Campus Network Security: High Level Overview

Campus Network Design & Operations Workshop

UNIVERSITY OF OREGON

Last updated 3rd October 2024

NSRC
Network Startup Resource Center

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

NSRC
Network Startup Resource Center

Policy Framework

Why are policies important?

- IT is part of the basic and foundational infrastructure of your institution
- You must have policies to guide how cybersecurity operates
- These policies need to be developed and approved by the institutional leadership

What kind of policies do you include?

- Policy to form cybersecurity group
- Policy to describe types or categories of data your institution holds and who is responsible for this data
- Policy to describe how to respond to security incidents
- You need to have procedures to handle common cases

Large Business or Institution Policies

- Larger organizations (particularly public organizations) must have policies about ***lots*** of things
- University of Oregon Policy Library (https://policies.uoregon.edu/)

Criminal, Credit and Related Background Checks on Applicants for University Positions	UO Policy Statement
Data Security Incident Response	
Definition of Unclassified Staff	Oregon Administrative Rule
Diversity	OUS Board Policy
Drug-free Workplace	UO Policy Statement
Electronic Signatures	UO Policy Statement
Employee Morale-Building Event Expenditures	UO Policy Statement
Employment of More than One Member of Household	Oregon Administrative Rule
Environment and Sustainability	UO Policy Statement
Equal Opportunity	OUS Board Policy

Policy to Create Cybersecurity Function

- A policy to grant authority to an Information Security Office to:
  - Develop policies, procedures, and guidelines for securing systems, networks, and data based on applicable laws, regulations, and best practices
  - Investigate information security issues, perform risk assessments, and propose products and processes to mitigate risk discovered
  - Monitor networks and systems to identify malicious activity
  - Provide incident response for information security incidents
  - And more (training, communication about security risks, evaluate new systems, provide advice to mitigate security risks, etc.)

Data Classification Policy

- Multiple Parts of this type of policy
  - Defines Roles and Responsibilities
    - Typically a hierarchy of personnel starting at the upper management of the organization to supervisors down the the personnel who manage and maintain the data
  - Defines Data Classification Types
    - Low risk – public data
    - Medium risk – data that should not be public, but only moderate risk if exposed
    - High risk – data that if exposed has high risk
  - All data held by various parts of the organization must identify the various personnel responsible as well as the classification of the data
    - The analysis of the data is typically not part of the main policy, but rather an appendix or a separate document

Data Classification Examples part 1

- Roles at University of Oregon
  - Chief Information Security Officer (CISO): develops policies and procedures to protect data and comply with laws and regulations
  - Data Trustee: the Chief Academic Officer or designee will have policy level and management responsibility for the data
  - Data Stewards: personnel assigned by the trustee who have operational responsibility for the the management of the data
  - Data Custodians: personnel assigned by the stewards who are responsible for the operation and management of the systems that hold the data
  - Data Consumers: University community members who have been granted access to specific data items due to their assigned duties and roles

Data Classification Examples part 2

- Data Classification levels at the University of Oregon
  - Low risk (or Green): data is classified as low risk if the loss of confidentiality of this data has minimal strategic, compliance, operational, financial or strategic risk
  - Moderate risk (or Amber): data is classified as moderate risk if the loss of confidentiality of this data has moderate strategic, compliance, operational, financial or strategic risk
  - High risk (or Red): this is the most sensitive/critical classification and is selected if the loss of confidentiality, integrity, or availability of the data would have *high* strategic, compliance, operational, financial, or reputational risk to the University. Often exposure of this data requires specific action by the University under local, state, or federal law

Samples of Types of Data

- Small portion of types from University of Oregon

Data Security Classification Table

Note: data may be represented in any format including digital records, audio or video recordings, and printed material.

