ATS®

Systems. People. Trust.

Network Perimeter Security

Advanced Technology Systems

Introduction

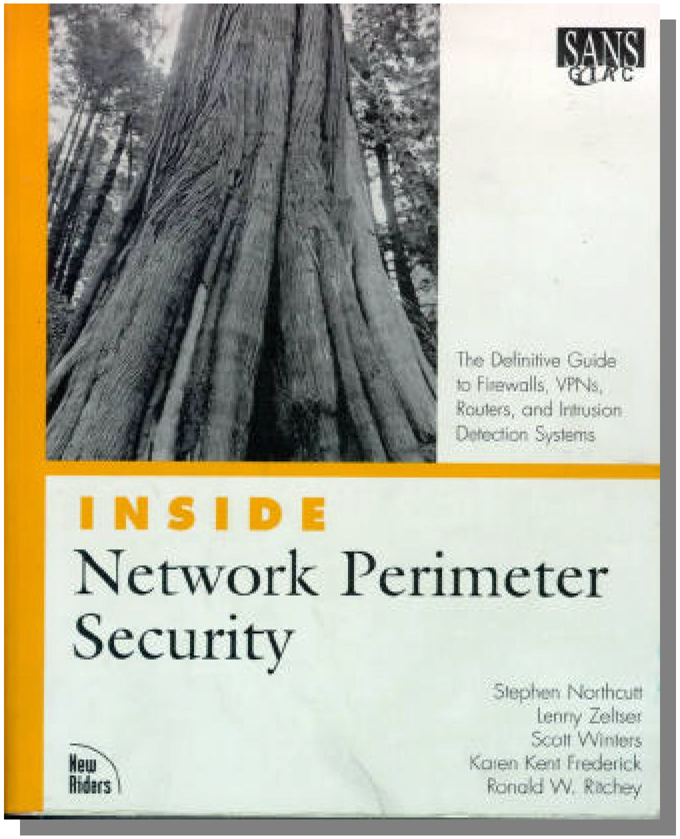
- Marty Gillespie
  - CISSP
  - 17 years experience
    - Information Security
    - Networking
  - Contact:
    - 937-431-3667 x260
    - mgillespie@atsva.com

Agenda

- Perimeter Security Fundamentals
- Perimeter Security Components
- Perimeter Design

Reference Material

Northcutt, Stephen, et al. Inside Network Perimeter Security. Indianapolis: New Riders, 2002. ISBN 0-7357-1232-8.


SANS GIAC
The Definitive Guide to Firewalls, VPNs, Routers, and Intrusion Detection Systems
INSIDE
Network Perimeter Security
Stephen Northcutt
Lenny Zeltser
Scott Winters
Karen Kent Frederick
Ronald W. Ritchey
New Riders

Additional Reference

- Capitol College – Laurel, Maryland
  - Degree: MS Network Security
  - Course: NS 680 Perimeter Security
  - Professor Dan Hickey

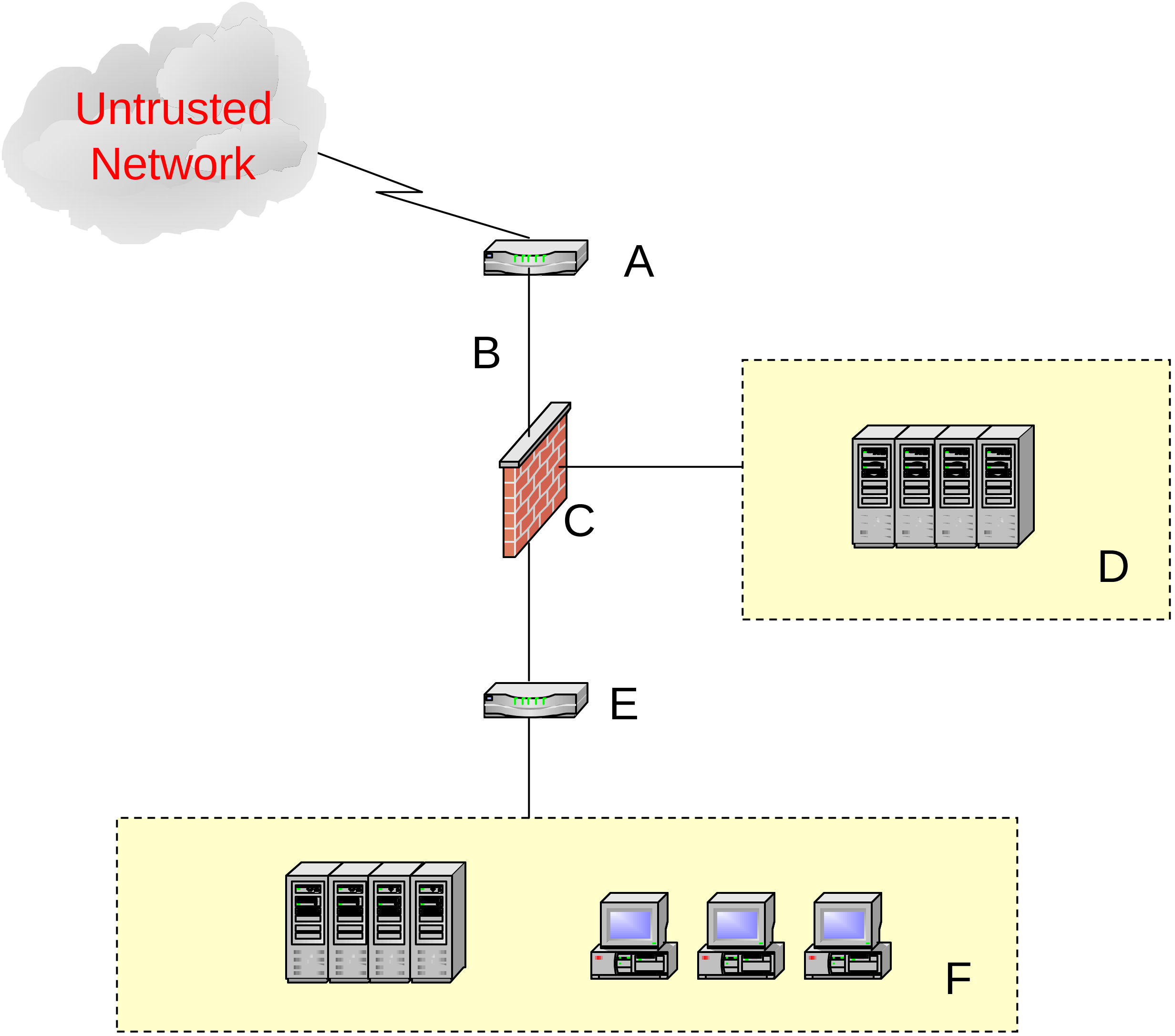
Perimeter Security Fundamentals

It's all about Defense in Depth!

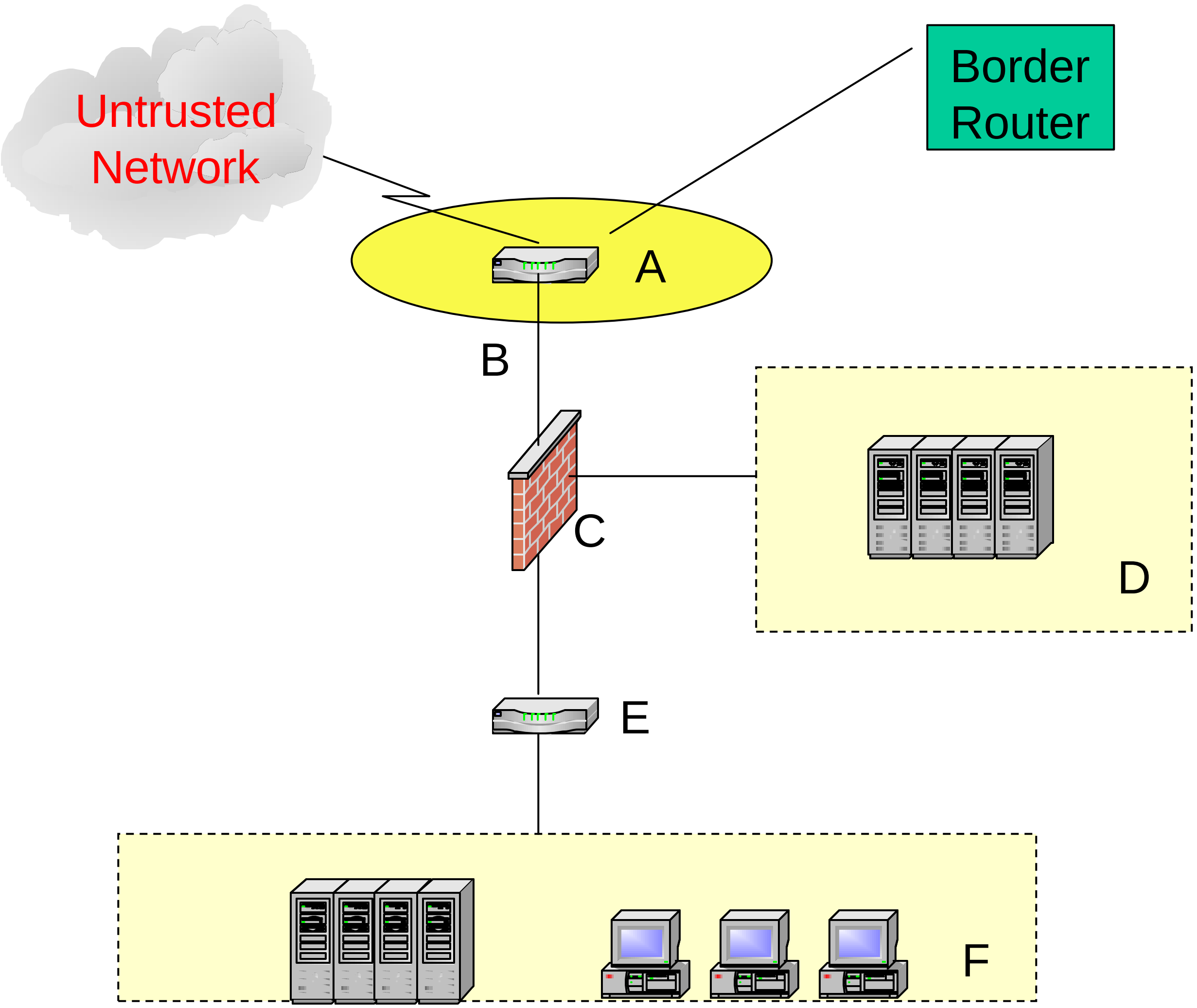
Terms of the Trade

- The Perimeter
- Border/Exterior/Screening Router
- Firewall
- Interior/POP Router
- Intrusion Detection System
- Virtual Private Network
- Software Architecture
- DMZs and Screened Subnets
- Defense in Depth

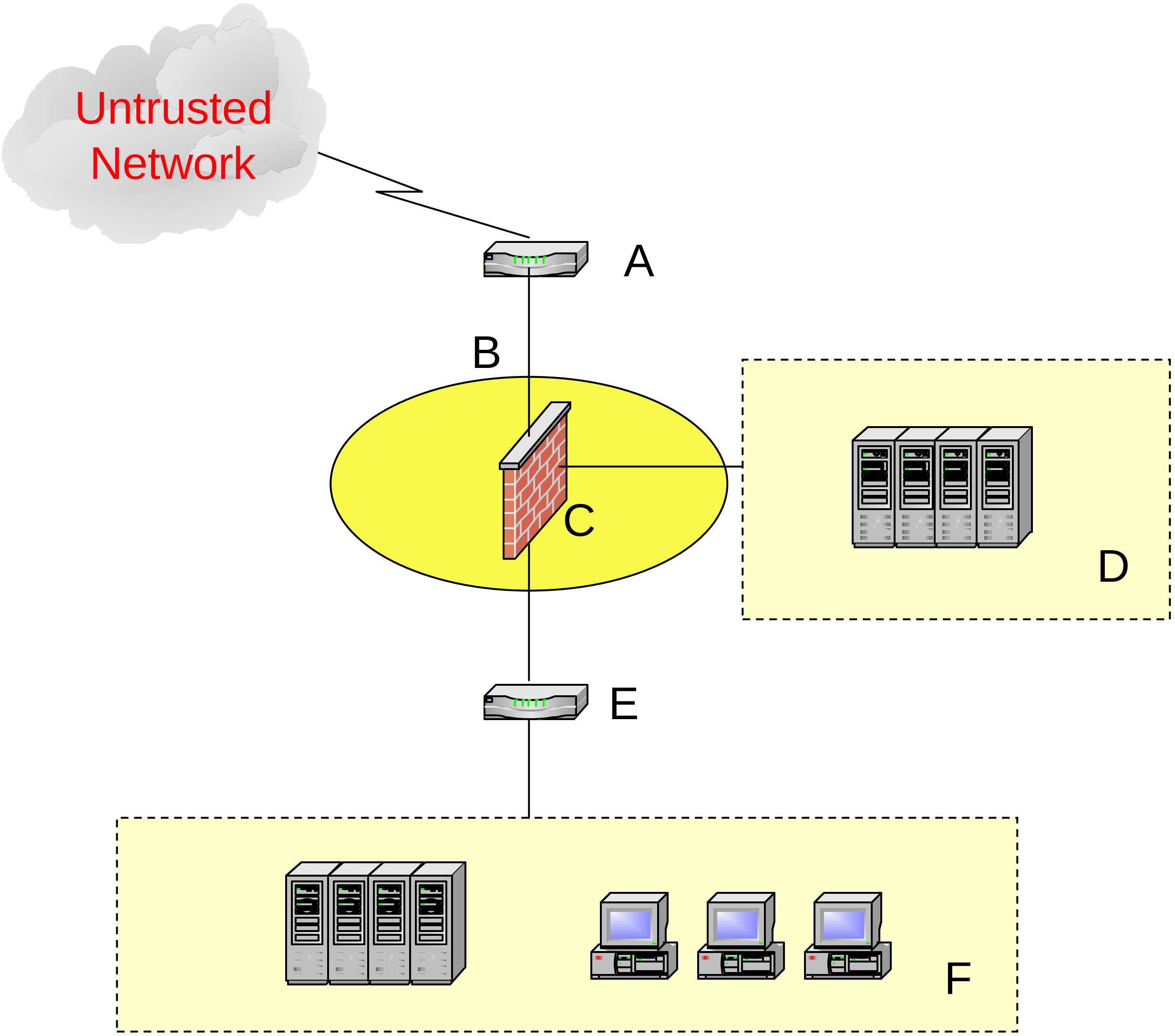
The Perimeter



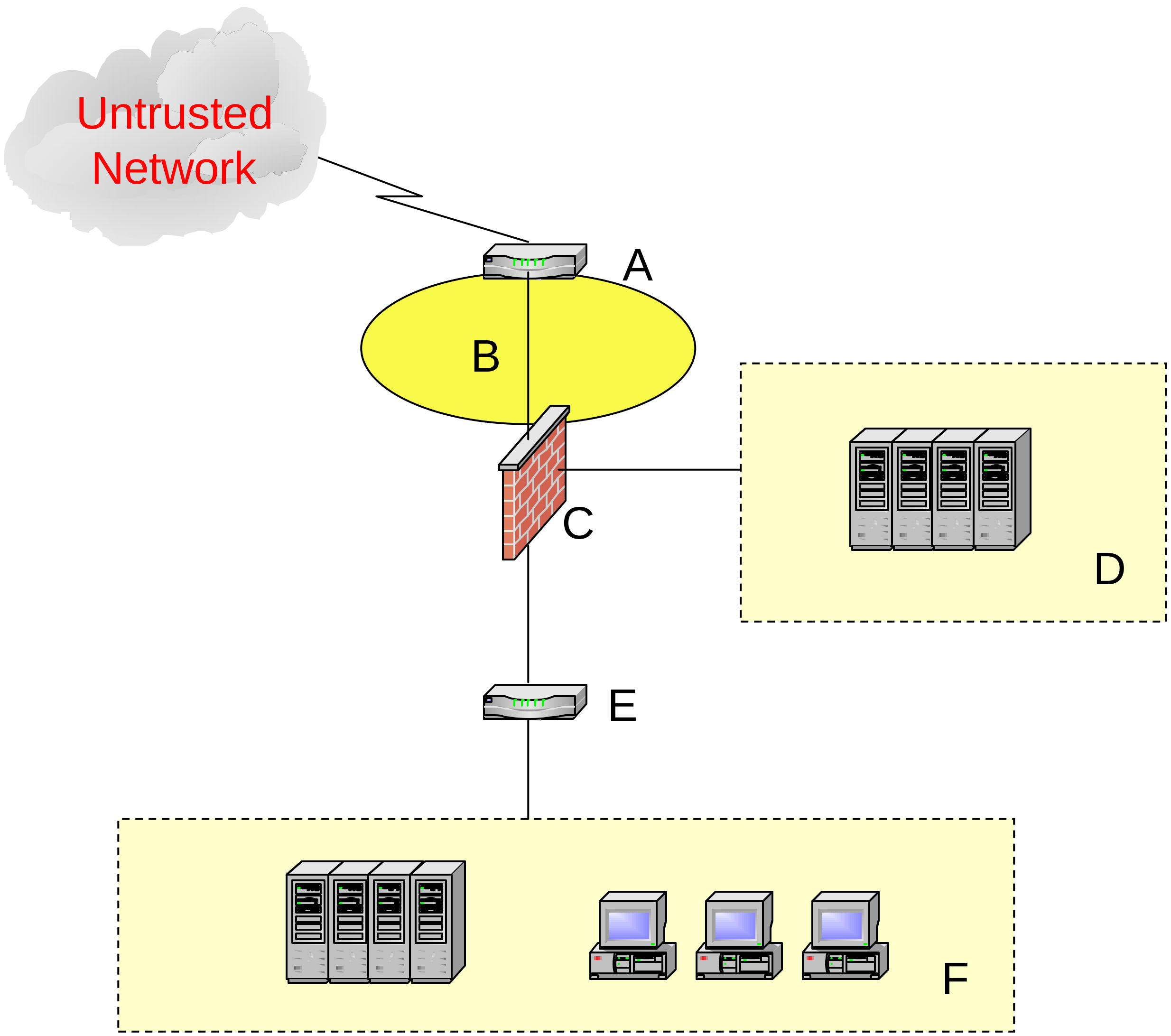
Border/Screening Router



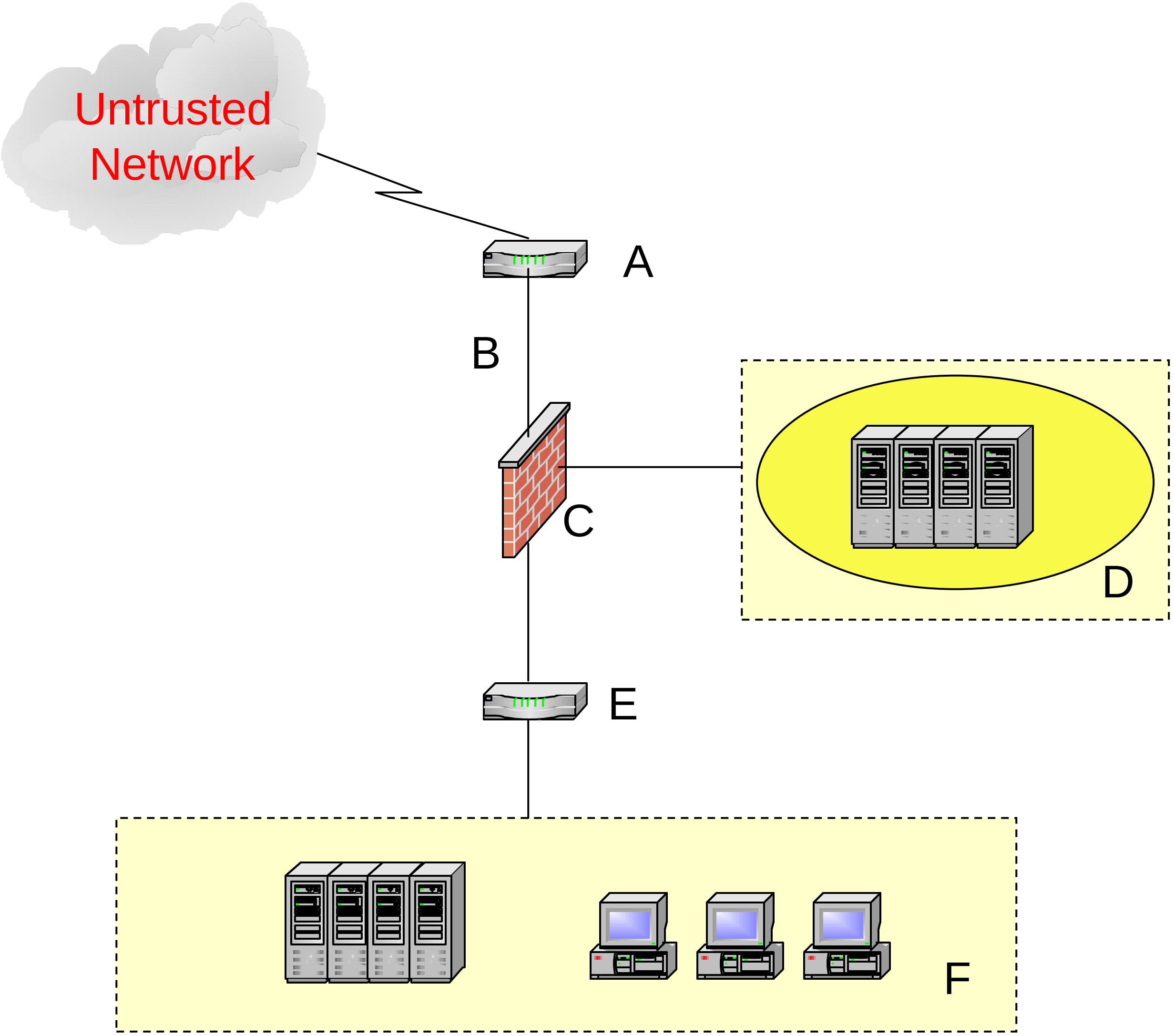
The Firewall



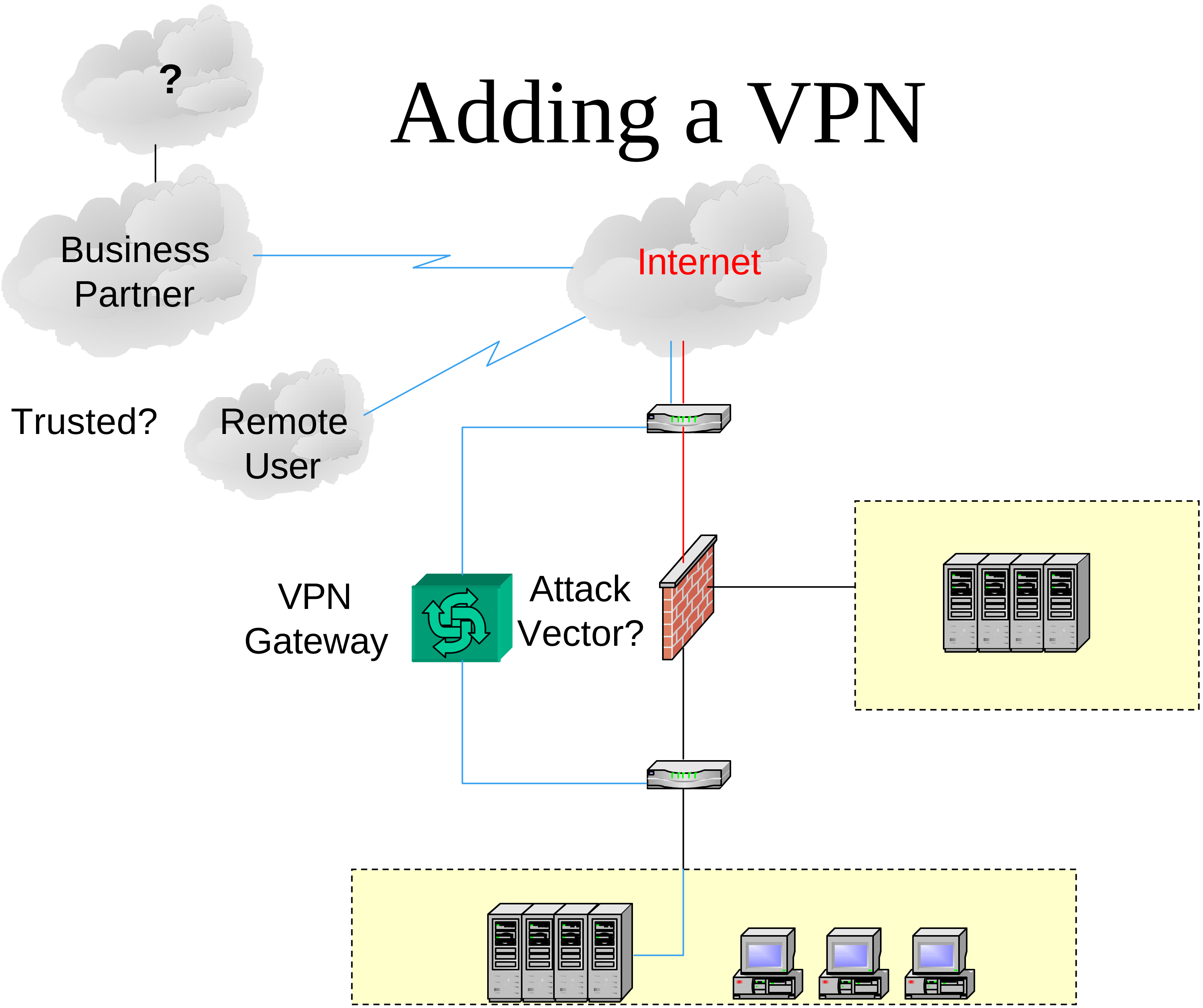
The DMZ



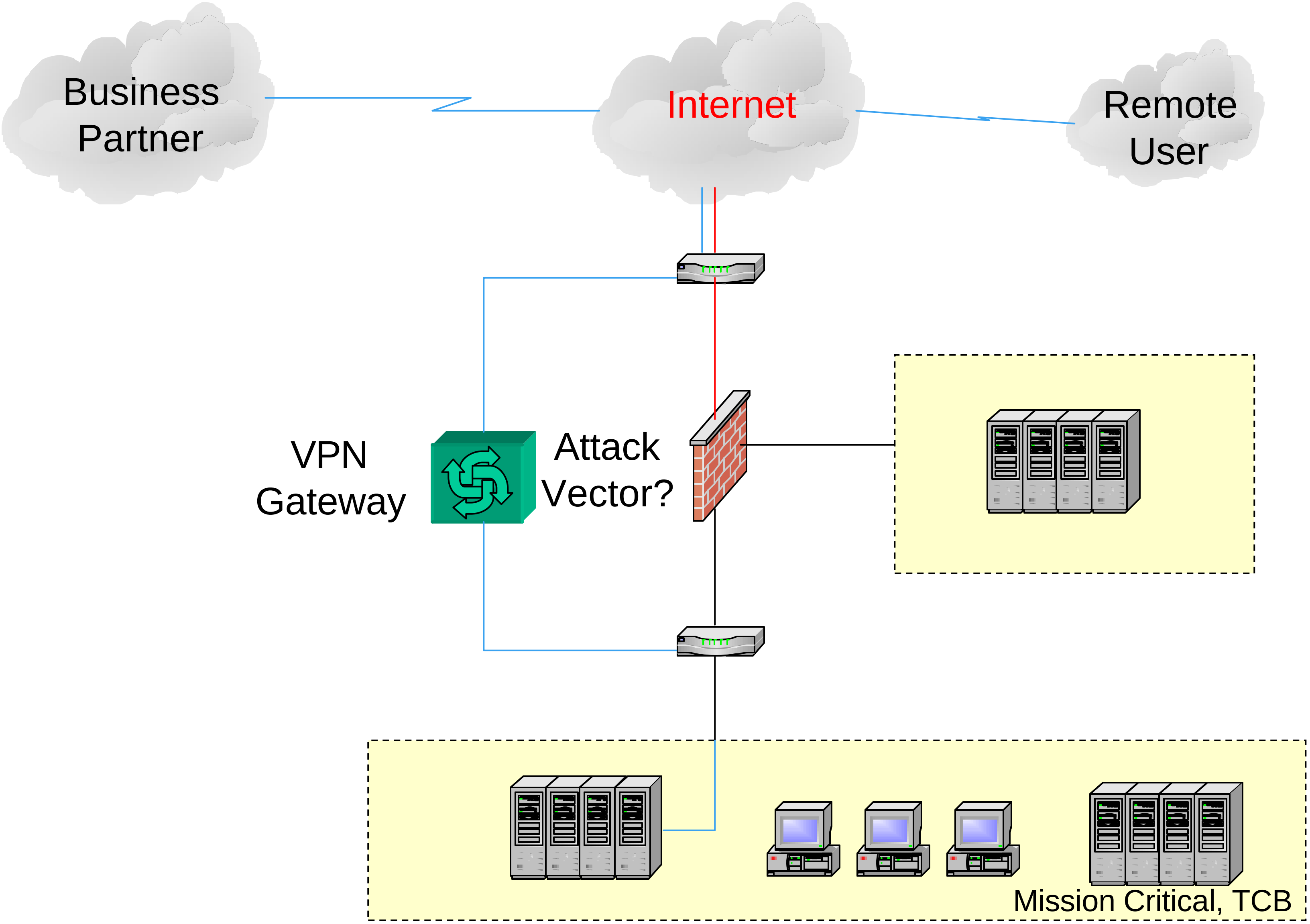
The Screened Subnet



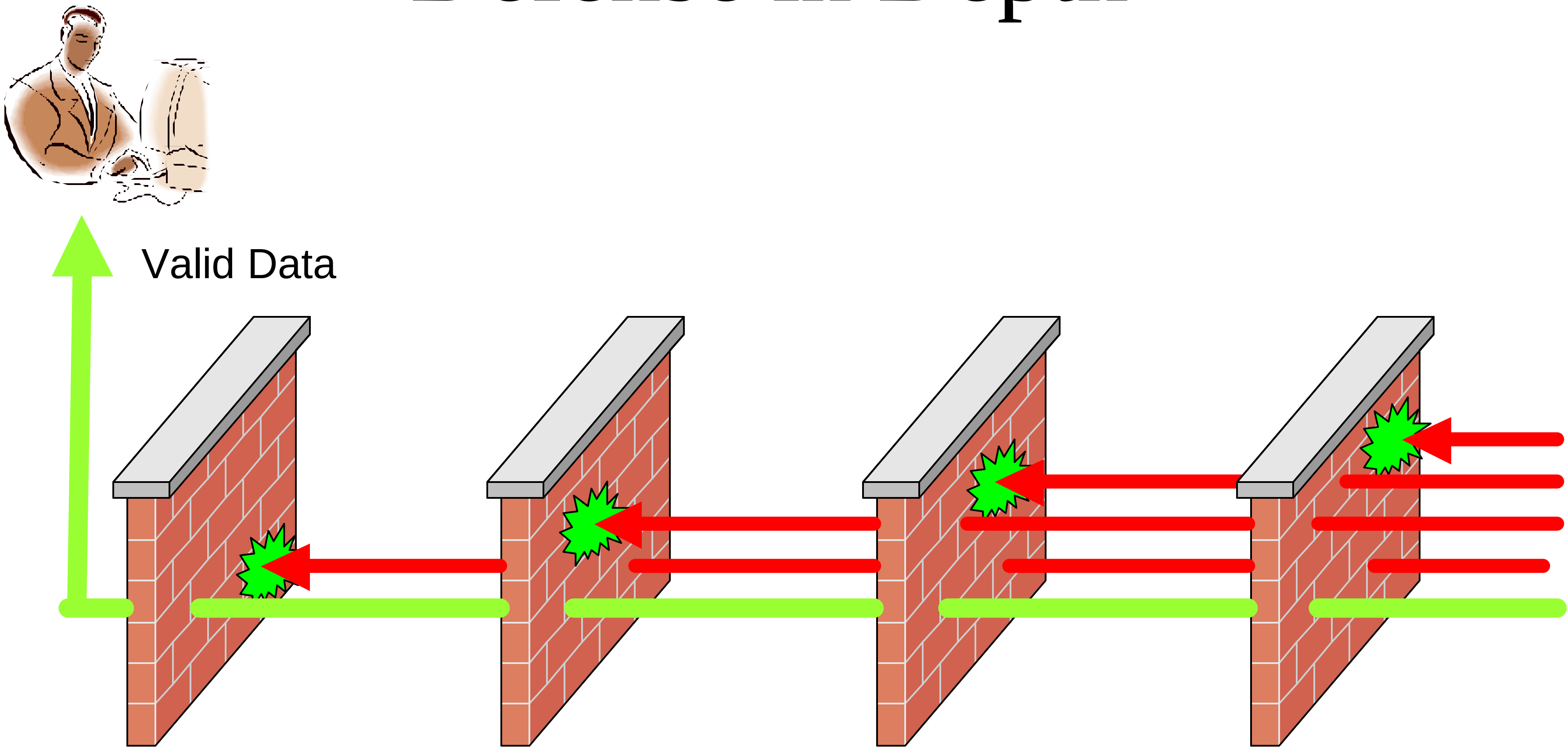
Adding a VPN


?
Business Partner
Internet
Trusted?
Remote User
VPN Gateway
Attack Vector?

Intrusion Detection



Defense in Depth



Valid Data

B4
AV
Pwd
CM
Training
Policy

B3
IDSs
AV
CM
Training
Policy

B2
ACLs
IDSs
AV
CM
Training
Policy

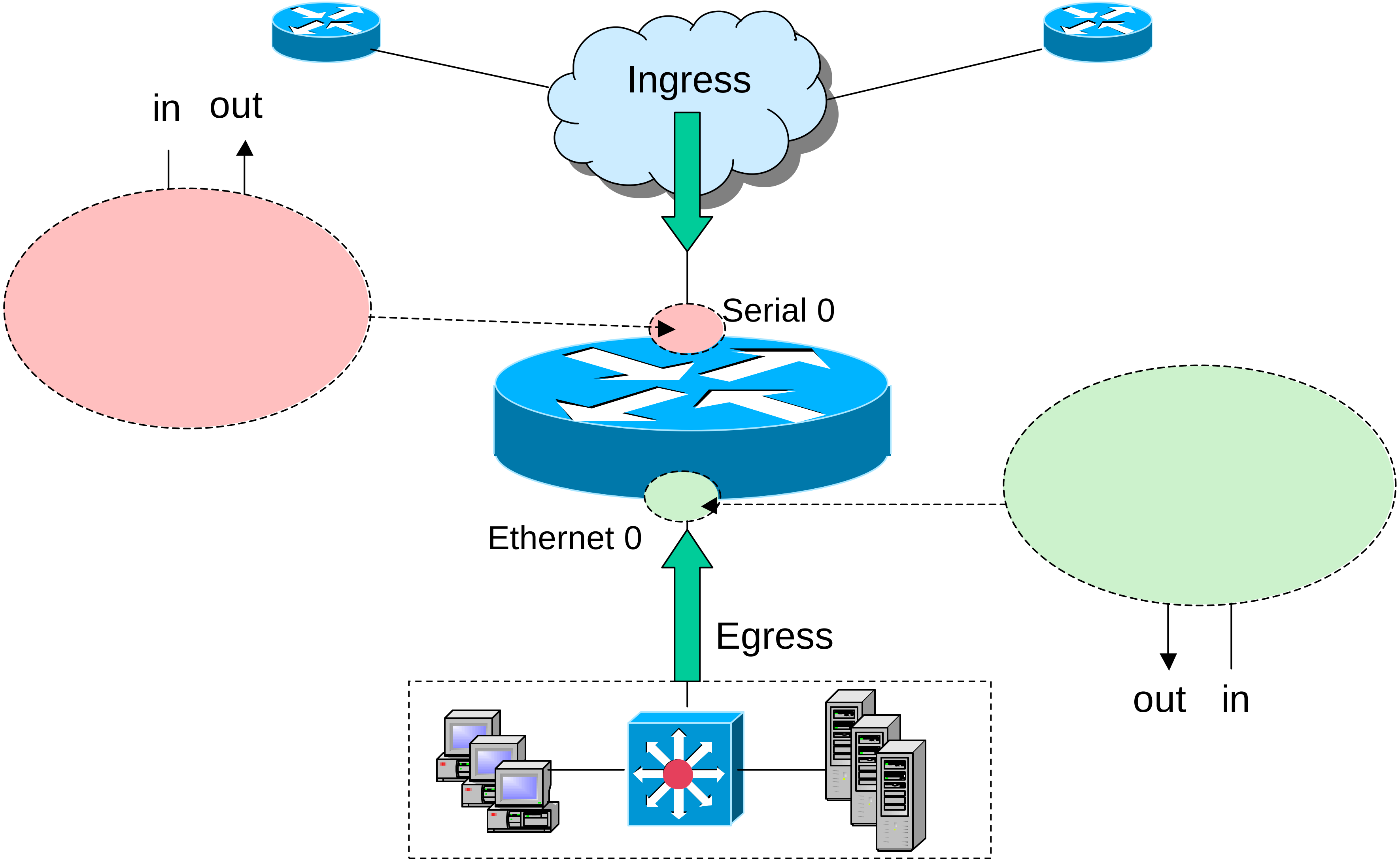
B1
ACLs
FWs
IDSs
Honeypot/net
CM
Training
Policy

Packet Filtering

Static Packet Filtering

- Can be used throughout the DiD
- Implemented on hosts, servers, firewalls and routers
- Applied to both ingress and egress
- At perimeter – 90% solution
  - Blocks the “noise” – absolute filtering
  - Relieves FW of burden
  - Fast filtering based on organizations rules
- Minimum – applied on border router

In or Out?



Tenants of Packet Filtering

- Implicit deny applies
- List specific rules at the top…and more general rules at the bottom
- Filter as it enters router – ingress or egress
- Ingress filtering
  - Deny reserved IPs
  - Deny your internal IPs
  - Deny loopback/broadcast/multicast
  - Deny bad actors – carefully
  - Deny firewall subverting services – AOL-IM?
  - Permit only as necessary – not w/standard ACL!
- Egress filtering
  - Permit only your IPs
  - Deny critical local use only IPs

Use ending "deny any log"

Packet Filtering

The Importance of Position

- Implicit deny all
  - One ACL added to router interface
  - Open routing stops
    - Rules of ACL applied
- Rules applied fm top to bottom
- First rule match applied to each packet
- Position of rules in ACL is critical!
- Create, manage, and post from TFTP server
- One access-group per protocol per interface

Packet Filtering

Cisco ACLs

- Three ACL types
  - Standard
    - Filters on source IP address only
    - Entered in numbered or named ACL
  - Static Extended
    - Filters on source, destination, protocol, port, flags, etc.
    - Entered in numbered or named ACL
  - Advanced - Reflexive
    - Dynamic ACL entries generated and deleted
      - Not based on TCP hdr flags – supports UDP and ICMP
    - Entered in named ACL, only

Standard ACL

- Strengths
  - Fast!
  - Generally used for
    - Blacklisting
    - Allowing specific IPs – caution
    - Ingress/Egress filtering
- Weaknesses
  - Only source IP
    - Doesn't do destination, ports, protocols, etc…
    - Vulnerable to source spoofing and source routing
    - Permit using standard ACL is big hole

Static Extended ACL

- Strengths
  - Significantly more granularity than standard
  - Allows some “state” awareness – established option
- Weaknesses
  - Spoofing and Source Routing
  - Fragmentation

Static Packet Filtering

Pros and Cons

Pros	Cons
Low impact on network performance.	Operates only at the network layer. Examines only lower layer headers.
Low cost – now included with many operating systems.	Unaware of packet payload – offers relatively low level of security.
Fills a niche. Great for filtering out the majority of network noise.	Lacks state awareness – may require numerous ports to be left open to facilitate services which use dynamically allocated ports.
	Susceptible to IP spoofing.
	Difficult to create rules (order of precedence).

Reflexive ACL

Pros	Cons
Lowest impact of all architectures on network performance when designed to be fully SMP compliant.	Operates only at the network layer – examines lower layer headers.
Low cost – now included with some operating systems.	Unaware of packet payload – offers relatively low level of security.
State awareness provides measurable performance benefit.	Susceptible to IP spoofing.
	Difficult to create rules (order of precedence)
	Can introduce additional risk if connections can be established without following the RFC-recommended 3-way handshake.

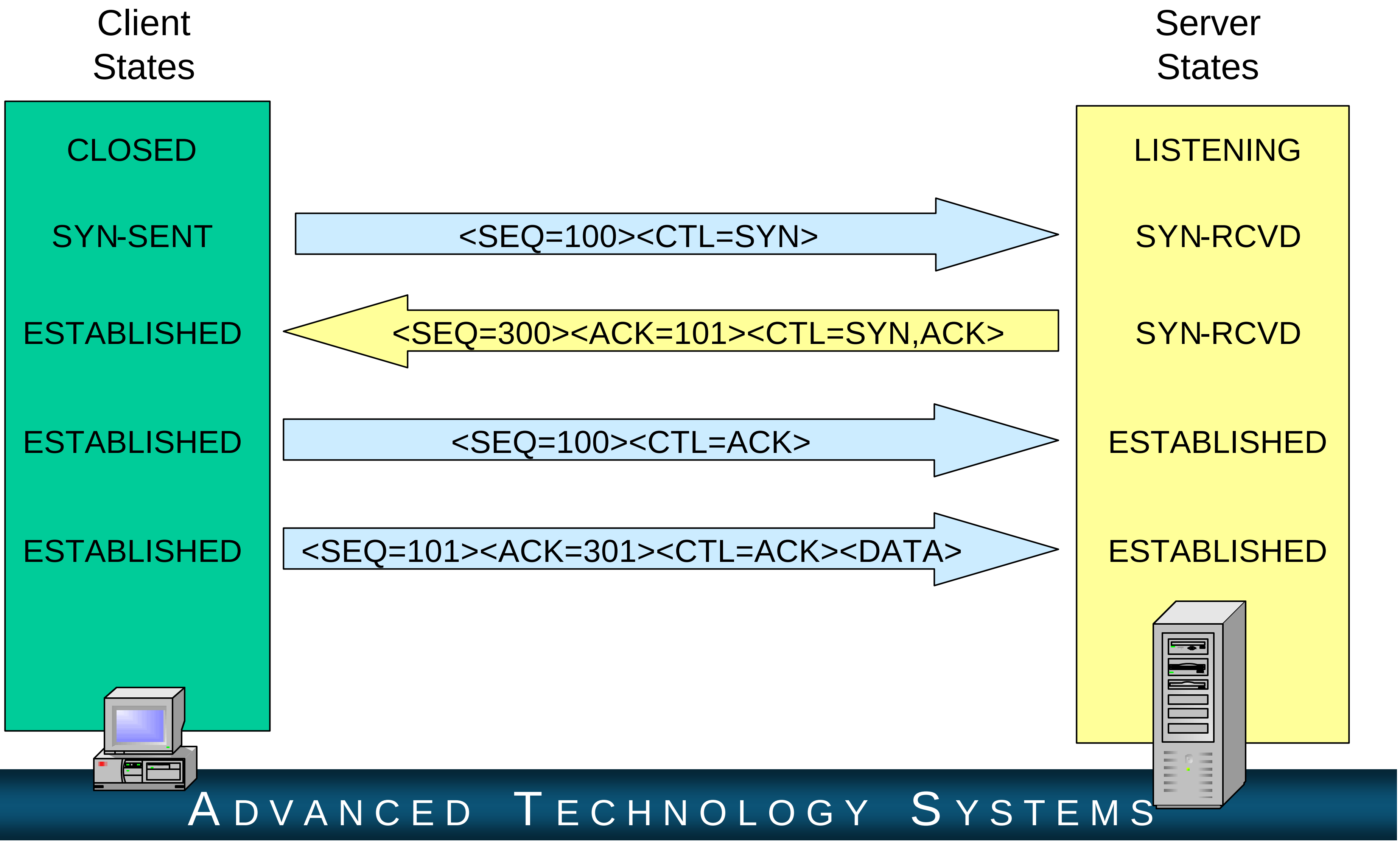
Stateful Firewalls

Stateful Firewalls

- Primarily layer 4 and below
- Layer 7 for initial packet inspection
- Uses “state table” entries to track established communications
- Faster than proxy firewall technology
- Less secure than full proxy
  - Only application aware for session establishment

Stateful Firewalls

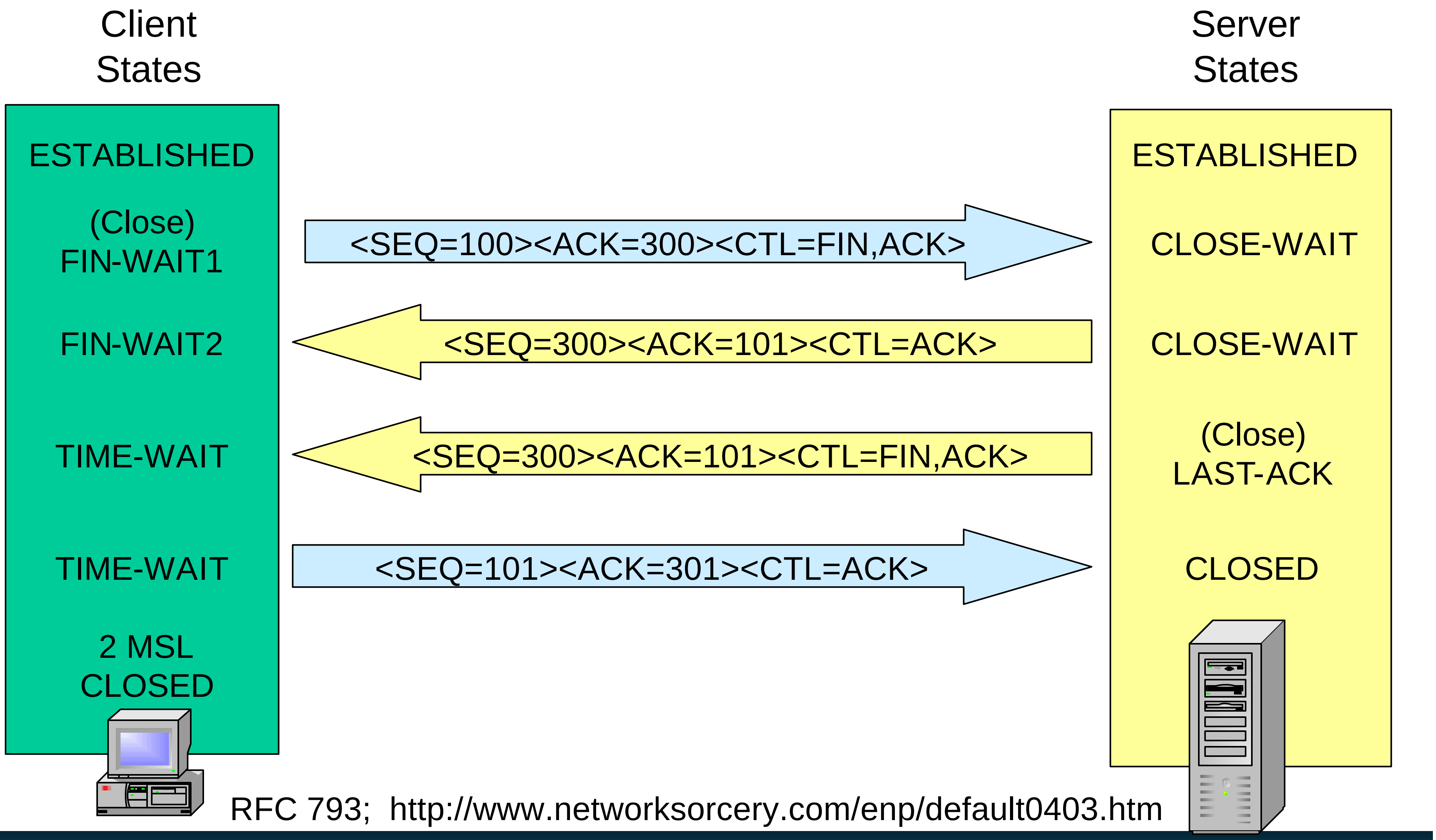
The Concept of State – TCP 3-Way Handshake



