

A.P. SHAH INSTITUTE OF TECHNOLOGY



	Data Science	A. C.
Semester	 Subject :(Academic Year: 2003-2024

FIREWALL A ffrewall is a network security device, either hardware or software based, which monflors all incoming and outgoing traffic and based on a defined set of security rules

acceptiveject or drop that specific traffic.

Reject: Block the traffic but reply with an unreachable error Accept: - Allow the traffic.

Drop: - Block the traffic with no reply. A firewall is a type of network security device that filters

incoming and outgoing network traffic with security policies that have previously been set up inside an organization. A firewall is essentially the way that separates a private internal network from the open Internet of its very

basic level.

Internal protected Firewall Network (eg) entirprise n/w.

External (with usted n/w) (eg) Internet

types of Firewall:

* Packet filtering Firewall

* Stateful packet Inspection (SPI).

* Application Level Gateway.

* Circuit Level Gateway

Subject Incharge: Prof. Sarala Mary Page No. 1.

Department of CSE-Data Science | APSIT



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering **Data Science**



Academic Year: 2003-2024.

Packet Follering Frewall:

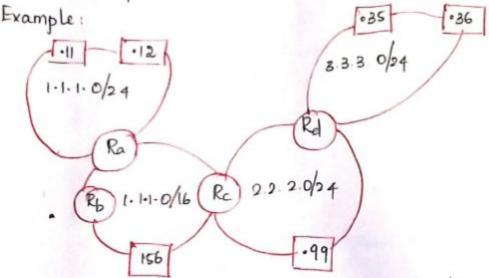
Semester VI

In packet filtering firewall we define the rules based on what should pass inside the network and what should go outside the relivork

Subject: CSS

The rules are set either to accept or to reject the packet Tilleration is done loased on I Paddress and port Number.

Every protocol has the own port number for eg https: 443, 8sh = 22, http = 80, Telned = 21.



Consider the above network diagram. Create a firewall table for the following rules

- (1) Block the external were from using the 8sh whach has the IP address 1.1.1.11
- (2) Block access to Webserver on Nelwork 3.3.3.0/24 for 12

Subject Incharge: Prof. Sarala Mary Page No. 2

Department of CSE-Data Science | APSIT



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering

Data Science



Semester	: VI	Subject : CSS		Academic Year: 2022-2024
Rule	Source	Destination	Poplocol	Action.
1.	*	1.1.1.11:22	TCP	DROP
g.	1.1.1.12:*	3 3 3 0/24	TCP	DROP
DefauH	* * *	*:*	*	ACCEPT.

Example 2:



Block compuler 2 from accusing Webserver on computer 1 with default holice as accept.

	Source	Destination	Protocol	Action.
4.	2222*	1.1.1.1 : 80	TCP	PROP
Default	* *	*:*	*	ACCEPT.

Stateful Packet Inspection:

Consider the below example:

1.1.1.1

Allow WebBrowser on computer O to access Weblerrer in computer a with default policy as DROP.

Rule	Source	Destination 1	Proloco 1	Action
1.	1.1.1.1 : *	2.2.2.2:80	TCP	Accept.
Defaut	*:*	* : *	*	Doob.

This lable will not give the expeded answer. Even the rule no I will not work.

Subject Incharge: Prof. Sarala Mary Page No. 3

Department of CSE-Data Science | APSIT

PARSHWANATH CHARITABLE TRUST'S



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering **Data Science**



Semester: VI Subject: CCC Academic Very 20.00 2.6
CSS Academic rear: 20 23 2024 .
Since TCP peolocol framemile 3 pachelis - SYN, SYN-ACK RACK
Since TCP prolocol transmile 3 packets - SYN, SYN-ACK RACK Source Syn 1-1-1-1 Banage Destination 2222
D=2.2.2.2.
BYN-ACK The BYN-ACK packet cannot
B:222,D:1-1-1 be transmitted because.
of the rules in firewall
table I will drop.
So even the rule 1 will not work properly.
To overcome this problem, we use stateful packet Inspection
9.0
It maintains the state information and allows the packet
to enter the network based on the state information.
Along with the normal frewall table it also creates
Along with the normal freeden
a SPI (Stateful Pockel Inspection) Table where the packel
informations are entered
Src Destination Prolocol Action State
1.1.1.1:35,200 2.2.2.2:80 TCP ACCEPT Setting up connection
Hotel open.
S 87N 3.23.2:80 Established.
SYN ACK DENTH SESSON DESCRIPTION When first packed BYN enters Clossed. SYN ACK DENTH SESSON THE NELLOOK, it checks the first table rule and makes the entry on SPI Table. When
SYN ACK DENTITIES the nelisork, it checks the first table rule
and makes the entry in SPI Table. When
Aca. Second packed (SYN-ACK) enters & refers the
IP addresses in SPI table, a if fit matches
The came proceed continues
till connection is closed. Once the connection
Is closed the entire SPI table is deleted and new table is subject incharge: Prof. Sarala Mary Page No. 4 Department of CSE-Data Science APSIT
Subject Incharge: Prof. Sarala Mary Page No. 4 Department of CSE-Data Science APSIT

PARSIEWARIATH CHARITABLE TRUST'S



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering Data Science



Semester: Y Subject : CSS Academic Year: 20 23 - 2024 (3) APPLICATION LEVEL GATEWAY: Internal connection Application Application Transport Transport Internal Internet Network Nelwork acous Access Physical Physical → II works in Application Layer. -) II we provide. Client and server connect to proxy. - Communication is done through proxy server. -> When client requests access to server resources such as file, webpage, dalabase then the client first connects with prony server, which then establishes connection with - Application Gateway nesides on the client and the - The prony server hides IP address and other secure information -> They decide whether to drop a packet or send them based on application information. -> They handle complex protocol (eg) attacks over http like sending long string in the host field would be dropped because they have been tampered by an Subject Incharge: Prof. Sarala Mary Page No. \$\square\$ \$\square\$ Department of CSE-Data Science | APSIT

PARSHWANATH CHARITABLE TRUST'S



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering **Data Science**



Semester : VI Subject : ____ CS.9 Academic Year: 2023 - 2024 . (4) CIRCUIT LEVEL GATEWAY: Internal Application Application External Circuit level Transport Gateway. Internet Internet Nelwork Acuss Network Physical Physical -> It provides UDP and TCP connection security. -) It monitors TCP data packet handshaking and session fulfillment of firewall rules and policies. → It checks the validity of connections (ie. circuitis) at the transport layer against a lable of allowed connections before a session can be opened and data exchanged. It acts as a priory and has the same advantage as an application level gateway in hiding the internal host from the serving host. -> Disadvantage is absence of checking and fiftering individual packet. - It can be implemented along with application-level gateway or as stand - alone systems. Provides high-level secure network connection. Subject Incharge: Prof. Sarala Mary Page No. 6 Department of CSE-Data Science | APSIT