Implementing Layered Security across the Enterprise

Ross Callon
Distinguished Engineer

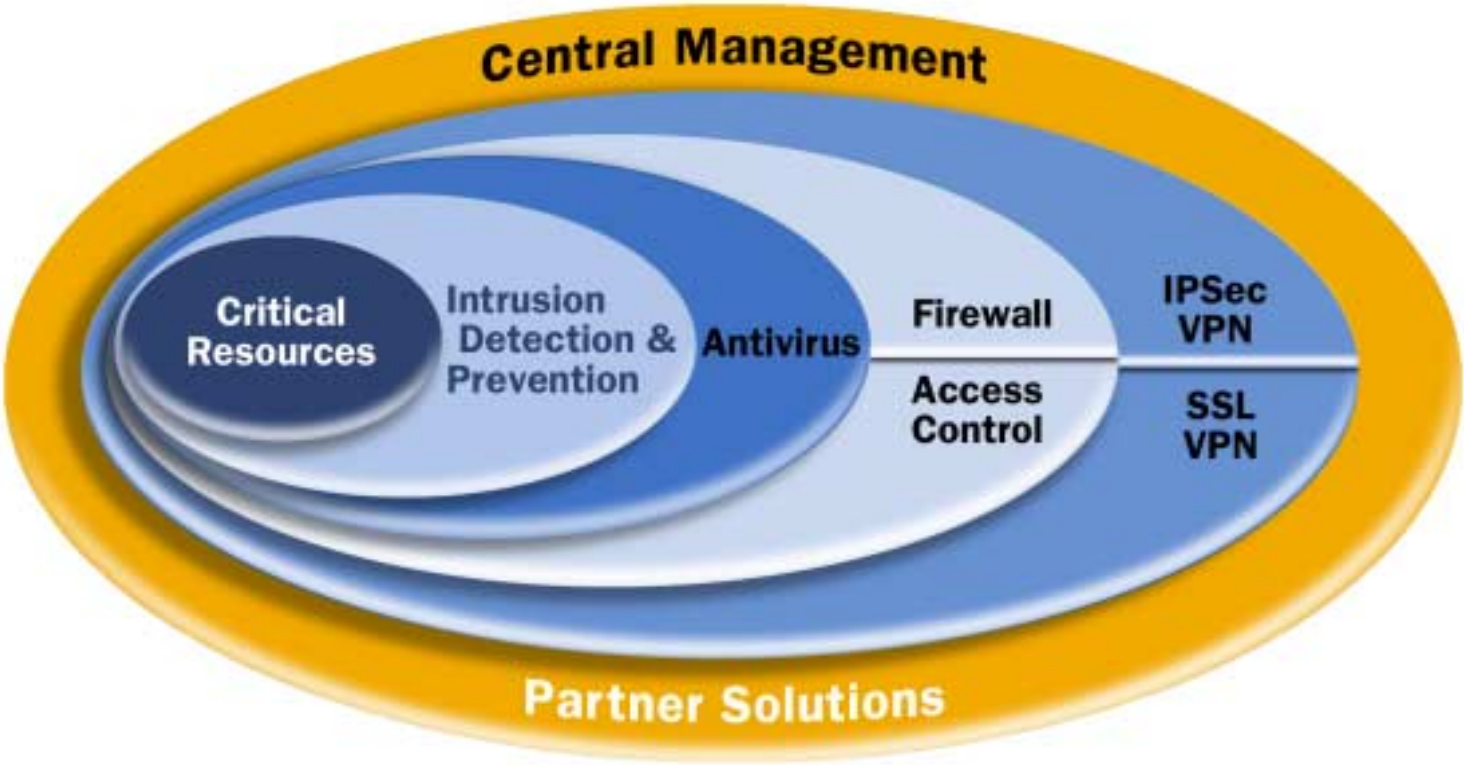
Andy Leung
Regional Security Product Manager

Juniper™ NETWORKS

Agenda

- Trends and Challenges
- Implementation Technologies
  - Overview of Router Security
  - Firewall
  - IDP
  - VPN
  - Remote Access
- Other considerations
- Managed services
- Summary

Layered Security Solutions



"Security professionals agree that network security requires a multi-layered defense. To meet the challenges posed by sophisticated and run-of-the-mill attacks, enterprises have been forced to deploy layers of security products."

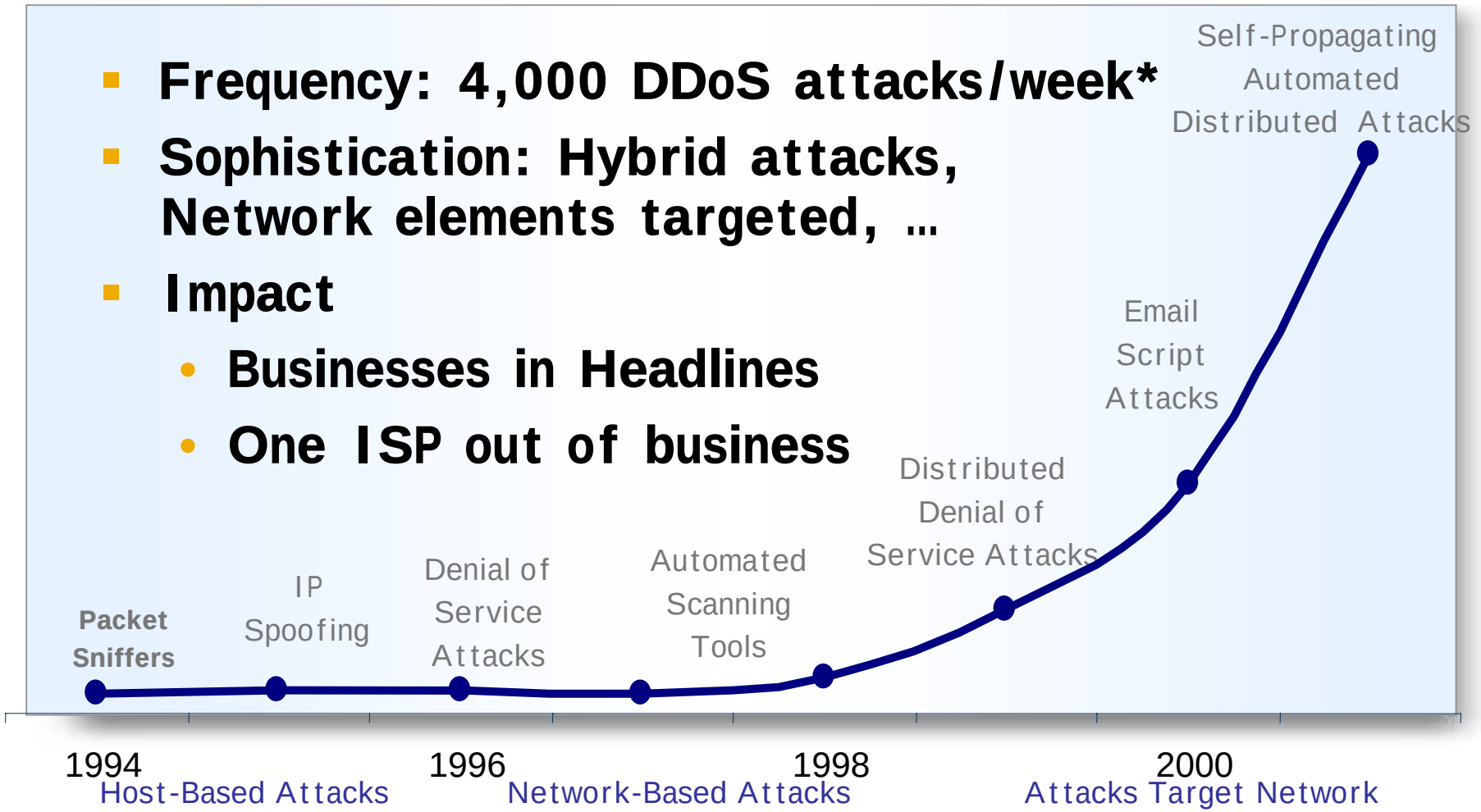
International Data Corp.

Implementation questions

- Are my routers stable and secure during an attack?
- When do you propose a new firewall?
- When do you propose an IDP?
- What VPN technology should you use?
- How to secure remote access?
- What are the security features you should look for?
- Single box or multiple box solution?
- How to implement the managed service?

Cyber Attacks Increasing

- **Frequency: 4,000 DDoS attacks/week***
- **Sophistication: Hybrid attacks, Network elements targeted, …**
- **Impact**
  - **Businesses in Headlines**
  - **One ISP out of business**