Client States		Server States
CLOSED		LISTENING
SYN-SENT	<SEQ=100><CTL=SYN> →	SYN-RCVD
ESTABLISHED	← <SEQ=300><ACK=101><CTL=SYN,ACK>	SYN-RCVD
ESTABLISHED	<SEQ=100><CTL=ACK> →	ESTABLISHED
ESTABLISHED	<SEQ=101><ACK=301><CTL=ACK><DATA> →	ESTABLISHED

Stateful Firewalls

The Concept of State – TCP Normal Close



Client States		Server States
ESTABLISHED		ESTABLISHED
(Close) FIN-WAIT1	<SEQ=100><ACK=300><CTL=FIN,ACK> →	CLOSE-WAIT
FIN-WAIT2	← <SEQ=300><ACK=101><CTL=ACK>	CLOSE-WAIT
TIME-WAIT	← <SEQ=300><ACK=101><CTL=FIN,ACK>	(Close) LAST-ACK
TIME-WAIT	<SEQ=101><ACK=301><CTL=ACK> →	CLOSED
2 MSL CLOSED		

RFC 793; http://www.networksorcery.com/enp/default0403.htm

UDP and State

- Connectionless protocol – has no state
- Tracking in pseudo-stateful manner
- State tracked by socket (?)
- No connection, no close
  - Tear-down table entries on time-out: <1min
- Reliant on ICMP for error correction
  - Stateful FW must allow associated ICMP

ICMP and State

- Connectionless protocol – has no state
- Tool used by TCP and UDP
- One way “response” for Layer 4 protocol
  - Difficult to include in state analysis
- Request/response (e.g. – ping) easier to track
  - Based on request/response message type
  - Offset 0 in ICMP header
- No close – time-out dictates retention
- Good Stateful FW has ability to look at ICMP payload (data)
  - Match to state table communications

Multimedia and Stateful FW

- MM protocols work in similar fashion to FTP
- TCP control channel directs establishment of (multiple) data channels
- Application aware Stateful FW allows establishment
- Beyond that – not application aware
  - Relative weakness of Stateful FW
- Support is on a per-protocol basis
  - Your mileage may vary….

Review of Stateful FW

- “Fast”
- More secure than regular packet filtering
- Less secure that proxy firewall
- Stateful inspection is application specific
  - Must know how to “inspect” protocol – stateful inspection
  - If not, stateful packet filtering is used
- If application not supported, may need to open holes
  - FTP, DCOM, ICMP unreachable errors
- Susceptible to covert channels on open ports
- AOL IM, Gnutella, go2mypc.com

Stateful FW Products

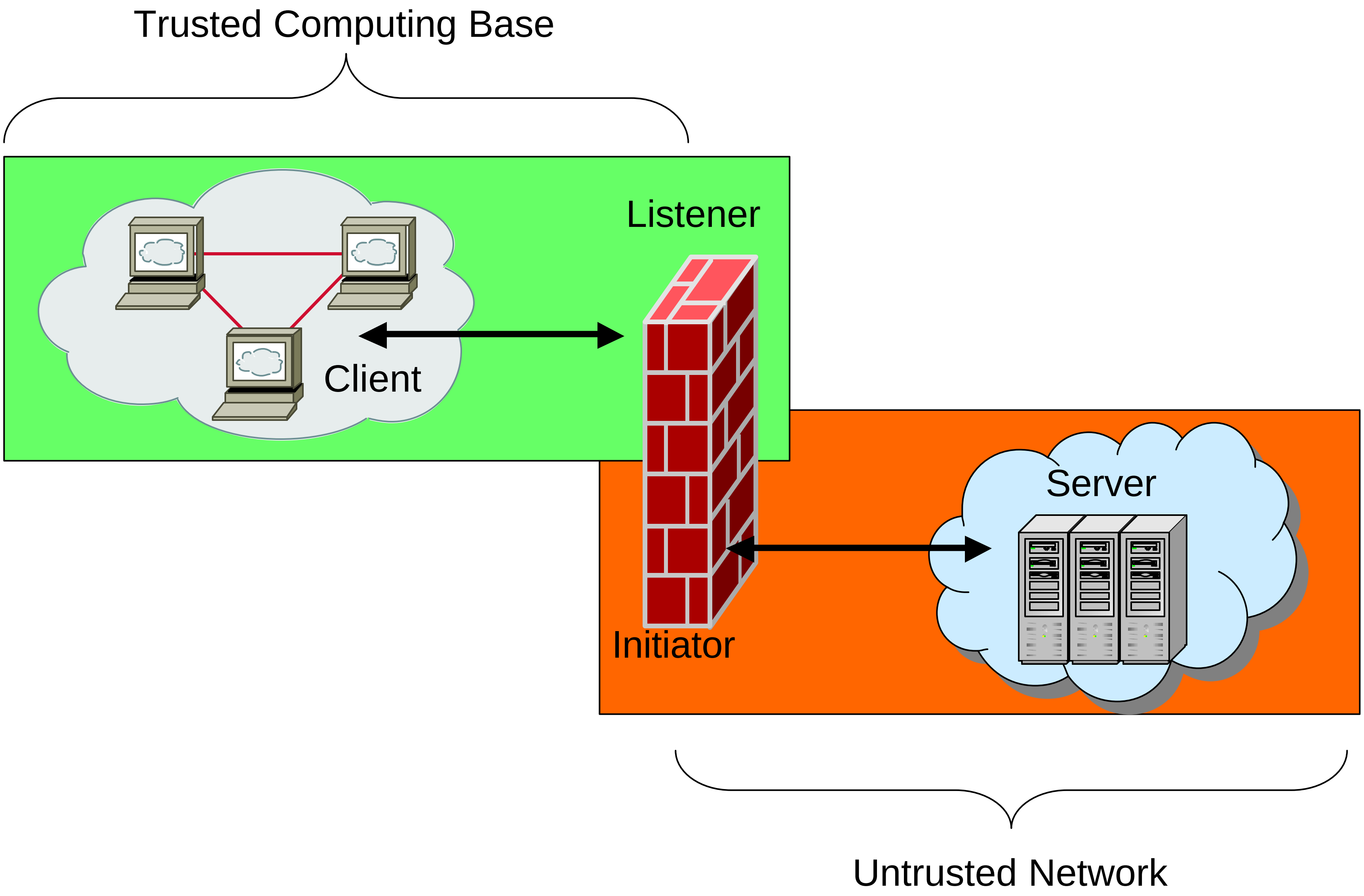
- Cisco Reflexive ACLs
- Netfilter/IPTables
- Check Point FireWall-1
- Cisco PIX Firewall
- NetScreen

Proxy Firewalls

Proxy Firewalls

- What is a proxy?
  - An application designed to act as the go-between
  - Accepts a request from a client
    - May screen or filter that request
  - If allowed, passes request to server
  - Receives server response
    - May screen or filter response
  - If allowed, passes response back to client
- So – fills role as both client and server, referred to as initiator and listener, respectively
- No direct end-to-end communications

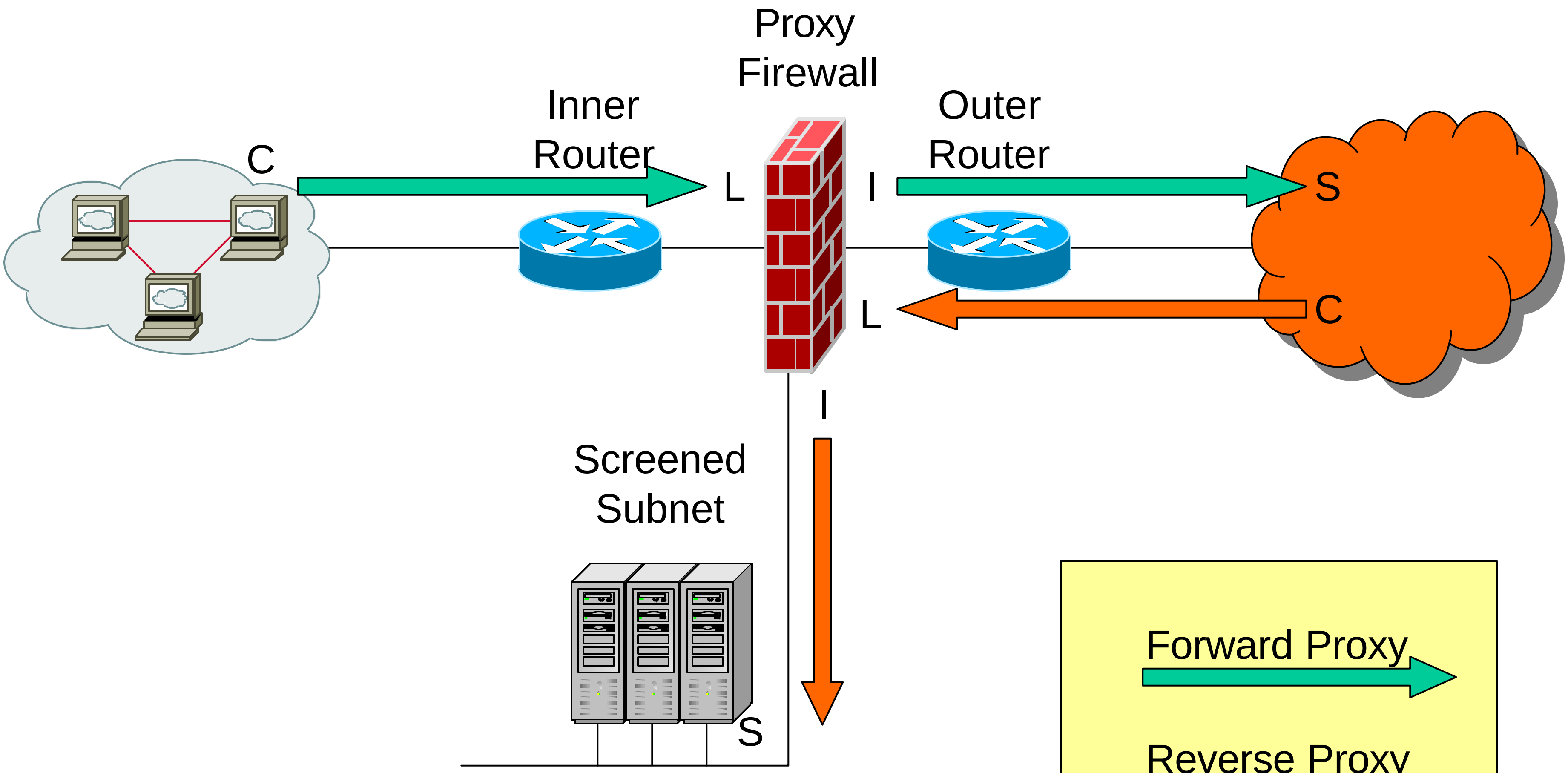
Proxy Firewalls



Proxy Firewalls

- Types of Proxies
  - Forward proxy
  - Reverse proxy
  - Circuit-level proxy
  - Application-level proxy
  - Cutoff Proxy

Forward/Reverse Proxies



Forward Proxy 🟩

Reverse Proxy 🟧

Proxy Firewalls

- Circuit-Level Proxy
  - Validates and monitors sessions – Layer 5
  - Verifies proper RFC 3-way handshake
  - Verifies legitimacy of sequence numbers in establishing connection
  - Expanded capabilities over SI / Packet Filter
    - In addition to ports, IPs, and protocols
      - User ID / Time of Day
- Application-Level Proxy
  - Application specific proxies
  - Prevents direct connection between trusted and untrusted
  - Proxies examine entire packet – can filter at application layer
  - Implemented for each service to be analyzed
  - If this is only way in / out, no proxy means no talk

Proxy Firewalls (cont)

- Cutoff Proxy
  - Verifies RFC 3-way handshake
  - Limited application-based authentication
  - Switches to dynamic packet filter mode after connection /authentication complete
  - Does not break client / server model for duration of connection

Advantages of Proxy Firewalls

- Internal addresses / topology shielded
- Robust logging
- User-based policies enforceable
  - including support for strong authentication
- Application awareness
  - Uses all 7 layers in making decisions
  - Spoof resistant
- Strong Application Proxy culls all unacceptable fields prior to forwarding
  - Buffer overrun and covert channel protection

Disadvantages of Proxy Firewalls

- Slower than SI and static packet filtering
- Proxy must be available for each application or protocol to be analyzed
- Proxy firewalls are vulnerable to OS and application level-bugs
- May be more complex to install, operate, and maintain

Firewalls in Summary

- Network security is the proper balance of trust and performance
- Higher up the OSI model – more processor intensive
- Higher up the OSI model – greater protection
- Newer computing technologies are narrowing the gap in performance issues

Security Policy

Security Policy

- Policy is the cornerstone of effective security
  - – The means by which effective DiD is achieved
  - – Provides authority for executing CND
  - – Requires support and commitment of senior management / leadership
  - – Must be enforceable….but won't always be!

Developing Security Policy

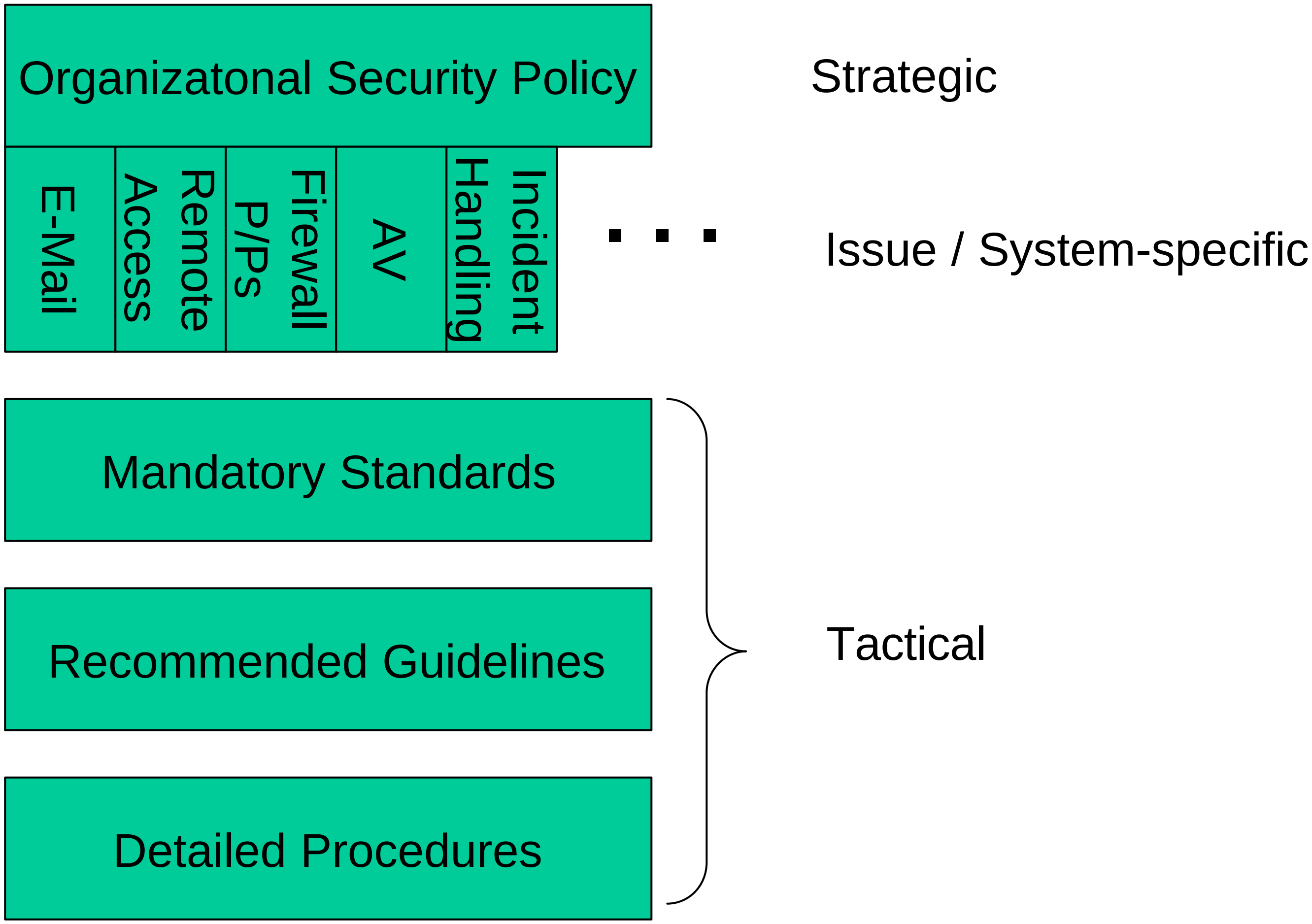
At the Enterprise Level

- Approach depends on where the organization is
  - Obtain senior management / leadership buy-in
  - Assessment of external laws and regulations
  - Assessment of external strategic plans
  - Assessment of internal strategic plans
  - Assessment of internal policies, standards, guidelines, and procedures
  - Identify the policy gaps
  - Draft and staff necessary policy(ies)
  - Senior management publishes

Developing Policy

At the Enterprise Level

Recommended structure



Organizatonal Security Policy

Strategic

E-Mail

Remote Access

Firewall P/Ps

AV

Incident Handling

. . .

Issue / System-specific

Mandatory Standards

Recommended Guidelines

Detailed Procedures

Tactical

Developing Policy

- Identify Risks
- Communicate your findings
- Create / update security policy as needed
- Determine Policy Compliance
- Sound out Organization's Rules and Culture

Key Elements of Policy

- Authority
  - – Where this policy draws it authority from
    - Signature of individual that holds authority
    - Higher level legislation or policy
- Scope
  - – Who, what, where
- Expiration
  - – When

Hallmarks of Good Policy

- Unambiguous, specific, clear
  - “The head of a Federal agency may employ standards for the cost effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.”
- Concise
  - “Federal agencies may implement standards that are more restrictive, but not less restrictive, than standards established by the Secretary of Commerce.”
- Realistic

Perimeter Considerations

- Presumption of privacy
  - Know organizational expectations
  - Know applicable laws and regulations
  - Get the lawyers involved
  - Capture in your policy and procedures
  - Publicize
  - Involve law enforcement where appropriate!
- E-Mail handling
  - See above
  - Capture in policy and publicize

Perimeter Considerations

- Incident Handling
  - Policy and procedures need to be clearly spelled out
  - Immediate action drill
  - Appropriate notifications
  - Roles and responsibilities
    - Who has authority to act? Limitations?
  - A detailed process flow, that is practiced and refined
  - After action review and adjustment

The Router

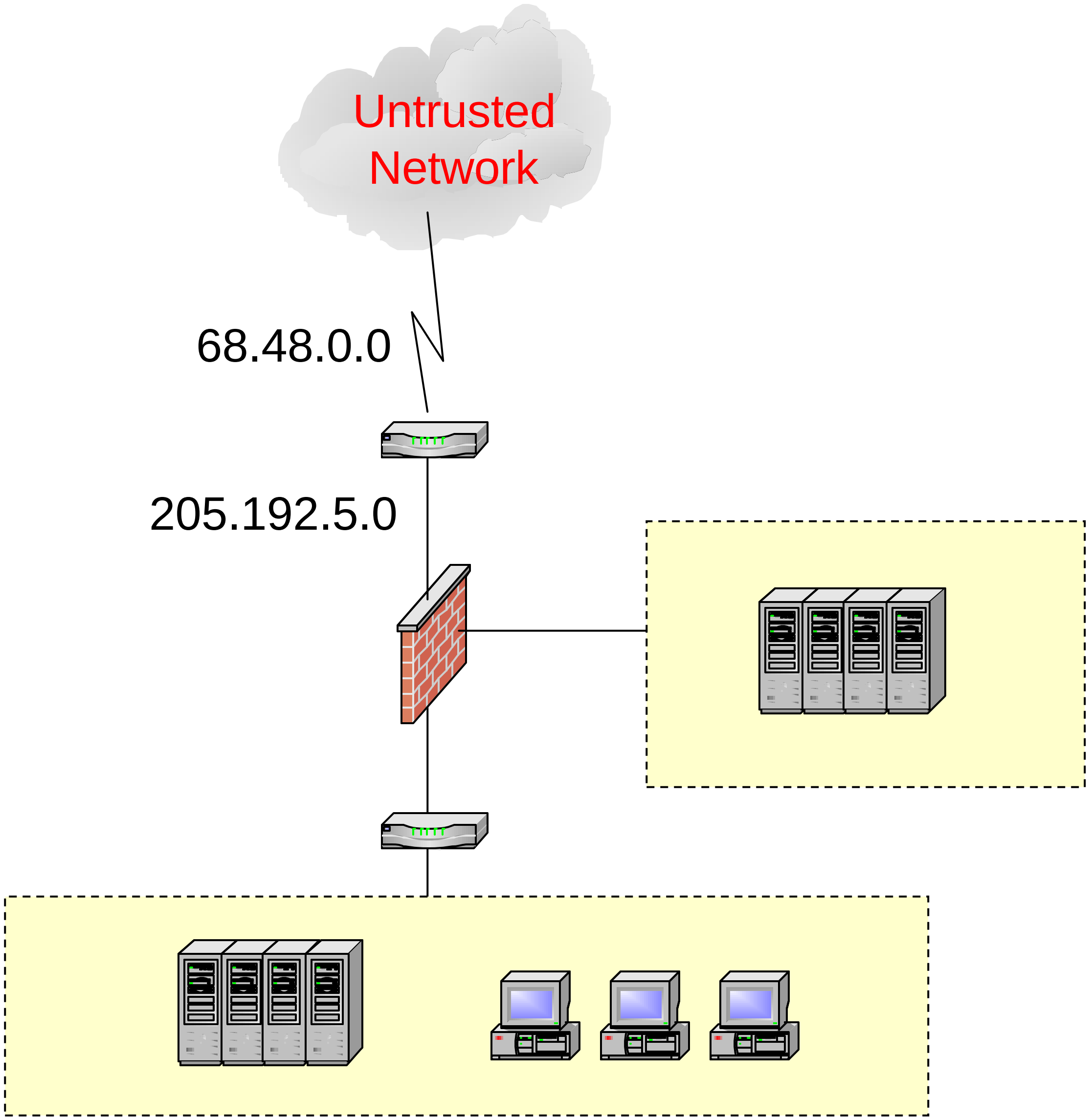
The Router as a Perimeter Device

- Interconnection Only
  - Provides connectivity between your net and internet
  - Reliant on other security elements
- Stand-alone Security
  - Low-risk environment
- Interconnection and Filtering
  - Focuses on routing and some filtering
  - One component of perimeter security and DiD
- Only perimeter security w/DiD
  - NIDS, HIDS, Anti-Virus, Host Firewalls

