

Screened Host / Subnet

(dmz)

A’merAshraf

# Screened Host

A screened host firewall architecture uses a host (called a bastion host) to which all outside hosts connect, rather than allowing direct connection to other, less secure, internal hosts. To achieve this, a filtering router is configured so that all connections to the internal network from the outside network are directed toward the bastion host.

**Tip:** If a packet-filtering gateway is to be deployed, then a bastion host should be set up so that all connections from the outside network go through the bastion host to prevent a direct Internet connection between the organization's network and the outside world

Screened Subnet

The screened subnet architecture is essentially the same as the screened host architecture, but the screened subnet architecture adds an extra stratum of security by creating a network in which the bastion host resides (often called a perimeter network), which is separated from the internal network.

**Tip:** A screened subnet should be deployed by adding a perimeter network to separate the internal network from the external. This ensures that if there is a successful attack on the bastion host, the attacker is restricted to the perimeter network by the screening router that is connected between the internal and the perimeter network

Proxy (When Use As Screened Host Firewall)

There are two types of screened host-one is single homed bastion host and the other one is dual homed bastion host. In this case we use single homed bastion host the firewall system consists of a packet filtering router and a bastion host. A bastion host is basically a single computer with high security configuration, which has the following characteristics:

Traffic from the Internet can only reach the bastion host; they cannot reach the internal network.

Traffic having the IP address of the bastion host can only go to the Internet. No traffic from the internal network can go to the Internet.

This type of configuration can have a web server placed in between the router and the bastion host in order to allow the public to access the server from the Internet. The main problem with the single homed bastion host is that if the packet filter route gets compromised then the entire network will be compromised.

Proxy (When Use As Screened Subnet Firewall)

This is one of the most secured firewall configurations. In this configuration, two packet filtering routers are used and the bastion host is positioned in between the two routers. In a typical case, both the Internet and the internal users have access to the screened subnet, but the traffic flow between the two subnets (one is from bastion host to the internal network and the other is the sub-network between the two routers) is blocked

Internal Router

The interior router (sometimes called the choke router in firewalls literature) protects the internal network both from the Internet and from the perimeter net.

The interior router does most of the packet filtering for your firewall. It allows selected services outbound from the internal net to the Internet. These services are the services your site can safely support and safely provide using packet filtering rather than proxies. (Your site needs to establish its own definition of what "safe" means. You'll have to consider your own needs, capabilities, and constraints. There is no one answer for all sites.) The services you allow might include outgoing HTTP, Telnet, FTP, and others, as appropriate for your own needs and concerns. (For detailed information on how you can use packet filtering to control these services

The services the interior router allows between your bastion host (on the perimeter net itself) and your internal net are not necessarily the same services the interior router allows between the Internet and your internal net. The reason for limiting the services between the bastion host and the internal network is to reduce the number of machines (and the number of services on those machines) that can be attacked from the bastion host, should it be compromised.

You should limit the services allowed between the bastion host and the internal net to just those that are actually needed, such as SMTP (so the bastion host can forward incoming email), DNS (so the bastion host can answer questions from internal machines, or ask them, depending on your configuration), and so on. You should further limit services, to the extent possible, by allowing them only to or from particular internal hosts; for example, SMTP might be limited only to connections between the bastion host and your internal mail server or servers. Pay careful attention to the security of those remaining internal hosts and services that can be contacted by the bastion host, because those hosts and services will be what an attacker goes after -- indeed, will be all the attacker can go after -- if the attacker manages to break in to your bastion host

External Router

In theory, the exterior router (sometimes called the access router in firewalls literature) protects both the perimeter net and the internal net from the Internet. In practice, exterior routers tend to allow almost anything outbound from the perimeter net, and they generally do very little packet filtering. The packet filtering rules to protect internal machines would need to be essentially the same on both the interior router and the exterior router; if there's an error in the rules that allows access to an attacker, the error will probably be present on both routers.

Frequently, the exterior router is provided by an external group (for example, your Internet provider), and your access to it may be limited. An external group that's maintaining a router will probably be willing to put in a few general packet filtering rules but won't want to maintain a complicated or frequently changing rule set. You also may not trust them as much as you trust your own routers. If the router breaks and they install a new one, are they going to remember to reinstall the filters? Are they even going to bother to mention that they replaced the router so that you know to check?

The only packet filtering rules that are really special on the exterior router are those that protect the machines on the perimeter net (that is, the bastion hosts and the internal router). Generally, however, not much protection is necessary, because the hosts on the perimeter net are protected primarily through host security (although redundancy never hurts).

The rest of the rules that you could put on the exterior router are duplicates of the rules on the interior router. These are the rules that prevent insecure traffic from going between internal hosts and the Internet. To support proxy services, where the interior router will let the internal hosts send some protocols as long as they are talking to the bastion host, the exterior router could let those protocols through as long as they are coming from the bastion host. These rules are desirable for an extra level of security, but they're theoretically blocking only packets that can't exist because they've already been blocked by the interior router. If they do exist, either the interior router has failed, or somebody has connected an unexpected host to the perimeter network.

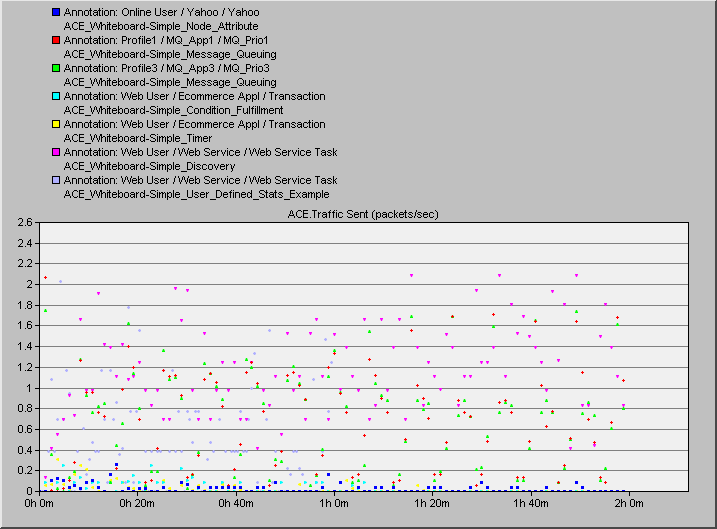
So, what does the exterior router actually need to do? One of the security tasks that the exterior router can usefully perform -- a task that usually can't easily be done anywhere else -- is the blocking of any incoming packets from the Internet that have forged source addresses. Such packets claim to have come from within the internal network but actually are coming in from the Internet.

The interior router could do this, but it can't tell if packets that claim to be from the perimeter net are forged. While the perimeter net shouldn't have anything fully trusted on it, it's still going to be more trusted than the external universe; being able to forge packets from it will give an attacker most of the benefits of compromising the bastion host. The exterior router is at a clearer boundary. The interior router also can't protect the systems on the perimeter net against forged packets.

Another task that the exterior router can perform is to prevent IP packets containing inappropriate source addresses from leaving your network. All traffic leaving your network should come from one of your source addresses. If not, then either you have a serious configuration problem, or somebody is forging source addresses.

Although filtering inappropriate source addresses outbound doesn't provide any network protection to you, it prevents an intruder from using your systems to launch certain types of attacks on other sites. If the exterior router is configured to alert you when forged source addresses are seen, this may be just the early warning alarm you need in order to detect a serious network problem. The practice of being a good network citizen may also be enough to keep the name of your site out of a possibly embarrassing news headline

|  |  |  |  |
| --- | --- | --- | --- |
| Qty | Component | Actual Name | Role |
| 1 | Ip\_32\_cloud | Internet | Send packet to Router |
| 1 | Application config | Application config | Configure files ,server processes and operating system settings |
| 1 | Profile config | Profile config | Distribute configuration information and large number of devices |
| 1 | Ip Attribute config | Ip Attribute config | Display all current TCP/IP network configuration values |
| 2 | Ethernet4\_slip8\_gtwy | Router | Connect and filter some packets between switch and ip |
| 1 | Ethernet2\_slip8\_firewall | Proxy | Control packets and protect network |
| 2 | Ethernet16\_Swith | Switch | Distribute packets and internet to Servers and Stations |
| 4 | Sm\_int\_wkstn | Station | Use internet and send packets back to switch |
| 3 | Sm\_int\_server | Server | Establish protocols and contained databases of network |

Results

