



Mise en conformité des outils logiciels de prise en main à distance : Utilisation de rustdesk



- Ludovic FOUR
- UAR 3156 CNRS
- Institut des Neurosciences Cellulaires et Intégratives

Sommaire

- 01 Contexte d'utilisation
- 02 Principe de fonctionnement
- 03 Réglementations
- 04 Solution(s) proposée(s)
- 05 Démonstration
- 06 Conclusion(s)

01 Contexte d'utilisation

Contexte d'utilisation de la PMAD

PMAD: Prise en main à distance

- Le concept n'est pas nouveau, mais s'est généralisé avec le télétravail et la crise COVID
- Intervention à distance de prestataires externes.
- Réduction des coûts d'intervention sur site (pas de frais de déplacements)
- Utilisation de logiciels grand public (Teamviewer, VNC, AnyDesk, DWS, splashtop etc..)
- Utilisation conviviale pour les utilisateurs-trices
- Ne nécessite pas de privilèges pour l'installation de l'outil de prise en main distante
- L'applicatif est généralement fourni par le télé-intervenant ou disponible librement sur internet

Utilisation à l'INCI

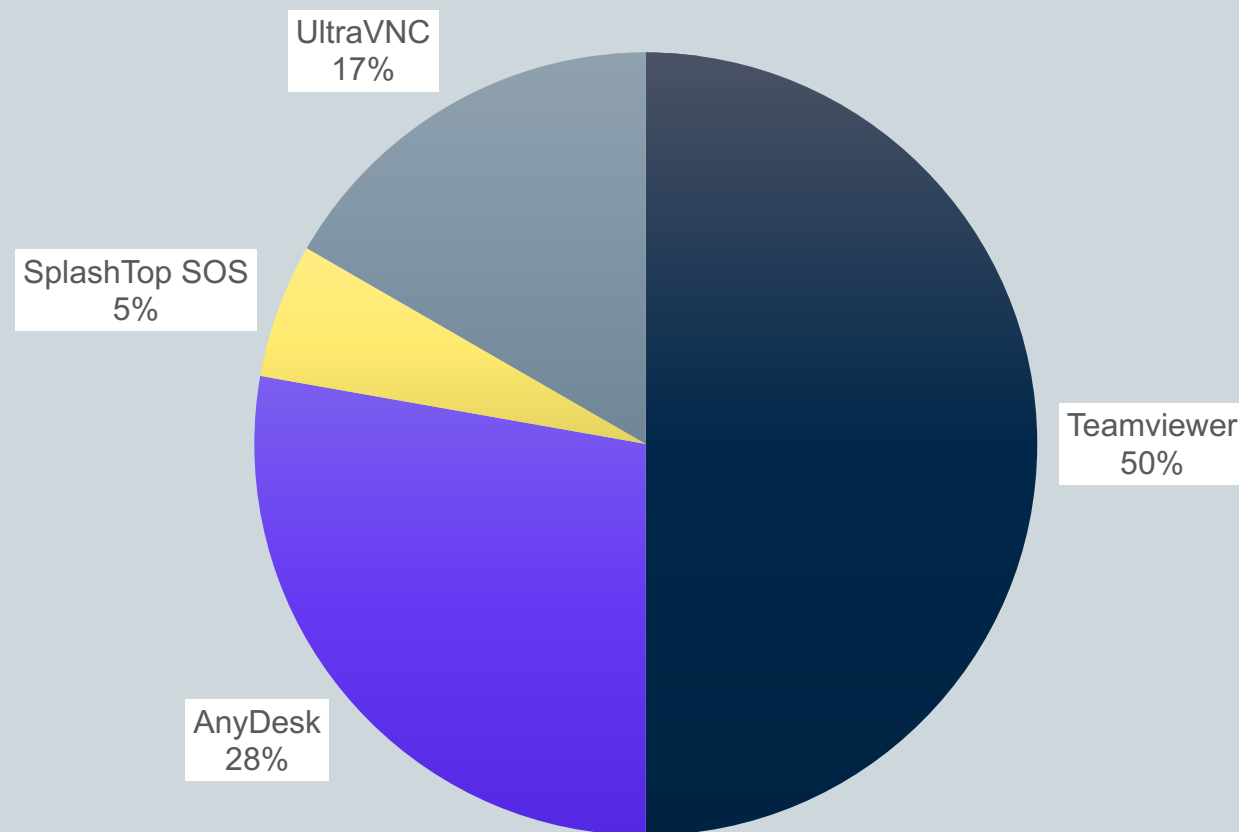
TLP: AMBER

Installations de logiciels d'accès distants sur les ordinateurs

Nom du logiciel	Nombre d'installations
Teamviewer	9
AnyDesk	5
UltraVNC	3
Splashtop	1

Source: OCS inventory INCI + analyses de trafic réseau

Note : Ces chiffres ne tiennent pas compte des installations autonomes ou hors du périmètre réseau de l'unité.



02 Principe de fonctionnement

Principe d'utilisation (comment contourner une PSSI facilement)

En temps normal, un Firewall bloque les intrusions directes (Fonction de sécurité du réseau)

Le logiciel d'accès distant est installé sur un poste informatique dans le périmètre réseau interne de l'unité (sans privilèges) et se connecte via un port standard (généralement: https) sur le premier serveur externe disponible **(1)**

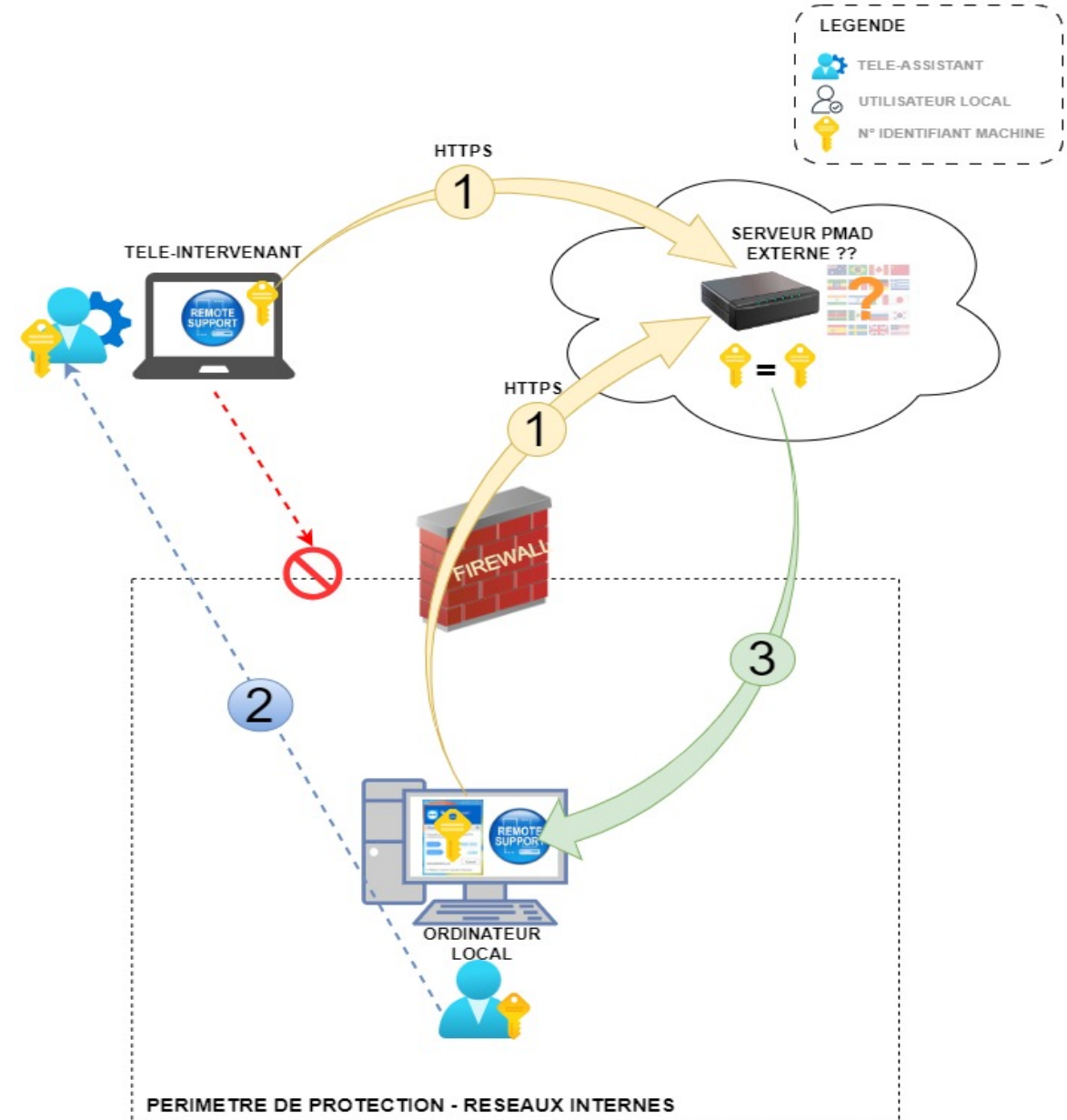
L'utilisateur local, communique son numéro d'identifiant machine (+ mot de passe) au télé-intervenant. **(2)**

