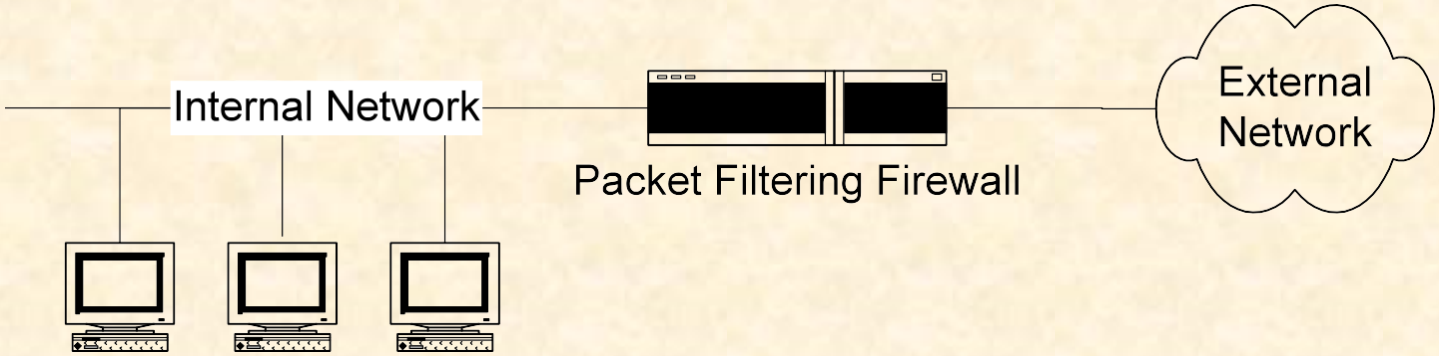
Introduction to Firewalls

Today's Topics:

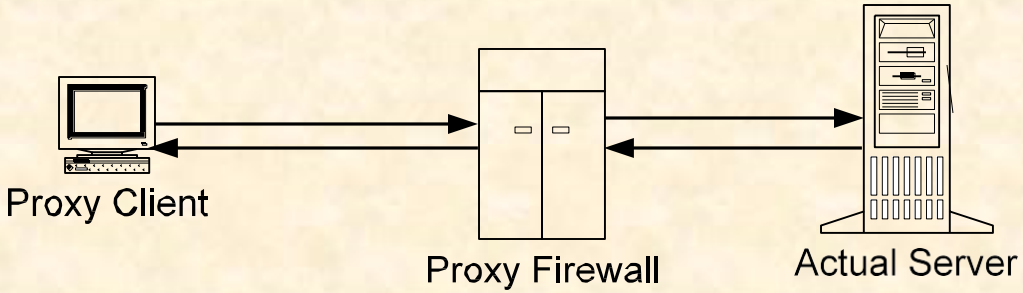
- Types of firewalls
  - Packet Filtering Firewalls
  - Application Level Firewalls
  - Firewall Hardware/Software
  - IPChains/IPFilter/Cisco Router ACLs
- Firewall Security
  - Enumeration
  - Identification
  - Attacking/Evading
  - Example Rule sets
  - Bypassing

Types of firewalls

- Packet Filtering firewall
  - Operate on transport and network layers of the TCP/IP stack



- Application Gateways/Proxies
  - Operate on the application protocol level



Packet Filtering Firewall

- Operate on transport and network layers of the TCP/IP stack
- Decides what to do with a packet depending upon the following criteria:
  - Transport protocol (TCP,UDP,ICMP),
  - Source and destination IP address
  - The source and destination ports
  - ICMP message type/code
  - Various TCP options such as packet size, fragmentation etc.

Packet Filtering Firewall: Terminology

- Stateless Firewall: The firewall makes a decision on a packet by packet basis.

- Stateful Firewall : The firewall keeps state information about transactions (connections).

- NAT - Network Address translation
  - Translates public IP address(es) to private IP address(es) on a private LAN.

