



Managed Security Services

Georgina Schaefer
Consulting Systems Engineer, SP Wireline EMEA
Solution Architect, Managed Security Services

Enterprise Security Drivers

The Security Dilemma



Poor Security Equals Business Loss

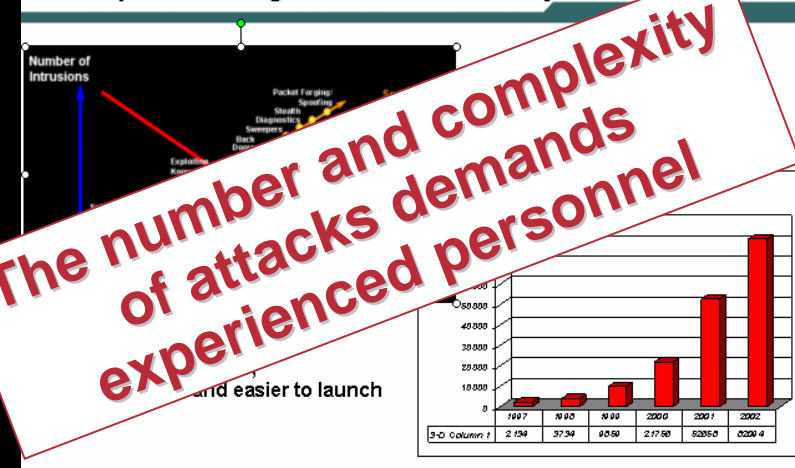
Type of crime	2000	2001	% Change
Theft of proprietary information	\$18.4	\$22.3	+21%
Financial fraud	\$13.1	\$16.4	+25%
Virus	\$69.8	\$36.9	-47%
Insider Net Abuse			+179%
Denial of Service			+184%
TOTAL	\$ 265M	\$455M	+172%

Other factors: Negative public perception, Loss of client/customer/partner confidence, Loss of proprietary information, Loss of revenue

2002 CSIFBI Computer Crime and Security Survey (223 Respondents for 2002)

Security is not just a "cost centre"

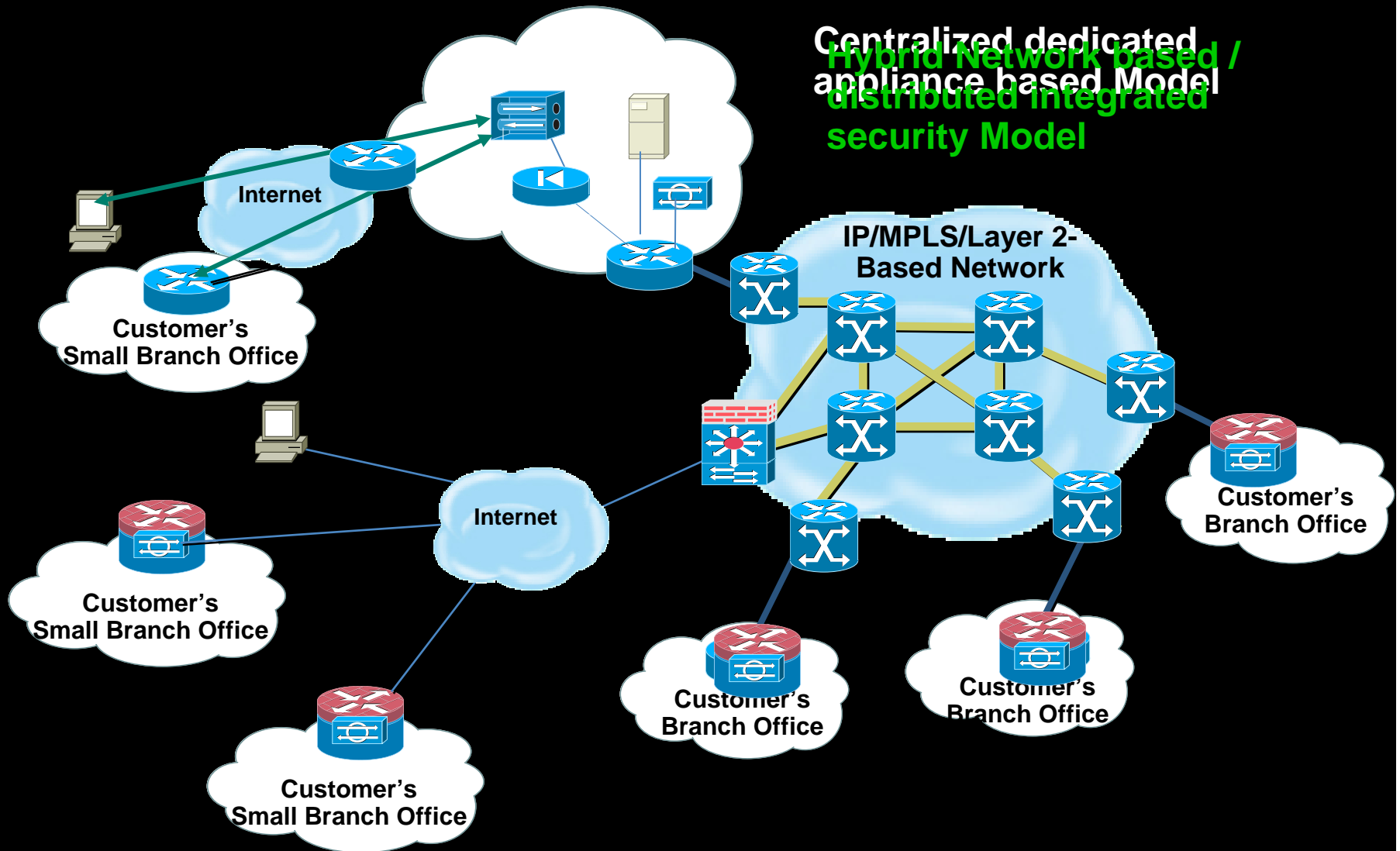
Exponential "growth" in IT security incidents



Broadband explosion through EMEA



Security Deployment Trends



Agenda

- **Managed Security Services Market**
- **Managed Security Services**
 - Managed Threat Defense**
 - Managed Trust Identity**
 - Managed Secure Connectivity**
- **Summary - Q&A**

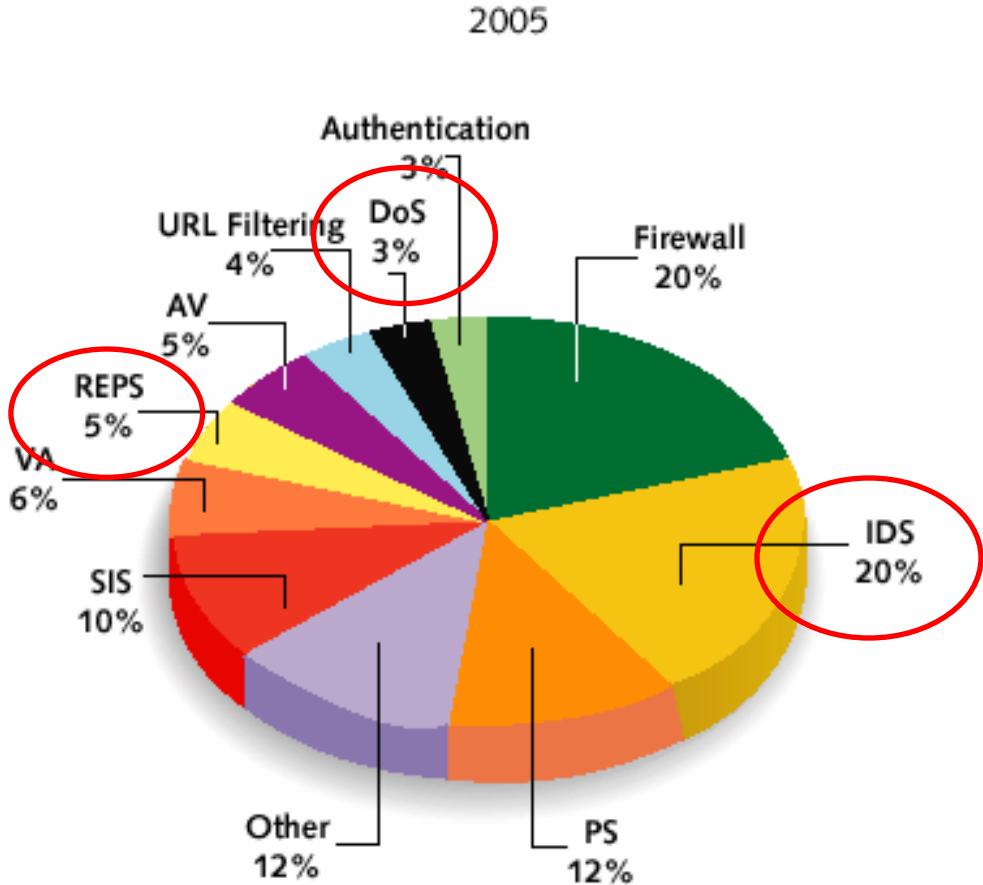
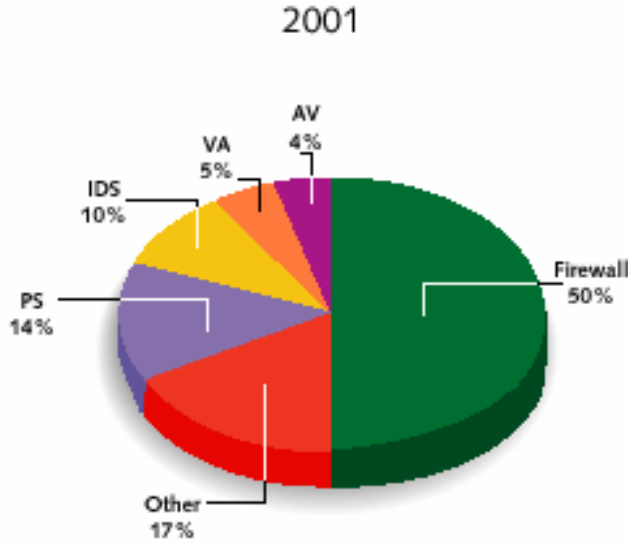
Managed Security Services Portfolio

MSS offerings have been around for sometime

Services include:

- **Managed Firewalls (bulk of revenue)**
- **Managed VPNs**
- **Managed IDS**
- **Managed Anti-Virus**
- **Managed Authentication**

