Crouching Admin

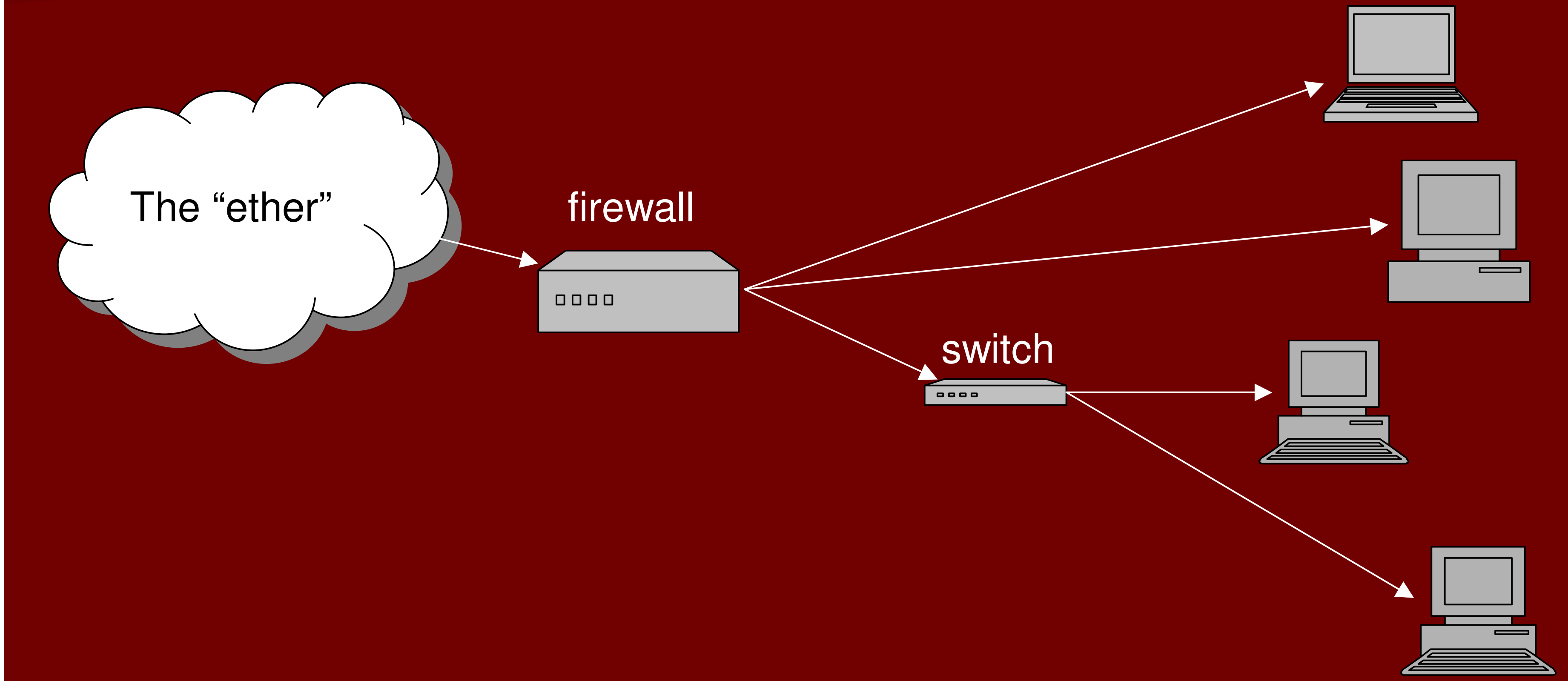
Hidden Firewall

Bridging or Stealth firewalls what is a bridging firewall?

“A bridge is a way to connect two Ethernet segments together in a protocol independent way. Packets are forwarded based on Ethernet address, rather than IP address (like a router). Since forwarding is done at Layer 2, all protocols can go transparently through a bridge.”

