FIREWALL ARCHITECTURES

The configuration that works best for a particular organization depends on three factors: The objectives of the network, the organization‘s ability to develop and implement the architectures, and the budget available for the function.

There are FOUR common architectural implementations of firewalls.These implementations are packet filtering routers, screened host firewalls, dual-homed firewalls,a nd screened subnet firewalls.

I. Packet Filtering Routers

Most organizations with a n Internet connections have some form of a router as the interface to the Internet at the perimeter between the organization‘s internal networks and the external service provider. Many of these routers can be configured to reject packets that the organization does not allow into the network. This is a simple but effective way to lower the organization‘s risk from external attack. The drawbacks to this type of system include a lack of auditing and strong authentication. Also, the complexity of the access control lists used to filter the packets can grow and degrade network performance. Fig

6-4 is an example of this type of architecture.

II. Screened Host Firewalls

This architecture combines the packet filtering router with a separate, dedicated firewall, such as an application proxy server. This approach allows the router to pre-screen packets to minimize the network traffic and loads on the internal proxy.The application proxy examines an application layer protocol, such as HTTP, and perform the proxy services. This separate host is often referred to as a bastion host; it can be a rich target for external attacks, and should be very thoroughly secured.Evn though the bastion host/application proxy actually contains only cached copies of the internal Web documents, it can still present a promising target, because compromise of the bastion host can disclose the configuration of internal networks and possibly provide external sources with internal information. Since the bastion host stands as a sloe defender on the network perimeter, it is also commonly referred to as the Sacrificial Host.

To its advantage, this configuration requires the external attack to compromise two separate systems, before the attack can access internal data. Inthis way, the bastion host protects the data more fully than the router alone. Fig 6-11 shows a typical configuration of a screened host architectural approach.

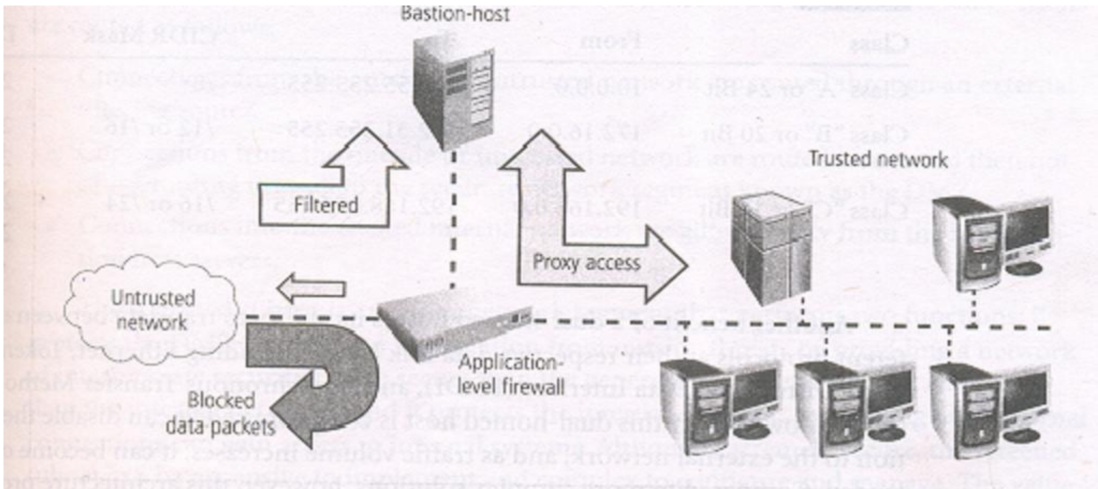

FIGURE 6-11 Screened Host Firewall

III. Dual-Homed Host Firewalls

The next step up in firewall architectural complexity is the dual-homed host. When this architectural approach is used, the bastion host contains two NICs (Network Interface Cards) rather than one, as in the bastion host configuration. One NIC is connected to the external network, and one is connected to the internal network, providing an additional layer of protection. With TWO NICs , all traffic must physically go through the firewall to move between the internal and external networks.

Implementation of this architecture often makes use of NATs. NAT is a method of mapping real, valid, external IP addresses to special ranges of non-routable internal IP addresses, thereby creating yet another barrier to intrusion from external attackers.

