任务背景

某创业公司刚刚起步，随着业务量的增多，咨询和投诉的用户也越来越多，公司的客服部门由原来的2个增加到5个。客服部门平时需要处理大量的用户反馈，不管是邮件，还是ＱＱ，还是电话，客服人员都会针对每一次的用户反馈做详细的记录，但是由于客观原因，客服人员没有成熟稳定的客户服务系统，所以希望运维部门能够提供一个可以通过浏览器查看并下载的方式来管理这些文档，并且随时跟踪客户的反馈情况。

任务要求

1. 客服人员必须使用用户名密码(kefu/123)的方式登录服务器来下载相应文档。
2. 不允许匿名用户访问
3. 客服部门的相关文档保存在指定的目录里/data/kefu
4. 客服用户使用用户kefu/123登录后就只能在默认的/data/kefu目录里活动

课程目标

- 了解FTP服务的工作模式
- 能够禁止FTP服务匿名用户登录
- 能够禁锢FTP服务本地用户的家目录
- 能够指定FTP服务本地用户和匿名用户的默认数据目录

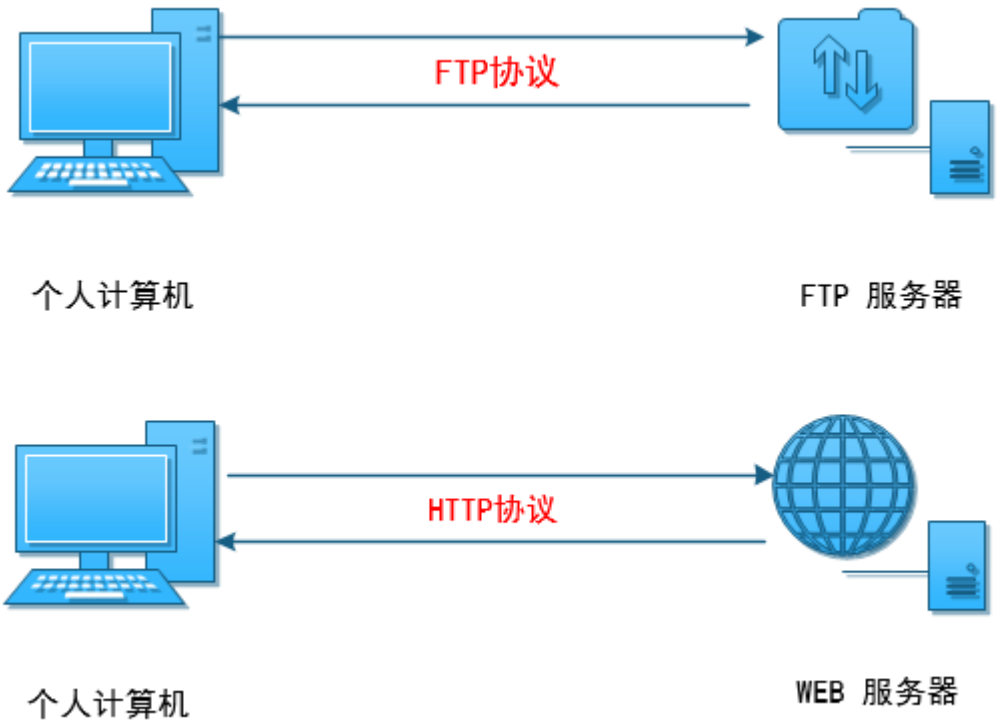
涉及知识点

- FTP服务的搭建（掌握）
- FTP服务的基本配置（**重点**）

理论储备

一、FTP服务介绍

FTP（File Transfer Protocol）是一种应用非常广泛并且古老的一个互联网文件传输协议。



- 主要用于互联网中文件的双向传输（上传/下载）、文件共享
- 跨平台 Linux、Windows
- FTP是C/S架构，拥有一个客户端和服务端，使用TCP协议作为底层传输协议，提供可靠的数据传输
- FTP的默认端口 21号（命令端口） 20号（数据端口，主动模式下） **默认被动模式**下
- FTP程序（软件）vsftpd

