Tales From The Early Days of the Firewall

Marcus J. Ranum
<mjr@trusecure.com>

WARNING!!!

Some of this (just some of it) is tongue in cheek

You figure it out!

Who?

- Who am I, and how did I get here?
  - Security products designer since 1989
  - Wrote the first commercial firewall product
  - Designed an early VPN that didn’t succeed
  - Early innovator in IDS market
  - Today: consultant, industry analyst, farmer, horse-trainer, senior analyst for TruSecure, teacher, writer, etc, etc.

So What's This About?

- "In the beginning… "
  - If you grow up around historians, you're doomed to become one!
- Computer Security, as an industry, has a lot of hype (always something *new*!)
  - If you know about the evolution of a technology, can you tell something about its future?

Who is this guy?

Dave Presotto,
Bell Labs
For most firewall stuff, it turns out that “Dave was there first”

Earliest Days

- Nobody has determined for sure who coined the term “firewall”
  - Gene Spafford wants to, but Cheswick says he’d heard it used a long time before Spaf got into security
  - Brian Reid may be the originator, but Brian says he thinks someone else used it first
  - “hackers” (movie) 1983 uses “firewall”

.. Lost in the mists of time.

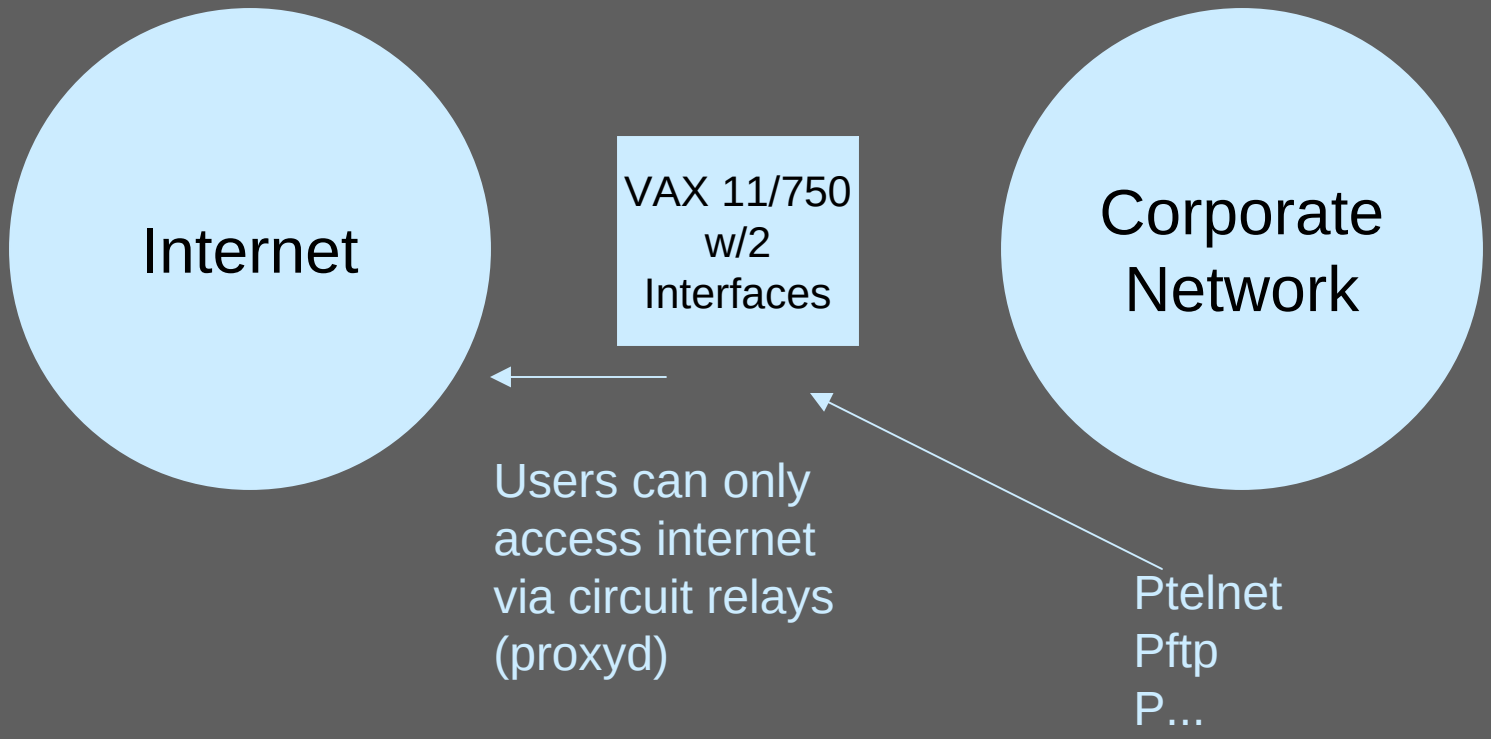
Round 1: The Players

- The AT&T guys
  - Dave Presotto
  - Bill Cheswick
  - Steve Bellovin
- The DEC gang
  - Brian Reid
  - Jeff Mogul
  - Paul Vixie

The AT&T Gateway

- Originally built by Dave Presotto and Fred Trickey
  - Taken over by Bill Cheswick in 1987
  - Definition of firewall: “A single point between 2 networks where all traffic must pass. Traffic can be controlled and may be authenticated. All traffic is logged.”
  - Described by Cheswick and Bellovin in 1990 USENIX proceedings

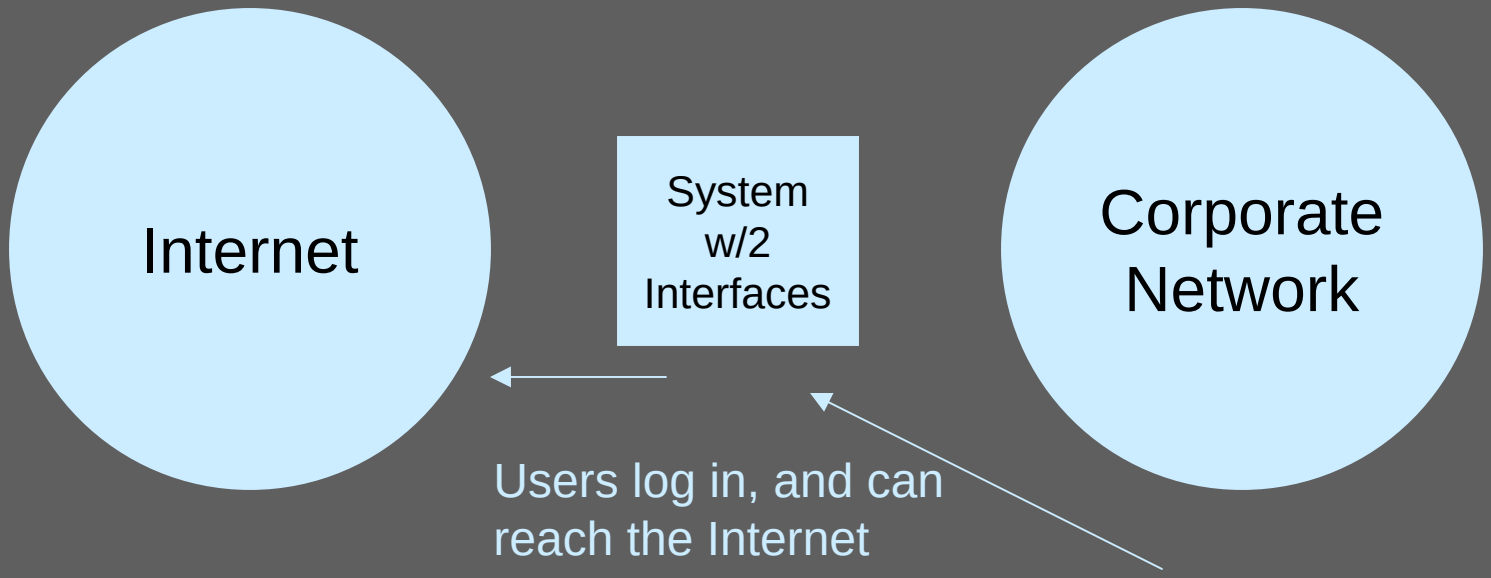
The AT&T Gateway



The DEC gang

- Brian Reid had “the internet disease”
  - DEC was connected at 3 places (Palo Alto first, Cambridge second, DC third)
    - Most of these connections were “gatekeepers”
    - 9600 baud was the highest (initial) connection
    - 56k in 1987(?)
    - Upgraded to T1 in 1988

