

Firewalls: Building a Better Wall

Harvard Townsend

Kansas State University

Chief Information Security Officer

harv@ksu.edu

2009 IT Security Training Event

October 5, 2009

October is

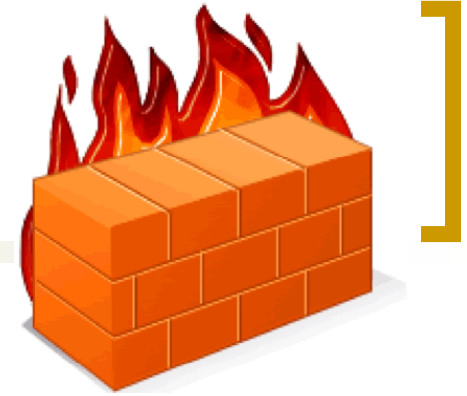


NATIONAL
CYBER SECURITY
AWARENESS MONTH

Our Shared
Responsibility

staysafeonline.org

[Agenda



- Terminology
- Firewall functions
- Role in IT security
- Types of firewalls
- Configuring a personal host-based firewall
- General recommendations/considerations

[Terminology]

“You keep using that word. I don’t think it means what you think it means.” Inigo Montoya in *The Princess Bride*

- *Firewall* – a collection of components through which all network traffic must pass where only traffic authorized by local security policy is allowed to pass.



Terminology



- **Packet** – bundle of data packaged into a discrete unit
- **Network traffic** – packets moving through a network
- **Incoming** – packets received by a host
- **Outgoing** – packets sent by a host

Firewalls are primarily interested in which host *initiated* the communication since most network communications have traffic flowing in both directions. Thus denying inbound FTP prevents a remote computer from initiating a file transfer request with the local computer but doesn't prevent the use of FTP to fetch a file from a remote server.

[Terminology

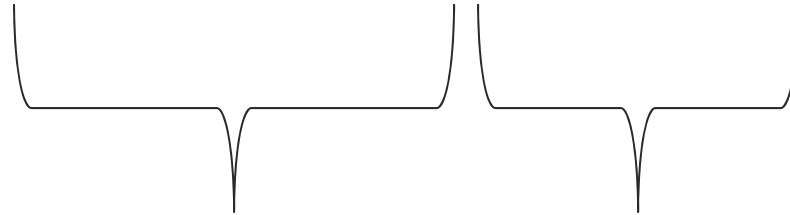
TCP/IP

- **TCP/IP** – a collection of protocols used in most network communications over the Internet; think of it as a way to organize and deliver packets as they flow over networks
- **IP** – “Internet Protocol”, the base protocol in TCP/IP that manages delivery of packets between devices communicating on a network; routing typically occurs at this layer
- **IP Address** – a set of four numbers (“octets” valued 0-255) separated by dots (“dotted-decimal notation”) that uniquely identifies a device communicating with TCP/IP. Example = 129.130.12.87

[IP Address

TCP/IP

129.130.12.87

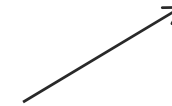


Network portion
All K-State IP addresses
start with this

Host portion
Uniquely identifies the device
on K-State's network

K-State's network is specified by **129.130.0.0/16**

Number of bits in the network
portion of the address (129.130)



[Terminology

TCP/IP

- **TCP** – the “Transmission Control Protocol” provides a reliable, ordered stream of bytes between programs running on two computers; retransmits a packet if it is lost, reassembles packets into proper order, ensures data integrity, does flow control.
- **UDP** – the “User Datagram Protocol” is an unreliable data transmission service: “Just throw the packets onto the network and hope they get there intact.” Packets may arrive out of order, altered, or not arrive at all.
- Most applications use TCP so they don’t have to manage the network transmission
- TCP is more complex and has greater overhead than UDP
- UDP assumes reliability and orderly delivery is not required or is handled by the application