Packet Filtering Firewall: Functions

- Forward the packet(s) on to the intended destination
- Reject the packet(s) and notify the sender (ICMP dest unreach/admin prohibited)
- Drop the packet(s) without notifying the sender.
- Log accepted and/or denied packet information
- NAT - Network Address Translation

Packet Filtering Firewall: Disadvantages

- Filters can be difficult to configure. It's not always easy to anticipate traffic patterns and create filtering rules to fit.
- Filter rules are sometimes difficult to test
- Packet filtering can degrade router performance
- Attackers can "tunnel" malicious traffic through allowed ports on the filter.

Application Gateway (Proxy Server)

- Operate at the application protocol level. (Telnet, FTP, HTTP)
- Application Gateways “Understand” the protocol and can be configured to allow or deny specific protocol operations.
- Typically, proxy servers sit between the client and actual service. Both the client and server talk to the proxy rather than directly with each other.

Application Gateway (Proxy Server): Disadvantages

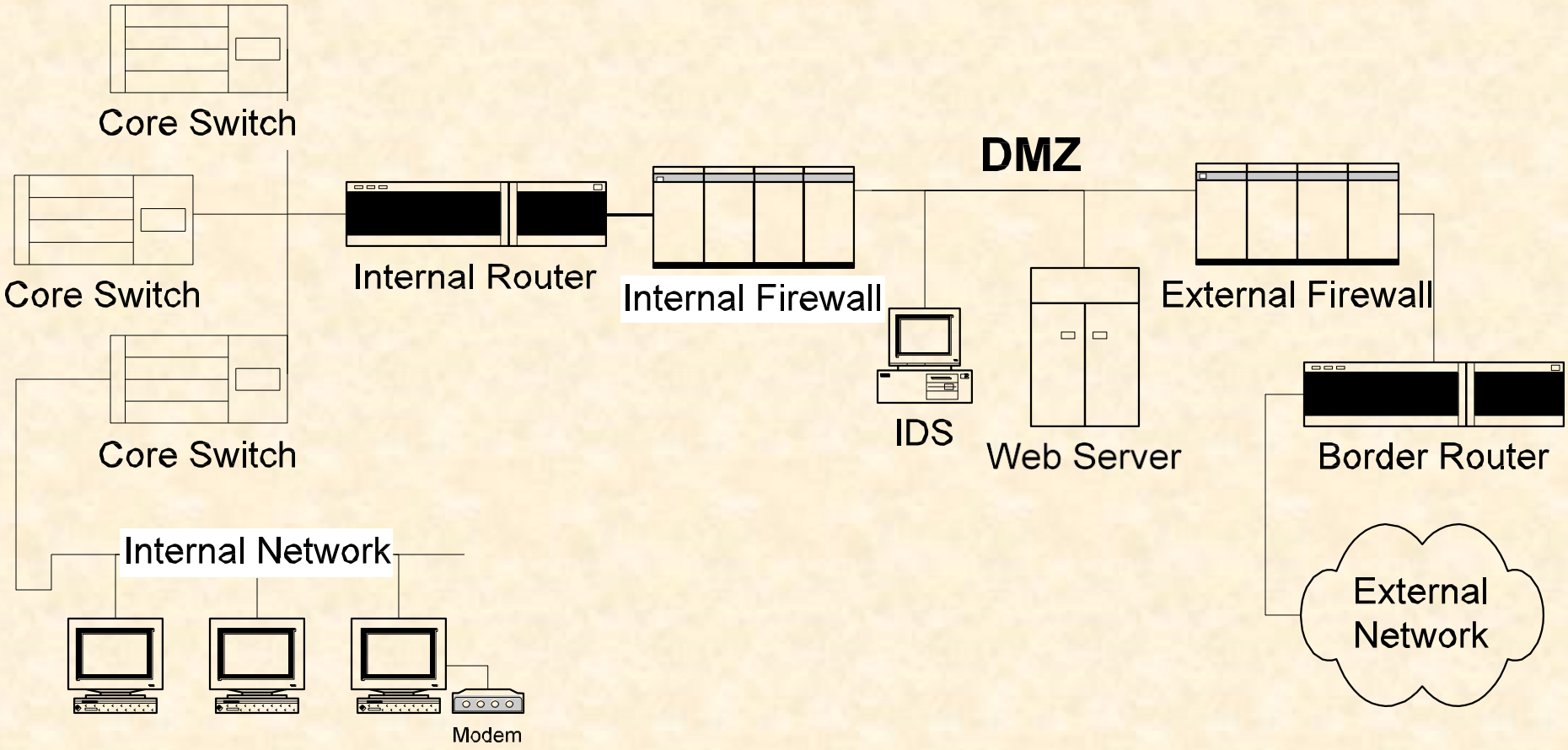
- Requires modification to client software application
- Some client software applications don’t accommodate the use of a proxy
- Some protocols aren’t supported by proxy servers
- Some proxy servers may be difficult to configure and may not provide all the protection you need.

