The mail forwarder is likewise configured to forward messages destined for the Intranet to the internal mail server[18]. It is this mail forwarder that is advertised via the Domain Name Server (DNS) as the mail server for the organization. Mail sent from the Internet to the organization will be received by the mail forwarder and subsequently sent to the internal mail server. Content checking such as virus scanning should be performed in the DMZ and the mail forwarder should be made as secure as possible by applying the applicable OS guidelines and disabling all unnecessary services.

Any time e-mail from an untrusted source is allowed into an organization there is a risk that an attacker can take advantage of that path. The advantages of this approach are in its simplicity. Full e-mail connectivity is provided with minimal additional hardware and the impact to the firewall rule set is very limited – only the SMTP port has to be opened. Additional benefit is derived from the fact that the mail forwarder offers an excellent place to focus malicious code countermeasures; however, it should be noted that this can not be a replacement for malicious code countermeasures on the client machines as encrypted messages can not be effectively scanned in transit. Finally, the option of reader-writer encryption is preserved with this solution through the use of S/MIME.

The disadvantage of this approach is that is strictly intended to allow internal users to send and receive mail to/from the Internet or other external network. It does not provide a means for users to access their Exchange mail store from the external network as might be required, for example, to support users who are traveling.

Solution 2 – Front-end/Back-end Servers

The second solution deals with a scenario where it is necessary to give users access to the Exchange environment from an external network such as the Internet. This situation could arise in support of employees who are traveling or to support an external partner, for example.

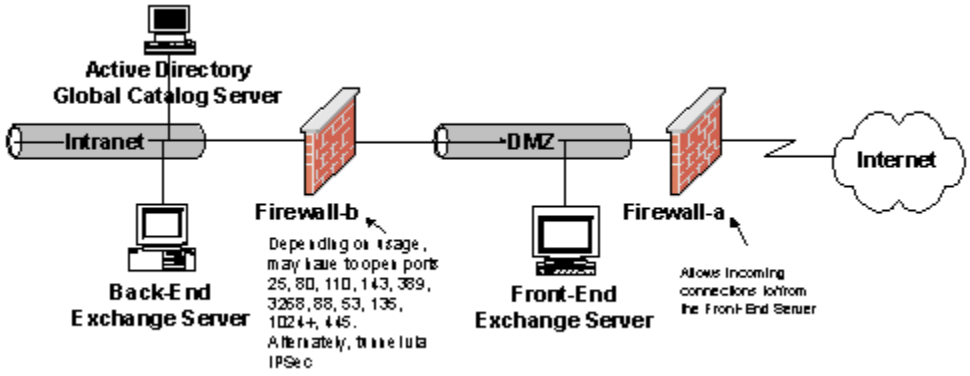

Figure 64. Front-end/Back-end Servers

The basic tenet of this solution is the concept of a back-end, front-end server. Microsoft has provided this capability in Exchange 2000 primarily as a means of loading sharing tasks between Exchange Servers. Under this architecture users can connect via POP3, IMAP4, or HTTP to a front-end server. This front-end server does not hold any mail accounts but simply forwards the request to the Exchange server where the users mail folders and public folders reside. It determines which Exchange server to forward the request based upon an Active Directory query.

[18] The mail forwarder could be another Exchange server or any of a number of other SMTP servers.