Hardening Exchange Server 2007 – Part I

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.

Exchange Server 2007 permissions

In Exchange 2003, the following security roles were available through the Delegation Wizard in Exchange System Manager:

- Exchange Full Administrator
- Exchange Administrator
- Exchange View Only Administrator

This model was relative static and doesn't provide granular access out of the box. This permission model was often a problem in large and largest environments where it is absolutely necessary to distribute different administrative work to different users and groups without negative effecting security in Windows Server 200x and Exchange Server 2007. Exchange Server 2007 comes with a completely different permission model. There are new administrator roles that are similar to the built-in Windows Server security groups and you can use the Exchange Management Console (EMC) and the Exchange Management Shell (EMS) to view, add, and remove members from any administrator role.

There are different areas of Exchange permissions:

- Global Data
- Recipient Data
- Server Data

Global data

Global data is not associated with a specific Exchange Server and is stored into the Active Directory configuration container which is replicated forest wide, so only trusted users should have access to this data.

Recipient Data

Recipient data are Exchange recipients in the Active Directory domain partition. Recipient data contains e-mail enabled users, contacts, distribution groups and mailboxes and something more.

Server Data

Server data is Exchange specific data in the Active Directory domain partition under the specific Exchange Servers object. Examples of this data include receive connectors (send connectors are forest wide), virtual directories and many more.

Exchange Server 2007 Administrators

- Exchange Organization Administrators
- Exchange Recipient Administrators
- Exchange View-Only Administrators

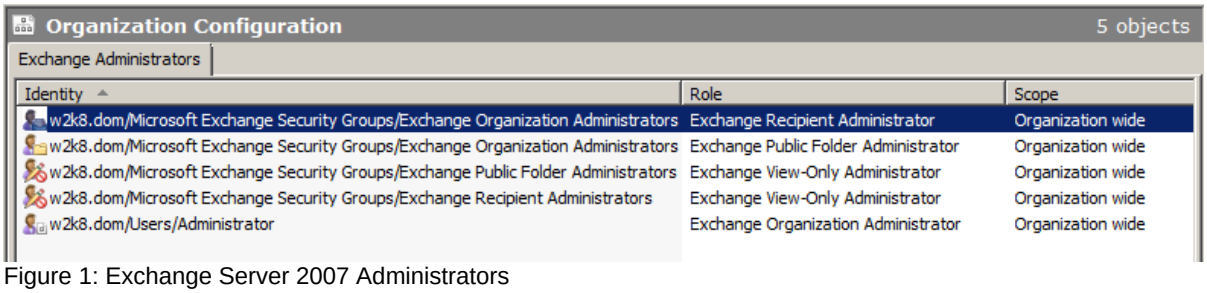

Figure 1: Exchange Server 2007 Administrators

As a final overview I used the table of the different Exchange Server permission roles from the Microsoft TechNet website which should give you a good understanding how to use the different Exchange permissions.

Administrator role	Members	Member of	Exchange permissions
Exchange Organization Administrators	Administrator, or the account that was used to install the first Exchange 2007 server	Exchange Recipient Administrator Administrators local group of <*Server Name*>	Full control of the Microsoft Exchange container in Active Directory

Administrator role	Members	Member of	Exchange permissions
Exchange Recipient Administrators	Exchange Organization Administrators	Exchange View-Only Administrators	Full control of Exchange properties on Active Directory user object
Exchange Server Administrators	Exchange Organization Administrators	Exchange View-Only Administrators Administrators local group of <*Server Name*>	Full control of Exchange <*Server Name*>
Exchange View-Only Administrators	Exchange Recipient Administrators Exchange Server Administrators (<*Server Name*>)	Exchange Recipient Administrators Exchange Server Administrators	Read access to the Microsoft Exchange container in Active Directory. Read access to all the Windows domains that have Exchange recipients.
Exchange Servers	Each Exchange 2007 computer account	Exchange View-Only Administrators	Special

