Global Information Assurance Certification Paper

Security Issues For Exchange 2000 Outlook Web Access Implementation
Name: Paula Kohrt
GSEC Practical Assignment Version 1.4b

Abstract
The purpose of this paper is to cover the fundamental security considerations during the implementation of an Exchange 2000 Outlook Web Access (OWA) Front End (FE) server in a demilitarized zone (DMZ) using secure HTTP access. In my own personal research I was unable to find one comprehensive document that covers the various aspects for this implementation. I have consolidated what I consider to be important steps along with some tips for securing an OWA FE server in a DMZ to provide outside access of email to internal users.

The following topics will be covered in this document: establishing and enforcing a strong password policy, implementing a comprehensive virus protection program, keeping service packs and security patches up to date, eliminating unnecessary services and setting permissions properly, determining the type of web presence desired, and finally opening only the minimum required ports on the firewall. The goal of this document is to provide system administrators with the basic points they need to consider when securing their OWA 2000 FE server to minimize the risk of providing secure HTTP access to their users. This document was written for administrators with a basic level of experience on firewall configuration, Windows 2000, IIS, and Exchange 2000.

Establish and Enforce A Strong Password Policy
Before any server is exposed to the Internet that relies on usernames and passwords for access, you as the system administrator, need to make sure that you protect your users from themselves. One of the largest problems in my organization is the lack of understanding that my users have on password compromise and the potential ramifications. The majority of users do not think about how easy it is to pick up their keyboard and read the password they wrote on the sticky note underneath it. They think nothing of letting someone else use their computer under their logon, and they often do not think twice about leaving their password for a substitute. I just had to go through the painful process of getting approval and implementing the first mandatory password change policy throughout my organization to eliminate numerous security threats I inherited when I took this job. In my environment the biggest threat to security is password compromise from my internal users.

The fortunate thing about Windows 2000 is that there are many features and tools available to implement and correct password problems. You can use the Group Policy editor snap-in at the domain level to enforce password complexity requirements, set maximum password age, minimum password age, minimum password length, enforce password history, and set account lockout policies. There is a fine balancing act when determining what level of security your environment needs without going too far. If your users have to write their

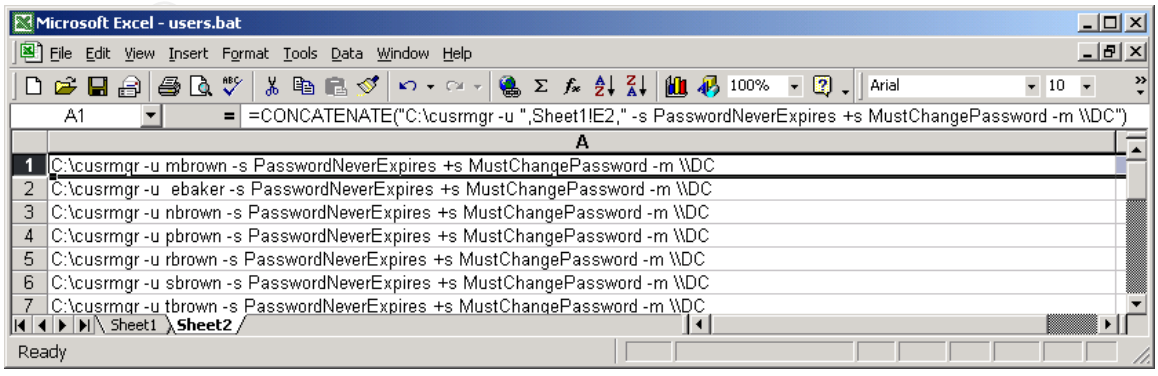
passwords down because you implemented an impossible password policy, you went overboard. It is also not enough to simply set a minimum password length, you must set a maximum password age to force routine password changes and then you must also enforce the password history and minimum password age policies to prevent users from repeatedly resetting their passwords in an effort to get back to one they like [1].

One of the areas often overlooked when implementing a password policy is follow up by the system administrator. If you didn't build the network from the ground up, how do you know that everyone is being forced to change his or her password? Do you really know if anyone set the password never expires option on any accounts? You need to know because it will prevent your group policy and password changes from being enforced on those accounts.

