Hacking ha.ckers.org

Who we are.

- James Flom (id)
- COO SecTheory Ltd
- http://ha.ckers.org
- http://sla.ckers.org
- http://www.sectheory.com

In the beginning…

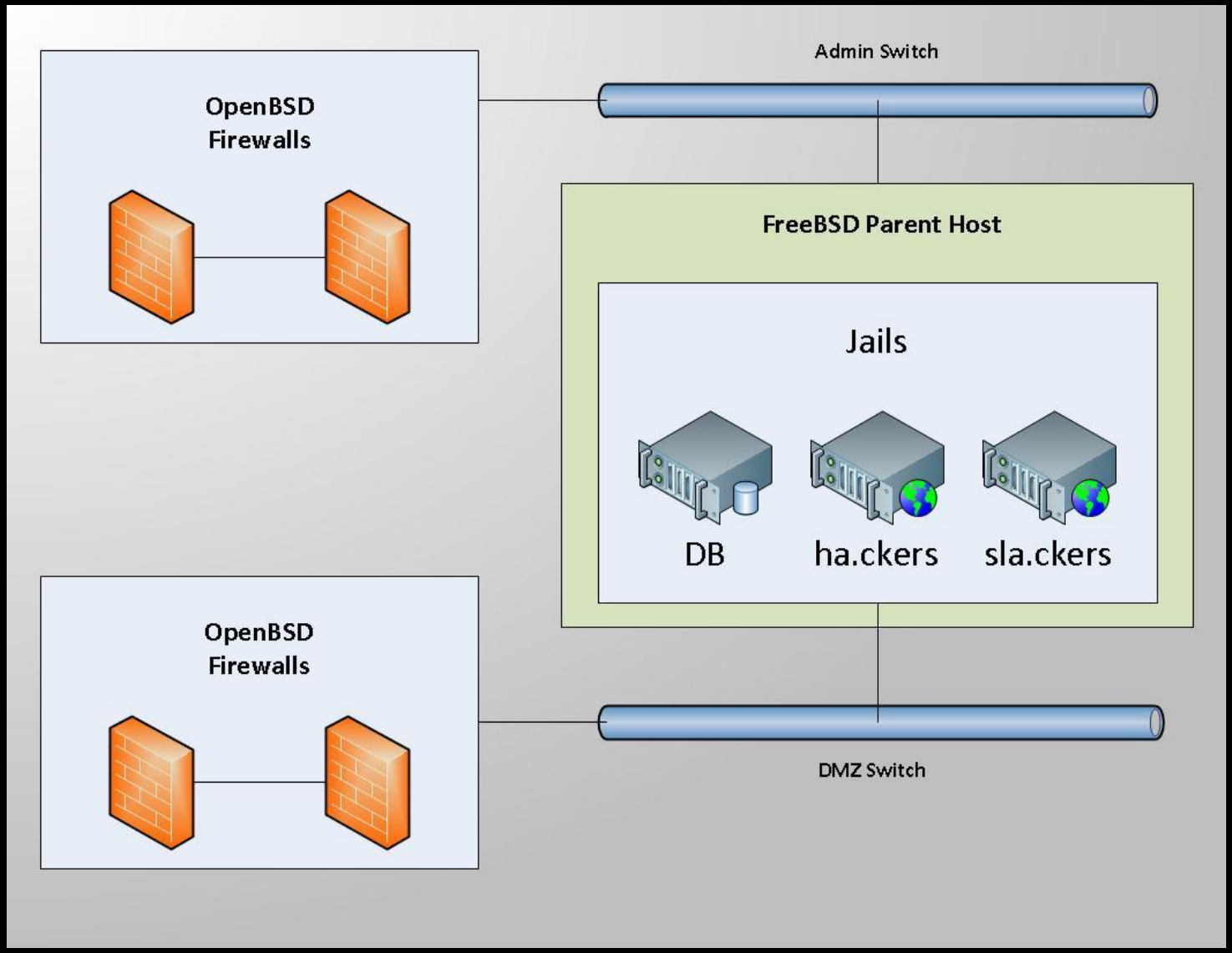
RSnake….Hey id, you've got a server, want to host this ha.ckers.org site for me?

