# Table of Contents

Overview ........................................................................................................................................... 3

Acknowledgements ........................................................................................................................... 3

Introduction to TLS .............................................................................................................................. 3

  How TLS works.................................................................................................................................. 3
  How Can My Organization Use TLS/SSL? .......................................................................................... 4

Detecting TLS ....................................................................................................................................... 4

Implementing TLS on Windows Exchange 2007 .................................................................................. 5

  Verifying x.509 Certificate in Exchange 2007 .................................................................................... 5
  Create Send Connector ....................................................................................................................... 7
  Create Receive Connector .................................................................................................................. 11

Implementing TLS on Windows Exchange 2003 ................................................................................. 15

  Configuring the Default SMTP Virtual Server .................................................................................. 15
  Creating and Configuring the Secure SMTP Virtual Server ............................................................... 16
  Configuring the Secure SMTP VS to use a certificate ................................................................. 17
  Set TLS encryption levels for the Secure SMTP Virtual Server ......................................................... 19
  Creating and Configuring the Secure SMTP Connector ................................................................. 21

Conclusion .......................................................................................................................................... 25

See also (suggested references) ........................................................................................................ 25
Overview

This document is intended for insurance companies and brokerages in Canada that operate within the Property & Casualty insurance industry. It provides technical details to guide staff on the implementation of secure email communications using the TLS protocol.

Acknowledgements

CSIO would like to acknowledge the Agents Council for Technology (which is part of the independent Insurance Agents & Brokers of America) as well as Jim Rogers, Director at The Hartford for developing much of the original research material.

Introduction to TLS

TLS (Transport Layer Security) is a system for providing security to communications over the Internet. Specifically, it uses encryption to provide confidentiality (privacy) and authentication (authorization). TLS is the successor to SSL, which is an older protocol. There are three major versions of SSL (v1, v2, and v3); the fourth version was renamed before release, to become "TLS v1". SSL and TLS are based upon a) public key encryption and decryption, b) simple identifying information, and c) trust relationships. In combination, these elements make SSL/TLS useful for protecting a broad range of Internet communications.

How TLS works

TLS protocol creates an encrypted communication channel between email servers at transmission time, as shown in the below diagram.

The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged. In a typical scenario, only the server is authenticated and its identity is ensured while the client remains unauthenticated. The mutual authentication of the servers requires public key deployment to clients. When a server and client communicate, the TLS protocol ensures that no third party can eavesdrop, tamper with any message or commit message forgery.
How Can My Organization Use TLS/SSL?

Most uses of TLS require a digital certificate from a certification or certificate authority (CA), which is a trusted authority that can attest to the identity of the certificate owner. Organizations will also need a system or network administrator who is familiar with whichever client-server applications need to be secured to enable TLS encryption.

Certificates are usually issued for a one-year period, and different security features may be available, depending on the vendor. Most of these features are targeted at organizations that will install these certificates on email / web servers.

There are several commercial certification authorities, including VeriSign (http://www.verisign.com), Comodo (http://www.comodo.com), GeoTrust (http://www.geotrust.com/), and GoDaddy (http://www.godaddy.com). Visit each of these organization's websites to compare prices or request a certificate.

Detecting TLS

There are two (2) ways to tell if a server is TLS capable:

The first is to send and receive a message from the server and then to examine the headers on the message. If you see anything TLS-related (highlighted in red below), the server is likely TLS-enabled.

The second is to test the server by using a Telnet connection. Below is an example of a Telnet session in one of our datacenters that shows the STARTTLS option. You may perform this test on any mail server. The following example was taken from our servers:

CMD: telnet mail.global.frontbridge.com 25
220 mail77-red.bigfish.com ESMTP Postfix EGGS and Butter
CMD: ehlo test
250-mail77-red.bigfish.com
250-PIPELINING
250-SIZE 15000000
250-ETRN
250-STARTTLS
250 8BITMIME
CMD: starttls
220 Ready to start TLS

The "220 Ready to start TLS" indicates that the server is ready to start a TLS connection.

Implementing TLS on Windows Exchange 2007

Verifying x.509 Certificate in Exchange 2007

Step 1:

- Start>Run >MMC
- File> then select Certs MMC (if already created)
- View all Personal Certificates for authenticity, version and expiration dates.

Note:

- To add Certificate Manager to Microsoft Management Console
- Click Start, click Run, type mmc, and then click OK.
- In the File menu, click Add/Remove Snap-in.
- In the Add/Remove Snap-in box, click Add.
- In the Available Standalone Snap-ins list, click Certificates, and then click Add.
- Click Computer Account, and then click Next.
- Click the Local computer (the computer this console is running on) option, and then click Finish.
Step 2:
Verify SSL Certificate version, under the Details Tab, to ensure that it is a ‘Version 3’ (TLS) Certificate.