二、FTP服务的客户端工具

> Linux：ftp、lftp（客户端程序）

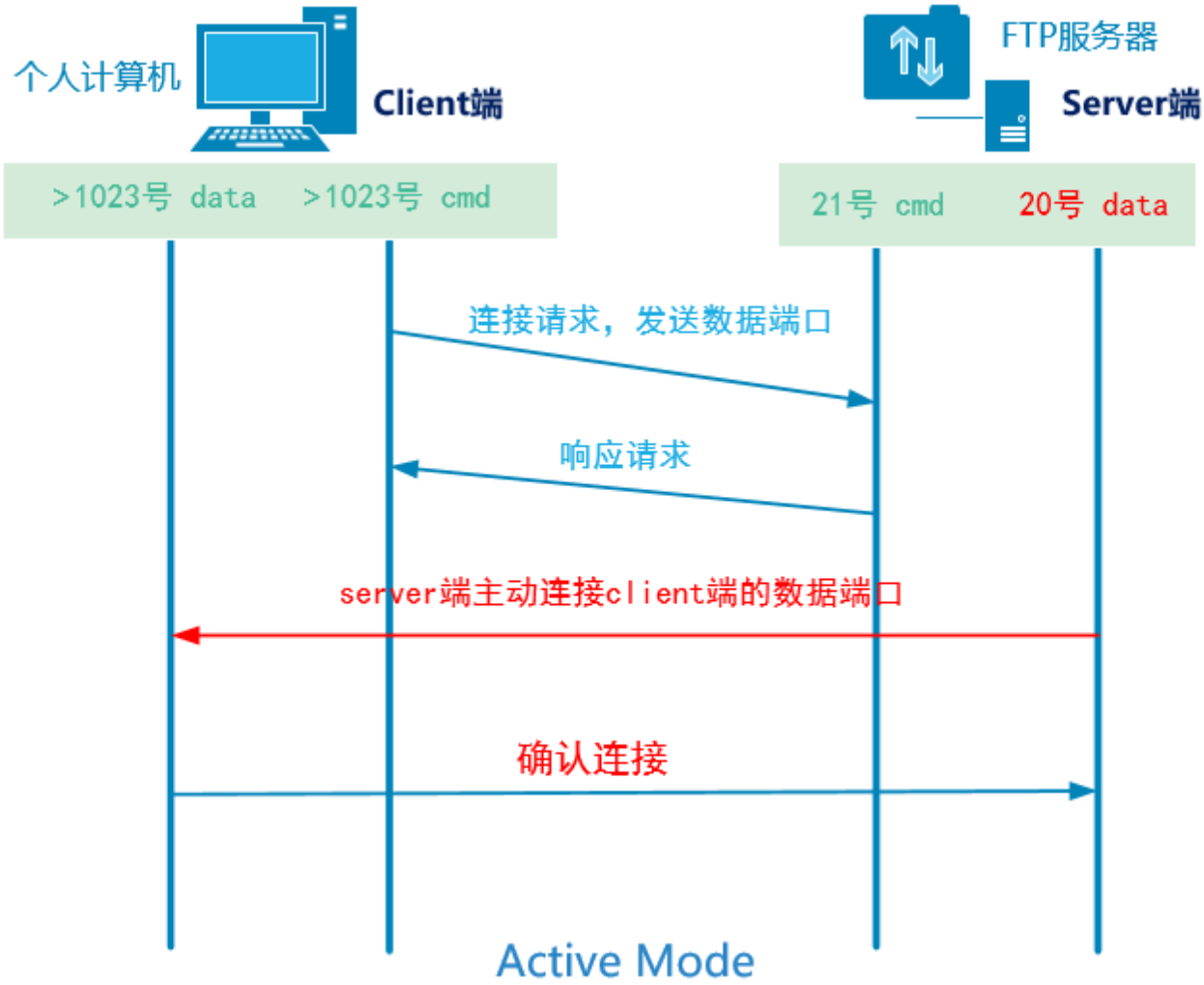
> Windows：FileZilla、IE、Chrome、Firefox
>
> lftp和ftp工具区别：
>
> lftp:默认是以匿名用户访问
>
> ftp：默认是以用户名/密码方式访问

- lftp可以批量并且下载目录

```
lftp localhost:~> mirror remote local  下载整个目录到本地
lftp localhost:~> mirror -R local remote  rename 上传整个目录到远程同时可以重命名
```

