EngageOne Connect 2.2

Technical Requirements

Overview

Connect's Secure & Interactive delivery System is an automatic system which is designed to answer most of Email security threats and protect both Email senders and recipients – For example an Email that contains PHI (Patient's health information) sent between 2 Users located in 2 different Organizations. Connect's product is 'Transparent' for both Email Senders and Recipients and enables among other things the following tasks:

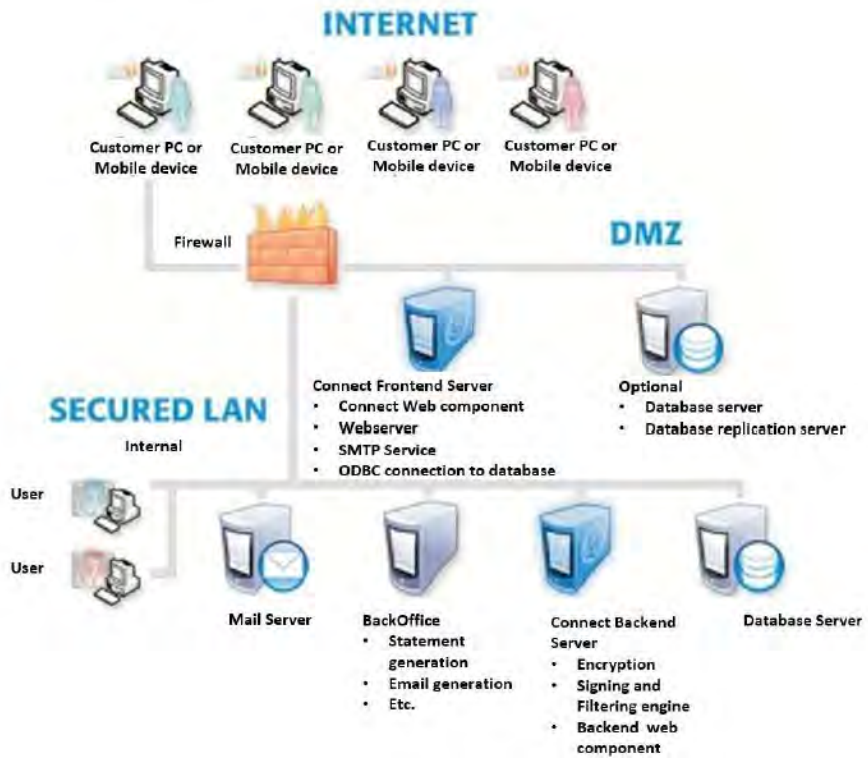
- Design rich transactional and interactive HTML5 responsive and adaptive communications, through several channels, like SMS & Push Notifications.
- Get communication real-time analytics
- Incoming/Outgoing Email virus scan.
- Email encryption.
- Email Text Content Filtering.
- Email Malicious codes detection.
- Email digital signing.

Connect's solution combines different software and hardware components and utilises Connect's PrivaWall Policy Based Email Security Server. PrivaWall is the component which acts the software's delivery engine

The following document will guide you on what is needed to prepare before a Connect implementation can take place. In order to complete a successful and quick implementation it is necessary to fulfill all mentioned requirements in this document.

The below diagram details the standard installation which consists of

- The server located at the DMZ will be referred as the *DMZ* server.
- The server located at the Internal will be referred as the *Internal* server.



Connect Secure & Interactive delivery System

Please note that general security & Redundancy elements were not taken into consideration in this configuration (Firewall, Load Balance and Backup), it is taken into consideration while using Enterprise APS with more than 15,000 users.

Description

DMZ (External) Server

ODBC Service

This is a connectivity component for the SQL Server in the internal machine: an ODBC System DSN that refers to your SQL server database.

MS SMTP Service

This Microsoft service located on the DMZ machine will enable outgoing emails while leaving PrivaWall to be routed directly to the recipient mail server.

Authentication Server (optional for enterprises that will want to communicate between them point to point in a secure encrypted way)

This authentication server called 'PrivaWall ASP Proxy' is located on the DMZ machine and responsible for:

1. Relaying queries between the end user's Secured Email Client tool and the MS-SQL server, that is on the secured zone, in order to confirm/verify whether a secured email sender is an authorized registered sender or not (The confirmation and queries are Completed using SSL protocol).

2. 'Translate' from SSL into SMTP and forward the email messages that arrive from a Secured Email Client sender all the way to the PrivaWall server.

Note: Security is increased by conducting the whole process on the RAM memory, so no email sensitive information is written/saved on the HD.

Frontend Services Application

This is a small application (Usually installed where the IIS Web Server exists – DMZ Machine) that receives the Sender's and Recipient's statistics information from the IIS Web Server and delivers it, to the Backend Services Server application – Internal machine.