Le télé-intervenant se connecte au serveur externe avec l'identifiant machine du poste informatique **(1)**

Le serveur (teamviewer, anydesk etc..) crée un pont entre les deux ordinateurs au travers de la liaison réseau autorisée par le poste **(3)**.

Le télé-intervenant peut accéder à l'ordinateur.

FIGURE 1: PRINCIPE DE FONCTIONNEMENT DES OUTILS DE PMAD



C'est très pratique...MAIS!

- ☐ On retrouve de nombreux outils de pmad différents installés sur le parc informatique, pour la même fonction de « bureau à distance » ...
- ☐ Origine du serveur qui gère les appairages ? (peut-on avoir confiance ?)
- ☐ Les outils utilisent généralement des ports de communication « communs » (http, https) difficiles à filtrer ou surveiller. (comment différencier une page web d'un accès au bureau distant ??)
- ☐ N'importe quel utilisateur qui connaît le couple Identifiant / mot de passe peut se connecter à distance.
- ☐ Si l'utilisateur local qui a lancé le logiciel, a un privilège élevé (admin), le télé-intervenant hérite de tous ses privilèges.
- ☐ Conditions d'utilisation du logiciel : Licence valide dans le cadre d'une utilisation professionnelle ?

En pratique : utilisation en interne par les utilisateurs : accès distants sans autorisation d'un responsable, et sans passer par les méthodes d'authentification réglementaires : AD / CAS / fédérations d'identités etc...

Argument d'utilisation : C'est plus pratique que le bureau à distance de l'OS... et moins contraignant.

➡ Les règles de PSSI et filtrage de sécurité du firewall sont contournées.

03 Rappel des règles (tutelles)

Règlementation ANSSI

L'utilisation d'outils de télé-assistance est réglementée au niveau gouvernemental

ANSSI : Agence nationale de la sécurité des systèmes d'information

Le CNRS applique directement les recommandations de l'ANSSI et s'applique à TOUS ses agents (y compris utilisateurs)

Documentation officielle :

http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf.

