From Mobile Workers to IPv6 - How to Secure Todays Networks

Randy Lee
Director of Systems Engineering

November 4, 2011

The Network is No Longer Between Four Walls

The network has evolved to include:

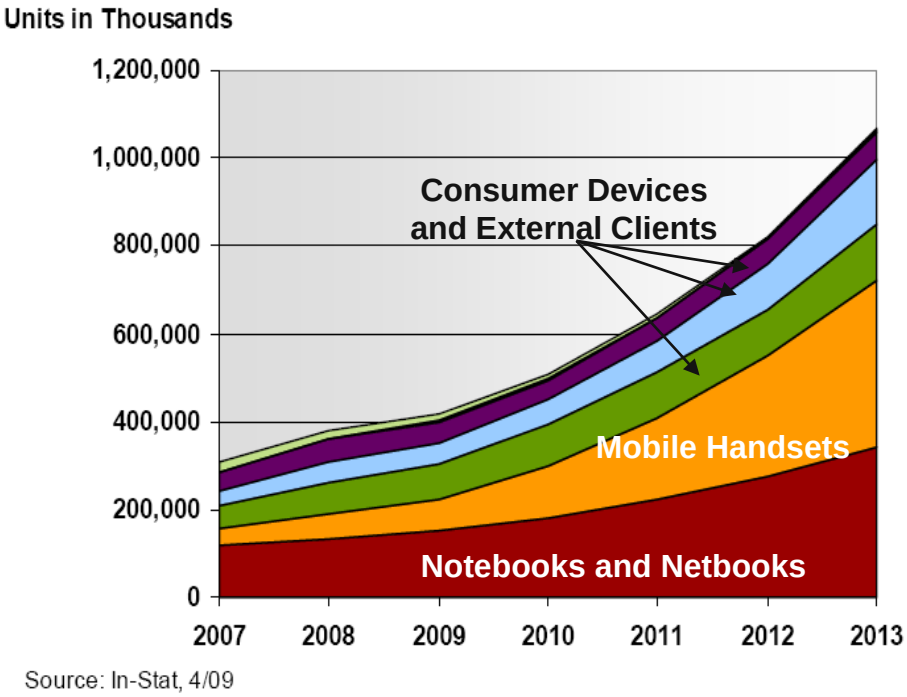
- Wireless mobile devices
  - Phones
  - iPads
  - Scanners
- Remote workers with laptops
- SOHO deployments
- Business partners

- The network must securely protect all points of access to the network and no longer just the headquarters' network

Wireless Network Adoption and Drivers

Wi-Fi enabled devices, cost and PCI compliance are driving WLAN adoption

- Mobile handsets & netbooks necessitate wireless connectivity
- Key industries are already moving to a wireless edge design
  - Examples: education and healthcare
  - Wireless is less costly to deploy vs. an edge switch and wiring
- PCI Compliance requires Rogue Access Point detection and Wireless IPS at retail locations



Source: In-Stat, 4/09

CAGR of >50% for Mobile Handsets with Wi-Fi 2009-2013

Network Requirements are Changing

- IPv4 is no longer
- Now in a world of IPv6
- Threats are being proliferated throughout networks in more advanced ways than ever
- Fortinet is ready!
  - Tested and verified by third-party test labs appointed by the U.S. government
  - Achieved the U.S. Department of Defense IPv6 product certification conducted by the Joint Interoperability Test Command (JITC).
  - FortiGate appliances have been listed on the DoD's Unified Capabilities Approved Products List for IPv6 since 2008
  - FortiGuard Labs provides regular updates delivering real-time protection for any corporation or government agency migrating to an IPv6 network
  - FortiGate platforms have supported IPv6 since 2007

IPv6 Deployment Landscape

- Historical Drivers of IPv6
  - U.S. Federal government
  - Japan
  - Specific carrier or education projects
- Recent Activities
  - IPv4 address space exhaustion
  - Carriers are motivated
  - More & more requests from large carriers

