Secure secure SMTP mail flow between different Exchange Server 2007 organizations

In this article, I will show you how to create secure SMTP traffic mail flow between Exchange Server 2007 systems in various Exchange organizations. Protecting SMTP traffic between Exchange 2007 organizations is much simpler than its previous versions.

In this article, I will show you how to create secure SMTP traffic mail flow between Exchange Server 2007 systems in various Exchange organizations. Protecting SMTP traffic between Exchange 2007 organizations is much simpler than its previous versions.

The basics

Is it necessary to protect SMTP traffic between different Exchange Servers? Let's try a little test later.

Launch the network detector with your favorite traffic analyzer. In this example, I use Microsoft Network Monitor 3.0. While the network detector is running, start the Telnet session in Exchange Server with port 25 and send a message through it. Stop the Netmon detection program and filter the traffic packed by the SMTP protocol. What do you see? Yes, the entire authentication program of the SMTP session is plain text!

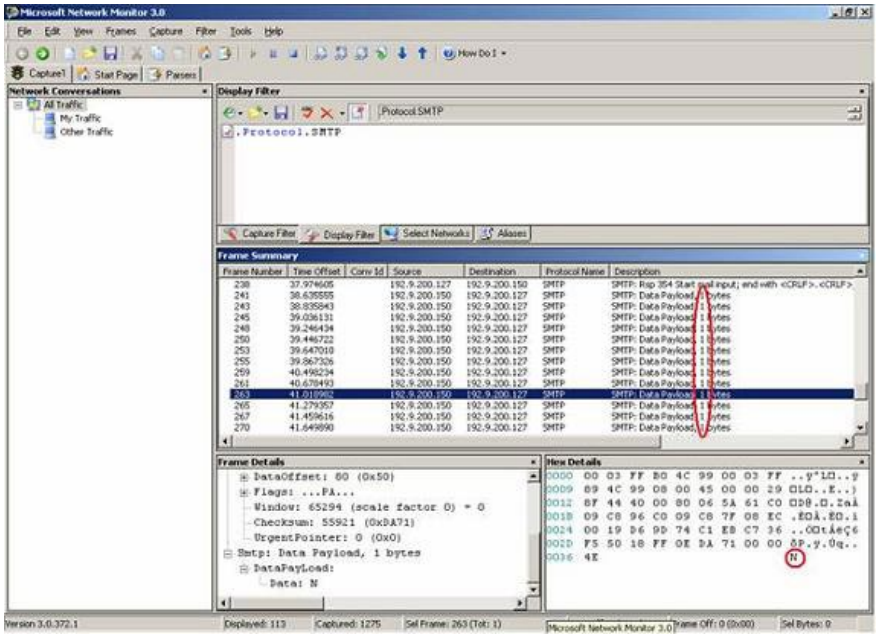

Figure 1: Detection of SMTP networks with Netmon

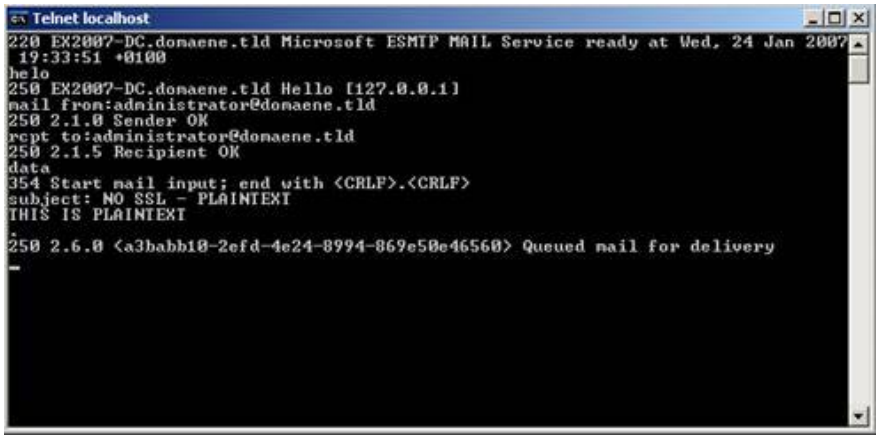

Figure 2: Sending an SMTP message via Telnet

Now, you know that you need to deploy some security programs between Exchange Servers. But which solution is best? If IPSEC is used, what will it mean when it is dynamic? At the very least, you must use 'pre-shared' keys to deploy IPSEC between servers. And the program will work well if your Exchange server number is only a few. Another solution, deploy IPSEC on multiple Exchange Server systems, use certificates. If you want to deploy certificates between Exchange Servers, you will need a PKI (Public Key Infrastructure).