Firewall Hardware/Software

- Dedicated hardware/software application such as Cisco PIX Firewall which filters traffic passing through the multiple network interfaces.
- A Unix or Windows based host with multiple network interfaces, running a firewall software package which filters incoming and outgoing traffic across the interfaces.
- A Unix or Windows based host with a single network interface, running a firewall software package which filters the incoming and outgoing traffic to the individual interface.
-

Firewall Architecture

In the real world, designs are far more complex



Popular Free Packet Filtering Firewall software for Unix

- IPchains - Linux 2.2.x kernels
  - http://www.linuxfaq.com/LDP/HOWTO/IPCHAINS-HOWTO.html
- IPTables (NetFilter) - Linux 2.4.x kernels
  - First stateful firewall package for Linux
  - http://netfilter.kernelnotes.org
- IPFilter - For Solaris, HP-UX, IRIX, *BSD
  - http://coombs.anu.edu.au/ipfilter/

Popular Free Application Layer (Proxy) Firewalls.

- TIS FWTK - Firewall Toolkit
  - http://www.tis.com/research/software/fwtk_over.html
- SOCKS - Proxy Server
  - http://www.socks.nec.com
- Squid - HTTP, SSL, FTP proxy cache

Firewall Security

We are going to start with network firewall security and then cover proxy firewall security.

- Enumeration
- Identification
- Attacking/Evading
- Example Rule sets
- Bypassing

Firewall Enumeration

- First, we have to find the firewall
  - How about a port scan
    - Noisy
    - Won’t work in a well configured environment
  - Traceroute
    - Find out which system in the chain does not respond

Firewall Identification

- Identifying the firewall
  - Banner grabbing
    - Various firewalls run services with obvious banners
  - Fingerprinting
    - Firewalls may behave differently, given different stimuli
  - Port identification
    - Firewalls may run services
    - E.g. Old checkpoint FW-1 keeps 257/tcp open for SNMP
  - Stateless vs. Stateful

Misconfiguration

- Liberal ACLs (a.k.a., firewall creep)
  - Problem:
    - Some organizations use a allow all, deny some rule set
  - Solution:
    - Use a deny all, allow some rule set
    - Policy

Stateless Packet Filters

- Source port scanning
  - Attack:
    - The attacker send port scans with a source port of an allowed service
    - E.g. Scan with a source port of 53/tcp (dns)
  - Countermeasure:
    - Use a properly configured stateful firewall

Stateless Packet Filters

- Fragmentation Attacks
  - Attack: Tiny fragmentation
    - IP and TCP headers are broken up across multiple fragmented packets
    - Large TCP packets may exhaust resources
  - Countermeasure:
    - Set a minimum packet size for fragmented packets (potential for DoS)
    - Packet reassembly (Watch out for pathological offsets though)

Stateful packet filters

- Tunneling
  - Attack: Tunneling/Covert channels
    - Encapsulate blocked traffic over allowed protocols (e.g. tunnel ssh over http or ICMP)
  - Countermeasure:
    - Allow these types of traffic only to/from specific hosts
    - Disable ICMP through your firewall
    - Implement multiple layers of security

Firewalls

Note that Routers, Hosts, Bandwidth Managers and LoadBalancers can and have been used as network "Firewalls".

