Deloitte & Touche

Firewalls & Middleware

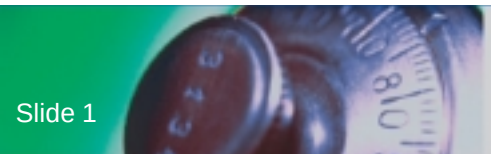
Neil Jarvis

Principle Consultant
Information Security Services
Deloitte & Touche

ISACA - 23rd May 2002

Information Systems Audit and Control Association

Information Security Services



Enterprise Risk Services

Agenda

Deloitte & Touche

- Definitions
- Potential Problems
- Potential Solutions
- Conclusion
- Questions

Information Security Services

Definitions

Deloitte & Touche

- Firewall
  - a dedicated system which controls the flow of traffic between two or more networks with different levels of trust.

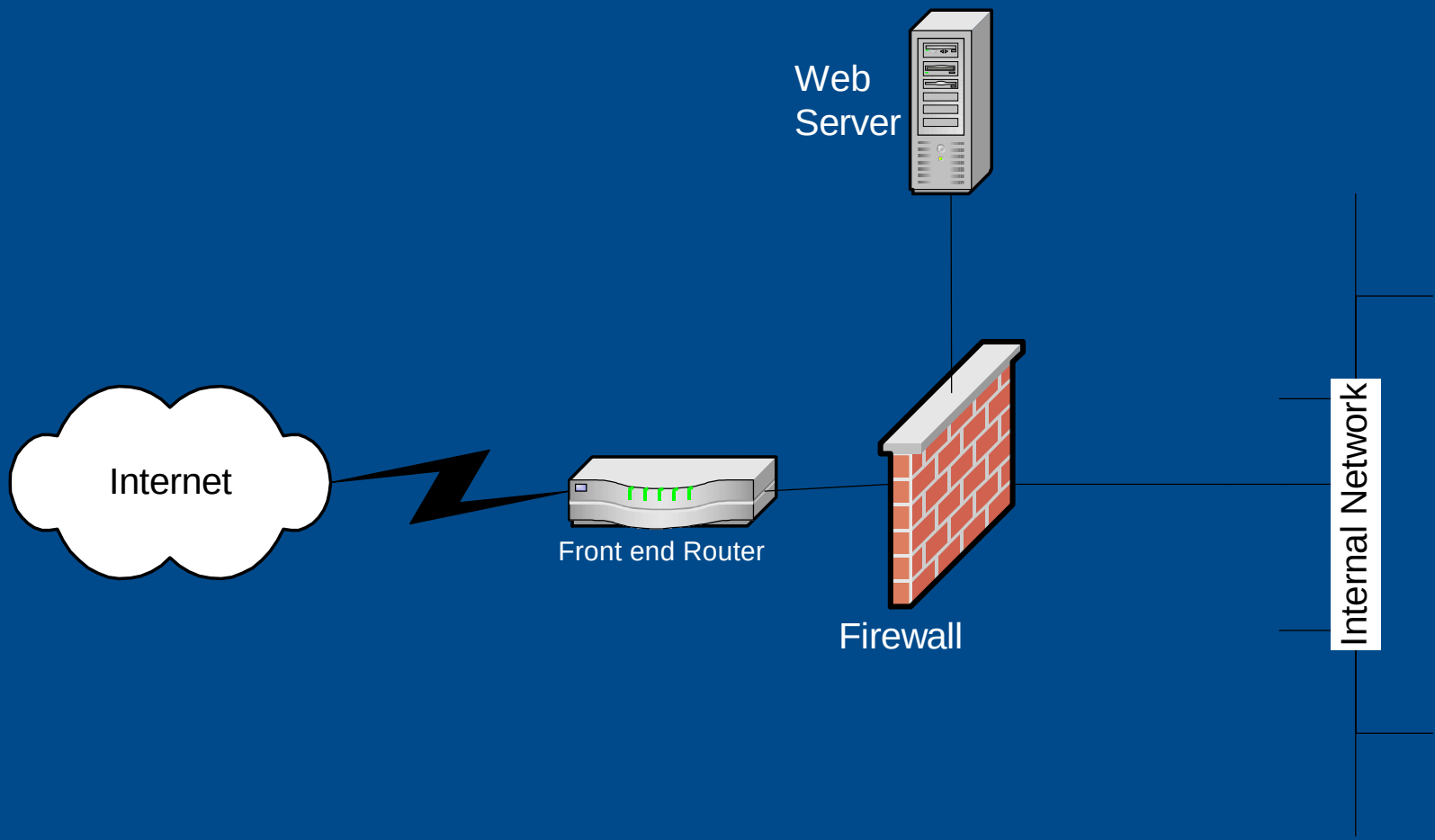
Firewall Types

Deloitte & Touche

- Packet filtering
  - 1st Generation Firewalls
  - Routers
- Application Proxy
  - 2nd Generation Firewalls
- Stateful Inspection
  - 3rd Generation Firewalls
  - Checkpoint Firewall-1
- Dynamic Packet Filtering
  - 4th Generation Firewall

Security Architecture

Deloitte & Touche



Information Security Services

Potential Problems

Deloitte & Touche

- Firewalls
  - Seen as providing total protection
  - Most attacks occur on the Inside
  - Most external attacks occur via port 80 or port 443
  - Logs
  - Firewalls are Reactive/Detective
  - Attacks against the firewall

Problems

Deloitte & Touche

- Diverse Systems
  - 4 (or more) IDS
  - Router
  - Firewall
  - Web Server
  - Databases

Problems

Deloitte & Touche

- Volumes
  - Firewall Logs ~ 100's MB per Day
  - Web Server Logs ~ 100's MB per Day
  - IDS Logs ~ 100's MB per Day

Problems

Deloitte & Touche

- Analysis
  - Need a Holistic View
  - Consolidation
  - Synchronisation/Common Reference Point
- Escalation
  - What?
  - Who?
  - How?

