

The Evolution of the Firewall

Chris Spain
Senior Director of Enterprise Product
& Solutions.
Security Products Group



JuniperTM
NETWORKS

Key Enterprise Drivers

Increased Productivity

- Ubiquitous Access
Anytime, Anyplace,
Anywhere
(IP WAN / VPN)
- Rapid Site Deployment
(IP WAN / VPN)
- Rapid Deployment of
New Applications
- Application Acceleration
(More Bandwidth &
overcome latency issues)

Reduced Cost

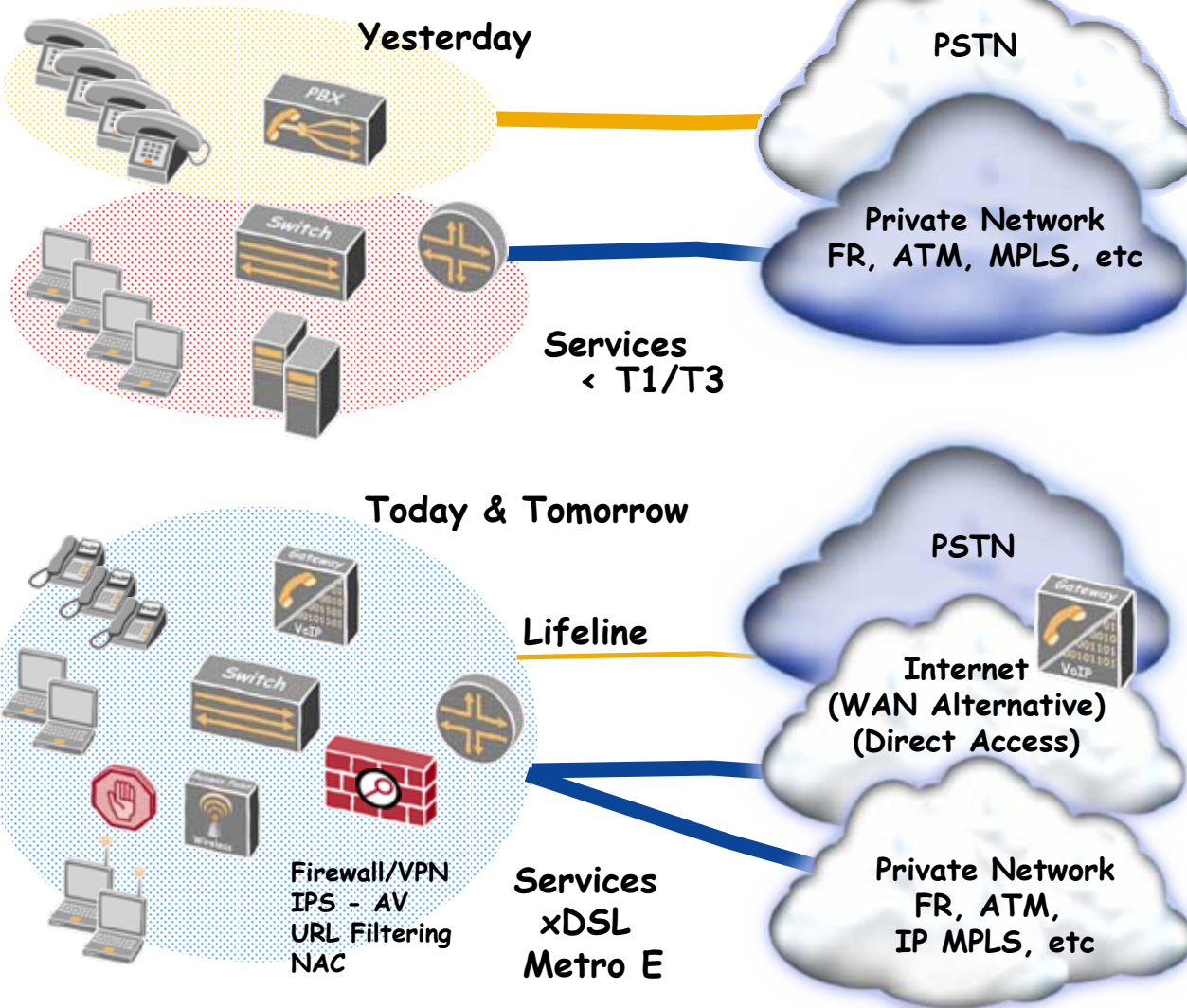
- Lower WAN Costs
(IP WAN / VPN)
- Centralize Assets
(Servers)
- Web Applications
(Clientless provisioning)
- Device Consolidation
- Simplify
Upgrade, Configuration,
Management

Business Continuity

- Connectivity
Redundancy
(IP WAN / VPN)
Primary/backup/both
- Rapid Site Deployment
(IP WAN / VPN)
- Remote (Home) Access
(In Case of Emergency)
- Security
(Risk Management)

A business expectation is that the network infrastructure will intelligently respond to their needs.

Enterprise Evolution



- Many disparate Networks
- Few (1) Perimeters
- T1/T3 centric connectivity

- One (IP) Network
- 100's of Perimeters Per Site Intra Site
- xDSL/Metro Ethernet as WAN