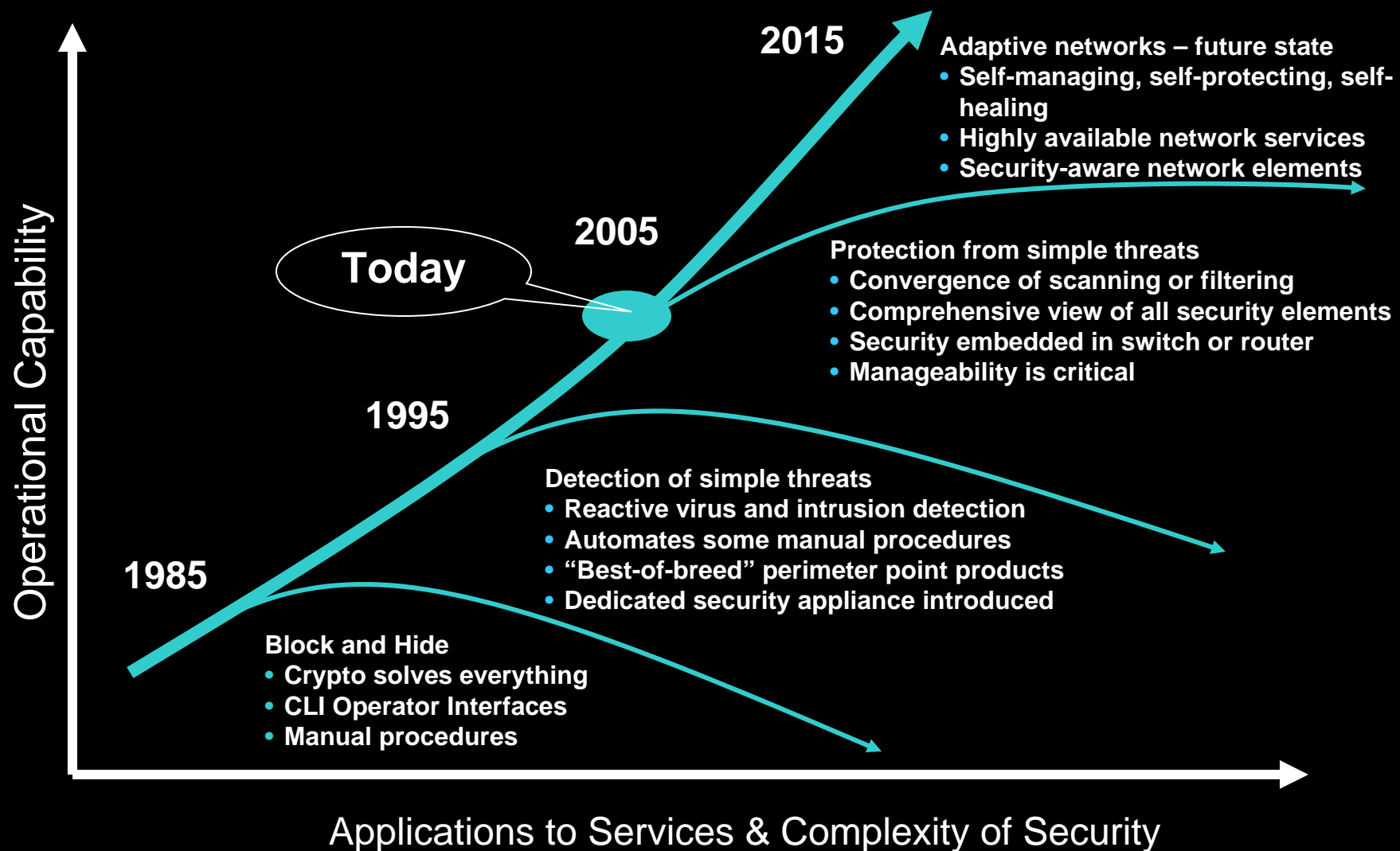
MSSP Revenues Shift



PS = Professional Services
 AV = Anti-Virus
 VA = Vulnerability Assessment
 IDS = Intrusion Detection System
 SIS = Security Intelligence Services
 REPS = Remote End-Point Security

Source: Yankee Group, 2002

Network Security Evolution



MSSP Players

Mainly from 4 different categories:

- **Network/Systems Integrators (e.g. CGEY, Unisys, IBM)**
 - Focus on global outsourcing deal with custom solutions
- **Pure play security SP (e.g. Ubizen, Getronics, NetSec)**
 - Often positioned as niche players
- **Technology owners/Software vendors (e.g. Symantec, ISS, Baltimore)**
 - Services tend to be limited to their own technology
- **Service Providers (e.g. BT, DT, FT, C&W, Equant, AT&T)**
 - Traditionally deliver connectivity services

Status of the MSS market

- **Most of the current portfolios are targeted at medium/large enterprises and are based on appliances each solving a single problem**

SPs started to build Managed Security Services 2-3 years ago when not all the required security features were available in routers

Difficult to address the price-sensitive and mass-markets (high capex, high opex, integration complexity)

Market Inhibitors

- **Enterprises unwilling to outsource security**
- **Lack of perceived need for extensive security**
- **Unproven reputation of MSS Provider**
- **SPs unwilling to go beyond CPE**
- **Perceived higher costs of Outsourced service**
- **Too many offerings with unclear definitions**
- **Product oriented vs Global Security Solution**

Market Segregation

Custom

- SLAs (bronze, silver, gold)
- High Price
- 24X7
- Detailed reports
- On-going monitoring
- Log analysis
- Redundancy

1500-3000 euro/month

Value/price ↑ +

Bundled

- Delta Price to CX
- Packaged with CX
- Basic reports
- Network/CPE

Medium (50-249)

50-150 euro/month

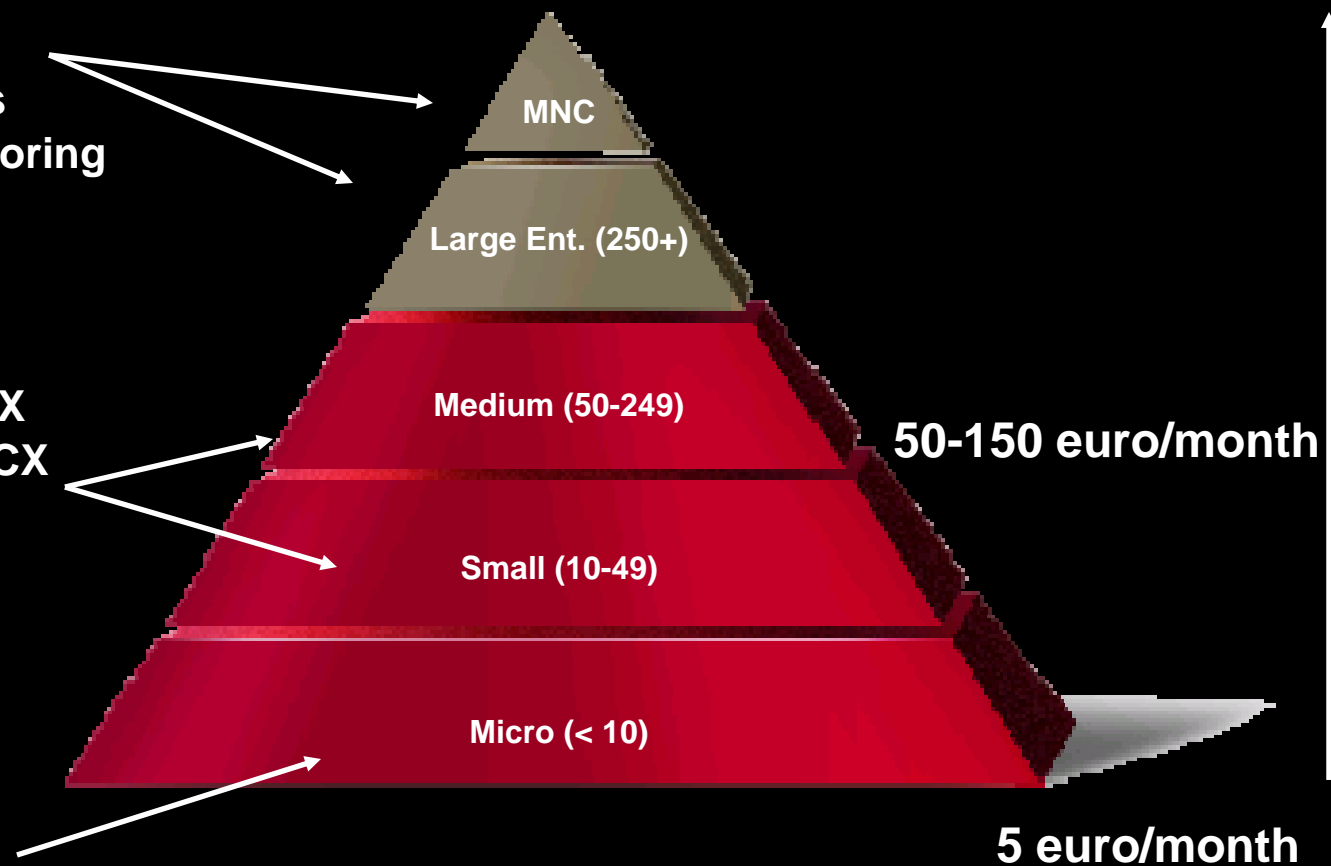
Small (10-49)

Mass market

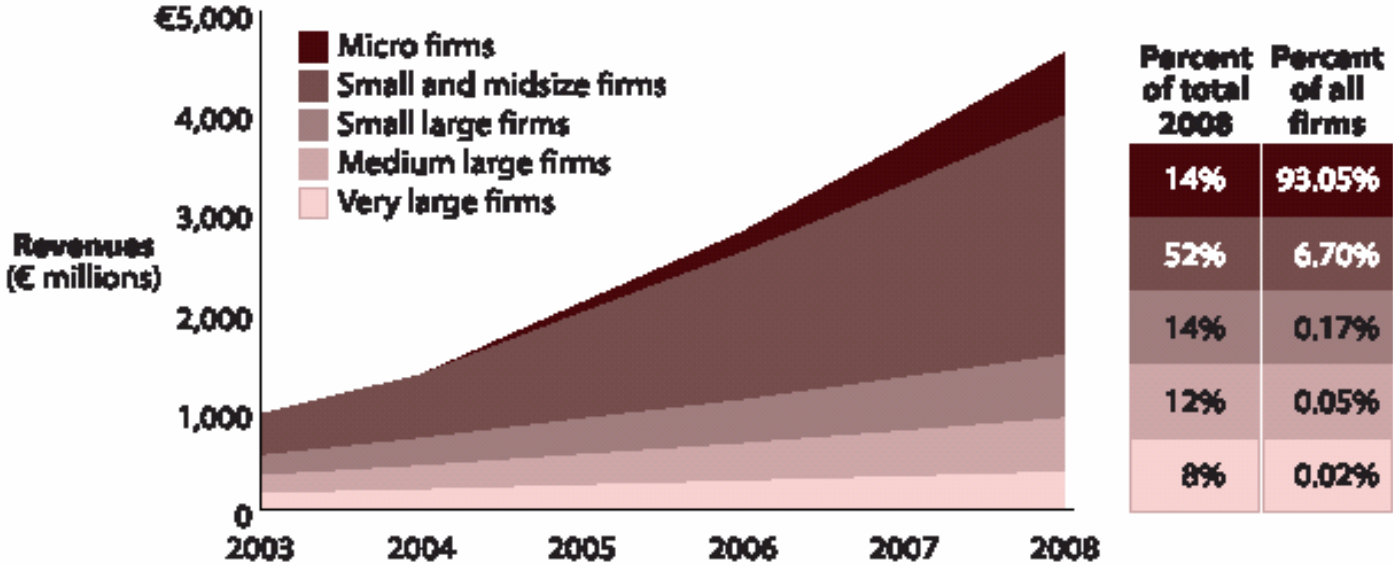
- Price sensitive
- Point product
- Self managed

Micro (< 10)

5 euro/month



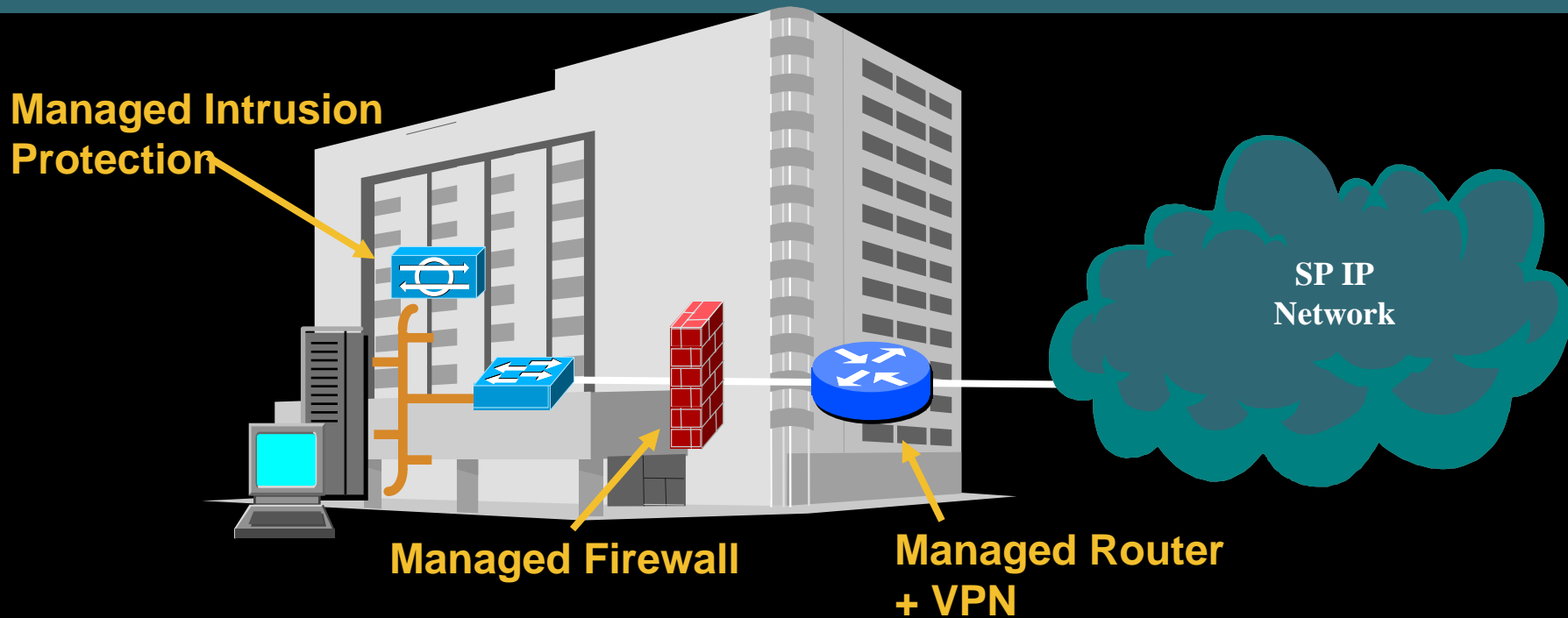
MSS and European Companies



Source: Forrester Research, Inc.

