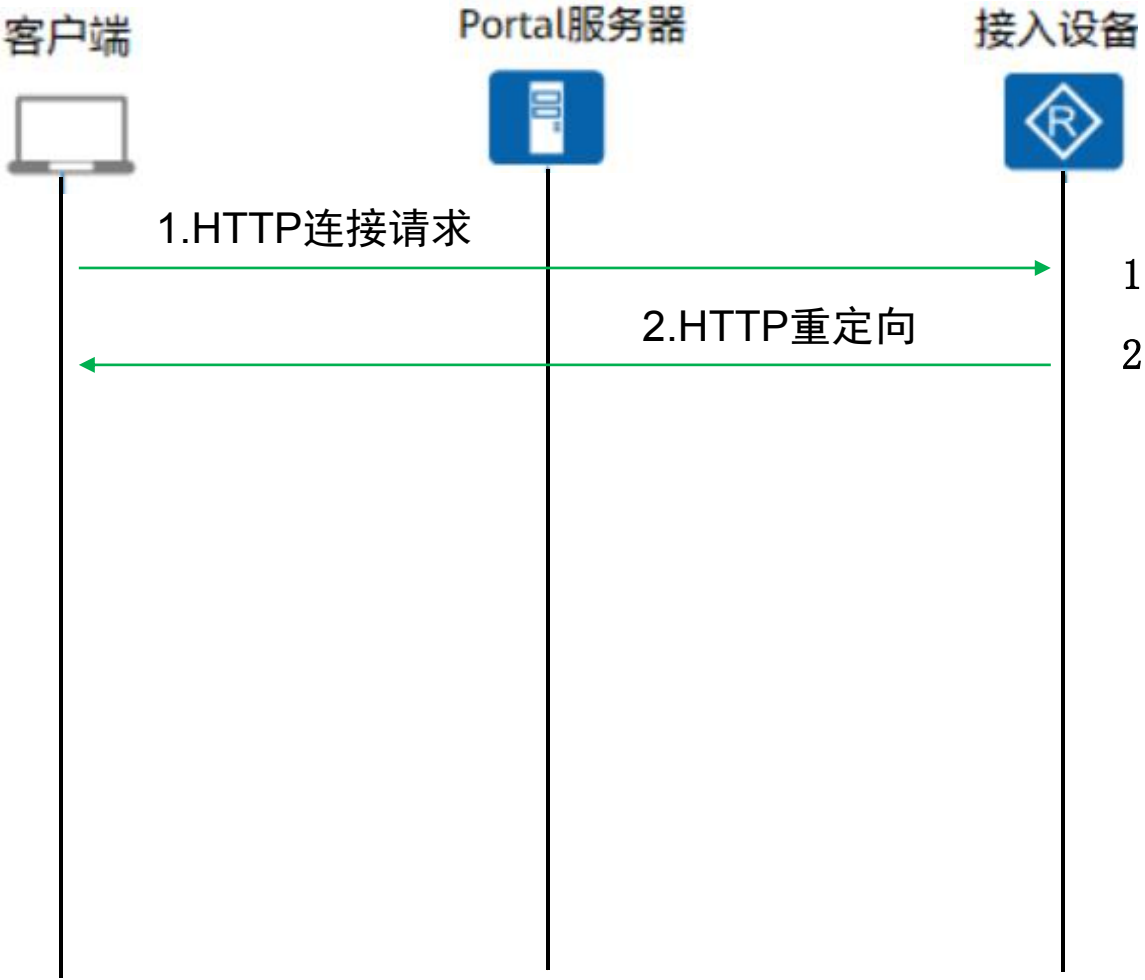
- 主动认证
  - 用户通过浏览器主动访问Portal认证网站时，即在浏览器中直接输入Portal服务器的网络地址，然后在显示的网页中输入用户名和密码进行认证，这种开始Portal认证过程的方式即为主动认证，即由用户自己主动访问Portal服务器发起的身份认证。
- 重定向认证
  - 用户输入的访问地址不是Portal认证网站地址时，将被强制访问Portal认证网站（通常称为重定向），从而开始Portal认证过程，这种方式称作重定向认证

用户与认证 —— 本地认证

- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 讨论6：Portal认证流程

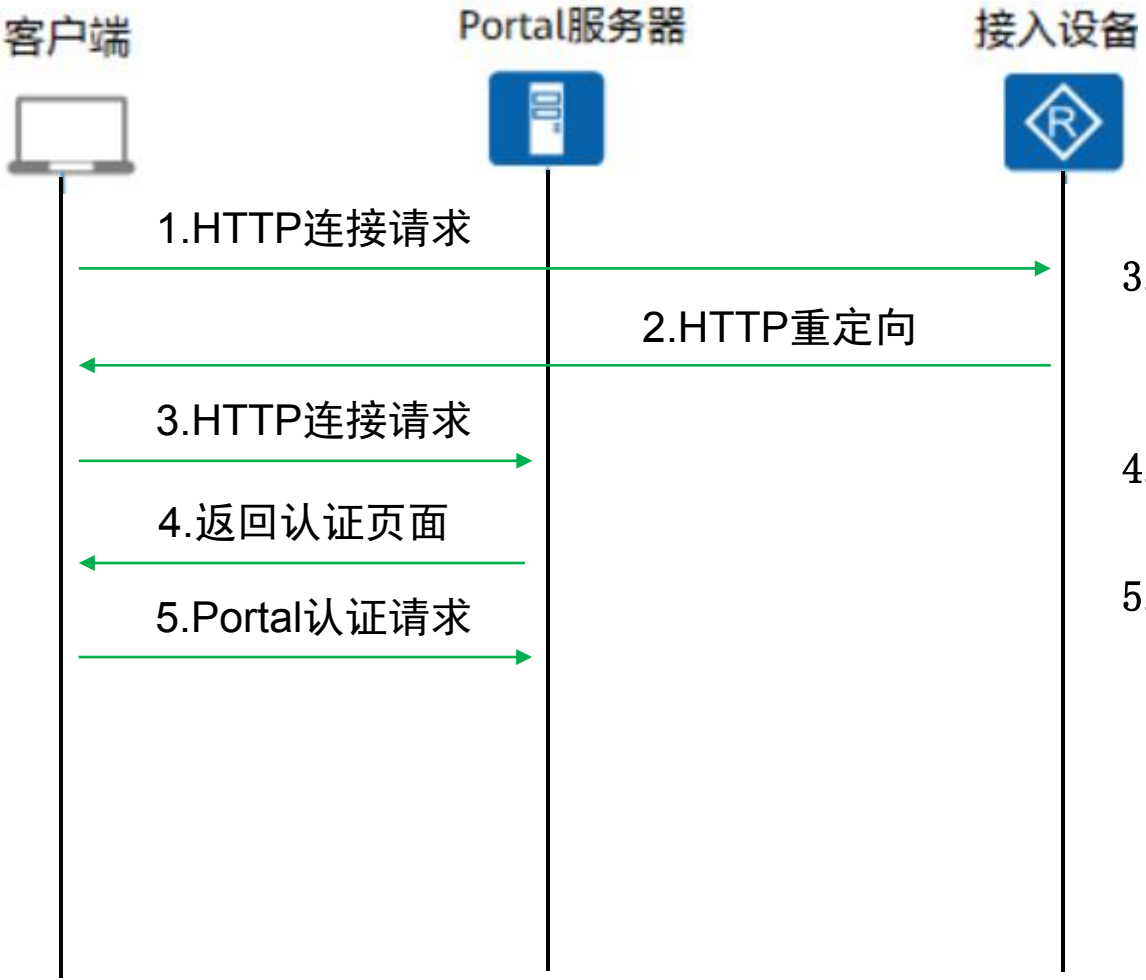
内置Portal服务器的认证流程，与外置Portal服务器的认证流程类似：

  - 见下图



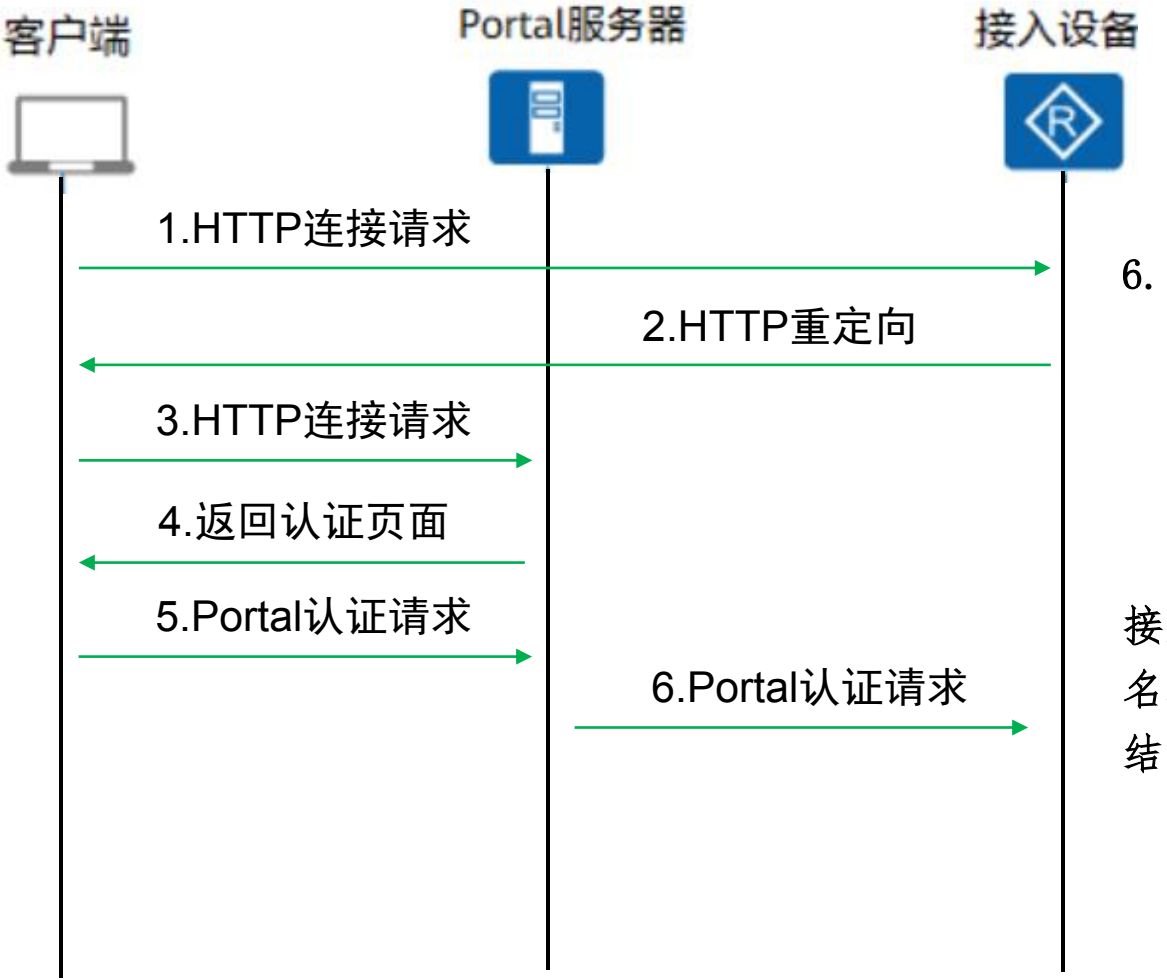
Portal认证流程

1. 客户端发起HTTP连接请求。
2. 接入设备收到HTTP连接请求报文时，如果是访问Portal服务器或免认证网络资源的HTTP报文，则接入设备允许其通过；如果是访问其它地址的HTTP报文，则接入设备将其URL地址重定向到Portal认证页面。



Portal认证流程

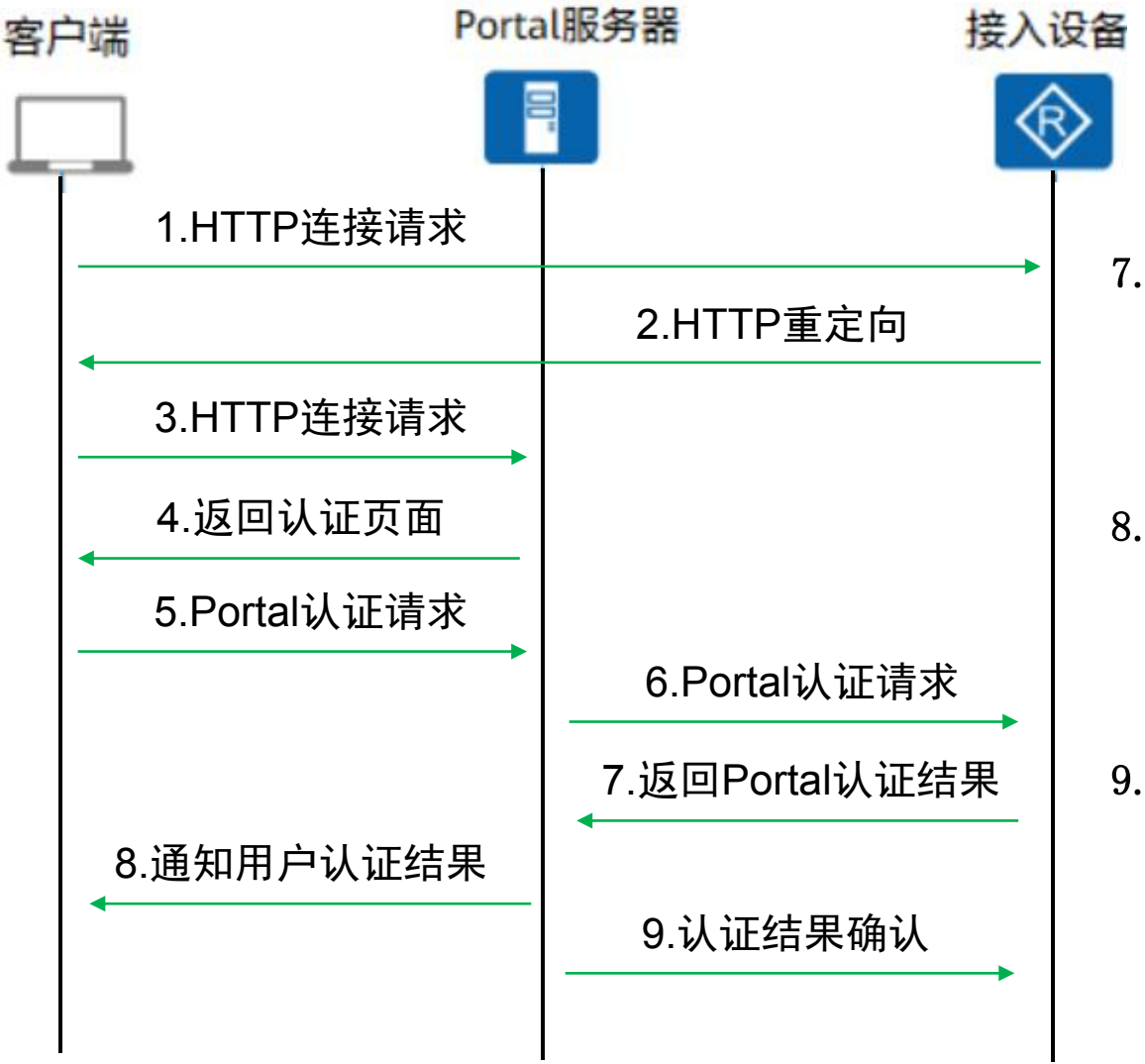
3. 客户端根据获得的URL地址向Portal服务器发起HTTP连接请求。
4. Portal服务器向客户端返回Portal认证页面。
5. 用户在Portal认证页面输入用户名和密码后，客户端向Portal服务器发起Portal认证请求。



Portal认证流程

6. Portal服务器将用户输入的用户名和密码封装在Portal认证请求报文（REQ_AUTH）中，并发送给接入设备。

接入设备（本地认证）对用户名和密码进行认证。根据认证结果接入/拒绝用户。



Portal认证流程

7. 接入设备向Portal服务器返回Portal认证结果（ACK_AUTH），并将用户加入自身在线用户列表。
8. Portal服务器向客户端发送认证结果报文，通知客户端认证成功，并将用户加入自身在线用户列表。
9. Portal服务器向接入设备发送认证应答确认(AFF_ACK_AUTH)

用户与认证 —— 本地认证

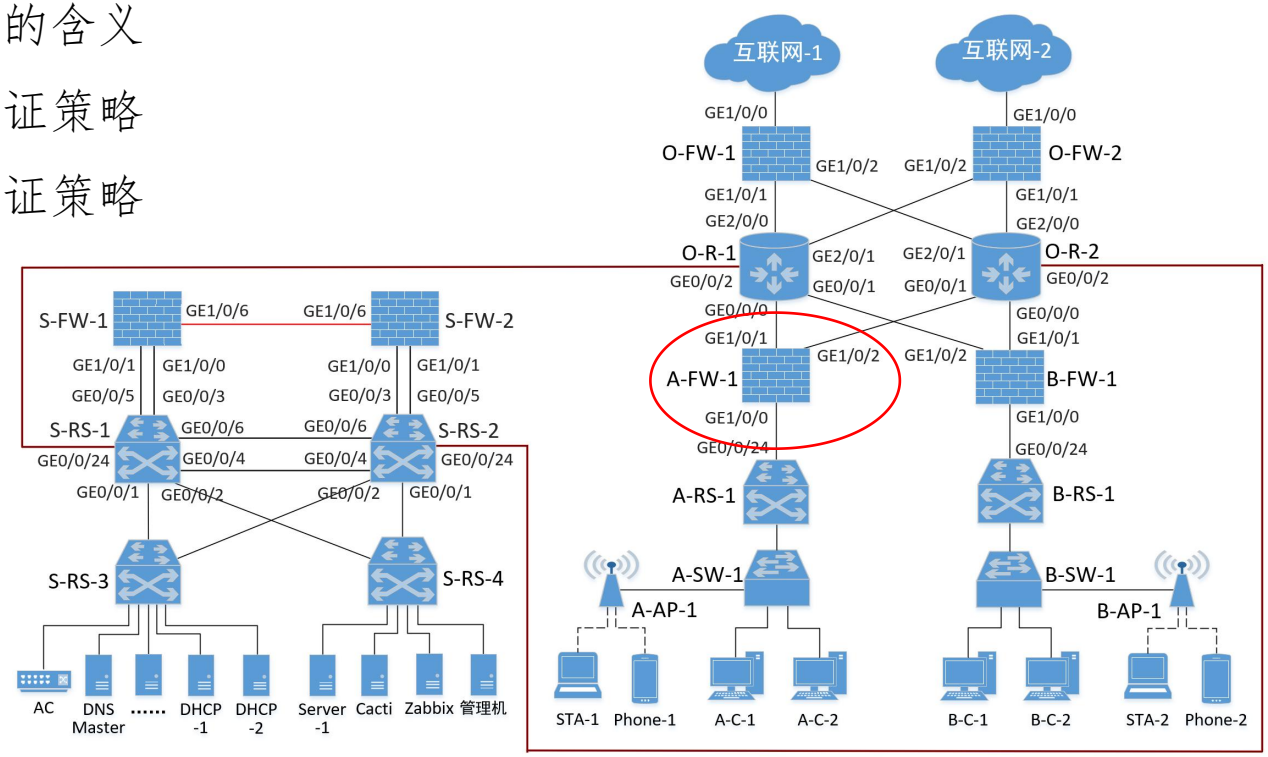
- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 讨论7：添加用户组和认证用户
    - 此处创建的用户，是供上网用户进行身份认证时使用的。步骤1中创建的用户是供管理员以Web方式登录防火墙使用的，两者不要搞混了

用户与认证 —— 本地认证

- 步骤2：设置防火墙A-FW-1的认证方式并添加认证用户
  - 讨论7：添加用户组和认证用户

用户与认证 —— 本地认证

- 步骤3：在防火墙A-FW-1上添加认证策略
  - 要点：
    - 理解认证策略的含义
    - 了解默认的认证策略
    - 添加所需的认证策略



用户与认证 —— 本地认证

- 步骤3：在防火墙A-FW-1上添加认证策略
  - 讨论1：什么是认证策略？
    - 认证策略用于决定FW需要对哪些数据流进行认证，匹配认证策略的数据流必须经过FW的身份认证才能通过

用户与认证 —— 本地认证

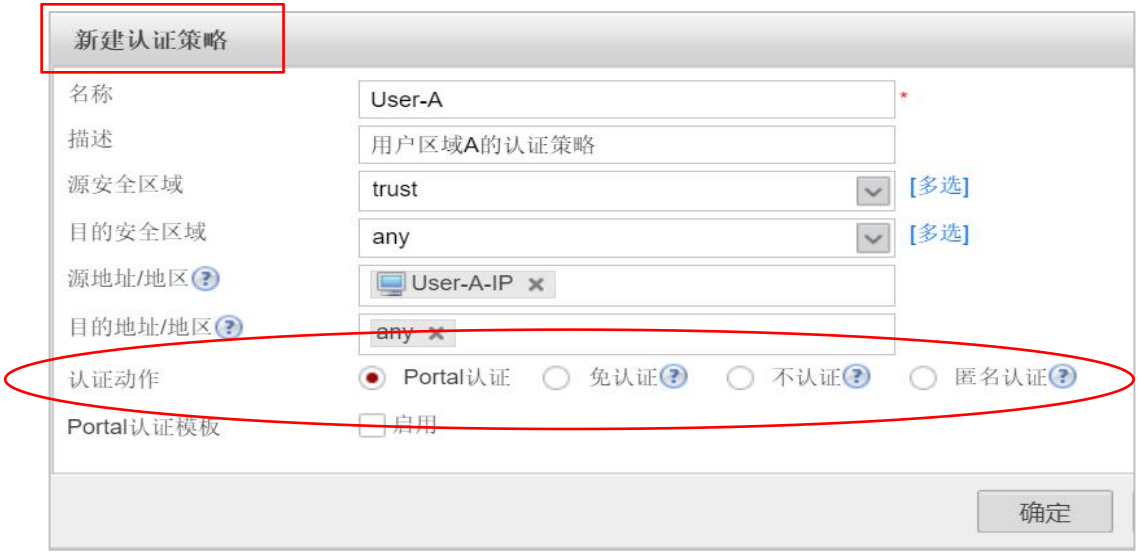
- 步骤3：在防火墙A-FW-1上添加认证策略
  - 讨论2：哪些数据流可以不认证？
    - DHCP数据流？
      - 默认情况下，华为防火墙开启认证后，某些协议报文不受认证的影响。例如用户区域中的主机不用通过认证，其发出的DHCP报文就可以通过防火墙到达数据中心的DHCP服务器，从而获取到IP地址，读者可自行验证；
    - AC与AP间的管理数据？
      - 通过AC（无线控制器）来管理和配置AP。无线接入点控制与规范（Control And Provisioning of Wireless Access Points，简称CAPWAP），是实现AP和AC之间互通的一个通用封装和传输机制，用来传送AC与AP之间的管理报文（数据）。所以必须保证AC和AP之间能正常通信CAPWAP报文。

用户与认证 —— 本地认证

- 步骤3：在防火墙A-FW-1上添加认证策略
  - 讨论3：认证策略的组成？
    - 认证策略是多个认证策略规则的集合，认证策略决定是否对一条流量进行认证。认证策略规则由条件和动作组成；
    - 条件指的是FW匹配报文的依据，包括：
      - 源安全区域
      - 目的安全区域
      - 源地址/地区
      - 目的地址/地区

用户与认证 —— 本地认证

- 步骤3：在防火墙A-FW-1上添加认证策略
  - 讨论3：认证策略的组成？
    - 认证策略规则动作指的是FW对匹配到的数据流采取的处理方式，包括：
      - Portal认证
      - 免认证
      - 不认证
      - 匿名认证



用户与认证 —— 本地认证

- 步骤3：在防火墙A-FW-1上添加认证策略
  - 讨论3：认证策略的组成？【动作】
    - 免认证：对符合条件的数据流进行免认证，FW通过其他手段识别用户身份。主要应用于以下情况：
      - 对于企业的高级管理者来说，一方面他们希望省略认证过程；另一方面，他们可以访问机密数据，对安全要求又更加严格。为此，管理员可将这类用户与IP/MAC地址双向绑定，对这类数据流进行免认证，但是要求其只能使用指定的IP或者MAC地址访问网络资源。FW通过用户与IP/MAC地址的绑定关系来识别该数据流所属的用户。
      - 在RADIUS单点登录的场景中，FW已经从其他认证系统中获取到用户信息，对单点登录用户的业务流量进行免认证。
      - 如果需要对VPN接入用户配置基于用户的策略，必须为VPN解封装后的私网地址配置认证策略。 此时需要配置动作为免认证的认证策略。

用户与认证 —— 本地认证

- 步骤3：在防火墙A-FW-1上添加认证策略
  - 讨论3：认证策略的组成？【动作】
    - 不认证：对符合条件的数据流不进行认证，主要应用于不需要经过FW认证的数据流，例如内网之间互访的数据流。

用户与认证 —— 本地认证

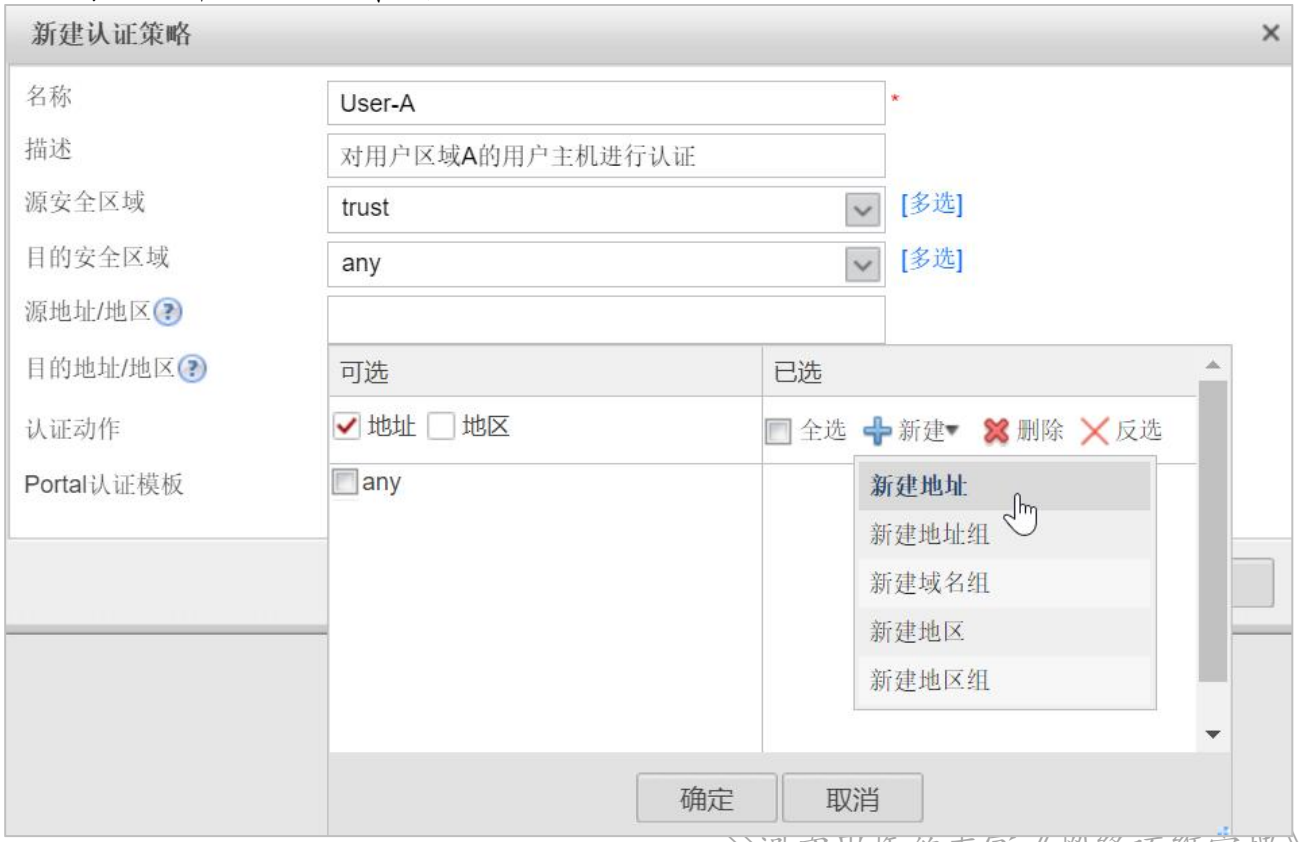
- 步骤3：在防火墙A-FW-1上添加认证策略
  - 讨论4：认证策略的匹配顺序？
    - FW匹配报文时总是在多条认证策略规则之间进行，从上往下进行匹配。当数据流的属性和某条规则的所有条件匹配时，认为匹配该条规则成功，就不会再匹配后续的规则。如果所有规则都没有匹配到，则按照缺省认证策略进行处理。
    - FW上存在一条缺省的认证策略，所有匹配条件均为任意（any），动作为不认证。

用户与认证 —— 本地认证

- 步骤3：在防火墙A-FW-1上添加认证策略
  - 讨论5：添加新的认证策略
    - 此处保持default认证策略不变，在A-FW-1上添加一条新的认证策略：仅对源地址属于192.168.64.0/22（用户区域A中主机的IP地址段，含无线终端用户）的通信进行认证。
    - 这样，A-AP-1（IP地址属于10.0.200.0/28地址段）发出的报文就不需要通过防火墙的认证了。