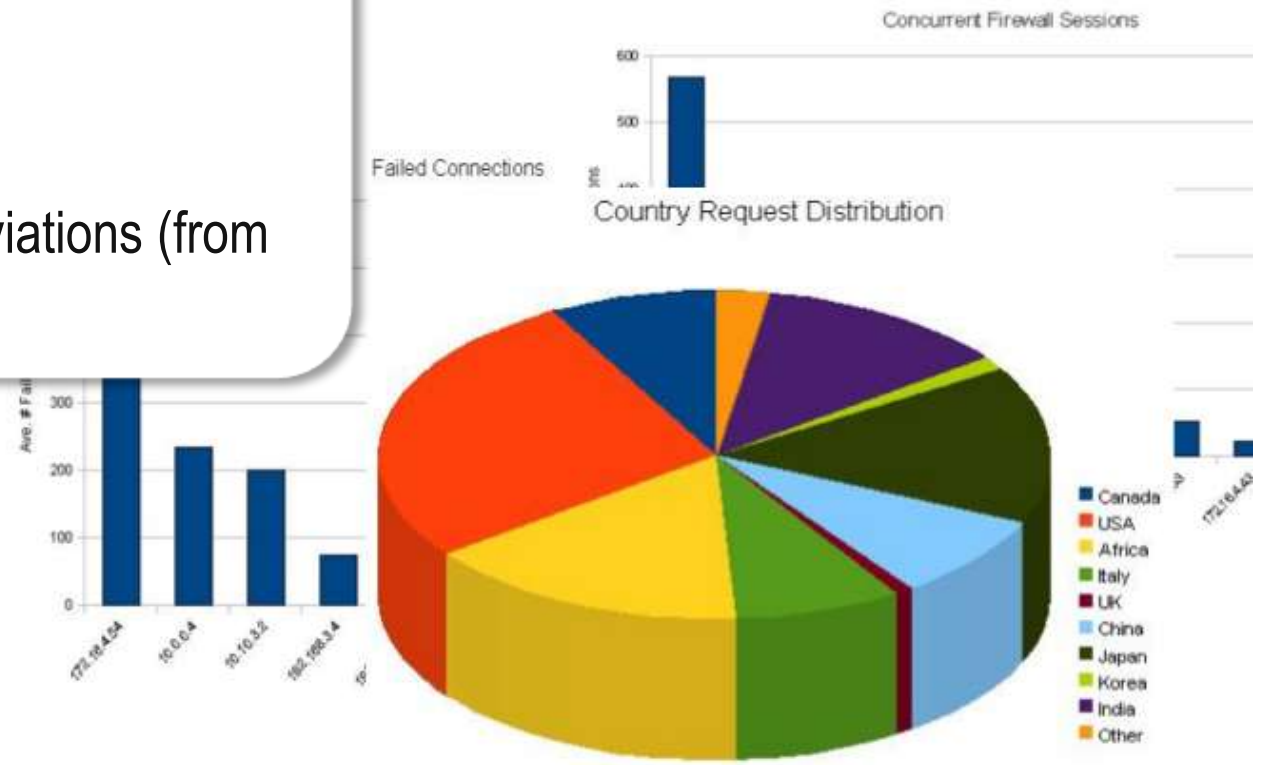
Current Threats Need More than Signature Detection

