INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

The Real Deal on Plug n' Play Security Appliances

Scott Sidel
May 9, 2005

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Security Servers vs. Appliances

- **Introduction**
  - **Servers**
    - **Pros**
    - **Cons**
  - **Appliances**
    - **Pros**
    - **Cons**
  - **Servers vs. Appliances**
    - **Firewalls, VPNs, IDS, Anti-Virus**
  - **Integrated Security Appliances**
  - **The Future of Security Servers**

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

What is a server?

- **Heavy duty commodity hardware**
- **Heavy duty commodity software**
- **Customized to your requirements**
- **Integrated based on your requirements, typically by you**

INFORMATION SECURITY DECISIONS

Hosted by

What is an appliance?

- **Purpose built device**
- **Specialized hardware**
- **Specialized software**
- **Highly integrated**
- **Support options**
- **Branding**

INFORMATION SECURITY DECISIONS

Hosted by

What are the pros of a server?

- **Commodity hardware, multiple vendors**
- **Low up-front cost of hardware**
- **High level of configuration options**
- **Utilize existing in-house expertise**
- **Easy to upgrade**
- **Replacement parts close at hand**

INFORMATION SECURITY DECISIONS

Hosted by

What are the cons of a server?

- **Integration**
- **No single point of contact for support (one throat to choke)**
- **Complexity of integration**
- **Performance bottlenecks**
- **Ongoing security patching**

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

What are the pros of an appliance?

- **Pre-integrated**
- **Pre-secured, minimized attack surface**
- **High performance**
- **Dedicated support organization**
- **Streamlined updates**

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

What are the cons of an appliance?

- **Up front costs are higher**
- **Ongoing annual maintenance and support costs**
- **It's a black box**
- **Reliance on external support organizations**

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Business types

- **Appliance**
  - **Small / Medium Business**
  - **Remote Office / Branch Office**
  - **Enterprise**
- **Server**
  - **Enterprise with specialized expertise**

INFORMATION SECURITY DECISIONS

Hosted by

Is size a factor?

INFORMATION SECURITY DECISIONS

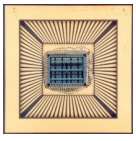
Hosted by

Security Appliance – commodity hardware meets specialized hardware

INFORMATION SECURITY DECISIONS

Hosted by

Security Appliance – ASICs



- **Application Specific Integrated Circuits (ASICs) are ideal for high speed acceleration of a task is needed.**
- **However, ASICs force the logic designer to make critical decisions very early in the product's life cycle, at initial design time. This is because once an ASIC device is made, it can not be altered.**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Security Appliance – Attack Surface

- **Specialized OS**
- **Hardened OS**
- **Only Required Services**
- **Unpublished, proprietary APIs**
- **Restricted locally addressable interface**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Security Appliances – Firewalls

vs.

- **Throughput**
- **Specialized hardware optimizations**
- **High availability**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Servers – Firewalls

+

=

- **Check Point's SecurePlatform installs and VPN-1/FireWall-1 software on Intel and AMD-based PCs and servers.**
- **configures a fully hardened/secured operating system**

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Security Appliances - IDS

- **Throughput**
- **HA**
- **In-line optical fail pass-through**

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Security Appliances – VPN

- **Throughput**
- **Connections**
- **Co-processors**

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Security Appliances – Anti-Virus

INFORMATION SECURITY DECISIONS

Hosted by

Security Appliances – Content Filtering

- **Manage access to sites by type of content**
- **Manage P2P**
- **Manage IM**

INFORMATION SECURITY DECISIONS

Hosted by

Integrated Security Appliances

- **Firewall**
- **Intrusion Detection**
- **Content Filtering**
- **VPN**
- **Anti-Virus**

INFORMATION SECURITY DECISIONS

Hosted by

Server vs. Appliance – The Future

Questions