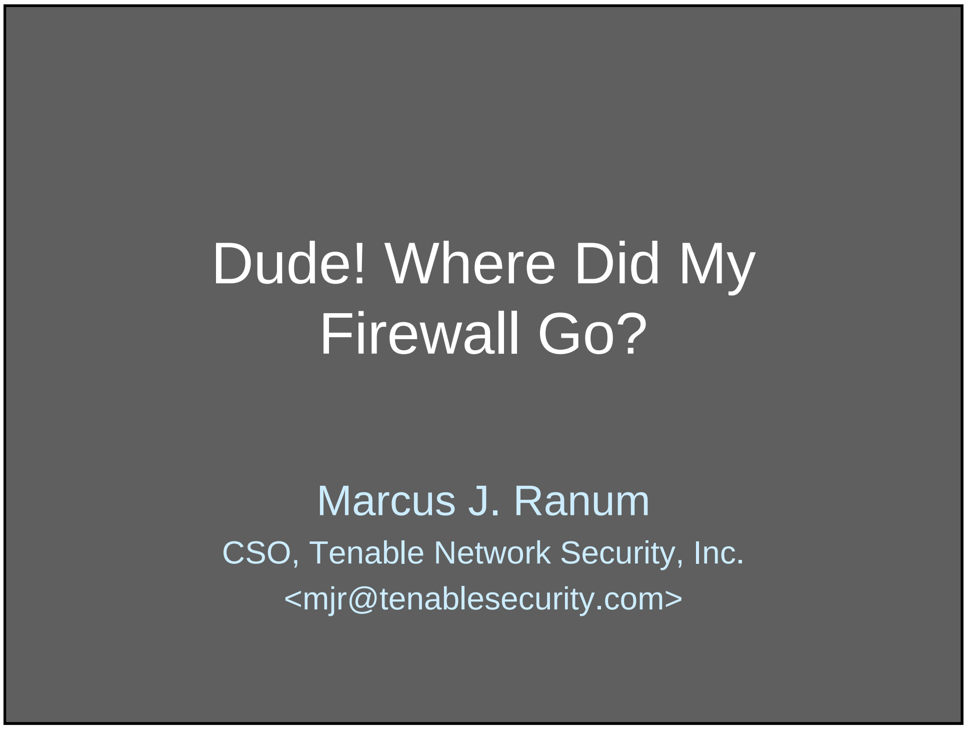
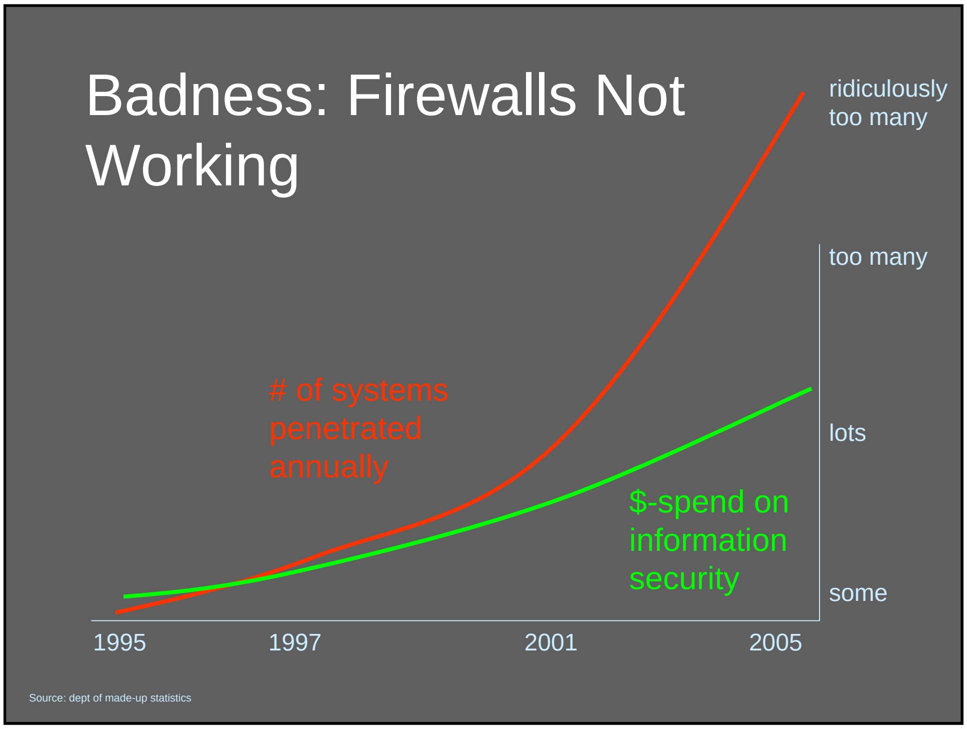


