**点对点内网穿透**

这个示例将演示如何通过点对点 (P2P) 连接来访问内网服务，流量不会通过服务器中转。

frp 提供了一种新的代理类型 xtcp，用于在需要传输大量数据且不希望流量经过服务器的情况下实现内网穿透。

与 stcp 类似，使用 xtcp 需要在两端都部署 frpc 以建立直接连接。

需要注意的是，xtcp 并不适用于所有类型的 NAT 设备，如果穿透失败，可以尝试使用 stcp 代理。

### 步骤

1. **配置需要暴露到外网的机器上的 frpc.toml 文件**

在 frpc.toml 文件中添加以下内容，确保设置了正确的服务器地址和端口以及共享密钥 (secretKey)，以及本地服务的 IP 地址和端口：

serverAddr **=** "x.x.x.x"

serverPort **=** **7000**

*# 如果默认的 STUN 服务器不可用，可以配置一个新的 STUN 服务器*

*# natHoleStunServer = "xxx"*

**[[**proxies**]]**

name **=** "p2p\_ssh"

type **=** "xtcp"

*# 只有共享密钥 (secretKey) 与服务器端一致的用户才能访问该服务*

secretKey **=** "abcdefg"

localIP **=** "127.0.0.1"

localPort **=** **22**

1. **在想要访问内网服务的机器上部署 frpc**

在 frpc.toml 文件中添加以下内容，确保设置了正确的服务器地址和端口，共享密钥 (secretKey) 以及要访问的 P2P 代理的名称：

serverAddr **=** "x.x.x.x"

serverPort **=** **7000**

*# 如果默认的 STUN 服务器不可用，可以配置一个新的 STUN 服务器*

*# natHoleStunServer = "xxx"*

**[[**visitors**]]**

name **=** "p2p\_ssh\_visitor"

type **=** "xtcp"

*# 要访问的 P2P 代理的名称*

serverName **=** "p2p\_ssh"

secretKey **=** "abcdefg"

*# 绑定本地端口以访问 SSH 服务*

bindAddr **=** "127.0.0.1"

bindPort **=** **6000**

*# 如果需要自动保持隧道打开，将其设置为 true*

*# keepTunnelOpen = false*

1. **通过 SSH 访问内网机器**

使用 SSH 命令访问内网机器，假设用户名为 test：

ssh -oPort=6000 test@127.0.0.1