Sure…

ha.ckers get’s a new home in TX

ha.ckers get’s a second new home in TX

The Network


Admin Switch
OpenBSD
Firewalls
FreeBSD Parent Host
Jails
DB
ha.ckers
sla.ckers
OpenBSD
Firewalls
DMZ Switch

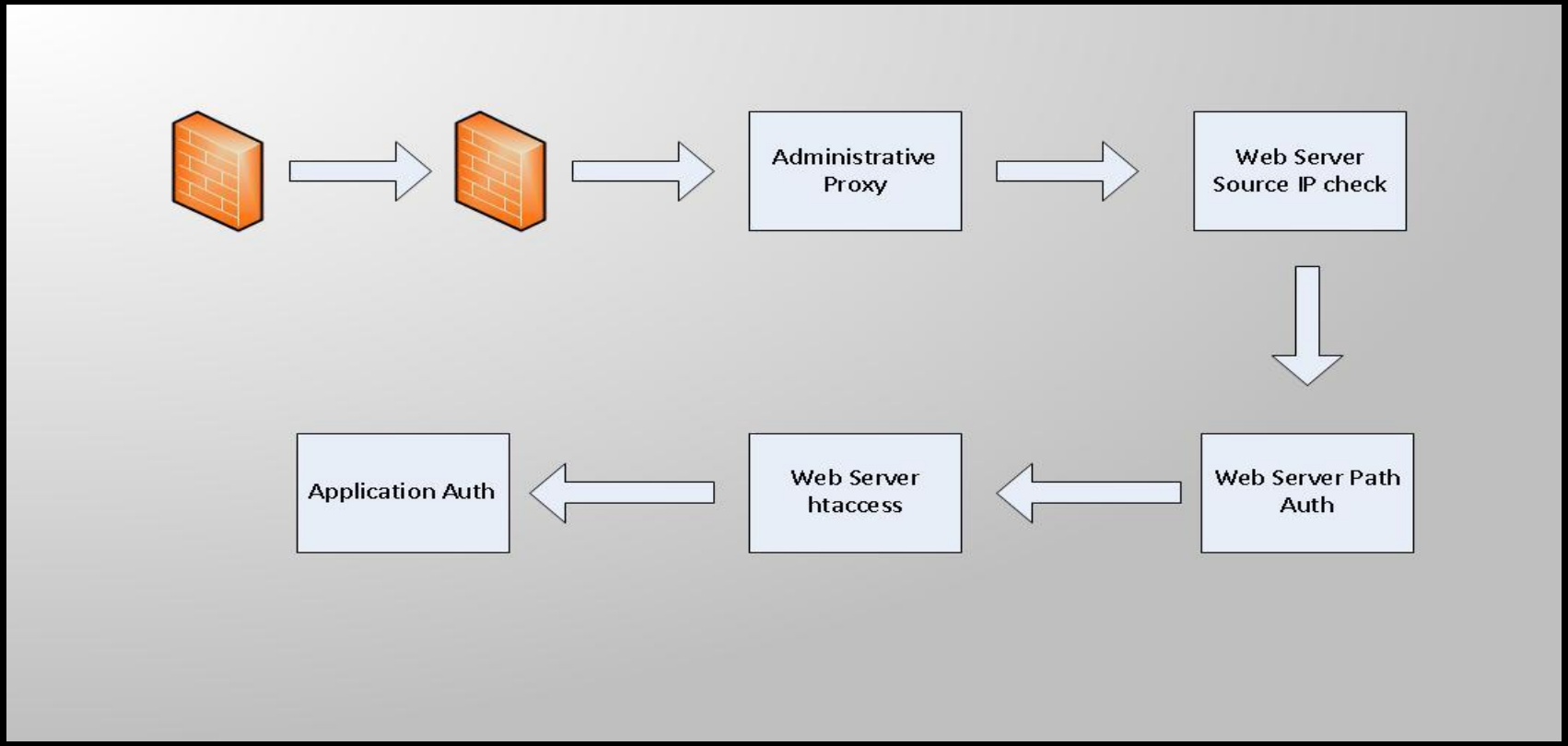
Network Features

- Firewall PF (OpenBSD)
  - Redirects traffic similar to a Cisco “static” translation
  - No egress traffic allowed from DMZ *ever*
  - DoS protection
    - Floods
    - Slowloris style attacks
  - Network separation
    - Admin traffic never traverses the DMZ network.