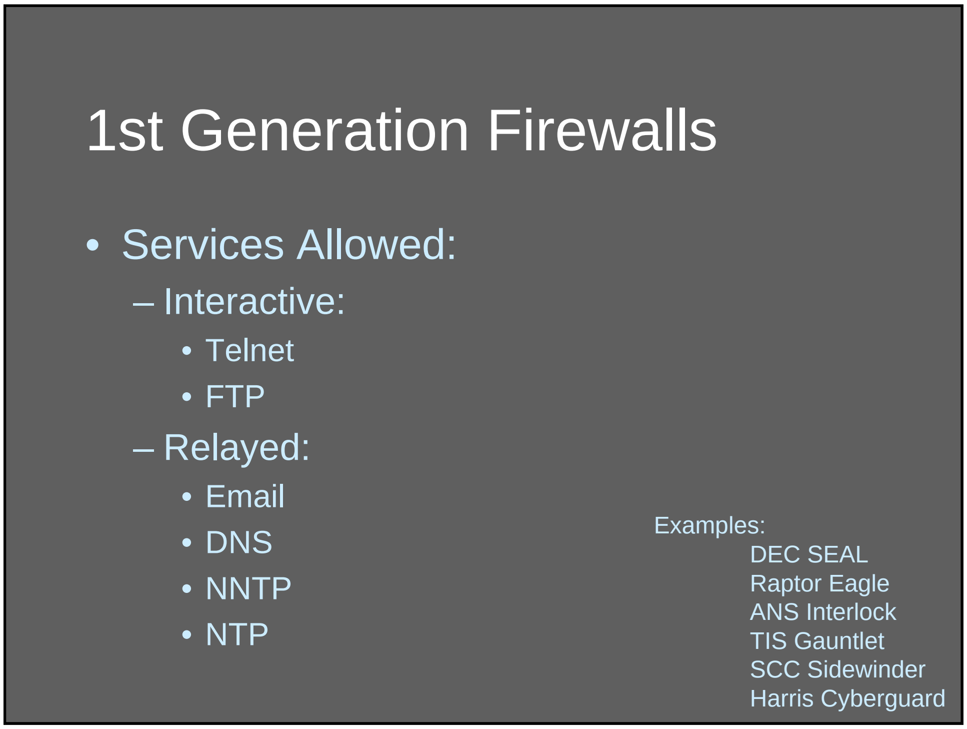
Dude! Where Did My Firewall Go?