NT-004/ANSSI/SDE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 13 janvier 2017

N° DAT-NT-004/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 8

NOTE TECHNIQUE

RECOMMANDATIONS DE SÉCURITÉ RELATIVES À LA TÉLÉ-ASSISTANCE



Public visé :

Développeur	
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	✓

Règlementation CNRS

Le CNRS s'appuie sur les directives de l'ANSSI

NOTE du CNRS OFFICIELLE du 23/01/2017 (mise à jour le 08/07/2019)

<https://securite-si.cnrs.fr/html/EXP-RES-6-implementation.html>

<https://securite-si.cnrs.fr/consignes/systemes/pmad/>

Date Modifié par Approuvé par Objet de la mise à jour
02/10/2013 F. Morris L. Di Benedetto Version initiale
01/07/2017 F. Morris M. Chabanne Intégration PSSIE

Implémentation

La prise de main à distance sur le poste de travail d'un utilisateur ne peut être réalisée que dans les conditions suivantes :

1. L'intervenant doit être clairement identifié et habilité par l'unité à administrer les postes de travail
2. La présence de l'utilisateur habituel ou du propriétaire du poste de travail est obligatoire
3. L'outil de prise de main à distance utilisé doit lui-même répondre à plusieurs critères :
 - a. Outil sûr et référencé par l'ANSSI et/ou le CNRS en connexion point à point sans utilisation de solution type "cloud", sauf si celle-ci est interne à l'unité ou au CNRS et complètement maîtrisée.
NOTA: les outils non maîtrisés (en particuliers les outils tiers utilisant des services hébergés sur Internet en mode SaaS) sont proscrits pour la prise de main à distance.
 - b. Avoir un mécanisme qui oblige une acceptation préalable, par l'utilisateur du poste, à la prise de main par l'intervenant.
 - c. Visibilité totale par l'utilisateur des actions réalisées par l'intervenant
 - d. Possibilité pour l'utilisateur de forcer la déconnexion de l'intervenant à tout moment

Cas particulier d'intervention sur des postes situées en ZRR:

Dans le cas où un poste de travail situé en ZRR nécessite une intervention avec prise de main à distance, il faut s'assurer que le personnel intervenant réponde aux critères de conditions d'accès à la ZRR concernée.

Règlementation ANSSI + CNRS

Ce qu'il faut retenir des réglementations imposées par les tutelles

R1 : L'opération de télé-assistance doit s'effectuer dans le contexte de l'utilisateur, avec ses droits [...]

➡ Pas de télé-assistance directement sur un compte administrateur (c'est à l'utilisateur local d'autoriser l'élévation de privilèges, idéalement via les fonctions intégrées de l'outil de PMAD ou avec un compte admin local connu et référencé)

L'utilisateur doit être en mesure de voir ce que fait le télé-assistant (supervision)

➡ L'utilisateur-trice doit rester devant l'ordinateur pendant la prestation de télé-assistance

R11: La télé-assistance ne doit pouvoir être opérée que depuis des adresses IP sources bien identifiées comme étant celles des postes des télé-assistants

➡ Protection au niveau du firewall (filtrage réseau) et limitation sur le poste informatique ciblé (filtrage côté client)

Remarque : Il est important de bien distinguer la télé-assistance de la télé-administration par prise en main à distance. La première s'opère dans le contexte de l'utilisateur, à la différence de la deuxième qui s'opère avec un compte à privilèges dédié à cet usage (compte « admin »)

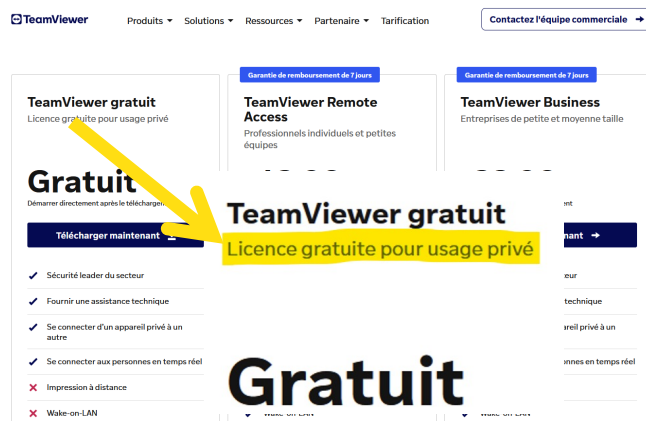
Règlementation : Contrats de licence

La totalité des logiciels, qu'ils soient payants, libres, ou « gratuits » sont soumis à des licences d'utilisation (CLUF*)

Comparatif des différentes solutions rencontrées dans le laboratoire, et contrats de licences associés

TEAMVIEWER

<https://www.teamviewer.com/fr/download/free-download-with-license-options>



ANYDESK

<https://anydesk.com/fr/commander>

GRATUIT dans le cadre personnel

Quelle est la différence entre la licence gratuite et la licence payante ?