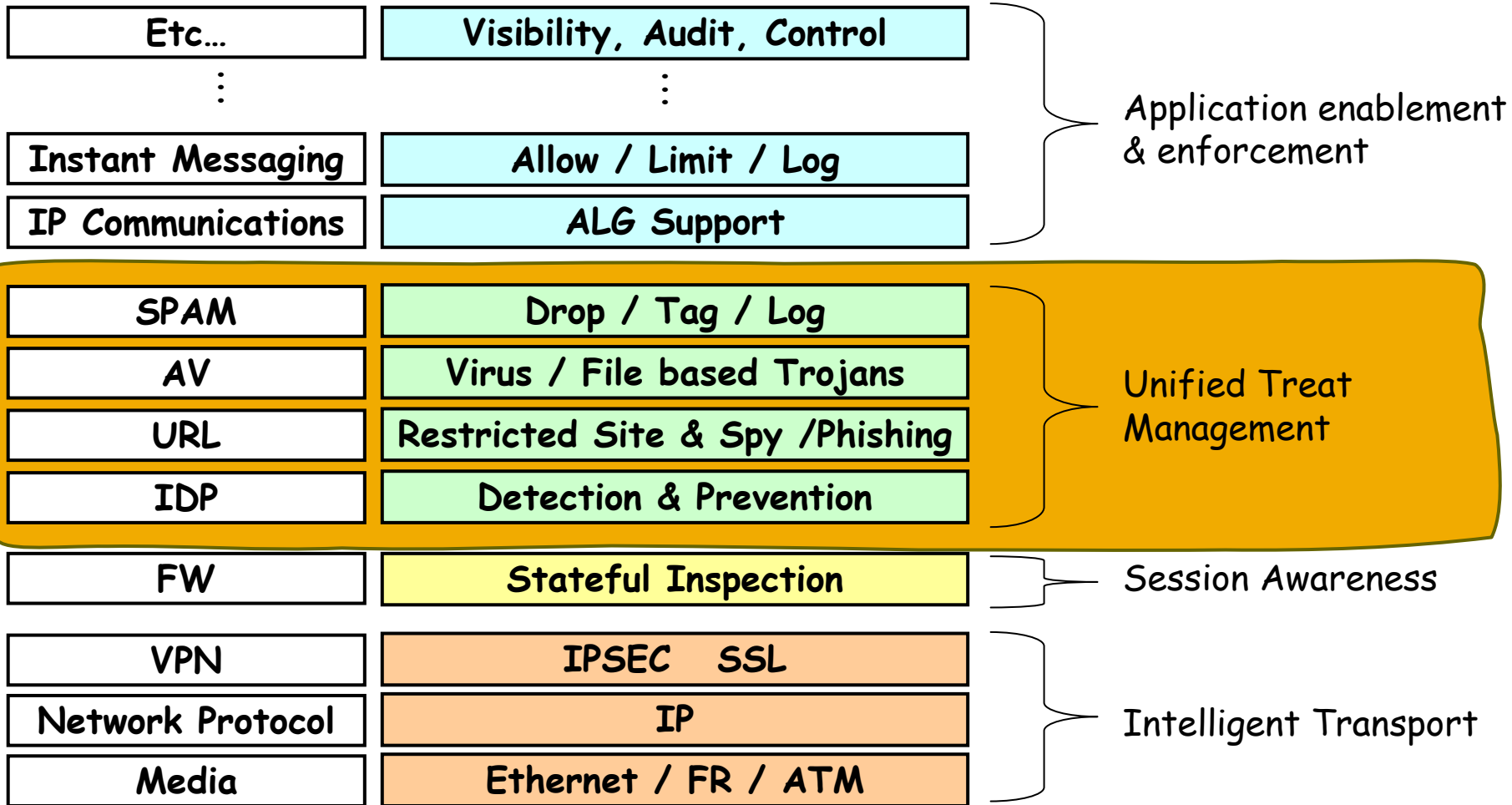
Juniper your Net

Up
Layers of security

Out
Extended Enterprise / Branch Office

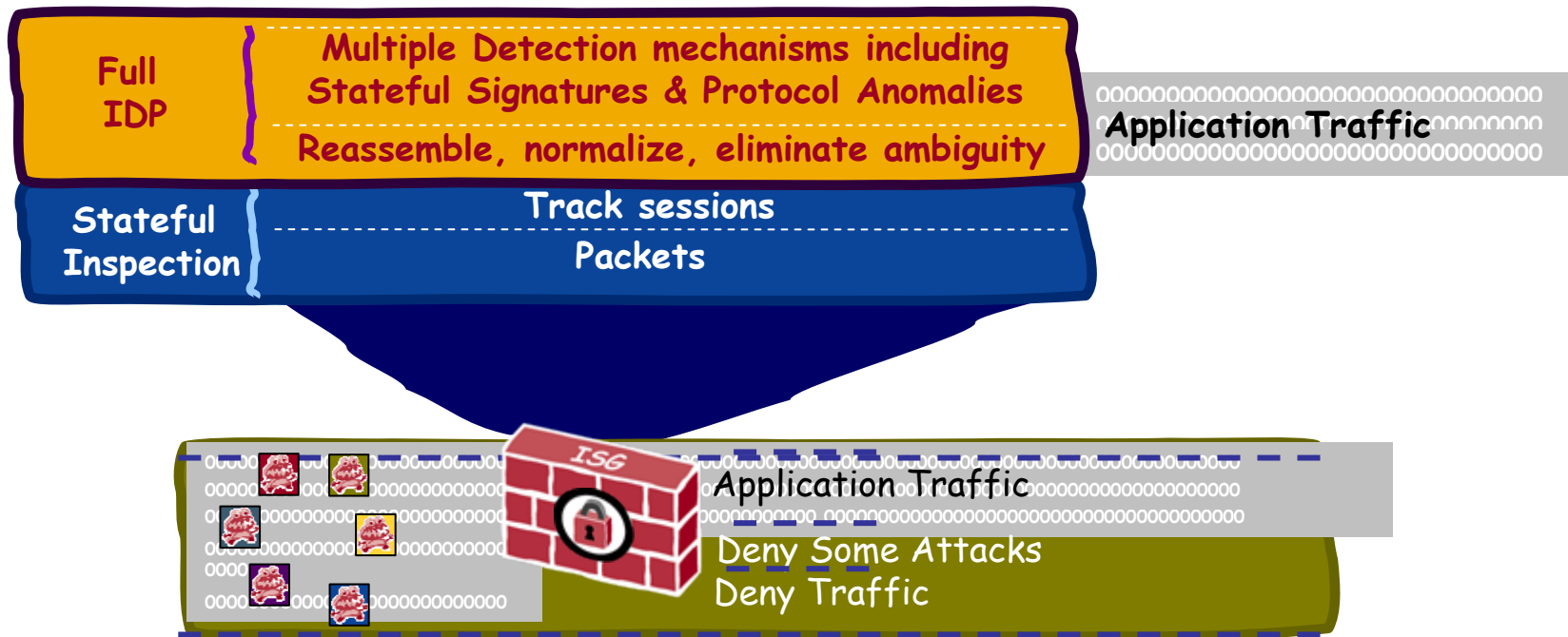
In
(Intra-Site)

Evolution of Security Upward UP



IDP

Stop Network & Application Level Attacks

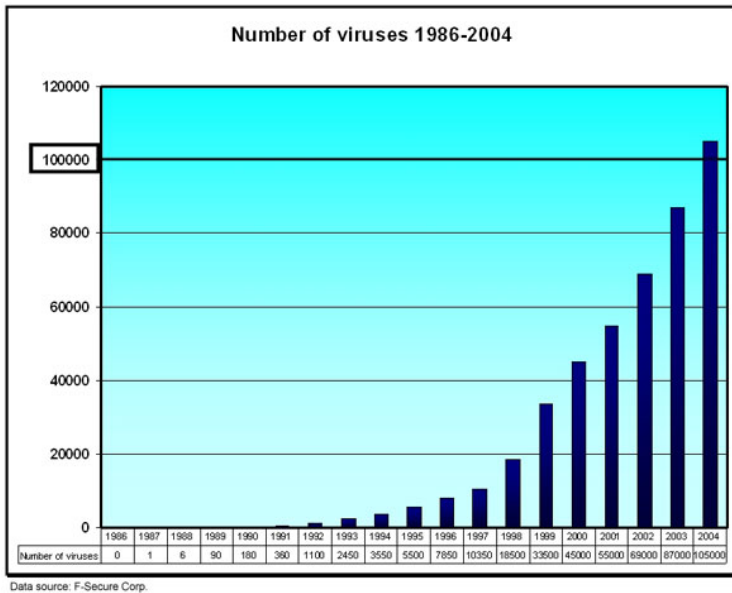


- Awareness of L2-7, Full protocol decode & application context
- Protect Network against protocol attacks, worms, Trojans, DDOS, recon & scans
- Day Zero Coverage via anomaly detection
- Best-in-Class; Detection Methods, Protocol coverage, Threat coverage, response time, accuracy & performance