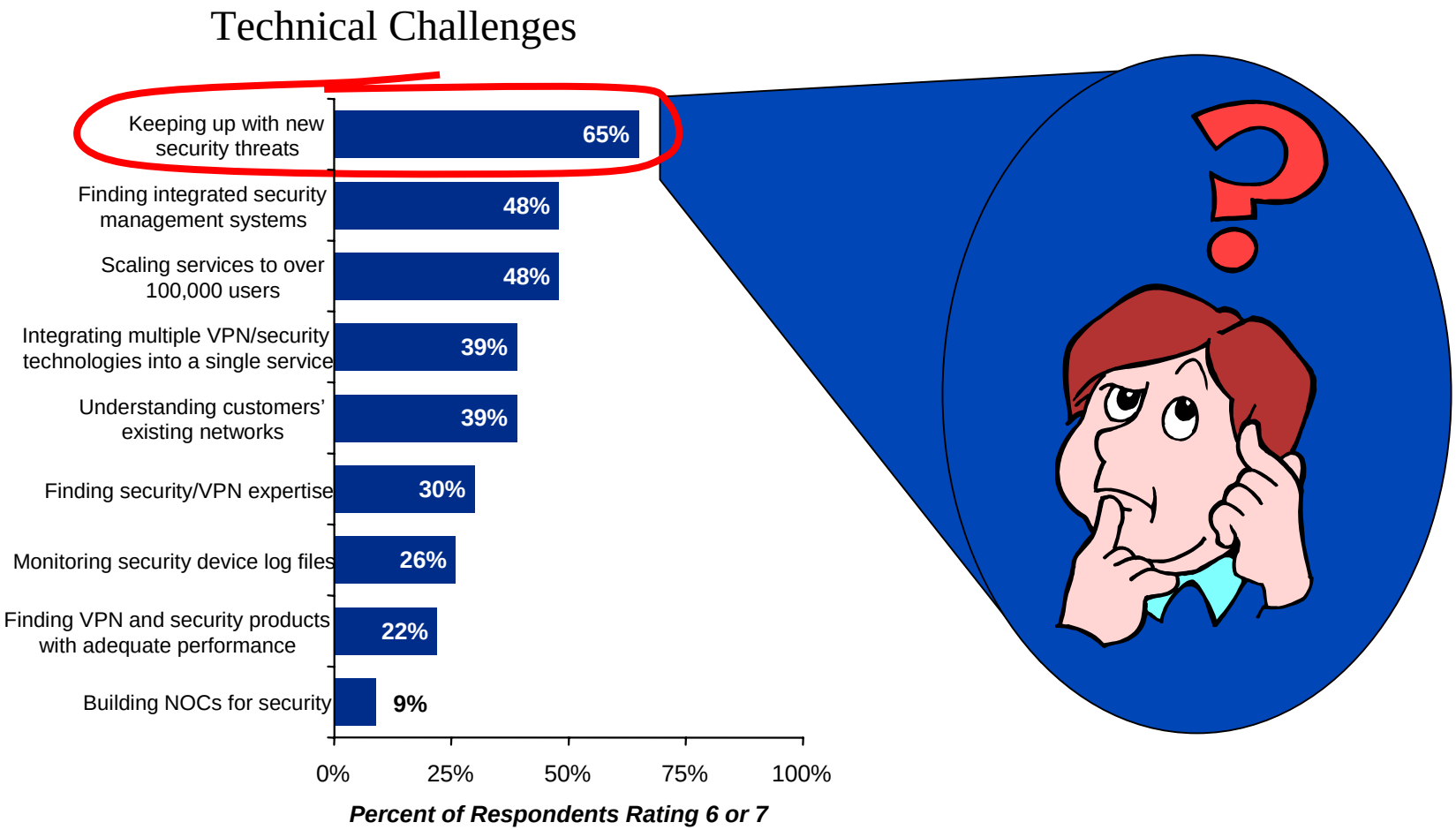
Source: Published CERT figures

* http://www.caida.org/outreach/papers/2001/BackScatter/

Consequences of Slammer

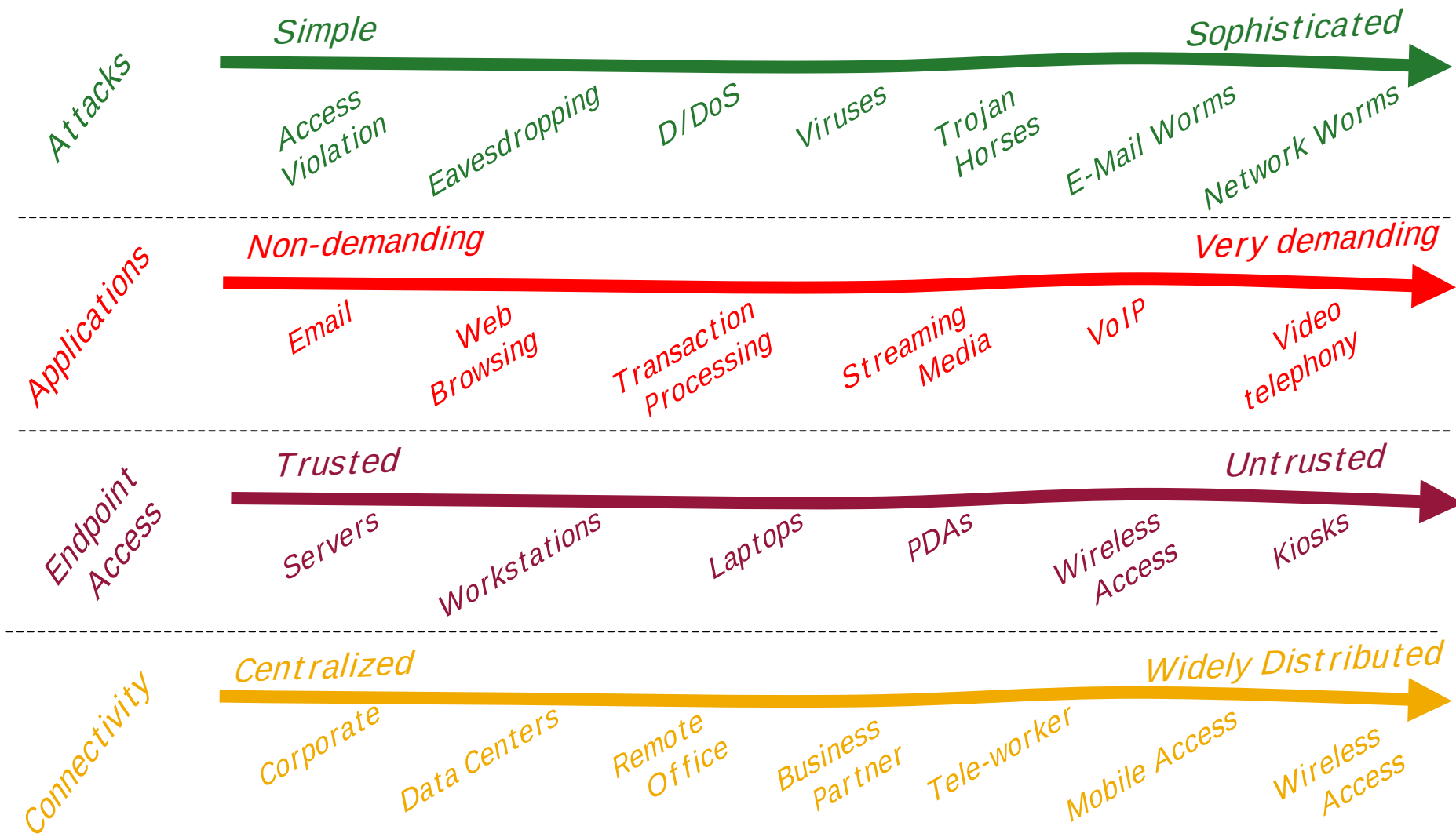
- Global loss of 20% of all Internet traffic
- Loss of emergency services in Washington
- No mobile network for 27m South Koreans
- Shutdown of 13,000 cash machines
- Flights delayed
- Cleanup costs of more than $1bn
- Spread in just 10 minutes
- One major service provider was unaffected!

Top Technical Challenge for Service Providers

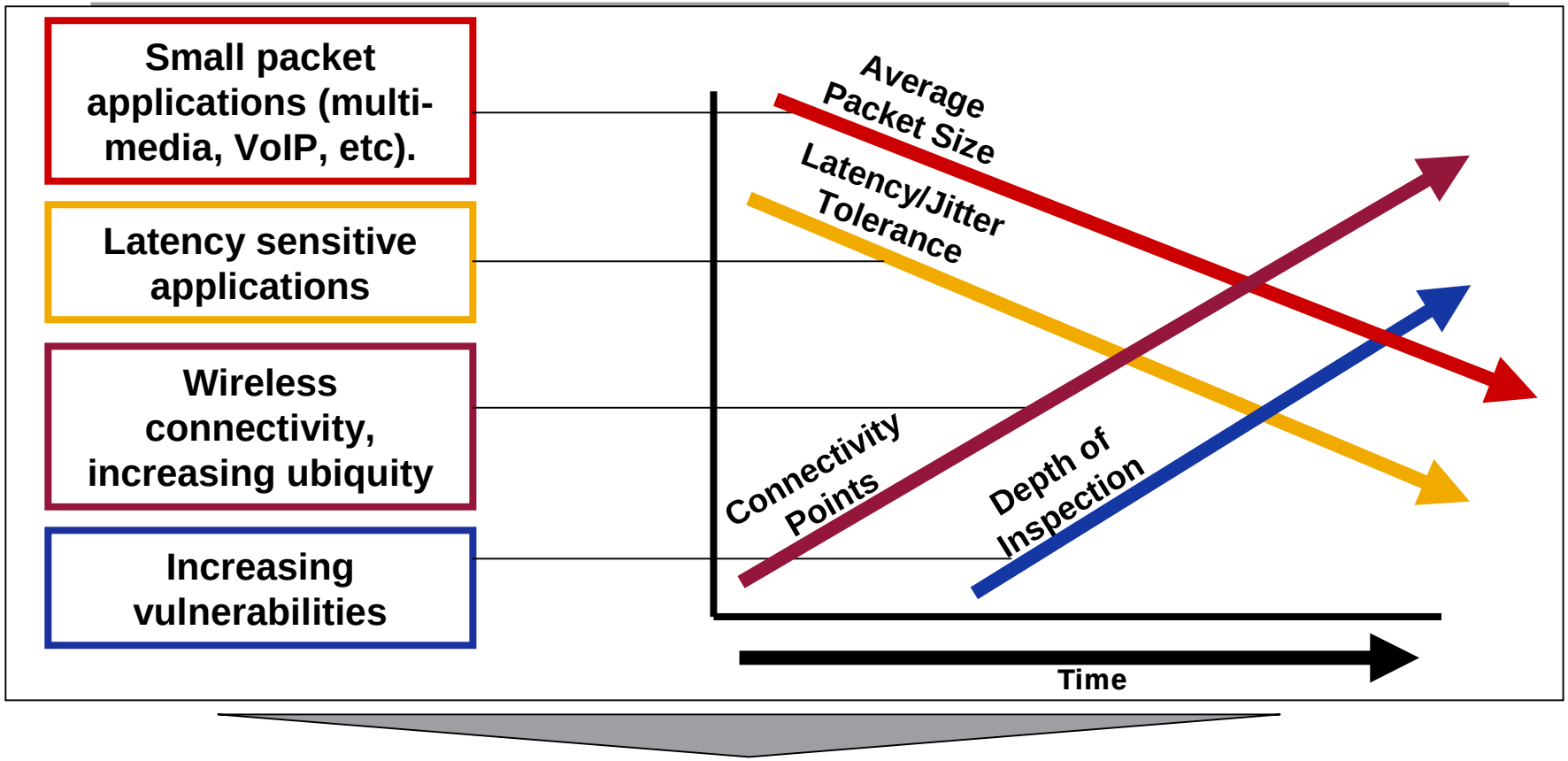


Source Infonetics: Service Provider Plans for VPNs and Security NA, EUR, APAC 2004

Why - Networking is Evolving



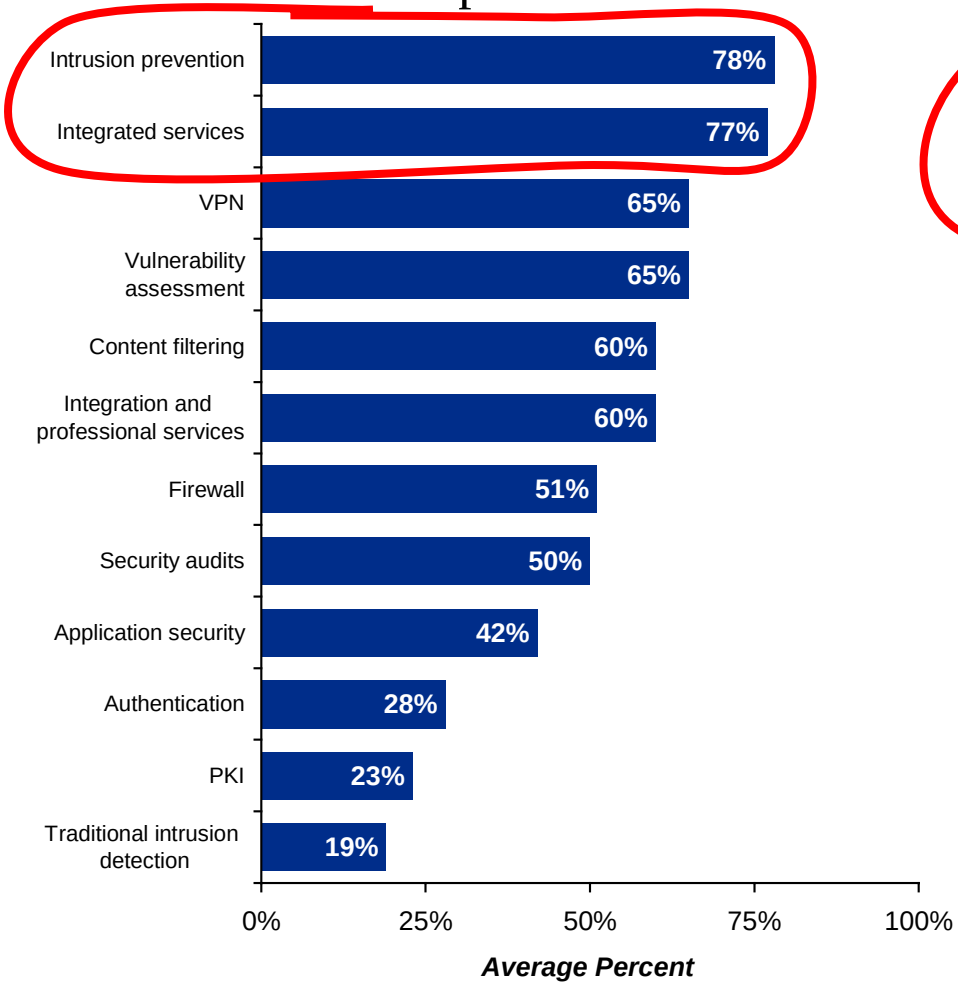
Trends Affecting Solution Requirements



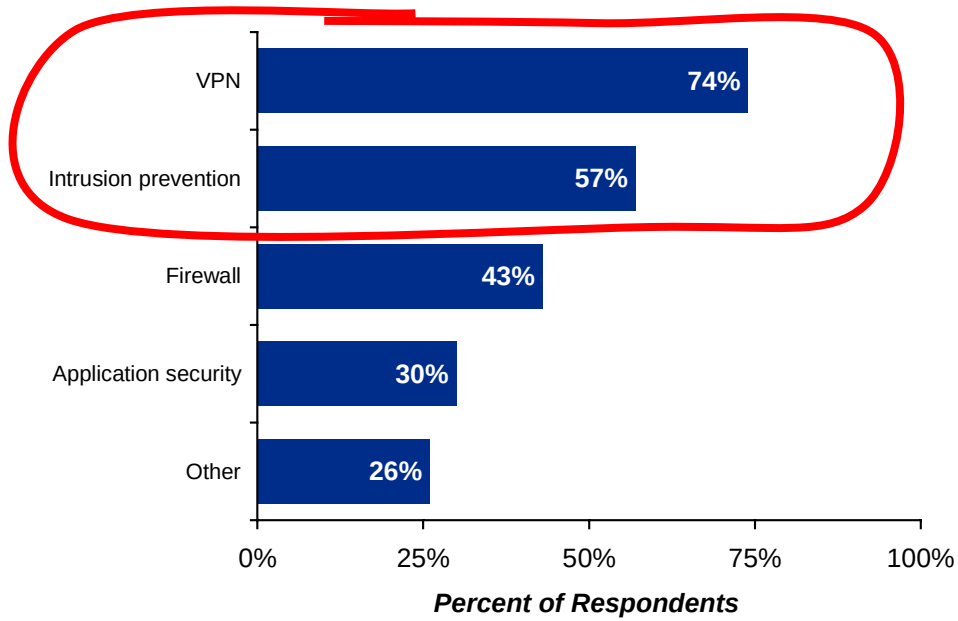
- Provide linear performance for large and small packet traffic mix
- Make traffic decisions with low latency so applications are not affected
- Increasing traffic load and number of connection points
- Prevent/mitigate network and application-level attacks