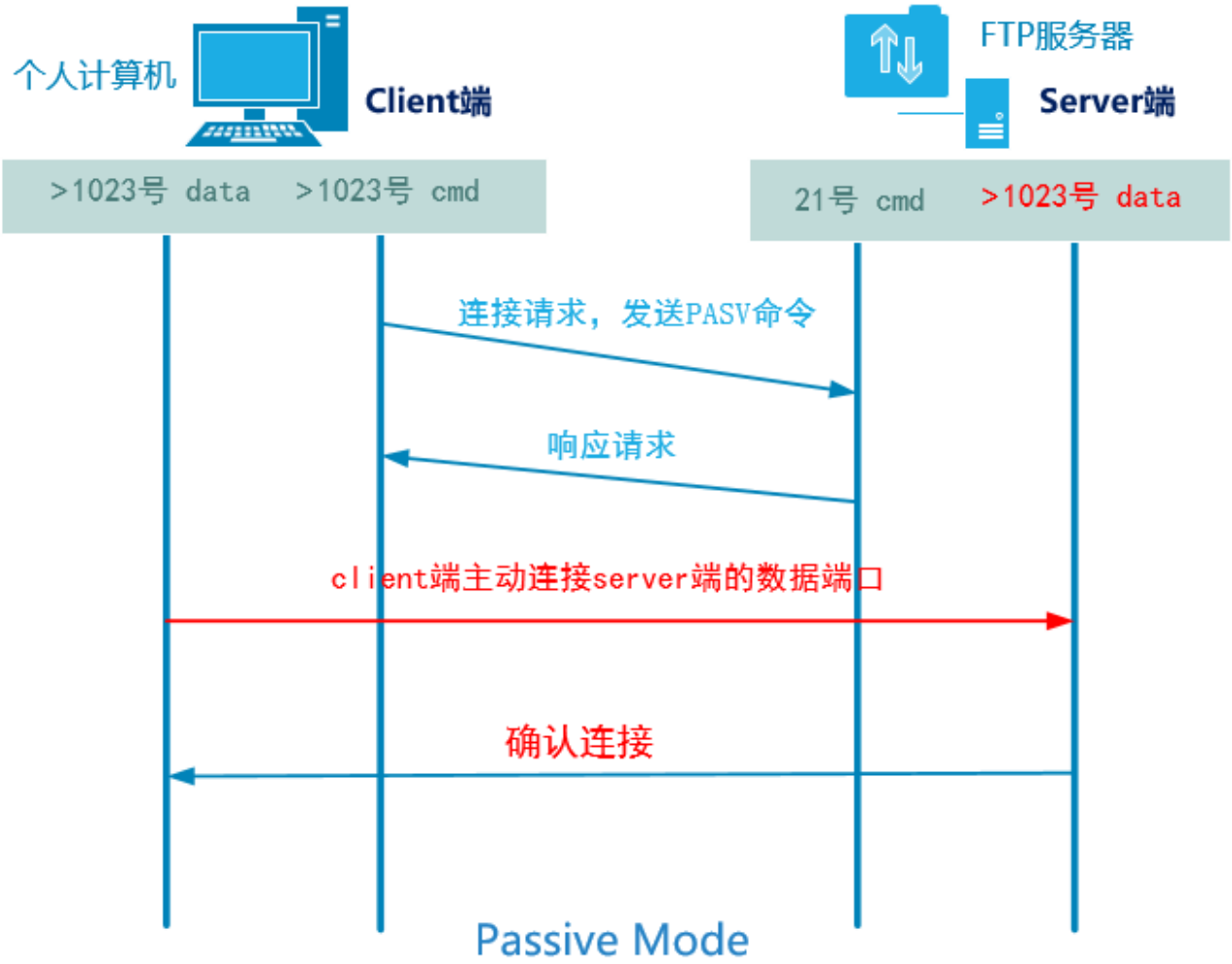
三、FTP的两种工作模式

- 主动模式



1. 客户端打开大于1023的随机**命令端口**和大于1023的随机**数据端口**向服务的的21号端口发起请求
2. 服务端的21号命令端口响应客户端的随机命令端口
3. 服务端的20号端口主动请求连接客户端的随机数据端口
4. 客户端的随机数据端口进行确认

- 被动模式



1. 客户端打开大于1023的随机命令端口和大于1023的随机数据端口向服务的的21号端口发起请求
2. 服务端的21号命令端口响应客户端的随机命令端口
3. 客户端主动连接服务端打开的大于1023的随机数据端口
4. 服务端进行确认

