

Network Security

ITL

Network Security - What

- Integrity
 - Data won't get changed accidentally
- Confidentiality
 - Only the intended recipient sees the data
- Availability
 - Users have access to network resources as planned
- Authorization
 - We know who is allowed to do what on the network

Network Security - How

- Integrity
 - User Authentication, Cryptographic Signatures
- Confidentiality
 - User Authentication, Access Control, Encryption
- Availability
 - Access Control, Monitoring, Redundancy, Business Resumption Plan
- Authorization
 - User Authentication, Access Control, Monitoring

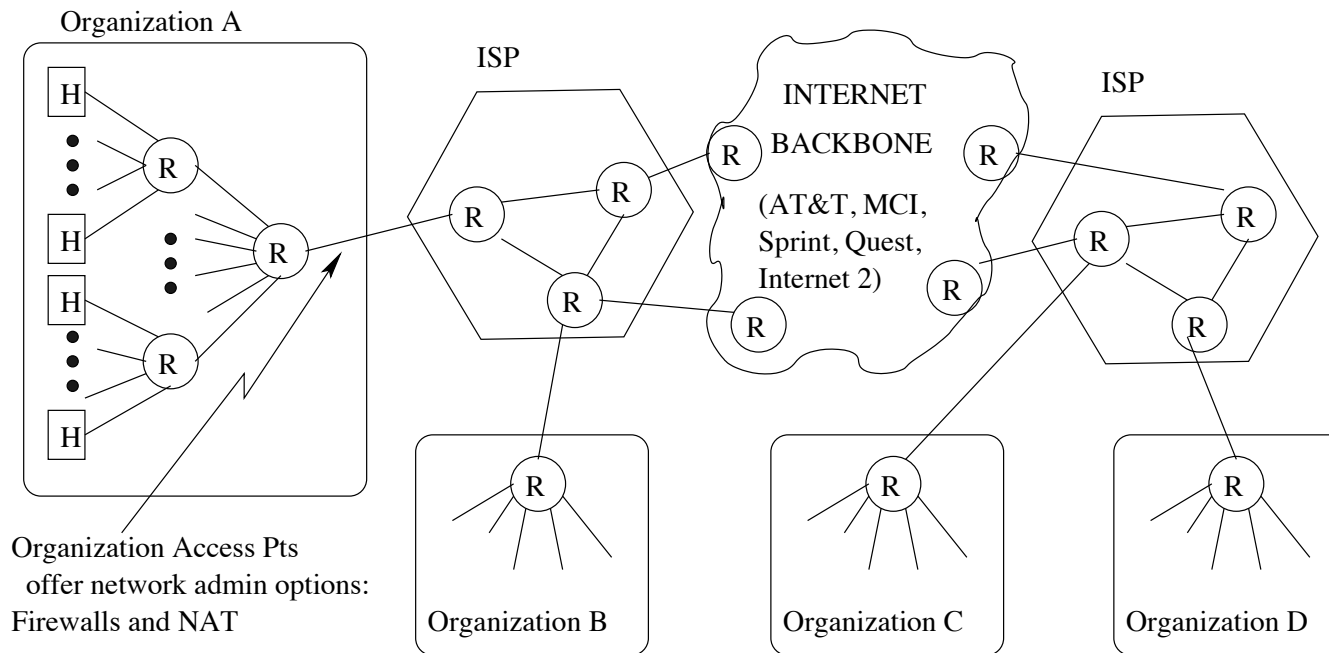
Network Security Tasks

- Access Control
 - Lab 4
- User Authentication
- Cryptographic Signatures, Encryption
- Monitoring
 - Lab 5
- Redundancy
- Business Resumption Planning

Access Control

- Based on inspection of packets
 - “Firewall”
 - “State-Less” Firewall - act on each packet in isolation
 - “State-Full” Firewall - keep track of what packets you have seen in the past
- Sometimes Connected to User Authentication
 - “Network Access Control”
 - “Agent” program running on the user’s workstation
 - User interacts with an authentication system, e.g.
 - Web site (OU wireless network)

Security Implementation Points



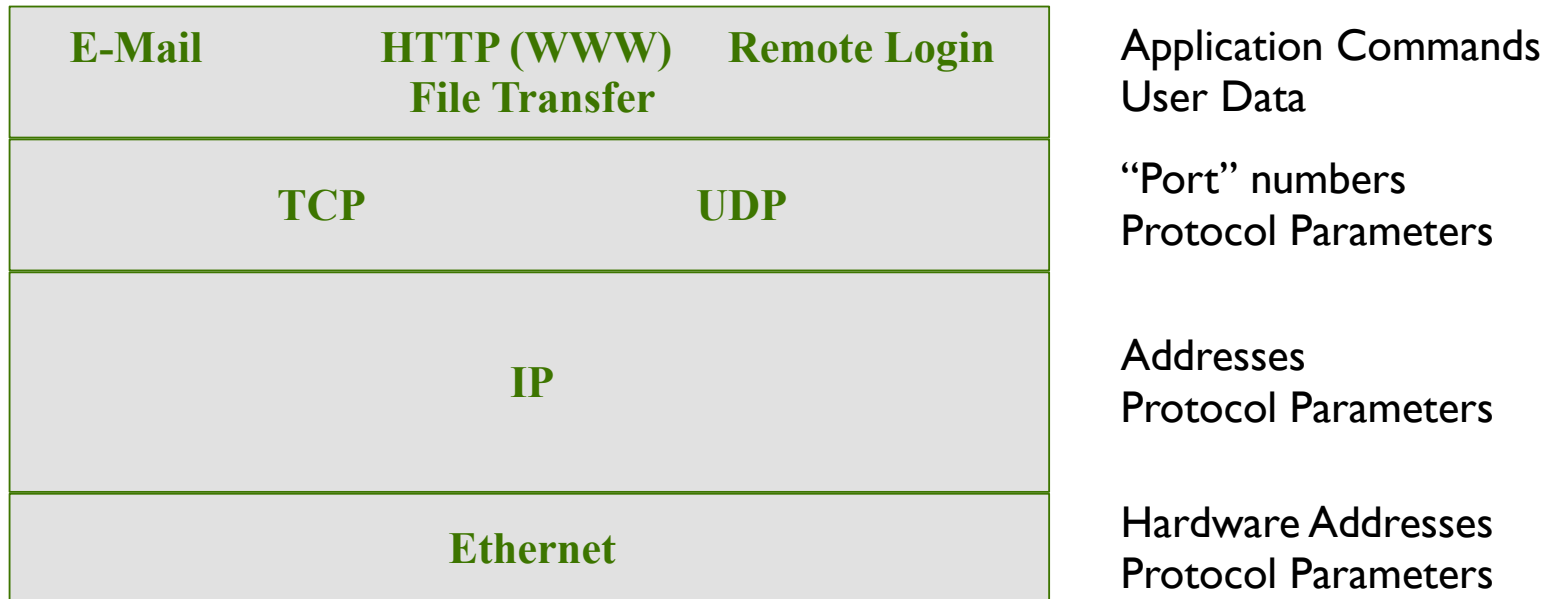
Packet Content

- In the lab we only work with Firewalls (without user authentication)
- What can the Firewall “see”?
- Packets contain information needed by the protocols involved, and the user data

Note:

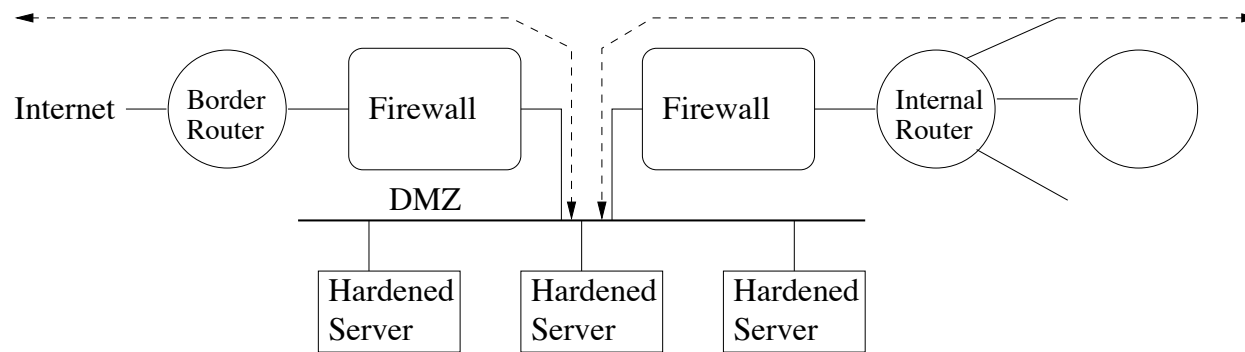
The term “Firewall” comes from the construction industry

Protocol Layers

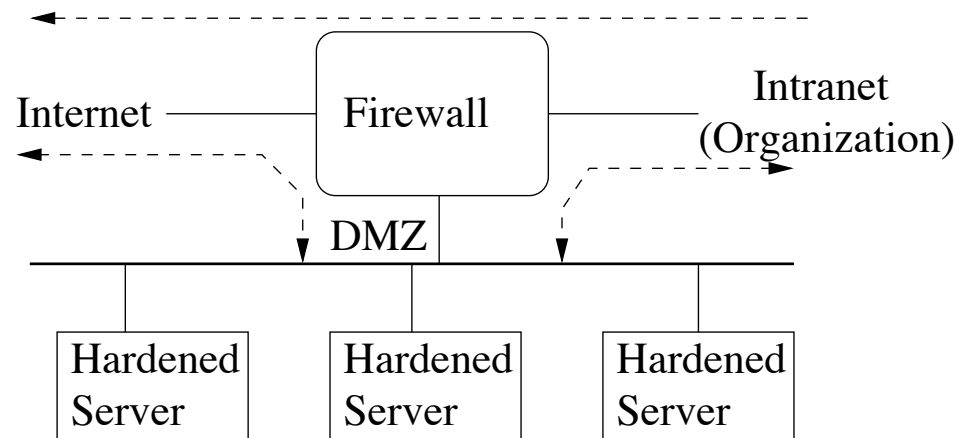


More in a moment, but first ...

Full Firewall



A simpler Version



The Firewall

- Each network interface runs a packet capture
 - In-bound and out-bound packets are separated
 - A different set of rules applies to each set of packets (by interface and direction)
 - These rule sets are called Access Control Lists (ACLs)
 - A packet is compared to rules in the set in a specified order, until a match is found
 - If a packet matches a rule:
 - Take the action specified by the rule
 - Go to the next packet
 - A default rule applies if there is no match

Firewall Actions

- Permit
 - aka Accept, Pass
 - Route the packet as if the Firewall was not there
- Deny
 - aka Drop, Block
 - Delete the packet, do not route it any further on the network
 - May return an error message to the sender; many firewalls however drop packets “silently”.

Things to put in Rules

- IP Layer
 - Source Address
 - Destination Address
 - Protocol
 - TCP, UDP, ICMP, ARP, etc.
- TCP and UDP
 - Source Port
 - Destination Port

What are Port Numbers?

- Applies to both TCP and UDP
 - “Ports” identify a program on a host (all programs share the same IP address, but they all must use different ports)
 - Some ports are “well-known ports”
 - Port 80 is usually a web server
 - Packets from a web server: source port is 80
 - Packets to the web server: destination port is 80
 - Web clients use an arbitrary high-numbered port unique to the host it is on

TCP is a bit more complex

- TCP is a “Connection Oriented” protocol
 - A special packet is used to start the connection; we can check whether a TCP packet is such a special (so-called “SYN”) packet, or whether it is part of an established connection
 - Every TCP packet must be “answered” by a matching reply (*we’ll talk more about this next week*)
 - We only need to drop packets in one direction to block the connection
 - To be thorough, we often still drop packets in both directions...

Some examples

- Permit TCP from anywhere, any port to port 80 on 132.235.201.2/32
- Permit TCP from anywhere, any port to 132.235.201.0/25, any port, only as part of an established connection
- Permit ICMP echo from anywhere to 132.235.201.2/32
- Permit ICMP echo-reply from anywhere to 132.235.201.0/25
- Deny IP from anywhere to anywhere

Next lecture -- how to do this on a cisco router