The internal addresses used by NAT consist of three different ranges. Organizations that need Class A addresses can use the 10.x.x.x range, which has over 16.5 million usable addresses. Organization's that need Class B addresses can use the 192.168.x.x range, which has over 65,500 addresses. Finally , organiazations with smaller needs , such as those needing onlya few Class C addresses, can use the c172.16.0.0 to 172.16.15.0 range, which hs over 16 Class C addresses or about 4000 usable addresses.

See table 6-4 for a recap of the IP address ranges reseved fro non-public networks. Messages sent with internal addresses within these three internal use addresses is directly connected to the external network, and avoids the NAT server, its traffic cannot be routed on the public network. Taking advantage of this , NAT prevents external attacks from reaching internal machines with addresses in specified ranges.If the NAT server is a multi-homed bastion host, it translates between the true, external IP addresses assigned to the organization by public network naming authorities ansd the internally assigned, non-routable IP addresses. NAT translates by dynamically assigning addresses to internal communications and tracking the conversions with sessions to determine which incoming message is a response to which outgoing traffic. Fig 6-12 shows a typical configuration of a dual homed host firewall that uses NAT and proxy access to protect the internal network.

Table 6-4 Reserved Non-Routable Address Ranges

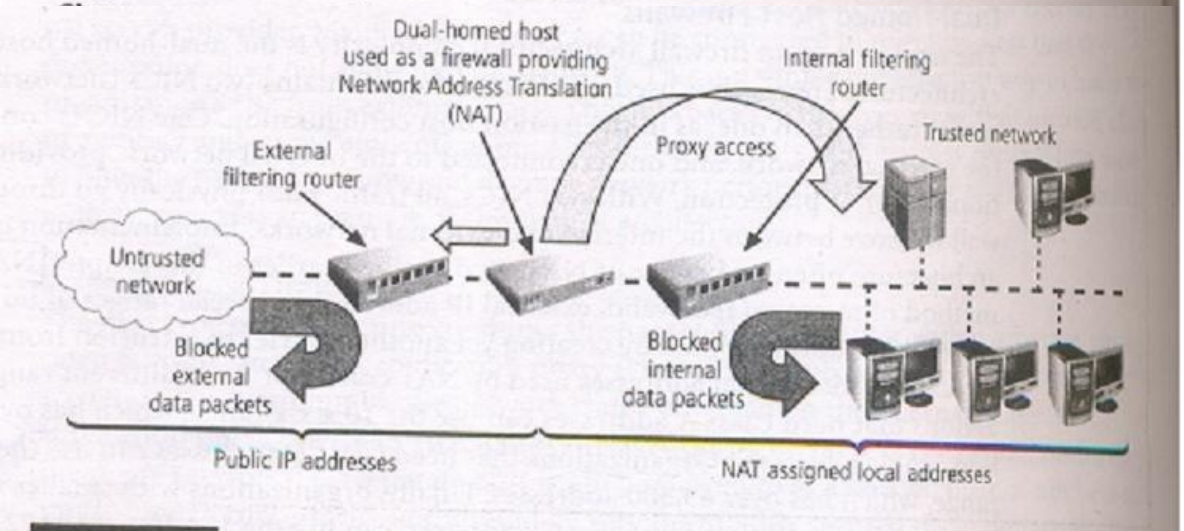
Dual-homed host used as a firewall providing Network Address Translation (NAT)
Internal filtering router
Trusted network
External filtering router
Proxy access
Untrusted network
Blocked external data packets
Blocked internal data packets
Public IP addresses
NAT assigned local addresses

FIGURE 6-12 Dual-Homed Host Firewall

Another benefit of a dual-homed host is its ability to translate between many different protocols at their respective data link layers, including Ethernet , Token Ring, Fiber Distributed Data interface (FDDI) , and Asynchronous Transfer Method (ATM). On the downside, if this dual-homed host is compromised, it can disable the connection to the external network, and as traffic volume increases, it can become overloaded. Compared to more complex solutions, however, this architecture provides strong overall protection with minimal expense.

