GIAC Certified Windows Security Administrator-(GCWN)
Practical Assignment
Version 4.0 Option 2

Enhancing E-mail Security using Exchange Server 2003 and Outlook 2003

Cheryl L. Jones

July 23, 2004

ABSTRACT: Over the past decade, email has become a vital form of communication for many organizations. It provides communication with multiple parties, more rapid communication, and written record of conversations, or documentation in legal situations. It is the most widely used collaborative technology used today. Without email systems, some businesses would cease to function. There are two main obstacles with email systems: maintaining them and keeping them secure. These can be very demanding tasks.

One technology, which offers the opportunity to accomplish this goal and increase enterprise security, is Microsoft Exchange Server 2003. Designed to function on the Windows Server 2003 platform, Exchange 2003 delivers greater security than previous versions of the software. There are many documents written on Exchange Server 2003. However, they aren't many documents that focus solely on the new security features in Exchange 2003. Most documentation focuses on how to migrate from previous versions of Exchange (5.5 or 2000), or provide a broader comprehensive overview of Exchange server administration, but fail to expand on the new security features found in Exchange Server 2003 and the security advantages they provide in one document. The goal of this document is to discuss the new security features found in Exchange Server 2003 and Outlook 2003. I will describe each new feature in detail, and provide graphic illustrations of how each new enhancement works in a Windows 2003 environment. Finally, I will also cover how security is increased with these new features in a Windows 2003 Server to prevent against vulnerabilities within an enterprise environment.

Introduction

There are many potential risks involving an email system including SPAM or UBE (Unsolicited bulk mail), vulnerabilities, exploits, and viruses. According to Microsoft, the Microsoft Exchange 2003 team performed a security audit during the development of the Exchange 2003 product. They examined Exchange components and performed a threat analysis for each possible security threat. As each threat appeared, they provided additional design and testing to try to combat some of the possible security risks. This resulted in the following server and client security features in Exchange 2003 (the server that manages the sending, receiving and storage of mail) and Outlook 2003 (provides the client with e-mail from the server) to help address these issues: restricting user access to the Exchange Server, disabling unnecessary services, enforcing message limits, restricting distribution lists to Authenticated Users, connection filtering, inbound recipient filtering, IPSec (Internet Protocol Security Protocol) on front-end and back-end clusters, anti-spoofing, Kerberos and Exchange 2003, Exchange Intelligent Message Filter, Information Rights Management, Kerberos and Outlook 2003,Anti-spam, restricting access to the Outlook Address Book , and IIS 6.0 Security and Dedicated Application Mode.

This document will provide information on each security enhancement and discuss how they function.

Part I. Exchange 2003 Security Enhancements

There are three key ingredients needed to successfully install an Exchange 2003 server. First, the Windows Server 2003 operating system needs to be installed. Second, IIS 6.0 needs to be installed. It is integrated in the Windows 2003 operating system, but is not installed by default like in previous systems. Third, the client or Outlook 2003 needs to be installed. It is integrated with Exchange 2003. Exchange 2003 is only as secure as the operating system it's running on because they work together. Exchange 2003 utilizes Active Directory for ease of administration. Administrative components are signed and sealed by default when using LDAP (Lightweight Directory Access Protocol) to communicate with Active Directory in Exchange 2003. This reduces the risk of "man-in-the-middle" attacks. User information and configuration, as well as information to deliver e-mail, process rules, and enforce quotas are stored in Active Directory.

The goal of security on Windows 2003 is to restrict the amount of access (least privileged) to both the server and application. The same principle applies for Exchange 2003. I would like to discuss the following email server security enhancements that are only found in this latest edition of Exchange: restricting user access to the Exchange Server, disabling unnecessary services, enforcing message limits, restricting distribution lists to Authenticated Users, connection filtering, Inbound recipient filtering, IPSec on front-end and back-end clusters, antispoofing, Kerberos and Exchange 2003, and Exchange Intelligent Message Filter.

Restricting Domain User Access to the Exchange Server

Whether an install, reinstall, or upgrade is performed to Exchange Server 2003, domain user logon is now disabled on the server by default. This has been enhanced from previous versions. In the case of an upgrade, the Exchange Server 2003 Setup local computer policy is configured to deny local access for Domain Users. Server Operators and local Administrators will still be able to log on locally. Why would Microsoft do this? It was done primarily to keep those people who aren't administrators from logging on the server even if they happen to have access physically or through Remote Desktop to the Exchange server. It provides ease of administration by reducing access to administrators in certain roles.

There are three Administrative roles that exist within Exchange Server 2003. They are Exchange Full Administrator, Exchange Administrator, and Exchange View Only Administrator. The Exchange Full Administrator has full control to manage Exchange objects throughout the entire enterprise with add, delete, and change permissions to objects. This role is not very restrictive at all. The “keys to the castle” are pretty much given as an Exchange Full Administrator. This administrator can control many sites and be the “ultimate” administrator. The Exchange Full Administrator role is required to install additional Exchange servers in the enterprise. The Exchange Full Administrator rights can be delegated to other administrators so that they can install Exchange servers at their location. This provides ease of management and gives the Exchange Full Administrator the authority to effectively organize and delegate responsibility throughout the enterprise. Also, this role has to be manually added to the local administrator group on the Exchange server.

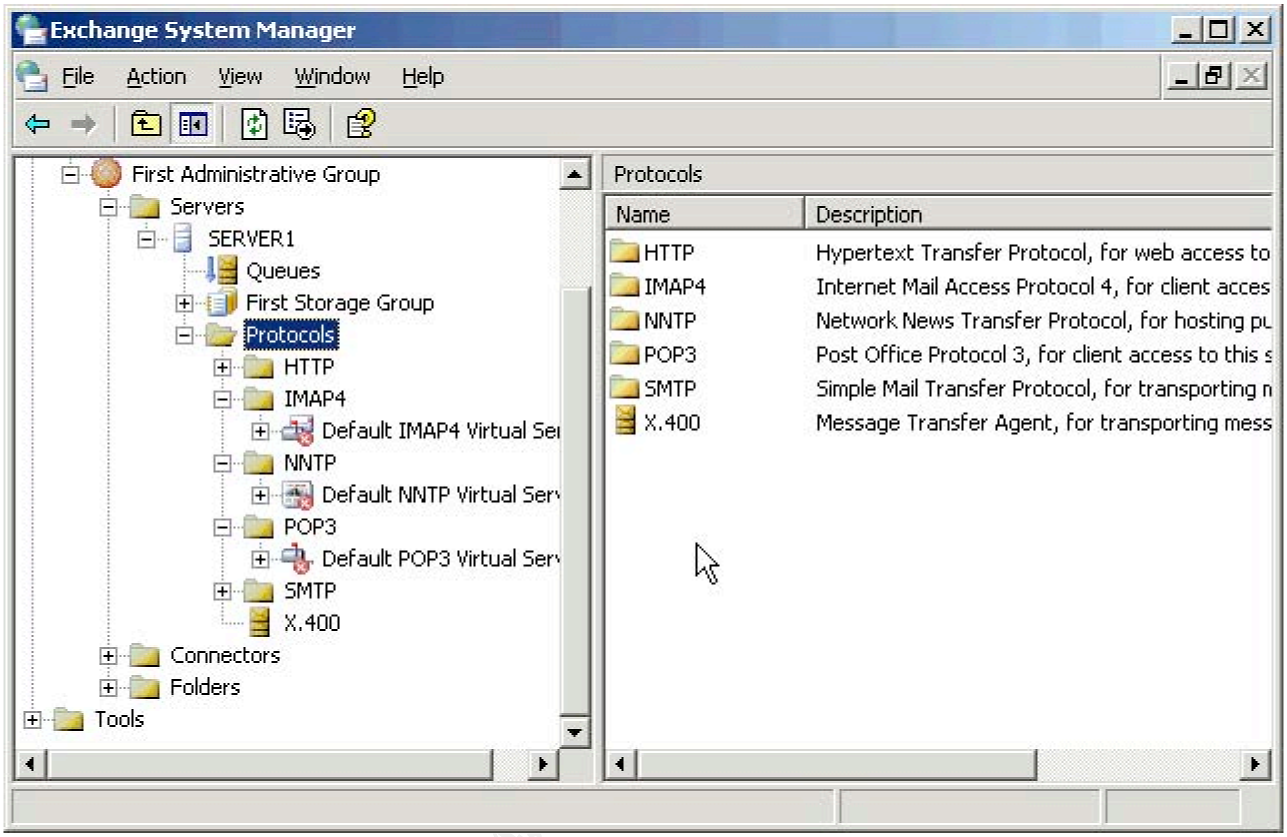
The Exchange Administrator role is designed for the day-to-day administrator and grants the ability to add, modify, or change objects. This day to day administrator cannot change permissions on the other two roles. The administrator for this role must also be placed in the local administrators group on the server.

The Exchange View Only Administrator is a very restrictive role and only allows the Exchange administrator to view objects. This role is used to restrict administrator rights between Exchange administrator groups.

Disable unnecessary services

In order to maintain the security of an Exchange Server 2003 environment, Microsoft has disabled all unnecessary services by default. In doing so, security is increased by limiting network interaction. The Microsoft Baseline Security Analyzer, available in Windows Server 2003, can scan the servers and look for additional unnecessary services that are still active. Addition services that are unnecessary clearly depend on the environment and configuration of the servers. However, Microsoft recommends that if a service isn’t needed by anything, it should be disabled. Disabling services frees up memory and resources to increase availability. It also helps prevent malicious attacks such as the viruses that rely on specific services being enabled.

The following four protocols available with Exchange Server 2003: Simple Mail Transfer Protocol (SMTP), Network News Transfer Protocol (NNTP), Post Office Protocol version 3 (POP3), and the Internet Message Access Protocol version 4 (IMAP4). SMTP is the most widely used protocol of the four because it is used to both send and receive email. The NNTP, POP3, and IMAP4 protocols aren’t enabled by default in Exchange Server 2003, unless an upgrade is taking place. Each protocol runs as a service. Figure 1 displays how it looks on the server:



Name	Description
HTTP	Hypertext Transfer Protocol, for web access to
IMAP4	Internet Mail Access Protocol 4, for client acces
NNTP	Network News Transfer Protocol, for hosting pu
POP3	Post Office Protocol 3, for client access to this s
SMTP	Simple Mail Transfer Protocol, for transporting n
X.400	Message Transfer Agent, for transporting mess

Figure 1 Exchange 2003 Protocols in Exchange System Manager

(12) http://www.petri.co.il/new_security_features_in_exchange_2003.htm

This section will focus on which services are disabled by default on Exchange Server 2003 front-end and back-end servers.

Exchange Server 2003 Front-end Server-Services Disabled by default

In a standard implementation of Exchange Server 2003, there is always a front-end and a back-end server. These types of servers will be mentioned when explaining other security enhancements such as IPSec and Kerberos. The front-server acts as a proxy to the back-end server. There are no mailboxes on this server, so essentially it is a bridge between the client and the back-end. This server also needs to be secure, mainly because it is the first line of attack. The front-end server must be secure in order to prevent vulnerabilities and exploits from attacking the back-end server. The services on the front-end server are disabled by default because some are only needed for backwards compatibility, migrations from previous versions, maintenance of the server, and if additional applications are being used on the server such as IIS. Below are the services that are now disabled by default on an Exchange 2003 front-end server:

- ***Microsoft Exchange System Attendant***-This service is required on the front-end server only if modifications of the configuration are needed on the server. Any changes that use the Exchange 2003 Front-end Security Policy, as well as servers designated as front-end servers have to start this service temporarily along with the services it is associated with. It's really only needed for when maintenance needs to be performed on the server, thus it is disabled by default.
- ***Simple Mail Transfer Protocol (SMTP)-*** If the front-end server is an HTTP, POP3, or IMAP4 server, it doesn't solely require SMTP. If the server is configured as a gateway server or a SMTP submission server for IMAP4 or POP3 clients, then SMTP or SMTPSVC service must be enabled. Any sort of transport of Exchange requires SMTP. A good example would be a virus scanner that utilizes multiple services such as the Microsoft Exchange Information Store and Exchange System Attendant services.
- ***Microsoft Exchange Information Store***- This service isn't required because there are no mailboxes or public folders on the front-end server. This provides heightened security because all of the mailboxes reside on the back-end server only. In the event that the server is configured as an SMTP gateway between the front-end and the back-end server, which also doesn't have mailboxes or public folders, the MSExchangeIS service is needed for virus scanning and to route public folder mail.
- ***Microsoft Exchange MTA Stacks***-This service is only needed if there are X.400 connectors on the machine and for backwards compatibility. X.400 is a directory found in earlier versions of Exchange.
- ***Microsoft Exchange Management***- This service allows specification of which global catalog or domain controller Exchanges 2003 uses through a GUI interface. MSExchangeMGMT is also used for message tracking. It can be enabled if message tracking is going to be done in the environment, otherwise it can remain disabled. Auditing some Exchange functionality might require message tracking. Since the front-end server is used to access the mail and not route mail, this service probably won't need to be enabled on the front-end server.
- ***IIS Admin Service***-This service is really only required if running the following services:

  World Wide Web Publishing Service, SMTP, POP3, IMAP4, or the NNTP services. If these services aren't running than IIS Admin Service can be disabled as well.
- ***World Wide Web Publishing Service***- This service is required for Outlook Web Access and Mobile Access servers. Since the front-end server doesn't contain mailboxes, this service isn't needed.

In addition, Exchange Event, Exchange Site Replication, NNTP, POP3, and IMAP4 are disabled on the front-end server because they provide additional functionality, not needed in order for Exchange to run. Microsoft recommends making sure that the Routing Engine Service (resvc) isn't disabled on the front-end or the back-end server. This service must be left running in order for the Exchange Server to function.

Exchange Server 2003 Back-end Server-Services Disabled by default

Below is a list of services that Microsoft has disabled by default on a back-end Exchange server. These services are disabled because they are not needed for the application to function, and are only needed for backwards compatibility. This is the server that contains all of the data and mailboxes, so it is important to limit the number of services running to only the ones that are needed for the server to function.

- ***Microsoft Search***- This service provides a way to search for documents within a message store. It can manage and create indexes for common key fields. This provides Outlook users with the ability to search for documents quickly. Full-text indexing, which allows the index to be built prior to any searches that are done by the client, makes the searches faster. Text attachments can also be included as part of the full-text index. MSSEARCH must run with the Microsoft Exchange Information Store service in order for the index to created, deleted, and updated. This is really an unnecessary service, as it isn't required for core functionality of the application. It just depends on the needs of r environment.
- ***Microsoft Exchange Event***- This is a service that has been around since Exchange 5.5. It handles server-side scripts that are triggered by folder events, either public folders or individual mailboxes. The service name is MSExchangeES, and it only appears in Exchange Server 2003 for backward compatibility with event scripts in Exchange 5.5. All new applications written for Exchange Server 2003 should use the Exchange store events that are native to the recent version of Exchange, thus the MSExchangeES should be seldom used.
- ***Microsoft Exchange Site Replication Service***- This service is also available for backwards compatibility with Exchange 5.5. In the event that an Exchange 2003 server belongs to a site that exists in Exchange 5.5, the MSExchangeSRS service replicates the Exchange 5.5 site and configuration information to the Active Directory configuration naming partition.
- ***Microsoft Exchange POP3***-This service is disabled on a back-end server because the server isn't configured for POP3 (POP3svc). This service provides access to mailboxes and is disabled by default on all new

Exchange 2003 installations. This service should only be enabled on servers that need the POP3 service.