Information Security Services

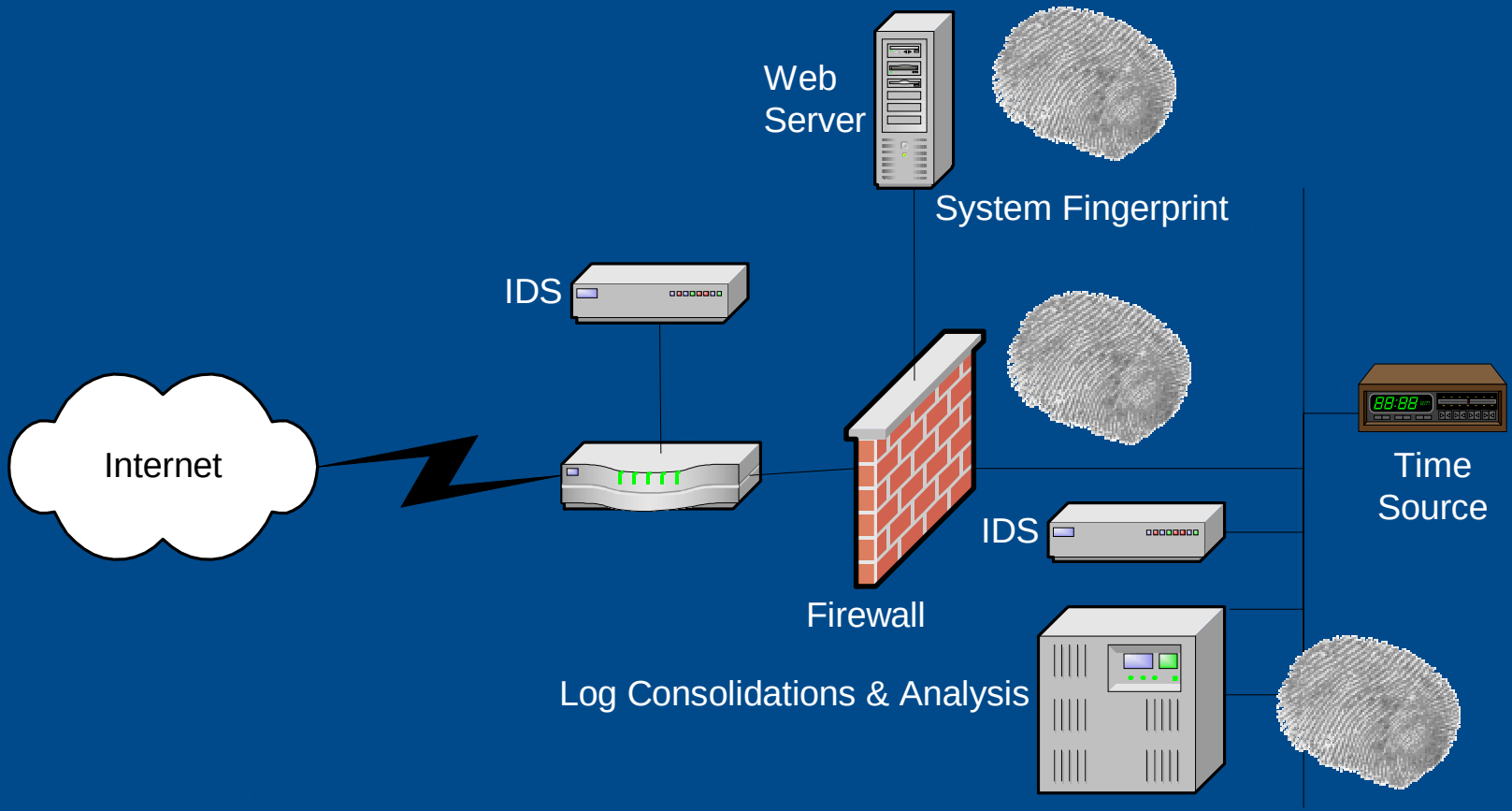
Problems

Deloitte & Touche

- IDS
  - False Positives
  - False Negatives
- Firewalls
  - Regular Scans/Attacks
- Web Servers
  - Connect Messages

Potential Solutions - Firewalls

Deloitte & Touche



Information Security Services

Definitions

Deloitte & Touche

- Middleware
  - Software which manages the exchange and format of messages between different systems
    - COM (Component Object Model)
    - DCOM (Distributed Component Object Model)
    - CORBA (Common Object Request Broker Architecture)
  - Products
    - IBM MQ-Series
    - Internet Transaction Server (SAP)
    - ROSE
    - Tuxedo

Middleware Architecture

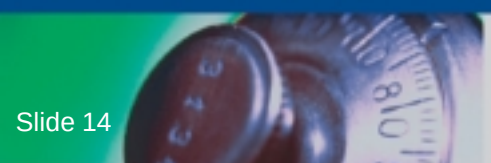
Deloitte & Touche

- Between two firewalls in a DMZ

Potential Problems

Deloitte & Touche

- Middleware
  - Messages have to be in clear text for translation
  - Messages may be stored locally in an un-encrypted form
  - Middleware systems may be trusted
  - Message Integrity may be at risk
  - Often involved queues - onqueue or dequeue



