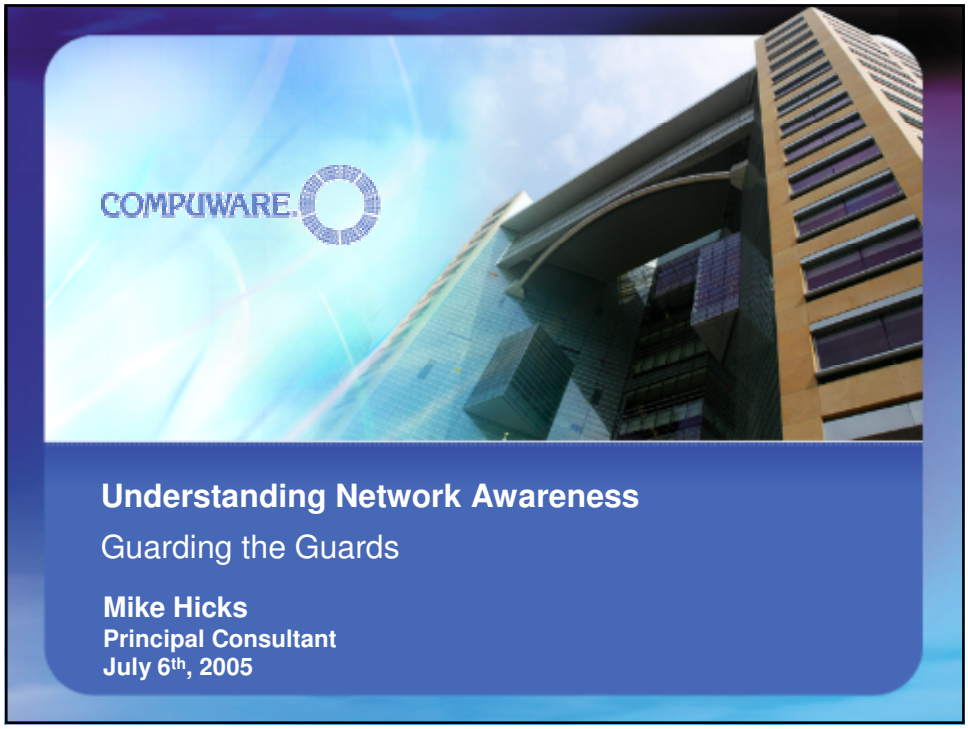


Understanding Network Awareness

Guarding the Guards

Mike Hicks
Principal Consultant
July 6th, 2005

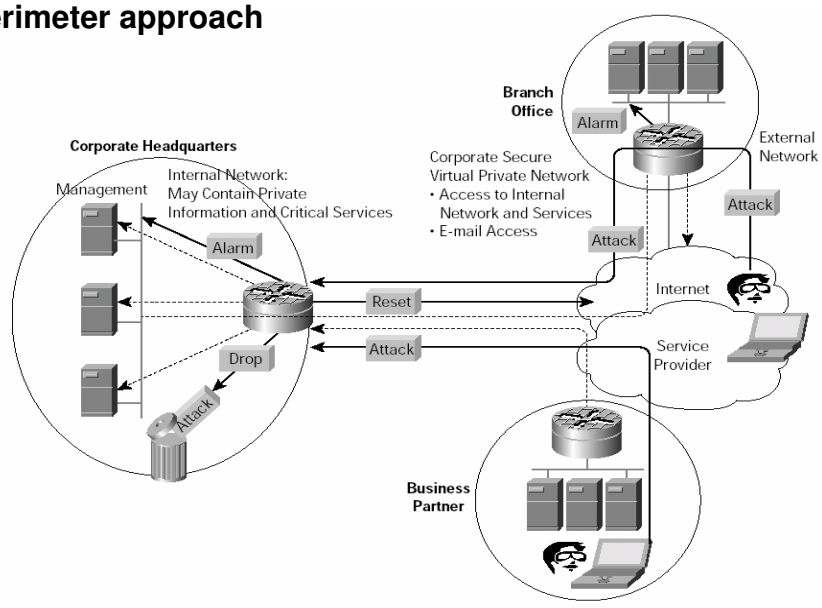
Agenda

- Who am I?
- General approach to security
- Case Study
- What is Network Awareness?
- Case study revisited
- Protection Vs Monitoring
- Organizational Benefits
- Summary

So who is Mike Hicks?