AnyDesk est gratuit pour un usage personnel et offre un ensemble limité de fonctionnalités et de support. Les utilisateurs professionnels ont besoin d'une licence. Cliquez ici pour obtenir davantage de détails sur les avantages d'une licence payante. Si vous n'êtes toujours pas sûr, cliquez ici pour en savoir plus sur les différences entre un usage personnel et un usage professionnel.

SPLASHTOP SOS

<https://www.splashtop.com/legal/terms-of-service>

4. END USER LICENSE AGREEMENT

b. Commercial Use. The Splashtop Business Products, Splashtop Classroom, Splashtop On-Prem, and Mirroring360 Products are fully licensed for commercial use in a professional environment. Splashtop Personal is for non-commercial use only, i.e. use it to access Your personal computers for non-work related purposes. Splashtop Secure Workspace, Splashtop Vault and Foxpass may be licensed for either commercial or non-commercial use.

CLUF : contrat de licence de l'utilisateur final (celui qu'il faut accepter en cochant une croix avant d'installer le logiciel)

Règlementation : conclusions

Les contrats de licence, et le mode de fonctionnement de la majorité des logiciels de pmad sont incompatibles avec la PSSI du CNRS.

1) La majorité des outils de prise en main à distance utilisés dans les laboratoires, ne répond pas aux critères fixés par les tutelles

- Les services sont externes, indépendants du laboratoire, et non maîtrisés. (Serveurs étrangers ou offres de type cloud)
- Teamviewer, AnyDesk, et slashtopSOS ne sont ni référencés, ni recommandés par l'ANSSI ou le CNRS
- L'hébergement externe, et non maîtrisé de ces solutions de pmad sont proscrites (= interdites) par les tutelles.

2) Les licences d'utilisation gratuites, excluent généralement toute utilisation à titre professionnel.

Rappel: Le contexte d'utilisation des logiciels dans un laboratoire de recherche financé par l'état, n'est pas d'ordre privé, ou personnel.

3) Constat : L'utilisation initiale des ces outils, destinée initialement pour les interventions de sociétés externes, a été étendue au périmètre du S.I et détournée (de manière involontaire ?), ce qui favorise le contournement de la PSSI du laboratoire.

04 Solution proposée à l'INCI

Solutions recommandées

Etude de cas : 2 solutions recommandées par l'ANSSI

1. Apache Guacamole (<https://guacamole.apache.org/>)

Solution « full-web » sans installation de logiciel, qui permet d'accéder aux ordinateurs depuis un simple navigateur internet (portail d'accès) via différents protocoles d'accès distants (vnc/ssh/rdp)
La solution s'avère être compliquée (Installation, mise à jour, migration de serveur en cas de panne, sauvegarde de configuration), et se limite encore nativement à l'accès aux postes windows et linux.

2. RustDesk (<https://www.rustdesk.com>)

Solution Client/Serveur alternative à Teamviewer, sous licence GPL, et libre d'utilisation. Il existe une version payante (~ 20\$/mois pour 20 utilisateurs et 100 ordinateurs) qui permet de gérer via une console centrale l'ensemble de la solution et de débloquent de nombreuses fonctionnalités.