Threat Examples

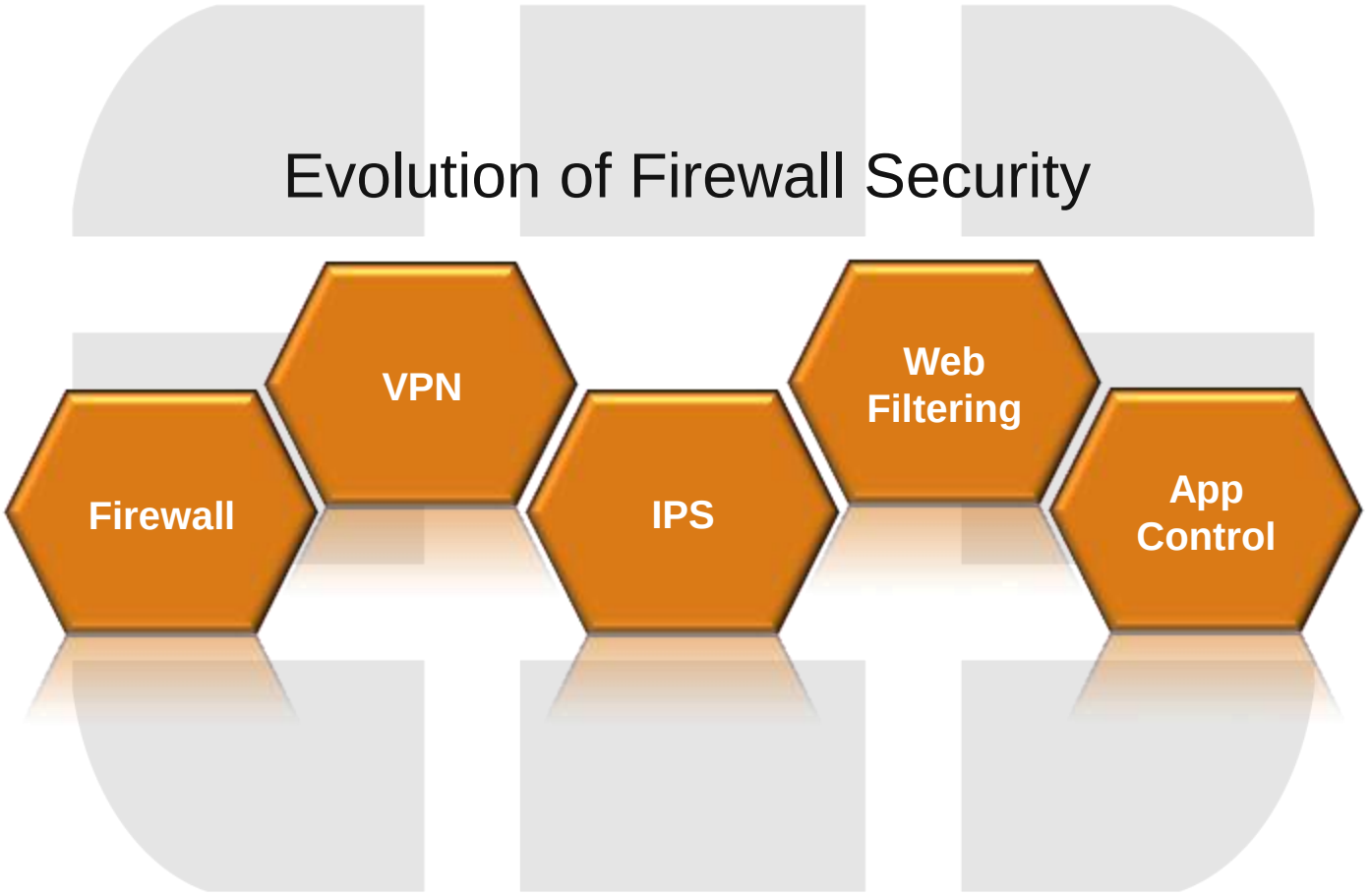
- Botnet
  - Main drivers for botnets are for recognition and financial gain
  - Conficker is one of the largest botnets out there that has infected an estimated 1 million to 10 million machines which attempts to sell fake antivirus to its victims
  - Newer botnets have even been capable of detecting and reacting to attempts to figure out how they work.
- Stuxnet
  - First discovered malware that spies on and subverts industrial systems,[3] and the first to include a programmable logic controller (PLC) rootkit.
  - Stuxnet contains, among other things, code for a man-in-the-middle attack that fakes industrial process control sensor signals so an infected system does not shut down due to abnormal behavior.[21][27] Such complexity is very unusual for malware.
- Evasion

Moving Beyond Signature-based Threat Detection

- Establish a Baseline:
  - Geography
  - Bandwidth
  - Applications
  - Failed connects
- Report Anomalies or Deviations (from baseline)