Potential Solutions - Middleware

Deloitte & Touche

- Trusted Systems
- Encrypted Channels
- Integrity Checking
- Authentication

Other Trends

Deloitte & Touche

- Wireless Networks

Information Security Services

Deloitte & Touche Survey

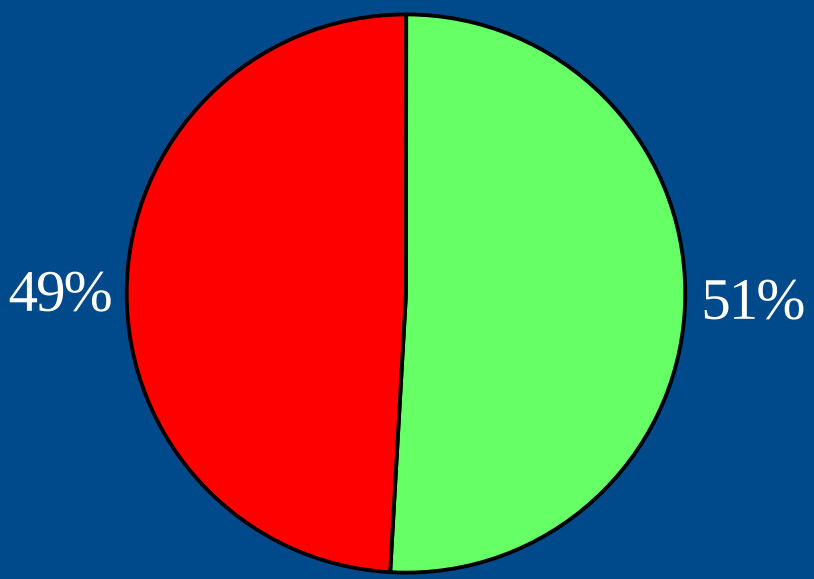
Deloitte & Touche

- Extensive survey of central London
- Extensive survey of other UK locations in progress
- 422 Access points located