[Terminology

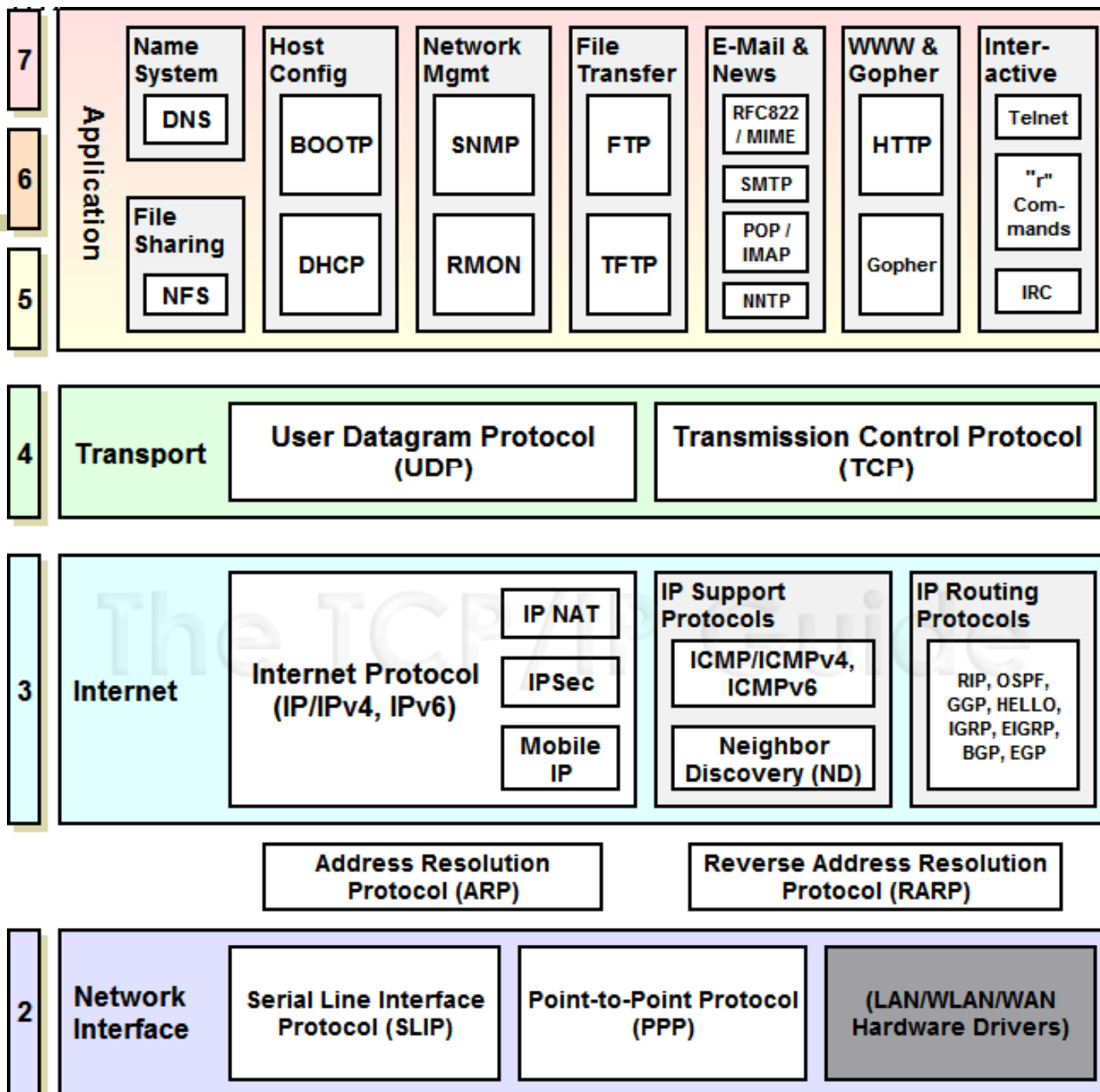


- **Port** – a communication end point used to connect to specific applications or processes.
 - managed at the transport layer (TCP or UDP – the concept is the same for both)
 - is assigned a number (0-65535)
 - usually designated as port/protocol, like 25/TCP or 53/UDP

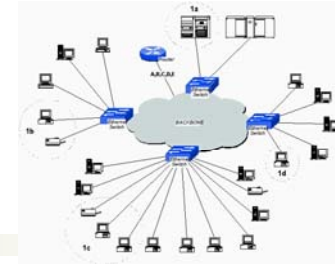
Port number assignments:

