Campus Network Security

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

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!
  - (evil, expensive devices do man-in-the-middle attacks against your users. Do you want to be part of the Internet privacy invasion?)

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

Countermeasures

- End-point security (e.g. up-to-date antivirus)
- Network-based detection and containment
  - allow 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 allows *anyone* on the Internet to connect inbound to a port that you are using outbound? (Used by peer-to-peer apps)
- NAT and firewalling are two different concepts and can be separated
- NAT (PAT) makes it harder to identify miscreants on your network

Outbound port blocking

- Seriously inconveniences users and visitors
  - may need ports 587, 993, 995 to send and receive mail; ssh on non-standard ports; etc
- And doesn't help security or policy
  - e.g. Bittorrent can tunnel through port 80

Exception: block SMTP

- Blocking port 25 outbound recommended
- Forces users to relay mail via your local SMTP server (or submit via port 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

Other reasonable firewall uses

- Can put servers behind a firewall
  - 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 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 very expensive
- 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 restate 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 explusion"

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
- 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

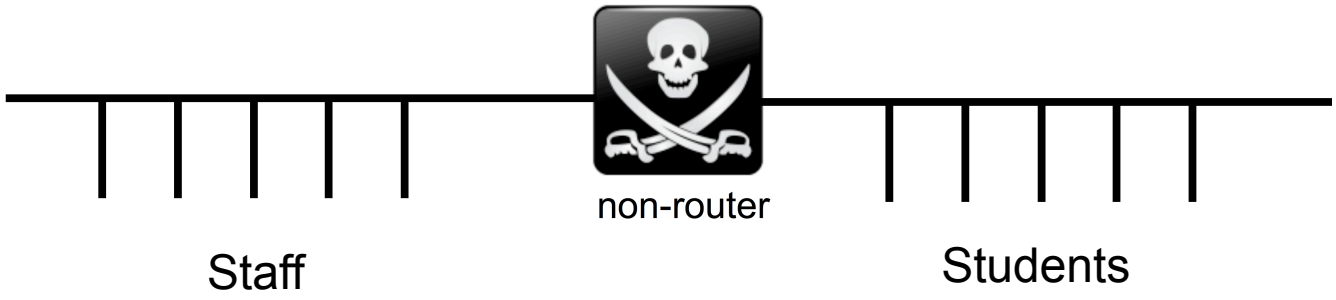
Part Four: Pitfalls

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

1. "Staff" and "Student" networks

- With a non-router in between

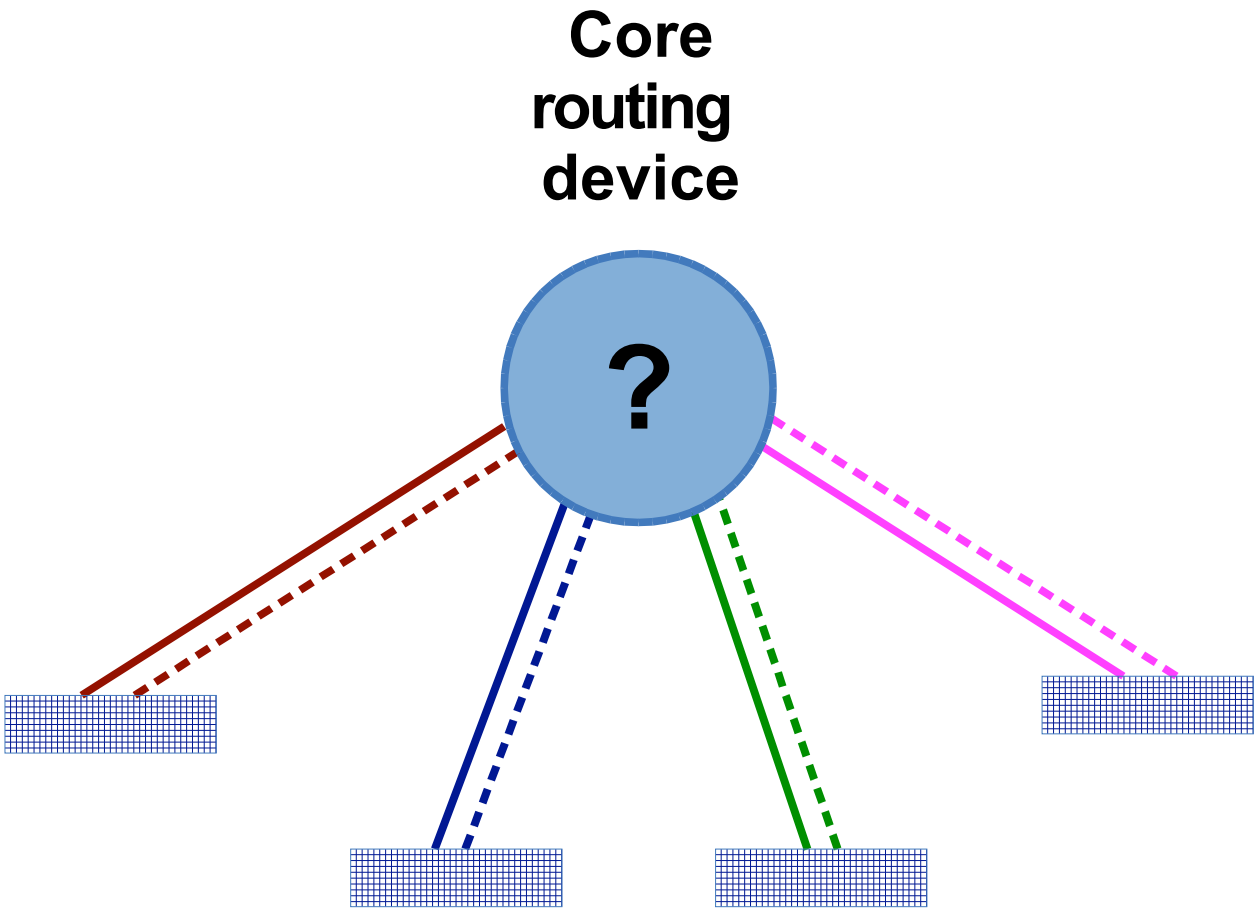


Problems with this approach

- It's inconvenient
  - Staff may be doing lesson in computer lab and find herself unable to access resources she needs
- 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
- Can't trunk the same "staff" and "student" VLANs everywhere
- Implies separate staff and student subnets for every building
- How are you going to isolate them? ACLs? VRFs? Adds much complexity


Core
routing
device
?
Staff network
Student network

Physical location is a poor indicator of identity and authorization

- Much better to get the identity directly, e.g. through a network login
- Rights can be assigned to users or groups of users

What problem is it trying to solve?

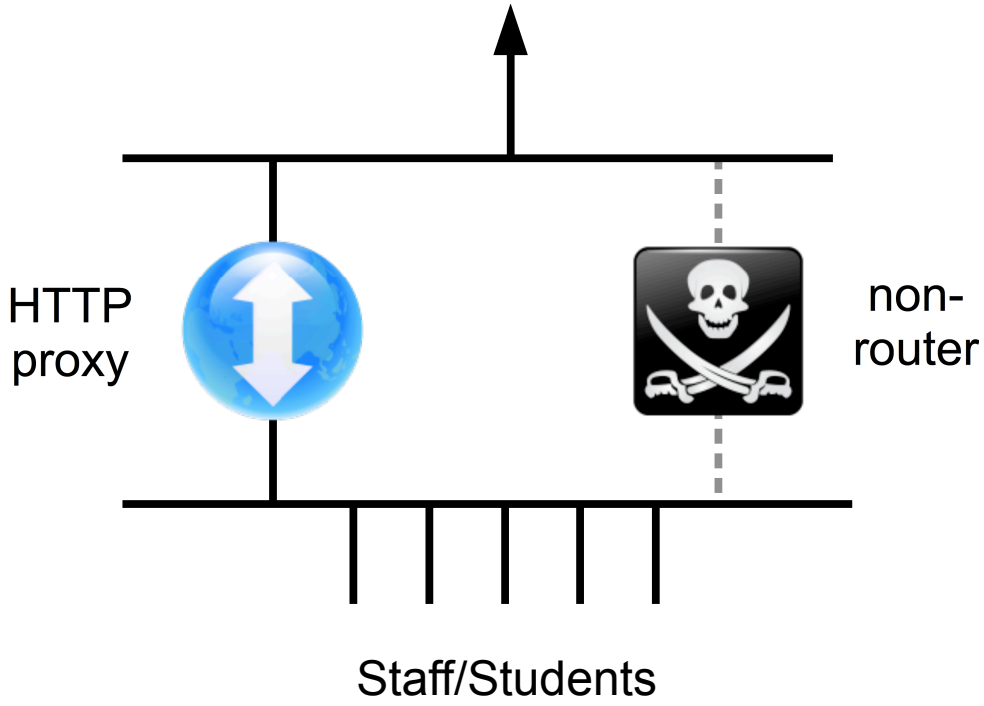
- You don't trust your students?
  - Monitor them, and discipline where required
- Network is too big to function properly?
  - Divide by building, not by staff/student
- Servers don't have access controls?
  - Add application access controls
  - Have an authentication/authorization database which has groups for "staff" and "students"

Where is the real threat anyway

- The students inside your institution, who you can monitor and control? Or the rest of the world?