Security Services Growth & Investment

Services Expected to Grow

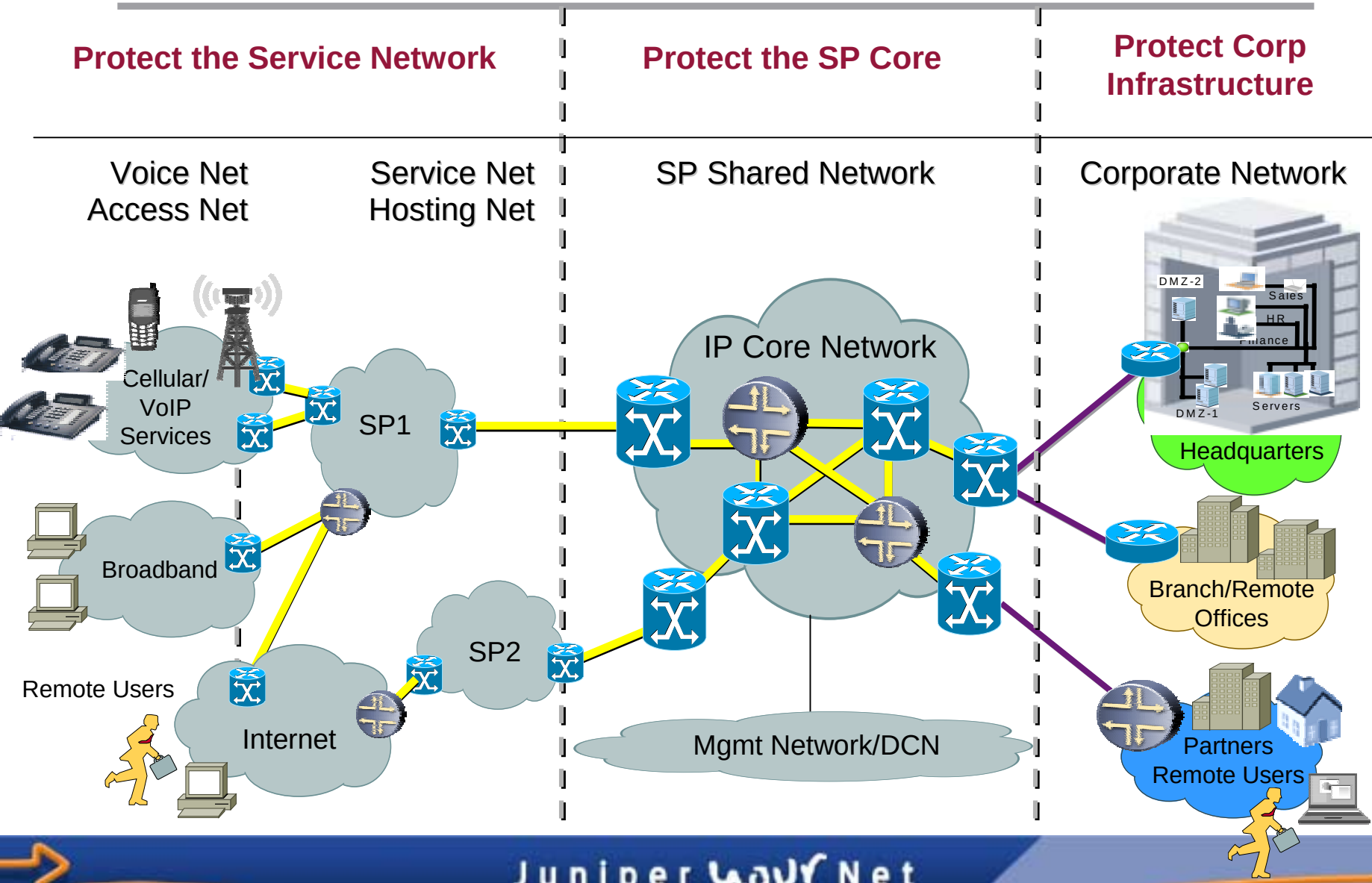


Security Technologies for Investment



Source Infonetics: Service Provider Plans for VPNs and Security NA, EUR, APAC 2004

Security Across the Network



Security Across the SP Network

Protect the Service Network

- Protect GPRS Network
- Protect VoIP Network
- Protect Broadband Network
- Protect Service Portal

Protect the SP Core

- Protect Control Plane
- Protect DCN
- VPN Services

Protect Corp Infrastructure

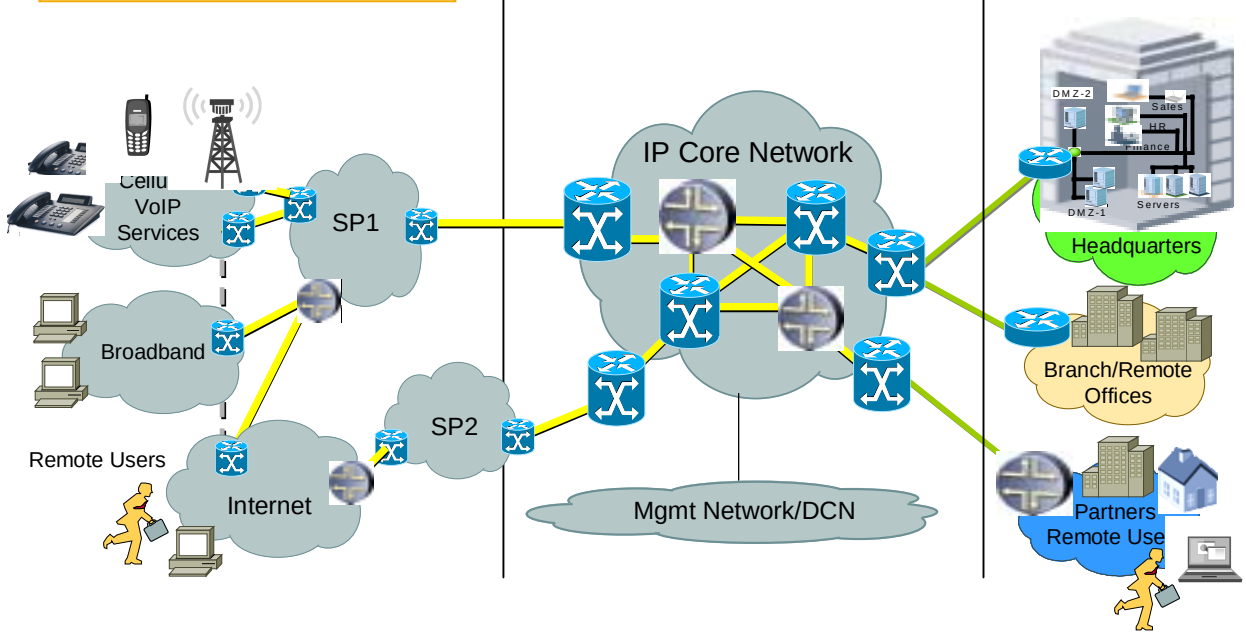
- Secure online meetings
- Remote secure access
- Protect Perimeter

Managed Secure Service

Secure BB, VoIP, etc.

Managed Security Service

FW, IPS, VPN, etc.



- Multiple virtual FWs on single platform
- Detect, suppress and prevent attacks
- Integrated security protects remote edge
- FW & IPSEC VPN WAN over Internet
- Secure access for mobile user, biz partner

Implementation Technologies

Securing the Router Infrastructure

- Links, routers, routing protocols, and management thereof
  - Are critical network components
  - Must work securely
- These can be strongly secured
  - Very few systems have a valid reason to send traffic *to* the router's control plane

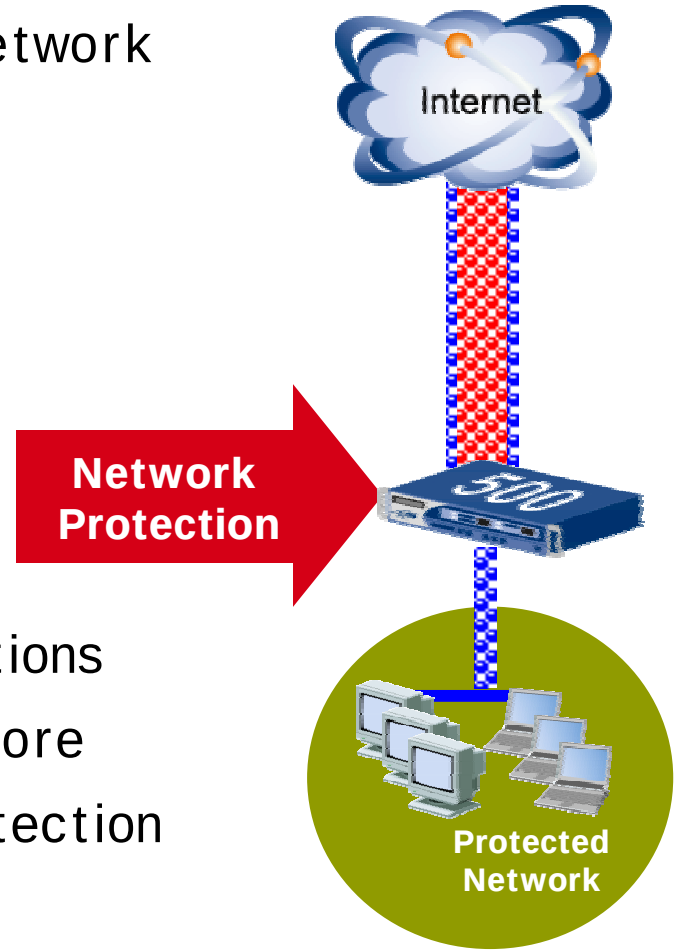
    (rather than *via* the router's data plane)

Basic Router Security

- Security with performance
  - Line rate packet filtering, rate limiting
  - Stability under stress (eg, routers need to prioritize control traffic)
- Limit who can send traffic to routers
- Secure network management
  - One-time passwords, authenticate access,…
- Secure routing protocols
- More details on Thursday

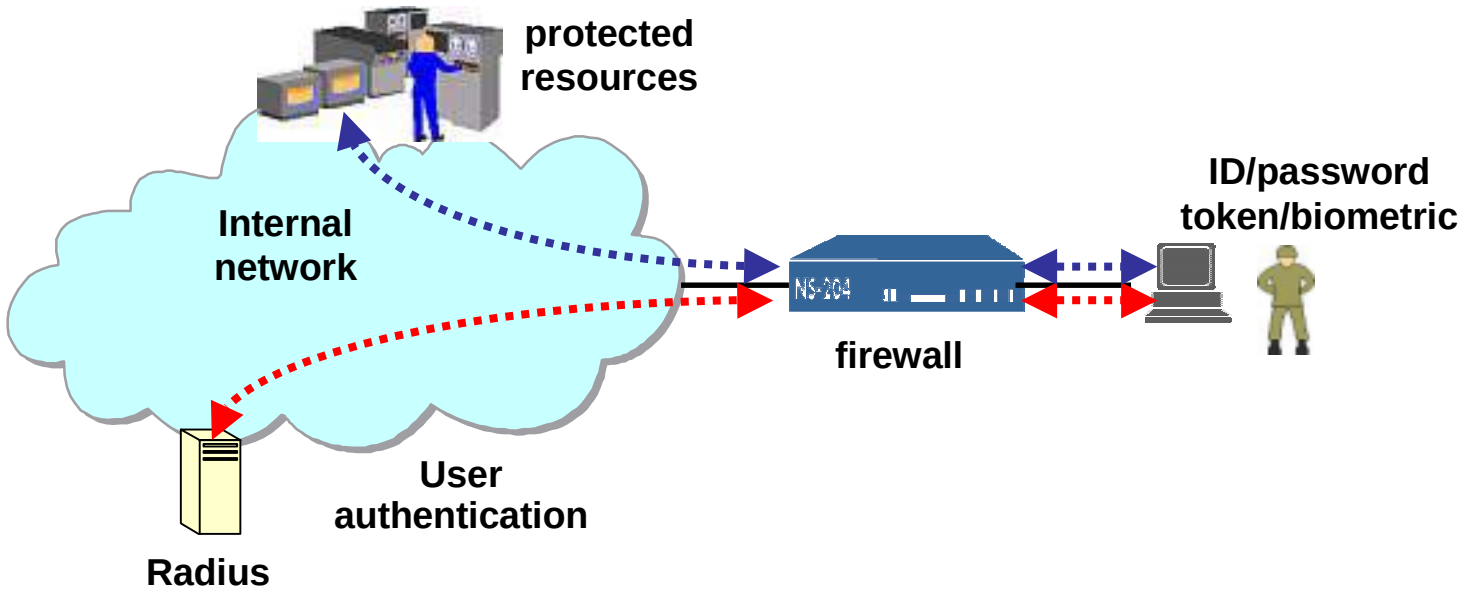
Firewalls: Access Control

- What it does:
  - Controls what / who gets in and out of network
  - Protects against common attacks
- How it works:
  - Scans for standard services
    - Ability to create custom services
  - Performs user authentication
- Where it's deployed:
  - An initial layer of defense for most locations
    - Remote, site to site, perimeter, and core
    - Commonly used for LAN segment protection