<http://www.iana.org/assignments/port-numbers>

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers



Terminology



- **ICMP** – the “Internet Control Message Protocol” is normally used by the host OS or network devices to send error messages, like a service is not available or a host cannot be reached on the network. Some implementations of Ping and Traceroute rely on ICMP; firewalls can usually filter ICMP packets
- **Subnet** – an identifiable portion of a network where the devices are part of the same “routing domain”; divides the network into smaller, more manageable segments, often based on geographic location, like a building, or a specific LAN.
- **VLAN** – Virtual LAN; segments a network like a subnet, but not restricted to geographic location; wireless access points a good example – they are all over the campus but on the same VLAN (sorta...); often firewall rules are applied to a VLAN

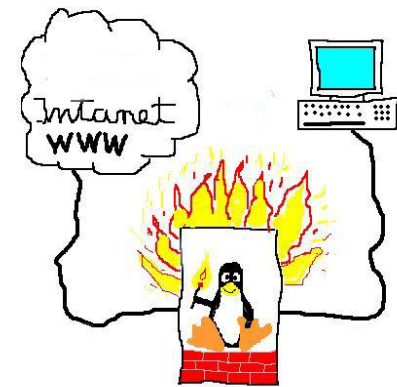
[Terminology]



- **NAT** – “Network Address Translation” hides computers from being visible on the Internet by assigning them local, non-routable IP addresses. Not necessarily a firewall function, but is often a service bundled with firewalls.
- **Firewall rule or ruleset** – instructions to the firewall on what to filter
- **Default deny** – a firewall rule that prohibits all traffic from passing through the firewall; many workstations can implement “default deny” for all incoming communication requests
- **Exception** – a firewall rule that creates an exception to a rule that has a larger scope; for example, start with a “default deny” on incoming traffic, then create an exception to allow Remote Desktop; can be confusing since the exception may deny or allow traffic, depending on the context.

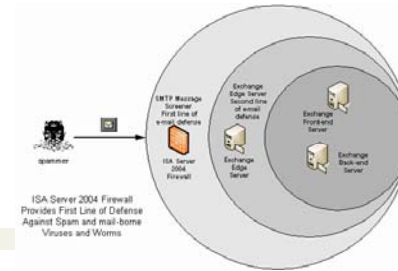
[Firewall functions

“The Internet is a bad neighborhood.”
Cheswick, Bellovin, and Rubin in
Firewalls and Internet Security