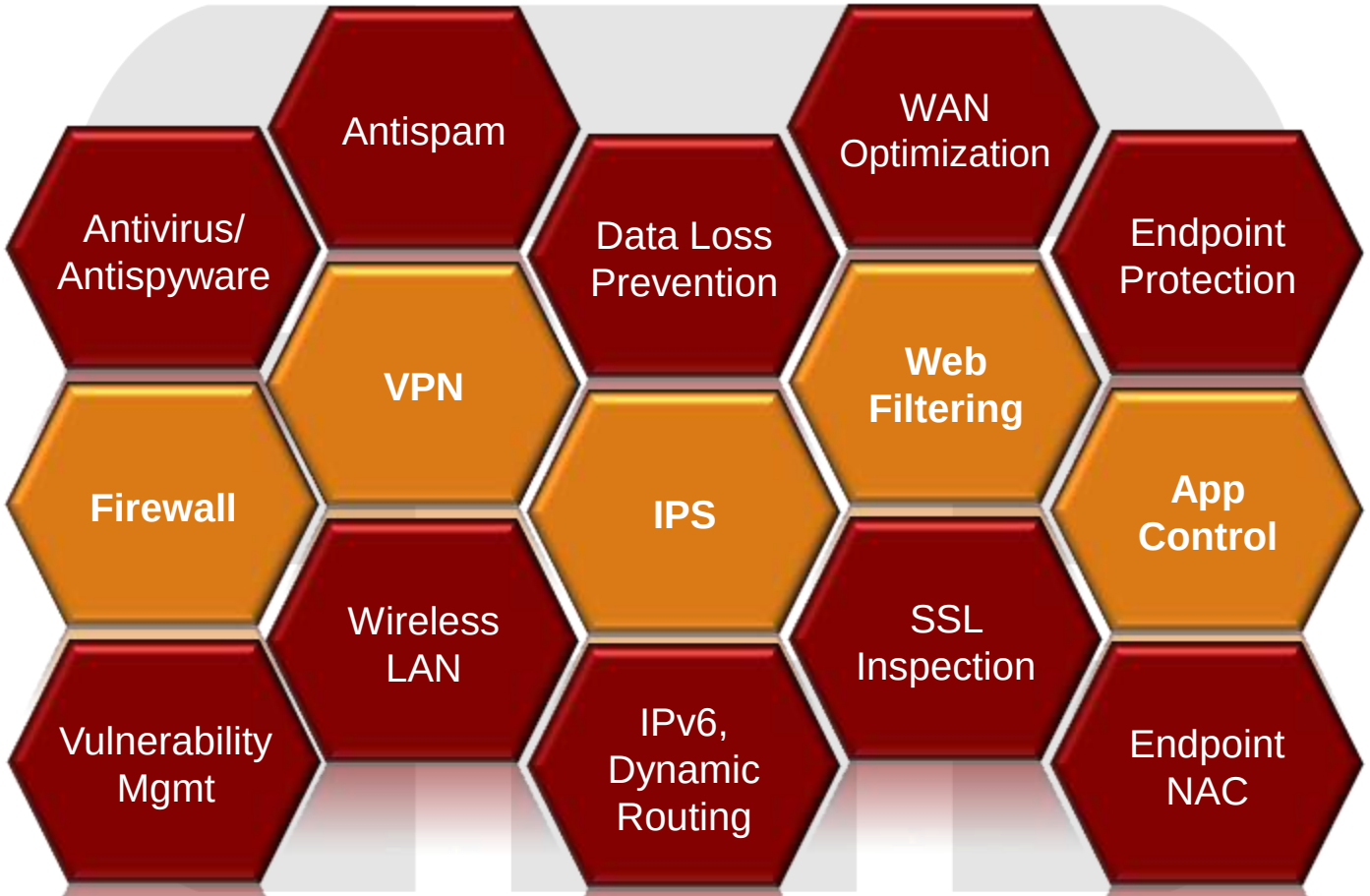


Evolution of Firewall Security



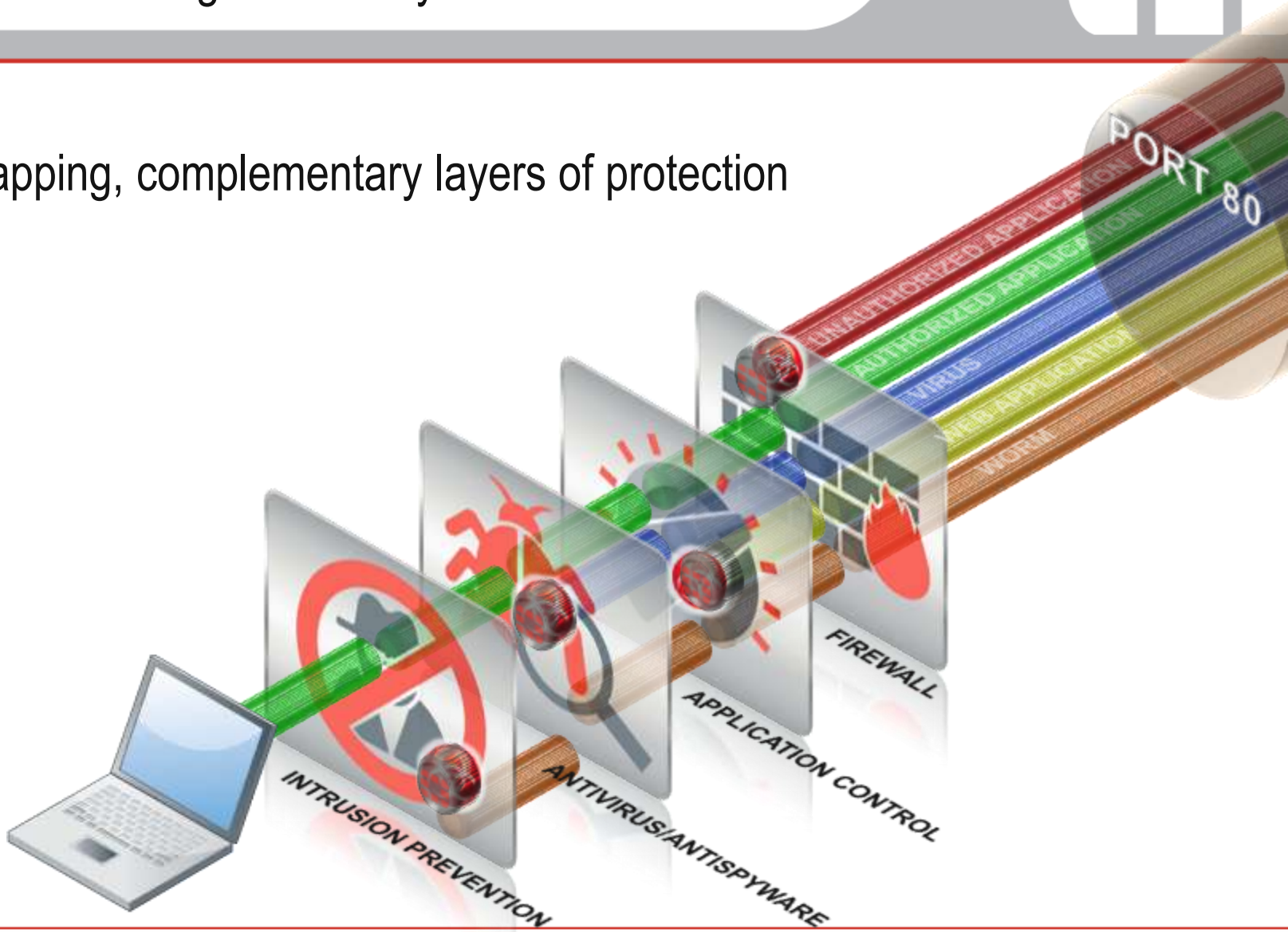
Evolution of Firewall Security

Complete Protection



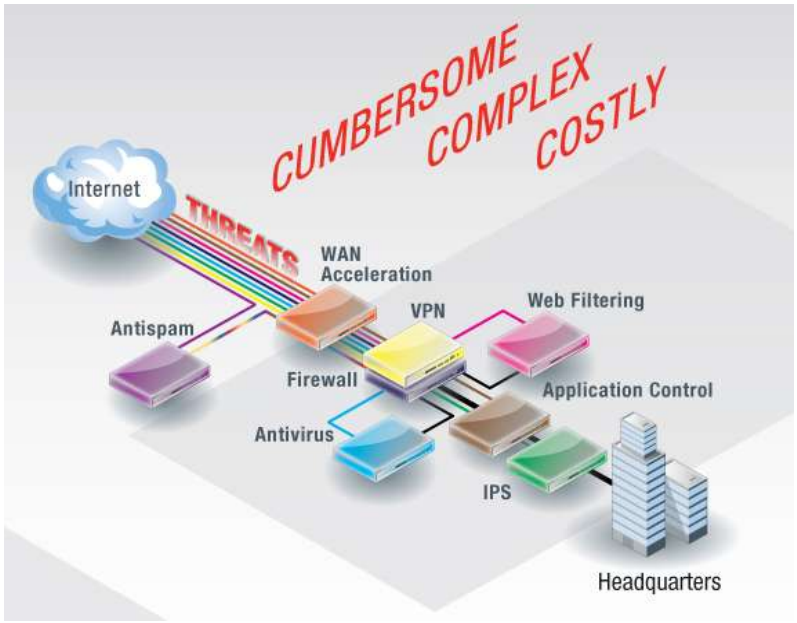
Layers of Protection Against Today's Threats

Overlapping, complementary layers of protection



