

Attendance



Firewalls

Network Engineering Association

What is a Firewall?

- Network Firewalls are the devices that are used to prevent private networks from unauthorized access. A Firewall is a security solution for the computers or devices that are connected to a network, they can be either in form of hardware as well as in form of software. It monitors and controls the incoming and outgoing traffic (the amount of data moving across a computer network at any given time).
- The major purpose of the network firewall is to protect an inner network by separating it from the outer network. Inner Network can be simply called a network created inside an organization and a network that is not in the range of inner network can be considered as Outer Network.





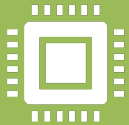
How it works

Firewalls match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization. From the perspective of a server, network traffic can be either outgoing or incoming.

How it works









































































Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication. Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP.



All these types have a source address and destination address. Also, TCP and UDP have port numbers.



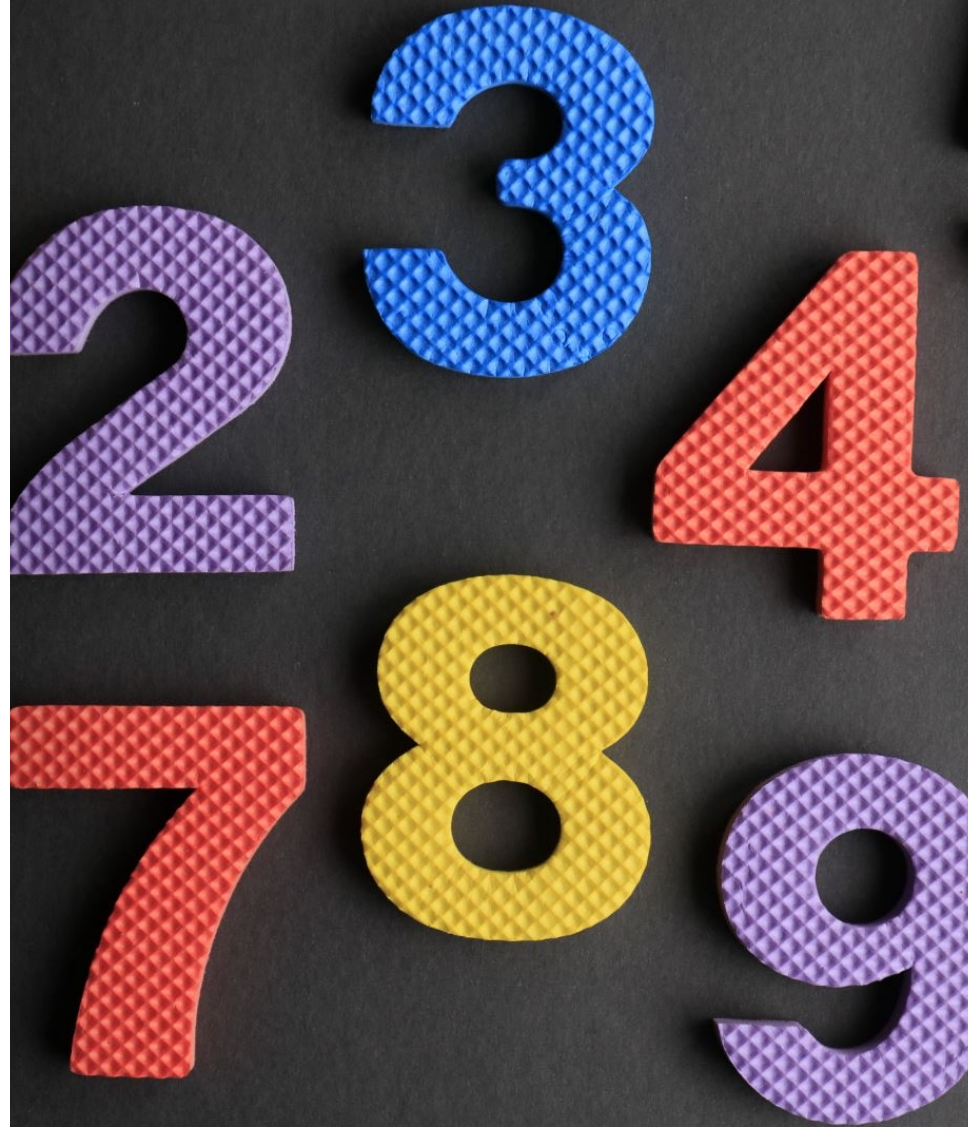
ICMP uses type code instead of port number which identifies purpose of that packet.

	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description 
Automatically generated									
   	IPv4 *	Comp2 net	*	10.1.199.76	*	*	*		
   	IPv4 *	Comp2 net	*	Management net	*	*	*		
   	IPv4 *	Comp2 net	*	Storage net	*	*	*		
   	IPv4 *	Comp2 net	*	Web net	*	*	*		
   	IPv4 *	Comp2 net	*	Comp1 net	*	*	*		
   	IPv4 *	Comp2 net	*	Comp3 net	*	*	*		
   	IPv4 *	Comp2 net	*	Comp4 net	*	*	*		
   	IPv4 *	Comp2 net	*	Comp5 net	*	*	*		
   	IPv4 *	Comp2 net	*	Comp6 net	*	*	*		
   	IPv4 *	Comp2 net	*	Comp7 net	*	*	*		
   	IPv4 *	Comp2 net	*	Comp8 net	*	*	*		
   	IPv4 *	Comp2 net	*	Comp9 net	*	*	*		
   	IPv4 *	Comp2 net	*	Comp10 net	*	*	*		
   	IPv4 *	*	*	*	*	*	*		
   	IPv4 *	*	*	*	*	*	*		
pass		block			reject			log	 in
pass (disabled)		block (disabled)			reject (disabled)			log (disabled)	 out



Firewall Demo

Rules to Create



Attendance