Marcus J. Ranum
CSO, Tenable Network Security, Inc.
<mjr@tenablesecurity.com>



Badness: Firewalls Not Working

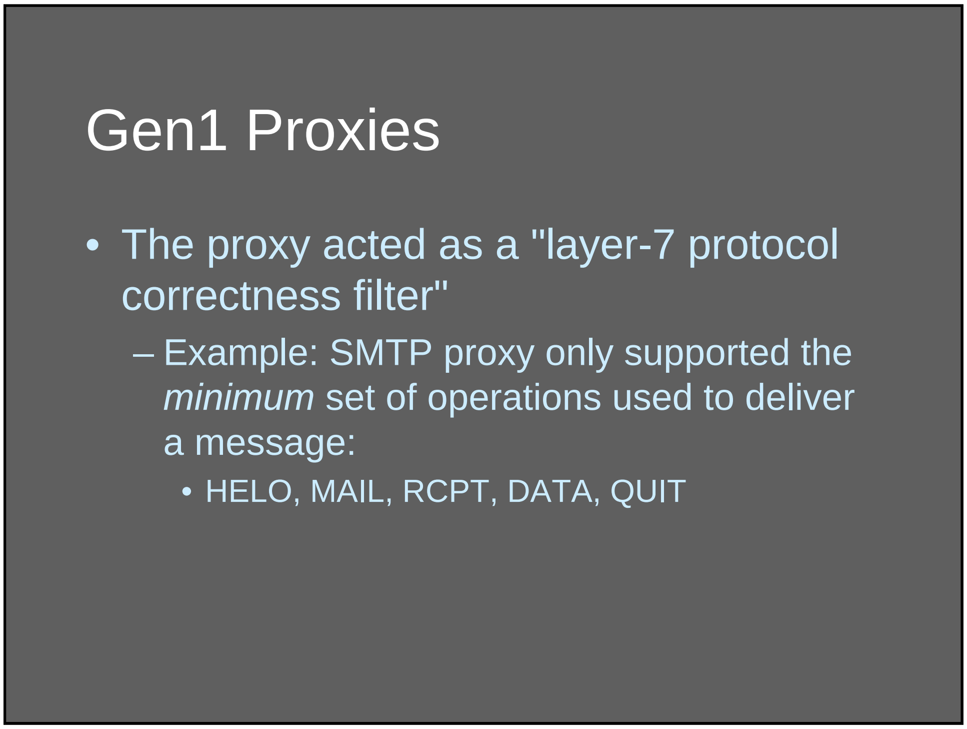
Source: dept of made-up statistics



1st Generation Firewalls

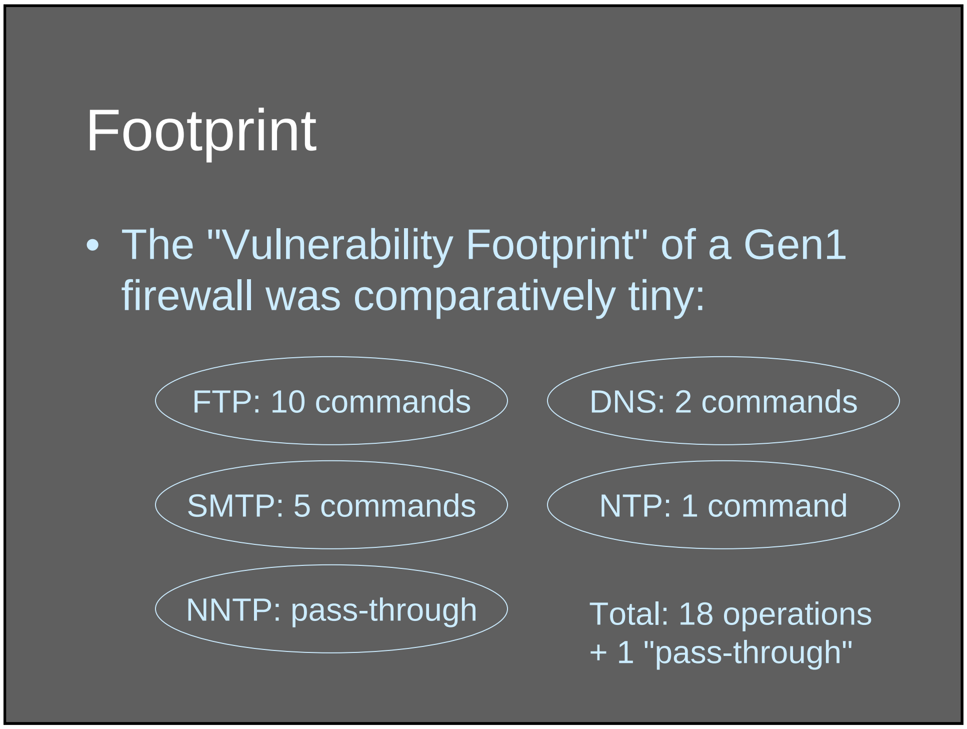
- Services Allowed:
  - Interactive:
    - Telnet
    - FTP
  - Relayed:
    - Email
    - DNS
    - NNTP
    - NTP

Examples:
DEC SEAL
Raptor Eagle
ANS Interlock
TIS Gauntlet
SCC Sidewinder
Harris Cyberguard



Gen1 Proxies

- The proxy acted as a "layer-7 protocol correctness filter"
  - Example: SMTP proxy only supported the *minimum* set of operations used to deliver a message:
    - HELO, MAIL, RCPT, DATA, QUIT



Footprint

- The "Vulnerability Footprint" of a Gen1 firewall was comparatively tiny:

FTP: 10 commands

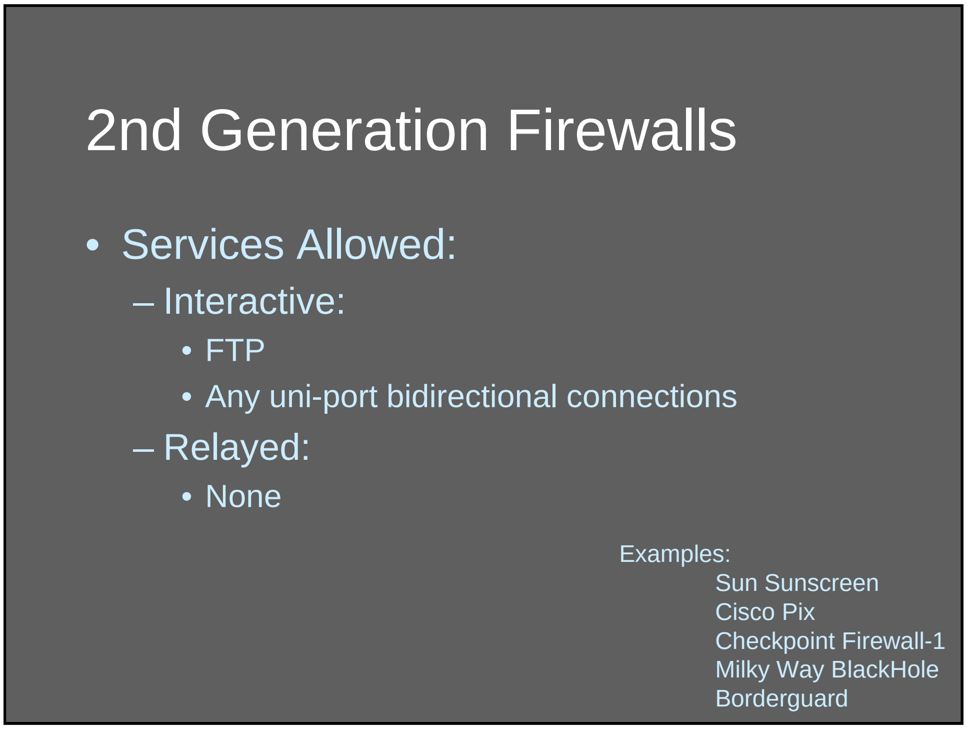
DNS: 2 commands

SMTP: 5 commands

NTP: 1 command

NNTP: pass-through

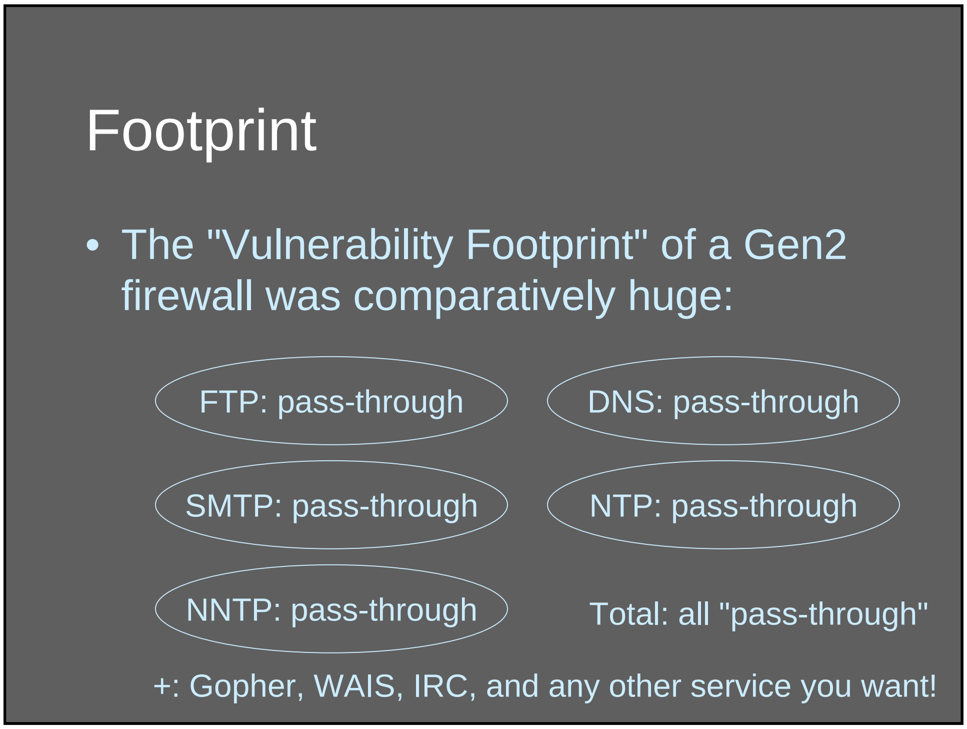
Total: 18 operations
+ 1 "pass-through"



2nd Generation Firewalls

- Services Allowed:
  - Interactive:
    - FTP
    - Any uni-port bidirectional connections
  - Relayed:
    - None

Examples:
Sun Sunscreen
Cisco Pix
Checkpoint Firewall-1
Milky Way BlackHole
Borderguard



Footprint

- The "Vulnerability Footprint" of a Gen2 firewall was comparatively huge:

