

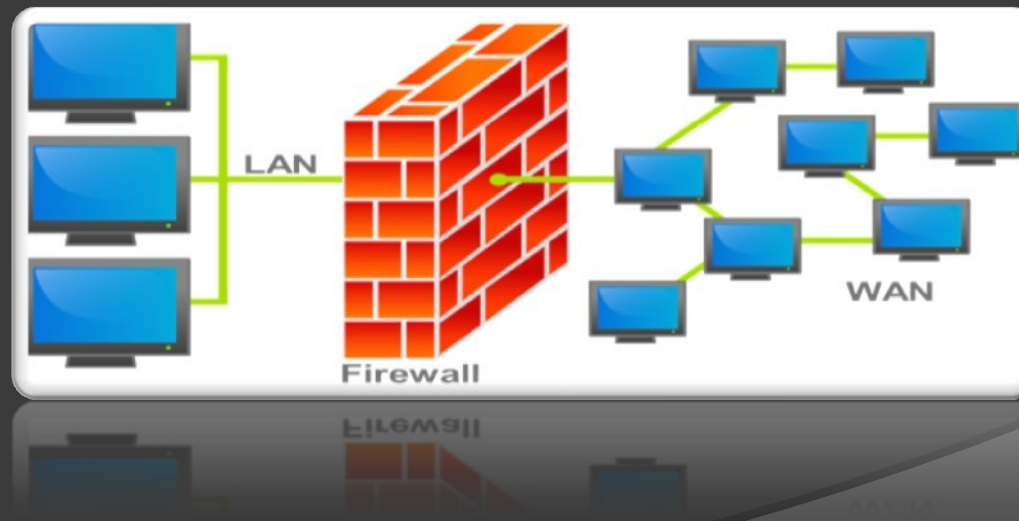
Firewall Architecture



Firewa



- In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.



Firewall Categories

- A **Host-based firewalls**
- A **Network firewalls**

Host Firewall

- A host firewall is a software application or suite of applications installed on a singular computer. Typically, operating system manufacturers include firewall software as part of the system. This is true of Windows (post-Windows 2000), Mac OS X and many distributions of Linux (Ubuntu, Fedora and SuSE). A personal host firewall is managed on the individual computer that the firewall is installed on. Therefore, the administrator has to have access to the computer to install and configure the firewall.

Network Firewall

- A network firewall functions on the network level. This means that the firewall filters data as it travels from the Internet to the computers on the network. The firewall operates with a set of data management rules that apply to the entire network. This sets up a sort of "perimeter" for the network as a first line of defense, regulating the flow of data before it even reaches the individual computers that comprise the network.

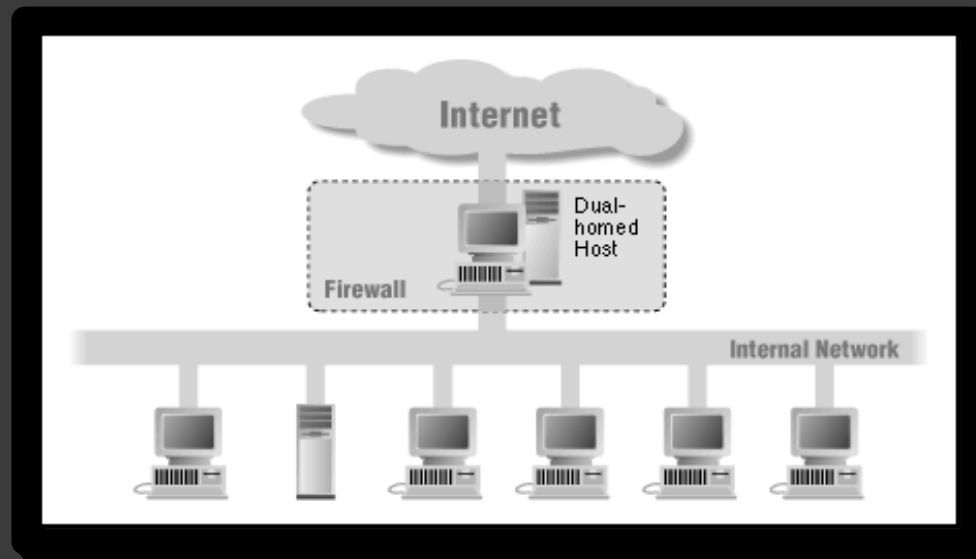
Firewall Architectures

Components of Firewall Architecture

- | **Dual-Homed Host Architecture**
- | **Screened Host Architecture**
- | **Screened Subnet Architecture**
- | **Screening router**

Dual-Homed Host Architecture

- Firewall dual-homing provides the first-line defense and protection technology for keeping untrusted bodies from compromising information security by violating trusted network space.



