

The Fortinet logo is displayed in a white, stylized font within a black rounded rectangular box. The letter 'O' is replaced by a red and white grid pattern. A small 'TM' trademark symbol is located at the end of the word.

FORTINET™

THE POWER IN NETWORK PROTECTION

Securing Networks Against A New Generation of Threats

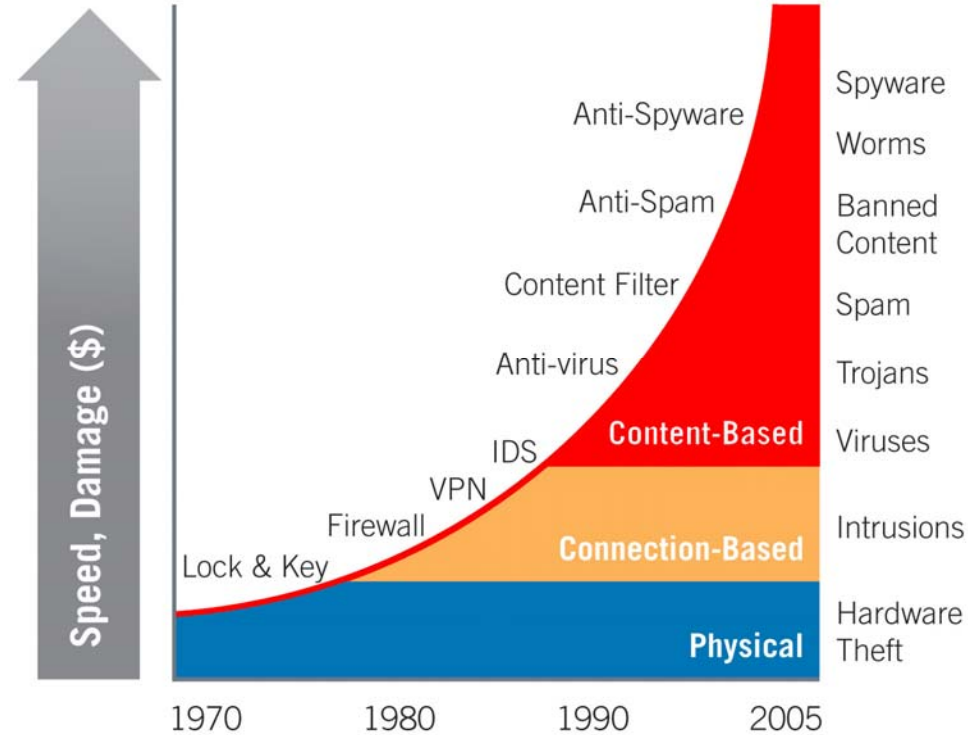
Current Security Trends

- Number of threats are increasing
- Sophisticated blended threats are bypassing traditional security defenses
- Time of infection is becoming faster – manual updates are no longer effective
- The motive and intent for attacking is changing
- Attacks with social engineering are rising – Phishing, Spyware, mass mailers leveraging address books, etc.
- Attacks are no longer obvious to users – Example is Pharming



Threat Evolution

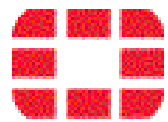
- Malicious code exposing confidential data has increased significantly
 - Blended attacks are now a common practice
 - Email is the most common delivery mechanism
 - Windows is not alone, attacks against Linux is increasing
- The motive and intent is changing
 - moving from notoriety to financial gain
 - theft of financial and personal information



The Rise of Blended Attacks

- Blended Threats:
 - Designed to maximize damage and speed of infection
 - Fast spreading network-based threat with multiple attack vectors:
 - Combination of virus, worm, and exploits vulnerabilities
 - Many leverage email to spread with a malicious payload attachment
 - Can self replicate acting as a hybrid virus/worm
 - Remote execution, DoS, Backdoor applications
 - Examples: Nimda, CodeRed, Blaster, MyDoom, DeadHat, DoomJuice, Bugbear, etc
- Use of Social Engineering Rising
 - Trick users into installing or launching malicious code
 - Phishing for identity information
- Spam was originally a nuisance but is now a corporate security concern