思考1：

FTP的主动模式好还是被动模式好？

软件的文件列表

```
/etc/logrotate.d/vsftpd        //日志轮转的文件
/etc/pam.d/vsftpd           //安全认证
/etc/rc.d/init.d/vsftpd        //启动脚本
/etc/vsftpd                 //配置文件的主目录
/etc/vsftpd/ftpusers        //用户列表（黑名单）
/etc/vsftpd/user_list          //用户列表（默认黑名单|可黑可白）
/etc/vsftpd/vsftpd.conf        //主配置文件
/usr/sbin/vsftpd         //二进制命令
```

```
/usr/share/doc/vsftpd-2.2.2/EXAMPLE/VIRTUAL_HOSTS
/usr/share/doc/vsftpd-2.2.2/EXAMPLE/VIRTUAL_HOSTS/README //虚拟主机
/usr/share/doc/vsftpd-2.2.2/EXAMPLE/VIRTUAL_USERS
/usr/share/doc/vsftpd-2.2.2/EXAMPLE/VIRTUAL_USERS/README //虚拟用户

/usr/share/man/man5/vsftpd.conf.5.gz          //man文档

/var/ftp       //匿名用户的默认数据的根目录
/var/ftp/pub       //匿名用户的默认数据目录的扩展目录
```

了解配置文件

主配置文件：man 5 vsftpd.conf

```
[root@ftp-server ~]# grep -v ^# /etc/vsftpd/vsftpd.conf
anonymous_enable=YES //支持匿名用户访问
local_enable=YES     //非匿名用户
write_enable=YES     //写总开关
local_umask=022         //反掩码  file:644  rw- r-- r-- dir:755
dirmessage_enable=YES   //启用消息功能
xferlog_enable=YES      //开启或启用xferlog日志
connect_from_port_20=YES   //支持主动模式（默认被动模式）
xferlog_std_format=YES     //xferlog日志格式
listen=YES              //ftp服务独立模式下的监听

pam_service_name=vsftpd //指定认证文件
userlist_enable=YES     //启用用户列表
tcp_wrappers=YES     //支持tcp_wrappers功能
```

四、FTP服务基本配置

```
环境：
ftp-server:10.1.1.1
client:10.1.1.2

1. 安装ftp服务相关的软件
1）配置yum源（本地）
挂载镜像到本地：
[root@ftp-server yum.repos.d]# mkdir /iso
[root@ftp-server yum.repos.d]# mount -o ro /dev/sr0 /iso
[root@ftp-server yum.repos.d]# echo "mount -o ro /dev/sr0 /iso" >> /etc/rc.local
[root@ftp-server yum.repos.d]# cat /etc/rc.local
...
mount -o ro /dev/sr0 /iso
修改配置文件：
[root@ftp-server yum.repos.d]# cat local.repo
[local]
name=xxx
baseurl=file:///iso
enabled=1
```

```
gpgcheck=0

2) 安装vsftpd软件
[root@ftp-server yum.repos.d]# yum -y install vsftpd
确认软件包成功安装:
[root@ftp-server yum.repos.d]# rpm -q vsftpd
vsftpd-2.2.2-11.el6_4.1.x86_64
[root@ftp-server yum.repos.d]# yum list installed|grep vsftpd
vsftpd.x86_64           2.2.2-11.el6_4.1

2. 查看文件所带来的文件列表
[root@ftp-server yum.repos.d]# rpm -ql vsftpd
/etc/rc.d/init.d/vsftpd       启动脚本
/etc/vsftpd                   ftp服务的主目录
/etc/vsftpd/vsftpd.conf       主配置文件
/var/ftp                      匿名用户的默认数据目录
/var/ftp/pub                  匿名用户的数据目录的扩展目录
/etc/vsftpd/ftpusers          用户列表文件（黑名单）
/etc/vsftpd/user_list         用户列表文件（黑名单或者白名单）

3. 启动服务
[root@ftp-server ~]# service vsftpd start
Starting vsftpd for vsftpd:                                [  OK  ]
[root@ftp-server ~]# netstat -nltp|grep vsftpd
tcp        0      0 0.0.0.0:21                  0.0.0.0:*                   LISTEN
 10172/vsftpd

4. 测试验证
windows: 匿名用户登录
IE:
ftp://10.1.1.1
资源管理器（我的电脑）:
ftp://10.1.1.1

Linux平台:
客户端需要安装ftp和lftp工具
ftp lftp (客户端工具)

[root@backup ~]# ftp 10.1.1.1
-bash: ftp: command not found    没有安装软件
[root@backup ~]# yum -y install ftp lftp

[root@backup ~]# ftp 10.1.1.1
Connected to 10.1.1.1 (10.1.1.1).
220 (vsFTPd 2.2.2)
Name (10.1.1.1:root): ftp     ftp代表匿名用户
331 Please specify the password.
Password:                     密码不输入直接回车
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (10,1,1,1,113,190).
```

```
150 Here comes the directory listing.
-rw-r--r--    1 0        0               0 Aug 29 07:12 file1
-rw-r--r--    1 0        0               0 Aug 29 07:12 file2
-rw-r--r--    1 0        0               0 Aug 29 07:12 file3
drwxr-xr-x    2 0        0            4096 Mar 01  2013 pub
226 Directory send OK.

[root@backup ~]# lftp 10.1.1.1
lftp 10.1.1.1:~> ls
-rw-r--r--    1 0        0               0 Aug 29 07:12 file1
-rw-r--r--    1 0        0               0 Aug 29 07:12 file2
-rw-r--r--    1 0        0               0 Aug 29 07:12 file3
drwxr-xr-x    2 0        0            4096 Mar 01  2013 pub
```