The DEC Gatekeeper V1



The View

- “Firewalls are barriers between ‘us’ and ‘them’ for arbitrary values of ‘them’”

-Steve Bellovin

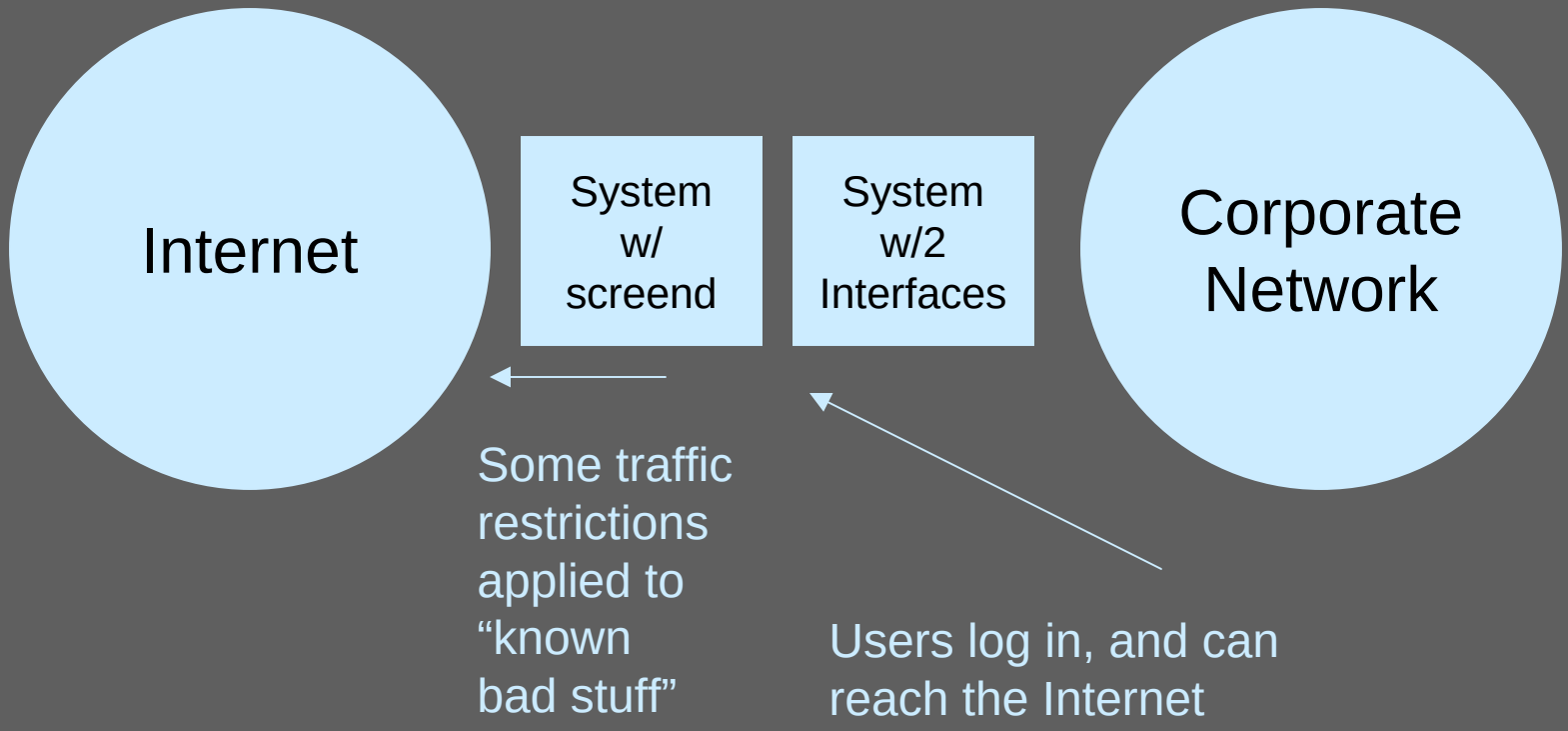
The First Policy

- “Allow anyone “in here” to get out, but keep people “out there” from getting “in”
  - This may be the ***only*** firewall security policy that has ever been used (barring fine details)