FTP: pass-through

DNS: pass-through

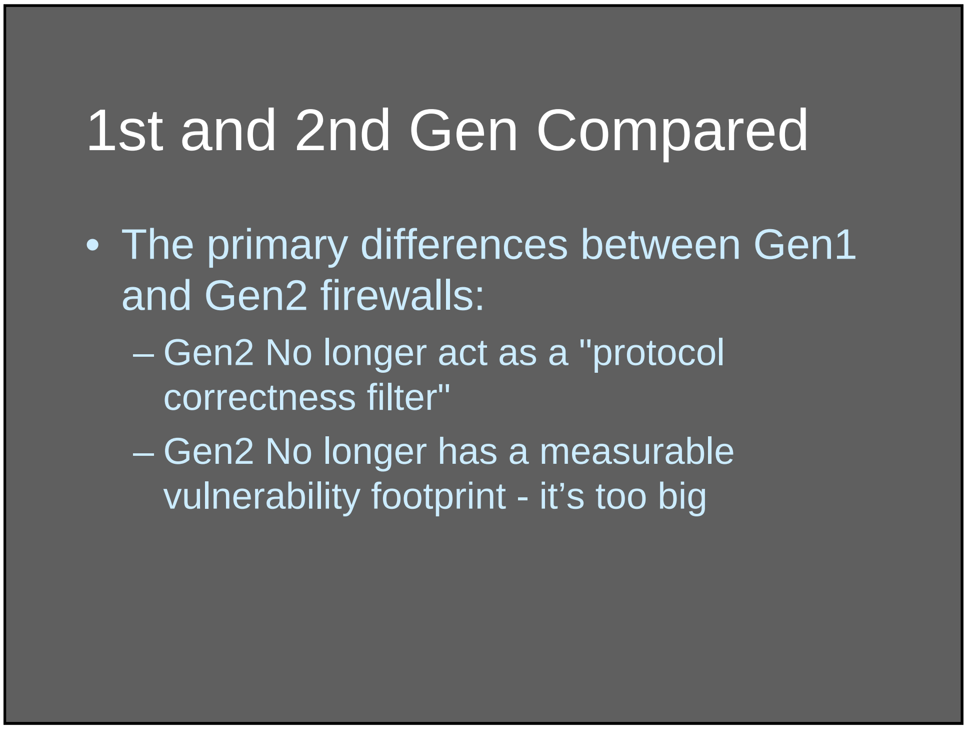
SMTP: pass-through

NTP: pass-through

NNTP: pass-through

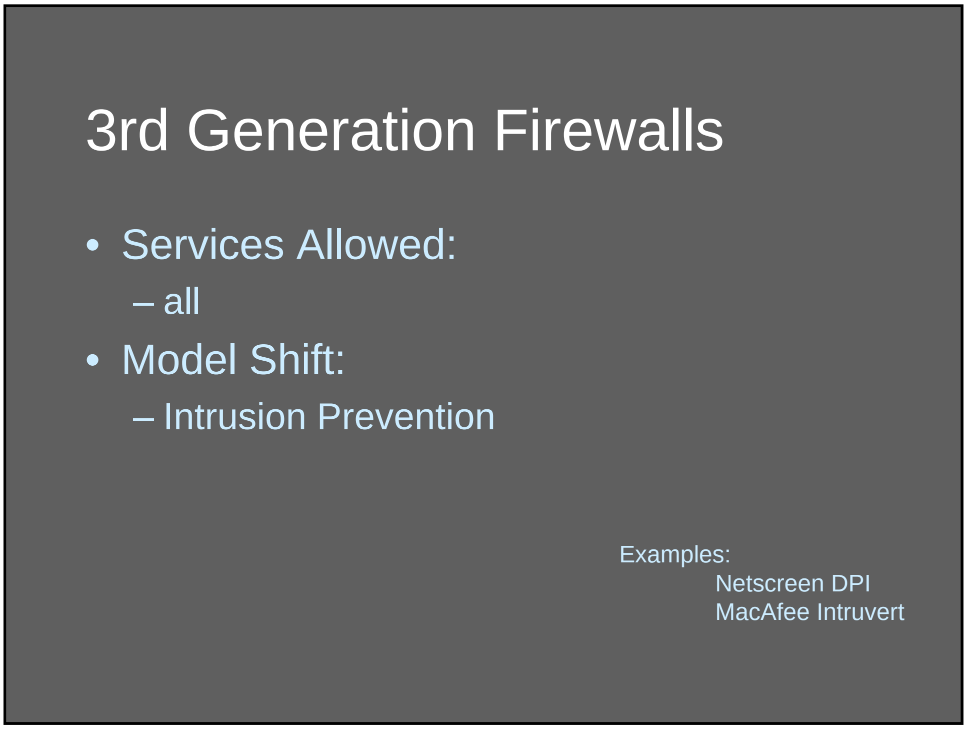
Total: all "pass-through"

+: Gopher, WAIS, IRC, and any other service you want!



1st and 2nd Gen Compared

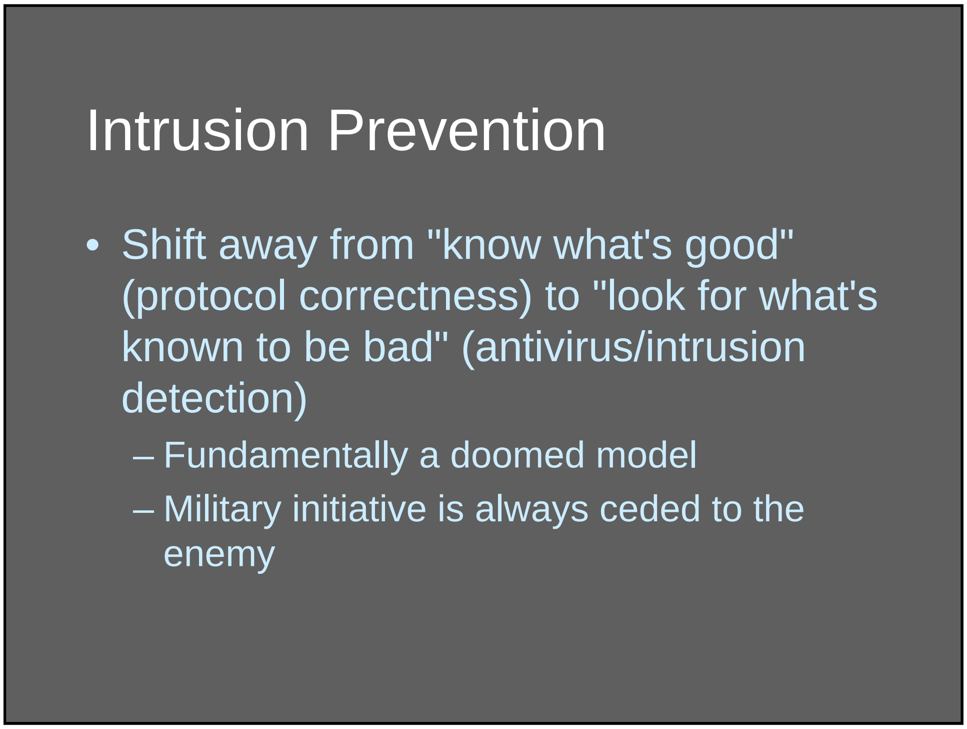
- The primary differences between Gen1 and Gen2 firewalls:
  - Gen2 No longer act as a "protocol correctness filter"
  - Gen2 No longer has a measurable vulnerability footprint - it’s too big