用户与认证 —— 本地认证

- 步骤3：在防火墙A-FW-1上添加认证策略
  - 讨论5：添加新的认证策略

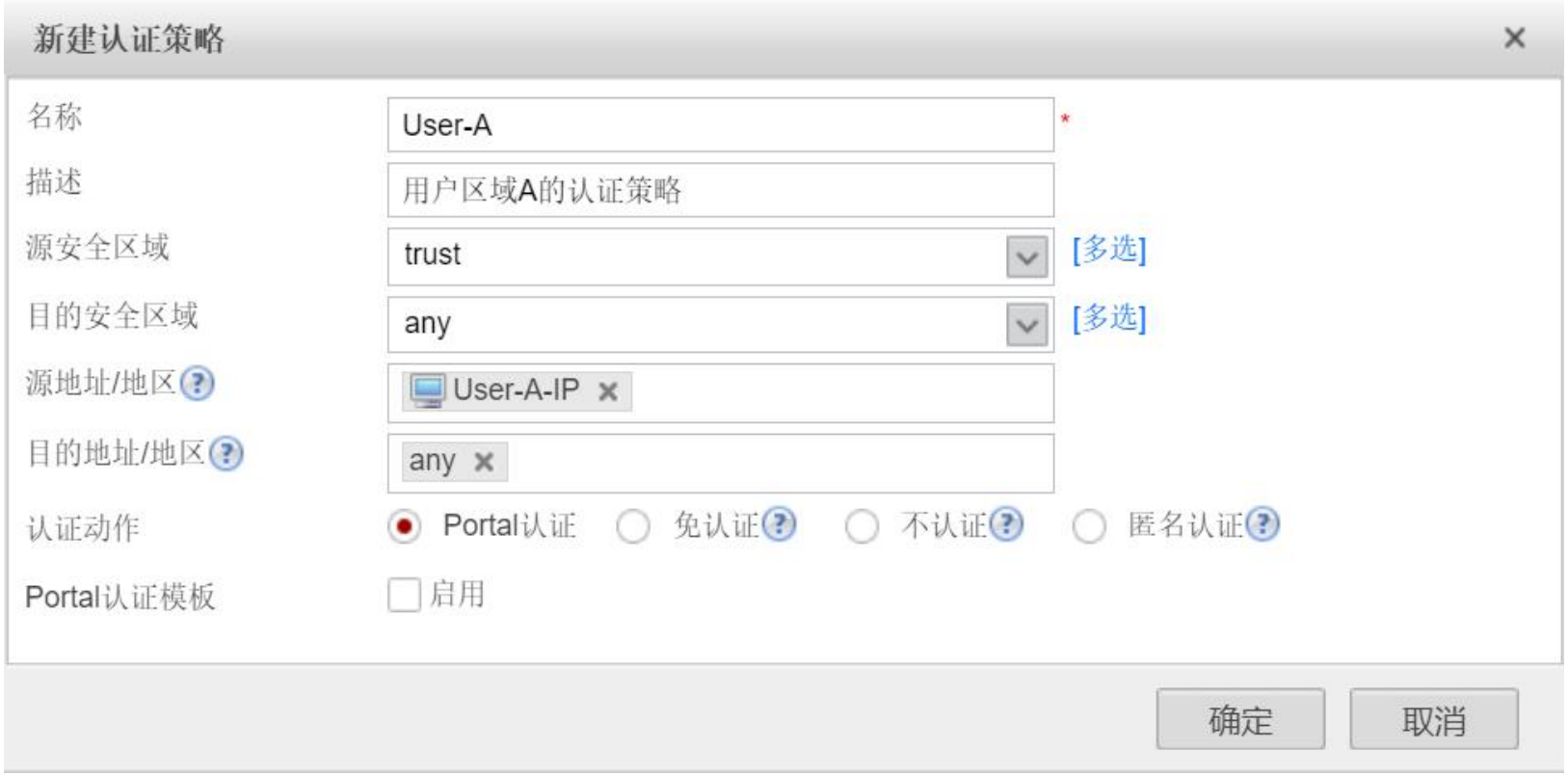


用户与认证 —— 本地认证

- 步骤3：在防火墙A-FW-1上添加认证策略
  - 讨论5：添加新的认证策略

用户与认证 —— 本地认证

- 步骤3：在防火墙A-FW-1上添加认证策略
  - 讨论5：添加新的认证策略

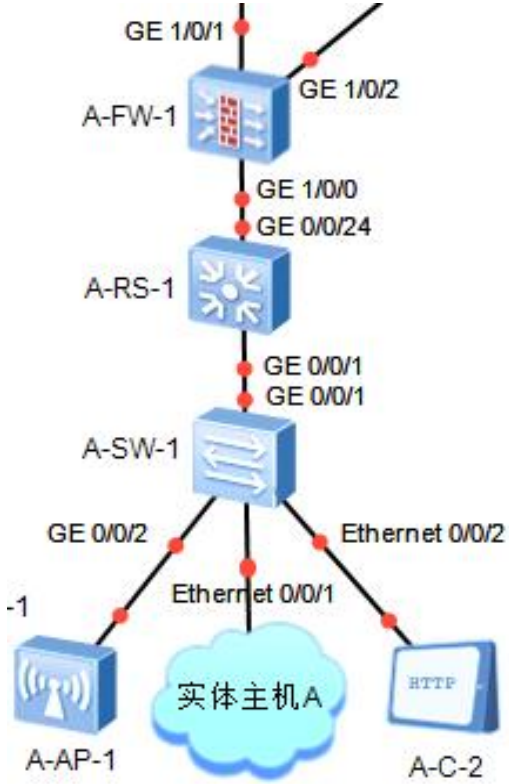


用户与认证 —— 本地认证

- 步骤3：在防火墙A-FW-1上添加认证策略
  - 讨论5：添加新的认证策略

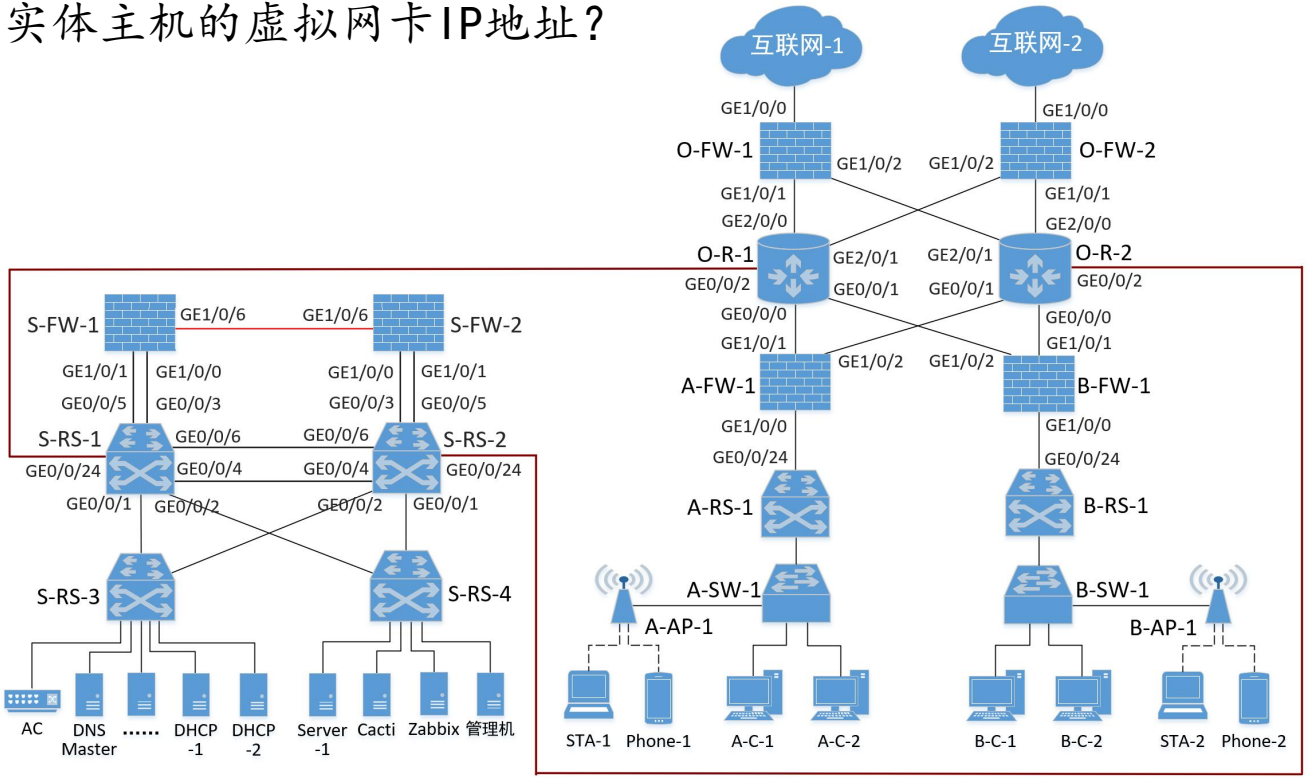
用户与认证 —— 本地认证

- 步骤4：设置本地实体机为用户区域A的主机并能够Web登录A-FW-1
  - 用户区域主机在进行认证时，需要通过浏览器以Web方式登录防火墙的认证界面，并且输入用户名和密码，eNSP中的仿真终端没有浏览器，无法实现这一功能。
  - 所以，需要在园区网的用户区域中接入一台虚拟机（例如在VirtualBox中创建一台Windows虚拟机并接入eNSP），或者直接将本地实体机通过虚拟网卡接入eNSP中的用户区域网络，然后利用浏览器Web登录A-FW-1，从而进行认证操作。



用户与认证 —— 本地认证

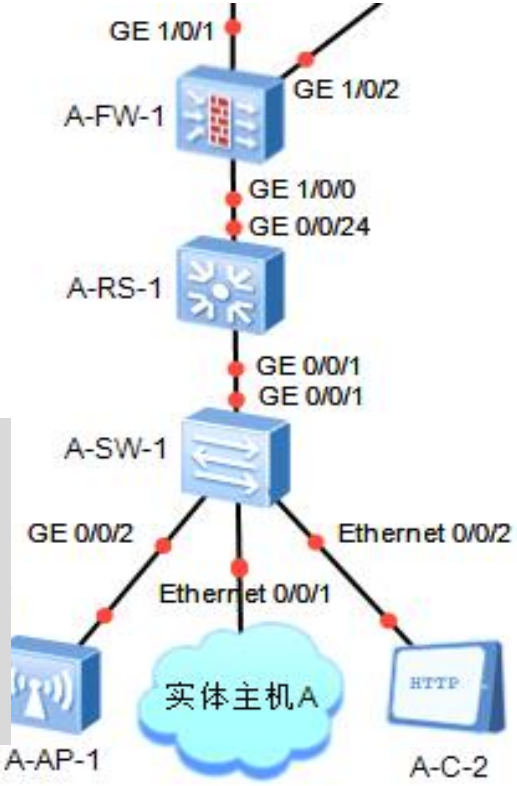
- 步骤4：设置本地实体机为用户区域A的主机并能够Web登录A-FW-1
  - 讨论1：实体主机的虚拟网卡IP地址？



用户与认证 —— 本地认证

- 步骤4：设置本地实体机为用户区域A的主机并能够Web登录A-FW-1

  - 讨论2：本地实体主机访问防火墙A-FW-1认证界面的路由策略？



【实体机上的配置】

```
>route add 10.0.1.1 mask 255.255.255.255 192.168.64.254
>route add 172.16.65.10 mask 255.255.255.255 192.168.64.254
```

【防火墙上的配置】

```
[A-FW-1]interface GigabitEthernet 1/0/0
[A-FW-1-GigabitEthernet1/0/0]service-manage http permit
[A-FW-1-GigabitEthernet1/0/0]service-manage https permit
[A-FW-1-GigabitEthernet1/0/0]quit
```

用户与认证 —— 本地认证

- 步骤5：上网认证
  - 要点
  - 在本地实体主机的浏览器中输入防火墙A-FW-1的认证地址https://10.0.1.1:8887（ 8887是防火墙默认的认证端口），可以看到防火墙的认证界面，输入用户名test和密码abcd@1234并点击“登录”按钮，可以看到登录成功界面

用户与认证 —— 本地认证

- 步骤5：上网认证

用户行为管理

一、用户与认证

—— 服务器认证

用户与认证 —— 服务器认证

- 认证服务器
  - 认证时常用的服务器，包括RADIUS服务器、HWTACACS服务器、LDAP服务器、AD服务器。
  - RADIUS服务器
    - FW与RADIUS服务器之间使用RADIUS协议通信，RADIUS协议使用UDP协议作为传输协议，具有良好的实时性；同时也支持重传机制和备用服务器机制，从而具有较好的可靠性。FW与RADIUS服务器之间使用共享密钥对传输的报文进行加密，具有较好的安全性。
    - RADIUS协议的实现比较简单，适用于大用户量时服务器端的多线程结构。

用户与认证 —— 服务器认证

- 认证服务器
  - HWTACACS服务器（Huawei Terminal Access Controller Access Control System ）
    - FW与HWTACACS服务器之间使用HWTACACS协议通信，HWTACACS协议是在TACACS基础上进行了功能增强的一种安全协议，主要用于用户的认证、授权和计费。
    - 与RADIUS协议相比，HWTACACS协议具有更加可靠的传输和加密特性，更加适合于安全控制

用户与认证 —— 服务器认证

HWTACACS协议与RADIUS协议的主要区别

HWTACACS	RADIUS
使用TCP协议，网络传输更可靠	使用UDP协议
除了标准的HWTACACS报文头，对报文主体全部进行加密	只是对认证报文中的密码字段进行加密
认证与授权分离	认证与授权一起处理
适于进行安全控制	适于进行计费
支持对配置命令进行授权	不支持对配置命令进行授权

用户与认证 —— 服务器认证

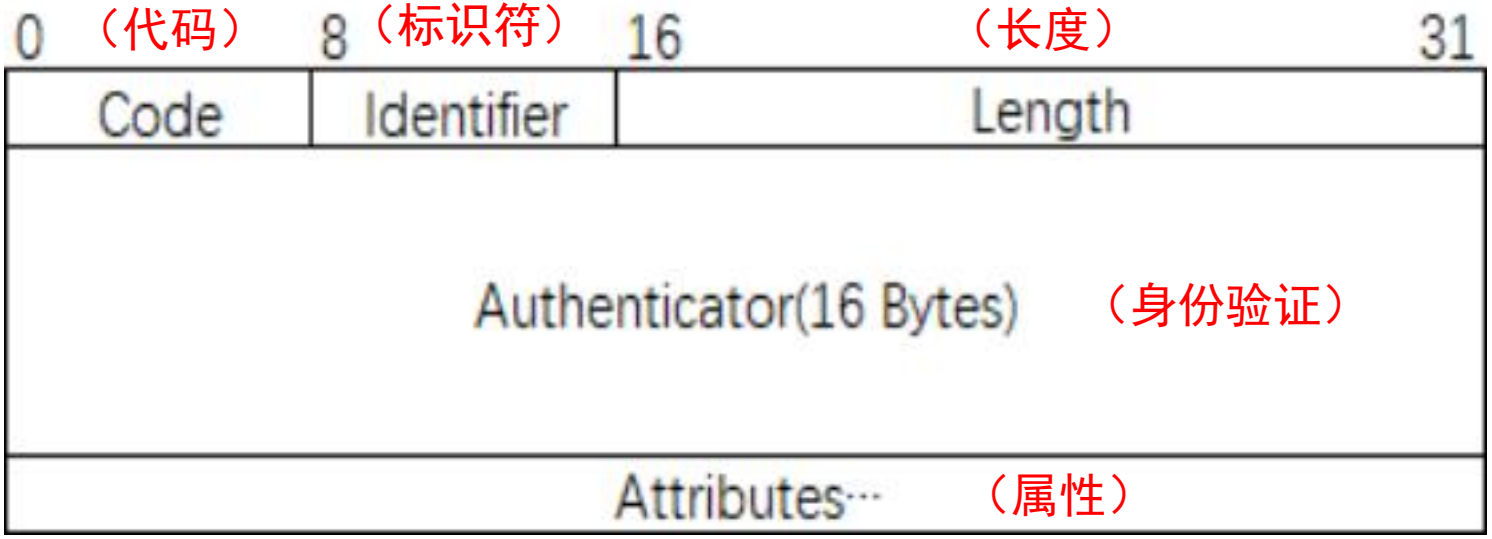
- 认证服务器
  - AD服务器
    - AD是Windows Server域环境中提供目录服务的组件，可以将活动目录理解为目录服务在微软平台的一种实现方式。
    - 活动目录将登录身份验证以及目录对象的访问控制集成在一起，管理员可以管理分散在网络各处的目录数据和组织单位，经过授权的网络用户可以访问网络任意位置的资源。

用户与认证 —— 服务器认证

- 认识RADIUS
  - RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证系统），协议定义了基于UDP的RADIUS报文格式及其传输机制，并规定UDP端口1812、1813分别作为认证、计费端口。
  - RADIUS服务器通常需要维护三个数据库Users、Clients、Dictionary。
    - Users：用于存储用户信息，如用户名、口令以及使用的协议、IP地址等配置信息；
    - Clients：用于存储RADIUS客户端的信息，如接入设备的共享密钥、IP地址等；
    - Dictionary（词典）：用于存储RADIUS协议中的属性和属性值含义的信息。

用户与认证 —— 服务器认证

- RADIUS报文结构



用户与认证 —— 服务器认证

- RADIUS报文结构

报文字段	报文说明
Code	长度为1个字节，说明RADIUS报文类型。
Identifier	长度为1个字节，用来匹配请求报文和响应报文。
Length	长度为2个字节，用来指定RADIUS报文的长度。
Authenticator	长度为16个字节，用来验证客户端与RADIUS服务器的消息
Attribute	不定长度，报文的内容主体，用来携带专门的认证、授权和计费信息，提供请求和响应报文的配置细节。

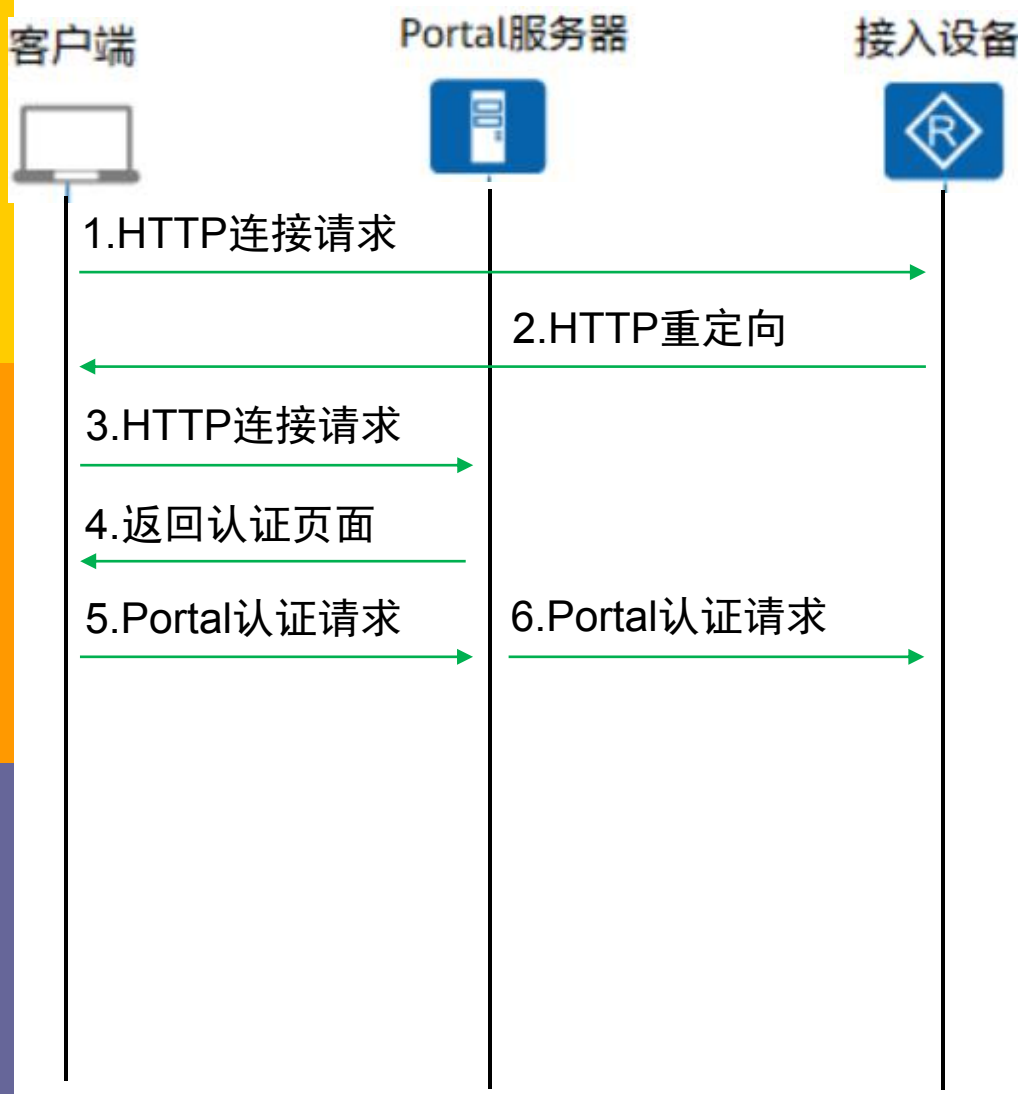
用户与认证 —— 服务器认证

RADIUS报文结构 （RADIUS的认证报文）

报文名称	报文说明
Access-Request	认证请求报文，是RADIUS报文交互过程中的第一个报文，携带用户的认证信息（例如：用户名、密码等）。认证请求报文由RADIUS客户端发送给RADIUS服务器，RADIUS服务器根据该报文中携带的认证信息判断是否允许接入。
Access-Accept	认证接受报文，是服务器对客户端发送的Access-Request报文的响应报文。如果Access-Request报文认证通过，则发送该类型报文。客户端收到此报文后，认证用户才能认证通过并被赋予相应的权限。
Access-Reject	认证拒绝报文，是服务器对客户端的Access-Request报文的拒绝响应报文。如果Access-Request报文即认证失败，则RADIUS服务器返回Access-Reject报文，用户认证失败。
Access-Challenge	认证挑战报文。EAP认证时，RADIUS服务器接收到Access-Request报文中携带的用户名信息后，会随机生成一个MD5挑战字，同时将此挑战字通过Access-Challenge报文发送给客户端。客户端使用该挑战字对用户密码进行加密处理后，将新的用户密码信息通过Access-Request报文发送给RADIUS服务器。RADIUS服务器将收到的已加密的密码信息和本地经过加密运算后的密码信息进行对比，如果相同，则该用户为合法用户。

