Campus Network Design Workshop

Campus Network Security

This document is a result of work by the Network Startup Resource Center (NSRC at http://www.nsrc.org). This document may be freely copied, modified, and otherwise re-used on the condition that any re-use acknowledge the NSRC as the original source.

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Part One: Firewalls

(What people think about first when talking about security)

How useful are firewalls?

- A long time ago, client machines used to get infected through direct network attacks
- Windows (since XP SP2) has built-in firewall
- This is no longer an issue
- However, people still design networks as if it were still a problem

Actual methods of infection

- Opening malicious E-mail attachments
- Clicking malicious links
- Gmail and the like 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 will not stop it

Countermeasures

- Keep all your systems up-to-date with patches
- Get rid of obsolete operating systems (esp. WinXP)
- Use the security features built into the hosts
  - Such as the built-in Windows firewall (Do not turn it off)
- Deploy anti-virus and keep it up-to-date
- Use strong authentication and crypto where 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 ☹

Aside: NAT != Firewall

- And NAT != Security
  - Did you know that a cone NAT (one-to-one NAT) allows anyone on the Internet to connect inbound to a port that you are using outbound?
- NAT and firewalling are two different concepts and can be separated
- NAT overload (port address translation/PAT) makes it harder to identify miscreants on your network

Outbound port blocking

- Port block seriously inconveniences users and visitors
  - Many sites block lots of TCP ports.
  - Even simple things like email may need ports 465, 587, 993, 995 to send and receive mail
  - Remember, you want as open of a network as possible
- Blocking mostly doesn't help your security or policy
  - e.g. Bittorrent can tunnel through port 80

Exceptions to Blocking

- There are some ports that are recommended to be blocked. These include:
  - 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
  - 161 and 162 UDP – SNMP
  - 1025 TCP – Microsoft RPC exploit
  - 1433 TCP – Microsoft SQL worm
  - 1434 UDP – Microsoft SQL worm
  - 2049 UDP – Sun NFS

SMTP notes

- Blocking port 25 outbound recommended
- Forces users to relay mail via your local SMTP server
  - Or submit via ports 465 or 587 authenticated
  - Local SMTP server can log and apply rate limits (e.g. exim can do this)
- Easier to detect and control virus-infected machines which are sending spam and affecting your network's reputation
- You will need to allow port 25 for your campus email servers

Reasonable Firewall Use

- Can firewall just the servers with sensitive data
- Use two levels of defense: hardware firewall and host based firewall. If one fails, you are still protected
  - Limit inbound access to administrative ports
  - 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

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) 1M each? It only takes 50 abusers to burn 50M 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 opaque
- There are legitimate uses for Bittorrent
- 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) useful for detecting malicious activity

Performance

- Any device you put in-line with all your traffic can become a bottleneck
- You may only have 10M today, but soon it will be 100M, then 1G, then 10G
- Traffic filtering / inspection / shaping at higher rates is ruinously expensive
- Search 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? ☹

Part Two: People

Let’s re-state 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

Setting the rules

- You need to define what activities are allowed, and what are explicitly disallowed
- You need to inform people that their activity is being monitored and logged
- You need to define the consequences if they breach the rules
- This is an **Acceptable Use Policy** which all your users must agree to

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)

Part Three: Monitoring

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

- IDS (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, Observium
- 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

Joining the dots

- 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

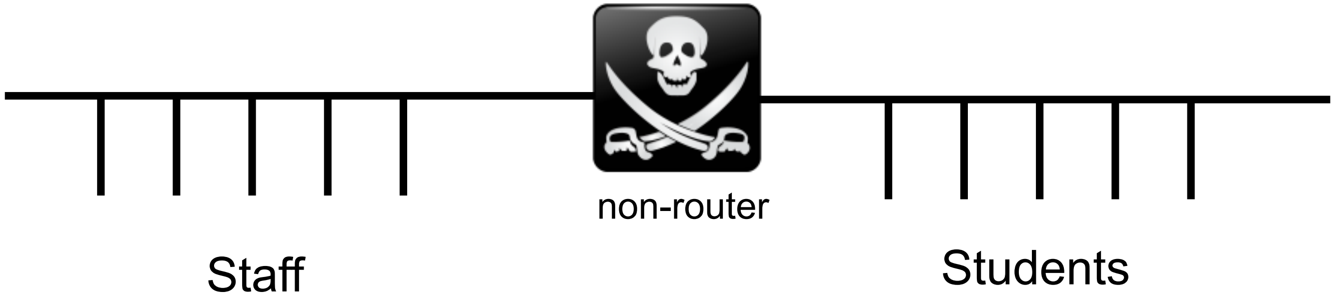
Part Four: Pitfalls

Security and Network Architecture

- A campus network is very different to an “enterprise” network, so an “enterprise” template may not be appropriate
- Every situation is different and you need to build what's right for you
- However here are some questionable practices we often come across