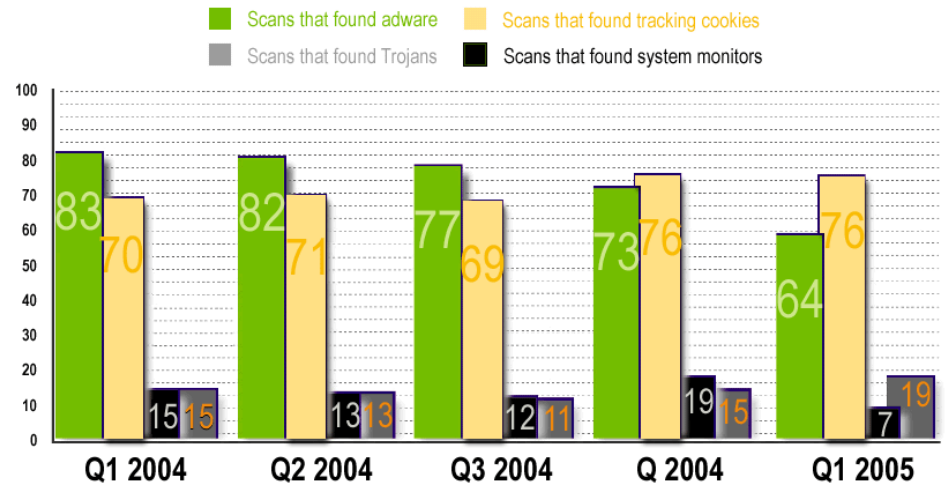
Juniper your Net

Anti-Virus

Stop Payload-based Attacks in the network



Spyware Found on Consumer Computers by All Categories, Q4 2004 and Q1 2005 (%)



Source: Webroot Corporate SpyAudit, 2005

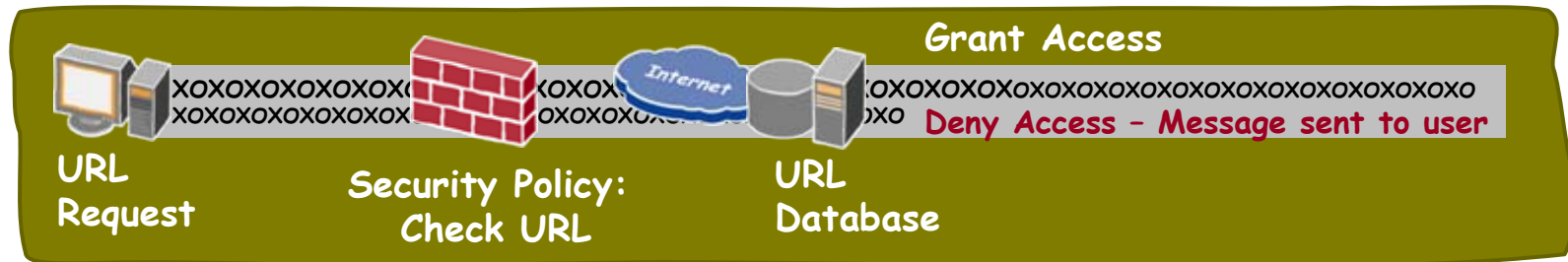
- Protect network against viruses, spyware / adware / keyloggers
Search & destroy viruses in SMTP, POP3, Webmail, FTP, IMAP & HTTP
- Protect against non owned (Guest/Contractor) & non compliant (out of date or AV disabled) endpoints
- Best-in-Class; Protocol coverage, Threat coverage, response time & performance

Juniper your Net

Web Filtering

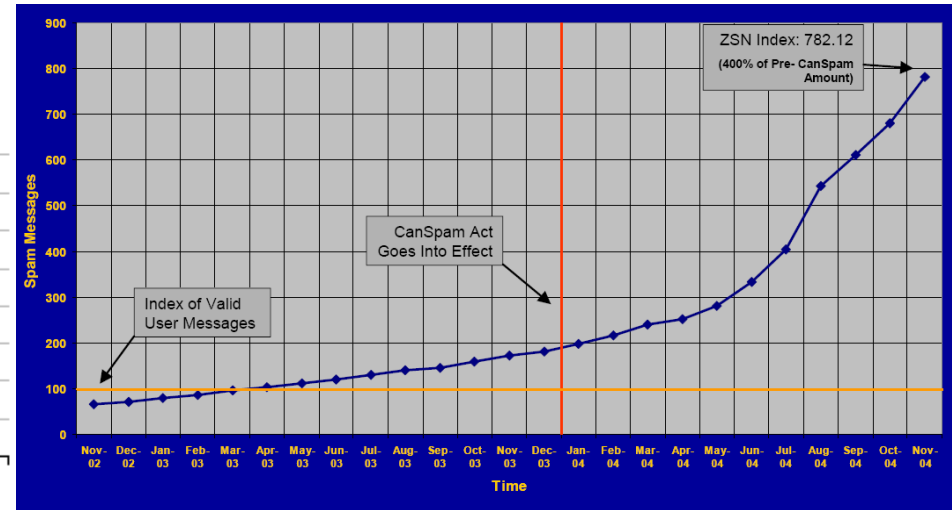
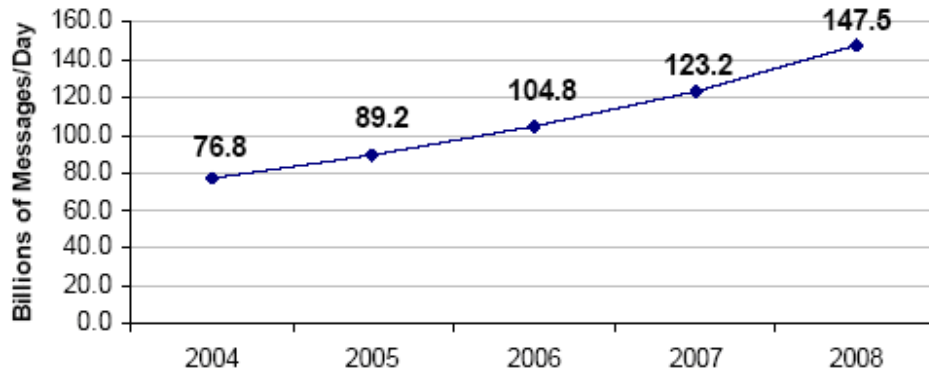
Enforce Web Usage Policies at the Firewall

- Control Web usage to improve employee productivity, network resource utilization & avoid litigation
 - Stop users from visiting known spyware, and phishing sites
 - Control sites visited through pre-defined or customized URL listings
- Policies can be based on site, type of content or user groups
- Best in Class; Coverage; ease of use & flexibility
 - Millions of urls, Billions of pages growing at 50K per week