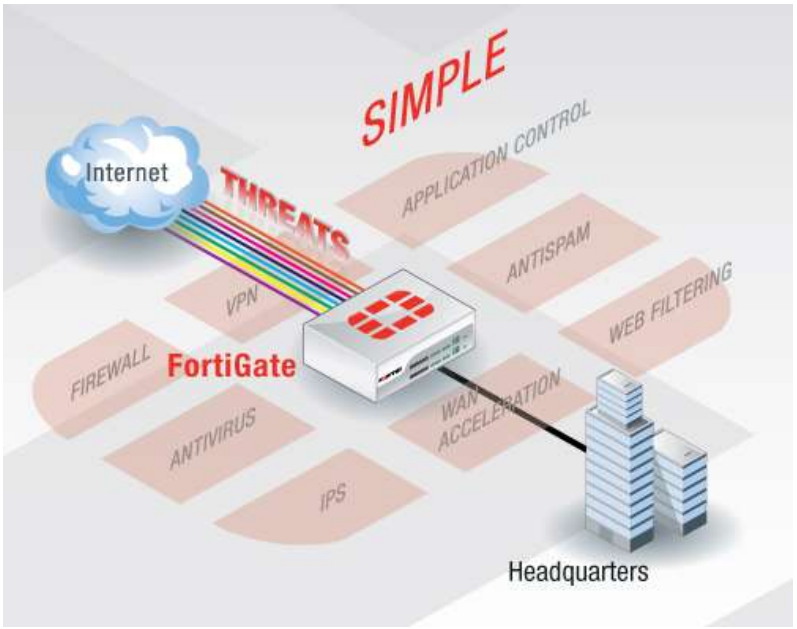
A New Approach

Traditional Network Security Solutions



- Stand-alone, non-integrated security
- Mix of off the shelf systems and applications
- Higher total cost of ownership – multiple vendors and licensing fees
- Difficult to deploy / manage / use

Integrated Solution



- Real-time, integrated security intelligence
- ASIC-accelerated performance
- Lower total cost of ownership – single vendor and no per user licensing fees
- Easy to deploy / manage / use

Thank you!

Randy Lee
Director of Systems Engineering

The leader in consolidated security solutions