



Securing Exchange Server 2007 Messaging

Using the Microsoft’s suite of security products to protect your Exchange Server 2007 environment

Published: November, 2006

For the latest information, please see http://www.microsoft.com/exchange

Contents

Introduction 1

Protecting your users from Viruses 1

Perimeter virus protection 2

Transport antivirus protection 7

Mailbox virus protection 7

Client antivirus protection 8

How it all works together 8

Protecting your users from spam 10

On-premise protection 10

Off-premise protection 12

Protecting your Internet clients 14

Encrypting the client session 14

Types of user authentication 14

Protecting e-mail content 15

Advantages of using Microsoft® Internet Security and Acceleration Server 2006 17

Choosing a Solution and Developing a Protection Plan 20

Choosing a Solution 20

Developing a Protection Plan 21

Conclusion 23

Appendix A – Anti-spam Technologies 24

# Introduction

Information system security is a hot topic and a major focus for most organizations. As technology spreads throughout your business, so do security threats associated with technology. E-mail, one of the most prevalent IT systems, reaches into all areas of business. It can pose a security threat because e-mail transports information between users and from the Internet to your user desktops.

E-mail security is a vast topic with several important aspects. Securing servers, securing clients, securing message transport, e-mail access and rights management, are all aspects of e-mail security that every organization must be vigilant about.

This paper deals with a particular aspect of e-mail security, securing e-mail transactions that involve the Internet. From the Internet, come messages from anyone. From the Internet, clients connect to internal corporate e-mail servers. This paper outlines the solutions available with Microsoft® Exchange Server 2007 than can help secure Internet clients and protect users from e-mail born viruses and unsolicited commercial e-mail, also known as spam.

### Viruses

Key findings in the 2006 CSI/FBI Computer Crime and Computer Survey show that “Virus attacks continue to be the source of the greatest financial losses.” A virus is a malicious computer program that can generate copies of itself and spread from computer to computer. Aside from propagating, most computer viruses or worms often carry a destructive payload that can collect and destroy information. This survey shows that a full 65 percent of computer system attacks are virus-related.

Exchange Server 2007 now offers multiple antivirus solutions for different types of organizations. This paper will outline those defenses and give you the guidance you need to choose the best option for your organization.

### Spam and Phish

It is estimated that spammers send approximately 55 *billion* messages a day. That’s roughly 8.5 spam messages per day for each person on earth, nearly double what was estimated a year ago, costing companies billions of dollars. Spam is sent by unscrupulous individuals and companies through an organization’s unprotected network to its users, consuming computer and network resources, along with the valuable time of your users. In addition to viruses and spam users are also potential targets for phishing. Phishing can mislead and deceive users into disclosing personal information such as credit card numbers and passwords.

Exchange Server 2007 now offers multiple anti-spam and anti-phishing solutions for different types of organizations. The list of anti-spam defenses offered by Exchange is long. This paper will outline those defenses and give you the information needed to decide which solution is best for you.

### Internet Clients

The 2006 CSI/FBI Computer Crime and Security Survey states; unauthorized access to networks is the second greatest source of financial loss to US companies. E-mail is a critical business communication tool that needs to extend beyond corporate walls to keep users connected and productive. Securing Internet clients to avoid unauthorized access to data can be challenging because the computers used to connect to the corporate network may not be owned or managed by the organization. To secure Internet client access, applications must protect data and user credentials, and must encrypt the connection from the Internet to the corporate network.

Microsoft offers security solutions for Internet clients to protect data and user credentials, and to encrypt the connection from Internet clients to the Exchange organization.

# Protecting Your Users from Viruses

Until recently, most Exchange administrators were content to run antivirus software at one or two locations in their e-mail infrastructure. In front of the Exchange servers to ensure scanning of message traffic before messages were delivered to Exchange mail stores, and/or on the Exchange mail servers themselves to allow both real-time and manual removal of viruses hidden in Exchange information stores. Exchange Server 2007 with Exchange Hosted Services and Microsoft Forefront Security for Exchange Server enhance virus protection at both the perimeter and on the mailbox server, as well as extending virus protection to include scanning messages during transport on the Hub Transport server. Scanning and detecting viruses during transport, before they reach the mailbox server, is preferred. In addition, virus protection on mailbox servers is meant to provide protection from changed or posted messages that may not leave these servers, and for detecting viruses with updated virus signatures after they’ve been delivered.

## Perimeter virus protection

Defending against virus laden messages entering your organization is the preferred first line of defense; that is, securing the perimeter of your network. Stopping unwanted and dangerous messages here reduces the potential for exposure because viruses are never allowed into your production network in the first place.

One of the many unique features of both Microsoft’s antivirus protection solutions is the integration and management of multiple antivirus engines at the most critical points in your network. Unlike most antivirus applications, Exchange perimeter and client antivirus solutions benefit from a multiple antivirus engine approach by integrating technologies from several different antivirus companies.

In a recent study conducted by AVTest.org, antivirus response data was collected for a four month period of time ending in July 2006. , Microsoft analyzed data on the amount of time each these engines took to publish new virus signatures as viruses were discovered. Five random combinations of the antivirus engines included with Forefront Security for Exchange Server were compared with single engine solutions from the leading antivirus firms.



Table 1

From this data you can clearly see the advantages of using multiple engines. With five different engines making up a set, the amount of time from virus discovery to signature update is greatly decreased in most cases when compared to antivirus solutions using a single antivirus engine. The sooner a virus signature is available, the sooner your organization will be protected. It’s like having five antivirus applications lined up in front of your Exchange organization but without the hassle of managing five different products.