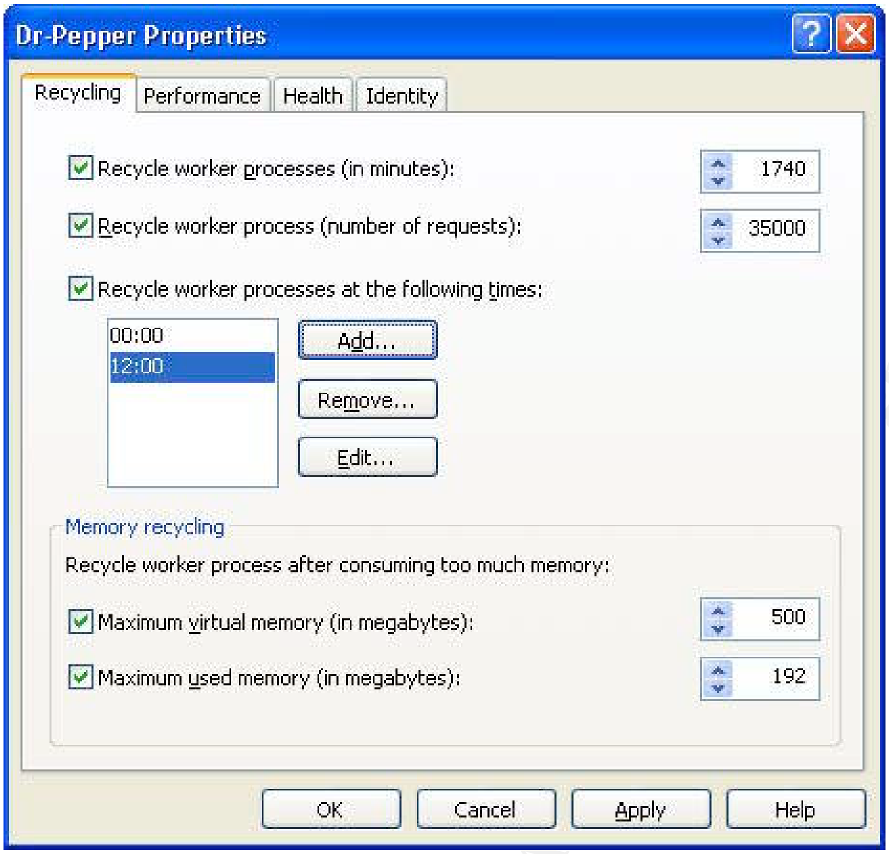
- ***Microsoft Exchange IMAP4***- This service is also disabled on a back-end server because the server isn't configured with IMAP4. The IMAP4svc service provides IMAP4 access to mailboxes and public folders and is also disabled by default on all new Exchange 2003 installs. This service, just like POP3, should only be enabled on servers that need the IMAP service.
- ***Network News Transfer Protocol (NNTP)-*** This protocol is only needed during setup and for access to newsgroups maintained within public folders. The NntpSvc is disabled by default on all new Exchange 2003 installs. This is a back-end only protocol.

IIS 6.0 Security and dedicated application mode

IIS (Internet Information Server) 6.0 has been redesigned, integrated, and disabled by default on the Windows 2003 platform, thus enhancing the level of security. It includes many new features, but the one that Exchange Server 2003 utilizes is the ability to run in dedicated or Worker process application mode. The name of the program that runs worker processes is W3WP.exe (World Wide Web Worker Process). IIS 6.0 must be installed on a Windows 2003 server in order for the Exchange 2003 server to function. It is needed for such functionality as Outlook Web Access.

Dedicated application or worker process isolation mode is a major addition to the redesign of IIS 6.0. Running dedicated application mode allows services the ability to take advantage of the memory features of IIS 6.0, enhancing both performance and security. Dedicated application mode runs with Network Service privileges, which is much more secure than the LocalSystem account used in IIS 5.0. IIS 6.0 provides isolation without a performance hit, because there aren't any process hops. All application code functions in an isolated environment, which makes it more secure. This also makes it so that Web applications cannot affect other Web applications. If one application decides to go down, it doesn't bring down the entire universe (IIS). The core Web server is totally isolated for security. There are specific features that are enabled when this mode is selected. Below is a list:

1) Applications can be restarted based on their failure, duration of operation, number of requests treated, scheduled times, or memory consumption. Figure 2 displays these settings:



☑ Recycle worker processes (in minutes): 1740

☑ Recycle worker process (number of requests): 35000

☑ Recycle worker processes at the following times:

00:00
12:00

Memory recycling

Recycle worker process after consuming too much memory:

☑ Maximum virtual memory (in megabytes): 500

☑ Maximum used memory (in megabytes): 192

Figure 2 Web Application Recycling Settings

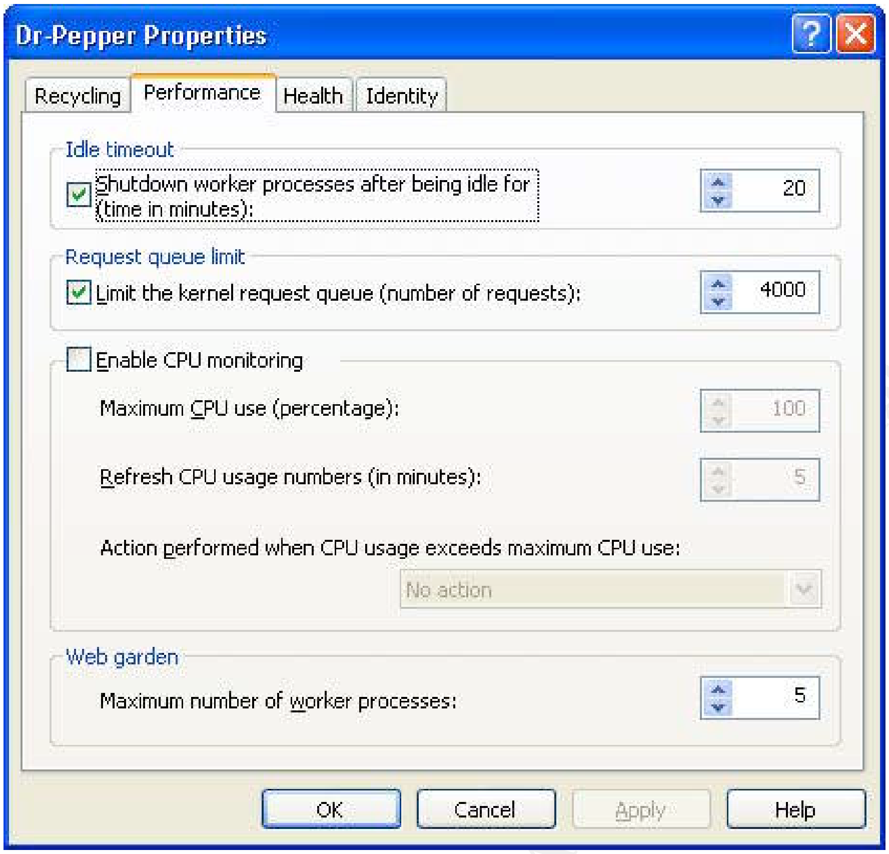
(4) http://www.ftponline.com/wss/2004_03/magazine/features/nruest/page2.aspx

2) Individual pages or multiple Web sites can be defined as an application pool (group of applications). The pool can be managed, monitored, or stopped as one unit. The application pool can be run using methods other than the System account. There are certain process boundaries that separate each application pool from the other application pools so that these pools can't interrupt an application that is routed to one pool. Each pool has it's own independent resources.

3) IIS releases resources until the user makes a call to the application again, if the application is idle for a set period of time.

4) Allows the ability to configure a Web Garden, which is two or more of the same Web site configured to serve the same files and applications on the same machine. Web gardens work well on multiple-CPU servers, so multiple worker processes to one CPU or multiple CPUs and have several worker processes service the same content. This will protect the worker process from hanging and allows the ability to scale out on a single server.

Figure 3 displays the settings below:



Idle timeout

☑ Shutdown worker processes after being idle for (time in minutes): 20

Request queue limit

☑ Limit the kernel request queue (number of requests): 4000

☐ Enable CPU monitoring

Maximum CPU use (percentage): 100

Refresh CPU usage numbers (in minutes): 5

Action performed when CPU usage exceeds maximum CPU use: No action

Web garden

Maximum number of worker processes: 5

Figure 3 Web Application Performance Settings

(4) http://www.ftponline.com/wss/2004_03/magazine/features/nruest/page2.aspx

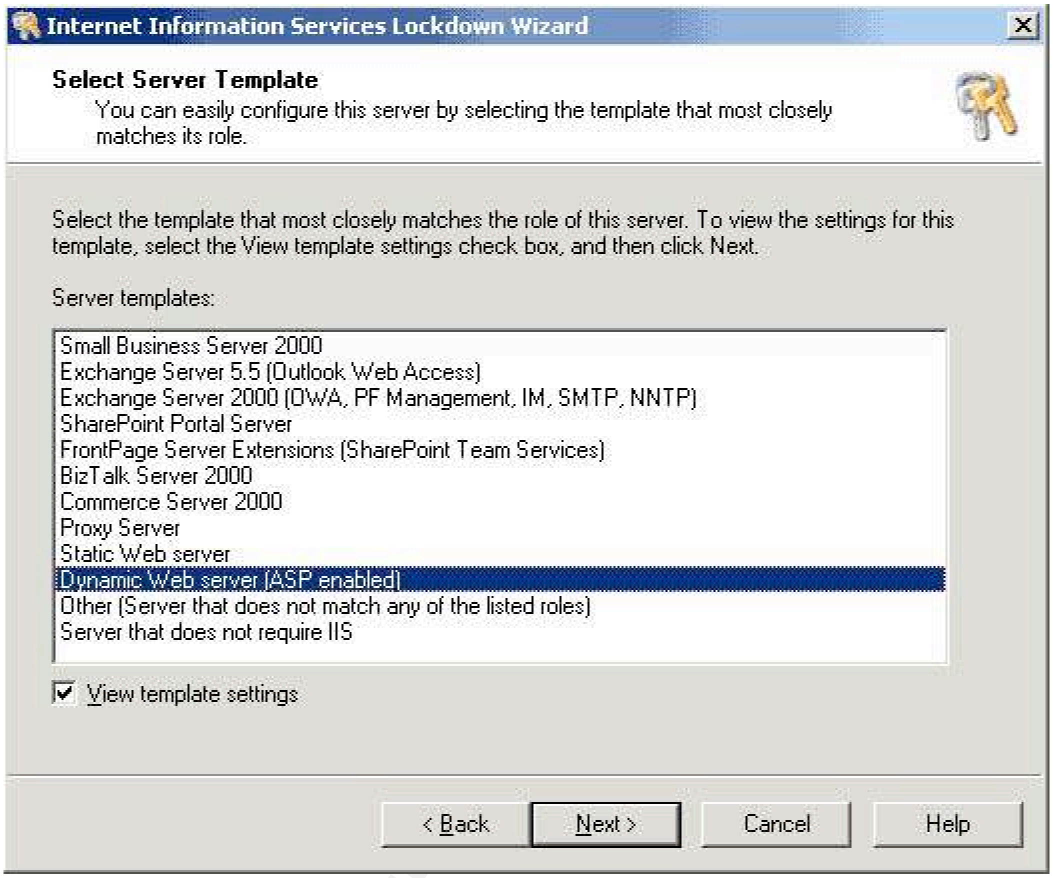
The dedicated application process makes IIS much more reliable for the simple fact that the main services it uses, such as the World Wide Web Publishing Service (WWW Service), IIS Admin, and HTTP.sys are continuously running regardless of any service interruptions that occur in the process.

IIS Lockdown Wizard-URL Scan Tool

IIS 6.0 is utilized by Exchange Server 2003, thus the IIS Lockdown functions in Windows Server 2003 are also used. IIS 6.0 is integrated but disabled in Windows Server 2003. A brief description of both the IIS Lockdown and URLScan tool will be provided for basic understanding.

IIS Lockdown tool v.2.1

This tool reduces attacks by turning off unused or unnecessary features. URLScan has been integrated into the IIS Lockdown Wizard. The integration allows the ability for the Lockdown Wizard to provide additional security offered by URLScan with the need for the administrator to design a custom URLScan filter for the particular server application and configuration. It also has customized templates for each server role to provide defense. The server roles include Microsoft Exchange 2000/2003 Server, Microsoft Commerce Server, Biztalk Server, Small Business Server 2000, SharePoint Portal Server, FrontPage Server Extensions, and SharePoint Team Services. Figure 4 shows a sample of how the interface looks:



Internet Information Services Lockdown Wizard

Select Server Template

You can easily configure this server by selecting the template that most closely matches its role.

Select the template that most closely matches the role of this server. To view the settings for this template, select the View template settings check box, and then click Next.

Server templates:

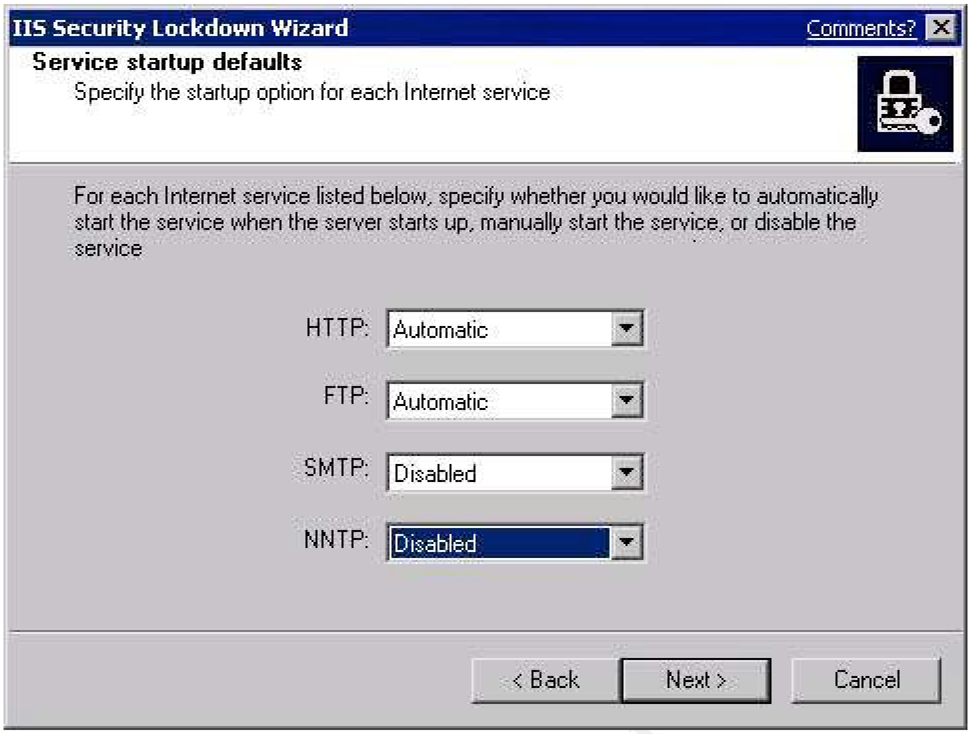
- Small Business Server 2000
- Exchange Server 5.5 (Outlook Web Access)
- Exchange Server 2000 (OWA, PF Management, IM, SMTP, NNTP)
- SharePoint Portal Server
- FrontPage Server Extensions (SharePoint Team Services)
- BizTalk Server 2000
- Commerce Server 2000
- Proxy Server
- Static Web server
- Dynamic Web server (ASP enabled)
- Other (Server that does not match any of the listed roles)
- Server that does not require IIS

☑ View template settings

Figure 4 IIS Lockdown Wizard

(6) http://techrepublic.com.com/5100-6268_11-1031802-2.html

Take notice of the Exchange 5.5 and Exchange 2000, the functions in parenthesis are also available in Exchange Server 2003. This tool also provides the ability to remove or disable IIS services such as HTTP, FTP, NNTP, and SMTP. IIS Lockdown can read from an answer file for scripted or unattended installation. Figure 5 shows what these settings look like in the wizard:



IIS Security Lockdown Wizard

Service startup defaults

Specify the startup option for each Internet service

For each Internet service listed below, specify whether you would like to automatically start the service when the server starts up, manually start the service, or disable the service

HTTP: Automatic

FTP: Automatic

SMTP: Disabled

NNTP: Disabled

Figure 5 Service startup defaults IIS Lockdown Wizard

(5)
http://www.windowsecurity.com/articles/Locking_Down_IIS_60_with_NET_The_Default_Security_Wizard.html

URLScan Security Tool v.2.5

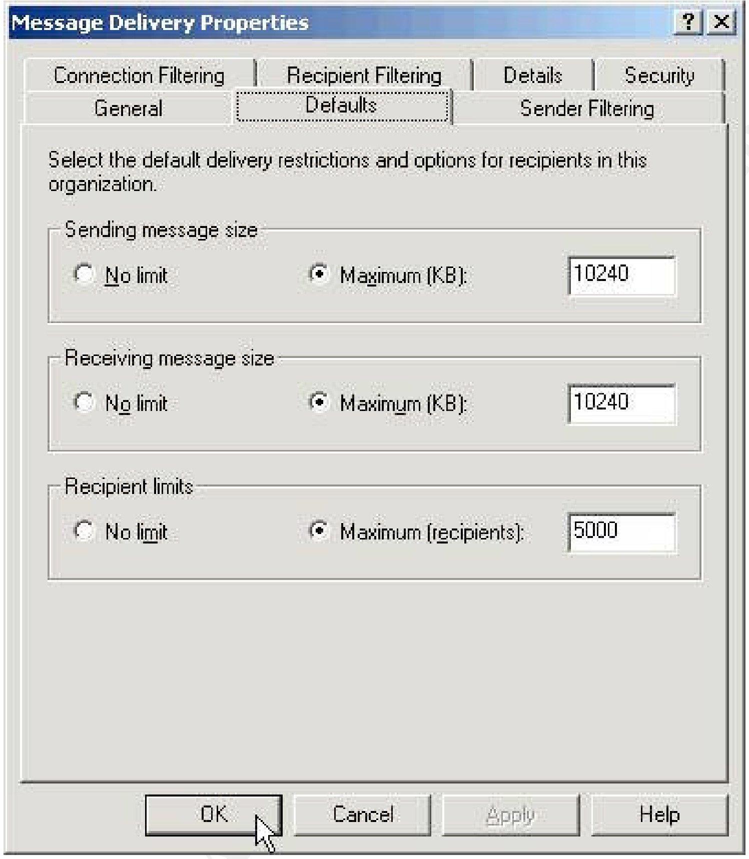
This tool works with the IIS Lockdown tool to provide the ability to turn off unneeded features and restrict the type of HTTP requests that a server processes. This tool also prevents harmful requests from causing damage to the server by blocking specific requests. For instance, most attacks have certain unusual characteristics. These type of request might be unusually long, request unusual actions, are encoded using a different character set, or include strange sequencing that is much different than the normal request. This tool isn't extremely necessary in Windows 2003, since IIS 6.0 has built-in features that provide equal security functionality, but it's still used because there are some a few functionality differences, but for the most part, most environments just use the integrated feature.