**SMEs represent more than 99% of companies!
By 2008 they should generate 66% of European MSS sales**

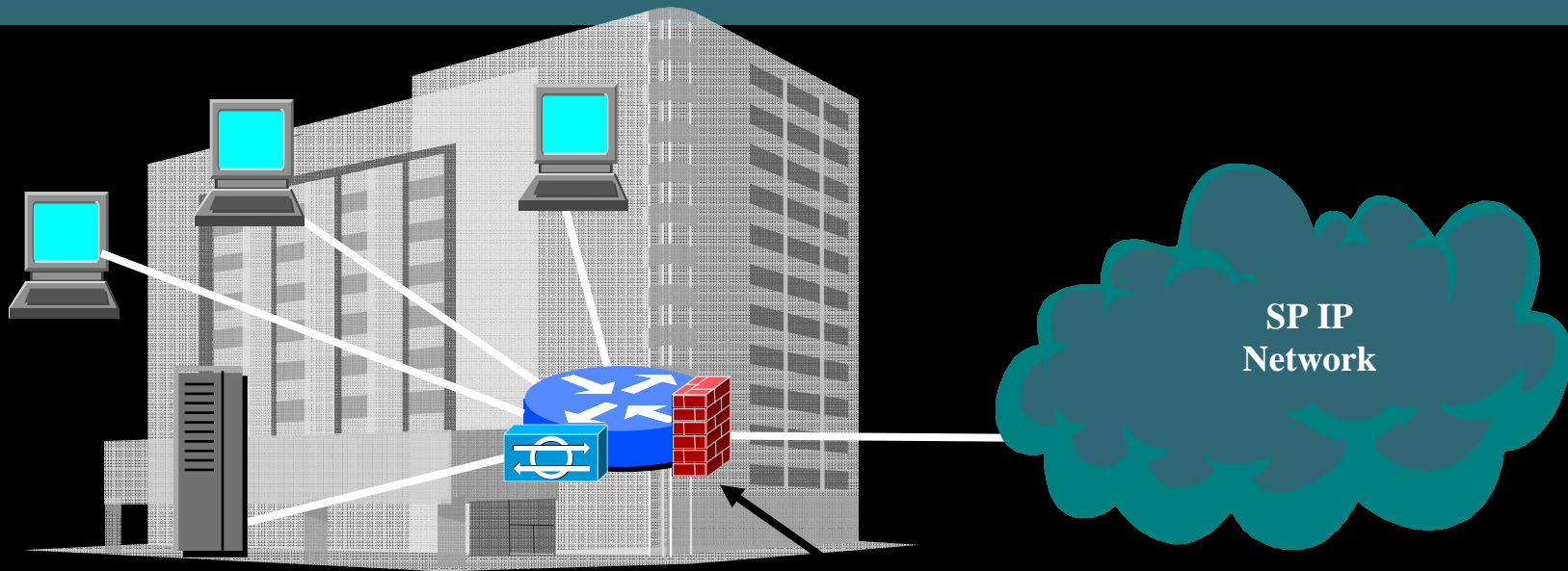
Managed Services – Multi-device



- Many devices → High CAPEX
- Labour intensive operation → High OPEX
- Different services coming from different providers (SP, SI, MSSP, ...) → Lack of consistency in Security Policy

Not the best model to address small offices or SMBs

Managed Services – Single Device



Full Managed Security Services

- Service are turned on on-demand → extending CPE lifecycle
- 1 or 2 devices for the full service portfolio → Lower CAPEX
- Less truck-roll and devices to manage → Lower OPEX
- Decreased churn through a comprehensive Portfolio

Better Model for mass-deployment services

Moving from Managed Security Services to Secured Managed Services ...

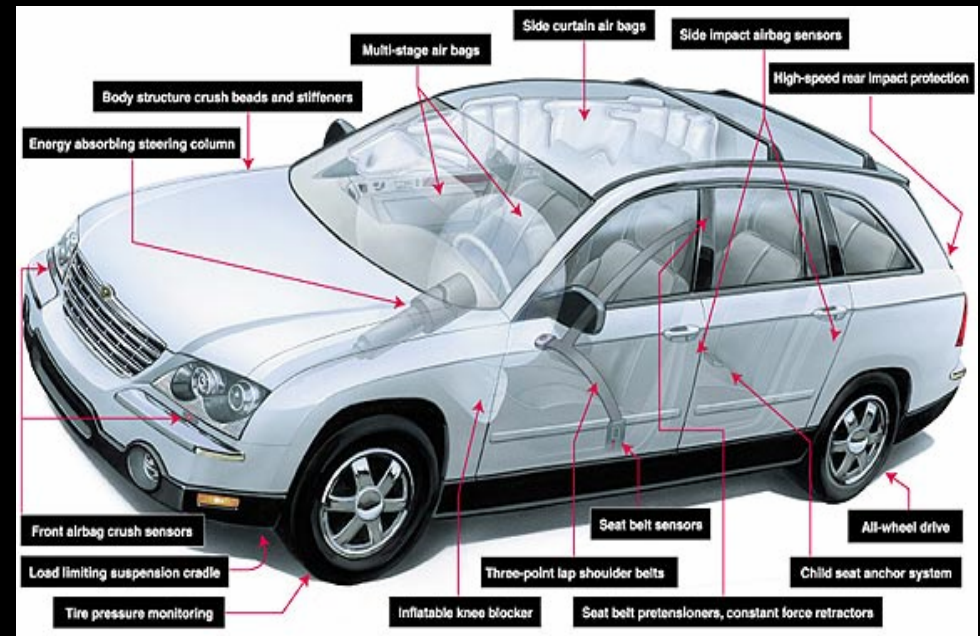


Managed Security as a Option

Security is an add-on

Challenging integration

Not cost effective



Secured Managed Services

Security is built-in

Intelligent collaboration

Appropriate security

Gartner: By 2006, 60 percent of firewall and intrusion detection functionality will be delivered via network security platforms

Managed Security Service Examples



Service Provider Security *Fundamentals*

Security Policy

Security Policy Defines Network Design Requirements

Trust & Identity

Leverage the network to intelligently protect endpoints

Secure Connectivity

Secure and scalable network connectivity

Network Infrastructure Protection

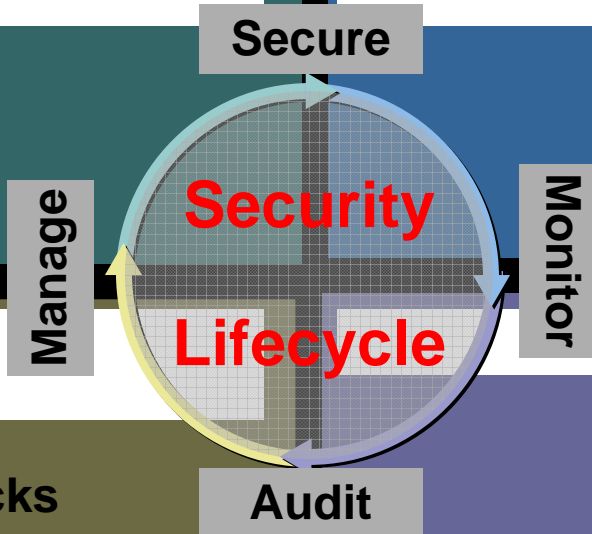
Protect the network infrastructure from attacks and vulnerabilities

Threat Defense

Prevent and respond to network attacks and threats such as worms

Security Operation

Security Management and Monitoring, Incident Response processing



Managed Security Service Portfolio

- **Threat Defense Services**

- Managed Firewall - • Ability to customize security rules, policies and ports

- Managed Intrusion Protection - Protection of vital information from intruders

- Managed DDOS Protection

- Managed Endpoint Protection (Server and Desktop protection)

- Email Virus Protection - Protection against spam attacks and virus spread

- Content Filtering

- **Secure connectivity Services**

- Secure remote-user access to company information

- Virtual Private Network (VPN) Services using IPSec or SSL VPN

- **Trust and Identity Services**

- On single factor or Two-factor authentication (token/smart USB or card)

- PKI certificate

- Endpoint security compliancy (Network Admission Control)

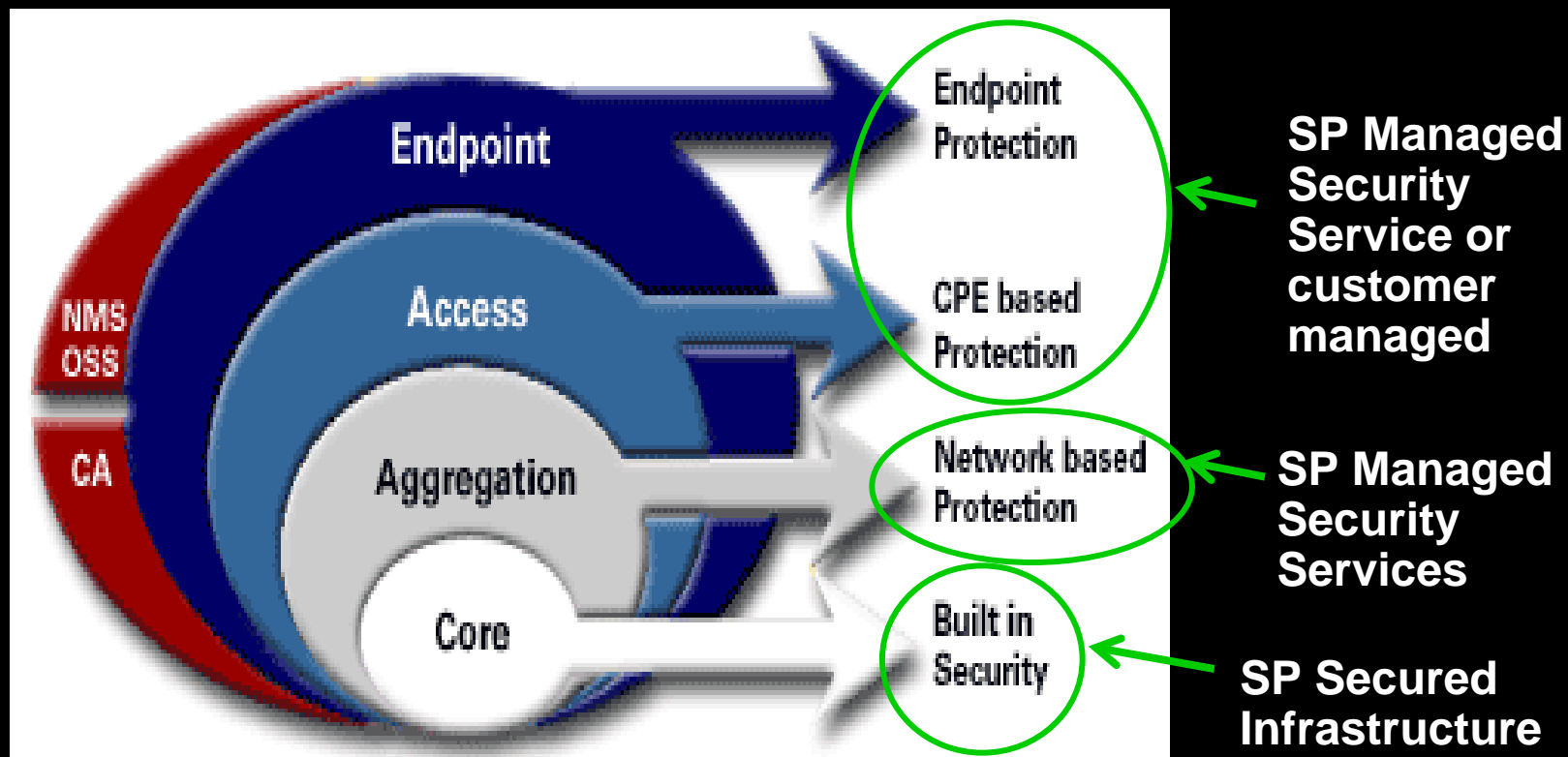
Managed Services / Market Segment

Threat Defense Services	FW	Content Filtering	IPS	Email Spam & Virus protection	DDOS protection	Endpoint Protection	Security Monitoring	Threat Intelligence
residential market	✓			✓				
small Business	✓			✓		✓		
medium Business	✓	✓	✓	✓		✓		
large enterprise	✓	✓	✓	✓	✓	✓	✓	✓

