authpf
Houston Area Hackers Association

Aaron Poffenberger

2016-03-03 Thu

Outline

What is authpf?

- AUTHPF(8) man page:
  - authpf is a user shell for authenticating gateways. It is used to change pf(4) rules when a user authenticates and starts a session with sshd(8) and to undo these changes when the user's session exits.

What are the use case for authpf?

- AUTHPF(8) man page:
  - Typical use would be for a gateway that authenticates users before allowing them Internet use, or a gateway that allows different users into different places. Combined with properly set up filter rules and secure switches, authpf can be used to ensure users are held accountable for their network traffic.

Where does it work?

- AUTHPF(8) man page:
  - It is meant to be used with users who can connect via ssh(1) only, and requires the pf(4) subsystem to be enabled.

What is pf?

- PF(4) is the stateful firewall built into OpenBSD and ported to several other BSDs including Mac OS X.
- It has a simple grammar that's very powerful and easy to write rules in.

```
# $OpenBSD: pf.conf,v 1.54 2014/08/23 05:49:42 deraadt Ex
#
# See pf.conf(5) and /etc/examples/pf.conf

set skip on lo

block return    # block stateless traffic
pass            # establish keep-state
pass on enc0
```

Configuring your server to work with authpf

- Create a user and set their shell to /usr/sbin/authpf
- Add simple rules to /etc/pf.conf

```
# rules for authpf
table <authpf_users> persist

pass in quick on egress inet proto tcp from <authpf_users
    to port $mail_ports rdr-to lo0
```

- Reload rules: pfctl -f /etc/pf.conf

Demo

Why not use a VPN?

- No special software required
  - At least for *nix-based systems, or perhaps BSD, ssh is already installed
- authpf is not necessarily an inbound port lock/unlock tool
  - Can be used for outbound port blocking
  - http(s)
  - telnet
  - ftp
- Quick to setup, at least on an OpenBSD box

Questions

- Questions - You have them, I may have answers

Contact Details

- Aaron Poffenberger
- akp@hypernote.com
- `http://akpoff.com`
- @akpoff
- This presentation, look for blog post on `http://akpoff.com`
- KG5DQJ

Links

- authpf man page
- pf man page
- pf.conf man page

License and Credits

- Copyright Aaron Poffenberger
- Attribution 4.0 International (CC BY 4.0)
  - `http://creativecommons.org/licenses/by/4.0/`