Le HTTPS est un prérequis pour activer les protocoles HTTP modernes, voir l'article support de HTTP/2 et HTTP/3.

Il est aussi recommandé très fortement d'avoir suivi une formation sécurité internet, et de ne pas juste dérouler une procédure d'installation de certificat HTTPS.
Toute erreur dans la manipulation d'un certificate peut entraîner de graves manquement à la sécurité, et de fait, invalider tout l'interêt d'utiliser un certificat.
Si les termes si dessous vous interpellent ou vous semblent être du chinois, n'allez pas plus long et contactez votre administrateur web.

Paramètres du serveur Qubes relatif à HTTPS

Le paramètres du server.cfg relatif à HTTPS sont les suivant.

- SSLEnabled=Y active le HTTPS
- SSLPort (optionnel) spécifié le port du HTTPS (par défaut 443, il est recommandé de ne pas le modifier)
- BindDomain spécifie le domaine du certificat HTTPS, il est recommandé de le définir afin de ne pas servir de certificat en « catch all » sur un port et une IP
- SSOBindDomain permet de spécifier un sous domaine pour le SSO s'il est utilisé (sans quoi HTTP/2 et HTTP/3 seront non disponibles)
- BindRelativeURI permet de spécifier un sous-chemin et une priorité pour le serveur web. Ce réglage permet à plusieurs serveurs web d'opérer sur le même domaine.

Il est aussi possible de spécifier plusieurs domaines, plusieurs sous chemins et plusieurs certificats avec l'option BindURLACLs, en indiquant une ou plusieurs urlacl séparées par des virgules.
Il est alors possible d'établir une hiérarchie de services QubesExpress, en configuration de failover ou de load balancing, au niveau domaine ou chemin d'URL.

Pour plus de détails, une documentation Microsoft est disponibles à Configuring HTTP and HTTPS.

Les modifications du server.cfg ne seront prise en compte qu'au redémarrage du service.

Installation du certificat en ligne de commande

Qubes utilise la même couche Microsoft http.sys que IIS et WCF.
La procédure officielle Microsoft en ligne de commande utilise netsh et httpcfg, elle est décrite sur

https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-configure-a-port-with-an-ssl-certificate

Cette approche est a préférer pour les déploiements, car elle evite d'exposer le certificat dans une fichier en clair.

Il n'est pas nécessaire de redémarrer les services Qubes pour une mise à jour de certificat.

Installation avec IIS Manager

Il est possible d'utiliser IIS Manager inclus dans Windows (cf. Installation Certificat SSL Cloudflare Origin qui décrit la procédure similaire pour l'intégration du certificat).
Il ne faut pas activer le site dans IIS (sans quoi il prendrait le pas sur QubesExpress), mais uniquement définir et paramétrer le site.

Il n'est pas nécessaire de redémarrer les services Qubes pour une mise à jour de certificat.

Installation historique avec httpsysmanager

La procédure ci-dessous est historique et utilise httpsysmanager (qui est un outils non maintenu)***, elle n'est pas recommandée pour les serveurs Windows 2016 et ultérieurs.***

1. Récupérer le fichier QubesUpdate.zip
2. Ouvrir le fichier zip, et aller dans le dossier httpsysmanager-bin-1.5 et copier le contenu de ce dossier dans Qubes\Bin\Tools
3. Lancer httpsysmanager.exe
4. Saisir l'IP du serveur dans la zone IP, ou 0.0.0.0 si le serveur doit être exposé sur toute les IPs.
5. Saisir le port (pour connaitre le port aller dans Qubes\Bin\=>qubesexpress, lancer maincfgfileditor.exe, saisir ssl dans la zone de texte et sélectionner sslenabled, puis cliquer sur la case à cocher, puis aller dans l'onglet sslport et voir le port renseigné (si le port est 0 donc ça sera le port par défaut))
6. sélectionner le certificat qui doit être au format .pfx
7. cliquer sur add certificat
8. redémarrer les services lorsque le certificat est en place