Early Firewalls were of either of the two basic types, commercial Firewalls today are often hybrids:

1. Packet Filters – originally based on routers
   - Static (E.g. most routers)
   - Dynamic/Stateful/Multi-level (dedicated commercial firewalls and newer routers with firewall feature sets)
2. Proxies – originally based on dual-homed hosts
   - Application-aware Application Level Gateways (ALGs)
   - Generic, circuit or plug proxies (SOCKS, RWS, etc.)
   - Kernel proxies Transparent and "cut-thru" proxies

- New: Application level content filtering. Igear, Websweeper, MIMEsweeper, etc.

Add'l Adv. Firewall Functions

- Virus (malicious software) scanning.
- E-Mail attachment stripping/renaming.
- URL or (web) content blocking.
- Privacy protection (cookie & webbugs blocking)
- NAT & PAT (Network/Port Address Translation)
- Virtual Private Networking
- IDS/IDP inclusion with rule updates.
- Bandwidth Management, Flood/DoS Control.
- Load Balancing for scalability, redundancy and failover.
- Port Forwarding and virtual hosting.

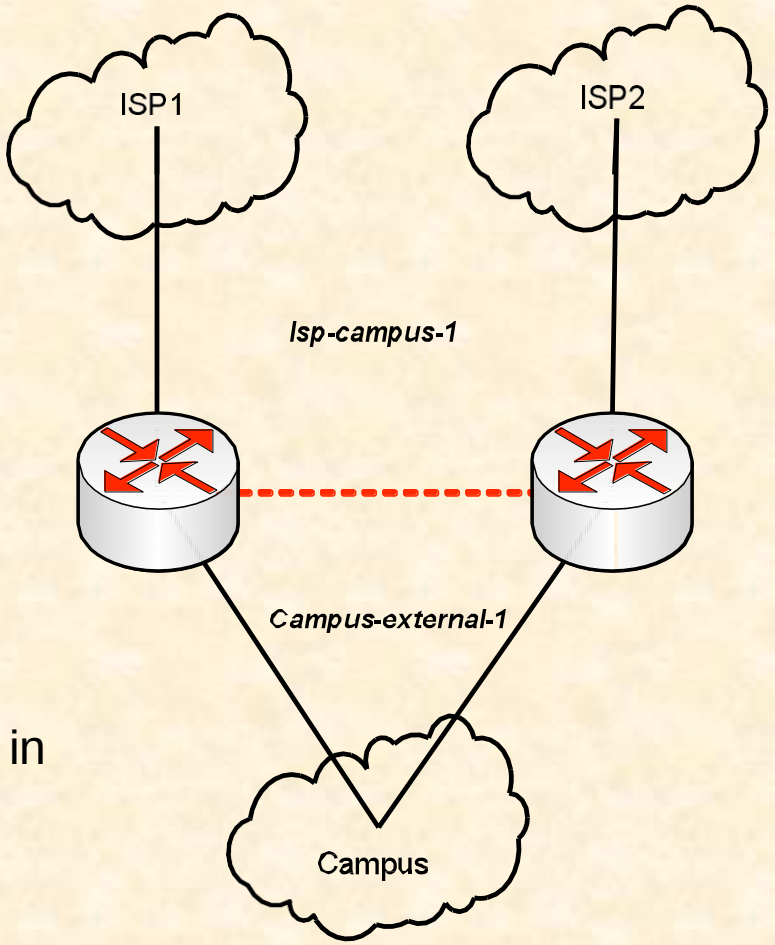
Configuration: Router interfaces

interface GE-WAN6/5

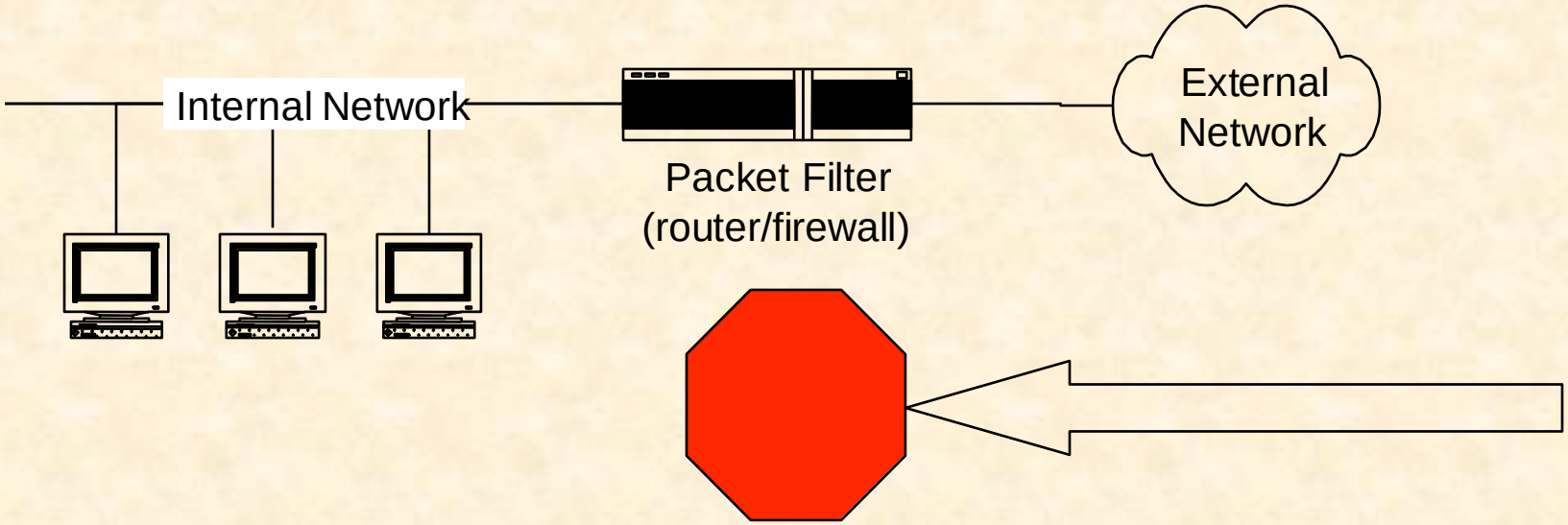
description ISP1 (vlan 5)
bandwidth 1234567
ip address 10.125.51.1 255.255.255.252
ip access-group ***isp-campus-1-in*** in
no ip proxy-arp
ip route-cache flow

interface GigabitEthernet3/8

description campus (vlan 4)
ip address 10.125.52.1 255.255.255.252
ip access-group ***campus-external-1-in*** in
ip pim sparse-dense-mode
ip route-cache flow



Ingress Filtering



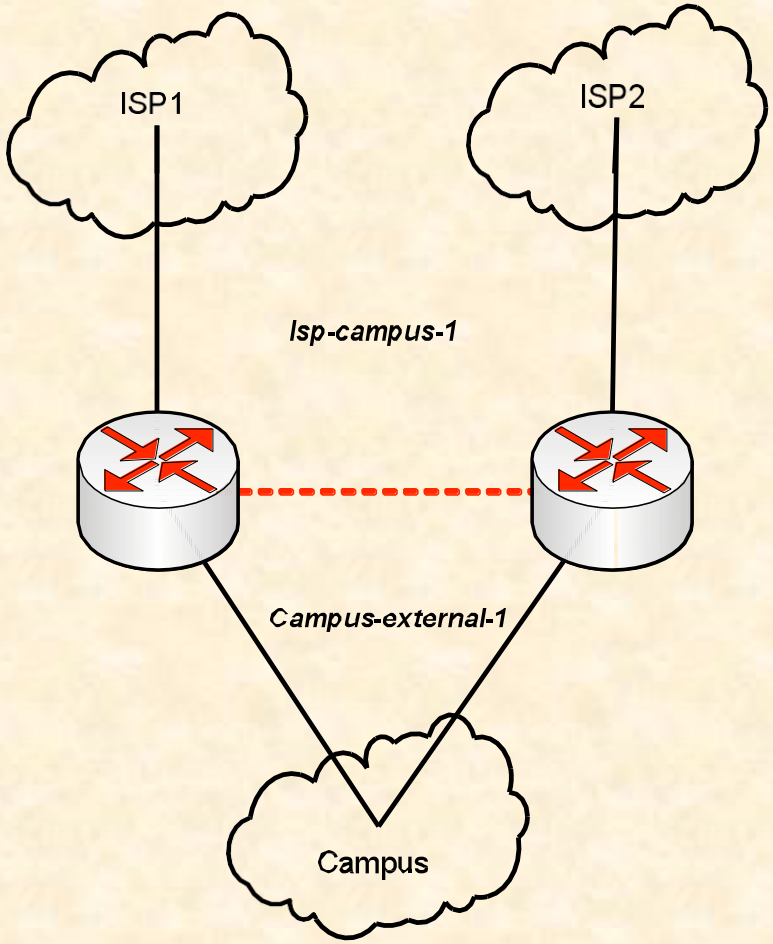
- Filter incoming traffic to your network
- Disallow packets with rfc1918 source addresses
  - (e.g. 10.0.0.0/8, 192.168.0.0/16)
- Disallow packets with local source addresses
- Disallow insecure services
  - Windows Networking
  - SNMP?

