Hardening Exchange Server 2007 – Part II

Written by Marc Grote - mailto:grotem@it-training-grote.de

Abstract

In this small article series I will show you how to harden an Exchange Server 2007 environment with SP1 (Beta), installed on Windows Server 2008 (also Beta) as I wrote these articles. We will talk about the necessary steps how to harden the underlying operating system by only installing a minimal number of server roles and services. The second article will deal with installing and operating a secure Exchange Server 2007 installation and the third article will explain how to secure client access from OWA, POP3/MAP4 and how to fight against viruses and Spam.

Let's begin

Before we begin, please note that this article is based on a beta version of Windows Server 2008 and Exchange Server 2007 SP1 and it is possibly that some features will be changed or removed in the final versions of these products.

First, I do not want to write the same things that Rui Silva wrote in his article series about Hardening Exchange Server 2003 here at www.msexchange.org, so that I tried to only write some new things especially to Exchange Server 2007 and Windows Server 2008. If you want to find additional information about securing the environments, educating user and much more, I recommend reading his articles.

Trustworthy Computing

Microsoft said that Exchange Server 2007 is "Secure by Design". Exchange 2007 was designed and developed in compliance with the Trustworthy Computing Security Development Lifecycle (TWC) which was first introduced in October 2002. Microsoft has changed a lot in this system and multiple security related improvements were built into Exchange Server 2007. Microsoft says that Exchange Server 2007 is more secure than earlier versions of Exchange.

Secure by default

Microsoft tried to secure Exchange Server 2007 with existing security technologies. One goal was that nearly every important traffic should be encrypted by default. Except for Server Message Block (SMB) cluster communications and some Unified Messaging (UM) communications, Microsoft has met this goal. Exchange Server 2007 is the first messaging system from Microsoft which uses self-signed certificates. In addition Exchange Server 2007 uses Kerberos for special communications, Secure Sockets Layer (SSL) and other encryption techniques.

Certificates

Exchange 2007 uses X.509 certificates to establish secure Transport Layer Security (TLS) and Secure Sockets Layer (SSL) transport channels for communication with protocols such as HTTPS, SMTP, IMAP4 and POP3.

Please note

POP3 and SMTP access is deactivated by default like in previous versions of Exchange Server

Exchange Server 2007 uses certificates for several components.

SMTP

Certificates are used for encryption and authentication for Domain Security (new in Exchange Server 2007) between different Exchange organizations. Certificates are used for secure connections between Hub Transport servers and Edge Transport servers. Every SMTP communication between Hub Transport servers is encrypted.

EdgeSync synchronization

Exchange Server 2007 uses a self-signed certificate to encrypt the LDAP communication between the Edge Transport servers ADAM instance and the internal Active Directory server over which the Microsoft Exchange EdgeSync service communicates with Active Directory to replicate Active Directory information to ory to the ADAM instance on the Edge Transport server.

POP3 and IMAP4

Exchange Server 2007 uses certificates to authenticate and encrypt every session between Post Office Protocol version 3 (POP3) and Internet Message Access Protocol version 4 (IMAP4) clients and Exchange Server 2007.

Unified Messaging

Certificates are used to encrypt the SMTP session to Hub Transport servers and to the Unified Messaging (UM) IP gateway.

Autodiscover

Certificates are used to encrypt the HTTP communication between the client and the Client Access server (CAS).

Client Access applications

Exchange Server 2007 uses certificates to encrypt the communication between a Client Access Server and clients like Outlook 2007 (Outlook Anywhere aka RPC over HTTPS), Microsoft Outlook Web Access (OWA), and Exchange ActiveSync.

For security purposes, Microsoft recommends using certificates from own internal certification authorities ore commercial third party certification authorities if you have

a lot of clients accessing Exchange Server 2007 from non domain member computers.

Messaging connectors

Exchange Server 2007 uses several connectors to relay traffic from source to destination servers. Exchange Server 2007 uses two different types of connectors. Connector for inbound traffic which can be configured on every Exchange Server 2007 and one or more connectors fro outbound mail traffic which focus is Exchange organization wide.

Exchange Server 2007 supports a lot of different authentication mechanism to secure the message transport or to secure the authentication or both.