The critical hours between the discovery of a new threat in the wild and the delivery of a signature to catch it leave a business highly vulnerable to attack. Dependence upon a single-engine solution only increases this risk. One security vendor may be first to deliver a signature for one threat, but last to deliver the signature for the next one, giving single-engine solutions fluctuating levels of effectiveness. With multiple-engine solutions multiple vendors are responding to a new virus at once, increasing the odds for a quick response and lowering a business’ overall risk of exposure to each new threat, regardless of its origin around the world.

Microsoft offers a choice of *two* different perimeter security solutions, each using multiple antivirus engines. Both provide best-of-class virus protection, but deliver it in different ways; on-premise or off-premise.



Figure 1

One decision you’ll make if you chose to implement the highest level of virus protection is whether to implement antivirus services within your perimeter network, using one or more Exchange Server 2007 Edge Transport servers with Forefront Security for Exchange Server, or outside your perimeter network as a hosted service, using Exchange Hosted Filtering. This section provides an overview of each solution to help you decide which option is best for your organization.

### On-site virus protection using Forefront Security for Exchange Server

Forefront Security for Exchange Server is an antivirus application that is used inside your production network on Hub Transport servers and Mailbox servers. It is also one of the solutions for perimeter antivirus and anti-spam security. For perimeter protection, Forefront Security for Exchange Server is installed on the Edge Transport server.



Figure 2

Forefront Security for Exchange server uses multiple antivirus engines to provide comprehensive protection on Edge Transport servers. It includes industry-leading antivirus engines from global security firms such as Kaspersky Labs, CA and Sophos. You can run up to five scan engines at once, and in different combinations across servers. This provides rapid response to new threats regardless of where the threat originates. Forefront Security for Exchange Server automatically downloads the latest signatures and can select the optimal combination of engines to use, ensuring a high level of protection and reducing the window of exposure to any given threat. Diversity of antivirus engines across messaging servers and client devices protects against a single point of failure in your IT environment. You can configure the engines with a weight, or bias, giving preference to individual engines or you can choose to have all chosen engines scan incoming and outgoing messages for viruses.

|  |  |  |
| --- | --- | --- |
| * Sophos Virus Detection Engine
 | * VirusBuster Antivirus Scan Engine
 | * CA InnoculateIT
 |
| * Norman Virus Control
 | * Microsoft Antimalware Engine
 | * Kaspersky Antivirus Technology
 |
| * CA Vet
 | * Authentium Command Antivirus
 | * AhnLab Antivirus Scan Engine
 |

Which virus engines you chose is up to you, based on the needs of your organization. Some engines are provided by large global organizations with mature virus signature libraries. Others excel at detecting viruses specific to a geographic region. Each uses slightly different technologies to detect viruses, for example pattern matching or heuristic engines, so that choosing five out of nine different independent antivirus engines, is like having five antivirus applications in front of your Exchange organization.

When Forefront Security for Exchange Server is implemented at the network perimeter on an Edge Transport server, each inbound or outbound message is delivered to the Edge Transport server and scanned by one or more of the antivirus engines. Each scanned message is stamped with an Antivirus Transport Stamp in Exchange Server 2007 to ensure that if a message is scanned once at an Exchange Server 2007 Edge or Hub server, it does not need to be scanned again later in the pipeline. The stamp makes virus scanning much more efficient because internal Exchange Server 2007 servers only have to scan outbound messages or those originating from within the organization. Mailbox servers with Forefront Security for Exchange installed will not spend cycles scanning messages that have already been scanned by the Edge Transport or Hub Transport server.

Virus signatures for the nine engines are collected by Microsoft and packaged for download by the Edge Transport server and other servers using Forefront Security for Exchange Server. A distribution server (Figure 3) can be configured so that the signatures are only downloaded once and then distributed to the remaining Forefront Security servers. For environments that have multiple Exchange Server 2007 servers, Forefront Server Security Management Console automatically distributes the signature and engine updates to all Forefront Security for Exchange Server 2007 deployments within the environment.

Messages that contain a virus can be quarantined on the Edge Transport server for review by an Administrator, cleaned (if possible) and delivered, or deleted.



Figure 3

Another key feature of Forefront Security for Exchange Server is attachment filtering. Exchange Server 2007 without Forefront can also block attachments, but these are blocked based on the file extension (.exe, .bat, .chm, etc.). Forefront Security for Exchange Server file filtering improves on this method by inspecting the attachment contents and blocking specific attachments regardless of the file extension. Therefore, if an executable is renamed .TXT it can still be blocked.

Forefront Security for Exchange server is a powerful antivirus solution that is recommended for all Exchange Server 2007 customers. Multiple virus-scanning engines and interoperability with Exchange Server 2007 both within the organization and on the perimeter makes Forefront Security for Exchange Server a complete on-premises antivirus solution. Whether Forefront for Exchange is the right perimeter antivirus solution for your organization depends on several factors outlined in this paper.

Exchange Server 2007 antivirus application programming interface (API) allows antivirus software vendors to integrate their applications with the different Exchange Server 2007 roles. Using this API, software vendors can write antivirus agents that interact with the built-in Exchange transport agents directly. As messages are introduced into an organization through an Edge Transport server or Hub Transport server, the transports can call the antivirus agent to inspect messages and filter those that contain viruses and stamp those that have been inspected so that they don’t have to be inspected again inside the Exchange organization.