默认情况下，vsftpd服务支持本地用户(/etc/passwd)访问。

总结:
默认情况下，vsftpd服务允许匿名用户下载文件，但是不允许匿名用户上传文件;
允许本地用户上传和下载文件，本地用户是ftp服务端的普通用户。

任务解决方案

1. 在ftp-server端创建用户并且给密码

```
[root@ftp-server ~]# useradd kefu
[root@ftp-server ~]# echo 123|passwd --stdin kefu
```

2. 禁止匿名用户访问FTP服务

```
[root@ftp-server vsftpd]# vim vsftpd.conf
anonymous_enable=NO
```

重启服务测试验证

```
[root@client ~]# ftp 10.1.1.1
Connected to 10.1.1.1 (10.1.1.1).
220 (vsFTPd 2.2.2)
Name (10.1.1.1:root): ftp
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> exit
221 Goodbye.
[root@client ~]# lftp 10.1.1.1
lftp 10.1.1.1:~> ls
Interrupt
lftp 10.1.1.1:~> exit
```

3. 客服人员相关的文档保存在指定的目录里/data/kefu

1) 在ftp服务端创建相应的目录来保存文件

```
# mkdir /data/kefu -p
```

2) 通过修改配置文件告诉ftp服务将文件保存到指定目录里

```
local_root=/data/kefu
```

3）重启服务测试验证

```
[root@client ~]# ftp 10.1.1.1
Connected to 10.1.1.1 (10.1.1.1).
220 (vsFTPd 2.2.2)
Name (10.1.1.1:root): kefu
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/data/kefu"
```

问题：上传不成功

解决：目录本身没有权限

```
setfacl -m u:kefu:rwx /data/kefu
```

4．禁锢本地用户的数据目录

修改配置文件

```
chroot_local_user=YES
```

重启服务测试验证

```
[root@client ~]# ftp 10.1.1.1
Connected to 10.1.1.1 (10.1.1.1).
220 (vsFTPd 2.2.2)
Name (10.1.1.1:root): kefu
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
ftp> cd /etc
550 Failed to change directory.
ftp> cd /home
550 Failed to change directory.
```

补充：关于禁锢用户的家目录选项

1．禁锢所有人的家

```
chroot_local_user=YES
```

2．禁锢大部分人，允许小部分人

```
chroot_local_user=YES
chroot_list_enable=YES      开启用户列表文件
chroot_list_file=/etc/vsftpd/chroot_list   指定用户列表文件

echo stu1 >> /etc/vsftpd/chroot_list
```

3．允许大部分人，禁锢小部分人

```
chroot_local_user=NO
chroot_list_enable=YES      开启用户列表文件
chroot_list_file=/etc/vsftpd/chroot_list   指定用户列表文件
```

```
echo kefu >> /etc/vsftpd/chroot_list
```

