

Computer System- B Security

Introduction to Network Security
Firewalls

Sanjay Rawat

bristol.ac.uk

Firewall's (in)capabilities

- ✓ Provide a focal point for monitoring.
- ✓ Provide a central point for access control (who can do what).
- ✓ Limit the damage that a network security problem can do to the overall network.
- ✗ Protect against malicious insiders.
- ✗ Protect a connection that doesn't go through it!!
- ✗ Protect against completely new threats.
- ✗ Protect against viruses, Trojans etc.

4

Firewall Overview

- Introduction to Firewall
- Types of Firewalls
- Firewall configuration and deployment

2

Firewall Deployment

- All traffic from inside to outside, and vice versa, must pass through the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass
- **Ideal Assumption: The firewall itself is immune to penetration. E.g. Cisco IOS vulnerabilities, Juniper Junos vulnerabilities.**

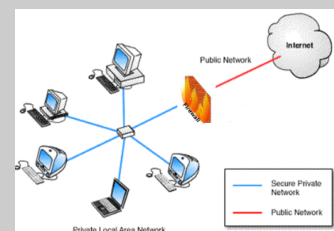
5

Firewalls

- *A mechanism used to protect a trusted network from an untrusted network .*
- A mechanism to enforce access control policy.
- Software or Hardware based.
- Deployed as gatekeeper.
- Examples: Iptable/Iptable, Cisco PIX, Juniper, MS ISA.

3

Typical Deployment



All images are taken from doc at <http://www.vicomsoft.com/learning-center/firewalls/>

6

Generic Techniques for Enforcing policy

- **Service control:** Determines the types of Internet services that can be accessed.
- **Direction control:** Determines the direction in which particular service requests are allowed.
- **User control:** Controls access to a service according to which user is attempting to access it. IP based filtering or authentication with IPSec.

7

Example packet filters

Rule No	Action	Src IP	Dst IP	Src Port	Dst Port	Direction	Description
1	Block	IP1	*	*	*	IN	Block packets from IP1
2	Pass	*	IP_SMTP	*	25	IN	Allow packets to mail gateway
3	Pass	*	*	*	*	OUT	Allow outgoing
4	Block	*	*	*	*	IN	Block Everything Else

10

Types of firewalls

- Packet Filtering Firewall
- Stateful Inspection Firewall
- Application Level Gateway
- Circuit-level gateway

8

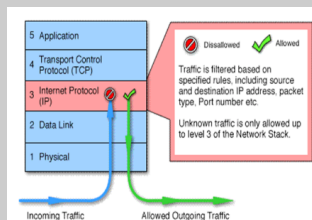
Problems with Packet filters

- Less visibility in the network stack -> less control.
- Hard to define rules as normal connections are request-response
 - Disallowing incoming traffic will prevent response!

11

Packet filters

- Works at most up to transport layer, but at individual packet level.
- Stateless
- Fast processing



9

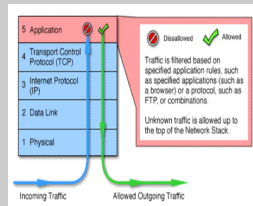
Stateful Inspection

- Keeps session information
- Decision is based on the established connections -> a table of established connection is maintained.
- Fast processing of subsequent packets.

12

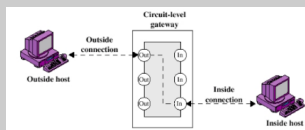
Application gateway (aka Proxy)

- Filters traffic at application layer
- Specific to applications which are configured.
- Works at client-server mode
- Offer High level of security
- Have impact on network performance



13

Circuit Level gateway



- Client-server mode.
- Always two connections (NAT/PAT).
- Hides internal network!
- Uses [SOCKS protocol](#) for client server connection.
- Often used with application gateway.

14

Our generic design