### Off site virus protection using Exchange Hosted Filtering

The same type of multi-engine virus protection is provided by Microsoft Exchange Hosted Services. One service in particular, Exchange Hosted Filtering, provides anti-spam and antivirus protection for your organization. The virus protection provided by Exchange Hosted Filtering gives you the same level of protection as Forefront Security for Exchange Server on an Edge Transport server.



Figure 4

Blocking viruses before they reach the corporate network reduces the risk of infection and has the added benefit of increasing the resources available for corporate use. Because stopping viruses is time-critical, Exchange Hosted Filtering employs a layered approach to deliver zero-day protection for both inbound and outbound e-mail. Taking advantage of partnerships with numerous best-of-breed providers of antivirus technologies, Exchange Hosted Filtering ensures the most complete, up-to-date coverage against viruses and other e-mail threats. Heuristic engines scrub every message to provide protection even during the early stages of a virus outbreak. The service enjoys close developer relationships with its antivirus partners, integrating each antivirus engine at the API level. As a result, it receives and integrates virus signatures and patches before they are publicly released, often working directly with the antivirus partners to develop virus remedies. Virus signatures are applied to the global filtering network every 10 minutes.

With multiple datacenters worldwide, Exchange Hosted Filtering is very scalable and can continue to meet the filtering demands of your organization as you grow. Multiple large-scale datacenters also mean you’re protected from spikes in e-mail traffic and denial-of-service attacks. The service you’ll receive from Exchange Hosted Filtering is defined in a Service Level Agreement (SLA). The SLA details network availability (99.999 percent), performance, spam filtering (95 percent spam capture and 1:250,000 false positives), and virus detection (100 percent) for known threats. The average processing time to filter a message less than 1 megabyte (MB) in size is usually less than one second. With an SLA in place you know what to expect from a service that is protecting your organization from inbound spam and e-mail viruses.

An additional benefit of Exchange Hosted Services is the message disaster recovery feature that’s part of the Exchange Hosted Filtering package (Figure 5). This feature ensures that if your Internet connection goes down, inbound messages will queue in the Exchange Hosted Filtering cloud.



Figure 5

Once network and messaging services become available, EHF streams the messages into your organization at a pace that won’t overwhelm your network bandwidth or Exchange servers.

Deployment of Exchange Hosted Filtering doesn’t require any hardware procurement, software setup, maintenance or monitoring. Simply point your organizations mail exchange (MX) records to Exchange Hosted Filtering, setup some anti-spam preferences, configure your Exchange servers or firewall to only accept Simple Mail Transport Protocol (SMTP) from Exchange Hosted Filtering, and you’re ready to go.

**Different solutions to the same problem**

Exchange Server 2007 has two strong antivirus solutions for the perimeter. Both provide unmatched virus protection for your organization, but in different ways. Which perimeter antivirus solution is best for your organization is not based on which solution is better at protecting you from viruses, but which solution is best for the way your organization is run and the direction it’s heading. The differences between Exchange Hosted Filtering and Forefront Security for Exchange Server are not the level of virus protection each provides, but how each is implemented and maintained.

## Transport antivirus protection

Within your network, Exchange Server 2007 with Forefront Security for Exchange Server offers virus protection as messages flow through your organization. The Hub Transport server is specially suited for this role because of the compliance and other transport rules it was designed to enforce. When Forefront Security for Exchange Server is installed on a Hub Transport server, every message that passes through the hub that has not already been scanned for viruses is scanned by the multiple antivirus engines used by Forefront Security for Exchange Server.



Figure 6

When a Microsoft® Office Outlook® user sends a message to another Outlook user on the same Exchange Server 2007 Mailbox server, the sent message is passed to a Hub Transport server where transport rules are applied. When Forefront Security for Exchange Server is installed on the Hub Transport server, the message sent between two Outlook users on the same mailbox server is also scanned for viruses.

## Mailbox antivirus protection

Forefront Security for Exchange Server should also be installed on the Mailbox servers. Most messages that reach the mailbox store will have been scanned and stamped by either the Hub Transport server or the Edge Transport server (if used). With this architecture, Forefront Security for Exchange Server installed on a Mailbox server acts differently than Forefront Security for Exchange Server installed on a Hub Transport or Edge Transport server. Rather than scan messages upon submission, as with the Hub Transport and Edge Transport servers, messages are scanned upon access.



Figure 7

The Mailbox server also provides background scanning of messages in mailbox databases. Forefront installed on a Mailbox server does not have to scan every message submitted to the mailbox database because most messages will have already been scanned by Forefront on another Exchange server in the organization. Mailbox database scanning is therefore limited to messages that have not been stamped by another Forefront server and to messages that are scanned during background scanning. Background scanning on the Mailbox server is periodically performed on messages based on message age. Background scanning can be configured to:

* Scan all messages
* Scan only messages delivered in the past 1, 2, 3, 4, 5, 7, or 30 days
* Scan only messages with attachments
* Scan only messages that have never been scanned before

Only recent messages are scanned during each background scan, limiting the performance impact on the Mailbox server during a mailbox database scan.

Scanning messages when acted upon and with background scanning gives you virus protection for messages that are created or modified but never sent through the Exchange organization. For example, if a message is opened by a user, modified and saved, the message will be scanned during background scanning or if the message is sent.

Another important aspect of background scanning is how it works with new virus signatures. Background scanning is done on recent messages using all selected antivirus engines with the most recent updates. This means that if a message is received before a virus signature is available and makes it to the mailbox, the background scan will detect the virus in the message after the signature is available.