Internal Server

PrivaWall Email Security Server

The PrivaWall™ server is located on the internal machine - It is a secure e-mail server that automatically applies rule-based operations to any e-mail that are routed through it. Unlike other automatic other encryption systems that secure messages on the protocol level (where messages are not "in the clear" while they wait for transmission or after being received by the server); PrivaWall™ provides complete end-to-end protection securing messages at the content level, which means that messages and their attachments are secured completely from point of origin to final destination.

MS SQL Standard Edition Database

The MS SQL database is used as the main repository of Connect products, as an example, keeping Emails in the 'Parking' Mode, Logs, users information encrypted and more, and for storing the users encryption passwords and registration details.

Technical Requirements prior to Connect Implementation

Please follow the list below step by step and make sure each item is available and ready:

☑ Prepare network architecture diagram, which will describe the organization network and the PW location and deliver it to your Connect technical contact person.

☑ Internet Connection Line (Min. 15 MBps inbound and outbound)

☑ Secured and Air-conditioned Server Room

☑ One registered IP addresses and domain name, for the DMZ Machine:

For example connect.company.com

☑ One X.509 V3 Digital certificate for the above domain names – Can be purchased from an authorized CA such as Verisign.com (We use it for the SSL encrypted communication between the recipient and Connect FrontEnd.

☑ Optionally, One X.509 V3 Digital certificate - Can be a self generated certificate from a Windows 2008 & UP (We use it for the SSL encrypted communication between the different Connect components).

☑ *Internal* Server and *DMZ* server must be updated with the latest Service Packs.

☑ Microsoft SQL server 2012 & Up should either be available on the network, or installed on the backend service (Internal), as specified on the installations guide.

☑ Enable Connect Technicians with remote access to the 2 servers using Windows Remote Desktop application.

☑ Create a 'Connect' user with administrative rights on each of the 2 servers for Connect Technicians to be able and remotely access the 2 servers as described earlier.

Firewall Configuration

The system requires a Firewall server with NAT capabilities. The Firewall does not have to be dedicated to this system, but for security reasons, both of the subnets must be dedicated: one for the *DMZ* and one for the *Internal.*

Required Network connectivity

The Connect FrontEnd server will receive connections from the Internet on several ports, while Connect BackEnd *Internal* server will be hidden, secured and blocked from any external access.

List of required available ports:

***DMZ* to *Internal*:**
HTTP 80 or 443 (According to the security restrictions)
8888-8889 (Connect specific ports)

***Internal* to *DMZ*:**
SMTP 25

***Internal* to All:**
DNS 53 (TCP and UDP), FTP 21, HTTPS 443 and/or HTTP 80 (For Antivirus signatures updates)

***DMZ* to All:**
DNS 53 (TCP and UDP), FTP 21, HTTPS 443, HTTP 80, SMTP 25

All to *DMZ*:
HTTPS 443, HTTP 80, SMTP SSL 465 (or 443, according to the security restrictions)

Connect Gateway IP (e.g. **62.90.61.226)** to *DMZ* and *Internal* (remote control):
Either one of the following:

- Microsoft Remote desktop 3389
- NetSupport 5405
- VNC 5900

Required Email addresses

The system must have support Email address to be used while delivering for example administrative notifications for to the end users.

You must create a mailbox for the account, to collect responses and to avoid rejection by Mail relays. For example: connect.support@company.com .

In addition, an administrator must be assigned for the system. The administrator mail address will be used in the different component to receive alerts and notifications. For example: postmaster.connect@company.com

The two Email addresses must be operational before performing the Connect installation itself.

Hardware Machines and Software requirements

- Hardware (minimum requirements)
  - Two Servers, Xeon based, 2.1 GHZ & Up
  - 16 GB of memory (Recommended 32 GB) each.
  - 120 GB HD minimum, for system installation and other components
  - 300 GB HD minimum, for Data, logs & basic statistics info a
  - Optional: 1x CD-ROM for installations purposes
- Software
  - Windows 2008 r2 (English Edition) or Up for each server
  - Microsoft SQL 2008 (English Edition) or up with file index feature and mixed mode. Can use existing MS-SQL installed.
  - AV software – recommended.