There is another new solution in Exchange Server 2007 that uses built-in functions.

Exchange Server 2007 uses some of the following methods to ensure integrity and encryption for mail:

1. Mutual TLS
2. Opportunistic TLS
3. Direct Trust
4. Domain Security

Mutual TLS

TLS (Transport Layer Security), ie the transport layer security protocol is the continuation of Secure Sockets Layer (SSL) - a secure socket layer protocol. SSL is used to encrypt mail flow in Exchange 2007. The Multual term means that both Exchange Server systems in the mail delivery process will check the TLS certificate before the connection is established. Mutual TLS is deployed in the configuration, in which both the sender and the receiver authenticate each other before sending data.

Opportunistic TLS

Opportunistic TLS is a new component in Exchange 2007. Exchange Server 2007 attempts to secure mail flow to another Exchange 2007 system, or to an external mailing system. It also tries to allow a TLS session with another mailing system in the form of an anonymous TLS request. This is different from Exchange 2003. In Exchange 2003, you must enable TLS 'manually' between two different Exchange Server systems.

Direct Trust

All mail traffic is automatically encrypted between Exchange Server systems, regardless of the role used as the Hub Transport or Edge Transport. The Direct Trust does not use the validation mechanism of aggregated X.509 certificates. Instead, it uses a direct validation mechanism for the presence of a certificate in Active Directory. You will not have problems using self-signed certificates or internal certificate authentication mode.

Domain Security

Domain Security is a combination of different technologies and components, such as certificate management programs, Exchange Server connector functions and the operation of email support services (Microsoft Outlook 2007). The purpose of building Domain Security in Exchange Server 2007 also aims to establish a secure connection with Mutual TLS.

Implement TLS security

In order to secure mail flow with mutual TLS, you can use Hub Transport servers. Or if you have deployed the Edge Server, you can also use it with Exchange Server systems.

In the first step, you must set up a trusted Forest certificate with two Exchange organizations. At least you must add the Root CA certificate from the external Certification authority (CA) authentication mechanism to a trusted Root CA certificate stored on the Hub Transport or Edge Transport Server. If there are multiple Edge or Hub Transport Servers, it is better to deploy the CA certificate to trust or add the Root CA certificate to the Trusted Root CA store via Group Policies. The figure below shows the organization's Root CA certificate image.

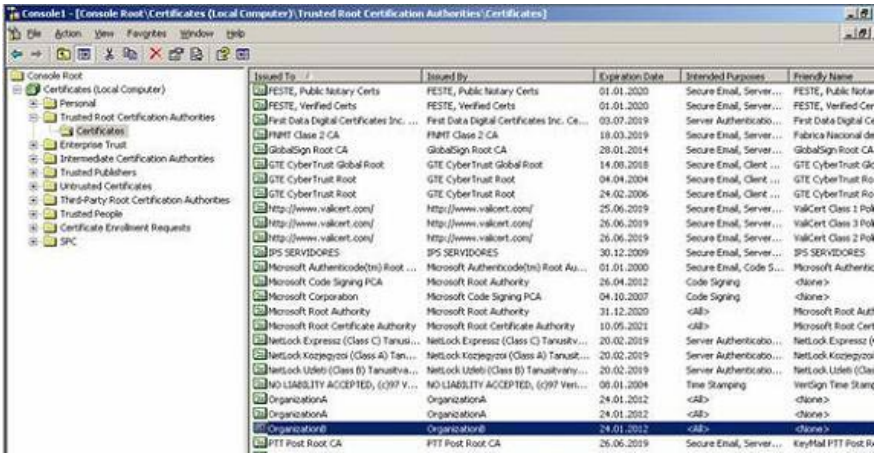

Figure 3: Root CA certificate from another Exchange organization.

Subject Name

Subject Name holds an important position in certificates used by Exchange 2007. The object name of a TLS certificate is used by DNS identification services. The DNS identity service will call the object name of a certificate and compare it to the request. ISA Server is a good example. When launching Outlook Web Access or Outlook Anywhere in an HTTPS bridge, their name on the certificate must exactly match the name in the URL, which is used to access OWA or Outlook Anywhere. The Subject Name field in a certificate binds that certificate to a single server or to a particular domain name.