## Client antivirus protection

Although outside the direct scope of messaging security, client antivirus software is an important component of a complete messaging protection solution. In this context, client antivirus protection includes both client workstations and servers, such as Exchange Server 2007 servers.



Figure 8

Aside from Forefront Security for Exchange Server, all Exchange Server 2007 servers should also have the Forefront Client Security application installed to protect the server from non e-mail borne viruses. As with any client antivirus solution installed on an Exchange Server 2007 server, the directories that contain the mailbox and public folder databases and transaction log file should be excluded.

## How it all works together

Understanding how each Exchange role is used in a virus protection solution is important, because they each work a bit differently. Seeing how they work together highlights the advantage of having Forefront Security for Exchange Server installed on all Exchange Server 2007 servers. The following provides some examples:

Messages received from the Internet are scanned by the Edge Transport server with Forefront Security for Exchange Server (Figure 9), stamped as checked, passed to the Hub Transport server, and then delivered to the users Mailbox server. Since the message was stamped by the Edge Transport server, it is not scanned again during transport.



Figure 9

Messages received from the Internet using Exchange Hosted Filtering and Forefront Security for Exchange Server are scanned for viruses and spam in the Exchange Hosted Filtering cloud and again by the Hub Transport server before being delivered to the user mailbox (Figure 10).



Figure 10

Messages sent to the Internet are scanned and stamped by the Hub Transport server using Forefront Security for Exchange Server. The Edge Transport server does not rescan stamped messages before delivering to the Internet recipient (Figure 11)



Figure 11

Messages sent between users within the Exchange organization are scanned by a Hub Transport server with Forefront Security for Exchange Server (Figure 12)



Figure 12

# Protecting Your Users from Spam

As with antivirus protection, anti-spam protection is an integrated part of Exchange Server 2007. Spam controls can extend from the production network into the perimeter with an Edge Transport server or can extend into the Exchange Hosted Filtering cloud. Anti-spam protection has evolved into an approach that detects spam at several levels. Exchange Server 2007 extends this layered approach by improving existing methods of detection and with new methods for detecting spam. Exchange Server 2007 offers three different anti-spam solutions

* Hub Transport server configured with the anti-spam agents (on-premise)
* Edge Transport server (on-premise)
* Exchange Hosted Filtering (off-premise)

Each of these solutions is outlined below.

## On-premise protection

As with perimeter antivirus protection, Exchange Server 2007 offers a choice between on-premise and off-premise anti-spam protection. Two different levels of on-premise anti-spam protection can be implemented. The Hub Transport server with the anti-spam agents installed, an enhanced version of what is available in Exchange Server 2003 Service Pack 2 (SP2), can be implemented to provide basic anti-spam protection. Advanced anti-spam protection is implemented by using an Edge Transport server. This section focuses on the anti-spam protection provided by both of these solutions and the how they work.

### Connection-level protection

Keeping spam from ever entering your organization is the best strategy. Connection-level protection does this by not allowing the connection that would deliver the spam. Connection-level protection does this by evaluating each incoming SMTP connection for the probability that it is a source of spam. If the connecting SMTP host is identified as a host that sends spam or a host that would not normally send SMTP messages, the connection can be refused. This eliminates costly cycles spent determining if the inbound message is spam. Connection filtering is done in two ways, through Internet Protocol (IP) connection filtering and by using Reputation Lists.



Figure 13

Using IP connection filtering you can explicitly choose to deny SMTP connections based on IP address. This is the most rudimentary method of protecting an Exchange server because the connection-filtering lists are manually administered. Reputation lists are a more dynamic means of providing connection-level protection than through the use of block lists. Reputation lists are lists of IP addresses that are either known sources of spam, open relays, or part of an IP scope that should not include an SMTP host, such as an IP address from a dynamic IP address pool from a consumer Internet service provider (ISP). You can set the reputation list trigger threshold for blocking senders, exclude senders on the list to block, and how long to block the sender. The reputation service can also be configured to check if the sender is an open SMTP relay by simply trying to relay a message through the sending SMTP host.

### Protocol-level protection

SMTP messages that are allowed past connection-level protection are next analyzed at the protocol level. The SMTP dialog between the sending SMTP host and the receiving Exchange SMTP host is analyzed to verify that the sender and recipients are allowed, and to determine the sender’s SMTP domain name. Sender blocking allows you to specify individual SMTP addresses or domains to block. You can also disallow messages that have a blank sender address. Recipient filtering allows you to filter messages sent to a specific recipient. You can also block recipients who are not listed in the directory.



Figure 14

At the protocol level, Exchange Server 2007 also can enforce Sender ID. Sender ID attempts to verify that the sending SMTP host is approved to send messages from the domain specified in the sending e-mail address. Many spam messages are spoofed so that the message appears to come from a legitimate e-mail address. By deceiving the e-mail recipient into thinking the e-mail is from a legitimate authority (bank representative, customer service, etc.), users may be tricked into disclosing valuable information that can lead to identity theft or larceny. Sender ID attempts to reduce or eliminate spoofed messages.

### Content-level protection

After connection-level and protocol-level filtering have been applied to determine if an inbound message is spam, the next line of defense is to analyze the message content, on-premise content level protection can be implemented in one of two ways; by using the Hub Transport server with the anti-spam agents for basic spam protection and by using the Edge Transport server for advanced protection.



