Network Security

Defense-in-Depth

By

Dilum Bandara

Certified System Professional WatchGuard

Certified Server Security Expert WatchGuard

Objective

- To provide an overview of security threats in a networked environment , countermeasures & relating technologies

Threats

- Viruses/Worms
- Buffer Overflow
- Denial of service (DoS)
- Spoofing & Sniffing
- Address/Port scanning
- Hacking
- Trojan horses
- Logic Bombs
- Trap Doors

Covered Today

Outline

- Security risk
- Defense-in-Depth
- Threats in more detail
- Counter measures
- Firewalls
- Server Protection
- Enterprise level antiviral solutions
- Security Vs Sri Lanka
- Demo

Risk

- Hackers are getting smarter
- They don’t need to be TCP/IP guru
- Enough tools are freely available
- More badly – they don’t have idea of what they are doing

- The security chain is only as strong as its weakest link - users

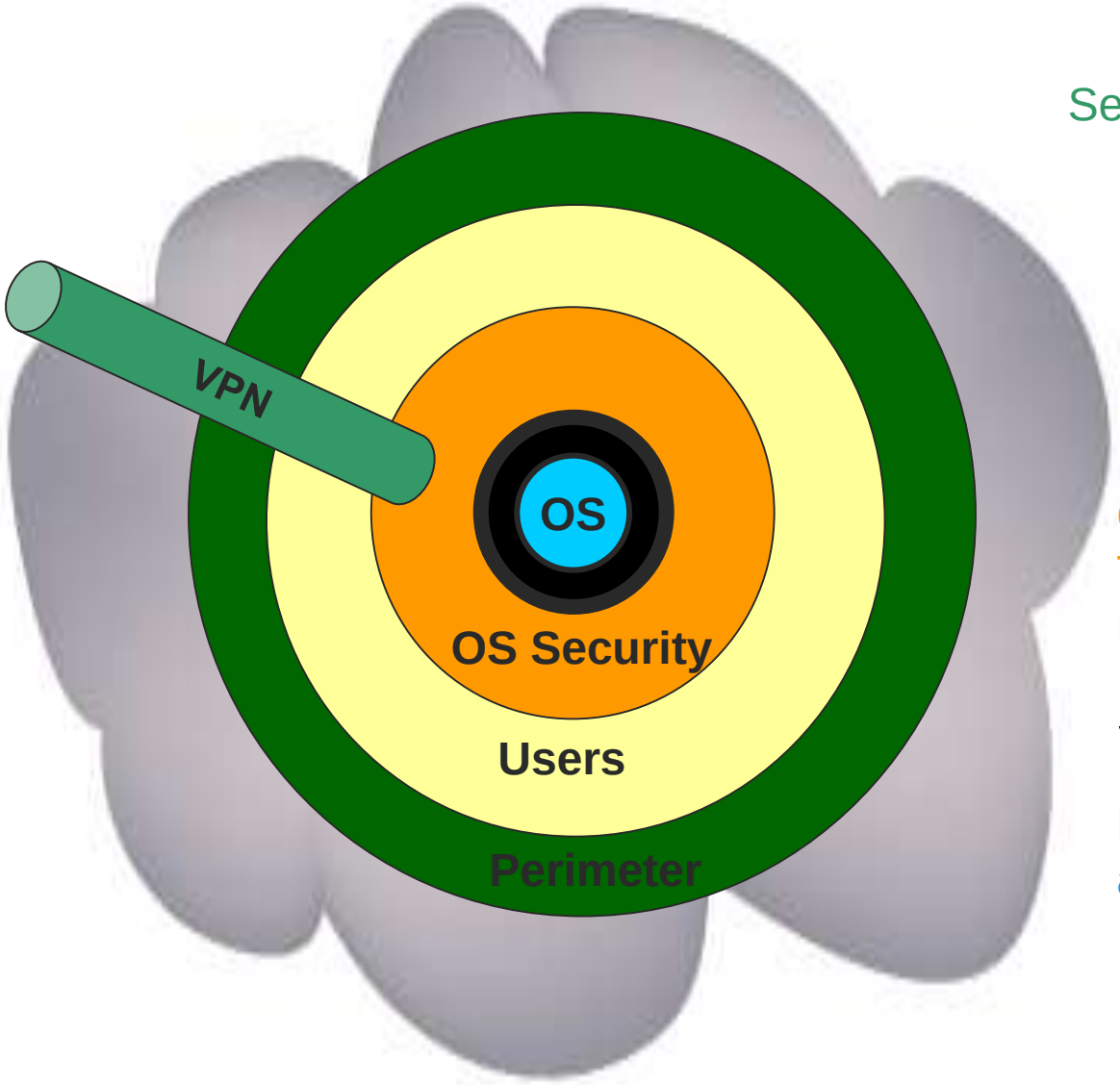
Who should be concerned?

- Any 1 who has access to Internet
- Regardless of their size
  - Every 1 in 2 small business will be hacked in end of 2003
- 60% of companies won’t be aware until serious damage happens

Defense-in-Depth

- No single product could deliver all
- It is advisable to combine
  - Awareness and Commitment
  - Firewall
  - Network and System Monitoring
  - Access Control & Authentication
  - Anti-Virus
  - Encryption
  - VPN
  - Server Integrity
  - Auditing

illustrated…



Secured Private Communications

Firewalls
Intrusion Detection
Perimeter Anti-Viral

Internal Users and Dial-up Access

OS Authentication
Trusted OS Access Control
Host-Based Anti-Viral

Server Security

Files, Directories, Applications and Configuration Settings

Total access Vs no access

- User wants world to be at their fingertip
- Sys Admin want to stop as much as
- The best way to survive is to have no access

- We need a compromise
  - Answer is :

Security Policy

Security Policy

- I need to protect things but how?
- Security policy is a compromise that organization decides to adopt between absolute security & absolute access
  - Who can get in/out
  - Where they can go
  - When they can get in/out
  - What they can bring in/carry out
  - **Physical access**
  - Protecting management station

Security should be from your door step to the Internet gateway

If there is a open door

surely some one will probe in

Benefits of a policy

User is the key

- Users gain a sense that the organization is looking out to protect their files and their livelihood
- Users often find that they have access freedoms they were not previously aware of
- Users gain an understanding that access limitations are implemented to protect the organization from disaster

Done?

- I published the policy
- I have all the necessary devices
- My virus guard gets updated automatic

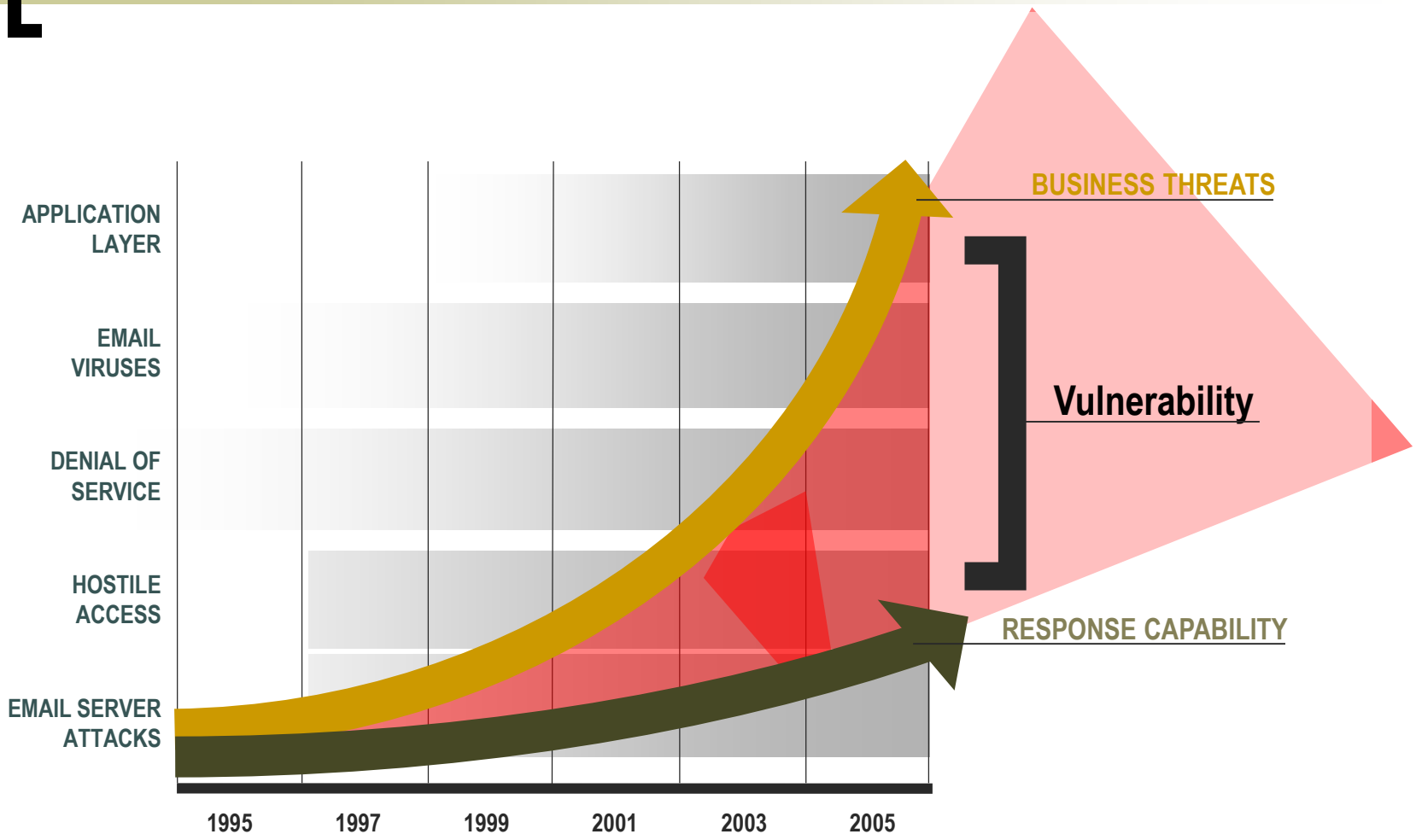
Hahaha….I’m Secure!!!

No, wait
I’ll show you another magic

Why?

- Security is a dynamic process
- Its like a Cricket match
  - When one hacker goes off another hacker of a different style comes to bat
- Not a 1 step solution
- So you are never done
- It needs lot of vigilance & maintenance

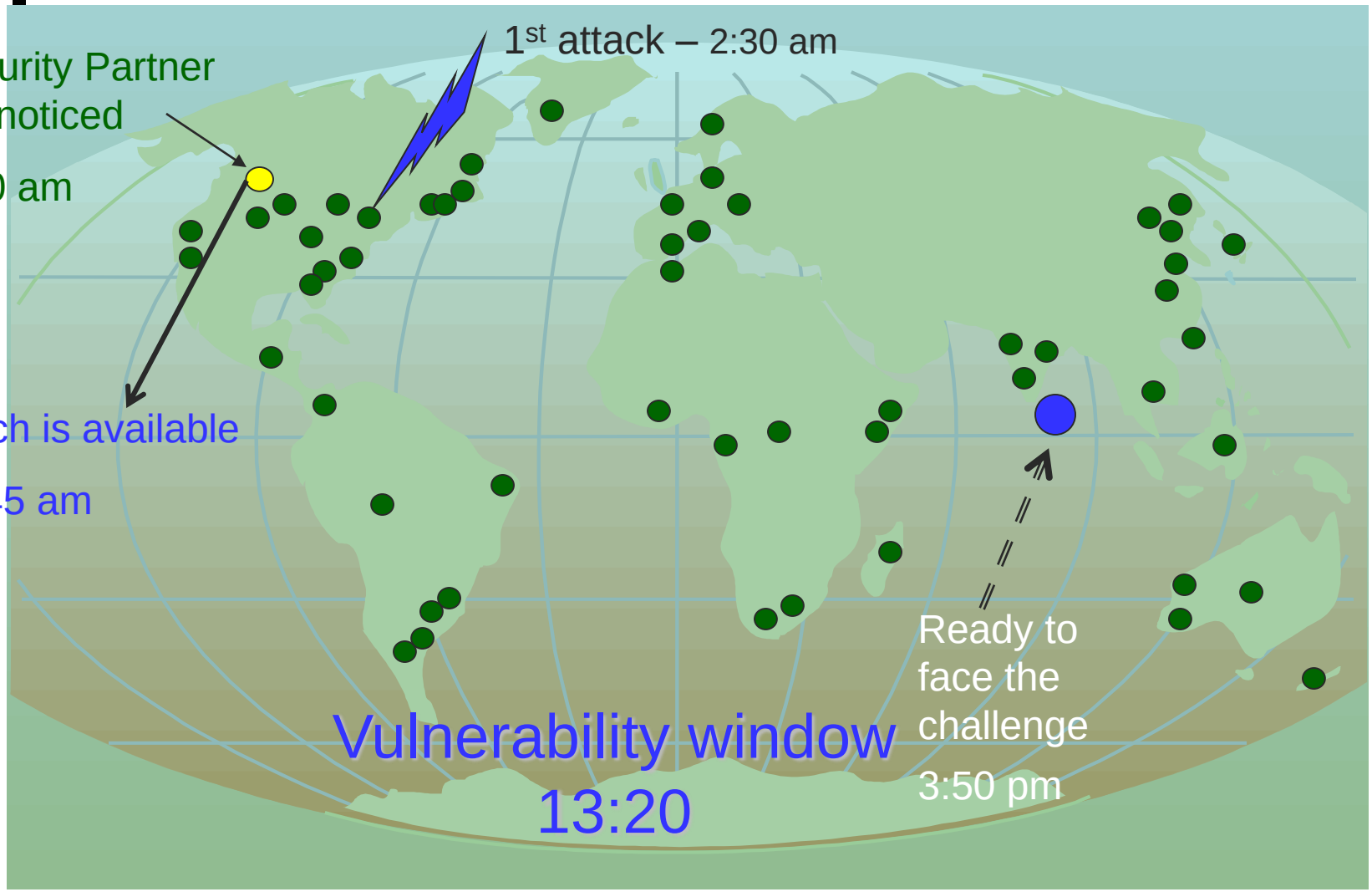
The growing Vulnerability gap



Vulnerability Window

- Is the time gap between 1st attack and until you get ready to face it
- Indicate how vulnerable you are
- Higher the window size more vulnerable you are

Illustration – Time in GMT



Narrowband Vs Broadband

- Narrowband
  - Dial-up
  - Dynamic IPs
- Broadband
  - Always connect
  - Static IPs
  - Door is always open

But….