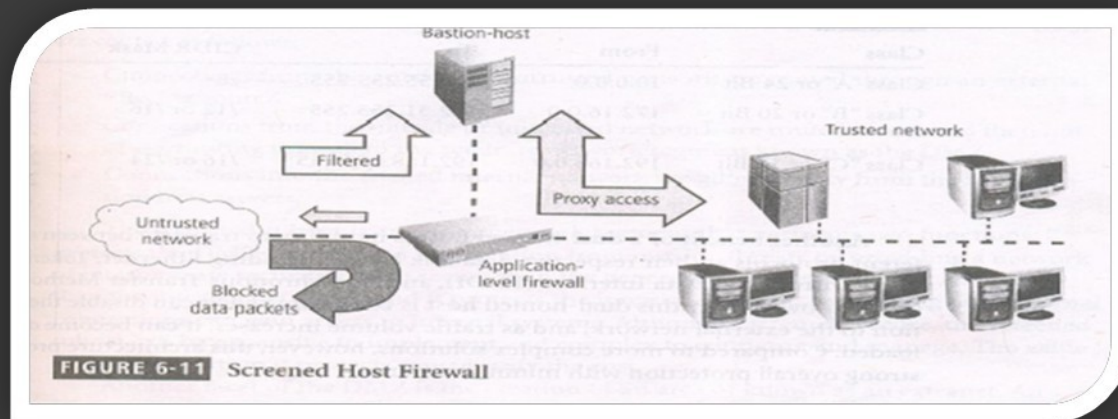
Conti

...

- □ A dual-homed host (or dual-homed gateway) is a system fitted with two [network interfaces](#) (NICs) that sits between an untrusted network (like the Internet) and trusted network (such as a corporate network) to provide secure access. Dual-homed is a general term for [proxies](#), [gateways](#), firewalls, or any server that provides secured applications or services directly to an untrusted network.

Screened Host Architecture

- 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.



Conti

...

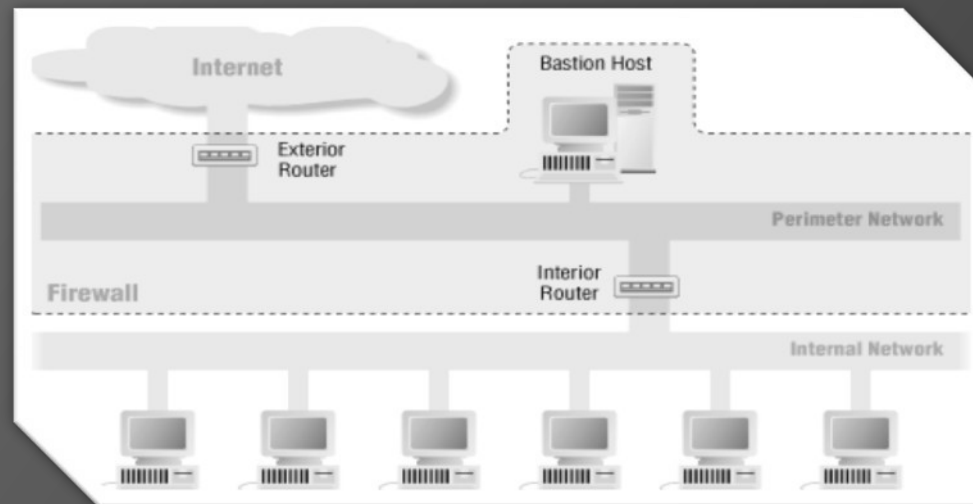
- The application proxy examines an application layer protocol, such as HTTP, and perform the proxy services. This separate host is often referred to as a bastion host; it can be a rich target for external attacks, and should be very thoroughly secured.

Screened Subnet Architecture

- In [network security](#), a **screened subnet firewall** is a variation of the dual-homed gateway and screened host firewall. It can be used to separate components of the firewall onto separate systems, thereby achieving greater throughput and flexibility, although at some cost to simplicity. As each component system of the screened subnet firewall needs to implement only a specific task, each system is less complex to configure.