Secure Connectivity Services	Site to site IPSec VPN	Remote Access IPSec VPN	Remote Access SSL VPN
residential market			
small Business	✓	✓	✓
medium Business		✓	✓
large enterprise		✓	✓

Trust & Identity Services	One factor authentication	Two factors authentication	PKI	Endpoint Security compliancy
residential market				
small Business	✓			✓
medium Business	✓	✓		✓
large enterprise	✓	✓	✓	✓

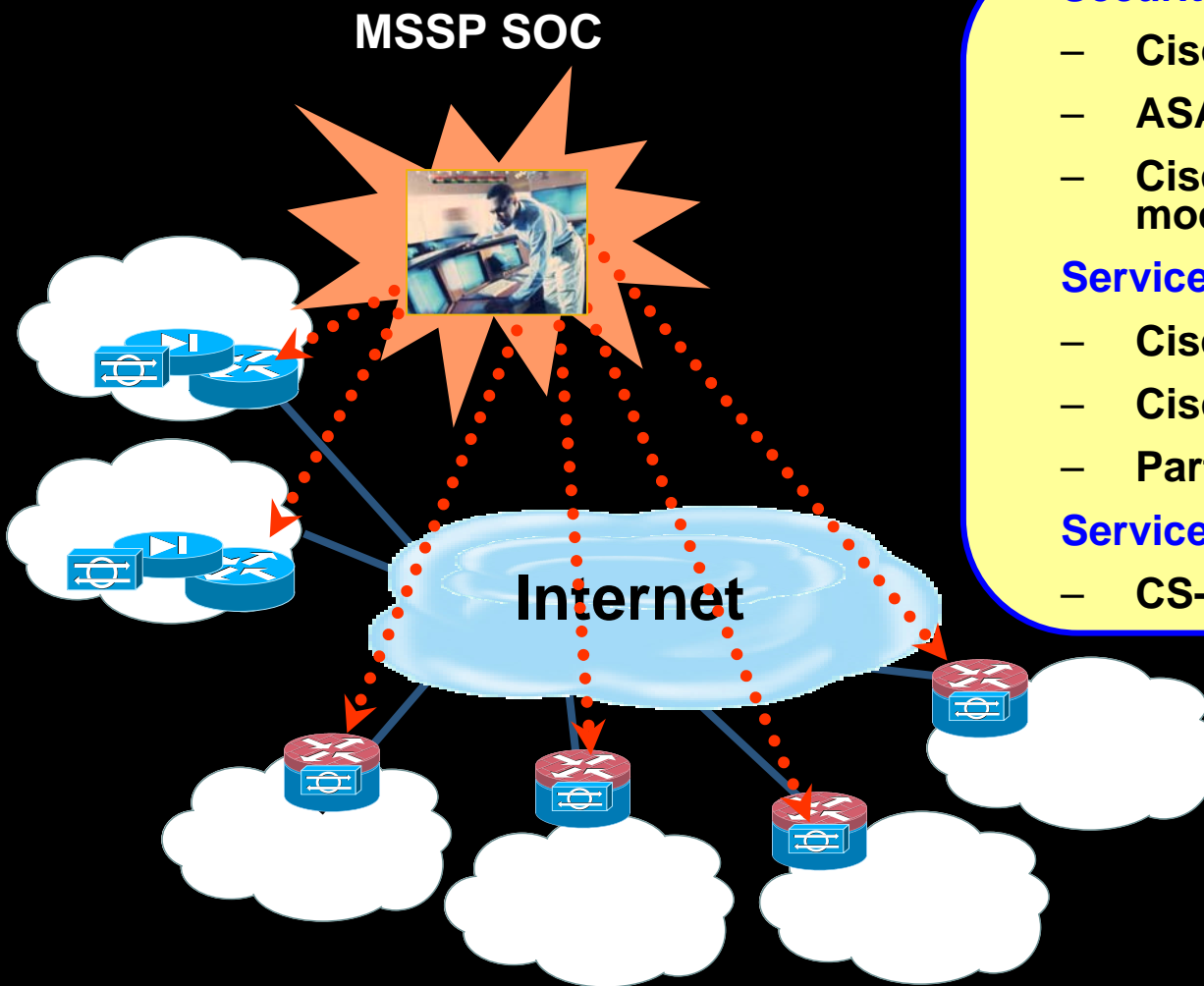
Protection at every Network Layer



Cisco can help SP provide a *complete* security portfolio

- CPE & network-based VPN, firewalls & IDS/IPS
- Endpoint threat protection
- Identity management
- Security service provisioning
- Security threat management

CPE Based Managed Service



Security Devices / Products

- Cisco ISR with integrated security
- ASA, PIX, IPS appliances
- Cisco 7600 with security service modules

Service Provisioning

- CiscoWorks VMS
- Cisco Configuration Engine
- Partner product

Service Monitoring

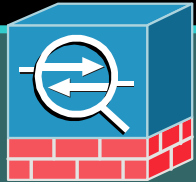
- CS-MARS

Managed Services

- Firewall
- IPS
- IPSec / SSL VPN
- Managed authentication

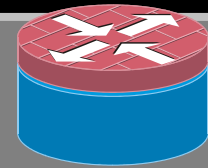
Cisco ISR Routers and ASA 5500 Series

Flexible Security and VPN Deployment Options



Adaptive Security Appliance

- Preference for dedicated security devices
- LAN interfaces
- Delivers latest threat mitigation innovations
- Most feature rich remote access VPN solution
- Dedicated functions ensure maximum software versioning simplicity



Integrated Services Routers

- Preference for and familiarity with IOS-based devices
- LAN and WAN interfaces
- Delivers best of breed routing and QoS functionality
- Consolidates maximum network and security functions on single platform
- Most feature rich site-to-site VPN solution
- Leverage existing router investment

Tailored Solutions for Every Deployment Environment

Managed Security Services Trends

Primary services

- Threat Defense
 - Firewall
 - Virus scanning
 - Intrusion & DDoS detection
- Secure Connectivity
 - VPN/tunneling
- Trust & Identity
 - Authentication

Application FW
Deep Packet
Inspection

Day Zero Attack
Protection

IPS

SSL VPN

Security
Compliance
Check

Managed Service Implementation & delivery

- Quality guarantees (SLAs)
- Sales, lease
- Setup/installation
- Configuration
- Proactive fault, life-cycle, and performance management
- Immediate alert response
 - Trouble-ticket process
 - Analysis
 - Configuration
 - Troubleshooting
- Emergency response - threat or service outages



Managed Threat Defense





Managed Firewalling

- **Analyses all data traffic flowing from one network to another**
- **Allows or denies access based on pre-defined security policies**
- **High-volume packet inspection**
- **Internal address masking (NAT/PAT)**
- **Most common managed security service:**
 - CPE based service (FW installed at customer's premise)**
 - Network based service**
- **User authentication and Content filtering as a service option**

Managed Firewall Service

▶ **Baseline service**

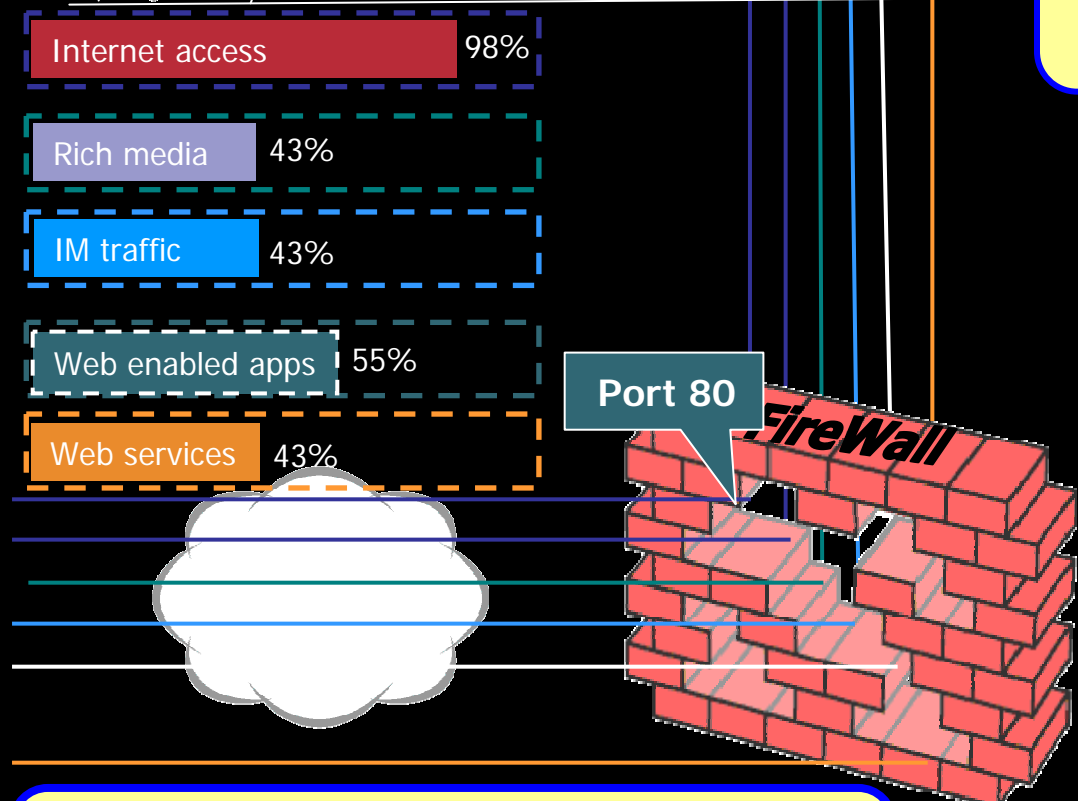
- **Stateful packet filtering**
- **Address translation support**
- **Routing**

▶ **Service options**

- **Advanced Application Support**
- **Redundancy / High Availability**
- **Authentication**
- **Web content Filtering**
- **Virtual Firewall**

Advanced Application Support

Attacks based on Web Applications

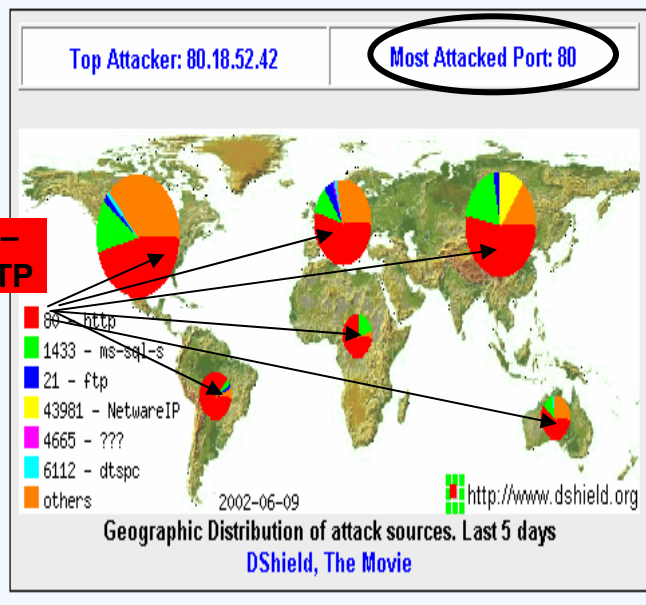


“...75% of successful attacks against Web servers are entering through applications and not at the network level.”