With the Windows NT 4 usermanager you could select multiple accounts at one time and implement changes on the password attributes with a few mouse clicks. This is no longer the case in Windows 2000. If you have created an organizational unit (OU) structure that reflects your user environment then it is a relatively easy process to do with a Windows 2000 Resource Kit tool called cusrmgr. You can use the Active Directory Users and Computers snap-in to select each individual OU containing users, right mouse click on it to run the Export List command and save the results to a tab delimited text file. Before you export the users you must change the view to include the Pre-Windows 2000 Logon Name column. You can then use Excel to import the text file as tab delimited. Insert a new worksheet in Excel and add the following command:

=CONCATENATE("C:\cusrmgr -u ",Sheet1!E1," -s PasswordNeverExpires +s MustChangePassword -m \\DC")

- This example assumes the location of the cusrmgr.exe is at the root of the C drive, that on Sheet1 the values in the E column correspond to the Pre-Windows 2000 Logon Name column (you will use the fill handle to populate this formula to the number of rows that correspond to the number of users on Sheet1), you want to remove the Password Never Expires attribute, you want to force the user to change their password at the next logon, and you need to substitute the name of a Domain Controller for the variable DC



The final step in Excel is to save Sheet2 with a filename such as user.bat and as file type MS-DOS text file under the File Save As menu. This will create the batch file you run to change the password attributes on the user accounts. Make sure your domain controller can communicate with the machine you run this file on and that the account you use has the appropriate administrator privileges.

If you need to implement controlled password changes simply rewrite the command to suit your needs. I had to implement passwords changes for 21 geographically separate sites so I needed to phase in password changes location by location for supportability reasons. When you have users that have never been forced to change their passwords you should not make them all change their passwords on the same day unless you have unlimited support resources and love to work long hours dealing with angry users. I needed to remove the User Cannot Change Password attribute and I also needed to make sure every account had the Password Never Expires attribute set before I used Group Policy to apply the new password rules. This was done so password changes could be forced to occur in a controlled manner after the users were trained. Since each OU in my Active Directory was broken out by site it was a fairly easy process to export user accounts into text files named by the site. Once I imported the data into Excel, I used the following command in the spreadsheet to accomplish this task:

=CONCATENATE("C\cusrmgr -u ",Sheet1!E1," +s PasswordNeverExpires -s CanNotChangePassword -m \\DC")

I followed the same steps I mentioned in the first example to save this as a batch file and executed it for each site. The group policy was then applied to enforce password changes. Once the schedule of dates and password change instructions were distributed I ran the batch files created by the first example and forced users to change their passwords on a site-by-site basis. The following link contains the syntax for the cusrmgr command:

http://www.tburke.net/info/reskittools/topics/cusrmgr_syntax.htm

One of the most important things you must do when implementing a drastic security policy change is to prepare your users by communicating with them. Let them know why the policy change is necessary, when the change will occur, and also educate them on how the change impacts them.

Implement a Comprehensive Virus Protection Program

In my organization, the majority of the viruses attempt to come in via the email system, the second highest percentage are carried in on floppy disks by users, and the smallest percentage come from infected web sites. By making the OWA client available to your users from any browser you will see a larger volume of virus problems. This is due to the fact that you cannot control what users do on their home computers and the majority of home users do not keep their virus

software up to date and most do not even have any installed [2]. It is crucial that all of your Exchange servers have virus protection software, your Windows 2000 servers are protected, and you consider whether or not you want to take the extra precaution to limit the type of attachments you will allow your email system to accept. Some very extreme system administrators exist who only allow text based emails into their system but this type of policy is unrealistic and defeats the features built into an Exchange server environment. According to an Osterman Research Survey "76 percent of organizations block some attachments and fewer than 2 percent block all attachments." [3]

I use a product called NeaTSuite for Microsoft Exchange by Trend Micro, which contains Exchange ScanMail to protect the Exchange servers, ServerProtect to protect the Windows 2000 servers, Interscan VirusWall to scan gateway traffic, and OfficeScan to protect the desktops [4]. I also block the following types of attachments from coming in via email:

> Attachments with specified extensions
> ASF;BAT;CHM;COM;EXE;HLP;HTA;HTO;JS;JSE;LNK;PIF;REG;SCR;SHB;SHS;SWF;VB;VBE;VBS;WSC;WSF;WSH;
>
> Attachments with specific names
> win5a.*;music_1.htm;

Some administrators do not believe in "putting all their eggs in one basket" and choose to select individual products from multiple vendors hoping that if a virus escapes one vendor's product that another vendor's product they have deployed in their environment will detect it before damage occurs. I prefer to stay with a suite for ease of management and pricing. I use the Trend Virus Console to centrally manage engine and pattern updates and deployments, receive email alerts about server update status, and to monitor virus statistics. The server was originally configured to check for updates once a week but I have changed it to check for updates every day due to the increase in virus activity.

Once you choose an antivirus product, make sure you have installed the latest engine and virus pattern. You also need to test it thoroughly after installing and configuring it. With a previous version of the Trend Micro ScanMail engine it was a well-known fact among the technicians that you could rename a banned file attachment to get it through the email server. Trend Micro has since updated the engine and renamed attachments can no longer pass through the system if the original extension is on the banned list. You also need to see what impact blocking file attachments will have on the existing user email stored on the servers before you deploy it. In some cases if you block attachments not previously blocked the anitvirus software will rescan the Information Store and quarantine or delete these attachments. You need to let your users know prior to implementing this change so they have time to save these attachments somewhere else.

Keep Service Packs and Security Patches Updated

In an Exchange 2000 environment you must ensure Windows 2000, IIS, and Exchange service packs and security patches are kept current and updated. You must also be cautious and realize that Microsoft does not always include all of the security patches in future service pack releases. Upon the installation of Windows 2000 Service Pack 3, the option to allow updates to automatically download but not install is selected by default. Scheduling automatic installs of updates often requires rebooting machines which is undesirable at many organizations. You would be placing machines at the mercy of any Microsoft updates posted and would not be able to give your users advance notice of service loss. Instead, most people are relying on the Software Update Service (SUS) from Microsoft. The URL for this free download is: http://www.microsoft.com/Windows2000/downloads/recommended/susserver/default.asp [5]. The biggest issue with these two approaches is that they only address the core operating system (OS) patches, and SUS only supplies critical updates or patches and cannot distribute service packs [6]. System administrators still have to find a way to track all of the security updates, not just the critical ones for the OS, and still have to keep track of IIS and Exchange updates. Microsoft's Systems Management Server 2.0 with the free SMS Value Pack supports all Microsoft products including service pack and update distribution [7]. There are also some third party products that can perform similar functions. The following URLs contain information about SMS and some of the other products available.

http://www.microsoft.com/smserver/evaluation/overview/secure.asp
http://www.stbernard.com/products/updateexpert/products_updateexpert.asp
http://www.securitybastion.com/
http://www.patchlink.com/media_room/nwc92002.pdf

I have not listed all of the products available and most of these products come with a fairly high price tag. If you are in a smaller organization and cannot afford to purchase one of the commercial update packages then you should at least be taking the steps to track your own server status:

1. Create a database to track servers, OS versions, and application software. There should be room to break out the service packs and critical updates for the OS, IIS, and any other applications installed (such as Exchange).
2. Subscribe to listservers for Windows security threats and research the recommended action. Microsoft has a security notification service you can sign up for but you should not rely on just their service for alerts and updates. Here is a list or URLs for some of the sites with alert services or information on security resources available:
   http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp
   http://www.cert.org/contact_cert/certmaillist.html

http://server2.sans.org/sansnews
http://www.parallaxresearch.com/news/advisories.html

3. Download tools to determine check the patch status of your machines. One tool available is the Microsoft Network Security Hotfix Checker. The URL for this tool is http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=34935A76-0B20-4F91-A0DE-BAAF969CED2B

Be proactive about staying on top of security issues so you don't get forced into a reactive damage control mode. This is truly a case where every administrator needs to be part of the solution and not part of the problem.