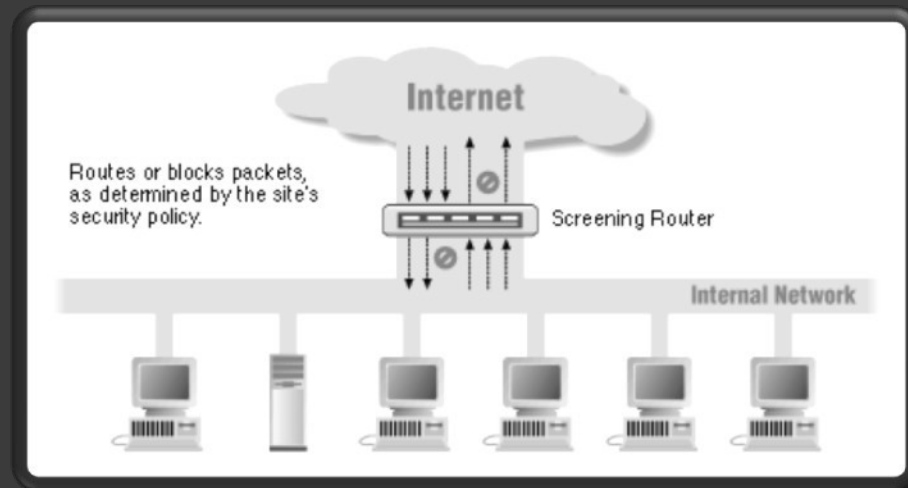
Conti...

- A screened subnet firewall is often used to establish a demilitarized zone (DMZ).



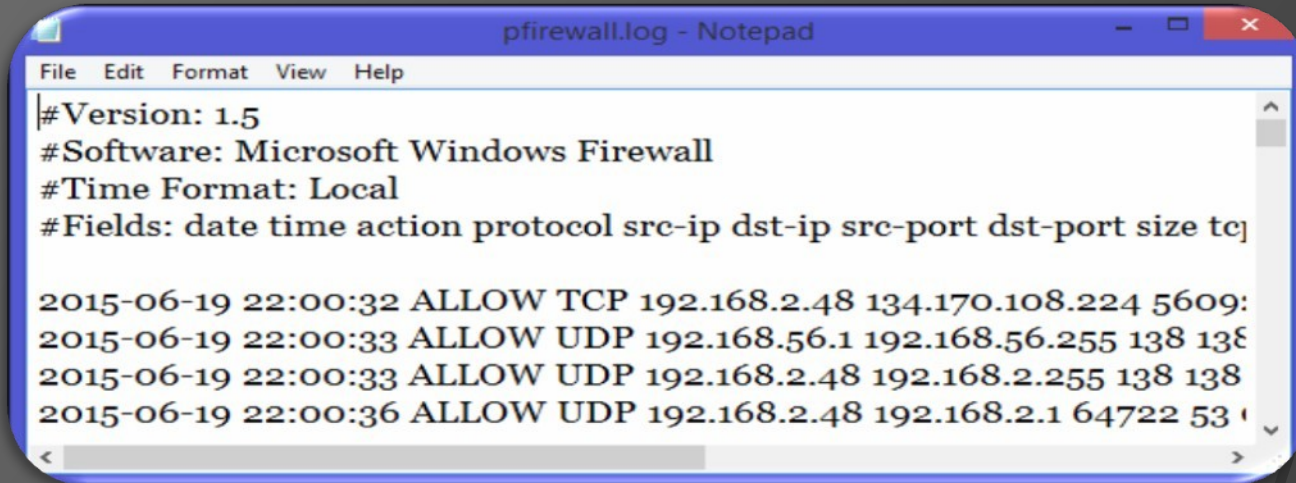
Screening router

- A **screening router** performs packet-filtering and is used as a firewall. In some cases a screening router may be used as perimeter protection for the internal network or as the entire firewall solution.



Firewall Logs

- In the process of filtering Internet traffic, all firewalls have some type of logging feature that documents how the firewall handled various types of traffic.



The screenshot shows a Notepad window with the title 'pfirewall.log - Notepad'. The menu bar includes 'File', 'Edit', 'Format', 'View', and 'Help'. The text content of the log file is as follows:

```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tot

2015-06-19 22:00:32 ALLOW TCP 192.168.2.48 134.170.108.224 5609:
2015-06-19 22:00:33 ALLOW UDP 192.168.56.1 192.168.56.255 138 138
2015-06-19 22:00:33 ALLOW UDP 192.168.2.48 192.168.2.255 138 138
2015-06-19 22:00:36 ALLOW UDP 192.168.2.48 192.168.2.1 64722 53
```

Conti

...

- These logs can provide valuable information like source and destination IP addresses, port numbers, and protocols. You can also use the Windows Firewall log file to monitor TCP and UDP connections and packets that are blocked by the firewall.