

# Campus Network Security: High Level Overview

Campus Network Design & Operations Workshop



These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license (<http://creativecommons.org/licenses/by-nc/4.0/>)



UNIVERSITY OF OREGON

Last updated 28<sup>th</sup> June 2019



# Security Outline

- Policy Framework
- Security Foundation = Network Management
- Encryption
- Virus Protection
- Authentication and Authorization
- Blocking Certain Types of Traffic
- Network Architecture and Firewalls



# Security is Hard

- Securing and monitoring the security of a campus network is difficult
- Campus networks need to be fairly open
- Always will have viruses, attacks, and people generally acting bad



# Campus Networks and Security

- Goal: Prepare for problems you **will** have
  - You will have compromises and hackers
  - You will have viruses
- You get a call from your ISP saying that they have a report that one of your hosts is participating in a Denial of Service (DoS) attack
  - What do you do?
  - How do you find the host (can be very hard with NAT)?



# Security is a Process

You can never achieve security – it is a process that you have to continually work on

- Assessment – what is at risk
- Protection – efforts to mitigate risk
- Detection – detect intrusions or problem
- Response – respond to intrusion or problem
- Do it all over again



# Policy Framework



UNIVERSITY OF OREGON



# Policy Framework

## Why is policy important?

- How do your users know what is permissible?
- How do you know what you can do?
  - Can you disconnect users from the network?
  - Can you eavesdrop on network traffic?

## What do you include?

- Typical policy framework for a University is an “Acceptable Use Policy” or AUP
  - Google for “University Acceptable Use Policy”
  - Here is an example:
    - <http://ict.kln.ac.lk/guids/ITPolicy/AcceptableUserPolicy.pdf>



# Writing an AUP

- This is your opportunity to say how you want people to behave on your network
- Keep it short and clear – 1 or 2 pages?
- Feel free to borrow from AUPs at other institutions
- Link to your existing disciplinary procedure
- Tell people where to go for help and advice





# Example: Allowed activity

- “You may use the network for reasonable purposes relating to your studies or academic research”
- “You may use the network for limited recreational use between the hours of 8pm and 6am, but must stop if requested to do so by a member of staff”



# Example: Disallowed activity

- “You may not use the network for viewing obscene material or for any activity which may bring the university into disrepute”
  - (Intentionally vague. e.g. pornography may be legal in your country, but your AUP can still ban it)
- “Questionable material will be brought to the attention of the Academic Vice Chancellor, whose decision is final”



# Example: Disallowed activity

- “You may not access any service or data for which you are not authorized, or attempt to bypass any access controls”
- “You must not use anyone else’s account, or allow your account to be used by anyone else”
- “You must keep your password secret. If you suspect someone else knows it, change it immediately”



# Example: Monitoring

“All use of the network and computing facilities is monitored and recorded for the purposes of enforcing this AUP. Your use of university facilities implies that you consent to your activity being monitored”



# Example: Consequences

“Failure to comply with this policy may result in your access to computing facilities being suspended or permanently withdrawn. It may also result in action being taken under the university disciplinary procedure, which could lead to expulsion”



# Process

- All users must see, and preferably sign, the AUP
- Include this as part of an existing process (e.g. student enrollment or username/password setup)



# Typical Acceptable Use Policy

- Use of University computing and network for University-related use only (prohibits commercial use)
- Shall not interfere with use of computing or network of others (prohibits hogging of resources)
- Copyright must be respected
- Violators can be denied access
- Use of computing and network is not private and can be monitored by IT Staff
- And more. Use Google and find examples
- Make this an official University Policy so that violations of AUP will be treated as violations of University policy



# Restating the key problems

- Some people are using excessive amounts of limited resources, e.g. bandwidth
- Some people are using the network for purposes not related to their studies
- Some people are using the network for undesirable or even illegal activities
- Put like this, it's a question of behavior and discipline, not technology
- That is why policy is important
  - Treat violations same as any other violation of University policies.





