FIREWALL FUNDAMENTALS

Network Firewalls Primer

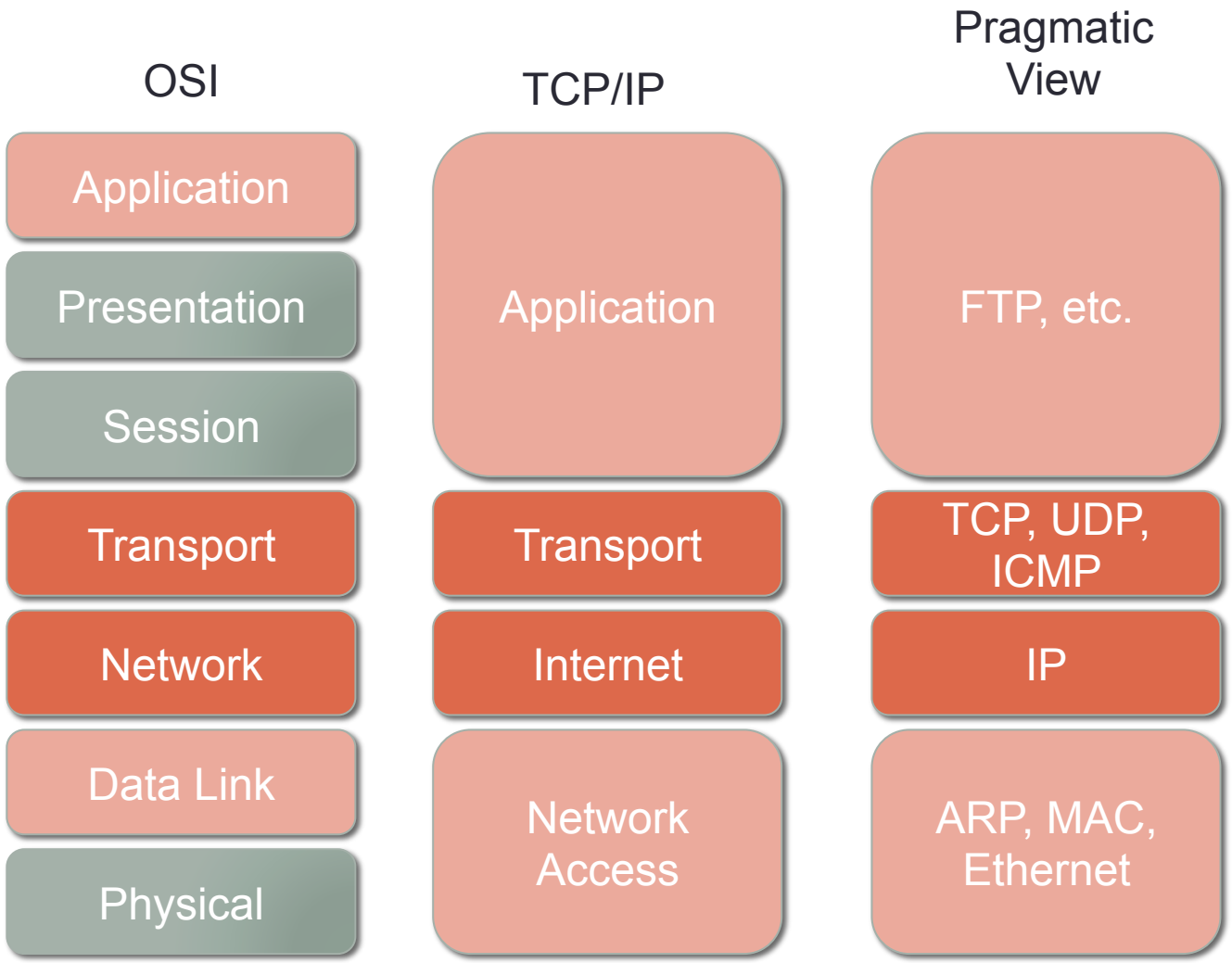
Rob Vinson
IT Security Architect
The University of Iowa
July 13th, 2011

Agenda

- TCP/IP
- Network Architecture 101
- Netmasks
- Packet filters (Stateless firewalls)
- Stateful Firewalls
- Resources

TCP/IP

Models


OSI
Application
Presentation
Session
Transport
Network
Data Link
Physical
TCP/IP
Application
Transport
Internet
Network Access
Pragmatic View
FTP, etc.
TCP, UDP, ICMP
IP
ARP, MAC, Ethernet

IPv4 Header

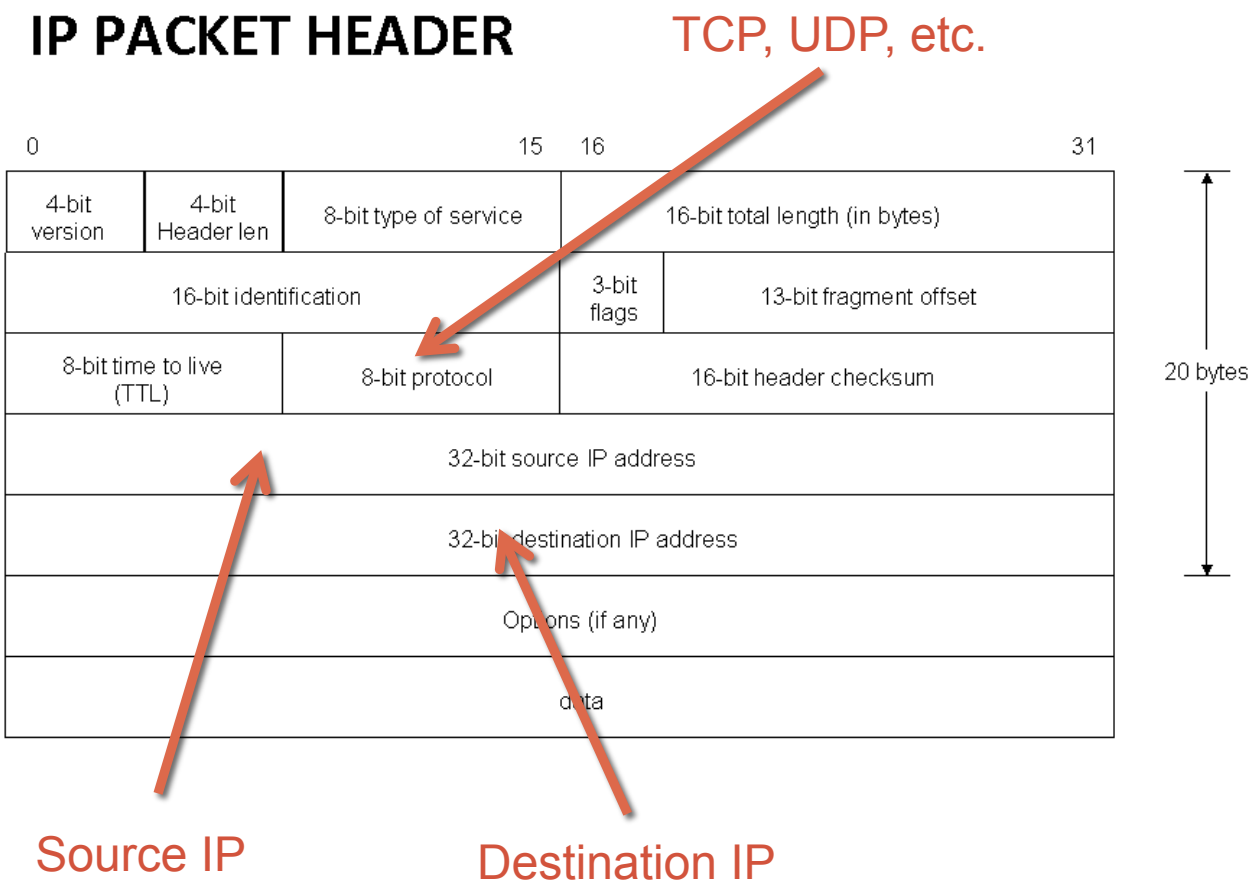
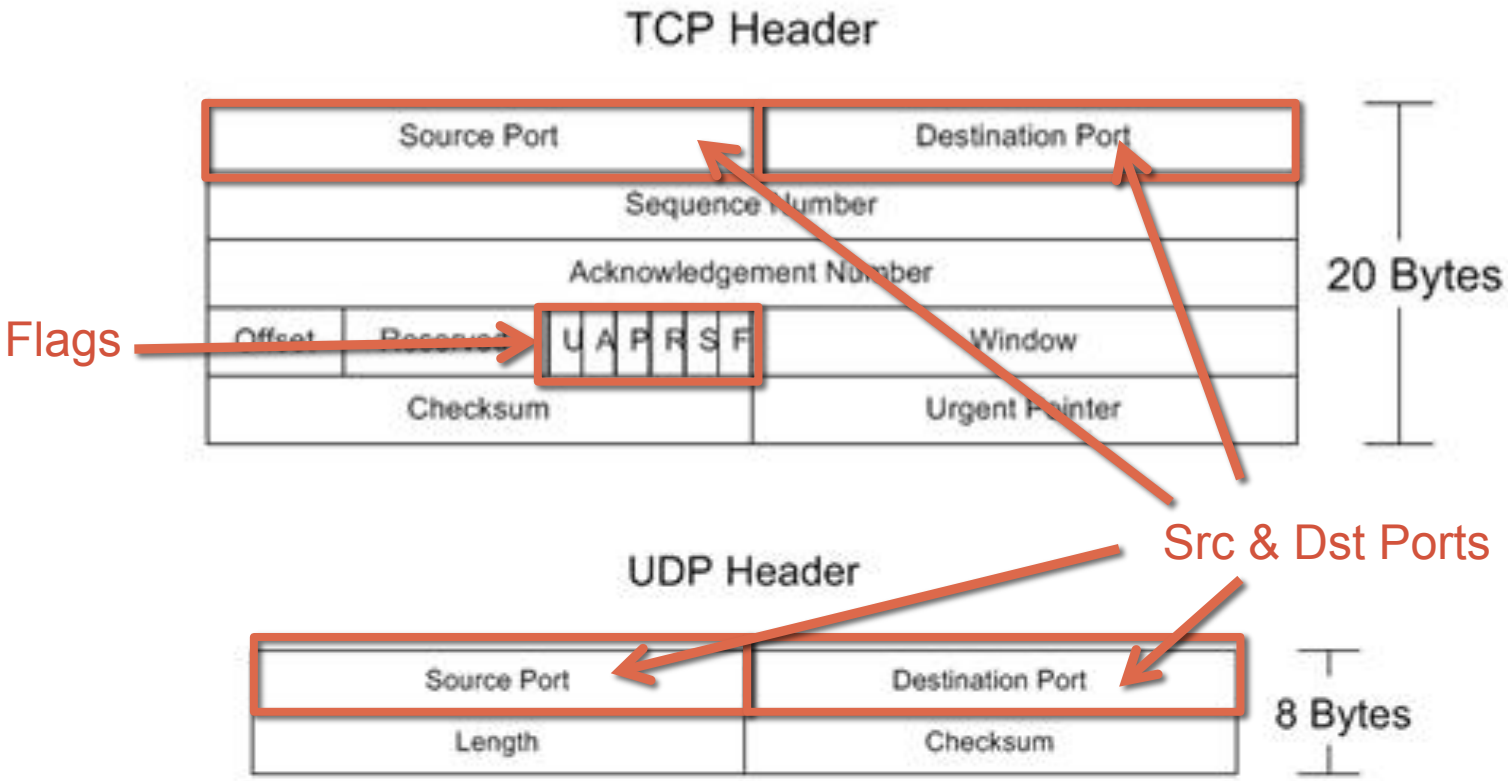


Image from: http://www.debugall.co.uk/2008/10/25/ip-packet-header/

TCP & UDP Headers



Images from: http://www.tamos.net/~rhay/overhead/ip-packet-overhead.htm

Pragmatic Notes: TCP/IP

To make network firewall rules you need to know:

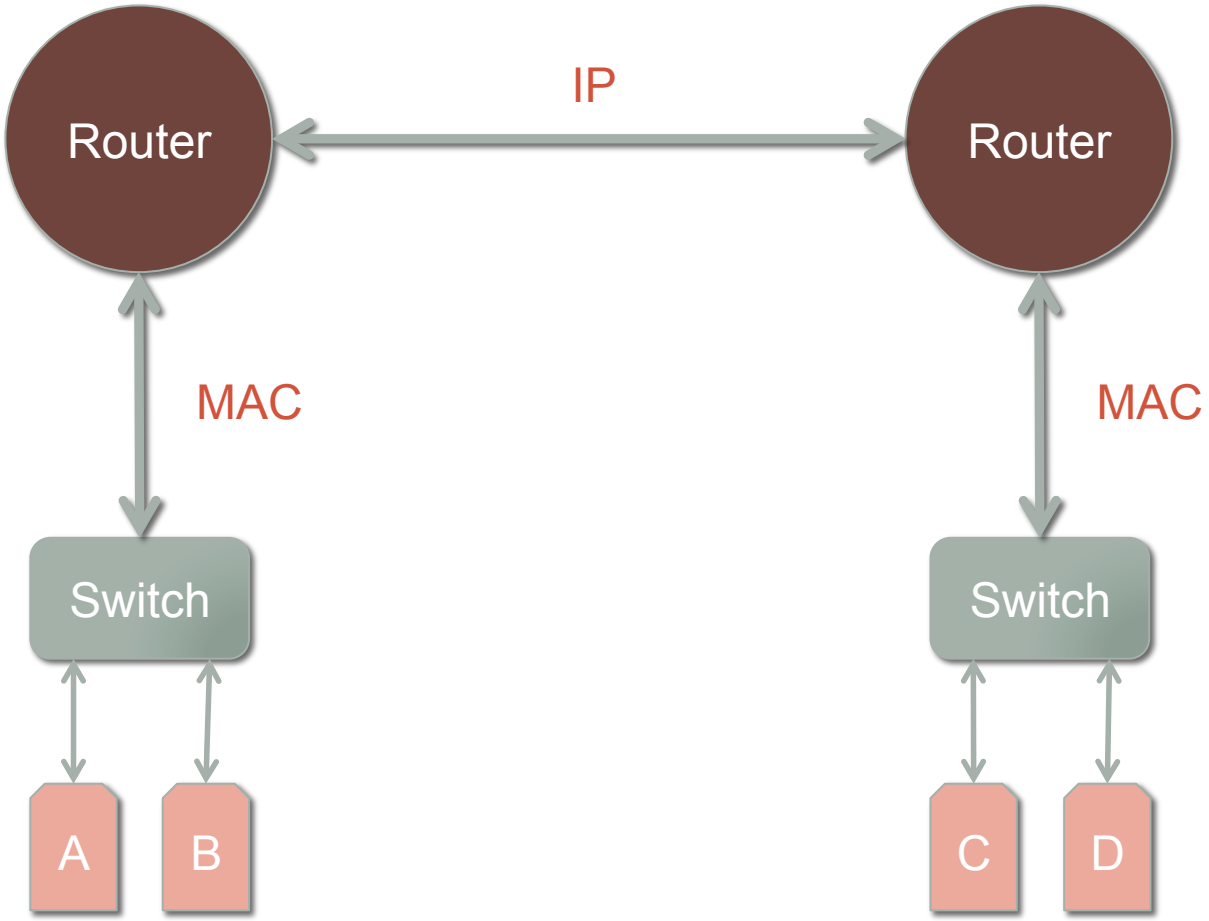
- IP addresses involved
- Ports involved
- Protocol used (TCP/UDP/ICMP)

Useful Information:

- IPv4 addresses are 32bits & IPv6 addresses are 128bits
- Ports are 16bits (which can represent 0-65535)
- Ports 0-1023 are privileged ports.
- Client applications dynamically use high-number ports

NETWORK ARCHITECTURE & SUBNETTING

Routing & Switching



CIDR Notation and Netmasks

- 10.10.20.0 – 10.10.21.255
- 10.10.20.0/23
- 10.10.20.0 255.255.254.0

In Binary:

Min: 00001010.00001010.00010100.00000000

Max: 00001010.00001010.00010101.11111111

Pragmatic Notes – Networking & Subnets

- Systems in the same subnet communicate through switches.
- Systems in different subnets communicate via routers.
- Netmasks are a way to denote how many bits are allowed to be used to address hosts on a network.
- A /24 (or netmask of 255.255.255.0) indicates a subnet size of 254 (256-2) hosts.
- The number of host addresses in a subnet doubles with every bit removed from a netmask, and gets cut in half with every bit added to a netmask.

STATEFUL FIREWALLS AND PACKET FILTERS

PACKET FILTERS

- Operate on IP Addresses and Ports
- Lack a concept of an established “session” or connection.
- This means for each direction of communication (system A -> system B, and system B -> system A) rules must exist for the traffic to pass.

Stateful Firewalls

- Rules exist for the communication which initiates the communication. The response traffic is automatically allowed through the firewall without need to define these rules.
- Works well for connection-oriented protocols like TCP.
- Timers are implemented for protocols without a sense of a “session”. When the timers expire the response traffic is no longer allowed.

Pragmatic Notes: Stateful Firewalls and Packet Filters

- Use stateful firewalls, your life will be much easier!
- Some protocols behave atypically by redirection connections to other ports/systems. Most firewalls you'll care about have workarounds/solutions implemented to making handling these easier.

CHALLENGES

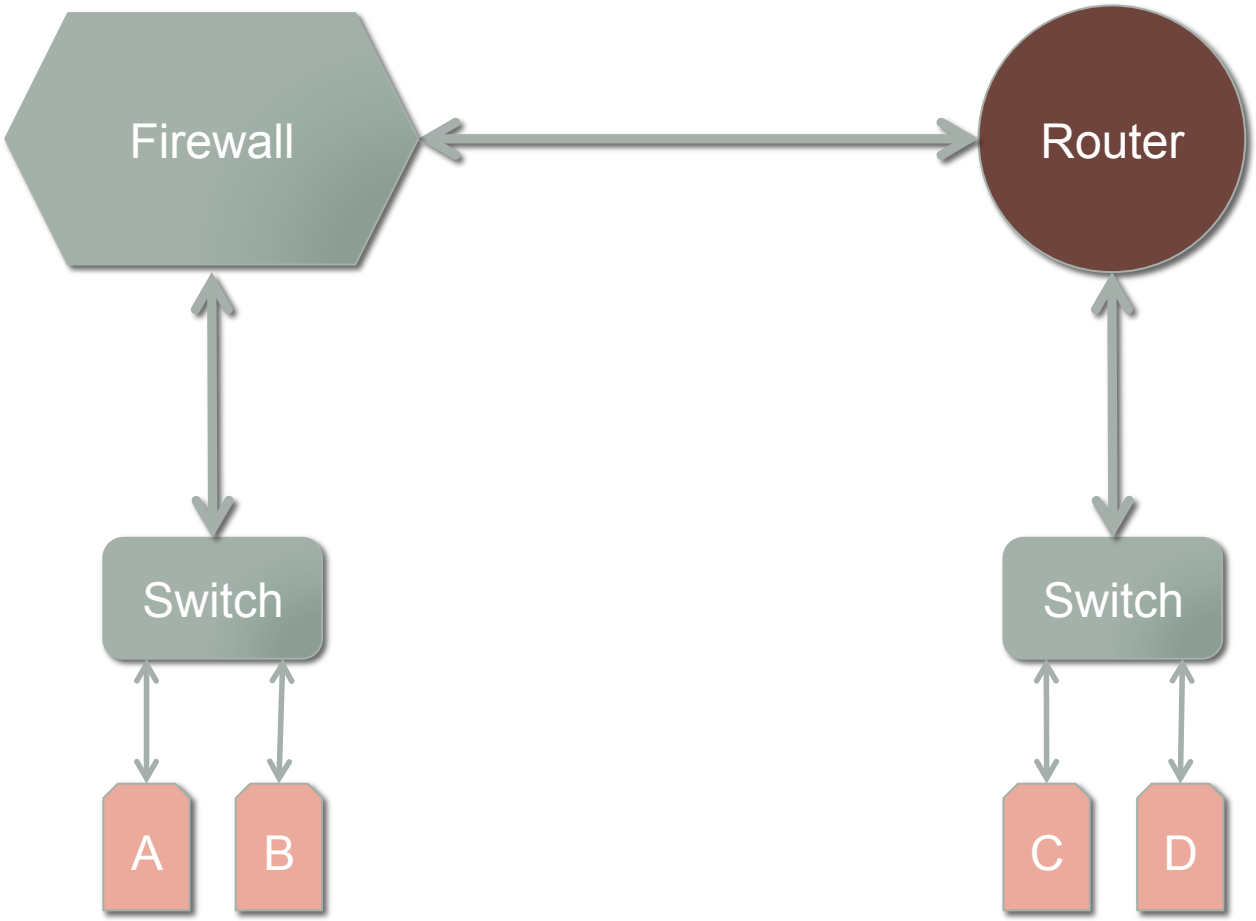
Pseudo Allow Rules – A Challenge

A) host 192.168.1.1 port 52312 host 10.10.10.1 port 80
B) host 192.168.1.1 host 10.10.10.1 port 80
C) host 10.10.10.1 port 80 host 192.168.1.1 port 52312
D) host 10.10.10.1 port 80 host 192.168.1.1

Q1) Which rule(s) would be needed to allow web browsing from 192.168.1.1 to the 10.10.10.1 webserver through a packet filter?

Q2) Which rule(s) would be needed to allow web browsing from 192.168.1.1 to the 10.10.10.1 webserver through a stateful firewall?

A Contrived Network – A Challenge



RESOURCES

Resources I Like

packetlife.net

The cheat-sheets are awesome, I have a few pinned up around my desk.

www.networksorcery.com

The protocols under the RFC Sourcebook section is a handy reference if you need the details of some protocol, like IP headers, TCP headers, etc.

Wireshark, tcpdump, etc

Not really a resource, but packet capture tools are incredibly useful.