Firewalls

ADVANCED NETWORKS

GORDON REYNOLDS | 2016

1

What is a firewall?

A firewall is a device (or software feature) designed to control the flow of traffic into and out-of a network.

In general, firewalls are installed to prevent attacks.

2

What is an attack?

'Attack' covers many things:

1. Someone probing a network for computers.
2. Someone attempting to crash services on a computer.
3. Someone attempting to crash a computer
4. Someone attempting to gain access to a computer, server and/or services to use resources or information.

3

Firewalls DO

- Implement security policies at a single point
- Monitor security-related events (audit, log)
- Provide strong authentication
- Allow virtual private networks
- Have a specially hardened/secured operating system

4

Firewalls DON'T

- Protect against attacks that bypass the firewall
  - Dial-out from internal host to an ISP
- Protect against internal threats
  - Disgruntled employee
  - Insider cooperation with an external attacker
- Protect against the transfer of virus-infected programs or files

5

Types of Firewalls

6

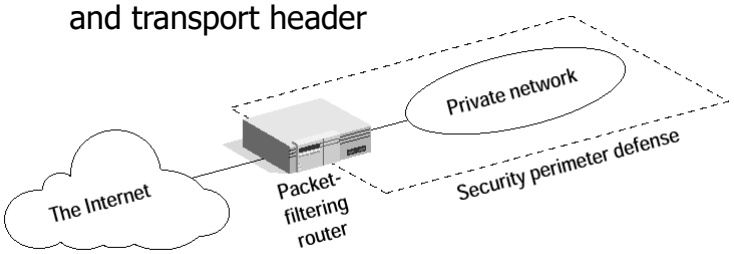
Types of Firewalls

- Packet-Filtering Router
- Application-Level Gateway
- Circuit-Level Gateway
- Hybrid Firewalls

7

Packet Filtering Routers

- Forward or discard IP packet according a set of rules
- Filtering rules are based on fields in the IP and transport header



8

What information is used for filtering decision?

- Source IP address (IP header)
- Destination IP address (IP header)
- Protocol Type
- Source port (TCP or UDP header)
- Destination port (TCP or UDP header)

9

Web Access Through a Packet Filter Firewall

TABLE 14.1 Web Access Through a Packet Filter Firewall

Action	Src	Port	Dest	Port	Flags	Comment
block	*	*	*	*	*	Block all by default
allow	*{Internal net}*	*	*	80	*	Outgoing Web
allow	*	80	*	*	ACK	Incoming Web
allow	*{Internal net}*	*	*	21	*	Outgoing FTP control channel
allow	*	21	*	*	ACK	Incoming FTP control channel
allow	*{Internal net}*	*	*	≥1024	*	Outgoing FTP data
allow	*	≥1024	*	*	ACK	Incoming FTP data
allow	*{Internal net}*	*	*	443	*	Outgoing SSL
allow	*	443	*	*	ACK	Incoming SSL
allow	*{Internal net}*	*	*	70	*	Outgoing Gopher
allow	*	70	*	*	ACK	Incoming Gopher

10

Packet Filtering Routers pros and cons

Advantages:

- Simple
- Low cost
- Transparent to user

Disadvantages:

- Hard to configure filtering rules
- Hard to test filtering rules
- Don't hide network topology(due to transparency)
- May not be able to provide enough control over traffic
- Throughput of a router decreases as the number of filters increases

11

Stateless Firewalls

- Stateless firewalls watch network traffic and restrict or block packets based on source and destination addresses or other static values.
- They're not 'aware' of traffic patterns or data flows.
- A stateless firewall uses simple rule-sets that do not account for the possibility that a packet might be received by the firewall 'pretending' to be something you asked for.

12

Stateless Firewall

A stateless firewall filter, also known as an access control list (ACL), does not statefully inspect traffic. Instead, it evaluates packet contents statically and does not keep track of the state of network connections.

13

Statefull Firewalls

- Stateful firewalls can watch traffic streams from end to end.
- They are aware of communication paths and can implement various IP Security (IPsec) functions such as tunnels and encryption.
- In technical terms, this means that stateful firewalls can tell what stage a TCP connection is in (open, open sent, synchronized, synchronization acknowledge or established).

14

Location of Firewalls

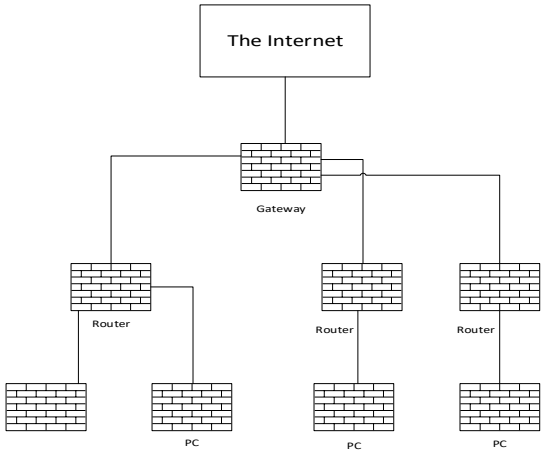
15

Edge Firewall

- An edge firewall is usually software running on a server or workstation.
- An edge firewall protects a single computer from attacks directed against it.
  - Examples of these firewalls are:
    - ZoneAlarm
    - BlackIce
    - IPFW on OSX

16

Edge Firewall



17

Firewall Appliance

- An appliance firewall is a device whose sole function is to act as a firewall.
- Examples of these firewalls are:
  - Cisco PIX.
  - Netscreen series.

