Table des matières

Public : personnels du Cnam

Accès distants

Passerelle VPN

Le service VPN est destiné au personnel du Cnam. Il permet de se connecter au réseau du Cnam depuis n'importe quelle connexion Internet. Une fois connecté, l'utilisateur peut alors lancer ses applications comme s'il se trouvait physiquement au Cnam. Ce service VPN chiffre les données sur le client et les transmet ainsi sécurisées au serveur du Cnam.

Pour pouvoir se connecter au service, utiliser les identifiants « Cnam EP » (cf. compte « établissement public »).

Il est fortement conseillé lors de l'accès à la messagerie, à l'intranet du Cnam, ou aux autres ressources de l'établissement d'utiliser le VPN. Ainsi connecté, le poste accède aux mêmes ressources (internes comme externes) que s'il était connecté au réseau local. De plus, le contenu des communications est chiffré et reste donc confidentiel.

Attention : l'usage d'un VPN peut être restreint à l'étranger, voir les recommandations du RSSI pour voyager à l'étranger.

Lors de l'usage d'un *smartphone* professionnel, l'activation du mode « VPN toujours actif » est également recommandée. L'objectif est de garantir la sécurité des échanges, et ce, quel que soit le réseau GSM ou Wi-Fi utilisé.

Installation du client VPN

Règle L'usage du VPN ne doit se faire que depuis un équipement professionnel, dont les couches logicielles sont tenues à jour et protégées par un antivirus.

En effet, il serait regrettable qu'un logiciel malveillant soit introduit sur le réseau de l'établissement par un équipement mal géré.

L'installation requiert des droits d'administration sur l'équipement.

Android

Sur les équipements sous Android, GlobalProtect est disponible sur le play store.

iOS

Sur les équipements Apple iPhone et iPad, installer GlobalProtect depuis l'App Store.

Linux

Pour Linux, voir VPN GlobalProtect pour Linux.

macOS et Windows

Pour macOS ou Windows, ouvrir un navigateur web et se connecter à https://portailvpn.cnam.fr avec les identifiants « établissement public ». En haut à droite, suivre le lien « Clients VPN à télécharger » et choisir la version de GlobalProtect correspondant au système d'exploitation de l'ordinateur.

Configuration générique

Une fois installé, lors du lancement, le client GlobalProtect demande l'adresse du portail : il s'agit de `vpn.cnam.fr`. Pour s'authentifier, utiliser à nouveau les identifiants « établissement public ».

Configuration spécifique pour l'ESGT au Mans

Une fois installé, lors du lancement, le client GlobalProtect demande l'adresse du portail : il s'agit de `vpnesgt.cnam.fr` pour se connecter aux ressources locales au Mans. Pour s'authentifier, utiliser à nouveau les identifiants « établissement public ».

Portail VPN

Il est possible d'utiliser le portail VPN pour se connecter à certaines applications métiers, et ce, sans installer de client VPN comme ci-dessus.

Passerelle RDP

Le service est aussi appelé « Applications métiers disponibles en ligne ».

La DSI propose, depuis le portail VPN, l'accès à différentes « applications métiers ». Ce service permet la connexion depuis un navigateur web à une session Windows dans le réseau du Cnam. Entre autres, les applications Sifac, Siscol et les partages Windows sont ainsi accessibles. L'authentification repose sur un compte « Domaine SIGNTD ».

Pour plus d'information, contacter assistance@cnam.fr.

Passerelle SSH

La DSI fournit une passerelle SSH, `gw-ssh.cnam.fr` pour accéder à des machines internes. Pour pouvoir l'utiliser, la direction du laboratoire ou de l'EPN doit en faire la demande auprès de la DSI à l'adresse assistance@cnam.fr en précisant :

- le nom et prénom du bénéficiaire
- son identifiant LDAP s'il existe
- les adresses IP des équipements auxquels cet utilisateur devra pouvoir accéder par SSH

L'authentification se fait par clef SSH et mot de passe. Pour les propriétaires de clefs FIDO U2F, seule la clef SSH est requise (la DSI peut conseiller dans le choix de jetons FIDO).

Documentations d'utilisation :

- Utiliser SSH
- Copier des fichiers à travers un bastion SSH
- Authentification U2F et passerelle SSH

Attention : l'usage de SSH peut être restreint à l'étranger, voir les recommandations du RSSI pour voyager à l'étranger.