You can use:

- Transport Layer Security (TLS)
- Domain Security (Mutual Auth. TLS)
- Basic Authentication after starting TLS
- Exchange Server authentication
- Integrated Windows Authentication

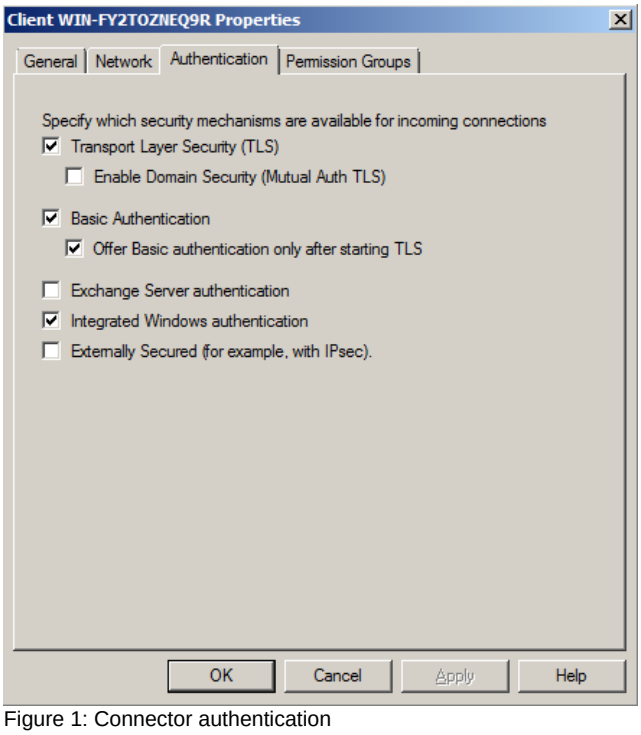

Figure 1: Connector authentication

You can read more about securing SMTP message flow between different Exchange Server 2007 organizations in my article on www.msexchange.org. You will find the link to this article at the end of this article.

Microsoft Edge Transport Server

The Microsoft Edge Transport Server role is a role that must be exclusively installed on A Windows Server 2003 or Windows Server 2008 machine. Edge Transport

servers are the messaging relay servers of Exchange Server 2007 and in addition they provide integrated Anti Spam functionality and optional anti virus functionality with Microsoft Forefront Edge Scurity or other third party products. A Microsoft Edge Transport Server is installed into a Windows workgroup and is not part of a domain. Edge Transport Server uses AD/AM (Active Directory Application Mode) to synchronize relevant Active Directory data with the Edge Transport Server. The synchronization process is called Edge sync.
Edge Transport Server provides feature like:

- Content Filtering
- IP Allow and Block List Provider
- Sender Filtering
- Sender Reputation
- SMTP Tarpiting

and many more.