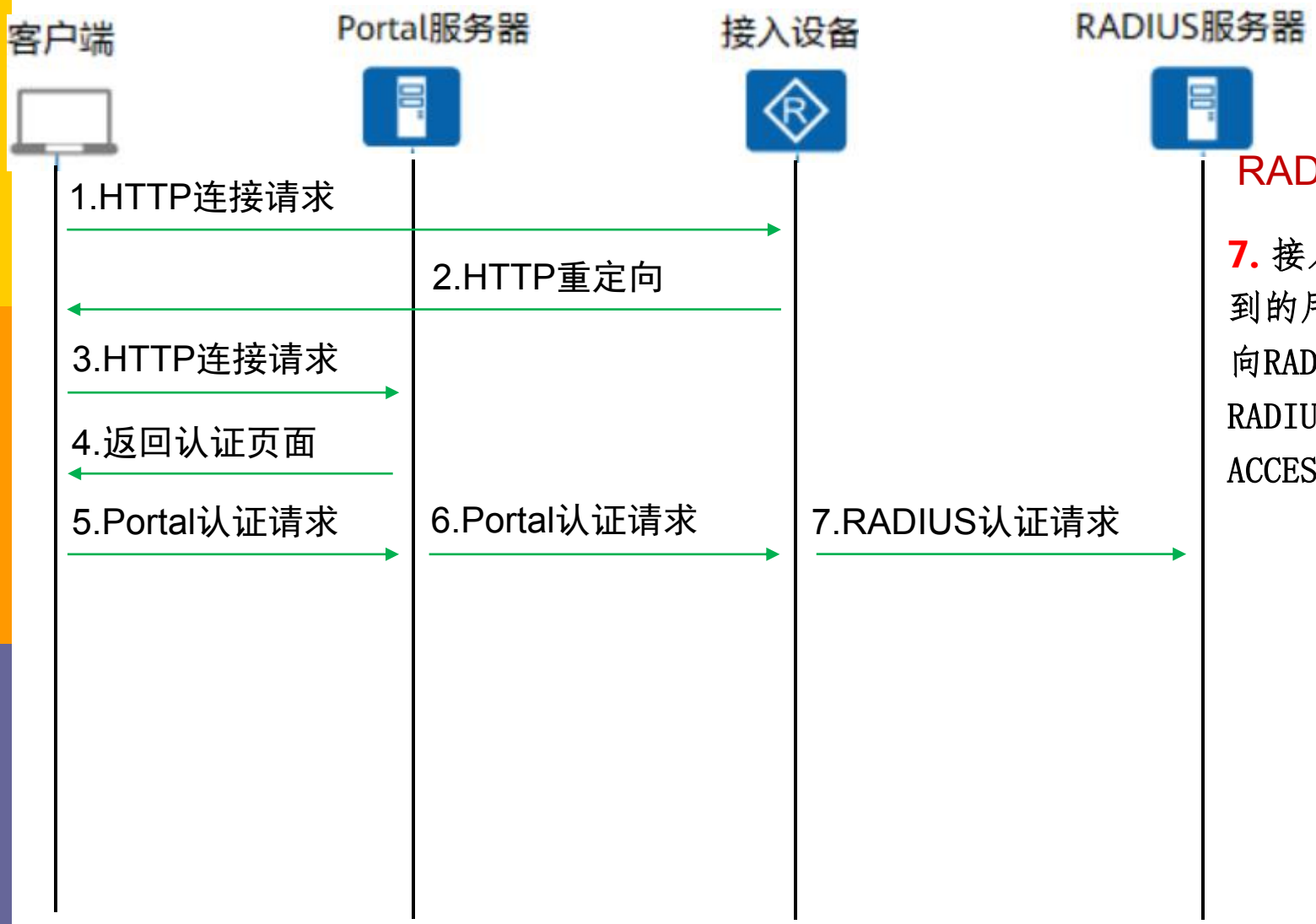
用户与认证 —— 服务器认证

- 基于RADIUS服务器的认证流程



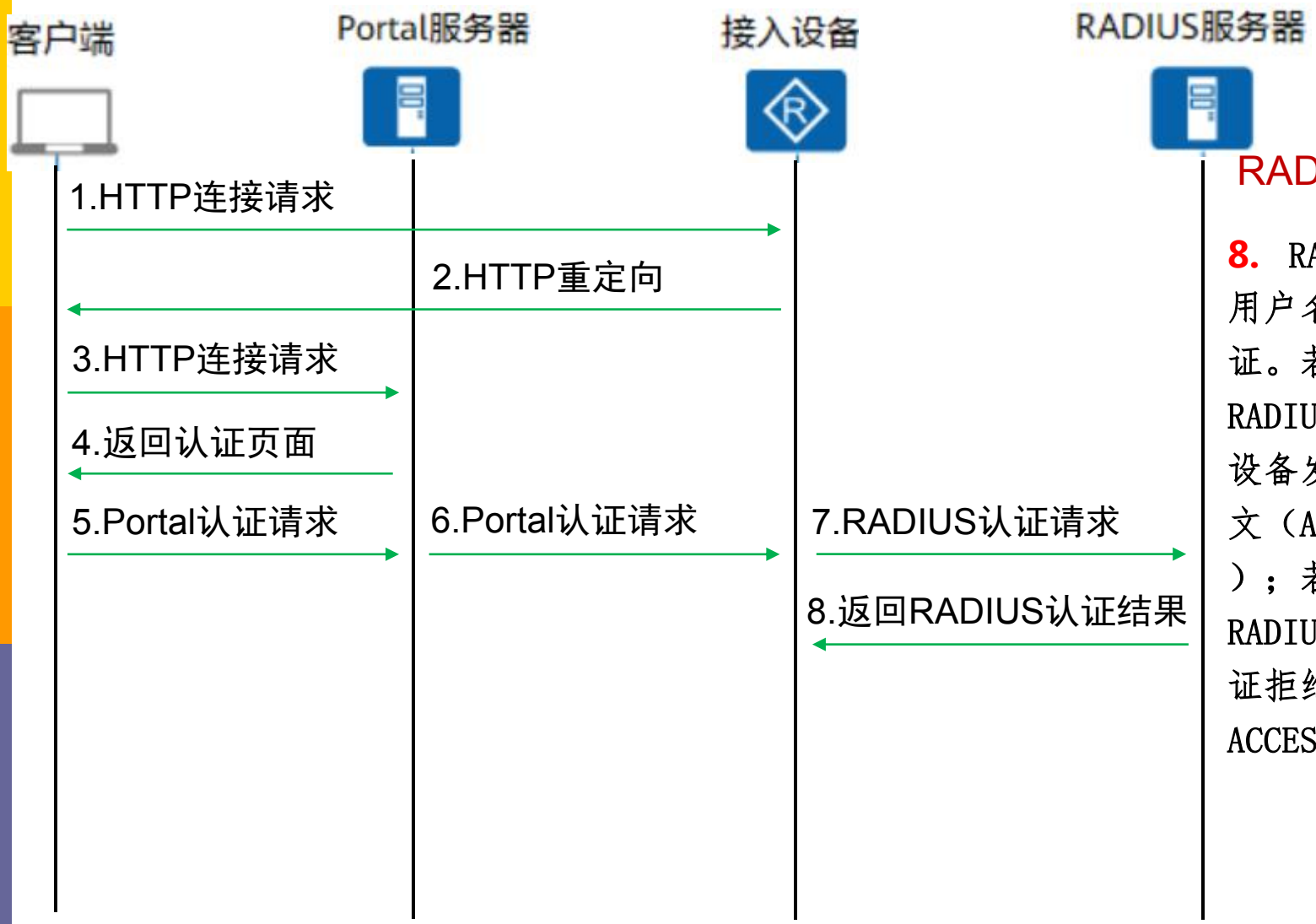
RADIUS认证流程

6. Portal服务器将用户输入的用户名和密码封装在Portal认证请求报文（REQ_AUTH）中，并发送给接入设备。



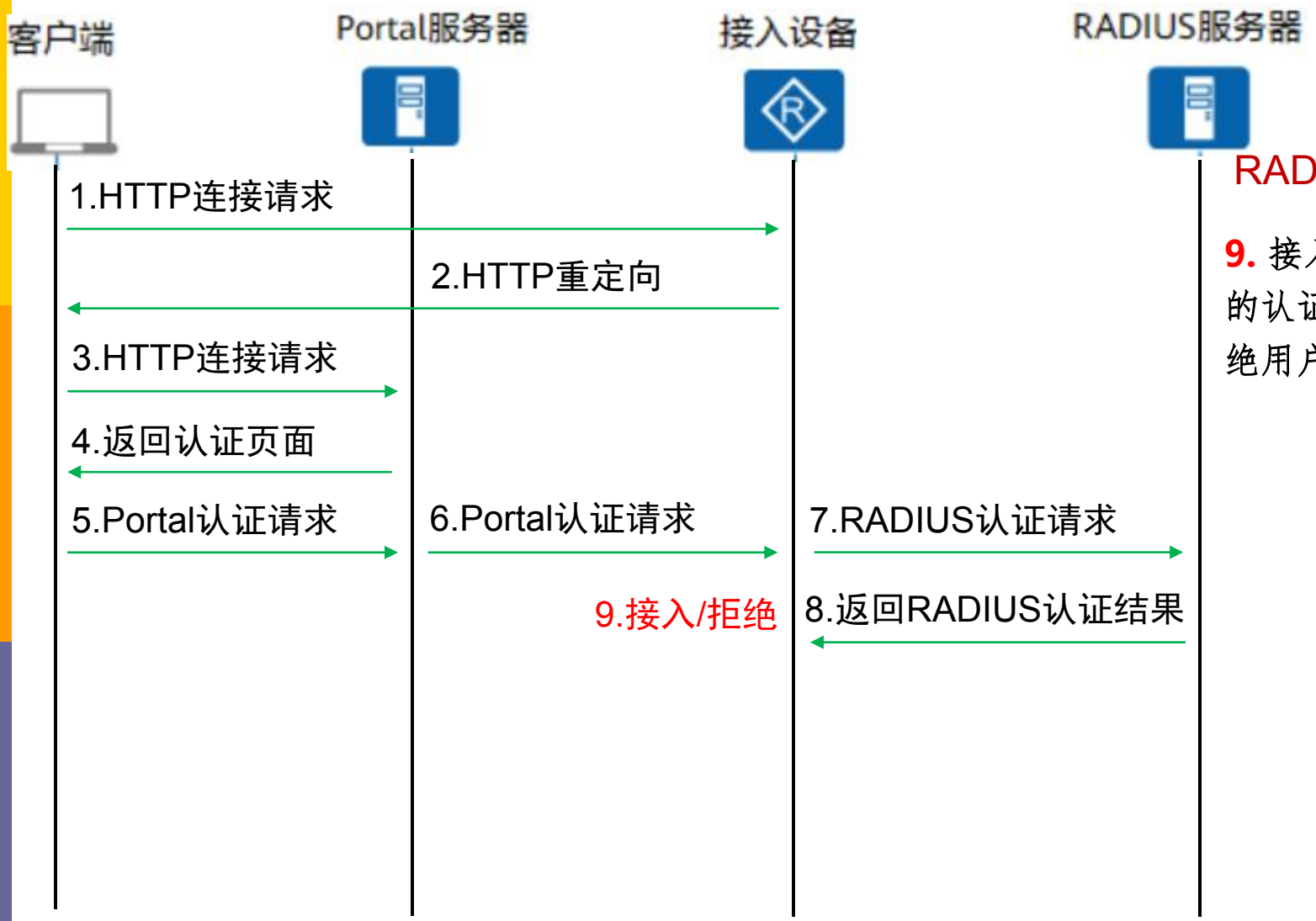
RADIUS认证流程

7. 接入设备根据获取到的用户名和密码，向RADIUS服务器发送RADIUS请求（ACCESS-REQUEST）



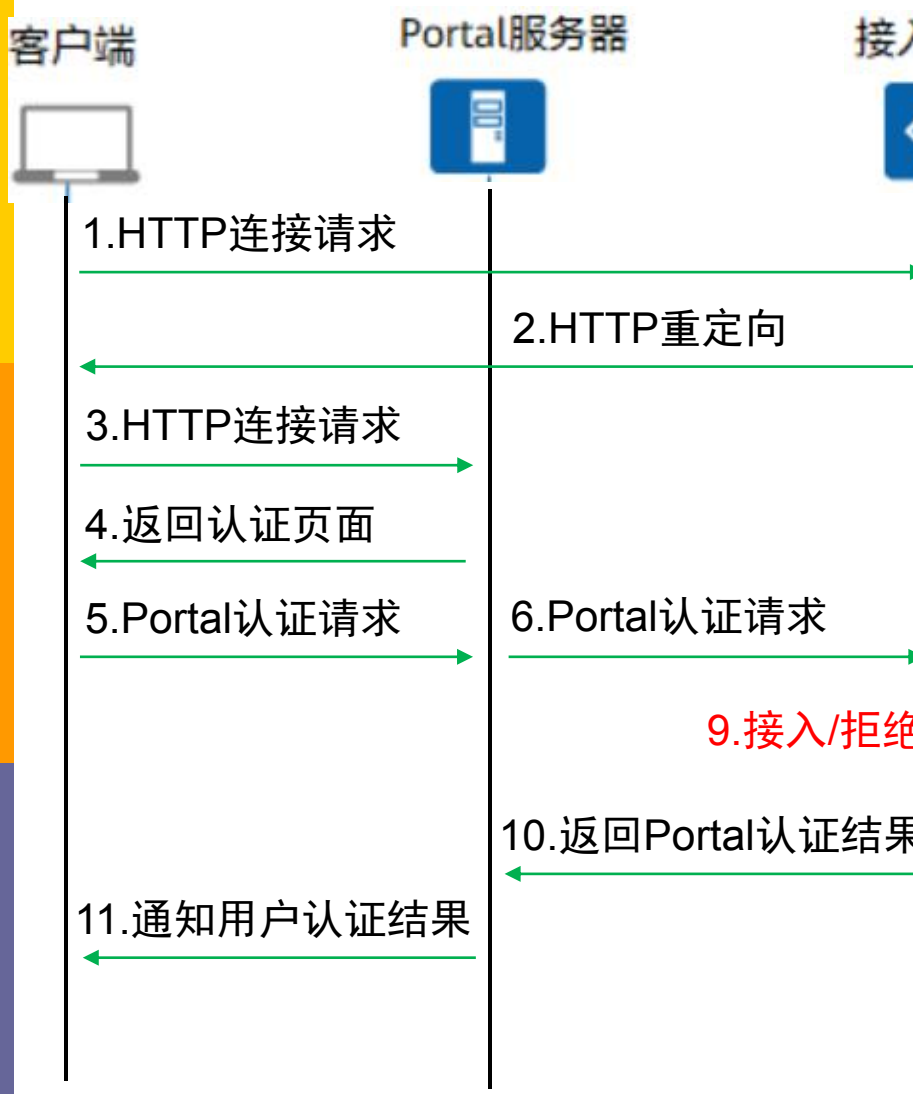
RADIUS认证流程

8. RADIUS服务器对用户名和密码进行认证。若认证成功，则RADIUS服务器向接入设备发送认证接受报文（ACCESS-ACCEPT）；若认证失败，则RADIUS服务器返回认证拒绝报文（ACCESS-REJECT）



RADIUS认证流程

9. 接入设备根据收到的认证结果接入/拒绝用户。



RADIUS认证流程

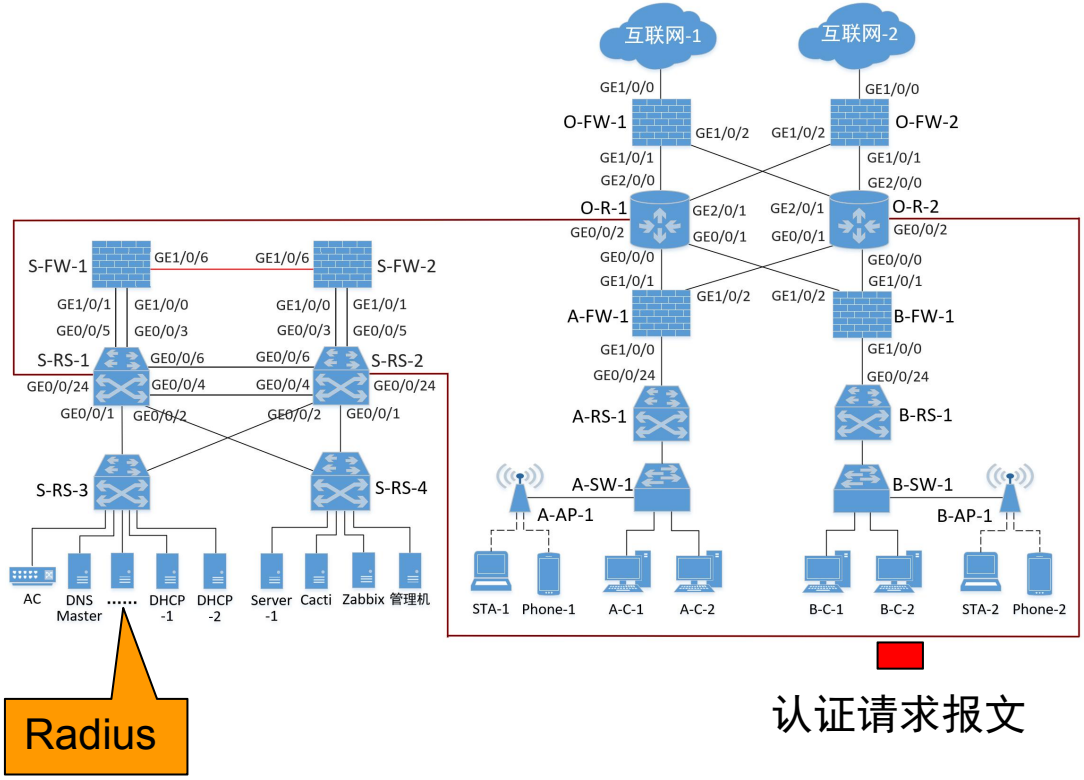
10.接入设备向Portal服务器返回Portal认证结果（ACK_AUTH），并将用户加入自身在线用户列表。

11. Portal服务器向客户端发送认证结果报文，通知客户端认证成功，并将用户加入自身在线用户列表。

用户与认证 —— 服务器认证

【实验案例】服务器认证

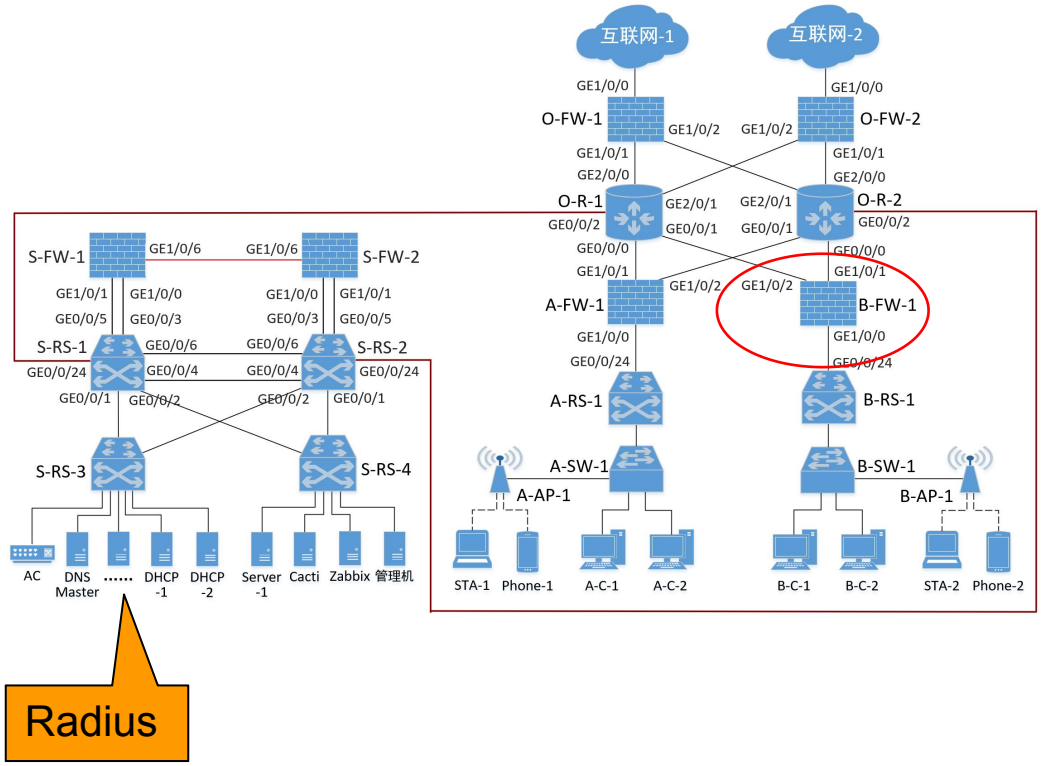
- 在园区网数据中心区域部署RADIUS服务器。
- 防火墙收到认证请求后，会将认证请求转发至RADIUS服务器，并在RADIUS服务器中完成认证。
- 这种认证方式也称为全网统一认证。



用户与认证 —— 服务器认证

- 【实验案例】服务器认证
- 要点：

1. 创建RADIUS服务器，并接入数据中心网络
2. 配置RADIUS服务器（添加客户端、认证用户）
3. （Web方式）配置用户区域B的防火墙(RADIUS服务器信息、认证方式、认证用户、认证策略）。



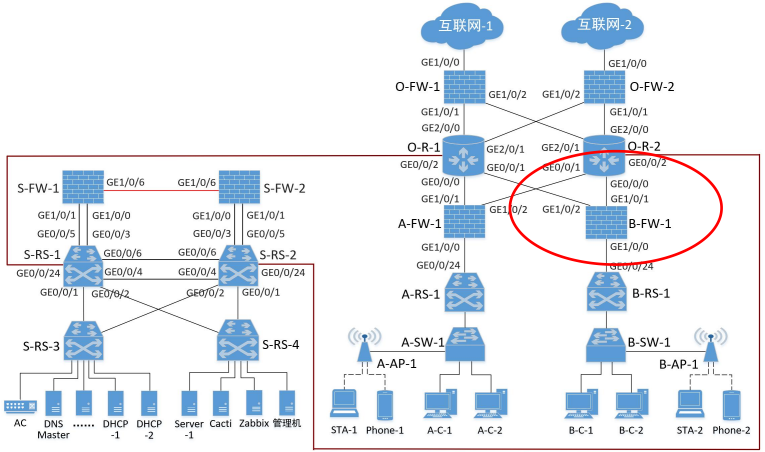
用户与认证 —— 服务器认证

要点1：创建RADIUS服务器

① 在VirtualBox中创建虚拟机。

② 由于接下来要在线安装FreeRADIUS等软件，所以虚拟机创建好以后，暂不接入eNSP的仿真网络，其网卡连接方式保持默认设置“网络地址转换（NAT）”。

③ 接入eNSP网络



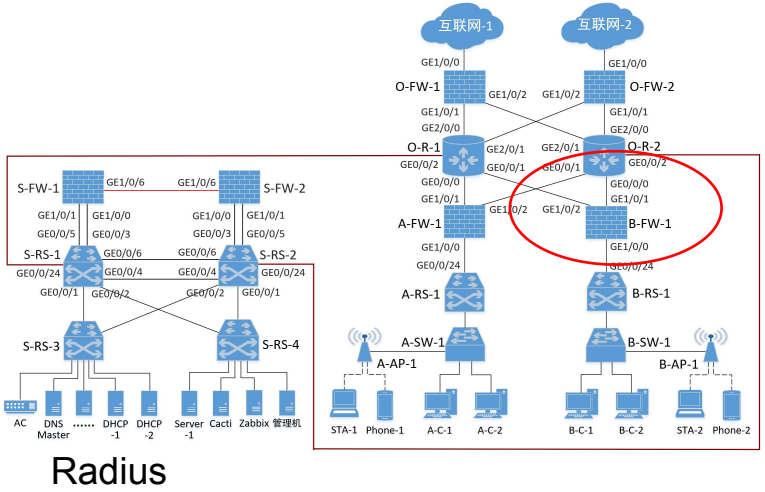
Radius

用户与认证 —— 服务器认证

要点2：配置RADIUS服务器

① 在Radius服务器中增加B-FW-1客户端。

修改配置文件/etc/raddb/clients.conf，指明RADIUS服务器能够接收哪些客户端（此处即防火墙）发来的认证请求。此处在配置文件中添加B-FW-1防火墙，其地址为10.0.255.101，密钥设置为secret255101，允许RADIUS支持的所有协议。



Radius

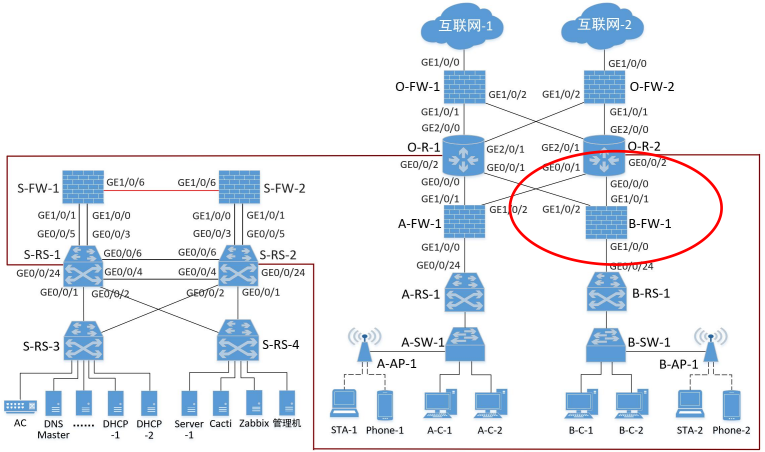
```
[root@localhost ~]# vi /etc/raddb/clients.conf
client B-FW-1 {
        ipaddr = 10.0.255.101
        secret = secret255101
        proto = *
}
```

用户与认证 —— 服务器认证

要点2：配置RADIUS服务器

② 在Radius服务器中添加认证用户。

由于各个防火墙收到认证请求以后，会将认证请求转发至RADIUS服务器，因此需要在RADIUS服务器中添加所有上网用户的认证信息（用户名和密码），实现全网统一认证。



Radius

采用修改认证文件（/etc/raddb/mods-config/files/authorize）的方式来添加认证用户信息。此处添加两个认证用户，用户名分别是testuser1和testuser2，密码都是abcd@1234

```
[root@localhost ~]# vi /etc/raddb/mods-config/files/authorize
//在配置文件的最上方增加两个用户
testuser1 Cleartext-Password := "abcd@1234"
testuser2 Cleartext-Password := "abcd@1234"
……
```

用户与认证 —— 服务器认证

- 要点3：配置防火墙B-FW-1

① 在B-FW-1中添加RADIUS服务器信息

用户与认证 —— 服务器认证

- 要点3：配置防火墙B-FW-1

① 在B-FW-1中添加RADIUS服务器信息

用户与认证 —— 服务器认证

- 要点3：配置防火墙B-FW-1

② 设置B-FW-1的认证方式

用户与认证 —— 服务器认证

- 要点3：配置防火墙B-FW-1

③ 在B-FW-1中添加认证用户

在通过服务器进行认证的方式中，防火墙上也需要添加认证用户，并且必须与认证服务器上的用户名保持一致，否则无法认证成功。

与本地认证方式不同的是，此处不需要设置用户的密码

用户与认证 —— 服务器认证

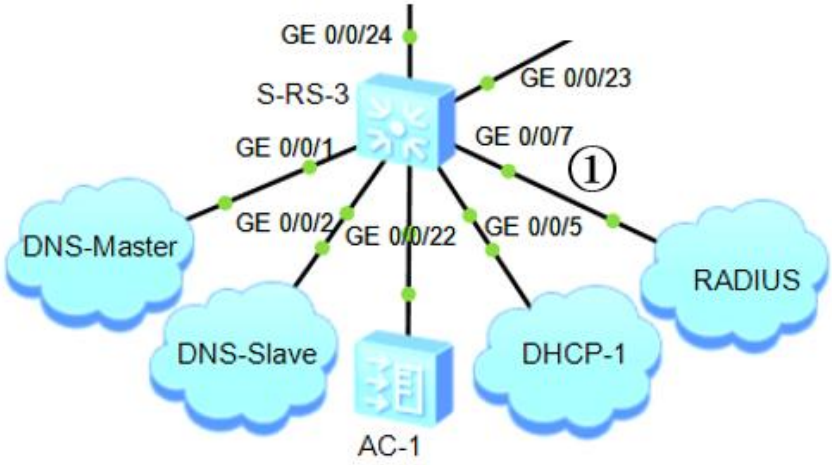
- 要点3：配置防火墙B-FW-1

④ 在B-FW-1中添加认证策略

保持default认证策略不变，添加一条名为User-B的新认证策略：仅对源地址属于192.168.68.0/22（用户区域B中主机的IP地址段，含无线终端用户）的通信进行认证。B-AP-1（10.0.200.16/28地址段）发出的报文不需认证

用户与认证 —— 服务器认证

- 要点4：抓包验证
  - 第16号报文是从防火墙B-FW-1（10.0.255.101）发给RADIUS服务器（172.16.64.20）的Access-Request报文。
  - 第17号报文是从RADIUS服务器返回防火墙B-FW-1的Access-Accept报文



radius

No.	Source	Destination	Protocol	Info
16	10.0.255.101	172.16.64.20	RADIUS	Access-Request id=2
17	172.16.64.20	10.0.255.101	RADIUS	Access-Accept id=2

用户与认证 —— 服务器认证

第16号报文是从防火墙B-FW-1发给RADIUS服务器的报文。

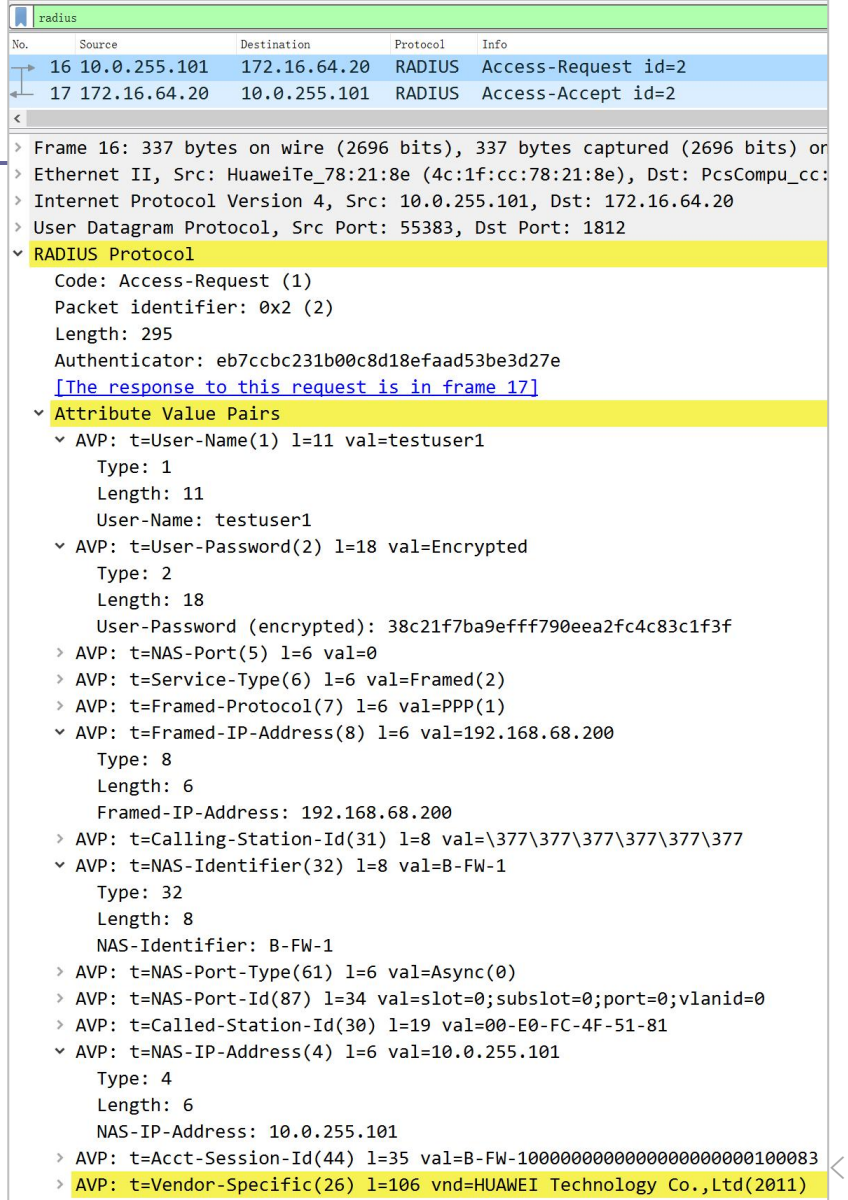
B-FW-1：10.0.255.101

RADIUS服务器：172.16.64.20

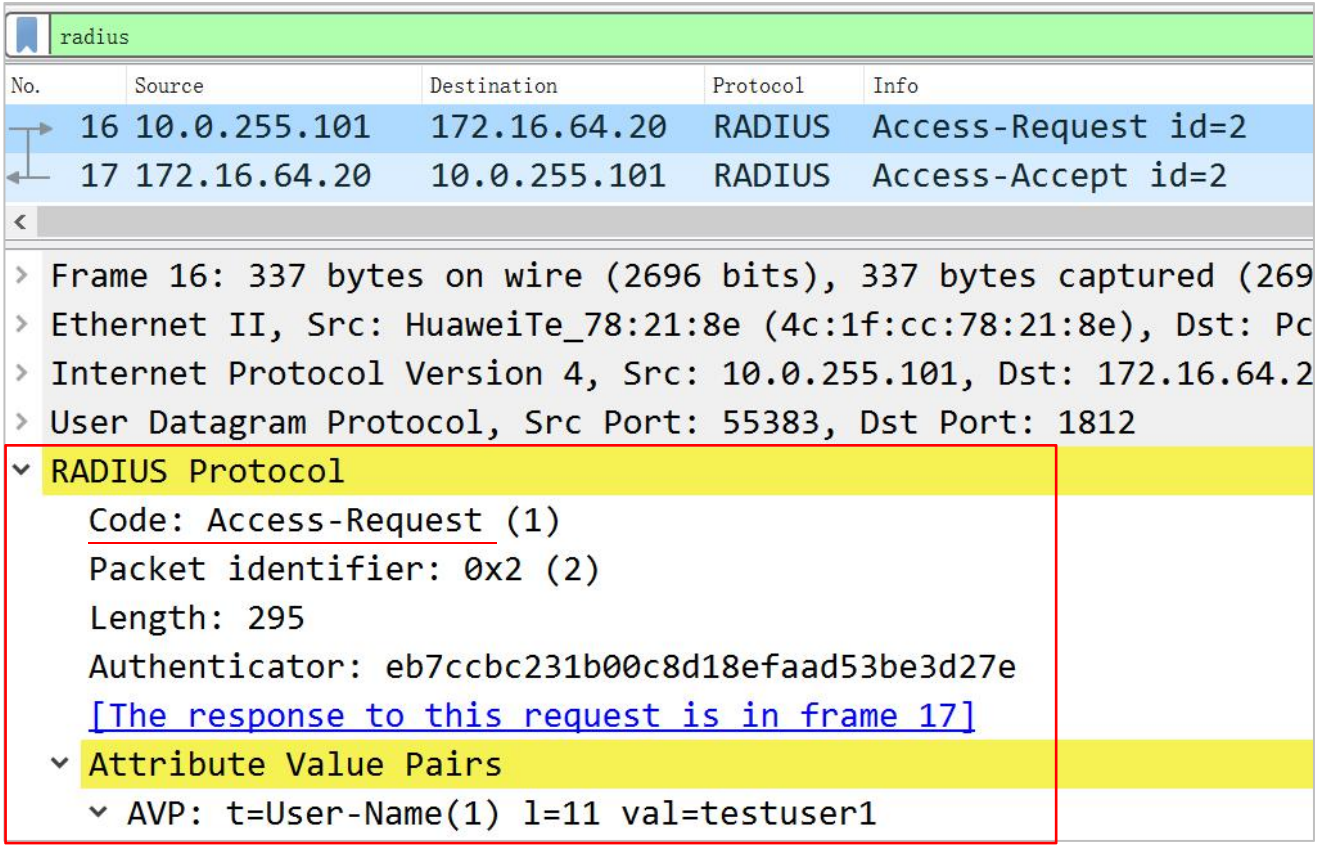
报文类型：Access-Request

用户主机：192.168.68.200

认证用户：testuser1



Radius认证请求报文—— 基本字段

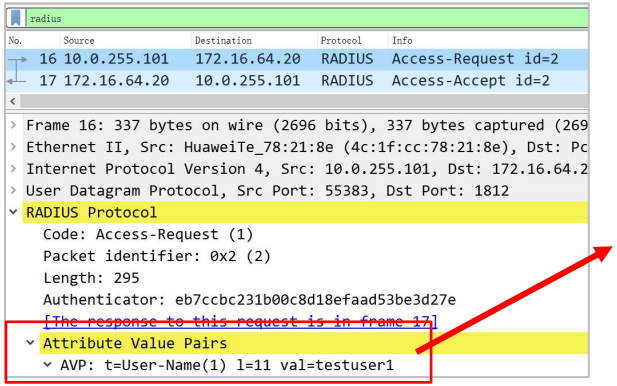


用户与认证 —— 服务器认证

- 【回忆：RADIUS报文结构】

报文字段	报文说明
Code	长度为1个字节，说明RADIUS报文类型。
Identifier	长度为1个字节，用来匹配请求报文和响应报文。
Length	长度为2个字节，用来指定RADIUS报文的长度。
Authenticator	长度为16个字节，用来验证客户端与RADIUS服务器的消息
Attribute	不定长度，报文的内容主体，用来携带专门的认证、授权和计费信息，提供请求和响应报文的配置细节。