3rd Generation Firewalls

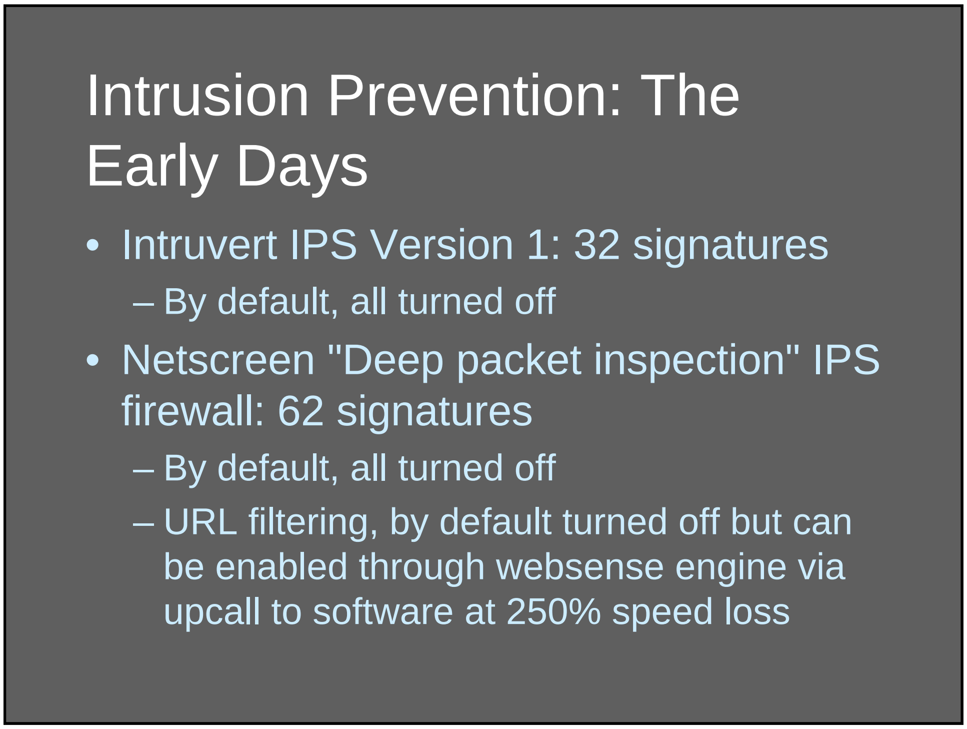
- Services Allowed:
  - all
- Model Shift:
  - Intrusion Prevention

Examples:
Netscreen DPI
MacAfee Intruvert



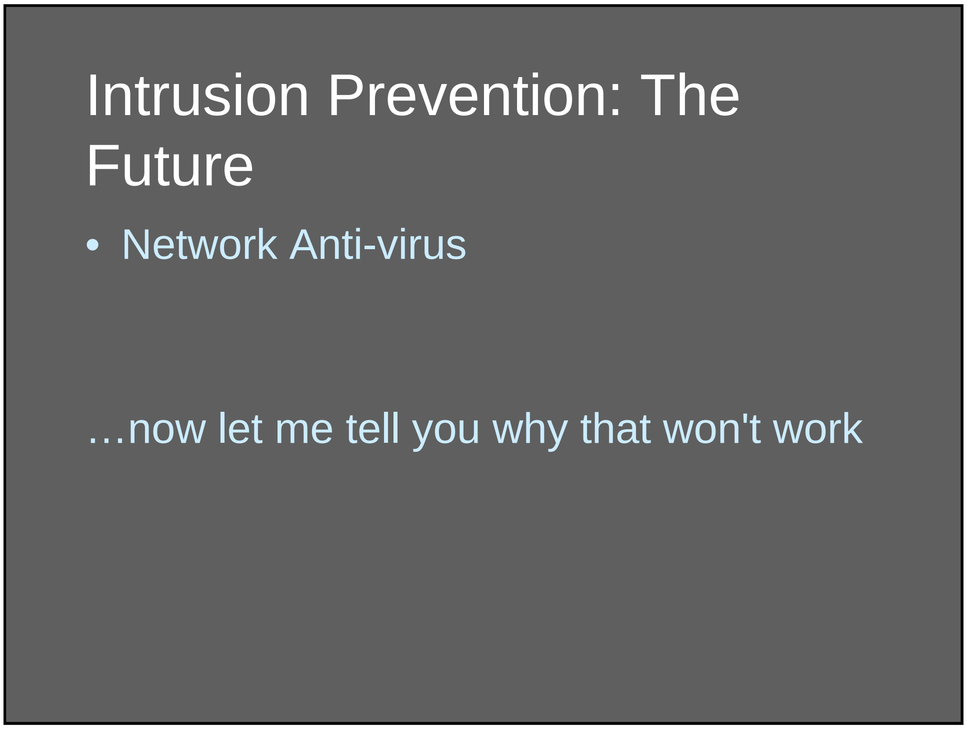
Intrusion Prevention

- Shift away from "know what's good" (protocol correctness) to "look for what's known to be bad" (antivirus/intrusion detection)
  - Fundamentally a doomed model
  - Military initiative is always ceded to the enemy



Intrusion Prevention: The Early Days

- Intruvert IPS Version 1: 32 signatures
  - By default, all turned off
- Netscreen "Deep packet inspection" IPS firewall: 62 signatures
  - By default, all turned off
  - URL filtering, by default turned off but can be enabled through websense engine via upcall to software at 250% speed loss