# Network Management



UNIVERSITY OF OREGON



# Security Foundation

- You must have managed equipment in your network
- You must have some basic network management running
- Network Management is the foundation that virtually all of the security framework operates on



# Key Network Management Tools

- Are some devices not responding or responding poorly, possibly because of a DoS attack or break-in?
  - Nagios
  - Smokeping
- Are you seeing unusual levels of traffic?
  - Cacti
  - LibreNMS
  - NetFlow with NfSen (sFlow, J-Flow, IPFix)



# Network Traffic Analysis

- It is important to know what traverses your network
  - You learn about a new virus and find out that all infected machines connect to 128.129.130.131
  - Can find out which machines have connected?
- What tools are available?
  - NetFlow: you will learn about this
  - Snort: open source intrusion detection system that is very useful to find viruses



# Log Analysis

- Can be just as important as traffic analysis
- Central syslog server and gather logs from:
  - DHCP server, DNS servers, Mail servers, switches, routers, etc.
  - Now, you have data to look at
  - Given an IP, you can probably find user
- Lots of tools to correlate logs and alarm on critical events



# Enforcing the AUP

- You need to be able to monitor what your users are doing
- Sometimes this is really simple
  - In a public computer lab or hostel, someone “shoulder surfing” may be sufficient deterrent
- But there are useful technical tools too
- Getting to know what's normal helps you identify when things are abnormal



# NetFlow

- Routers can generate summary records about every traffic session seen
  - src addr, src port, dst addr, dst port, bytes/packets
- Software to record and analyze this data
  - e.g. Nfdump + NfSen
- Easily identify the top bandwidth users
- Drill down to find out what they were doing



# Beware: Netflow and NAT

- You need to see the real (internal) source IP addresses, not the shared external address
- If you are doing NAT on the border router that's not a problem
  - Generate NetFlow on the interface before the NAT translation
- If you are doing NAT on a firewall then you need to generate NetFlow data from the firewall, or from some device behind the firewall





# Anomalous Traffic

- Intrusion Detection Systems (e.g. Snort) can identify suspicious traffic patterns, e.g.
  - machines using Bittorrent
  - machines infected with certain viruses/worms
  - some network-based attacks
- Typically connect IDS to a mirror port
- Risk of false positives, need to tune the rules
- Starting point for further investigation



# Associating IP address to user

- ARP/DHCP logs map IP to MAC address
- Bridge tables map MAC address to switch port
  - Several tools can do this, e.g. Netdot, LibreNMS
- 802.1x/RADIUS logs for wireless users
- AD logs for domain logins to workstations
- Network Access Control
  - e.g. PacketFence, forces wired users to login



# Using Net Management

- BAYU: “Be Aware You're Uploading”
- Detect P2P like Bittorrent and automatically send a warning E-mail telling the user to check whether what they're doing is legal
- Amazingly effective when people realize they're being watched!
- Some users may not be aware they had Bittorrent installed, and will uninstall it
- University of Oregon did this and Bittorrent use is now virtually non-existent.



# Encryption



UNIVERSITY OF OREGON



# Encryption

- Encryption is important to prevent eavesdropping by bad actors
  - Protect sensitive data
  - Protect passwords
- Disable clear-text password protocols
  - Disable telnet, ftp (and use ssh, scp)
  - Only allow TLS based POP3 and IMAP
  - Move all web traffic to HTTPS. Browsers are making this more imperative.
    - Let's Encrypt (<https://letsencrypt.org/>) makes this *so much easier*.