- Neither is secure
- Because
  - Example:

    FBI’s Carnivore machine

Terminology

- Hacker – people who get in but no harm (or help for better security)
- Cracker – people who get in & do harm
- Hacking – unauthorized probing
- Cracking – applying patches to software for illegal registration

DoS attacks

- Denial of Service
- Degrade performance or crash the server
  - Ping of Death
  - SYN Flooding
  - Ping Flood ←→ Smurf Attacks
  - Buffer Overflow
  - Exploiting the CGI

Ping of Death

- Exploits bugs on UNIX, Windows, MacOS
- Host crashes when large Ping packet arrives (ICMP Echo > 64KB)

- Solution
  - OS patch can correct the problem
  - No longer an attack

SYN Flooding

- Make use of TCP 3 way handshaking
- Use unavailable IP address

- Solution
  - No solution
  - Minimize
    - the no of uncompleted connections
    - the validation timeout

Ping Flood & Smurf Attacks

- Send large number of Pings to the host same time
- Send large number of pings as coming from the host
- Solution
  - Configure routers, NATing device or Firewall

Buffer Overflow

- Caused when more data is given to a program than that it can handle
- Extra data contains malicious code
- If overwrite system memory area could execute easily
- E.g. Nimda, Code Red II

- Solution
  - Protect the stack buffer

Exploiting the CGI

- If program blindly accept request from browser, could provide access to shell
- With privileges of CGI program
  - E.g.

```
http://fake.name.com/cgi-
    bin/name.cgi?fgdn=%Acat%20/etc/passwd
```

- Solution
  - Filter unwanted commands
  - Remove the shell

Address/Port probing

- Sequential search of IP address with open ports
- Then exploit vulnerabilities of programs
- Make use of running Trojan horses
  - Back Orifice

- Solution
  - Stateful packet filtering

Port scanning how?

- TCP SYN scanning
  - Send a packet with SYN to initiate a connection
  - If reply comes with SYN ACK port is open
- TCP FIN Scanning
  - Send a FIN (finish) to host
  - If reply with RST (reset) comes port is open

Use of IP Options

- Use of Optional header in IP header
- Used for testing purposes
  - Source routing
- If any authentication is done according to the path ???

- Solution
  - Block all packet with optional header

Spoofing attacks

- Use of false identity to cheat the server, router or firewall and gain access
- E.g. sending external packet with internal source IP

- Solution
  - Block at the router, NAT or firewall
  - Both incoming & outgoing

Solutions

- ID (Intruder Detection)
- Firewalls
- NAT
- VPN
- URL filtering
- DMZ
- Server Protection
- Antiviral solutions

ID (Intruder Detection)

- Use all sorts of login to check for vulnerabilities
- Cannot prevent attack but could detect after or when immerging
- Too complicated, need lot of vigilance
- Passive security

IP (Intruder Prevention)

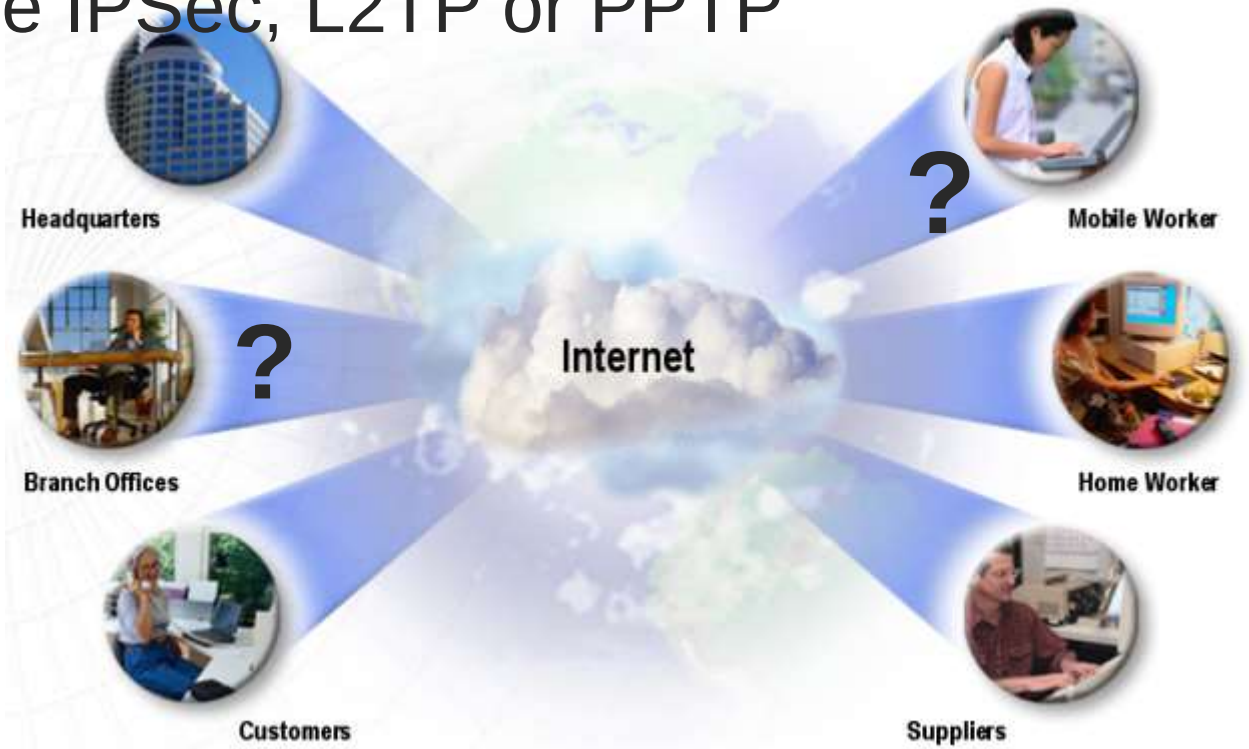
- Prevent before it happens
- Active security
- Need more processing power
- Methods
  - Protocol anomaly detection
  - Signature based detection
  - Behavior based detection
- Prevention is better than detection

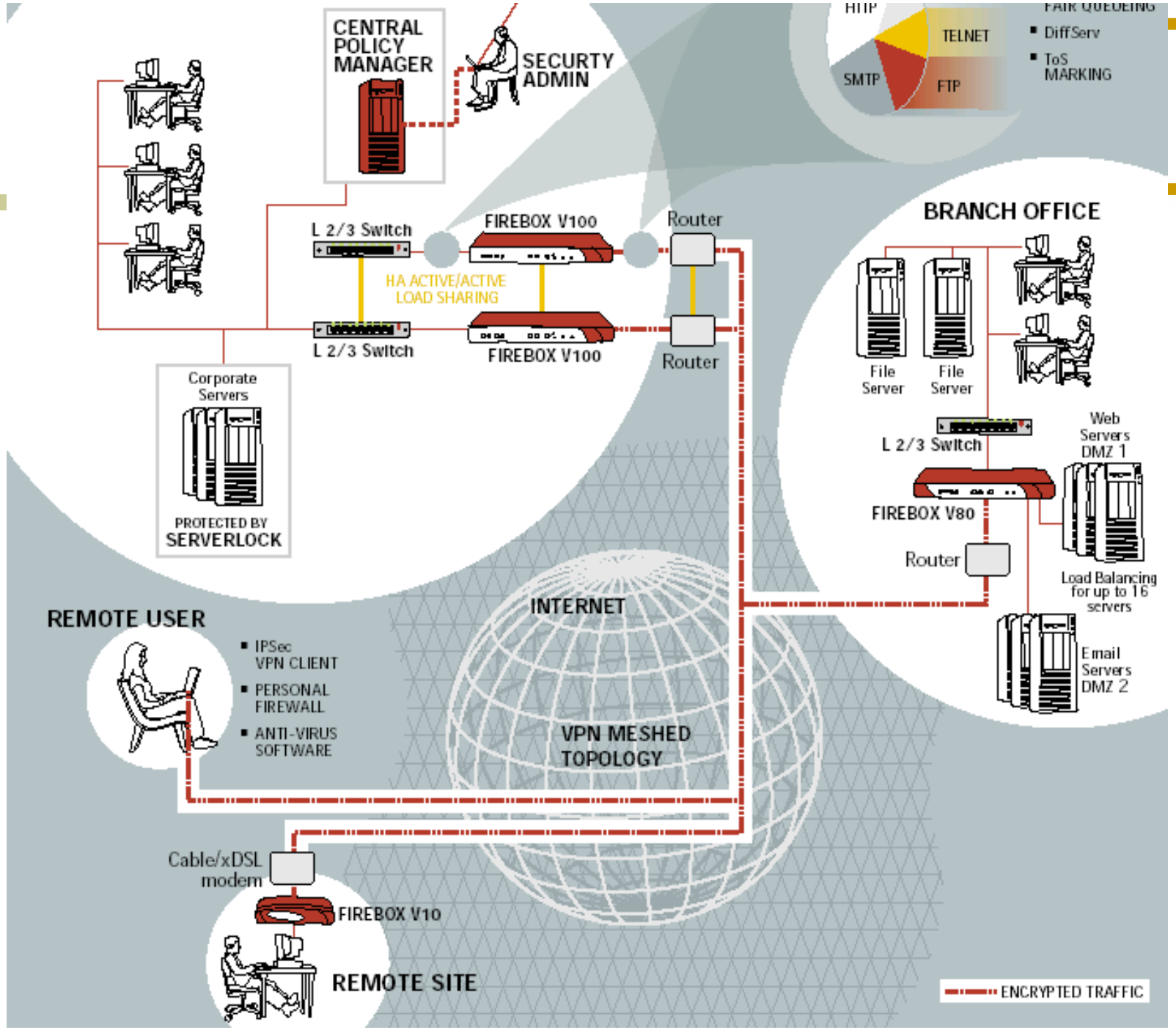
NAT (Network Address Translation)

- IP masquerading or port forwarding
- Take address from one network & translate to a IP address of another
- Hides hosts of one network from others
  - Dynamic NAT
  - 1-to-1 NAT
  - Static NAT

VPN (Virtual Private Network)

- Gives you a private path (channel) in a public path
- End to end encrypted
- Use IPSec, L2TP or PPTP




CENTRAL POLICY MANAGER
SECURTY ADMIN
HTTP
TELNET
SMTP
FTP
FAIR QUEUEING
DiffServ
ToS MARKING
L 2/3 Switch
FIREBOX V100
Router
HA ACTIVE/ACTIVE LOAD SHARING
L 2/3 Switch
FIREBOX V100
Router
BRANCH OFFICE
File Server
File Server
L 2/3 Switch
Web Servers DMZ 1
FIREBOX V80
Router
Load Balancing for up to 16 servers
Email Servers DMZ 2
Corporate Servers
PROTECTED BY SERVERLOCK
INTERNET
VPN MESHED TOPOLOGY
REMOTE USER
IPSec VPN CLIENT
PERSONAL FIREWALL
ANTI-VIRUS SOFTWARE
Cable/xDSL modem
FIREBOX V10
REMOTE SITE
ENCRYPTED TRAFFIC

VPN Cont….

