OLYMPUS
Your Vision, Our Future

Knowledge Exchange (KE) System Cyber Security Plan

OVERVIEW

This document provides recommendations to enhance the security profile of the Knowledge Exchange (KE) System. You are responsible for identifying the security option(s) most appropriate to the risks identified in your environment. Do not attempt to implement any of these settings without first testing them in a non-operational environment. Use of this document is at the discretion of the user. Following these recommendations does not guarantee that the KE system will be secure.

This document discusses the following cyber security issues:

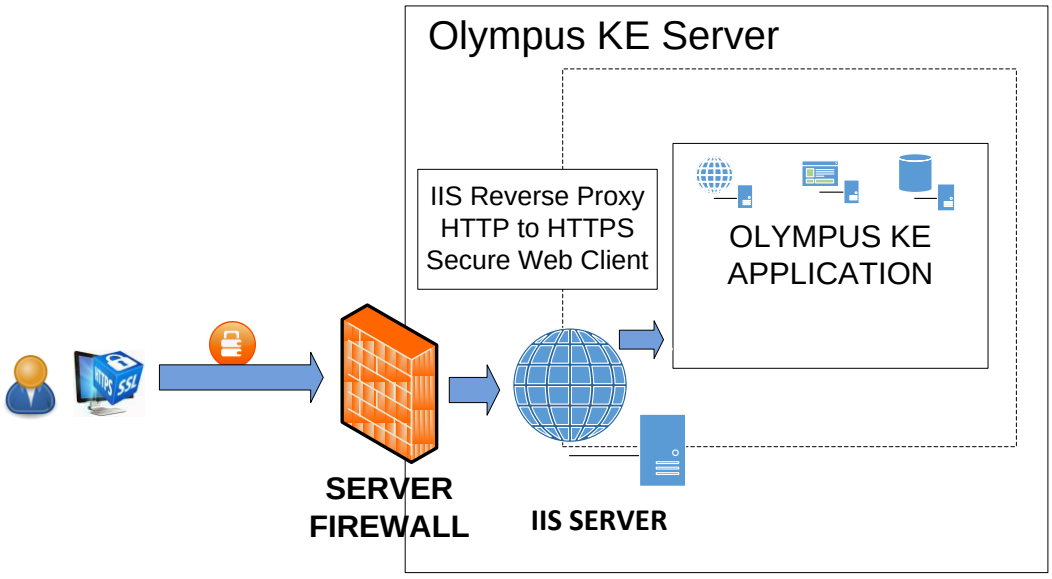
- Application Data Encryption in Motion
  - HTTPS Support
  - HTTP Re-Routing (using URL Rewrite)
  - Secure Headers to Web Client Communication
- Device Data Encryption in Motion
  - Legacy Device Communication Encryption (OER-Pro, CV-190)
- Application Attack Footprint
  - Server Firewall Settings
  - Web Server Obsolescence

This plan uses industry best practices and solutions. There are links for each plan item within this Security Plan, at the end of the document.

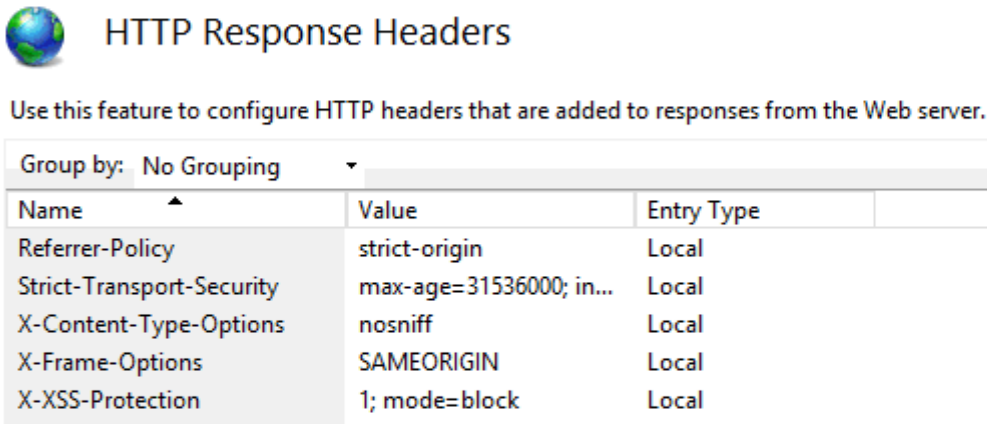
APPLICATION DATA ENCRYPTION IN MOTION

HTTPS support can be provided by installing the Microsoft IIS 8.5 feature on the Microsoft Windows Server® 2012 R2, where your KE system is installed. The following steps can be used to configure IIS 8.5:

1. Set the first rule to configure *URL Rewrite* as a reverse proxy.
2. Create the second rule *Redirect HTTP to HTTPS*.
3. Edit the IIS web configuration for secure headers.
4. Set up bindings to TCP ports 80 and 443, using a self-signed certificate, or a CA certificate, to TCP 443 port only.



To prevent vulnerability with the web client connection, industry standards recommend adding secure headers to Web Client communication. Add these by customizing the HTTP response header in IIS (see list of HTTP Response Headers below).



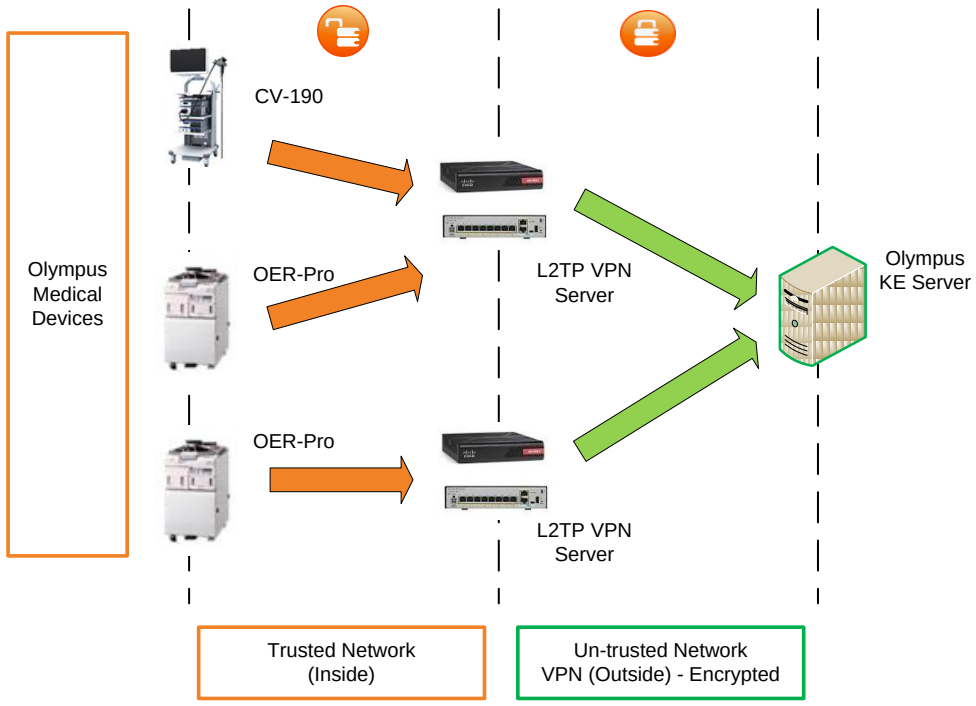
DEVICE DATA ENCRYPTION IN MOTION

Configure an encrypted VPN tunnel between the trusted network (i.e., the Olympus medical device) and the KE server network indicated on the network adapter.