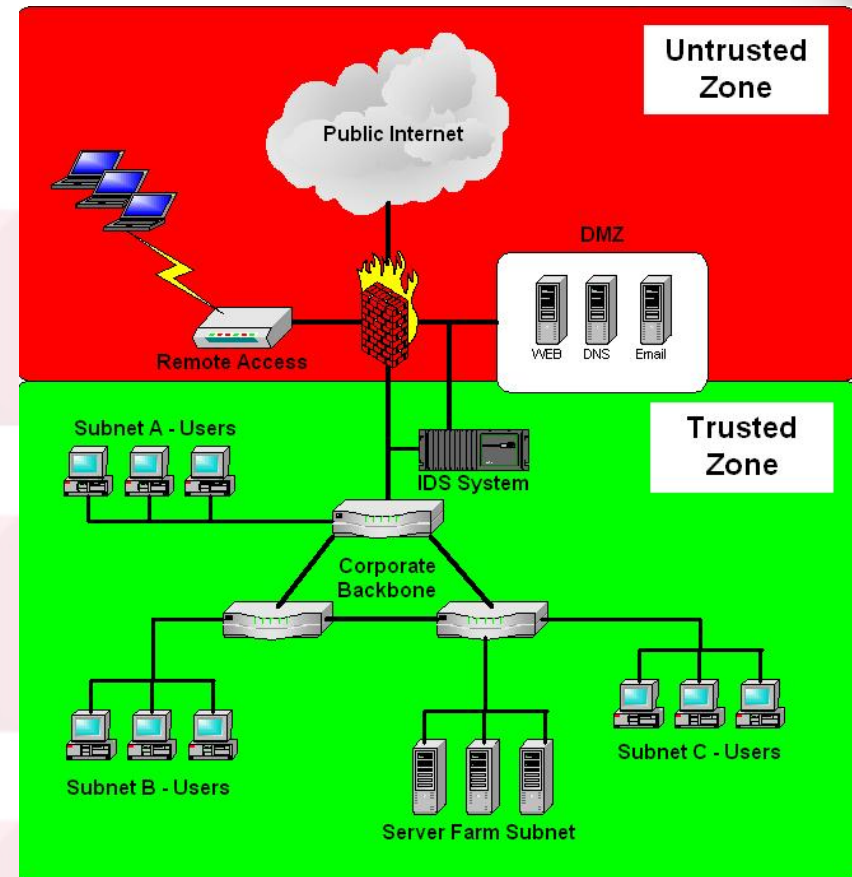




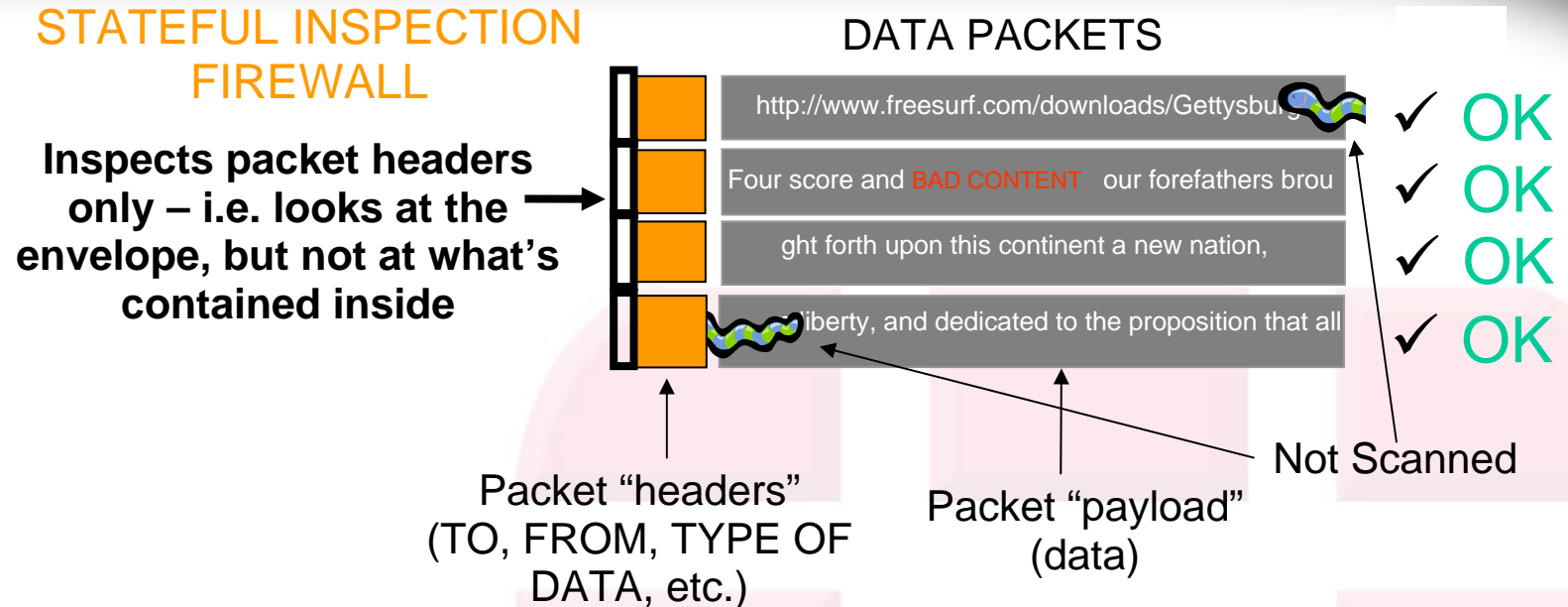
Traditional Security Defenses

The Problems With Traditional Security

- Traditional security tends to be Perimeter Based only
- Firewall & IDS at perimeter are ineffective against new threats