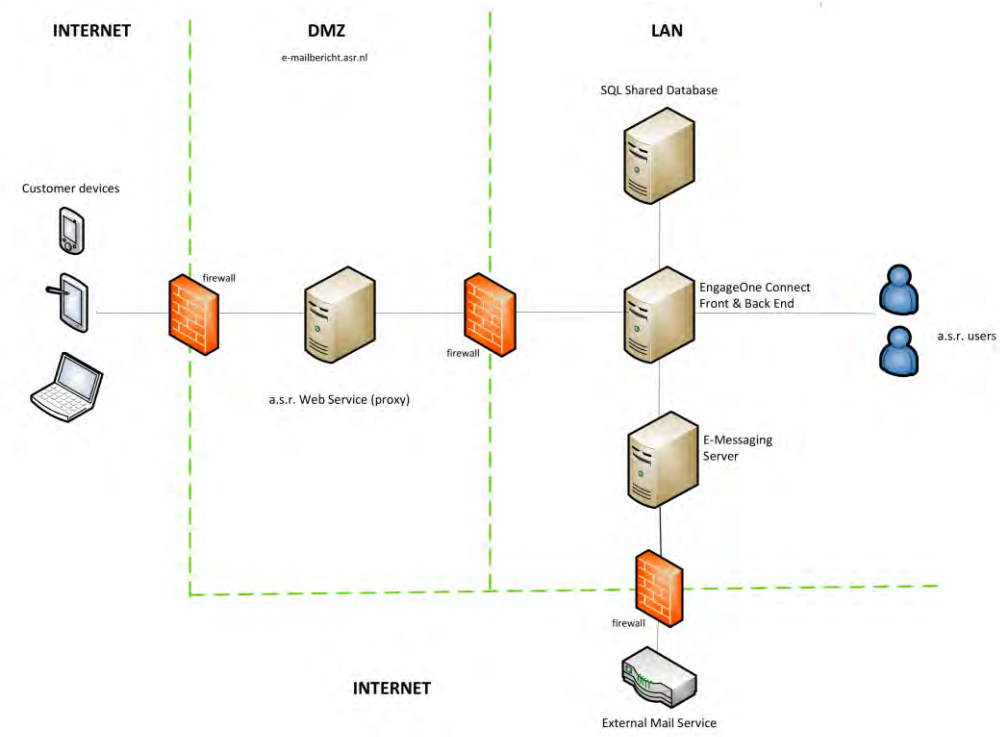
Checklist

For your convenience we prepared a checklist to assist you to easily follow your preparation process.

Task	Status
Infrastructure	
• Prepare network architecture diagram and deliver to Connect	☐ Completed
• Prepare Internet Connection Line (Min. 2.5 MBps inbound and outbound)	☐ Completed
• Prepare Secured and Air-conditioned Server Room	☐ Completed
• Purchase Credit Card billing service for your SES site (optional)	☐ Completed
Hardware	
• Prepare 2 Servers	☐ Completed
• Configure your Firewall	☐ Completed
Network Connectivity	
o DMZ->Internal:	
▪ HTTP 80/443	☐ Completed
▪ HTTP 8888/8889	☐ Completed
o Internal->DMZ	

▪ SMTP 25	☐ Completed
o Internal->All	
▪ DNS 53 (TCP and UDP)	☐ Completed
▪ FTP 21	☐ Completed
▪ HTTPS 443	☐ Completed
▪ HTTP 80	☐ Completed
o DMZ->All	
▪ DNS 53 (TCP and UDP)	☐ Completed
▪ FTP 21	☐ Completed
▪ HTTPS 443	☐ Completed
▪ HTTP 80	☐ Completed
▪ SMTP 25	☐ Completed
o All->DMZ	
▪ HTTPS 443	☐ Completed
▪ HTTP 80	☐ Completed
▪ SMTP SSL 465	☐ Completed
o Connect **IP external Address** to *DMZ* and *Internal* (remote control,optional): ▪ Microsoft Remote desktop 3389 ▪ NetSupport 5405 ▪ VNC 5900	☐ Completed
Software and Others	
• Install Windows 2012 R2 Server standard edition on the internal server and make sure it is updated with the latest service packs	☐ Completed
• Install Windows 2012 R2 or up Server standard edition on the external server and make sure it is updated with the latest service packs	☐ Completed
• Create a 'Connect' user with administrative rights on each of the 2 servers	☐ Completed
• Purchase and Install Anti-Virus software on the two server and make sure they are updated (optional, recommended)	☐ Completed
• Purchase MSQL 2012 Standard edition (Optional to use an existing MS-SQL Server	☐ Completed
• Enable Connect Technicians a remote access to the 2 servers using Windows Remote Desktop application.	☐ Completed
• Prepare two registered IP addresses and domain names, both for the DMZ Machine as in the following:	
▪ For the website, for example: ses.company.com	☐ Completed
▪ For the authentication server: auth.company.com	☐ Completed
• Purchase two X.509 V3 Digital certificates for the above domain names	☐ Completed
• Generate one standard self created X.509 V3 Digital certificate (Optional)	☐ Completed
• MS Windows I386 Folder can be copied to the local disk of the 2 servers.	☐ Completed
• Create 2 email addresses:	
o For support issues for example: ses.support@company.com	☐ Completed
o For administrative issues for example: postmaster.ses@company.com	☐ Completed
• Update Connect product dashboard according to your own theme	☐ Completed

Alternate Installation



The above diagram applies for the following circumstances, where:

- Installation will be done in an all-in-one server.
- The customer's Web Service (a.k.a Proxy) will reroute all communications from within the organization on port 80 to the outside world on port 443, and all incoming communication on port 443 will be routed to the internal Connect server on port 80

Finally…

Once you have fully completed all requirements mentioned in this document, please contact Pitney Bowe's Connect's Services or Support team to complete implementation.