

Network Firewalls

John Kristoff

jtk@depaul.edu

+1 312 362-5878

DePaul University

Chicago, IL 60604

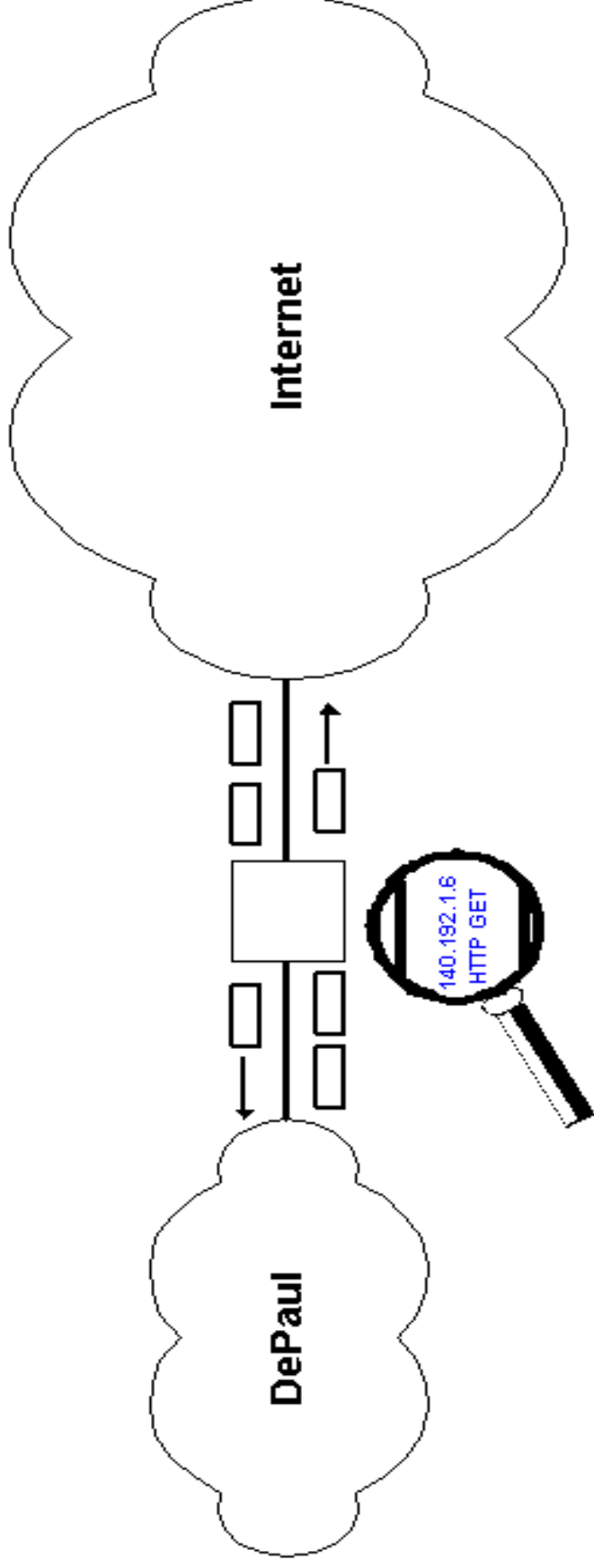
The network is just a highway

- How do you secure the highway
- Police patrol
- Toll booths
- Licensed drivers
- Vehicle inspections and standards
- Rules of the road
- Are the highways completely safe now?

What network firewalls do

- Define untrusted and trusted boundaries
- Inspect traffic traversing firewall boundary
- Limit communication traversing boundary
- Help shield insecure hosts

Network firewalls illustrated



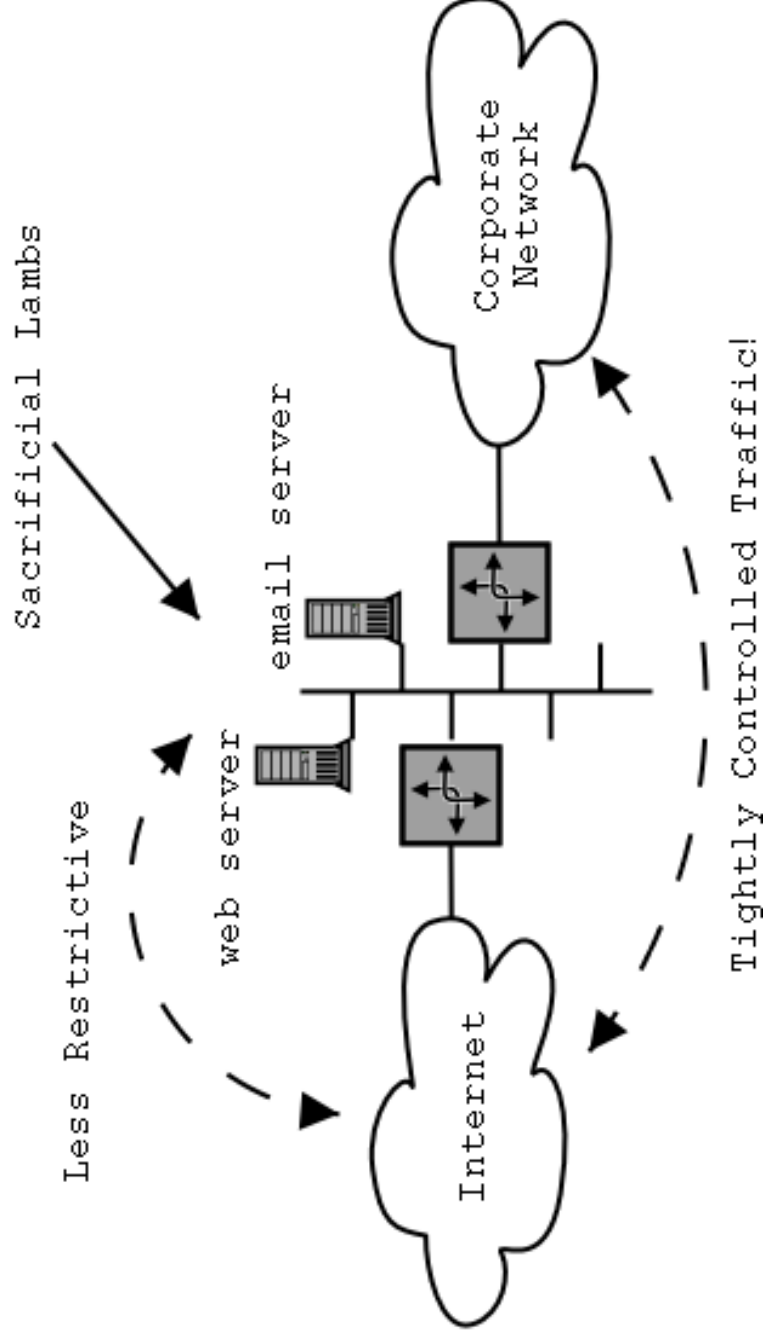
Key ideas

- Firewalls should be unnecessary
- They're a *network* solution to a *host* problem
- They don't solve the real problem and...
- ..make it hard/impossible to do certain things
- Ultimate control of hosts is out of our hands
- Securing a LOT of hosts is hard!
- But.. network solutions are *sigh* necessary

Packet filtering firewalls

- Filter everything – not very useful
- Filter by IP address
- Filter by application type (TCP, UDP)
- Filter on field/flag settings (source route)
- Filter invalid packets (SYN/FIN packets)
- Other pattern match

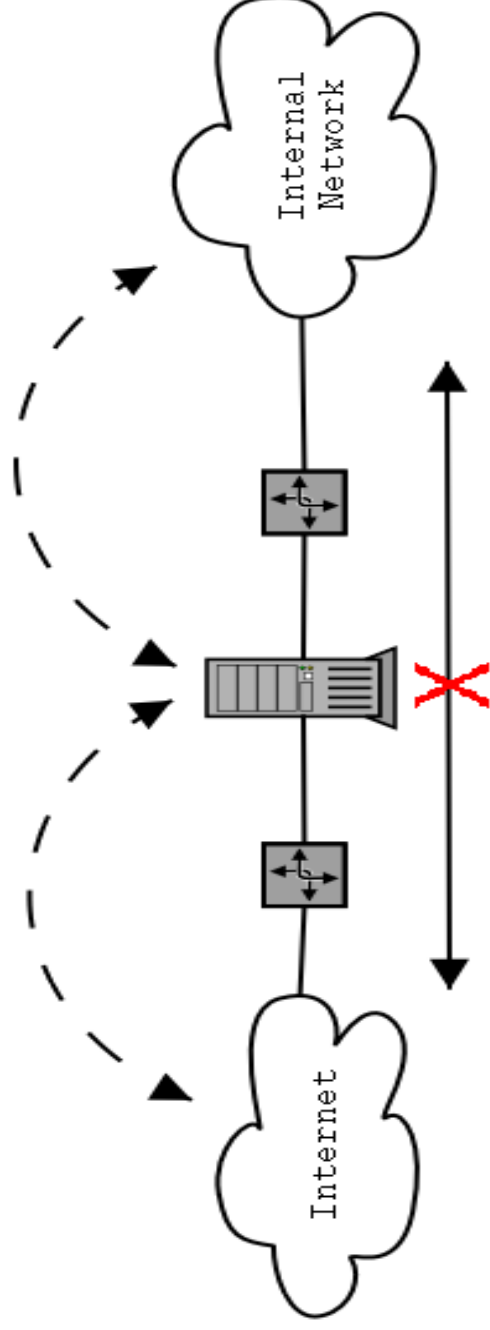
Screened subnet implementation



Application Layer Gateway (ALG)

- Also commonly called a proxy firewall
- These permit no direct communication
- Firewall intercepts all traffic in each direction
- Very intelligent device...
- ...must understand what a user is doing
- Difficult to install if it doesn't currently exist

Proxy/ALG illustrated



Other common firewall features

- Stateful inspection
- Network address translation (NAT)
- Authentication (VPNs)
- Dynamic triggers
- Reporting, logging and IDS support

What can't a network firewall stop?

- Bad packets that look good
- Denial of service (DoS) attacks
 - Well, they can stop them at the firewall
 - But then the firewall has just been DoS'd
- Stupid user tricks
- Things that go around the firewall
- Things that don't cross the firewall boundary

So you're saying...?

- It would be nice if all hosts could be secured
- Network solutions can help
- Malicious insiders can get by anything you got
- A holistic approach is needed. Including:
 - Audits, detection and response
 - Education
 - Standards and best practices

What does DePaul do?

- We stop some obvious stuff in various places
- We're beginning to do more at the edges
- Note: the network will be very fast soon...
- ...big firewalls get in the way big time
- Regardless of what you may have heard...
- We're better off than we were 2 years ago
- Of course so are the attackers

Final thoughts

- Overly secure systems are not at all useful
- Big border firewalls are obsolescent
- *Distributed firewalls* are getting a lot of talk
- Firewall vendors of course like this approach
- You should demand open AND secure access
- We can do it, but it ain't gonna easy
- If we fail, the Internet will become very boring

References

<http://networks.depaul.edu/security/>

<http://condor.depaul.edu/~jkristof/>

<news://news.depaul.edu/dpu.security>

<http://www.cert.org>

<http://www.sans.org>

<http://www.cerias.purdue.edu>

<http://www.neohapsis.com>

<http://www.lists.gnac.net/firewalls/>

<http://www.interhack.net/pubs/fwfaq/>