Anti-Spam Filter Unwanted Email at the FW / Gateway

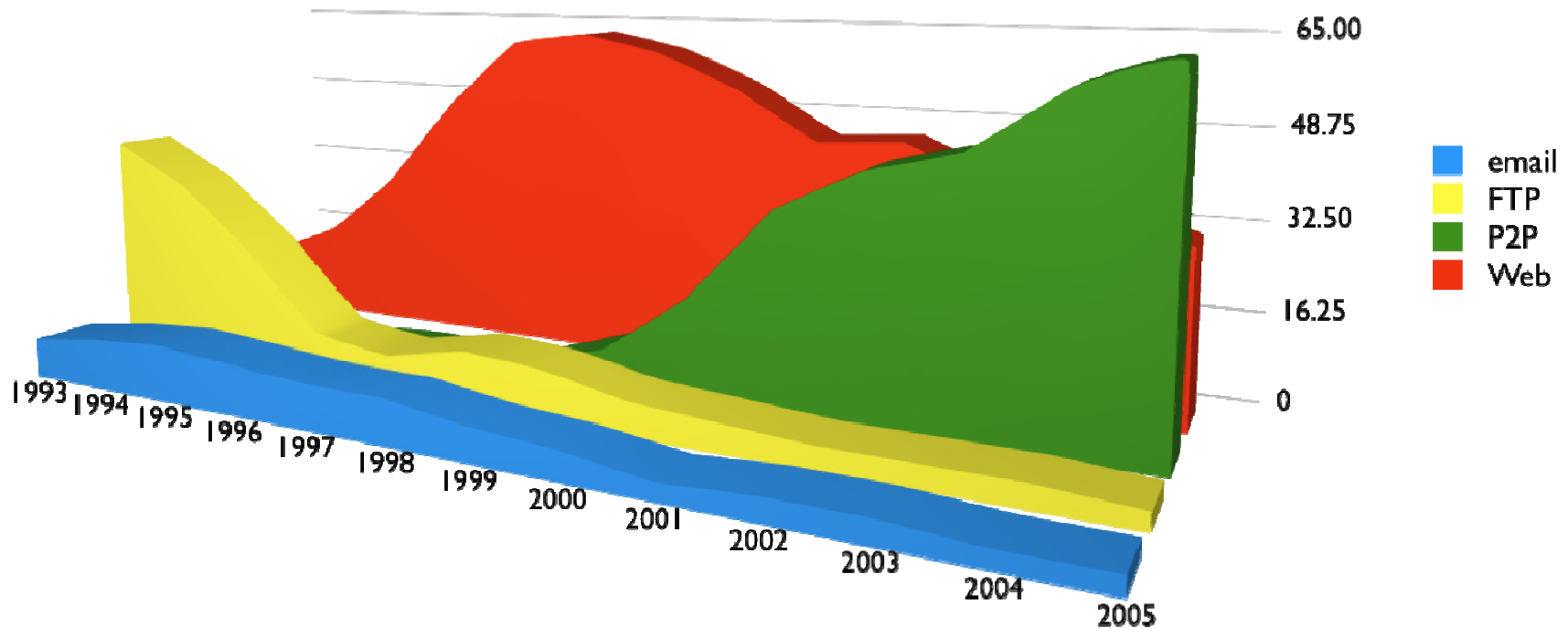
Email Traffic, 2004-2008



- Stop SPAM & Phishing attacks
- Best-in-Class; IP and Address based, constantly updated database
- Would Augment server based solutions

The Need for application awareness

Example - P2P traffic growth



- P2P represented 60% of the internet traffic at the end of 2005
 - P2P outstrips every other communication and distribution protocol and is still growing
- Desirable and undesirable use of P2P in the business
 - Desirable, lower Telephony Costs
 - Undesirable, File sharing, Embedded threat

Using IDP to control P2P

- Coverage for top P2P networks and enterprise applications (Application Identification)
- Policy - Allow, Deny, Log usage, Rate Limit
- Application Volume Tracking (AVT)
 - bandwidth usage/host
- QoS marking of traffic deemed inappropriate (Action)

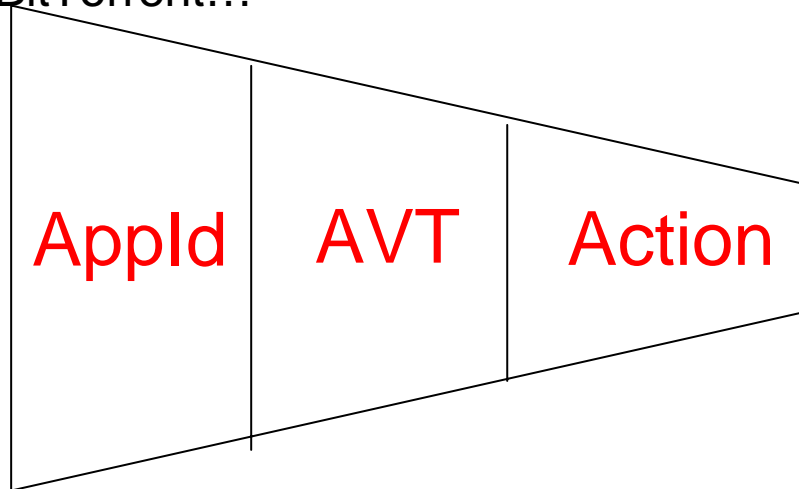
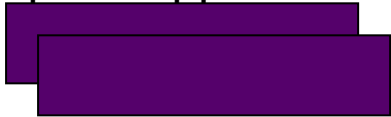
Kazaa, Skype, Napster, BitTorrent...



Gaming...