Eliminate Unnecessary Services and Set Permissions Properly

One of the most common security recommendations is to use dedicated servers to provide specific services. If you need an SMTP server, an Internet server, an OWA FE server, etc. try to use separate machines so security can be tightened as much as possible. You can disable all of the Exchange services on a dedicated OWA FE server if it does not perform any other Exchange function and is only used for providing secure HTTP access to email. I have compiled a list of some often overlooked steps to take to secure an Exchange 2000 OWA FE server. These steps assume that this server will only be used for HTTP access and it assumes all applicable service packs and security updates are installed up to Exchange Service Pack 3. The steps below contain information from Microsoft's white paper "Using Microsoft Exchange Front-End Servers" available at for download at URL: http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=AFAD8426-572E-40F8-99DA-EB7198F374C4 [9]

1. Install Exchange Enterprise as a Front End server by going into Exchange System Manager (ESM) and locating the server and displaying its properties. You will then select the "this is a front-end server" option.
2. Use Internet Service Manager (ISM) to apply 128 bit SSL to all of the subfolders in the Exchange Web directory.
3. Use ESM to turn on Basic Authentication for each Exchange virtual directory and then use ISM to set up a redirect to the secure OWA site. OWA FE servers only support Basic Authentication and this is why SSL is turned on in step 4 to reduce this risk and it will also be required for users to remotely change their passwords [8]. The ability to change passwords via to OWA client is turned off by default but the instructions are available at the following URL to turn this feature on: http://support.microsoft.com/default.aspx?scid=kb;en-us;267596
4. The "Log On Locally" right is no longer required for OWA 2000. Users only need the "Access this computer from the network" [10].
5. Use the IISLockdown tool version 2.1 available at the following URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp Version 2.1 includes templates for Exchange

2000, URLscan is included, and it can remove or disable unwanted IIS services. You should remove all unnecessary components such as IISSamples, IISHelp, sample virtual directories, remove all unused services such as FTP, Telnet, etc..

6. Disable the Windows File Protection and move the command line tools out of the \winnt\system32 directory and assign permissions only to the Administrators group or if you don't want to move the tools then restrict the permissions on this directory to the Administrators group and the System account [11].
7. Dismount the stores and disable the Exchange System Attendant and other related Exchange services such as the Microsoft Search service, the Routing Engine service, the Message Transfer Agent, and the Exchange Event service. The only time the Exchange System Attendant needs to be running is when you make a changes to the to Exchange Web directory. "For Exchange setup to run, you must install and enable (but not necessarily start) Network News Transfer Protocol (NNTP), SMTP, w3SVC and IIS Admin. If the MSExchange MTA, IMAP4, POP3, and MSExchangeIS services are disabled, Setup still runs; however, Setup will enable these services after it starts. After setup is complete you can disable unnecessary services."[9] Every time you service pack Exchange you will need to disable services again.

I want to stress one more time that the steps above are specifically for a secure HTTP implementation on an OWA 2000 FE server. If you want to also provide IMAP, POP3, and SMTP access then you will not be able to disable certain Exchange services.

Determine the Type of Web Presence Desired

The type of users you need to support will determine the need for an external certification authority source versus an internal certification authority. There are many things to consider when you make this decision. Do you want to support your own certificate server? What type of users do you need to support and where will they be trying to access their email? Do you want to register your server with a public name server? Is it more cost effective to purchase and maintain your own certificate server or is there a cheaper total cost of ownership by using a third party certification authority?

An external certification authority such as Verisign will allow you to provide secure connectivity to Internet users, will allow you to support access from Internet kiosks, and is supported by a large variety of browsers since the root certificate for Verisign is preinstalled in most browsers. However, it costs money to purchase a certificate from a third party certificate authority and your OWA server must be properly registered and resolvable by public DNS. The advantages are a larger range of client support because the root certificate is already installed in the browser, the fact that you do not have to make sure that

your certificate server is available 100 percent of the time, and your organization does not have to make the investment in hardware and support staff.

An internal certificate authority will allow you to provide secure access to users but can cause error messages about a certificate coming from an untrusted source. If you are only supporting internal users working from home locations or traveling with company computers you will be able to provide recommended minimum configurations for browsers and you can provide your users with instructions on how to preinstall your root certificate into their browsers. Refer to the article at URL http://support.microsoft.com/default.aspx?scid=kb;en-us;297681 for instructions on how to preinstall your certificate. You can also get by with only registering your OWA server on your private internal DNS as long as it can communicate with your certificate server. You still must have a public IP address to assign to the OWA server. If you already have a publicly registered Internet server you can establish an unadvertised link to your OWA server that will redirect your users to its assigned valid public IP address. By an unadvertised link, I mean one that is known to your internal users but not advertised on your Internet server home page. This can give an additional level of anonymity to your OWA server but it does not replace the final security step in this scenario and that is the function of the firewall.