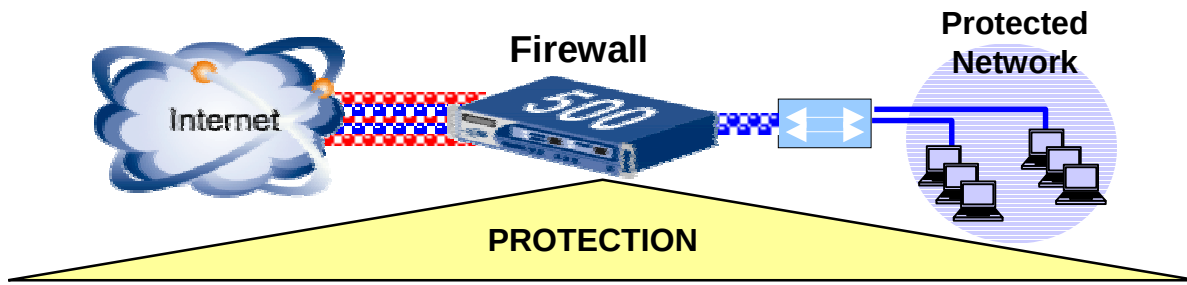
Firewalls: User Authentication

- Control who gets in and out of network
  - Verifies sender is who they claim to be
  - Support for tokens, digital certificates, ID/password
  - Interoperate with RADIUS, LDAP, PKI, internal DB, and SecurID



Firewalls: Denial-of-Service Protection

- Protection against common DoS attacks
- Another layer to prevent network attacks
- Deployed at Remote site, perimeter, core, or LAN



Firewall Protection
- Stateful inspection firewall (i.e., TCP and UDP)
- TCP sequence checking
- MAC address checking
- CRC packet checking

Content Protection
- Java/ActiveX/Zip/Exe blocking
- User-define malicious URLs
- URL blocking (Websense, SurfControl)

Reconnaissance Protection
- Port scan
- IP address sweep

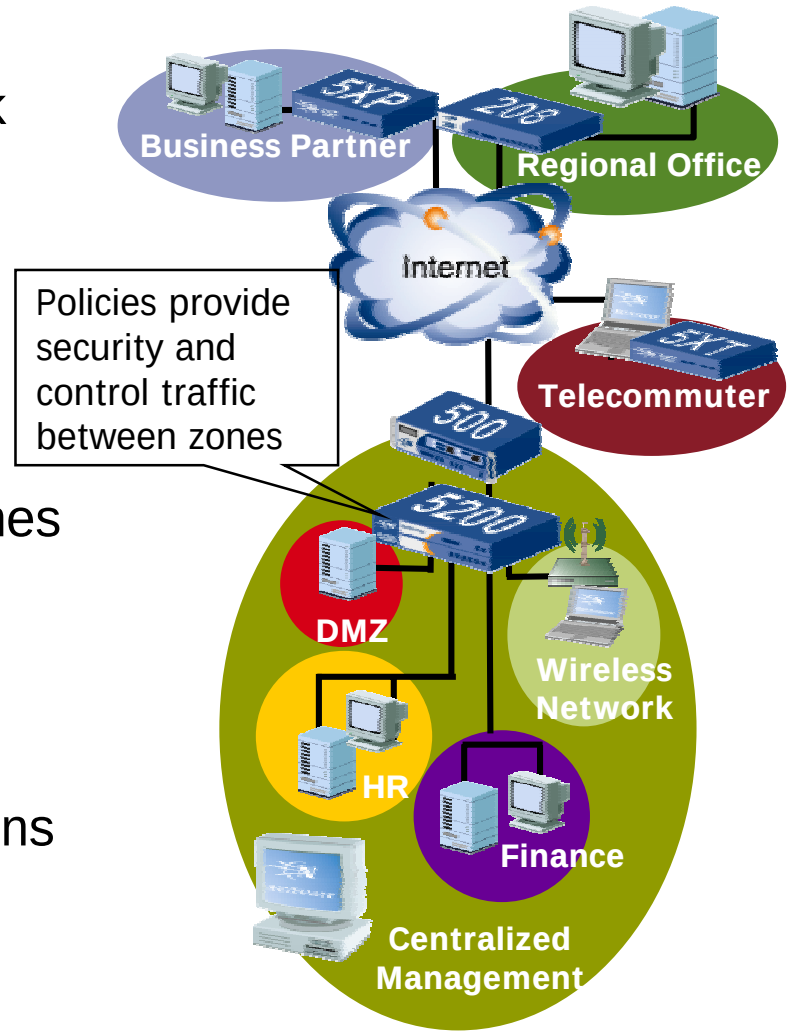
DoS and DDoS Protection
- SYN flood
- ICMP flood
- UDP flood
- IP spoofing
- Per-session limiting
- SYN fragments
- Default packet deny
- SYN-ACK-ACK attack

Malicious Packet Protection
- Ping of death
- Land attack
- Tear drop attack
- WinNuke attack
- IP source route
- Loose source route

Malformed Packet Protection
- SYN and FIN bit set
- No flags in TCP
- FIN with no ACK
- ICMP fragment
- Large ICMP
- IP source route
- IP record route
- IP security options
- IP timestamp
- IP stream
- IP bad options
- Unknown protocols

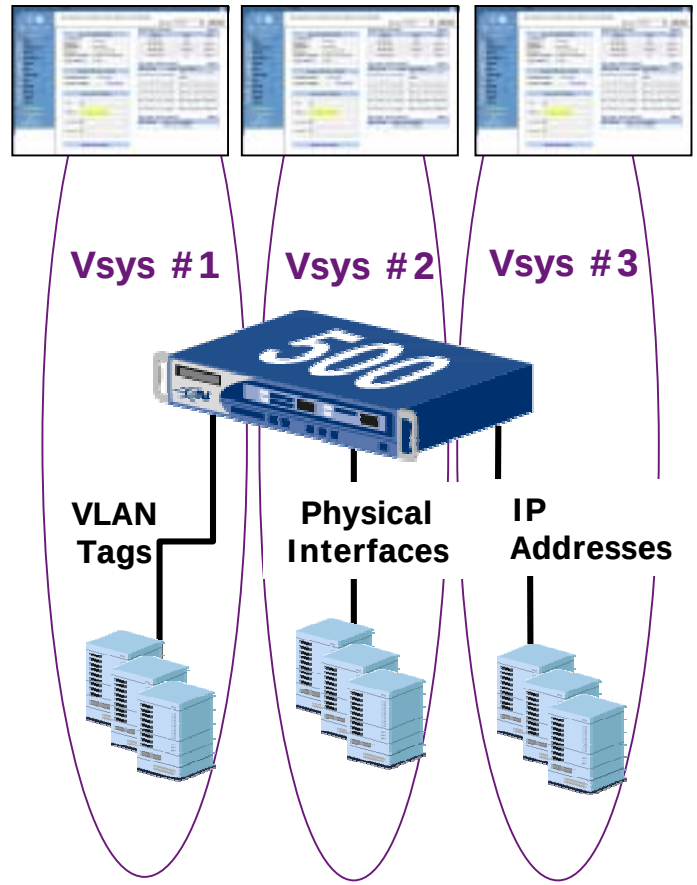
Security Zones: Internal Firewalls

- What it does:
  - Use security zones to divide network into logically managed zones - HR, finance, wireless, etc.
- How it works:
  - Zones no longer bound to physical interfaces
  - Policies applied between security zones and to interfaces within zones
- Where it's deployed:
  - Used in Core/LAN scenarios
  - Segments network into secure domains
  - Protects against internal attacks
  - Distributed security at low cost

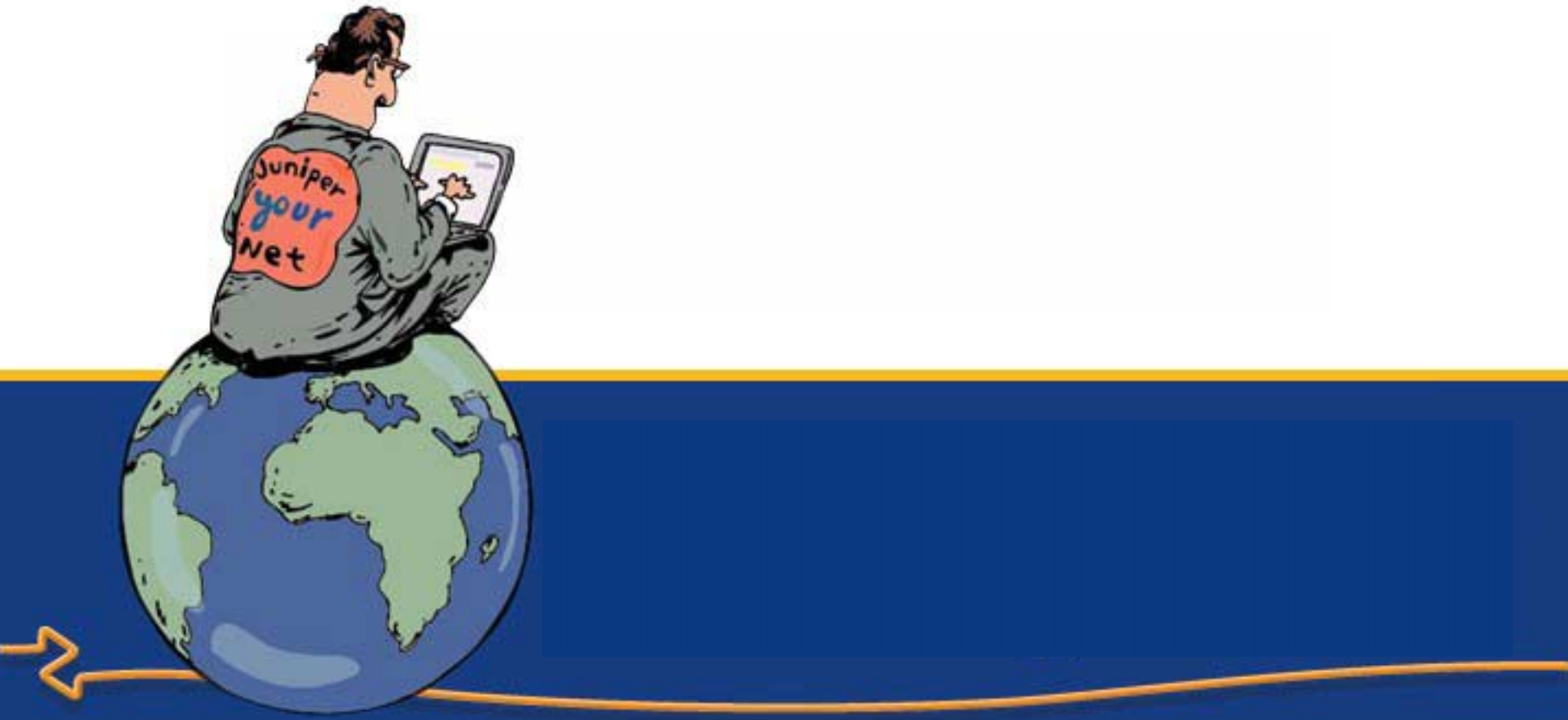


Virtual Systems: Another Security Layer

- What it does:
  - Provides virtual FW/VPN
  - Each with their own address book, policies, and management
  - Separate management facilitates for division of labor
- How it works:
  - Traffic routed to VSYS by IP addr, physical interface, or VLAN
- Where it's deployed:
  - Used in Core/LAN scenarios
  - Augments Security Zones as a means of of segmenting network
  - Used in scenarios where administration must be separate.