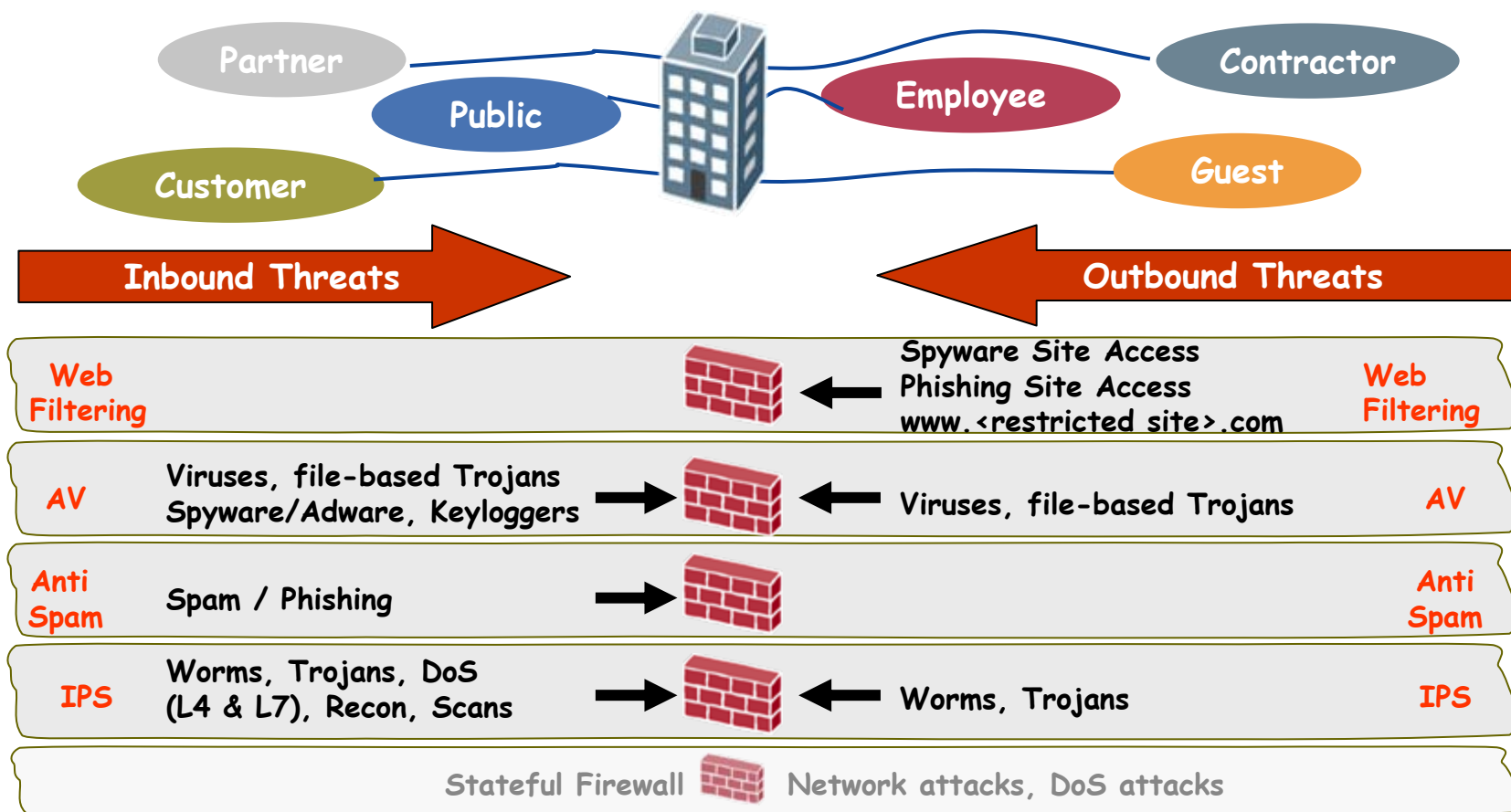
Enterprise apps...



Evolution of Security Upward

- Need for Deeper Levels of Inspection

The Solutions of Tomorrow Must Stop Known & Emerging Threats From All Directions



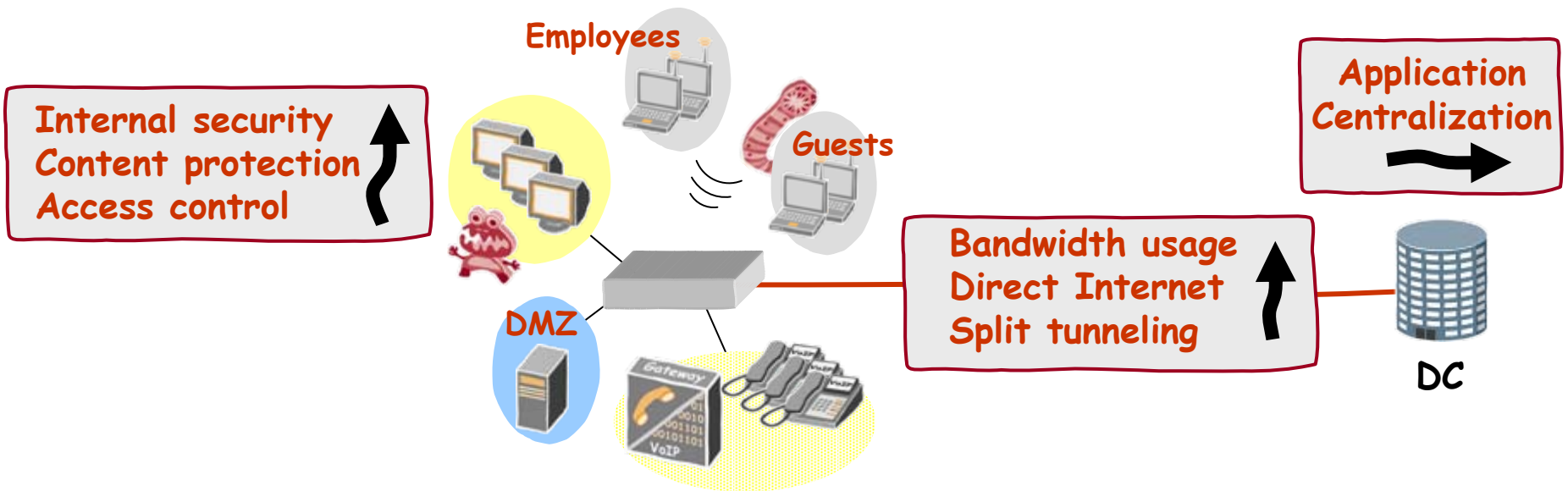
Juniper your Net

Up
Layers of security

Out
Extended Enterprise / Branch Office

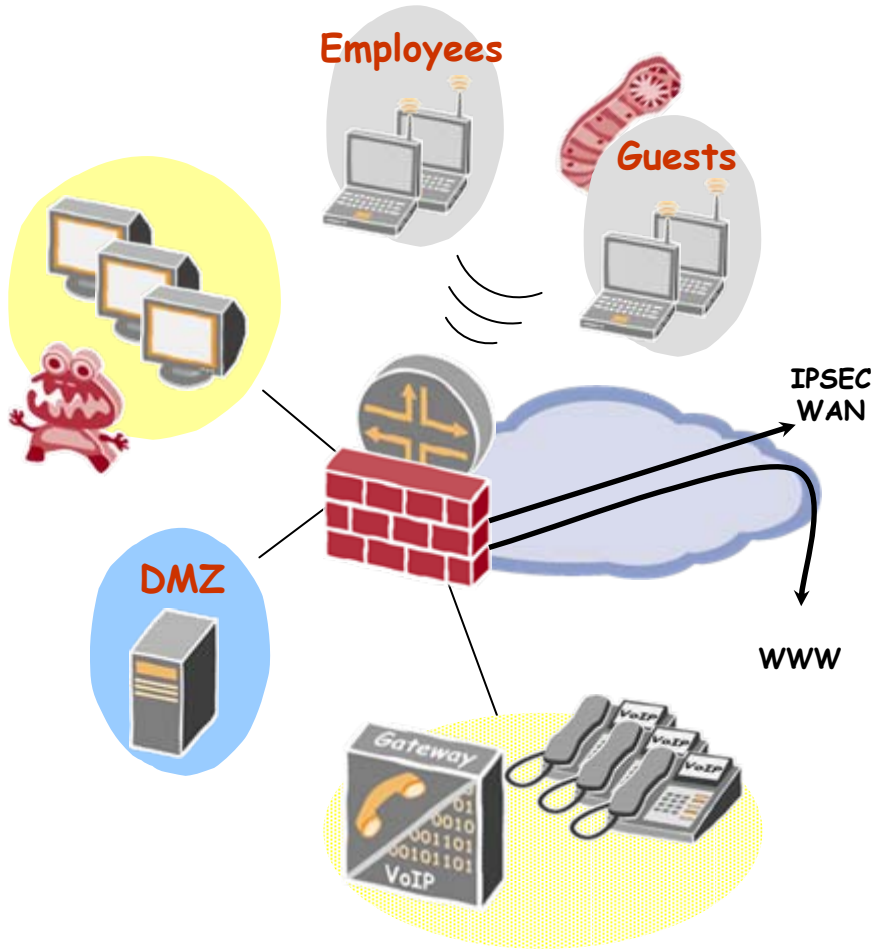
In
(Intra-Site)

