**A great reference for all these firewall architectures –** <http://www.windowsecurity.com/whitepapers/misc/The_IT_Security_Cookbook/The_IT_Security_Cookbook__Firewalls_Securing_external_Network_connections.html>

**Packet filtering** - a technique for improving network security that removes packets whose fields match certain patterns. Even though it is called "filtering", packet alteration before accepting is available.

**NAT** – Network Access Translation – translates IP addresses

**SNAT** (Static Network Access Translation) – group of private IP addresses mapped to a single public IP address.

**DNAT** (Dynamic Network Access Translation) – table of public IP addresses where one is selected for a private IP address when its looking to connect to the internet.

**Strict NAT**( Strict Network Access Translation) – two machines permitted to communication with the internet at a given time.

**Dual – homed firewall** 🡪 one connection for the internet and the other connection for the internal network

**Hardware** (based protections) **firewalls** – automatically built into a router; tag all outgoing traffic with a specific network ID that is also attached to any corresponding incoming traffic. This allows the router to determine the origin of the incoming packets and blocking any transfers that weren’t initiated from behind the firewall. It also prevents files from being downloaded without the user’s knowledge and stops first step intrusions known as port scan attacks – updates are truly updates and not spyware.

**Software** (based protections) **firewalls** – monitoring the integrity of flowing traffic processes through variables such as, incoming and destination IP addresses, transfer times, download sizes, and killing connections that don’t meet expectations. Monitor outgoing and incoming traffic; thus, blocking programs like IP spoofing from attacking individual machines once inside a network.

**Screened host firewall** – more flexible than the dual-host firewall. Combines packet-filtering with application gateway located on the protected subnet side of the router. (router filters or *screens).*

**Screened Subnet Firewall** (DMZ – Demilitarized Zone) Uses an outer/external router and bastion (no protections and outside the firewall) host. It’s a semi-trusted area of the network. It’s not internal nor is it external. <http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/>

1. It has a different network ID from the internal network
2. It is separated from both the Internet and the internal network by a firewall