Using a Network to Identify People

- With a non-router in between



Problems with this approach

- It's inconvenient
  - Staff may be doing lesson in computer lab and find themselves unable to access resources they need
  - Only students use labs so we won’t let anyone from the lab to access the faculty file server
- It adds support overhead
  - Continual requests to move a physical port from one network to the other, or open up firewall holes
  - Some students have legitimate use for “staff” resources, e.g. postgrads

It doesn’t scale

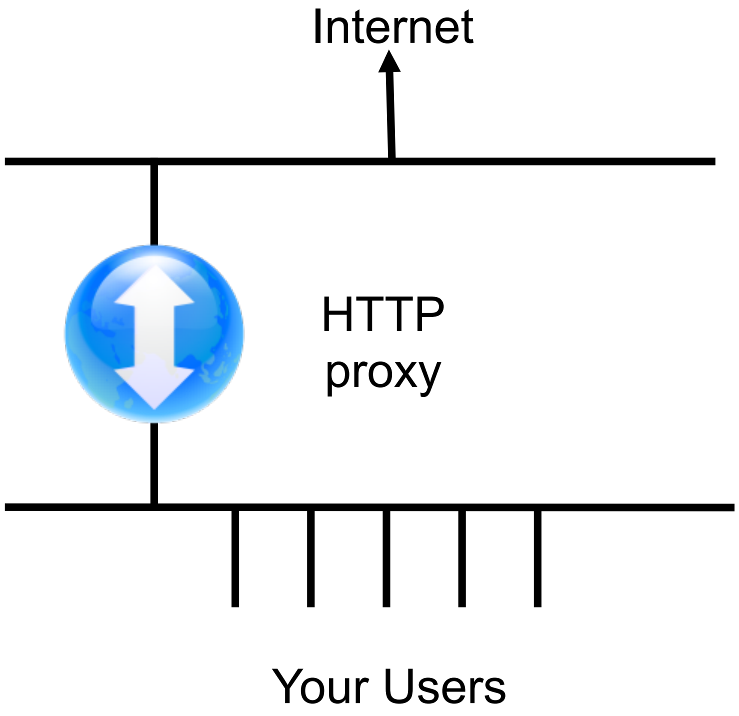
- Campus networks are about scale: thousands of users, maybe hundreds of buildings
- Need to route at the core to scale
- Just because you are in a specific location or on a specific network, does that really mean anything?
- You really need to have access to resources controlled by credentials (usernames and passwords)

What problem is it trying to solve?

- You don't trust your users?
  - Monitor them, and discipline where required
- Network is too big to function properly?
  - Divide your network by each building, not by staff, student or department
  - What do you do when a department moves and is in two buildings?
- Must use application access controls
  - Make sure your store of credentials for users know about who the users are (student, faculty, department, manager, etc.) so the application can use that information

2. Forcing all access via proxy

- Attempt to save bandwidth (proxy cache) and block undesirable traffic (e.g. torrents)



Well-intentioned, but…

- The Internet is much more than the Web
  - Severe inconvenience caused by not being able to reach other services
- Much content these days is dynamic and hence non-cacheable
  - Many websites use cache-busting techniques to track visitors and increase page impressions
- Since the Snowden revelations, more and more of the web traffic is encrypted so it can’t be cached

Alternative Approach

- Route IP properly
- Have a proxy cache, but keep it to one side
- Use proxy auto-configuration so most users use it automatically
  - WPAD, PAC
  - Just some entries in DNS and a web page
- Allows people to opt-out if they need to
- As more web traffic is encrypted, this becomes less and less useful

4. Firewalls with content filtering

- One vendor has a feature where if URL contains a keyword from a blocklist, e.g. “breast”, it blocks the request
- Google results pages are HTTPS, so subsequent searches are encrypted anyway!
- What about people researching breast cancer?
- Inconvenience without benefit. Turn it off.

Finally, do you agree or disagree?

- “The network exists to support the education and research activities of the university”
- “The network's job is to deliver traffic, not enforce security policy”
- “An open policy promotes more effective and innovative uses of the network”

- Think about these when building your network

Questions / Discussion ?

This document is a result of work by the Network Startup Resource Center (NSRC at http://www.nsrc.org). This document may be freely copied, modified, and otherwise re-used on the condition that any re-use acknowledge the NSRC as the original source.

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center