Round 2: The Newbies

- Marcus Ranum starts working at DEC DC late 1988
- Jeff Mogul at DEC Palo Alto starts screend
- Geoff Mulligan at DEC Palo Alto starts thinking about firewalls
- Bob Braden (ISI) starts looking at “Visas” under DARPA funding

The DEC Gatekeeper V2



Round 3: Break Out

- Fred Avolio assigns Marcus to “build a firewall like the one in Palo Alto”
- Marcus Ranum instead designs “no user” firewall
  - Premise: 99% of security problems involve having a user logged into a system
  - Therefore: if the user can’t get on the system, the security will be much better

(Dave Presotto was way ahead on this point)

Firewall Services

- USENET news
- FTP
- Telnet
- Mail (DNS)

Round 3: Break Out

- Geoff Mulligan starts writing what (today would be called) a “stateful firewall”
  - Track outgoing connections
  - Allow incoming responses
  - Keep state at IP level

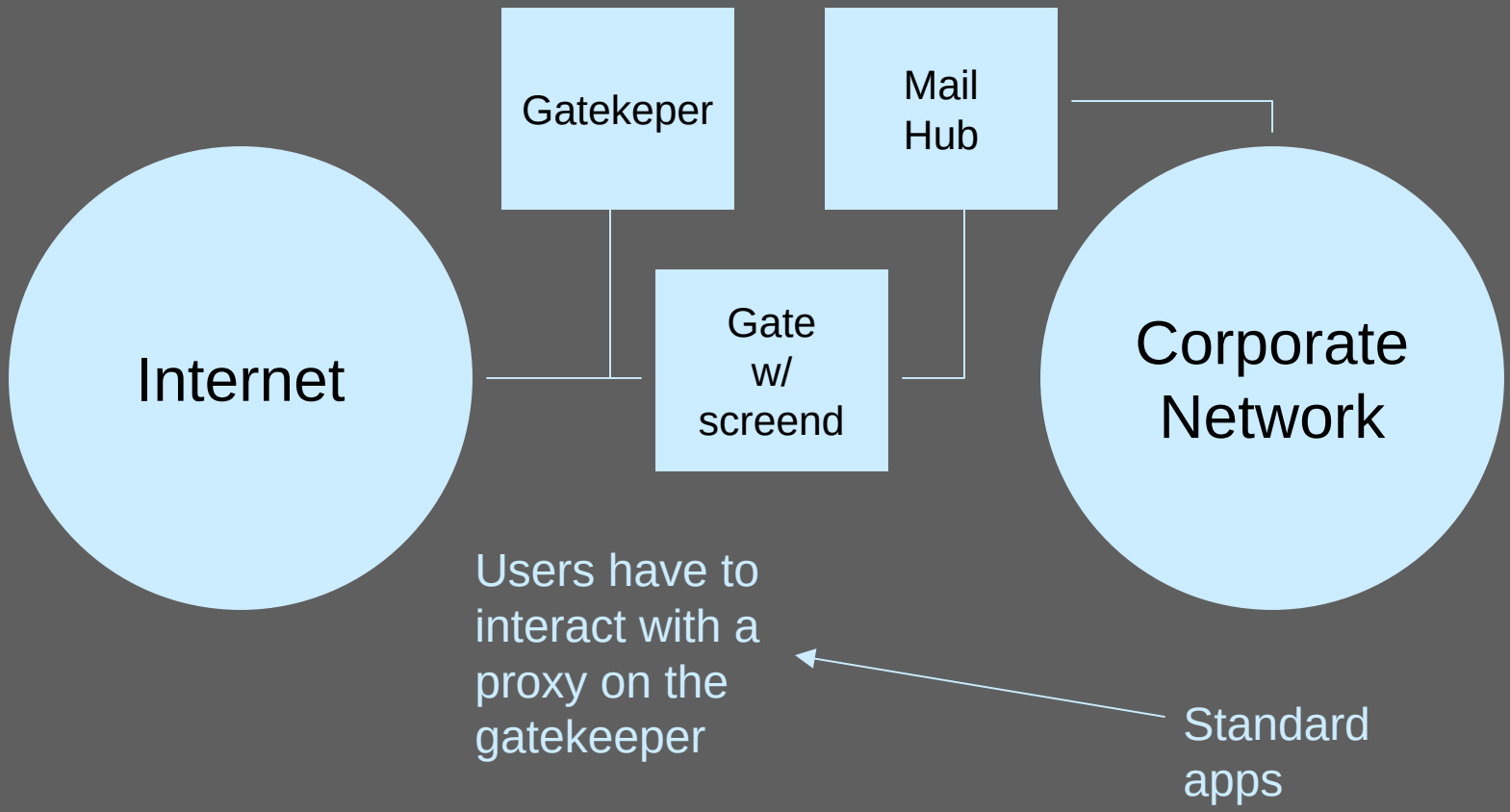
Product

- Marcus Ranum's firewall goes live mid-late 1990
  - Rolled-out internally to Cambridge
  - ***Not*** adopted in Palo Alto
    - First documented case of firewall users refusing to adopt a more stringent policy and blocking installation of a security technology through use of office politics or passive-aggression

Product

- Ranum’s firewall sold to Dupont, Jun 1991
  - $75,000 + install
- Name:
  - Packaged Internet Gateway (PIG)
  - Screening External Access Link (SEAL) (Fred Avolio came up with this one)

The DEC SEAL


Gatekeper
Mail Hub
Internet
Gate w/ screend
Corporate Network
Users have to interact with a proxy on the gatekeeper
Standard apps

SEAL Facts

- All told the SEAL was less than 10,000 lines of code
- User interface was “vi(1)”
- Took a total of about a week to write
- Marcus always felt guilty for throwing more hardware at the problem than was necessary
  - If you recall, DEC sold computers not software - being hardware-heavy was a plus

Round 4: Emerging Market

- After the DEC SEAL there were a number of products coming to market
  - Raptor Eagle (founded by Dave Pensak, a research scientist at Dupont's facility where the first SEAL was installed)
  - ANS Interlock

The Firewall Toolkit

- Marcus Ranum designed and developed for DARPA on behalf of The Whitehouse
  - Modular set of proxies for facilitating firewall-building