Records Added

Last Month	Last Week	Today
45,535,289	7,563,848	1,356,235

As of June 10, 2002 01:20 pm GMT



64% of enterprises have opened Port 80 on their firewalls for their growing web application traffic

Source: Aug 2002 InfoWorld/Network Computing survey of IT Professionals

Advanced Application Support

Web-Traffic Inspection Services



Supported on IOS / PIX 7.0 / ASA / FWSM 3.1

HTTP Inspection Engine

- Delivers application level control through inspection of web-based (port 80) traffic
- Prevents port 80 misuse by rogue apps that hide traffic inside http to avoid scrutiny e.g.
 - Instant Messaging (AIM, MSN Messenger, Yahoo....)
 - Peer-to-Peer Protocols (Kazaa...)
 - Example: Instant messaging and peer-to-peer applications such as Kazaa
- MIME type/content filtering....

Email Inspection Engine

- Control misuse of email protocols
- SMTP, ESMTP, IMAP, POP inspection engines

Inspection Engines provide protocol anomaly detection services

Belgacom Managed VPN service and Firewall

belgacom

info & help | contact GO

petites entreprises professionnel | privé | Groupe Belgacom

- téléphonie
- ▶ internet & data
 - accès
 - équipement
 - votre site web
 - réseau & télétravail
 - télétravail
 - sds
 - lignes louées
 - e-link
 - options
 - sécurité
 - tarifs
- promotions
- e-Services
- newsletters

Vous êtes ici : [internet & data](#) / [réseau & télétravail](#) / [e-link](#)

e-Link

La solution VPN pour PME, une solution fiable et flexible gérée pour vous par Belgacom

Commandez maintenant !

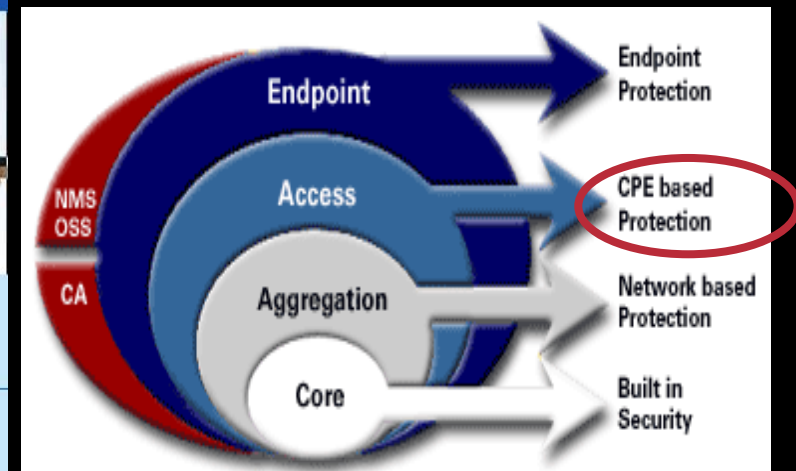
Livraisons à domicile

Voir aussi
▶ [e-Link en bref](#)

Belgacom e-Link est une nouvelle solution réseau spécialement développée pour répondre aux besoins des PME. Cette solution interconnecte les différents réseaux locaux (LAN) de vos sites entre eux et avec la maison mère. Ceci de manière à protéger votre intranet contre tout accès non autorisé. En outre, cette solution vous offre les avantages de l'Internet sans en comporter les risques.

Pour un montant mensuel fixe par site, cette solution globale englobe:

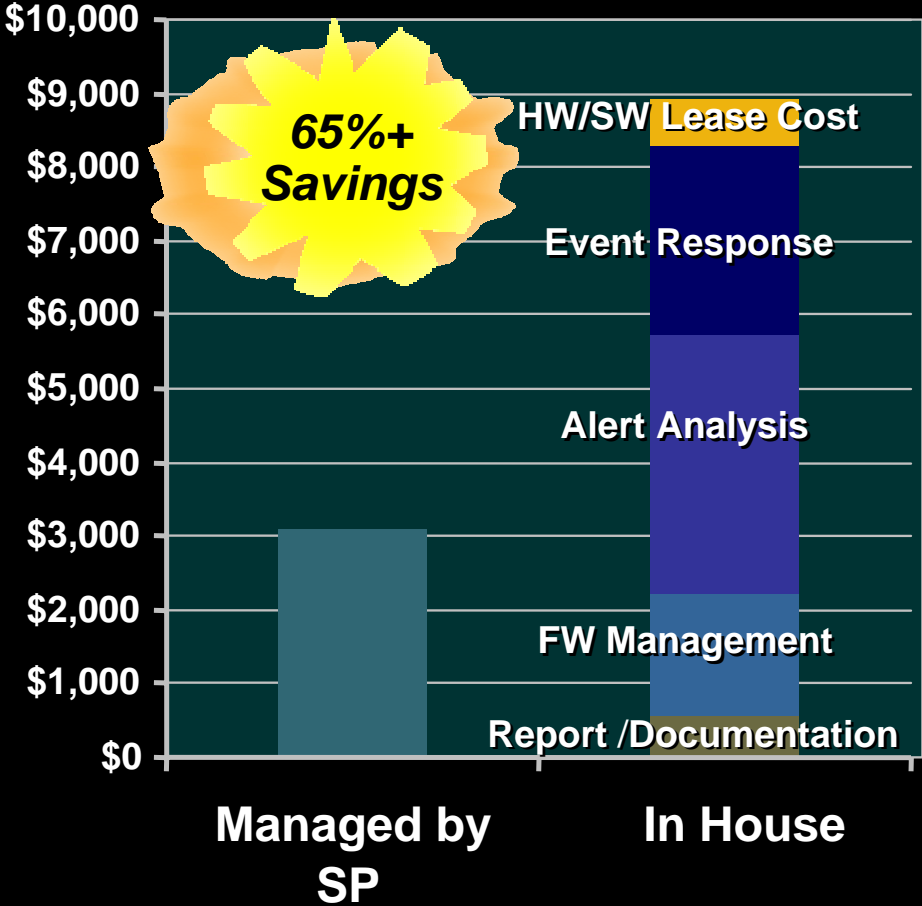
- Un paquet comprenant:
 - un routeur d'accès sur chaque site (Cisco 826 ou 827);
 - la ligne d'accès via la technologie DSL et la connexion au Virtual Private Network (VPN);
 - l'accès à l'internet avec protection firewall;
 - l'installation, la configuration et la gestion des différents éléments du Wide Area Network.



SP Managed Firewall Service vs. In House customer management

- **Benefits of out-tasking**
 - Reduced monthly recurring management cost (65%)
 - Increased network reliability (24-hour monitoring)
 - Lower implementation and training cost
 - Flexibility to reallocate IT staff to strategic projects

Monthly Recurring Cost (Nine Sites, 2500 Users)



Intrusion Prevention

- **80% of the recent attacks have been performed over port 80**
- **It is not enough to firewall to counter attack**
- **In-depth inspection of traffic is required to identify attacks within legal traffic on both the network and the critical hosts**
- **IDS services only generate alarms – Intrusion “Prevention” Services or “Inline IDS” can DROP traffic matching attack signatures**

False positives will drop good traffic!!

- **Not very common today in the low end space**

Managed IPS or “Anti-X” services



- Provides protection against :
 - Viruses, Worms, Spyware / Adware, Denial of Service..**
- Use IDS/IPS hybrid technology – Signature based, anomaly based, behaviour based
- Signatures must be updated on a regular basis
- Events must be regularly monitored and False Positives / Negatives tuned
- IPS services require powerful and complex management, monitoring and response procedures
- Need 24x7 service operation hence required a well automated system

Managed IPS Service

▶ **Baseline service**

- **24 x 7 Service and Support**
- **Intrusion monitoring**
- **Event correlation / Alarm filtering**
- **Web Portal: Log trending and analysis with periodic traffic and alert reports**

▶ **Service options**

- **Vulnerability Assessment**
- **Signature updates (Managed IPS / Anti-Virus service)**
- **Incident handling**
- **Anti-X services (Anti Virus, Anti-Spyware, Intrusion / Worms/ DOS attack prevention)**
- **Redundancy/failover**

Equant Intrusion Detection



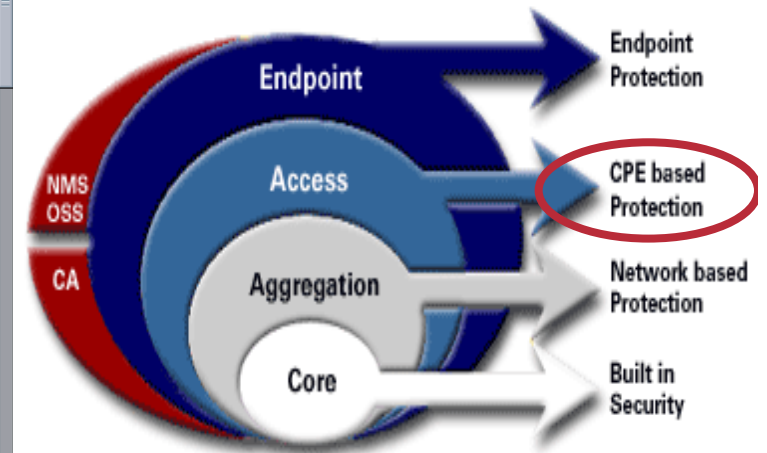
Equant Intrusion Detection

24x7 global surveillance and support

Detect, prevent and respond to unwanted intrusions that threaten your network. Equant Intrusion Detection is a managed, network-based security solution that can detect in near real-time malicious activity targeted at your networks, devices, appliances, servers and operating systems.

Key elements

- Helps to protect your resources through ongoing monitoring, management and incident response
- Features market-leading Cisco technology
- Goes one step further than automated response solutions to provide constant support by specialists at Security Operations Centers
- Guaranteed by service level agreements



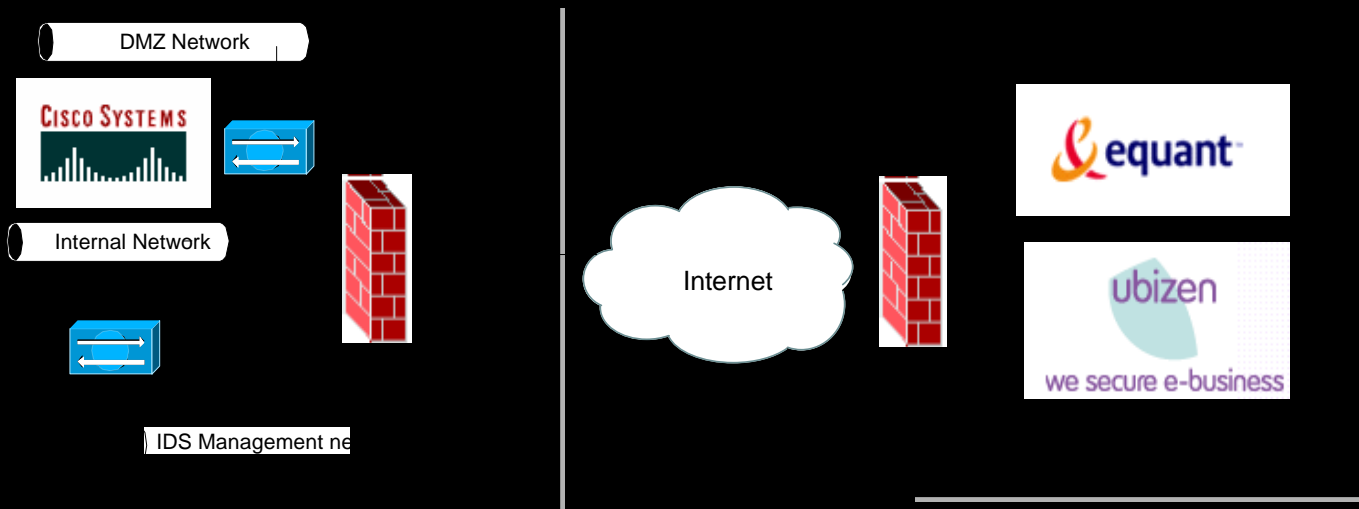
Equant Intrusion Detection cont'd

- Service is based on Cisco IDS/IPS appliances
- Monitoring and management is **provided by Ubizen (Cybertrust)**

Ubizen analyzes the IDS logs and identifies the threats that require immediate action

Customer benefits: real-time discovery of attacks with predictable turn-around time and consistent procedures; reduction of false alarms; lower TCO

Service is integrated with Equant delivery



Equant Intrusion Detection Service Profile

Who does what?