# SSL Certificates

- Don't use self-signed for public services
  - They teach users bad habits (that it is OK to click through an unknown certificate dialogue)
- Get certificates from well known certificate authorities (CA)\*
  - Let's Encrypt is a relatively new Certificate Authority providing free, automated and open certificates:
    - <https://letsencrypt.org/>
- Larger campuses may want to provide a certificate service



# Virus Protection



UNIVERSITY OF OREGON



# Virus Protection

- Almost all viruses are spread through the actions of users
  - Poor browsing habits
  - Opening email attachments
  - Clicking “OK” or “Install” when they shouldn’t
- Server-based viruses or intrusions are typically caused from attacks on those servers (external to campus, and from users)
  - Firewalls might help
- See the discussion on architecture that discusses where firewalls might best be placed





# Actual methods of infection

- Opening malicious E-mail attachments
- Clicking malicious links
- Gmail and other public mail services all use HTTPS by default
- Your firewall cannot inspect this traffic!
- All your firewall does in this case is act as a bottleneck for legitimate traffic



# When a machine is p0wned...

- It may connect outbound to a command-and-control center
  - Firewall will almost certainly permit this
- It may attack other machines inside your network
  - This traffic does not go through the firewall
- It may start spewing spam
  - Looks like the machine owner sending E-mail so the firewall may not stop it (see SMTP discussion)
- Firewall does not stop the infection.



# Countermeasures

- Keep all your systems up-to-date with patches
- Get rid of obsolete operating systems (esp. Windows XP)
- Use the security features built into the hosts
  - Use the built-in host-based firewall (**Do not turn it off**)
- See earlier discussion about anti-virus
- Use strong authentication and crypto wherever possible
  - e.g. RSA keys instead of passwords for SSH authentication
- Network-based detection and/or containment
  - Allows cleaning up machines once they are infected
- User education. No quick fix ■■



# Windows Virus/Malware Protection

- Very important to keep all systems up to date
- For virus protection
  - Windows 10: Windows Defender is probably adequate
  - Windows 8.1: Windows Defender
  - Windows 8: update to Windows 8.1
  - Windows 7: disable security essentials and install virus protection
  - Windows XP: just say no



# Free Windows Protection

- There are a number of free products
  - Microsoft Windows Defender Antivirus
    - Works on Windows 10 and 8.1
    - There is a version of Windows Defender that works on Windows 8
      - but only removes spyware, you still need Anti Virus
  - Bitdefender Antivirus Free Edition
  - Avast Free Antivirus
  - Sophos Free Edition
  - Kaspersky Labs
    - Some concerns in US Government about Russia ties



# Authentication and Authorization



UNIVERSITY OF OREGON



# Centralized Authentication

- How do you know who is using your network?
- AAA: Authentication, Authorization, and Accounting
- Central database of users
  - Can be a single system that everyone has a login (or password file entry)
  - LDAP or Microsoft Active Directory
- Systems and Devices use database
  - Protocols: Radius, LDAP, Kerberos, and Active Directory



# Importance of Central Authentication

- You need to restrict use of your facilities (labs, wireless, email, etc.) to users who are affiliated with your campus
  - If you don't do this, campus security will be very difficult
- Best practice is to have a central LDAP or Active Directory that has all users
  - This database should be synchronized with the human resources and student systems so when someone quits or leaves school, their credentials are no longer valid
- If you don't have this, you can start with a database and a radius server
  - But realize you need LDAP or Active Directory in the future





# Wireless

- Do not run an open network or one with a pre-shared key
  - If you do, you will have many users who aren't associated with your institution
- Best practice is to authenticate users
  - This allows you to know who your users are
  - Requires central AAA database
  - Log the access to your central syslog server
- How to force authentication on wireless?
  - Captive Portal
  - 802.1x WPA2 Enterprise
- Who can install access points (AUP)?



