e-KerMed – Paramètres de pares-feu

Contact APIZEE :
Support/Project Team
support@apizee.com
+33 2 57 98 01 16

Table des matières

historique

VERSION	DATE	AUTEUR	MODIFICATIONS
1.0	06/11/2019	Yves Jacq	Initial revision
2.0	31/12/2021	Arnaud VALLEE	Mise à jour suite migration serveur et proxy ENRS

1. Introduction

Ce document vise à présenter les paramètres de pare-feu et antispams nécessaires au bon fonctionnement de la solution e-KerMed.

2. Configuration des pares-feux

2.1 Diagramme des flux

Le diagramme ci-dessous décrit l'ensemble des flux échangés entre le patient, le professionnel de santé et la plateforme eKermed

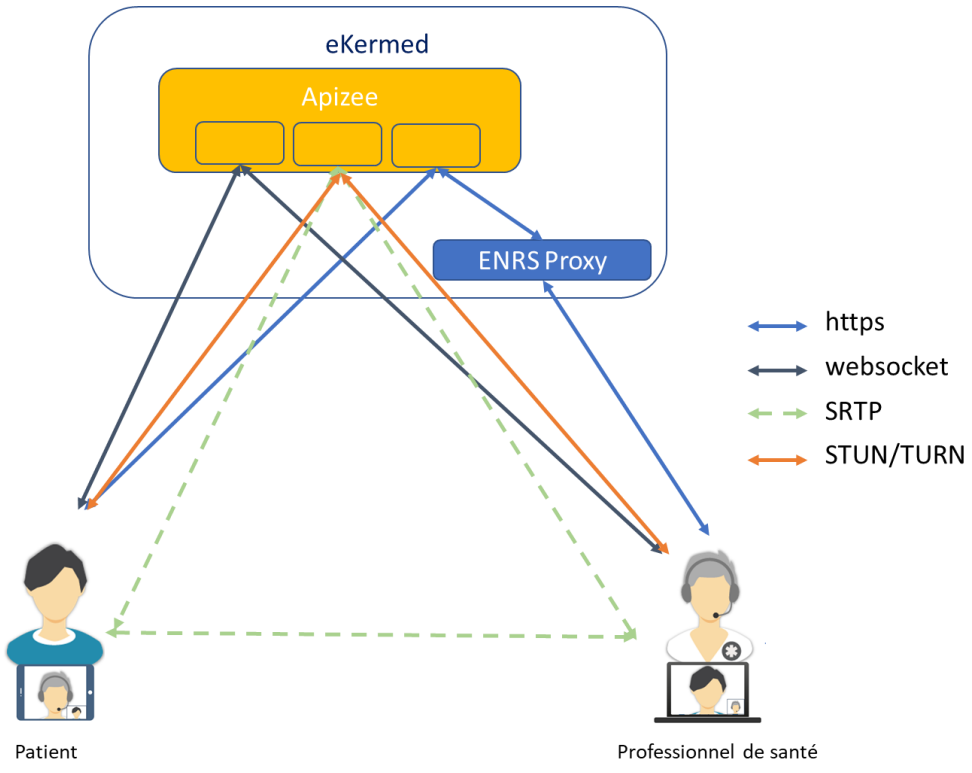

Figure 1 : Diagramme de flux

2.2 Paramètres de pare-feu: Ports et protocoles

La communication temps-réel est opérée et supervisée par Apizee. Les différents flux en temps réel seront établis entre la page web de l'appelant, la plateforme Apizee et la page web de l'appelé. Selon la configuration du réseau, les flux média (protocole SRTP) seront échangés en direct entre les utilisateurs ou acheminés via la plateforme Apizee.

2.2.1 Flux de signalisation

Les flux de signalisation utilisent des protocoles standards du Web (HTTPS et Websocket sécurisé) et permettent de gérer:

- L'établissement et le contrôle de la communication et des flux média
- la présence des utilisateurs
- L'authentification
- La récupération des informations de configuration

Une partie de la signalisation transite via le proxy ENRS mis en place par le GCS Bretagne (telesantebretagne.org)

domaine	Port(s)	Transport	Application
• services.telesantebretagne.org • ekermed.telesantebretagne.org • hds.apizee.com • izeeconf-hds.apizee.com • hds-diag.apizee.com • h.apizee.com • h.apz.fr	443	TCP	HTTPS
• ccs-hds.apizee.com	443	TCP	Secured Websocket / proprietary

2.2.2 Flux Media

Cas 1 : Les flux UDP sont autorisés

Plages de port à ouvrir pour **mp-hds.apizee.com & mp2.apizee.com** :

Server	Port(s)	Transport	Application
Media Proxy mp-hds.apizee.com (146.59.148.218 , 135.125.9.9) mp2.apizee.com (94.23.195.133)	443,49152…65535	UDP	SRTP

Plages de port à ouvrir pour les serveurs média (SFU):

Server	Port(s)	Transport	Application
Media Server 135.125.98.211 51.178.91.64	49152-65535	UDP	SRTP

Cas 2: les flux UDP ne sont pas autorisés

Information importante: Ce cas ne permet d'obtenir une qualité vidéo optimale pendant une téléconsultation

Port à ouvrir pour **mp-hds.apizee.com & mp2.apizee.com** :