The following table gives you an overview of the frequently used Relative Distinguished Names, ie RDN.

TenViet tatKieuKich large suatMuc nhatMuc large nhattan use in evidence in the self chiYeu cauTrat tuongNuoc / VungCASCII2111Domain Component (domain component) DCASCII255Nhieu1Bang or TinhSUnicode 12812Vi triLUnicode12813To chucOUnicode 64114Don organization have calculated chucOUUnicode64Nhieunhieu5Ten chungCNUnicode64Nhieu16

Table 1: Relative Distinguished Name names are commonly used.

Request a certificate

The next step is certificate requests, through the Exchange Management Shell. The certificate request file can be used to issue a certificate from the internal CA.

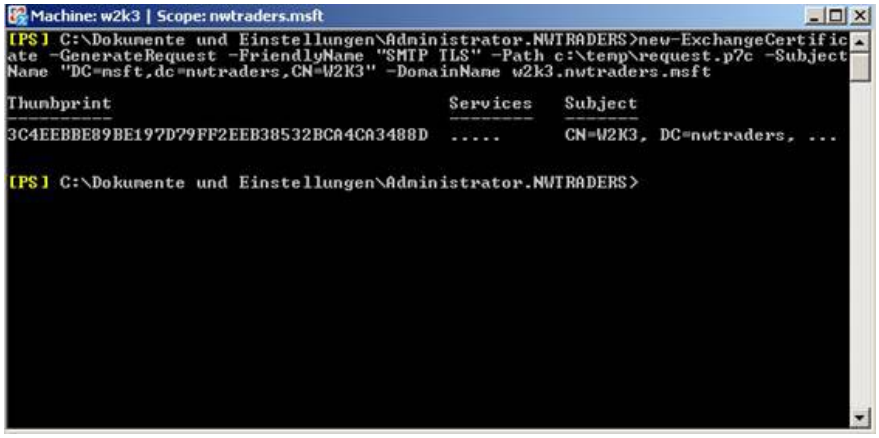

Figure 4: Requesting an Exchange certificate.

Open the CA web console and issue a certificate request using either PKCS # 10 file or 64-bit encrypted CMC file.

Figure 5: Allow the certificate with the web console.

The figure below shows an example of a certificate request file. If your browser does not allow file opening, you can copy and paste the entire text from the request file into the certificate request area of ??the web console.

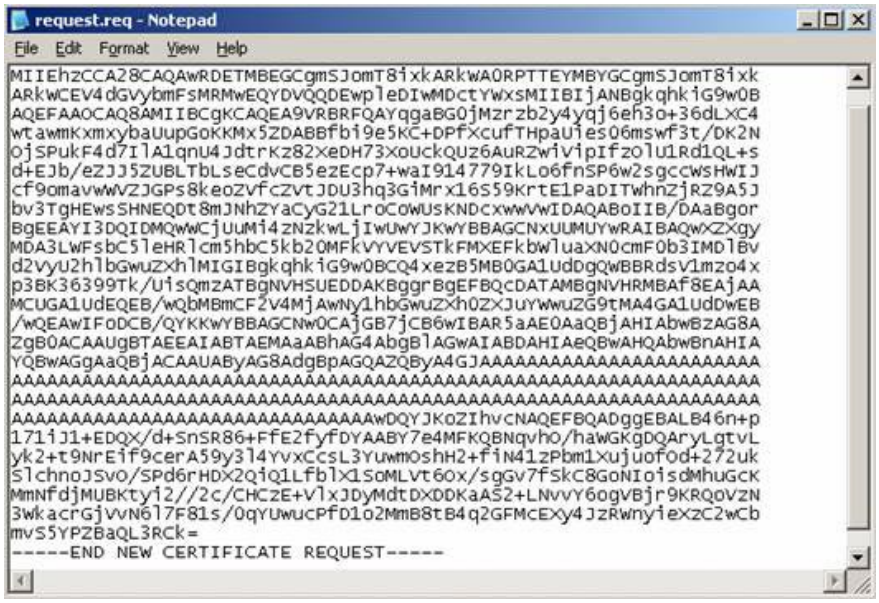

Figure 6: Certificate request file.

Provide a certificate request.

