TCP/IP
Gateways and Firewalls

Prof. Jean-Yves Le Boudec
Prof. Andrzej Duda
ICA, EPFL

CH-1015 Ecublens
http://lcawww.epfl.ch

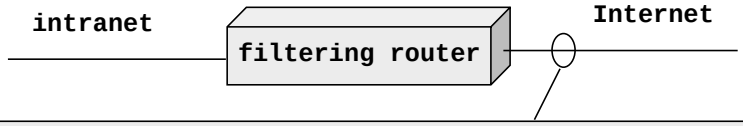
Firewalls

- TCP/IP architecture separates hosts and routers
  - network = packet transportation only
  - private networks may want more protection
    - "access control"
  - one component is a firewall
- definition: a firewall is a system that
  - separates Internet from intranet: all traffic must go through firewall
  - only authorized traffic may go through
  - firewall itself cannot be penetrated
- Components of a firewall
  - filtering router
  - application or transport gateway

3

Filtering Routers

- A router sees all packets and may do more than packet forwarding as defined by IP
  - filtering rules based on :
    - port numbers, protocol type, control bits in TCP header (SYN packets)
- Example



	prot	srce addr	dest addr	srce port	dest port	action
1	tcp	*	198.87.9.2	>1023	23	permit
2	tcp	*	198.87.9.3	>1023	25	permit
3	tcp	129.132.100.7	198.87.9.2	>1023	119	permit
4	*	*	*	*	*	deny

The example show 4 rules applied to the ports shown

- rule 1 allows telnet connections from the outside to the machine 198.87.9.2
- rule 2 allows email to be sent to machine 198.87.9.3
- rule 3 allows news to be sent to machine 198.87.9.2, but only from machine 129.132.100.7
- rule 4 forbids all other packets.

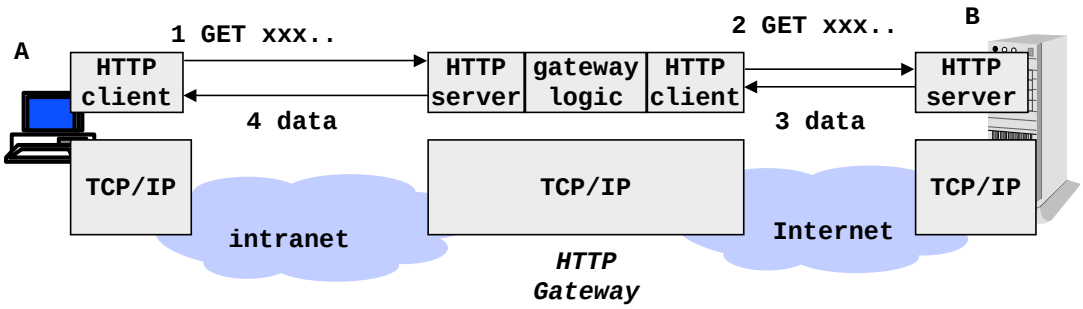
Designing the set of rules employed in a firewall is a complex task; the set shown on the picture is much simpler than a real configuration.

Packet filtering alone offers little protection because it is difficult to design a safe set of rules and at the same time offer full service to the intranet users.

4

Application Layer Gateways

- Application layer gateway is a layer 7 intermediate system
  - normally not used according to the TCP/IP architecture
  - but mainly used for access control
  - also used for interworking issues
- Principle:
  - proxy principle: viewed by client as a server and by server as a client
  - supports access control restrictions, authentication, encryption, etc



1. User at A sends an HTTP request. It is not sent to the final destination but to the application layer gateway. This results from the configuration at the client.

2. The gateway checks whether the transaction is authorized. Encryption may be performed. Then the HTTP request is issued again from the gateway to B as though it would be originating from A.

3. A response comes from B, probably under the form of a MIME header and data. The gateway may also check the data, possibly decrypt, or reject the data.