Intrusion Prevention: The Future

- Network Anti-virus

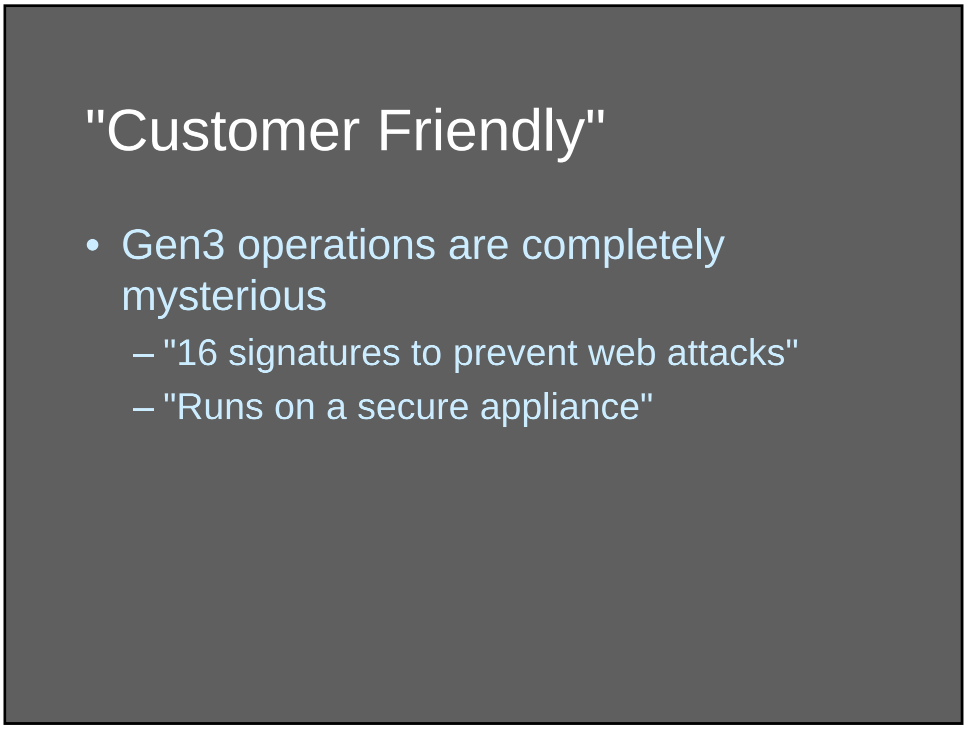
…now let me tell you why that won't work

"Firewall Friendly"

- Gen1 and Gen2 firewalls did not have to deal with protocol-over-protocol tunnelling
  - – Today it's the norm
  - – Makes protocol correctness verification effectively impossible
    - Makes protocol attack detection effectively impossible as well: what about SSL?

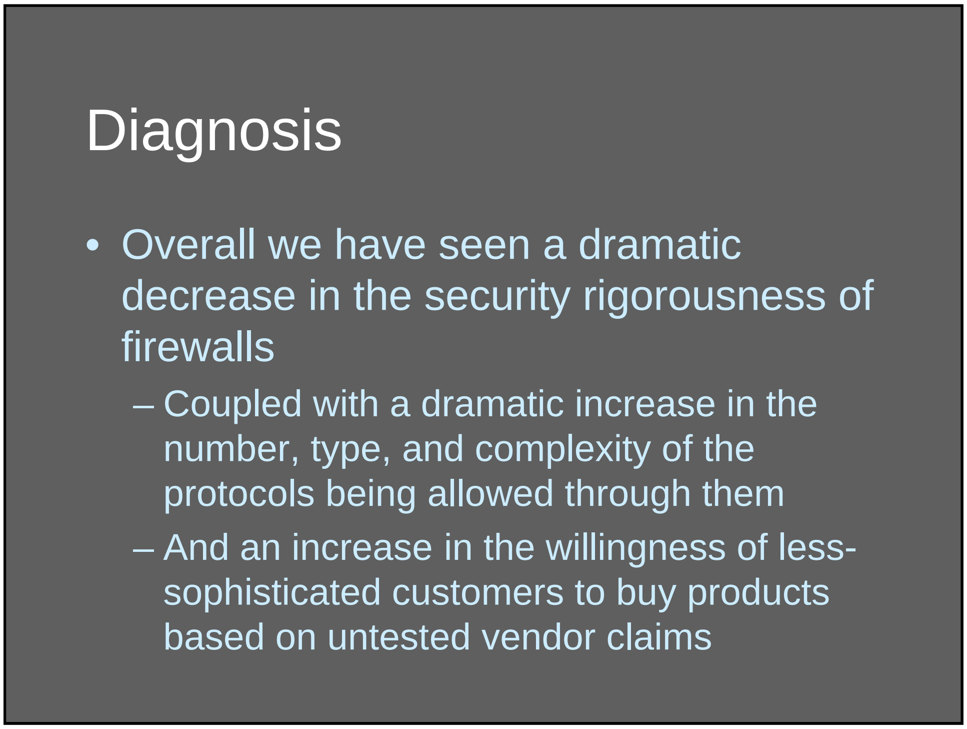
"Customer Friendly"

- Gen1 operation was largely transparent to the customer
  - – Features and algorithms documented
  - – Protocols supported listed
- Gen2 operation was largely closed to the customer
  - – Stateful multi-level packet inspection (what the heck is that?)
  - – Protocols back and forth not specified