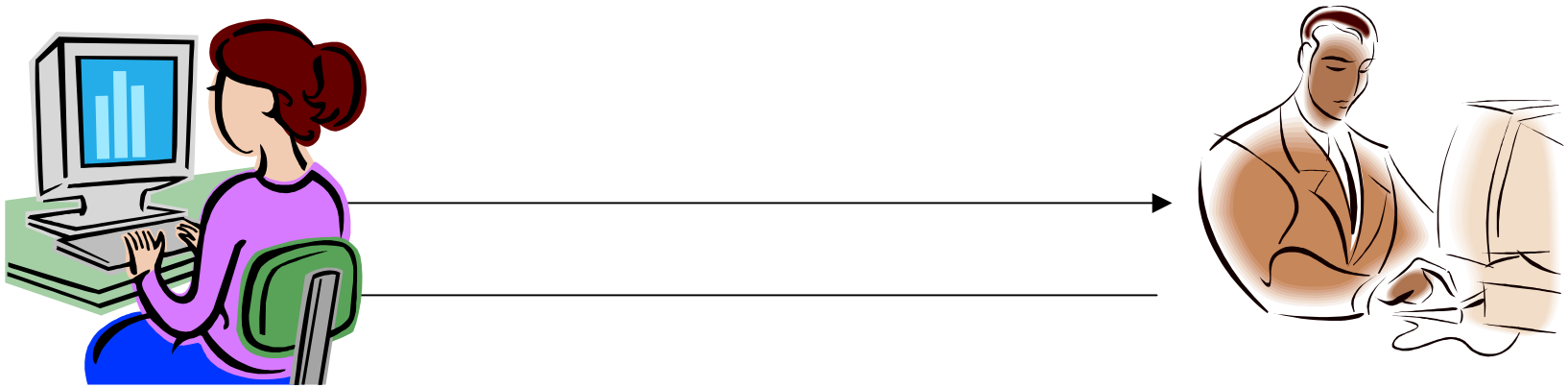


IPsec VPN vs SSL VPN



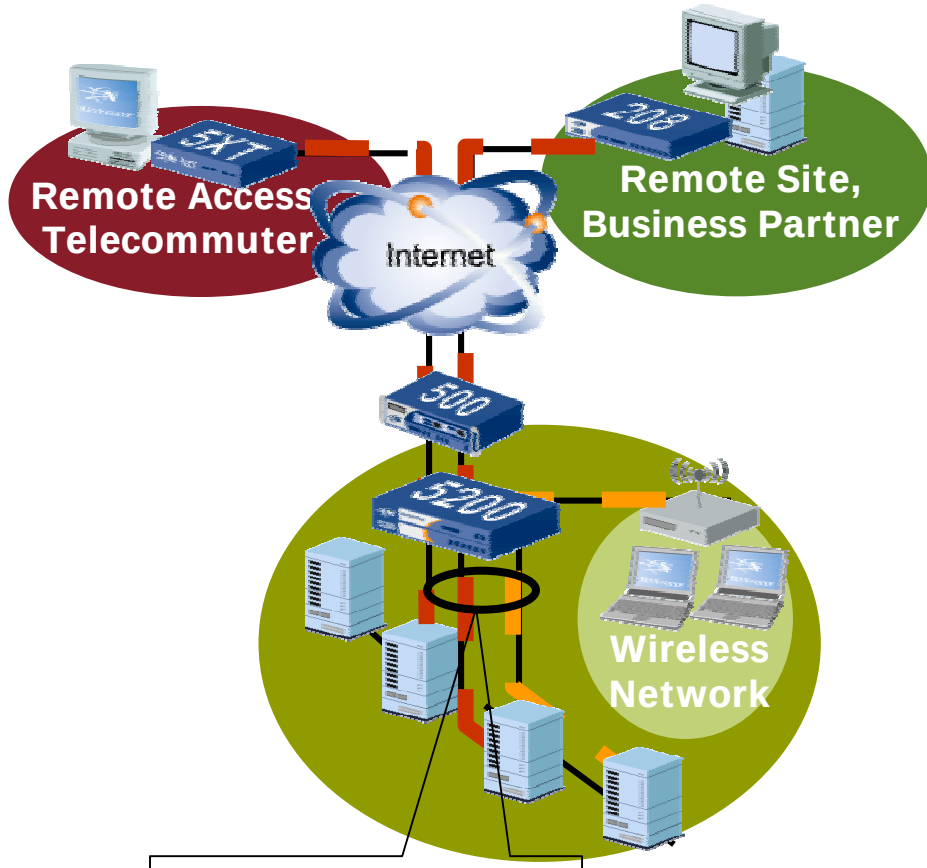
What does VPN do?

- Confidential
- Integrity
- Authentication

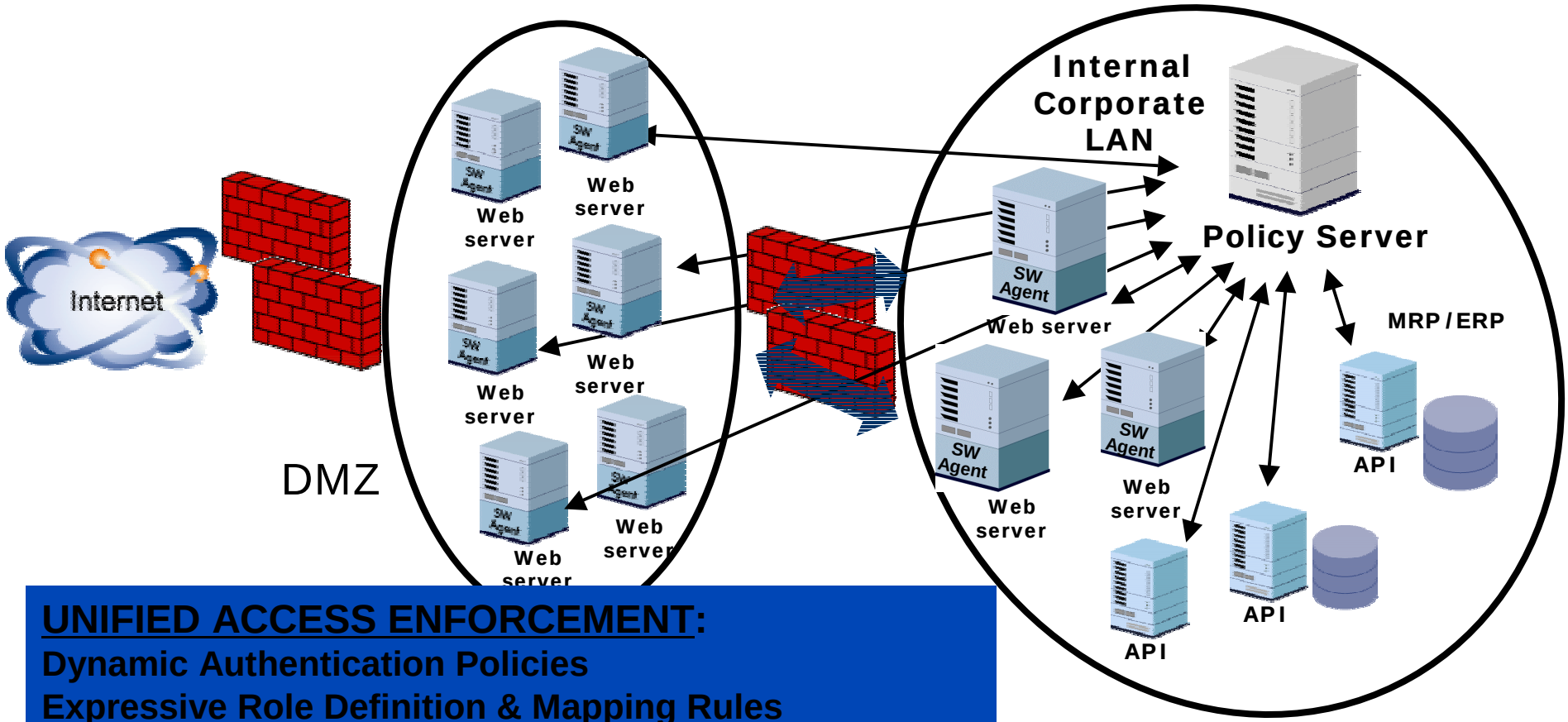


IPsec VPN: Protecting Communications

- What it does:
  - Encrypts and authenticates
- How it works:
  - Establishes secure tunnel between remote site/user
- Where it's deployed:
  - Encryption and non-repudiation are another layer of protection
  - Used for secure communications across the enterprise
  - Remote user, site-to-site, Internal LAN communications



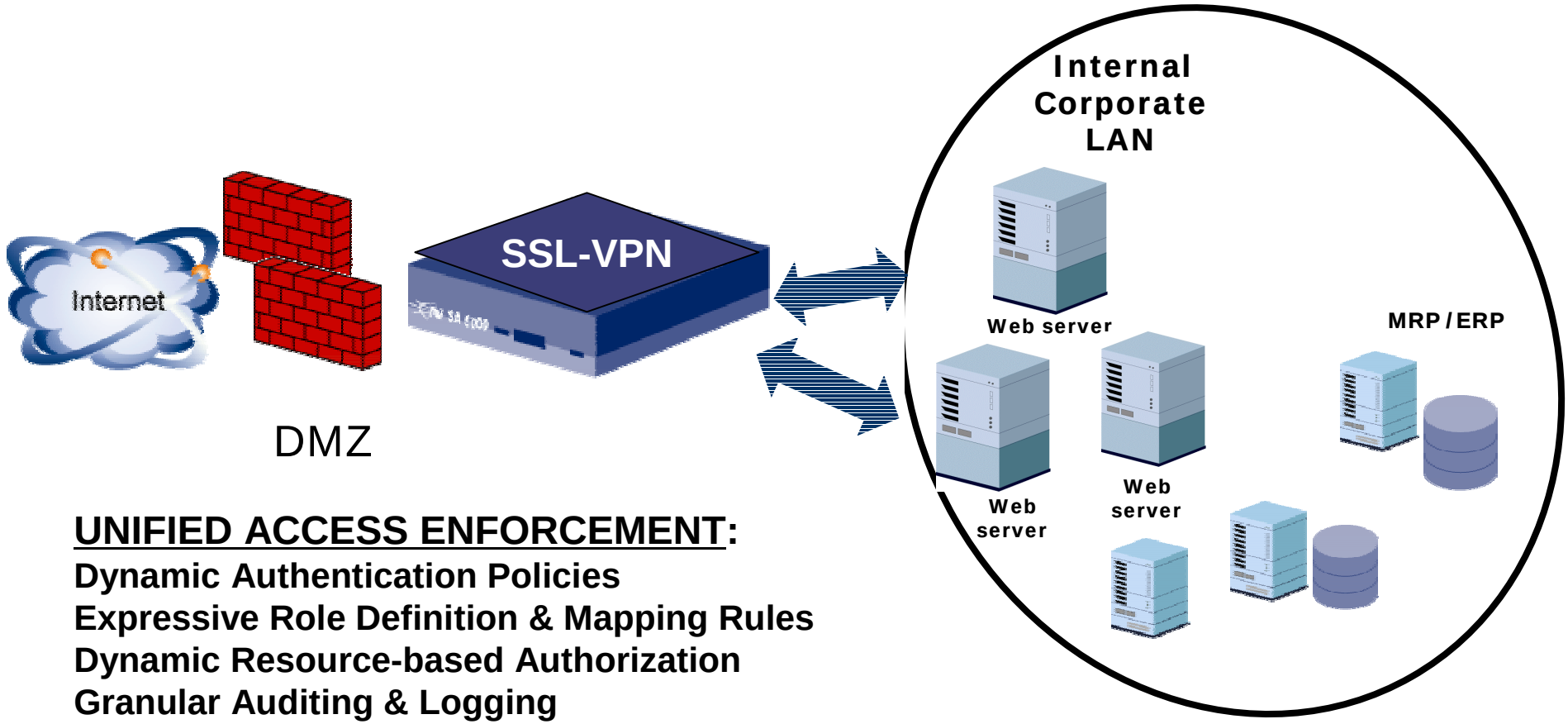
SSL VPN: Secure Remote Access



<u>UNIFIED ACCESS ENFORCEMENT</u>:

Dynamic Authentication Policies
Expressive Role Definition & Mapping Rules
Dynamic Resource-based Authorization
Granular Auditing & Logging
Web Single Sign-On (SSO)
Password Management Integration
Multiple Hostnames & Customizable UI
Endpoint Policy Enforcement

SSL VPN: Secure Remote Access

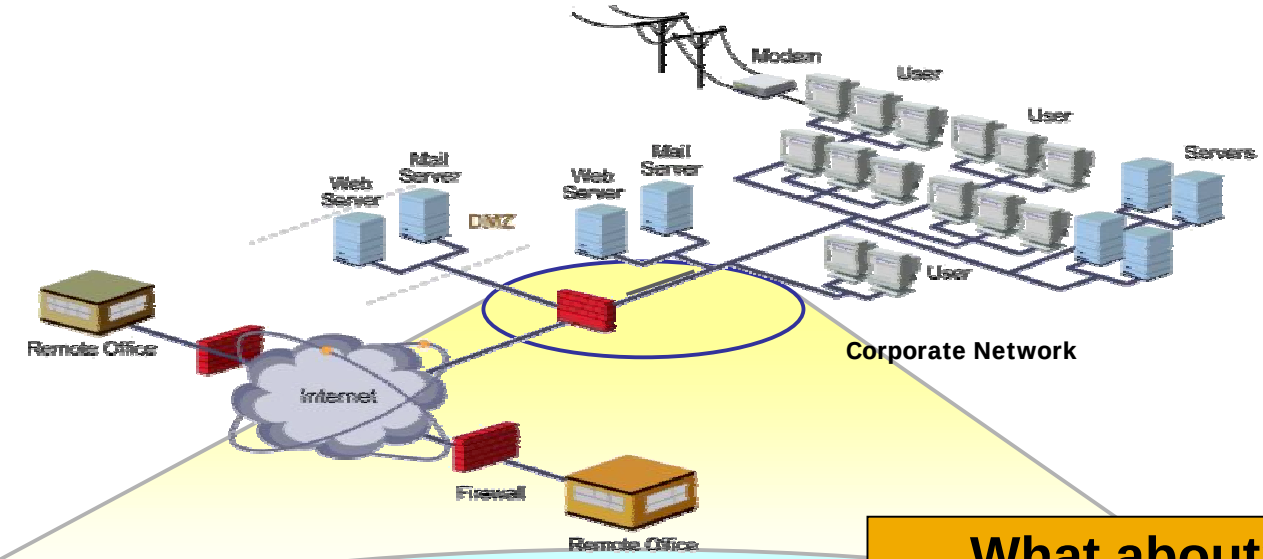


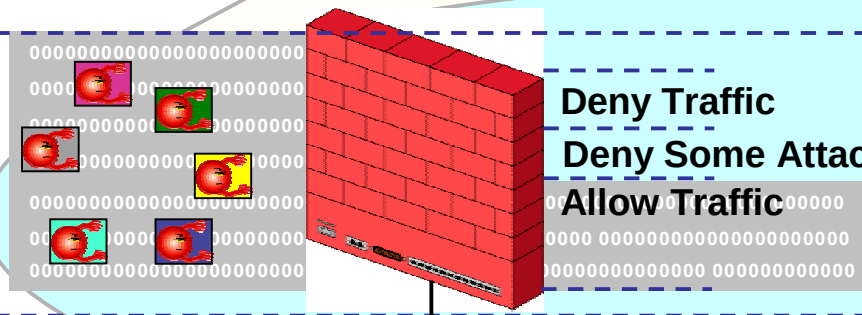
UNIFIED ACCESS ENFORCEMENT:

Dynamic Authentication Policies
Expressive Role Definition & Mapping Rules
Dynamic Resource-based Authorization
Granular Auditing & Logging
Web Single Sign-On (SSO)
Password Management Integration
Multiple Hostnames & Customizable UI
Endpoint Policy Enforcement

Intrusion Prevention System

Firewalls are *only* 1st layer of defense





Deny Traffic

Deny Some Attacks

Allow Traffic

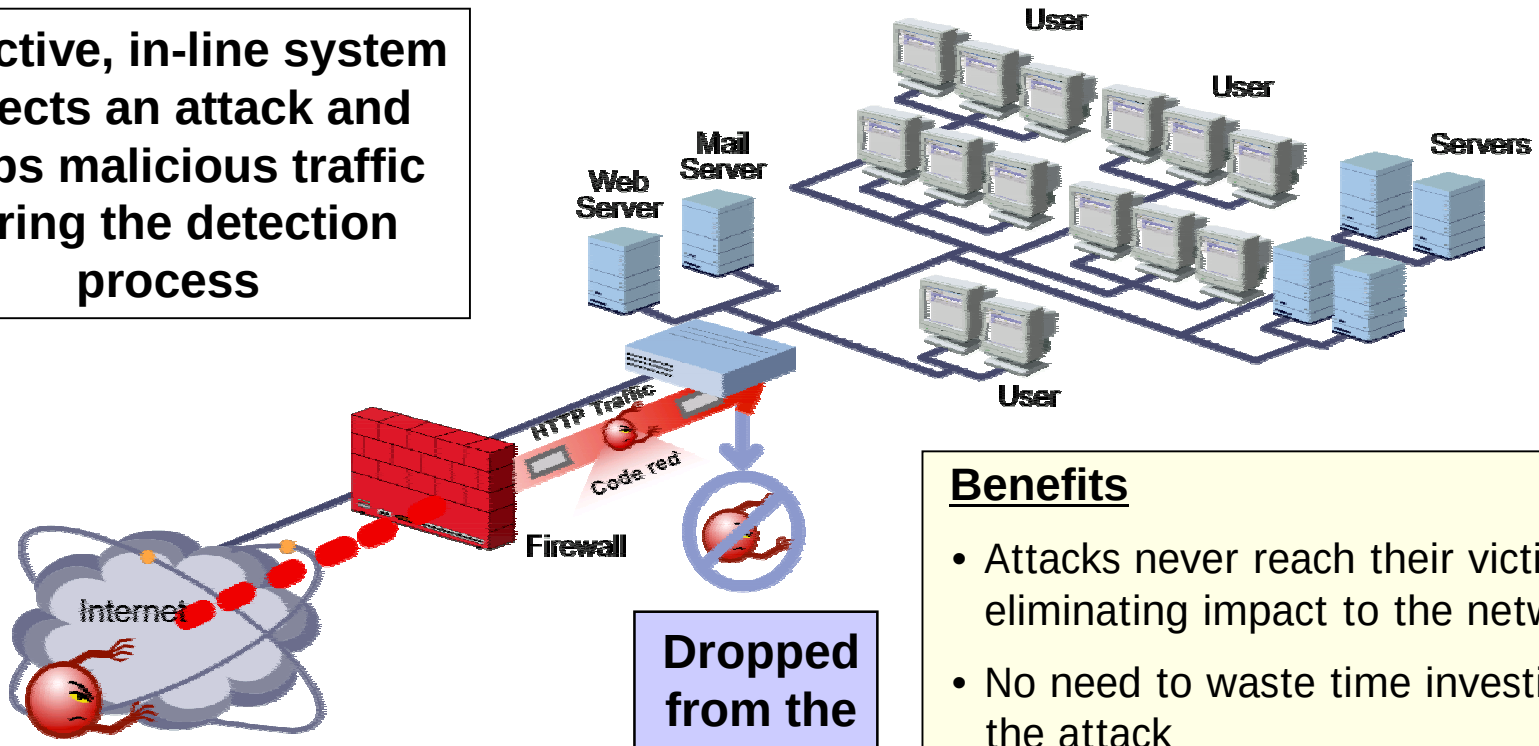
What about??

- **P2P traffics e.g. BT, WinMX, Kazaa …. etc**
- **IM traffics e.g. Yahoo! Messenger, MSN, ICQ**
- **Real time application: VoIP, H.323, SIP, Streaming video**

Firewall provides access control

In-Line Attack Prevention

An active, in-line system detects an attack and drops malicious traffic during the detection process

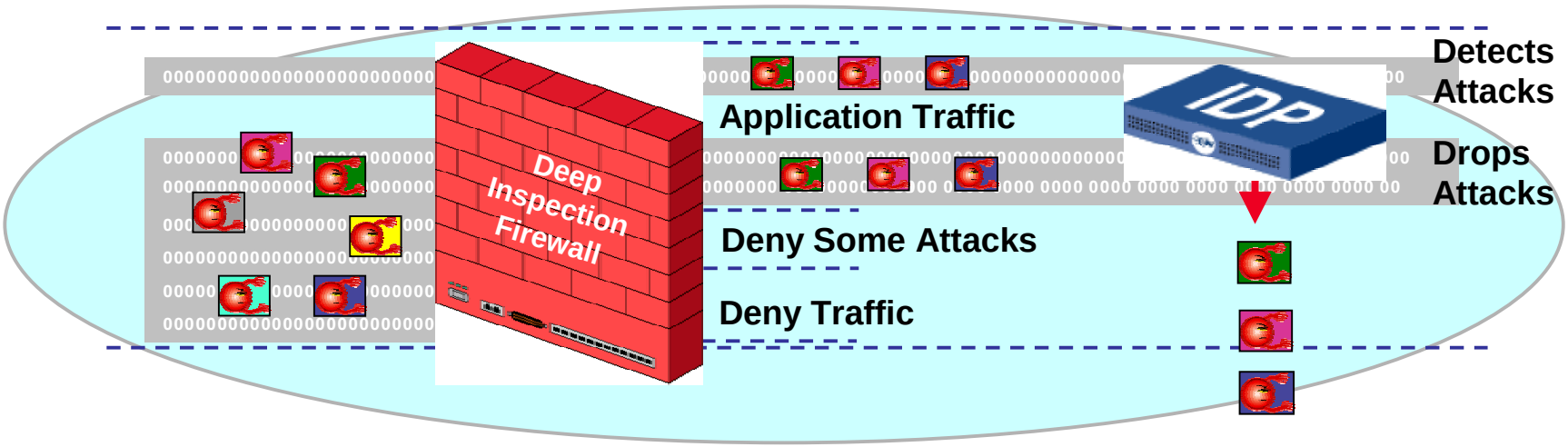


Dropped from the network

Benefits

- Attacks never reach their victim, eliminating impact to the network
- No need to waste time investigating the attack
- Works for all traffic (IP, TCP, UDP, etc.)
- Drops only the offending traffic

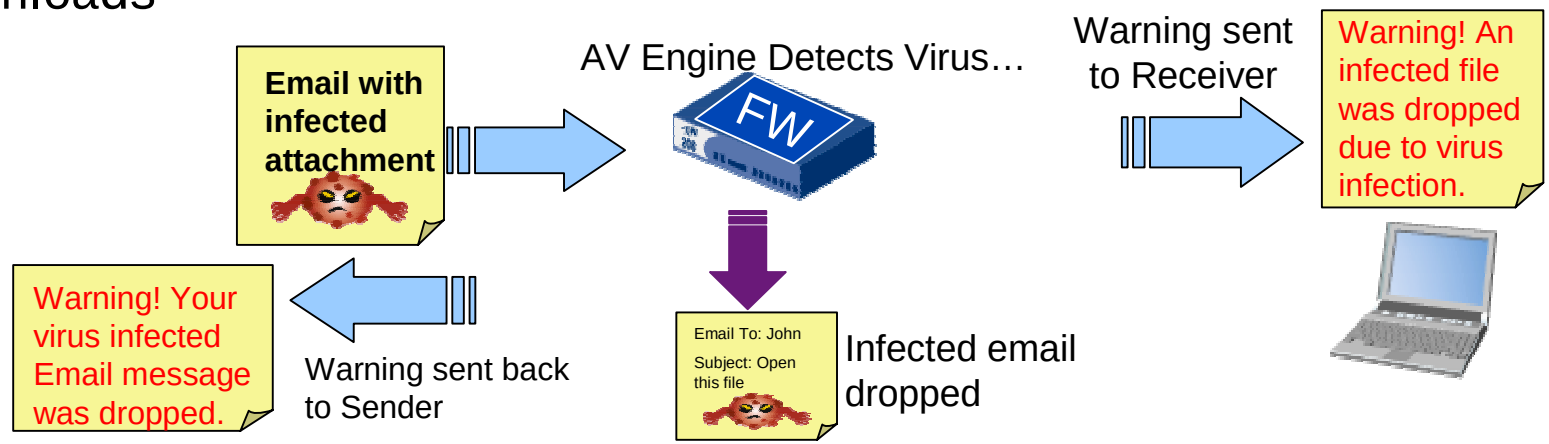
Intrusion Prevention vs. Deep Inspection



Purpose	Deep Inspection Firewall	Intrusion Detection and Prevention
Access Control	✓	
Protect Network Layer	✓	
Protocol conformance	✓	✓
Application layer protection	specific protocols	broad range of protocols
Compliance monitor		✓
Suspicious activity monitor		✓
Traffic Decision	100%	0% - 20%
Forensic analysis	As needed	80% - 100%

Gateway Anti-Virus: Preventing Virus Proliferation

- What it does:
  - Protects corporate network from telecommuter generated virus proliferation
- How it works:
  - Embed leading AV engine into FW/VPN appliance
  - Scan Mail traffic and web downloads
- Where it's deployed:
  - Deployed at the gateway
  - Embedded AV stops viruses before the infect the user



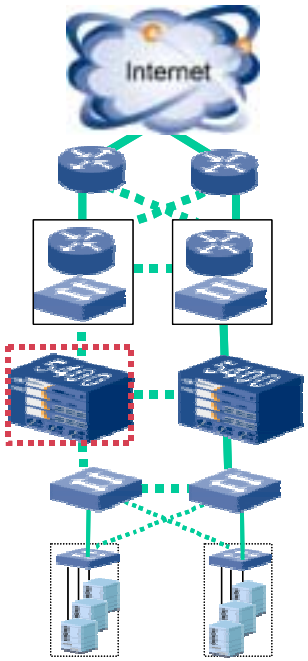
Layered Security Summary

Layered Security Component	Remote Access Security	Site-to-site Security	Perimeter Security	Network Core Security	LAN Security
Firewall	No	✓	✓	✓	✓
Denial Of Service	No	✓	✓	No	✓
IPSec VPN	✓	✓	✓	No	✓
IDP	No	✓	✓	✓	No
Antivirus/ Web filtering	✓	✓	✓	✓	No
SSL VPN	✓	No	✓	No	✓

Network and Performance Considerations

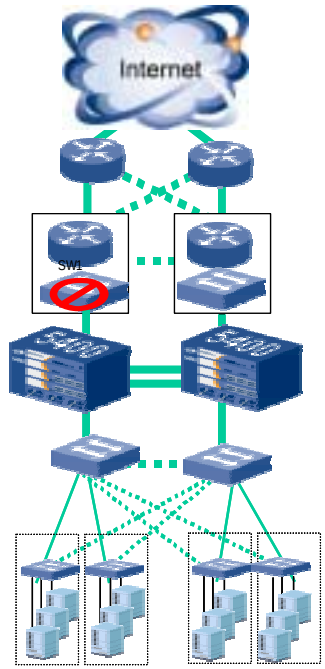
Additional Considerations: High Availability