Open Only the Required Ports on the Firewall

The purpose of a firewall is to provide a controlled level of access between the public network (Internet) and your private network. A DMZ is where you would place all of the servers with services that need to be made available to users on the public network. If you need to open ports to one server for a specific type of access then you open those ports to only that server and not the entire subnet reducing your security risks.

The following diagram identifies the ports and the direction of flow for this implementation. It is assumed that your firewall rule set allows outgoing established connections and has an implicit “deny all” for all other incoming ports.

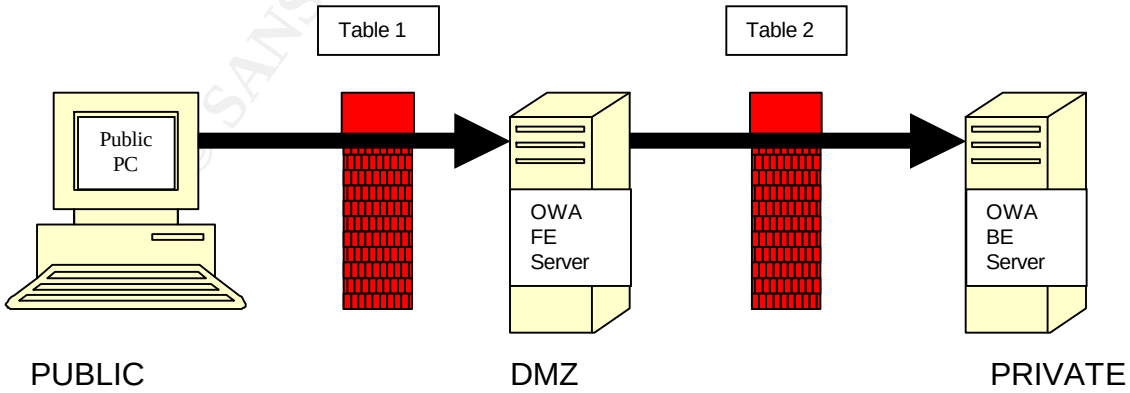


Table 1 – Ports to open from the Internet to the OWA server in the DMZ

Protocol	Port	Description
TCP	443	SSL for HTTP

Table 2 – Ports to open between OWA FE server and OWA BE server

Protocol	Port	Description
TCP	53	DNS
UDP	53	DNS
TCP	80	HTTP
TCP	88	Kerberos
UDP	88	Kerberos
TCP	389	LDAP
UDP	389	LDAP
TCP	1025	Statically set port for RPC, refer to Q224196
TCP	3268	Global Catalog

In Table 1, only port 443 is open to support SSL HTTP access. You can add TCP port 80 if you used ISM to redirect your users to the secure link. In Table 2, the above example shows the ports all open to only an OWA BE server, however, most environments do not run DNS, a Domain Controller, and Exchange on the same machine. You will have to adjust the firewall source and destination IP addresses based upon where the applicable servers with the corresponding services are placed in your private network. You could simply open all of these ports from your OWA FE server in the DMZ to all IP addresses on your private network but that is not the preferred or most secure method. If you have multiple OWA BE servers on your private network and have implemented a set range of IP addresses for those servers setting the rules for the firewall will be easier. It will also require less processing due to a smaller rule set. You will also notice the TCP port 135 is not included on this list and is explained in the following excerpt below:

"Some corporations that have deployed perimeter network topologies for other services have policies that restrict computers located within the perimeter network from initiating connections with servers inside the corporate intranet. A front-end server running Exchange is not supported in this configuration, because it must initiate connections.

Additionally, in this configuration, it is recommended that you completely configure the front-end server before the intranet firewall is put in place or locked down. Configuring settings on the front-end server in Exchange System Manager requires the System Attendant (MSExchangeSA) service to be running so that the configuration information can replicate to the metabase. The MSExchangeSA

service requires RPC access to the back-end servers, and RPCs often are not allowed across an intranet firewall in a perimeter network.