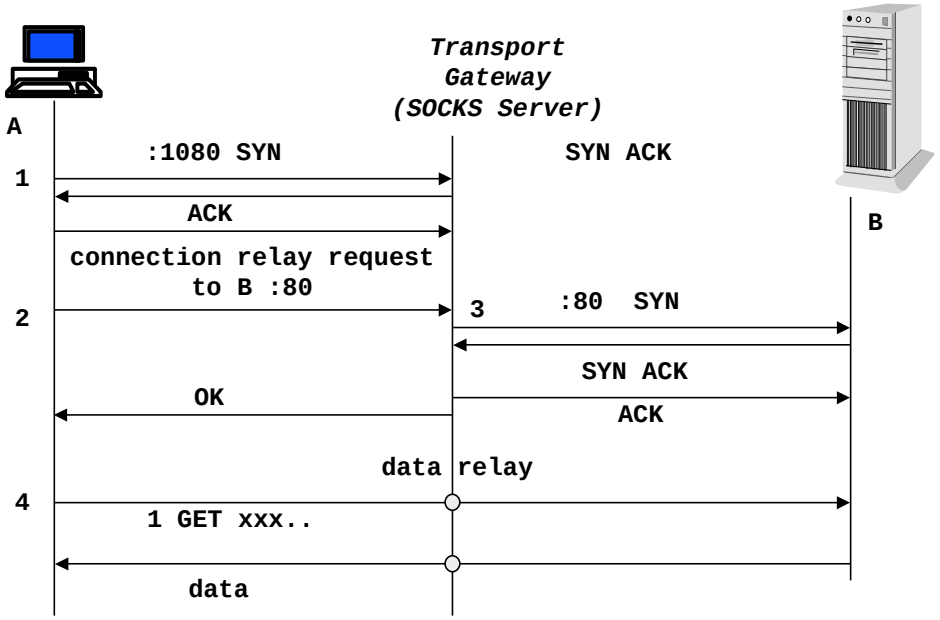
4. If it accepts to pass it further, it is sent to A as though it would be coming from B.

Application layer gateways can be made for all application level protocols. They can be used for access control, but also for interworking, for example between IPv4 and IPv6.

5

Transport Gateway

- Similar to application gateways but at the level of TCP connections
  - independent of application code
  - requires client software to be aware of the gateway



The transport gateway is a layer 4 intermediate system. The example shows the SOCKS gateways. SOKCS is a standard being defined by the IETF.

1. A opens a TCP connection to the gateway. The destination port is the well known SOCKS server port 1080.

2. A requests from the SOCKS server the opening of a TCP connection to B. A indicates the destination port number (here, 80). The SOCKS server does various checks and accepts or rejects the connection request.

3. The SOCKS server opens a new TCP connection to B, port 80. A is informed that the connection is opened with success.

4. Data between A and B is relayed at the SOCKS server transparently. However, there are two distinct TCP connections with their own, distinct ack and sequence numbers.

Compared to an application layer gateway, the SOCKS server is simpler because it is not involved in application layer data units; after the connection setup phase, it acts on a packet by packet level. Its performance is thus higher.

However, it requires the client side to be aware of the gateway: it is not transparent. Netscape and Microsoft browsers support SOCKS gateways.

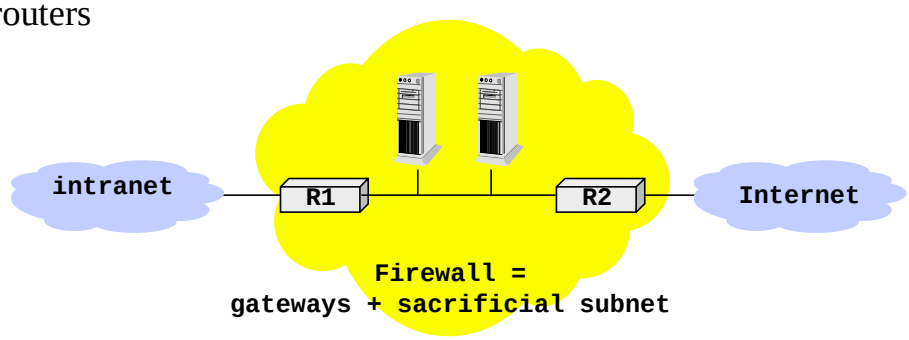
6

Typical Firewalls Designs

- An application / transport gateway alone can be used as firewall if it is the only border between two networks

Firewall =
one dual homed gateway

- A more general design is one or more gateways isolated by filtering routers



Firewall =
gateways + sacrificial subnet

The simple firewall made of one host is an efficient solution, relatively simple to monitor. It is typically made of a Unix workstation with two interfaces (often: Linux). Care must be taken to disable IP packet forwarding, otherwise, the station works as a router.

This simple solution is a single point of failure and a traffic bottleneck. Large intranets need a mores elaborate solution, as shown on the figure. The filtering routers force all traffic to go through the collection of gateways, by forbidding any traffic not destined to one of the gateways. Attacks are still possible, but only gateways need to be closely monitored.

Facts to Remember

- The simple architectures can be combined to address various real life needs
  - connection oriented networks such as Frame Relay, ATM and X.25 are used to interconnect routers or even hosts, in competition or by complementing the native IP method
  - application or transport gateways are introduced to satisfy security or interworking needs
  - routers perform packet processing not only based on destination address but also other protocol information visible in the packets.