Threat Management and Perimeter Protection

Don't let the bad guys in!

28 July 2011

Biography

Chris Polkinghorne

Security Technical Lead

- Oversight of all security operations
- Security capabilities development

Located in Brisbane, Queensland, Australia

Six years in security industry working in banking and Defence environments.

Melbourne IT

Provides services to over 350,000 customers across the world to a variety of clients from small business through to large government departments.

Service offerings range from DNS, web hosting and online brand protection, through to complete managed IT services.

Challenges

One major client is a large Australian Government Education Organisation

- 488079 students
- 39600 teachers
- 1235 state schools
- 231447 computing devices
- Approximately 20 Terabytes monthly traffic volume
- High public profile
  - Anything involving security and kids needs to be treated very seriously
  - Very sensitive data.

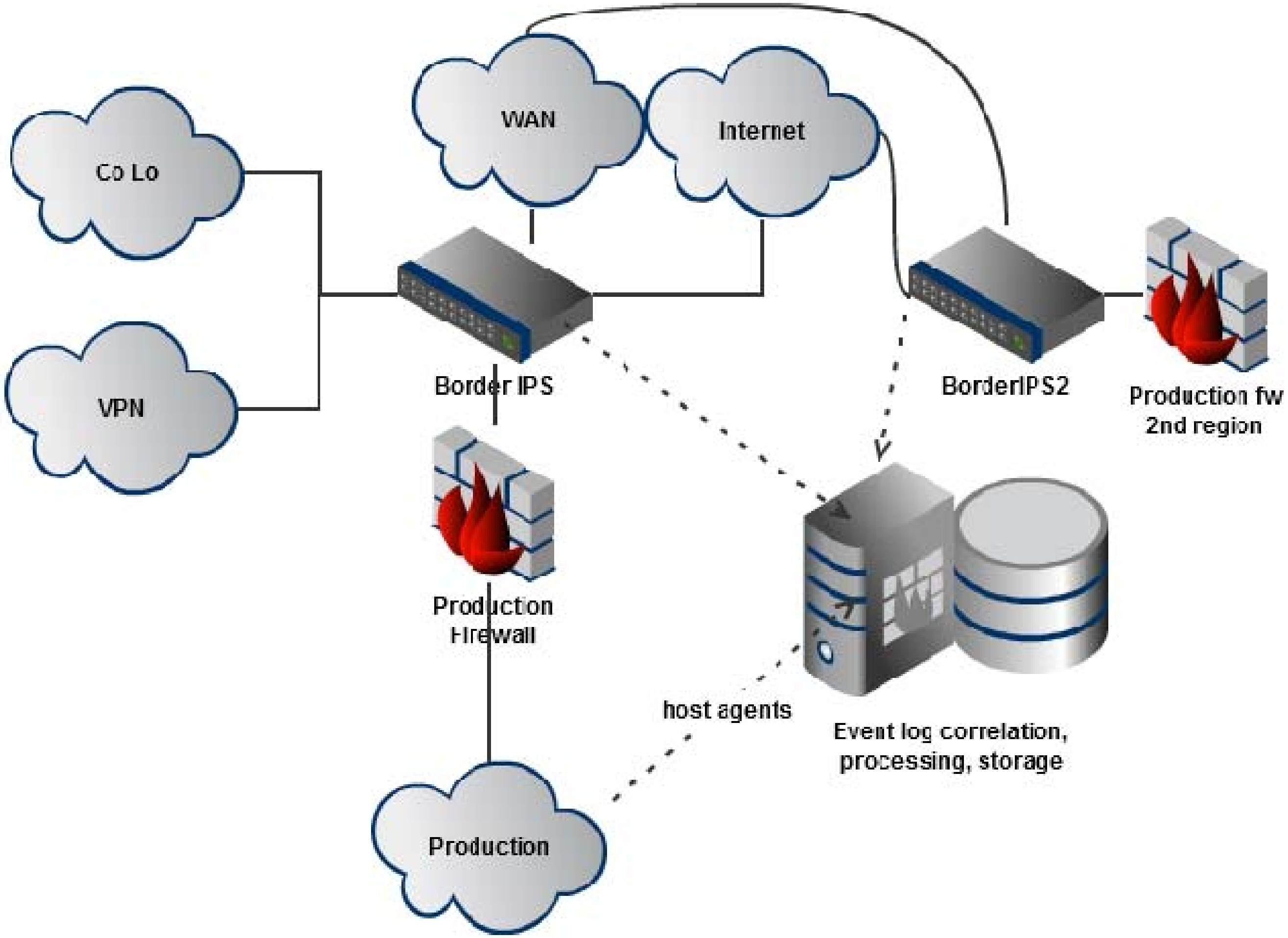
- *Stats taken Feb 2011*

IPS 101

Intrusion Prevention System (IPS)

- Deep packet inspection (using PAM)
- Looking for signs of attack
- If an attack is discovered, then perform an action defined by a policy
- Can be an appliance, software host agent, or hypervisor level.
- Pushes events to a central system for correlation. (security analyst interacts with this system)

Environment



Our solution – Hardware / Software

2x GX5108 appliances

- 2.5Gbps throughput per appliance
- 4 network segments per appliance (4 cables in 4 out)
- Physically cabled inline with network segments to protect

75 x host agents

- Windows, linux, solaris.

All pushing to Siteprotector

- Event database is about 100GB in size.
- Enterprise scanner – feeds vulnerability scan results into Siteprotector. Adds context to attacks.

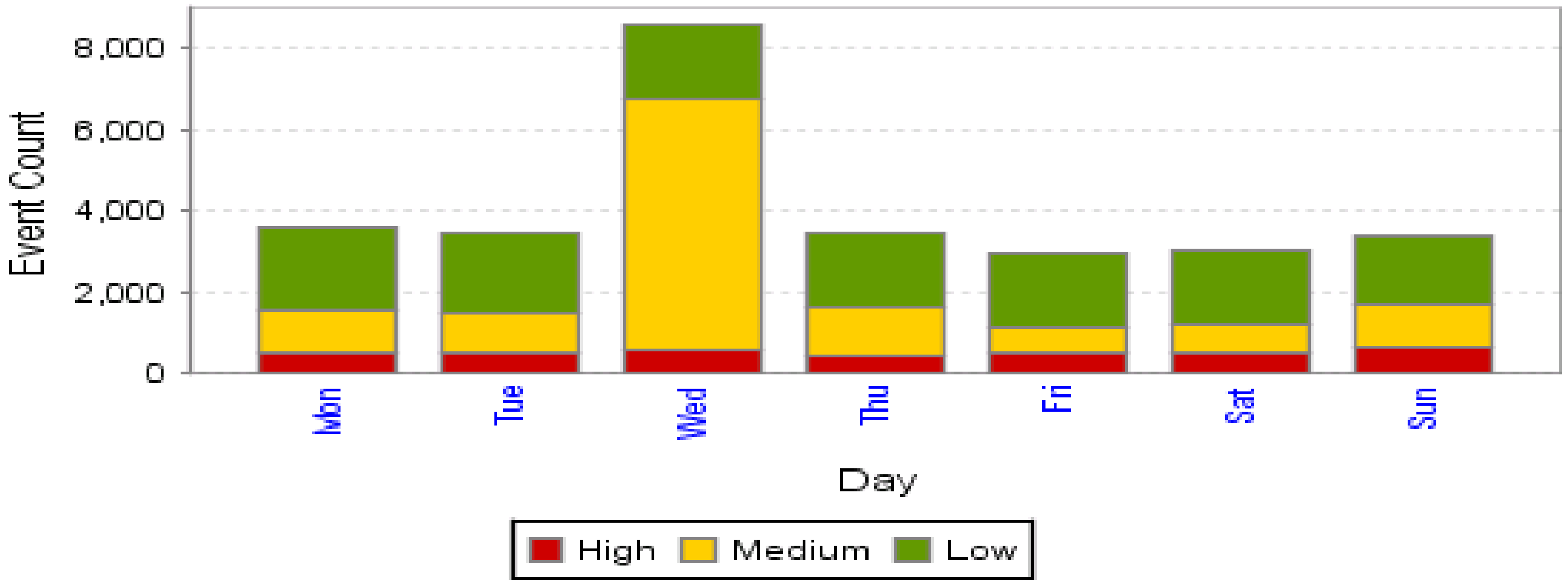
Design decisions

Why run firewalls inline with separate IPS appliances?

Why run border IPS appliances and internal host agents?