18

Network Firewall

Router/Bridge based Firewall

- A firewall running on a bridge or a router protects from a group of devices to an entire network.
- Cisco has firewall feature sets in their IOS operating system.

Computer-based Network Firewall

- A network firewall runs on a computer (such as a PC or Unix computer).
- These firewalls are some of the most flexible.
- Many free products are available including IPFilter, PF and IPTables.

19

Why use a firewall?

- Protect a wide range of machines from general probes and many attacks.
- Provides some protection for machines lacking in security.
- Great First Line of Defense:
  - Having a firewall is a necessary evil.
  - It's like living in a gated community.
    - The gate may stop 99% of unwanted visitors. The locks on your doors stop the remaining 1%.
  - Don't let the firewall give you a false sense of security.
  - Harden your machines by turning off services you don't need.

20

How does a firewall work?

- Blocks packets based on:
  - Source IP Address or range of addresses.
  - Source IP Port
  - Destination IP Address or range of addresses.
  - Destination IP Port
  - Some allow higher layers up the OSI model.
  - Other protocols

21

How does a firewall work?

Common ports

80	HTTP
443	HTTPS
20 & 21	FTP
23	Telnet
22	SSH
25	SMTP

22

Sample firewall rules

Protected server: 134.71.1.25

Protected subnet: 134.71.1.0/24

$internal refers to the internal network interface on the firewall.

$external refers to the external network interface on the firewall.

23

Sample rules:

Can you find the problem?

(For this example, when a packet matches a rule, rule processing stops.)

Pass in on $external from any proto tcp to 134.71.1.25 port = 80

Pass in on $external from any proto tcp to 134.71.1.25 port = 53

Pass in on $external from any proto udp to 134.71.1.25 port = 53

Pass in on $external from any proto tcp to 134.71.1.25 port = 25

Block in log on $external from any to 134.71.1.25

Block in on $external from any to 134.71.1.0/24

Pass in on $external from any proto tcp to 134.71.1.25 port = 22

Pass out on $internal from 134.71.1.0/24 to any keep state

24

Sample rules:

Can you find the problem?

Pass in on $external from any proto tcp to 134.71.1.25 port = 80

Pass in on $external from any proto tcp to 134.71.1.25 port = 53

Pass in on $external from any proto udp to 134.71.1.25 port = 53

Pass in on $external from any proto tcp to 134.71.1.25 port = 25

Block in log on $external from any to 134.71.1.25

Block in on $external from any to 134.71.1.0/24

Pass in on $external from any proto tcp to 134.71.1.25 port = 22

Pass out on $internal from 134.71.1.0/24 to any keep state

The SSH rule would never have a chance to be evaluated. All traffic to 134.71.1.25 is blocked with the previous two rules.

25

To log or not to log…

Logging is both good and bad.

If you set your rules to log too much, your logs will not be examined. If you log too little, you won't see things you need. If you don't log, you have no information on how your firewall is operating.

26

Where does a firewall fit in the security model?

- The firewall is the first layer of defense in any security model.
- It should not be the only layer, think of DiD.
- A firewall can stop many attacks from reaching target machines. If an attack can't reach its target, the attack is defeated.

27

Designing a Rule Set

28

Ruleset design

Two main approaches to designing a ruleset are:

1. Block everything then open holes.
2. Block nothing then close holes.

29

Ruleset design – Block Everything

Blocking everything provides the strongest security but the most inconvenience. Things break and people complain.

The block everything method covers all bases but creates more work in figuring out how to make some applications work then opening holes.

30

Ruleset design – Block Nothing

Blocking nothing provides minimal security by only closing holes you can identify. Blocking nothing provides the least inconvenience to our users.

Blocking nothing means you must spend time figuring out what you want to protect yourself from then closing each hole.

31

Filtering bad traffic

(RFC 1918, bad headers, options, etc.)

- Sending bad traffic or malformed packets is a form of attack easily blocked at a firewall.
- The firewall inspects every packet and rejects those that are not properly formed or are intentionally malformed, protecting devices that may be susceptible.

32

Black hole or Return-RST

(or how to respond to things you don't want.)

- Should you tell a sending machine that their traffic was blocked or let them wait until they timeout?
- For some traffic, it's better to let the sending machine wait.
  - This slows down the rate of attack.
- For other traffic (such as SMTP) it may be nice to tell the sender that the SMTP port is closed.