Enforcing Messaging Limits

Sending and receiving message limits

Message limits keep users from sending extremely large messages through the Exchange server. Sending large messages often cause problems for the server such as weighing down processing time, queue availability, and disk storage. This is why users should use file shares, compression of attachments, and document management portals as delivery methods instead. These methods help by keeping information secure and increasing the availability of the server.

Exchange 2003 configures the messaging limits on the server if there are none already confirmed. The first Exchange server in the environment restricts the sending and receiving message size to 10 MB or 10240KB by default, but can be set to whatever the administrator or organization feels is sufficient. If the message size has already been set from a previous version, then those settings will stay in tact. Navigate to the Exchange System Manager-Global Settings-Message Delivery-Properties-Defaults as shown in Figure 6 to view these settings:



Message Delivery Properties

Select the default delivery restrictions and options for recipients in this organization.

Sending message size
○ No limit ● Maximum (KB): 10240

Receiving message size
○ No limit ● Maximum (KB): 10240

Recipient limits
○ No limit ● Maximum (recipients): 5000

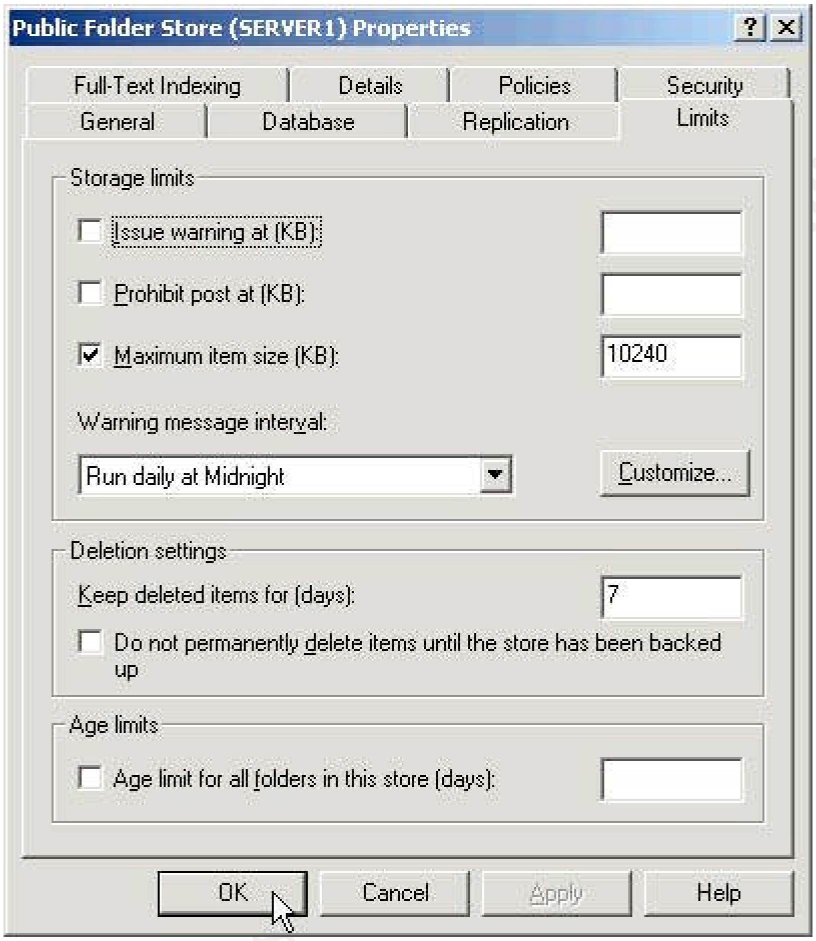
Figure 6 Message Delivery Limit Default Settings

(12) http://www.petri.co.il/new_security_features_in_exchange_2003.htm

Limiting the maximum number of recipients keeps users within the company or organization from spamming the entire enterprise with a large number of emails. Exchange Server 2003 is set to 5,000 participants by default.

Public Folder Limits

The public folder is also set to 10MB by default on every Exchange 2003 server, install, upgrade or otherwise. If those limits imposed are used along with the maximum number of recipients set to 5,000, this will help provide a more efficient Exchange environment by keeping the maximum amount of recipients at a reasonable level to balance performance and the management of the servers, in case there is a vulnerability, such as an e-mail virus. This setting affects new Public Folder stores created within the Exchange System Manager. Figure 7 shows the message size limit setting that is on each Public Store within Active Directory:


Public Folder Store (SERVER1) Properties

Full-Text Indexing | Details | Policies | Security
General | Database | Replication | Limits

Storage limits

☐ Issue warning at (KB):

☐ Prohibit post at (KB):

☑ Maximum item size (KB): 10240

Warning message interval: Run daily at Midnight

Deletion settings

Keep deleted items for (days): 7

☐ Do not permanently delete items until the store has been backed up

Age limits

☐ Age limit for all folders in this store (days):

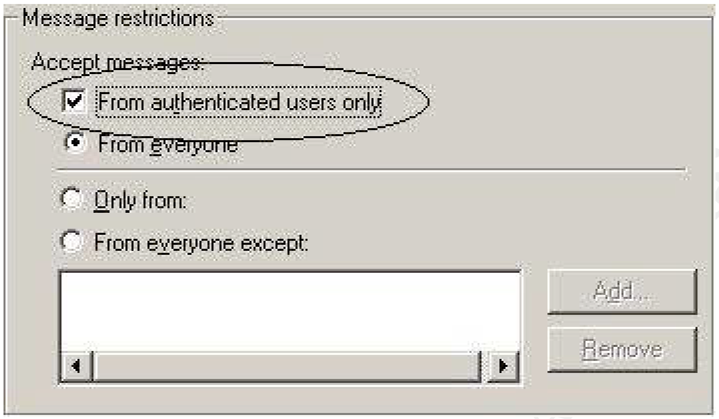
Figure 7 Public Folder Settings

(12) http://www.petri.co.il/new_security_features_in_exchange_2003.htm

There are three storage limits that can be set. A warning can be issued and prohibit mail when a mailbox gets to be a certain size, or the maximum size of email client will receive can be set. There are times that the warning message can be set to appear.

Restricting distribution lists to Authenticated Users in Exchange Server 2003

In previous versions, a specific user could be blocked from sending email to a distribution list or group, or email could be restricted to a particular list of specified users. There is a new feature in Exchange Server 2003, not available before, that now allows administrators the ability to put a restriction on distribution lists, allowing sending from "authenticated users" only. The administrator can also specify which users can or can't send messages to a certain distribution list. This enhances security by allowing the administrator more control over email traffic and provides better management of email users. This can be done by going to Active Directory Users and Computers and selecting the properties of the user's ID. Select the Exchange General Tab, and click on the Delivery Restrictions button. The dialog box shown in Figure 8 will appear:



Message restrictions

Accept messages:

☑ From authenticated users only

● From everyone

○ Only from:

○ From everyone except:

Figure 8 Message Restriction Settings

(17) http://www.msexchange.org/tutorials/MF025.html

Check the box that says "From authenticated users only". This means that the user will be able to receive messages from within the organization but won't be able to receive mail from any user that can't authenticate to the server.

Administrators can also restrict the usage of the group by allowing only a certain security group to use it. Select either the "Only From" or "Everyone except" buttons and "Add" to add the restricted users.

Connection Filtering

Connection filtering helps reduce the number of unsolicited emails sent internally in an organization. In Exchange 2003, filtering only needs to be enabled on each IP that is used on the SMTP servers, just once. Also, connection filtering in Exchange 2003 provides the ability to use third-party blocking services or internal blocking services and only applies rules to anonymous connections and not to authenticated users and computers. In previous versions of Exchange, connections could be blocked based on IP address, but every virtual server within the physical box had to be blocked. The Connection Filtering feature and the IP deny list is global in Exchange 2003.

There are a couple of ways to deny access to SMTP connectivity. It can be done based on the IP address of the server attempting the delivery of the message to the server. Connections can also be blocked from one or more computers. The IP address can either be blocked manually or as a group. SMTP is used on the server with connection filtering enabled to contact a special list, called the Real-time Block List or (RBL). This list provides information as to whether an email was sent from a computer that is on the “blacklisted” list. With Exchange Server 2003, every email can be filtered whether the sender is on the list or not. The RBL serves as a database that attempts to track down the source of annoying SPAM or bulk mail. It is a part of the MAPS system, Mail Abuse Prevention System. Again, the computer is identified through the IP address.

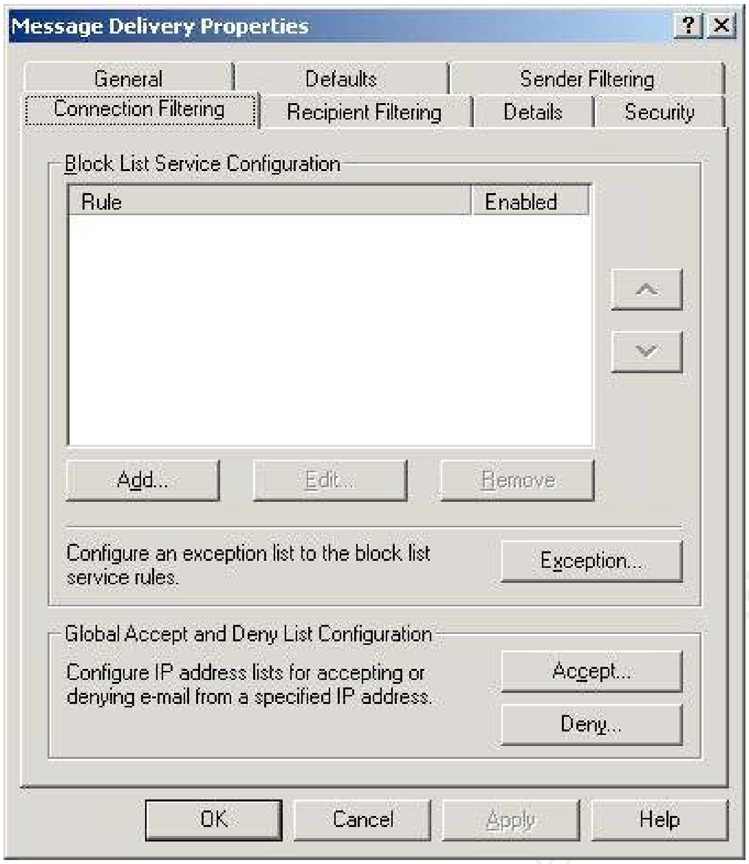
When an outside server connects to an Exchange 2003 SMTP virtual server, the IP address of the external server is forwarded through a DNS query to a block list service provider’s DNS server to check for the existence of a special resource record. If a resource record is located, the provider will return a status code. Below are the default codes and their functions that are blocked on Exchange 2003:

127.0.0.2-Open Relay
127.0.0.3-Dialup spam source
127.0.0.4-Confirmed spam source
127.0.0.5-Smarthosts
127.0.0.5-Spamware software developer
127.0.0.7-Listserver
127.0.0.8-Insecure formail.cgi script
127.0.0.9-Open proxy server

If the external server’s IP address isn’t on the list, then the provider returns a “host not found” message.

Configuring Connection Filtering

Connection Filtering needs to be properly configured in order to be effective. Figure 9 below shows the settings for configuring Connection Filtering. This is found by going to Start\Programs\ESM (Exchange System Manager)\Global Settings (within Scope)\Results. Right click on Message Delivery, select Properties and go to the Connection Filtering tab.



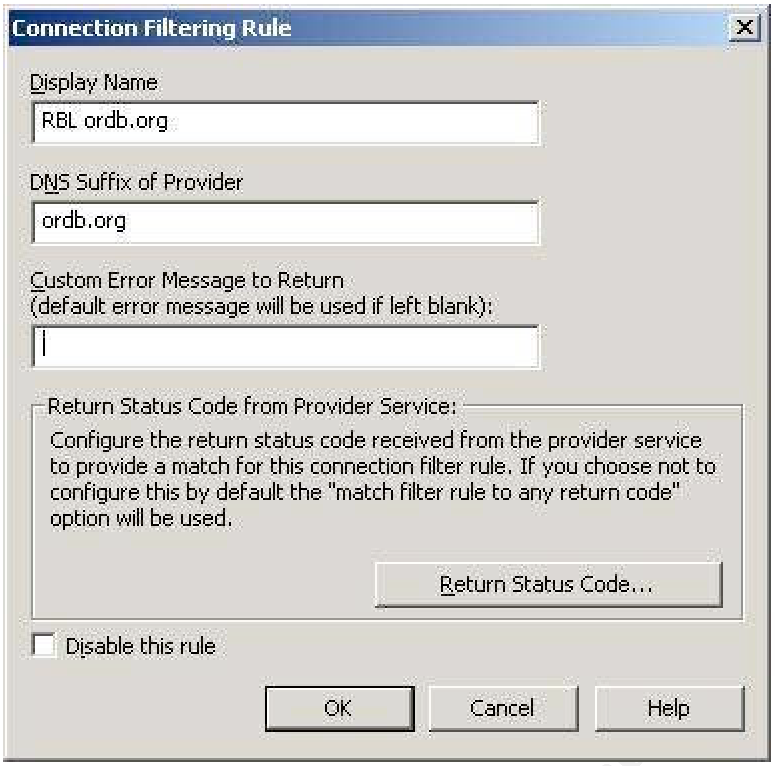
Configure an exception list to the block list service rules.

Configure IP address lists for accepting or denying e-mail from a specified IP address.

Figure 9 Connection Filtering Settings

(16)
http://www.msexchange.org/tutorials/Blacklist_Support_Exchange_2003.html

There is a Block List Service Configuration setting that can be used to add multiple blacklist provider rules, once they are subscribed to. They can be input in the order that the rules are desired to run in. By clicking on the "Add" button, the blacklist filtering rules can be configured as shown in Figure 10 below:



Connection Filtering Rule

Display Name

RBL ordb.org

DNS Suffix of Provider

ordb.org

Custom Error Message to Return
(default error message will be used if left blank):

Return Status Code from Provider Service:

Configure the return status code received from the provider service to provide a match for this connection filter rule. If you choose not to configure this by default the "match filter rule to any return code" option will be used.

Figure 10 Connection Filtering Rules Setting

(16)
http://www.msexchange.org/tutorials/Blacklist_Support_Exchange_2003.html

In the field "Display Name" field, type a brief description of the rule. This name is used for displaying purposes in the Block List Service Configuration area of the Connection Filtering tab. This name should be something meaningful, like the name of the service.

In the "DNS Suffix of Provider" field, type the DNS suffix of the blacklist provider itself. This is generally the namespace of the provider. Disable the rule by choosing the appropriate button if the blacklist provider is having problems.