- Overhead of encryption is too much – need lot of processing power
- Bandwidth of high speed connections would drop dramatically
- If VPN server to be use it should be dedicated

Firebox® 4500
200 Mbps firewall/100Mbps VPN

Firebox® 2500
200 Mbps firewall/75Mbps VPN

Firebox® 1000
200 Mbps firewall/60Mbps VPN

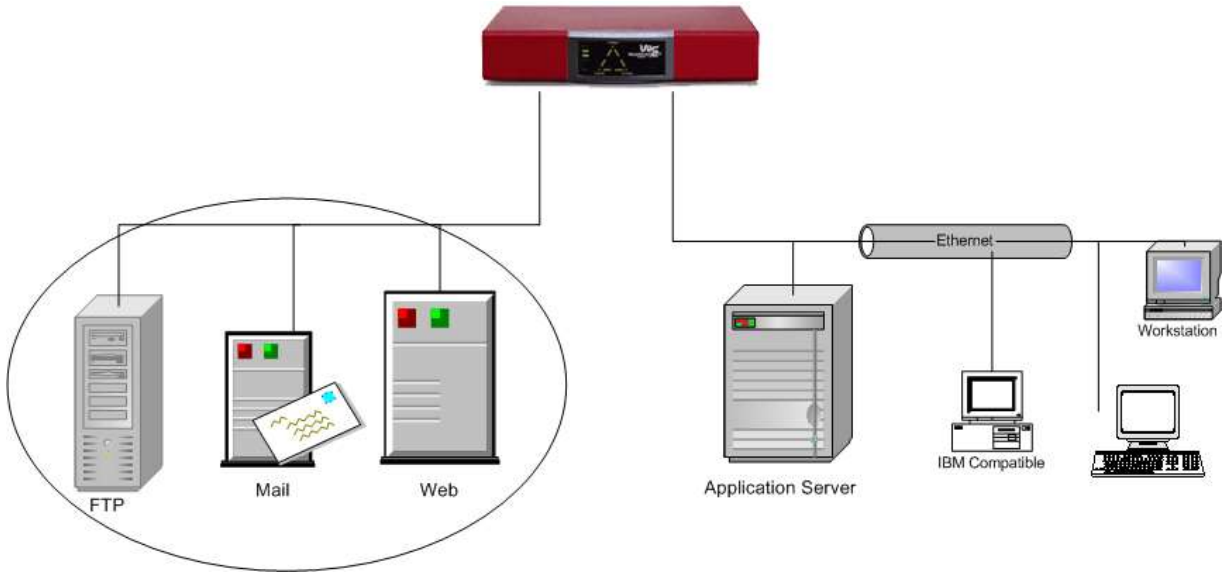
Firebox® 700
150 Mbps firewall/5Mbps VPN

URL Filtering

- Filtering of web pages against a filtering database
- Database is controlled by 3rd party
- You can add your own sites or exceptions
- Filtering is based on user, user group, time of the day, etc.

DMZ (Demilitarized Zone)

- Place where you keep your publicly available servers
- Separate from other local hosts and application servers
- Provides better security

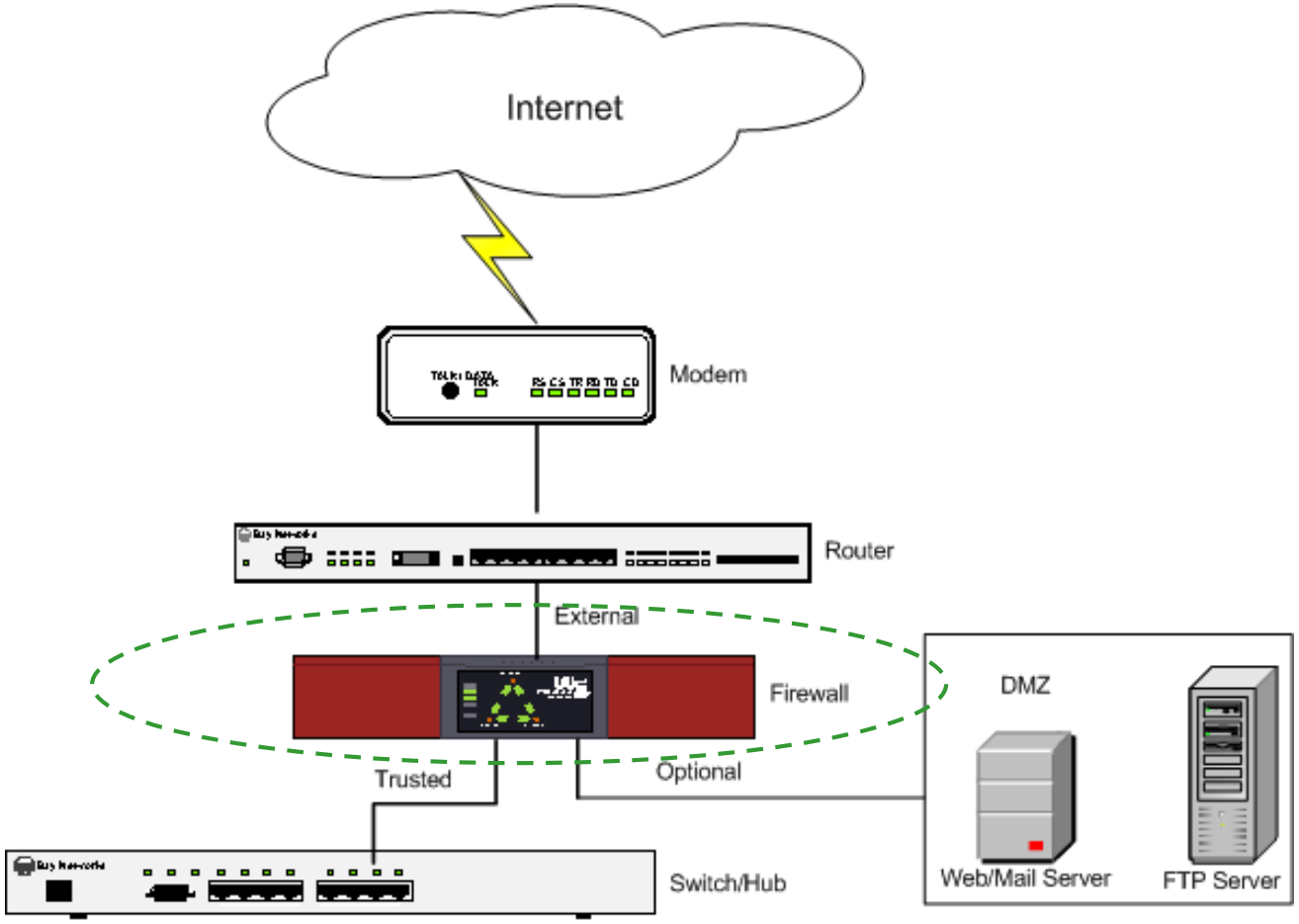


Firewalls

- Device which protects resources of private network from **outside** intrusions
- Firewall examines each packet passes through it against assigned set of rules
- Not a virus guard

- Stance
  - Stance dictates what firewall does when absence of a rule
  - Stance is to block everything unless specifically allowed

Where does it fits in



Interfaces

- External Interface
  - connection to external interface (typically Internet)
- Trusted Interface
  - connection to internal interface which needs maximum protection
- Optional Interface
  - connection to DMZ or free areas. Public Web, e-mail FTP, DNS servers could be connected here

Firewall Security Policy

- Which
  - hosts send/receive which kinds of traffic
  - communication links require authentication and/or encryption
  - users are authorized to use various services through the Firewall
- What
  - communication protocols and content types are allowed
  - times of day organization members are able to browse the Web
  - types of Web sites organization members can visit

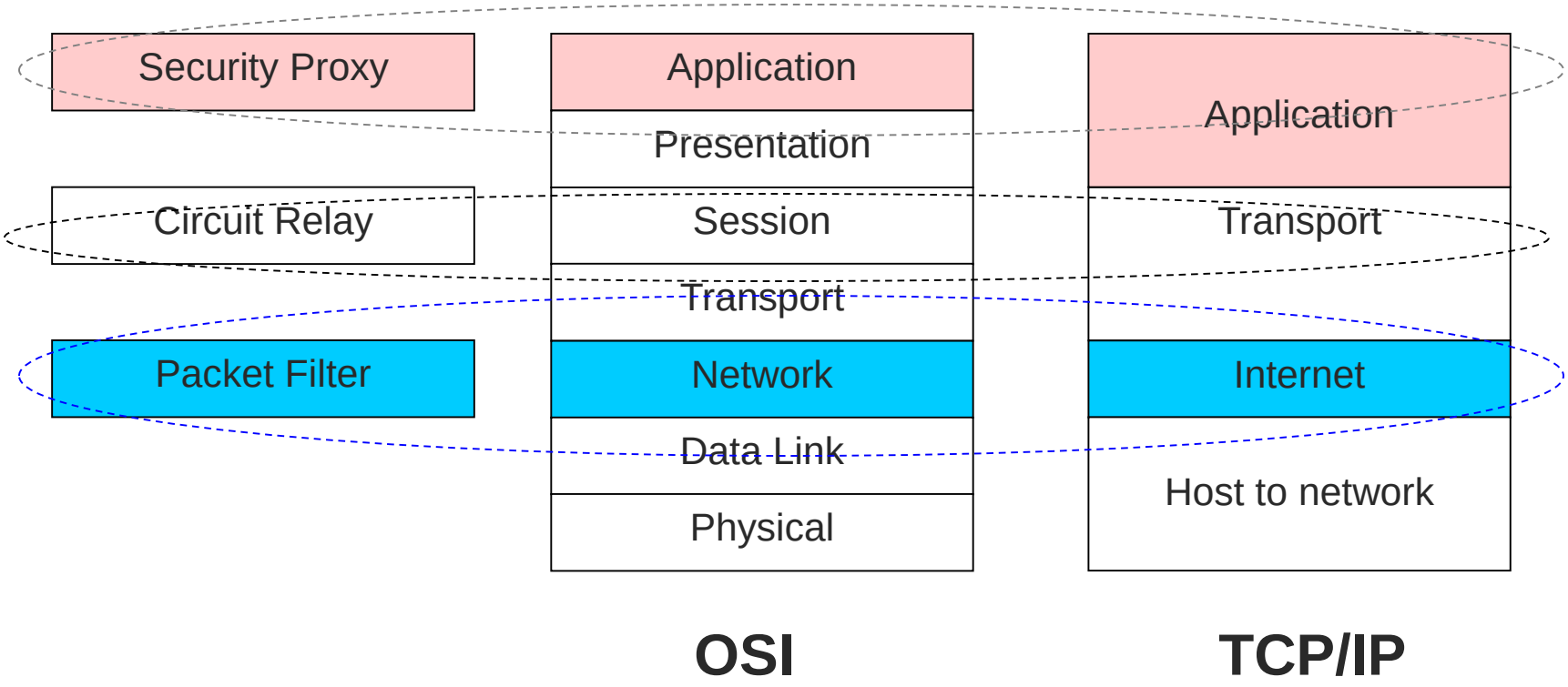
Technology – Packet filtering

- Based on the header information
- Incoming & outgoing packets are treated separately
- Filter packets bases on
  - IP address, Port, Protocol, Type of service
- Works on Network & Transport layers
- Very effective but can not detect (stateless) attacks like DoS