Radius认证请求报文——属性值字段

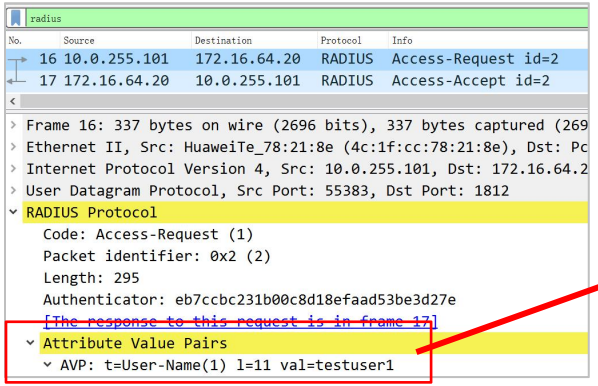


【回忆】

HWTACACS协议与RADIUS协议的主要区别

HWTACACS	RADIUS
使用TCP协议，网络传输更可靠	使用UDP协议
除了标准的HWTACACS报文头，对报文主体全部进行加密	只是对认证报文中的密码字段进行加密
认证与授权分离	认证与授权一起处理
适于进行安全控制	适于进行计费
支持对配置命令进行授权	不支持对配置命令进行授权

Radius认证请求报文—— 属性值字段




```
AVP: t=Framed-IP-Address(8) l=6 val=192.168.68.200
    Type: 8
    Length: 6
    Framed-IP-Address: 192.168.68.200
AVP: t=Calling-Station-Id(31) l=8 val=\377\377\377\377\
AVP: t=NAS-Identifier(32) l=8 val=B-FW-1
    Type: 32
    Length: 8
    NAS-Identifier: B-FW-1
AVP: t=NAS-Port-Type(61) l=6 val=Async(0)
AVP: t=NAS-Port-Id(87) l=34 val=slot=0;subslot=0;port=0
AVP: t=Called-Station-Id(30) l=19 val=00-E0-FC-4F-51-81
AVP: t=NAS-IP-Address(4) l=6 val=10.0.255.101
    Type: 4
    Length: 6
    NAS-IP-Address: 10.0.255.101
```

用户主机IP

防火墙名称

防火墙IP

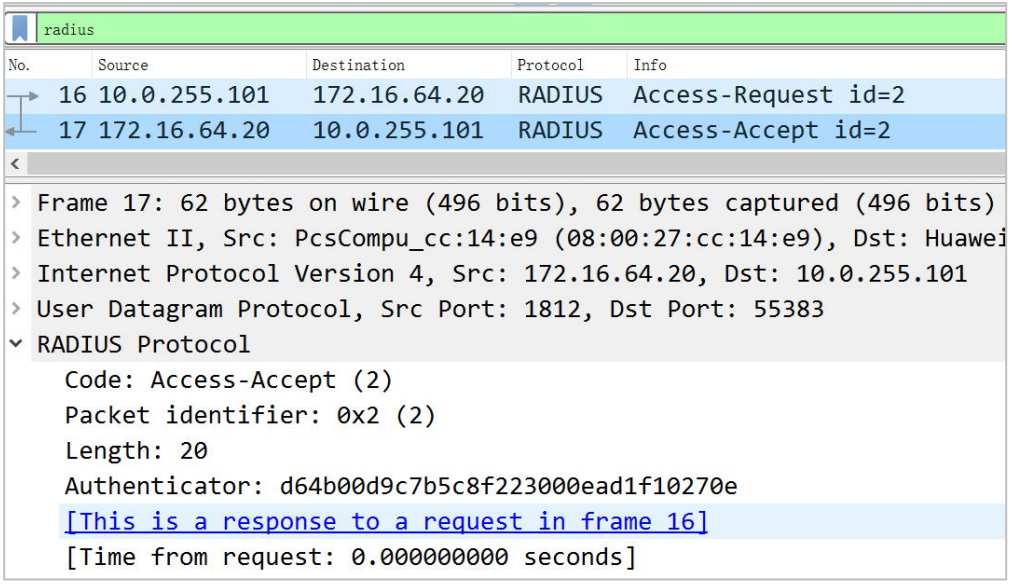
Radius认证接受报文—— 属性值字段

第17号报文是从RADIUS服务器发给防火墙B-FW-1的报文。

B-FW-1：10.0.255.101

RADIUS服务器：172.16.64.20

报文类型：Access-Accept



- 认证接受报文，是服务器对客户端发送的Access-Request报文的响应报文。如果Access-Request报文认证通过，则发送该类型报文。客户端收到此报文后，认证用户才能认证通过并被赋予相应的权限。

用户行为管理

二、日志管理

日志管理

- 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。

日志管理

日志类型

FW支持输出如下日志：

- 会话日志
  - 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。
- 丢包日志
  - 报文被FW丢弃后，FW支持将报文的信息以及被丢弃的原因输出。报文被丢弃的原因包括未命中会话表而被丢弃、以及未通过安全策略检查而被丢弃。

日志管理

- 日志类型
  - 业务日志
    - FW支持输出威胁日志、内容日志、策略命中日志、邮件过滤日志、URL过滤日志以及审计日志等业务日志。
  - 系统日志
    - FW支持将功能模块在运行过程中产生的信息输出，管理员可以通过查阅《日志参考》来了解FW上各个功能模块产生的系统日志信息。

日志管理

日志格式

FW支持的日志格式如下：

- 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。
- Syslog格式
  - 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。

日志管理

日志格式

FW支持的日志格式如下：

- 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。

日志管理

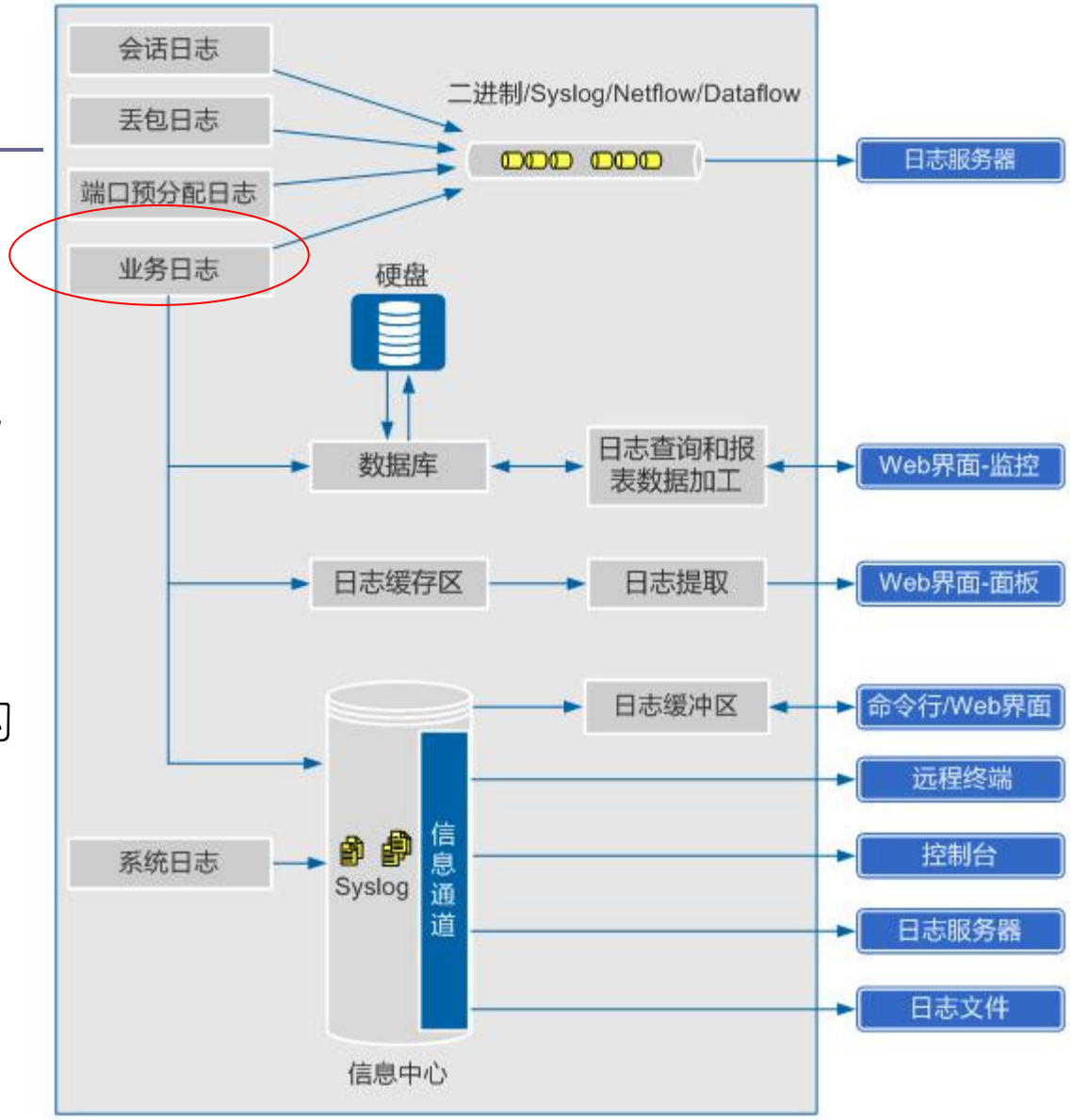
日志的输出原理

- 在防火墙上，不同类型的日志其输出原理也有区别。
- 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。

日志的输出原理

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



日志管理

日志服务器

- 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主机，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

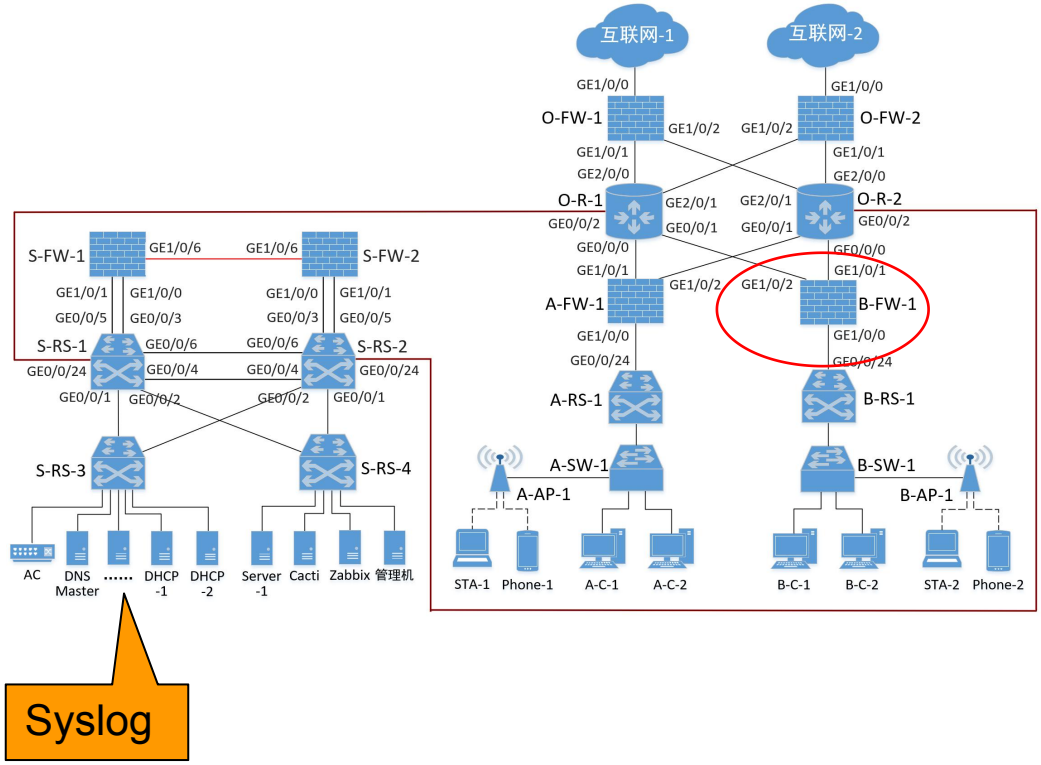
日志格式	默认情况下日志服务器的接收端口
二进制格式	9002
Dataflow格式	9903
Netflow格式	9996
Syslog格式	514

日志管理

- SysLog
  - 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。
  - 在UNIX/Linux系统、路由器、交换机等网络设备中，系统日志记录系统中任何时间发生的大小事件。在Unix/Linux系统中，日志是通过syslogd这个进程记录系统事件、应用程序运行事件。通过配置可以实现运行syslog协议的机器间通信，通过分析这些网络行为日志，掌握设备和网络的状况。

日志管理——记录用户上网行为

- 【实验案例】记录用户上网行为
- 要点：
  1. 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. 查看分析防火墙日志



日志管理——记录用户上网行为

- 要点1：安装配置Syslog服务器

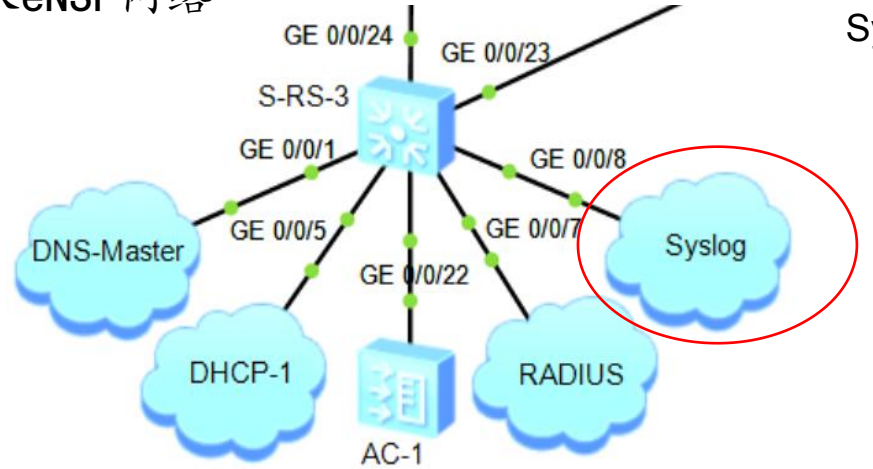
① 在VirtualBox中创建Centos虚拟机。

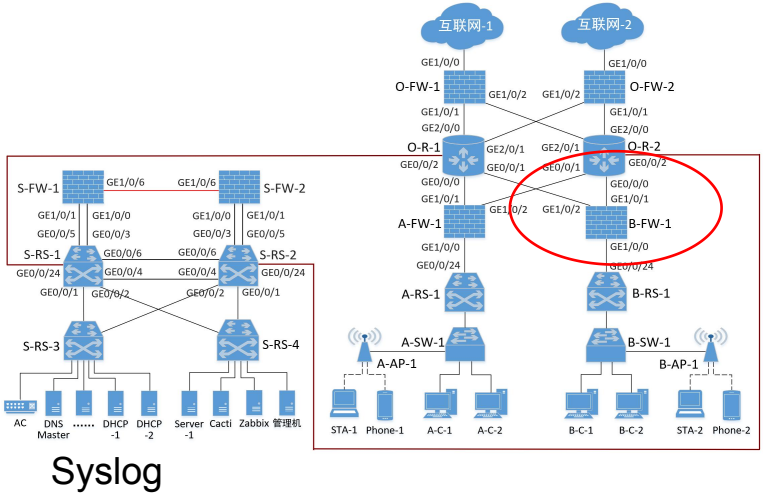
② 配置Syslog日志服务器。

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

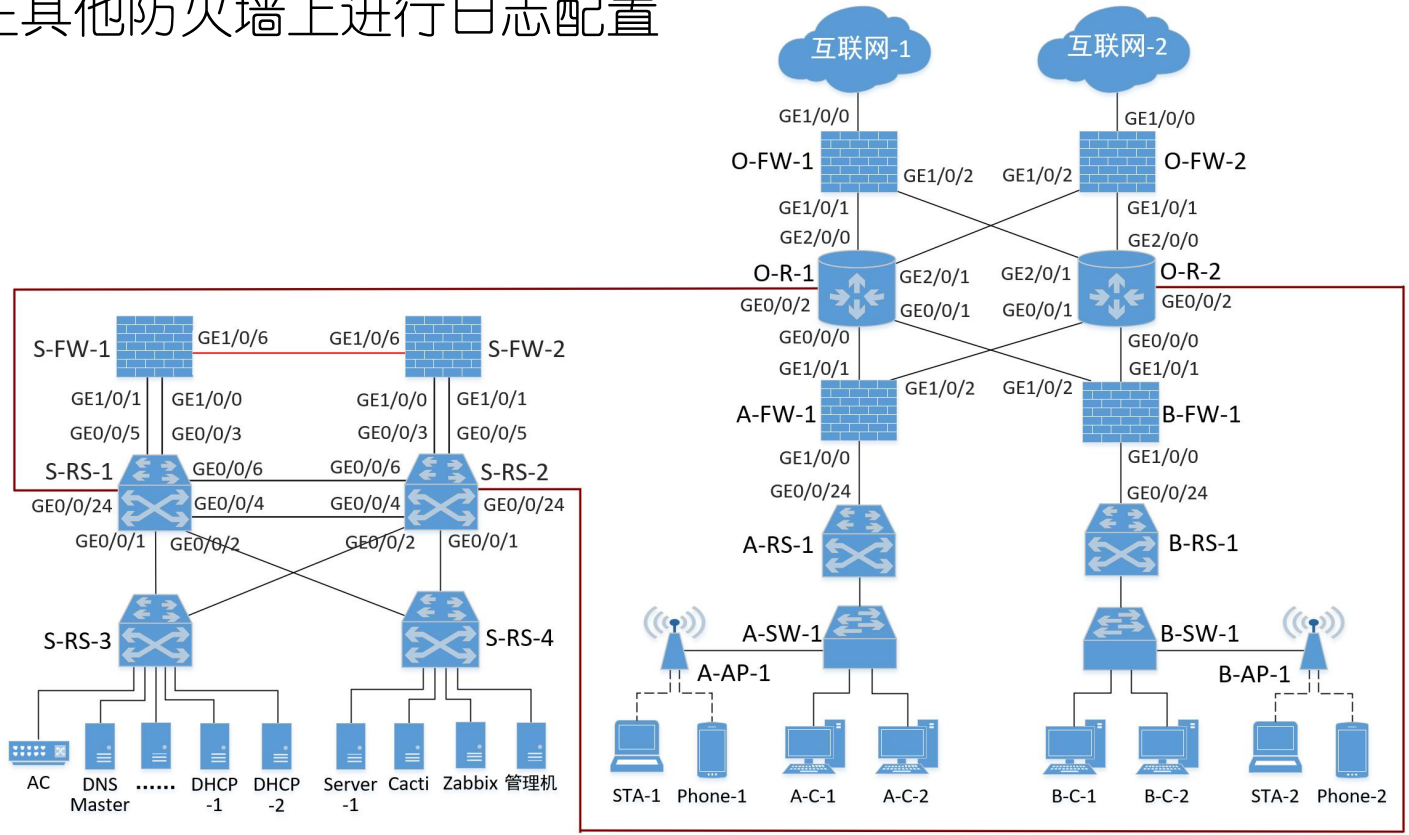
日志管理——记录用户上网行为

- 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

日志管理——记录用户上网行为

- 要点3：在其他防火墙上进行日志配置

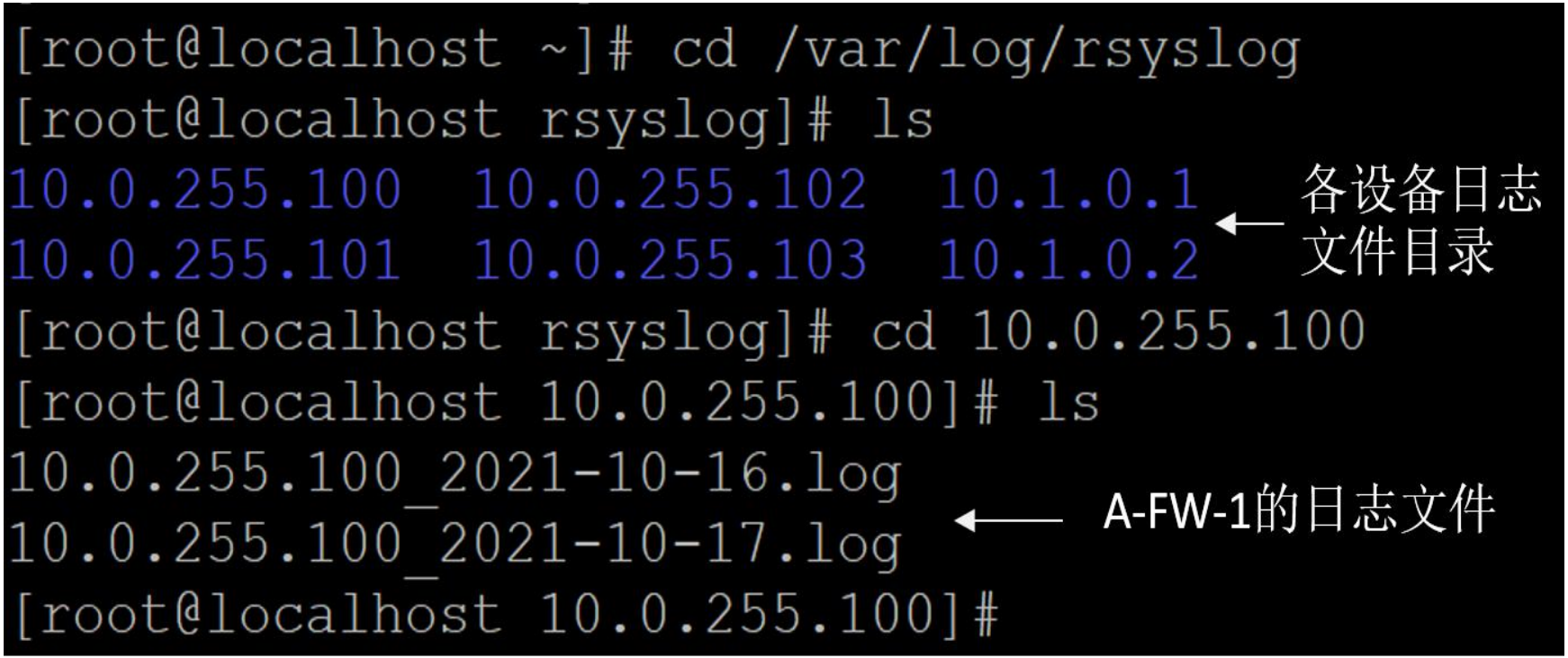


日志管理——记录用户上网行为

- 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

日志管理——记录用户上网行为

- 要点4：在日志服务器上查看日志文件



日志管理——记录用户上网行为

- 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;

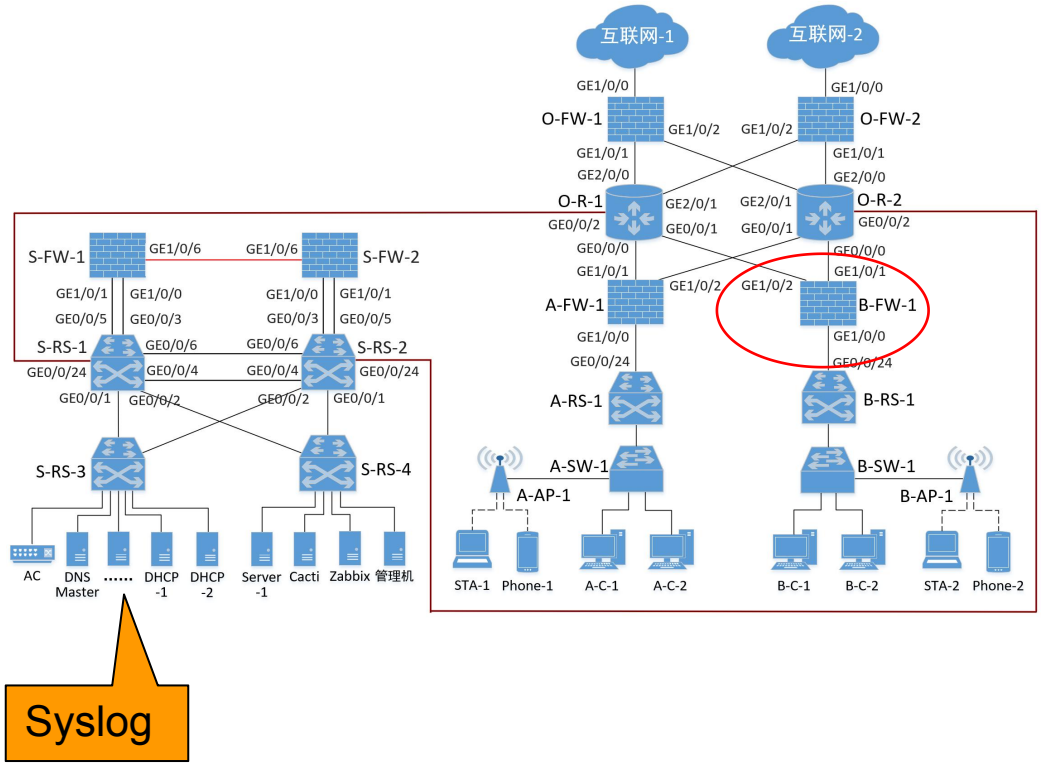
【内容字段含义见下页】

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

日志管理——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. 2、实现使用Tableau分析防火墙日志及用户上网行为



日志管理——分析用户上网行为

- 要点1：在本地实体主机上安装Tableau软件

日志管理——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：

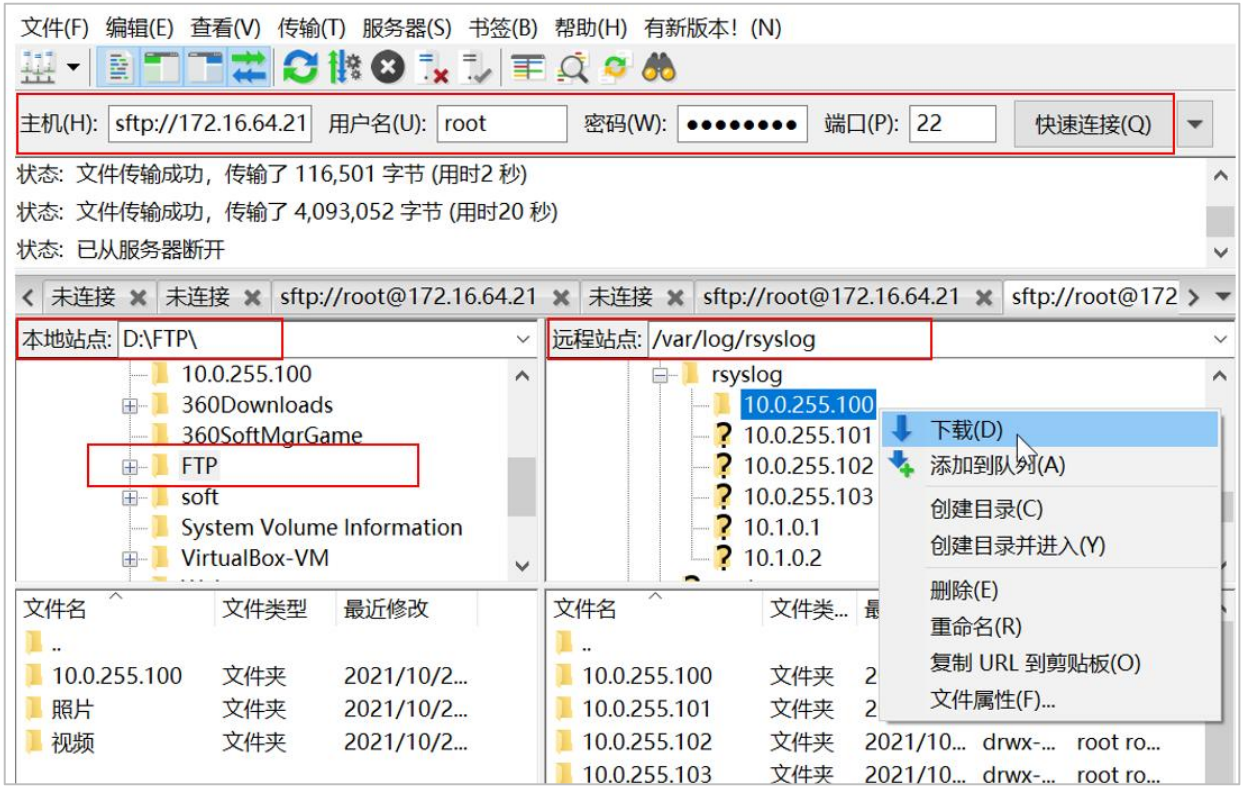
$protocol $srcip:$srcport -> $dstip:$dstport BeginTime :$begintime EndTime: $endtime SendPkts=$sendpackets, SendBytes=$sendbytes, RcvPkts=$rcvpackets, RcvBytes=$rcvbytes

