This architecture can be implemented with the front-end server placed within the DMZ in order to offer the internal network a measure of protection. This would allow external users to connect to the front-end server from the external network with the request forwarded to an internal back-end Exchange server. SSL can be used between the front-end server and the user to protect the data in transit. This architecture is illustrated in Figure 64 and is described in detail in a Microsoft white paper, *Exchange 2000 Front-end and Back-end Topology,* available at http://www.microsoft.com/exchange/techinfo.

The advantage of this solution is that it gives users more complete access to the Exchange environment than was available under the mail forwarder solution. Users can send and receive mail and, if using Outlook Web Access, access their calendars. This solution has a very notable drawback in that it requires the opening of a large number of ports on the internal firewall (firewall-b). If an attacker compromised the DMZ, this could place the internal network in jeopardy. This solution is generally not recommended if sensitive data exists on the internal network, but as always a final decision in this regard would be under the purview of local authorities.

Solution 3 – Terminal Server

Microsoft Terminal Server offers an interesting mechanism for extending the Exchange environment in a more secure manner. Terminal Server allows users to log into a Windows 2000 server and to execute their desktop on that machine. Only mouse movements and keyboard entries are sent from the client machine to the Terminal Server and only screen refreshes are returned – all execution occurs on the Terminal Server computer.

This ability to restrict where the user is executing programs can be used to reduce the risk of the extending the Exchange environment outside of the trusted network. In this example, users on the internal network log into a terminal server machine in the DMZ to execute their mail clients. The mail client executes exclusively on the terminal server

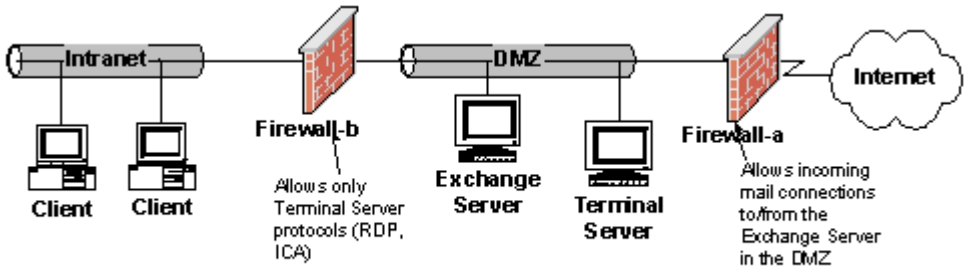

Figure 65. Terminal Server Solution

computer with only screen refreshes being passed back to the client machine. While malicious code could still do damage to the terminal server computers and the data that resides on them, if the firewall is sound damage should be limited to the DMZ. Also, it is administratively easier to concentrate countermeasures on the terminal server machines vice having to apply them to a plethora of client machines. The figure below outlines the concept. Note that the firewall between the terminal server and the user workstations (firewall-b) only allows terminal server protocols to pass. These are the protocols necessary for screen refreshes to pass to the client. By blocking all other protocols, any malicious code is limited in its potential "reach" to the terminal server computers where countermeasures could be strenuously applied. As is always the case when configuring

a DMZ, the computers within the DMZ should not be part of any internal Windows domain.

Access to users on the external network (Internet) can be granted by allowing them to connect to the Terminal Server via Firewall-a. This would allow roaming users complete access to Exchange data including their calendars, to-do lists, and etc.

This approach has several advantages. First, it can be scaled to simply allow internal users to share e-mail with users on the Internet or it can be used as a way of supporting users who need access to the Exchange environment from the external network. Second, when used in conjunction with a sound firewall policy it restricts the ability of malicious code to compromise data on the internal network. Finally, having all e-mail execute within a fixed number of terminal server machines can reduce the administrative burden of applying malicious code countermeasures.

There is one notable disadvantage. Under this scenario all Exchange data is stored in the DMZ and would be subject to compromise in the event that the DMZ is successfully attacked. If this is a concern the risk can be mitigated by giving users two Exchange accounts – one which resides in the DMZ and reserved for non-sensitive data and another on the Internal network which would be used for data requiring greater protection.

The use of the Terminal Server solution has it's own unique set of security concerns; reference NSA Guide, *Guide to Securing Microsoft Windows 2000 Terminal Services*.

Solution 4 – Remote Access

The Remote Access Service (RAS) can be used to allow users to dial into the network and obtain complete access to the internal network. This kind of access should not be used unless absolutely required for operational reasons; however, if remote access is required there is information available on securely connecting to networks using the Remote Access Security Program (RASP) which can use devices such as FORTEZZA modems for dialing into networks. More information on this technology is available at http://ias.itserealm.com/rasp.

Important Security Points

Consider that extending the Exchange Environment cannot be accomplished without increased security risk. One should weigh the operational benefits verses the risk carefully before proceeding.

Consider the use of a mail forwarder or terminal server architecture if it is necessary for users to send mail to/from the Internet.

Consider the use of a terminal server architecture if it is necessary to extend the Exchange environment so those external users have full connectivity to their message store. A front-end, back-end architecture or dial-in access can be used as well but is generally not preferred.