Figure 15

Both solutions offer similar anti-spam protection using a long list of anti-spam technologies (see Appendix A). However there are several very important benefits to using an Edge Transport server to protect your organization from spam:

* Edge Transport servers are deployed in your perimeter network and are not part of your domain. They securely receive directory and approved sender list information from a Hub Transport server, but do not initiate communications (other than SMTP) into your network. With this approach, no additional firewall ports need be allowed from your DMZ into your network. Hub Transport servers with the anti-spam agents require domain membership and a connection to the Microsoft® Active Directory® directory service.
* With more than 70 percent of SMTP mail being spam, an Edge Transport server isolates this traffic from your production network and Hub Transport servers inside your Exchange organization are free to perform routing, compliance, and other mailbox-to-mailbox operations.
* The Edge Transport server Rules Agent is built for anti-spam and anti-phishing. The Hub Transport server, even with the anti-spam agents, is built primarily for compliance.

When Forefront Security for Exchange Server is installed on a Hub Transport server with the anti-spam agents or an Edge Transport server, the server will receive daily Exchange Intelligent Message Filter (IMF) content filter updates, multiple intra-day IP reputation updates, and multiple intra-day spam signatures.

## Off-premise protection

As with virus protection, Exchange Hosted Filtering provides an off-premise anti-spam solution that includes an SLA that stops 95 percent of spam from entering your organization.

Exchange Hosted Filtering blocks a significant portion of spam at the edge of the Exchange Hosted Services network. Using several of the same types of technologies as on-premise protection, Exchange Hosted Filtering can also detect spam by analyzing common messages that are sent to all Exchange Hosted Filtering customers. Building a Real-Time Attack Prevention (RTAP) list, or reputation list, messages that are determined to be spam for one customer are identified as spam for all Exchange Hosted Filtering customers.



Figure 16

Once the message is allowed into the Exchange Hosted Filtering cloud it is evaluated by multiple filtering engines and an around-the-clock team of anti-spam experts. The spam signature database used by Exchange Hosted Filtering has over 20,000 spam signatures and rules. Each message is given a score; if the score exceeds the spam threshold, the message is classified as spam, which is quarantined by default.

Quarantined spam can be accessed by administrators or end users at any time through an intuitive web-based interface. Administrators can configure the filtering service to send each end user an HTML notification that lists newly quarantined spam. This improves the end user experience by making review of spam simple and effective. Exchange Hosted Filtering further enhances the experience for end users by offering the spam quarantine web-based interface and HTML notifications in several languages.

By stopping spam before it reaches your corporate network and Exchange Server 2007 servers, bandwidth and storage is preserved for legitimate corporate use. Another added protection you can use with Exchange Hosted Filtering is restricting allowed SMTP connections into your organization to only SMTP servers in the Exchange Hosted Filtering cloud. With this approach, SMTP threats such as denial of service attacks can be avoided. Also, if inbound Exchange service is interrupted, either because of network or server problems, SMTP messages addressed to your organization are queued by Exchange Hosted Filtering for 5 days, retrying every 20 minutes, until service is restored. Once it is restored, messages are streamed to your Exchange organization at a stable pace that won’t overload your network connection or Exchange server.

# Protecting Your Internet Clients

Internet clients fall into one of two categories for most organizations; computers that are managed by your organization and those that are not. Formulating a security policy that addresses each category is done using a combination of technology and user training. Exchange Server 2007 has several features that allow secure Internet client access. This section outlines those features and how they can be used to protect your Internet clients.

## Encrypting the client session

Aside from traditional session security that can be provided by a virtual private network (VPN), Exchange Server 2007 relies on Secure Socket Layer (SSL) encryption to encrypt client sessions outside your organization. Outlook Anywhere Access (RPC/HTTP), Microsoft Office Outlook Web Access, and Microsoft Exchange ActiveSync® all use SSL to communicate through your network firewalls to the Exchange Server 2007 Client Access server.



Figure 17

In addition to providing a secure connection, this common connection simplifies configuration and minimizes the number of ports necessary to open on your firewall.

## Types of user authentication

Authentication, which is different than encryption, uses credentials to verify access to network resources. Authentication can be provided using a couple of different mechanisms depending on the Internet client.

Exchange Server 2007 Client Access servers enforce the authentication mechanism used by Internet clients. Exchange Server 2007 virtual directories have two primary authentication methods:

* Digest authentication transmits passwords over the network as a hash value for additional security and is available only on Exchange Server 2007 virtual directories.
* Integrated Windows authentication does not prompt users for user names and passwords. Instead, the server negotiates with the Microsoft Windows® security package installed on the client computer. The authentication credentials are protected, but all other communication will be sent in clear text format so it is important to also use SSL to encrypt the session.

With kiosks and other unmanaged computers, both digest and basic authentication cache credentials can pose a security risk if the user kiosk cannot close the browser and end the browser process between sessions. This risk occurs because a user's credentials remain in the cache when the next user accesses the kiosk. If you cannot ensure that users can end a kiosk session or close browsers, and this is not an acceptable risk to your organization, consider using a product, such as Microsoft® Internet Security and Acceleration Server 2006, which incorporates two-factor authentication. Two-factor authentication requires users to present a physical token together with a password to use Outlook Web Access on the kiosk.

## Protecting e-mail content

Providing encrypted connections and secure authentication to Internet clients may not be adequate for some organizations when unmanaged computers are used. Additional services provided by Exchange Server 2007 can increase security and help keep corporate information within your organization.