Table of Contents – Data Type

Sample of a specific data type

Architectural diagrams for the physical spaces where critical systems or functions exist

Functional Classification/Corresponding Retention Schedule Series	Data Type	Description & Examples	Security Classification	Office of Record	Data Steward	Data Custodian
IV.05. FINANCE/Public safety and Risk Services IV.06. FINANCE/Information technology IV.07. FINANCE/Property, facilities and planning; sustainability IV.09. FINANCE/Purchasing and contracting	Architectural diagrams for the physical spaces where critical systems or functions exist.	Information resides in multiple systems (GIS, CPFM Asset Management) and includes location and in some cases what specific equipment is in them. Examples of sensitive locations include: • Animal Labs (e.g., Zebra Fish) • Tunnels • UE Facility • Datacenters • Building Mechanical Rooms	High Risk (Red)	Safety & Risk Services (SRS) Campus Planning & Facility Management (CPFM)	Chief Resilience Officer Associate Vice President for Campus Planning and Facilities Management	Lead IT service provider(s) for Office of Record

Security Incident Response Policy

- Requires anyone associated with institution to report a security incident the security team (duty to report)
- When a report has been submitted, requires that the policy be followed
- The activities for following up on a report might well be a stand-alone document that is a procedure
  - Procedures are easier to develop and modify than a policy

Student or Employee Conduct

- This is a non-technology specific document that outlines what is expected from the student or employee. Typically the student conduct and the employee conduct codes are separate/different documents. Covers things like:
  - Improper use of organization resources (anything from stealing copier paper to using IT resources for personal gain)
  - Improper use of access controls (anything from letting someone borrow keys or access control cards to passwords and accounts)
  - Cheating or plagiarism (could involve technology or not)
  - Bullying or hate speech (could involve technology or not)

NETWORK MANAGEMENT

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Security Foundation

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

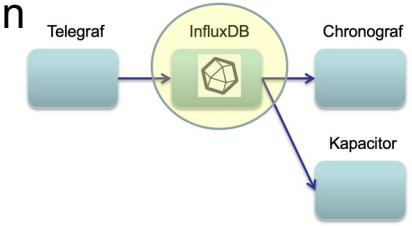
Classical Network Management Tools

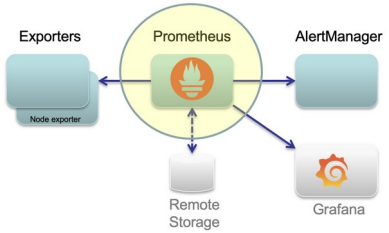
- Are some devices not responding or responding poorly, possibly because of a DoS attack or break-in?
  - Nagios
  - Smokeping
- Are you seeing unusual levels of traffic?
  - Cacti
  - LibreNMS
  - NetFlow with NfSen (sFlow, J-Flow, IPFix)

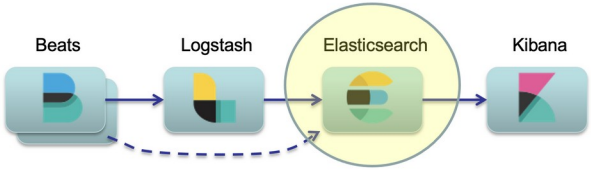
NET MANAGEMENT	NETFLOW / IPFIX / SFLOW	LOGS / SIEM	DOCUMENTATION
Cacti	ElastiFlow	Beats	diagrams.net
LibreNMS	Filebeat/Packetbeat	Elasticsearch	GLPI
Nagios/check_mk	NfSen	Fluentd/fluent-bit	InvenTree
Netdata	ntop-ng	Loki	IPplan
OpenNMS	pmacct	OSSEC/Wazuh	Netbox
Prometheus	**SECURITY / NIDS**	Sagan	Netdisco
Sensu	Nessus	**TICKETING**	phpIPAM
Zabbix	Prelude	OSticket	Snipe-IT
PERFORMANCE	Snort	OTRS	**CHANGE MGMT**
perfSONAR	Suricata	RT	Oxidized
Smokeping	Zeek	Trac	RANCID