Regional/Branch Office in Transitions



- By 2007, 50% of the companies surveyed will significantly increase their WAN access bandwidth - Infonetics
- In 2005, 56% of companies had at least 1 internal attack
 - 65% had at least 1 external attack - CSI/FBI 2005 survey
- By 2009, over 50% of enterprise locations will be on the Internet (5% today) - Gartner Strategic Planning Assumption
- Increased migration towards the branch/remote offices (from ~85% of employees in the branch in 2003 to 91% today) - Nemertes Research

Secure Branch Office Challenges



- First line of defense against threats (yet often the weakest link)
- Performance for securing between internal zones
- Support local Internet access
- Secure internal access to local resources by user and groups, e.g. employees vs. guest access
- Too many devices leads to high capital and operations costs
- Remote management (Limited or no IT support at branch location)

Evolution of Security Upwards & Outwards

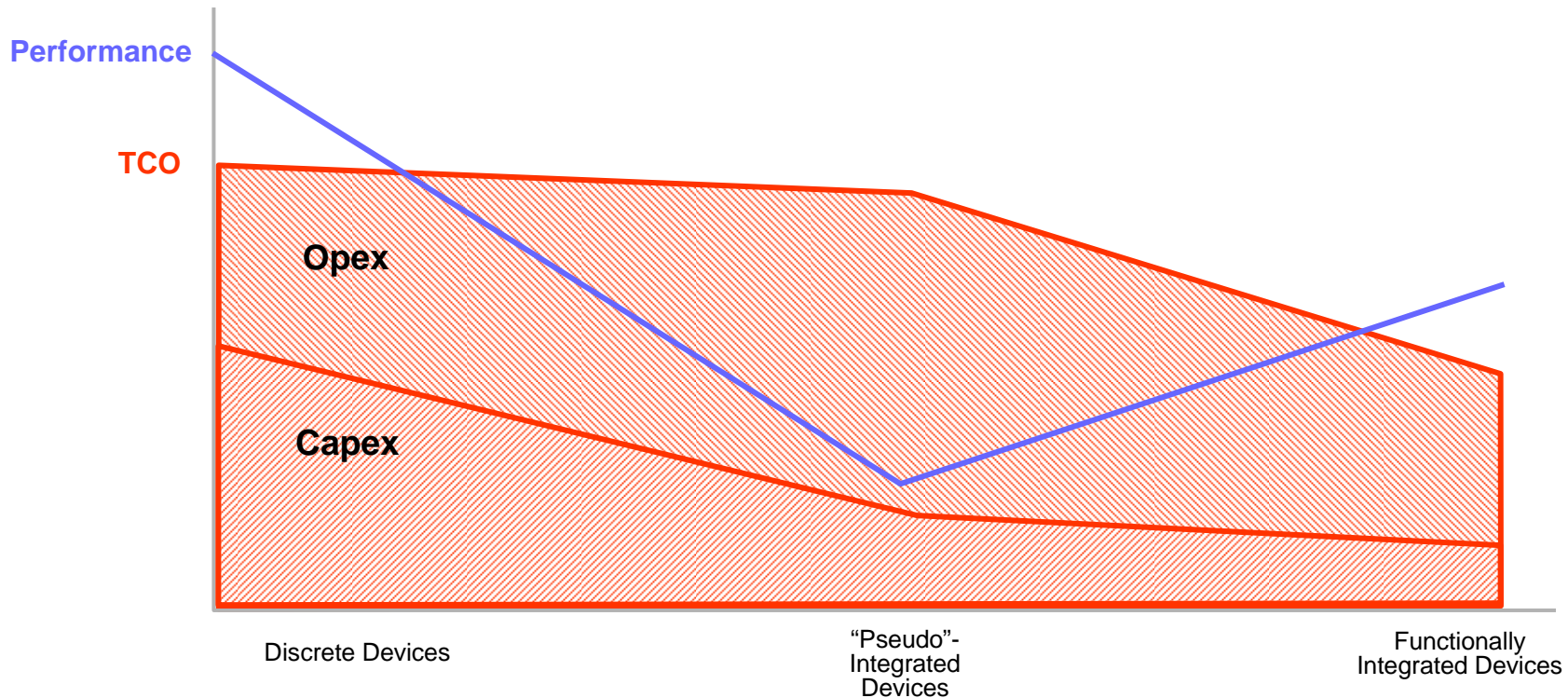
- Degree of Integration?



SPAM	AV	URL	IPS	FW	VPN	NAC	xDSL	T1	T3	Metro Eth	Eth SW	WiFi
Micro Branch												
Regional / Branch Office												
Medium Enterprise / SME												



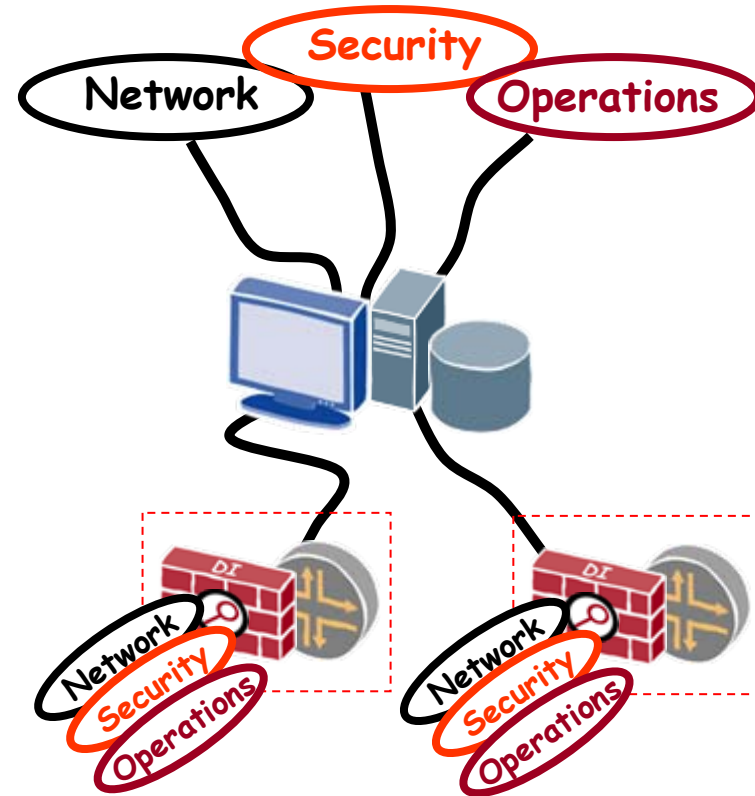
Integrated Devices to meet business need