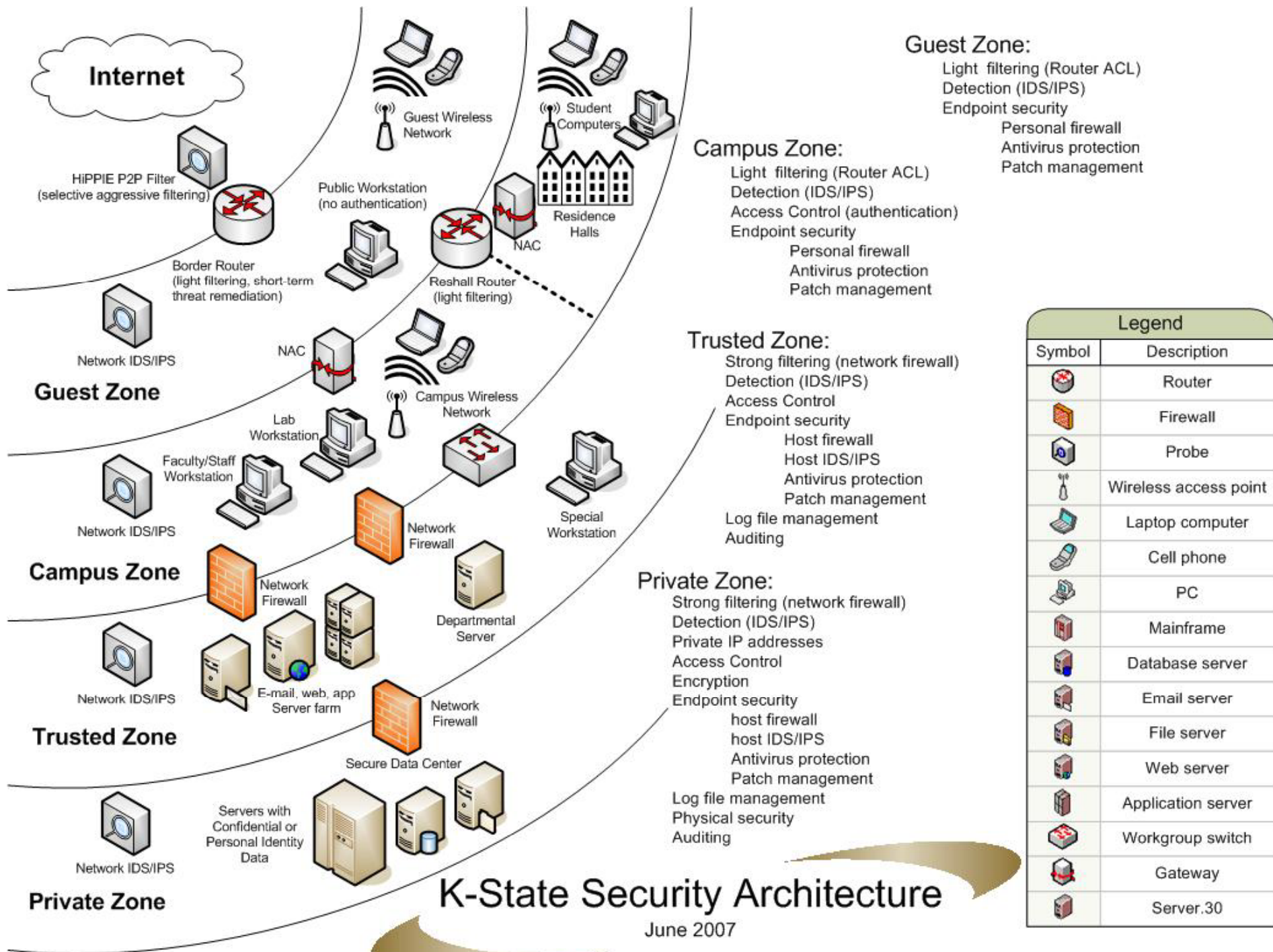


- Packet filtering – let the good stuff in, keep the bad stuff out; a “traffic cop”
- Enforce security policy – allowing what is approved, denying what is not
- Protect a computer from network-based attacks or probes/scans
- Enforce system “trust relationships”
- Intrusion detection/prevention (set thresholds to notify, block)
- Hide your computer from the Internet with “Network Address Translation” (NAT)
 - Is a NAT-only device a firewall? No more so than a DHCP server

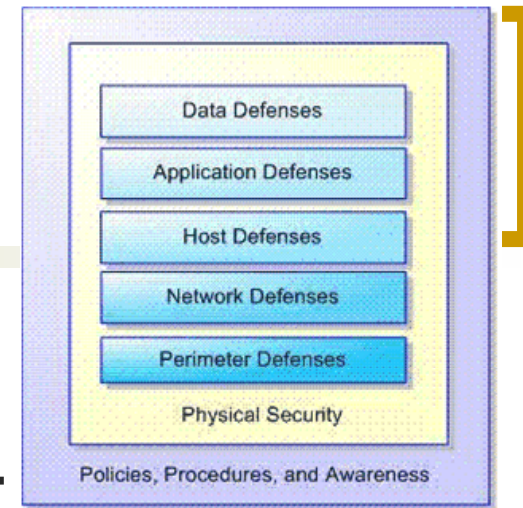
Role in IT Security



- Critical part of “layered security” or “defense in depth”
 - Need protection from threats originating from different locations on the network
 - Internet
 - Campus (residence halls, wireless)
 - Same network segment
 - Other trusted host
 - Protection when security at another layer fails or hacker penetrates a layer
 - Improves chances of detection/prevention
 - When designing a layer, assume all other layers breached