- **Done By Equant**
 - Professional consultancy engagement
 - **Device** Installation, Management and Monitoring
- **Done by Ubizen (under Equant branding)**
 - 24x7 Real-time intrusion monitoring
 - 24x7 Real-time event correlation & interpretation
 - 24x7 Incident handling
 - « Real-time » customer alerting and recommendations
 - Full Reporting capabilities
 - Real-time reports at Equant Intrusion Detection Report Center
 - Consolidated Monthly reports, SLA's

SP Managed IDS/IPS Service vs. In House

- **Benefits of Managed IDS/IPS**

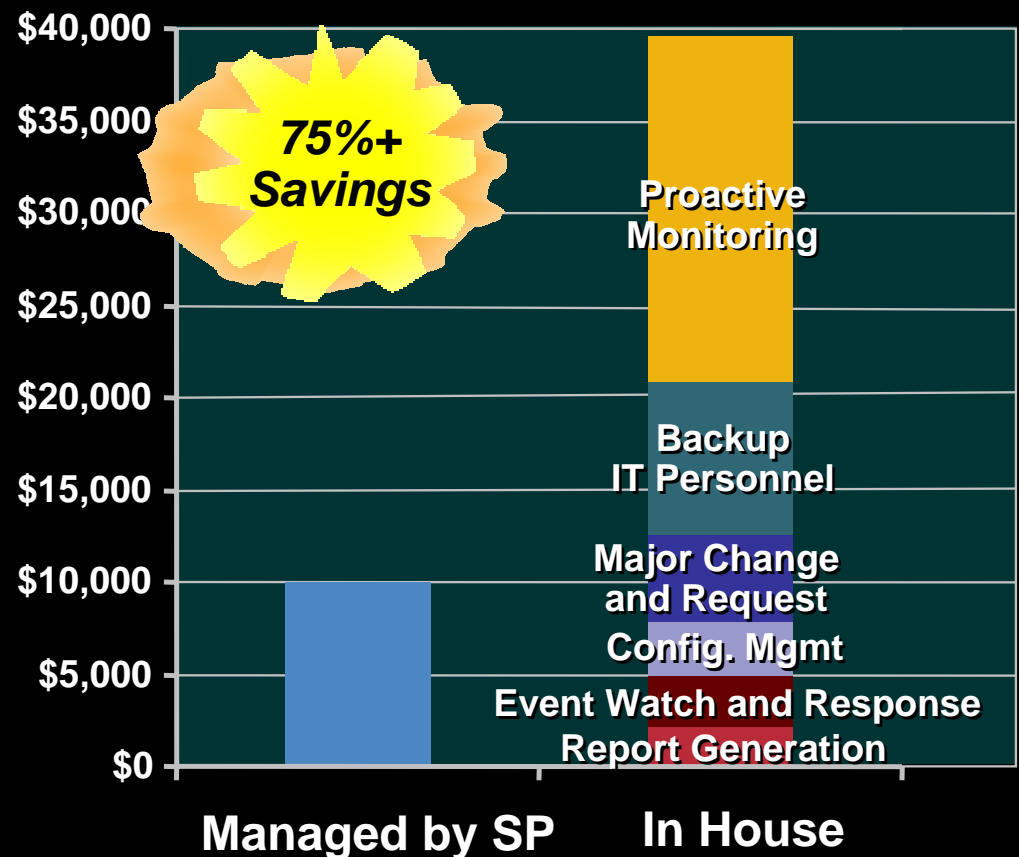
Reduced monthly recurring management cost (75%)

Increased network reliability (24-hour monitoring)

Lower implementation and training cost

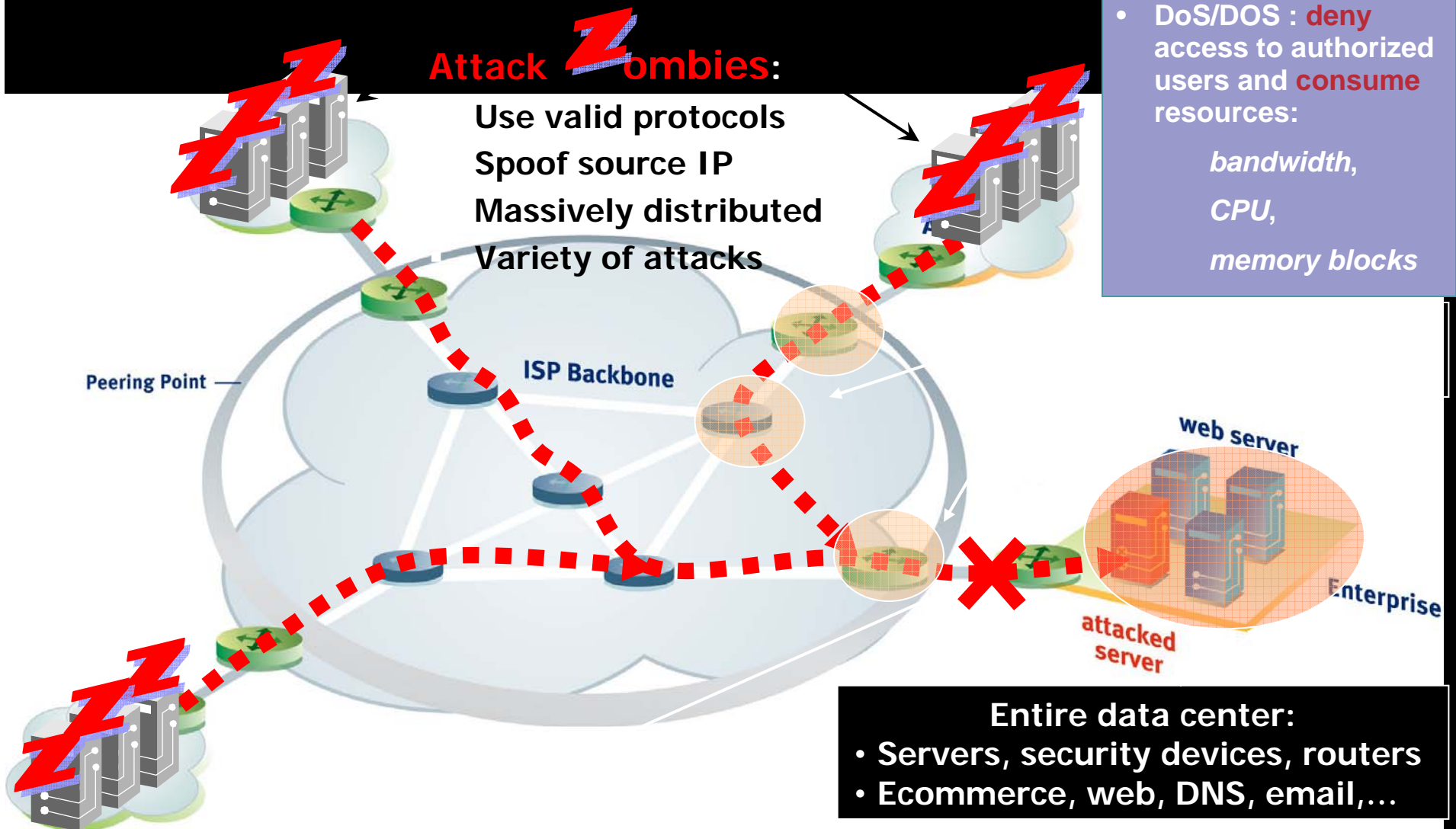
Flexibility to reallocate IT staff to strategic projects

Monthly Recurring Cost (4-IPS Sensors)