Version libre : serveur hébergé dans le périmètre S.I (on-premise) et qui remplit en grande partie les critères imposés par les tutelles. C'est la solution qui a été retenue de par sa simplicité d'utilisation, et sa compatibilité avec l'ensemble des systèmes. (windows/mac/linux/android)



<https://rustdesk.com/>

Le télé-intervenant et l'utilisateur local installent et lancent le programme d'accès distant, qui contient l'adresse IP publique du serveur, et son certificat d'identification unique chiffré (1)

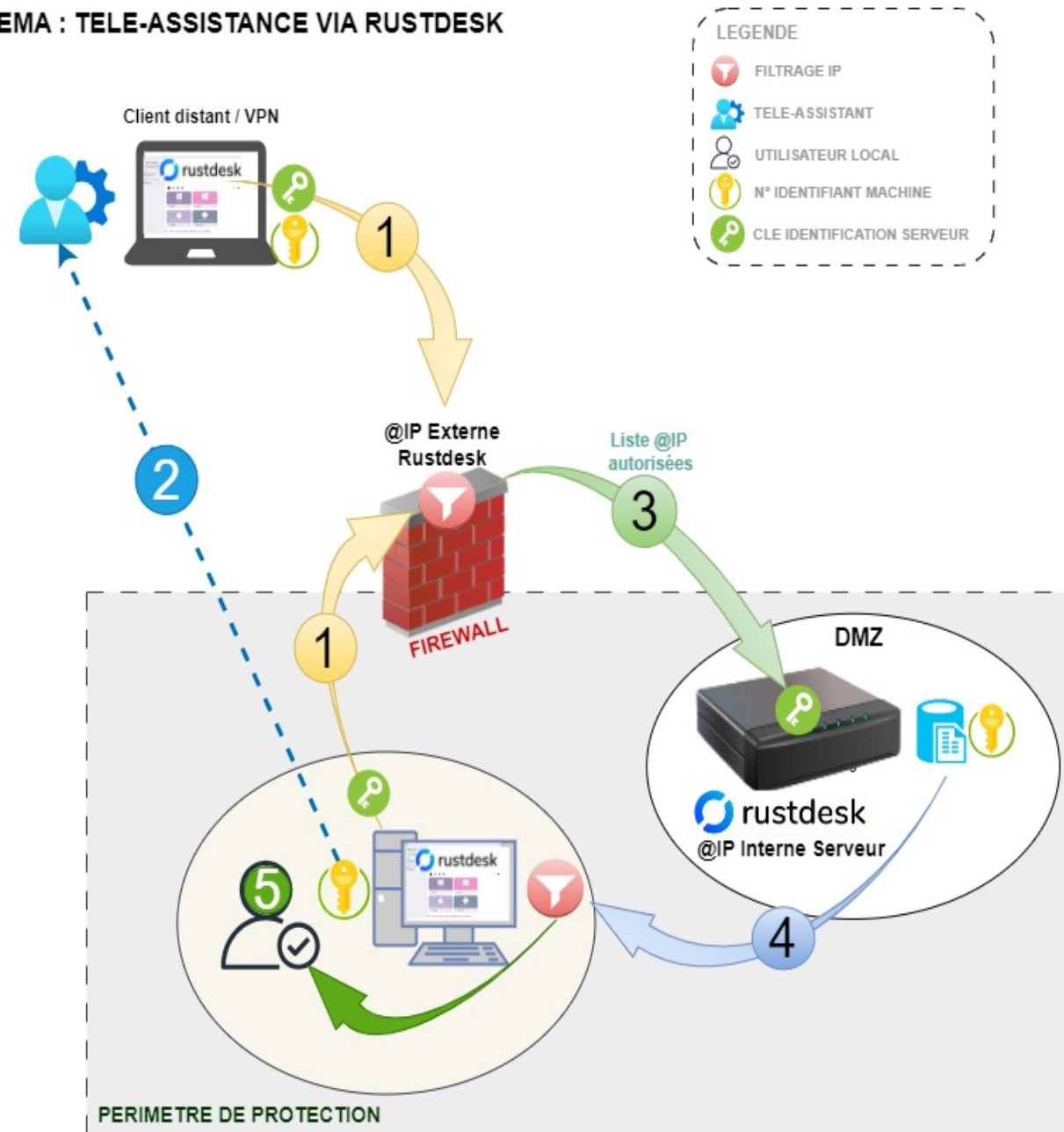
L'utilisateur communique le numéro d'identifiant machine de son ordinateur au télé-intervenant (2).