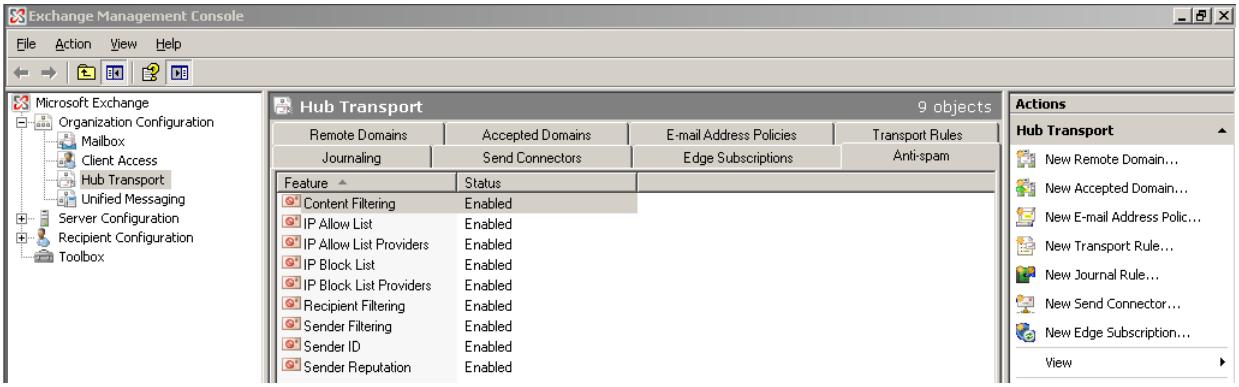

Figure 2: Edge Server Anti Spam

Microsoft Forefront

Microsoft Forefront is a Anti Virus and Anti Spam solution from Microsoft which is available for several Microsoft products like Exchange Server 2007, Microsoft Sharepoint Portal Server, Microsoft Windows clients and more. One solution for Microsoft Exchange is Microsoft Forefront Edge Security. You can use Forefront Edge Security on Microsoft Edge Transport Server and Hub Transport Servers, but it is recommended, using Forefront Edge Server Security in your DMZ on Microsoft Edge Transport servers. You will find more information about Microsoft Forefront here.

Functions of Microsoft Forefront Security

- Provides layered protection through Multiple Scan Engine Management to secure messaging systems
- Offers sophisticated scanning options for added value and flexibility, including:
- "In-memory" scanning that minimizes impact on Exchange servers for optimum protection and efficiency
- Real-time, scheduled, and on-demand scanning of multiple storage groups and databases

- Full protection of Outlook Web Access
- SMTP and Exchange Information Store scanning for reinforced protection and performance
- MTA message scanning for all messages routed through Exchange MTA Connectors (X.400, MS Mail, CC Mail, etc.)
- Includes Microsoft-approved virus scanning API integration for Exchange 2000 and 2003
- Minimizes worm-generated spam and safeguards the Information Store through Forefront® Worm Purge™
- Identifies all messages with unwanted attachments through flexible file-filtering rules
- Diverts infected attachments into a quarantine repository with Forefront® Quarantine Manager
- Automatically uploads the latest virus signatures
- Notifies administrators of virus incidents and scan events through e-mail, event logs, and SMTP pagers
- Includes customizable multiple disclaimers for outbound messages based on sender, recipient, and domain name criteria set by administrators