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

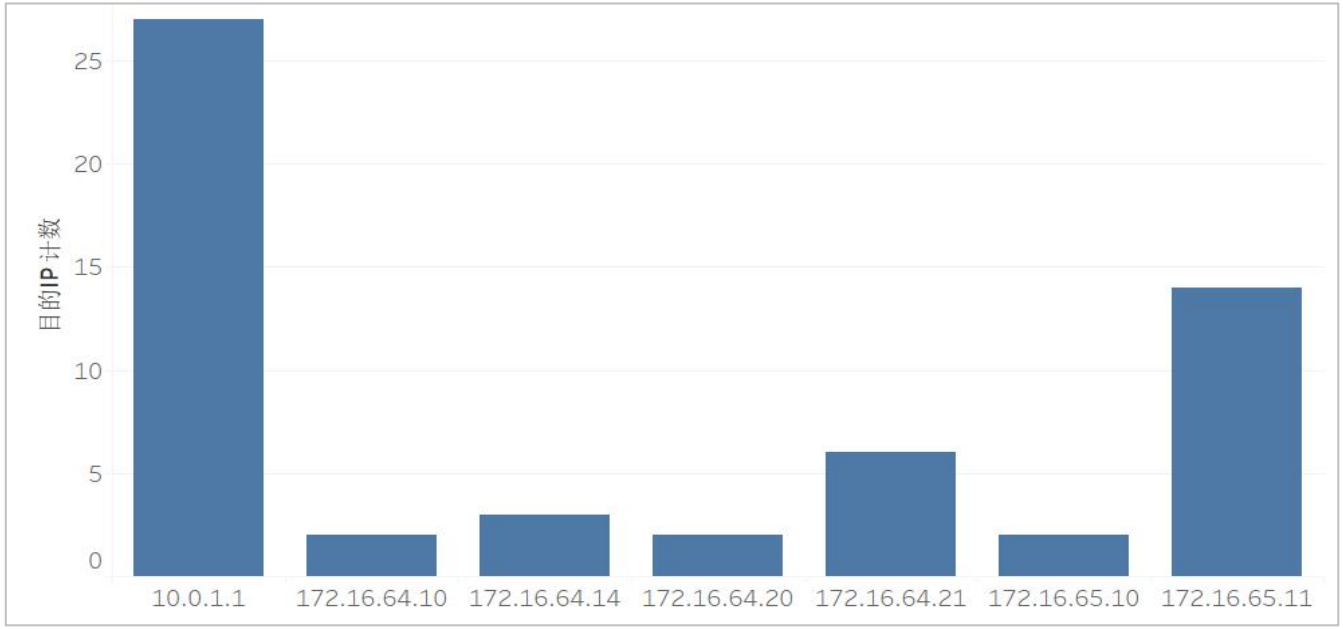
日志管理——分析用户上网行为

- 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



日志管理——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】

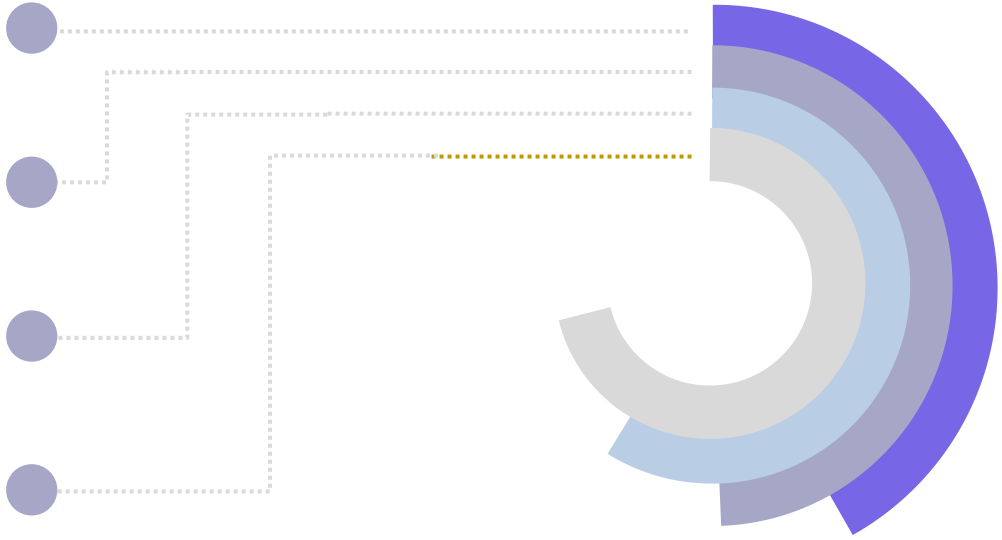
分析内容设计

用户活跃度分析

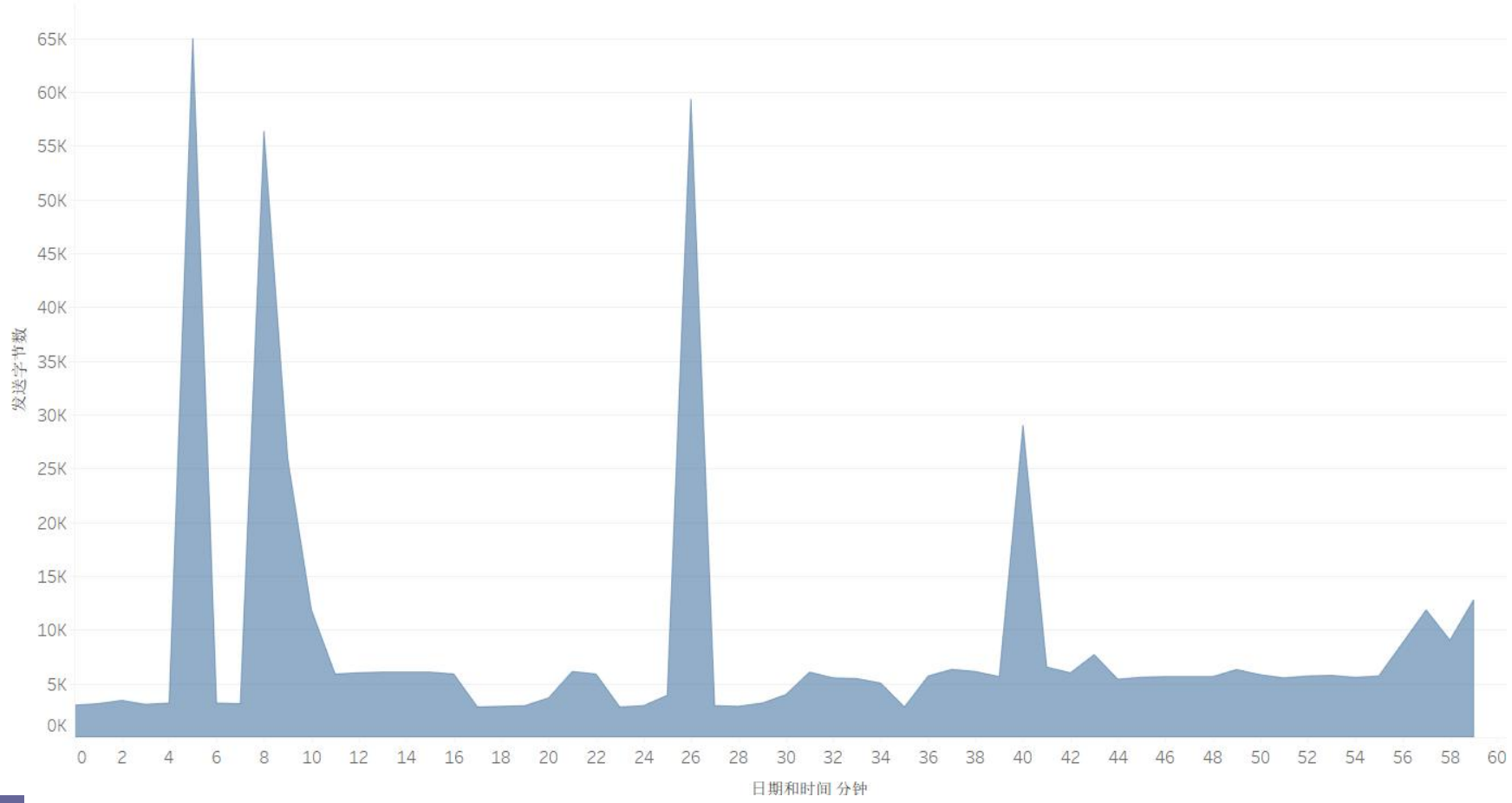
目的IP分析

协议组分析

被拒主机排行分析

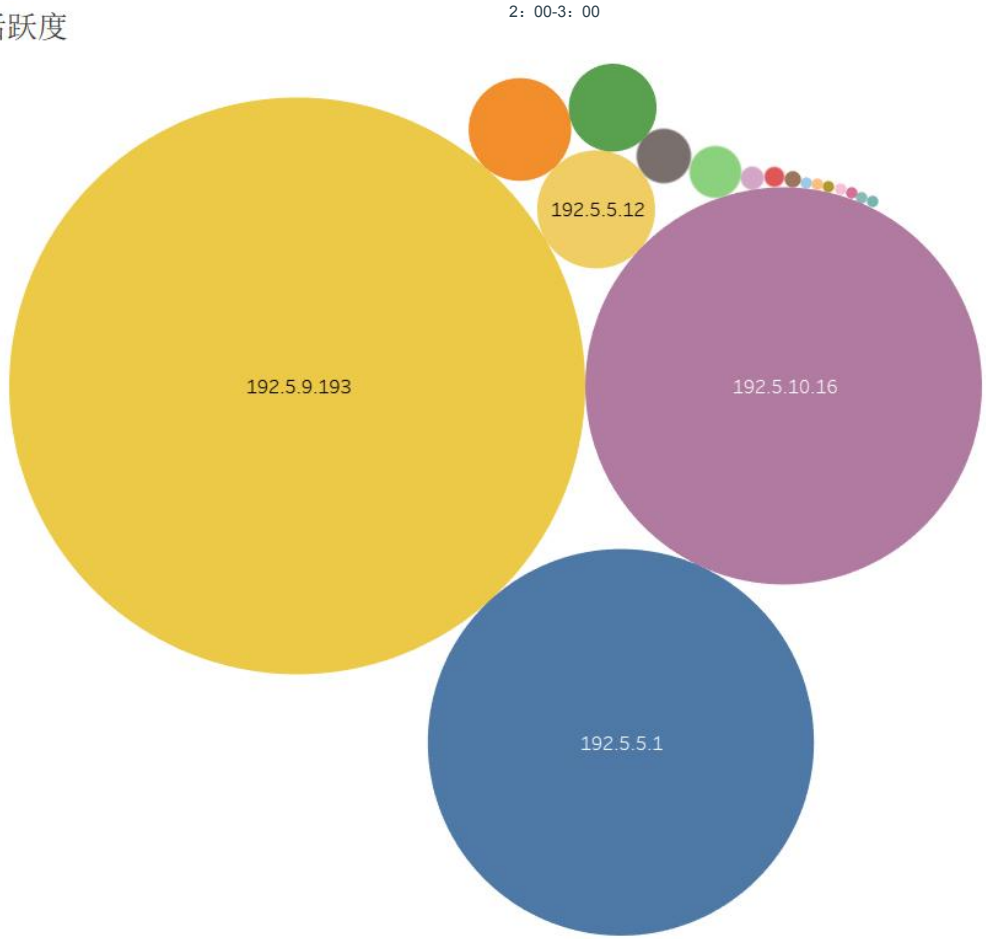


夜间2：00-3：00的流量报表

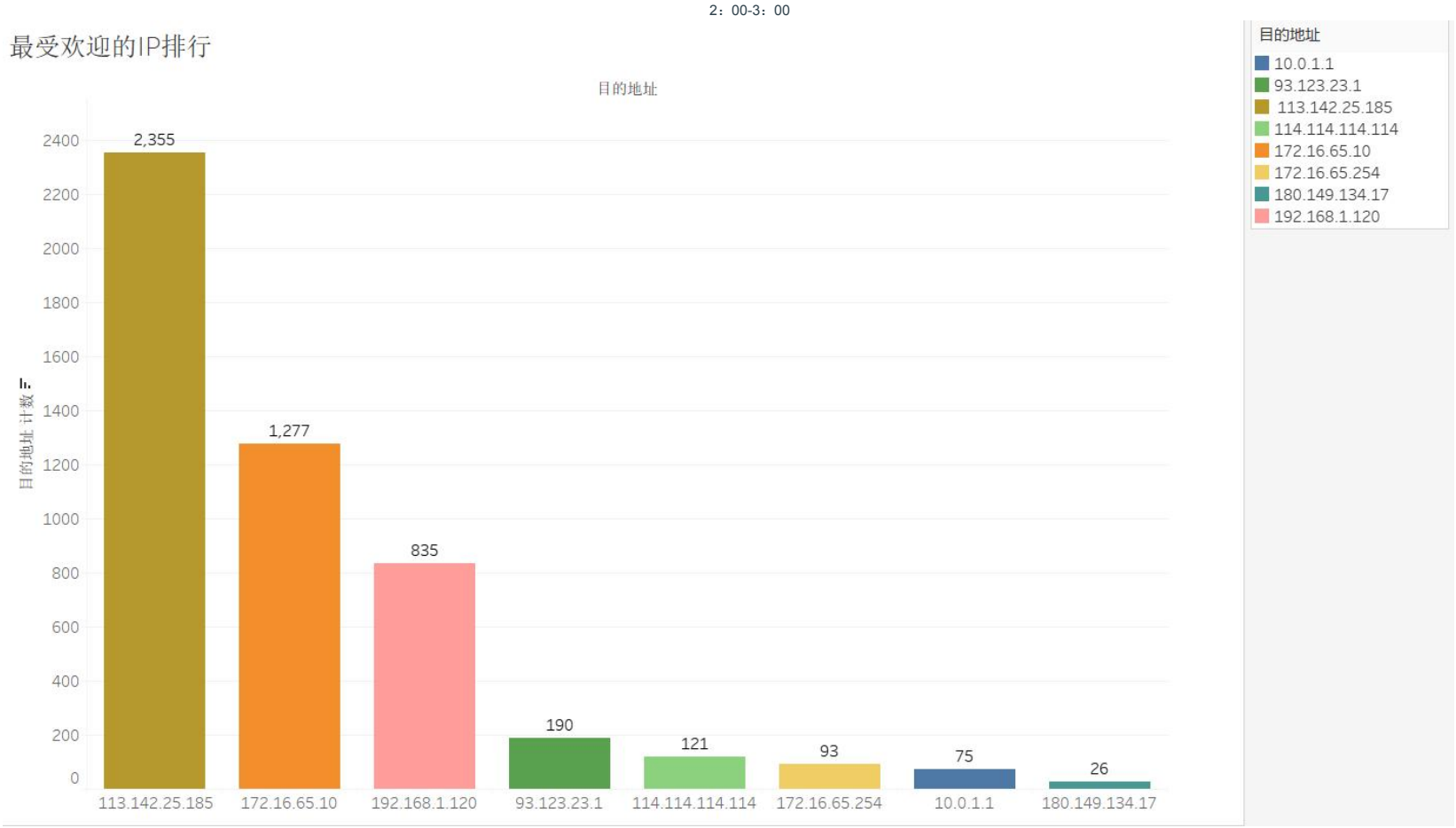


用户活跃度分析

夜间2点-3点用户活跃度



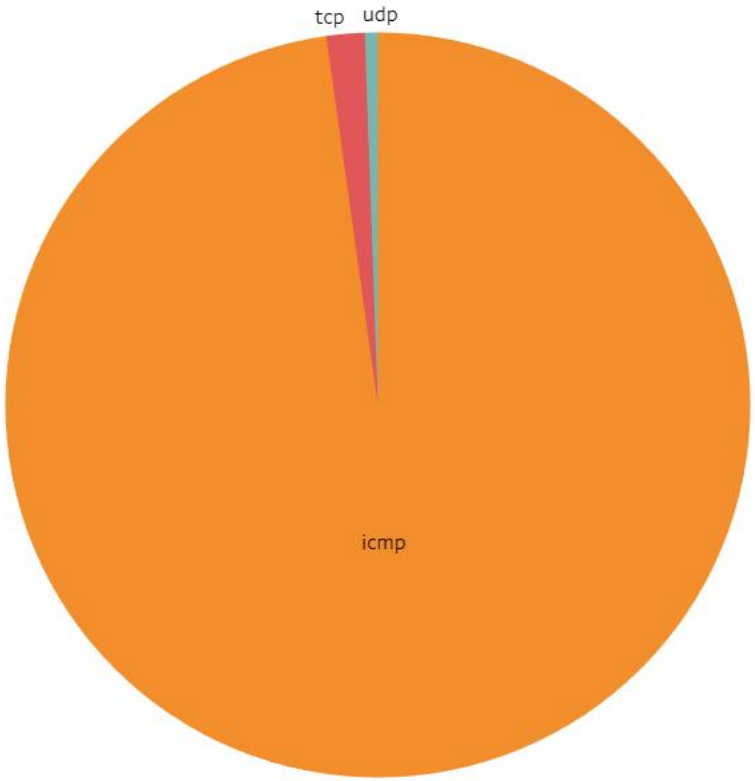
目的IP分析

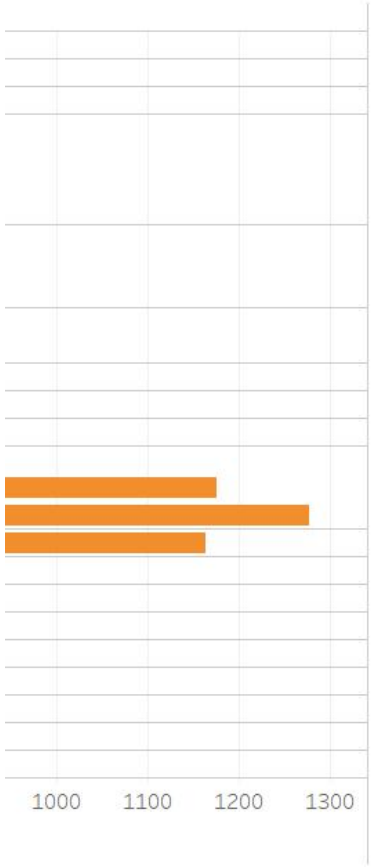

2：00-3：00
最受欢迎的IP排行
目的地址
目的地址 计数
2,355
1,277
835
190
121
93
75
26
113.142.25.185
172.16.65.10
192.168.1.120
93.123.23.1
114.114.114.114
172.16.65.254
10.0.1.1
180.149.134.17
目的地址
10.0.1.1
93.123.23.1
113.142.25.185
114.114.114.114
172.16.65.10
172.16.65.254
180.149.134.17
192.168.1.120

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.