Configuration: Cisco Ingress ACL

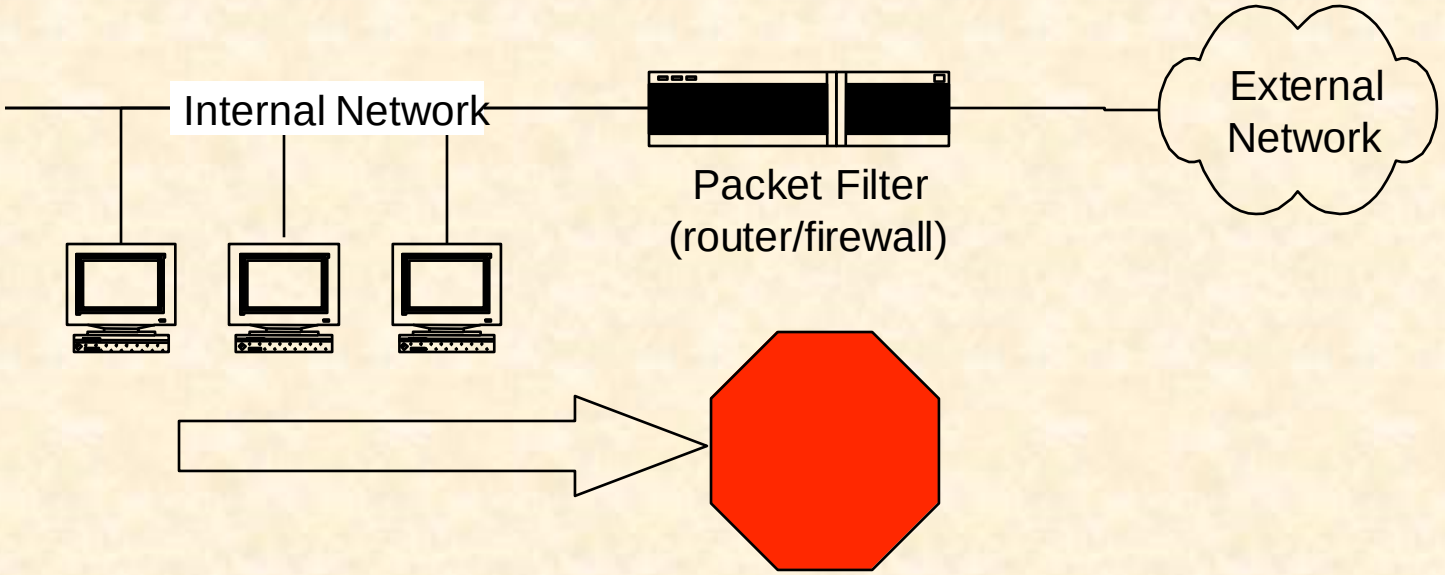
ip access-list extended

isp-campus-1-in

deny ip 10.0.0.0 0.255.255.255 any
deny ip 127.0.0.0 0.255.255.255 any
deny ip 169.254.0.0 0.0.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip host 255.255.255.255 any log
deny udp any *local mask* range 137 139
deny tcp any *local mask* range 137 139
deny udp any *local mask* eq 445
deny tcp any *local mask* eq 445
permit udp any *local mask* eq 135 log
permit tcp any *local mask* eq 135 log