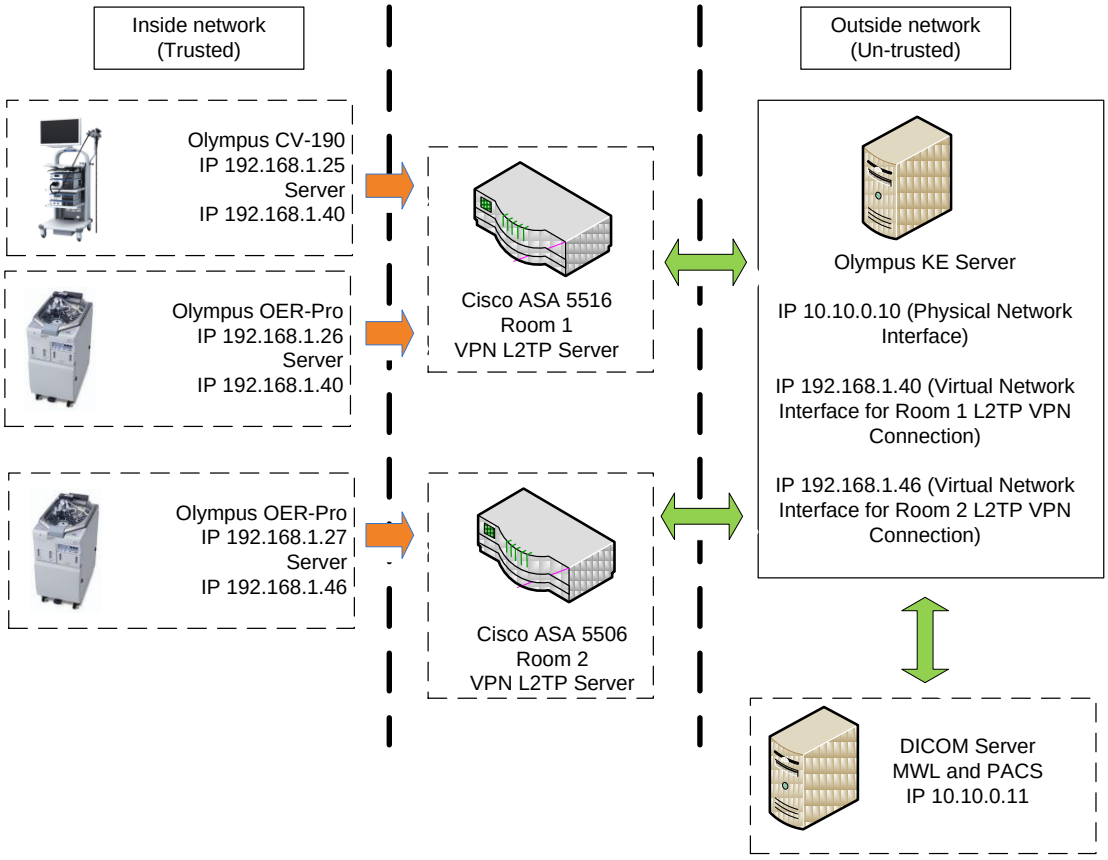
The VPN server must be a physical network device, and configured to enable a L2TP server to connect to a software-configured L2TP Client WAN miniport, using MS CHAP v2. Examples of such servers include the Cisco® ASA 5506X and 5516X, among others. Consult with your network administrator on availability of any of these devices.

Be aware of username creation on the physical network device for use in L2TP VPN. Usernames may require specific encryption of passwords for use with MS CHAP v2.

If Olympus medical devices, from multiple locations within your facility, must connect, additional physical network devices may be required as shown in the diagram below.



Cyber Security network configuration example below:



REDUCE APPLICATION ATTACK FOOTPRINT

Configure the Windows Server 2012 firewall to allow traffic only on ports TCP 443, TCP 9722, and TCP 80. Ports TCP 9722 and TCP 80 are required for Olympus remote support.

Block the *Olympus KE – Glassfish (Receiving HTTP requests)* entry, TCP port 8080 to remove accidental access to obsolescent web server.

Configure only the ports required for Olympus medical devices to communicate with KE, such as OER-Pro and CV-190 units. Allow these ports over the encrypted WAN miniport(s) configured on the KE server. This only allows connection through the VPN.

Please consult *Knowledge Exchange (KE) IT Specifications* (TR0094) for port details.

WEB RESOURCES

- IIS Reverse Proxy:
https://blogs.msdn.microsoft.com/friis/2016/08/25/setup-iis-with-url-rewrite-as-a-reverse-proxy-for-real-world-apps

- IIS Server Name Change:
https://scotthelme.co.uk/hardening-your-http-response-headers/

- IIS Security Headers:
https://securityheaders.io

- Application Request Routing v3:
https://www.microsoft.com/en-us/download/details.aspx?id=47333

If additional information is needed, contact the Olympus Technical Assistance Center (TAC) at (800) 848-9024.