2. Forcing all access via proxy

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



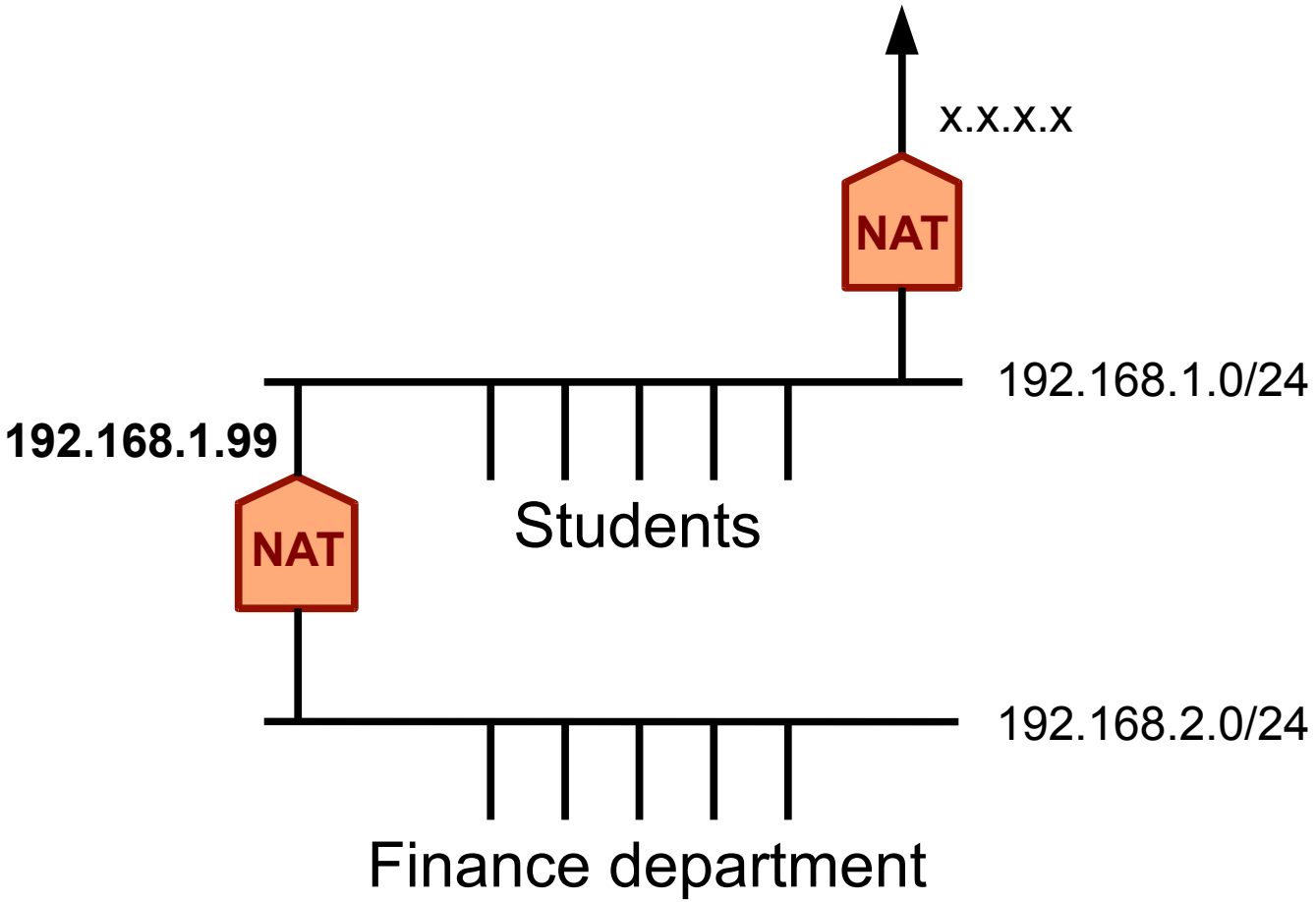
Well-intentioned, but...

- 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
- Proxies are hard to scale and can easily degrade service rather than improve it

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

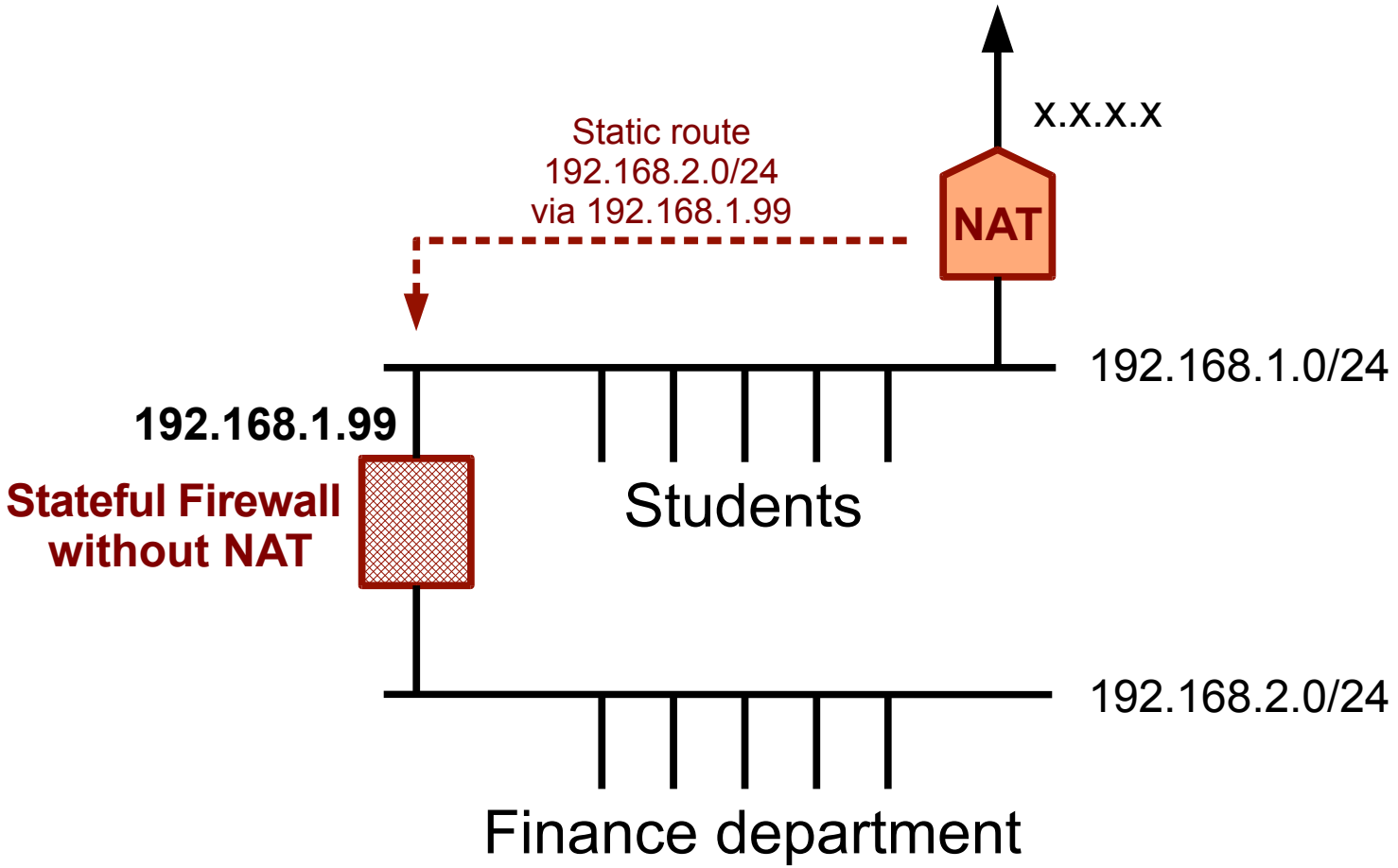
3. Multi-level NAT



Issues

- Border IDS/Netflow can't tell which person in Finance is infected/streaming YouTube
- How do you manage devices inside Finance network?
  - Port-forwarding is a pain
- Sometimes done just to avoid IP routing :-)

A better approach



4. Firewalls with content filtering

- One vendor has a feature where if URL contains a keyword from a blocklist, e.g. "tunnel", it blocks the request
- Google results pages are HTTPS, so subsequent searches are encrypted anyway!
- What about people researching tunnel construction/engineering?
- 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"
- "My job as network administrator is to enable access to the network, not to block it"
- "An open policy promotes more effective and innovative uses of the network"
- Think about these when building your network