- Click **Close**, and then click **OK**.
Create Send Connector
To use TLS to send e-mail messages to a third-party e-mail program, you must configure a Send connector. Send connectors are configured on computers that are running Exchange 2007 and that have Hub Transport or Edge Transport server roles installed. The Send connector represents a logical gateway through which outgoing messages are sent.

Step 1: Press Start>select Exchange Management Console.

Step 2: SETUP SEND CONNECTOR

- Select Organization Configuration>Hub Transport.
- Select the Send Connectors Tab.
- ‘Right Click’ and select New Send Connector.

Step 3: Enter Name describing your new Mutual TLS configuration.
Select Custom, and then Next.

**Step 4:** Select Add, then enter the receiving party’s assigned IP address to receive mail. Then press OK, then Next.

**Step 5:** Select the ‘None’ radio button, then press Next.
Note: if your Smart Host requires authentication, you will be required to enter the necessary username, password and appropriate radial button. Contact your Smart Host prior to setting up a Mutual TLS session to obtain all the correct information for this portion of the Send Connector configuration.

Step 6: Verify that you select the correct mail server (within you domain). Press Next.

Step 7: Verify that you have entered all the correct information for your new Send Connector, then press New.
Step 8: Verify that the configuration was accepted and successfully completed, and then press Finish.

Step 9: Verify that your new Send Connector is displayed in the Send Connectors Tab, and that it is enabled.
Create Receive Connector

To use TLS to send e-mail messages to a third-party e-mail program, you must configure a Receive connector. Receive connectors are configured on computers that are running Exchange 2007 and that have the Hub Transport or Edge Transport server roles installed. Receive connectors represent a logical gateway through which all inbound messages are received.

**Step 1:** Expand Server Configuration, and select Hub Transport. ‘Right Click’ within the designated mail server and select New Receive Connector.

**Step 2:** Provide proper name describing the new Receive Connector. Select Custom, and then press Next.
Step 3: Depending on the company’s network configuration and needs, select the desired IP address in which your Receive Connector is to receive incoming mail from the sender’s mail server.

Press Next.

Example: press Add, and then enter the new IP address that you had created for your mail server network adapter.

Step 4: Edit existing default entry.

Enter the IP address (range) provided by the sender. Ensure you enter the IP Address in both the Start and End Address fields.

Press OK, and then Next.
Note: If there is only one IP address provided (**normal situation**), ensure that it is entered in both the Start and End Address fields.

**Step 5:** Verify that the information that you enter is correct, and then press New.

**Step 6:** Verify that your new Receive Connector is successfully completed, with no error. Press Finish.
Step 7: Verify that your new Receive Connector is displayed and enabled.

Step 8: Enable the Receive Connector Mutual TLS Security Setting
Server Configuration>Hub Transport
Right-click on the 'TLS The Hartford' Receive Connector, and select Properties.
Select the Authentication tab, and select both the Transport Layer Security (TLS) and the Enable Domain Security (Mutual Auth TLS) buttons.
Then select OK.
This will complete the configuration of the Mutual TLS Receive Connector.

**Implementing TLS on Windows Exchange 2003**

**Configuring the Default SMTP Virtual Server**

First we need to configure the Default SMTP Virtual Server to receive the main IP address.

1. Click **Start**, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Expand **Administrative Groups** *(if appropriate)*, expand **Administrative Group** *(if appropriate)*, expand **Servers**, expand **Server Name**, and then expand **Protocols**.
3. Right-click the **Default SMTP Virtual Server** object, and then click **Properties**.
4. On the **General** tab, for **IP address**, select the primary IP address from the drop-down list.
Creating and Configuring the Secure SMTP Virtual Server

Add a new SMTP Virtual Server (suggested name "Secure SMTP VS") that will serve as the Secure SMTP Connector Bridgehead, and configure this Secure SMTP VS to receive the secondary IP address added in the "Configuring an Additional IP Address" section of this document.

1. Click Start, point to Programs, point to Microsoft Exchange, and then click System Manager.
2. Expand Administrative Groups (if appropriate), expand Administrative Group (if appropriate), expand Servers, expand Server Name, and then expand Protocols.
3. Right-click SMTP, point to New, and then click SMTP Virtual Server.

4. In the Name box, type the name of the virtual server (suggest Secure SMTP VS), and then click Next.
5. Select the **IP address** that you want to use (we suggest using the additional IP address that was added in the "Configuring an Additional IP Address" section of this document), and then click **Finish**.

