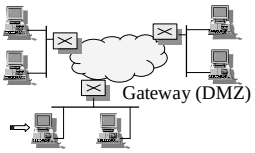
Firewalls and Firewall Testing Techniques

Sonia Fahmy
Department of Computer Sciences
Purdue University
fahmy@cs.purdue.edu
http://www.cs.purdue.edu/homes/fahmy/

Overview

- What is a firewall?
- Firewall types and architectures
- Firewall operations
- Firewall testing

What is a Firewall?



- A firewall is a method of achieving security between trusted and untrusted networks
- The choice, configuration and operation of a firewall is defined by policy, which determines the the services and type of access permitted
- Firewall = policy+implementation
- Firewall = "zone of risk" for the trusted network

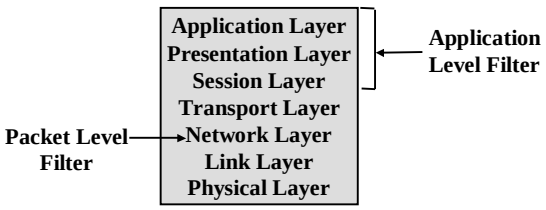
Firewalls Should…

- Support and not impose a security policy
- Use a "deny all services except those specifically permitted" policy
- Accommodate new facilities and services
- Contain advanced authentication measures
- Employ filtering techniques to permit or deny services to specific hosts and use flexible and user-friendly filtering
- Use proxy services for applications
- Handle dial-in
- Log suspicious activity

Firewalls Cannot…

- Protect against malicious insiders
- Protect against connections that do not go through them (e.g., dial-up)
- Protect against new threats or new viruses

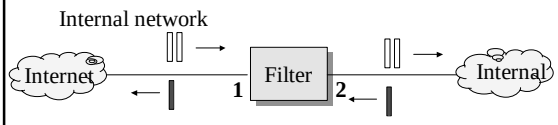
Firewalls in Relation to 7 Layers



Simple Packet Filters

- Example:

Interface	Source	Dest.	Prot.	SPort	Dport
2	*	*	TCP	*	21 (FTP)
1	128.5.*.*	*	TCP	*	25 (SMTP)

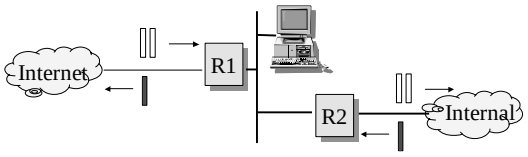


Difficult to handle X-Windows, RPC (including NFS and NIS), rlogin, rsh, rexec, rcp, and TFTP

Stateful Inspection

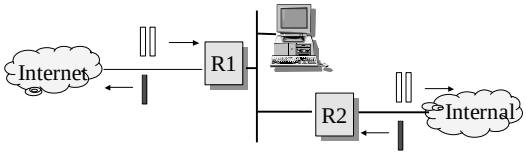
- Also known as dynamic packet filtering (dynamic rule set)
- Requires storing state for each stream, assuming:
  - If there is one packet, there will be more
  - If there is one packet, responses will be returned
- Prime candidate for resource starvation attacks
- What should be done when table is full?
  - Least recently used
  - Random early drop
  - Time out entries
  - Wait for FIN messages, etc.

Bastion Host



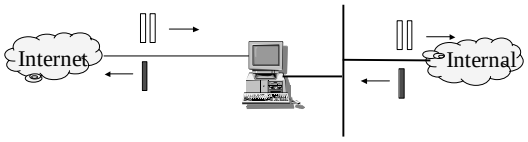
- Inside users log onto the bastion host to use outside services
- Outside snoopers cannot see internal traffic even if they break in the firewall (perimeter = stub network = DMZ)

Firewall Architectures



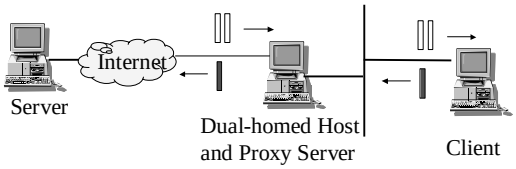
- Screened host: Bastion host and exterior router
- Screened subnet: Exterior and interior routers
- Multiple bastion hosts, multiple interior routers, multiple exterior routers, multiple internal networks (with/without backbone), multiple perimeter networks
- Merged interior and exterior routers, bastion host and exterior router and bastion host and interior router (not recommended)

Dual-homed Host



- The dual-homed host is the firewall in this case

Application-Level Gateways

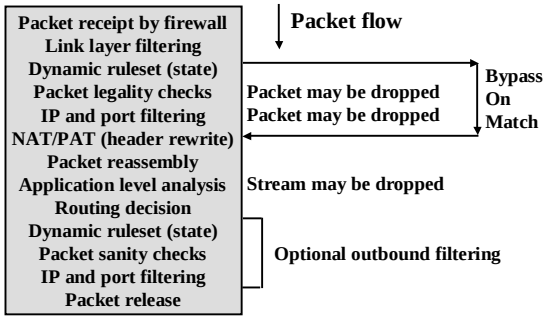


- Specialized programs on bastion host relay requests and responses, enforcing site policies (refusing some requests)
- Sometimes referred to as “proxy servers”
- Transparent with special “proxy client” programs
- Full protocol decomposition, e.g, Raptor, or “plug mode” e.g., Firewall-1 and PIX

Policies

- Network service access policy
  - Defines which services are to be explicitly allowed or denied+ways in which these services are to be used
- Firewall design policy
  - Defines how the firewall implements restricted access and service filtering specified by the NSAP
- FDP must be continuously updated with new vulnerabilities

Packet Traversal in a Firewall



Firewall Testing

- Vulnerabilities = design or coding flaws = invalid assumptions, e.g., insufficient verification, memory available, user data, trusted network object, predictable sequence, etc.
- Develop a vulnerability-operation matrix
- Place Common Vulnerabilities Exposure (CVE), and its candidates (CAN), and other known and new firewall problems in appropriate matrix cell
- Find clusters in matrix
- Predict problems
- Automate firewall testing through focusing on common problems

Example

- CVE-1999-0158
- Cisco PIX firewall manager (PFM) allows retrieval of any file whose name and location is known
- PIX proxy's verification failure
  - Application level
  - Insufficient verification

Key Points

- Firewalls can employ:
  - Packet filters
  - Stateful inspection
  - Application-level gateways (many types)
  - Also circuit-level
- Large variations, e.g., Raptor, PIX, Firewall-1, Gauntlet
- Several architectures to prevent all-or-nothing effect
- Importance of policy
- Firewall testing automation underway

References

- RFC 2647, "Benchmarking" + drafts
- Simonds, "Network Security", 1996
- Hunt, "Internet/Intranet firewall security", Computer Communications, 1998
- Frantzen et al, "A framework for understanding vulnerabilties in firewalls using a dataflow model of firewall internals", in preparation
- Kamara et al, "Testing firewalls", in preparation
- Chapman, "Network (In)Security through IP packet filtering"
- http://cve.mitre.org/, www.sans.org, www.cert.org
- Web pages and mailing lists

Thank You!

Questions?