- Pseudo integrated devices
 - Sheet metal integration, lightweight &/or mutually exclusive functionality, unacceptable multi-function performance
- Functionally integrated devices
 - Integrated management, heavyweight functionality, moderate multi-function performance impact

Secure, Centralized Management

- Remote Management
 - Secure remote management of firewall, VPN, content security, & routing across all devices from one location
- Role-based administration
 - Delegate administrative access to key support people with Assign specific tasks to specific individuals
- Centralized activation/deactivation of security features
 - Application attack protection, Web usage control, Payload attack protection, Spam Control



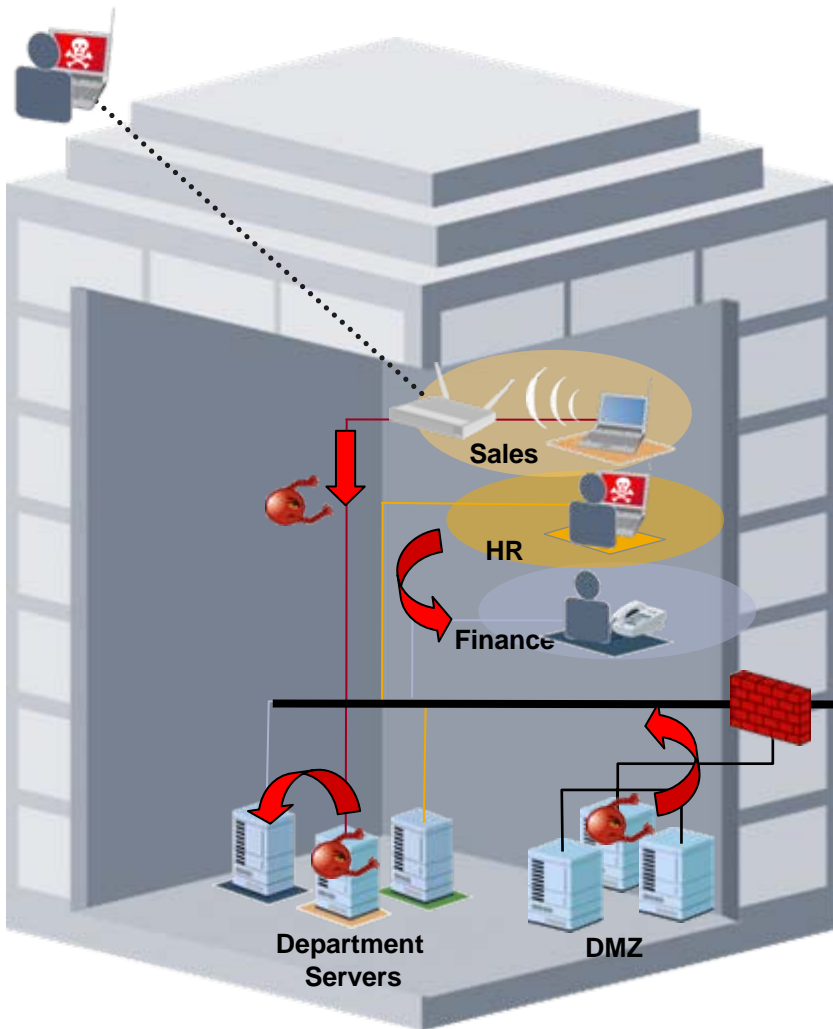
Up
Layers of security

Out
Extended Enterprise / Branch Office

In
(Intra-Site)

Evolution of Security Inward

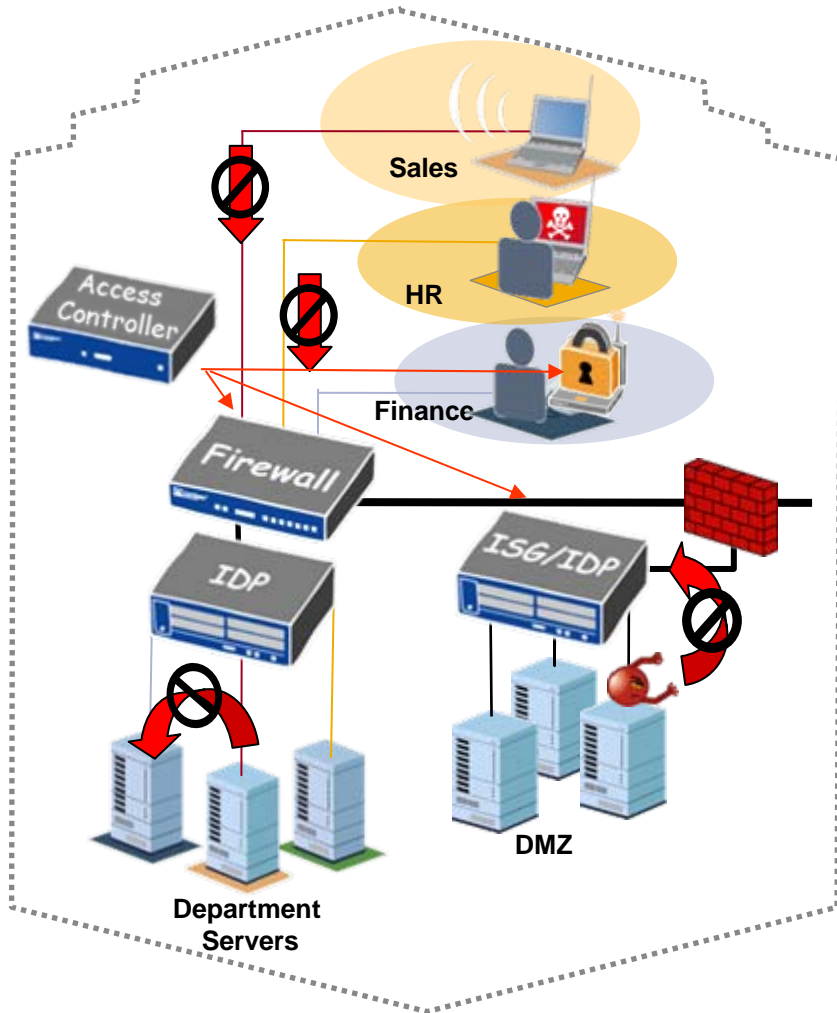
- Controlling the Infrastructure LAN



- Infrastructure LAN Issues
 - Varying levels of trust behind traditional firewalls
 - Mixing of customer data & customer & extended workforce / partner access
 - Increased security regulation & liability
 - High level of hybrid attacks