---

### Configuring the Secure SMTP VS to use a certificate

To configure the Secure SMTP VS to use a certificate, follow the steps below:

1. Click **Start**, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Expand **Administrative Groups** *(if appropriate)*, expand **Administrative Group** *(if appropriate)*, expand **Servers**, expand **Server Name**, and then expand **Protocols**.
3. Right-click the Secure SMTP VS, and then click **Properties**.
4. Click the **Access** tab, and then click **Certificate** to set up new key certificates and to manage key certificates that are installed for the SMTP virtual server. See the appropriate article for more details on using certificates with Virtual Servers in Exchange Server: [http://support.microsoft.com/kb/319574/](http://support.microsoft.com/kb/319574/)
Set TLS encryption levels for the Secure SMTP Virtual Server

To configure the Secure SMTP VS to require inbound TLS Encryption, follow these steps:

1. Click Start, point to Programs, point to Microsoft Exchange, and then click System Manager.
2. Expand Administrative Groups (if appropriate), expand Administrative Group (if appropriate), expand Servers, expand Server Name, and then expand Protocols.
3. Right-click the Secure SMTP VS, and then click Properties.
4. Click the Access tab, and then click Authentication.
5. Click to select the Requires TLS encryption check box.
6. Click OK, then click OK again.

Note: Under the Access tab on the Secure SMTP VS properties, Communication button, there is an additional level of security that can be enabled. "Require Secure channel" will require TLS communication between all SMTP emails to or from the Secure SMTP VS.

This applies even to SMTP Virtual Servers on the same Exchange server, and would require a certificate be installed on the Default SMTP VS, as well as any other SMTP Virtual Servers within the same Exchange 200x Organization.
Note: The Delivery Tab of the Secure SMTP VS, Outbound Security button has a TLS encryption checkbox. We recommend not enabling this setting. If this is enabled, it will force TLS encryption between the Secure SMTP VS and other Exchange/SMTP Servers within the same Exchange Organization, and could cause mail flow from the remote Exchange Organization with which you require secure SMTP mail to get stuck in the queue.

Creating and Configuring the Secure SMTP Connector

Create a new SMTP Connector and configure it as follows:

1. Click **Start**, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Expand **Administrative Groups (if appropriate)**, expand **Administrative Group (if appropriate)**, then expand **Routing Groups**, and then expand the routing group that you want to use as the originator of the connection.
3. Right-click **Connectors**, point to **New**, and then click **SMTP Connectors**.
4. In the **Properties** dialog box, click the **General** tab. In the **Name** box, type a descriptive name for the connector (*suggested name: Secure SMTP Connector*).

5. Also on the **General** tab, click **Forward all mail through this connector to the following smart hosts**, and then type the IP address of the remote Bridgehead Server through which you want to route the secure mail flow to the other Routing Group. Enclose the address in square brackets, *e.g.*

   [192.168.1.51];[10.10.10.1] or server518.appriver.com

6. Also on the **General** tab, click **Add**. Under the **Local bridgeheads** settings dialog box, select the Secure SMTP VS that was created in the "Creating and Configuring the Secure SMTP Virtual Server" section of this document, and then click **OK**.
7. Click the **Address Space** tab, and then click **Add**.
8. Select **SMTP**, and then click **OK**.
9. Type the SMTP Address Space of the remote Exchange 200x Organization with which you require secure SMTP mail flow, then click **OK**.

**Note:** You will also have to define the address space for the secure domain by correctly entering the domain name with which you wish to communicate. The domain name has to match the IP address of its SMTP server.
10. Next, click the Advanced tab, click the Outbound Security button, and check the TLS Encryption check box.
11. Click OK, then click OK again.
Note: To verify that the SMTP Traffic is encrypted, start a Network Monitor capture on one of the Secure SMTP Bridgehead Servers, and then initiate an SMTP mail message from a client on one side of the secured mail flow environment. Once the mail is delivered, stop the capture and examine the packets that were sent. All SMTP packets between the Secure SMTP Bridgehead Servers with a destination of port 25 (0019h) are encrypted.

This will complete the configuration of TLS on Windows Exchange 2003.

Conclusion

No single security measure will fully protect your organization from unauthorized data breaches, but implementing security protocols like TLS/SSL can reduce the chance of such threats. The Canadian insurance industry is obligated by law to secure its clients’ Personal Identifiable Information (PII). Stakeholders, staff and constituents who are concerned about the safety of their information will appreciate these safeguards. When it comes to data security, erring on the side of caution is always the prudent choice.

See also (suggested references)

1. CSIO webinar - “Implementing an Effective Information Security Program: Safeguarding Network Data and Email with TLS” on the CSIO Vimeo channel
2. CSIO document: Protecting Client Data with Transport Layer Security (TLS), available on CSIO.com
3. How to configure Lotus® Domino® for secure SMTP sessions using the STARTTLS extension
4. Configuring TLS on Google Business email accounts: the below links provide details on configuring inbound and outbound TLS on Gmail business accounts
   a. Transport Layer Security for Inbound Mail
   b. Transport Layer Security for Outbound Mail