# Blocking Traffic



UNIVERSITY OF OREGON



# Blocking Traffic

- Best practices requires a balance of blocking bad traffic and allowing other traffic
  - Default needs to be to allow traffic, not to block traffic
- Need to allow the network to be used in creative ways
- But stop things that are big vulnerabilities
  - Vulnerabilities need to be blocked from the external network until they are fixed
- Don't need a firewall for this; an Access Control List on the border router is just as effective
  - It costs less, is less complicated, and doesn't impact performance



# Blocking Inbound Traffic

- The best practice today for blocking inbound traffic simply involves not allowing packets sourced from:
  - The Campus public IPv4 & IPv6 address space
  - Private IPv4 address space
  - Unused IPv6 address space (outside of the 2000::/3 block)
  - RFC6890 describes the special purpose IP address blocks many of which are not routed on today's Internet
- These filters can be easily implemented on the campus border router



# Blocking Inbound Ports

- Today there is minimal blocking of incoming ports required
  - All end-user devices have firewalls
  - All servers have built-in firewalls, and are protected by firewalls (see firewall placement discussion)
  - Campus infrastructure does need to be protected (simple border router filters are enough)
- Campuses need to be monitoring incoming traffic to look for any unusual trends
  - Standard practice using IDS and/or NetFlow



# Blocking Outbound Traffic

- The best practice today for blocking outbound traffic simply involves not allowing traffic from any source IP addresses apart from those **public** IPv4 & IPv6 addresses in use on the campus
- Plus:
  - Private IPv4 address space usually lives behind NATs and will be NAT'ed to a public address
    - Private IPv4 address space which has not been NAT'ed must be blocked
  - For IPv6, 2000::/3 is the global unicast address space
    - Traffic sourced from any other IPv6 addresses must be blocked
- These filters can be easily implemented on the campus border router



# Blocking Outbound Ports

- Blocking outgoing ports seriously inconveniences users and visitors
  - Some sites block lots of TCP ports
  - Even simple things like email may need ports 465, 587, 993, and 995 to send and receive mail
  - Remember, you want as open a network as is possible
- Some things are hard to block
  - e.g. Bittorrent can tunnel through port 80 or 443



# Outbound ports to block

- There are some outbound ports that are recommended to be blocked
- Here are some examples:
  - 25 TCP – Unauthenticated SMTP (see slide discussing SMTP)
  - 123 UDP – Network Time Protocol (must allow campus NTP servers)
  - 135 through 139 both TCP and UDP – Microsoft NetBIOS





# SMTP notes

- Blocking TCP port 25 outbound is strongly recommended
  - You will still need to allow port 25 outbound for authorized campus SMTP servers
- Forces users to relay mail via your local SMTP server (or use 465 or 587 authenticated SMTP to external SMTP servers)
  - Local SMTP server will log all emails and can apply a rate limit on number of emails sent per user (e.g. exim) can do this.
- Easier to detect and control virus-infected machines which are sending spam and affecting your network's reputation



# Block YouTube / Facebook etc?

- There are many valuable educational videos on YouTube
- Staff have legitimate uses for Facebook to maintain professional connections
- Clever students will find ways around
  - Universities are designed to attract clever people



# Bandwidth shaping

- Give your users (say) 1Mbps each? It only takes 50 abusers to burn 50Mbps between them
- Give them much less and you are penalizing everyone
- There are legitimate users of large amounts of bandwidth (e.g. research datasets)
- Shaping and prioritization won't fix not having enough bandwidth to meet demand



# Deep Packet Inspection (DPI)

- Classify, shape, or even block traffic by content
- Much traffic is HTTPS and therefore cannot be inspected
- No DPI box can distinguish between humorous cat videos and veterinary medicine videos
- In-line control products are very expensive and cause significant bottlenecks
- Out-of-line (e.g. Snort) much more useful for detecting malicious activity



# Performance

- Any device you put in-line with all your traffic can become a bottleneck
- You may only have 10Mbps today, but soon it will be 100Mbps, then 1Gbps, then 10Gbps
- Traffic filtering / inspection / shaping at higher rates is extremely expensive
- Search on-line for “science DMZ” – many sites now bypassing firewall entirely



# Executive summary so far

- Firewalls are useless
- Bandwidth shaping is useless
- DPI is useless
- What do we do now? ■■



# Campus Network Architecture



UNIVERSITY OF OREGON



# Architecture to Help With Security

Key architectural issue to help with security is segmentation and IP addressing schemes

