Security

About

Security is about mitigating risks while providing ease of use, problem detection, and remediation while protecting the most important characteristics of the system. This section will provide a number of points to consider.

Considerations

- What are your security best practices?
- What techniques do you use?
- How do you balance security vs. ease of use?

General Recommendations

If you are not using a VPN nor on a local intranet with the FS server make sure to use SIP_TLS as all sip traffic and authentication is in the clear otherwise.

The most basic things for any system include:

- Have a router with SPI firewall between your system and the Internet; do not put your system in the router DMZ (where all default incoming traffic will be sent)
- Change all system passwords and set them to strong ones.
- Install the latest patches for your OS
- Setup an IDS like Snort or AIDE
- Use fail2ban to limit SIP password / id guessing (linux only)
- Setup a firewall - configuration to be described later in the page
- Install an Anti-Virus (Windows); remember that AVG seems to interfere with compilation
- Use ipset to manage your own i.p. addresses, ports, MAC addresses, etc at much lower performance penalty
- bkw's example script f-off friendly scanner.pl

Sources to consider:

- SNORT [1]
- Linux only: AIDE [2]
- Windows only: Threats and Countermeasures Guide: Security Settings in Windows Server 2008 and Windows Vista [3]

Freeswitch Configuration

Passwords and Other Confidential Information

Your FreeSWITCH™ configuration will have a number of areas where confidential information is stored. Here is a list to start with:

- User names and passwords
- Proxy or Gateway names and passwords
- Other module configuration... please add ...

Please change the following elements of the default configuration:

- users 1000 to 1019 and their passwords (good ideas to remove them completely)
- change the default voicemail password

Local Registrations

- Companies that accept only static IP address should use registeracl and add their customer's IP to the ACL for registration protection.

- Limit the number of connections per second or per minute, depending on your setup, on your firewall. This way if there are more attempts than there should be, your firewall should block them before they even get to FS. Your firewall rules may follow this general scheme:
    - (1) Accept signaling or media traffic from trusted IPs and apply connections-per-second rules based on their traffic pattern;
    - (2) Accept signaling or media traffic from any IP but with the condition that if a single IP exceeds a certain connections-per-second number then block that IP temporarily or permanently (depending on the situation). pfSense blocks that IP for one hour automatically if the rule has this setting enabled. Using iptables it is also easy to create such a rule (see Using iptables to rate-limit incoming connections).

Firewall configuration

An example configuration for iptables can be found at Iptables on debian.

Rate-Limit Examples

by Bret McDanel

It may be interesting to add rate-limiting of incoming SIP traffic. Below is an example of how this can be done. If you use the default internal and external sip profiles then you should block on both ports 5060 and 5080.

DoS Rate-Limiter

```
# Trixter's SIP rate limiter (This helps protect you from DoS attacks)
iptables -A INPUT -p udp --dport 5060 -m limit --limit 5/s --limit-burst 5 -i eth0 -j REJECT
iptables -A INPUT -p udp --dport 5080 -m limit --limit 5/s --limit-burst 5 -i eth0 -j REJECT
```

BEWARE 5 per second TOTAL may be too low for your usage. This ended up rejecting all my many 5 UAs from registering.

DoS REGISTER Attack Prevention

DoS Register Attack 1

```
iptables -A INPUT -m string --string "REGISTER sip:" --algo bm --to 65 -m hashlimit \
    --hashlimit 4/minute --hashlimit-burst 1 --hashlimit-mode  srcip,dstport \
    --hashlimit-name sip_r_limit -j ACCEPT

iptables -I INPUT -j DROP -p udp --dport 5060 -m string --string "friendly-scanner" --algo bm
```

-Or-

DoS Register Attack 2

```
iptables -A INPUT -d YOUR_FS_IP -p udp -m udp --dport YOUR_FS_PORT -m string \
    --string "REGISTER" --algo kmp --from 20 --to 60 -j dos-filter-register-external

iptables -A dos-filter-register-external -m hashlimit --hashlimit 5/sec \
    --hashlimit-burst 8 --hashlimit-mode srcip --hashlimit-name REGISTER \
    --hashlimit-htable-size 24593 --hashlimit-htable-expire 90000 -j RETURN

iptables -A dos-filter-register-external -j REJECT --reject-with icmp-admin-prohibited
```