Evolution of Security Inward

- Controlling the Infrastructure LAN



■ Solutions

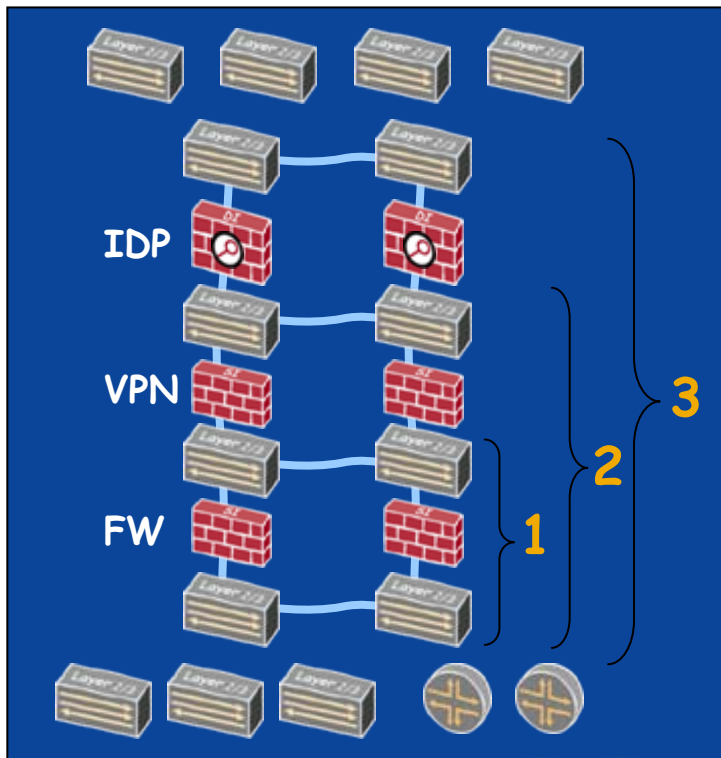
- Device Consolidation
- User Segmentation
- Intrusion Prevention
- Access Control

■ Requirements

- Virtualization
- Performance = LAN Speeds
- High Availability
- Accuracy
- Manageability

Evolution of Security Upwards & Inwards

- Degree of Integration?



- Degree of Integration will be less due to elevated performance requirements for the
HQ Perimeter
Internal LAN
Data Center

- However opportunities exist to combine functions: -

- 1 Additional Ethernet Ports
- 2 FW + VPN
- 3 FW + VPN + IDP
etc

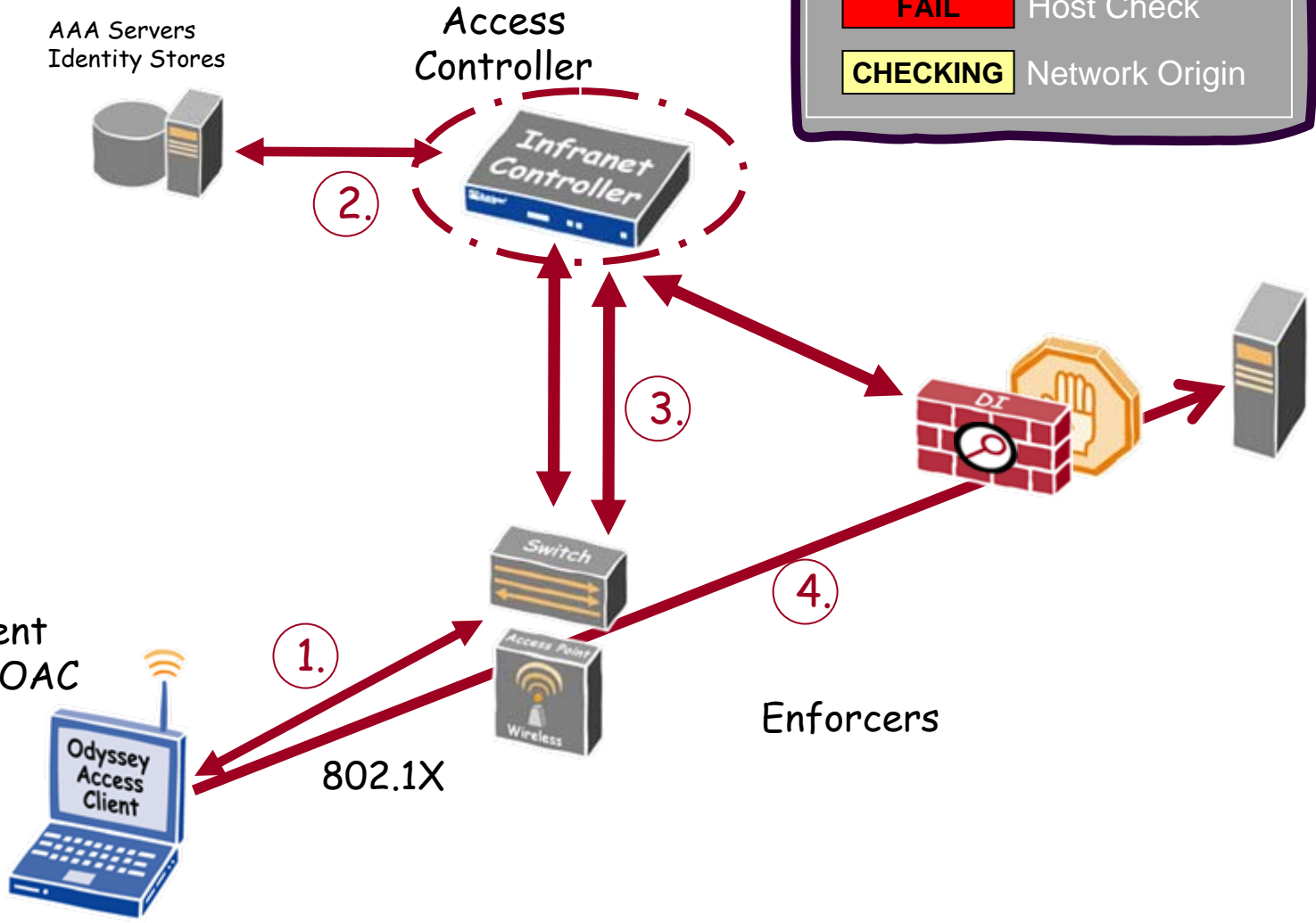


The future of Access Control

Layer 2 + Layer 3

Endpoint Enforcement

- PASS** Authentication
- FAIL** Host Check
- CHECKING** Network Origin



Summary of Firewall Evolution

- Security is an integral infrastructure component
 - Without Security, the network is useless...
- The Firewall & its session awareness is the basis for security integration
 - FW
 - FW + VPN + Routing
 - FW + VPN + Routing + IPS
 - FW + VPN + Routing + IPS + url filtering +
 - Anti-Virus + Anti-Spyware + Anti-Phishing + Anti-Spam....
- All with expanded media coverage
 - WAN Interfaces
 - LAN Interfaces



Q & A



JuniperTM
NETWORKS