Information Security Services

Deloitte & Touche Survey - Encryption Results

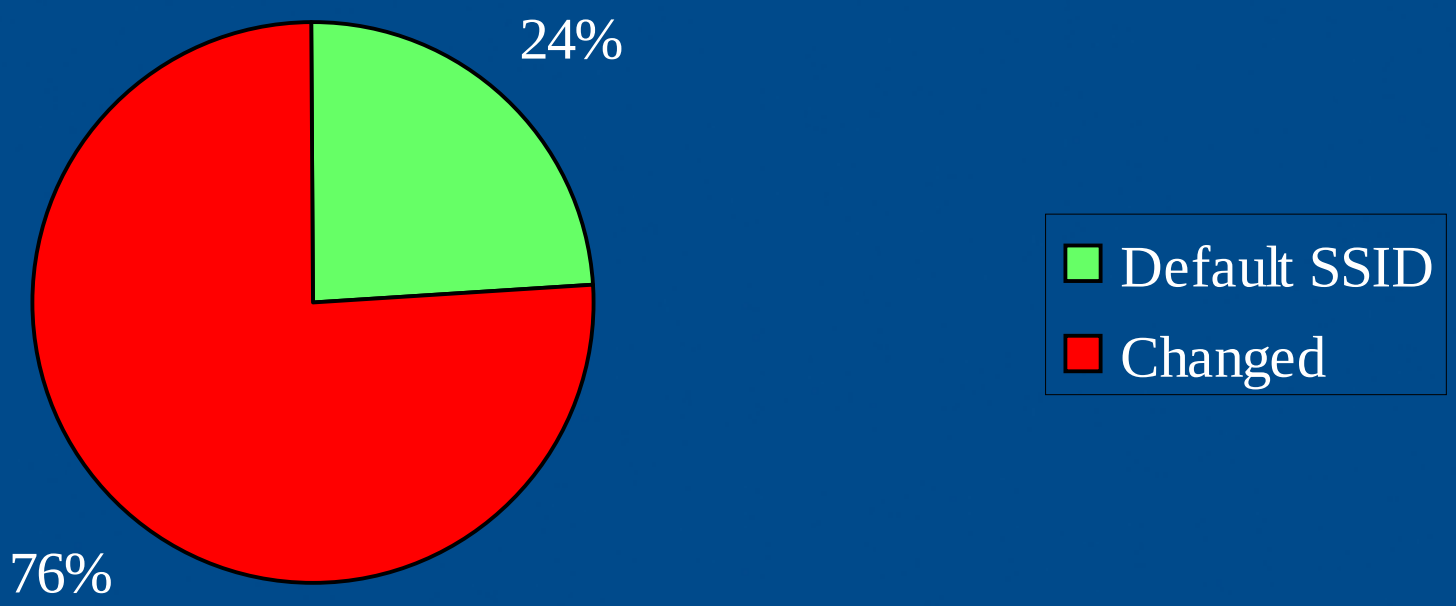
Deloitte & Touche



Information Security Services

Deloitte & Touche Survey - SSID Results

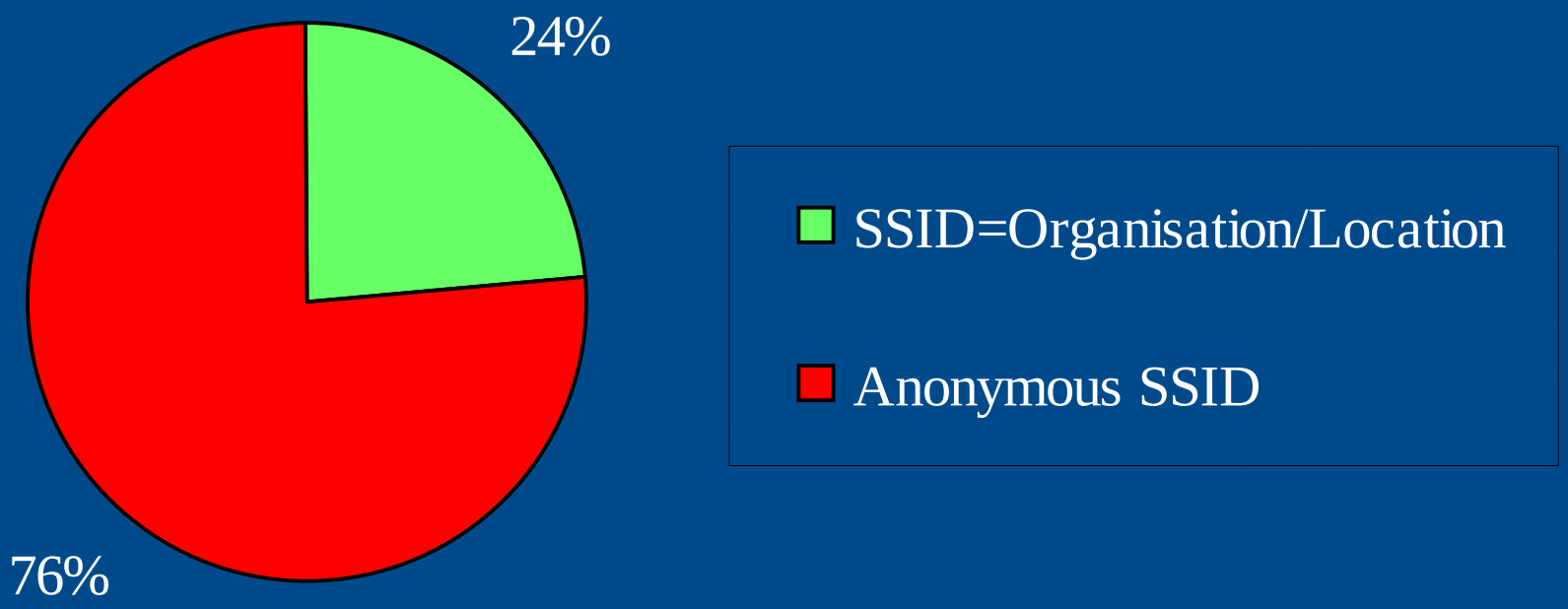
Deloitte & Touche



Information Security Services

Deloitte & Touche Survey - SSID = Organisation/Location

Deloitte & Touche



Information Security Services

The Way Forward

Deloitte & Touche

- Holistic risk-based approach to security
- Appropriate risk management strategy
- Appropriate security countermeasures
- Audit & Control
- Proactive monitoring of the impact of new technologies, tools and methods
- Incident response and escalation plans

Questions To Consider

Deloitte & Touche

- How are you going to balance the benefits of operating portals against the levels of risk faced?
- Do you have systems and network architectures that are scaleable?
- Have you ever tested the security of your networks and processes?

Questions

Deloitte & Touche

?

Information Security Services

Deloitte & Touche

Information Security Services

Enterprise Risk Services