- Follow campus network best practices
- Route in the core
- One IP Subnet per building
- Put campus-level servers on IP subnet that is separate from users
- Servers with sensitive information (for example, Moodle) should be on different subnets





# How useful are firewalls?

- A long time ago, end user machines used to get infected through direct network attacks (no action by the user)
- All end-user systems have firewalls turned on by default
  - Windows (since XP SP2), MacOS, and Linux
  - **Don't turn the end-user systems firewalls off!**
- User machines don't get viruses without users help
- We've already discussed how firewalls don't help
- People still design networks as if firewalls would help



# Where to put Firewalls

- Traditional recommendation for firewalls is based on old experience with Windows prior to XP service pack 2
  - Windows machines would get infected from the Internet just by being on the network
- Firewalls were placed to do NAT and to protect entire campus
- This is a very “Corporate” approach and doesn’t allow for innovation by users

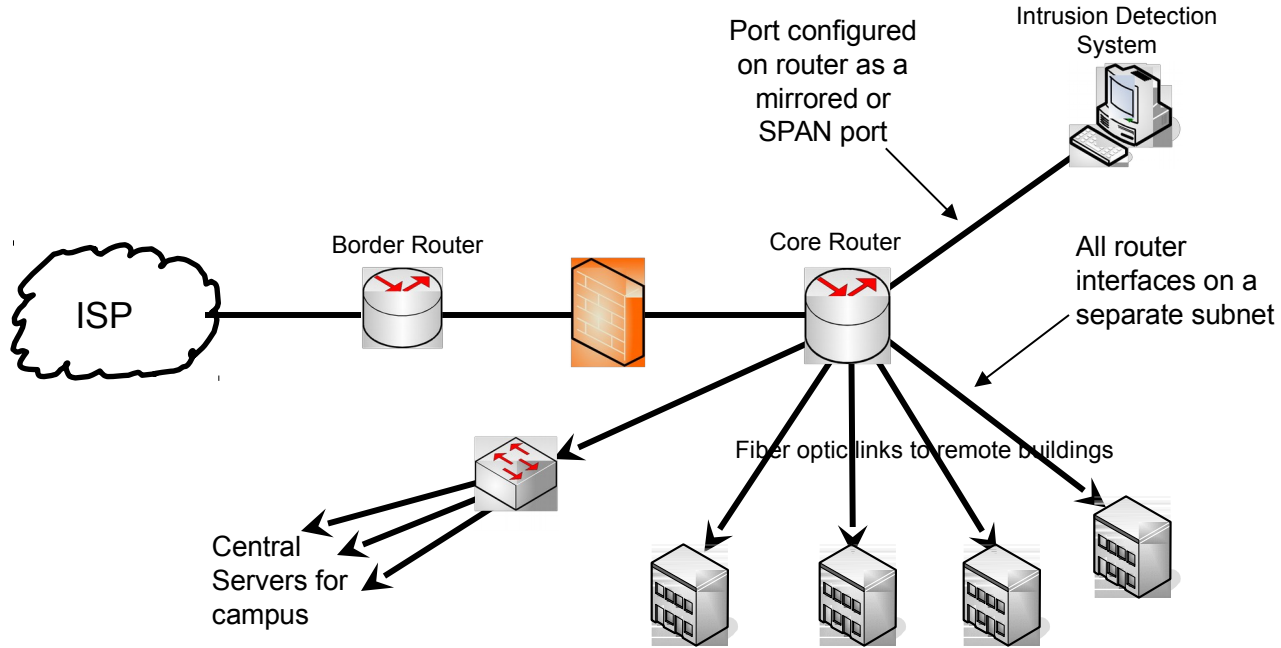


# Firewall Placement

- Firewalls don't protect users from getting viruses that come via the two most common mechanisms
  - “clicked links” while web browsing
  - Email attachments
  - Both are encrypted and firewalls won't help
- As bandwidth increases, in-line firewalls limit performance for all users. This gets to be a bigger problem at higher speeds.



# Traditional Design



# A Newer Approach to Firewalls

- Traditional design doesn't protect servers from on-campus users
- Firewalls limit performance and cause bottlenecks
- This drives a new approach to firewalls
  - Firewalls should only protect critical assets
  - This allows firewalls to more tightly protect the critical assets even from attacks from “inside”

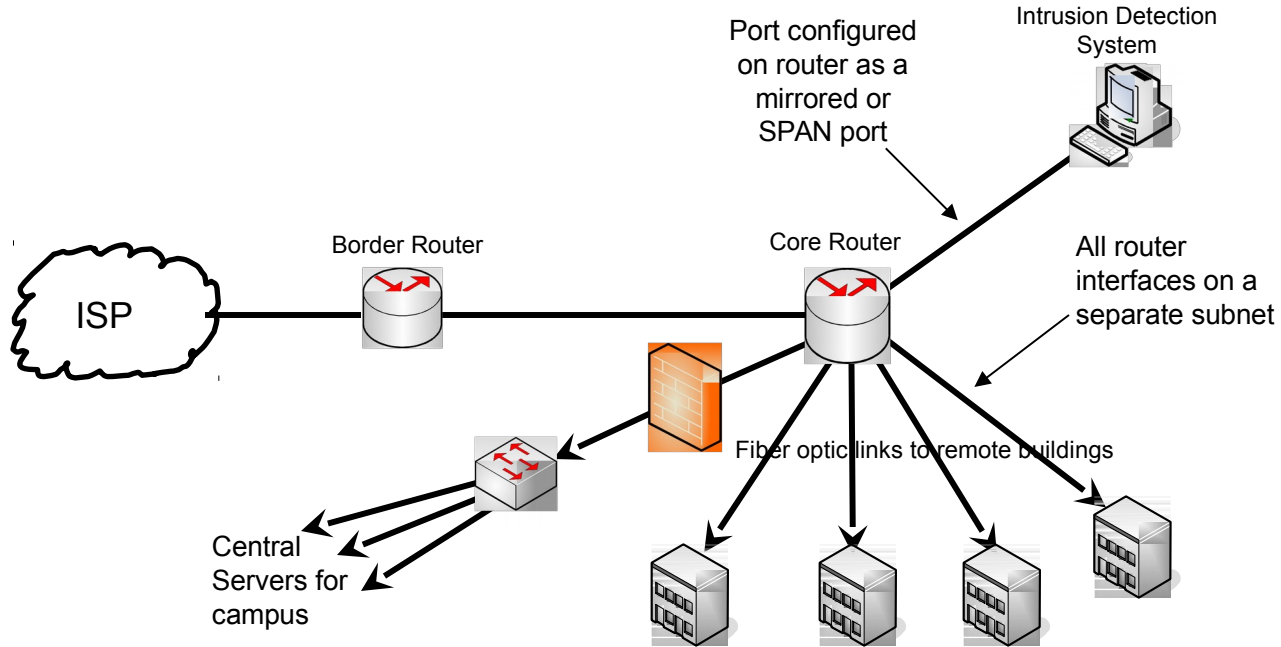


# Recommended Firewall Use

- We recommend that you firewall just the servers with sensitive data
- Always use two levels of defense: hardware firewall and host based firewall. If one fails, you are still protected
- Firewall should protect
  - Limit inbound access to servers to only those ports needed for access to the application (e.g. HTTPS).
  - Limit access from server to rest of network – if compromised, further attacks are contained (“DMZ”)
  - Block sensitive servers from Internet and require VPN authentication+encryption to access
- But beware that stateful firewalls are themselves vulnerable to DDoS / exhaustion attacks

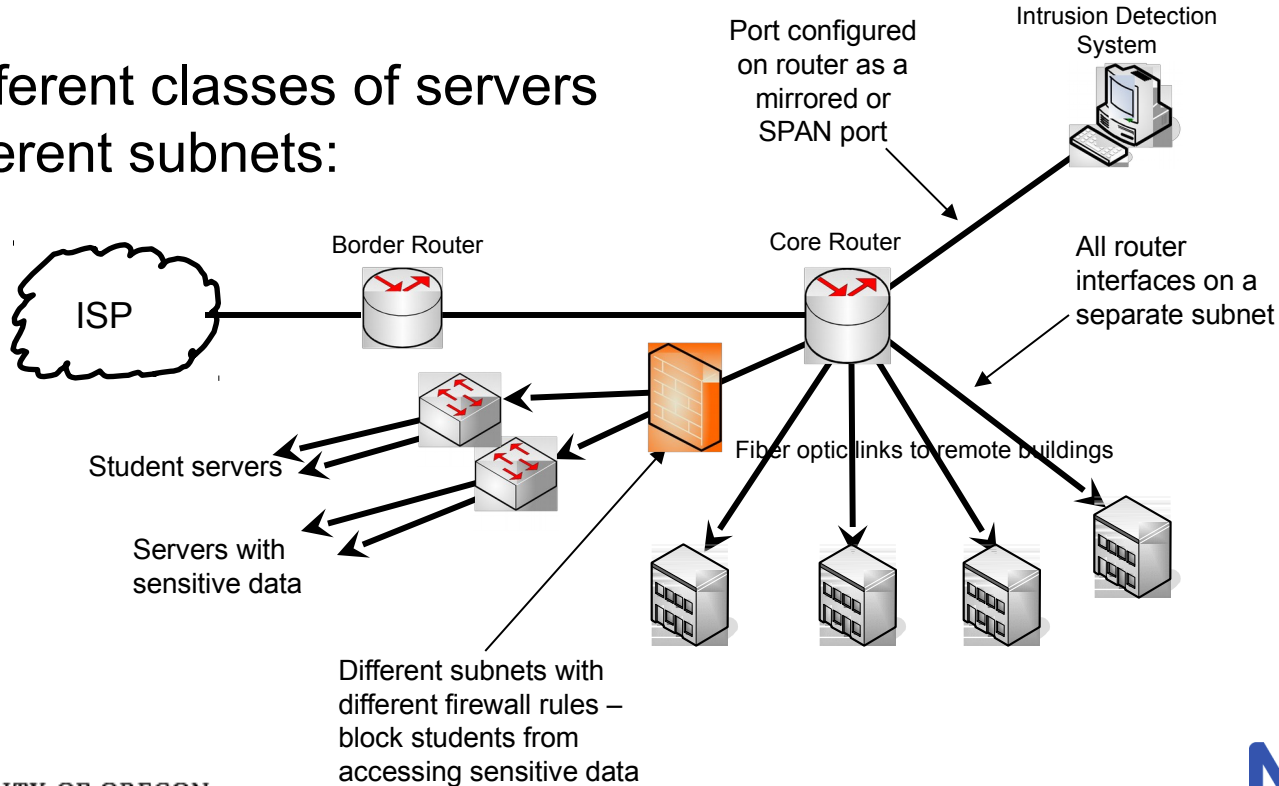


# Newer Design



# Newer Design

- Put different classes of servers on different subnets:





# Summary

- Policy is important
- Network management tools are used for security
- Take action on specific issues
  - Encryption
  - Virus Protection
  - Authentication and Authorization
- Use firewalls only to protect sensitive servers



# Resources

- Lots of resources on the Internet
  - [www.sans.org](http://www.sans.org) – subscribe to the SANS newsletter
  - [www.team-cymru.org/templates.html](http://www.team-cymru.org/templates.html) – a great set of templates for secure configuration of routers and some services
  - [www.manrs.org](http://www.manrs.org) – Mutually Agreed Norms for Routing Security: filtering, routing security, route validation, global coordination
  - [www.cert.org](http://www.cert.org) – a good resource for lists of vulnerabilities
  - [www.google.com](http://www.google.com) – having a problem? Seeing an error message? Google it.



# Questions/Discussion?



UNIVERSITY OF OREGON

