

Networking

About

A discussion of various issues to consider when configuring a FreeSWITCH™ installation.

Bandwidth

The bandwidth required by a FreeSWITCH installation depends on the codecs used to transport the RTP voice streams and the maximum simultaneous number of calls expected.

Network Address Translation (NAT)

NAT is a pox upon the house of SIP, but there are techniques to solve some of the problems on the [NAT Traversal page](#).

Privileged Ports

In the unlikely event that your FreeSWITCH™ installation requires access to privileged ports (numbered below 1024), the portable method is to map the lower port number to a higher port number to which FreeSWITCH™ already has common access. An alternate method is to use the setcap command to change the effective and permitted capabilities of the freeswitch binary to allow it to access privileged ports. You must have root privileges on the machine that runs FreeSWITCH™ in order to use these commands.

IPtables

```
iptables -t nat -I PREROUTING --src 0/0 --dst 127.0.0.1 -p tcp --dport 443 -j REDIRECT --to-ports 5061
```

This will redirect incoming tcp packets arriving for privileged port 443 to common port 5061 on which FS is listening.

Some examples omit the `--src` and `--dst` arguments; presumably this applies the rule to all interfaces. Also, different firewall frontends require different formatting of the command and install rules in different files, so this is only a guide to direct you in the correct direction. There is MUCH more information in the links below.

IPTables Additional Info

[Debian wiki](#)

[Frozen Tux tutorial](#)

[Debian Administration article](#)

[Stack Overflow discussion](#)

Linux Capabilities

```
# install the capabilities package
apt-get install libcap2-bin
# allow FreeSWITCH binary to access privileged ports
setcap 'cap_net_bind_service+ep' /usr/local/freeswitch/bin/freeswitch
```

Capabilities are only available on newer linux kernels, so this is not a preferred solution.

The documentation and articles do not indicate whether this is a persistent change or must be done before each invocation of the target binary. If you know, please let us know in the comments below or by opening a ticket on the [Docs JIRA](#) system. Thanks.

Capabilities Additional Info

[Stack Overflow discussion](#)

SonicWall Port Remapping

Some FS users have discovered that SonicWall firewalls can munge the results of a STUN lookup by remapping the candidate port to something other than what FS expects.

Solve this problem by disabling "Source Port Remap" in the SonicWall Network NAT Policies Advanced page.