Si l'IP distante est autorisée, le firewall redirige la connexion sur le serveur RustDesk local situé dans la DMZ (3)

Le serveur appaire les deux postes et redirige la requête de connexion vers l'ordinateur local (4)
L'utilisateur reçoit et accepte la demande de connexion distante (5)

➡ Le télé-intervenant a accès au bureau distant

SCHEMA : TELE-ASSISTANCE VIA RUSTDESK



05 **Démo (Live)**

Mise en œuvre de rustdesk

Déploiement dans le périmètre

- ❑ **Installation du serveur :** <https://rustdesk.com/docs/fr/self-host/rustdesk-server-oss/install/>

En comptant l'installation du serveur (debian) : ½ journée (avec la pause café)

- ❑ **Déploiement manuel du client**

L'installation du client avec ses paramètres peut durer entre 5-10 minutes selon les paramètres à appliquer (autorisation IP, mise en place 2FA etc..)

- ❑ **Déploiement du client via un paquet**

La version payante de rustdesk permet d'automatiser le déploiement à grande échelle, avec un paquet vraiment customisé pour l'entreprise (logo, paramètres etc..)

Pour la version « libre » il faut construire un paquet soi-même et ruser. (ex: innosetup), et déployer le fichier de configuration toml dans le dossier appdata (windows) de l'utilisateur (session-setup wapt ou gpo par exemple)

06 Conclusion(s)

Retex RustDesk a l'INCI

AVANTAGES

- Fonctionnement identique à Teamviewer ou Anydesk
- Multi-OS (++++)
- Interface intuitive et simple pour les utilisateurs (++++)
- Licence GPL (<https://www.gnu.org>)
- Depuis la 1.2.6 : Double authentification (2FA) (++++)
- Solution logicielle recommandée par les tutelles (++++)
- La solution est gérée dans le périmètre S.I (+++)
- Maîtrise des accès (filtrages @IP distants/locaux)
- Ports de communication réseaux dédiés, et identifiés
- Infrastructure légère (VM/conteneur possible)

INCONVENIENTS

- Pas de contrôle au niveau utilisateur (version payante: oui)
- Pas de console de gestion centrale (version payante: oui)
- Pas de support sur le logiciel (version payante: oui)
- Serveur actuel : récupération (Dell R200 hors garantie)
- Maîtrise et compréhension des translations d'adresses (NAT) nécessaire sur les routeurs (firewall).
- Identification préalable des ordinateurs distants (liste blanche d'adresses IP à définir)
- **Déploiement automatisé du Client** : Nécessite de créer un paquet innosetup qui contient la clé publique et les fichiers de configuration toml du client rustdesk (appdata user)

RustDesk : une solution de prise en main à distance valable

- ✓ Le cahier des charges des tutelles est en majorité respecté.
- ✓ La surcouche de protection (certificats, filtrages, 2FA) est transparente pour les utilisateurs
- ✓ C'est une solution de télé-assistance ergonomique pour les usagers
- ✓ La mise en oeuvre sur le périmètre local ne nécessite pas de gros moyens
- ✓ Le coût de licence est abordable (200\$/an pour 10 utilisateurs / 100 postes)
- ✓ Solution unique, qui remplace efficacement l'ensemble des solutions d'accès à distances existantes (RDP, VNC, Teamviewer etc.) et qui est multi-écrans !

Utilisation globale: prestataires externes, supervision de plateformes, support informatique

- ✓ La solution payante permettrait de faciliter la gestion de la PMAD sur le parc informatique (console de gestion centrale), et apporte des fonctionnalités en matière de sécurité informatique (droits utilisateurs)
- ✓ Déploiement à l'INCI : réalisé depuis fin Juin, le serveur est opérationnel. (a compléter : documentation)

Questions ?