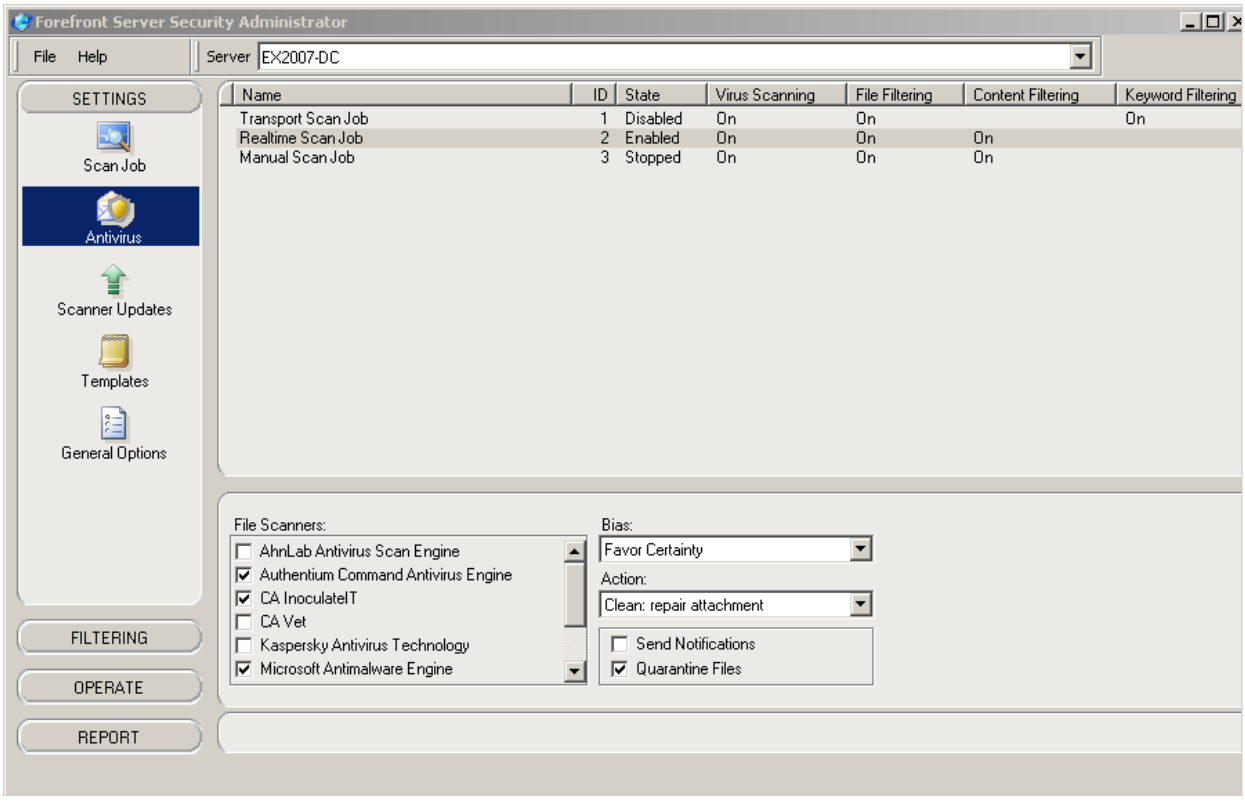

Figure 3: Microsoft forefront Security

Security Configuration Wizard (Windows Server 2003 SP1)

Exchange 2007 provides an SCW template for each Exchange 2007 server role. By using this template with the SCW, you can configure Windows Server 2003 to lock down services and ports that are not needed for each Exchange server role. When

you use the Security Configuration Wizard, you create a template XML file which you can use to secure this or other Exchange Sever 2007.

Figure 4: Security Configuration Wizard

Because the SCW was first introduced with Windows Server 2003 Sp1 – before Exchange Server 2007 was RTM, you must enable the SCW to configure Exchange Server 2007. Exchange Server 2007 comes with two SCW config file which you must install on the server from where you want to run the SCW.

For Hub Transport server

scwcmd register /kbname:Ex2007KB /kbfile:"%programfiles%\Microsoft\Exchange Server\scripts\Exchange2007.xml

For Edge Transport server

scwcmd register /kbname:Ex2007EdgeKB /kbfile:"%programfiles%\Microsoft\Exchange Server\scripts\ Exchange2007Edge.xm

Conclusion

In this second part of this small article series we discussed how to secure Exchange Server 2007 and it's subcomponents by using Edge Transport Servers, Anti Spam and Antivirus technologies and the third article will show you how to secure client access to Exchange Server 2007 but also some necessary configuration changes in the Exchange Server 2007 configuration. Please note that this article could not focus all security enhancements and new security features of Exchange Server 2007.

Links

Exchange Server 2007 – Security and protection
http://technet.microsoft.com/en-us/library/aa996775.aspx

Securing Exchange Server 2007 Client Access
http://technet.microsoft.com/en-us/library/bb400932.aspx
Hardening an Exchange Server 2003 Environment (Part 1)
http://www.msexchange.org/tutorials/Hardening-Exchange-Server-2003-Environment-Part1.html
Hardening an Exchange Server 2003 Environment (Part 2)
http://www.msexchange.org/tutorials/Hardening-Exchange-Server-2003-Environment-Part2.html
Hardening an Exchange Server 2003 Environment (Part 3)
http://www.msexchange.org/tutorials/Hardening-Exchange-Server-2003-Environment-Part3.html
Hardening an Exchange Server 2003 Environment (Part 4)
http://www.msexchange.org/tutorials/Hardening-Exchange-Server-2003-Environment-Part4.html
Introduction to Exchange 2007 Server Roles
http://www.msexchange.org/tutorials/Introduction-Exchange-2007-Server-Roles.html
Microsoft Forefront
http://www.microsoft.com/forefront/default.mspx
Edge Transport Server Role: Overview
http://technet.microsoft.com/en-us/library/bb124701.aspx
Microsoft Trustworthy Computing
http://www.microsoft.com/mscorp/twc/twc_whitepaper.mspx
Securing SMTP Message Flow between different Exchange Server 2007 organizations
http://www.msexchange.org/tutorials/Securing-SMTP-Message-Flow-between-different-Exchange-Server-2007-organizations.html