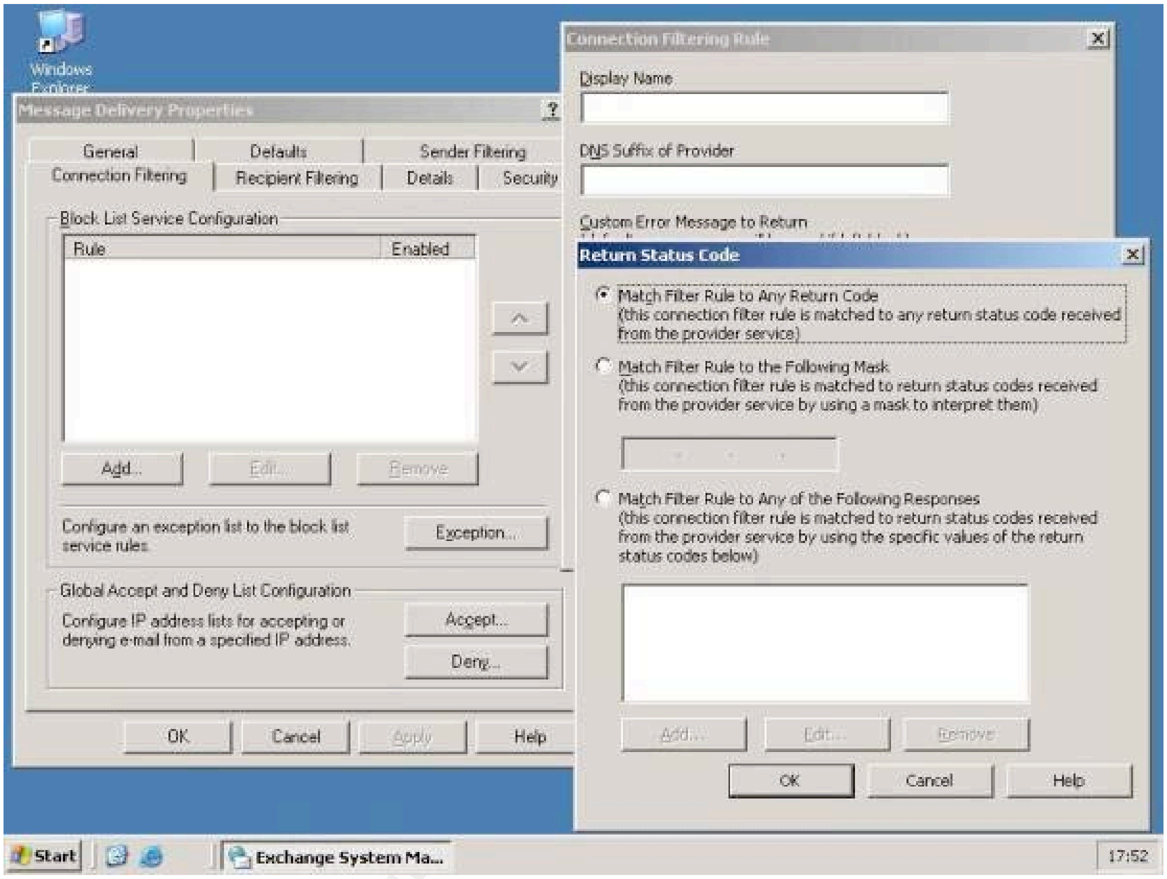
The "Custom Error Message to Return" is an optional custom message that will be returned to the sender when the connection is denied. And by default, every return status code means a blocking of that email. The default settings if left blank are as follows: the <Sender's address> has been blocked by <Connection Filtering Rule Name>." This message will also include the 550 5.7.1 SMTP return code. If a custom message is preferred then there are three environment variables that can be used in this field shown below:

0% Sender's IP address

1% Connection Filtering rule name

2% Block list service provider

Click on the Return Status Code button, the following choices in Figure 11 below appear for custom configuration:



Configure an exception list to the block list service rules

Configure IP address lists for accepting or denying e-mail from a specified IP address.

● Match Filter Rule to Any Return Code
(this connection filter rule is matched to any return status code received from the provider service)

○ Match Filter Rule to the Following Mask
(this connection filter rule is matched to return status codes received from the provider service by using a mask to interpret them)

○ Match Filter Rule to Any of the Following Responses
(this connection filter rule is matched to return status codes received from the provider service by using the specific values of the return status codes below)

Figure 11 Return Status Code Settings

(16)
http://www.msexchange.org/tutorials/Blacklist_Support_Exchange_2003.html

There are three choices: Match Filter Rule to Any Return Code, Match Filter Rule to the following Mask, and Match Filter Rule to Any of the Following Responses.

The first choice, Match Filter Rule to Any Return Code, is the default setting for newly created rules. This option triggers the rule to return all status codes.

The second choice, Match Filter Rule to the following mask, is used to configure a mask that can be used to interpret the return status codes.

The third choice, Match Filter Rule to Any of the following responses, is used to configure the rule to match any of the multiple status codes. Figure 12 shows where return status codes can be added below:

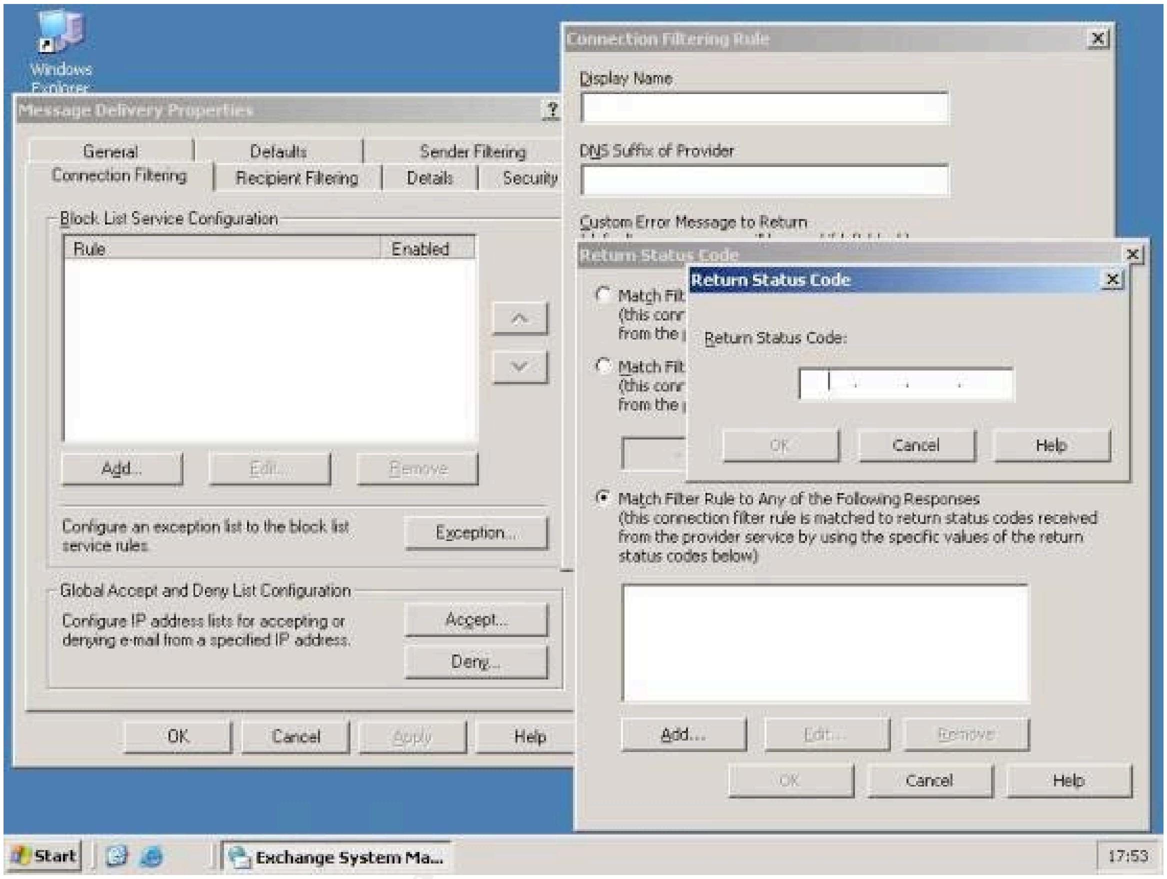

Windows Explorer
Message Delivery Properties
General
Defaults
Sender Filtering
Connection Filtering
Recipient Filtering
Details
Security
Block List Service Configuration
Rule
Enabled
Add...
Edit...
Remove
Configure an exception list to the block list service rules
Exception...
Global Accept and Deny List Configuration
Configure IP address lists for accepting or denying e-mail from a specified IP address.
Accept...
Deny...
OK
Cancel
Apply
Help
Connection Filtering Rule
Display Name
DNS Suffix of Provider
Custom Error Message to Return
Return Status Code
Match Filt
(this conn
from the
Match Filt
(this conn
from the
Return Status Code
Return Status Code:
OK
Cancel
Help
Match Filter Rule to Any of the Following Responses
(this connection filter rule is matched to return status codes received from the provider service by using the specific values of the return status codes below)
Add...
Edit...
Remove
OK
Cancel
Help
Start
Exchange System Ma...
17:53

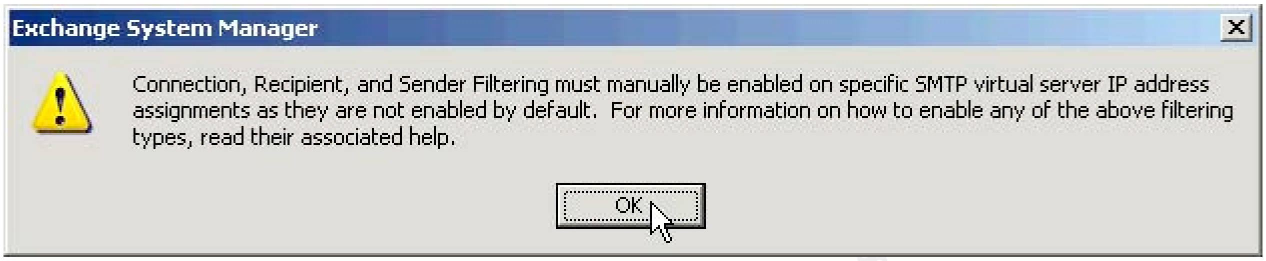
Figure 12 Entering Return Status Code Information

(16)
http://www.msexchange.org/tutorials/Blacklist_Support_Exchange_2003.html

There two exceptions to the rules that can be specified within the Connection filtering rules: exceptions to block list service rules and global accept and deny lists. Refer back to Figure 9 again to see where Exceptions can be set under the Connection Filtering configuration. The Exception option is used to add one or more recipient SMTP addresses that need to be excluded from the Connection Filtering Rules or that need to receive messages even if their server's IP addresses are on one or more Real Block Lists.

In order to configure this option, click on the Exceptions button. The Block List Service Configuration will appear. In the "Recipient" field, enter the internal SMTP address that needs to be excluded from the Connection Filtering rules.

The following warning in Figure 13 appears with a notification that filtering needs to be enabled on the SMTP virtual server:



Connection, Recipient, and Sender Filtering must manually be enabled on specific SMTP virtual server IP address assignments as they are not enabled by default. For more information on how to enable any of the above filtering types, read their associated help.

Figure 13 SMTP Error Notification

(9) http://www.petri.co.il/block_spam_with_exchange_2003.htm

Click "OK" on the button and go to the properties of the SMTP virtual server. Open up the ESM/Administrative Groups/Servers/Protocols/SMTP/Default SMTP Virtual server, and right click on properties as shown in Figure 14 below:

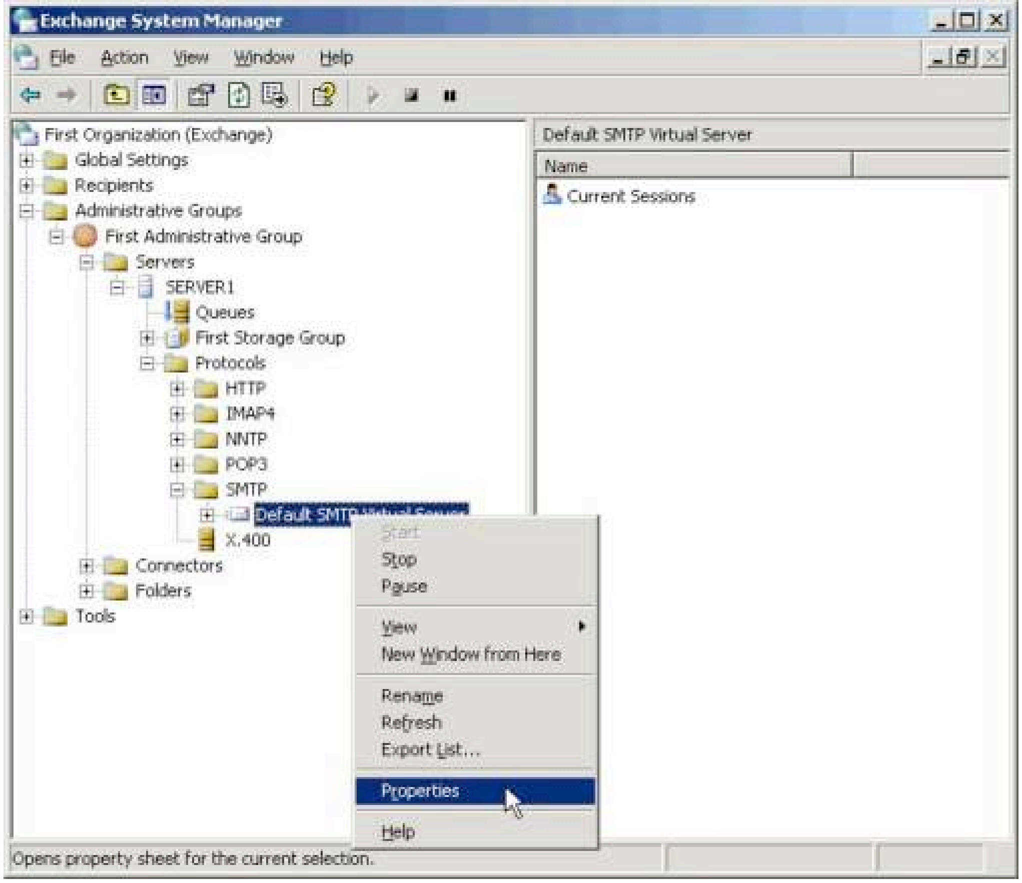
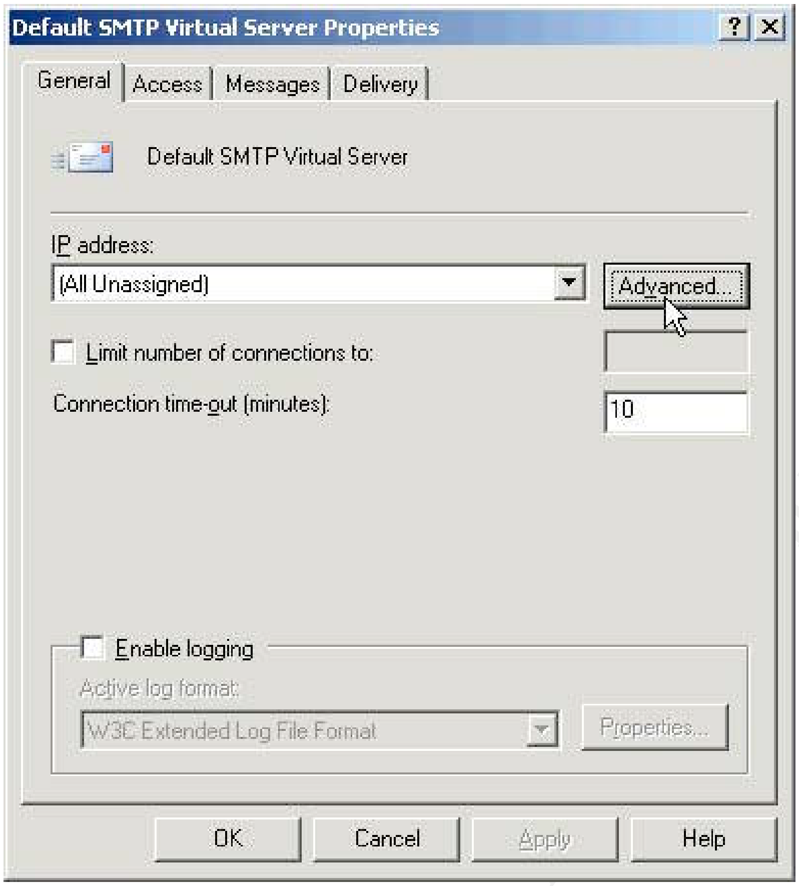


Figure 14 SMTP Virtual Server Properties

(9) http://www.petri.co.il/block_spam_with_exchange_2003.htm

At the "General" tab, click on the "Advanced" button, as shown in Figure 15:



Default SMTP Virtual Server Properties

Default SMTP Virtual Server

IP address: (All Unassigned)

□ Limit number of connections to:

Connection time-out (minutes): 10

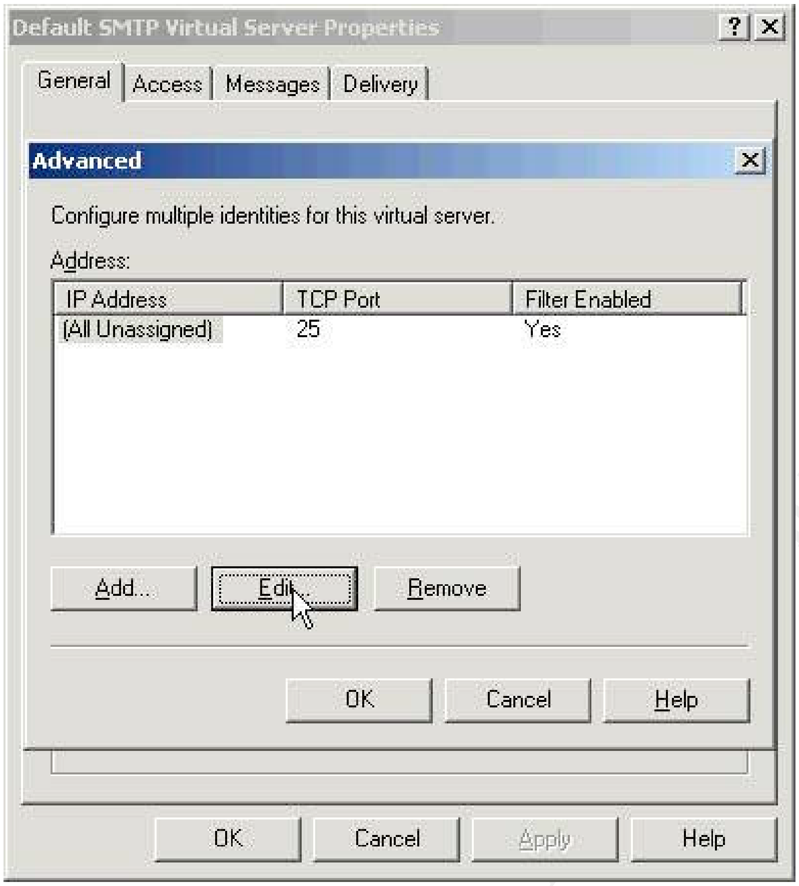
□ Enable logging

Active log format: W3C Extended Log File Format

Figure 15 SMTP Virtual Server Properties Page

(9) http://www.petri.co.il/block_spam_with_exchange_2003.htm

Then click on the “Edit” button shown in Figure 16:



Configure multiple identities for this virtual server.