Modern Network Management Tools

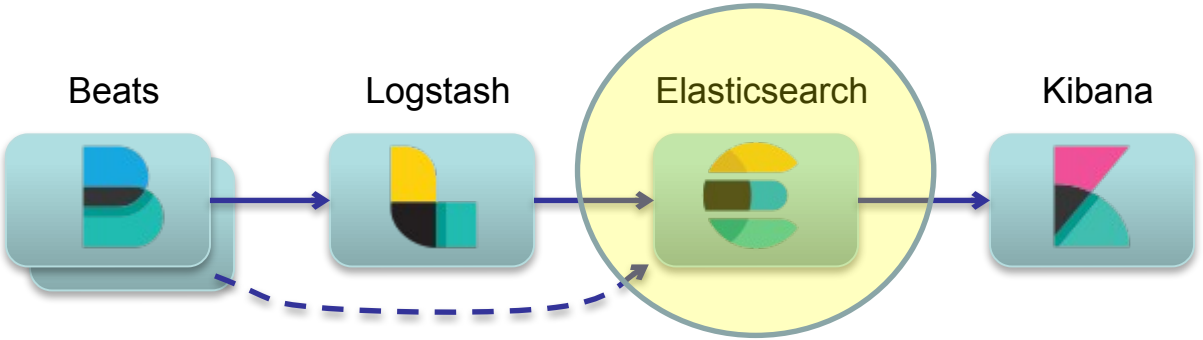
- Software stacks that allow for real-time network state monitoring
- Generally, involve the mixed use of SNMP, http and agents in on servers using both a *pull* and *push* models
- Are more complex, but provide
  - alerting on events,
  - detailed dashboards of network state,
  - detection of anomalies,
  - trend analysis
  - network traffic inspection using network flows
- Some popular software stacks include:
  - Prometheus
  - ELK
  - TICK and many others





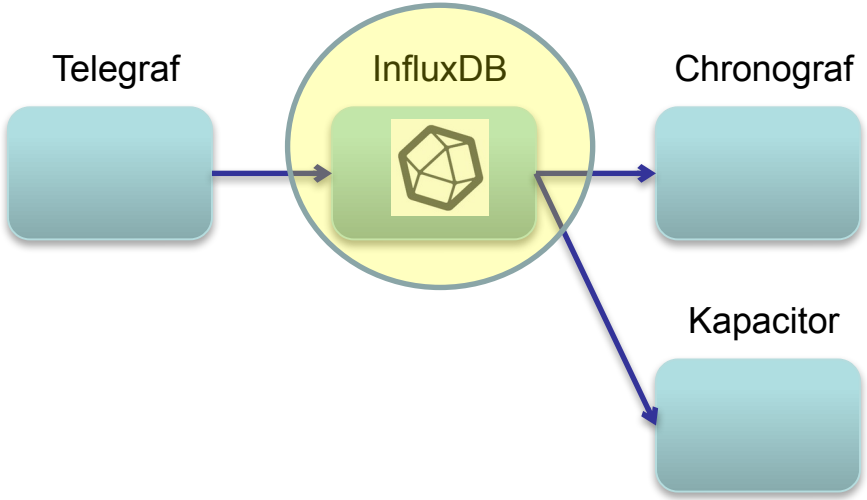


The Elastic Stack (ELK)