Defense in Depth



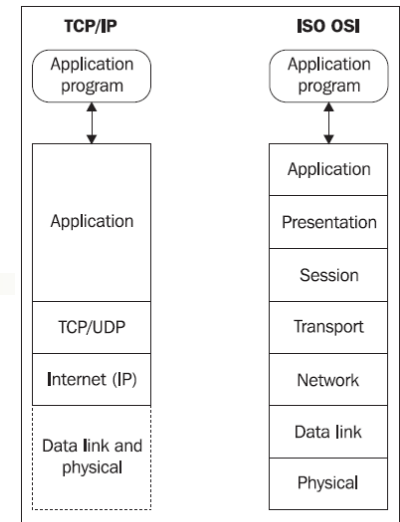
- Is more than the network - consider security @ 5 layers:
 - *Perimeter* (firewall, ACLs, VPN, DMZ)
 - *Internal Network* (hw firewall, IDS/IPS, network segmentation, IPsec, NAC, etc.)
 - *Host* (sw firewall, OS hardening, patching, authN/authZ)
 - *Application* (authN/authZ, secure coding)
 - *Data* (ACLs, encryption)
- Physical security
- Policies, procedures, awareness

“The Jericho Forum” strategy

- “De-perimeterization” or erosion of the effectiveness of perimeter defenses
- Strategy is to move protection closer to things you want to protect (data!)
- Promotes limited filtering at the campus border
- Strong protection directly in front of and on the host
- <http://www.jerichoforum.org>
- A similar perspective:
<http://www.uoregon.edu/~joe/architectures/architecture.pdf>

[Types of Firewalls

- Packet filter (layer 2 or 3) vs. application-level (layer 7) filtering – we're mostly talking about the former
- Stateful vs. stateless filtering
 - **Stateful firewall** keeps track of the state of a network connection or session so it is able to recognize all packets that are part of that session (like an SMTP email delivery). Is more efficient since can simply pass through packets that are part of an established (i.e., pre-screened) session
 - **Stateless firewall** treats every packet by itself in isolation and therefore has to fully evaluate every one against the ruleset; less efficient performance, less sophisticated filtering capability



[Types of Firewalls



- Hardware firewall (includes software!)
 - Aka “Stateful firewall”, “network firewall”, “firewall appliance”
 - Standalone network appliance performing firewall functions
 - Examples:
 - Cisco PIX, FWSM, ASA
 - Checkpoint Firewall-1
 - Linux computer running ipf with two network interfaces separating two networks or subnets
 - Home network “router”
- Trend is toward integrated security appliance, like Cisco Adaptive Security Appliance (ASA) which has firewall, VPN, and Intrusion Detection (IDS/IPS) capability
- F5 load balancing appliance provides some firewall functions (port filtering, NAT), but should not be used as a replacement for a firewall

[Types of Firewalls]

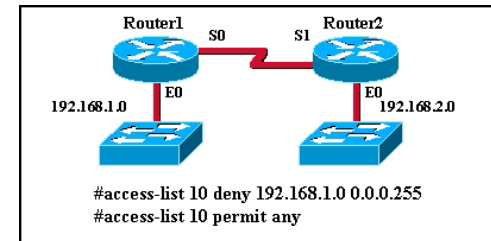


- Application firewall
 - Works at the application layer of the network stack
 - Understands behavior of different protocols or applications so it can recognize (and therefore block) anomalous traffic that may be trying to cause harm or simply be the result of an unintended error
 - Often implemented as a proxy server for the application

[Types of Firewalls]

- Software firewall
 - Aka “Host-based firewall” – software providing firewall functions protecting only the computer it is running on
 - Often called a “personal firewall” when running on a personal workstation/laptop
 - Examples:
 - IPFilter/lpf (Linux) open source firewall and NAT
 - Trend Micro OfficeScan firewall (required on K-State computers)
 - Windows Firewall (getting better)
 - MacOS X firewall (built into MacOS)
 - Freeware firewalls (ZoneAlarm, Comodo)
 - Other commercial firewalls (often part of security suites)

Router ACLs – poor man's firewall?