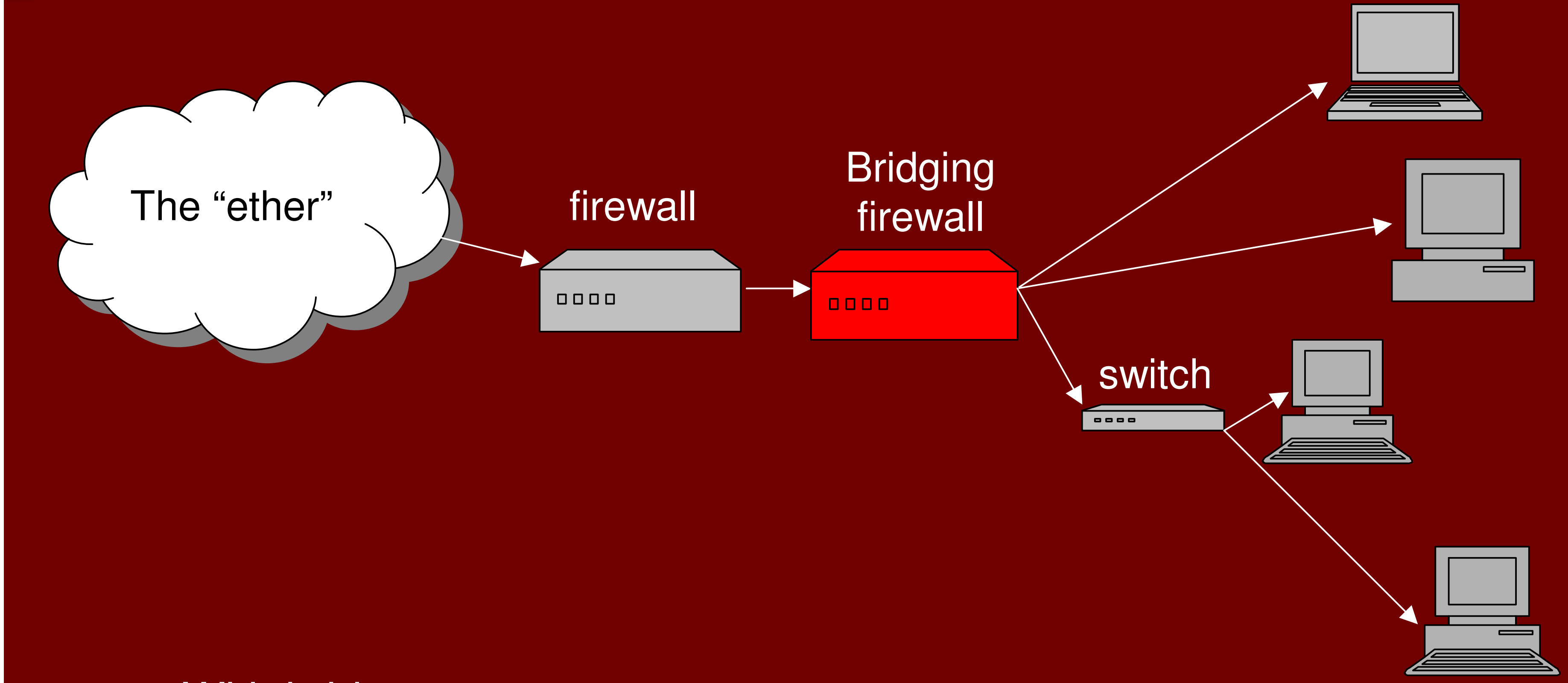
From LinuxNet

Bridging or Stealth firewalls
what is a bridging firewall?



The usual story

Bridging or Stealth firewalls where is a bridging firewall?



With bridge

Bridging or Stealth firewalls what is a bridging firewall?

- Device to monitor network segments
- Inline Packet scrubbing (antivirus too!)
- Device to further secure your firewall
- Manage traffic

Bridging or Stealth firewalls
Bridging firewall HOWTO

- Reasonably powered processor
- Decent memory
- If logging, consider your Disk space & speed
- 2 network cards (minimum) 3 recommended
- Linux kernel 2.2* or above

*the 2.2 kernel does not natively support bridging

Bridging or Stealth firewalls
Bridging firewall HOWTO

- Installation, strip down kernel!
- Make sure you have *bridge-utils*
- Make sure your network cards are all working
- Make sure your hardware is stress tested & tuned
- Make sure your drivers are stable

Bridging or Stealth firewalls sample setup

```
# ifconfig eth0 down
# ifconfig eth1 down
# brctl addbr mybridge
# brctl addif mybridge eth0
# brctl addif mybridge eth1
# ifconfig eth0 inet 0.0.0.0 up
# ifconfig eth1 inet 0.0.0.0 up
# ifconfig mybridge inet 0.0.0.0 up
```

Your interfaces must be down!

Call it “betty”

Adding interfaces

Interfaces up!

Finally!

Bridging or Stealth firewalls more funky commands!

```
# brctl show       (shows bridge info)
# brctl Betty showmacs       (shows mac ad)
port no   mac addr              is local?      ageing timer
  1     00:00:4c:9f:0b:ae         no                17.84
  1     00:00:4c:9f:0b:d2         yes                0.00
  2     00:00:4c:9f:0b:d3         yes                0.00
  1     00:02:55:1a:35:09         no                53.84
  1     00:02:55:1a:82:87         no                11.53
```

Set mac aging timers with

# brctl setageing *bridgename time*

Bridging or Stealth firewalls programs to strengthen the ‘wall

- tc, great for bandwidth management
- Snort
- Clamav
- Use blacklists
- Squid
- The “tables” family

Ebtables, what else?

- Ethernet protocol filtering.
- MAC address filtering.
- Simple IP header filtering.
- ARP header filtering.
- 802.1Q VLAN filtering.
- In/Out interface filtering (logical and physical device).
- MAC address nat.
- Logging.
- Brouter facility.

Inline snort

- Snort_inline is a modified version of Snort
- It then uses new rule types (drop, sdrop, reject)
- Tell iptables whether the packet should be dropped, rejected, modified, or allowed to pass based on a snort rule set.
- Think of this as an IPS that uses IDS signatures

Squid inline

- Intercept port 80 traffic
- Redirect that to localhost:3128
- Easy deploy due to transparency
- Bandwidth cut for often-accessed pages
- No need to configure individual machines
- Beware bridge performance!
- Web reporting
- Web filtering

Bridging or Stealth firewalls practical scenarios

- I cannot replace hub’s, what do I do?
- How can auditor check client firewall docs?
- How can pentester quietly watch network?
- How can I separate sensitive internal sections?
- How can I easily manage web traffic?
- How can I fight back against malware & viruses?
- How can I start addressing insider threats?
- Is it really that easy?

Queries ?

Bridging firewall project site- http://linux-net.osdl.org/index.php/Bridge

Ebtables- http://ebtables.sourceforge.net

Iptables- http://netfilter.org

inline snort- http://snort-inline.sourceforge.net

squid- http://www.squid-cache.org

Clamav- www.clamav.net

All due apologies to the great Bruce Lee (R.I.P.)