Modern Challenges to Perimeter Security

Security Conference 2004, London, UK

Franjo Majstor
Fortinet Inc.

Agenda

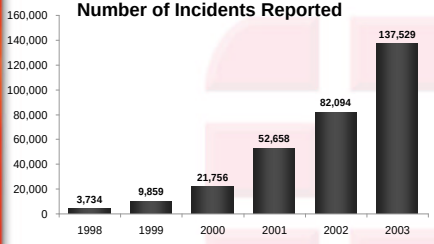
- Perimeter Threats Evolution
- Perimeter Technologies
- Modern Perimeter Challenges
- Modern Perimeter Solution

Perimeter Threats Evolution

Threats Increasing in Quantity and Cost

- Number of Threats is increasing exponentially
- If not protected, costs are astronomical

Number of Incidents Reported



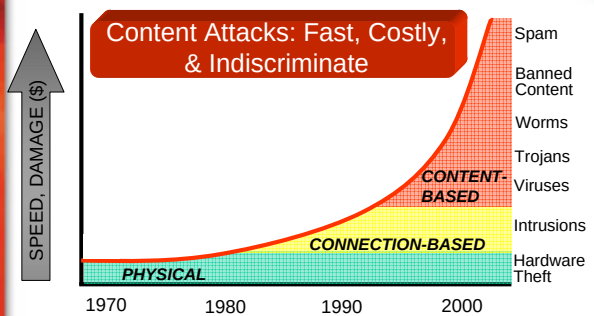
Source: CERT® Coordination Center, Carnegie Mellon University, Feb 2004

Costs of Threats*

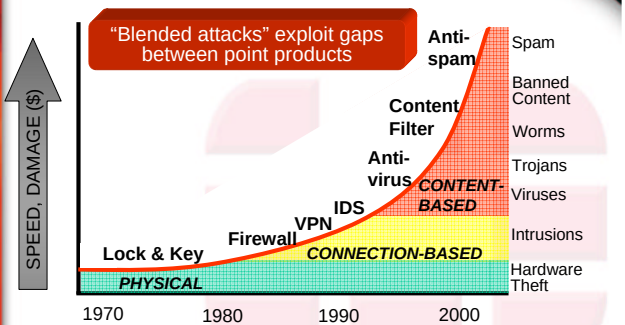
Outbreak	Cost
Code Red	*$2.62B*
Sobig	*$2.0B*
Nimda	*$2.0B*
Melissa	*$1.9B*
Love Bug	*$2.1B*
Slammer	*$1.0B*

Source: Computer Economics

The Nature of Threats Has Evolved…



…Fueling an Explosion of Point "Solutions"



Content Threats: Then

	Virus	**Infects a host file by self-replication via executable file**
	Worm	**Infects systems via auto-distribution through network**
	Trojan	**Malicious function such as create a backdoor**
	Mobile code	**Infects via active content**

Content Threats: Now

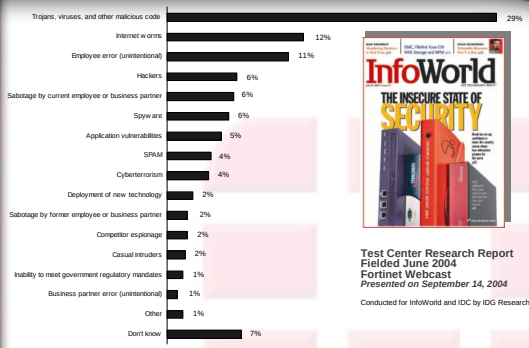
	Blended Threat	Combines the functionality of worms, viruses, trojans, malicious mobile code, more

Example: Sobig.F

Vector	***Function***	***Propagation***	***Payload***
Email with .PIF or .SCP attachment	Harvest email addresses	Send email using spoofed source address with built-in SMTP engine	At pre-designated time, ping one of 20 sites to retrieve URL. Download file referenced in URL. Execute the downloaded program.

Greatest Threats to Enterprise Network Security

Source: InfoWorld IT Solutions Study- June 2004



Test Center Research Report
Fielded June 2004
Fortinet Webcast
Presented on September 14, 2004

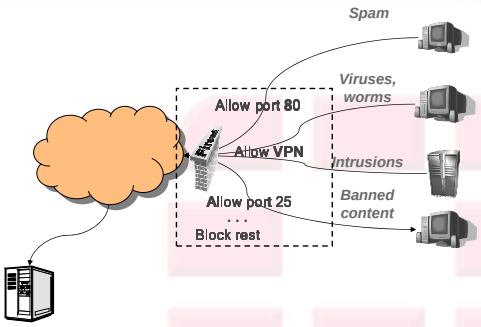
Conducted for InfoWorld and IDC by IDG Research Services Group

Among those involved in the acquisition of security products and services and employed at companies with 50 or more employees. (Base 437) Q20-What is the single greatest threat to your company's enterprise network security?