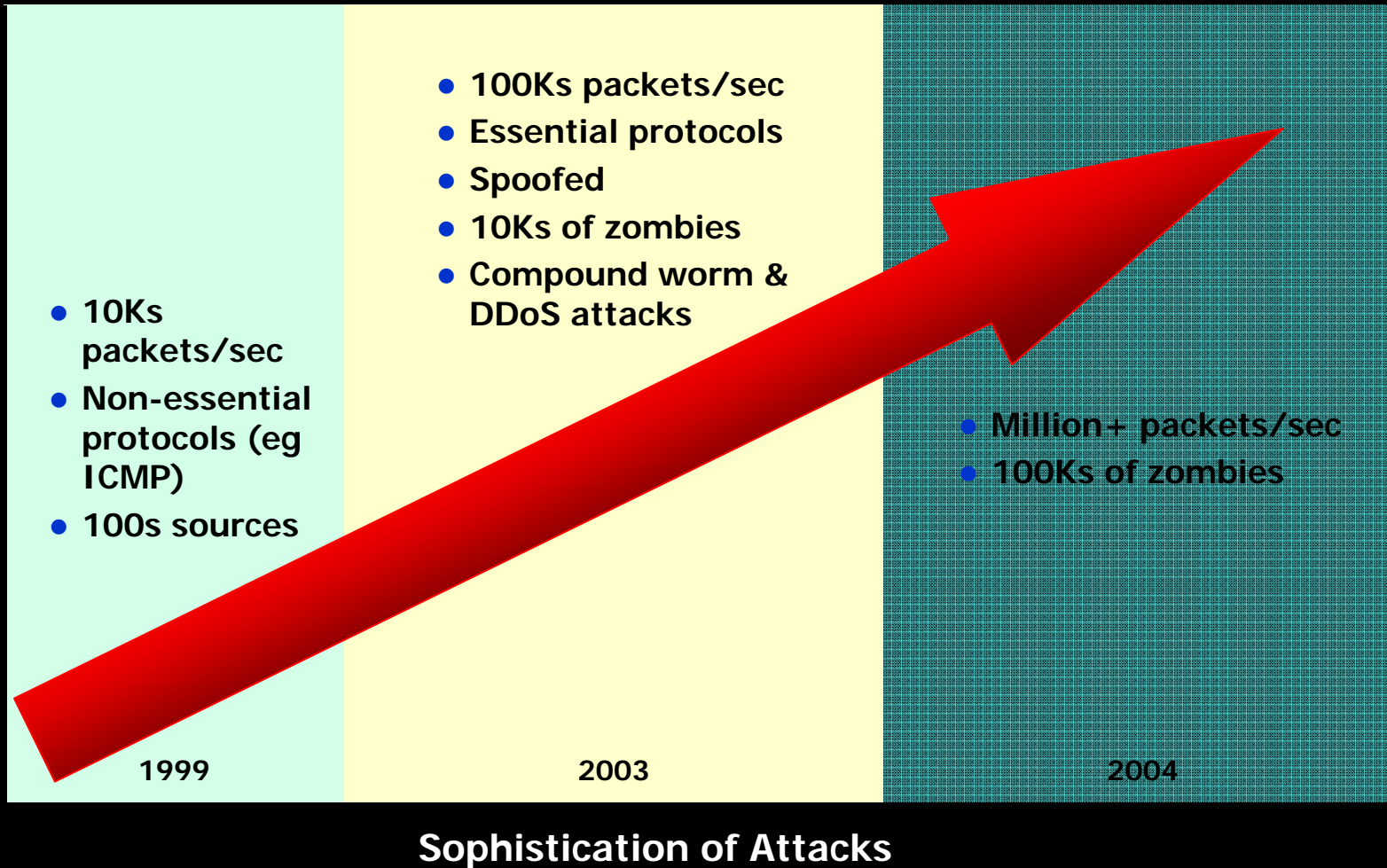
DoS/DDoS Attacks

Multiple Threats and Targets



Two Dimensions to DDoS: Number of Attacking Hosts, Total Bandwidth

Scale of Attacks

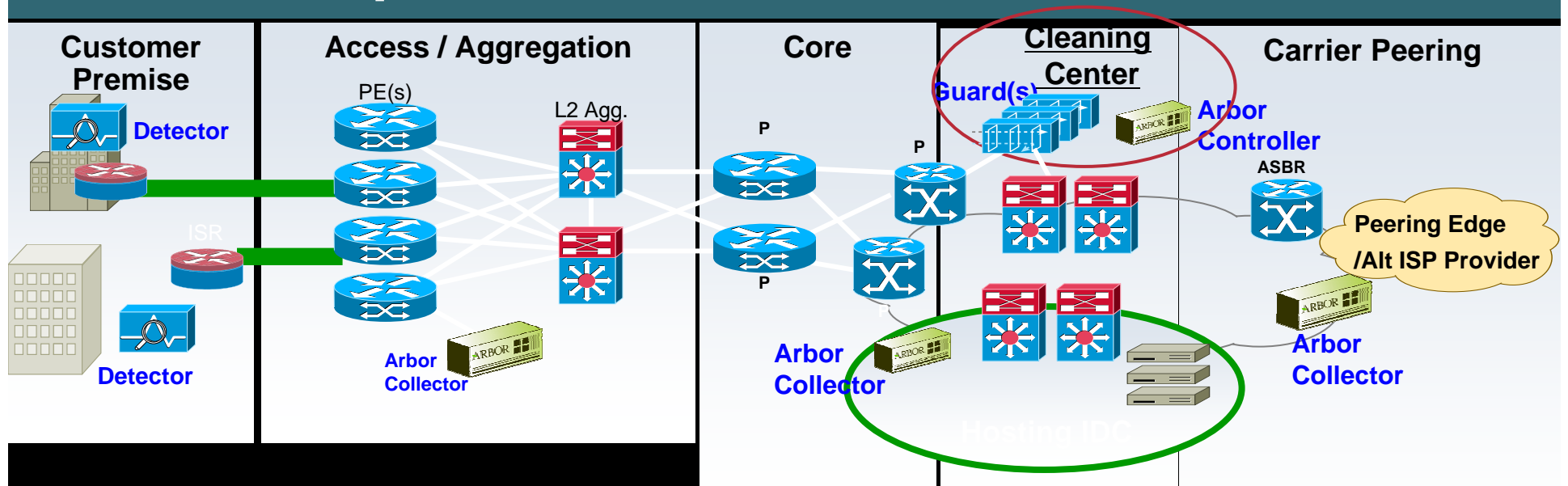


Analysts on DDoS

“Effective protection against DoS attacks rests in the hands of the ISPs providing the physical connection. E-businesses should demand quality-of-service statements from their ISPs requiring them to control a DoS attack.”

J. Pescatore and W. Malik from Gartner Group

Clean Pipes Solution Overview



Detection

Identify and classify attacks based on its characteristics.

Diversion/Injection

Divert “attack” traffic to the cleaning center to be “**scrubbed**”, inject clean traffic back to Enterprise customer

Mitigation

Anti-spoofing, anomaly recognition and packet inspection and cleaning (i.e. **scrubbing**) of “bad” traffic

Provisioning and Management – WBM for Guard/Detector, Controller based Mgmt for Arbor

Built on Cisco Network using Infrastructure Security “Best Common Practices”

Cisco Anomaly / DDoS Protection Solution

Detects and automatically mitigates the broadest range of Distributed Denial of Service (DDoS) attacks:

- Ensures legitimate transactions get through
 - Multiple defenses including source verification
 - Behavioral anomaly recognition engine
- Performance for largest enterprises and providers
 - On-demand diversion for attack scrubbing
 - 1Mpps+ per appliance and clustering capability

R3
Aug 04

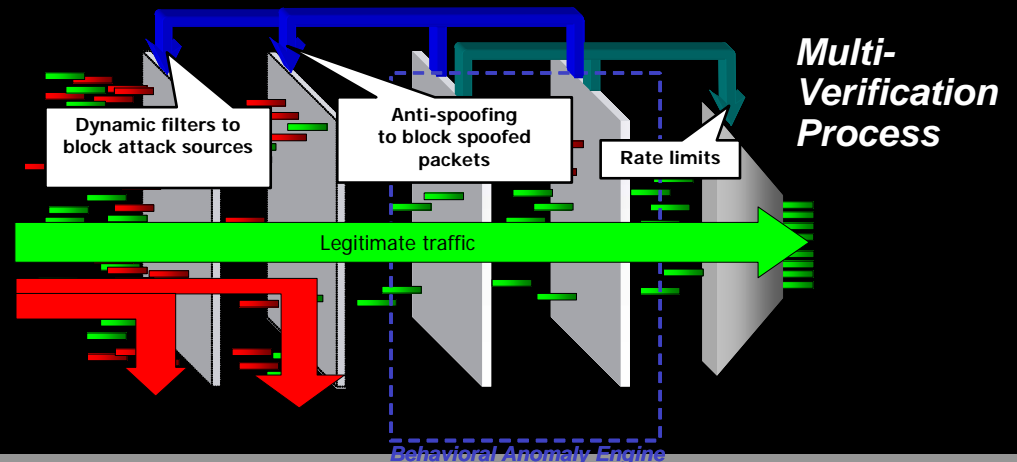
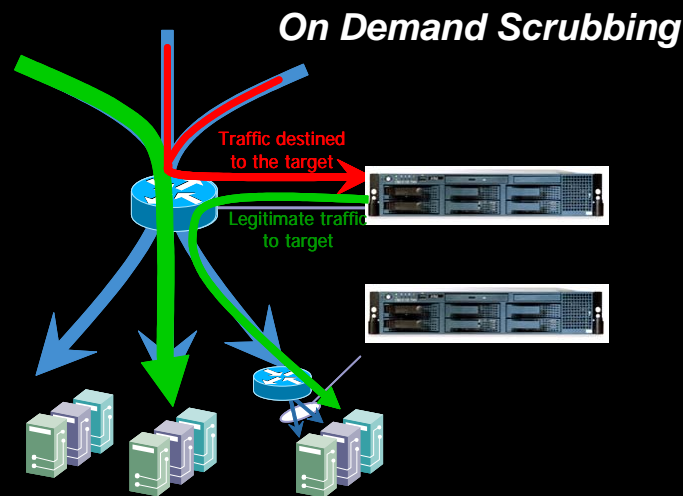


Cisco Guard XT 5650 &
Traffic Anomaly Detector XT 5600

R4
1QCY05



Cisco Catalyst 6500 / 7600
Anomaly Guard Module &
Traffic Anomaly Detector Module



SP Revenue Models

SUBSCRIPTION SERVICE - A

Customer pays X% of markup on transit/bandwidth purchased for guarantee of availability







SUBSCRIPTION SERVICE- B

Customer pays normal rates for transit/bandwidth, then pays extra flat fee for detection and mitigation (pricing subject to business model)

ON-DEMAND

Customer pays premium for 'scrubbed' bandwidth after calling during an attack (not seen often).

Managed DDoS Services Cisco Powered Providers

Customer	Service Name	Deployment Model	Scenario
AT&T 	DDoS Defense Option for Internet Protect managed services	Managed Network DDoS Protection Service	NetFlow + Arbor Peakflow SP + Guard
SPRINT 	IP Defender managed service	Managed Network DDoS Protection Service	Detector + Guard
Cable & Wireless 	DDoS Attack Mitigation Service	Managed Network DDoS Protection Service	Detector + Guard
Telecom Italia 	DDoS Peering Point Protection	Peering Edge DDoS Protection Service	NetFlow + Arbor Peakflow SP + Guard
Rackspace 	Preventier DDoS Mitigation service	Managed Hosting DDoS Protection Service	Arbor PeakflowSP + NetFlow Detector + Guard
DataPipe 	SureArmour DDoS protection service	Managed Hosting DDoS Protection Service	Detector + Guard

Endpoint Security

Cisco Security Agent

- **A new kind of Host Protection product for desktop, laptop, & server computers**
 - Windows NT, Windows 2000, Windows XP, Solaris 2.8, Linux
 - Aggregates multiple security functions in one agent
- **Shift from Signature-based to **Policy-Based****
 - Effective against existing & previously unseen attacks
 - Stopped Slammer, nimda & code red sight unseen with out-of-the-box policies
- **Centrally administered, with distributed, autonomous policy enforcement**
 - Scales well & also works with intermittently connected hosts
 - Can also adapt defenses based upon correlation of events from different hosts

Definition of active endpoint protection

What is Cisco Security Agent ?

**Personal
Firewall**

**Personal Data
protection**



**OS
Hardening
tool**

**Distributed
IPS**

Server & Desktop Protection

CSA Aggregates Multiple Endpoint Security Functions

	CSA	Conventional Distributed Firewall	Conventional Host-based IDS
Desktop/Laptop Protection	✓	✓	
Block Incoming Network Requests	✓	✓	
Block Outgoing Network Requests	✓	✓	
Stateful Packet Analysis	✓	✓	
Detect /Block Port Scans	✓	✓	
Detect /Block Network DoS Attacks	✓	✓	
Detect /Prevent Malicious Applications	✓		✓
Detect/Prevent Known Buffer Overflows	✓		✓
Detect/Prevent Unknown Buffer Overflows	✓		✓
Detect/Prevent Unauthorized File Modification	✓		✓
Operating System Lockdown	✓		✓

CSA Complements Traditional Desktop AV

	CSA	Anti-Virus
Malicious Code Protection		
Stop Known Virus/Worm Propagation	✓	✓
Stop Unknown Virus/Worm Propagation	✓	
Scan/Detect Infected Files		✓
“Clean” Infected Files		✓
Identify Viruses/Worms by Name		✓
No Signature Updates Required	✓	
Distributed Firewall Functionality	✓	
Operating System Lockdown	✓	
Correlates Events Across Endpoints	✓	

Managed CSA Value Proposition

- **Lower Operating Costs**

Remove monitoring/maintenance tasks, remove need for hiring/training of security experts

- **Higher Level of Security**

MSSP has more extensive IT resources, 24x7x365 protection of systems, **reduced implementation time, and faster resolution for security incidents**

- **Reduced False Positives**

MSSP has extensive knowledge of **best practices** to customize the technology

- **Increased Security Posture Awareness**

MSSPs offer real-time and historical perspectives of device security easily accessible via the web

Which SPs could offer Managed CSA?

- **If you already have existing know-how/infrastructure to support IDS services**
 - Similar type of service – define policies, implement, monitor and correlate events, tune....
- **Do not necessarily need to be involved in “desktop management” if the customer has the resources to do this**
- **Probably best to partner with an established MSSP e.g. Ubizen?**

Managed Trust and Identity



Cisco Network Admission Control (NAC)

- **Restricts and Controls Network Access**

Endpoint device interrogated for policy compliance

Network determines appropriate admission enforcement: permit, deny, quarantine, restrict

- **Cisco-led, Multi-partner Program**

Limits damage from viruses & worms

Coalition of market leading vendors

- **A Cisco Self-Defending Network Initiative**

Dramatically improves network's ability to identify, prevent, and adapt to threats