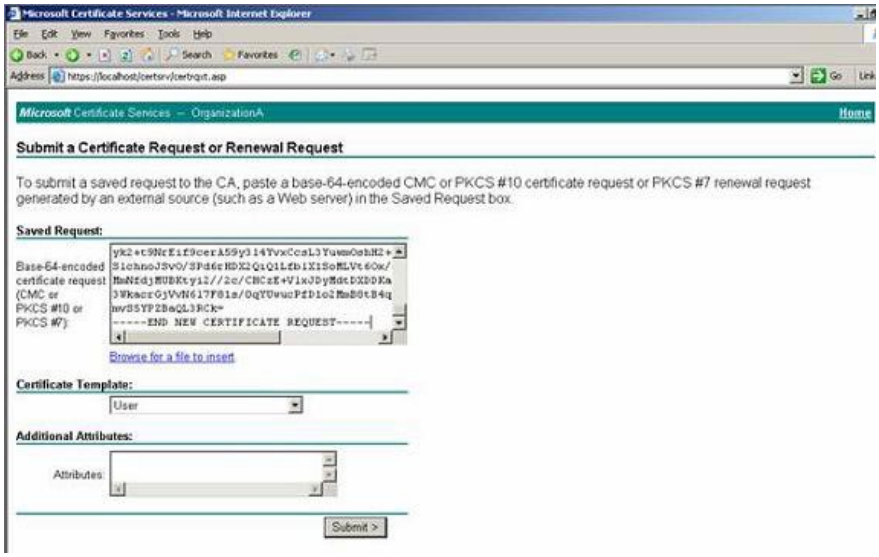

Figure 7: Request a certificate.

In the following figure, you will see the certificate issued from the internal Certificate Authority.

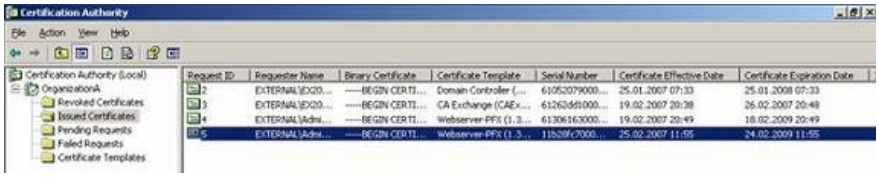

Figure 8: Certificates are issued.

Enter the certificate

An important issue is that you must use Exchange Management Shell to import certificates.

Import-ExchangeCertificate -Path c: certificatesimport.pfx | Enable-ExchangeCertificate -Services SMTP

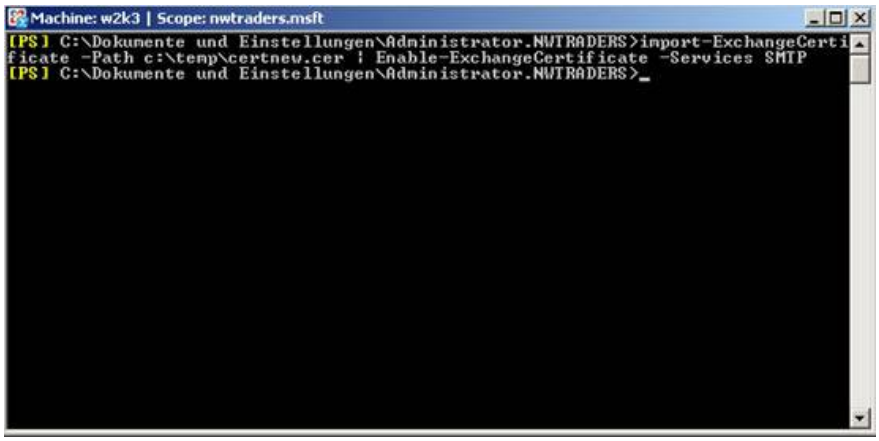

Figure 9: Enter the certificate into Exchange.

Allow the domaene.tld domain to act as a domain list with the Exchange Management Shell