- Principal Consultant advanced networking at Compuware
- Over 17 years experience in networking and more than 5 years working in the field of APM
- Author of:
  - Managing distributed applications – Prentice Hall 2001
  - Optimizing applications on Cisco networks – Cisco press 2004
- Provided support for large complex networks including
  - Ford Motor Company
  - European Space agency

Perimeter approach



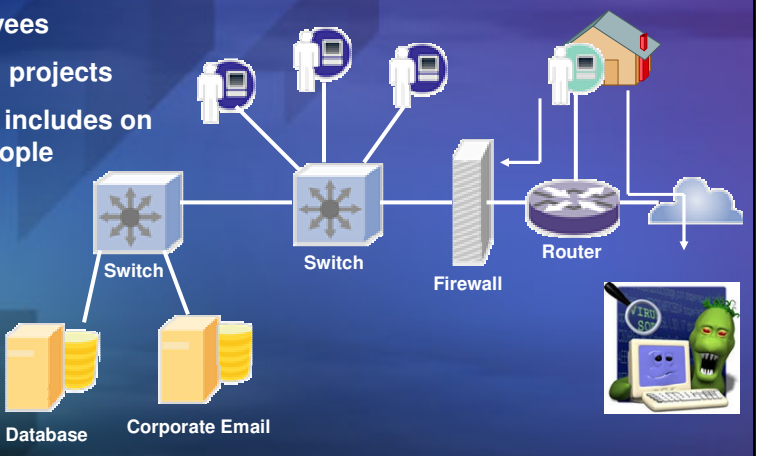
Chasing Ghosts!

