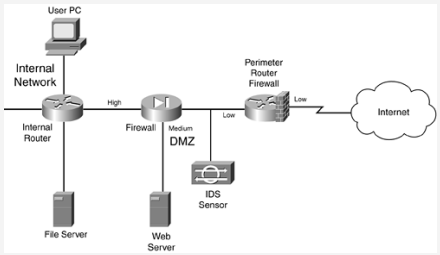
What is a firewall

Firewalls are one of the most important components of a good security system.
A **firewall is any computer you set up to evaluate the traffic** coming and going through your Internet connection.
Many self-proclaimed security experts fail to address the issue of outgoing packets when implementing a firewall. To ensure the security of the corporate network, it is not enough just to use a vpn, as is the case with a home computer. Not only is it important to manage the traffic coming in to your network but you must also filter the outgoing traffic as well.

Inbound Filtering

Inbound firewall filtering monitors the packet types and the source and destinations and decides if the packets should allowed, blocked, or changed in some way.
This is how you would set up a DMZ so the machines aren't visible to the outside world. The rule could say if it's a packet coming from outside the local network and outside the DMZ then it should be blocked. At this point the originating address could also be blocked for all types of traffic just in case they're trying to break in.

Firewall Design



Outbound Filtering

Just as important as inbound firewall rules are the outbound rules. If a machine on your local network gets compromised these outbound rules will prevent it from reaching the machine that is trying to control it.

DMZ

A DMZ, or de-militarized zone (sometimes referred to as a perimeter network or screened subnet), is a network that you can build that connects to the Internet. In this network are all the machines that must talk to the Internet but doesn't contain any of the machines used by your employees.
The purpose of this DMZ is it allows your company to protect the machines on this network so they can only accept connections securely and the traffic on this network is expected to be either non-critical information of any critical data is encrypted. This way if any of the servers in the DMZ become compromised, then only the DMZ is at risk.

General Firewall Filtering

Generally speaking, most Internet routers can be configured as a firewall. The firewall looks at each packet as it comes and goes though it and determines what rules apply and directs the packets according to those rules.
This means if you wan no traffic coming or going to certain hacker domains or YouTube or any other such domains, then tell that to the firewall and they'll stop all packets to or from that address.

By **Shirley Gifford** (Husell)
cheatography.com/husell/

Published 2nd February, 2020.
Last updated 2nd February, 2020.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com