diff types of firewalls

Date :- 31/03/22 PKI IN

Netfilter firwall is statefull packet.

Circuit - evaluate payload of packet but not specific packet.

Two firewall

1) Dimilitarized Zone N/w :-
Some server that available publically :-
→ It is protected by external firewall.
→ also protected by internal firewall.

VLAN → most suited to implement the IPsec.

1) Behind the firewall
→ processing overhead.
→ IPsec traffic is encrypted.
→ circuit level proxy & application level proxy can not be evaluated.

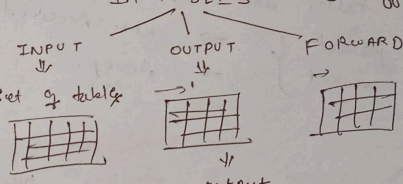
* Distributed firewalls :- (software) Linux, Windows firewall, Bitdefender Box, Cisco next Generation (Hardware).

Take firwall decision :-
→ only entry / exit point for the host / n/w
→ distinguish authorized & unauthorized.
System administrative write some rule that this packet allow or not.
→ secure attacks.

If single computer then use setup the antivirus to detect the firewall work in computer or not.
but if 100 computer then connect one computer with security application and protect the 100 computer n/w.

* Linux firewall - Netfilter
order to Access this firewall
it is System that help us to use the firewall
← IPTABLES
use to administrate the firewall i.e. Netfilter.

IPTABLES → 3 diff set of Rules.



Input the packet → F
then INPUT Rule is apply.

output the packet from the firewall apply this rule.

→ I/p table is checked rule matching according to header
→

validate the above claim ?
• Weak collision resistant.

Rules

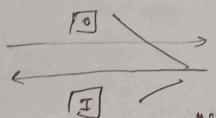
→ packet is evaluated from top to bottom so than more than one rule apply and may be chance, wob rule apply based on header.

→ first matching, take the appropriate decision.

Default ~~Rules~~ for

1) Default policy is : Accept and if match then Rule → matching rule and drop the packet

→ Received a packet } → not Received
→ Drop the packet } → Accep.



matched → drop the packet
not matched - Accep.

→ one way rule is sufficient

2) Default → Drop.

You receive the packet and table carry accept the packet.

→ two way rule is required from client → server and server → client

→ the rules are required in i/p table & o/p table both

validate the above claim ?

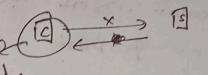
Weak collision resistant.

from client

Rule.

→ If the default policy is ~~accept~~ drop and we accep the packet then we have two way rule is required. from client to server and from server → client.

→ In default is Accept
In order to block the channel in any way then client not able to understand the always client not understand.



Co, it called one way rule.

→ If default is drop, two communication is write. at both server & client side.

Netfilter have.

Seperate Rule table

1) filter :-

2) NAT - Network Address Translation.
↳ Read Born net.

3) Mangle → To alter the packet

Suppose we want to change the SIP, DIP, SPort No & D Port No, we do it with Netfilter firewall.

Syntax of Rules:-

1) ip tables <options> <chain> <Matching criteria>

- -A Append the rule (Append at end)
- -I Insert the rule. (Insert at front)
- -D Delete the rule
- -R Replace the Rule

<chain> → particular insert the i/p chain input, output or forward

<chain>
INPUT
OUTPUT.
FORWARD

<Matching criteria>
If matching then Action take place action can be DROP, ACCEPT, FORWARD.

2) ip tables <options> <chain> <matching criteria> <Action>
DROP
ACCEPT
FORWARD

→ In matching Criteria, there are some Syntax:-

1) ~~-s <ip address> → drop the packet.~~

2) i) If SIP = ___ drop the packet
-s <ip address>

ii) If DIP = ___
-d <ip address>

3) If source port = ___
-- sport port no.

4) If destination port no.
-- dport port no.

5) If packet coming through diff interfaces, to block packet ~~coming~~ coming from particular interface.

6) i/p interface
-i interface
packet received at i/p interface

7) packet received at o/p interface.
-o output

If ~~packet received at~~
Rules of interfacing the packet :-

validate the above claim ?

Node 1 — Router — Node 2

192.168.1.101 — 192.168.1.1 / 192.168.2.2 — 192.168.2.2

[F1] [F2] [F3]

If Node 1 want to communicate node 3 then it communicate through Router.

implement firewall at each level.

Date:- 1/04/21.

PRATIM

connection use @ client :-

1) ping 192.168.1.1 ch router

2) ping 192.168.20.1 ch - server.

@ Server

1) 192.168.1.101

192.168.1.102

1 - 20

Q. Drop all icmp packets forward/obey the Router

Router Side :-

Rule 1 :- iptable -A FORWARD -p icmp -j DROP,

-A : Append the packet. -p : protocol -j : jump

* Command to check forward chain, input chain
→ sudo iptables -L (All rules show) output chain

* sudo iptable -D FORWARD -p icmp -j DROP.
↓
DROP.

Q.) write a rule at a router to accept only those icmp packets that come as a response.

Rule 1 :- iptables -A INPUT -p icmp -j ACCEPT

this rule accept the all packet but question is to only accept the response.

for response packet, we have to mentioned the destination address.

If I want to change the default policy of Input chain.

→ sudo iptable -P INPUT DROP.

Q. Stop access to google from router.

iptable -A INPUT -s www.google.com -j DROP.

Q. To drop a Tcp packet for :—

IP address :- 192.168.1.0/24 source IP

port no :- 25 — destination port.

iptable -A INPUT -s 192.168.1.0/24 -s 192.168.1.0/24 -p tcp --dport 25 -j Drop.

Q. If we have multiple

completely delete O/P, I/P & FORWARD chain

1) to flush a specific chain

2) all chain

3) we can delete the rule by matching criteria

4) Without delete the rule, we check the

1) Sudo iptable -F INPUT delete I/p chain

2) iptable -D INPUT 1.
Delete the Rule 1 in Input table.

*) Delete all chain
-Sudo iptable -F.

* iptable -D Input -s 192.---.

Netcat defn :—
To read / write data across network connections using Tcp / UDP protocols.

webpage
→ Ls
w = wait → keyur.text. (file)
→ nc -w5 192.168.2.201 ftp < keyur.text
netcat command

(a) client

(a) Server.
→ iptables -F
→ sudo nc -l 21 > keyur.text. (port no.)

(1) Drop ftp packets at client
(2) " " Router
(3) " " server.

→ . Drop packet at client side.

sudo iptable -I OUTPUT -p ftp -j DROP

Date:- 5/04/24.

PKITM

Fermat's Theoram Galois

के मा

Euler

Euler