补充扩展

FTP服务的访问控制

1. 对象访问控制

ftpusers 黑名单

user_list 默认是黑名单（可以成为白名单）

```
[root@client ~]# ftp 10.1.1.1
Connected to 10.1.1.1 (10.1.1.1).
220 (vsFTPd 2.2.2)
Name (10.1.1.1:root): root
530 Permission denied.
Login failed.
ftp> exit
原因：root用户在黑名单里.ftpusers

[root@client ~]# ftp 10.1.1.1
Connected to 10.1.1.1 (10.1.1.1).
220 (vsFTPd 2.2.2)
Name (10.1.1.1:root): stu1
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp>

原因：stu1用户在黑名单里。ftpuses

为什么两个用户的提示信息不一样?
原因：默认情况下user_list文件也是黑名单，如果在该文件里直接拒绝，不给输入密码的机会。

user_list要成为白名单，需要再配置文件里增加：
userlist_deny=NO
注意：如果user_list是白名单，那么必须在该文件里的用户才可以访问ftp服务。
```

总结：

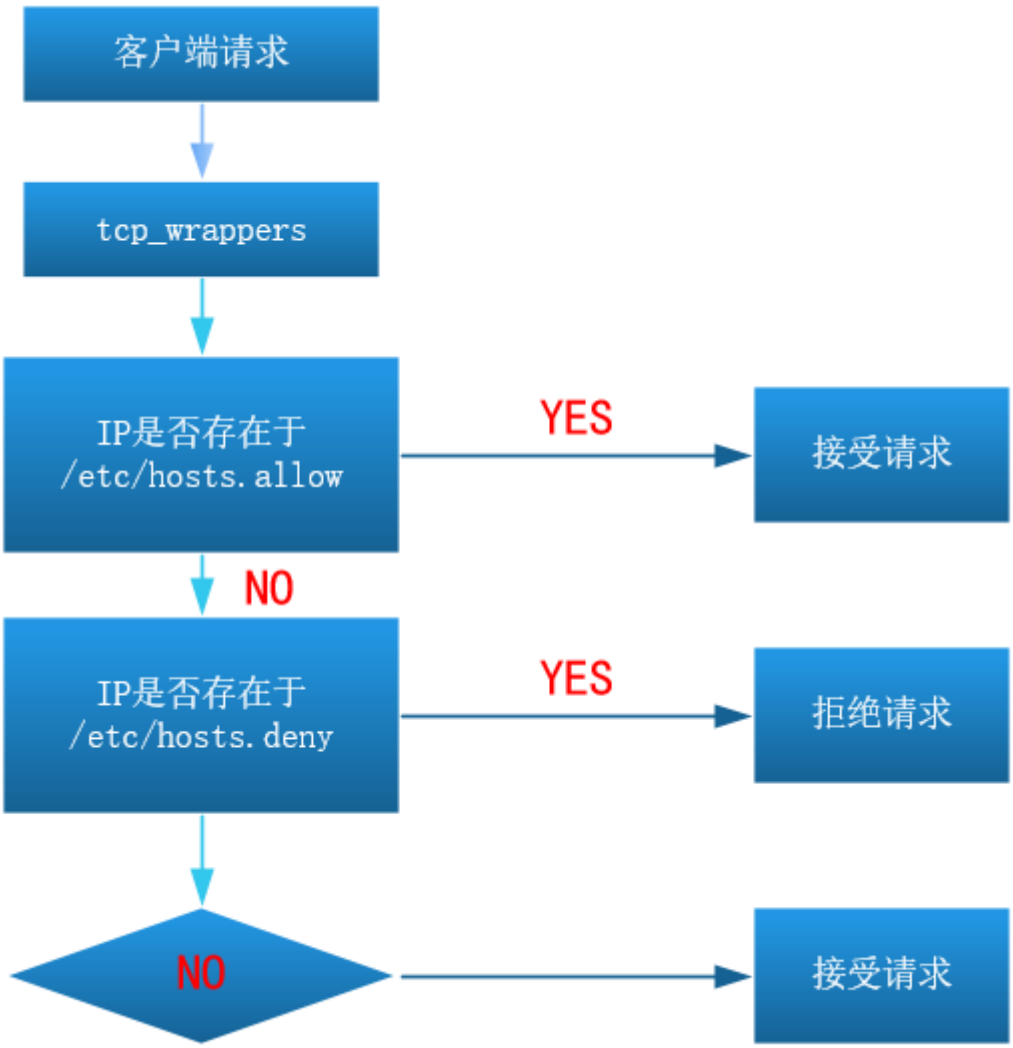
1. 用户在ftpusers文件中，那么用户不能访问ftp服务器
2. 用户在user_list文件中，如果该文件是白名单，那么只在该文件中的用户可以访问ftp服务
3. 如果user_list文件是白名单，用户即在ftpusers中又在user_list中，那么ftpusers拒绝优先