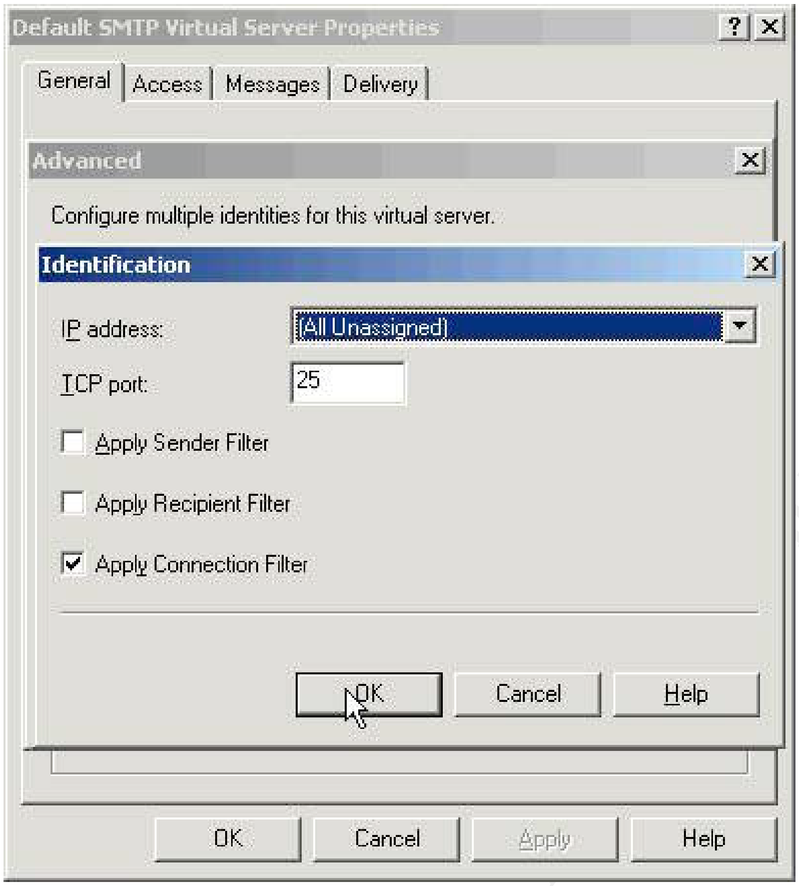
Address:

IP Address	TCP Port	Filter Enabled
(All Unassigned)	25	Yes

Figure 16 SMTP Virtual Server Edit Properties

(9) http://www.petri.co.il/block_spam_with_exchange_2003.htm

Then select the “Apply connection filter” option at the Identification screen to apply the filter as shown in Figure 17:



Configure multiple identities for this virtual server.

IP address: (All Unassigned)

TCP port: 25

☐ Apply Sender Filter

☐ Apply Recipient Filter

☑ Apply Connection Filter

Figure 17 Applying Connection Filtering on the SMTP Server

(9) http://www.petri.co.il/block_spam_with_exchange_2003.htm

There is no way to modify or edit entries on the Exception list, so if an entry is incorrect, the entry must be deleted and recreated. In order to delete an entry, just select it and click the "Remove" button on the Block List Service Configuration Settings dialog. After the exceptions are entered and connection filtering is enabled on the SMTP virtual servers, just click "OK" to save the changes and return to the Connection Filtering tab. Once this is done, the Exchange Server 2003 checks every configured blacklist before it reroutes the email.

The Accept/Deny List Configuration can be used to set or view IP restrictions on the SMTP virtual server, and to add or remove IP addresses from the global accept and deny lists. Exchange 2003 provides connection and relay control for its SMTP virtual servers. Within the global accept and deny setting, IP addresses can be configured to accept connections or always deny connections. These controls can be used to limit the computers that connect to a virtual server or that relay emails outside of the organization.

The global accept and deny lists can be viewed as being separate from the Connection Filtering rules. Exchange checks the global accept and deny lists, before sending any queries to any block list service providers. If the IP address is located on either list, Connection Filtering rules are not processed for messages with that IP. If the IP address is found on the accepted list, then Exchange accepts it without checking the Connection Filtering rules. If the IP is found on the deny list, the Exchange serves the SMTP connection after the MAIL FROM command is received.

In Exchange 2003, there is just one global accept and deny list that needs to be managed. Instead of adding and removing entries from each SMTP server, they can be added and removed once and then they are globally applied to all SMTP virtual servers that have the filtering option enabled.

The configuration of the Accept or Deny list is done the same as the other settings. To configure an Accept list do the following: Click on the "Accept" button under the Global Accept and Deny Configuration in the Connection Filtering settings, click "Add", then select either a single IP address to add or a group of IP addresses to add a subnet of address. The Deny option works the same way, only the "Deny" button needs to be selected instead. A single address or a group of addresses can be denied as well. Keep in mind that the global accept list overrides the global deny list. Exchange 2003 will accept or deny the connection and doesn't check any connection filter rules, if the global accept list is used or the global deny list in conjunction with a provider service.

Inbound Recipient Filtering

Receipt filters can also be configured to prevent email from being delivered to certain people in a company or to recipients who aren't employed by the company. It only applies to messages that come from anonymous connections. It is used to block incoming messages destined for invalid recipients or restricted internal addresses. When Inbound Recipient Filtering is applied, Exchange Server simply rejects messages for nonexistent or blocked recipients during the Simple Mail Transfer Protocol (SMTP) session, rather than sending a Non-Delivery Report (NDR) back to the sender. Without this feature, Exchange Server would normally return an NDR to the sender, which, because SPAM typically originates from false addresses, could be a waste of server resources. This is a security enhancement that didn't exist in previous versions. If a person is not a recipient, they don't receive email. This is another addition to the heightened awareness SPAM and other attacks.

There is great benefit to Recipient filtering. Within Exchange 2003, Recipient Policies are in control of incoming messages by accepting messages for specific SMTP domains only. This prevents receiving messages that were destined for another company; however it won't prevent Exchange from accepting messages from another company address.

There are two ways to filter recipients with this new feature. Filter recipients that aren't in Active Directory or block any properly formatted SMTP address. The feature of blocking all recipients that aren't in Active Directory is good because it eliminates not only messages sent to unknown addresses in the companies SMTP namespace, but also those messages sent to former employees. In the absence of filtering, the Exchange server accepts the messages each time it receives them, determines that the recipient isn't in Active Directory and promptly deletes the message. The other feature is blocking any properly formatted SMTP address, even if it resides in Active Directory. Recipient Filtering is a lot like Connection filtering the fact that it doesn't apply to authenticated users and computers within the organization. This feature enables the blocking of external mail without affecting internal mail. So even if there are no SPAM issues on the network, this feature can be used to essentially block incoming Internet email from single or multiple users.

Recipient filtering is implemented as an SMTP event sink protocol known as Turf List Transport Sink. This sink uses the information in the SMTP RCPT TO: command. If the Recipient Filtering option is enabled, then each time an SMTP virtual server receives the RCPT TO: command, the data transmitted through the command is compared to a list of addresses. If the address is on the filter list, the SMTP virtual server will return the following message, "550 5.7.1 Requested action not taken: mailbox not available."

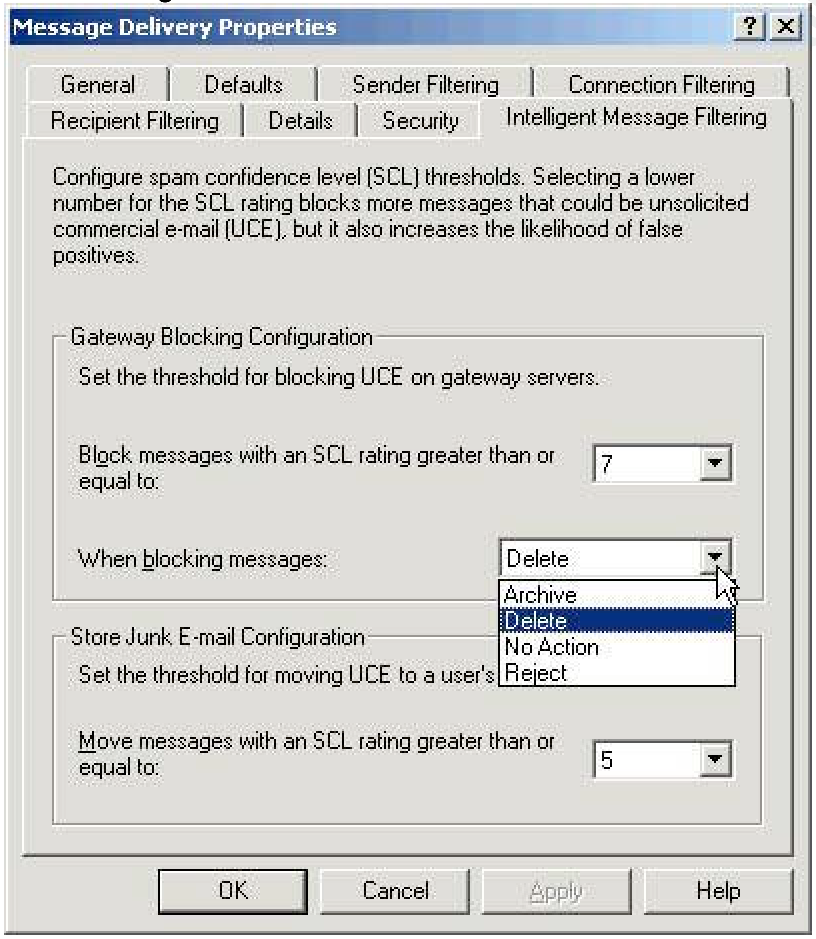
The Recipient filtering configuration is very similar to the Connection Filtering configuration. Global settings must be configured and the filter enabled on the desired virtual servers. This is done by navigating to the ESM/Global Settings/Scope/Message Delivery/Properties/Recipient Filtering tab. The next step is to click on the "Add" button to do filtering on a certain address, and just type in the address or addresses and click "OK". If emails need to be filtered that are addressed to recipients that aren't within Active Directory, click on the "Filter recipients who are not in Active Directory" check box.

If the administrator desires to block messages addressed to one or more recipients, click on the Add button. The Add Recipient dialog will appear. The recipients can be entered using three formats: Wildcard addresses, properly formatted SMTP addresses, and quoted display names. Click "OK" and add the address to the recipient filter list. Click the "OK" button to save the changes.

Exchange Intelligent Message Filter

The Exchange Intelligent Message Filter (IMF) is new in Exchange 2003 and made a debut in May of 2004. It was developed by Microsoft to help companies reduce the amount of SPAM their users receive. IMF can help determine if incoming mail is SPAM, utilizing the Smartscreen technology tracking features that it is based on. Based on the information, email messages can be blocked at the gateway or mailbox store. IMF is available for download from Microsoft's website for Exchange 2003 only. It is designed to work like Outlook message filtering. There are over 500,000 variables used to tell whether a message is SPAM or not in IMF. As opposed to the 250,000 variables found in Outlook filtering. IMF evaluates the content of the messages and assigns the message a probability rating, which tells whether or not the message is SPAM. This is called an SCL rating (Spam Confidence Level). A rating is assigned to all incoming messages, no matter what the threshold is set to. The rating is added to the other message properties. The message properties are then sent to other Exchange servers, along with the message.

If want to configure IMF, go to the ESM/Organization/Global Settings/Message Delivery/Properties/Intelligent Message Filtering as shown below in Figure 18:



Configure spam confidence level (SCL) thresholds. Selecting a lower number for the SCL rating blocks more messages that could be unsolicited commercial e-mail (UCE), but it also increases the likelihood of false positives.

Gateway Blocking Configuration

Set the threshold for blocking UCE on gateway servers.

Block messages with an SCL rating greater than or equal to: 7

When blocking messages: Delete

Archive
Delete
No Action
Reject

Store Junk E-mail Configuration

Set the threshold for moving UCE to a user's

Move messages with an SCL rating greater than or equal to: 5

Figure 18 Intelligent Message Filtering Settings

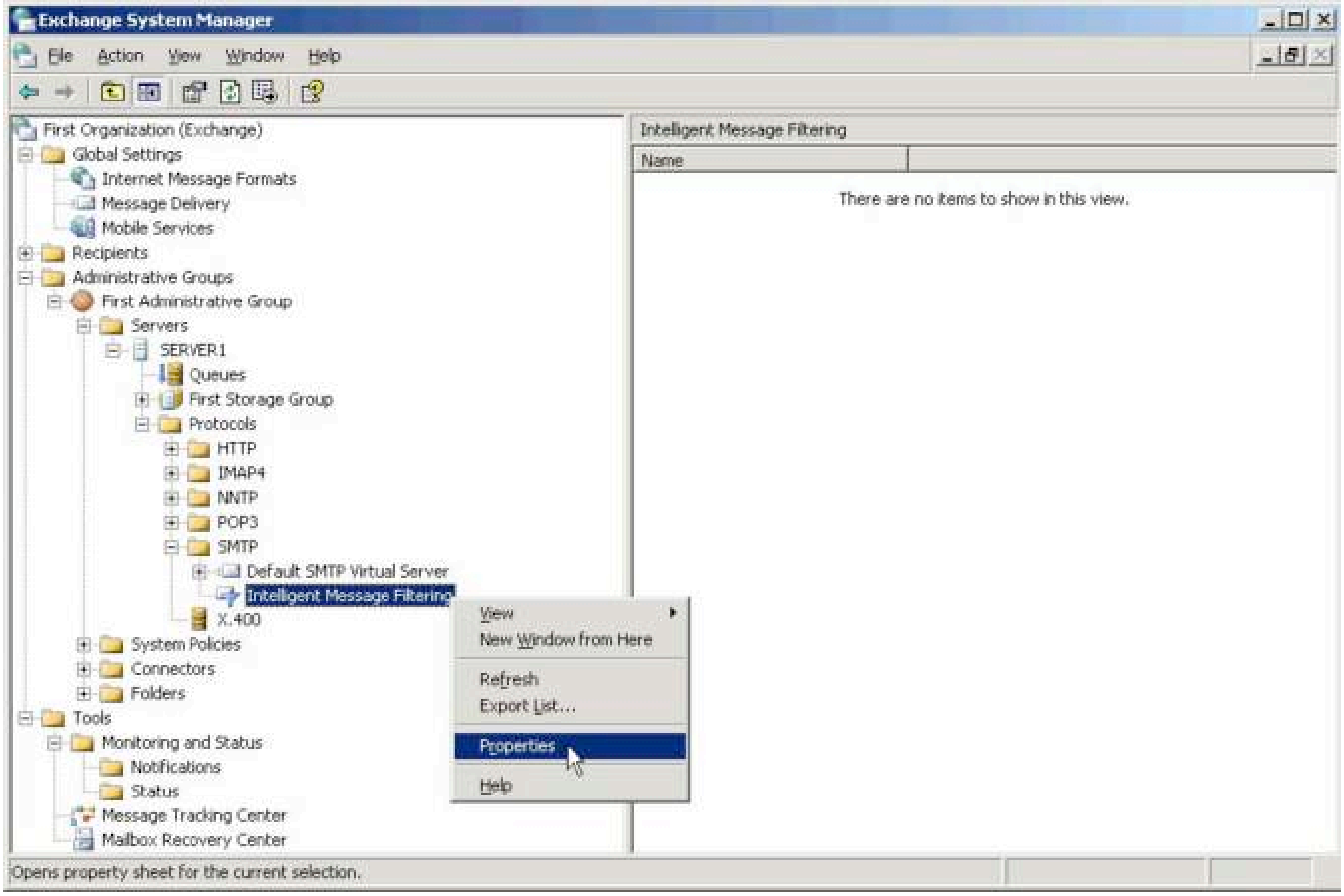
(9) www.petri.co.il/block_spam_with_exchange_2003_imf.htm

