Procera Networks at UNE

Inspecting the packets, truly, madly, deeply

Gordon Smith
Principal IT Officer
Information Technology Directorate
University of New England

Part 1 – ancient history

- Once upon a time …
  - AARNet connections were 48 kbit/s
  - Cisco HyBridge bridge/router
  - We ran IP and DECnet (yes, Australia-wide DECnet)
  - Much better than previous 4800 baud AUSTPAC X.25 that connected us to ACSnet (munnari) for store and forward email and USEnet news (and a bit of file transfer)

Part 1 – ancient history

- Firewall?
  - Nope, not in early 1990
  - Wide open incoming / outgoing
  - No such thing as HTTP
  - Telnet, SMTP and FTP
  - In general, PC's didn't do TCP/IP (Trumpet Winsock anybody?) so connectivity was from Unix systems

Part 1 – ancient history

- The easy life came to an end
  - Vulnerabilities with Sun RPC were reported (for example)
  - Simplistically, port 111 was block
  - A single firewall rule (above) began the journey to the concept of keeping the baddies out
- More blocking rules were imposed on incoming
- Outgoing was usually wide open

Part 1 – ancient history

- Further along the timeline new applications appeared
- Gopher (port 70)
- "The world wide web" (port 80)
- NNTP Network News (port 119)
- Traffic built up (remember Mosaic browser? 1992)

Part 1 – ancient history

- Better access controls were required
- The great ACL flip (reverse thinking)
- New default posture was block everything, except where permitted by policy
- No more blocking "baddies" one by one
- Proxy servers came along (could nominate a handful of IP addresses that required outgoing access, block the rest) [1998]

Part 1 – ancient history

- This was OK as long as people believed that applications were locked to a layer-3 port.
  - Eg SMTP on port 25
  - HTTP on port 80
  - NNTP on port 119
  - etc.

Part 1 – ancient history

- Number of ACL's "grew like Topsy"
- The "permit by policy" meant that huge lists of ACLs were generated.
- Performance was enhanced in Cisco-land with use of reflexive ACLs and CBAC (context-based access control)

Part 1 – ancient history

- This was "The Big Lie"
  - The was no linkage between port number and the protocol passing through that port
- CBAC was enhanced to help (eg if port 110 was defined to be POP, were POP commands seen passing through?)

Part 1 – ancient history

- Such was the state of affairs
- Alternative technologies were non-existent or just an itch in an engineers knee-cap

Part 2 – recent history

- Then …
- Those itches for a better life became a reality, albeit infant reality
- …

Part 2 – recent history

- Several QUESTnet's ago …
  - One-day workshop demonstrated two products
    - Packetlogic traffic management appliance – Netintact[1]
    - Jet Billing end-user quota management – Obsidian[2]

[1] http://en.wikipedia.org/wiki/Netintact
[2] http://www.obsidian.com.au/

Part 2 – recent history

- The new innovation (at least for me) was Packetlogic's Deep Flow Inspection
  - Monitor connection at startup until
    - Protocol was determined by signature
    - Or deemed to be "unknown"
- Jet Billing monitored usage per-user and acted if user approached or exceeded quota

Part 2 – recent history

- We purchased two PL7600 traffic management devices and a PL1000 statistics device
- Sat inline between AARNet and campus network
- Run in addition to Cisco ACLs to pass traffic by signature-based rules

Part 2 – recent history

Part 3 – current era

- More time passed
- For various technology and business reasons we had to replace Packetlogic PL7600's.
  - became end of life
  - didn't understand IPv6
  - couldn't be upgraded to 10 gigabit/s
  - was clumsy to keep two boxes sync'ed with same configuration (one on each AARNet link)

Part 3 – current era

- Review of devices in the market was undertaken
  - some still didn't do IPv6
  - some couldn't do 10 Gbit/s (or had 10g interface but couldn't process packets at anywhere near line rate)
  - Some still didn't "get it" that applications aren't locked to a layer-3 port

Part 3 – current era

- Packetlogic is currently in use in nearly half of Australia's universities
- Some innovative interfacing being done to customise to university-specific use (John Croft @ JCU)
- Every edge port on our network uses 802.1x authentication so access to end-user ID is easy(ish) to match users to IP addresses (IP address → MAC address → username)
- At the end of the day we stuck with something we knew – decided to purchase new Packetlogic devices

Part 3 – current era

- We purchased
  - Two PL8720 devices, one for each diverse path gigabit link to Sydney
  - One PL1200 statistics aggregator / reporting device
  - One PL5600 low end device for use in test lab
- Gives us
  - 3 x 10 gigabit/s channels
  - IPv6 firewalling
  - Smart rate-limiting
  - Live traffic monitoring

Part 3 – current era

Part 3 – current era

- Devices are managed by client-side GUI software
- Config changes on one device are automatically proxied to the other device to keep configs in sync
- Protocol signatures are updated fortnightly
- Easy process to generate PCAP file to send off to get new protocols generated

Part 3 – current era

- Annoying negatives:
  - Interface to configure firewall rules gets clumsy when more than a few tens of rules are in place
  - Signatures are updated fortnightly, but there is no easy way to map firewall rules to new signatures set
- Both issues being addressed in next major firmware release (v13.0, v13.1)

Part 4 – realtime

- Realtime (I hope) demo

- Questions ?