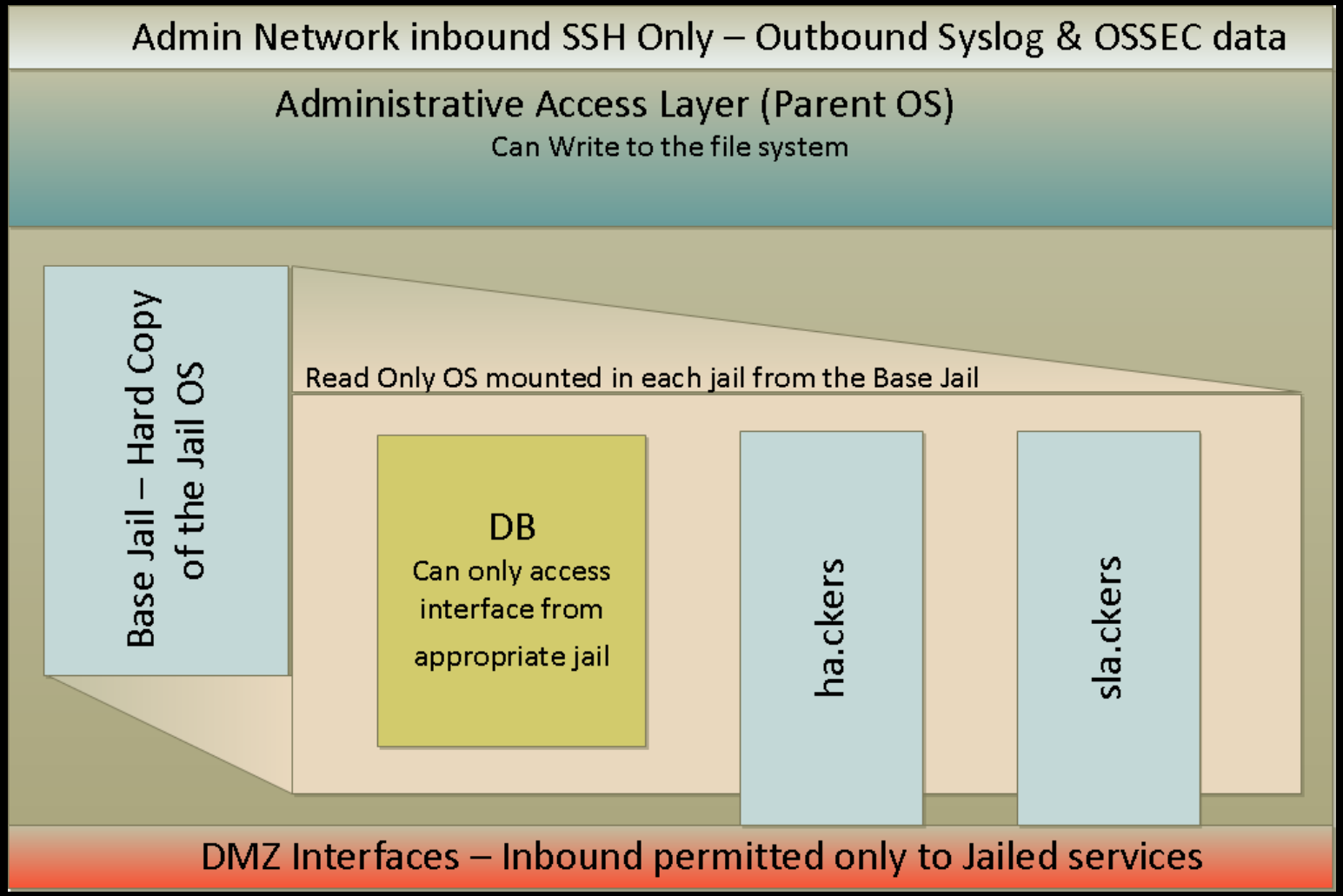
Who are you?

- Do you have a permitted source IP to connect to the firewall?
- Do you have the correct cert?
- Do you have a user/pass (SSH)
- Do you have a permitted source IP to connect to the administrative proxy?
- Do you have the right path?
- Do you have a user/pass for htaccess?
- Do you have authentication to the application?

I don’t trust you



Going to jail



OS Security

- Can only access the administrative interfaces via secure admin network
- Jails are mounted read only – even if compromised they cannot be rootkitted
- Only have to upgrade the Base Jail
- No real users live in the jails – files owned by no known user to the jailed OS
- No binaries not needed by the jails are in the Base Jail

Logging

- Everything that can log does log
- All logs are aggregated to log host that is not reachable by any DMZ host
- OSSEC used to aggregate and monitor logs with custom rules
- Logs are off the host and onto the log host as they are generated
- Forensics are done everyday

Next Generation Network

- Switching to relayd
  - OpenBSD implementation
  - SSL acceleration so packets can be read on the egress
- Each virtual interface gets it’s own network and firewall ruleset
- Already implemented for our hosting customers

Next Generation OS

- Completely read only jails
- Unique Base Jails for each type of server
- Logging via UNIX socket to parent OS – nothing touches the disk
- Further improvements in removing unneeded software
- Each jail has it’s own network stack and on host firewall

Questions?

james@sectheory.com

sl@cker.org