SAND2007-3053C

Web Proxy / Filter Appliance

John Long
jplong@sandia.gov
505-845-8622

The context…

- Sandia interacts with the web in two primary ways – email and browsers
- Email team could stop only a (high) percentage of threats with one filter, another filter found more
- If there is enough traffic, multiple filters save money
- Burton and Gartner also recommend multiple filters
- Our current filter does a good job, but malware does occasionally sneak through
- Okay, but what about latency? Vendors claim very low latency, but we think we have to try it.

A divided marketplace, 1 --

- The marketplace is split between large and small businesses
- The small business approach:
  - Selling software for your platform appeals to smaller firms
  - Performance is adequate
  - Their people feel comfortable with the machine setup
- The large enterprise approach:
  - Special hardware (configuration?)
  - Special operating system to speed context switching
  - And of course, their application software
  - Some recommend two boxes with functions split between them

A divided marketplace, 2 --

- “Set and forget” vs “hands on”
- Set and forget:
  - Buy an appliance and install it in the back room
  - Let me know when I need to update something
  - Updates are vetted, which takes time
- Hands on:
  - Buy an appliance and put it with other servers
  - Carefully set up the software to do the best job
  - Tweak the setup as the environment changes
  - Monitor intrusion attempts, modify filter rules when appropriate
  - Install vendor updates when they are releasedd

Okay, that's not unusual (?)

- Burton and Gartner explain why the appliance should be chosen to fit its new home
- Most vendors target their marketing info to a specific group
- Yes, there are always arrogant vendors – watch their statements carefully, ask questions
- Most reviews recommend a specific context
- Some vendors try to broaden their appeal, but most aren't very successful

Approaches to filtering

- There is no single approach to web filtering, and the more you look at vendors, the more differences you see
- Rather than equally good approaches, we must choose the best from the equally mediocre
- Gartner believes that vendors should have deep expertise in several areas (filtering, scanning, AV, AM, etc.). Some buy one capability from other vendors.
- Make sure that the vendor's philosophical approach matches yours (top down, not bottom up)

We are a moderately large enterprise, and we work “hands on”

- Since we plan to have multiple filters in serires, speed is important
- Since we expect to often do deep packet inspection, speed is important
- We have load balancing and will use filters in parallel
- The number one requirement is flexibility and granularity of control of the filter’s rules
- We are aggressive with new threats, and want as much protection as possible as soon as possible – even before we know much about the threat

Isn’t that expensive?

- Let’s look at the costs –
  - Cost of the filter
  - Training and installation
  - Maintenance is kind of absorbed into “hands on” tweaking, log inspection, and setting up new rules
- And the alternative –
  - When malware intrudes we must analyze it and track it down, often visiting the desktop in the process
  - Slow, painful work is necessary
  - We think stopping a little more malware saves enough money to pay for the filter

Improving security saves money!

- Good cyber security at Sandia is a requirement
- We are being asked to look for ways to save money in our processes
- Installing a new filter will increase labor costs for a short while, and then reduce workloads

Market survey

- We looked at specialized devices and specialized operating systems
- We looked for flexibility in configuration
- Blue Coat and IronPort fit our needs best
- Blue Coat seems to be a more mature product than IronPort
- Having both of them in series would be nice

Random data

- I was not overly impressed with the support from any vendor contacted. They all have folks who care, but there is always a hole in their support somewhere.
- Beware of getting locked into lengthy contracts to save yearly costs as the market matures
- Email and web filtering are beginning to converge, and this will help detect phishing and other scams.
- Two-factor authentication is almost ready and it's important
- We have a lot of internal disagreement on priorities concerning how a filter should work

Conclusion

- Added filtering (in series) for web content would be helpful and stop some malware
- The marketplace is fractured
- No single approach wins consensus approval
- In this context, better security saves money
- We would like to have Blue Coat first, but both would be nice