Technology – Circuit Relay

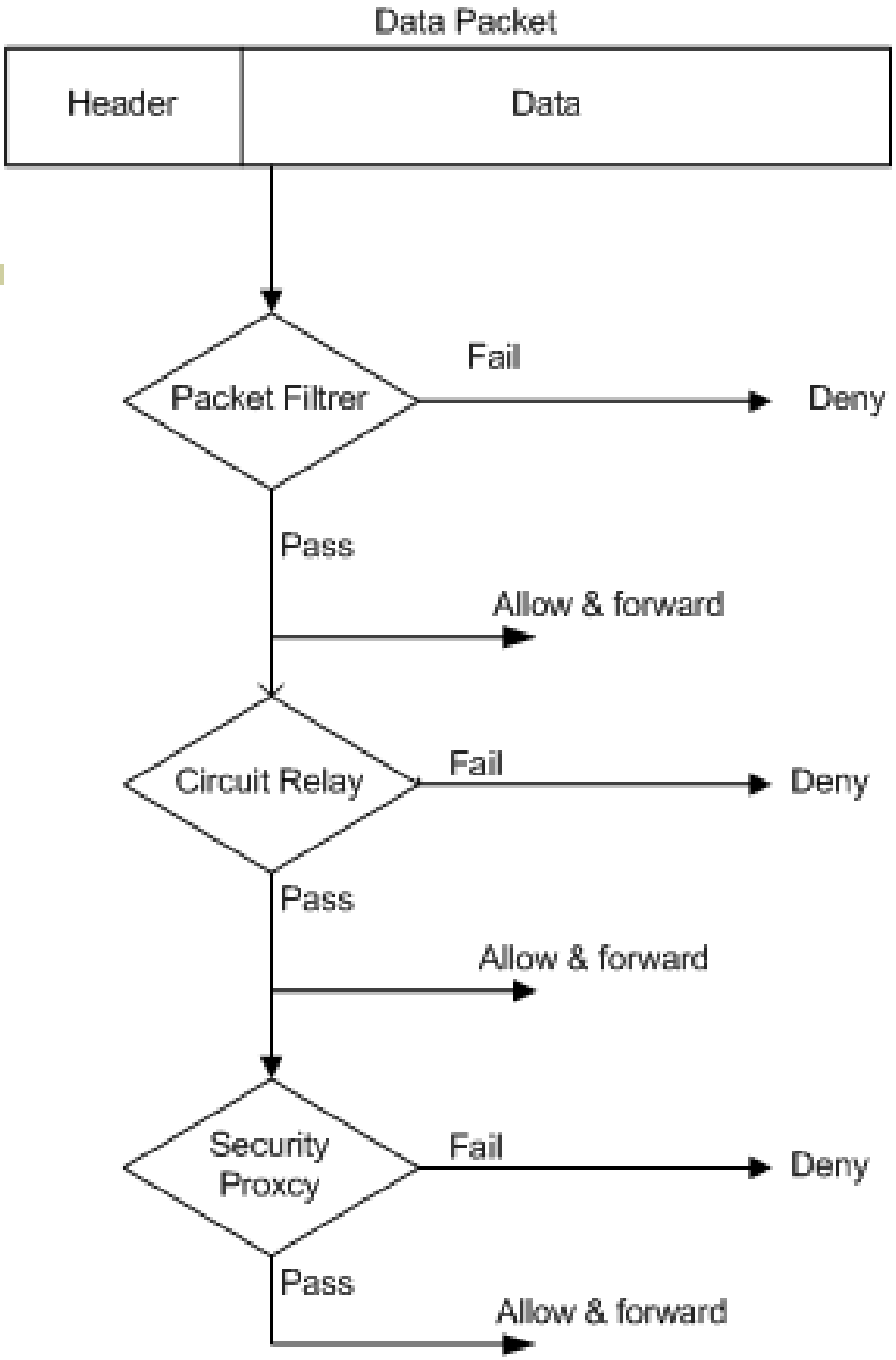
- Use none header information
  - User, time of day
- Dynamic packet filtering
  - Keep track of states
- Really effective when both packet filtering & circuit relay are combined together

Layer Comparison



Security Proxy

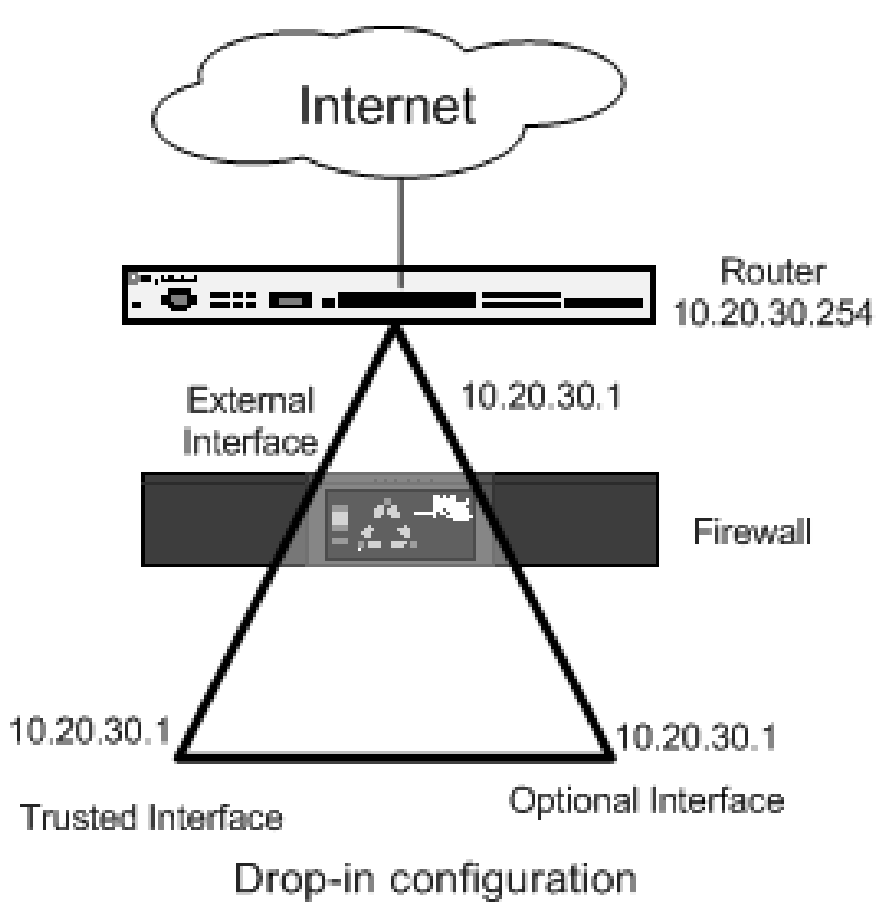
- Proxy is a program which intercepts packets, examine content, take some action to safeguard the server
- Firewall goes beyond packet filtering & circuit relay
  - Detect forbidden contents
- Each packet is stripped of its wrapping, analyzed, processed, re-wrapped & forwarded
  - Add some delay as well


Data Packet
Header
Data
Packet Filtrer
Fail
Deny
Pass
Allow & forward
Circuit Relay
Fail
Deny
Pass
Allow & forward
Security Proxcy
Fail
Deny
Pass
Allow & forward

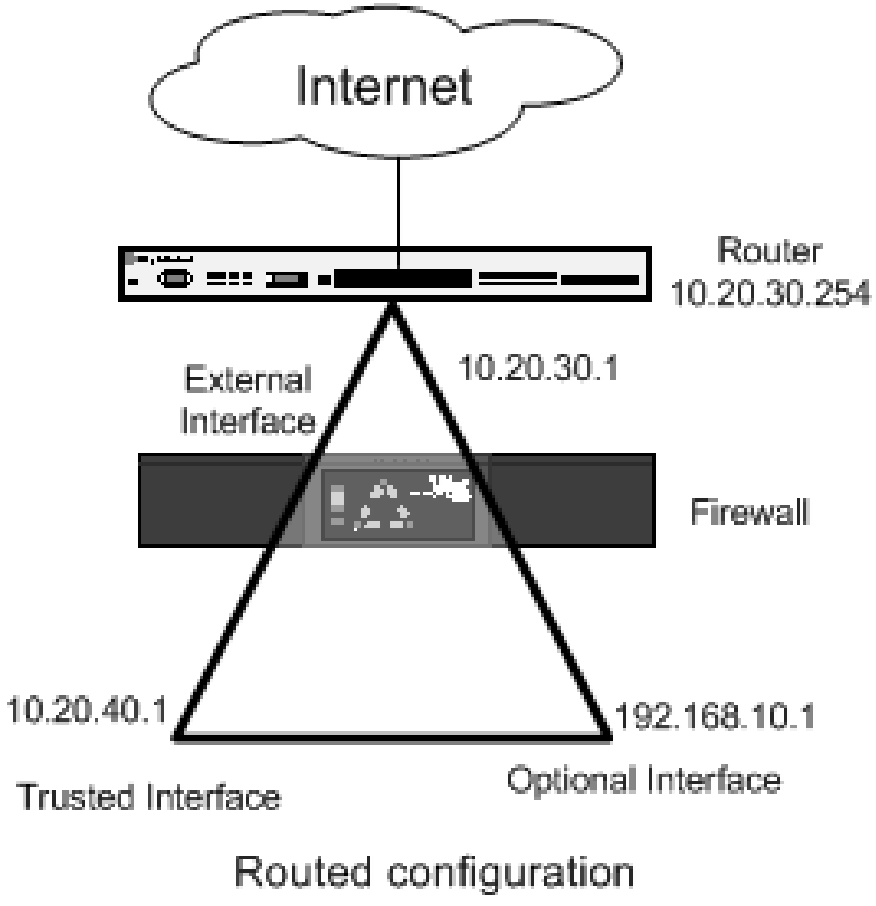
Proxies - Advantages

- make networks harder to hack by
  - blocking entire categories of commonly used attacks
  - concealing details about internal network servers from the public Internet
- help to use network bandwidth more effectively by
  - preventing unwanted or inappropriate traffic entering to the network
- Proxies reduce corporate liability by
  - preventing a hacker from using networks as a launch point for further attacks
- Simplify the management of networks by
  - providing administrator with tools and defaults that can be applied broadly, rather than desktop by desktop