- Internal network is completely trusted
- Modern mobile computing is breaking the traditional model
- Many are still not layering key defenses for content-based security



Why Traditional Firewalls Miss The Latest Attacks



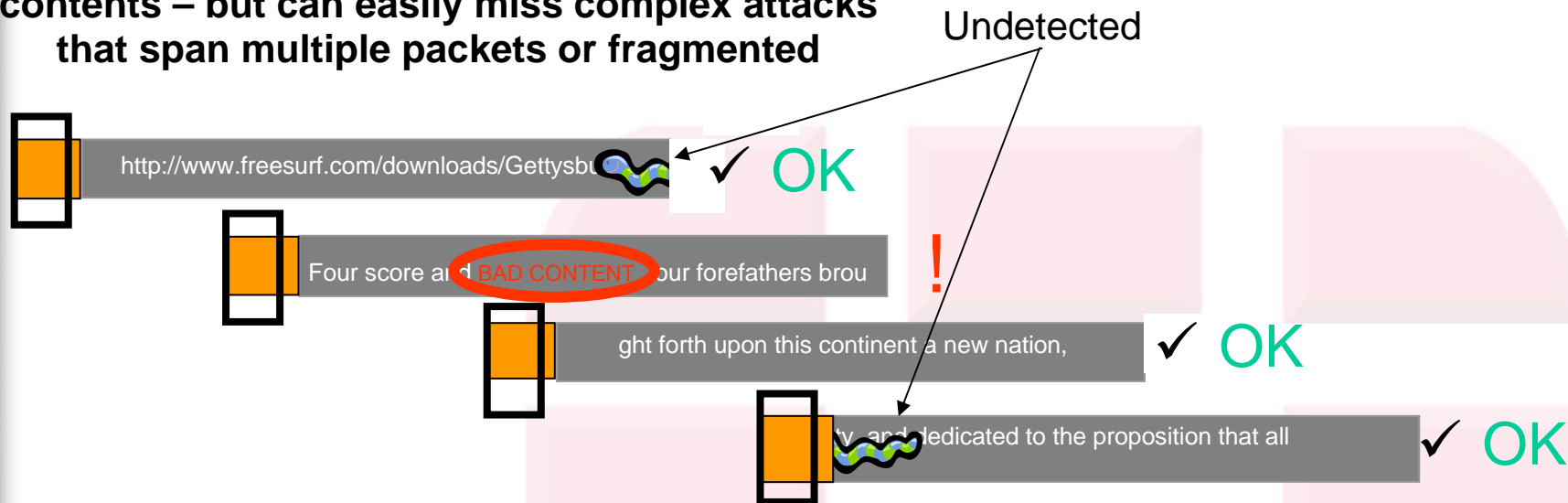
Traditional Firewall Weaknesses Include:

- No Deep Packet Inspection capabilities to spot malicious payloads
- Per-Packet forwarding with no packet reassembly
- Malware is tunneled through trusted ports
- Traditionally deployed only at the perimeter and can't defend against internal threats

How Traditional IDS Are Missing Modern Attacks

DEEP PACKET INSPECTION

Performs a packet-by-packet inspection of contents – but can easily miss complex attacks that span multiple packets or fragmented



Traditional IDS Weaknesses Include:

- Mirrored traffic analysis, not inline with network flow
- Alert only, will not proactively block attack traffic
- Damage is done before alert can be responded to
- Deep Packet Inspection IDS systems may be overrun by GB links

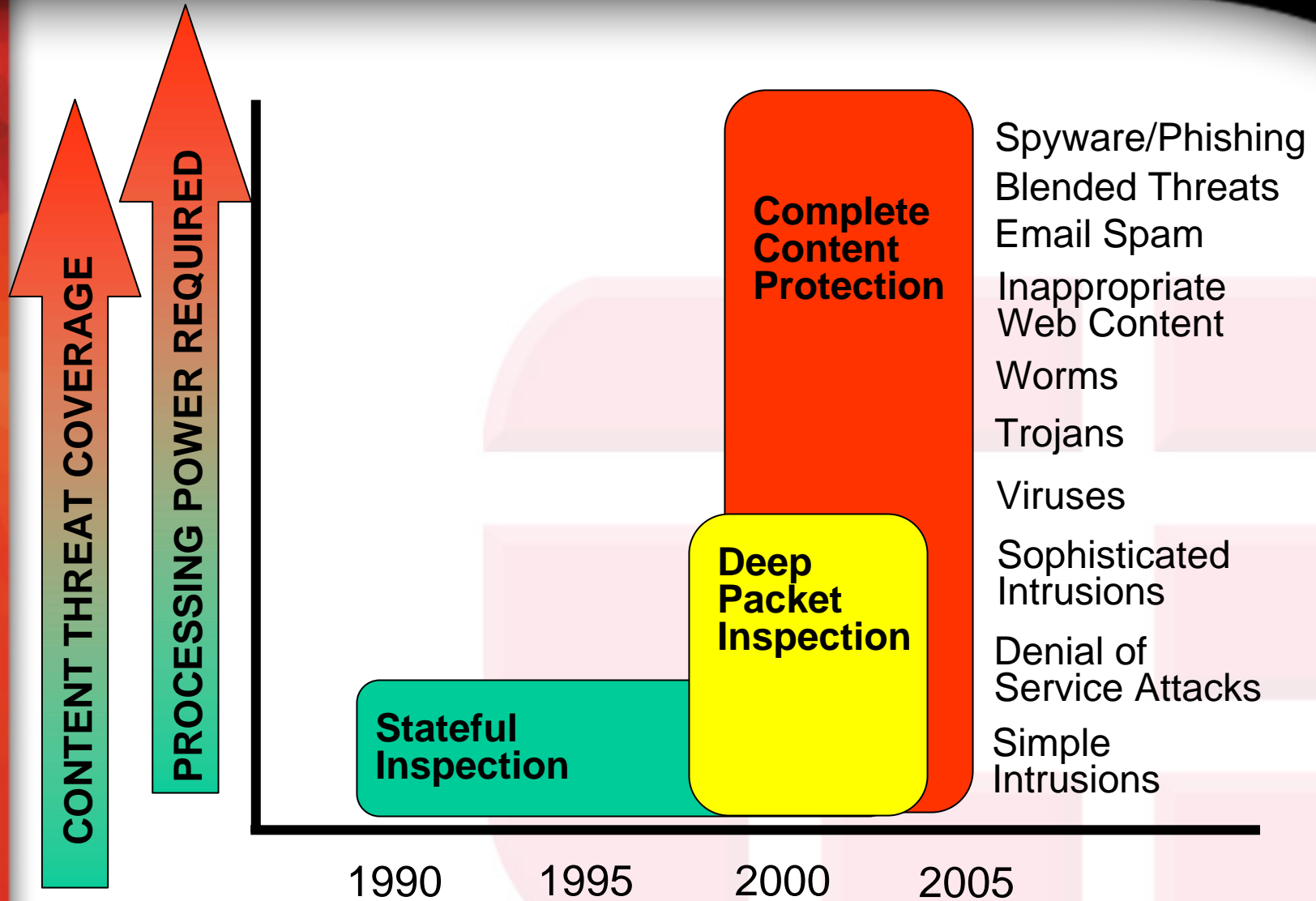
Traditional Security Being Superseded

- IDC Analyst predicts UTM multiple featured security appliances to grow 80% year over year
- Traditional Firewalls/VPN appliances see shrinking market share