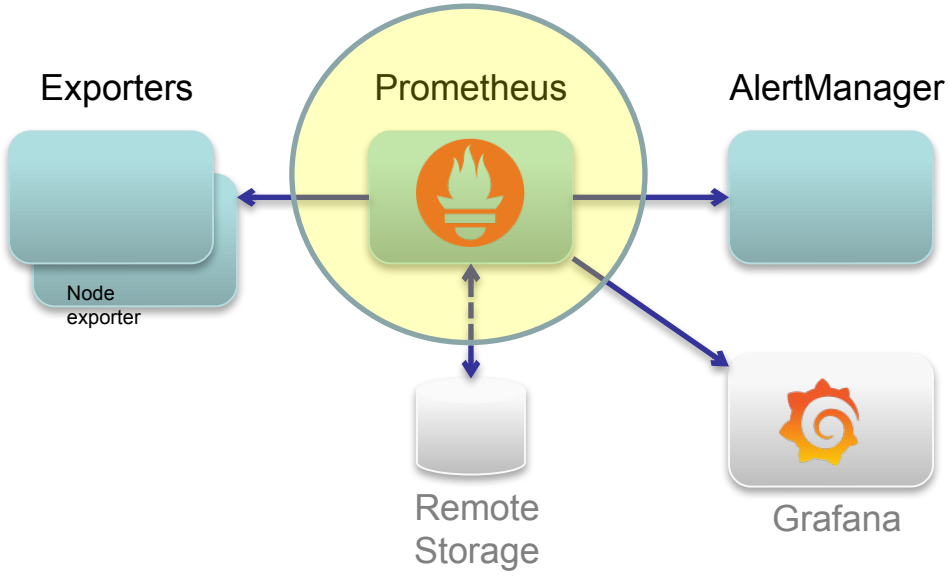


("The BLEK Stack" doesn't sound as good)

The TICK Stack

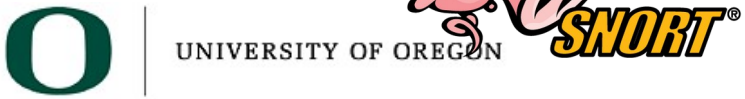


Prometheus


Exporters
Prometheus
AlertManager
Node
exporter
Remote
Storage
Grafana

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, Suricata, Zeek (formerly Bro) and others: open source intrusion detection systems that are very useful to find viruses

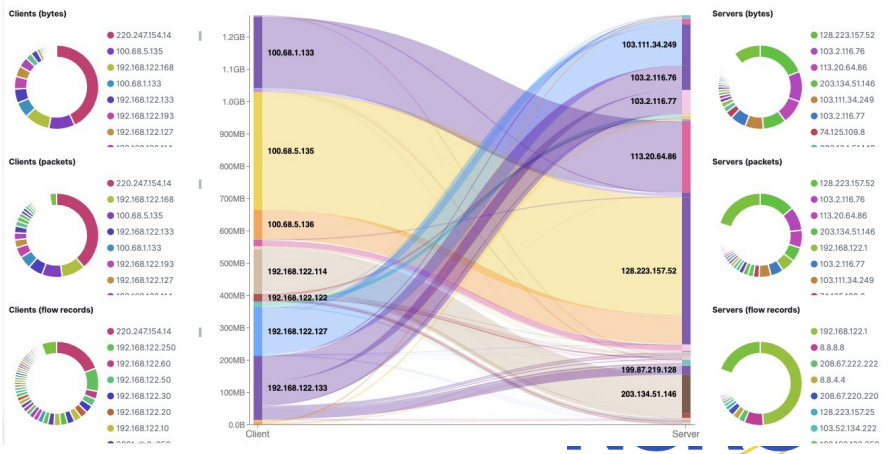


Log Analysis

- 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

Network Flows

- 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
  - Nfdump + NfSen (traditional)
  - ElastiFlow, ntop-ng (modern)
- Easily identify the top bandwidth users
- Drill down to find out what they were doing



UNIVERSITY OF OREGON

ElastiFlow

Network Startup Resource Center

Beware: Network Flows 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
  - Depends on firewall placement

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 on a switch
- 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, Netdisco, LibreNMS
- 802.1x/RADIUS logs for wireless users
- Active Directory (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 some years ago when Bittorrent was commonly used for sharing copyright material
  - This dropped Bittorrent use from many megabits per second to virtually nothing

