Security – Perspectives and Positioning

Doug Klein

CEO

Date of Presentation

How do we think about security?

- What are we trying to protect?
  - Our data?
  - Our computer?
  - Our network?
- What are we protecting from?
  - Damage?
  - Theft?
  - Abuse/Misuse?
- Where do the various technologies fit?
  - On your laptop?
  - In the network?
  - Around the network?

What are we trying to protect?

- Data
  - From theft
  - From corruption
- A client computer
  - From abuse/destruction
  - From hijacking
- Host(s)
  - From abuse/destruction

- Networks
  - From misuse
  - From overload
- Network components
 - From abuse/destruction

How do we protect?

VPN's: protecting traffic as it passes through foreign domains

Wireless encryption: protecting traffic from sniffing in the air

Firewalls: protecting one network from another

Personal firewalls: protecting your computer from the network

Vernier: protecting the network from the untrusted traffic

User A — Company B — Company A
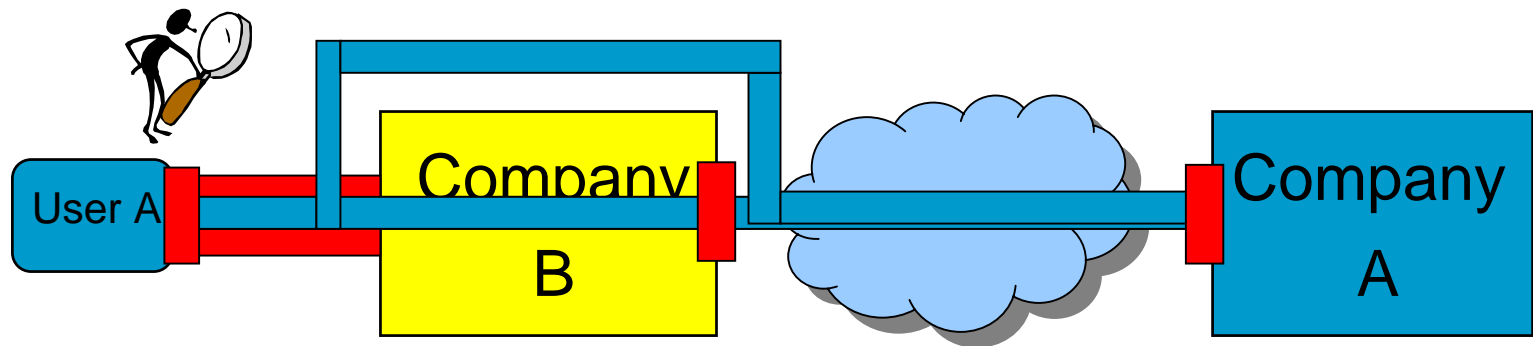
Why protect the network from traffic?

- The network itself has become the most mission critical component of the enterprise computing environment

- The "exposed" edge is no longer just the external Internet connection
  - Laptop PC's becoming the "desktop" of choice
  - Viruses/trojan horses becoming smarter about hitching a ride

What is different about wireless?

- Physical security not sufficient anymore
  - The parking lot problem: RF goes through walls
  - Traditional wired workarounds aren't appropriate: Location is a poor proxy for the user in wireless networks

- The demands for connectivity are changing
  - Users expect connectivity everywhere: Conference rooms, training centers, cafeteria's, hallways
  - It's not just PC's anymore: Everything becomes an IP client, how do you manage/secure them all?

What should you do?

- Access management at the edge of the network
  - Protect all of the network

- User based granularity on the control
  - Protect based on level of trust/authority on the network

- Detailed logging and accounting of all activity
  - Have the tools to react/correct quickly and accurately to network issues