### Web-ready document viewing

This innovative Exchange Server 2007 feature lets users view Microsoft Office documents using Outlook Web Access without using Microsoft Office. Viewing an attached document using Outlook Web Access requires the attached document be downloaded to a temporary location on the local computer and then opened using the application. Downloading the document to a kiosk computer moves corporate information from your internal network to an unmanaged computer. To prevent attached documents from being downloaded to the local computer, Exchange Server 2007 Outlook Web Access users can chose to open attachments as a Web page.



Figure 18

When web-ready document viewing is used, the Client Access Servers transcribes the attachment document, converting it to HTML and presenting it to the browser.



Figure 19

Web ready document viewing can be configured to ensure that viewed attachments are not downloaded to an unmanaged computer so they cannot be exploited by other computer users or processes.

### Attachment filtering

A more restrictive method of securing attachments is to apply attachment filtering. Attachment filtering disallows attachments from being displayed by Outlook Web Access clients.

### Local and remote wipe

Another security enhancement in Exchange Server 2007 is local and remote wipe of Microsoft Windows Mobile® 5 and Windows Mobile 6 devices. Local wipe is defined in a policy that defines how many times a Windows Mobile 5 or Windows Mobile 6 user can enter an incorrect password before the device is wiped. To avoid inadvertently wiping a device due to accidentally pressing keys while the phone is in your pocket or bag, the device prompts the user to enter a word or codebefore the final password attempt is allowed.

Remote wipe can be initiated by either an Exchange administrator or the user in Outlook Web Access. On the Options page of Outlook Web Access, users see the mobile devices they have registered and can initiate a remote wipe. The next time the device synchronizes with Exchange, the device is wiped. With Exchange Server 2007 SP1 a notification e-mail is sent to the user letting them know that the device was wiped. If, for example, the user finds the device before the wipe request is sent the user may choose to cancel the wipe request, Exchange Server 2007 SP1 facilitates that request.



Figure 20

### Windows Mobile Policies

In addition to configuring required passwords for Windows Mobile 5 and Windows Mobile 6 devices, new policies in Exchange Server 2007 SP1 allow administrators to enforce granular security polices for the next version of Windows Mobile. Policies can be configured to control items such as:

* The types of networks a device can connect to
* Encryption requirements for the device, storage card, and e-mail messages
* Allow and block specific applications on the device
* Disable key features of the device such as the camera and Wi-Fi capability

When creating policies for your mobile devices, be sure to take into account both the security requirements of your organization and the access level your users need.

## Advantages of using Microsoft Internet Security and Acceleration Server 2006

Most organizations have one or more firewalls that separate their production network from the Internet. If your organization does not, set this paper down (after reading this section) and go get one immediately. It only takes a few moments of looking at denied firewall traffic to be shocked at the number of Internet hosts trying to gain access to your network.

Microsoft’s Internet security solution is Microsoft Internet Security and Acceleration (ISA) Server 2006 (http://www.microsoft.com/isaserver/default.mspx). ISA can either be run on a server or be purchased as part of an appliance, like a traditional firewall.



Figure 21

### ISA Server 2006 is designed from the ground up to integrate very well with other Microsoft products like Exchange Server 2007. At its core, ISA Server 2006 helps protect your corporate applications, services and data across all network layers with stateful packet inspection, application-layer filtering and comprehensive publishing tools.

### Inspect encrypted traffic

### To guard against embedded attacks in HTTP traffic, ISA Server 2006 uses SSL bridging that allows SSL protected packets to be decrypted, inspected, and then re-encrypted.

### Publishing Web applications

The ISA Server 2006 Outlook Web Access Publishing Wizard walks you through creating a firewall rule and creates the Outlook Web Access SSL connection to your Exchange Server 2007 server. All network elements can be created in the wizard, and you never need to leave the wizard to create a policy element. The wizard also allows publishing of Exchange Server 2007 for remote access via Outlook Anywhere Access, Outlook Mobile Access, and Exchange ActiveSync.

### Load balancing and maintaining state as needed

The ISA Server 2006 Web farm load balancing feature provides real-time failover and load balancing of connections made through ISA Server 2006 to Exchange Server 2007 Web farms. This is accomplished without interrupting the stateful connection required by Exchange Server 2007 clients like Outlook Web Access.

ISA Server 2006 also integrates with Windows Server Network Load Balancing (NLB) to provide high availability of ISA 2006 Enterprise Edition arrays. This capability evenly distributes connections across array member servers to prevent network slow-downs related to impacted firewalls, while maintaining stateful connections so your users are not affected.

### Pre-authentication

Users can be authenticated using built-in Windows, Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), or Rivest, Shamir, and Adelman (RSA) SecurID authentication. Single sign-on is supported for authentication to Outlook Web Access. ISA Server 2006 can generate the forms used by Outlook Web Access sites for forms-based authentication. This enhances security for remote access to Outlook Web Access sites by preventing unauthenticated users from contacting the Outlook Web Access server

A list of new ISA Server 2006 authentication features includes:

* Single sign on (SSO) so that users authenticate once with ISA Server and then can access any number of servers that are behind ISA Server, including Exchange Server 2007 and Microsoft Windows SharePoint® Server 2007.
* Two-factor authentication using forms-based authentication and a client certificate for Outlook Web Access.
* Forms-based authentication support for publishing any Web server, including Exchange Server 2007 Outlook Web Access. Forms-based authentication and forms for mobile clients, are customizable and use of per-user-agent authentication schemes
* Delegation of credentials by using NTLM or Kerberos authentication. Kerberos constrained delegation is also supported.
* Password management allows ISA Server to check and report the status of the user's account. This feature can also be configured to enable Outlook Web Access users to change their passwords.
* Support for Active Directory authentication using LDAP. This way, ISA Server does not need to be a member of your domain to authenticate remote users, increasing security in your DMZ.