Table 1: Exchange Server 2007 permission – Source: Microsoft Technet

Property Sets in Exchange Server 2007-11-06

You can use property sets in Exchange Server 2007 for attribute grouping that enables access control for specific object properties. Property sets use one single Access Control Entry (ACE) instead of an ACE for each individual property. Exchange Server 2007 creates two new property sets exclusively for itself and doesn't use existing Active Directory property sets. During Active Directory Schema extension, Exchange Server 2007 performs the following actions:

- Extends the Active Directory schema with new classes and attributes.
- Creates the property sets for Exchange Server 2007 and Exchange Information and Exchange Personal Information.
- Adds the appropriate attributes to the Exchange Information and Exchange Personal Information property sets.

Exchange server roles

Exchange Server 2007 introduces a new role based concept. It is possible to install five different Exchange Server 2007 roles. These roles are:

- Mailbox server role
- Hub Transport server role
- Client Access server role
- Unified Messaging server role

- Edge Transport server role

Every role has special functions and enterprises can combine several roles on the same or different machines. All roles can be combined without one exception: The Edge Transport Server role cannot be installed with other Exchange roles on the same machine. This is also true for the Active and passive Exchange Cluster service node, but the Exchange Cluster function will not fall into a Exchange server role category.

Exchange Server 2003 officially never had a role based installation but it was possible to configure one or more servers as a Front End Server (like the Exchange Server 2007 CAS role). A server which holds mailboxes and public folders in a Front End Server scenario is called Exchange Back End Server. With Exchange Server 2003 it is also possible to configure an Exchange Server as a mail routing server only. This Server doesn't have mailboxes and public folder databases but is responsible for e-mail routing.