2. 网络访问控制

- 支持tcp_wrappers

  /etc/hosts.allow

/etc/hosts.deny



- 写法

```
/etc/hosts.deny
vsftpd:all                          全部拒绝
vsftpd:all  EXCEPT 192.168.0.2      拒绝所有除了192.168.0.2
vsftpd:192.168.0.254        拒绝单个ip地址=hosts.allow文件里增加vsftpd:192.168.0.254:deny
vsftpd:192.168.0.0/255.255.255.0    拒绝某个网段
vsftpd:192.168.0.0/255.255.255.0 EXCEPT 192.168.0.254    拒绝某个网段，但是除了某个ip地址
注意：子网掩码不支持192.168.0.0/24这种写法
```

思考2： 如何判断一个服务是否支持tcp_wrappers?

1）./configure --enable-libwrap 表示支持tcp_wrappers访问控制

2）rpm安装

```
[root@ftp-server vsftpd]# ldd /usr/sbin/vsftpd |grep libwrap*
   libwrap.so.0 => /lib64/libwrap.so.0 (0x00007f2956480000)

[root@ftp-server vsftpd]# ldd /usr/sbin/sshd |grep libwrap*
   libwrap.so.0 => /lib64/libwrap.so.0 (0x00007f015ff29000)
```

示例：拒绝10.1.1.0/24和192.168.91.0/24网段的所有人访问，除了10.1.1.3服务器

```
vim /etc/hosts.deny
vsftpd:10.1.1.0/255.255.255.0,192.168.91.0/255.255.255.0 EXCEPT 10.1.1.3
```

课后作业

- 准备环境：

主机1（server）：FTP服务器 主机2（client）：FTP客户端

- 根据需求搭建自己的FTP服务器：

1. 匿名用户可以到/anon/data目录里上传下载文件，同时也可以下载其他人所上传的文件;

```
1. 默认 /var/ftp 更改到 /anon/data 目录
1）创建一个数据目录
mkdir /anon/data -p
2）修改配置文件
anon_root=/anon/data

2. 默认匿名用户不能上传  修改 为匿名用户上传
修改配置文件
anon_mkdir_write_enable=YES
anon_other_write_enable=YES
anon_upload_enable=YES


lftp 10.1.1.1:/> put demo.sql
put: Access failed: 553 Could not create file. (demo.sql)
原因：ftp-server端的数据目录没有写权限
解决：
[root@ftp-server vsftpd]# chmod o+w /anon/data/
另外问题：
其他匿名用户再次访问ftp服务报以下错误：
lftp 10.1.1.1:~> ls
ls: Login failed: 500 OOPS: vsftpd: refusing to run with writable anonymous root
原因：匿名用户的默认数据根目录权限太大。chmod o+w /anon/data
解决：
chmod o-w /anon/data（不能永久解决）
修改该配置文件，指定匿名用户的默认数据根目录为/anon/
chmod o+w /anon/data
3. 其他人可以下载另外的匿名用户上传的文件
```

```
anon_umask=022       dir:755 file:644  rw-r--r--
```

2. 客户端可以使用zhangsan（自己名字），访问你的ftp服务器，但是不能登录ftp服务器的操作系统，并且只能在自己的家目录中活动;

```
ftp-server:
useradd -s /sbin/nologin zhangsan
echo 123|passwd --stdin zhangsan

修改配置文件:
chroot_local_user=YES          //禁锢所有的本地用户的家目录
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list

禁锢大部分本地用户允许小部分人可以切换跳转:
禁锢zhangsan, user01和user02允许
zhangsan   user01 user02
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list

echo user01 >> /etc/vsftpd/chroot_list
echo user02 >> /etc/vsftpd/chroot_list

禁锢小部分用户允许大部分用户:
#chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
echo zhangsan >> /etc/vsftpd/chroot_list
```

