LIYANA ARACHCHIGE RANIL

SHORT NOTES / NETWORK ARCHITECTURE

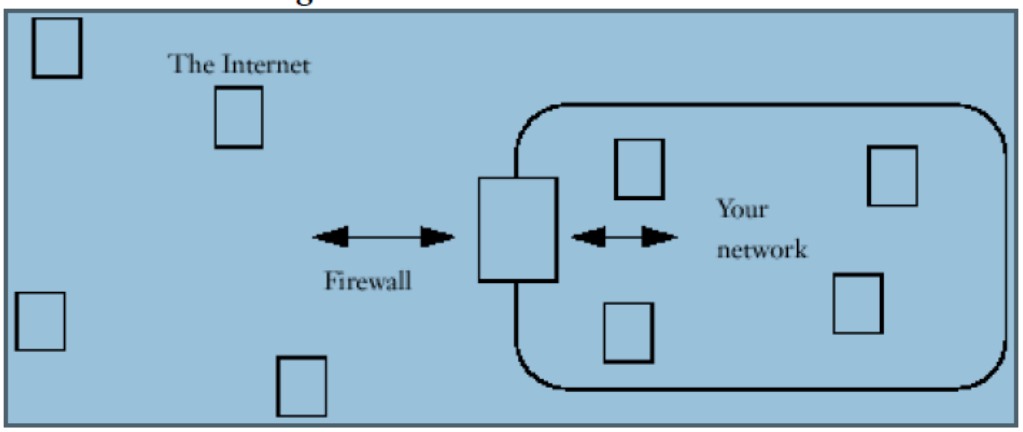
1. IP ADDRESS – Identifies a location or hardware within TCP/IP
2. SWITCH or HUB – Supports multiple machine to participate in a network
3. ROUTER – A device which knows where to route the traffic
    a. Some routers might perform the function of a Firewall as well
    b. Some routers are programmable
4. GATEWAY – Gateway is a router that provide users in a network access to INTERNET
    a. Gateways are typically provided by the ISP
5. FIREWALL – Provides security for a network
6. LOAD BALANCING APPLIENCE – The load balancing appliance distributes traffic over identically configured web servers
7. DNS – Tracks labels of IP addresses
8. DMZ – network sandwiched between TWO firewalls with the INTERNET outside one firewall and the cooperate network outside the other
9. CLUSTER – A group of servers that service the same applications and are configured in such a way that they share ONE IP address

SIMPLE FIRE WALL INSTALLATION

1. The below configuration is better for a situation where only email incoming traffic is allowed and relatively simple to configure. But this is not sufficient for a cooperate firewall as once broken , the whole network is exposed

2.

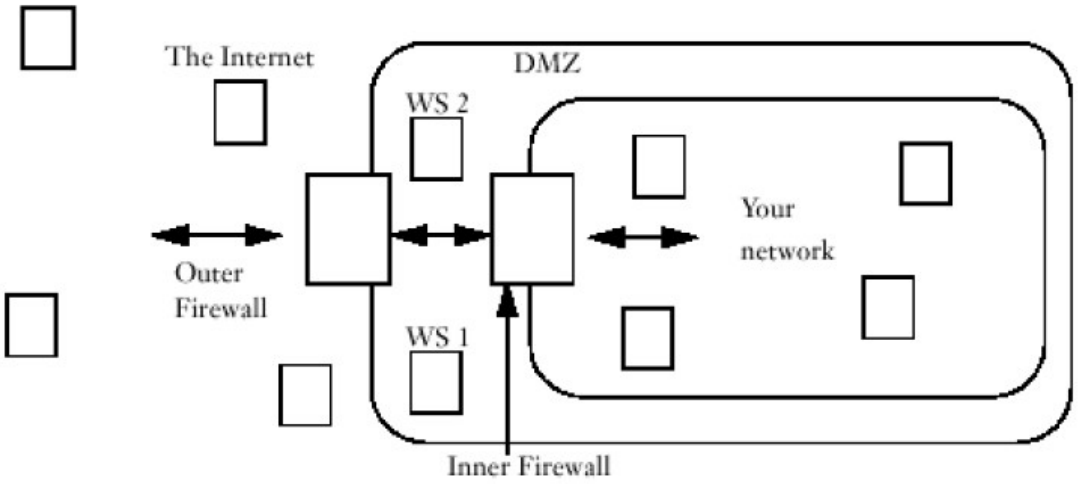
Figure 5-1. Firewall Installation



TWO FIREWALLS and a DMZ

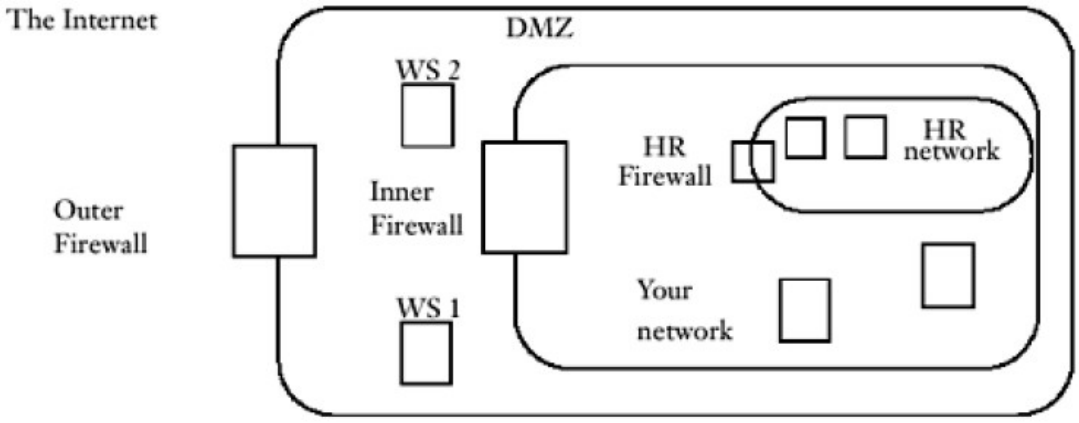
1. Many networks must provide more than one service to the outside world
2. This is a better approach than the single firewall configuration
3. The area sandwiched between the two firewalls is know as DEMELITERIZED ZONE

4.



5. Usually WEB SERVERS are placed in the DMZ zone and only requests from DMZ zone is allowed to come further inside the other fire wall
6. Usually no traffic is allowed between the INNER FIREWALL region and the Internet. But in case where Internet access is needed in side the inner fire wall it is generally passed through a PROXY SERVER in DMZ
7. In bound messages are never sent directly to the INNER FIREWALL , instead it goes through the PROXY SERVER
8. To address the issue of INTERNAL attacks use the below setting

9.



10. Firewalls must be monitored at all the times to make sure those are working properly
11. TUNNELING is a one way of creating a COVERT channel , that is , a communication path for messages of one type that uses a path actually intended for some other type of message
12. TUNNELING can be used to SNEAK past a firewall restriction either to GET OUTSIDE or GET INSIDE the FIRE WALL
13. TUNNELING most of the time makes you to loose both SECURITY and PERFORMANCE