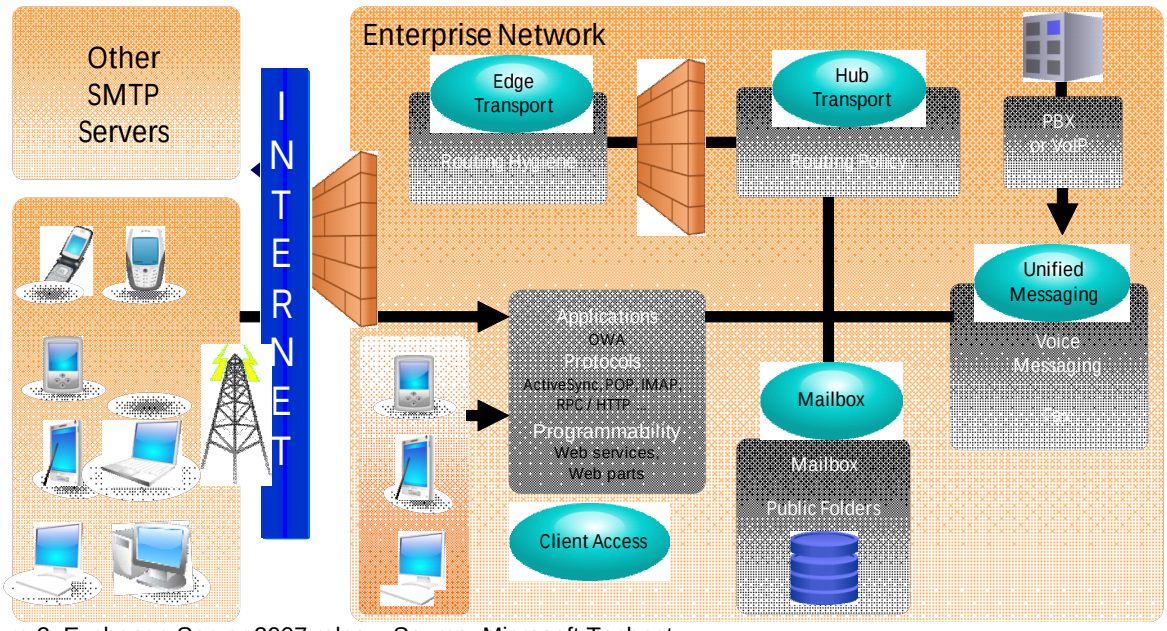

Figure 2: Exchange Server 2007 roles – Source: Microsoft Technet

Firewall

Windows Server 2008 Firewall with advanced networking is per default turned on for incoming and outgoing connections. It is possible to manually configure Firewall port extensions or programs which are allowed to communicate with other hosts. The Security Configuration Wizard which was used in Windows Server 2003 SP1 to Establish a role based security configuration, which was responsible to create Firewall exceptions based on the configured roles is no more used in Windows Server 2008. Windows Server 2008 uses a new tool called Server Manager and it's corresponding tool ServerManagerCMD.

Please note:

Don’t compare Server Manager from Windows Server 2008 with the Server Manager in Windows NT4. These are total different programs.

The Server Manager in Windows Server 2008 is used to provide role based security for installed Windows services and features, but I think that the Server Manager will be used in the future for advanced role based security for installed applications like Microsoft SQL Server 200x and more. With the current Windows Server 2008 Beta version and the Beta version of Exchange Server 2007 SP1, the Exchange setup opens the required ports and programs depending on the Exchange roles you install.