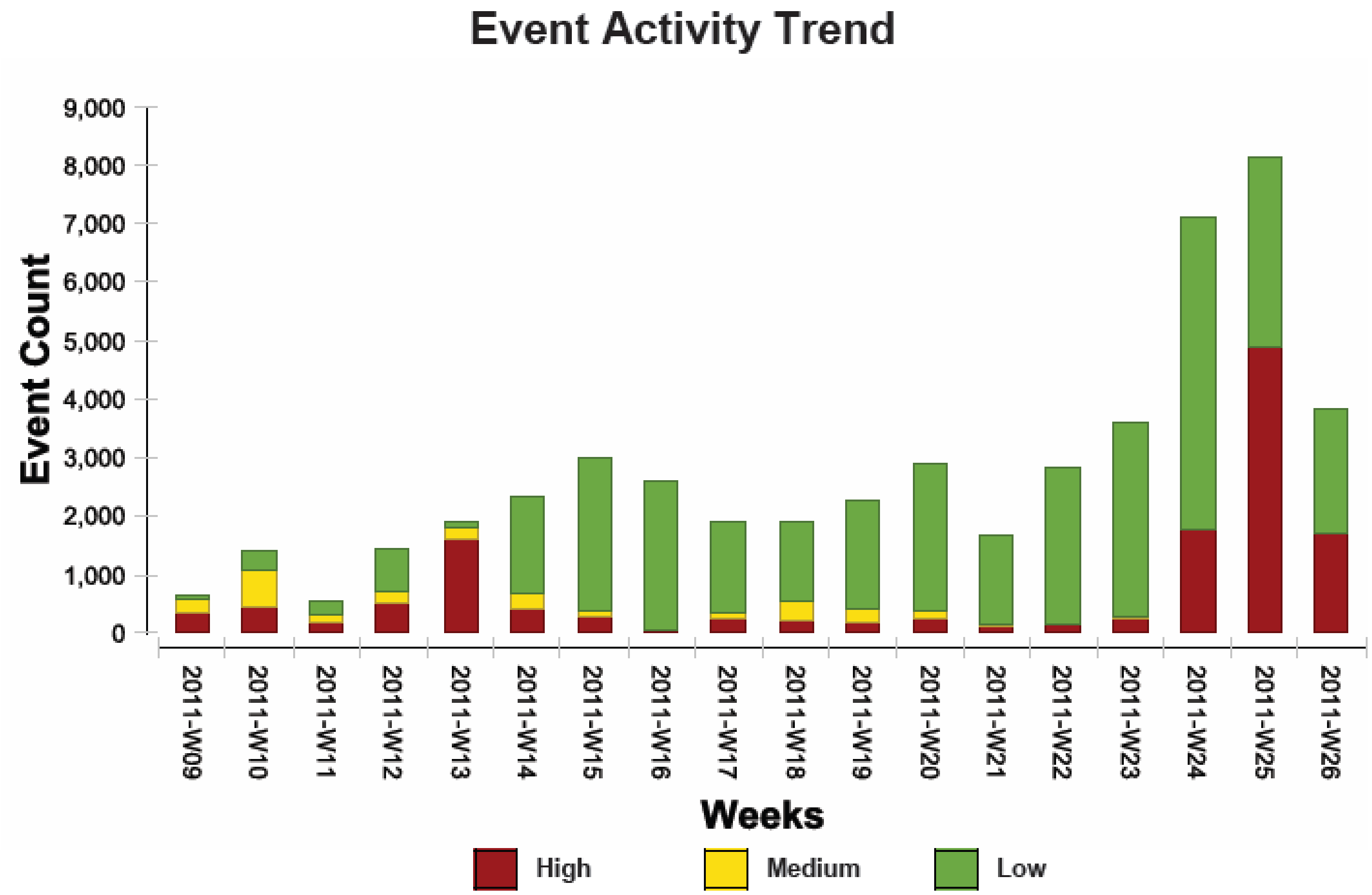
Why have wan traffic on the IPS? Isn't this internal?

Data Views



Event Count
8,000
6,000
4,000
2,000
0
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Day
High
Medium
Low

Web attacks view



What have we learned?

- IDS/IPS can either me a checkbox exercise or it can actually be a useful defensive layer.
- You will encounter issues.
  - Not the equipment's fault.
  - Every network is different.
  - Every network runs some strange applications.
- Support matters.
  - When you run into what was said above.
- Profile, profile and more profiling.
- Flexibility and agility matter.