Drop-in & Routed Networks

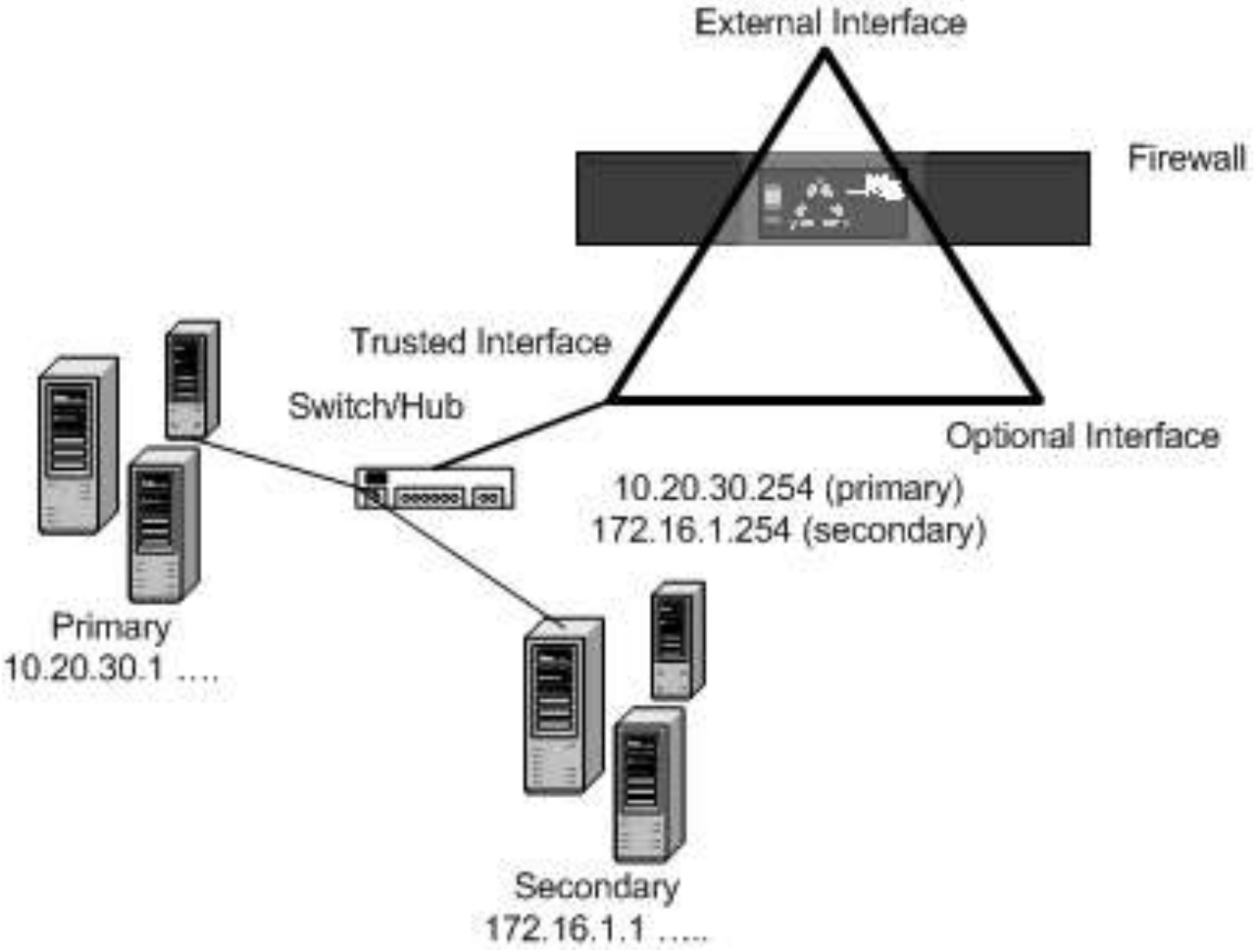


Drop-in configuration



Routed configuration

Secondary Network



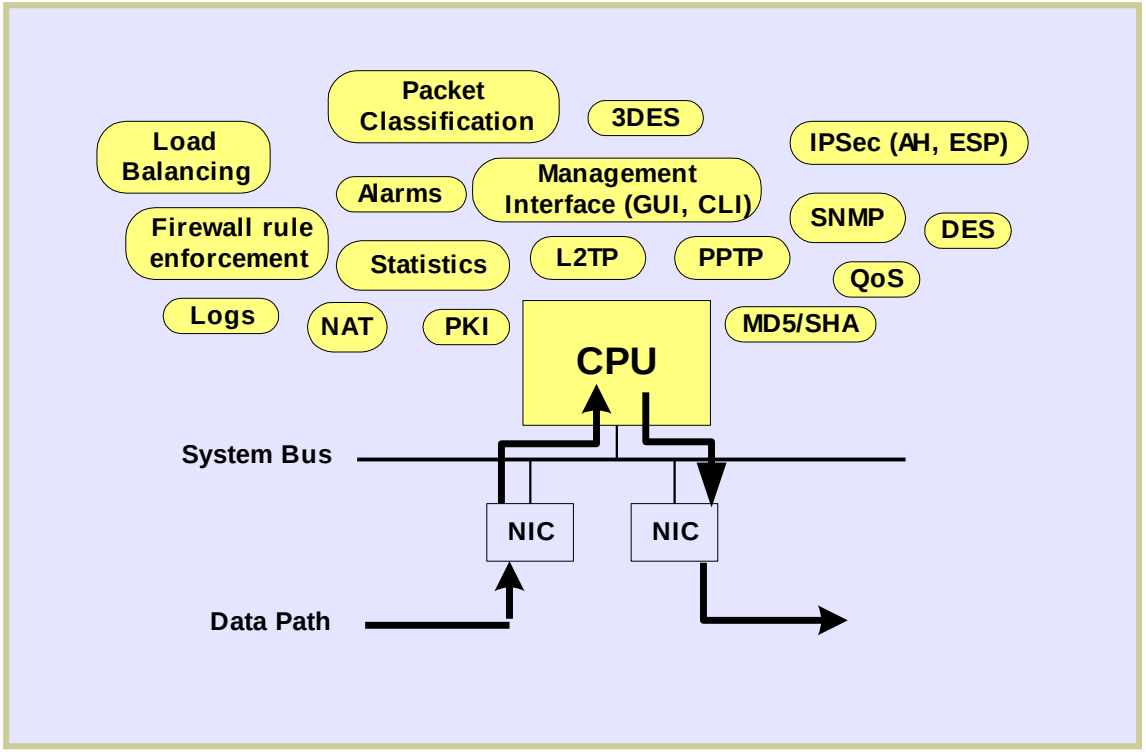
Software Vs Hardware

- Server based – dedicated
- Insecure OS
- Not a real-time OS
- Pay for things that are not necessary
- 3 vendors
- Frequent patches
- Licensed based
- Although initial cost is low TCO is high

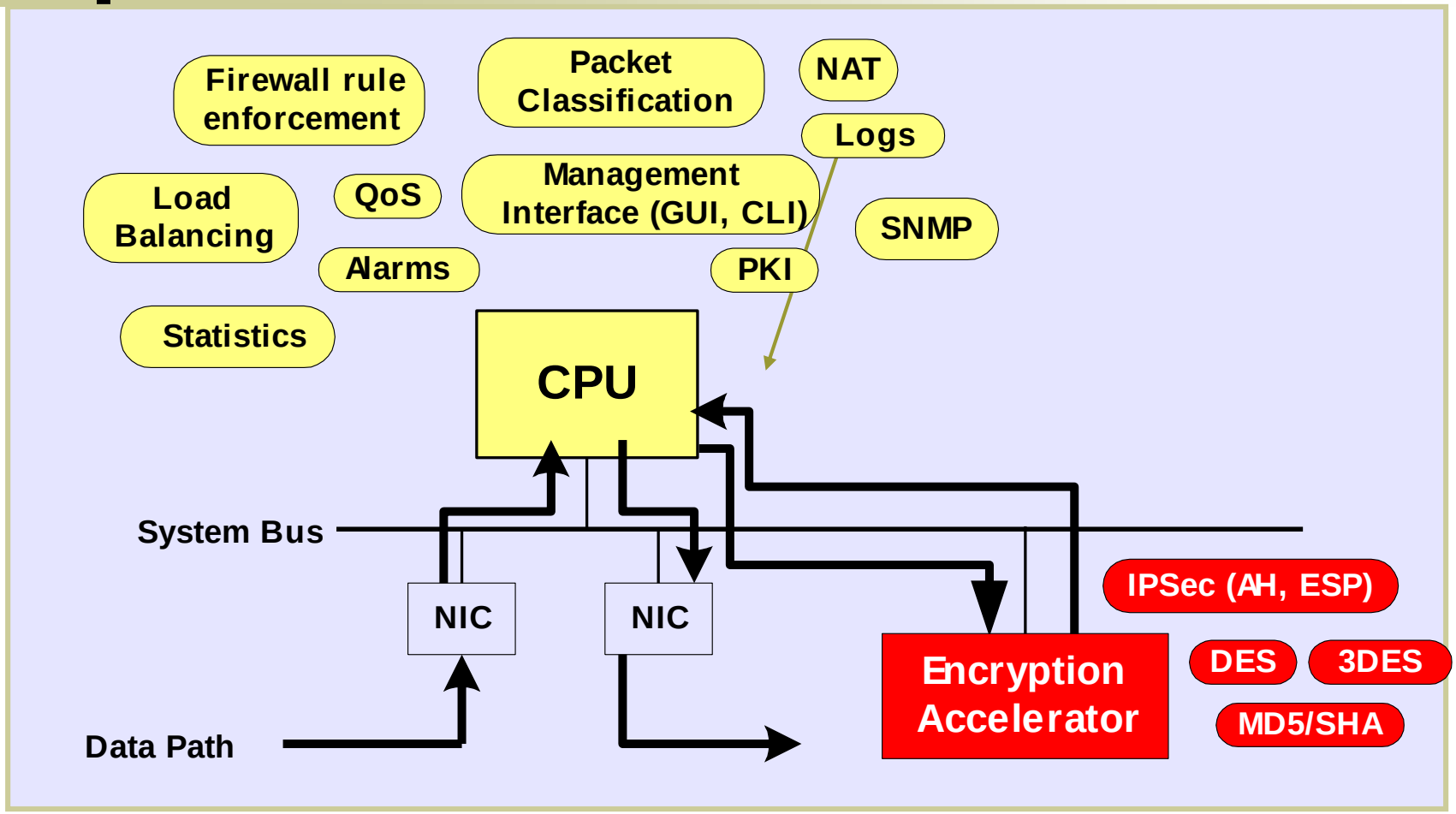
- Dedicated box
- Hardened OS
- Single vender
- Product based
- Hard to apply firmware updates
- No hard disk (not in all firewalls)
- Initial cost is bit high but TCO is significantly lower

ASIC (Application Specific IC)

- Hardware beats software because of ASIC
- Software is hard coded to chip

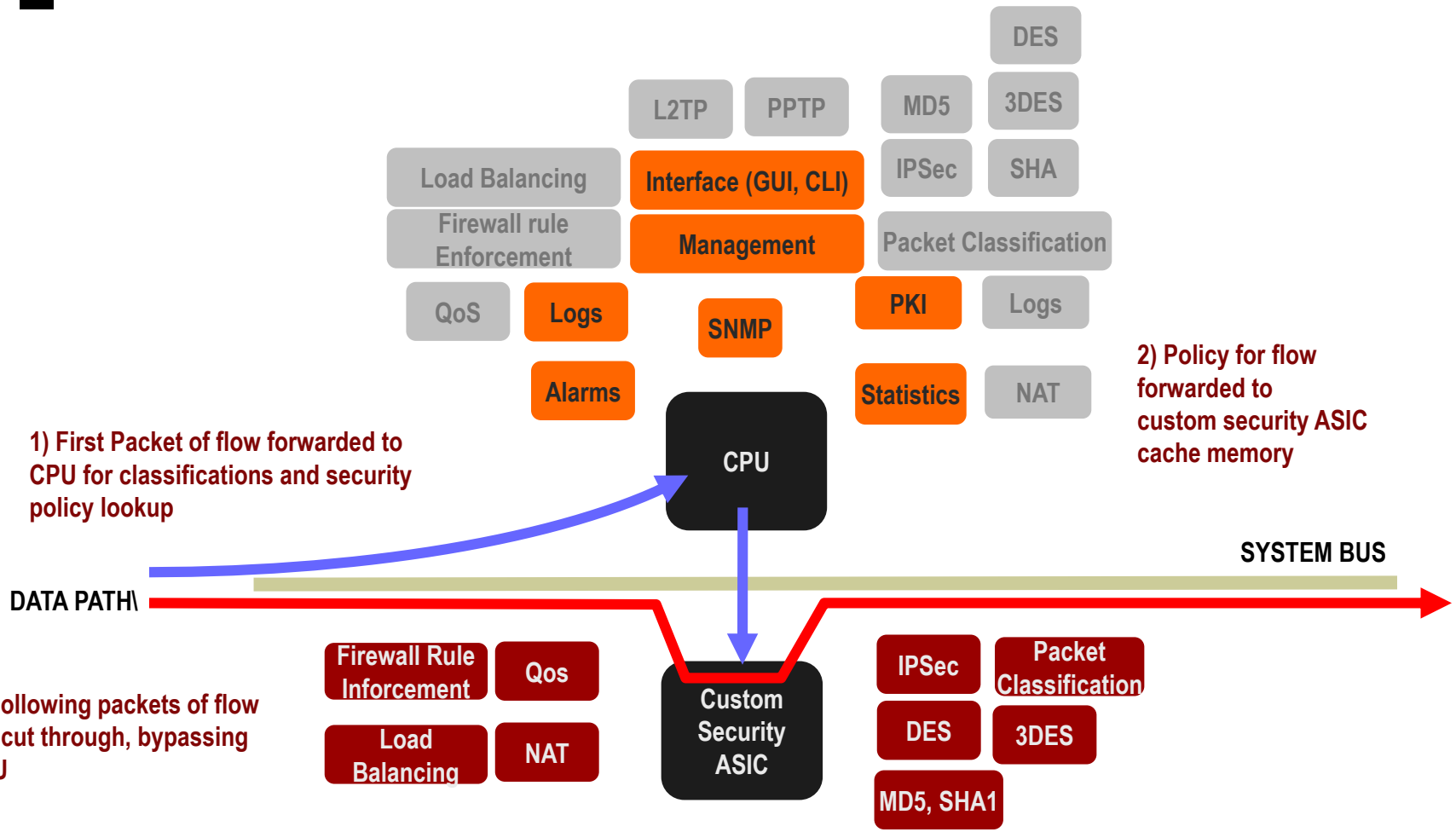


ASIC…



System Bus becomes the bottleneck

Intelligent ASIC



WatchGuard®

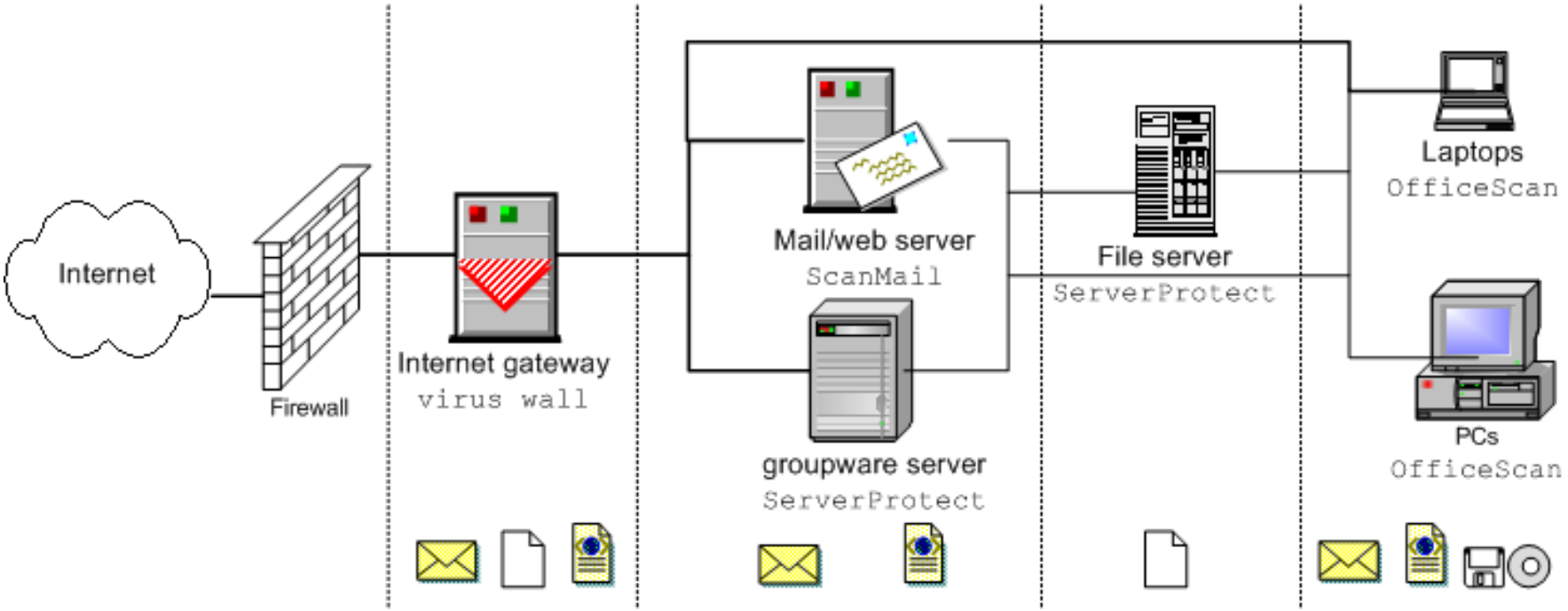
Features

- QoS
  - Active Active
  - Active Passive
- Server load balancing
- Centralized management
- Value added service
- No hard disk
- Hardened Linux
  - (Proprietary Vs Open)

Demo

Server Protection

Server Protection



Why?