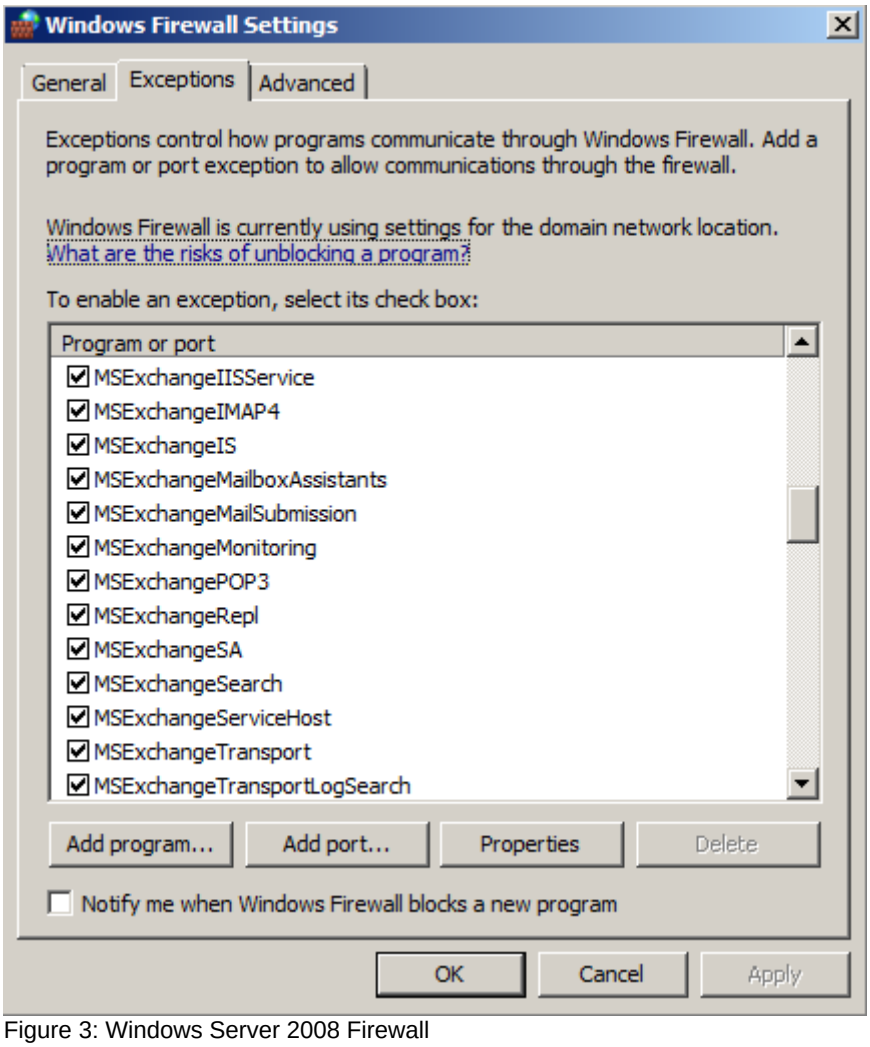

Figure 3: Windows Server 2008 Firewall

Installed Exchange Server 2007 services

Depending on the Exchange roles selected during installation, only the necessary services will be installed and there is no much clearance to provide additional security.

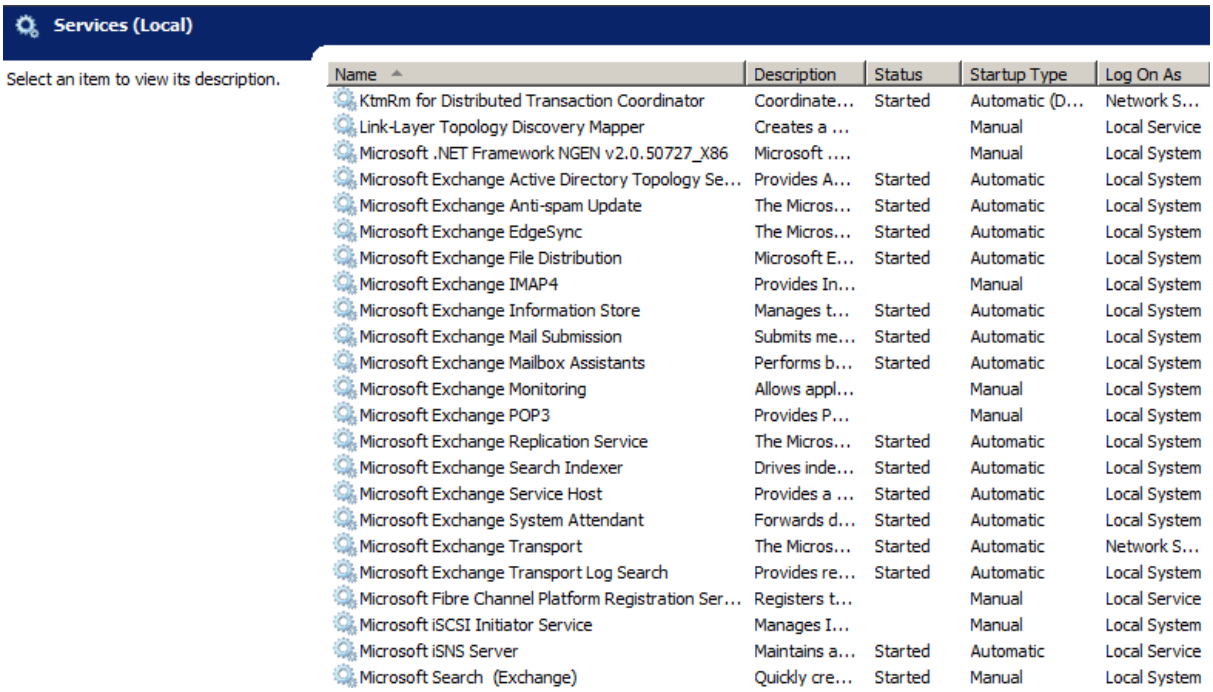

Figure 4: Exchange Server 2007 services on Windows Server 2008

Conclusion

In this first part of this small article series we discussed some methods how to harden the underlying operating system Windows Server 2008 and how some parts of the Exchange Server 2007 role based installation plays an important part in an entire security solution. We also discussed the new Exchange Server permission model and talked about installed Exchange Server 2007 services. The second part of this article will deal with securing Exchange Server 2007 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.

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