# Choosing a Solution and Developing a Protection Plan

Given all the information above you are now on your way to choosing the solution that is best for your organization and developing a protection plan. A protection plan is a part of a larger Exchange Server 2007 design architecture. Once you have a solution, you can develop your plan and then test, pilot, train, and implement it.

## Choosing a solution

There are two aspects of a messaging system design where you must strike a balance between your organization’s tolerance for risk and costs; service availability and security. You should weigh the cost of corporate information getting into the wrong hands, viruses affecting your servers and clients, and users spending time dealing with spam, against the cost of minimizing or eliminating viruses and spam and securing your corporate data.

### Factors used to choose an antivirus and anti-spam solution

Exchange Server 2007 offers different solutions to protect your organization from messaging threats. Each solution has a different cost. Which solutions are best for your organization depends on several factors, including:

* Your organization size
* The licensing model you purchase from Microsoft
* The make-up of your IT staff and their level of expertise
* Growth and acquisition plans
* Hardware purchase and maintenance costs
* Existence of a well managed DMZ
* The cost to your organization from downtime or information loss as a result of a security breach.

On-premise anti-spam and antivirus protection requires hardware and hardware maintenance, software and software maintenance, and a staff that can keep the on-premise protection up and running. For organizations that can support an on-premises solution, an Edge Transport server together with Forefront Security for Exchange offers an ideal virus and spam solution.

Exchange Hosted Filtering provides excellent anti-spam and antivirus protection with little management or oversight required by your organization. The subscription-based services can be purchased as part of an enterprise licensing agreement.

**An Edge Transport server and Forefront Security for Exchange Server may be the best solution for you if…**

* You have the IT staff to effectively manage Edge Transport servers in your DMZ.
* You have the hardware and software resources available to implement Edge Transport servers and Forefront Security for Exchange Server.
* You require the highest level of on-premises protection from viruses and spam.

**An Edge Transport server and Forefront Security for Exchange Server may not be the best solution for you if…**

* The combination of hardware and staff required to implement Edge Transport servers and Forefront Security for Exchange Server is prohibitive for your organization
* You have a limited number of users or IT staff.

**Exchange Hosted Filtering may be the best solution for you if…**

* You require full anti-spam and antivirus protection but do not have the staff to support Edge Transport servers
* Your organization’s plans for rapid growth and scalability is a concern
* You have a limited number of users so the subscription costs are cost effective compared to purchasing the hardware and software needed for Edge Transport servers

**Exchange Hosted Filtering may not be the best solution for you if…**

* Your organization has a policy against outsourcing IT services
* You have a large number of users and no enterprise agreement with Microsoft

Hopefully you won’t be faced with having to decide how much security your organization can afford. If cost is no concern, then the decision of which security solution to implement is based more on whether on-premise or off-premise protection is best for your organization.

Cost is usually a consideration. Determining what affect downtime, loss of data, and user inefficiency will have on your organization will help you decide, and justify, the level of security you choose.

## Developing a protection plan

Your Exchange Server 2007 architecture describes how Exchange Server 2007 will protect your organization from spam and viruses, and how it will protect your Internet clients. Each section below should be included in your architecture and should define how Exchange Server 2007 will be configured to provide the protection you require.

### Developing a remote client protection plan

Remote client protection begins by defining what remote clients you will allow. Many organizations today allow some form of mobile client. Most organizations also allow users to access their mailboxes using Outlook and or Outlook Web Access. Describing how each of these services will be implemented and how they will be configured is what makes up this part of your design architecture.

#### Mobile Outlook users

Outlook Anywhere Access is configured to allow RPC/HTTP connections from the Internet to your Exchange environment. This is very beneficial to users who take their laptops home or on the road and need to have access to the same tool they use in the office. Define how Outlook Anywhere Access users will connect to your organization.

#### Outlook Web Access and ActiveSync

Outlook Web Access and ActiveSync (mobile devices) use the same path to connect from the Internet to your organization but can be enabled independently. For Outlook Web Access, define the how they will connect (URL), how that connection will be secured (SSL), and what options you will allow (attachment blocking).

### Developing an internal network protection plan

The internal network protection plan is larger than Exchange and should exist outside of your Exchange architecture. Add to this plan how Exchange servers and clients will be protected from viruses and unauthorized access.

Some organizations choose to put a firewall between their servers and their *internal* clients. If this is the case, the internal firewall will have to accommodate Outlook connections as well as connections from Internet clients.

Other organizations have an internal network protection plan that relies heavily on Virtual Private Networks (VPN) to grant Internet access to internal resources. Allowing Exchange Internet clients access outside the VPN system should be addressed in the internal network protection plan.

Forefront Security for Exchange Server provides protection to messages as they travel through your internal Exchange Server 2007 environment. Where Forefront Security for Exchange Server will be installed (Hub Transport and Mailbox servers) and how it will be configured, updated, monitored, and maintained should all be included in your network protection plan.

### Developing a perimeter network protection plan

Most organizations that use a perimeter network also have a perimeter network protection plan or policy that defines what resources are allowed in the perimeter network and how those resources are kept secure. Your perimeter network protection plan should be updated to include how Exchange is going to pass messages and Internet client traffic through the perimeter network securely.