Acme Corp-Case Study

2,000 employees

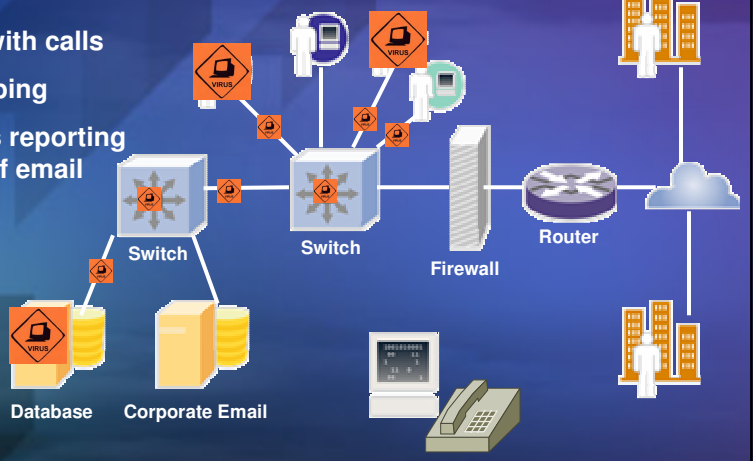
100 on going projects

Each project includes on average 5 people



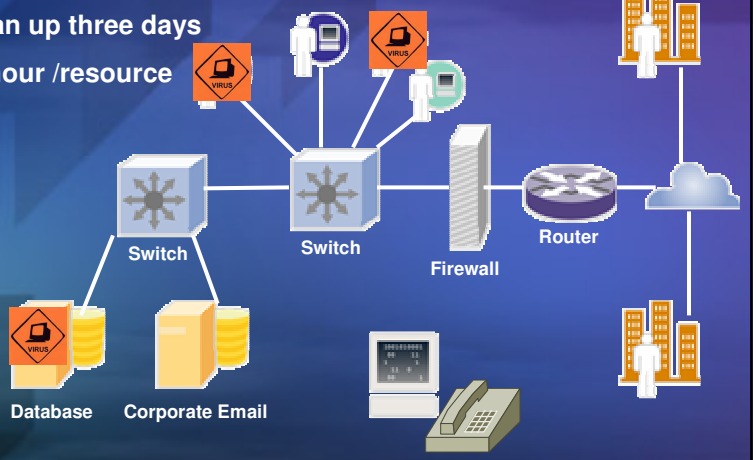
Acme Corp-Case Study

- Infected lap top enters ring fence
- IT inundated with calls
- Systems stopping
- External users reporting high volume of email



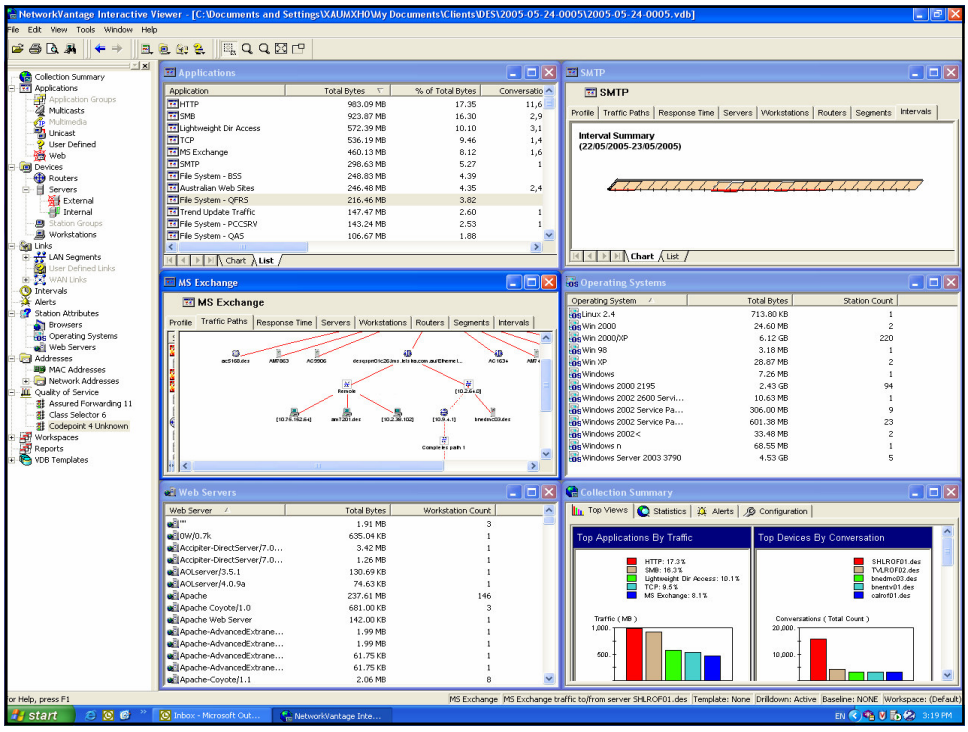
Acme Corp-Case Study

- Gather information took several hours
- Estimated clean up three days
- Approx $100/hour /resource



What is network Awareness?