IV. Screened Subnet Firewalls (with DMZ)

The dominant architecture used today is the screened subnet firewall. The architecture of a screened subnet firewall provides a DMZ. The DMZ can be a dedicated port on the firewall device linking a single bastion host, or it can be connected to a screened subnet, as shown in Fig 6-13. Until recently , servers providing services through an untrusted network were commonly placed in the DMZ. Examples of these include Web servers, file transfer protocol (FTP) servers, and certain database servers. More recent strategies using proxy servers have provided much more secure solutions.

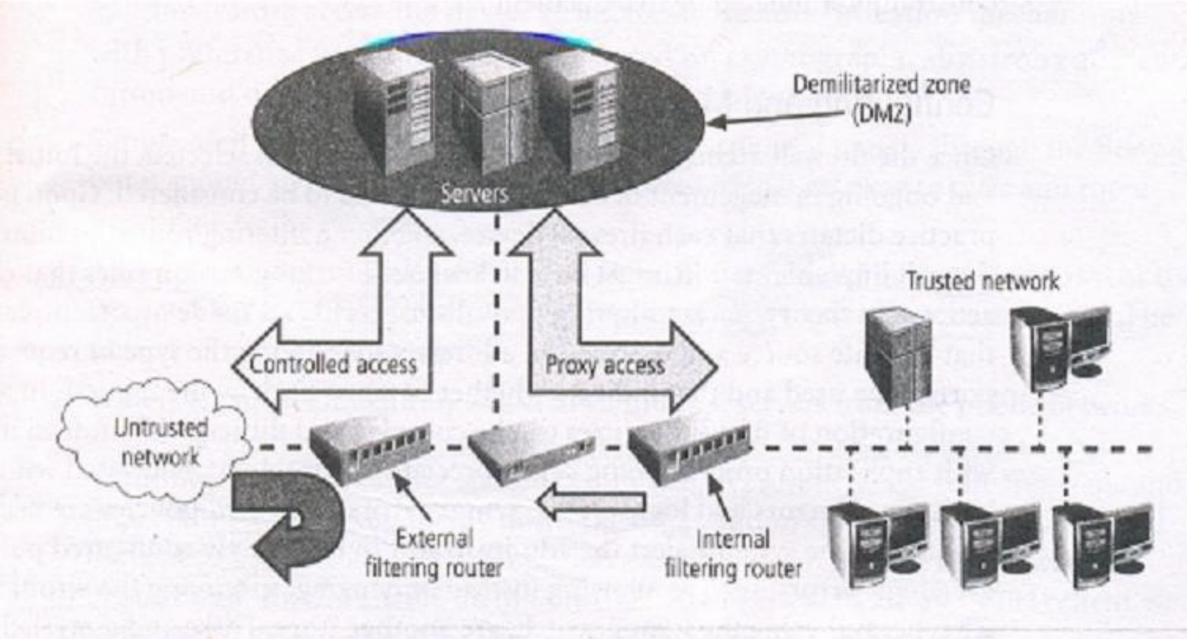

FIGURE 6-13 Screened Subnet (DMZ)

A common arrangement finds the subnet firewall consisting of two or more internal bastion hosts behind a packet filtering router, with each host protecting the trusted network. There are many variants of the screened subnet architecture. The first general model consists of two filtering routers, with one or more dual-homed bastion hosts between them. In the second general model, as illustrated in Fig 6-13 , the connections are routed as follows:

1. Connections from the outside or un trusted network are routed through an external filtering router.
2. Connections from the outside or un trusted network are routed into-and then out of – a routing firewall to the separate network segment known as the DMZ.
3. Connections into the trusted internal network are allowed only from the DMZ bastion host servers.

The screened subnet is an entire network segment that performs two functions: it protects the DMZs systems and information from outside threats by providing a network of intermediate security; and it protects the internal networks by limiting how external connections can gain access to internal systems. Although extremely secure, the screened subnet can be expensive to implement and complex to configure and manage. The value of the information it protects must justify the cost.

Another facet of the DMZ is the creation of an area of known as an extranet. AN extranet is a segment of the DMZ where additional authentication and authorization controls are put into place to provide services that are not available to the general public. An example would be an online retailer that allows anyone to browse the product catalog and place items into a shopping cart, but will require extra authentication and authorization when the customer is ready to check out and place an order.

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf