

HOWTO - Secure Networks Connected to the Internet

Jonathan Marks

jm (at) cmex (dot) org

\$id:\$

This document offers some insight into the options and tradeoff of some topologies for securely linking networks to the internet.

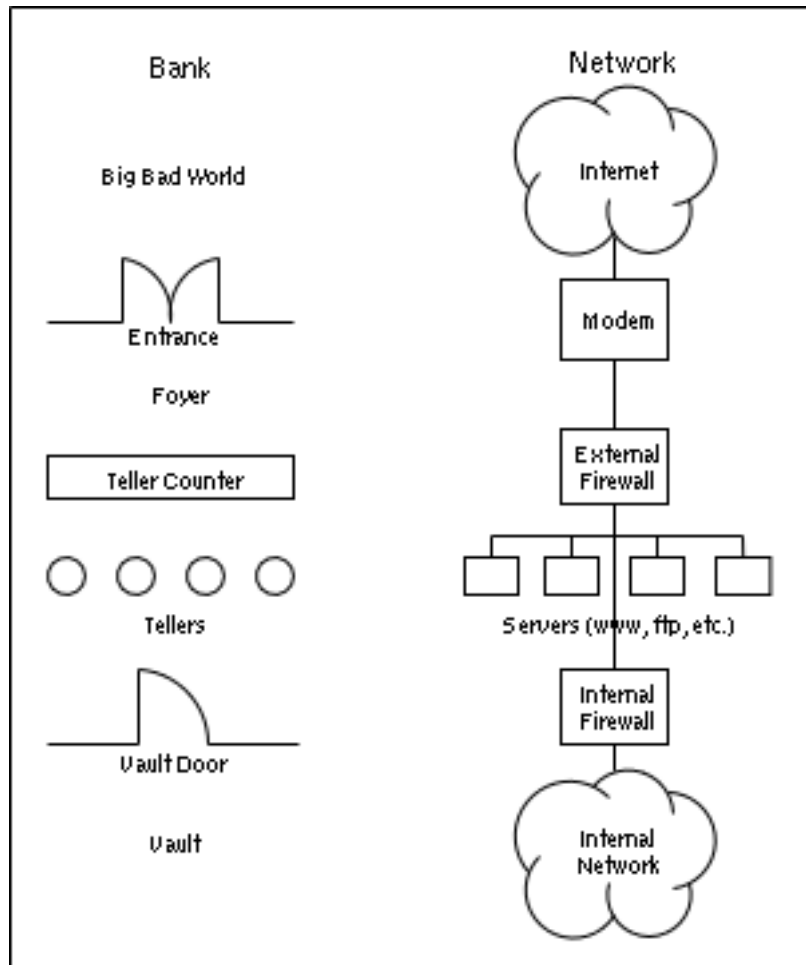
Table of Contents

1. A Secure (Series Firewall) Topology	2
1.1. Pro's and Con's.....	3
2. Other Less secure Topologies.....	3
2.1. Single Firewall Topology	3
2.2. Parallel Firewall Topology	4

1. A Secure (Series Firewall) Topology

There are many parallels between securing a bank and securing a network; it is useful to keep this analogy in mind, as illustrated in Fig 1. below.

Figure 1. Network Bank Analogy



In much the same way as anybody can enter a bank through its entrance, packets of data destined for the network's external address arrive at the modem. The modem can be dial up, ADSL, cable, ISDN, etc., etc..

From a security perspective, a bank's first line of defense is its Teller Counter. Tellers behind the counter serve the customers, much like http, ftp, etc., servers can serve the requests arriving in the packets of data. The teller counter offers a barrier, blocking unauthorized personnel from getting behind the counter. Similarly, data packets with no business behind the external firewall are blocked at the external firewall.

Packets permitted behind the external firewall that are not destined to a server, are destined to the internal network - for example, a response to an http request originating on the internal network coming back. In the bank example, only people authorized / permitted to go to the vault can do so.

Access to the vault (where the gold, money and jewels are kept) offers higher security than the Teller counter. This is no different in this network topology where the internal firewall provides a tighter level of security to data packets attempting to enter the internal network.

The network connecting the servers between the internal and external firewalls is often referred to as a perimeter network, peripheral network or "Demilitarized Zone" (DMZ). The servers located in this DMZ are referred to as Bastion Hosts. Some Terminology

1.1. Pro's and Con's

This a preferred topology as it provides two levels of defense to anyone attempting to break in. That is a perpetrator has to break through two firewalls to get to the internal network. The disadvantage is that two firewall boxes are required and need to be configured and maintained.

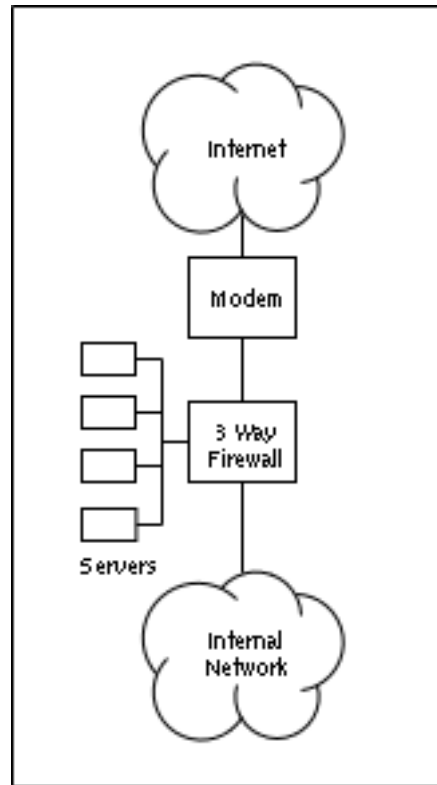
With this topology, a further level of security is provided by configuring the Bastion host server's to only accept packets on the port's of the content they are serving. For example a web server can only accept packets on port 80 from the external firewall. The server is configured to disallow all other packets from the external firewall. The servers are configured to only accept ssh access from the internal firewall, and only for one specific user. This way if a perpetrator has broken into the external firewall, the network is vulnerable to communications disruption, but the perpetrator has to break into the internal firewall before being able to attempt to gain shell access to any of the servers. It still affords authorized personnel to remotely gain access to the network by first connecting to the external firewall, then the internal firewall, before connecting to the server.

2. Other Less secure Topologies

2.1. Single Firewall Topology

This topology involves configuring a single three way router connecting to the internet, perimeter network and internal network as illustrated below.

Figure 2. Single 3 Way Firewall Configuration

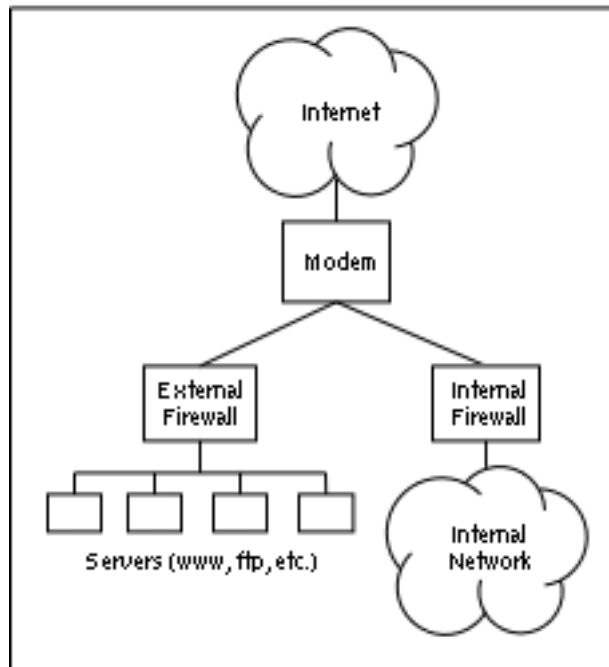


With a single router configuration, breaking into the router gives access directly to both the perimeter and internal networks.

2.2. Parallel Firewall Topology

This topology has the internal firewall of Figure 1 connect directly to the modem in parallel to the external firewall, as illustrated below.

Figure 3. Parallel Firewall Configuration



This configuration is a little more secure than the single 3 Way Firewall, as there are two physically separate firewalls. However if one of these firewalls is broken into, the whole network behind the firewall is vulnerable.