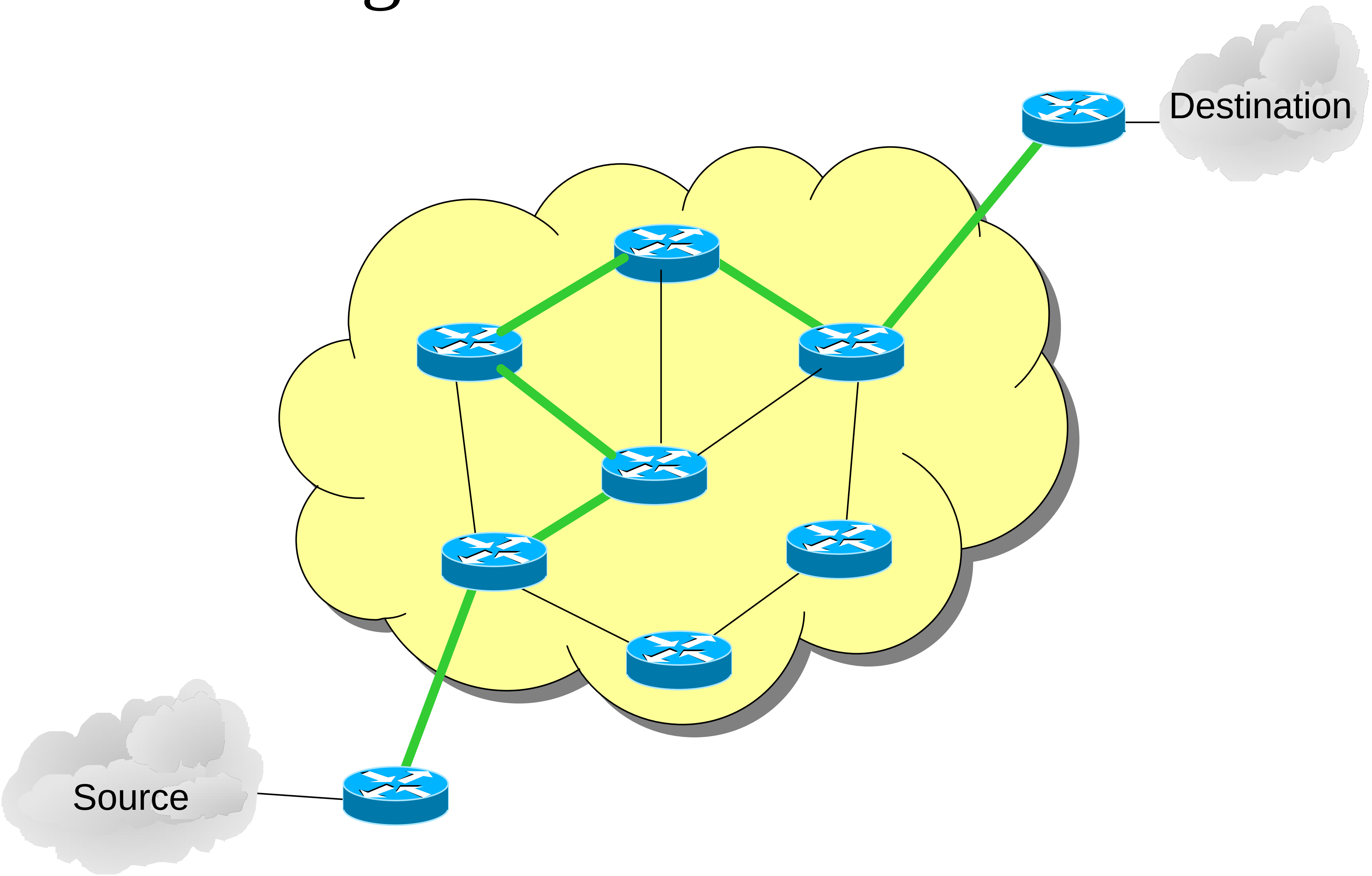
The Router as a Perimeter Device

- Primary role is interconnection
- Additional duties add load
  - May impact performance
  - Sizing router must be based on functions
  - Balance work among perimeter devices
  - Each to their strengths
  - Consider external storage
    - Not just for router configs/logs (FTP/TFTP, Syslog)
    - Firewall logs

Routing – What Routers do Best



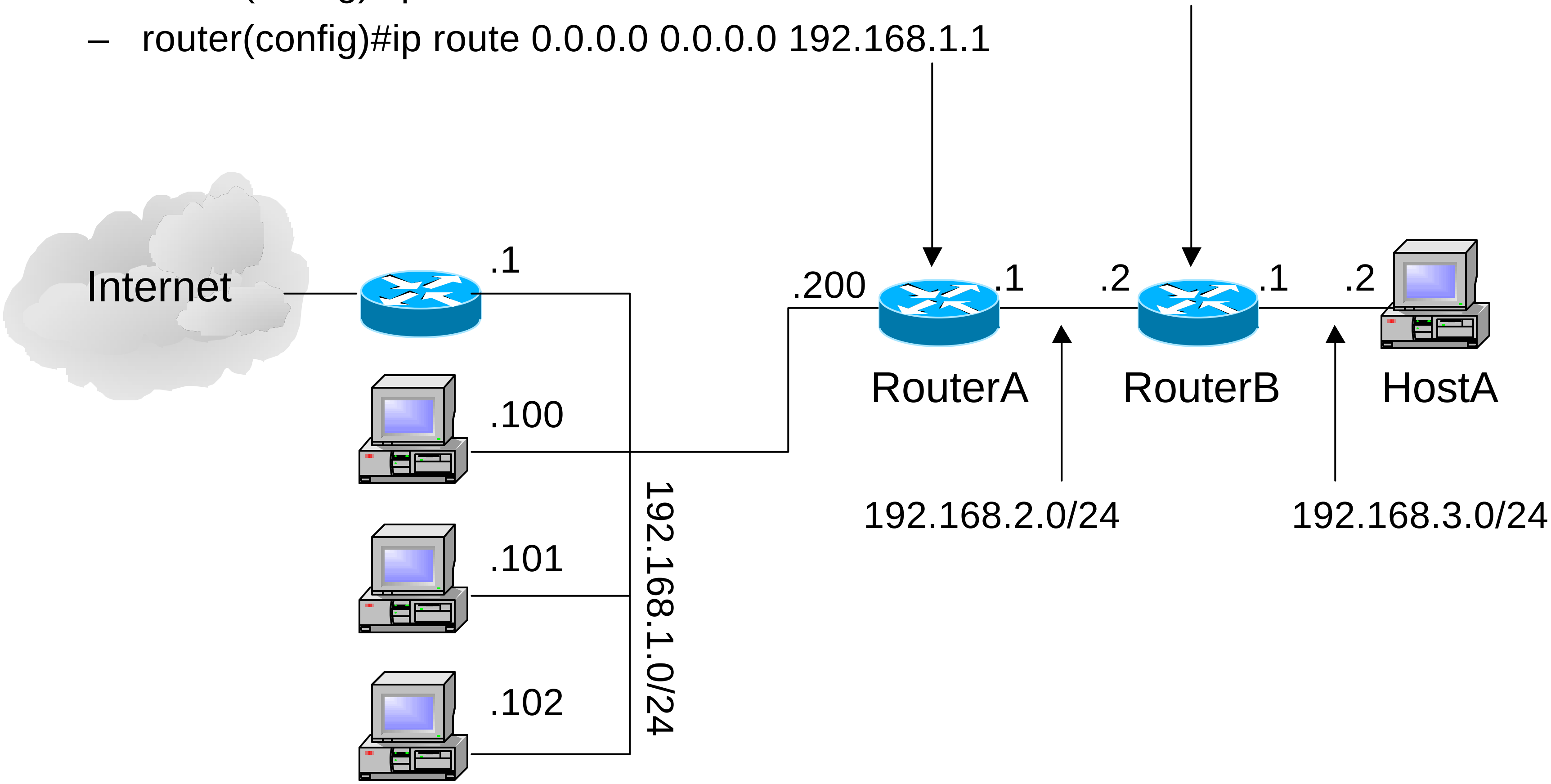
Routing – What Routers do Best



Static and Dynamic Routing

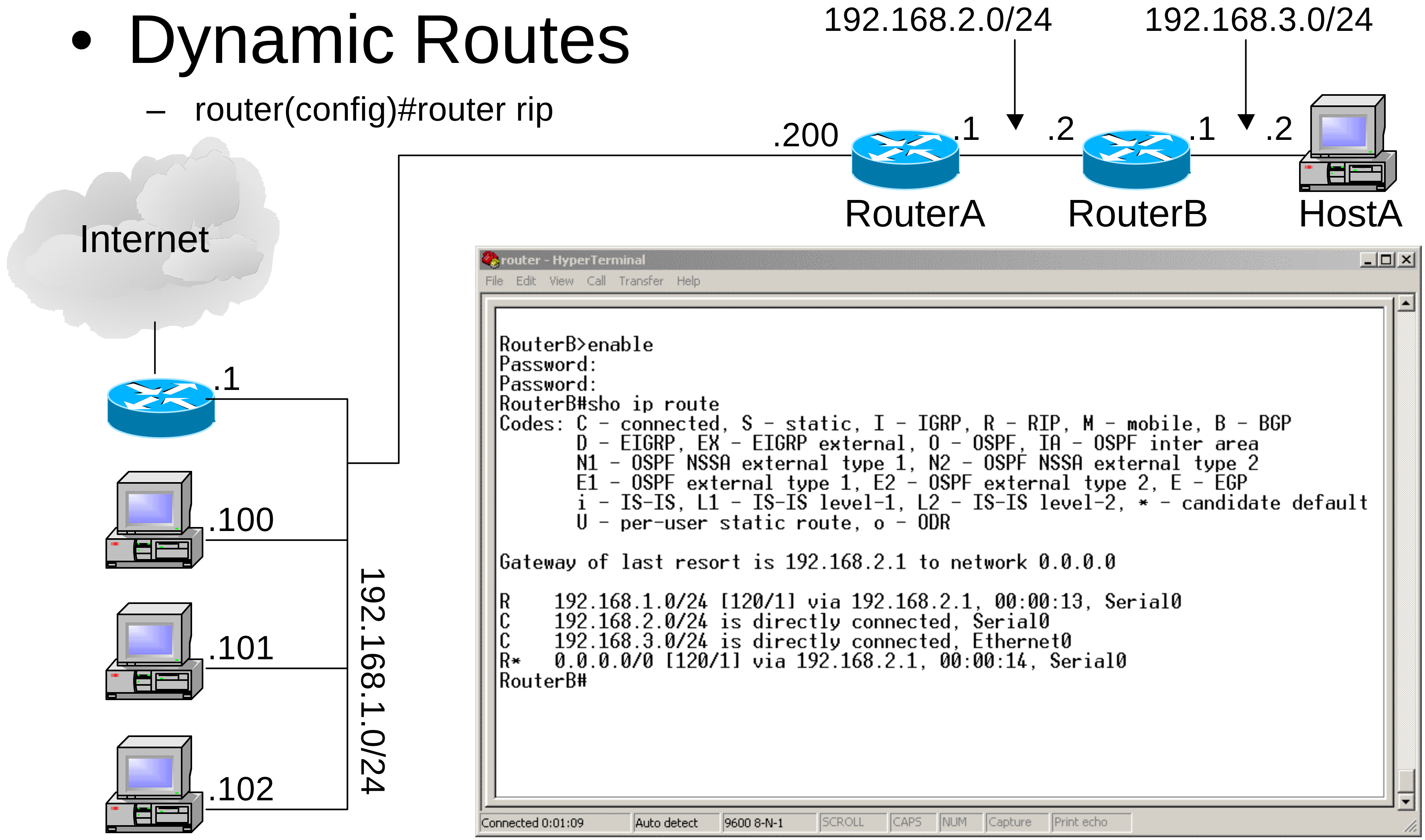
Static Routes

- router(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
- router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1



Static and Dynamic Routing

- Dynamic Routes
  - router(config)#router rip



```
RouterB>enable
Password:
Password:
RouterB#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is 192.168.2.1 to network 0.0.0.0

R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:13, Serial0
C    192.168.2.0/24 is directly connected, Serial0
C    192.168.3.0/24 is directly connected, Ethernet0
R*   0.0.0.0/0 [120/1] via 192.168.2.1, 00:00:14, Serial0
RouterB#
```

Secure Dynamic Routing

- Route Authentication
  - Secret keyword
  - Used along w/route update information
    - Generates MD5 hash signature
    - Sent w/route updates
  - Confirmed by recipient who has same keyword
  - Supported by RIPv2, OSPF, EIGRP & BGP
    - Not supported by RIPv1 or IGRP
      - Validate-update-source
      - Verifies source is valid for segment
      - Spoofable on segment
- passive interface <interface>
- distribute-list <number> <in | out> <interface>

The Router as a Security Device

- Support many security features
  - – Packet Filtering
  - – Network-Based Application Recognition (NBAR)
  - – Network Address Translation (NAT)
  - – Port Address Translation (PAT)
  - – Virtual Private Network (VPN)
  - – Context Based Access Control (CBAC)
- Role of the Router Based on:
  - – Requirements – Security Policies
  - – Overall Defense in Depth Architecture
  - – Funding Available

The Router as a Security Device

- Router as a Packet Filter
  - Covered extensively in previous session
  - Well suited for ingress and egress
- Network-Based Application Recognition
  - Serves as a governor on BW based on:
    - HTTP information (MIME Type, URLs, host names, static/dynamic port information)
  - Uses Packet Description Language Modules (PDLM) to enable for specific protocols
    - Many PDLMs available (60+)
    - New PDLMs can be added on the fly
  - Enables "QoS"
  - Prevents self-inflicted DoS on critical apps
  - Prevents DoS from network "noise"

Lone Perimeter Security

- Routers provide wide range of capabilities
- Stand-alone might be acceptable for:
  - Home environment
  - SOHO
  - Internal network segment
  - Low-risk environment
- Always use as part of DiD
- Always hardened

Network Address Translation

- Private Address Space
  - 10.X.X.X; 172.16.0.0 – 172.32.255.255; 192.168.X.X
- Static mapping supports bi-directional connections
- Dynamic mapping requires pool of assignable IP for public use
- Overloading, or PAT, allows more sessions than outside IPs
  - Your home network?
  - Uses dynamic port assignment to enable overload

Source IP/port	Translated IP/port	Contacted IP/port
192.168.1.100/1048	68.48.224.20/1048	167.216.198.40/80
192.168.1.102/1048	68.48.224.20/1111	64.82.100.87/80

Network Address Translation

Limitations

- Good for privacy
- Limited security once connection is established
  - Standard NAT especially vulnerable
    - No port awareness
    - Use of ACLs or CBAC to augment
  - PAT adds port awareness
- Outbound connections clear
  - Trojan
- NAT/PAT used as part of effective defense
  - Add packet filtering or stateful inspection

Context-Based Access Control

- Full-featured stateful inspection method for Cisco routers
- Supports most popular protocols
  - Full tracking of state
  - Dynamic access lists maintained
  - Verifies validity at the application layer
    - Prevents misuse of open ports
    - Helps prevent session hijacking
- Augment with ACLs, NBAR
- Router Resource Intensive

CBAC w/NAT Configuration Attached - © 1992-2001 Cisco Systems

Router Hardening

- Forward Line of Troops
- Disable Unneeded Services/Servers
- Block all Unnecessary Traffic Types
- Lock Down Configuration Methods
- Posting of Warning Banners
- Log Heavily and Monitor
- Keep Patches Current!!

Disable Unneeded Servers / Services

- Organizational Policy Driven
  - – Don’t need it, don’t run it!
  - – Applies to all computing devices in your network
  - – Examples - Servers:
    - SNMP, CDP, Bootp, TFTP, HTTP
  - – Examples – Services:
    - Small services (echo, chargen, discard); time; network time protocol, finger

Blocking Unnecessary Traffic

- Policy Driven – A Theme
- Varies Based on Requirements
  - Allow select ICMP to screened subnet
  - Disallow all ICMP to/from TCB (?)
    - Packet-too-big outbound an exception?
  - router(config-if)#no ip directed-broadcast
    - Prevents Smurf-like attacks
    - Implement on all router interfaces
      - www.powertech.no/smurf - Top 10!
  - router(config-if)#no ip redirects
  - router(config)#no ip source-route

Securing Administration Methods

- Where Policy Permits – Provide Controls
  - Control Telnet Access
  - Use SSH in Place of Telnet
  - Use of RADIUS or TACACS(+) for Authentication
  - Management and TFTP/FTP

Router Warning Banners

- Check with Legal Counsel
- Don’t give away information
- Let “users” know they should not be here
- Let “users” know they will be monitored
- Let “users” know they will be prosecuted

Example Warning Banner

DoD Warning Banner

Use of this or any other DoD interest computer system constitutes consent to monitoring at all times.

This is a DoD interest computer system. All DoD interest computer systems and related equipment are intended for the communication, transmission, processing, and storage of official U.S. Government or other authorized information only. All DoD interest computer systems are subject to monitoring at all times to ensure proper functioning of equipment and systems including security devices and systems, to prevent unauthorized use and violations of statutes and security regulations, to deter criminal activity, and for other similar purposes. Any user of a DoD interest computer system should be aware that any information placed in the system is subject to monitoring and is not subject to any expectation of privacy.

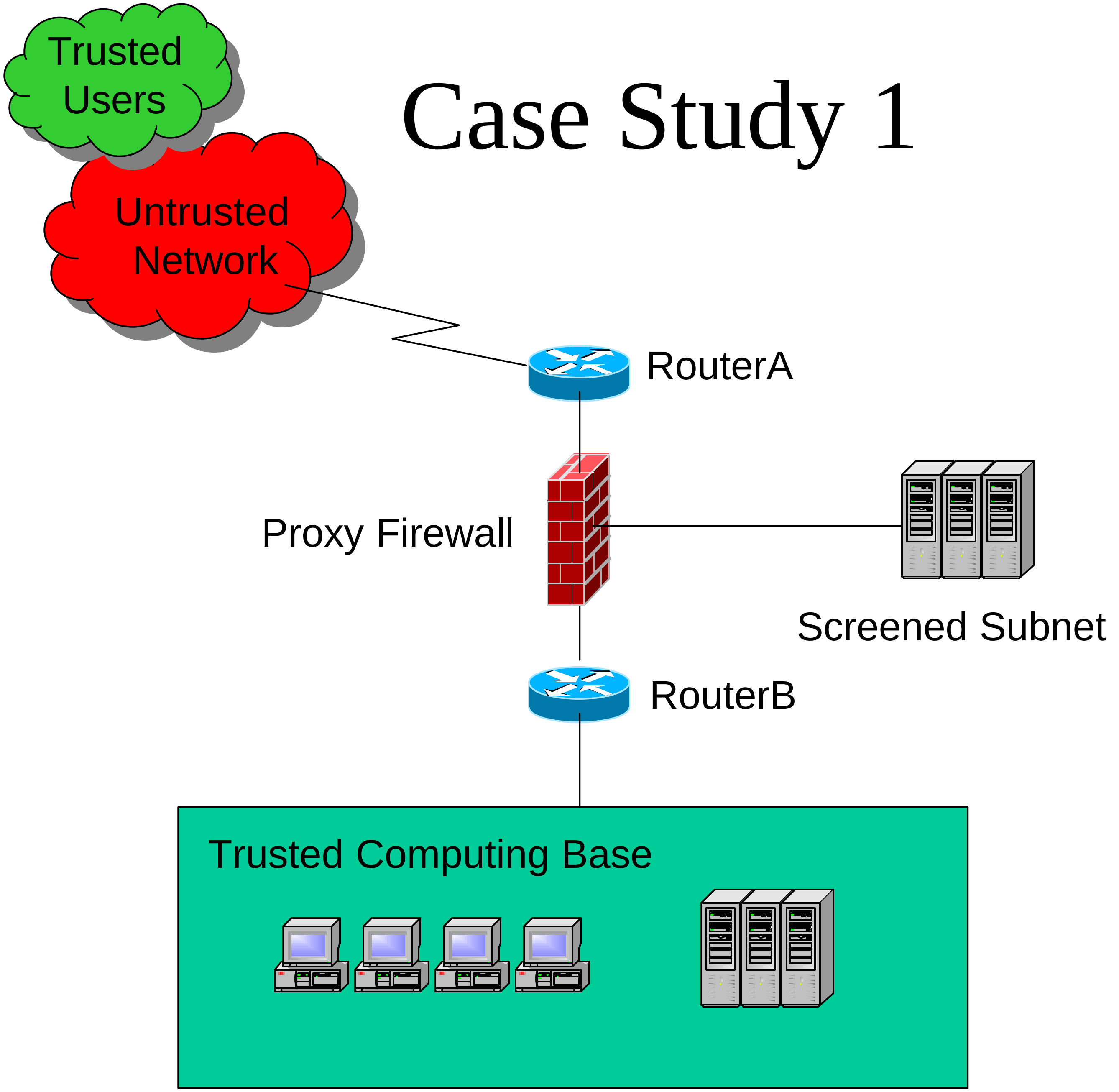
If monitoring of this or any other DoD interest computer system reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring of this or any other DoD interest computer systems reveals violations of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of DoD interest computer systems are subject to appropriate disciplinary action.

Use of this or any other DoD interest computer system constitutes consent to monitoring at all times.