- **Visualization of the living network fro the users perspective**
  - **People – Whose talking to who**
  - **Traffic – what , when and how much**
  - **Machines – Station Ids**
  - **Address – usage and location**



What is normal

- **Based on application traffic patterns create a "baseline" view of the environment**

Rule Name	Weighting	Trigger Event
Conversations	5	If the Device conversations are greater than 2000
Min Pckts Sent	5000	Devices that have not sent more than 5000 packets are excluded (This is in a 6 hour period)
Min Convstn	600	Devices that have sent more than 600 conversations are excluded. (This is in a 6 hour period

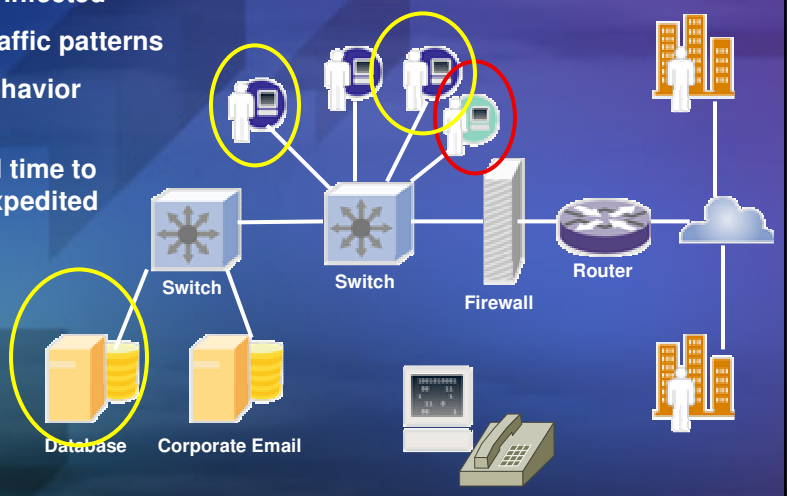
Acme Corp-Case Study -Revisited

Network still infected

Now know traffic patterns

Abnormal behavior identified

Isolation and time to resolution expedited



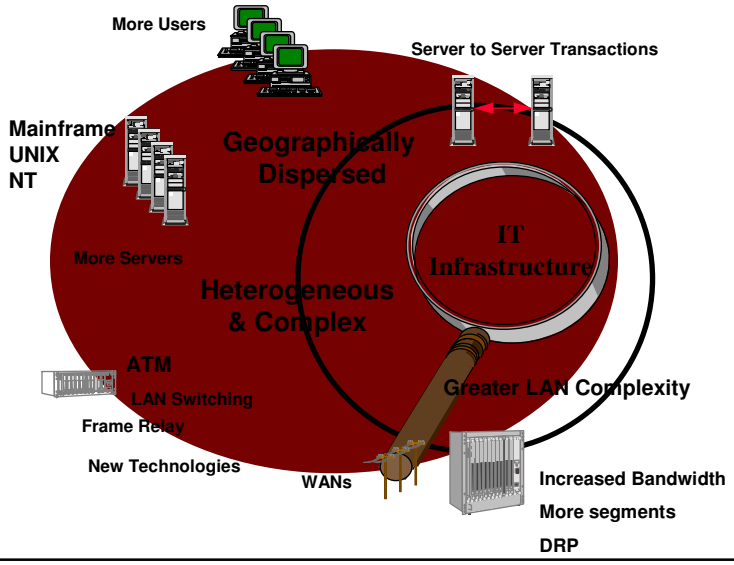
Protection vs. Monitoring

- You can't protect your environment from every single threat
- Monitor activity & adjust threat model accordingly
- Accountability
  - Track what people do
  - How do they access services?
  - What versions of web browsers are being used?
  - What types and volume of traffic do the users typically generate

Protection vs. Monitoring

- Authentication & Accessibility
  - Who is accessing your information
  - How do they access services?
  - How easily can you obtain this data?
  - Present it in a common useful format

Typical Network environment



Organizational Benefits

- Improved efficiency
  - Where is time spent
  - Improved reporting
  - Where should upgrade dollars be spent
  - Identification of non core/work related activities, such as file sharing, P2P, streaming video etc

Summary

- You can't protect your environment from every single threat
- How can you defend a fort if you don't know the landscape that surrounds it
- The ability to analyze developing or current problems will yield significant ROI.
- Network awareness is a necessity in a comprehensive security plan to provide a clear picture of:
  - What is happening
  - What has happened
  - What may happen