There are two main settings in the IMF, gateway blocking configuration and store junk e-mail configuration. The Gateway Blocking Configuration can be used to establish a threshold based on the SCL rating, which if it is above this rating, the gateway server can either archive, delete, take no action, or reject the message.   The gateway threshold should be a high number, so that the obvious

SPAM will be blocked the gateway and never make it to the Junk E-mail folder. If the message happens to make it past the gateway filter, it will be compared to the mailbox threshold value. If the message scores above this value, it will be placed in the recipients Junk E-mail folder. Any lower scoring messages will go to the user's inbox.

http://asia.cnet.com/itmanager/netadmin/0,39006400,39179389,00.htm

The Store Junk E-mail Configuration setting is used to define the thresholds based on the SCL rating that the Exchange 2003 mailbox stores in order to deliver messages to either the user's Junk E-mail folder or their Inbox. The threshold settings for both the Gateway Blocking and Store Junk E-mail can be set to whatever is desired. Then click the "OK" button. Once this is done, the filter needs to be enabled on all of the inbound gateway SMTP virtual servers. To accomplish this, navigate to the ESM/Administrative Groups/Servers/Protocols/SMTP/Intelligent Message Filtering/Properties, as shown below in Figure 19:

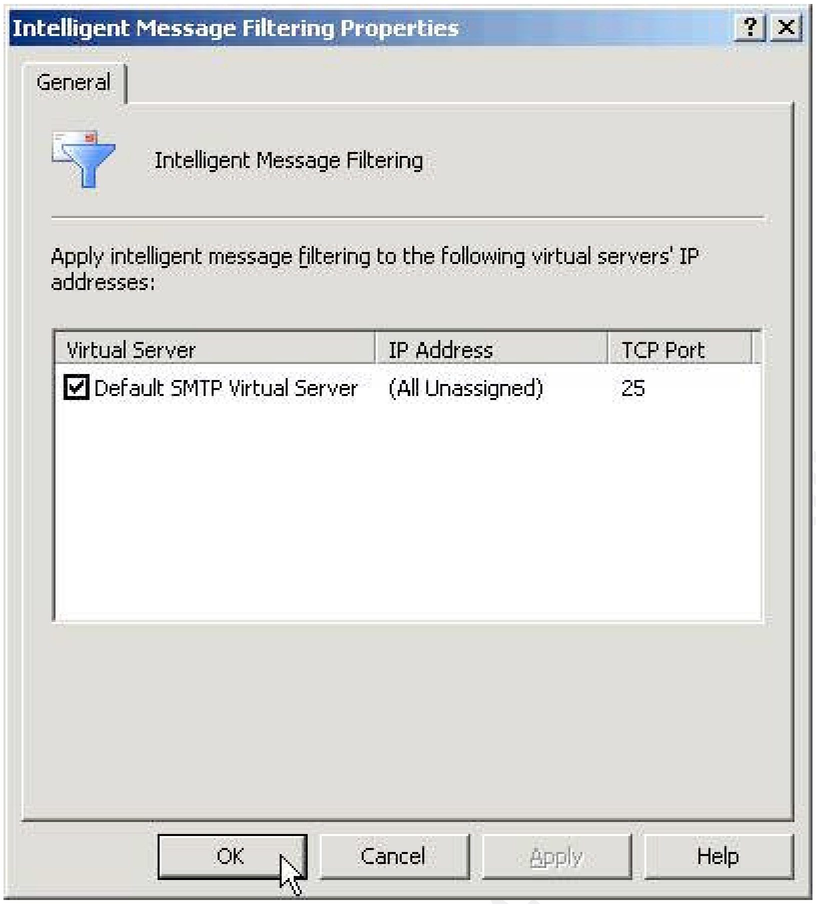


There are no items to show in this view.

Opens property sheet for the current selection.

Figure 19 Intelligent Message Filtering Properties

(9) http://www.petri.co.il/ block_spam_with_exchange _2003_imf.htm



Intelligent Message Filtering Properties

Intelligent Message Filtering

Apply intelligent message filtering to the following virtual servers' IP addresses:

Virtual Server	IP Address	TCP Port
☑ Default SMTP Virtual Server	(All Unassigned)	25

Figure 20 Intelligent Message Filtering Properties

http://www.petri.co.il/images/ block_spam_with_exchange _2003_imf.htm

Select the check box that displays the default SMTP Virtual Server then click "OK", as shown in Figure 20. Regularly monitor the Junk E-mail folder after configuration of IMF.

IPSEC front-end and back-end servers for clusters

In the typical installation, the front-end server resides in a demilitarized zone (DMZ). A DMZ is an isolated environment for servers that need to reside outside of the regular network for added security, such as a Web server. A cluster is a group of servers performing the same tasks. In Exchange 2003, the front-end and back-end servers will be communicating over a trusted boundary. This is different than previous versions, in the fact that IPSec now provides end-to-end security to Exchange cluster servers. Exchange doesn't support SSL, so as an alternative, IPSec can be used. Before I discuss how it functions with Exchange 2003, a brief overview will be provided of the IPSEC protocol. IPSec is made up of two protocols, the Authentication Header (AH) and Encapsulating Security Payload (ESP). The AH adds a cryptographic authentication header to

each IP datagram on a secured connection. It calculates and inserts a digital signature into the packet between the original IP datagram header and the packet's payload. AH provides security, but by no means confidentiality. Protected AH traffic can still be read during submission. The ESP provides confidentiality and integrity checking. It uses one of the two nodes to encrypt the datagram's contents. In tunnel mode, packets are protected to enable connections to two separate networks; transport mode provides end-to-end security between a client and a remote network.
(13) http://www.winnetmag.com/Articles/Print.cfm?ArticleID=38887

The AH and ESP protocols can be used at the same time or independently. There are several algorithms that are supported by each protocol. Two IPSec-capable computers begin communication by using the IKE (Internet Key Exchange) to exchange cryptographic keys. The computers then negotiate to find an algorithm and key length that they both support. This establishes a secure way to protect traffic between the two machines. This is called a security association or SA.

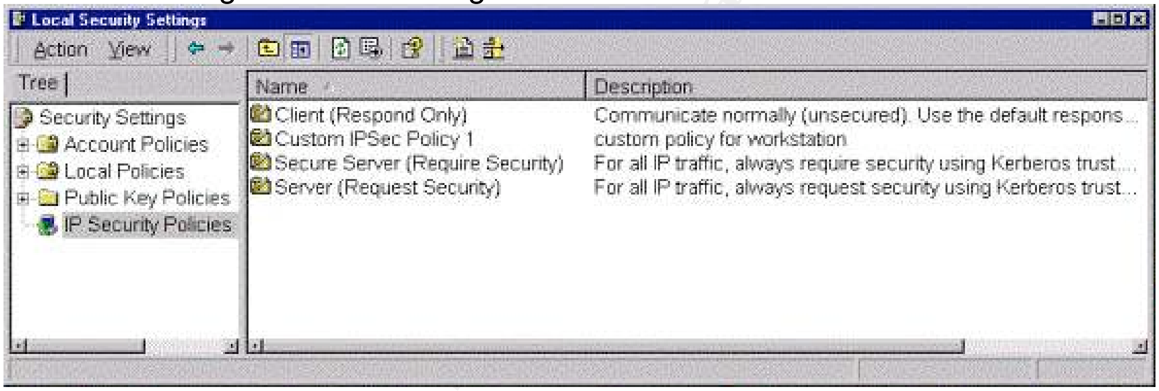
An IPSec policy can easily be built that does what is desired. Rules can be created that specify which protocols or ports need to be used for communication. The front-end servers can be told to initiate IPSec connections only to the back-end servers, not to any other servers. The back-end servers can accept IPSec requests they receive from front-end servers, but the back-end servers don't need to initiate outbound IPSec traffic because the back-end server will never initiate communications to the front-end server on its own.

IPSec is a policy for establishing encryption from end to end of all data packets sent between computers. It uses packets for all traffic between computers utilizing the IPSec policy. It is considered one of the best ways to secure the traffic generated in an environment. It is useful in securing both workstations and servers, in both Internet-access and private network configuration scenarios. All traffic between computers is encrypted. IPSec places a header of it's own on each encrypted packet and sends the packet to it's destination to be decrypted. This helps prevent information leakage and discourages unauthorized access.

IPSec on the Windows 2003 platform provides several features: Data Privacy, ensuring that information is sent from one machine to the other using strong encryption mechanisms such as 3DES (Triple DES encryption). Data Integrity, which is enforced through ESP headers, verifies that the information contained in the IPSec packet hasn't been tampered with. Anti-Replay capability prevents streams of captured packets from being resent. Per packet Authenticity, uses certificates and Kerberos authentication to secure that the sender of the packet is actually an authorized user. Also, NAT (Network Address Translation) traversal, which means that IPSec can be routed through current NAT implementations. Diffie-Hellman 2048-Bit Key Support, assures that the IPSec key cannot be easily broken.

IPSec has three policies that are built into the Windows Server 2003 operating system. They are the server, client, and secure server policies. The server or request security policy requests, but doesn't really require, IPSec communications. This option enables the server to communicate with other non-IPSec clients. It is recommended for companies with fewer security needs. The client or respond only policy enables the configured client computer to respond to requests for IPSec communications. The secure server or require security policy, is the most secure policy, stipulating that all network traffic to and from the server must be encrypted with IPSec.

To establish a really simple IPSec policy on a server, just go to Start/Administrative Tools/Local Security Policy and navigate to IP Security Policies on the Local Computer. Then right click on the Server (Request Security) and select Assign as shown in Figure 21 below:



Name	Description
Client (Respond Only)	Communicate normally (unsecured). Use the default respons...
Custom IPSec Policy 1	custom policy for workstation
Secure Server (Require Security)	For all IP traffic, always require security using Kerberos trust....
Server (Request Security)	For all IP traffic, always request security using Kerberos trust...

Figure 21 Configuring an IPSec Policy

Communications between the front-end and back-end servers are completely unprotected when HTTP, POP3, or IMAP4 are used. This is why it is most beneficial to use IPSec over the other three protocols. In order to enable IPSec traffic between the front-end and back-end server, all it requires is the opening of several ports. The IPSec key exchange uses UDP port 500 for the Internet Key Exchange (IKE) protocol, and it is essential that this protocol be active. Also, the Authentication Header, protocol 51, as well as the Encapsulating Security Payload, protocol 50, would need to be opened. For both of these protocols, they are dependent on the activation of port 500.

Ensure that IPSEC is granted via Group Policy. Group policies control the types of communications a server encrypts or authenticates. Filters are specified based on the IP address and port that traffic is going to or from. Microsoft supports Exchange 2003 on the Windows Server 2003 platform that is using the IPSec transport mode ESP. ESP is used to encrypt communication with clustered Exchange 2003 servers using Network Load Balancing or server clustering. Front-end Exchange 2003 servers such as OWA (Outlook Web

Access) cannot use SSL or TLS to encrypt traffic to the back-end Exchange 2003 server.

The HTTP protocol uses secure authentication whenever possible, in Exchange 2003. The Exchange front-end server uses Kerberos or NTLM authentication to communicate with the back-end server if the back-end server is configured with Windows authentication. Using Windows authentication helps to protect user password information from malicious users who might try to capture traffic between the two servers.

IPSec can be used to establish trust and encrypt network traffic between the front-end and back-end server. There are three scenarios where this configuration would apply. First, if the environment requires that user passwords have to be encrypted. Second, if all of the data transported between the front-end and back-end server needs to be encrypted. The third scenario is if a firewall is desired between the front-end and back-end server, permitting only IPSec connections.

There are several things that happen when IPSec is configured on a back-end server in a Windows Server 2003 cluster. First, the virtual IP address is removed from the first cluster. Second, the removal of the virtual IP from the first node causes IPSec to completely remove the IPSec security association from the front-end server. Third, if the front-end server still tries to connect to the back-end server, the IPSec Internet Key Exchange (IKE) negotiation protocol immediately tries to renegotiate a security association to the back-end server. Fourth, when the new back-end cluster node configures itself with virtual IP address, the IPSec component on that node responds to the front-end server and establishes new IPSec security associations.

There are many ways that IPSec policies can be used in Exchange 2003. IPSEC can be used to encrypt traffic to the back-end Exchange 2003 servers on port 80 (HTTP), port 110 (POP3), and port 143 (IMAP4). IPSec can also be used to encrypt all communications to domain controllers. It can encrypt all network traffic including port 389 LDAP (Lightweight Directory Access Protocol), port 135 RPC (Remote Procedure Call), and port 88 Kerberos.

Kerberos

I've always found Kerberos to be a very complicated protocol. It can be hard to understand and hard to explain. But in order to understand how Exchange Server 2003 and Outlook 2003 utilize Kerberos, I think it is beneficial to at least briefly discuss what it is and how it works. Well, I think this is a very good question. What is Kerberos exactly? Kerberos is the name of a three-headed dog that guarded Hell. Just think that this preferred Windows authentication method is named after a three-headed dog.

Kerberos is designed to protect networks and its data via encrypted and strong authentication over networks that aren't trusted, such as the Internet, where attackers are constantly lurking. It is a challenge response protocol, similar to NTLM. Its main functions are to protect against attacks that can be mounted against other authentication methods, including man-in-the-middle and replay attacks. Man-in-the-middle attacks are when an attacker impersonates both the client and the server. Replay attacks are when an attacker records credentials and then utilizes them to gain access to the server.

How does Kerberos work?

Figure 22 displays how the client/server process of Kerberos authentication works. This Logon process is explained in a simplified manner below.

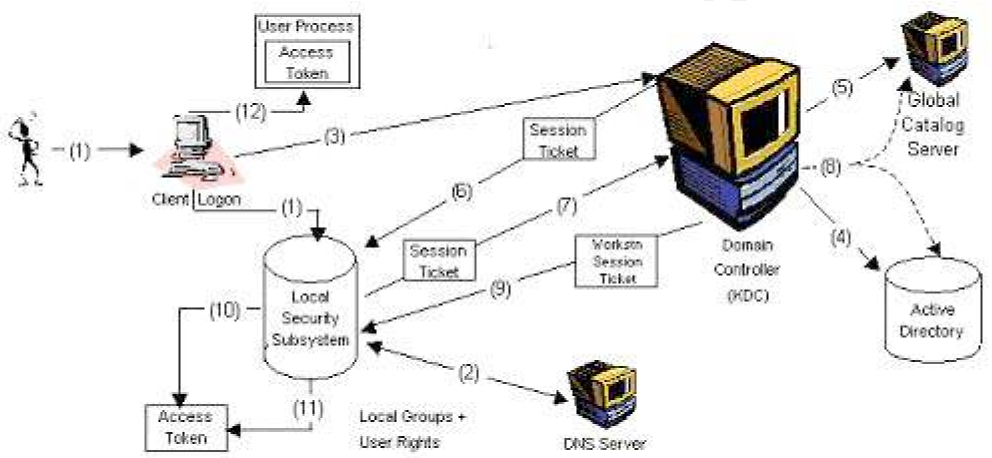


Figure 22 Kerberos Authentication Process

(2) http://www.mcmcse.com/win2k/guides/kerberos.shtml#howitworks

1) The client logs in with their user name, password, and domain name at the login screen. This information is passed to the local security subsystem.
2) The local security subsystem contains the domain name and other credentials specified by the user. It then utilizes the DNS (Domain Name Service) server to find a domain controller.
3) Once the domain controller is located, the local security subsystem goes to the Key Distribution Center or (KDC) on the domain controller. The KDC is the portion of the Kerberos authentication system that deals with the authentication of principles. It distributes the ticket-granting tickets to authenticated principles, and maintains a database of names and private keys of the clients and servers. A session or service ticket (a ticket that is handed out by the ticket-granting service, and permits a client to access application resources) is requested for the user. This ticket will be utilized by the user's computer to authenticate to the KDC.