- “ACL” = Access Control List
- Stateless packet filtering at layer 3
- Filters network packets based on protocol and/or source and/or destination
 - IP address
 - Port
- Can provide rudimentary firewall functionality
- Routers and switches optimized to move packets, not filter them
- Risks degrading router performance

[Host-Based Firewalls]

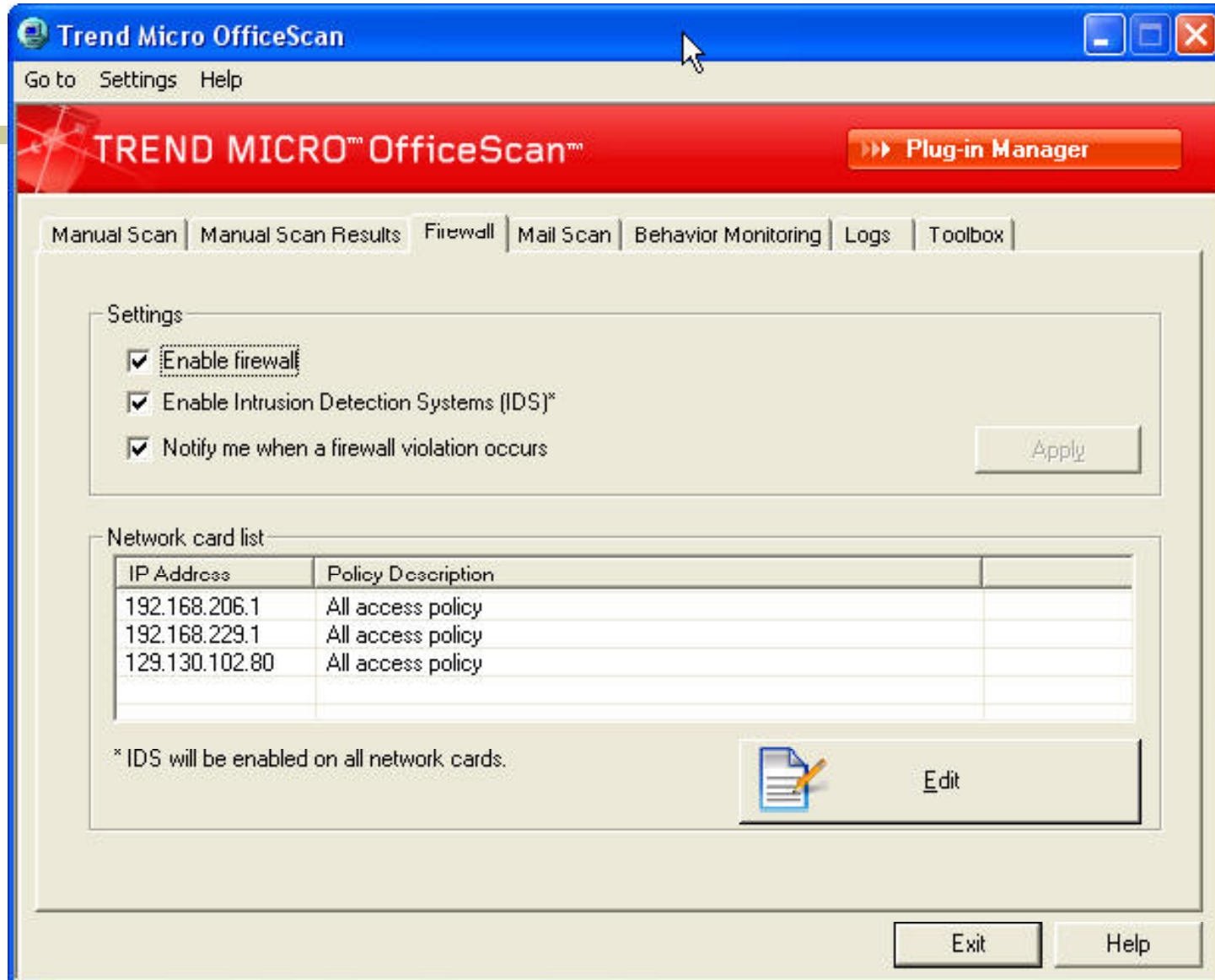


- Personal workstations/laptops
 - Required by K-State security policy
 - Windows Firewall in XP SP2 provides inbound filtering only; Vista does both inbound and outbound... sorta
 - Trend Micro OfficeScan adequate
 - MacOS X Firewall adequate