The DSAccess component in Exchange 2000 SP2 is redesigned to provide better support for perimeter networks in which RPC traffic is not allowed across the internal firewall. However, there are two additional registry keys that you should set on the front-end server to disable NetLogon and the Directory Access ping:

- **NetLogon** DSAccess connects to Active Directory servers to check available disk space, time synchronization, and replication participation by using NetLogon service with RPC. If you do not allow RPC traffic across the internal firewall, you should stop the NetLogon check by creating the DisableNetlogonCheck key on the front-end server.
- **Directory Access Ping** By default, Directory Access uses Internet Control Message Protocol (ICMP) to ping each server to determine whether the server is available. However, in a perimeter network, there is no ICMP connectivity between the server running Exchange and the domain controllers. Therefore, Directory Access determines that every domain controller is unavailable. Directory Access then discards old topologies and performs new topology discoveries, which impact server performance. To avoid these performance issues, you should turn off the Directory Access ping on the front-end server by creating the LdapKeepAliveSecs registry key for the Windows implementation of LDAP (wLDAP). " [12]

Microsoft recommends that the OWA FE server be installed before the firewall is locked down to the ports listed in Tables 1 and 2. I have included a quotation that I feel summarizes the overall purpose of this paper quite well:

"It is important to note that an Internet firewall is not just a router, a bastion host, or a combination of devices that provides security for a network. The firewall is part of an overall security policy that creates a perimeter defense designed to protect the information resources of the organization. This security policy must include published security guidelines to inform users of their responsibilities; corporate policies defining network access, service access, local and remote user authentication, dial-in and dial-out, disk and data encryption, and virus protection measures; and employee training. All potential points of network attack must be protected with the same level of network security. Setting up an Internet

firewall without a comprehensive security policy is like placing a steel door on a tent." [13]

There is a wide range of business, management, and policy decisions that have to be made along with the technical for network resource access. As system administrators, our goal should be to achieve the business goals in a secure and supportive manner without compromising our organization's infrastructure.

References:

[1] Ivens, Kathy. "Password Defense". September 2002. URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=25962&pg=1

[2] Leyden, John. "Home user insecurity spurs email virus growth in 2002." December 16, 2002. URL: http://www.theregister.co.uk/content/56/28585.html

[3] Osterman Research. "Osterman Research Survey on Email Content Filtering Issues". April 2002. URL: http://www.ostermanresearch.com/results/surveyresults_cf0402.htm

[4] Trend Micro. "NeaTSuite for Microsoft Exchange Overview". URL: http://www.trendmicro.com/en/products/suites/neatsuite-exchange/evaluate/overview.htm

[5] Dyck, Timothy. "Microsoft's Windows 2000 Service Pack 3 Rolls Out Trouble". August 19, 2002. URL: http://www.eweek.com/print_article/0,3668,a=30177,00.asp

[6] Stewart, James Michael. "Microsoft Makes Software Updates Simple". September 17, 2002. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2880514-1,00.html

[7] Stewart, James Michael. "Microsoft Makes Software Updates Simple – Limitations Not Fatal". September 17, 2002. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2880514-2,00.html

[8] McDonald, Barb. "SSL's Benefits on OWA". November 2000. URL: http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=15772

[9] Lemson, K.C. Martin, Michele. "Using Microsoft Exchange Front-End Servers". October 2002. URL: http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=AFAD8426-572E-40F8-99DA-EB7198F374C4

[10] Microsoft Knowledge Base Article – 311422. "XCCC: The "Log On Locally" Right Is Not Required For Outlook Web Access in Exchange 2000 Server". December 26, 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;311422

[11] McBee, Jim. "OWA 2000 Security and Scalability". January 2002. URL: http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=23139

[12]Microsoft Technet. "Microsoft Exchange 2000 Front-End and Back-End Topology. July 2002. URL: http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/maintain/optimize/e2kfront.asp?frame=true

[13] Yatsui, Hiroki. “Discussion of Internet Firewalls”. April 19, 1999. URL: http://www.fc.bus.emory.edu/~hiroki_yatsui/firewalls/003.htm