Summary

- Policy is important (i.e. AUP)
- Network monitoring and management tools are used for security
- Take action on specific issues
  - Encryption
  - Virus Protection
  - Authentication and Authorization
- Use firewalls only to protect sensitive servers
  - Public facing, separate network segment

ENCRYPTION

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Encryption

- Encryption is important to prevent eavesdropping by bad actors
  - Protect sensitive data
  - Protect passwords
- Use full-disk encryption on laptops and desktops
- 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

2FA

- Two Factor Authentication
- Password plus secondary authentication, e.g.
  - SMS/Text with a code that expires
  - Email with a one-time code that expires
  - Software with a time-based code (TOTP), e.g. Google Authenticator
  - Push to phone app, e.g. Duo, Ping Identity, Microsoft authenticator
  - Physical tokens, e.g. Yubikey, Webauthn/U2F

VIRUS PROTECTION

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

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**)
- Anti-virus, or more generally "EDR" ("Endpoint Detection and Response")
- 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 and earlier are now all out of support and should be eliminated

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

NSRC
Network Startup Resource Center

Centralized Authentication

- How do you know who is using your network?
- AAA: Authentication, Authorization, and Accounting
- Central database of 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
- Systems and Devices use database
  - Protocols: Radius, LDAP, Kerberos, and Active Directory
  - Web based auth: OpenID Connect, OAuth2 (e.g. Azure AD)

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
  - Can be a single system that everyone has a login (or password file entry)
- If you don't have a single, central database of all users, then you can start with a specific 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

Blocking Traffic

- Best practices require 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
- End users circumvent firewalls with VPN: then you lose visibility as well

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 (Windows in on by default)
  - 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, and will automatically switch if UDP is blocked

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 and 445, both TCP and UDP – Microsoft NetBIOS/SMB

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 and does not support large data flows
- 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

NSRC
Network Startup Resource Center

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’ action
- We've already discussed how firewalls don’t help
- People still design networks as if firewalls would help