Configuring/Monitoring Trend Micro OfficeScan Firewall

- Default configuration does very little
- Demo of changing the firewall configuration (check with your IT support before changing firewall config)
- Checking log files





Exception Rule

Name: Campus-only RDP

Action

- Allow network traffic
- Allow and log network traffic
- Deny network traffic

Direction

- Inbound traffic
- Outbound traffic

Protocol: TCP/UDP

Port(s)

- All
- Range
- Specified

Port(s): 3389

Computer(s)

IPv4 - IP Range

From 129 . 130 . 0 . 0

To 129 . 130 . 255 . 255

Save Cancel

Security Level and Exception Rule List

Security level

High Block all inbound/outbound traffic

Medium Block inbound traffic, allow outbound traffic

Low Allow all inbound/outbound traffic

Exception rule list

ID	Name	Port(s)	Action	Direction	Protocol
1	Campus-only RDP	3389	Log Only	Inbound	TCP/UDP

Add Edit Delete Move Up Move Down

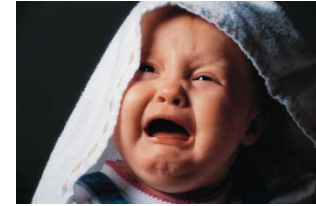
Apply Cancel

[Recommendations



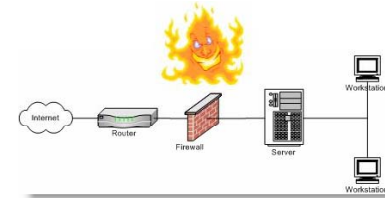
- Virtually everyone in IT services needs to understand firewalls and use them to the fullest
- If you're an application developer, ask the people managing your servers about firewall configurations (no matter what response you might get 😊)
- Include network/port behavior in your discussions with application vendors – you have to understand this to properly protect data and get the apps to work in a firewalled environment

[Recommendations



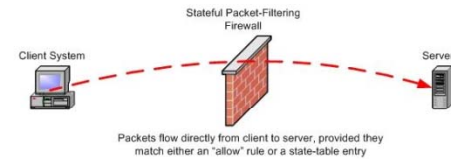
- Make sure the firewall is enabled and filtering traffic in both directions (incoming and outgoing)
- Configure firewalls to limit traffic to only what is absolutely needed for service to function
 - Protocol (TCP and/or UDP)
 - Port(s)
 - Source/destination IP ranges
 - Incoming vs. outgoing
- Start with a “default deny” configuration and open only the ports and IPs needed for the applications you MUST use

Recommendations



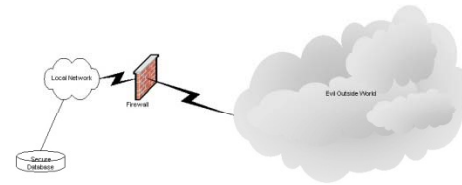
- Biggest threats to protect from:
 - Internet (lock down to campus IPs only)
 - Deny from residence halls and wireless
 - Open network jacks in the library a threat in theory, but I'm aware of only one incident on campus from this source
- Example: Configuring OfficeScan Firewall and Windows Firewall for safer use of Remote Desktop

Recommendations



- Beware of software installations or patches that reconfigure the firewall (open a port, for example, which is pretty common with Windows apps)
- Beware of opening a port permanently for a service needed temporarily (for example, to play a game or transfer a file)
- Don't ignore alerts from your firewall
- Check the firewall logs periodically

Recommendations



- Applications or malware may use a well-known port to get through firewalls, so don't get a false sense of security because you're running a firewall – remember defense in depth
 - PGP Whole Disk Encryption client communicates with the management server via TCP/80
- If the firewall seems to break an application, don't just disable the firewall and leave it – put in the effort to analyze the application and its network communications so it will work with the firewall(s)

[Finally...



- Don't assume since you have a firewall you are secure
 - Is only one part of a multi-layered approach to security
 - Some default firewall configurations are inadequate
 - Hackers are writing malware to get around/through firewalls
 - Doesn't stop a user from clicking on a malicious link and infecting the computer

[What's on your mind?]

