Firewall Approach to Internet Security: Firewall Architectures

www.s-w-r.com /Firewall/link5.html

Firewall Architectures

> *In this section we will see how firewall components described in section Firewall Components of this document can be combined together in various firewall architectures.*

Screening Router Architecture

> *In this architecture a firewall consists of nothing more than a screening router.*

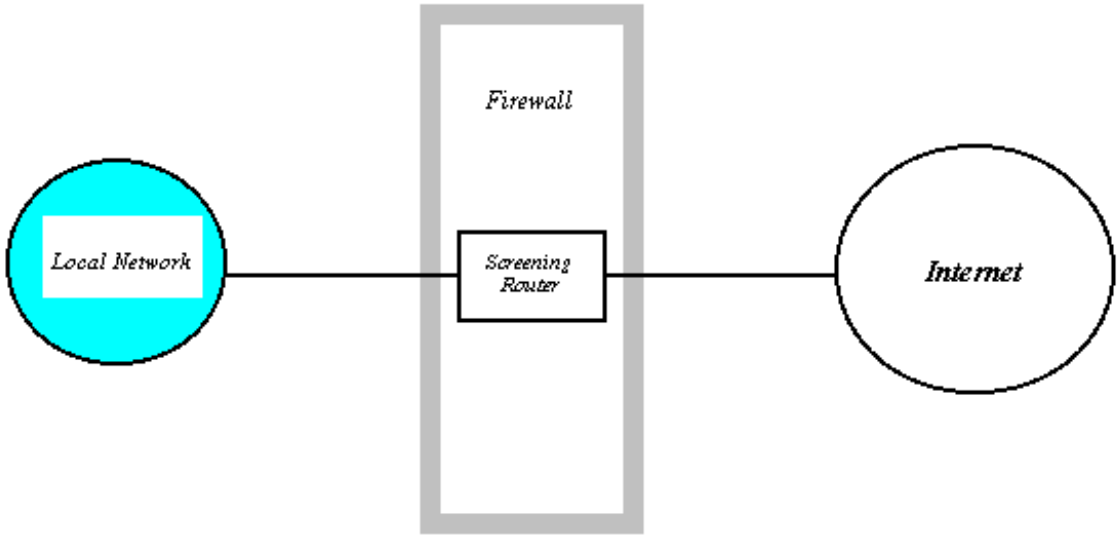


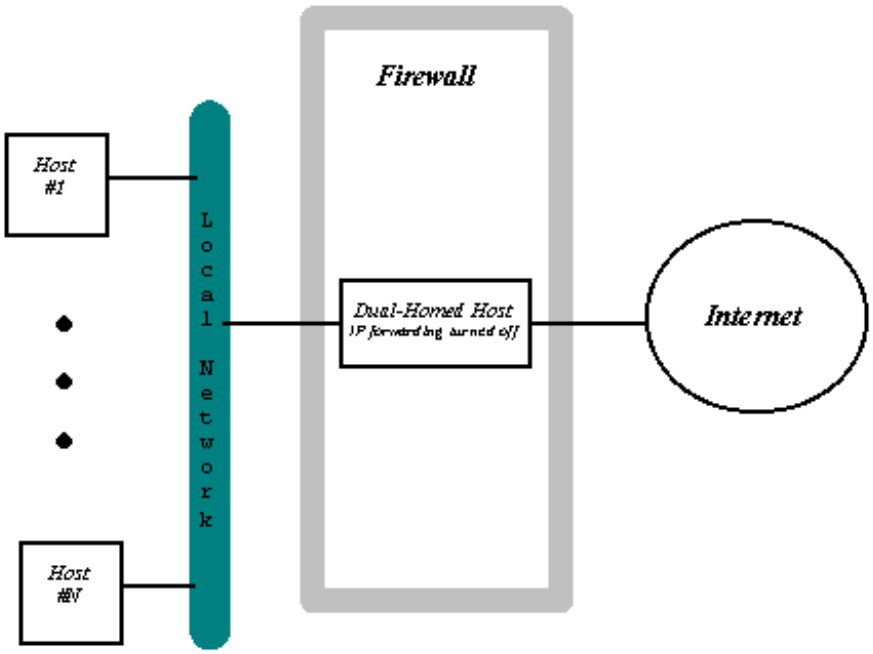
Figure 7: Screening Router Architecture.

Host on the Local Network and hosts on the Internet are allowed to communicate directly. The communication is restricted to the type that is allowed by a screening router. The security of the whole Local Network depends on the correct ACL of the router and on the amount of services permitted.

Dual-Homed Host Architecture

> *In this architecture a firewall consists of Dual-Homed Host machine (machine having two or more IP addresses each for specific physical port). One port of the machine connects to the Local Network and the other port/ports connects to the Internet. The IP datagram forwarding is turned off on the Dual-Homed Host machine, thus there is no direct TCP/IP connection between the Local Network and the Internet.*

Figure 8: Dual-Homed Host Architecture.



You permit communication between Local Network and the Internet in either of two ways:

1. *Users on the Local Network are given accounts on the Dual-Homed Host machine. In order to use Internet services the must rlogin on the Dual-Homed Host machine. The fact that you allow accounts on the machine weakens its security greatly (it now depends on each user and user that have access to it, more correctly it depends on the users' ability to choose "strong" passwords). Once the outsider succeeds to rlogin on the Dual-Homed Host machine he/she can access the entire Local Network.*
2. *Dual-Homed Host runs proxy program for each service you want to permit, thus there is no more need for users to rlogin to the machine in order to access the Internet. They can communicate via proxy software.*

The only host that can be accessed and thus attacked from the Internet is the Dual-Homed host machine. Thus it must have much greater level of security than the ordinary host on the Local Network. The excessive logging and auditing of system state must be performed, only secure software and necessary software installed and so on.

This architecture is much more secure than the Screening Router Architecture. But still once the Dual-Homed Host is subverted the entire Local Network is vulnerable to attack.

Screened Host Architecture

This architecture consists of the Screening Router and Screened Host.

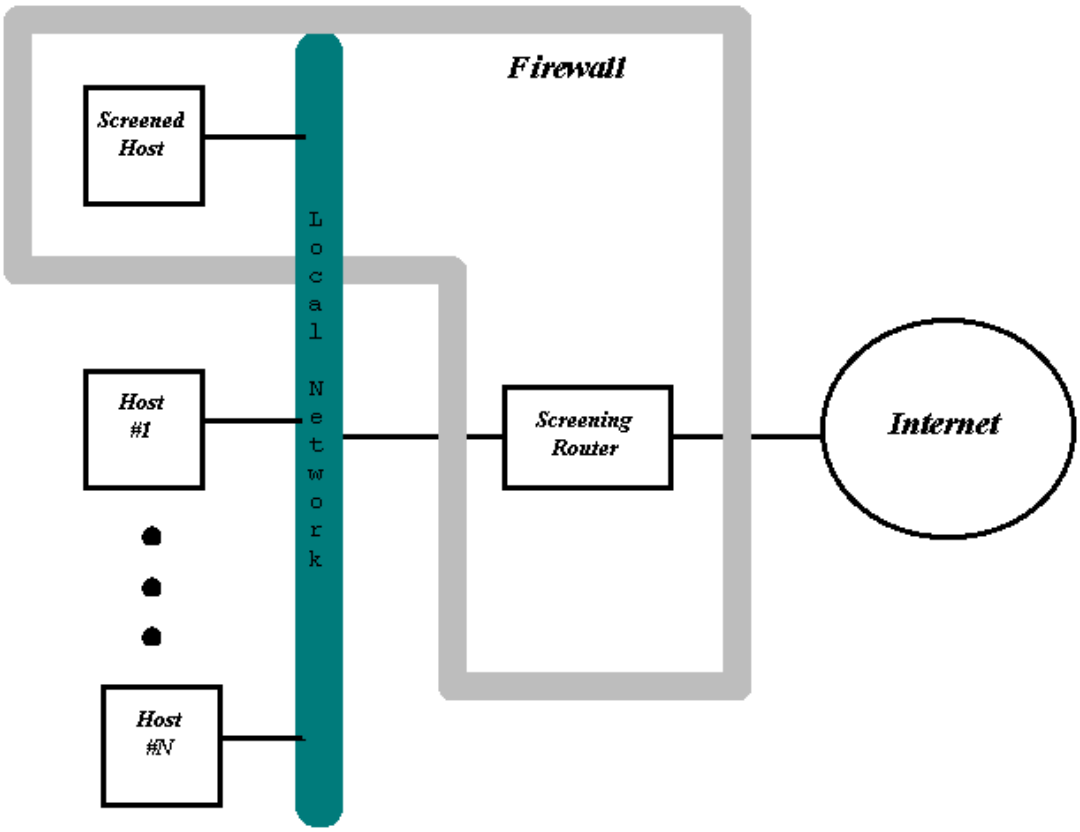


Figure 9: Screened Host Architecture.

Screening Router is placed between the Local Network and the Internet and its role is to block all the traffic between those two networks but the one that originates on the Internet and goes to the Screened Host or the one that originates on the Screened Host and destined for the Internet. That is Screening Router stops all the attempts to setup direct communication between ordinary host on the Local Network and the host on the Internet.

Screened Host is the host on the Local Network. It is the only host on the Local Network that can be accessed from the Internet and usually will run proxy programs for the allowed services. The other hosts on the Local Network must communicate with the Internet through proxy servers located on the Screened Host.

This architecture is more flexible than that of Dual-Homed Host with proxy services,because some secure services for which proxy software does not exist can be allowed to pass through Screening Router directly to a host on the Local Network.

Screened Host is also the only host that is subject to attack on an initial attempt. Thus an extra attention is paid to its security (because of this fact it is sometimes called in the literature "Bastion Host"). Once the Screened Host is subverted the attackers have access to all the hosts on the Local Network.

Screened Subnet Architecture

This architecture consists of the Screening Routers and Screened Hosts combined in such a way that when one of Screened Hosts is subverted the Local Network is not automatically open for an attack. In the figure bellow the Screened Subnet Architecture is shown using two Screening Routers and one Screened Host.

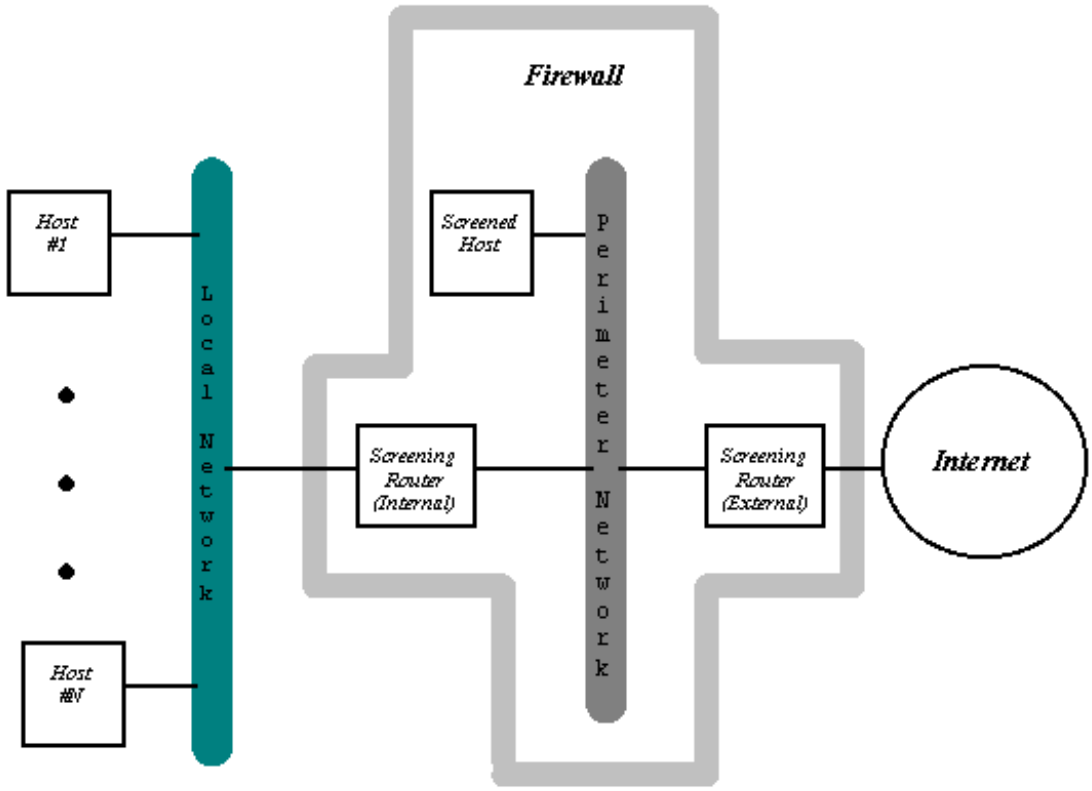


Figure 10: Screened Subnet Architecture.

What are the differences from the Screened Host Architecture?

1. *Screened Host is placed on the different physical segment than other hosts on the Local Network. Suppose that Screened Host is subverted. If it was connected to the same physical segment as other hosts in many network technologies it could to sniff all the traffic passing on the segment.*
2. *Local Network is guarded from the Screened Host by additional Screening Router. Thus in order to attack Local Network the attacker must pass through this additional router.*