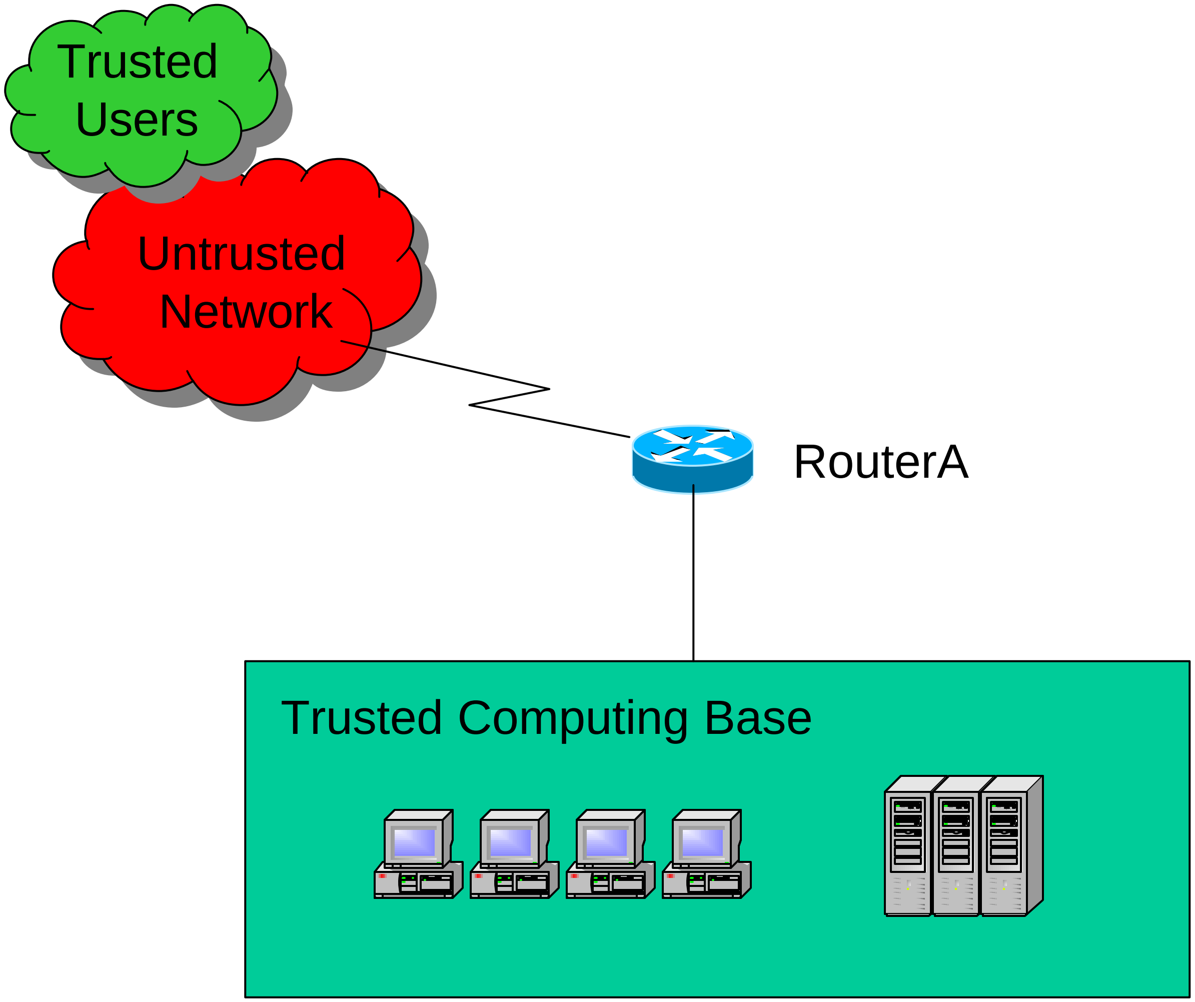
Summary

- Routers play a significant role in DiD
- Routing is what they do best
- Screening classic and appropriate role
- Can provide QoS and DoS defense
- As primary firewall: CBAC, ACLs, NAT
- As with all key devices – protect it!

Case Study 1


Trusted Users
Untrusted Network
RouterA
Proxy Firewall
Screened Subnet
RouterB
Trusted Computing Base

Case Study 2


Trusted Users
Untrusted Network
RouterA
Trusted Computing Base

Network Intrusion Detection

Network Intrusion Detection

Basics

- Host-based Intrusion Detection Systems
  - Monitors specific system and interfaces
  - Log analyzers
  - File integrity software
- Network Intrusion Detection Systems
  - Monitors network segment
  - Examines network traffic
  - Detects scans, probes and attacks
  - Two basic IDS methods:
    - Signature-based ID
    - Statistical anomaly-based ID
- You don’t know what you don’t know!

Network Intrusion Detection

Signature Matching

- Network-based IDS signatures
  - A pattern of network traffic to be matched
  - Generates a response
    - Alert, Log, Defensive Action
  - Signatures adapted to your environment
    - Running DNS?
    - Running IIS?
    - Running Unix?
  - Vendor specific depth of analysis
  - Updating signatures

Network Intrusion Detection

Tuning Your System

- Specific signatures
  - More accurate in positive ID
  - Resource Intensive
  - More likely to miss a morphed attack (false negative)
- General signatures
  - More likely to catch morphed attack
  - Less resource intensive
  - More likely to generate false positives
- Tuning and IDS system is critical
- Finding the balance is the art!

Network Intrusion Detection

Alerting, Logging, and Reporting

- Signature Matched or Anomaly Detected
  - Alert
    - Analyst Console, E-mail, SNMP trap
  - Logging and Reporting
    - Recommend centralized database/repository
    - Allows cross-sensor correlation
    - Helps identify low and slow attacks
  - Active Response – Pros and Cons
- Log analysis and event correlation
  - The brass ring

Network Intrusion Detection

Outsourcing

- Many organizations turning to outsourcing
  - – Real world example – NMCI
  - – NMCI only a segment of enterprise
  - – Correlation of all sensor data required
  - – USMC must retain response control
    - Faster, more surgical response is always the goal
    - Operational awareness is a critical element
  - – Parallels in industry?

Roles of NIDS in Perimeter Defense

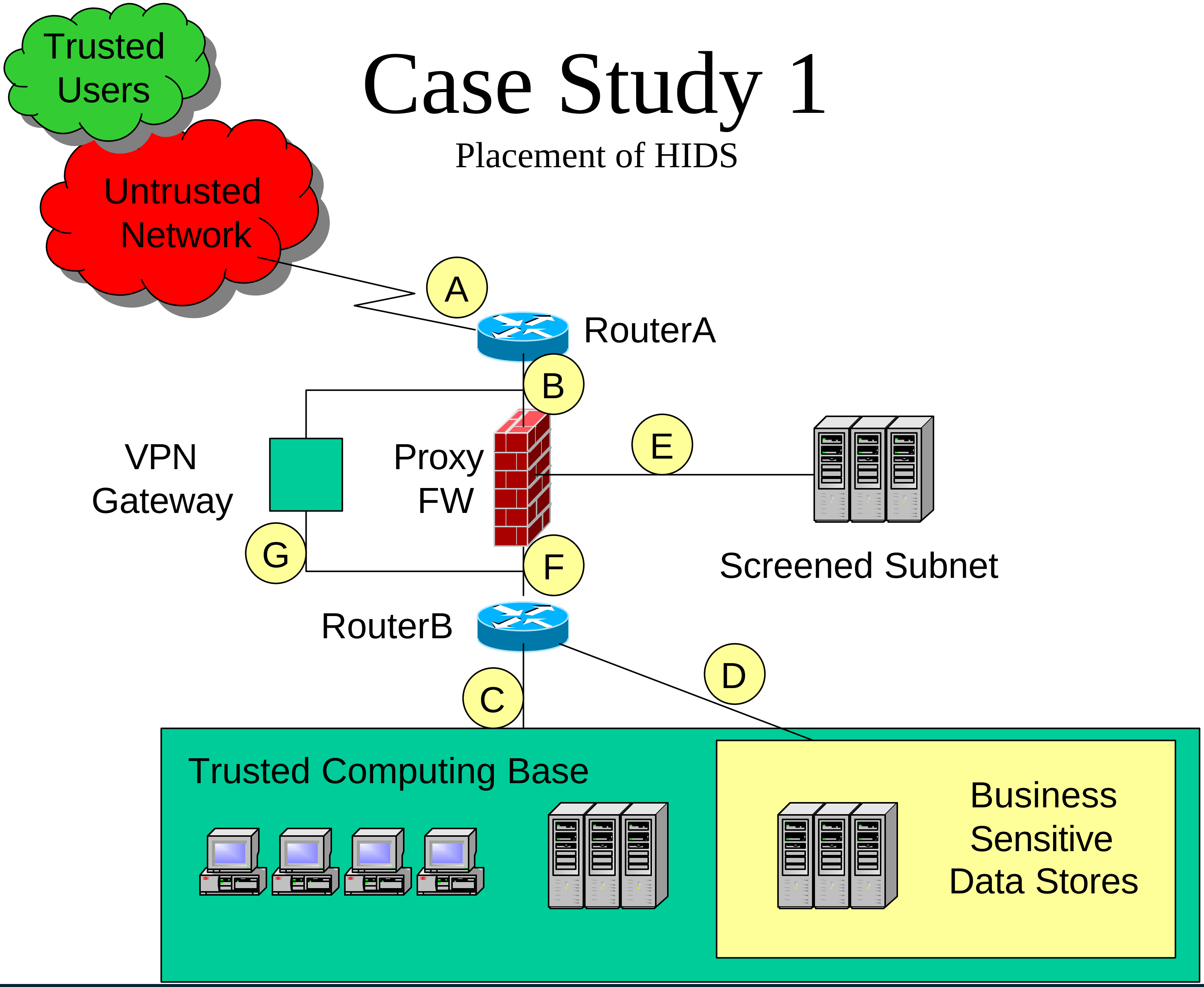
- Identifying Weaknesses/Vulnerabilities
  - Identify denied activity
  - Identify policy violations
- Detecting the Insider Attack
  - Unauthorized outbound traffic
- Incident Handling and Forensics
  - Tracking an attack
  - Tuning to a focused investigation
- Complementing Other Components
  - Correlation of network activities
  - Augment stateful firewall w/application analysis
    - Port 80 trojan discussion

IDS Sensor Placement

- Deploy Multiple Network Sensors
- Placing Sensors Near Filtering Devices
- Placing Sensors on Internal Network
- Working with Encryption
- Processing in High Traffic Situations
- Configuring Switches
- Using and IDS Management Network
- Maintaining Sensor Security
- Hybrid Firewall/IDS Solutions

Case Study 1

Placement of HIDS



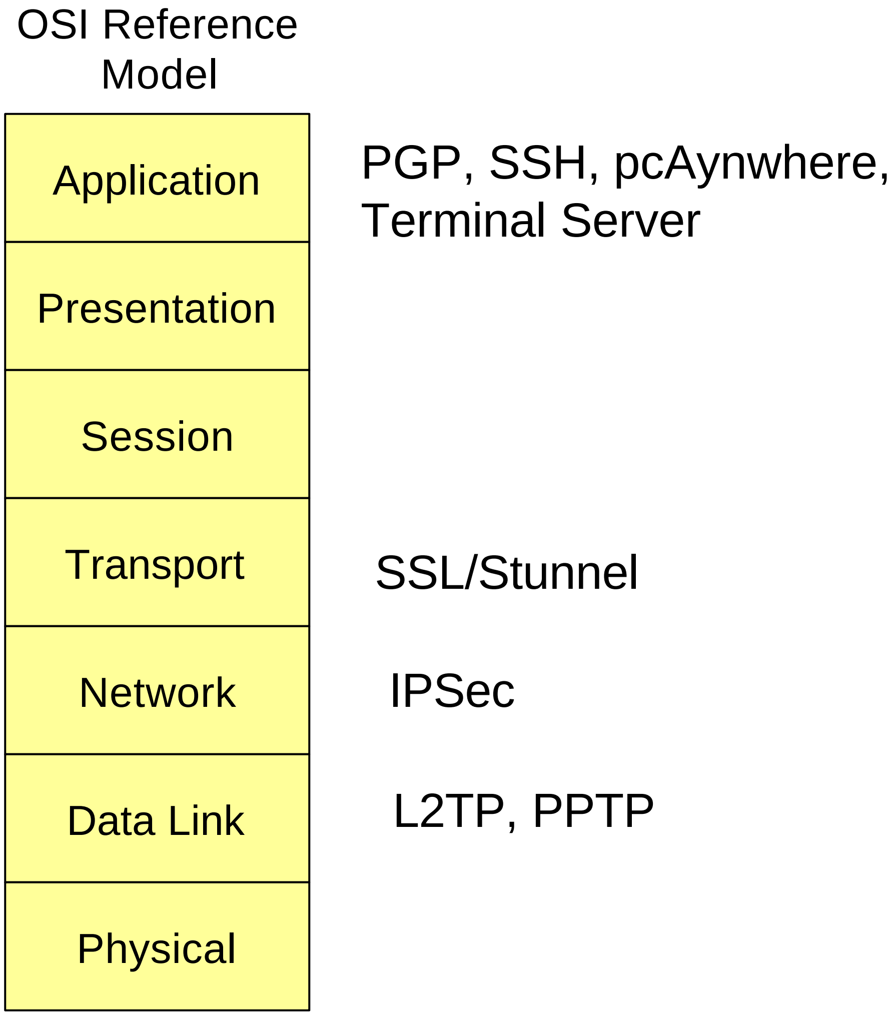
Summary

- HIDS play a critical role in DiD
- Tuning is critical, and hard to do right!
  - Tuning is continuous
  - Testing helps assess tuning efforts
- Placement is based on architecture and requirements
- Correlation and analysis is the brass ring

Virtual Private Networks

VPN Basics

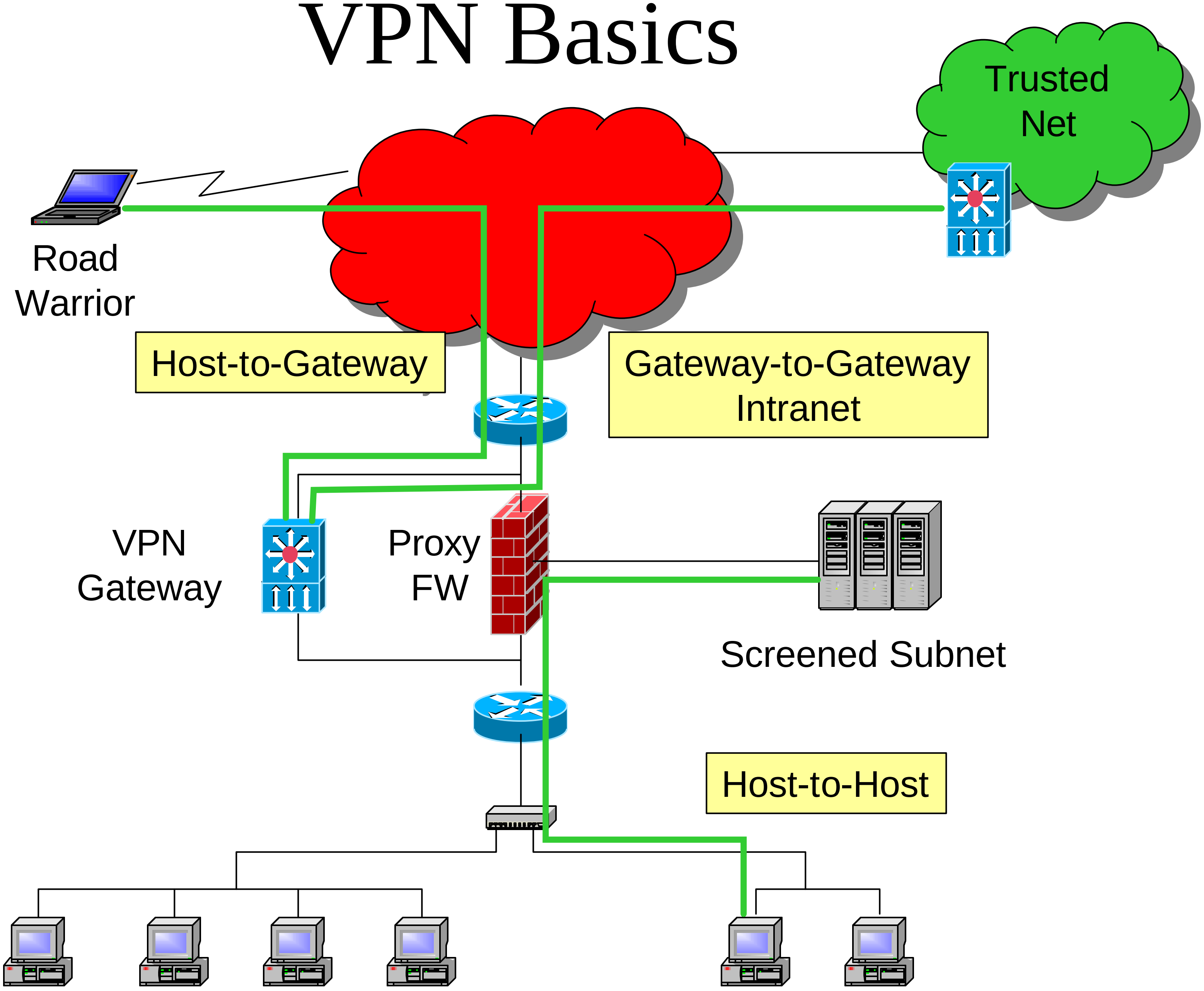
- Secure communications over unsecure path
- Three basic types
  - – Gateway-to-gateway
  - – Host-to-gateway
  - – Host-to-host
- Common VPN tools are found at various layers of OSI model



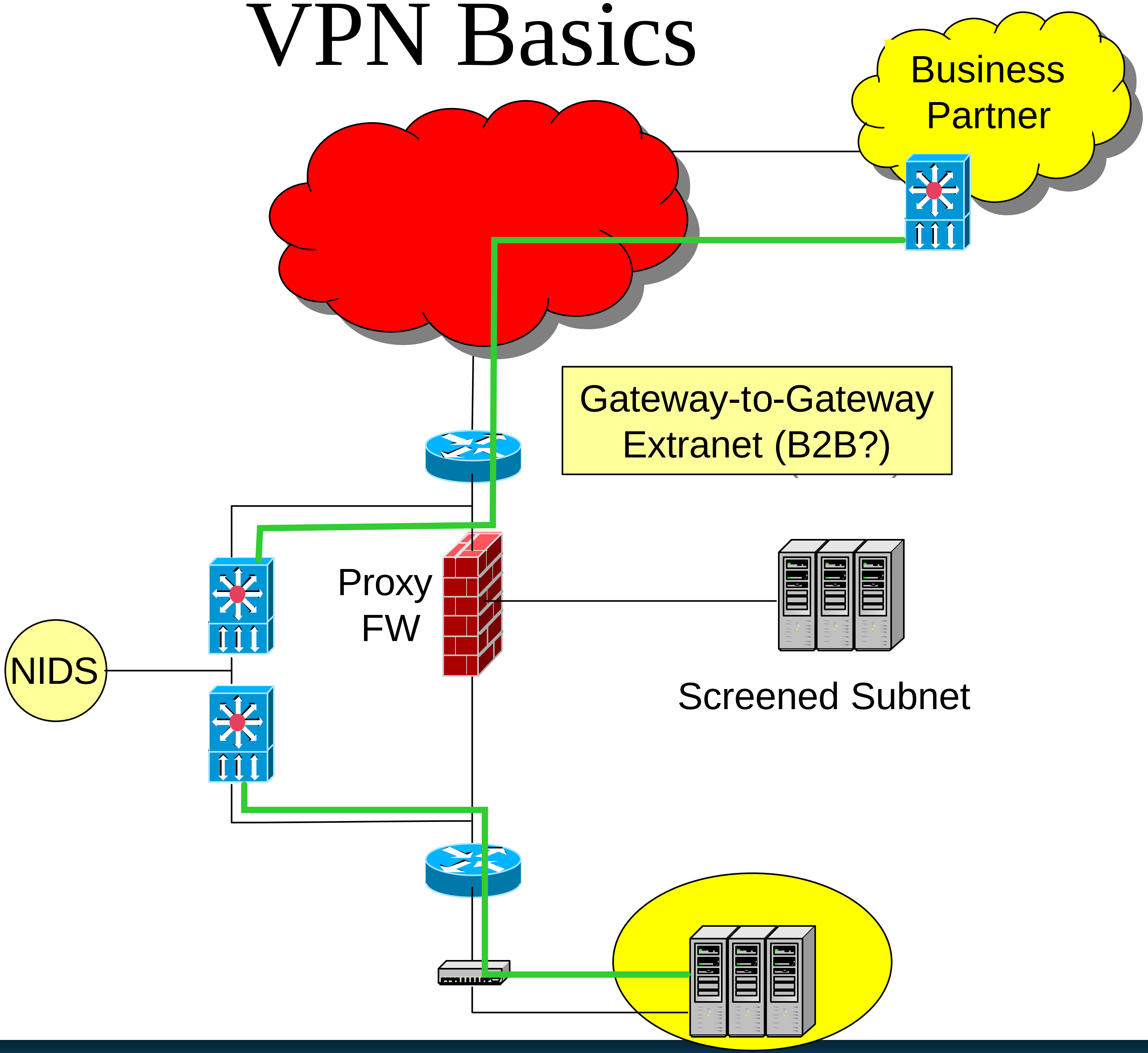
OSI Reference Model

Application	PGP, SSH, pcAynwhere, Terminal Server
Presentation	
Session	
Transport	SSL/Stunnel
Network	IPSec
Data Link	L2TP, PPTP
Physical	

VPN Basics


Trusted Net
Road Warrior
Host-to-Gateway
Gateway-to-Gateway Intranet
VPN Gateway
Proxy FW
Screened Subnet
Host-to-Host

VPN Basics


Business Partner
Gateway-to-Gateway Extranet (B2B?)
Proxy FW
Screened Subnet
NIDS

VPN Basics

- VPN Capabilities
  - Firewall
    - Augment VPN Security
    - VPNs configured to allow only authenticated, encrypted packets
  - Authentication
    - Part of every VPN – implementation varies!
      - PPTP uses ID/password
      - IPSec uses X.509 certificate (optional)
  - Encryption
    - Main defense against packet sniffing
  - Tunneling
    - Allows passing non-TCP/IP traffic across IP-based network

VPN Basics

- Types of VPNs
  - Firewall VPNs
    - Integrated w/firewall
    - Pros and Cons
  - Router/Appliance VPNs
    - Dedicated HW platform – Cisco, Nortel, Alcatel
    - Usually fastest VPN
  - Application VPNs
    - VPN provided by application on computing platform
    - Slower than Appliance, platform vulnerable (?)
  - Operating Systems
    - Windows 2000, Linux, etc….

Advantages of VPNs

- Potential cost savings
  - Allows shared packet switched networks
  - Alternative to secure RAS
- Security
  - Maintains confidentiality and integrity
  - Can provide strong authentication
  - Varies based on encryption technology
- Speed of deployment, flexibility

Disadvantages of VPNs

- Management can be complex
- WAN performance must support
  - Latency and packet loss
- Troubleshooting encrypted traffic
- Processor intensive! Plan for it.
- Packet overhead
- Extending trust!
- Availability!

