Security functions: Routers, Switches and Load Balancers

Although routers are used to separate networks and route traffic from one network to the other they also act as packet filters and thus provide another layer of security. Routers uses rules like filters called Access Control Lists (ACLs).

Switches

Switches are used to connect devices to the network, unlike hubs switches doesn't forward packets to all of the ports. When the destination MAC address is known it passes the packet to that port only, thus provides security against sniffing. However if the destination MAC is not known it passes the packet out to all of the ports except the one it originated from (ingress port). Ingress/egress means inbound/outbound traffic respectively.

This type of security (the switch provides) can be attacked physically/logically. If the attacker has physical access to the switch they can connect to the monitor/mirror port or configure the switch to see all data crossing it.

If the attacker only has logical access they can flood the switch with MAC addresses in an aim to push valid MAC addresses out of the switch's MAC address table, which will make the switch to fall back to a fault tolerance hub behaviour mode transmitting data out of all ports. Thus the attacker will be able to see all of the data crossing the switch. Because the attacker has to attack the switch for the attack to succeed or sometimes attack the hosts with ARP flooding, the attack also known as active flooding. More advanced switches have a feature that acts like an IDS used to sense when this type of action is used and prevent it.

Load Balancers

Load balancers are used to distribute the load to different links or devices, its main uses are to improve infrastructure utilisation, reduce bottlenecks, reduce response time, prevent overloading and enhance the performance of the network. The load is usually distributed to a server farm or cluster. Load balancers use different methods to balance the load.

Random – a destination is assigned to each packet or connection randomly.

Round-robin – a destination is assigned to each packet or connection in order (1, 2, 3, 4).

Load Monitoring – this basically based on the load, the device with lower load is assigned to the packet or connection.

Preferences – this method assigns destination to the connection or packet based on subjective preference or capacity difference. As an example let's say that device 2 can handle more than device 1 and 3, therefore the destination would be assigned in this order 2, 1, 2, 3, 2, 1, 2, 3…. And so on.

Load balancer can be hardware or software. They can also have many other features that depend on the protocol, applications, caching, SSL (Secure Socket Layer) offloading, compression, error checking, filtering, buffering or even IDS and firewall capabilities.

Proxy Servers

Proxy servers can be application or circuit-level firewalls or a combination. These devices are used as a middleman between servers and clients. They serve as shield that filters unwanted traffic coming into or going out of the network. It replaces the clients IP address with its own external IP address using Network Address Translation (NAT). This hides the IP address of the network devices from external users. This adds some sort of security. In addition to this proxies can also provide caching, which aids in improving the response time to requests. This is because the proxy server already has the content requested in its cache and it doesn't need to look for it and request it from other networks or servers on the internet.

Web Security Gateways

Web security gateways use URL and Keywords to monitor user's web activity and block any activity that violates the organization's usage policy. These devices may also have malware scanning capabilities and non-web filtering features such as Instant Message (IM) filtering, email filtering, spam blocking and spoofing detection.

Source : http://infosectutorials.com/2012/03/04/1-network-security-part-1/