4) The KDC contacts Active Directory in order to authenticate the user.
5) The KDC contacts the Global Catalog server which contains the Universal group membership information of the user.
6) The KDC returns the session ticket to the user's computer once authentication is complete. The session ticket includes the user's SID and the SIDs of all groups that the user belongs to. The information is stored and will be used for all future KDC negotiations.
7) The local security subsystem on the user's computer relays a copy of the user's session ticket to the KDC on the domain controller and requests another session ticket. This ticket is called a "workstation" session ticket. because it authenticates the user to the local computer's workstation service.
8) The KDC authenticates the user's session ticket using Active Directory and the Global Catalog server.
9) The KDC sends a Workstation session ticket with the user's session ticket to their computer, once authentication is verified.
10) The Local security subsystem creates a user access token consisting of the user and groups SID, from the Workstation session ticket.
11) The local security subsystem adds any local group memberships, rights and permissions of the user to the access token.

http://www.mcmcse.com/win2k/guides/kerberos.shtml#howitworks

Kerberos and Exchange Server 2003

Kerberos was an option in Exchange 2000; it is now used by default on Exchange Server 2003. If Kerberos authentication should happen to fail or is disabled then NTLM would be used between the front-end and back-end Exchange server.

Kerberos authentication is available for front-end and back-end servers. Exchange 2003 uses Kerberos delegation when sending user credentials between a front-end server, usually Outlook Web Access (OWA), and a back-end server, usually a mailbox store to make sure that credentials that are passed are secure. Exchange used Basic authentication to send user's credentials between a front-end and back-end server in previous versions. IPSec had to be used in order to encrypt the message. Exchange 2003 uses Kerberos to authenticate Outlook 2003 users as well.

Kerberos is also used in constrained delegation. Constrained delegation is a new feature of Windows Server 2003. Administrators can specify which specific services or servers a computer can request delegation to, choosing a specific service or computer account. There are benefits: It restricts a front-end servers delegating ability to the back-end Exchange server, where the mail stores are located. The front-end requires Windows 2003 in order to set up delegation;

however the back-end server can be running Windows 2000. The front-end server and user domain must be Windows 2003 servers. The server and user account must be in the same domain. Constrained delegation depends on Kerberos, so there are no clear text credentials exchanged between the front-end and back-end servers. When Kerberos constrained delegation is enabled, it is used regardless of the authentication mechanism of the front-end server, which could be basic, forms based authentication, or SSL client certificates. This is because the only thing that is required is a valid token that is authenticated to delegate a request to another server.

Antispoofing

What does it mean to "spoof"? It is the art of getting users to provide certain information, such as passwords to allow access to that is unauthorized into the enterprise. It is essentially stealing information. An email appears to be from a legitimate user. Address spoofing has become an increasing problem over the last few years. Exchange 2003 prevents someone from viewing email by providing the ability to verify if messages are coming from an authenticated sender or an anonymous person outside of the company. In Exchange 2003, it is required that authentication takes place before a sender's name is resolved to the name displayed in the Global Catalog List. So, if an organization has multiple forests, when a use sends mail from one forest to another, it isn't authenticated. The person's name isn't resolved in the display name in the Global Address List. This happens even if the user contact exists in the other forest.

Summary

In summary, through the following security enhancements in Exchange 2003: restricting user access to the Exchange Server, disabling unnecessary services, enforcing message limits, restricting distribution lists to Authenticated Users, connection filtering, Inbound recipient filtering, IPSec on front-end and back-end clusters, anti-spoofing, Kerberos and Exchange 2003, and Exchange Intelligent Message Filter email is more protected than previous versions. These enhancements carry over the client, which utilizes Outlook 2003.

Part II. Outlook 2003 Security Enhancements

Outlook 2003 is very much a part of any Exchange implementation. Outlook 2003 is used by the client to receive their mail. It is integrated in Exchange 2003. There are some new features that protect clients using Outlook 2003 more than before. The following features with be discussed: Information Rights Management, Kerberos and Outlook 2003, Anti-spam, and restricting access to the Outlook Address Book.

Information Rights Management

Microsoft Office works with Windows 2003 to perform Rights Management duties. This technology was originally used by Microsoft for Digital Rights Management of Windows Media, to help prevent content piracy. Microsoft realizes the importance of securing email and data, thus they are using IRM. Information Rights Management (IRM), which is an information protection technology, protects corporate information and content, including email. It also protects against such things as email forwarding, copying, or printing. Messages are encrypted during transmission. Outlook 2003 disables restricted rules applied by the sender. IRM can be configured with view, read-only, copy, print, and save permissions. There are three main ingredients that are needed to run IRM for a recipient. Windows 2003, Outlook 2003, and the Right Management add-on (RM) are needed. IRM is a dependent extension of this. RMS is used to configure permissions for sensitive info.

IRM can track email messages and attachments during and after being sent. It can provide information about who uses the document and what for. Office 2003 documents that are attached to messages that are protected are also protected. Email messages can be automatically encrypted when sent. This prevents any tampering with the files during transmission. The email messages and attached files have the same security for more control of files. When a document has been protected by IRM, both access and restrictions go where the information goes, even if it is sent outside of a firewall. Usage restrictions are enforced because IRM sets security on the file.

There are two ways to configure IRM. One way is to configure Passport authentication with the Microsoft online service. Another way is to configure RM within the company infrastructure. This is used to enable IRM within Office 2003.

Kerberos and Outlook 2003

In addition to Kerberos and Exchange Server 2003, which was discussed in Part I (pages 32-34), the client (Outlook 2003) has a new feature that improves availability and stability. Outlook 2003 now has the ability to use Kerberos authentication to authenticate to Exchange servers in multiple forests. This is also referred to as cross-forest authentication. A user can authenticate across multiple Windows forests to domain controllers in trusted forests, thereby enabling user accounts and resources to exist in different forests. This is available with the Windows 2003 operating system.

Anti-Spam

As mentioned in the server portion, the elimination of unsolicited email or SPAM and how to prevent from getting it, has been a very hot topic lately. The client is also affected, as they receive email from the server. Outlook 2003 includes new features such as a junk-mail filter, safe sender list, blocked senders list, safe recipients list, and autoupdate that help block as much junk e-mail as possible. The features give administrative control over the types of messages that are delivered to the clients Inbox, as well as provide control over who receives e-mail messages. These features, along with the use of rules, will help reduce the amount of incoming SPAM a great deal. Below is a brief description of each:

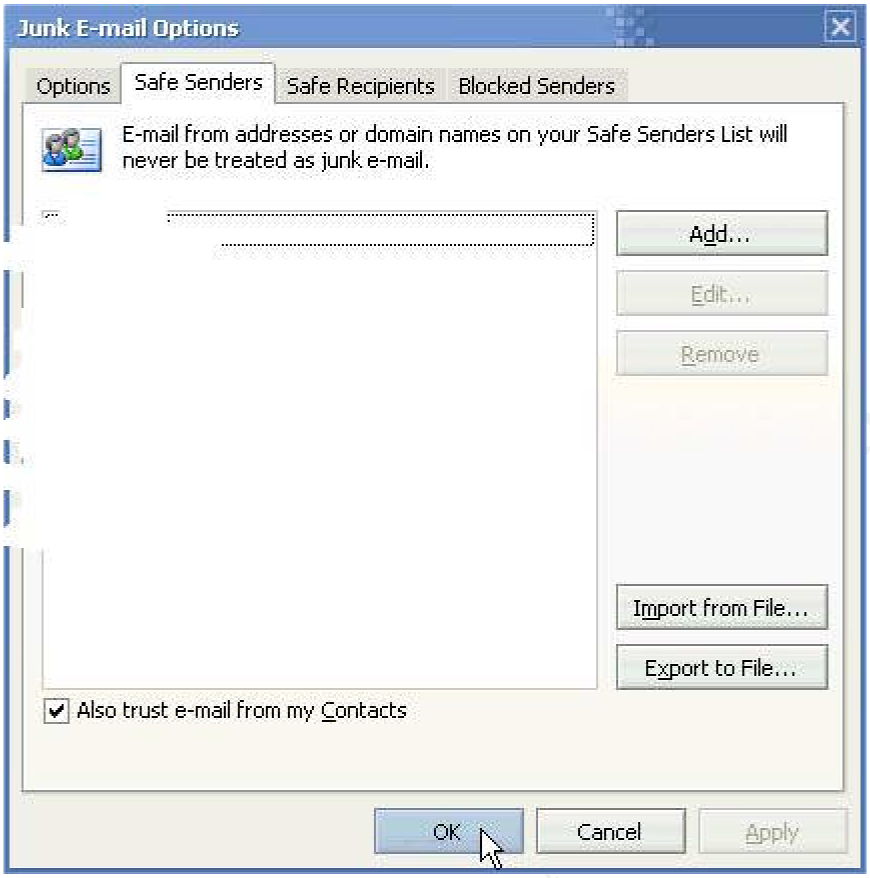
Junk e-mail filter

There are several ways that Outlook 2003 determines if an email is junk. It can be determined based on the time, content, and structure of the message. No particular sender or email type stands out to the filter. Instead, there is some analysis that takes place to determine the likelihood the mail could be junk.

This filter has a low setting by default, which will find most obvious junk email messages. Once the messages are caught, they are moved into the Junk E-mail folder. They aren't deleted, so they can still be accessed to make sure they are indeed junk and not important emails. The filter can also be configured to tougher settings to further check for junk e-mail. It can be configured so that all junk e-mail automatically gets deleted. This is a security improvement compared to previous versions because the level of filtering can be specified. Filtering junk email helps prevent attack, by taking email from an unknown sender and deleting them. It provides less likelihood, that in the case of an email virus, a user would open an email and an attachment, infecting their workstation.

Safe Senders List

In the event that an e-mail that is thought to be junk, is really valid, it can be added to the email address of the sender to what is called the "safe senders list". The email addresses on this list are not treated like junk email messages in any way, shape, or form and are trusted by default. This list can be imported or exported to another computer. To access these settings, go into Outlook 2003; Go to Tools/Options/Preferences/Junk Mail. At the Junk E-mail options, click on the Safe Senders tab, as shown in Figure 23:



E-mail from addresses or domain names on your Safe Senders List will never be treated as junk e-mail.

☑ Also trust e-mail from my Contacts

Figure 23 Junk E-mail Options

(11) http://www.petri.co.il/block_spam_with_outlook_2003.htm

In addition to importing and exporting a list from a file, the choice can be made as to whether or not to trust email from the list of Contacts. Outlook 2003 can be configured to only accept messages from the Safe Senders List.

Blocked Senders List

Email messages from a particular address can be blocked easily by adding the sender to the “Blocked Senders List”. The addresses contained on this list are treated like junk e-mail messages.

Safe Recipients List

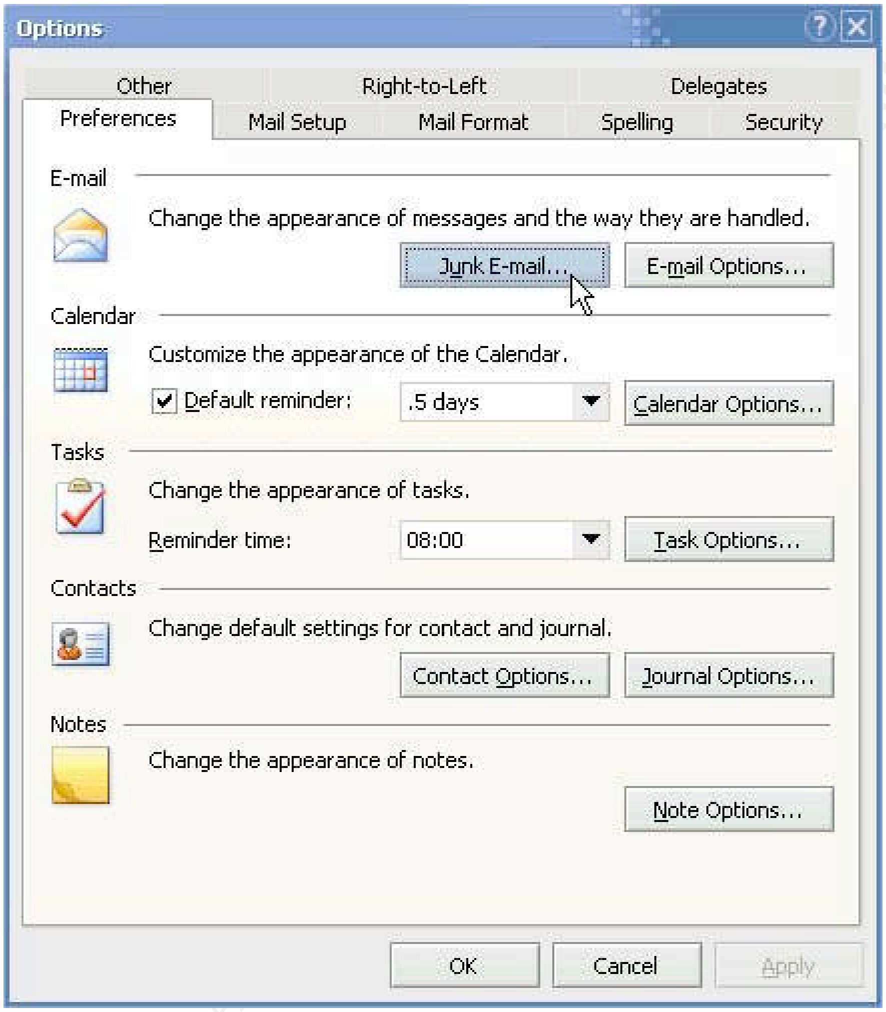
Email lists and groups the client belongs to can be added to the Safe Recipients list. Messages sent to the email addresses on this list, are treated as being safe.

Autoupdate

This feature is used to update the Junk E-mail Filter with updates from Microsoft. This is needed to keep current on blocking SPAM.

Junk e-mail setup in Outlook 2003

Junk e-mail is turned on by default in Outlook 2003. Outlook 2003 provides a notification message when a message is moved to the Junk e-mail folder for the first time. Settings can be changed by going into Outlook, clicking on Tools/Options/Preferences/Junk Mail, as shown in Figure 24 below:



E-mail

Change the appearance of messages and the way they are handled.

Calendar

Customize the appearance of the Calendar.

☑ Default reminder: .5 days

Tasks

Change the appearance of tasks.

Reminder time: 08:00

Contacts

Change default settings for contact and journal.

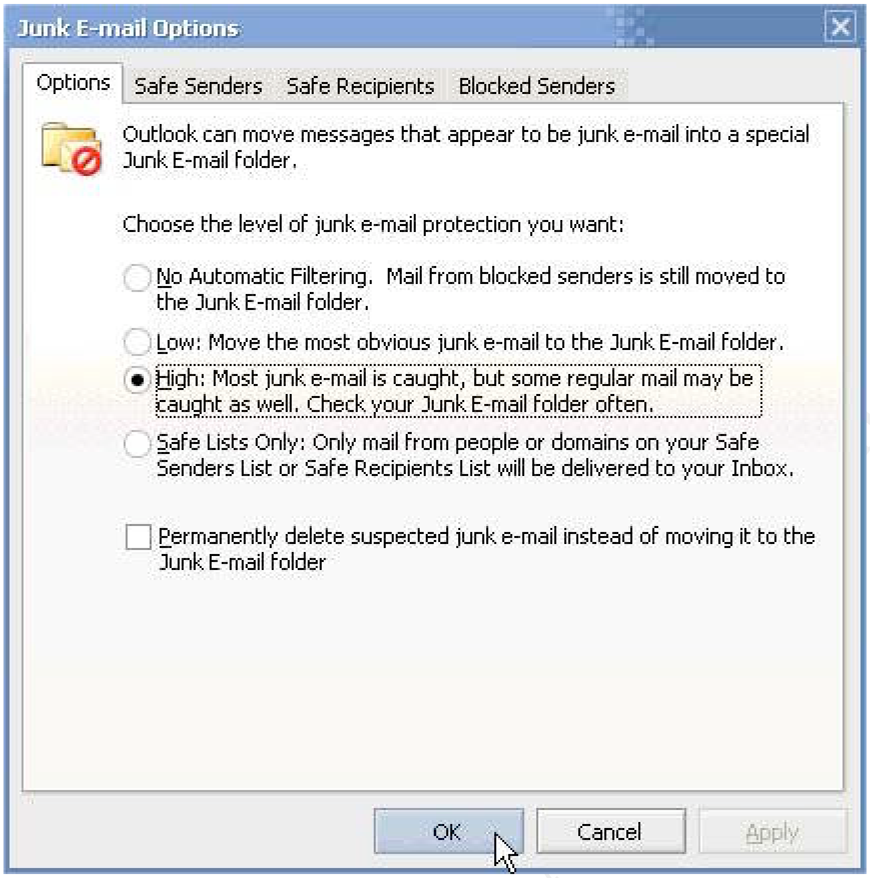
Notes

Change the appearance of notes.

