Reading: Chapter 9.1-9.4, 8.5, 8.8, 8.9 (6.5, 6.8, 6.9 in 1st ed.)

Lab 5: Network Security Lab. Pre-lab available this week.

Network Layers

Layer	Purpose	Examples

Headers

			<html>Foo Bar Cool Site!</html>			

- TCP header:
- IP header:
- Ethernet header:

IP Addresses

Metaphor: like _____. Gives the router (_____) information needed to get the packet to its destination.

e.g. _____._____._____._____ (_____)

- _____ network: Own all the addresses starting with _____._____._____.*
- _____: (refer to these IPs) e.g. _____._____._____.____/_____

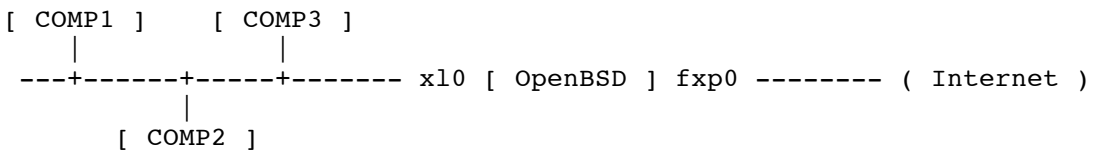
Ports

- Server ports: _____ (_____), _____ (_____), _____ (____)
- Client ports: _____ to _____

NAT: _____

- A limited number of _____. Many _____, few _____
- NAT: _____ network addresses translated at the gateway

Packet Filtering



The objectives are:

- Provide unrestricted Internet access to each internal computer.
- Use a "default deny" filter ruleset.
- Allow the following incoming traffic to the firewall from the Internet:
  - SSH (TCP port 22): this will be used for external maintenance of the firewall machine.
  - Auth/Ident (TCP port 113): used by some services such as SMTP and IRC.
- Redirect TCP port 80 connection attempts (which are attempts to access a web server) to computer COMP3. Also, permit TCP port 80 traffic destined for COMP3 through the firewall.
- By default, reply with a TCP RST or ICMP Unreachable for blocked packets.
- Make the ruleset as simple and easy to maintain as possible.

Note: rules operated _____ (Book example is the opposite!)

Macros

```
int_if="xl0"
tcp_services="{ 22, 113 }"
icmp_types="echoreq"
comp3="192.168.0.3"
```

Block Policy: _____

```
set block-policy return
```

NAT

```
match out on egress inet from !(egress:network) to any nat-to (egress:0)
```

Default Deny: _____

```
block in log
```

100% Allow: _____

```
pass out quick
```

Protect against _____

```
antispoof quick for { lo $int_if }
```

Anti-IP-spoofing alternative (int_if only):

```
block in on ! $int_if from 192.168.0.0/24 to any
block in inet from 192.168.0.1 to any
```

Allow traffic to the router

```
pass in on egress inet proto tcp from any to (egress) port $tcp_services
```

Redirect web traffic to the web server

```
pass in on egress inet proto tcp to (egress) port 80 rdr-to $comp3
```

Only Internal:

```
pass in on $int_if
```