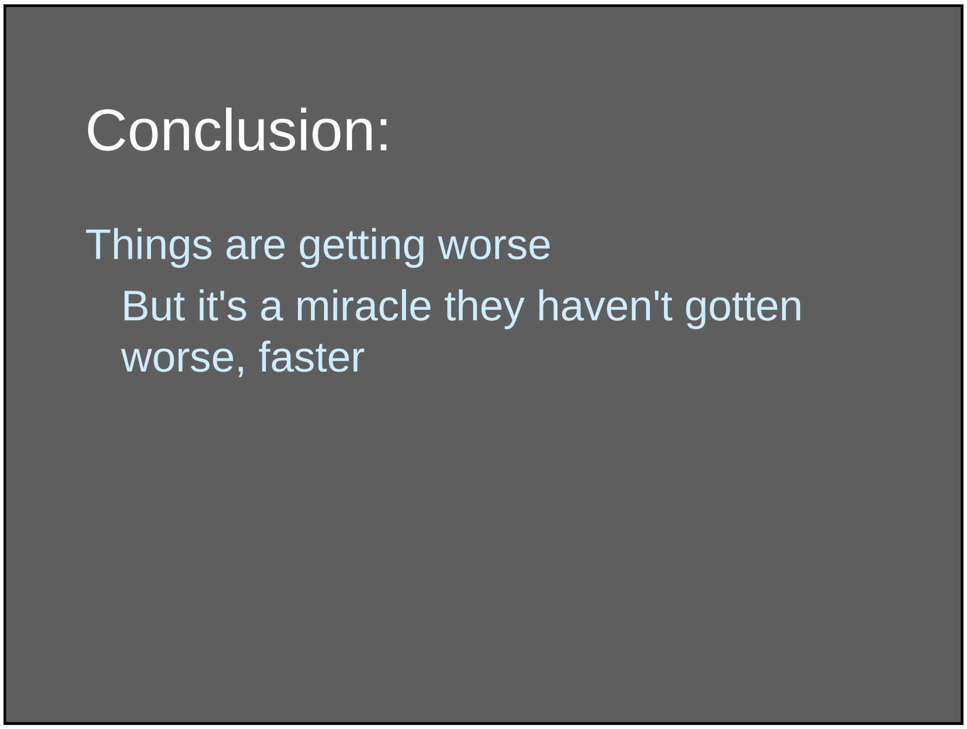
"Customer Friendly"

- Gen3 operations are completely mysterious
  - "16 signatures to prevent web attacks"
  - "Runs on a secure appliance"



Diagnosis

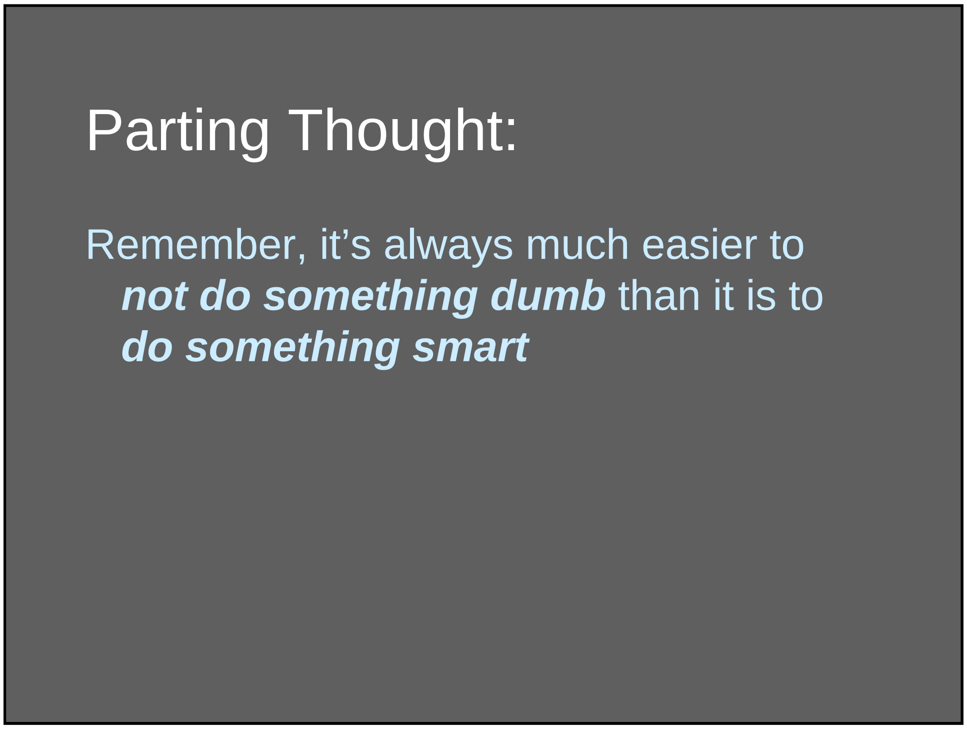
- Overall we have seen a dramatic decrease in the security rigorousness of firewalls
  - Coupled with a dramatic increase in the number, type, and complexity of the protocols being allowed through them
  - And an increase in the willingness of less-sophisticated customers to buy products based on untested vendor claims



Conclusion:

Things are getting worse

- But it's a miracle they haven't gotten worse, faster



Parting Thought:

Remember, it’s always much easier to ***not do something dumb*** than it is to ***do something smart***