Active/Passive



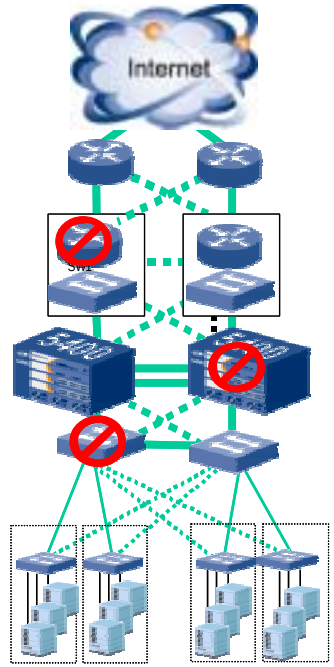
- Secondary device configuration mirrors primary
- Stateful failover for both firewall **AND** VPN
- Active sessions, NAT, VPN tunnels, security associations maintained

Active/Active



- Traffic split between devices – backup always under test
- Stateful failover for both firewall **AND** VPN
- Active sessions, NAT, VPN tunnels, security associations maintained

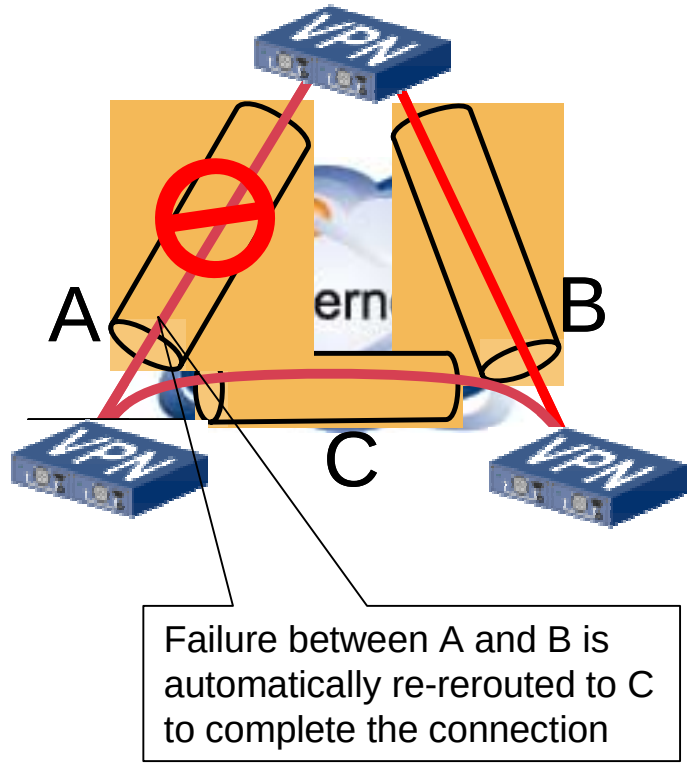
Active/Active Full Mesh



- Failure anywhere funnels all traffic through “up” device
- Stateful failover for both firewall **AND** VPN
- Active sessions, NAT, VPN tunnels, security associations maintained

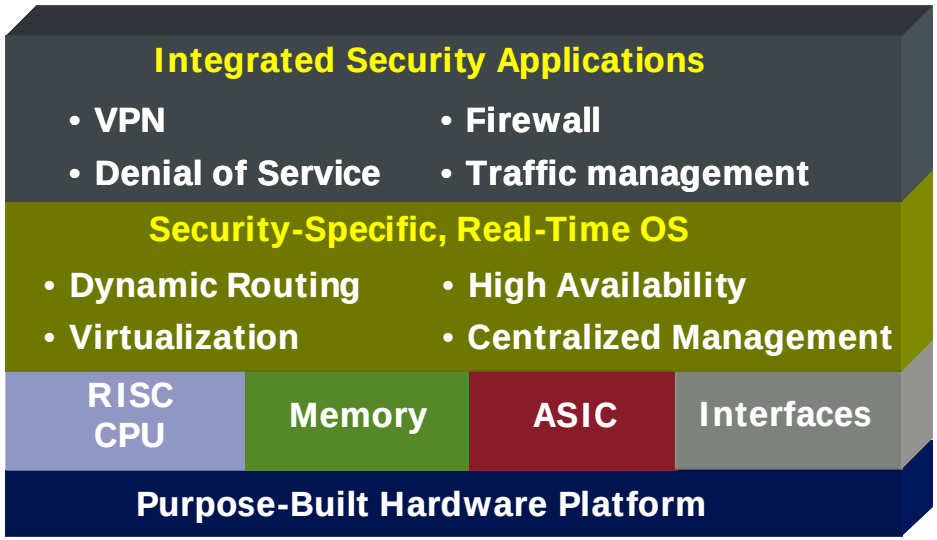
Network consideration: Route-based VPNs

- What it does:
  - Leverages built-in dynamic routing for VPN resiliency
- How it works:
  - Dynamic routing “learns” network and available routes automatically
    - Network or routes need not be defined for VPN
    - Routes around failures and topology changes
    - Helps ensure highly available network
- Where it’s deployed:
  - Encryption and non-repudiation are another layer of protection
  - Used for secure communications - Remote user, site-to-site, Internal LAN communications



Performance Considerations: Platform Architecture

- Purpose-built for rock solid security
  - Security specific processing for optimized performance
  - Entire platform controlled by security specific, real-time operating system
  - Includes security applications and integrated networking

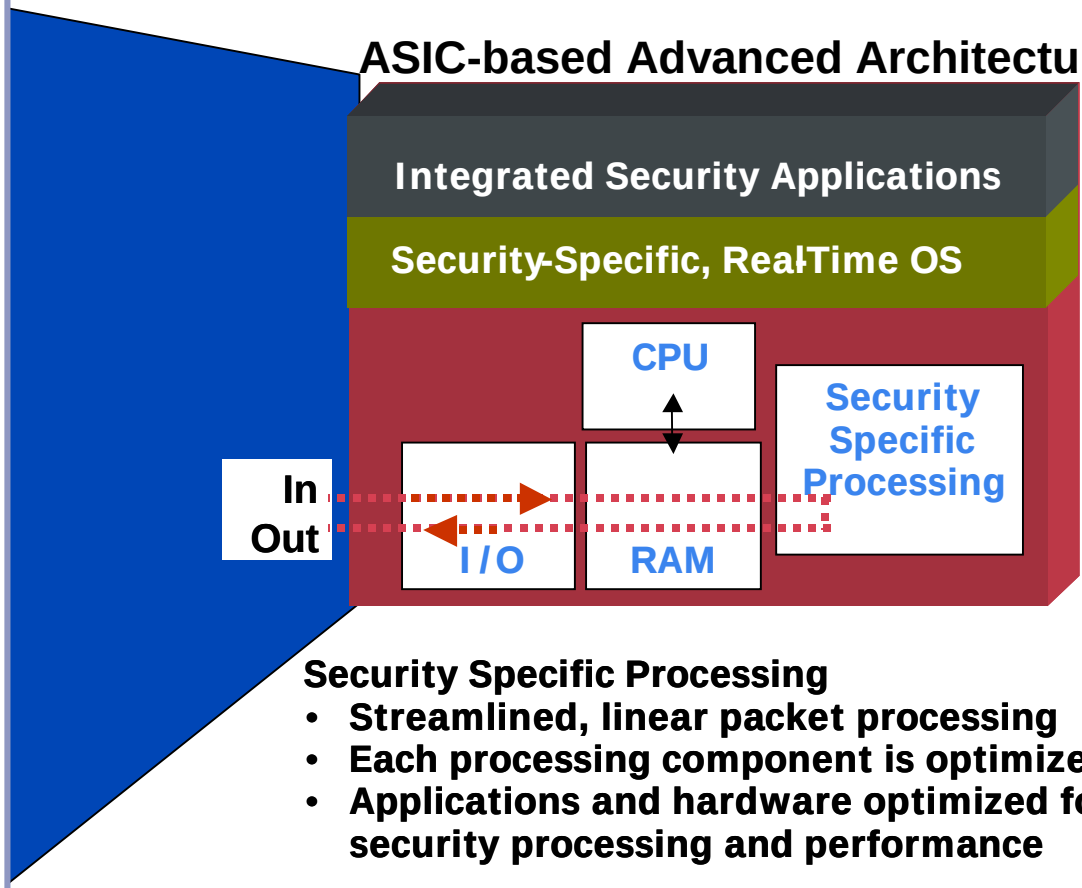


Advantages

- Eliminates OS hardening
- Facilitates network integration
- Ensures application interoperability
- Simplifies management
- Matches or exceeds performance requirements of today's networks

Purpose-built Architecture

- Purpose-Built Appliance
  - Tightly integrated platform, OS, Networking and applications
  - VPN, Firewall, DoS
  - Optimized for security performance
- Benefits
  - High performance throughput under load
  - Quick VPN session establishment
  - Accelerated IKE negotiation
  - Low latency
  - Improved security

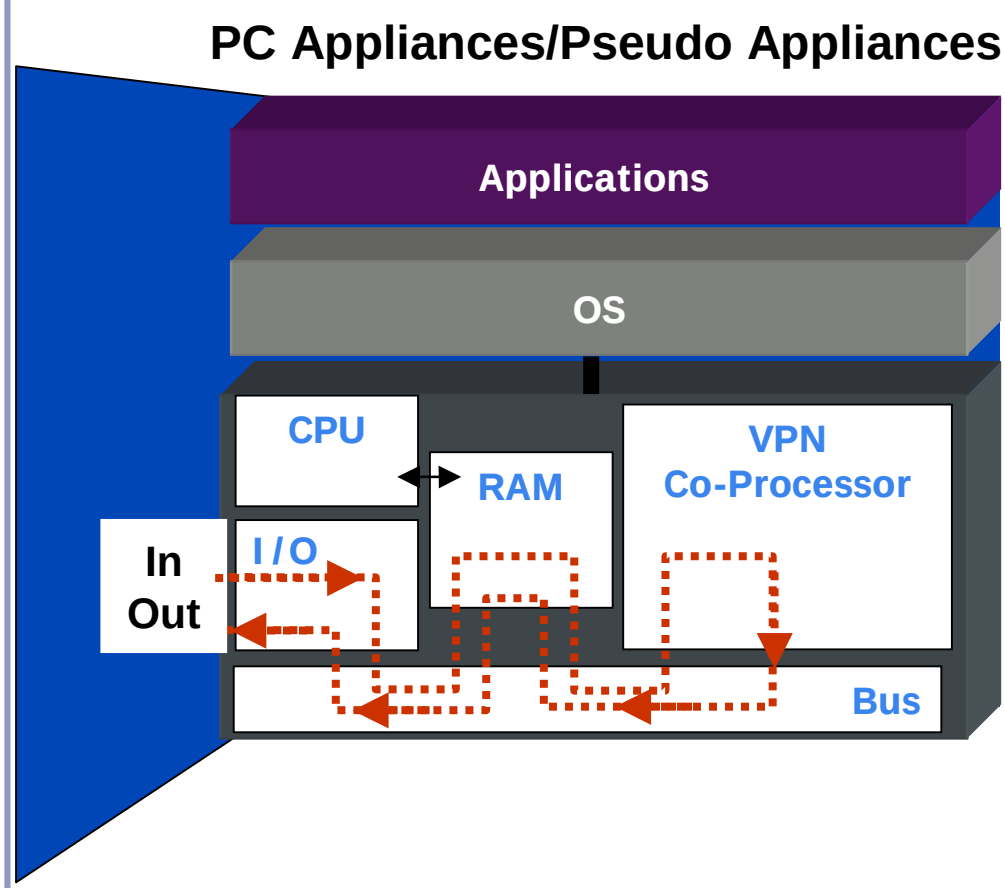


Security Specific Processing

- **Streamlined, linear packet processing**
- **Each processing component is optimized**
- **Applications and hardware optimized for security processing and performance**

Alternative Architectures

- Alternative architecture characteristics
  - Security applications added to networking architecture
  - Software applications on general purpose OS/platform
- Characteristics
  - High performance throughput under load
  - Quick VPN establishment with IKE negotiation
  - Low latency
  - Improved security