Worldwide Unified Threat Management Security Appliance and Firewall/VPN Security Appliance Revenue, 2003–2008 (\$M)							
	2003	2004	2005	2006	2007	2008	2003–2008 CAGR (%)
UTM security appliance	105	225	518	828	1,325	1,987	80.1
Firewall/VPN security appliance	1,479	1,668	1,792	1,804	1,623	1,462	-0.2

Source: IDC, 2004

Network Security Technology Needs to Evolve



Why Network Security Must Evolve

The Obvious...

- To detect the newer breed of threats that are evolving

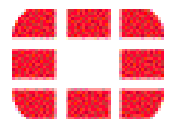
The Legal Implications...

- Government & industry regulations are causing unprecedented pressure on corporations to secure their electronic communications
 - HIPPA, Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA)
 - Various SEC regulations
 - California's SB 1386 (public disclosure of security breaches)
 - European Union Data Protection Directive
- Corporate concerns with employee productivity, legal liability, and network resources demonstrates the need to regulate Web content

Traditional security is evolving into...

...Secure Content Management

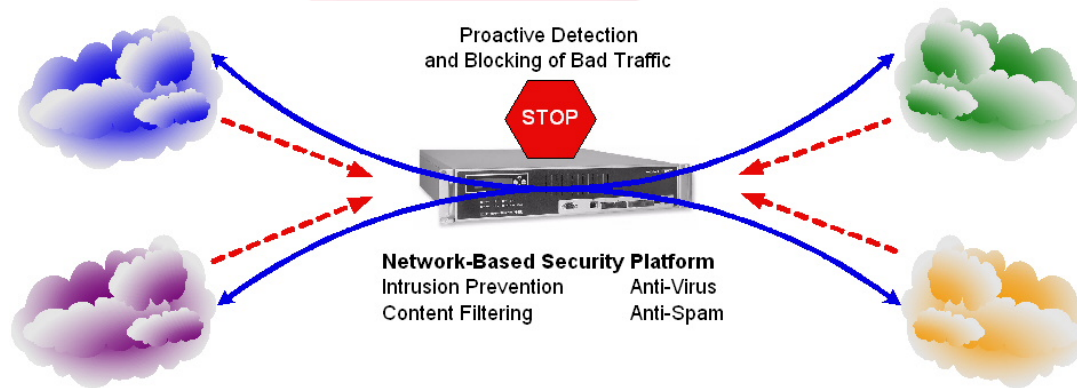




New Generation Security Defenses

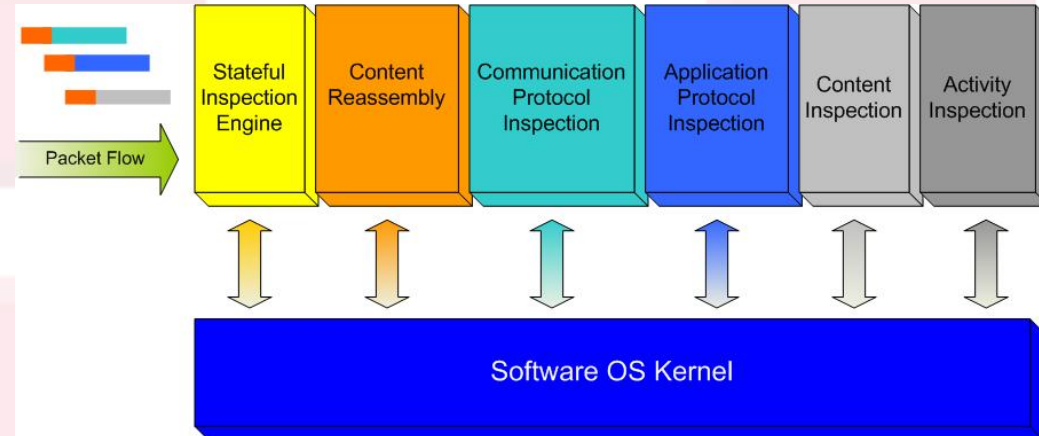
New Generation Security Characteristics

- **Network-Based**
 - Proactive defense designed to sit inline with network traffic
 - Not a “reactive” security system that works with alerts, TCP reset, and reprogramming of firewall rules (too slow for fast attacks)
 - Able to detect malicious traffic within normal network traffic regardless of application port
- **Layered Approach**
 - Firewall, IDS/IPS, Antivirus, Antispam, Web Content Filtering
- **Real-Time Updates**
 - Proactive approach for updating security devices
 - In-cloud services with fee structure
 - AV signatures, IDS & IPS attack updates, Detection Engine upgrades