IPSec Basics

Protocol Suite for Secure Communications

- Born of IPv6 – ported to IPv4
- Facilitates confidentiality, integrity and authentication
- Key protocols (we will look at each)
  - Internet Key Exchange (IKE)
  - Encapsulating Security Payload (ESP)
  - Authentication Header (AH)
- Open standard enables multi-vendor interoperability

IPSec Basics

Establishing a Security Association (SA)

- Many options available in IPSec
  - Protocols and communication modes used
  - Encryption algorithms used
  - Hash types used
- Negotiation between nodes drives how comms will take place
- Negotiated for every IPSec connection
- Details of established IPSec connections stored in Security Association DB (SAD)
- Node specific options supported built into host security policy database (SPD)

Other VPN Protocols: PPTP & L2TP

- Both Layer 2 Implementations
- PPTP
  - Encryption w/Microsoft PP Encryption
  - Authentication using MSCHAP, CHAP, PAP, EAP
  - Control channel – TCP port 1723
  - Encapsulated data channel – Variant of GRE (Generic Routing Encapsulation)
  - GRE supports tunneling of other than IP
  - Works great with NAT – Layer 2!
  - Widely available – HW and OS
  - Vulnerable to spoof and MITM

Other VPN Protocols: PPTP & L2TP

- L2TP
  - Hybrid of Cisco Layer Two Forwarding and PPTP – best of both worlds!
  - Authentication – MSCHAP, CHAP, PAP, etc.
  - Use of Control and Data Transmission Messages
    - First bit = 1 ; control, highest priority
    - First bit = 0 ; data
  - Lacks own encryption capability
    - Can use IPSec for encryption (Windows implementation)
  - Can create multiple tunnels btwn two hosts
  - Alone, vulnerable to spoof and MITM

Summary

- VPNs Offer Security, Reduced Cost, and Flexibility/Speed of Solution Deployment
- Popular VPN Protocols: IPSec, L2TP, PPTP – Pros and Cons of Each
- IPSec – Born of IPv6; includes, IKE, AH, and ESP
  - IKE is the negotiator
  - AH provides authentication and verifies integrity
  - ESP provides confidentiality
  - AH and ESP can be used together
- Layer 2 (L2TP and PPTP) solve NAT issues
  - Built on PPP – Vulnerable to spoofing/MITM
- VPNs can be difficult to manage, and may introduce vulnerabilities without careful planning

Host Hardening

The Reality

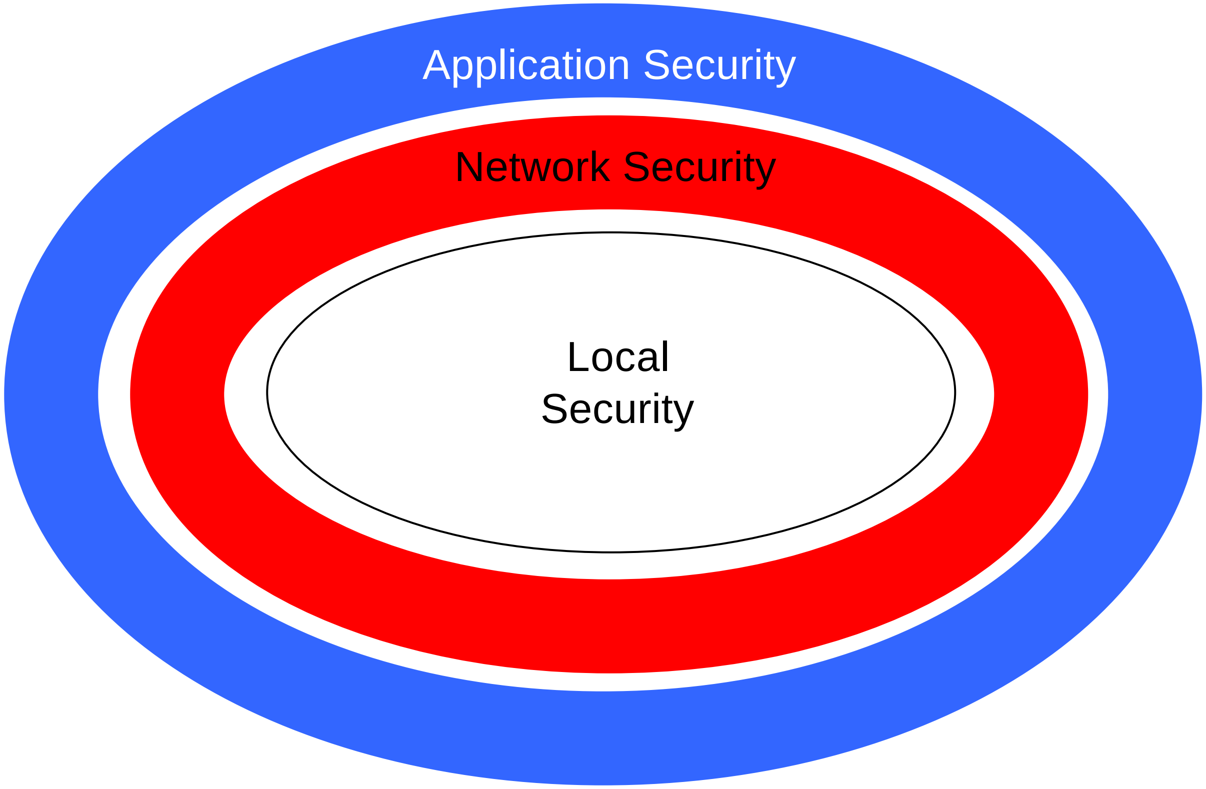
- Software/Systems Generally Ship Unsecure
  - Sold to “people”
  - Fielded to work out of the box in many environments
  - Convenience Tradeoff
- End-User is the Target
- Balance – As Always

Recommend Gold Disk Image

Develop in lab
Standard installation
Lock down
Manage Change

Book Shows 3 Layers

- Layer 1: Hardening Against Local Attacks
- Layer 2: Hardening Against Network Attacks
- Layer 2: Hardening Against Application Attacks

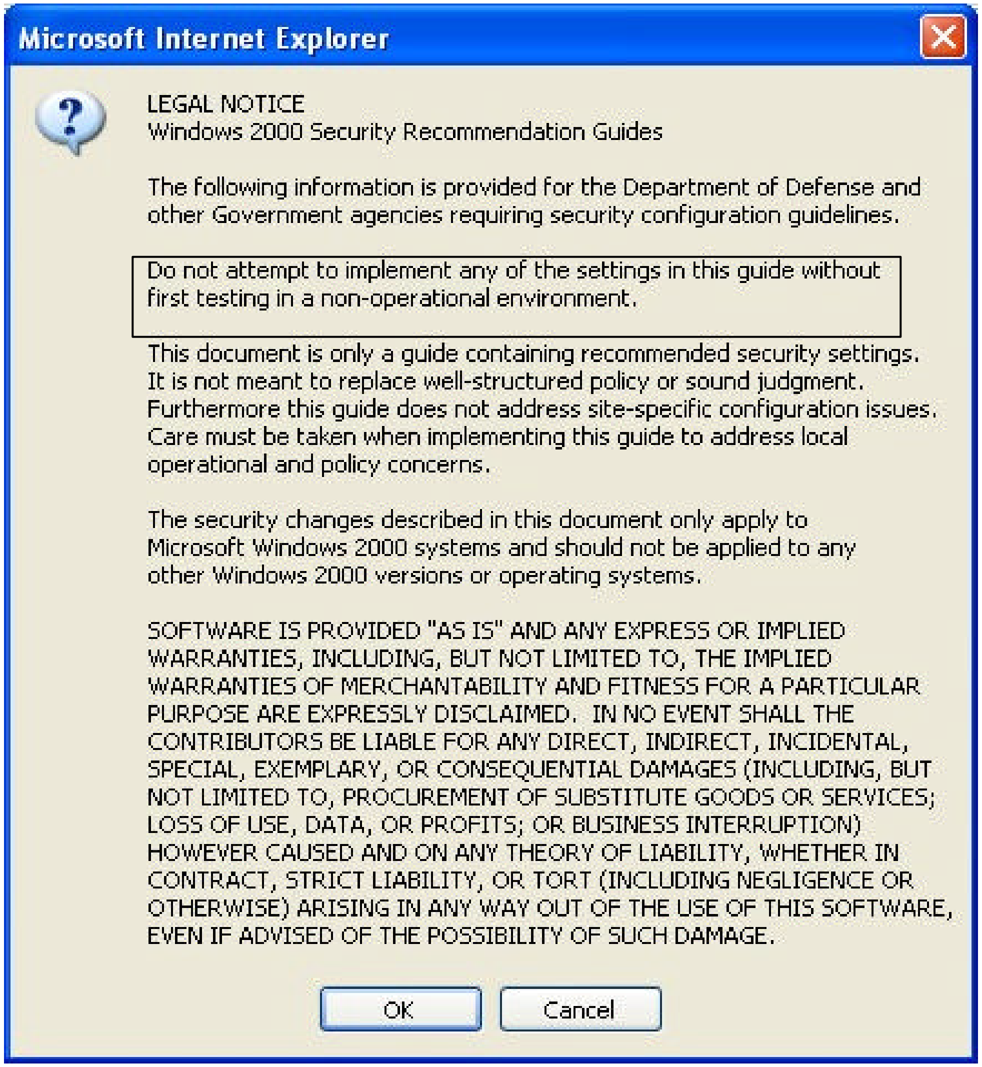


Hardening Against Local Attacks

- Use of Administrative Utilities
- File Permissions
- Manage Users
- Group Management
- Security Logging

Use of “Least Privilege”

NSA
Security Recommendation Guides



LEGAL NOTICE
Windows 2000 Security Recommendation Guides

The following information is provided for the Department of Defense and other Government agencies requiring security configuration guidelines.

Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.

This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.

The security changes described in this document only apply to Microsoft Windows 2000 systems and should not be applied to any other Windows 2000 versions or operating systems.

SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Administrative Utilities

- "Least Privilege" – As Default!
  - Like "implicit deny unless explicit permit"
- If not required – not available
- Win2k – computer management utility
- Solaris – admintool
- Linux – linuxconf
- At a minimum – Restrict Access
- If possible – Remove Them

Gold Disk

Monitor Critical System Files for Change

File Permissions

- DOS, FAT16, FAT32 do not support
- UFS and NTFS support
- Again – “Least Privilege”
- Lab Test Before Roll-out
- Monitoring Critical Files

Gold Disk

Manage Users

- Limit Power Users (Administrator/Root)
- Rename Administrator Accounts
- Restrict Root Login
- Solid Passwords (Not Default!)
- Many Recurring Themes!
- Don’t Run Services/Apps as Root
- Dummy Admin Account (?)

Group Management

- Simplifies Management of User Populations
- Better Control
- “Least Privilege” – Theme……
- Use of Sudo – Unix Surgical Root
  - Limits and Logs

Security Logging

- Must be Enabled
- Identify Malicious Activity
- Forensics
- Can be Targeted by Attacker
- After-the-fact – Not Protection
- Detect – Only if Analyzed
- HIDS for Automated Notification
- Outsourcing?

Gold Disk

Hardening Against Network Attacks

- Eliminate Unnecessary Accounts
- Enforce Strong Passwords
- Disable Unused Network Services
- Change SNMP Default Strings
- Disable Windows Resource Sharing
- Disable Unix Remote Access Services

Eliminate Unnecessary Accounts

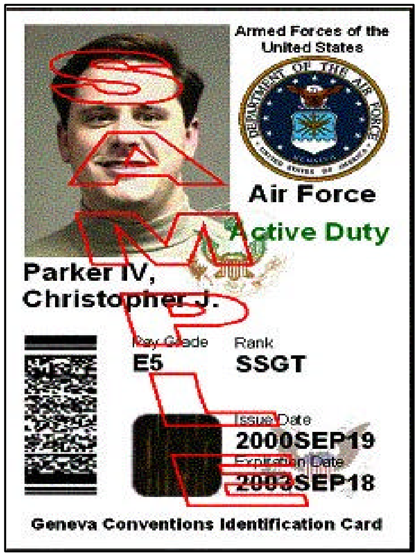
- Guest User and Unused Accounts
  - Disable OR DELETE
- Service Accounts
  - Limit Access
  - Complex Passwords
  - Solaris noshell (Titan hardening)
- Lab Test Security Adjustments

Gold Disk

Enforce Strong Passwords

- Weak or Default Passwords
  - Prime Attack Vector!
- Defaults Known
- Weak can be Cracked
  - L0pht Crack, John the Ripper
- Random Initial PW
- Minimum Password Strength
- Password Aging, Password History, Lockout
- Strong Authentication
  - Examples

Strong Authentication



Armed Forces of the United States

Air Force

Active Duty

Parker IV, Christopher J.

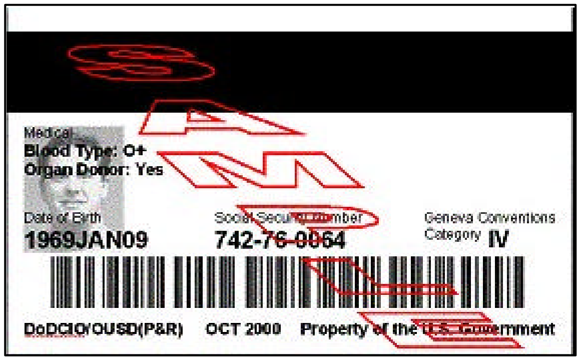
Pay Grade E5

Rank SSGT

Issue Date 2000SEP19

Expiration Date 2003SEP18

Geneva Conventions Identification Card



Medical

Blood Type: O+

Organ Donor: Yes

Date of Birth 1969JAN09

Social Security Number 742-76-0064

Geneva Conventions Category IV

DoDCIO/OUSD(P&R) OCT 2000 Property of the U.S. Government

Disable Unused Network Services

- Recall Lab – Fingerprinting
- Unused Services can be Exploited
- Disable OR DELETE
- Code Red: IIS and PWS!
- What Services are You Running?
  - Type: netstat –a | more
  - Do you need them?
  - Can you even identify them?

Gold Disk

Change Default SNMP String

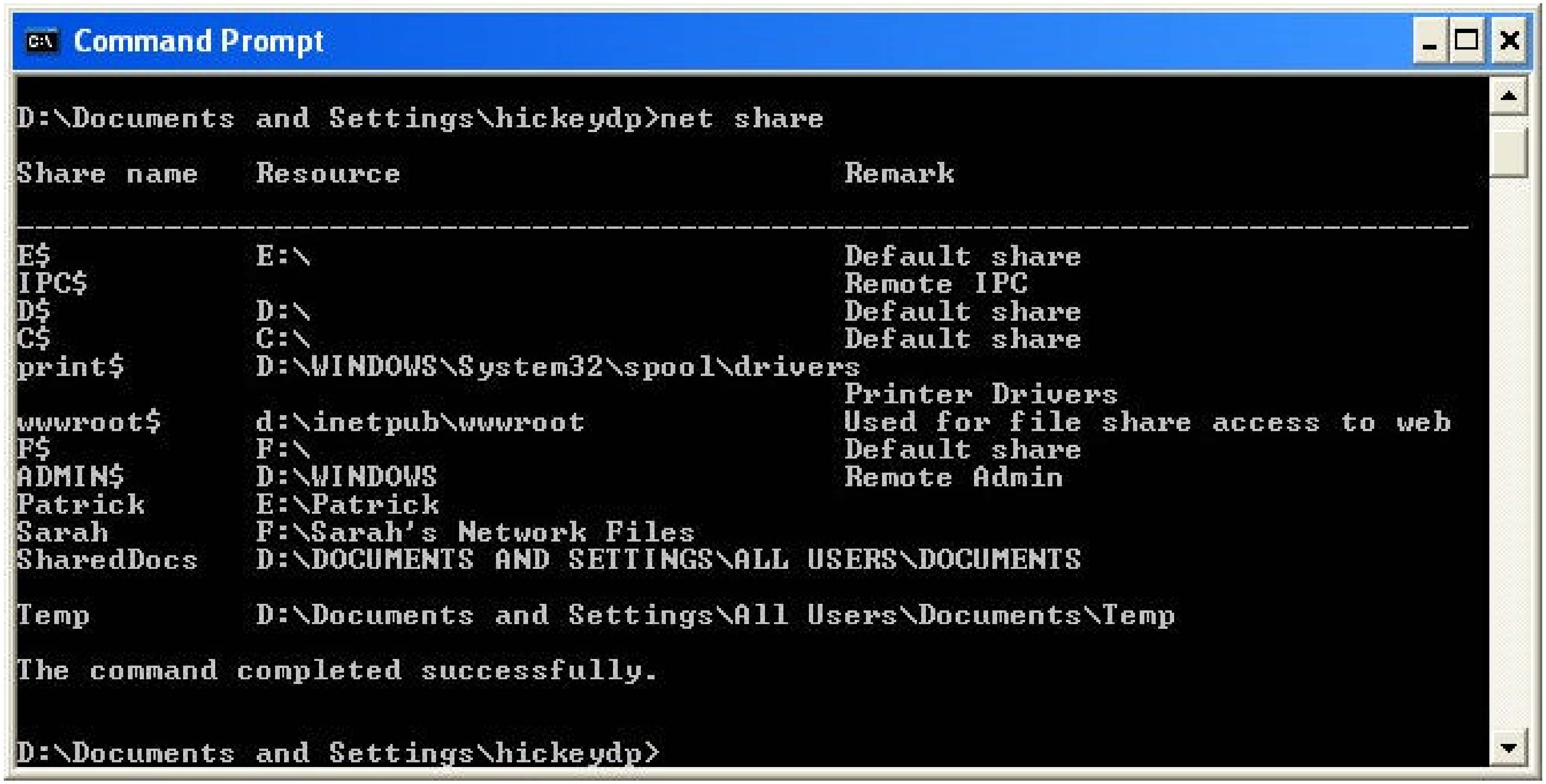
- Keys to SNMP Information
- Frequently *public* or *private* by default
- Change SNMP Community String
- Treat Like a Password
- Patch!

Gold Disk

Disable Windows Resource Sharing

- Number 4 on the Hit Parade!
- Limit Wherever Possible
  - – Depends on role of system
  - – If not needed:
    - Turn off Sharing
    - Or – Turn off NetBIOS altogether!
  - – Turn off hidden administrative shares
    - C$
    - ADMIN$
    - WINNT$

Admin Shares



```
D:\Documents and Settings\hickeydp>net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
E$           E:\                             Default share
IPC$                                         Remote IPC
D$           D:\                             Default share
C$           C:\                             Default share
print$       D:\WINDOWS\System32\spool\drivers
                                             Printer Drivers
wwwroot$     d:\inetpub\wwwroot              Used for file share access to web
F$           F:\                             Default share
ADMIN$       D:\WINDOWS                      Remote Admin
Patrick      E:\Patrick
Sarah        F:\Sarah's Network Files
SharedDocs   D:\DOCUMENTS AND SETTINGS\ALL USERS\DOCUMENTS

Temp         D:\Documents and Settings\All Users\Documents\Temp

The command completed successfully.


D:\Documents and Settings\hickeydp>
```

List Shares Using
net share

Disable UNIX Remote Access

- r-commands – rsh and rlogin
  - Unencrypted communications
  - Early versions IP authentication only (rhosts)
  - Current rsh and rlogin use Kerberos
- SSH Replacement of Telnet
- Use of TCP Wrappers
  - Intercept calls to services
  - Log, authorize, wake service

Hardening Against Application Attacks

- Two Primary Application Attack Vectors
  - Poor Default Configuration
  - Buffer Overflows
- Defining Access Methods
- Application Passwords
- OS and Application Patches

Host Defense Components

Overview

- Host's Perimeter, OS and Apps are Last Line of Defense
- Key Component of DiD
- Level of Hardening Based on Role and Risk
- Look at AV, HIDS, Host-Centric FWs

Workstation Considerations

- Routinely Exposed to Untrusted Environments
  - Internet Resources
  - Extranet Resources (Business Partners)
- Used to Access Critical Resources in Trusted Computing Base
- May Connect from Untrusted Source
  - Road Warriors
  - Home Users

Gold Disk

Workstation Considerations (cont)

- Establish Secure Configuration
- Gold Disk & Lock Down (Where Possible)
  - Control w/Policy Where Not
- AV Updates Pushed
  - Logon Script
- Host-Centric Firewalls – Especially RWs
- Ideally
  - Patch Validation Automated
  - Patch Update Pushed

Gold Disk

Server Considerations

- Generally do not Contact Untrusted
  - Server to Server Extranet One Exception
  - Client Access and Administration Vectors
- Theme – Limit Services/Applications to Bare Minimum Required
- Patch, patch, patch
- HIDS
- Policy

Anti-Virus Software

Gold Disk

- Critical HIDS
  - Signature Based
  - Behavior Based
- Strengths
  - Leverage Vendor Research/Development
  - Unobtrusive
  - Affordable – Easy Sell
- Implement on workstations, servers, gateways
- Pros and Cons of Homogeneous AV Environment?

Anti Virus (cont)

- Limitations of AV
  - Generally dependent on signatures
    - Extension Blocking and Exception
  - How fast does your vendor respond
  - How fast can you distribute new signatures
  - Ability to Detect Mutations
    - Altered by direct edit
    - Altered through “packing”
    - Not as effective against behavior based detection
  - Polymorphic Malware
  - AV/FW attacking malware – W32/Bugbear

Host-Centric Firewalls

- Augments AV Capabilities – Protects Against:
  - Unrestricted access to system’s file share
  - Anonymous access to the system
  - Undetected malicious code
  - Port scans and recon probes
  - Attacks against vulnerable network services
- Compare workstation and server based firewall capabilities

Workstation Firewalls

- Many no-cost/low cost products available
- Technologies vary by vendor
  - Packet filtering
  - Application based restrictions
    - By name or by hash of executable
    - User default “YES”
  - Integrated HIDS – BlackIce
- Default Configuration with the Customer in Mind
- Some Examples:
  - ZoneAlarm, Tiny Personal Firewall, Norton Personal Firewall, Sygate Personal Firewall, ConSeal PC Firewall, VPN-1 SecureClient, BlackIce
- Strengths and Weaknesses

Gold Disk

Server Firewalls

- In addition to other DiD Components
- Protection from Insider and Outsider Attack
- Unique Aspects (Relative to WS FW):
  - Performance impact more critical
  - Focus on inbound connections
  - Interactive configuration less desirable
- Some Examples
  - IPFilter, SunScreen Lite Firewall, FireWall-1 SecureServer, IPSec in Windows 2000

Host-Based IDS

- Optimized for Monitoring Individual Hosts
  - Network activity
  - File system
  - Log files
  - User actions

HIDS Advantages

- Can Associate Activity to User and User’s Privileges
- Can Analyze Encrypted Traffic as it is Decrypted
- Can Identify Attacks that Evade NIDS Detection
- Event Correlation Across Many Platforms

HIDS Categories

- Monitor Host’s File System
  - Tripwire
  - AIDE
- Monitor Host’s Network Connections
  - BlackIce
  - PortSentry – Psionic purchased by CISCO Systems
- Monitor Host’s Log Files
  - LogSentry – Psionic purchased by CISCO Systems
  - Swatch
- Monitor a Combination of the Above
  - ISS RealSecure Server Sensor
  - Entarasys Dragon Squire

File System Monitoring

- Detect Unauthorized Changes to Host’s File System
  - Snapshot of the File System in Trusted State
  - Compare current state to baseline
  - Reports noteworthy deviations
  - Tune to system characteristics
    - What should change, and how
    - What should not change at all
  - Signature through hash or copy

File System Monitoring

- Tripwire
  - – Academic Source is Freeware – UNIX only
  - – Commercial – UNIX, Win
    - Windows version monitors registry
    - Monitor routers and switches – push updates
    - Management through Tripwire Manager
- AIDE – Advanced Intrusion Detection Environment
  - – Freeware – maintained
  - – UNIX only
  - – Limited remote management through ICU scripting
- Integrated w/RS Server Sensor or Dragon Squire

Network Connection Monitoring

- Monitor Attempts to Connect to and from
- Can Associate Sockets, Processes, Users
- Less Susceptible to Traffic Overload
  - Compared to NIDS
- Can Execute Active Response/Defense
- As Previously Discussed – Can Inflict DoS
  - More Appropriate for WS than for Server

Log File Monitoring

- Monitors Contents of Critical Logs
- Alerts on Suspicious Events
- Swatch – Freeware UNIX Based
  - Report log entry – e-mail
- LogSentry – Psionic Partner of PortSentry
  - Report log entry anomolies – periodically
- Windows Based Products
  - TNT Event Log Monitor
  - LANguard Security Event Log Monitor
- Monitor Aggregated Logs

Challenges

- Compromised Hosts
  - Delete Security Logs
  - Create New Accounts
  - Install Backdoor Programs
  - Disable Locally Installed Security Programs
- Mitigation
  - Host Hardening
  - Tiny Trojan Trap (Windows)
  - Chroot (UNIX)
  - Embedded Firewalls!