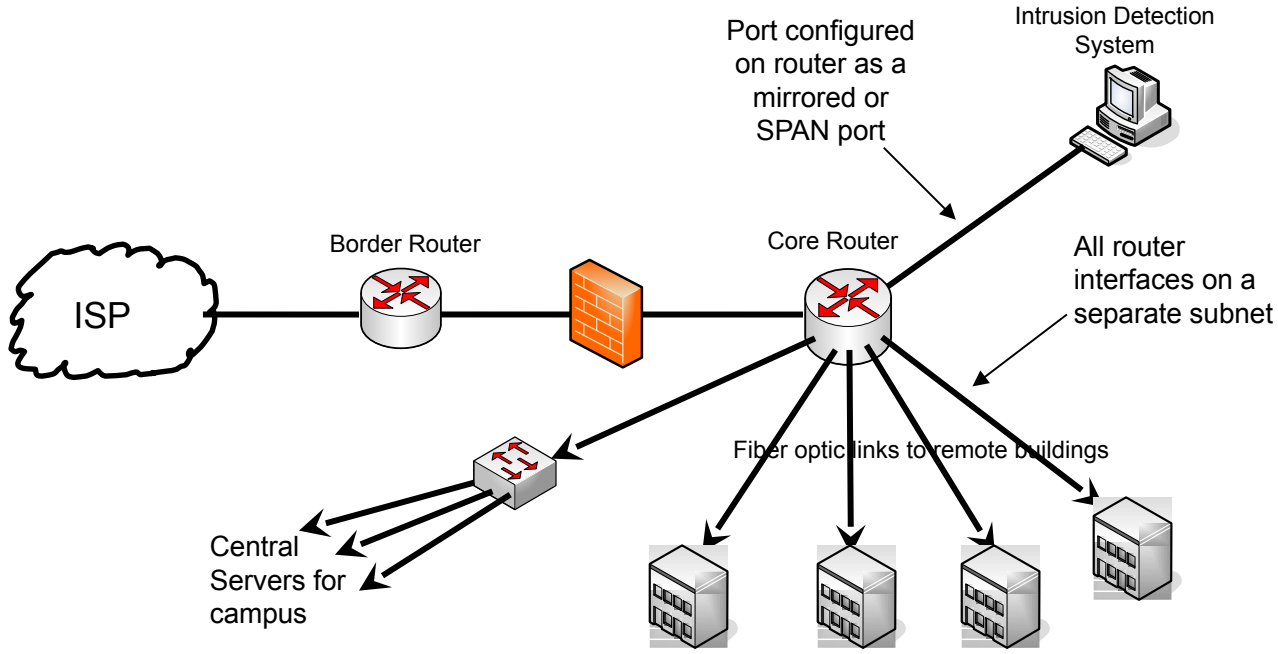
Where to put Firewalls

- 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



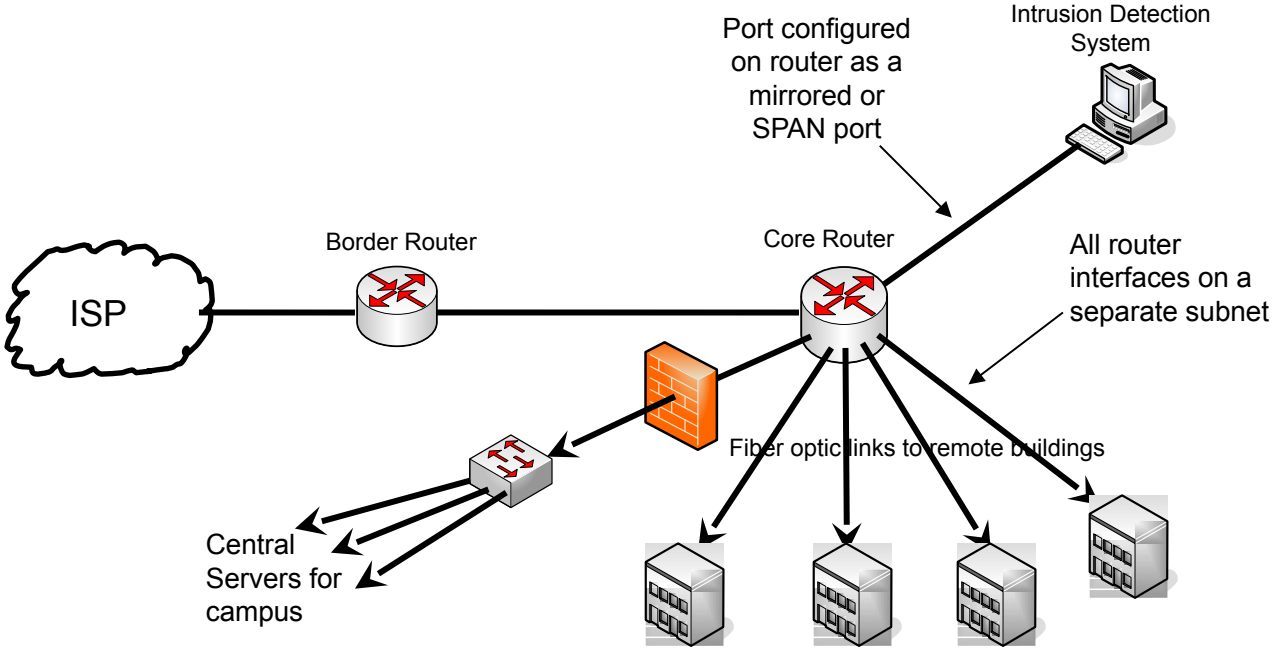
A Newer Approach to Firewalls

- 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

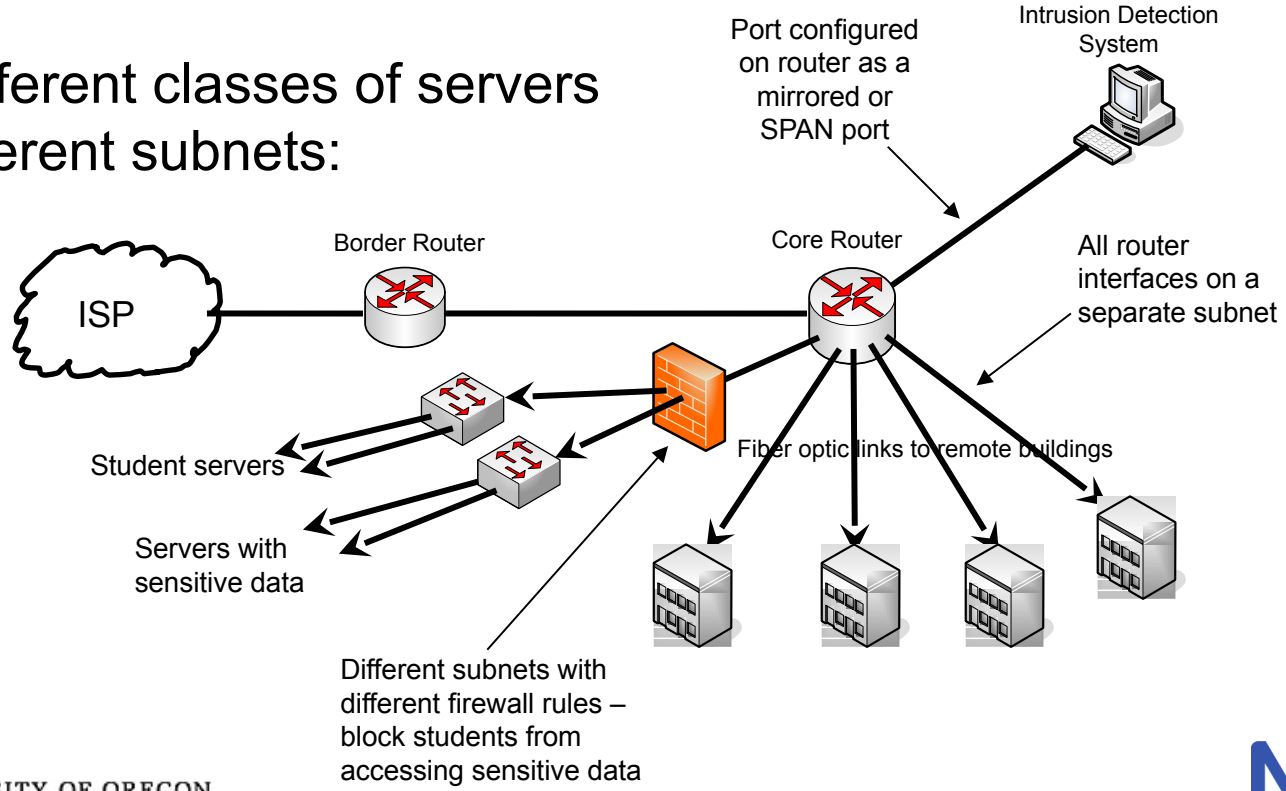
- We recommend that you firewall just the servers with sensitive data
- Always use two levels of defense: hardware firewall and host based firewall. If one fails, you are still protected
- Firewall should protect
  - Limit inbound access to servers to only those ports needed for access to the application (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 – subscribe to the SANS newsletter
  - https://github.com/team-cymru/network-security-templates – a great set of templates for secure configuration of routers and some services
  - www.manrs.org – Mutually Agreed Norms for Routing Security: filtering, routing security, route validation, global coordination
  - www.cert.org – a good resource for lists of vulnerabilities
  - www.shadowserver.org – reports on all the accessible nodes in the public address space of your network

Questions/Discussion?