Publishing eSuite

Secure Sockets Layer (SSL)

Tyler New World ERP clients are ultimately responsible for the hardware and computer network infrastructure that runs the ERP software at your location (unless otherwise specified in your contract).

The New World ERP software can contain Personally Identifiable Information (PII) of employees and other entities that do business with your institution. This PII can be exposed to attack when you present your eSuite web site to be accessible outside of your internal network.

The first line of defense for your eSuite web site is called *Secure Sockets Layer*, or SSL. An **SSL certificate** installed on your Internet-facing New World ERP eSuite web server allows the data sent between that site and the end user's web browser to be encrypted. Tyler strongly recommends purchasing an SSL certificate from a trusted certificate authority – self signed certificates are not recommended.

Please consult with your network provider or IT staff regarding the procurement and installation of an SSL certificate on your New World ERP servers. Certain modules of nwERP, like the myInspections mobile app, **require** SSL communication between an Internet-facing web server and the live nwERP application server. A "wildcard" SSL certificate may be a cost-effective solution to accommodate more servers.

Note: Tyler Technologies cannot provide direct assistance or support installing SSL certificates. These are specific to your network infrastructure and network domain configuration.

Demilitarized Zone (DMZ)

For customers and employees to use the data presented by the eSuite server, this server will probably be re-located to your **DMZ** (demilitarized zone) or otherwise configured to be securely accessible outside your Intranet (internal network). Additional **Domain Name Service** (DNS) entries may be required to make this server visible to end users and other computers. It is important that these DNS entries align with the DNS names defined in your SSL certificate(s).

Note: Tyler Technologies cannot provide direct assistance with your DMZ configuration. The process will be specific to your network security policy and local domain.

Firewall Considerations

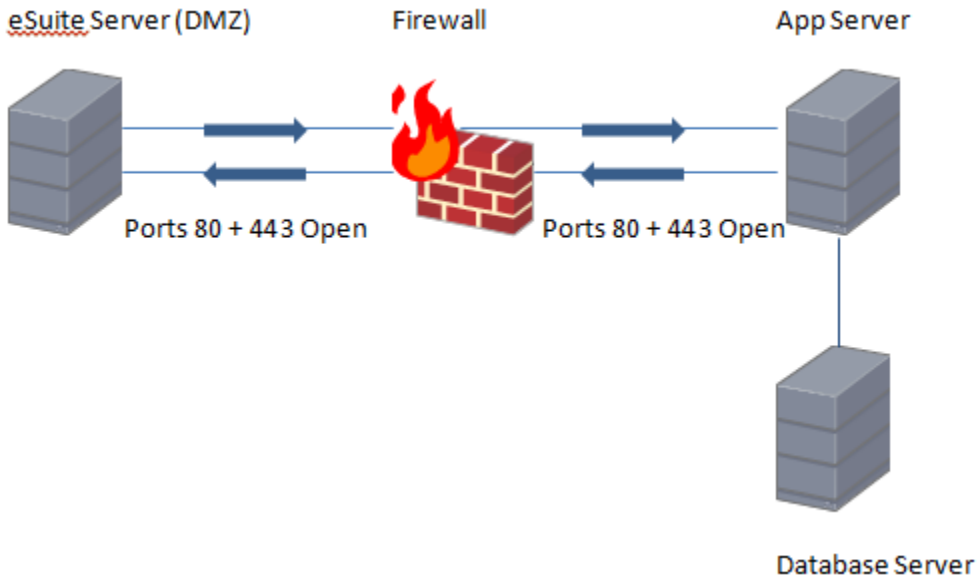
A network **firewall** is a hardware or software "filter" that allows or prevents communication between computers on certain "channels", or **ports**. Once an SSL certificate is purchased and installed on your server(s), and the server is in the DMZ, TCP 443 should be opened between the eSuite and the nwERP application server for web services to communicate if you have a SSL certificate on the application server and TCP port 80 if not. Communications between the Managed Internet Updater (MIU) on the app server and its Agent on the eSuite server takes place by default on TCP port 49876, which should also be opened for bi-directional traffic.

Publishing eSuite

Note: Tyler Technologies does not provide direct support for firewall configuration. The process will be specific to your network infrastructure and firewall product(s).

Diagram

A rudimentary diagram of a typical network configuration is included for illustration purposes.



eSuite URLs

The table below lists the standard naming conventions for the eSuite web sites.

eSuite Administration:	https://appSERVERNAME/esuite.administration
eUtilities:	https://webSERVERNAME.domain.gov/esuite.utilities
eSuite HR Portal:	https://webSERVERNAME.domain.gov/websites.HR.Portal
eBenefits:	Log in through the eSuite HR Portal
eTimesheets:	Log in through the eSuite HR Portal
eRecruit:	https://webSERVERNAME.domain.gov/esuite.Recruit
eRequest For Action:	https://webSERVERNAME.domain.gov/esuite.requestforaction
eLicensing:	https://webSERVERNAME.domain.gov/eSuite.licensing/default.aspx
ePermits:	https://webSERVERNAME.domain.gov/eSuite.Permits/Shared/WelcomePage.aspx
eSupplier:	https://webSERVERNAME.domain.gov/eSuite.Supplier/Shared/Default.aspx
eBids:	Log in through eSupplier
eMiscellaneous Billing	https://webservername.domain.gov/Websites.FM.MiscBilling/LoginScreen.aspx