FORTINET
THE POWER IN NETWORK PROTECTION

Perimeter Technologies

Traditional Perimeter Technology

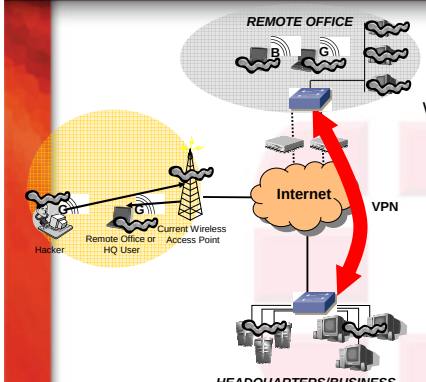


Allow Port 80?

http://www.nocrew.org/software/httptunnel.html

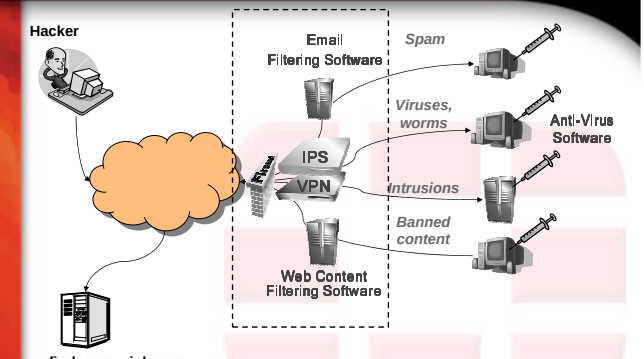
- ***httptunnel*** creates a bidirectional virtual data connection tunneled in HTTP requests. The HTTP requests can be sent via an HTTP proxy if so desired.
- This can be useful for users behind restrictive firewalls.
- If WWW access is allowed through a HTTP proxy, it's possible to use httptunnel and, say, telnet or PPP to connect to a computer outside the firewall.

Allow VPN?



Wireless User
- Connects to public hotspot
- Picks up a worm or virus from this unsecured access point
- Returns to office, authenticates to WLAN device
- Starts spreading the threat throughout the company

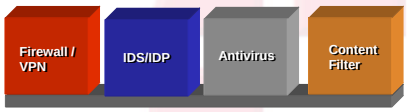
Current Perimeter Technologies



Modern Perimeter Challenges

First Generation: Stateful Inspection Firewall

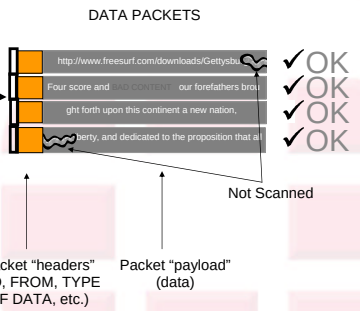
In point solution configuration, Stateful Inspection firewall delivers network level security services



Stateful Inspection Firewalls Don't Analyze Payloads so they Miss Content Attacks

STATEFUL INSPECTION FIREWALL

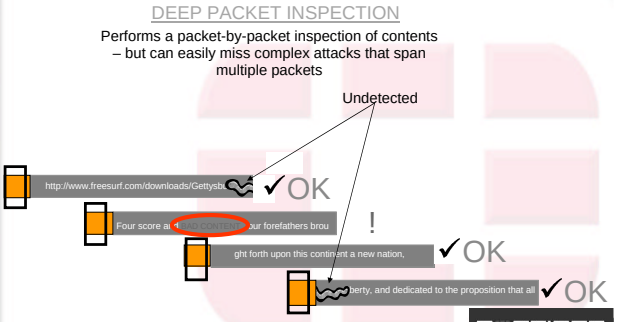
Inspects packet headers only – i.e. looks at the envelope, but not at what's contained inside



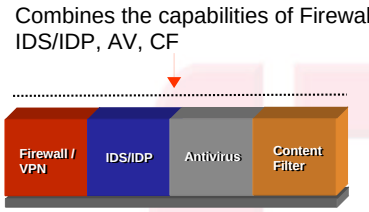
Second Generation: Deep Packet Inspection

Deep Packet Inspection typically combines functionality of IDS/IDP system with Stateful Inspection firewall