Challenges

- Controlling Distributed Components
  - Managing distributed components is complex and labor intensive
- Mitigation
  - Automated updates
  - Central management services
    - Tripwire Manager
    - ICEpac
    - Centrally Managed Desktop Security (Tiny)
    - Zone Labs Integrity

Embedded Firewalls

- Tamper-resistant protection
- Use to secure open Internet connections
  - VPN end points
  - broadband access gateways
- Use to secure critical servers – inside or outside perimeter
- Use policy server to configure security policies
- Firewall card accepts instructions only from authenticated firewall policy servers
- Firewall cards can support multiple levels of protection
- Deny "ping" requests, block unnecessary protocols and ports, and disable packet sniffing and IP spoofing
- Default to your highest level of security

Design Fundamentals

Gathering Design Drivers

- Identify the Baseline Architectures
- Identify the Applicable Law and Policy
- Identify the Business Requirements
- Identify Resources to Protect
- Identify the Threat

Identify Baseline

- Likely the Most Difficult
- Includes at a Minimum:
  - WAN Architecture
  - Enterprise Network Management Architecture
  - Enterprise Network Services
  - Enterprise Security Services
  - By Site:
    - CAN and LAN Architectures
    - Existing Defense in Depth – Includes Perimeter
    - Mission Critical Apps that Traverse the WAN
    - Extranet Requirements
    - Local Policy
    - Local Network Management Architecture
    - Local Network Services
    - Local Security Services
  - Others?

Identify Applicable Law/Policy

- Up-Front Collection of:
  - External Law and Policy
  - Internal Policy
- Read and Understand
  - Constraints
  - Restraints
  - Gaps

Identify Business Requirements

- Senior Management Guidance/Intent
  - Expectations for Confidentiality, Integrity, Availability
- Strategic Plans
- Valuation of Networked Resources
- Available Funding
- Timeline

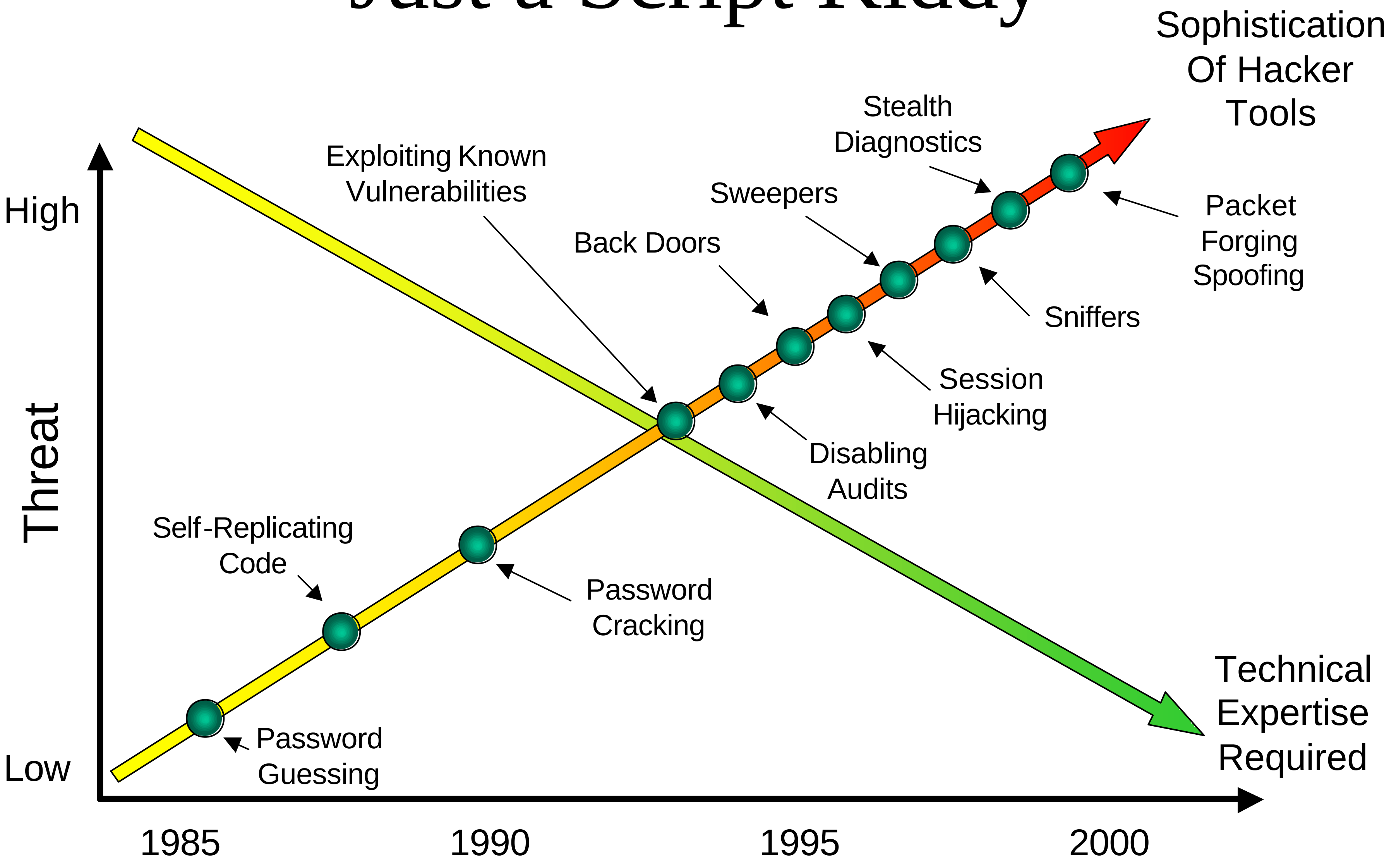
Identify Resources to Protect

- Based on Business Requirements
  - High-Value Networked Resources
    - Supporting Network Components
  - Vulnerable Attack Vectors
    - Security Components
    - Publicly Accessible Resources
    - Remote Access Resources
    - Management Systems
    - Wireless Networks – ACPs
    - Extranet Connections
    - Network Information
    - Very Large, Very High Latency Packets
    - E-Mail

Identify the Threat

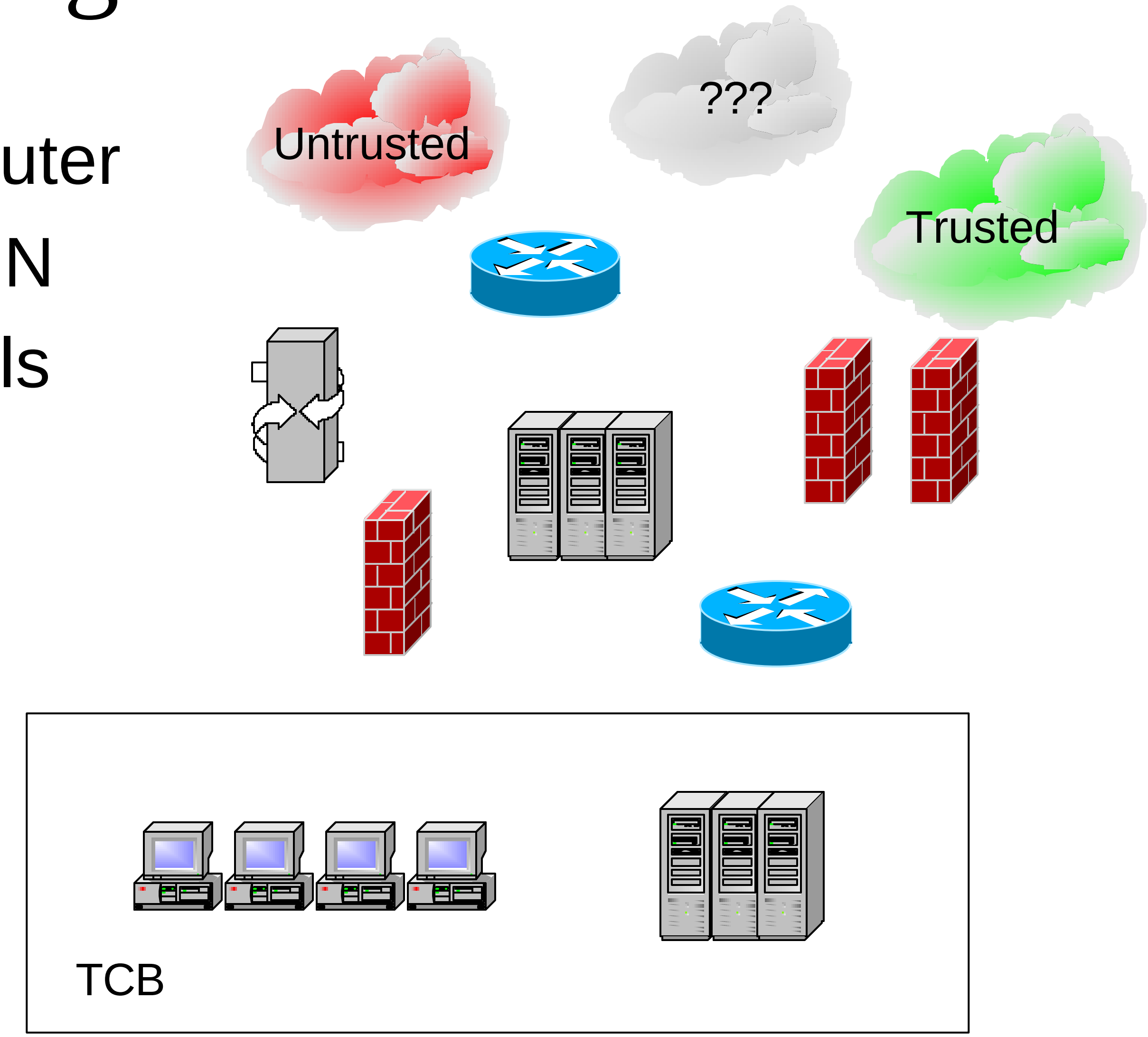
- Determined Outsider
  - What is the motive?
  - What are the goals/targets?
  - Value of attaining goals/targets?
  - Level of resources that might likely be brought to bear.
- Determined Insider
  - Easier access
  - Harder to detect
  - Security management controls?
- Script Kiddy
- Automated Malicious Agents

Just a Script Kiddy



Design Elements

- Firewall and Router
- Firewall and VPN
- Multiple Firewalls



Firewall and Router

- Most Common Perimeter Components
- Establishing Appropriate Roles
- Screening Router and Firewall
- Firewall Only (ISP Controlled Router)
- Router Alone

Firewall and VPN

- Separate Components
  - – Concerns with NAT compatibility
  - – Flexibility of placement
  - – Flexibility in technology selection
  - – Management Overhead
- Integrated Components
  - – Integrated management – less complex
  - – Limited to coupled technology
  - – Likely to preclude NAT compatibility issues

Multiple Firewalls

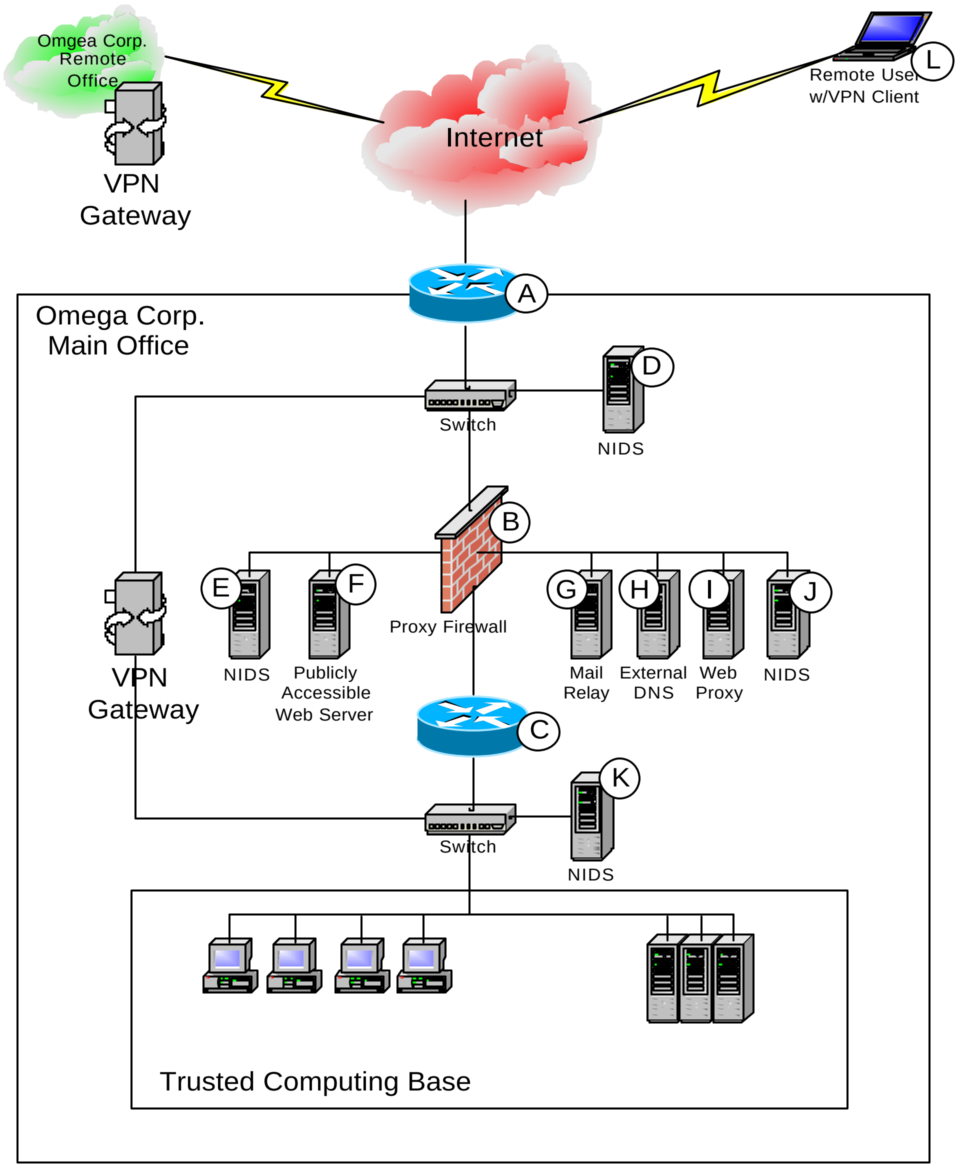
- Inline Firewalls
  - Provides layered protection
  - Increasing protection for screened subnets
  - Book Example – Internet to web servers, web servers to database servers.
  - Management complexity – TCB to world
  - Imbedded firewalls?
- Parallel Firewalls
  - Firewall technology and tuning based on specific task
  - Reduces management complexity for internal to world
  - Reduces latency of layered FWs (inline model)
- Parallel Firewalls – load balanced
  - Availability
  - Performance
  - Big IP

Separating Resources

Security Zones

- Logical Grouping of Resources
  - Similar degree of acceptable risk
  - Similar degree of required exposure
- A Single Subnet
  - Task specific servers (DNS, Mail, Web)
  - Multi-tasked servers (DNS and Mail)
    - Limit service account access
      - Not root!
      - Chroot
- Multiple Subnets

Security Zones



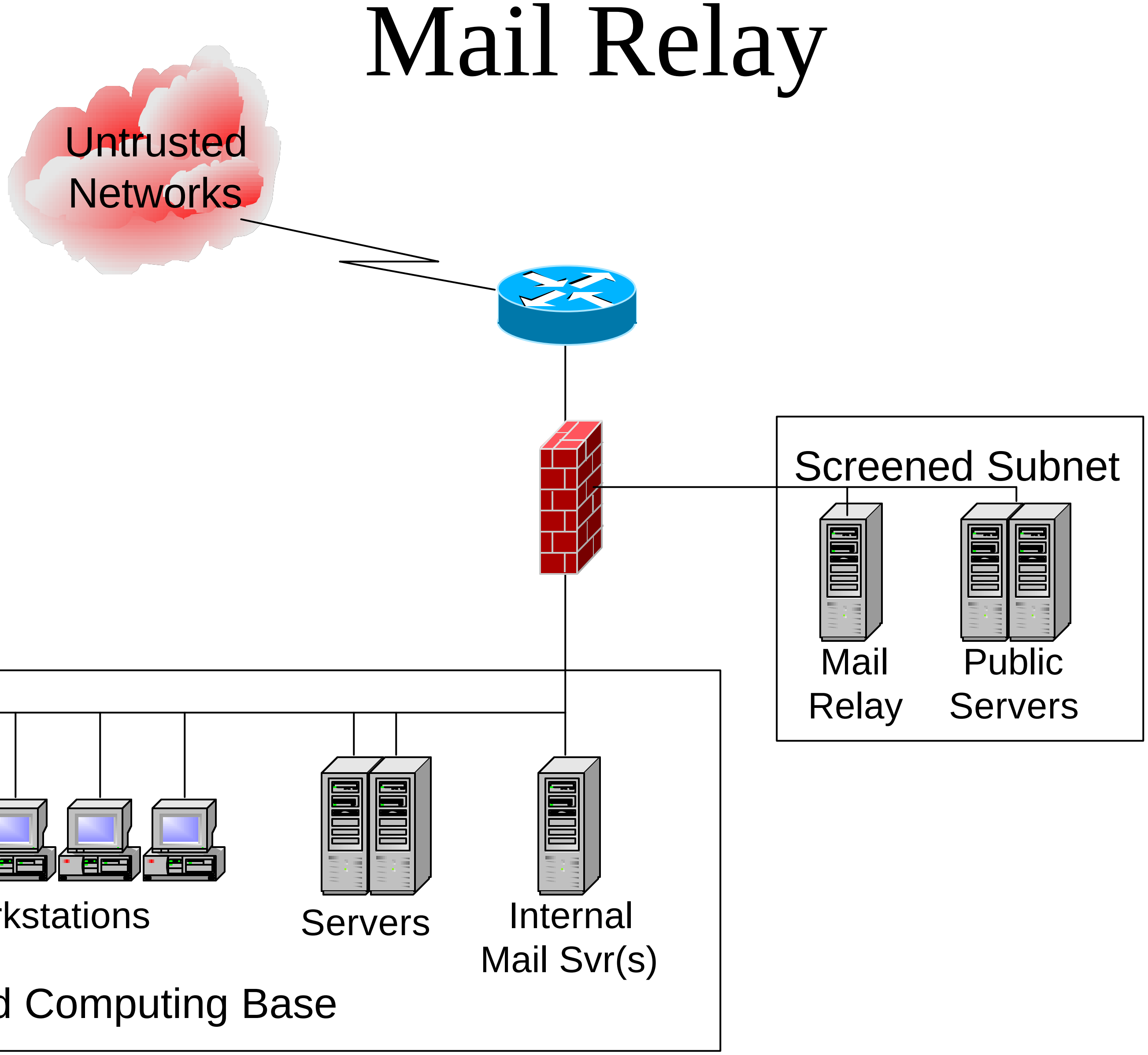
Common Design Elements

- Mail Relay
- Split Horizon DNS

Mail Relay

- Separate Risk in Separate Zones
- Isolates Internal Mail Servers
- Mail Relay – Bastion Host
  - Hardened
  - Least Privilege
  - Separate Server
  - HIDS, AV, Blocking
  - Specifically Control Access
    - Service net to world
    - Service net to TCB
- Technology Specific to Function

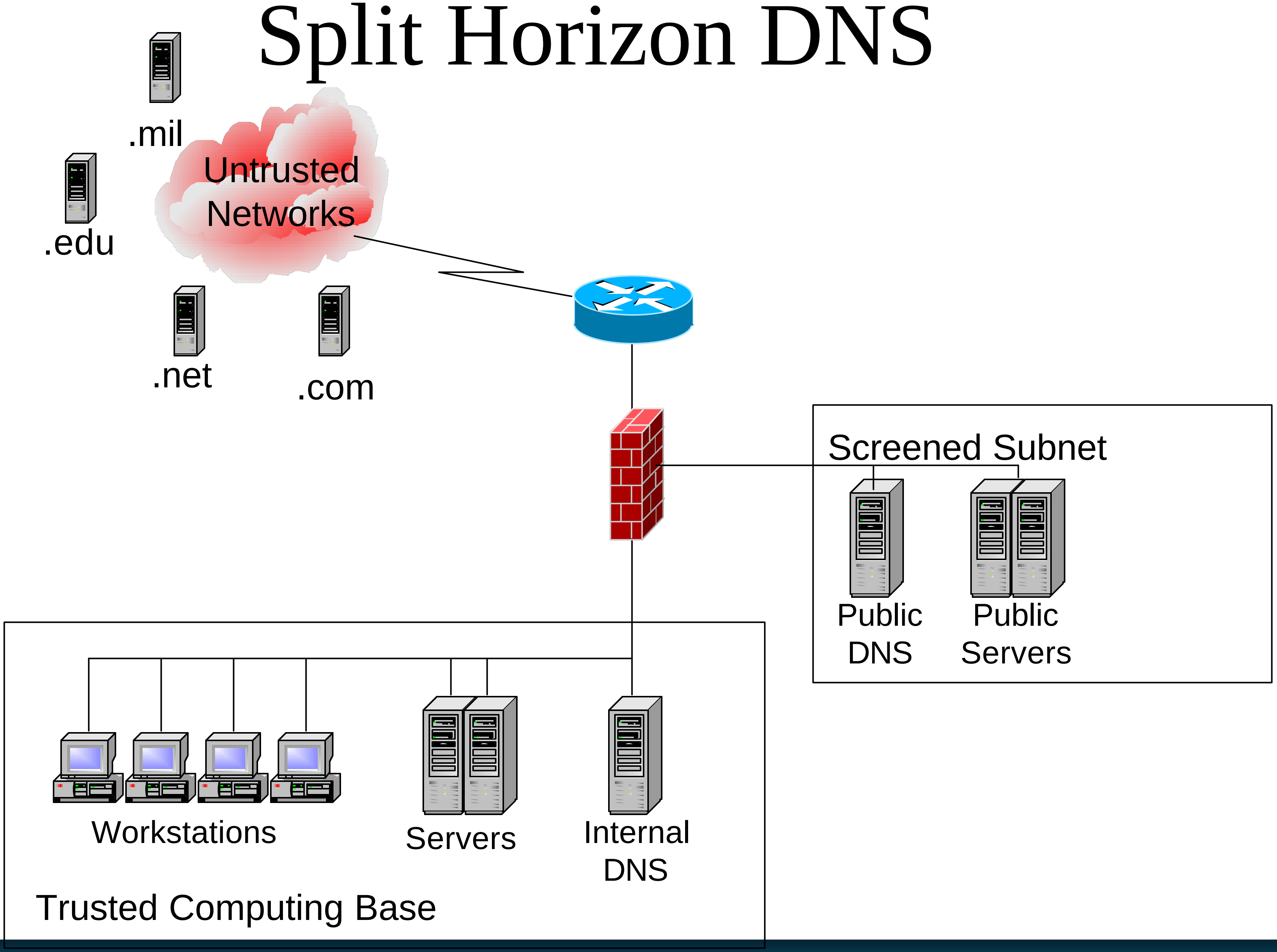
Mail Relay


Untrusted Networks
Screened Subnet
Mail Relay
Public Servers
Workstations
Servers
Internal Mail Svr(s)
Trusted Computing Base

Split Horizon DNS

- DSN Function – Hostname/IP Mapping
- Similar to Mail Relay
- Limits Information Available to Untrusted
- Provides Needed Functionality for TCB
- Provides Security Zone Protection for At-Risk Components
- Recursive Queries to Screened Subnet
  - Or directly to Internet (?)