Management Considerations

Life Cycle Management

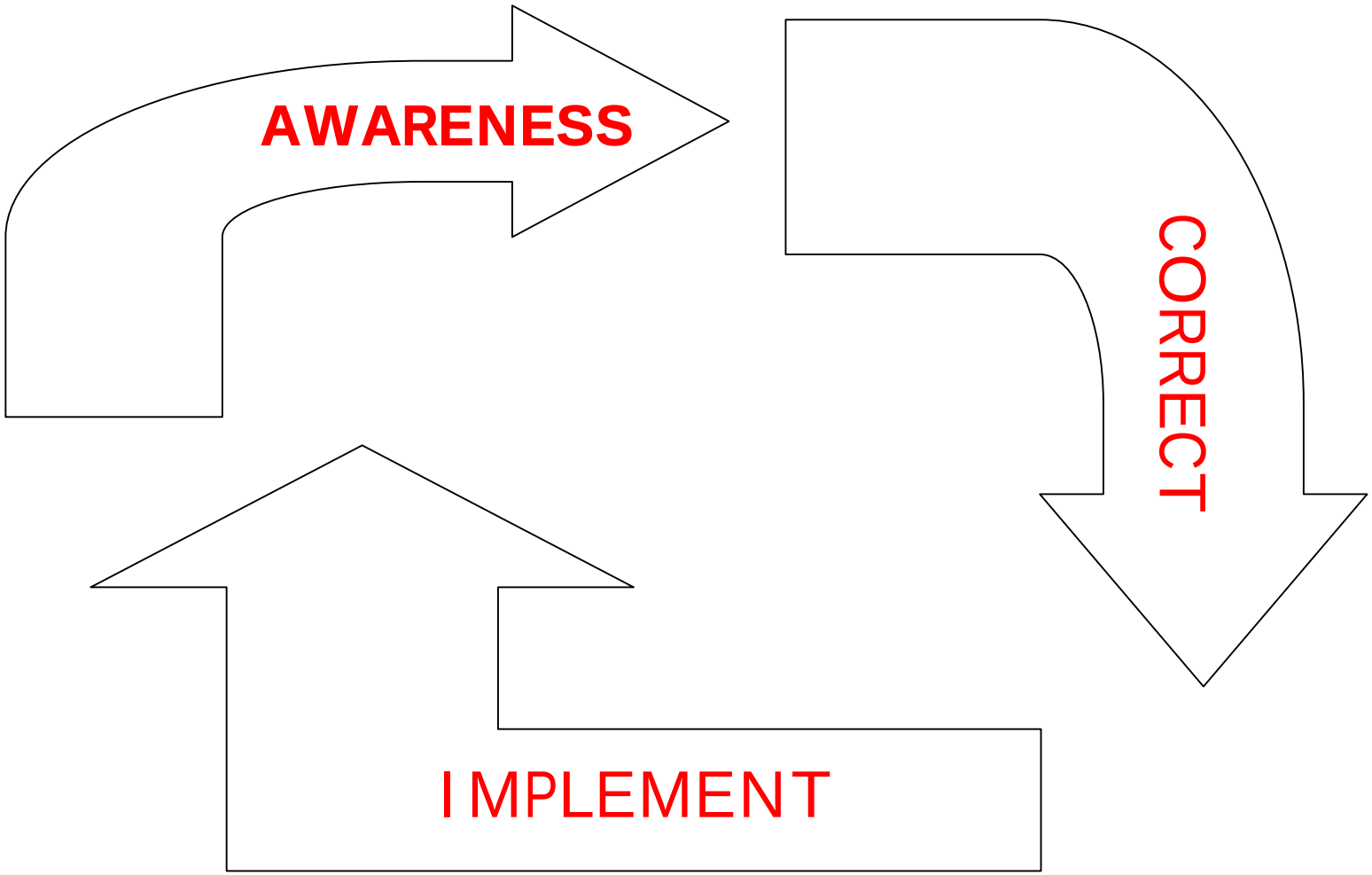
- Manages Device, Network, Security
- Support the entire device life cycle
- Enables delegation of roles, responsibility, access
  - Security Admin
  - Network Admin
  - Ops
  - Technician
- Enables Network and Security Team to work together
- Interact using CLI, Web or GUI

Device Lifecycle

Management Level

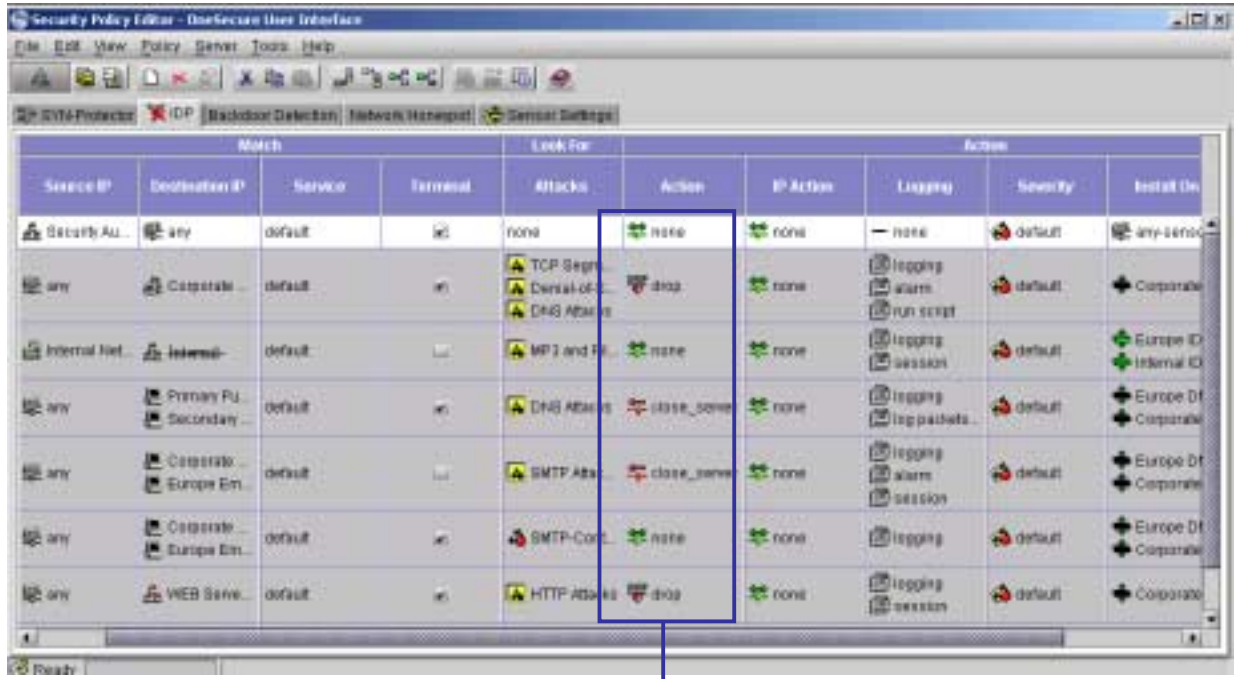
	Design, Deploy	Configure	Monitor, Maintain	Upgrade, Adjust
Security	• Define security of entire network (all devices) • Permission definitions	• Push device specific policy out • RAS user management • Admin management	• Attack log monitoring • Consolidation • Top attacks report • Log Investigation • Reports	• Signature updates • Policy adjustment
Network	• VPN modeling • L2/L3 specification • (Routing)	• VPN config • Route tables • Routing • VLAN	• VPN monitoring • Network failure recognition and response • HA failover monitoring	• VPN model • Adjust routing
Device	• Remote installation • Initial configuration	• Interface characteristics • Management access • Licenses • OS version	• HW monitoring (interfaces up/down, fan failure, power failure)	• OS upgrade • Device config changes

Network Awareness



Response Management Considerations

- New Mind Set
  - What is happening?
  - What has happened?
  - What may happen?
- Analyze
  - Dictate exactly what traffic to analyze, what to look for in that traffic and how to respond.
- Network Aware
  - Network awareness is visualizing the entire environment.

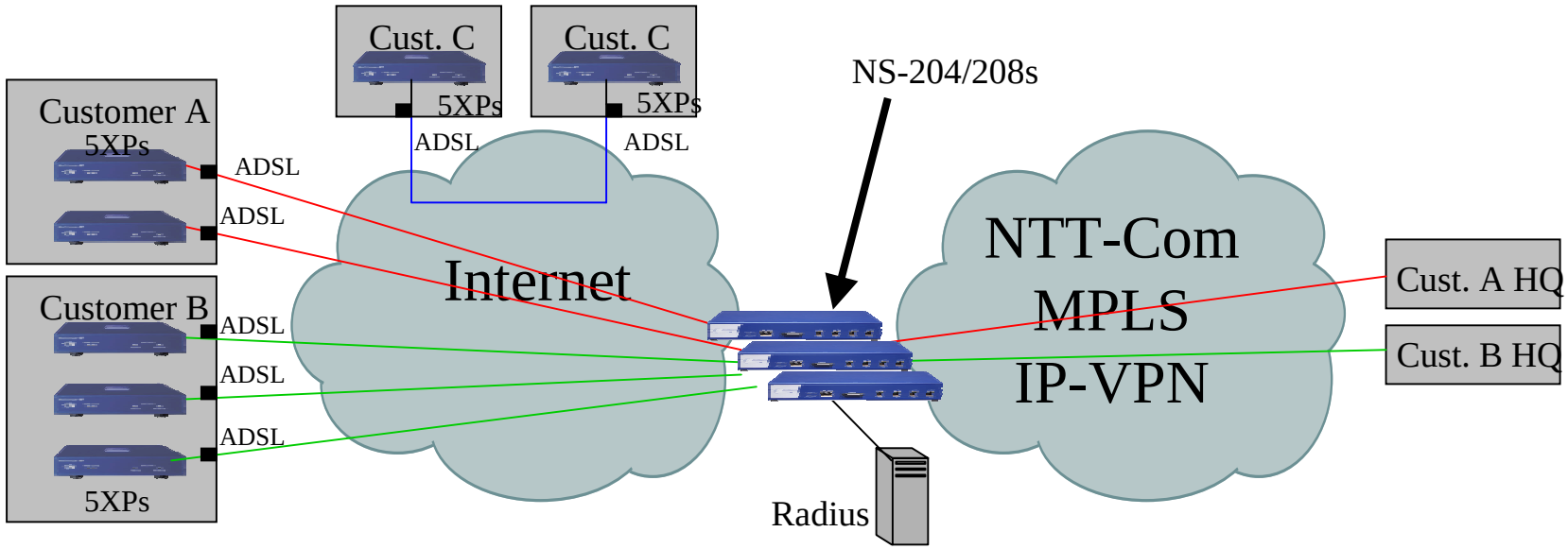


Understanding what happens in the network is critical!!

What about Managed Security Service (MSS)?

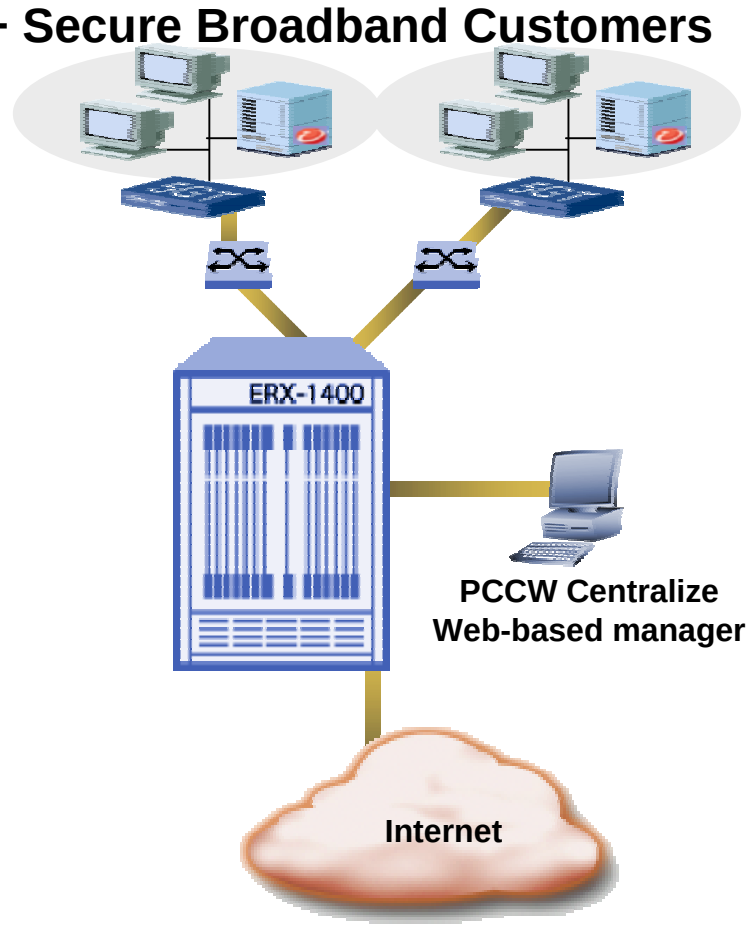
Managed CPE-based IPSEC VPN

- Lease Line is $2,000-$3,000/month/branch vs. IPSec VPN is $200/month/branch
- NTT-Com has end to end VPN solution by using MPLS and IPSec VPN



Managed Secure Broadband Svc

- SME Business Problem
  - Lack of IT resource/knowledge
  - Need business continuity
  - One-stop-shop for service
- Secure Broadband Solution
  - Increase service value
    - Protect customer network
    - Provide security advices
    - CPE provides tangible value
  - Account Control
  - Protect PCCW network
    - Keep virus/worms from spreading



Summary: Implementing Layered Security

- Defense in Depth
- Attack Protection
  - Secure routers maintain network availability / manageability
  - Combination of FW, IDP, Anti-Virus to detect broad range of network and application attacks with ability to drop malicious packet to eliminate impact
- Appliance
  - Performance and management consideration, high speed; high capacity; high availability
- Network Integration
  - Integrate BOTH networking and security applications and simplify deployment
- Management
  - Capable of centrally manage the growing number of network and security devices, events and response.

Juniper™ NETWORKS

Thank You