Server	Port(s)	Transport	Application
Media Proxy mp-hds.apizee.com (146.59.148.218 , 135.125.9.9) mp2.apizee.com (94.23.195.133)	443	TCP	secured TURN | STUN

3. Configuration des antispam emails

Les emails sont envoyés avec l'expéditeur **votre-teleconsultation@visiotlm.esante-bretagne.fr**

Le sous-domaine **visiotlm.esante-bretagne.fr** devra être placé en liste blanche de l'antispam

Annexe 1: Matrice de compatibilité des navigateurs Internet

Vous pouvez consulter la version en ligne toujours mise à jour : [Matrice de compatibilité]

OS / Browsers	Features	Chrome	Firefox	Opera	Vivaldi	IE	Edge	Edge(New)	Safari	Samsung Internet
Windows	Audio/video	v45+	v46+	v35+	v1+	v11 (plugin**)	v40.15+	v79+	-	-
	Whiteboard	✓	✓	✓	✓	View	✓	✓	-	-
	Screensharing	✓ (2)	V52+	✓	✓	View* / Plugin**	Windows 10 Pro or Enterprise	✓	-	-
	Conversation	✓	✓	✓	✓	-	✓	✓	-	-
	File transfer	✓	✓	✓	✓	-	v40.15+	✓	-	-
MacOS	Audio/video	v45+	v46+	v35+	v1+	-	-	v79+	v11+ (3)	-
	Whiteboard	✓	✓	✓	✓	-	-	✓	✓	-
	Screensharing	✓ (2)	V52+	✓	✓	-	-	✓	v13.0.2+	-
	Conversation	✓	✓	✓	✓	-	-	✓	✓	-
	File transfer	✓	✓	✓	✓	-	-	✓	✓ (4)	-
iOS	Audio/video	✓ iOS14.5+	✓ iOS14.5+	-	-	-	-	-	iOS11.2+(3)	-
	Whiteboard	✓	✓	✓	-	-	-	✓	✓	-
	Screensharing	-	-	-	-	-	-	-	View*	-
	Conversation	✓ iOS14.5+	✓ iOS14.5+	-	-	-	-	-	✓	-
	File transfer	-	-	-	-	-	-	-	✓	-
Android	Audio/video	v59+	v54+	v40+	-	-	-	v79+	-	Tested with v7.2.10.33+
	Whiteboard	✓	✓	✓	-	-	-	✓	-	✓
	Screensharing	View*	View*	View*	-	-	-	View*	-	View*
	Conversation	✓	✓	✓	-	-	-	✓	-	✓
	File transfer	✓	✓	✓	-	-	-	✓	-	✓
Linux	Audio/video	v45+	v46+	v35+	v1+	-	-	-	-	-
	Whiteboard	✓	✓	✓	✓	-	-	-	-	-
	Screensharing	✓ (2)	V52+	✓	✓	-	-	-	-	-
	Conversation	✓	✓	✓	✓	-	-	-	-	-
	File transfer	✓	✓	✓	✓	-	-	-	-	-

Chromium based browsers have the same support as Chrome (Brave, Epic browser ...) unless WebRTC is specifically deactivated.

Minimal supported version of Firefox ESR (Extended Support Release) is 78.

Minimum recommended OS versions: Windows 7+, macOS 10.11, Android 5, iOS 11.

- ✓ means that interoperability testings are still ongoing but it is likely supported
- (1) Non-optimized video quality
- (2) Screen sharing available with browser extension
- (3) An audio issue has been raised on Safari 14.0.1 on MacOS and 14.2 on iOS
- (4) An issue has been detected on file transfer support with specific version of MacOS 10.14.6 and Safari 14.0.1. This issue is corrected on newest versions
- * Consultation mode only. The user can see the screen shared by the other participant(s) but cannot share his own screen.
- ** Requires the installation of a software extension to the browser

Annexe 2: Protocoles

Le tableau ci-dessous détaille les protocoles sécurisés utilisés par la solution Apizee pour mettre en œuvre une téléconsultation:

PROTOCOLE	DESCRIPTION
HTTPS	> **H**yper**T**ext **T**ransfert **P**rotocol **S**ecure. > Accès sécurisé aux pages et services Web via des URLs. > Chiffrement SSL / TLS. > Certificats signés (SHA 256) avec clé publique de 2048 bits
SRTP	> **S**ecure **R**eal-time **T**ransport **P**rotocol. > Transport sécurisé des flux audio/vidéo. > Chiffrement AES et HMAC-SHA1. > Génération et échange des clés de chiffrement via DTLS-SRTP
WSS	> **W**eb**S**ocket **S**ecure. > Connexion réseau sécurisée entre un navigateur la plateforme Apizee. > Chiffrement SSL / TLS.
STUN	> **S**imple **T**raversal of **U**DP through **N**ATs. > Utilisé pour obtenir les informations requises pour permettre la communication en dehors d'un réseau NAT.
TURN	> **T**raversal **U**sing **R**elays around **N**AT. > Utilisé pour communiquer avec le Media Proxy pour obtenir les informations nécessaires à la traversée d'un NAT et/ou du pare-feu. > Les flux audio et vidéo peuvent être échangés via TURN avec chiffement SRTP ou DTLS
DTLS	> **D**atagram **T**ransport **L**ayer **S**ecurity. > Utilisé pour sécuriser les communications en mode Peer-2-Peer et SFU

- FIN DU DOCUMENT -