Split Horizon DNS



Software Architecture

Software Architecture and Network Defense

- This is the Issue of Balance
  - Risk versus operational requirements
- How to be Successful
  - Policy
  - Clear lines of authority
  - Flexible architecture
  - Clearly defined processes that are followed!

How it Affects Network Defense

- Firewall and ACL Changes
  - Wiggle room is delta between actual and policy – implicit deny in effect
  - We do not grant waivers, and do not break policy
    - Engineer an alternative solution
- Conflicts with Network Configurations
  - Solution frequently prohibitively expensive
    - Need a flat network with Win2k and AD? $40M should do it.
  - If no security issues, only issue is funding reengineering
  - Frequently a candidate for alternative approach
- Encrypting Connections
  - Policy is key – how will sensitive data be protected in transit, in processing, and when at rest
  - One issue is who determines what is sensitive and what is not

How it Affects Network Defense

- Performance and Reliability
  - Inverse relationship – performance and security – balance
  - Reliability is not an issue…given enough funding
  - What is acceptable? – not the security professionals call
  - How do we achieve five 9’s of availability – teaming with network engineers to design
- Atypical Operating System
  - Policy and standards set the baseline
  - Waiver authority when requirement can’t be met using standards - minimize

SW Component Placement

- Single System Applications
- Multitier Applications
- Administrator Access
- Applications for Internal Use Only

Identifying Potential Issues

- Software Evaluation Checklist
  - Communications Plan
  - Program managers will not normally be able to provide
  - Assist in completing correctly
- Source of Application Information
  - Programmers
  - Lab testing on representative architecture
- Unsecurable Applications
  - Quarantine, deny, reengineer app, buckle
  - Remember the policy and processes discussion?

Software Testing

- Policy sets the design to environment
  - Host, Server and Communications
  - Gold Disk!
- Test in dedicated lab environment
  - Includes security policies and components
  - Controlled testing on production network
  - Established testing team w/cross section of skills and responsibilities
  - Red team - pentest

Network Defense
Design Recommendations

- Design for the future
- Robust perimeter provides future flexibility
  - Industry is going towards convergence
  - Not there yet…you will be…plan for it
  - Spare capacity
  - Modular
- Spend the money – keep your engineers sharp

Products Required

- Written Assessment of Current Posture
- Written Assessment of:
  - Threats
  - Vulnerabilities
- Proposed Changes to:
  - Perimeter
  - As necessary to perimeter solution
    - Information architecture
    - Internal network/security architecture
    - Network/security management architecture
- Proposal includes written – what, where and why and site diagrams
- Policy (top five must do – now)
- Input to Web Site / Knowledge Portal Development Effort

Perimeter Design

VPN Integration

VPN Integration Overview

- Many Options Available
  - Each with its own complexities
- Matching Technology to Requirements
- Integrating with Security Architecture
- Management Complexities

Secure Shell (SSH)

- Recall Vulnerabilities of Telnet, rlogin
  - SSH provides secure alternative
  - Shell or command line access
  - Transfer files (sftp)
- Two Main Types of SSH
  1. Standard SSH
  2. SSH Tunnel

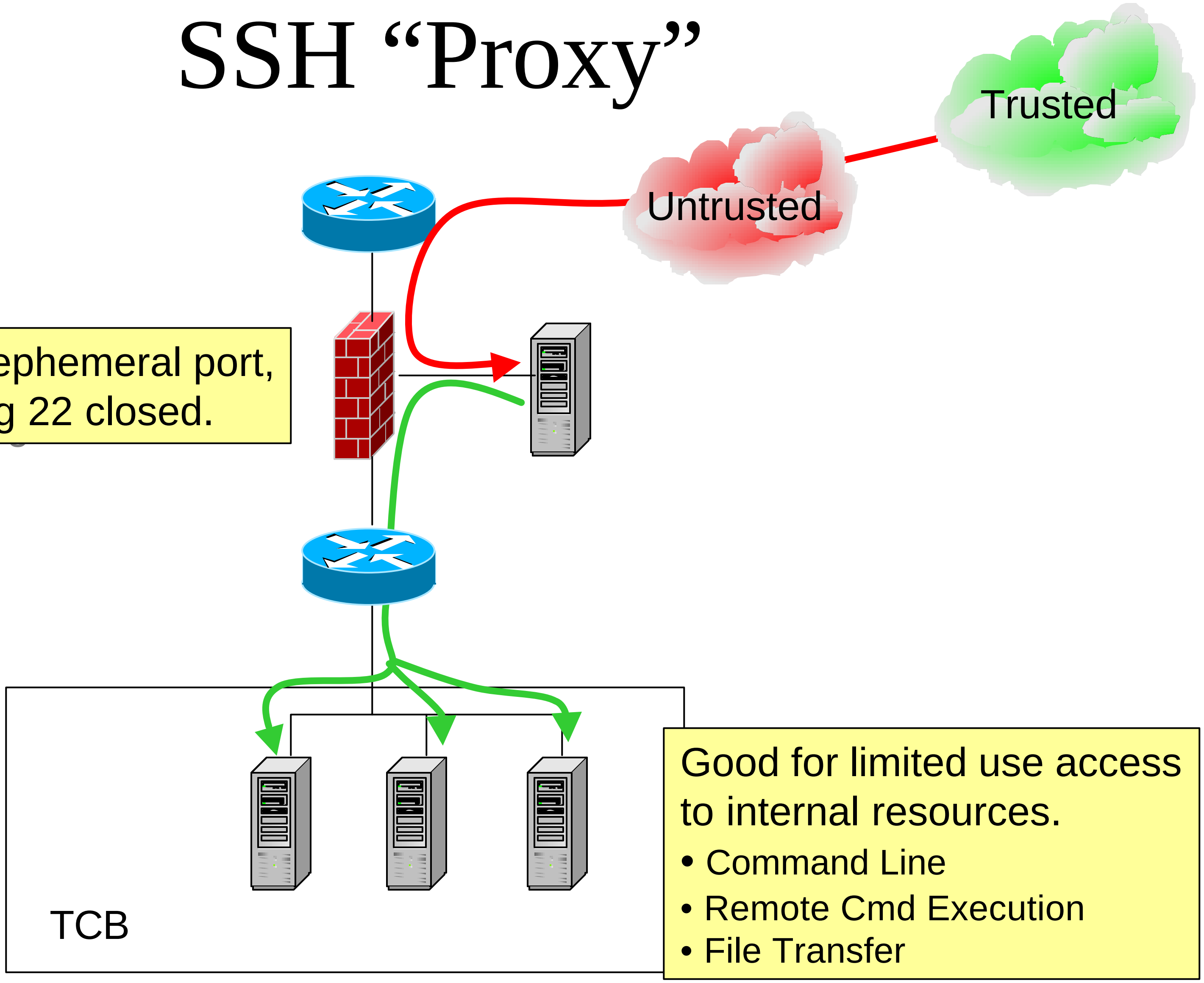
Standard SSH Connections

- Command Line, File Transfer, Remote Execute
- SSH Client
  - Comes packaged with most UNIX OSs
  - Free versions available for Windows
    - PuTTY is popular GUI FE to SSH Client
    - Many Windows apps can leverage SSH
  - Straight forward installation
- SSH Server
  - Common component w/UNIX OSs (sshd)
  - Windows – not standard
    - OpenSSH on Windows!
  - Server configuration more intensive – but straight forward
    - Login controls, SSH protocols allowed, Authentication

SSH Perimeter Adjustments

- Minimal Change in Most Architectures
- Permit Access to Server Port 22
  - IP to IP – Authentication and Encryption
  - Can adjust port to non-standard port
    - Both client and server must support
  - SSH Proxy?
    - All external to service net
    - Service net to internal servers

SSH "Proxy"



Can use ephemeral port, leaving 22 closed.

Good for limited use access to internal resources.

- Command Line
- Remote Cmd Execution
- File Transfer

SSH Tunnel

- Port Forwarding
  - Encrypted tunnel established
    - Client – any unused port
    - Server – well-known service port
  - Client application pointed to local port
    - 127.0.0.1:23 (Telnet)
    - Tunnel transports traffic to remote service
      - Authentication and encryption
- Limitations
  - One tunnel per remote host/protocol used
  - Only handles TCP traffic – UDP cannot be used

SSH Tunnel Implementation

- Client Integration
  - Client must support
  - Client local connections only
  - Local Applications Set to Near-End of Tunnel
- Server Integration
  - Configuration Server Dependent
    - Setup to Accept Tunneling

Perimeter Adjustments
SSH Tunnels

- Standard Implementation Opens Many Holes
  - Tunnels open holes to specific ports on internal servers
  - Many tunnels to access different services require many ports open in the FW
- Option – Tunnels within a Tunnel
  - "Proxy" SSH server on Service Net
  - Tunnel established to service net SSH server
  - Multiple tunnels through to TCB servers

When to Use SSH Tunnels

- Pros
  - Allows Use of Insecure Protocols
  - Rapid Deployment – Minimal Cost
- Cons
  - Technically challenging
  - May get complex based on numbers to manage
  - Some clients do not support
- Recommended for:
  - Technically proficient users
  - Limited in scope

Secure Sockets Layer

- SSL and TLS (Transport Layer Security)
  - Strong encryption
- Standard SSL Connections
  - Single SSL-enabled application
- Tunneled SSL Connections
  - One or more applications
  - SSL enabled or not

SSL Standard Connections

- Web-Based SSL Most Widely Used VPN
- All Major Browsers Support
  - https – port 443
- Other Protocols Supported
  - SMTPS, NNTPS, LDAPS, IMAPS, POP3S
  - Ports assigned
  - Not widely used

Standard SSL Client Integration

- Easy to Enable if Application Supports
  - Web browsers good example
- May not be Enabled by Default
- If Application not SSL Enabled
  - Probably prohibitively difficult to implement
  - Consider SSL tunneling

Standard SSL Server Integration

- For SSL Enabled Applications
  - Implementation fairly straightforward
  - PKI cert creation and installation is long pole
  - Public key created and submitted for signing
  - CA signs public key (certificate)
  - Certificate installed
- Matching Encryption Strength
  - Must keep in mind your user base clients

Standard SSL Perimeter Adjustments

- SSL Enabled Apps Use Different Ports
  - HTTP – Port 80; HTTPS – Port 443
  - IMAP – Port 143; MAPS – Port 993
  - LDAP – Port 389; LDAPS – Port 636
  - FTP-Data – Port 20; FTPS-Data – Port 989
  - FTP-Cntl – Port 21; FTPS-Cntl – Port 990
- Potential Use of SSL Enabled Web Proxy
  - Likely located on the service net

When to Use Standard SSL

- Commonly Used for Encrypted HTTP
  - E-Commerce
- Web Native Applications or Web Front Ends
- Outlook Web Access
- Many POP and IMAP Clients Support – But not All!
  - If supported, may not be enabled by default

SSL Tunnels

- Use of SSL Tunneling Server
  - Stunnel – www.stunnel.org
- Uses Port Forwarding – Like SSH Tunnel
  - Tunnel is built from local port A to remote port B
  - Local applications are pointed to port A
  - Tunnel forwards encrypted traffic to port B
  - Remote SSL server decrypts and passes to correct application port

SSL Tunnel Perimeter Adjustments

- Like SSH Tunneling – Might Require Many Tunnels to Many Hosts
- Use of SSL Tunneling Server
  - Users tunnel to tunneling server
  - Tunnel within this tunnel to individual points
  - Reduces impact on perimeter
  - Complicates management
  - Impact on performance – two levels of tunneling

When to Use SSL Tunnels

- Similar to SSH Tunneling
  - Technically savvy users
  - Limited number of tunnels
- Requires use of CA
- Not all OSs have SSL tunneling client available

IPSec

- Three Types of IPSec Architecture
  - Host-to-host
    - End-device to end-device encryption
    - Comparable to standard SSH and SSL connection
  - Host-to-Gateway
    - Encryption from host to gateway – not to server
    - Comparable to SSH and SSL host to SSH/SSL server tunnel
  - Gateway-to-Gateway
    - Gate to gate encryption – on service nets
    - Host and server to gate not encrypted
    - No host configuration requried

IPSec (cont)

- SSH and SSL
  - Additional tunnels and connections required for each application
  - Fine for limited use – technically savvy users
- IPSec – All Applications Can Share One Tunnel
  - Relatively easy to manage
  - Transparent to users
- Greatly Simplifies VPN Solution from Perimeter Perspective

IPSec Client Integration

- Comes Packaged with Many OSs
  - Windows 2000/XP; OpenBSD
- Non-Native IPSec Products Available
  - Shim technologies
    - Adds IPSec layer between network adapter and TCP/IP stack
    - Uses existing network adapter for both IPSec and non-IPSec traffic
  - Separate IPSec network adapter
    - Requires routing changes
    - IPSec and non-IPSec traffic divided between network adapters specific to that purpose

IPSec Server Integration

- Three Commonly Used IPSec Servers
  - – VPN Concentrators
    - Dedicated VPN device
    - Can also do filtering, firewalling, NATing
  - – Firewall as an IPSec VPN server
    - CheckPoint; NetScreen; CyberGuard; others
    - Less expensive than dedicated – watch for FW performance impact!
  - – Routers
    - Inexpensive gate-to-gate solution
    - Watch for performance hit!

IPSec Architectures and Uses

- Host-to-Host
  - Access to single internal device is required
- Host-to-Gateway
  - Remote user access to TCB
  - Remote client needs IPSec capability
  - No changes to internal networked devices
- Gate-to-Gateway
  - Extranet connection – extending trust
  - No changes to TCB of either network
  - Recall extending trust discussions

Other VPN Considerations

- Proprietary VPN Implementations
  - Interoperability
    - Users
    - Business partners
- Compromised or Malicious VPN Clients
  - Extreme trust discussions
  - VPN is clear attack vector
  - Encryption complicates monitoring
  - Appropriate DiD
    - Dual-sided VPN
    - Decrypt outside perimeter
    - Implement focused monitoring
    - Hardening internal resources

Tuning for Performance

Performance and Security

- Security Methods and Tools Will Impact Performance
- Careful Selection of Solutions is Necessary
- Must Understand Current Requirements
- Must Always Plan for Future

Performance Defined

- "Unacceptable" Performance Based on
  - User expectations – satisfaction
    - The user experience
  - Application requirements
- Bandwidth and Latency
- Response Time
- Throughput

Performance and Security

- Goals of Security – CIA
- Ultimately We Serve Two Masters
  - The need to protect
  - The need to enable
- What Services are Required Today?
- What Services will be Required Tomorrow?
- What are the Metrics that Enable Tomorrows Solutions?

Example of SLA Metrics

- End-to-End Availability >= 0.998
- Packet Loss - < 1%
- Latency - < 100 ms
- Shared Files Access – 1 MB < 2 sec
- Customer Satisfaction - >= 85%
  - – on approved survey responses

Design Elements that Impact Performance

- As Previously Discussed
  - Implementing security can, and does, impact network performance
    - Packet Filtering/Firewalling
    - Payload Inspection
    - Encryption
    - Authentication
  - It truly is a balancing act

Design Elements (cont)

- Recall:
  - More granularity in inspection = increased security = reduced performance (as a general rule)
  - High throughput to low throughput filters
    - Packet filters
    - Stateful firewalls
    - Proxy firewalls
    - Content filters
  - In general, each requires increasing CPU strokes
  - Recall discussion of overloading routers
    - Watch CPU utilization
    - Apply rules to ports inbound to the router
- Discuss Cause of Reduced Throughput

Network Architecture Considerations

- Broadcast Domains
  - Broadcast is expensive
  - Here is a solid use for VLANs!
- WAN Links
  - Adequate bandwidth
  - Acceptable packet loss
  - Availability
  - WAN is relatively small component of overall IT expenses (in general)
  - Investment but can enable huge gains

Network Architecture Considerations (cont)

- WAN Usage Tips
  - – Route, don’t bridge across WAN
  - – Build in autonomy of services
  - – Use traffic shaping or QoS
  - – Cache locally
  - – Schedule high-use jobs for low use periods
  - – Others?

Network Architecture Considerations (cont)

- TCP/IP Tuning
  - Not all stacks optimized by default
  - Maximum transmission unit (MTU)
    - Exceeding causes fragmentation
    - RFC 1191 – dynamic discover of optimum MTU
    - Uses ICMP!
  - Window size
    - Part of TCP error correction mechanism
    - How much can I send before I get an ACK
    - Dynamically adjusted by TCP - >800Mbps exceeds
    - RFC 1323 adds extension to TCP to accommodate high-performance networks
  - Socket buffer size
    - Buffer send and receive until ACK
    - Buffers too small – data exchange not maximized
    - Bandwidth-delay product identifies appropriate setting
  - Correctly adjusting above can make a significant difference in performance
  - Automated tools becoming available – hand tuning is non-trivial

Impact of Encryption

- Benefit can be Great
  - Confidentiality
  - Integrity
  - Authentication
  - Non-Repudiation
- Performance Hit can also be Significant
- Confidentiality/Integrity Services
  - Impact for duration of information exchange
  - Symmetric key support is common

Impact of Encryption (cont)

- Authentication and Non-Repudiation
  - Typically only performed once per session
  - Performance impact can be significant
  - Public key cryptography frequently provides these services
    - Authenticate user
    - Guarantee creator of message
- Common to Use Best of Both Worlds
  - Public key to authenticate and exchange communication details – including shared secret
  - Shared secret to generate key used for symmetric key cryptography
  - Caching of session details – allows resumption of previous session without overhead – SSL
  - Hardware accelerators – offload crypto functions to co-processor

Load Balancing to Improve Performance

- Spread Load Across Multiple Platforms
  - DNS, Firewalls, Web Servers, etc
- Increased Performance
- Increased Availability
- Complicates Management
- Additional Cost
- Layer 4 Dispatchers
- Layer 7 Dispatchers

Sample Designs

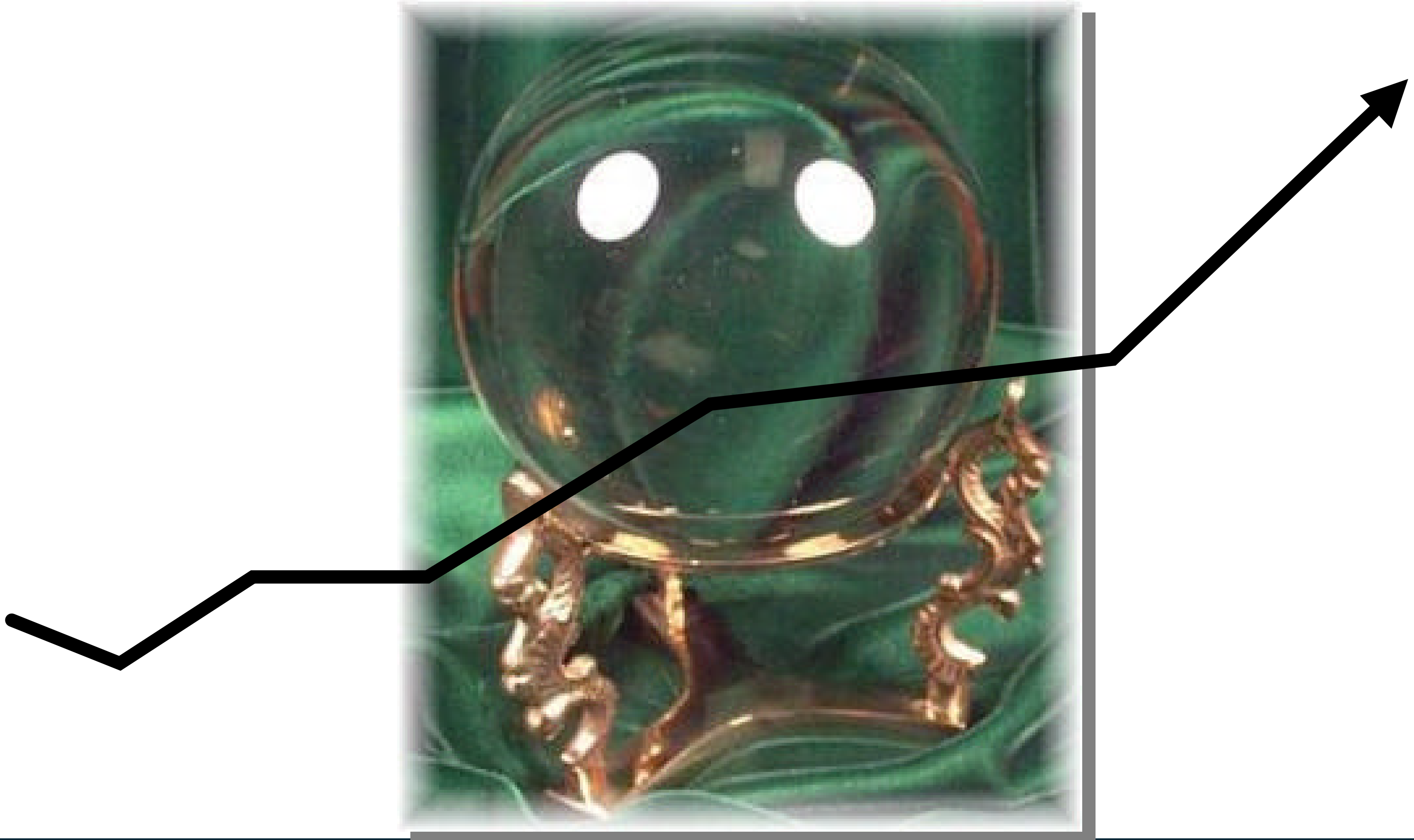
Review of Security Design Criteria

- Every Design Must Consider:
  - – What Needs to be Protected?
  - – What are the Threats?
  - – What are the Business Requirements?
- Let's Look at Omega Research
  - – Discuss design considerations above.
  - – Discuss potential solutions to the problem.

What Needs to be Protected?

What are the Threats?

What are the Business Requirements?



A Recap

- Defense in Depth
- Pull the Application Developers into the Inner Circle
- Complacency Could Easily be your Most Insidious Enemy
- Implement Disciplined Configuration Management
- Test Your Own Defenses
- It is 10-Fold Easier to Attack than to Defend
- No Detail is too Small to Look at Once (Auditing)
- Systems Administrators are Key to Organizational Success
- Make the Entire Workforce Part Owners in the Process

- Effectively Train Providers and Users
- No one Individual Holds All the Keys
- Automate Where Possible – But Verify!
- A Risk to One, is a Risk to All
- Trust but Verify (Hold Trust Close)
- Implicitly Deny Unless Specifically Allowed
- Balance Between Risk and Operations
- Eliminate Unneeded Services
- Least Privilege
- Policy is the Keystone
- Security is a Journey

Do the Basics Aggressively and Consistently!

Questions?