- Risk comes from out side so why do I bother about internal servers?
- In reality risk comes from inside than outside
  - Either planned or unplanned
- None of the commercial OSs are secure
  - It is a separate layer not a integrated part of the system

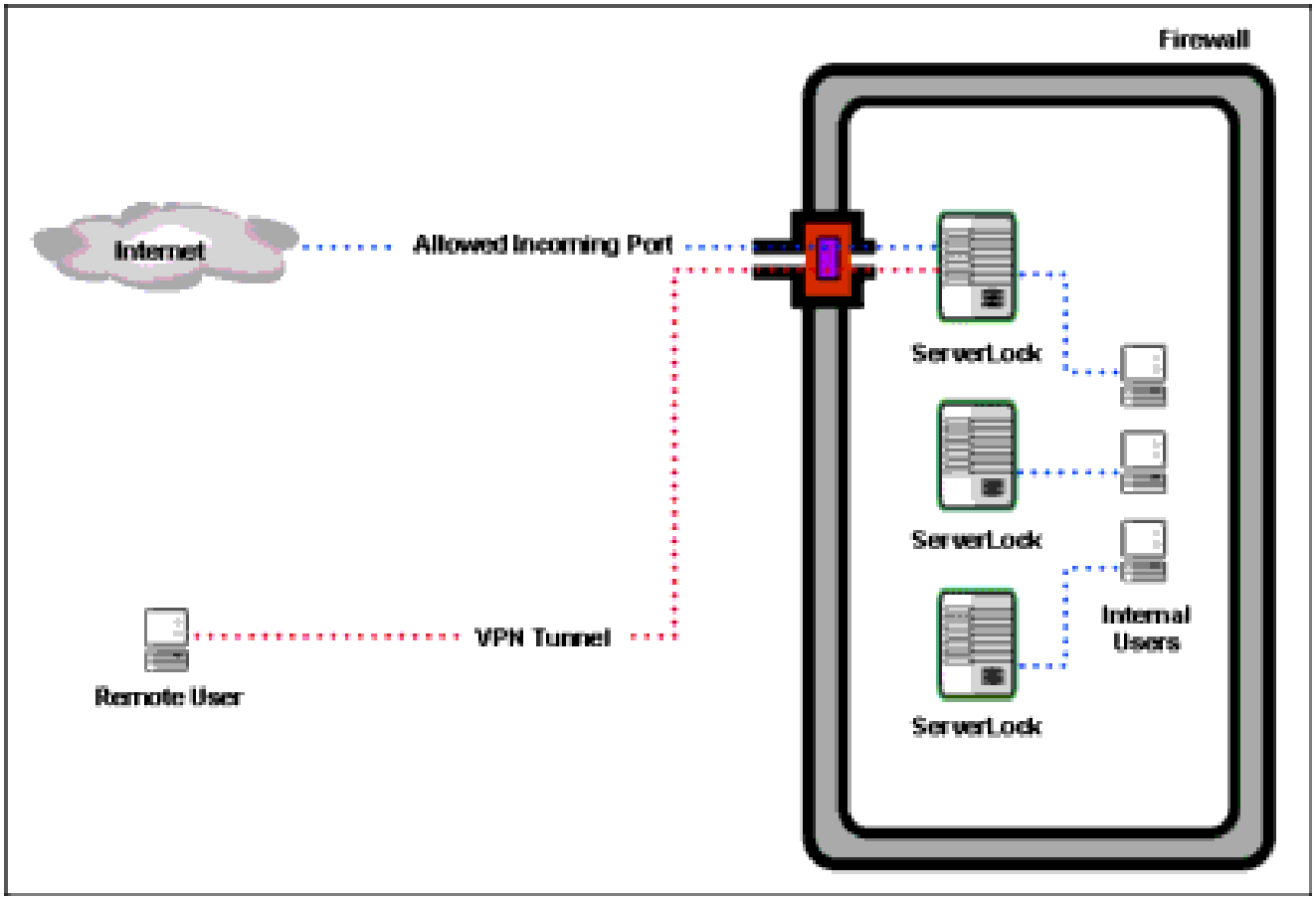
A legitimate user

- Any one who get access as the power user can do anything
  - Change the content of a web page to divert credit card information to a different location
  - Create a user account as a backdoor
  - Delete all the log entries that could indicate a system hack
  - System reconfiguration

ServerLock

- An immerging concept
  - Operating under the belief that protecting your data from unauthorized change is more effective than detecting attacks
- Locks
  - It self
  - Critical OS files & configurations
  - Registry
  - User defined resources

Protection

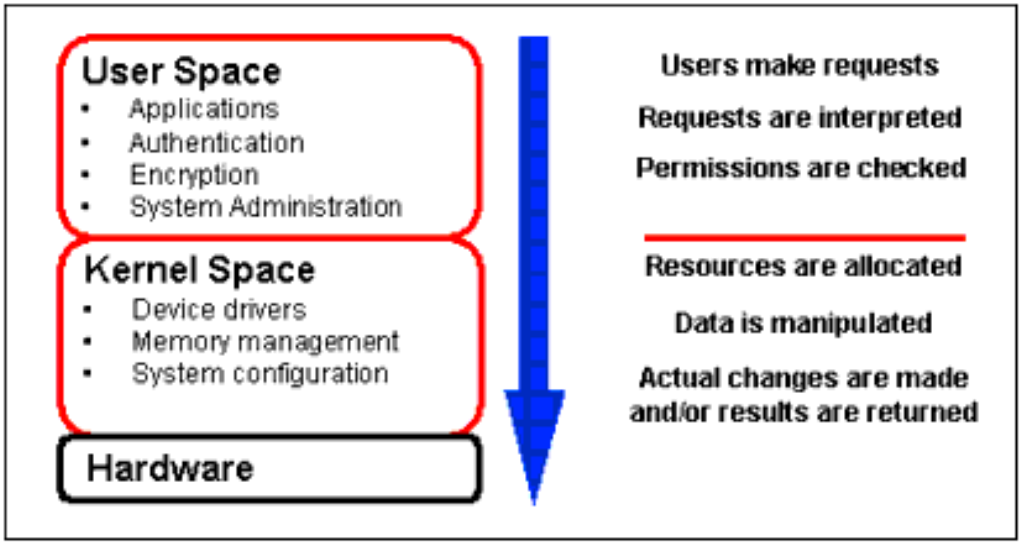

Firewall
Internet
Allowed Incoming Port
ServerLock
ServerLock
ServerLock
Internal Users
VPN Tunnel
Remote User

Policy

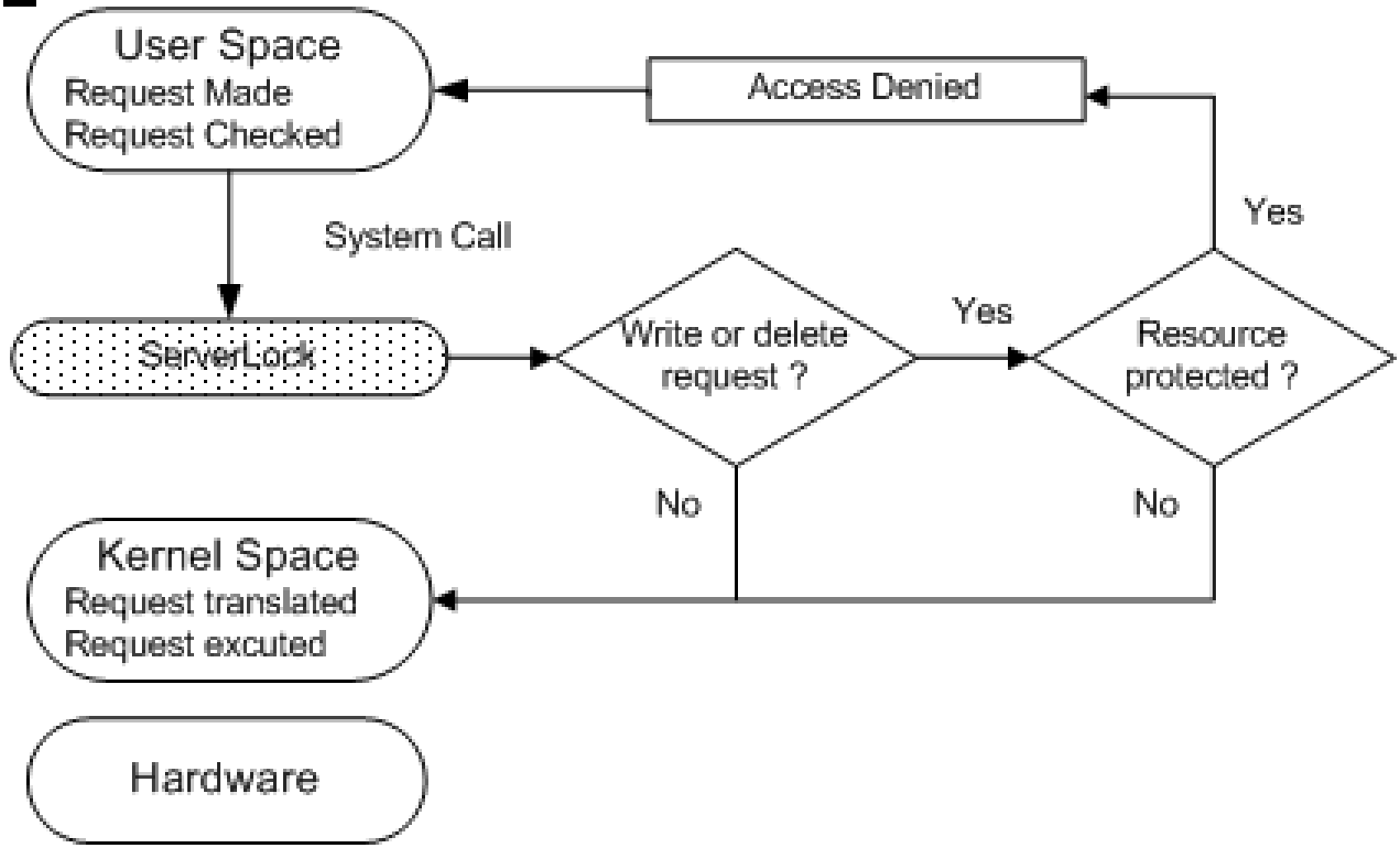
- Denies write or delete access based on
  - The resource
  - Not on the user
  - Even Sys Admin cannot do anything
- If need to change any protected resource first unlock the resource