Set-TransportConfig -TLSReceiveDomainSecureList domaene.tld

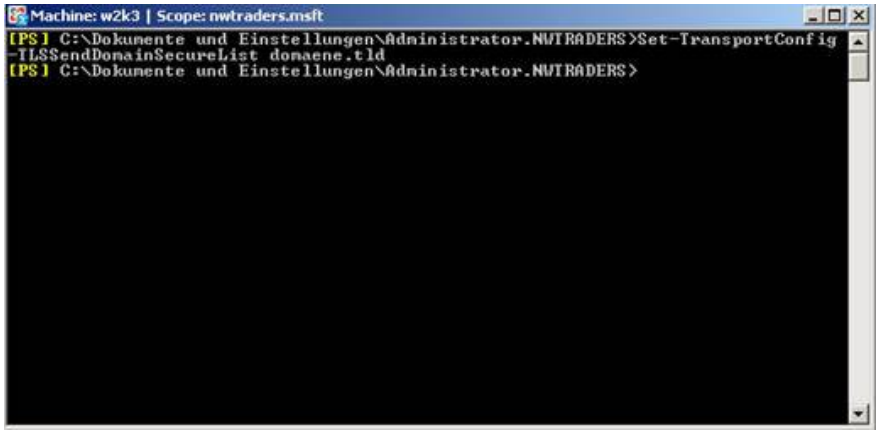

Figure 10: Allow Domain Secure List.

Allow Domain Security to work on SMTP sender named 'Outbound'

Set-SendConnector Outbound -DomainSecureEnabled: $ True

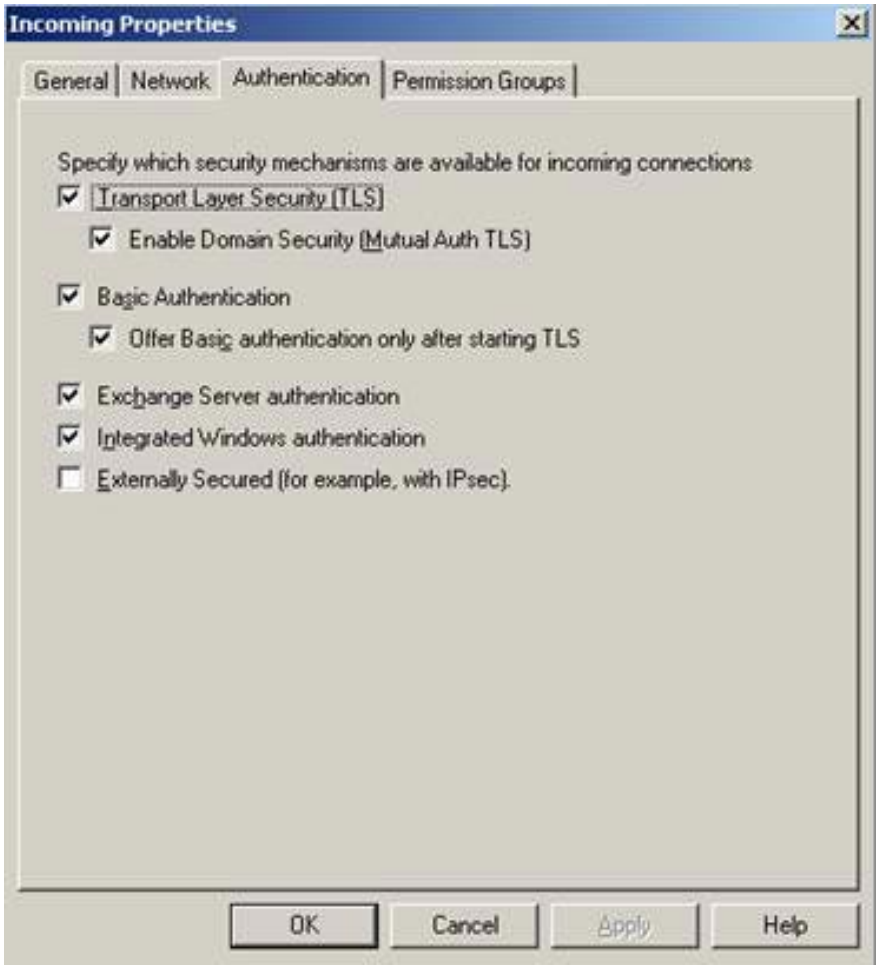

Figure 11: Allow Domain Security with TLS in the Exchange Management Console

Allow Domain Security on SMTP receive connector named 'Inbound'

Set-ReceiveConnector Inbound -DomainSecureEnabled: $ True -AuthMechanism TLS

Note :
Successful distribution of email through the domain that connects secure mail streams is displayed in Outlook 2007 as 'Domain Secure'.

Conclude

As you saw in this article, deploying secure SMTP mail flow between Exchange 2007 servers in different Exchange 2007 organizations is not too complicated. And so you do not need to resort to too advanced solutions like deploying IPSEC.

You finished reading the article "**Secure secure SMTP mail flow between different Exchange Server 2007 organizations**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.