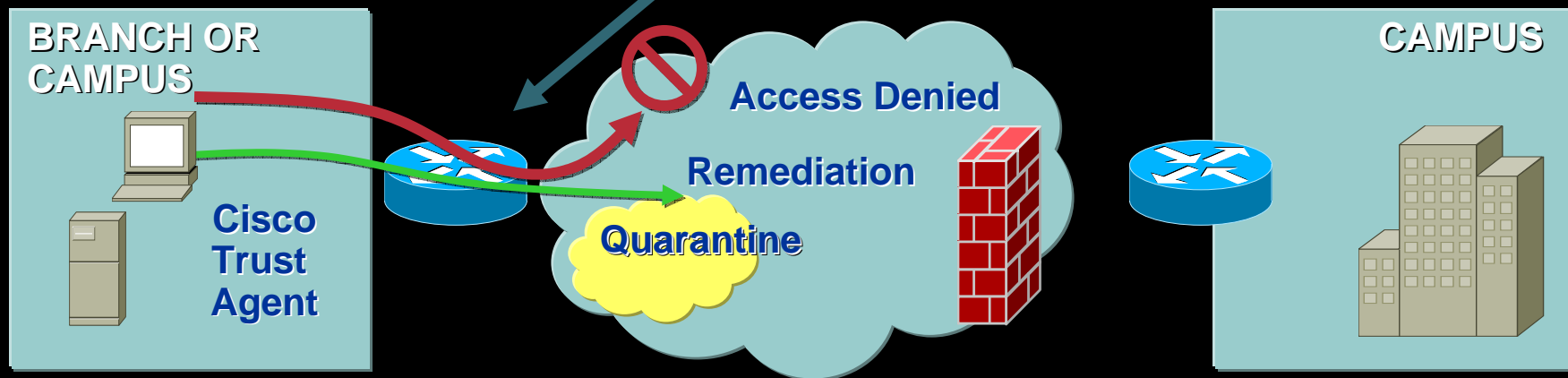


Cisco Network Admission Control: What It Does

1. Non-compliant endpoint attempts connection

2. Non-compliant status determined

3. Infection contained; endpoints secured



NAC Customer Benefits

- **Dramatically improved security**

 - **Proactive protection against worms & viruses**

 - **Leverage the network to audit & enforce host security policies**

 - **Network segmentation services for isolation and remediation**

- **Extend existing investment**

 - **Leverage investment in network infrastructure and host security**

 - **Focus operations on prevention, not reaction**

- **Increase enterprise resilience**

 - **Comprehensive admission control across all access methods**

 - **Ensure endpoints conform to security policy**

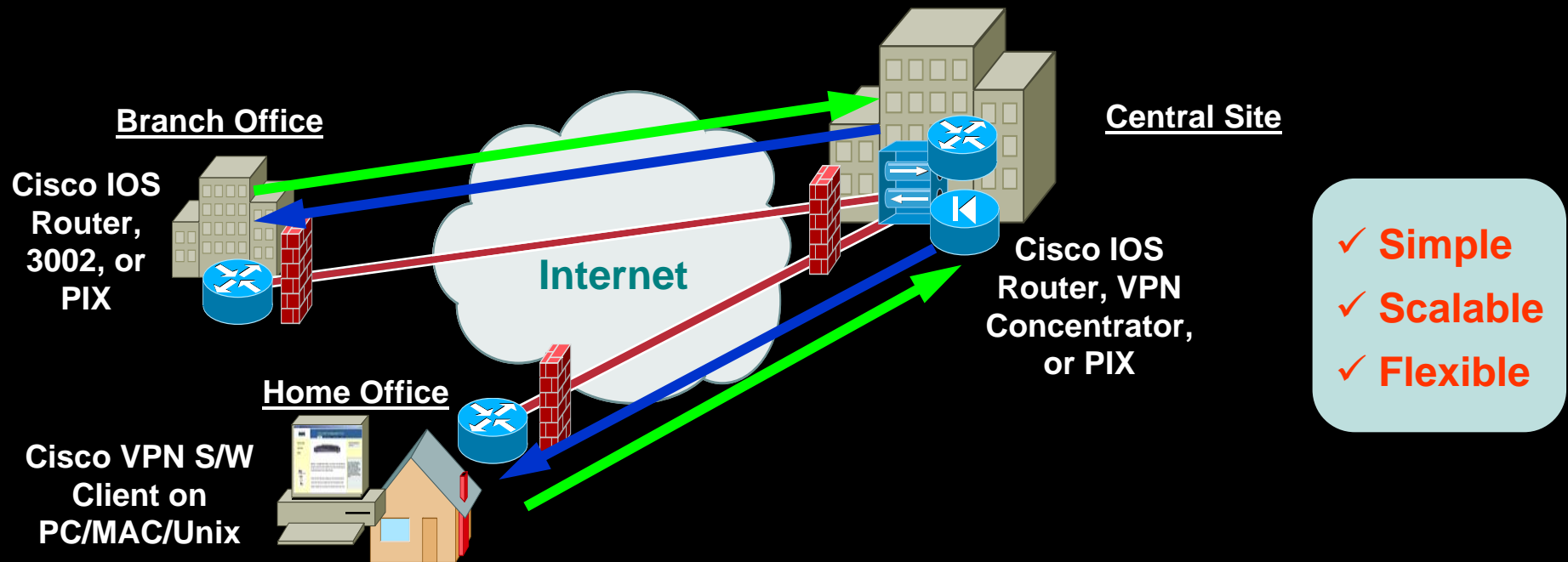


Secure Connectivity



Secure Connectivity

Easy VPN



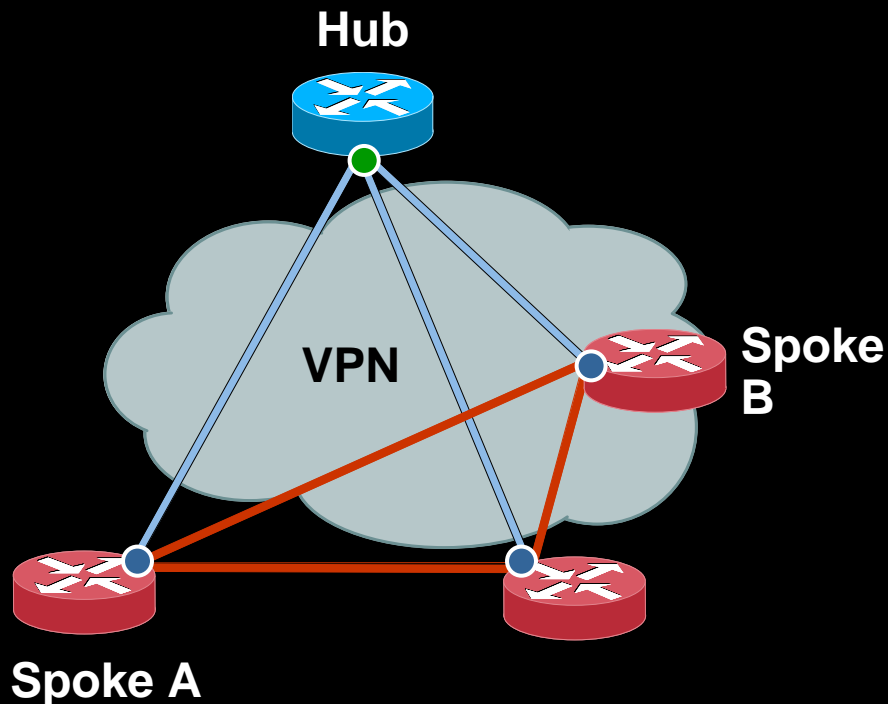
- ✓ Simple
- ✓ Scalable
- ✓ Flexible

- Remote/branch device can be a PIX, IOS router, 3002, or Cisco client software on a PC/Mac/Unix computer.
- Remote device contacts central-site router/concentrator, and provides authentication credentials.
- If credentials are valid, central-site “pushes” configuration data securely to the remote device and VPN is established.

Secure Connectivity

Dynamic Multipoint VPN (DMVPN)

Secure Meshed Tunnels Automatically!

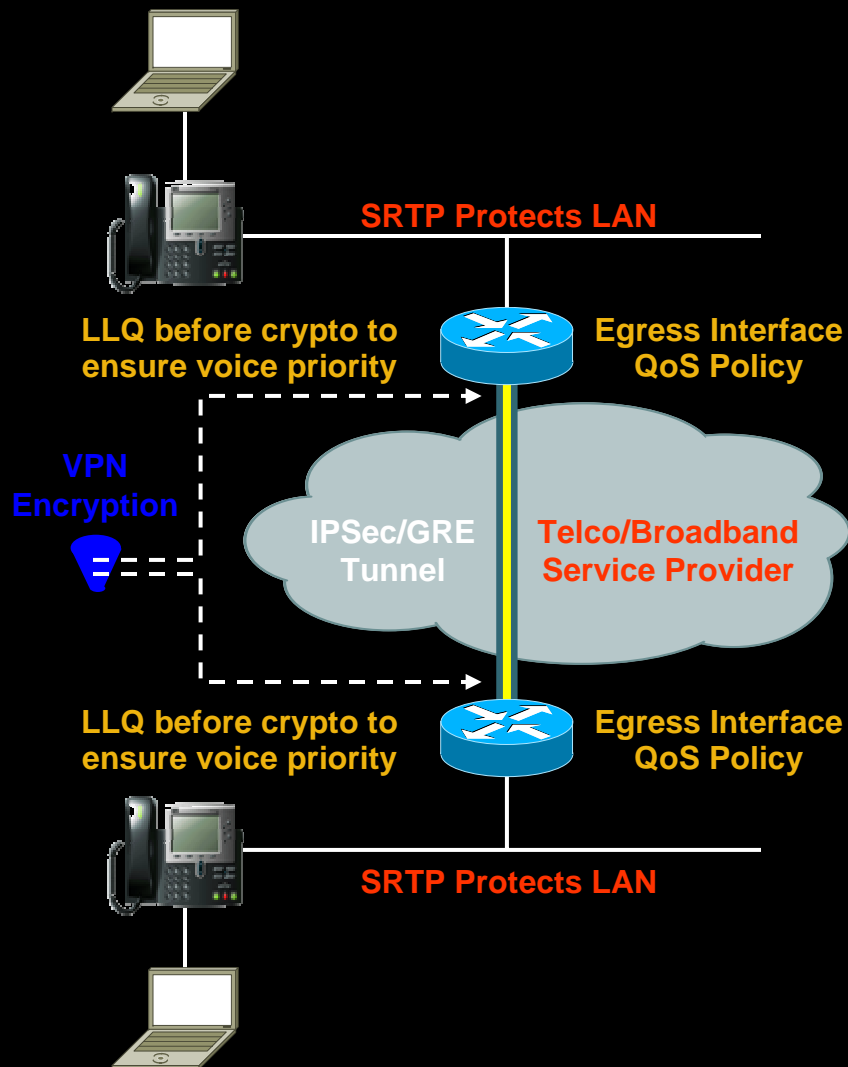


Benefits:

- Full Meshed connectivity with configuration simplicity of hub and spoke
- Preserves (central) bandwidth, minimizes latency
- Support for dynamically addressed spokes
- Zero touch configuration for addition of new spokes in the DMVPN

Secure Connectivity

V3PN: Secure, Toll Quality Voice, Video, Data

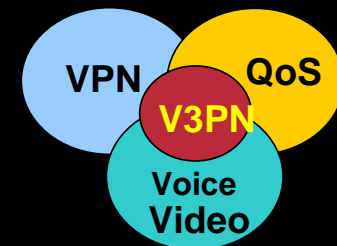


V3PN:

- **Data, voice and video** traffic delivered with **QoS** policies for latency sensitive traffic

Benefits:

- Wirespeed encryption
- Bandwidth conservation
- Toll quality, jitter-free voice and video
- LAN and WAN security



SSL VPN and IPsec

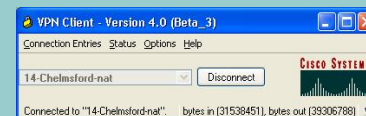
Connectivity Profiles

SSL VPN



- Uses a standard web browser to access the corporate network
- SSL encryption native to browser provides transport security
- Applications accessed through browser portal
- Limited client/server applications accessed using applets

IPSEC VPN



- Uses purpose-built client software for network access
- Client provides encryption and desktop security
- Client establishes seamless connection to network
- All applications are accessible through their native interface

SSL VPN

Deployment Environments

SSL VPN



- Anywhere access
- Access from non-corporate machines
- Customized user portals
- Granular access control
- Easy firewall traversal from any location

DEPLOYMENTS

- Unmanaged desktops
 - Extranets
 - Employee-owned computers
- “Lite” users
 - Employees who only need occasional access
 - Employees who need access to few applications
- Simple or locked-down access
 - Restricted server and application access by population



poweredbycisco.
networkers
2005

December 12 – 15
Cannes, France

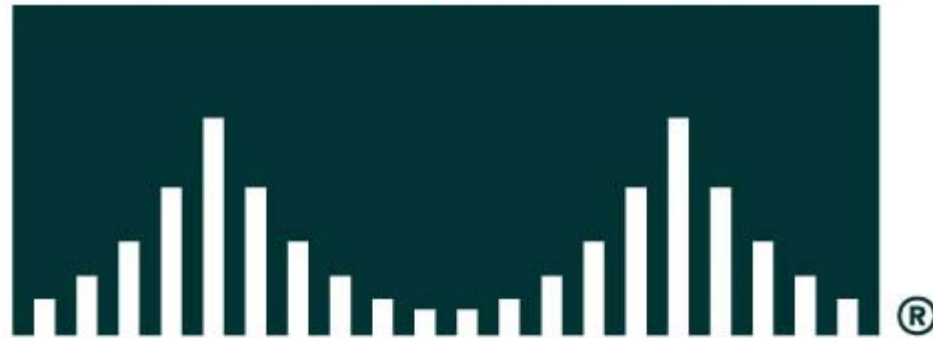
**Building the Intelligent
Information Network**



Session Number
Presentation ID

© 2005 Cisco Systems, Inc. All rights reserved.

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATION