Authentication Gateway
or
How to Stop Enemy at the Gate!

Michael Pounov <misho@aitnet.org>

Introduction

- OpenBSD 4.6 some new interesting features
- OpenBSD – an attempt to build a complete routing platform or why all PF functionality is available under OpenBSD only
- New changes in PF
- Now, what is “authentication gateway” and its common usage ...

Problems & Scenarios *(most frequently used)

- Defend host from botnets or other things
  - Block login services for illuminated users :)
- Granted authentication for known users
  - Pass traffic through gateway for authenticated users.

Authentication gateway – internals

- Setup authpf system for 'defended host' running on FreeBSD/NetBSD/OpenBSD
  - Make authpf group:: authpf:*:63
  - Create login class in login.conf (*optional)
  - Make key user and set password:: useradd -gauthpf -d /etc/authpf -s /usr/sbin/authpf 0pen && passwd 0pen
  - Make directory structure
    - mkdir /var/authpf root:authpf (0770)
    - mkdir /etc/authpf /etc/authpf/banned /etc/authpf/users/${user}
  - Create files in /etc/authpf:
    - authpf.conf, authpf.allow, authpf.rules
    - authpf.message, authpf.problem

- Update fstab and mount fdescfs
  - fdescfs /dev/fd fdescfs rw 0 0
- Add to rc.local and rc.conf

```
authpf_ssh="-f /etc/ssh/sshd_config_authpf"
if [ X"${authpf_ssh}" != X"NO" ]; then
  echo "AuthPF system"
  /usr/sbin/sshd ${authpf_ssh} >/dev/null 2>&1
fi
```

- Make sshd_config_authpf

```
AllowUsers 0pen
Port 54321
PermitRootLogin no
ClientAliveInterval 15
ClientAliveCountMax 3
```

- PF snippet rules …(*examples)

authpf.rules

```
pass in quick proto tcp from $user_ip to any
                                        port 22 no state
```

pf.conf

```
table <authpf_users> persist
block in
pass out
anchor “authpf/*”
block in quick from <bad>
pass in proto tcp to any port 54321 keep state
     flags S/SAFPRU (max 10, source-track rule,
    max-src-nodes 3, max-src-conn 5,
    max-src-conn-rate 3/10, overload <bad> flush)
```

End :)

- Authpfmgr software for lazy administrators http://openfest.aitnet.org/

- Questions ?
- Thanks for attention!

Michael Pounov <misho@aitnet.org>

Development of embedded, system and network software solutions