Egress Filtering



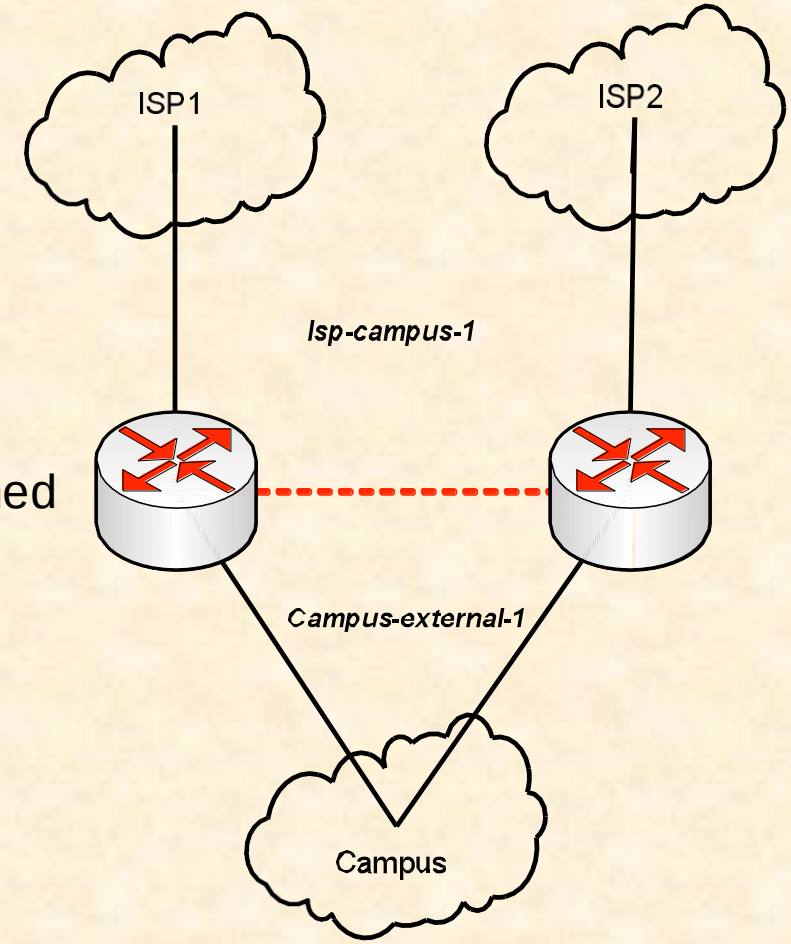
- Filter outgoing traffic from your network
- Disallow packets with rfc1918 source addresses
  - (e.g. 10.0.0.0/8, 192.168.0.0/16)
- Disallow packets with non-local source addresses
  - This helps prevent IP Spoofing
- Disallow insecure services
  - Windows Networking
  - SNMP?

Configuration: Cisco Egress ACL

ip access-list extended

campus-external-1-in

deny udp *local mask* any range 137 139
deny tcp *local mask* any range 137 139
deny udp *local mask* any eq 135
deny udp *local mask* any eq 1434
permit tcp *local mask* any eq 27374 established
deny tcp *local mask* any eq 27374
permit ip *local mask* any
deny ip any any log



Microsoft Networking

- Although a site specific decision, many sites choose to block Microsoft windows networking protocols at their border.

- NetBIOS/SMB is the ‘windows shares’ protcol
  - Frequent vector for virus infection
  - Too many non-password protected shares
  - VPN is a very good idea if you need NetBIOS
  - A LAN protcol, why should it traverse your border?

access-list XXX deny udp *local mask* any range 137 139
access-list XXX deny tcp *local mask* any range 137 139
access-list XXX deny udp *local mask* any range 445
access-list XXX deny tcp *local mask* any range 445

Microsoft Networking

- Although a site specific decision, many sites choose to block Microsoft windows networking protocols at their border.