Location

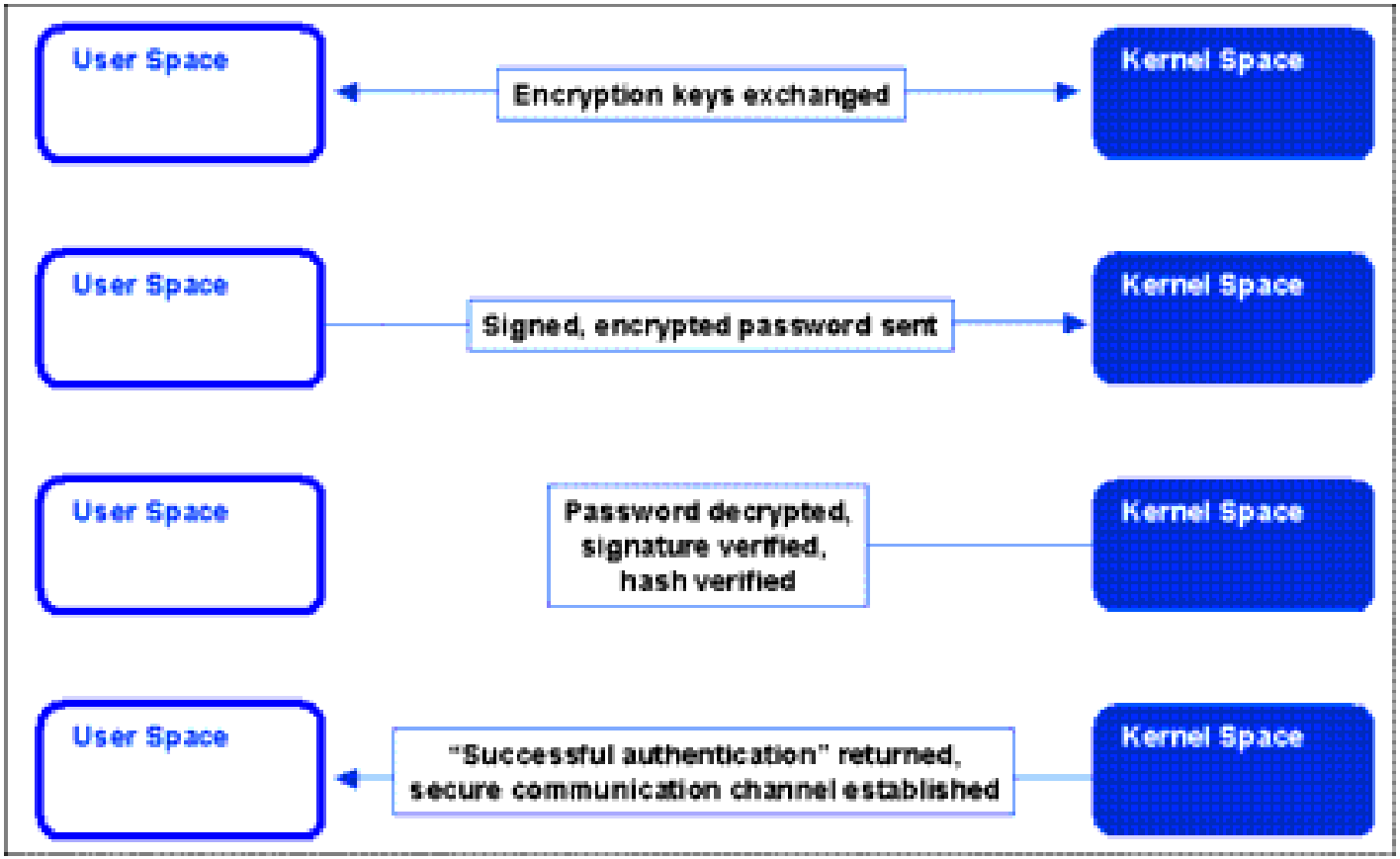
- Resides between user space & kernel space
  - As a device driver in Windows
  - As a loadable kernel module in Solaris
- Intercept all the system calls



Logic


User Space
Request Made
Request Checked
Access Denied
System Call
Yes
ServerLock
Write or delete request ?
Yes
Resource protected ?
No
No
Kernel Space
Request translated
Request excuted
Hardware

Internal Security

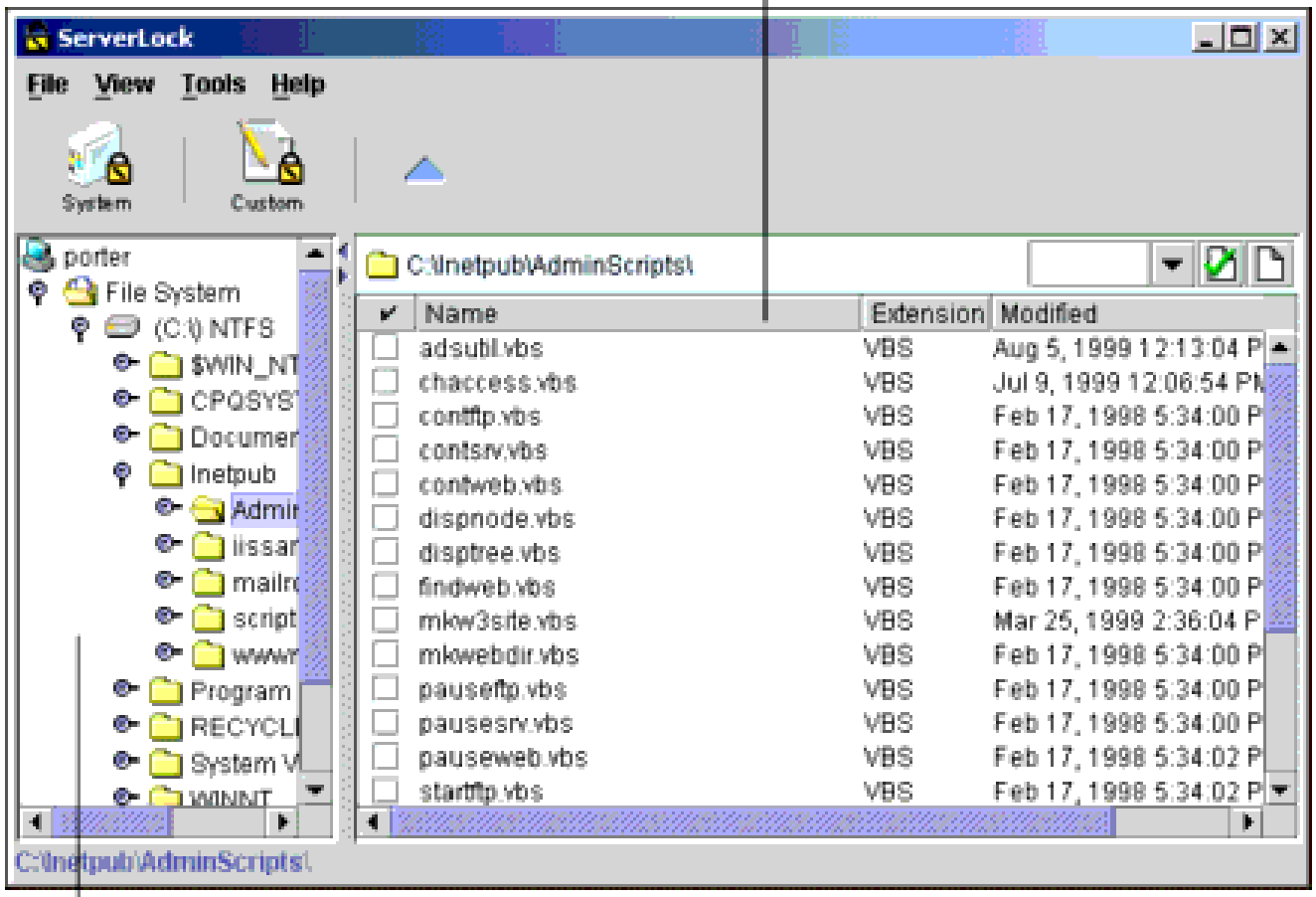


PKI + 239 bit ECC

Protecting it self

- Protects itself from being altered, disabled, or removed by unauthorized individuals, by securing:
  - Hardware profiles
  - File System
  - Registry

Results Pane



Tree Pane

Can guard against

- Changes to existing files or registry keys
- Creation of new files or registry keys
- Other resources
  - IIS Metabase
  - User Accounts
  - Date & Time
  - Stack Buffer
- Custom rules can be added to protect other resources

ServerLock Vs AppLock/Web

- Server Lock protects the entire server while AppLock protects only specific application
- Applock/Web is designed to protect web servers (IIS only)

AppLock/Web

$595 per server

ServerLock

$1295-1695 per server

ServerLock Manager

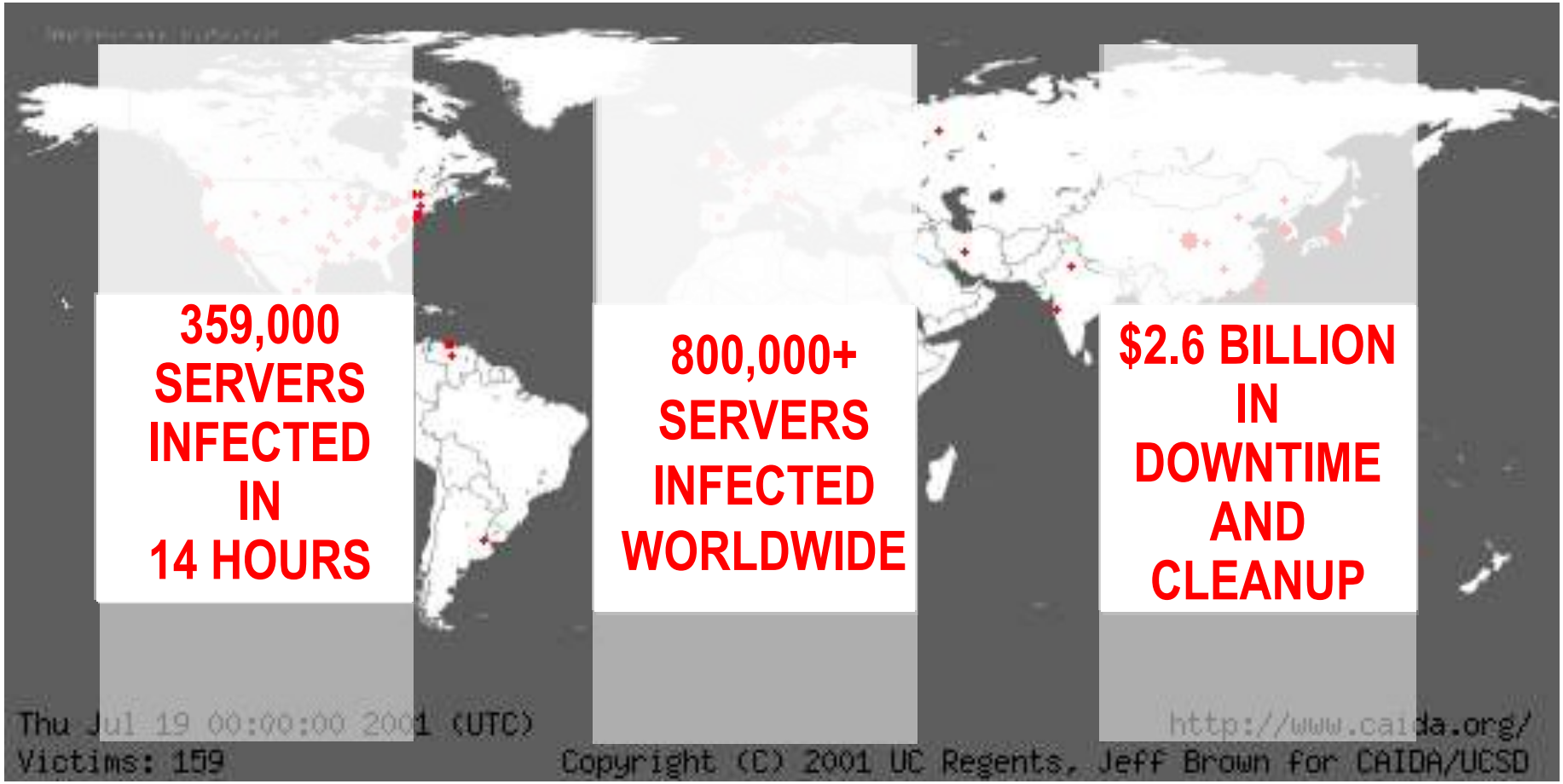
$5,000 – 15,000

Demo

Service	Incoming		Outgoing		Properties
	From	*To*	*From*	*To*	
HTTP	Any	Web server	Any	Any	Port 80
FTP	HQ only	170 & Dinky	Any	Any	Port 21
SMTP	Any	Mail server	Any	Any	Port 25
DNS	Any	170	Any	Any	Multi protocol on ports using client ports
Telnet	HQ only	170 & Dinky	Any	Any	Port 23
Ping	Dinky	Any	Any	Any	Do
Lotus Notes	HQ only	170	Any	Any	TCP on port 1352
WatchGuard	None	None	Trusted	Any	Multi protocol on port 4103
Virus Scan	None	None	Any	64.75.31.197	TCP on port 80
Authority	Admin PC	Firewall	Any	Any	TCP on port 113