3. zhangsan（自己名字）用户可以上传下载文件，并且所有本地用户上传的文件都存放在/local/data;

```
mkdir -p /local/data
local_root=/local/data
注意:
服务的控制，目录本身的控制
[root@ftp-server vsftpd]# ll -d /local/data/
drwxr-xr-x 2 root root 4096 Nov 10 10:16 /local/data/
[root@ftp-server vsftpd]#
[root@ftp-server vsftpd]# setfacl -m u:zhangsan:rwx /local/data/
```

4. 在客户端/tmp/zhangsan（自己名字）下面创建5个文件，叫file{1..5},通过客户端工具以匿名用户身份将/tmp/zhangsan整个以你名字命名的目录上传到FTP服务器的data目录中;

```
1. 允许匿名用户上传文件
vim /etc/vsftpd/vsftpd.conf
anon_mkdir_write_enable=YES
anon_other_write_enable=YES
```

```
anon_upload_enable=YES
2. 在匿名用户的数据根目录里创建一个data目录来保存上传文件
默认匿名用户数据目录：/var/ftp
mkdir /var/ftp/data
chmod o+w /var/ftp/data

get
mget 批量下载
put
mput 批量上传

[root@client ~]# lftp 10.1.1.1
lftp 10.1.1.1:~> ls
drwxr-xrwx    2 0        0            4096 Nov 10 02:29 data
-rw-r--r--    1 0        0             192 Nov 09 03:09 hosts
drwxr-xr-x    2 0        0            4096 Mar 01  2013 pub
lftp 10.1.1.1:/> mirror -R /tmp/zhangsan/ ./data/
Total: 1 directory, 5 files, 0 symlinks
New: 5 files, 0 symlinks


lftp 10.1.1.1:/> cd data/
lftp 10.1.1.1:/data> ls
drwxr-xr-x    2 0        0            4096 Nov 10 02:31 2018-11-10
drwx------    2 14       50           4096 Nov 10 02:30 zhangsan
lftp 10.1.1.1:/data> lcd /tmp/
lcd ok, local cwd=/tmp
lftp 10.1.1.1:/data> mirror 2018-11-10/ ./
Total: 1 directory, 1 file, 0 symlinks
New: 1 file, 0 symlinks
192 bytes transferred
lftp 10.1.1.1:/data>


lftp localhost:~> mirror remote local  下载整个目录到本地
lftp localhost:~> mirror -R local remote  rename 上传整个目录到远程同时可以重命名
```

5. 客户端通过redhat用户（密码redhat）下载FTP服务器上的"2018-11-10"文件(自己创建)到你本地/tmp/zhangsan(自己名字)目录里;

```
[root@ftp-server data]# useradd redhat
[root@ftp-server data]# echo redhat |passwd --stdin redhat
Changing password for user redhat.
passwd: all authentication tokens updated successfully.

[root@ftp-server data]# cd /local/data/
[root@ftp-server data]# ll
total 4
-rw-r--r-- 1 zhangsan zhangsan 6 Nov 10 10:20 1.txt
-rw-r--r-- 1 root     root     0 Nov 10 10:16 file1
-rw-r--r-- 1 root     root     0 Nov 10 10:16 file2
-rw-r--r-- 1 root     root     0 Nov 10 10:16 file3
```

```
[root@ftp-server data]# mkdir $(date +%F)


[root@client ~]# lftp redhat@10.1.1.1
Password:
lftp redhat@10.1.1.1:~> ls
-rw-r--r--    1 507      507             6 Nov 10 02:20 1.txt
drwxr-xr-x    2 0        0            4096 Nov 10 02:35 2018-11-10
-rw-r--r--    1 0        0               0 Nov 10 02:16 file1
-rw-r--r--    1 0        0               0 Nov 10 02:16 file2
-rw-r--r--    1 0        0               0 Nov 10 02:16 file3
lftp redhat@10.1.1.1:/> mirror 2018-11-10/ /tmp/zhangsan/
Total: 1 directory, 3 files, 0 symlinks
New: 3 files, 0 symlinks
lftp redhat@10.1.1.1:/>
```

6. 不允许192.168.0.254访问你的ftp服务。

```
网络访问控制:
vim /etc/hosts.deny
vsftpd:192.168.0.254
```

7. 固定服务器端被动模式下的端口号范围为2000~2050

```
pasv_max_port=2050
pasv_min_port=2000
测试验证:
netstat -na|grep vsftpd
```

8. 限制匿名用户下载文件的速率为500kbps，最大连接数为10个

```
anon_max_rate=500000
max_clients=10
```