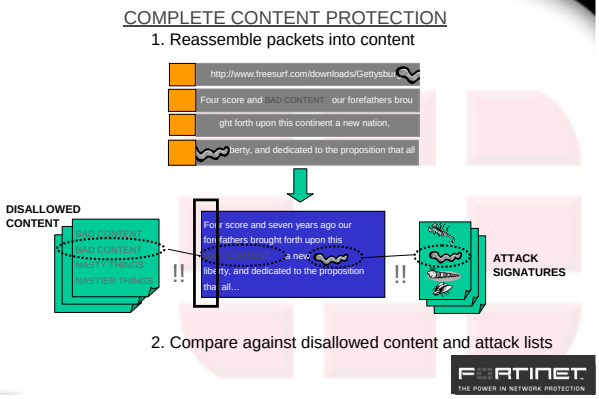
"Deep Inspection" Examines Individual Packet Payloads but Still Misses Most Content Attacks



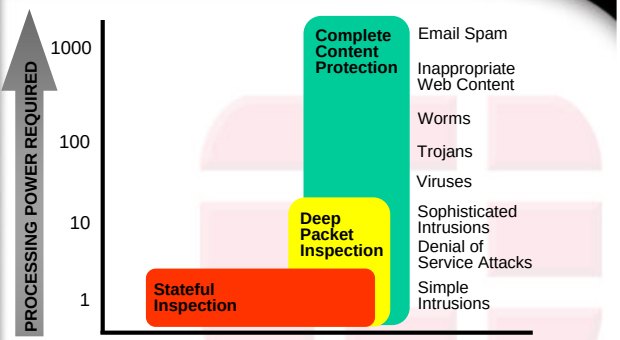
Next Generation: Complete Content Protection



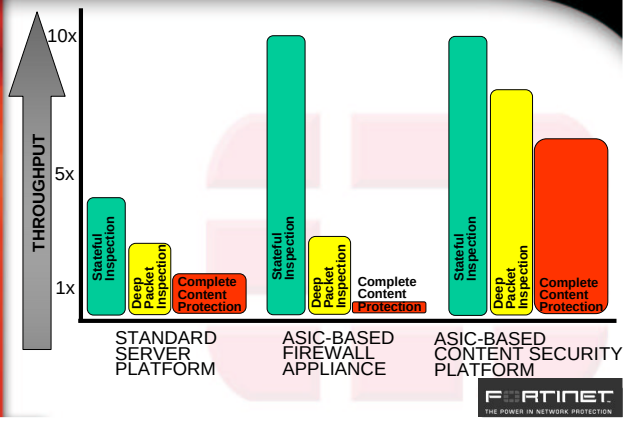
To Stop Content-Based Threats Requires More than Deep Packet Inspection



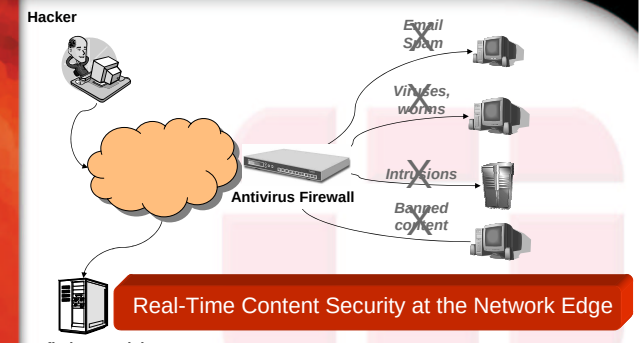
Complete Content Protection Requires Enormous Processing Power



A New Hardware Architecture is Required



Only Modern Perimeter Solution



Real-Time Content Security at the Network Edge

www.find_a new job.com
www.free music.com
www.pornography.com

Point Solutions vs. Integrated Solution

	Point Solutions	Integrated Solution
Configuration	• Inter-operable • Components may not be "talking"	• Tightly integrated
Platform	• Standard server architecture • Specialized ASIC (FW/IDP)	• Specialized ASIC (FW/IDP/AV/CF)
Management	• Resource intensive	• Resource efficient
Performance	• GB performance for FW/IDP w/ ASIC platform • Non-GB for AV	• GB performance for FW/IDP/AV/CF
TCO	• Costly • Multiple components	• 50-80% lower hardware cost • 50-80% lower management costs

Conclusion - Unified Threat Management

New **Unified Threat Management (UTM)** Security Appliance marketspace, unification of firewall and gateway anti-virus into a single platform - Fortinet ranked #1

IDC
Analyze the Future

- UTM market revenue in 2003 of $85 million -- over the next 5 years the revenue generated by the sale of UTM appliances will exceed that of standard firewall/VPNs
- Firewall/VPN segment, 2003 revenue of nearly $1.5 billion
- 17% annualized growth rate for combined category, $3.45 billion by 2008

FORTINET
THE POWER IN NETWORK PROTECTION

Thank You!

Modern Challenges to Perimeter Security

Security Conference 2004, London, UK

Franjo Majstor
Fortinet Inc.