  - Code made available October 1, 1993
  - First sold to Dun and Bradstreet October 2, 1993

The Firewall Toolkit V2

- Added http proxy (Peter Churchyard)
- Productized into TIS Gauntlet firewall
  - Added character-based user interface
  - Added documentation
  - Added BSDI-based system configuration
  - 2 floppy disks; $25,000

The Old School Guys

- Meanwhile DOD is trying to build systems (they call them “guards”) between classified and unclassified networks
  - Lots of Orange Book concepts
  - Problem is how to automatically “downgrade” classified material
  - The DOD researchers are getting left out

The Old School Guys Retrench

- Secure Computing (Sidewinder)
  - BSDI-based with “domain type enforcement”
  - First firewall to market using massive hype
    - … But otherwise another proxy firewall
- Harris’ CyberGuard
  - Proxy firewall built on a secure platform (based on B-1 target operating system)

More Commercialization

- Several other firewall companies appear on market
  - At least 2 are rip-offs of firewall toolkit code
    - One goes public, gets bought, and its founders get rich
    - The other gets bought (and its founders get rich)

The Israeli Connection

- 2 Israeli guys (Gil Shwed, Shlomo Kramer) arrive at TIS Glenwood
  - Try to sell Steve Walker and Fred Avolio a prototype firewall they call “Firewall-1”
  - Unable to locate a US reseller they started their own company: CheckPoint

(They did OK. Gil’s worth about $300million, now)

CheckPoint Eats Lunches

- CheckPoint's early "stateful inspection" didn't actually do much
  - So they sold the product based on its performance and flexibility
  - Security began to take second place to packets per second as a criterion

The Israeli Slam

- A sales rep from Raptor (we think…) starts a rumor that CheckPoint is backdoored
  - This craters CheckPoint's federal/DOD sales
  - NSA has a team examine the product; further weirdness happens
    - "Checkpoint Claims"

The Hardware Guys

- Once firewalls had become “a market” the hardware guys stepped in
  - Watchguard
  - Sonic Wall
- Premise: Fast = Good
  - Security permanently takes backseat to packets per second

Today

- Which brings us to today!
  - With rapid-spreading worms on the rise a good layer 7 firewall is ***important*** again!