Security Without Sacrifice: Delivering Affordable IT Security Without Breaking The Bank

Nelson Da Silva
Fortinet

Benefits of being online

• New Education Initiatives
  • Distance education
  • Audio/Video On Demand
  • e-Learning, e-Mentoring
• Collaboration
  • Students, Parents, Faculty, Community
• Communication
  • Social Networking, Research, Administrative, The Blogosphere

• And The List Goes On and On…
Education Network Challenges

• Rapidly increasing bandwidth: 10Mb, 100Mb, 1Gb, 10Gb…
  • New initiatives: Research, Audio/Video, P2P, Mobile, Web 2.0…
• Users: Students, Parents, Faculty, Community
• New Service Models
  • Time Sharing, Out Sourcing, Virtualization, Cloud computing
• Remotes access
• Malware and Illicit Web Sites/Content
• Commitment to open networks
• Limited Funding
• Duty of care

Not Just Windows-Based Clients
Navigating the Security Landscape

Connection Security
- **Firewall**  
  "External" threat protection
- **Virtual Private Network (VPN)**  
  "Secure" private traffic across public networks

Application Security
- **Web filtering**  
  Protection from harmful web sites and web content
- **Messaging security**  
  Detection and protection from malicious email message content

Content Security
- **Intrusion Prevention System (IPS)**  
  Monitoring and active protection from malicious traffic
- **Antivirus / Antimalware**  
  Detection and removal of malicious application content

Feature Priorities

<table>
<thead>
<tr>
<th>Feature</th>
<th>Firewall</th>
<th>AntiVirus</th>
<th>IPS</th>
<th>Web Filtering</th>
<th>VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tertiary Education</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
</tr>
<tr>
<td>K-12</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
<td>![Symbol]</td>
</tr>
</tbody>
</table>
Multiple Threat Vectors

- **Multiple Threat Types**
  - Various Application Entry Points
  - Different Attack Functions
  - Threat Payload Intent Varies
  - Broad Range of Propagation Techniques

- **Application Threat Vector**
  - Viruses & Spyware
  - Spam & Directory Harvest Attacks
  - Web Phishing
  - IM and P2P file transfers

- **Network Threat Vector**
  - Network Worms
  - DDOS/DOS
  - IP Packet Capture
  - Spoofing & Man-In-The-Middle

---

Blended Threats Leverage Multiple Threat Vectors

- **Malicious threats lead to**
  - Data loss
  - Identify theft
  - Database espionage
  - Network downtime
  - Bad publicity
  - Regulatory fines

- **The motive has changed**
  - From notoriety to criminal intent
  - More malicious in nature
  - Global in reach
  - Predatory behaviors
So... What is a blended Threat?

- **Blended Threats**
  - use *multiple infection and attack methods* to leverage vulnerabilities found in operating systems and applications
  - harder to detect and block, blended attacks are created with a hybrid of technologies such as *virus, worm, Trojan horse, and backdoor attacks* that are delivered with email, infected Web sites and even alternate media
  - May deploy social engineering techniques such as Phishing and Grayware

Threat Life Cycle

**Four Distinct Phases**

- Transmission
- Penetration
- Launch
- Propagation
Blended Threat – W32/Pushdo!tr

- **Multiple Attack Vectors**
  - Spam email with malicious attachment
  - Email contains a trojan downloader
    - Downloads a rootkit to cover activity
    - Downloads multiple other components
  - The trojan uses a command and control communication channel

W32/Pushdo!tr - Antispam

- Antispam recognizes email as spam
- Blocks message from user’s inbox
W32/Pushdo!tr - Antivirus

- Gateway antivirus detects the malicious attachments
- The trojan downloader
- The rootkit
- The various other components
- Removes malicious payloads, preventing accidental execution

W32/Pushdo

W32/Pushdo!tr – Intrusion Prevention

- IPS detects communications on the command and control channel
- Blocks the transmission of the infected host’s communication
The Changing Threat Landscape

- Threats vary and evolve over time
- Consolidated appliances provide broad coverage for consistent protection

Source: FortiGuard Research

Assessing Your Risk

- Business Impact Assessment
  - What’s the Impact of a negative event?
  - What’s the probability of it occurring?
- Threat and Vulnerability Assessment
  - What threats and vulnerabilities exist?
- Risk Assessment
  - Over Simplified:
    - Risk = Threat x Vulnerability x Impact
  - Keep It Real
    - Compare with others
    - Does it make sense?
Defense in Depth

• Strategy
  • Layer defenses against threats
  • Not just multiple vendor point solutions
  • Vendor agnostic strategy
  • Consolidation is your friend
  • Increase the difficulty for attacker
  • Ease of administration
  • Simplify enforcement
  • Educate faculty and students

Are You Maximizing Your Investments?

• Observe resources required to maintain systems
  • Moves, adds, changes, training, maintenance
• Re-Architect and/or Redeploy where needed
  • Media sharing and segregation
• Shape your traffic
  • Network and application level
• Consolidation
  • Infrastructure, Data, Web Services
  • Virtualization
Some Case Studies

School Deployment

- Lab Computers
- School Network
- Classroom Computers
- Faculty Computers
- School
- FortiGuard Rating servers
- Internet

Fortinet Confidential

Real Time Network Protection
TAFE College Deployment

"The $1.5 million savings will be achieved by reducing costs associated with outsourcing agreements, savings on equipment costs and software licenses, and reduced ongoing support costs."

"Regular automatic reports provide our executive team with valuable insight into the security risks we are dealing with on a daily basis."

Campus Perimeter Security

Using Firewall + IPS + Antivirus + Web Filtering

1. Firewalls alone aren’t enough to block today’s blended threats.

2. When single packets are examined by point products with no deep packet, antivirus, and intrusion inspection technologies, blended threats can often pass undetected.

3. Deep-packet inspection firewall technology, such as Fortinet’s 5000 series, with state-of-the-art antivirus and intrusion prevention allows packet flows to be tracked.

4. When multiple technologies examine entire packet flows, from content inspection through reassembly, threats are stopped at the perimeter before campus resources are compromised and application assurance is delivered.
Fortinet Overview

- **Leading provider of ASIC-accelerated Unified Threat Management (UTM) Security Solutions**

- **Company Stats**
  - Founded in 2000
  - Silicon Valley based with offices worldwide
  - Seasoned executive management team
  - 1,100+ employees / 500+ engineers
  - 400,000+ FortiGate devices shipped worldwide

- **Strong, validated technologies and products**
  - 24 patents; 85+ pending
  - Six ICSA certifications (Firewall, AV, IPS, IPSec VPN, SSL VPN, Anti-Spam)
  - Government Certifications (FIPS-2, Common Criteria EAL4+)
Thank You.

What other vendor can generate this type of feedback!

-----Original Message-----
From: xxxxxxx@k12.sd.us [mailto:xxxxxxx@k12.sd.us]
Sent: Friday, September 14, 2008 6:30 AM
To: Info@AVFirewalls.com
Subject:

fortiguard is next to the *&$(#$% thing i have ever seen, or experienced...whoever created this stupid program seriously has no friends and hates fun...you suck