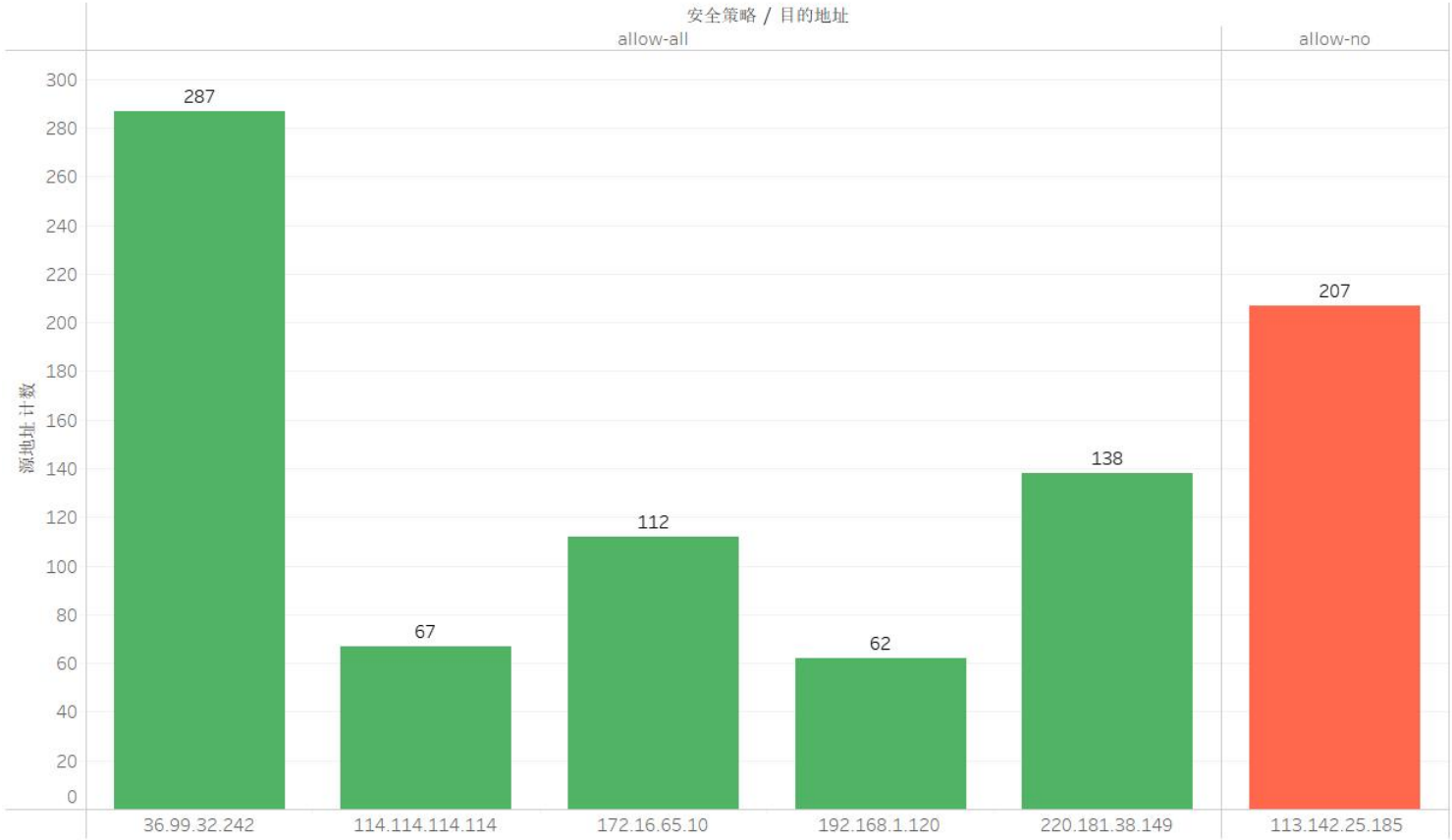




被拒绝访问的IP

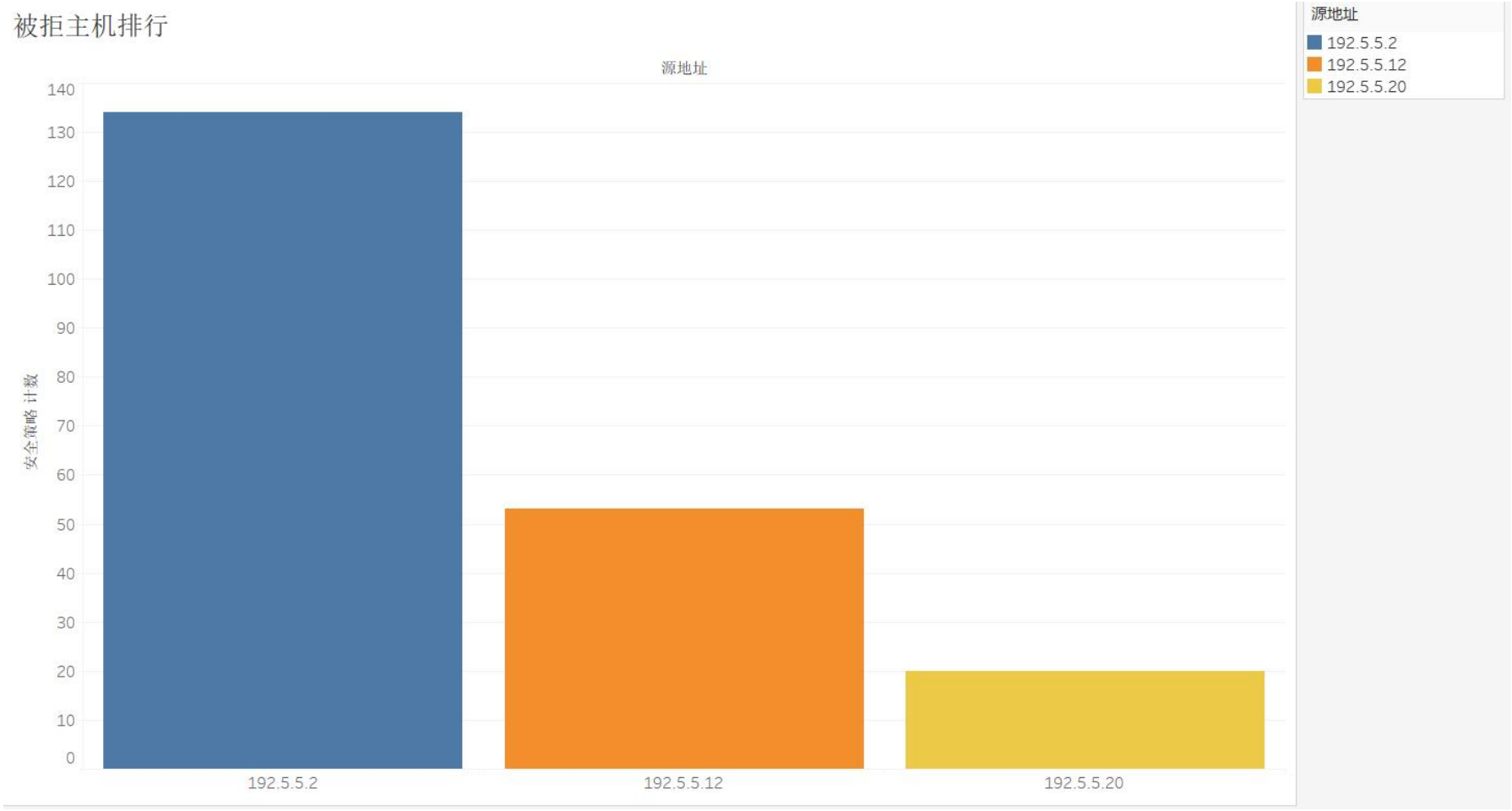
16：20-15：00

安全报表



16：20-15：00

被拒主机排行



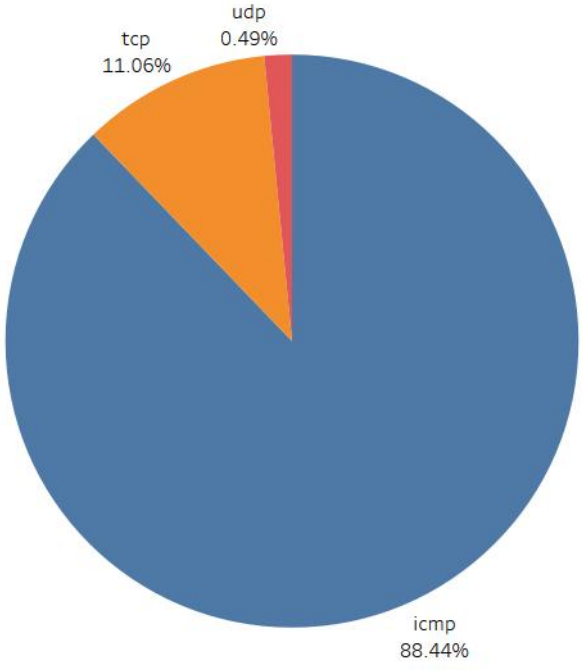
第四组

分析成果展示

Analysis of work difficulties

PART.02

分析成果展示



TCP类型报文

主要是在SSH连接的时候，产生的报文。
SSH在传输层使用的是TCP协议

ICMP类型报文

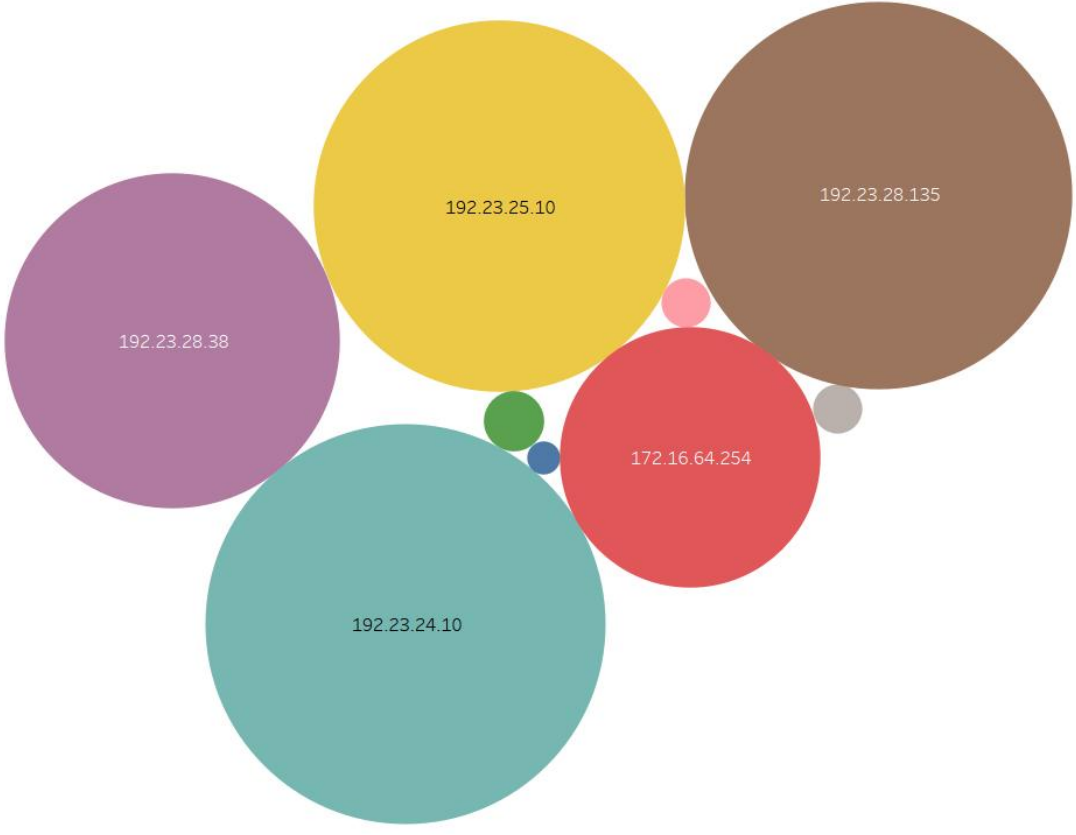
主要是主机ping外部的设备的，或者服务器产生的报文。

UDP类型报文

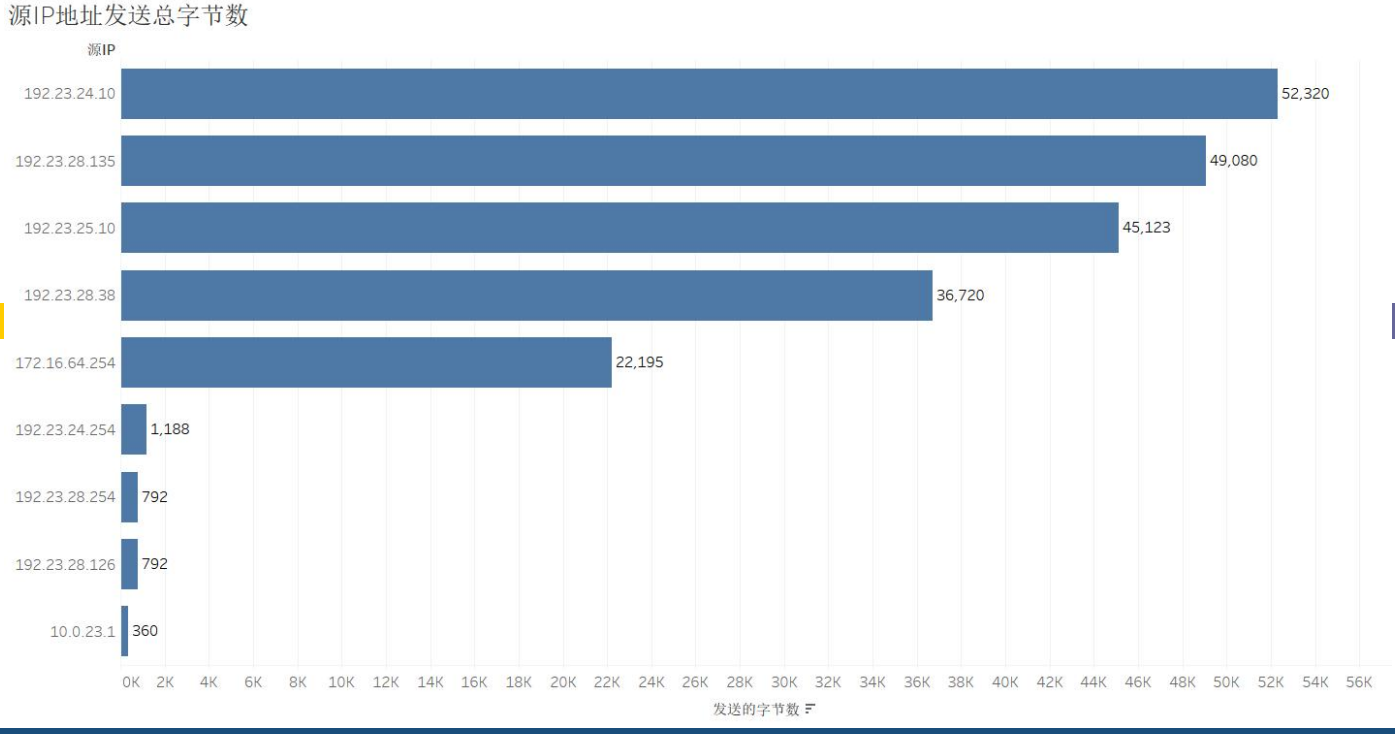
主要是获取IP地址时候的，产生的DHCP报文。
DHCP在传输层使用的是UDP协议。

分析成果展示

源IP地址发送总字节数



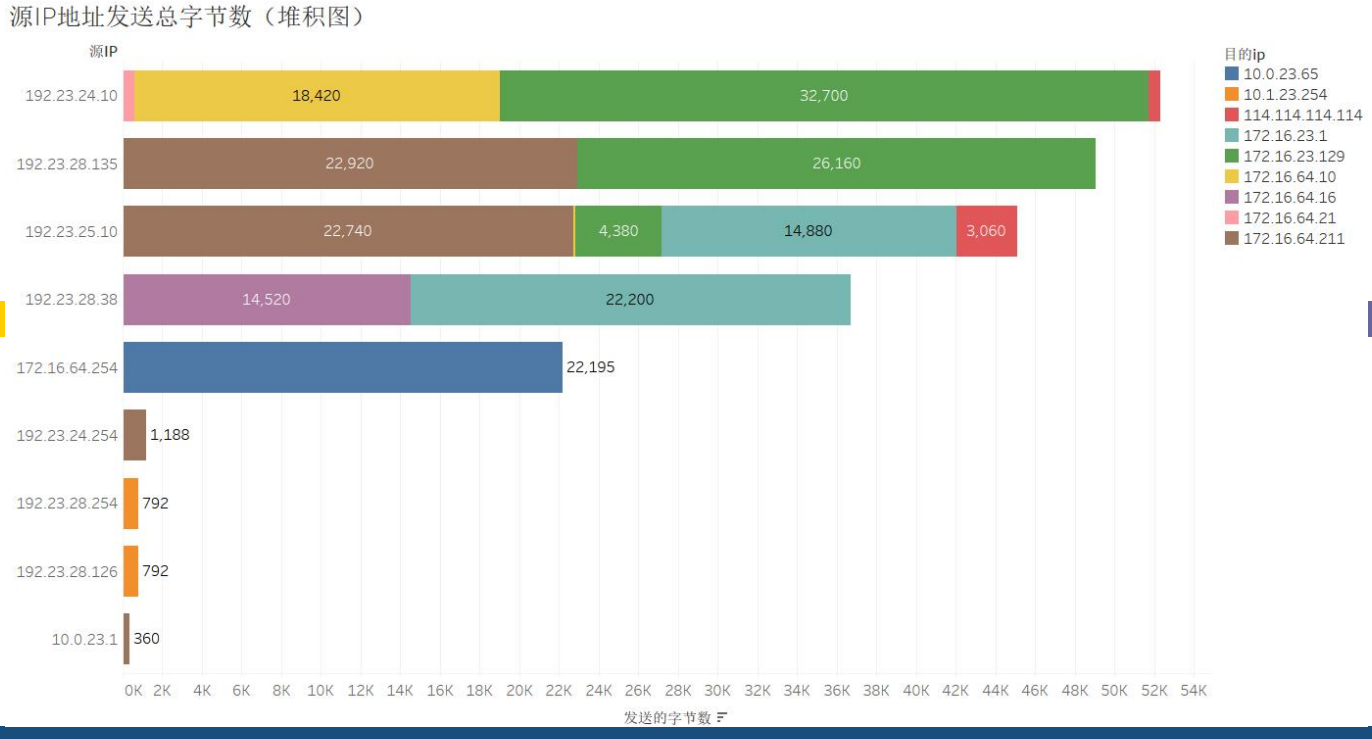
分析成果展示



源IP地址发送的总字节数-数据分析

通过上面的条形图，可以看到，192.23.24.10地址发送的字节的总数最多为52320字节，这个地址是主机A-C-1的地址。随后最多的是192.23.28.135，该地址是无线终端的Cellphone1，为49080字节，最少的是10.0.23.1，该地址是防火墙的GE1/0/1的地址，只有360字节。

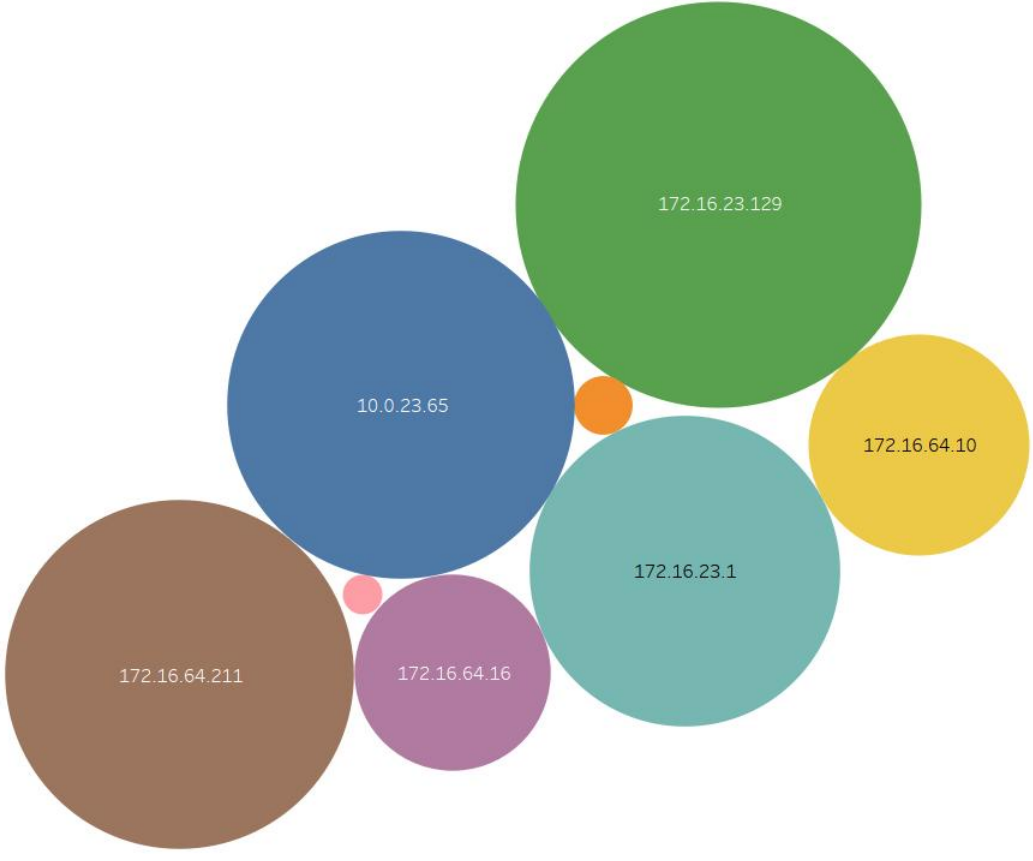
分析成果展示



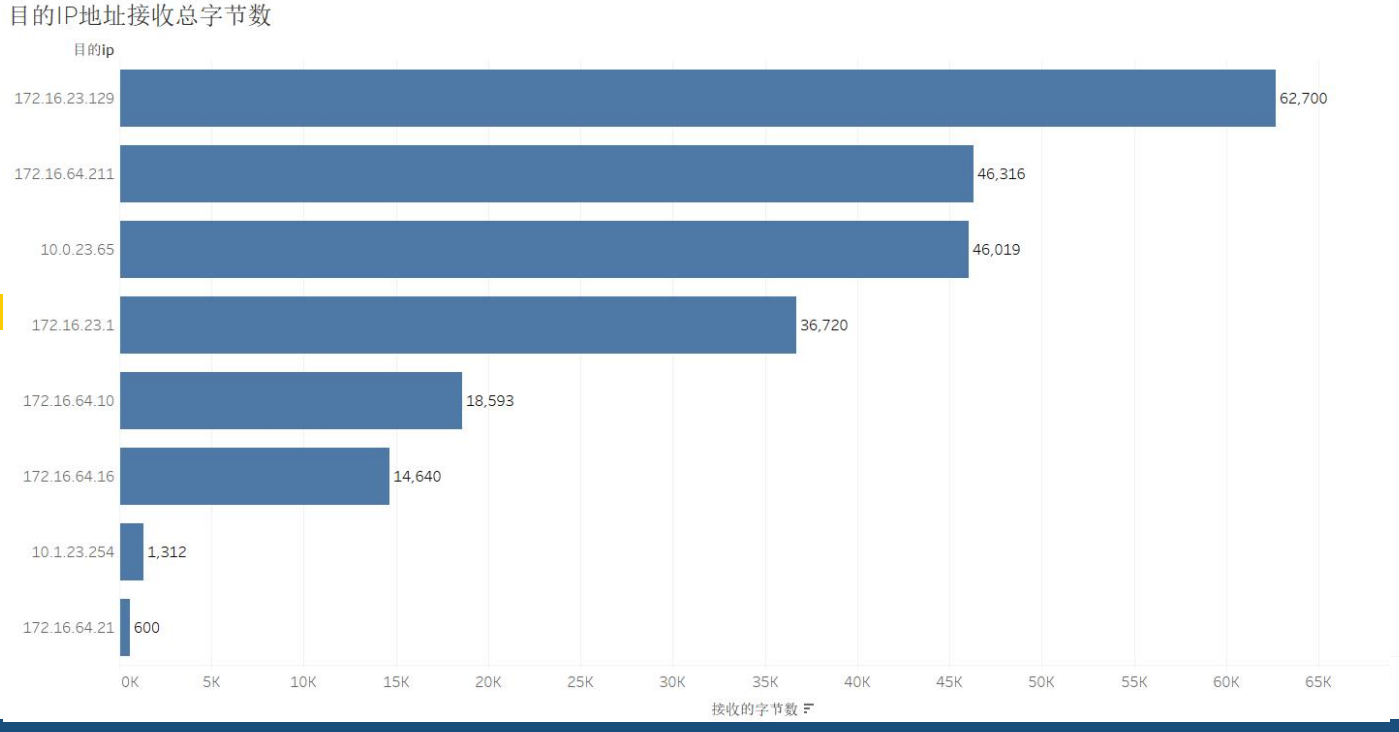
源IP地址发送的总字节数-数据分析

通过上面的条形图，可以看到，192.23.24.10地址发送的字节的总数最多，这个地址是主机A-C-1的地址，接收该地址发送最多的是172.16.23.129，接收了32700字节，该地址是服务器Server-2。随后最多的是192.23.28.135，接收最多的也是服务器Server-2，为26160字节，最少的是10.0.23.1，只给DHCP服务器发送过报文。

分析成果展示


目的ip
10.0.23.65
10.1.23.254
172.16.23.1
172.16.23.129
172.16.64.10
172.16.64.16
172.16.64.21
172.16.64.211
172.16.23.129
10.0.23.65
172.16.64.10
172.16.23.1
172.16.64.211
172.16.64.16

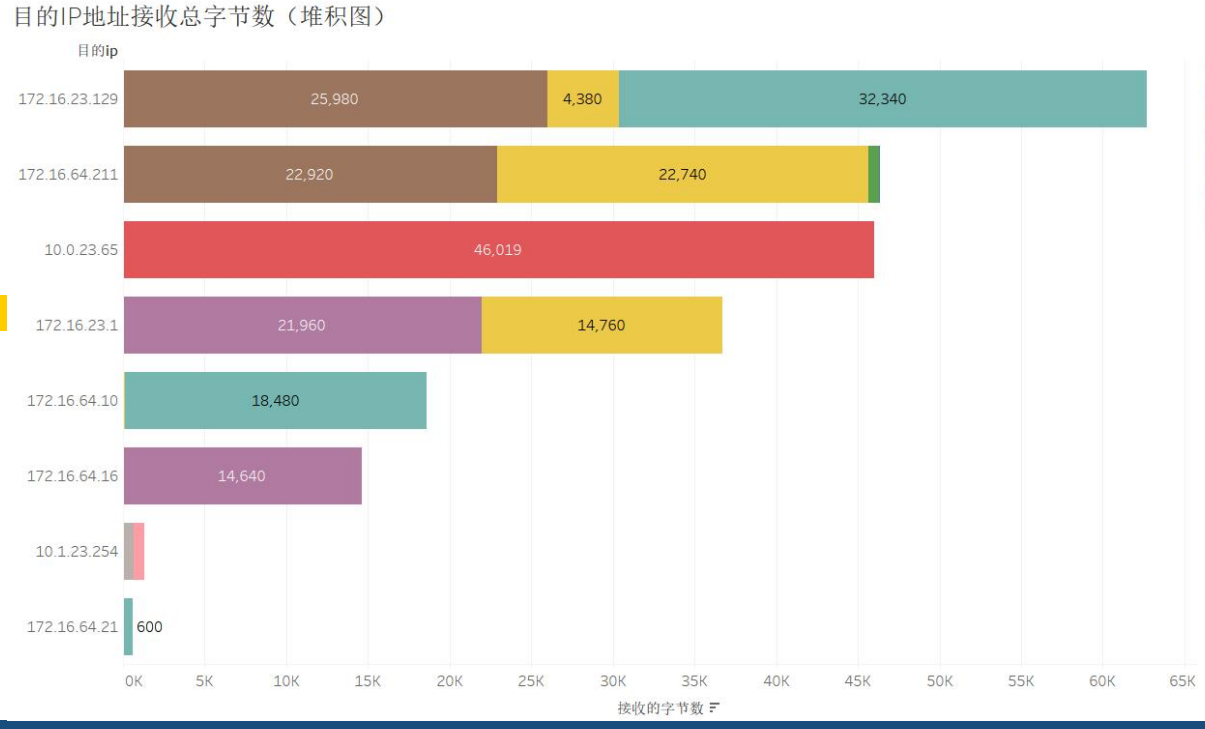
分析成果展示



目的IP地址接收的总字节数-数据分析

通过上面的条形图，可以看到，172.16.23.129地址接收的字节的总数最多，这个地址是服务器Server-2的地址。随后最多的是172.16.64.211，该地址是DHCP服务器，与其接近的是10.0.23.65，是A-RS-1的lookback地址，最少的是172.16.64.21是syslog服务器地址。

分析成果展示

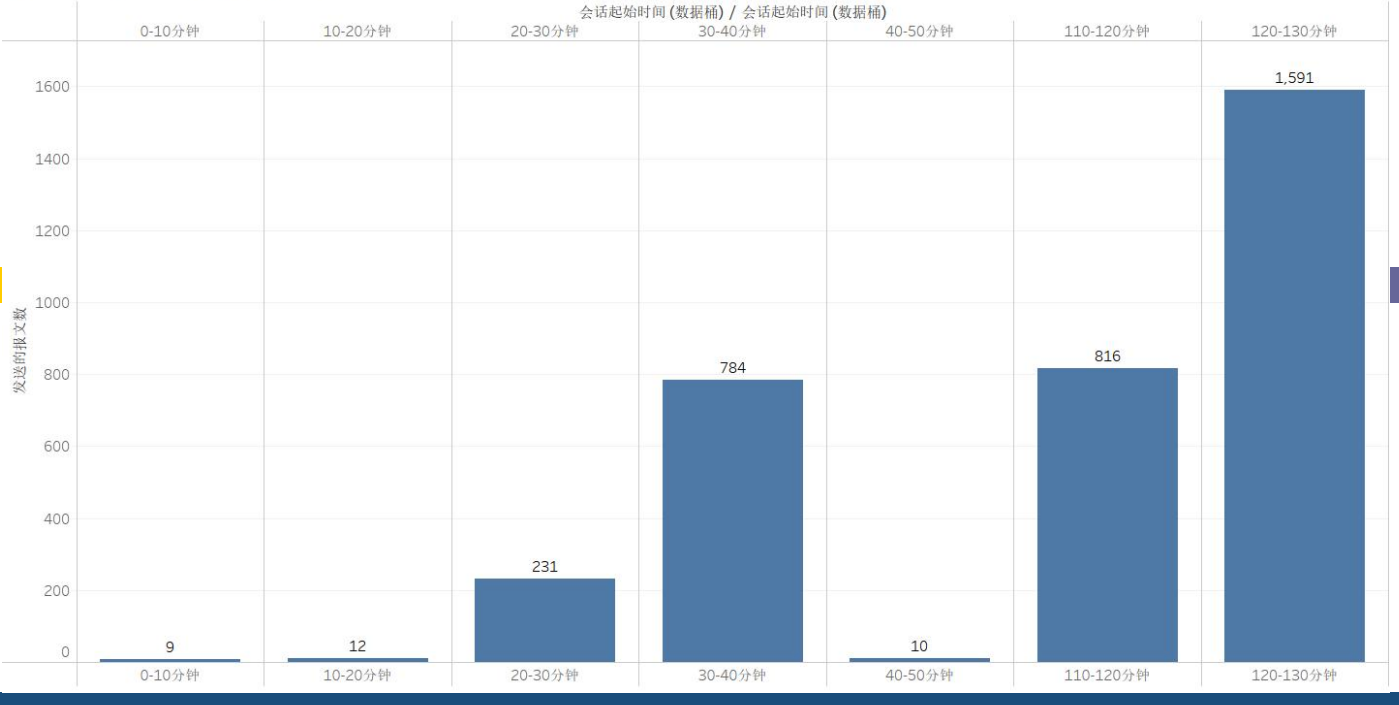


目的IP地址接收的总字节数-数据分析

通过上面的条形图，可以看到，172.16.23.129地址接收的字节的总数最多，接收192.23.24.10地址发送的最多。随后最多的是172.16.64.211，DHCP服务器，接收192.23.28.135地址发送的最多，与其接近的是10.0.23.65是Lookback口地址，接收的172.16.64.254地址发送的最多。

分析成果展示

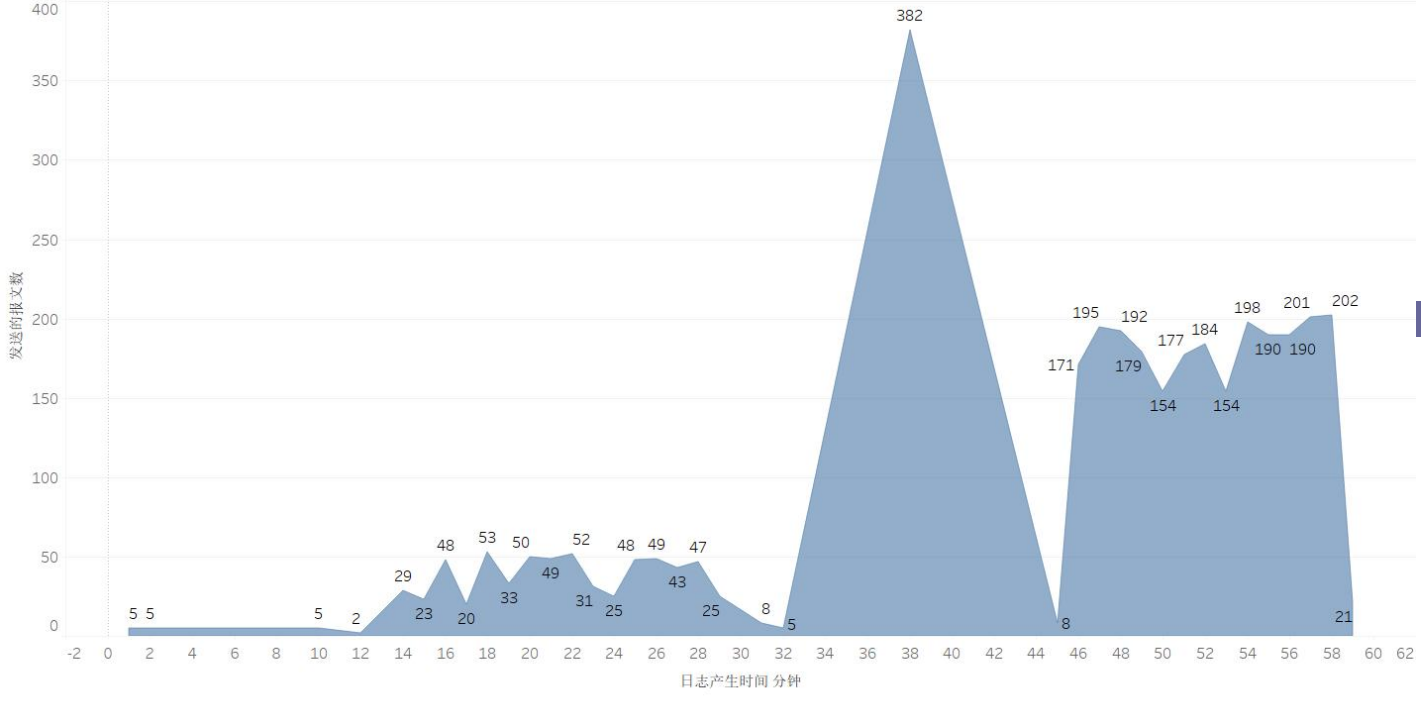
单位时间内经过防火墙的报文数



单位时间内经过防火墙的报文数（2小时）

可以看到在单位时间内经过防火墙的报文数，其中经过报文数最多的是在120-130分钟，在这10分钟，防火墙记录了1591条的数据。

分析成果展示



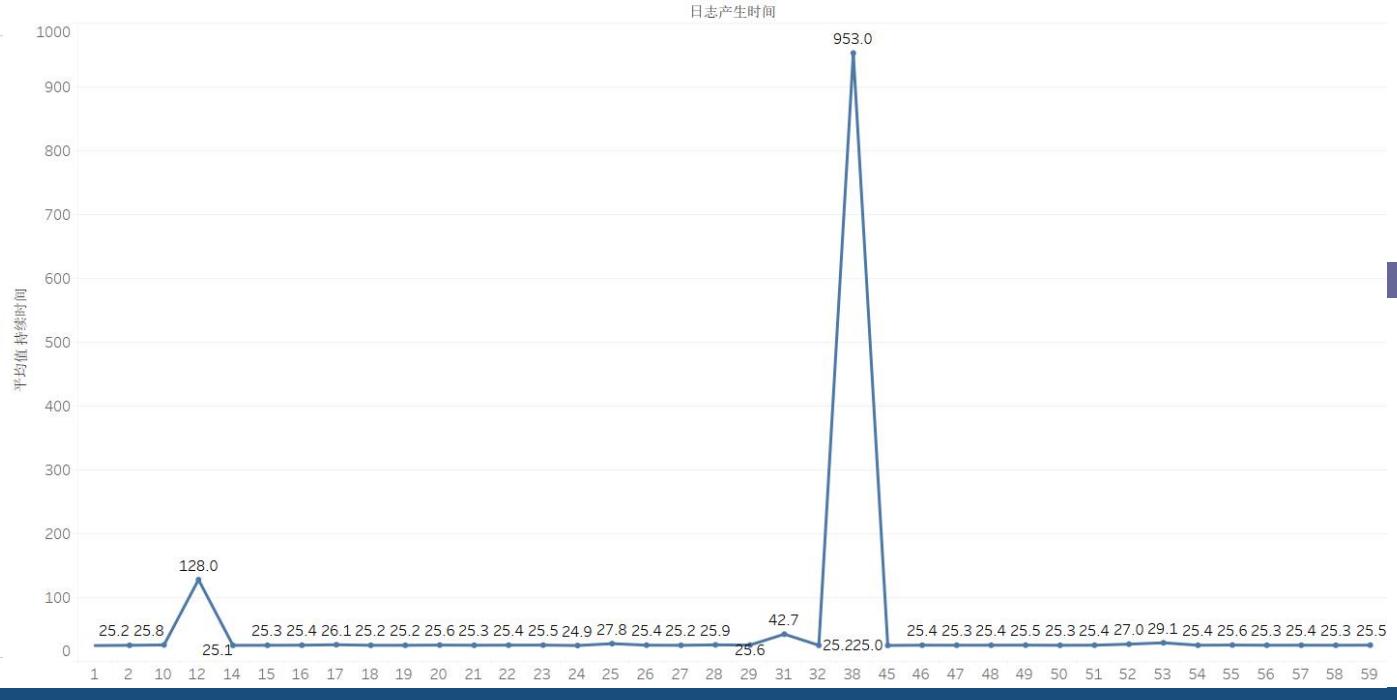
日志产生时间 分钟 的 发送的报文数 总和 的绘图。标记按 发送的报文数 总和 进行标记。