Figure 24 Junk e-mail preferences

(11) http://www.petri.co.il/block_spam_with_outlook_2003.htm

Within the Junk-Email options, the level of protection can be specified on junk email contained in the Junk-Email folder as shown in Figure 25 below:



Outlook can move messages that appear to be junk e-mail into a special Junk E-mail folder.

Choose the level of junk e-mail protection you want:

○ No Automatic Filtering. Mail from blocked senders is still moved to the Junk E-mail folder.

○ Low: Move the most obvious junk e-mail to the Junk E-mail folder.

● High: Most junk e-mail is caught, but some regular mail may be caught as well. Check your Junk E-mail folder often.

○ Safe Lists Only: Only mail from people or domains on your Safe Senders List or Safe Recipients List will be delivered to your Inbox.

□ Permanently delete suspected junk e-mail instead of moving it to the Junk E-mail folder

Figure 25 Junk E-mail Filter Options

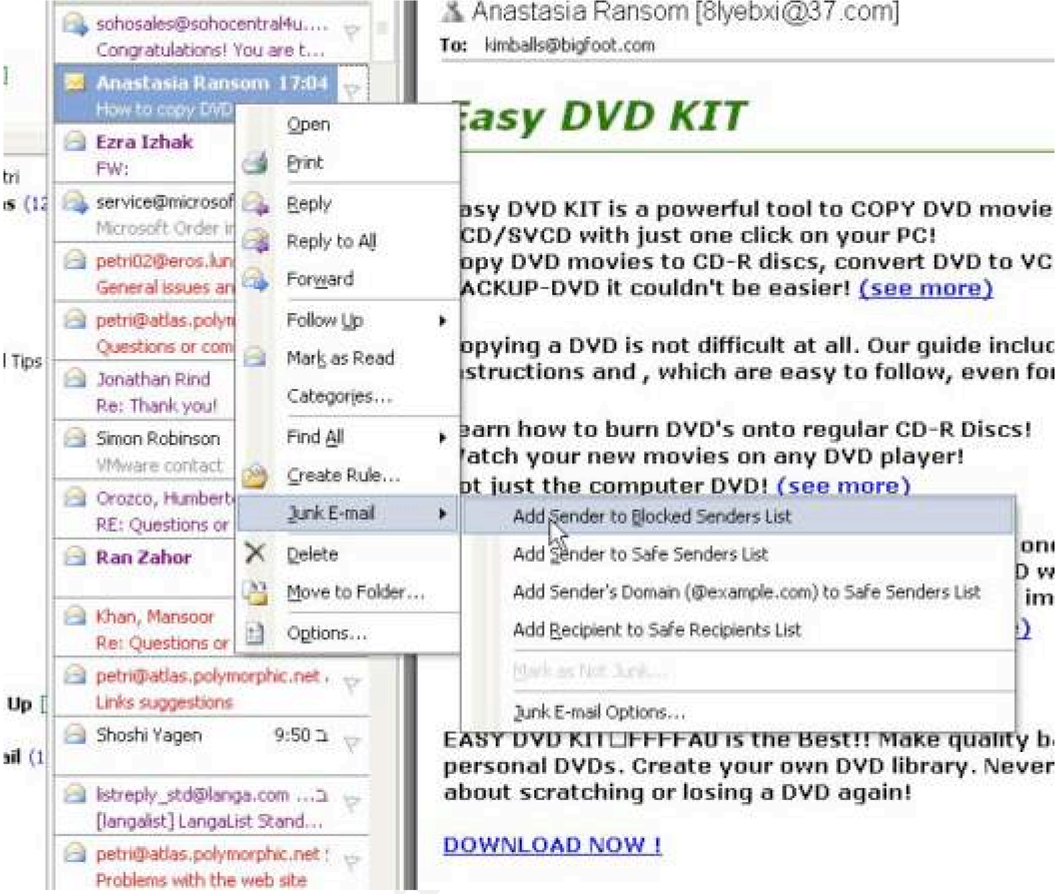
(11) http://www.petri.co.il/block_spam_with_outlook_2003.htm

Click the "OK" button. The Low setting is enabled by default. It is recommended from Microsoft that the Low setting be used for several weeks before attempting a high setting, which might block some regular email as well. It allows time to check the Junk E-mail folder to see what Outlook is interpreting as SPAM. It also allows time to take out the mail that isn't thought to be SPAM. Once Outlook appears to be blocking what it should, a higher setting can be used.

How does Outlook know what is SPAM and what isn't?

I found a great article by Brien M. Posey that explains this. "There are 250,000 MSN members that work to figure out if a message is SPAM or not. Microsoft uses a tool that analyzes certain characteristics of each message to determine if a message is SPAM or not. There are over 100,000 variables that Microsoft uses within this tool to analyze each message. If the numerical score is above a certain value, then the message is assumed to be SPAM. Changing the setting in Outlook from Low to High filtering just changes the threshold value used to determine whether or not the message is SPAM."
(14) http://asia.cnet.com/itmanager/netadmin/0,39006400,39179389,00.htm

Senders can be added to the Safe Senders, Safe Recipients, and Blocked Senders list, by right clicking on the message and going to the junk e-mail option as shown in Figure 26:



Anastasia Ransom [8lyebxi@37.com]
To: kimballs@bigfoot.com

asy DVD KIT

asy DVD KIT is a powerful tool to COPY DVD movie
CD/SVCD with just one click on your PC!
opy DVD movies to CD-R discs, convert DVD to VC
ACKUP-DVD it couldn't be easier! (see more)

opying a DVD is not difficult at all. Our guide incluc
structions and , which are easy to follow, even for

earn how to burn DVD's onto regular CD-R Discs!
/atch your new movies on any DVD player!
ot just the computer DVD! (see more)

EASY DVD KIT□FFFFAU is the Best!! Make quality b
personal DVDs. Create your own DVD library. Never
about scratching or losing a DVD again!

DOWNLOAD NOW !

Figure 26 Adding Junk e-mail to Lists

(11) http://www.petri.co.il/block_spam_with_outlook_2003.htm

Although this method is recommended by Microsoft often the individuals sending SPAM are equally as clever, and SPAM still remains difficult to combat because many spammers have a tendency to use multiple variations of the same address or different address to continue delivering their message. They can alter the names of the addresses ever so slightly so that the messages can't be blocked. Furthermore, the email addresses that they use are usually one time only, so those addresses may never be seen again. For example, the following address is blocked: ADV-consumerstoday.com, but it doesn't matter because email starts coming from ADV-booksonline.com, which isn't blocked. So the unblocked address is now blocked, now the user is receiving email from a different address. It is a constant battle to manage.

Senders can also be removed from the list. This is done by clicking on the message that has been mistaken as junk, and marking it "Not Junk" There is also an option within the Outlook toolbar entitled "Not Junk". An example is shown in Figure 27 below:

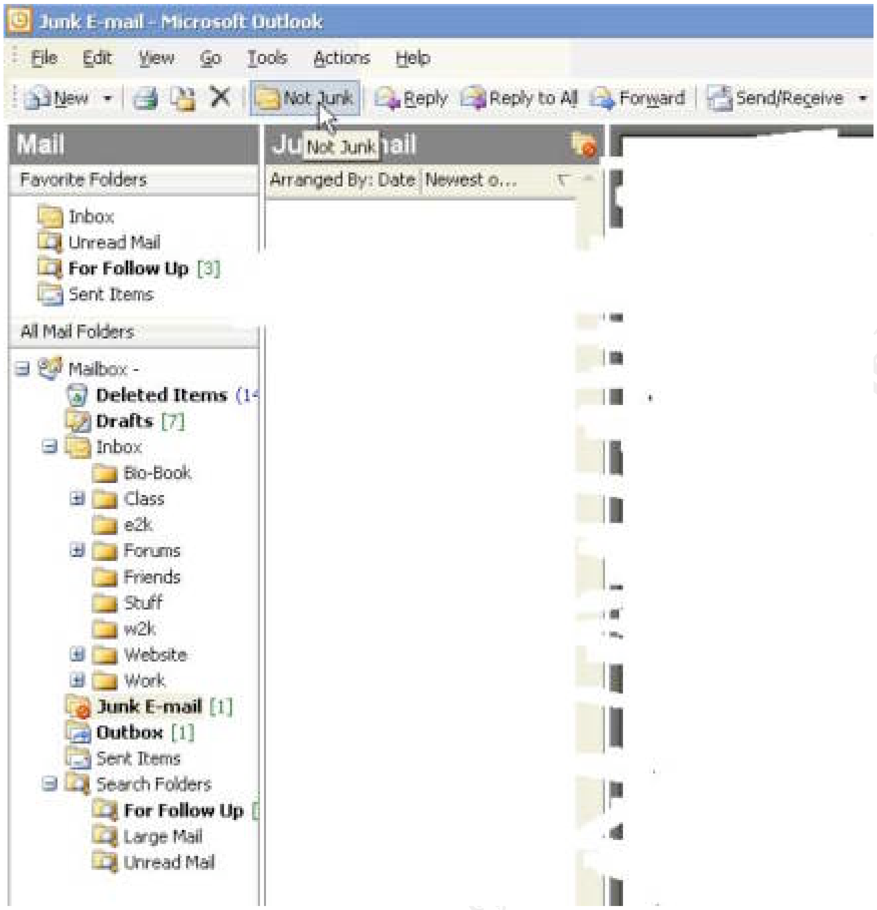


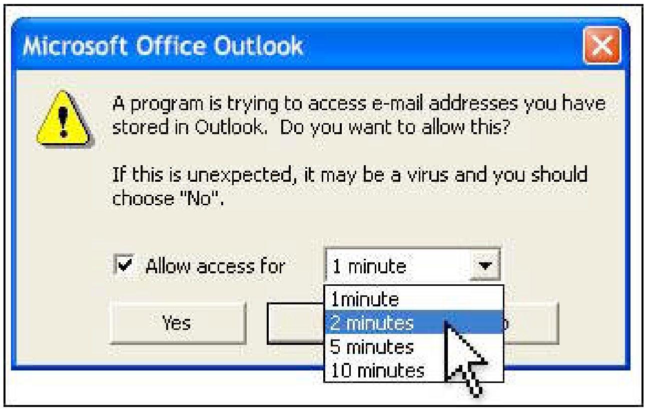
Figure 27 Not-Junk Option

(11) http://www.petri.co.il/block_spam_with_outlook_2003.htm

Outlook can also prevent SPAM by blocking HTML images and code from any sender that isn't on the list. This is good from the standpoint that SPAM does contain images and a lot of times they are appropriate. If it is configured it so that these type of images don't appear through email, it makes it less unpleasant for employees of the company, who might find certain images to be offensive. Preventing HTML scripts from running provides added protection against SPAM. Spammers sometimes plant scripts so that even more SPAM is received and can be used to compromise Internet Explorer to force spyware onto the computer of the client. So disabling HTML scripts is very wise.

Restricting access to the Outlook Address Book

In Outlook 2003, access is programmatically restricted to the Outlook Address book. The purpose of this is to prevent other programs from accessing the Address Book or Contact lists automatically. It also prevents unauthorized messages from being sent. Some programs need to access contact information, such as Palm Desktop for PDA synchronization, but a virus or any other malicious file can use this functionality for self propagation. A warning appears on screen, in the event that a program attempts to access the Address Book, like the one shown in Figure 28 below:



Microsoft Office Outlook

A program is trying to access e-mail addresses you have stored in Outlook. Do you want to allow this?

If this is unexpected, it may be a virus and you should choose "No".

☑ Allow access for 1 minute

Figure 28 Outlook Address Book Warning Message

(20) http://office.microsoft.com/assistance/preview.aspx?AssetID=HA011018701033&CTT=4&Origin=CH010393791033

Select “No” or select “Yes” and specify how the duration of the access.

Summary

Through the additions and enhancements in security that Information Rights Management, Kerberos and Outlook 2003, Anti-spam, and restricting access to the Outlook Address Book provide, Outlook 2003 has become much more secure for the client than previous editions. These enhancements not only address some of the SPAM issues on the client, but provide ways to protect documents insuring the confidentiality, integrity, and availability of the organization.

Conclusion

In conclusion, the new features and tools provided in Exchange Server 2003 such as restricting user access to the Exchange Server, disabling unnecessary services, enforcing message limits, restricting distribution lists to Authenticated Users, connection filtering, Inbound recipient filtering, IPSec on front-end and back-end clusters, anti-spoofing, Kerberos and Exchange 2003, and Exchange Intelligent Message Filter provide increased security and protect against vulnerabilities on the server.

The security enhancements found in Outlook 2003 such as Information Rights Management, Kerberos and Outlook 2003, Anti-spam, and restricting access to the Outlook Address Book protect against vulnerabilities on the client. By using Exchange 2003 and Outlook 2003 together, organizations can maintain their confidentiality, integrity, and availability. There is one common goal. This goal is to prevent SPAM and vulnerabilities in the enterprise and through continued security enhancements from Microsoft, and state laws and legislation, SPAM can be eliminated for good.

List of References

1. "Microsoft Exchange Server 2003 Security Enhancements"-Microsoft Corporation 2003
URL: http://www.microsoft.com/exchange/evaluation/Security_e2k3.asp

2. Cole, Graham -"Kerberos Security"
URL: http://www.mcmcse.com/win2k/guides/kerberos.shtml#howitworks

3. Hill, Brent-"IIS 6.0: The Next Generation" September 2001
URL:http://www.winnetmag.com/Article/ArticleID/21836/21836.html

4. Ruest, Danielle and Nelson-"Consolidate r Web servers with IIS 6.0" February 2004
URL:http://www.ftponline.com/wss/2004_03/magazine/features/nruest/page2.aspx

5. Shimonski, Robert J.-"Locking Down IIS 6.0 with .NET: The Default Security Wizard" 2002
URL:http://www.windowsecurity.com/articles/Locking_Down_IIS_60_with_NET_The_Default_Security_Wizard.html

6. Lowe, Scott-"Talking Shop: Analyzing the Microsoft Security Toolkit for IIS" 2001
URL: http://techrepublic.com.com/5100-6268_11-1031802-2.html

7. "How to Configure connection filtering to use Real Block Lists (RBLs) and how to configure recipient filtering in Exchange 2003"-Microsoft Corporation 2004
URL: http://support.microsoft.com/default.aspx?kbid=823866

8. Robichaux, Paul-"Secure Messaging with Microsoft Exchange Server 2003" 2004, pages 66, 70, and 343.

9. Petri, Daniel-"How can I configure Exchange Server 2003 to block spam?" 2004

URL: http://www.petri.co.il/block_spam_with_exchange_2003.htm

10. Petri, Daniel-“How can I configure Exchange 2003 to block unsolicited commercial e-mail (spam) with Intelligent Message Filter?” 2004
URL: http://www.petri.co.il/block_spam_with_exchange2003_imf.htm

11. Petri, Daniel-“How can I configure Outlook 2003 to block spam?” 2004

URL: http://www.petri.co.il/block_spam_with_outlook_2003.htm

12. Petri, Daniel- “What are the new security features found in Exchange Server 2003 in comparison to Exchange 2000?” 2004

URL: http://www.petri.co.il/new_security_features_in_exchange_2003.htm

13. Robichaux, Paul “Using IPSec with Exchange” 2003

URL: http://www.winnetmag.com/Articles/Print.cfm?ArticleID=38887

14. Posey, Brien M. “Get Anti-Spam savvy with Outlook and Exchange” 2004 pages.3-5

URL: http://asia.cnet.com/itmanager/netadmin/0,39006400,39179389,00.htm

15. Grimm, Michael and Nelte, Michael, “Exchange Server 2003 Security Hardening Guide” Microsoft Corporation 2004

URL: www.microsoft.com/exchange /library

16. Klein, Markus, “Implementing and Configuring Blacklist Support in Exchange Server 2003” 2003

URL:
http://www.msexchange.org/tutorials/Blacklist_Support_Exchange_2003.html

17. Fugatt, Mark “Restricting users from Sending and Receiving Internet Mail in Exchange 2003” 2004

URL: http://www.msexchange.org/tutorials/MF025.html

18. Shnoll, Scott “Stop Spam With Exchange 2003” 2004

URL: http://www.ftponline.com/wss/2004_03/online/sschnoll/default_pf.aspx

19. Morimoto, Rand “Microsoft Exchange 2003 Unleashed” 2003 pages 296, 311-317, 345, 346

20. URL: http://office.microsoft.com/assistance/preview.aspx?AssetID=HA011018701033&CTT=4&Origin=CH010393791033 Microsoft Corporation