#### Using on-premise Edge Transport server protection

If an Edge Transport server and Forefront Security for Exchange Server are to be used in your organization, your Exchange Server 2007 design architecture should define the number and placement of servers. It should also define how those servers will be configured to protect your users from spam and viruses – the antivirus engines used; their weight and signature update frequency; what reputation lists will be used; and what other connection-level protection will be provided.

#### Using on-premise server protection without Edge Transport

If you choose to implement on-premises protection without an Edge Transport server, but on a Hub Transport server, your design architecture should include how the Hub Transport server will be configured to protect your users from spam and viruses, what antivirus engines will be used, and how often they will be updated.

#### Using off-premise protection

If you choose an off-premise solution Exchange Hosted Filtering belongs in your protection plan. The SLAs provided by Exchange Hosted Filtering and how they are monitored should be part of your design architecture. How users access quarantined messages, how the Hub Transport servers will be configured to only receive SMTP messages from Exchange Hosted Filtering, and Exchange Hosted Filtering policies customized for your organization all should be defined and documented in your design architecture.

### Developing a mailbox protection plan

Because viruses can only be detected after a signature has been downloaded that can identify the virus, it is possible that messages with viruses will make their way into user mailboxes. Developing a mailbox protection plan can mitigate this risk by scanning messages within user mailboxes for viruses with the latest signatures. The mailbox protection plan defines this level of protection. Forefront Security for Exchange Server installed on the Mailbox servers provides this protection and should be described in this section of the architecture – particularly the age of messages that Forefront Security for Exchange Server will scan and what Forefront Security for Exchange Server does with infected messages.

# Conclusion

Exchange Server 2007 provides several powerful security solutions. Which solution is best for your organization depends on several factors, but the goal is to protect your data and to keep your users productive. Choosing which solution is best for your organization comes down to your organization’s tolerance for risk and the cost of implementing a solution based on the size and complexity of your environment. Finding a balance between acceptable risk and cost will allow you to implement a solution that meets your organization’s security requirements, while keeping corporate resources secure and users online and productive.

# Appendix A – Anti-Spam Technologies

| Anti-spam technologies |  |
| --- | --- |
| **Spam Filtering** | Spam Filtering uses patented machine-learning technology from Microsoft Research known as Microsoft SmartScreen® technology. SmartScreen is currently used by Microsoft MSN®, Microsoft Hotmail®, Microsoft Office Outlook, and Exchange. Content filtering evaluates the textual content of the messages and assigns each message a rating based on the probability that the message is spam. This rating ranges from 1 to 9 and is stored as a message property known as the spam confidence level (SCL) rating. You configure the two content filtering values, one of which is that if messages are greater than that value, it will delete or archive them. The other value tells Outlook and Outlook Web Access to put the message in the user’s Junk E-mail folder. |
| **Anti-Phishing** | Content Filtering also provides anti-phishing protection. Phishing is a type of deception designed to steal your identity. In phishing scams, scam artists try to get you to disclose valuable personal data, such as credit card numbers, passwords, account data, or other information, by convincing you to provide it under false pretenses; for example, an e-mail message asking you to verify account information. The anti-phishing technology assigns an appropriate SCL value and the message is dealt with accordingly. |
| **Protocol Analysis Data Gathering** | Protocol Analysis Data Gathering analyzes connections and messages locally to identify spamming hosts. With this information, a local reputation list is built to block spam from hosts with a reputation of sending spam, which have open proxies or protocol anomalies. |
| **Dynamic Spam Update Service** | With the Dynamic Spam Update Service, content filter updates, IP reputation lists from Microsoft, and spam signature data is all downloaded from Microsoft periodically, depending on the version of Exchange used or if Forefront for Exchange is installed. |
| **Admin Quarantine** | Messages with a Spam Confidence Level (SCL) that exceeds the value you’ve configured in your content filter can be quarantined. Administrators can review messages in the quarantine and delete, archive, or forward them to recipients. |
| **Automatic DNS block lists** | Real-time block lists are lists of IP addresses maintained by third parties that keep track of known spam sources. Exchange queries the block list as connections are made and deny connections from IP addresses on the block list. |
| **Outlook Safe Sender List Aggregation** | Users can add senders from whom they always want to receive e-mail to their Safe Sender List in Outlook. Inbound messages that make it past connection and protocol filtering will be allowed to the recipient regardless of the assigned SCL rating. Safe Sender lists are propagated from the Exchange Mailbox server, through the Hub Transport server to the Edge Transport server in the DMZ. |
| **Outlook E-mail Postmark**  | Outlook 2007 can create a message-specific puzzle and solution, known as a postmark, which is attached to each outgoing message. The postmark requires a number of CPU cycles to create and decipher. Spammers generally don’t have the time or computational resources to attach complex individual puzzles and solutions to thousands of outgoing messages, so they don’t use them. Therefore, when a message with an attached postmark is received by Exchange Server 2007, it verifies the puzzle and solution. The more complex the postmark, the less likely that the message is spam |
| **Quarantine and Spam Reporting** | Anti-spam counters are provided to Performance Monitor that include:* Messages Per SCL level
* Total Messages sent to Quarantine, Deleted, Rejected
* Aggregated in Exchange 2007 Server MOM

Anti-spam reports available include:* Hit Rate for Block Lists
* Top spam sender domain, top spam sending IP
* Top targeted domain/recipient
 |



This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS
DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2006 Microsoft Corporation. All rights reserved.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Microsoft, Active Directory, Excel, Outlook, SharePoint, Windows PowerShell, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.