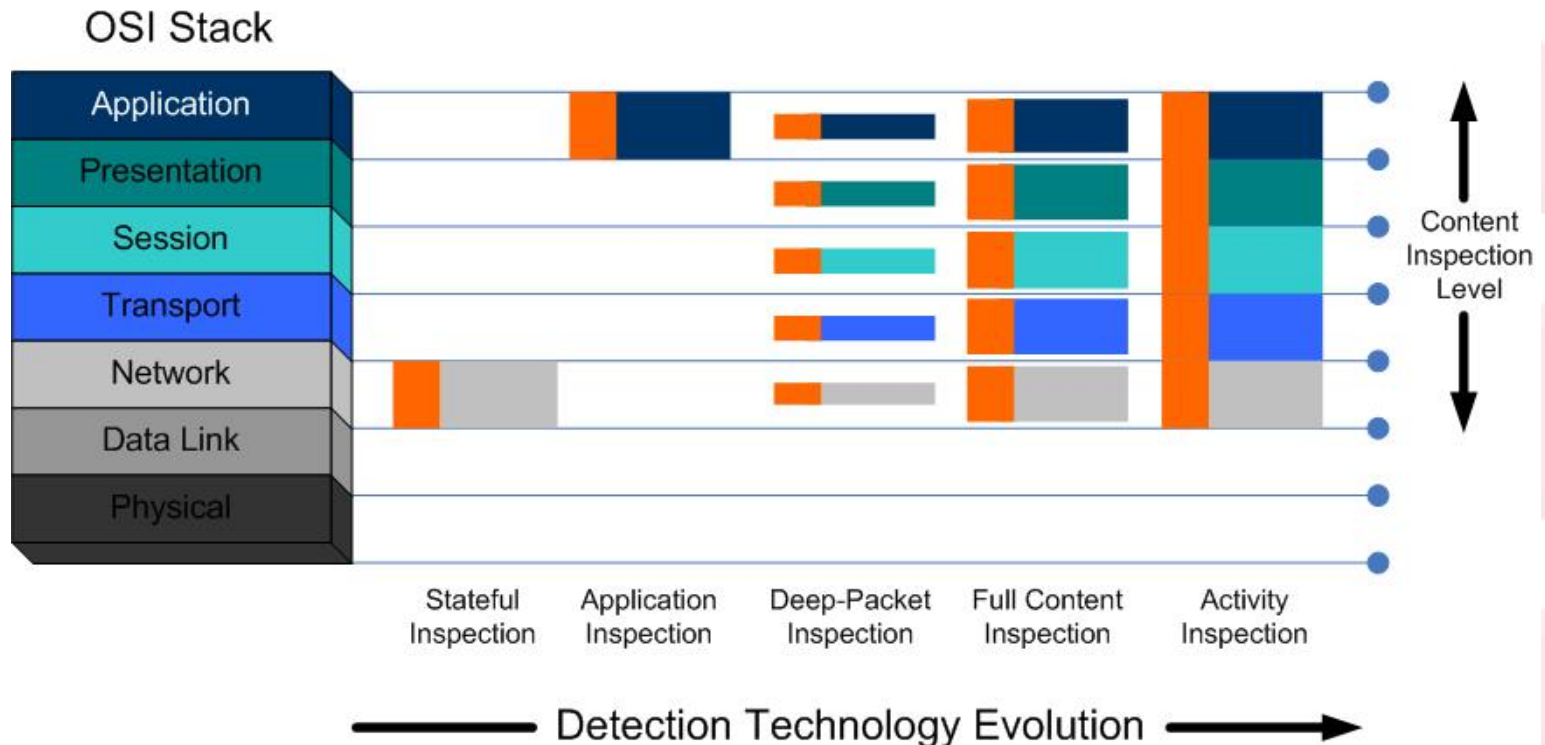
New Generation Security Characteristics

- **Multiple Detection Techniques**
 - Attack Signature
 - Heuristics
 - Traffic Anomaly
 - Behavioral (normal vs abnormal)
- **Supplements Other Technologies**
 - Host based AV, FW, IPS
 - Network Access Control (Cisco, Microsoft, TCG's TNC)
- **Combination of Approaches In Appliance**
 - Multiple security functions
 - Real-time protection
 - Automated updates
 - Real-time reporting



New Generation Security: Advanced Detection

- **Combination of Multiple Detection Technologies:**
 - Stateful Inspection
 - Deep Packet Inspection
 - Activity Inspection
 - Application Inspection
 - Full Content Inspection
 - Signatures, Heuristics, Anomaly



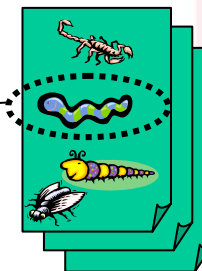
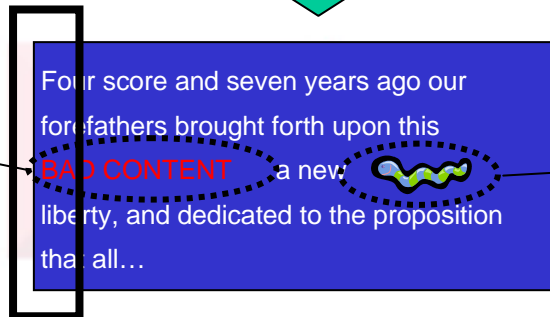
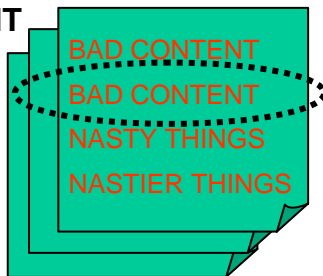
New Generation Security: Complete Content Protection