- Windows Messenger is what generates those University Diploma popup windows
  - And they are becoming decidedly less savory…

access-list XXX deny udp *local mask* any eq 135

- University of Connecticut Windows Protcols List
  - http://security.uconn.edu/

Example: ipfilter ACL

```
# In rules
block in log body from any to any

pass in on hme0 proto tcp from any port = 80 to 10.1.1.2 port
  > 1024 with no ipopts keep state

pass in on hme0 proto tcp from any port = 443 to 10.1.1.2 port
  > 1024 with no ipopts keep state

pass in on hme0 proto tcp from 10.1.1.0/24 to 255.255.255.255
pass in on hme0 proto udp from 10.1.1.0/24 to 255.255.255.255

# Out rules
block out on hme0 log body from any to any
pass out on hme0 log proto icmp from 10.1.1.2 to 10.1.0.0/16
pass out on hme0 proto tcp from 10.1.1.2 port > 1024 to any
  port > 1024 with no ipopts keep state
```

Example: iptables ACL

```
iptables -A INPUT -p tcp --sport 80 -d 10.1.1.2 --dport 1024: -j ACCEPT
iptables -A INPUT -p tcp --sport 443 -d 10.1.1.2 --dport 1024: -j ACCEPT
iptables -A INPUT -p tcp -s 10.1.1.0/24 -d 255.255.255.255 -j ACCEPT
iptables -A INPUT -p udp -s 10.1.1.0/24 -d 255.255.255.255 -j ACCEPT
iptables -A INPUT -j DENY

iptables -A OUTPUT -p icmp -s 10.1.1.2 -d 10.1.0.0/16 -j ACCEPT
iptables -A OUTPUT -p tcp -s 10.1.1.2 -sport 1024: -dport 1024:
```

Tunneling: VPNs

- Attack: Using a VPN for Tunneling
  - Encapsulate traffic over a VPN connection
  - This is tough to catch as all the payload is encrypted

- Countermeasure:
  - Only allow VPN traffic to/from VPN concentrators
  - Implement multiple layers of security

Rule Enumeration

- Firewalking
  - Attack: Send IP packets destined for internal hosts with a small TTL
    - Analogous to traceroute, except using TCP and UDP packets.
    - If the firewall drops the packet, the port is closed
    - If you get a TTL exceeded, the port is open
  - Countermeasure:
    - Drop ICMP TTL exceeded messages at your border
    - Unfortunately, this may cause problems for legitimate users

IP Spoofing

- Attack: Spoof traffic from allowed hosts
  - Send packets with a spoofed source IP/port to bypass filters
- Countermeasure:
  - Egress filtering. Unfortunately, everyone needs to do this for it to be successful

SYN flooding

- Attack: Overwhelm the firewall's stateful buffer hoping to evade
  - Send packets with a spoofed source IP/port to bypass filters
- Countermeasure:
  - Egress filtering. Unfortunately, everyone needs to do this for it to be successful

Dialup Hacking

- Why not physically bypass the firewall
  - Attack: Use war-dialing, etc. to find insecure dialup facilites
    - Potentially difficult to detect
    - Now you have an insider attack
  - Countermeasure: Secure all dialup facilities
    - Well, sounds good in theory

Insider Attacks

- Now you have a real problem
  - Problem:
    - Although firewalls filter traffic in both directions, they generally focus on incoming as opposed to outgoing
    - Generally ACLs are more permissive to hosts within the administrative domain
  - Solution:
    - Don’t let the attackers get in
    - Properly secure your firewall from the inside as well

Firewall Security Summary

- A well configured firewall is a critical piece of a security infrastructure
  - The key is “well configured”
  - Done correctly, a firewall will stop many of the most common attacks out there
- Some organizations don’t have them
  - E.g., Most major research institutions
- Just a piece of the puzzle
  - Layered defense is the real solution