Enterprise Level Anti-virus Solutions

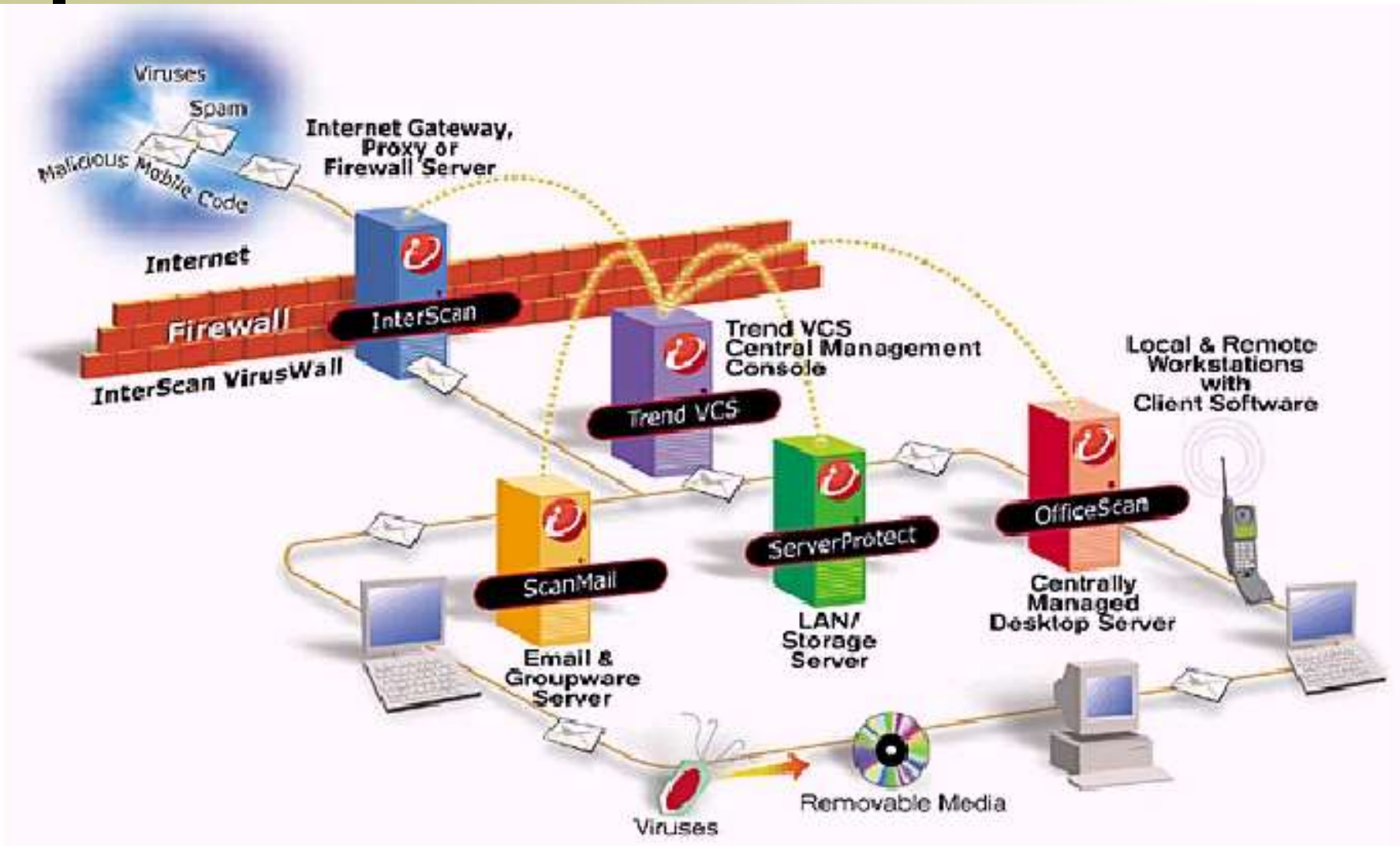
Code Red


359,000
SERVERS
INFECTED
IN
14 HOURS
800,000+
SERVERS
INFECTED
WORLDWIDE
$2.6 BILLION
IN
DOWNTIME
AND
CLEANUP
Thu Jul 19 00:00:00 2001 (UTC)
Victims: 159
http://www.caida.org/
Copyright (C) 2001 UC Regents, Jeff Brown for CAIDA/UCSD

Viruses & Worms

- Is the most destructive in terms of data losses, time to recover & money
- New destructive threat immerge in every 11 hours
- Safeguard requires frequently updating of virus patterns & applying patches

Defense-in-Depth

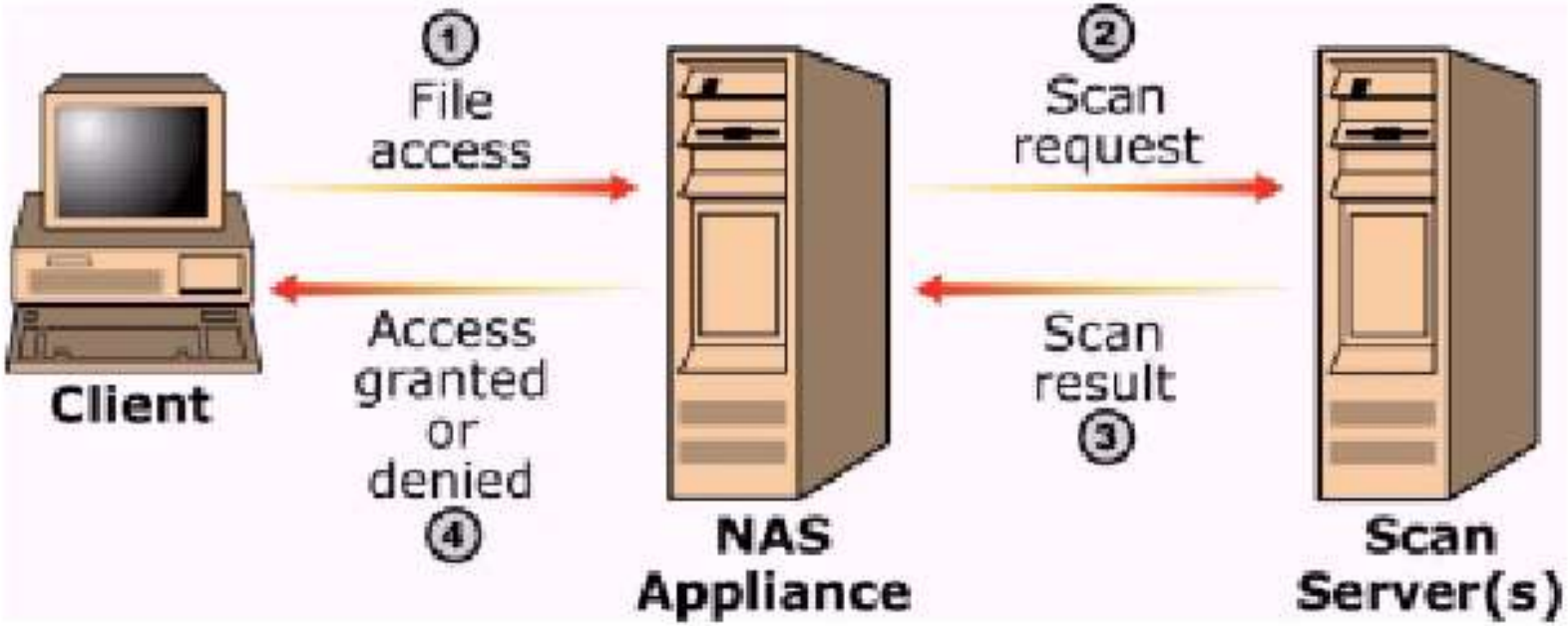


Definitios

- VirusWall
  - Resides just after the firewall (internet gateway)
  - All traffic (SMTP, HTTP, FTP) must pass through the Viruswall
  - Stops viruses, worms, spam at the entry point
  - Files are download to the VirusWall Server before sending to clients

Server Protection

- Server based virus guards are different than a PC based ones

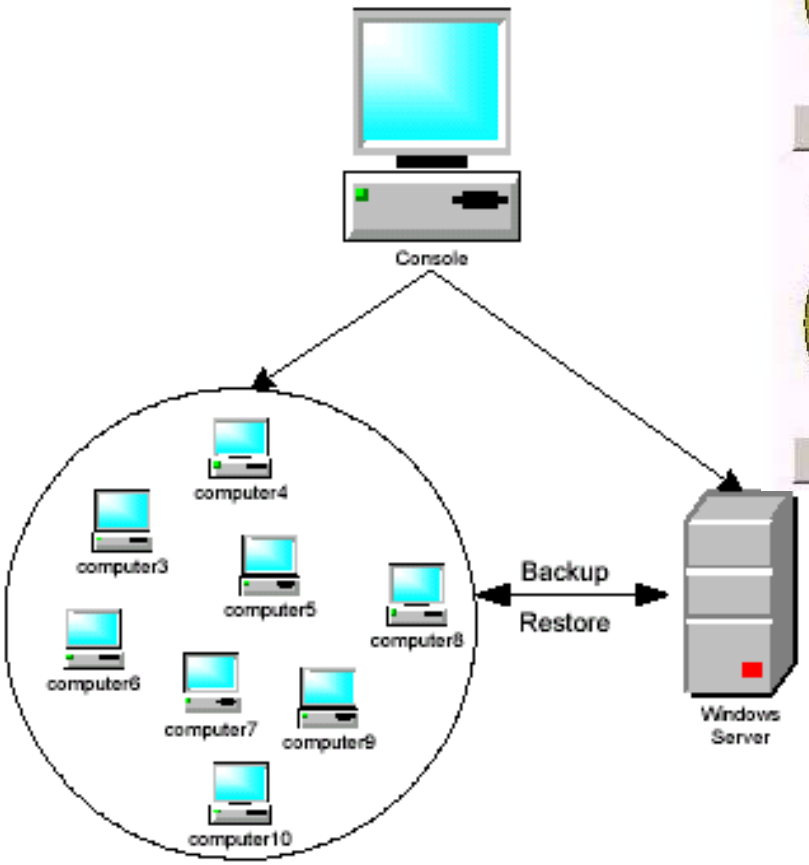


Server Protection Cont…

- Everything depends on the type of server
  - Mail servers must use specialized mail scanning software
- Centralized management of all servers allow one station to update virus definitions & deploy to others
  - Preserves bandwidth

Desktop Protection

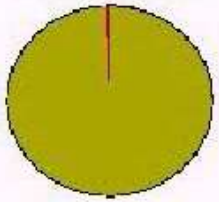
- Standalone solutions or centralized solution?
  - All PCs having same policy
  - Ease of management & policy enforcement
  - Preserve bandwidth
  - Extensive login
    - User state
    - Corporate image



Virus Pattern File

Last update : Tuesday, December 10, 2002 15:40:42

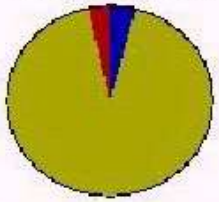
Online clients



Newest	410	1 client	0.42%
Older	409	234 clients	99.15%
Oldest	403	1 client	0.42%

See older clients | See oldest clients

Offline clients



Newest	409	3 clients	4.34%
Older	407 - 397	64 clients	92.75%
Oldest	395	2 clients	2.89%

See older clients | See oldest clients

What makes a good Network Security System

- Simplicity
  - If it is complex in design & configuration, hard to manage would course more security holes
  - Simple designs are more likely to be used consistently & correctly
- Scalability
  - When you (business) grow it should grow with you

Good Security System Cont…

- High uptime & quick recovery
  - High meantime between failure
  - Failover recovery
- Distributed architecture
  - Different tasks on different locations (or PCs)
- Dynamically secured
  - Cannot be static & one time product

Good Security System Cont…

- Economy of IP addresses
  - Hiding internal IPs
  - Reducing the number of public IPs
- Secure connection
  - VPN, management station, subcomponents
- Authentication

Good Security System Cont…

- Login & notification
  - Keep you informed
- Summarized & reports of NW activity
- Physically secured

Security Vs Sri Lanka

- Not aware of the threat
  - Every one is searching for low cost anti-virus solution that could protect everything
- I am not having anything to loose so why do I?
- Should I invest more on security?

If you spend more on Coffee (Tea) than security you are deserved to be hacked!

By advice for defense for US president

Conclusion

- Security is a dynamic process which you have a role to play (loose or winner)
- Third world countries should not be a playground for hackers
- Awareness is the best way of protection

References

- www.watchguard.com
- Or

Questions????

Thank you