Firewalls

Jonathan Windle

University of East Anglia

J.Windle@uea.ac.uk

June 6, 2017

Overview I

1. Intro

2. Basic Packet Filtering

Intro

- Essentially if a fire breaks out in one part of the building, it is contained, same concept applies to computing.
- Firewalls installed on routers.
- As traffic passes through, the firewall is configured to try and attempt to block malicious content.
- One way to do this is by packet filetering:
- A packet filer matches all packets that pass through the router against rules.
- The rules are based on security policies for the network.
- If a packet matches a rule, it is either accepted or rejected and the action logged.
- Default is to reject.
- Two types:
    - Basic packet filtering
    - Stateful packet filtering.

Basic Packet Filtering

- Examines each packet in isolation.
- Does not consider if the packet is a part of a stream or has a relationship with another packet.
- Stateless operation.
- Rules often based on a combination of source and destination addresses and protocols.
- For TCP and UDP, port may also be considered.
- A firewall could be set to block all traffic to a given port.
- Different rules may be specified for traffic travelling in each directon:
  - Allow host on private network direct access.
  - Limit access of hosts on the internet to the private network.
- Does not need to dig far into the packet:
- Most work is done at the first three layers of the OSI protocol.

The End