COMPLETE CONTENT PROTECTION

1. Reassemble packets into content



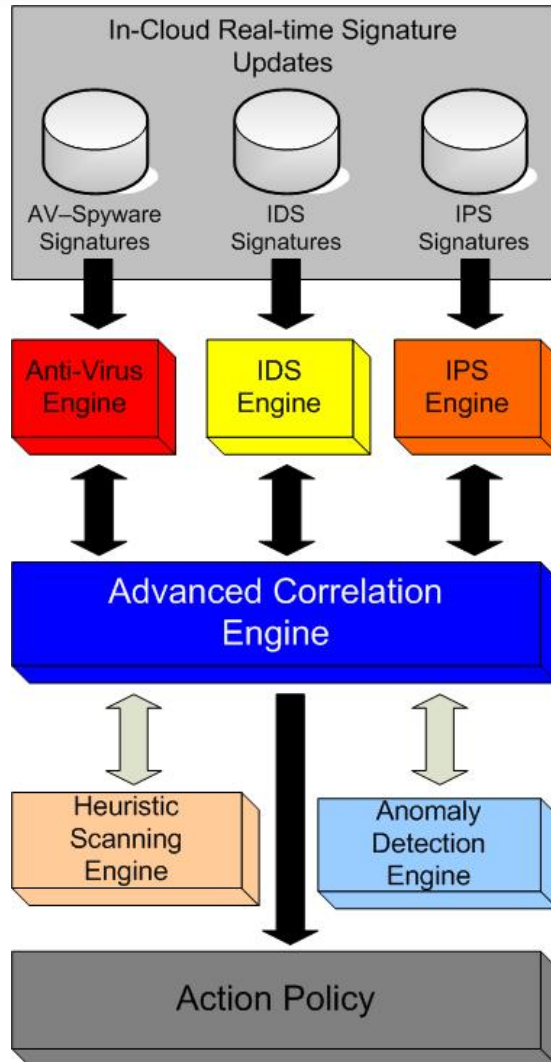
DISALLOWED
CONTENT



ATTACK
SIGNATURES

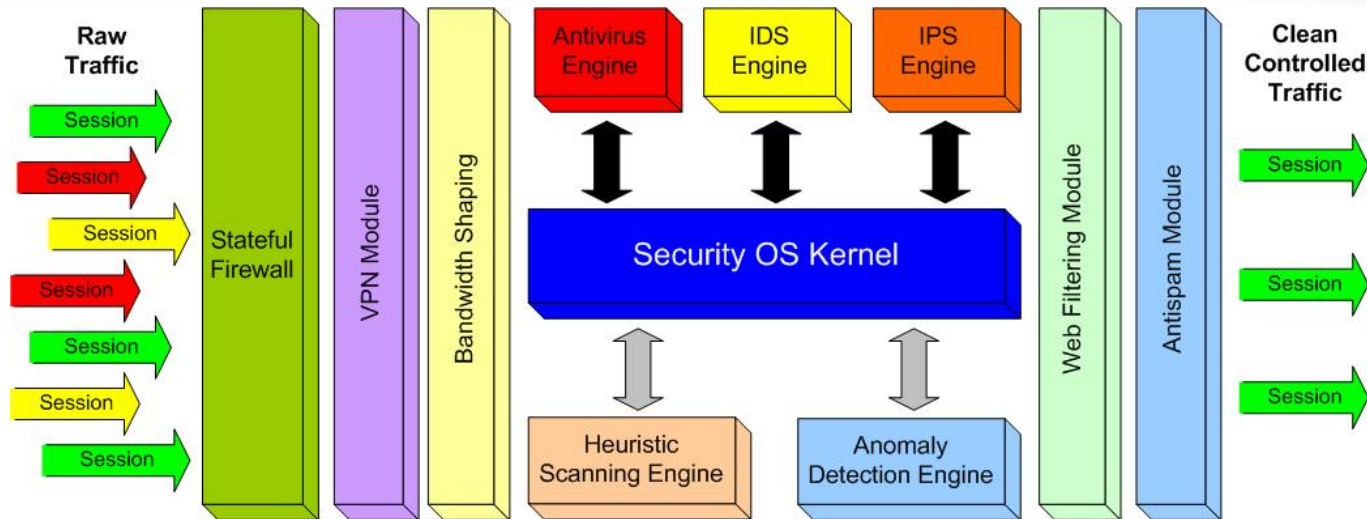
2. Compare against disallowed content and attack lists

New Generation Security: Advanced Correlation



- **Advanced Correlation Engine**
 - Increases detection effectiveness over signature only approaches
 - Raises bar against “zero-hour” threats
 - Leverages all detection engines to spot suspicious traffic
- **Hard to develop using multiple 3rd party security solutions**
 - Vendor A’s Firewall
 - Vendor B’s IDS / IPS
 - Vendor C’s Antivirus
 - Vendor D’s Antispam
 - Vendor E’s Web Filtering

Advanced Detection And Performance Issues



- Advanced detection requires much more processing power
- Ways to achieve higher performance:
 - Use more powerful platforms with multiple high-speed processors, more RAM, faster Bus, etc.
 - Use customized ASIC hardware for pattern matching acceleration
- Strategic chokepoint locations are key

Summary

- Blended threats will continue to get more sophisticated and harder to detect
- Layer Full Content security technology at perimeter, WAN, VPN, Wireless, and critical departmental or server farm connection points
- Don't treat internal networks as Completely Trusted – create security zones to with detection chokepoints
- Research and integrate Authentication technologies: 802.1X, Cisco NAC, MS NAP, etc.
- Centralize patch management and enforce
- Keep antivirus, personal firewalls, etc. up-to-date. Centrally manage if possible to prevent user manipulation
- Educate users on good security practices, develop good usage and security policies



The Fortinet logo is displayed in a stylized, white, blocky font. The letter 'O' is replaced by a red and white checkered pattern. The logo is set against a black rectangular background with rounded corners and a white border. The background of the entire slide features a dynamic, abstract design with orange and red geometric shapes, a grid pattern, and a glowing light effect in the bottom right corner.

FORTINET™

THE POWER IN NETWORK PROTECTION

Thank you

Philip Kwan
Director of Product Management