单位时间内发送的报文数（60分钟）

在60分钟内，在38分钟的时候，经过防火墙的报文数最多，最多经过了382条报文。

分析成果展示

60分钟内的平均持续时长

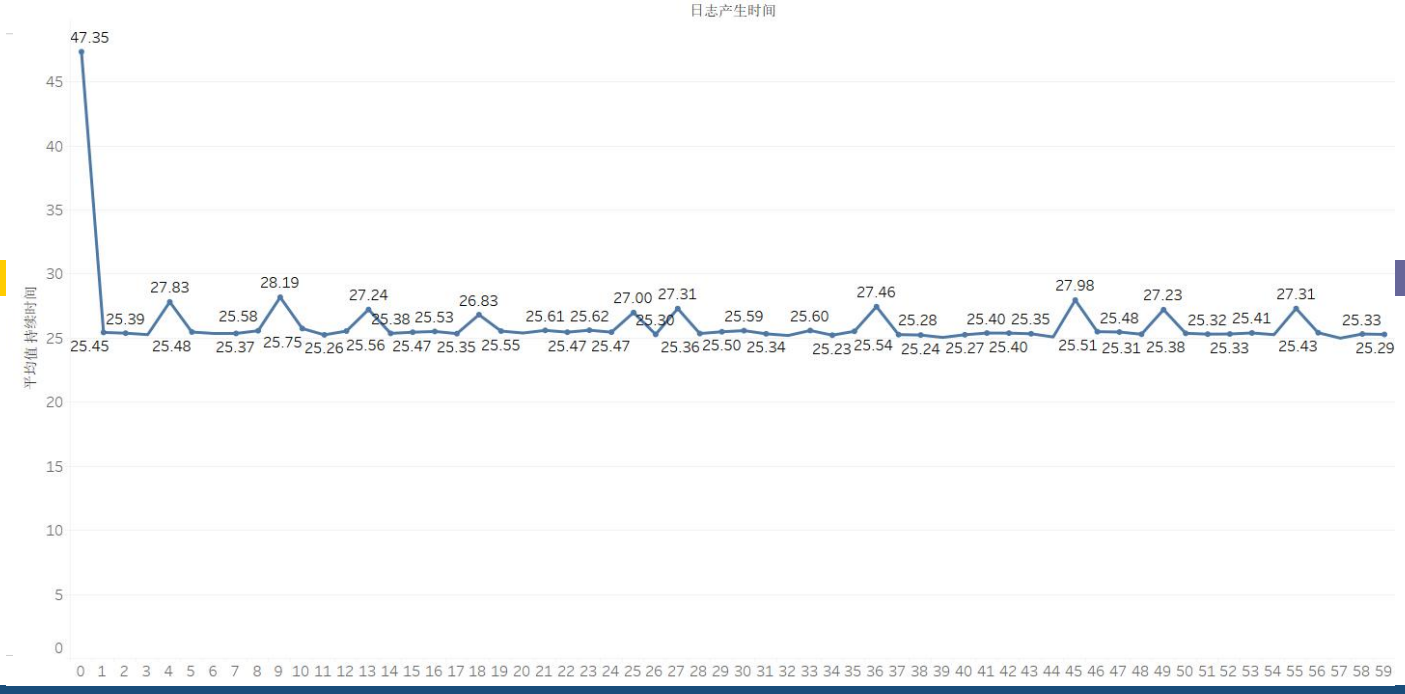


单位时间内报文会话持续时长（60分钟）

60分钟内报文平均发送时长，可以看到总体上每条报文发送的时长是平稳的，因为大多数是ICMP报文，只有在38分钟的时候，发送的平均持续时长有明显的增高。

分析成果展示

1分钟内的平均会话时长



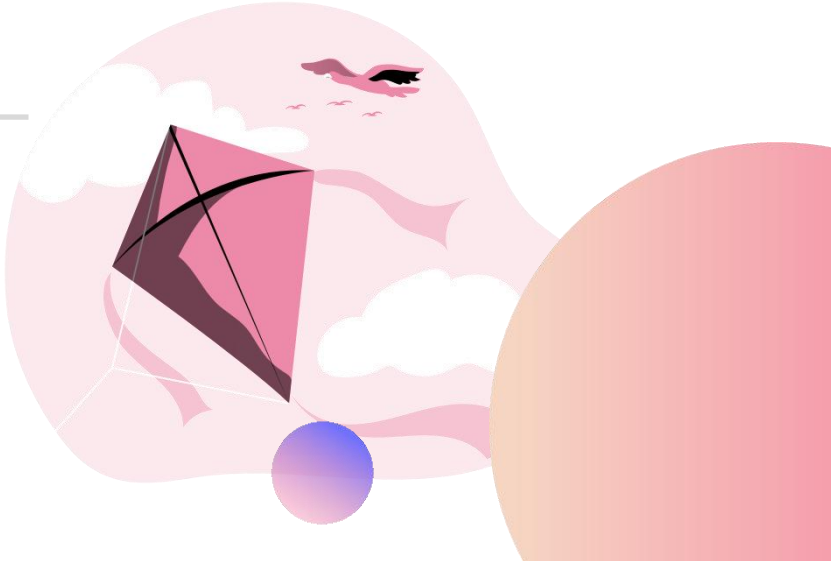
单位时间内平均会话时长（1分钟）

可以看到在1分钟内的平均时长，是平稳的，只有在最开的时候访问时长比较长，是因为在最开始有访问服务器的报文经过。

第五组

成果展示

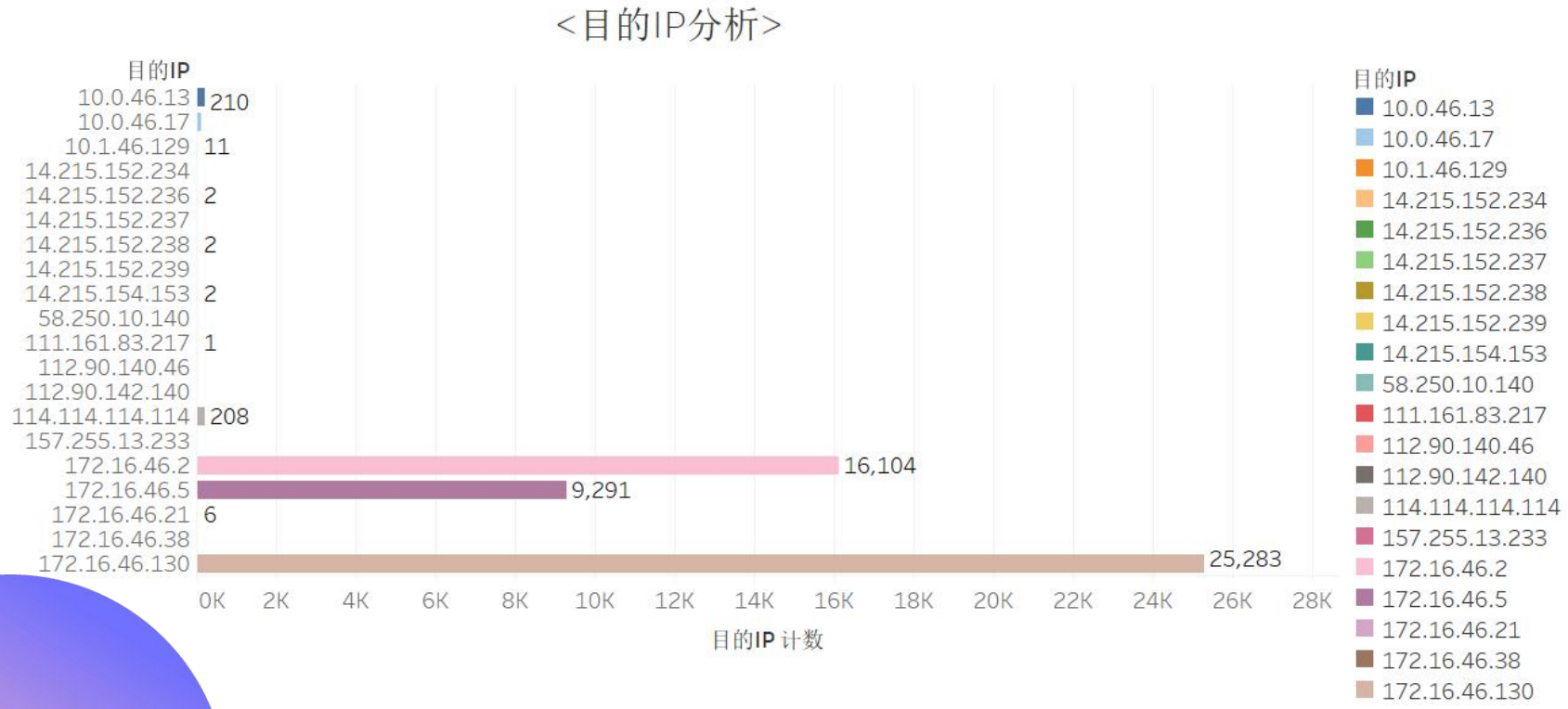
Achievement display



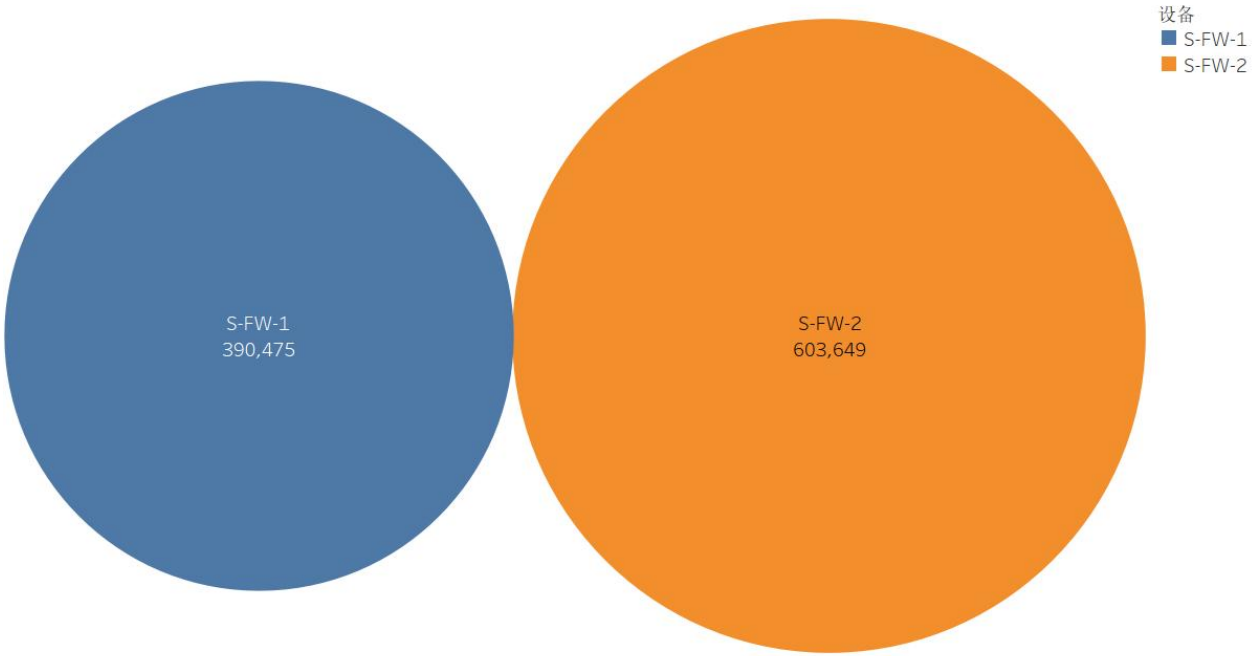
1、旁挂防火墙流量分析

2、有线与无线网络稳定性分析

旁挂防火墙流量分析


<目的IP分析>
目的IP
10.0.46.13
10.0.46.17
10.1.46.129
14.215.152.234
14.215.152.236
14.215.152.237
14.215.152.238
14.215.152.239
14.215.154.153
58.250.10.140
111.161.83.217
112.90.140.46
112.90.142.140
114.114.114.114
157.255.13.233
172.16.46.2
172.16.46.5
172.16.46.21
172.16.46.38
172.16.46.130
210
11
2
2
2
1
208
16,104
9,291
6
25,283
0K
2K
4K
6K
8K
10K
12K
14K
16K
18K
20K
22K
24K
26K
28K
目的IP 计数
目的IP
10.0.46.13
10.0.46.17
10.1.46.129
14.215.152.234
14.215.152.236
14.215.152.237
14.215.152.238
14.215.152.239
14.215.154.153
58.250.10.140
111.161.83.217
112.90.140.46
112.90.142.140
114.114.114.114
157.255.13.233
172.16.46.2
172.16.46.5
172.16.46.21
172.16.46.38
172.16.46.130

<防火墙流量比较>

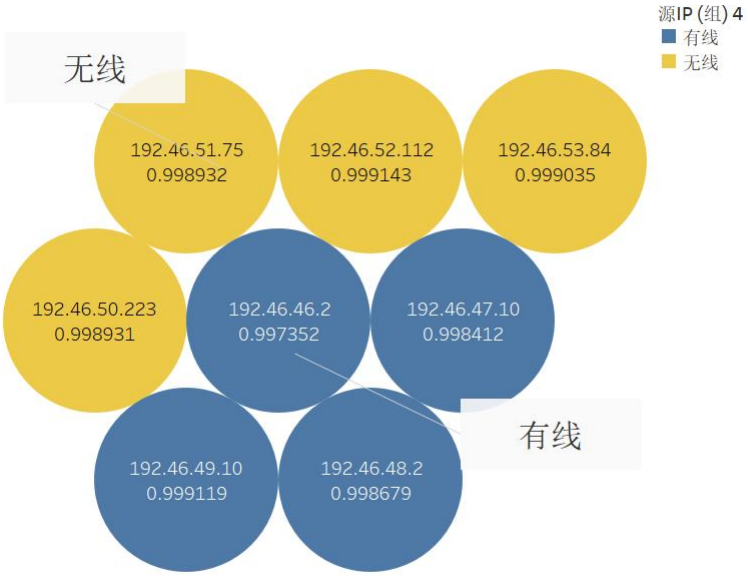


<防火墙流量比较>

设备	
S-FW-1	390,475
S-FW-2	603,649

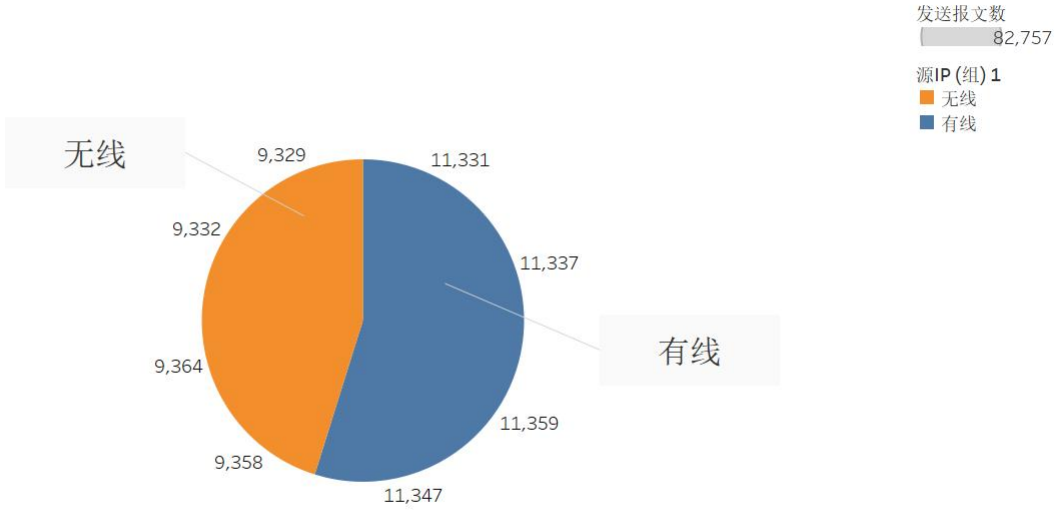
有线与无线网络稳定性分析

<报文接收率>



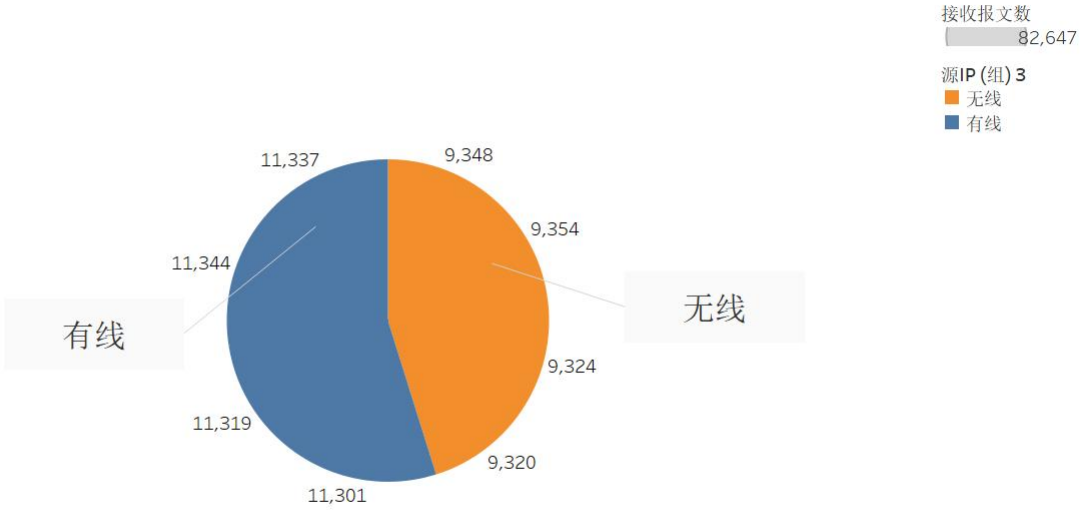
源IP	SUM([接收报文数])/SUM([发送报文数])
192.46.46.2	0.997352
192.46.47.10	0.998412
192.46.48.2	0.998679
192.46.49.10	0.999119
192.46.50.223	0.998931
192.46.51.75	0.998932
192.46.52.112	0.999143
192.46.53.84	0.999035

<发送报文数>



源IP	源IP (组) 1 无线	有线
192.46.46.2		11,331
192.46.47.10		11,337
192.46.48.2		11,359
192.46.49.10		11,347
192.46.50.223	9,358	
192.46.51.75	9,364	
192.46.52.112	9,332	
192.46.53.84	9,329	

<接收报文数量>



源IP	源IP (组) 2 无线	有线
192.46.46.2		11,301
192.46.47.10		11,319
192.46.48.2		11,344
192.46.49.10		11,337
192.46.50.223	9,348	
192.46.51.75	9,354	
192.46.52.112	9,324	
192.46.53.84	9,320	

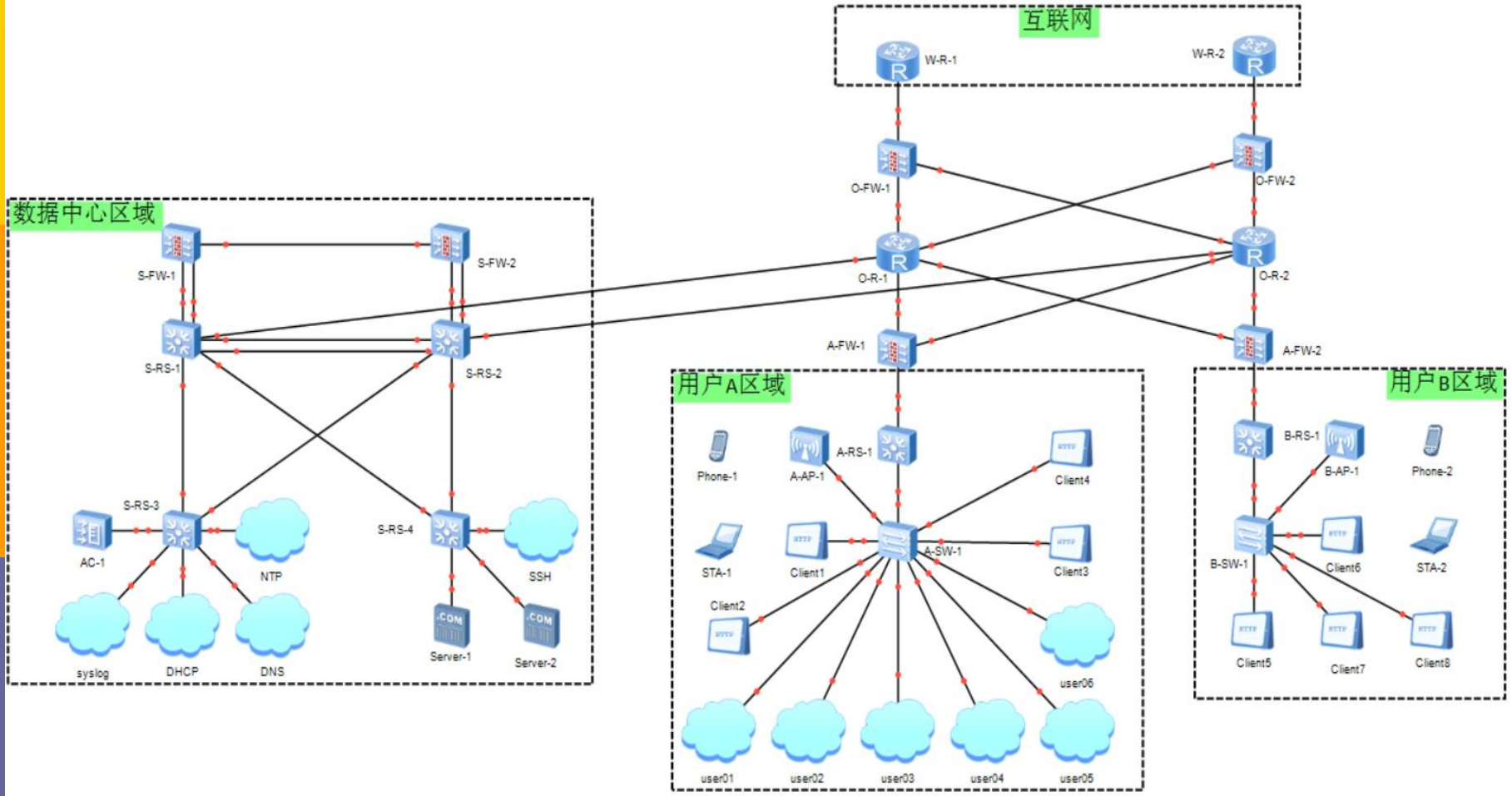
第六组

日志分析
Log analysis

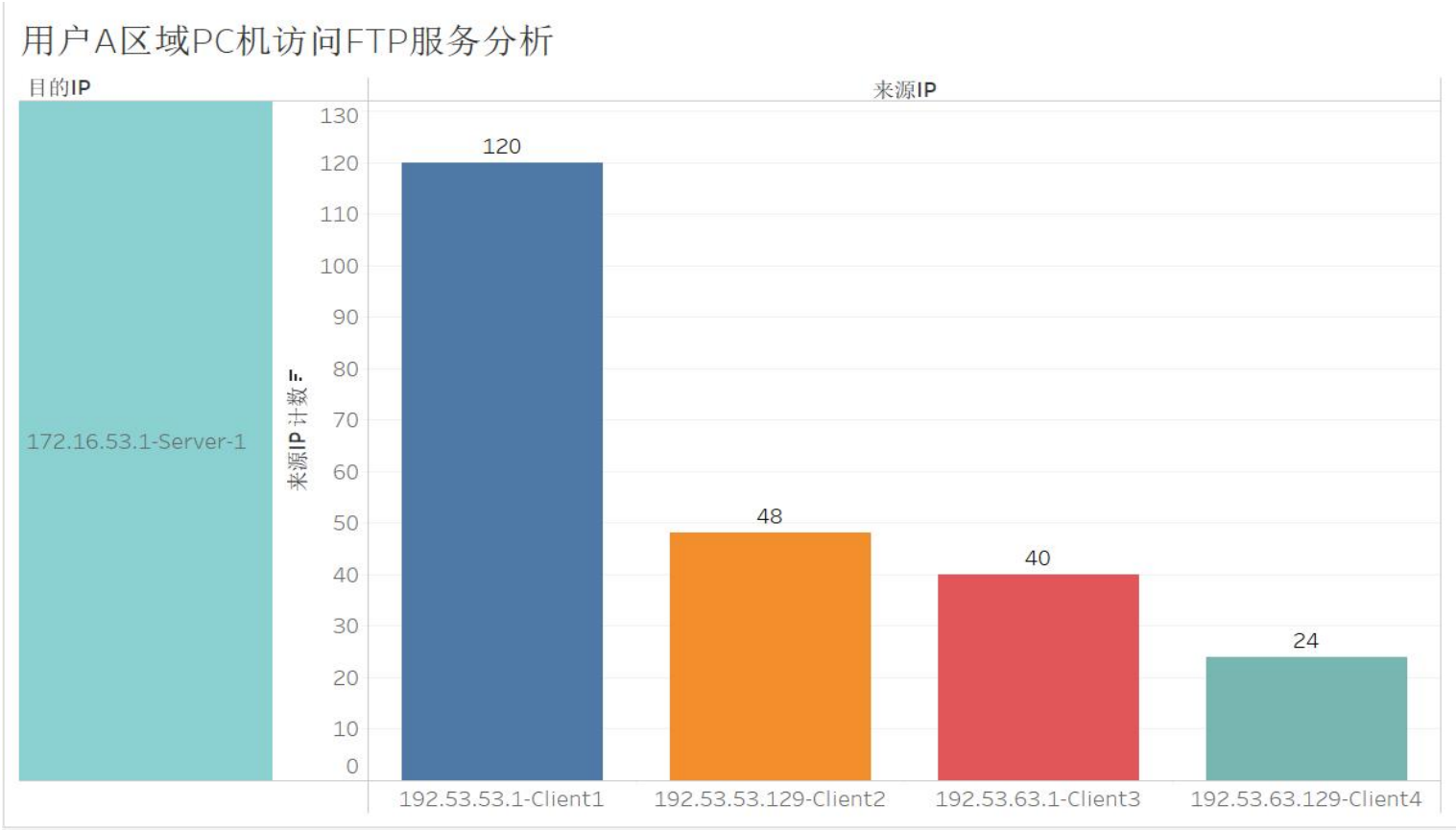
01 PC机访问FTP/Web服务

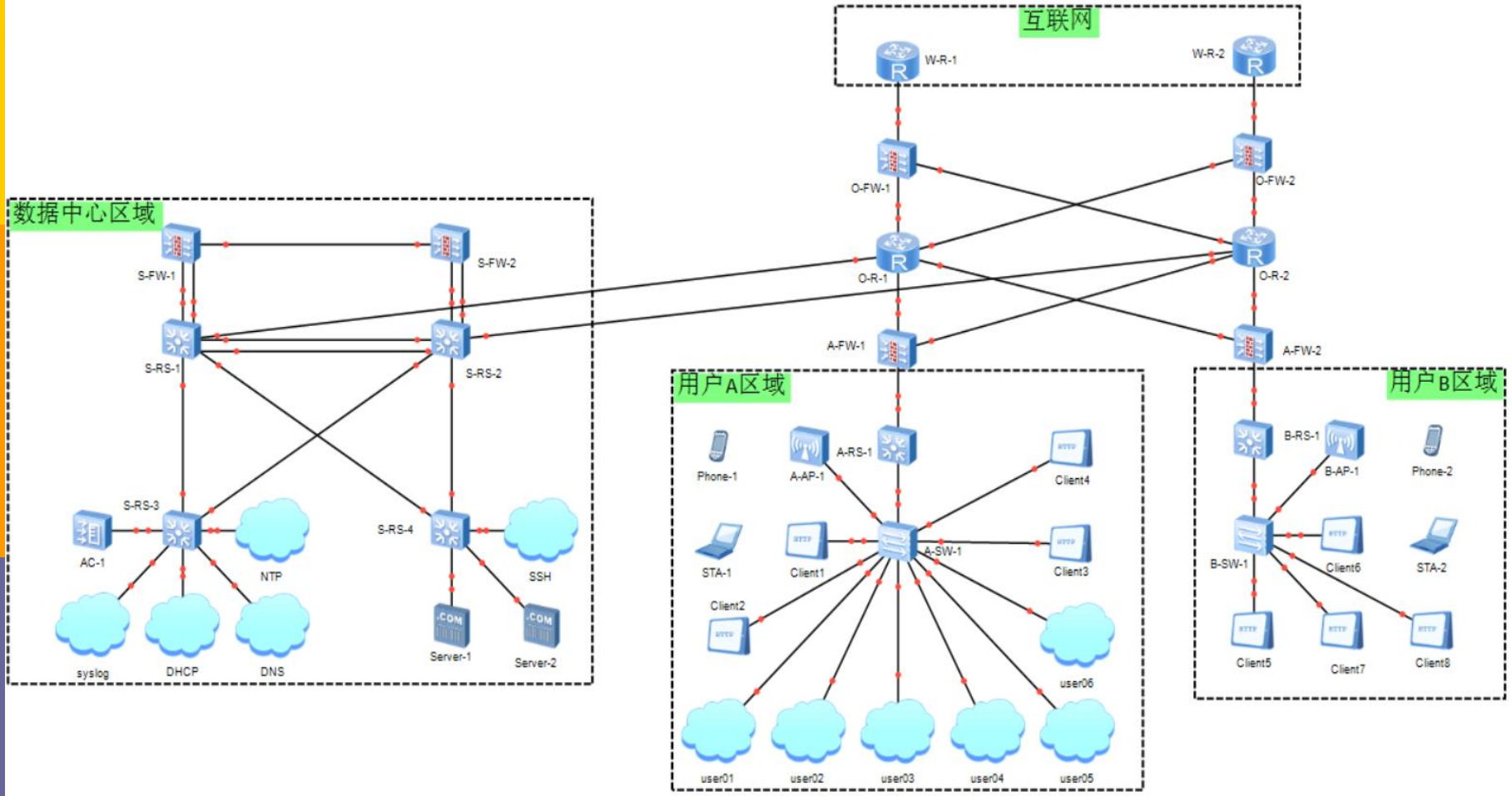
02 本地不同用户上网频率

03 有线、无线访问互联网

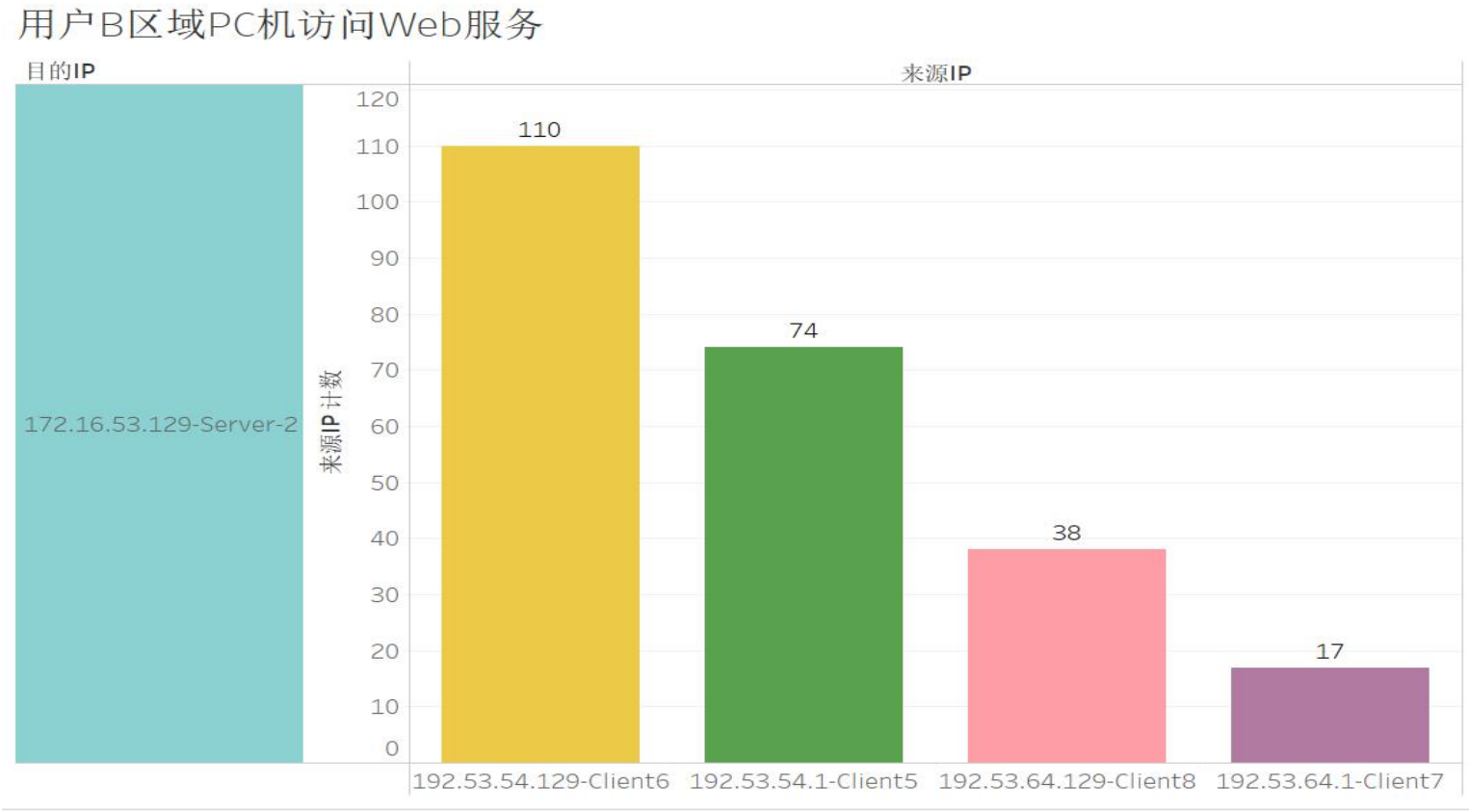

互联网
W-R-1
W-R-2
O-FW-1
O-FW-2
O-R-1
O-R-2
A-FW-1
A-FW-2
数据中心区域
S-FW-1
S-FW-2
S-RS-1
S-RS-2
S-RS-3
S-RS-4
AC-1
NTP
SSH
syslog
DHCP
DNS
Server-1
Server-2
用户A区域
Phone-1
A-AP-1
A-RS-1
Client4
STA-1
Client1
A-SW-1
Client3
Client2
user06
user01
user02
user03
user04
user05
用户B区域
B-RS-1
B-AP-1
Phone-2
B-SW-1
Client6
STA-2
Client5
Client7
Client8

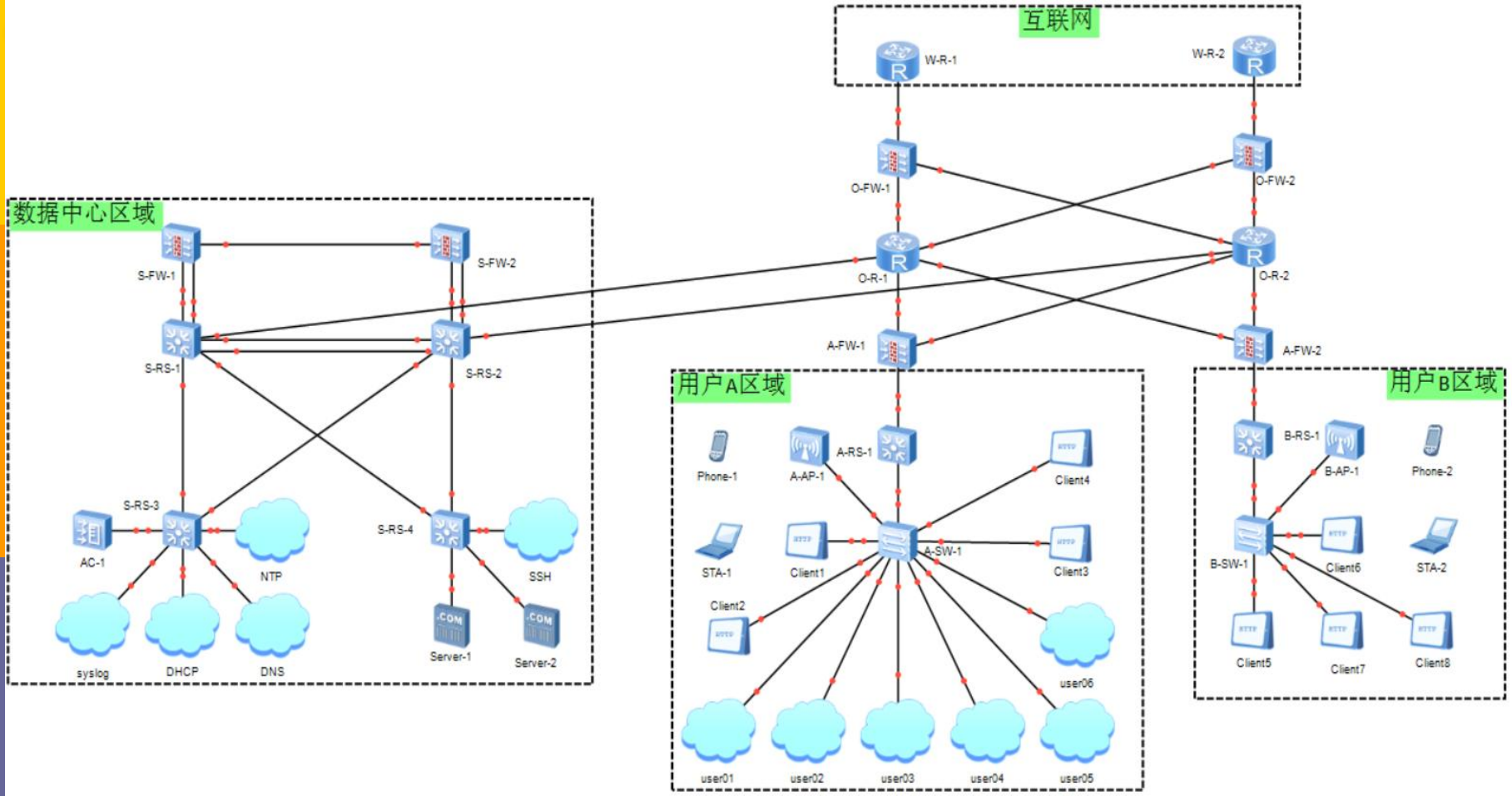
04 用户A区域PC机访问FTP服务




互联网
W-R-1
W-R-2
O-FW-1
O-FW-2
O-R-1
O-R-2
A-FW-1
A-FW-2
数据中心区域
S-FW-1
S-FW-2
S-RS-1
S-RS-2
S-RS-3
S-RS-4
AC-1
NTP
SSH
syslog
DHCP
DNS
Server-1
Server-2
用户A区域
Phone-1
A-AP-1
A-RS-1
Client4
STA-1
Client1
A-SW-1
Client3
Client2
user06
user01
user02
user03
user04
user05
用户B区域
B-RS-1
B-AP-1
Phone-2
B-SW-1
Client6
STA-2
Client5
Client7
Client8

04 用户B区域PC机访问Web服务

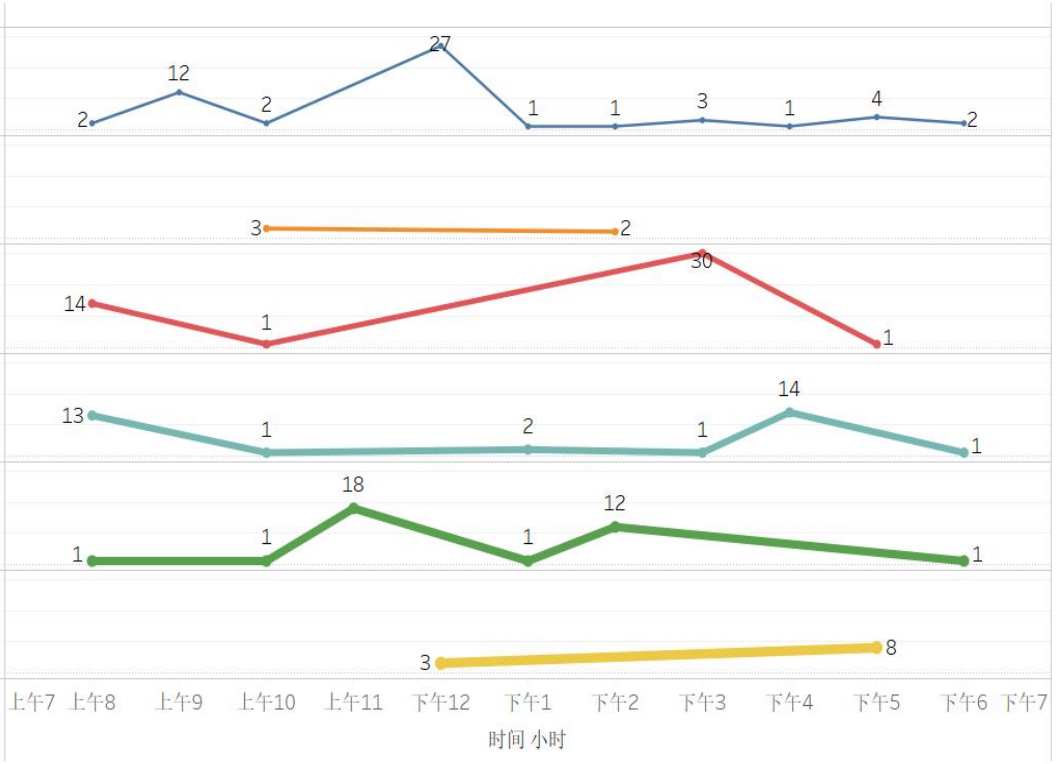


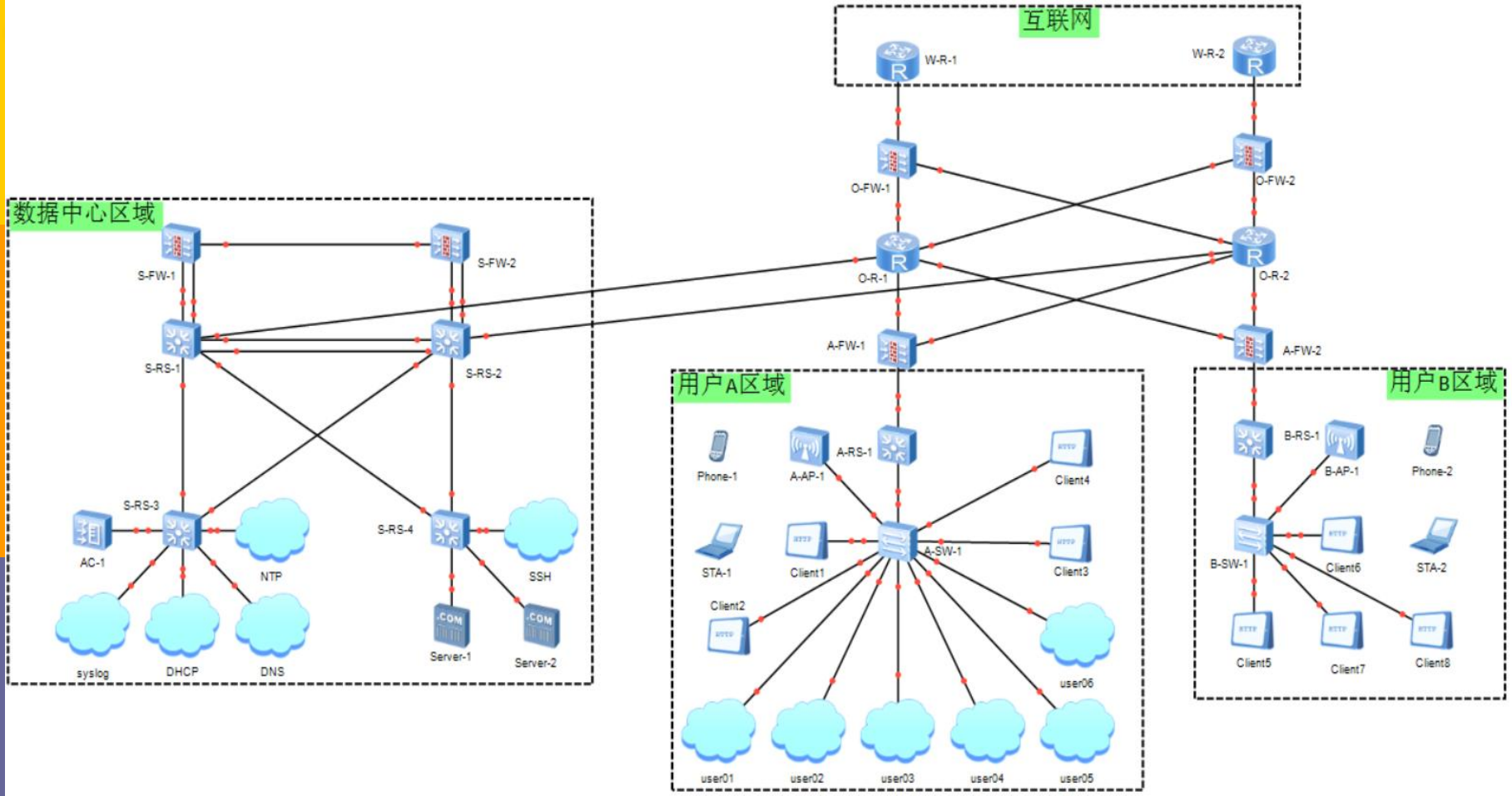

互联网
W-R-1
W-R-2
O-FW-1
O-FW-2
O-R-1
O-R-2
A-FW-1
A-FW-2
数据中心区域
S-FW-1
S-FW-2
S-RS-1
S-RS-2
S-RS-3
S-RS-4
AC-1
NTP
SSH
syslog
DHCP
DNS
Server-1
Server-2
用户A区域
Phone-1
A-AP-1
A-RS-1
Client4
STA-1
Client1
A-SW-1
Client3
Client2
user06
user01
user02
user03
user04
user05
用户B区域
B-RS-1
B-AP-1
Phone-2
B-SW-1
Client6
STA-2
Client5
Client7
Client8

04 12月12日 本地不同用户不同时间段上网频率

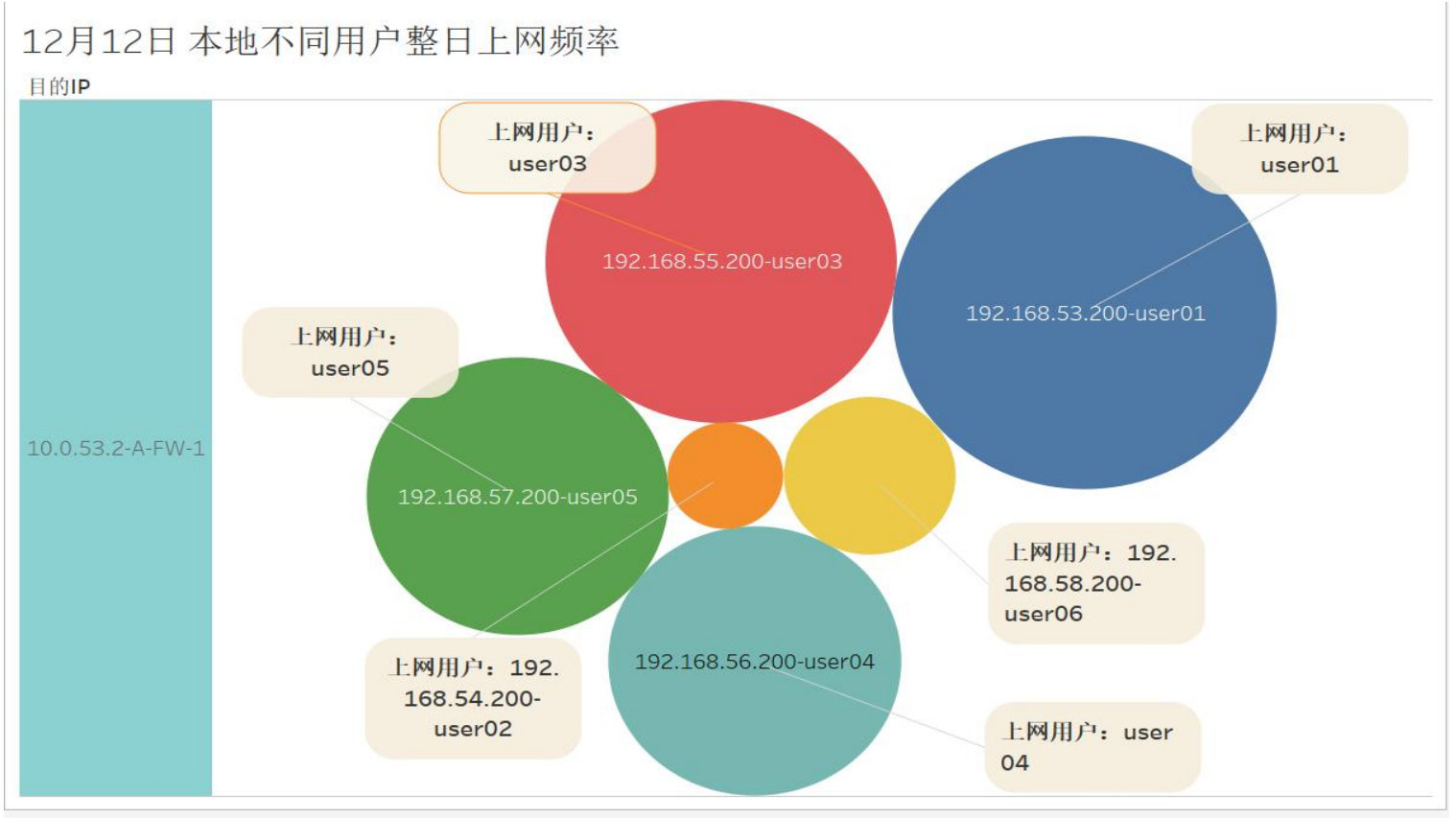
12月12日 本地不同用户不同时间段上网频率

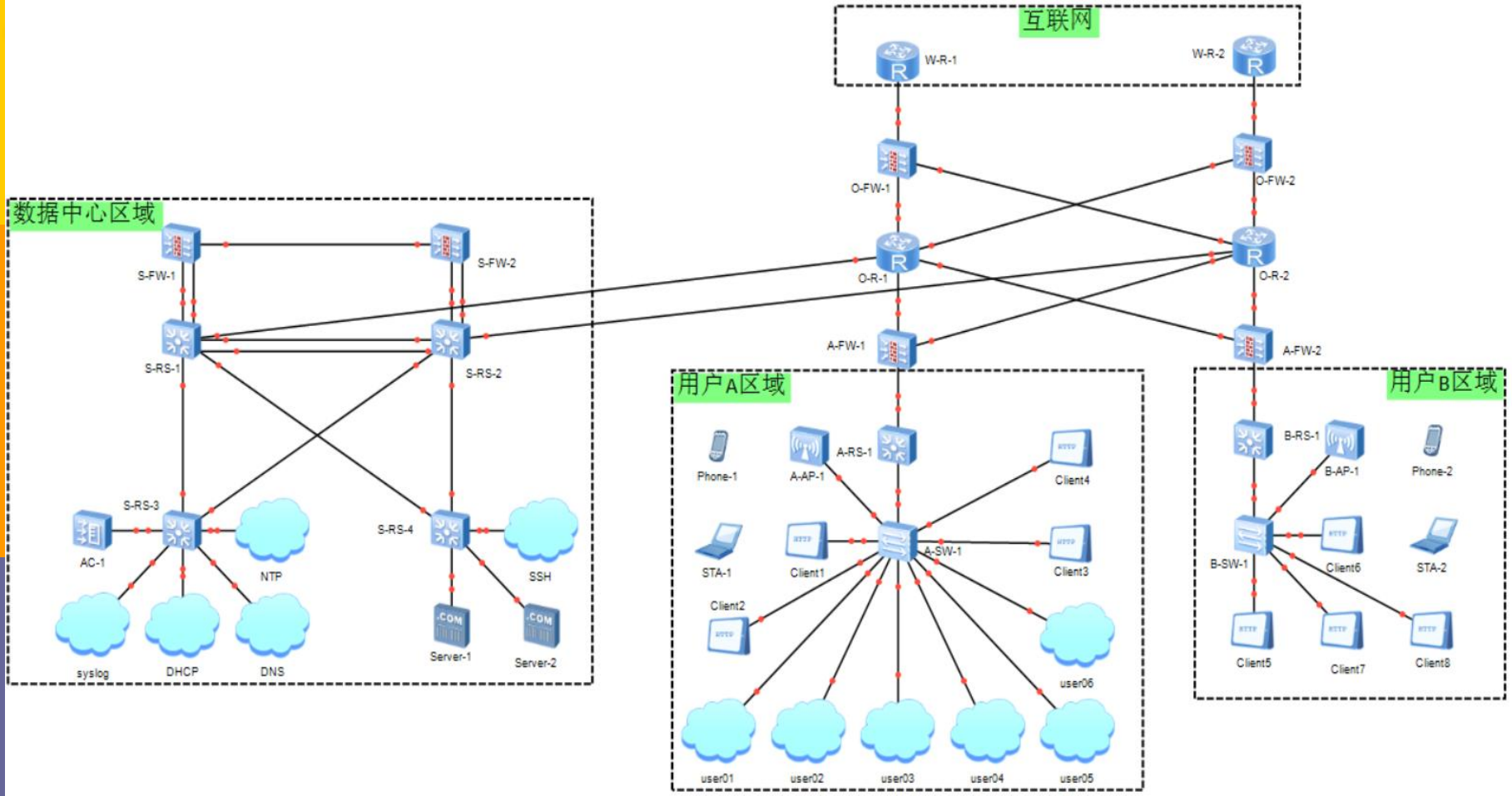
来源IP	目的IP
192.168.53.200-user01	10.0.53.2-A-FW-1
192.168.54.200-user02	10.0.53.2-A-FW-1
192.168.55.200-user03	10.0.53.2-A-FW-1
192.168.56.200-user04	10.0.53.2-A-FW-1
192.168.57.200-user05	10.0.53.2-A-FW-1
192.168.58.200-user06	10.0.53.2-A-FW-1



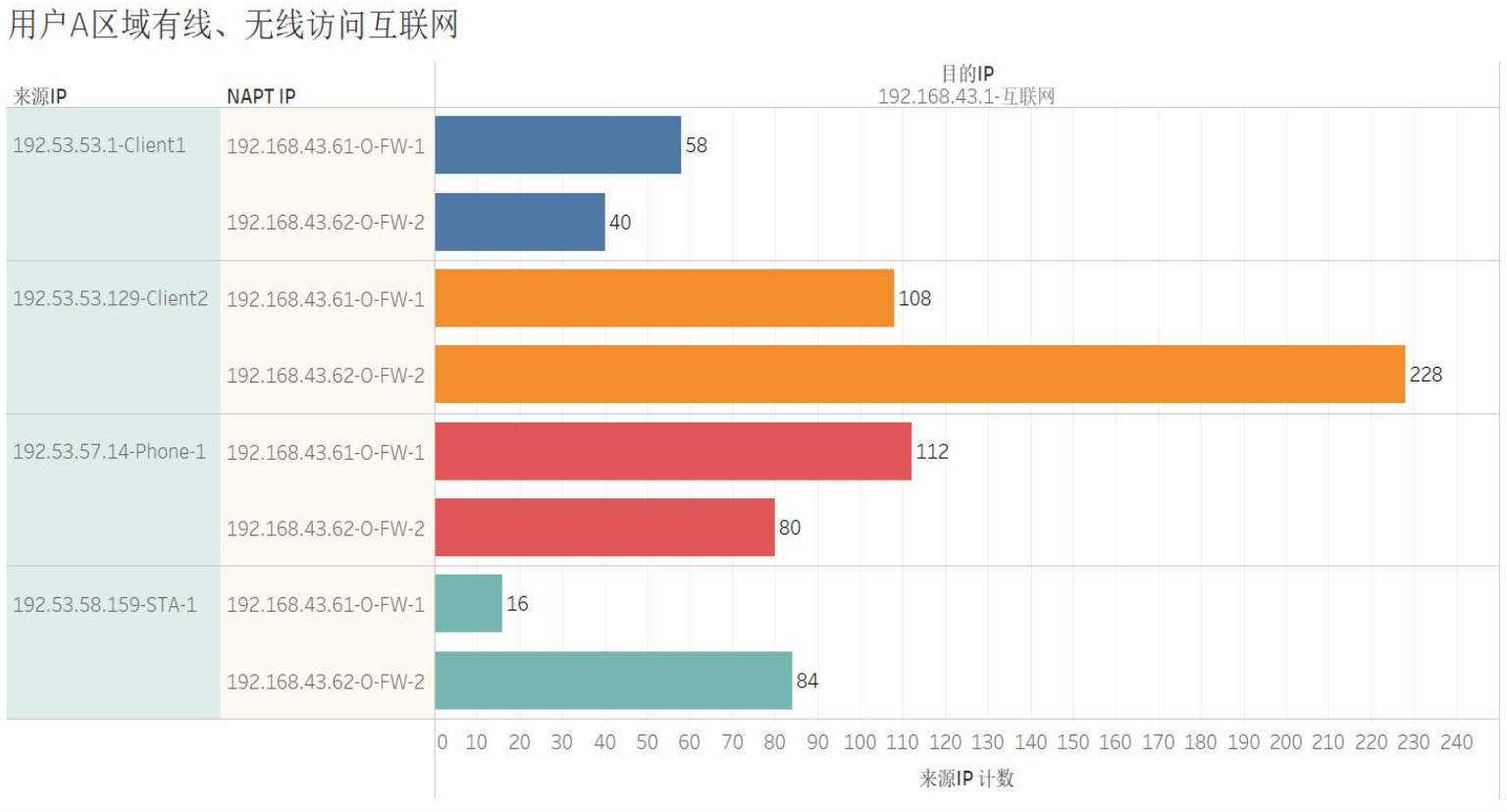

互联网
W-R-1
W-R-2
O-FW-1
O-FW-2
O-R-1
O-R-2
A-FW-1
A-FW-2
数据中心区域
S-FW-1
S-FW-2
S-RS-1
S-RS-2
S-RS-3
S-RS-4
AC-1
NTP
SSH
syslog
DHCP
DNS
Server-1
Server-2
用户A区域
Phone-1
A-AP-1
A-RS-1
Client4
STA-1
Client1
A-SW-1
Client3
Client2
user06
user01
user02
user03
user04
user05
用户B区域
B-RS-1
B-AP-1
Phone-2
B-SW-1
Client6
STA-2
Client5
Client7
Client8

04 12月12日 本地不同用户整日上网频率




互联网
W-R-1
W-R-2
O-FW-1
O-FW-2
O-R-1
O-R-2
A-FW-1
A-FW-2
数据中心区域
S-FW-1
S-FW-2
S-RS-1
S-RS-2
S-RS-3
S-RS-4
AC-1
NTP
SSH
syslog
DHCP
DNS
Server-1
Server-2
用户A区域
Phone-1
A-AP-1
A-RS-1
Client4
STA-1
Client1
A-SW-1
Client3
Client2
user06
user01
user02
user03
user04
user05
用户B区域
B-RS-1
B-AP-1
Phone-2
B-SW-1
Client6
STA-2
Client5
Client7
Client8

04 用户A区域有线、无线访问互联网



第九讲 用户行为管理

完