
PASSWORD PROTECT
1234
567
89
10
HACKING DETECTED
01010101110000101010111000
01010101110000101010111000

SÉCURITÉ

PROLIFÉRATION DES CYBERATTAQUES

DANS LE MONDE EN 2024

L'IA DÉCUPLE L'EFFICACITÉ DES VIRUS

98% DES ATTAQUES UTILISENT L'EMAIL COMME VECTEUR PRINCIPAL

+ 30 % DE CYBERATTAQUES PAR RAPPORT À 2023

EN FRANCE

+ 400% DE CYBERATTAQUES DEPUIS 2020 EN FRANCE

UNE CYBERATTAQUE **TOUTES LES 39 SECONDES**

69% DES VICTIMES SONT DES **TPE/PME**

PROLIFÉRATION DES CYBERATTAQUES

DANS LE MONDE EN 2024

L'IA DÉCUPLE L'EFFICACITÉ DES VIRUS

98% DES ATTAQUES UTILISENT L'EMAIL COMME VECTEUR PRINCIPAL

+ 30 % DE CYBERATTAQUES PAR RAPPORT À 2023

EN BELGIQUE

AUGMENTATION DE 69% D'INCIDENTS

1 231 ATTAQUES PAR SEMAINE

LE PHISHING A AUGMENTÉ DE 66%

PROLIFÉRATION DES CYBERATTAQUES

DANS LE MONDE EN 2024

L'IA DÉCUPLE L'EFFICACITÉ DES VIRUS

98% DES ATTAQUES UTILISENT **L'EMAIL** COMME VECTEUR PRINCIPAL

+ 30 % DE CYBERATTAQUES PAR RAPPORT À 2023

EN SUISSE

AUGMENTATION DE 15% DES CYBERATTAQUES

+25 000 INCIDENTS DE CYBERSÉCURITÉ

45% DES INCIDENTS SONT LIÉS AU **PHISHING**

LES DIFFÉRENTS TYPES DE CYBERATTQUES

N°1

Virus /
Malware

Parmi les malwares, le ransomware est le type de menace le plus répandu, représentant à lui seul 46% des attaques !

MAIS AUSSI

Hameçonnage
/ phishing

Arnaque au président
/ CEO fraud

Déni de service
/ DDOS

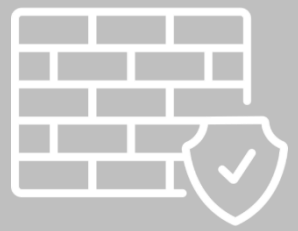
LA SÉCURITÉ AU CŒUR DES PRIORITÉS !

- Comment se prémunir des attaques ?

Dernière étape pour sécuriser ses données…

Antivirus/ anticrypto

Firewall

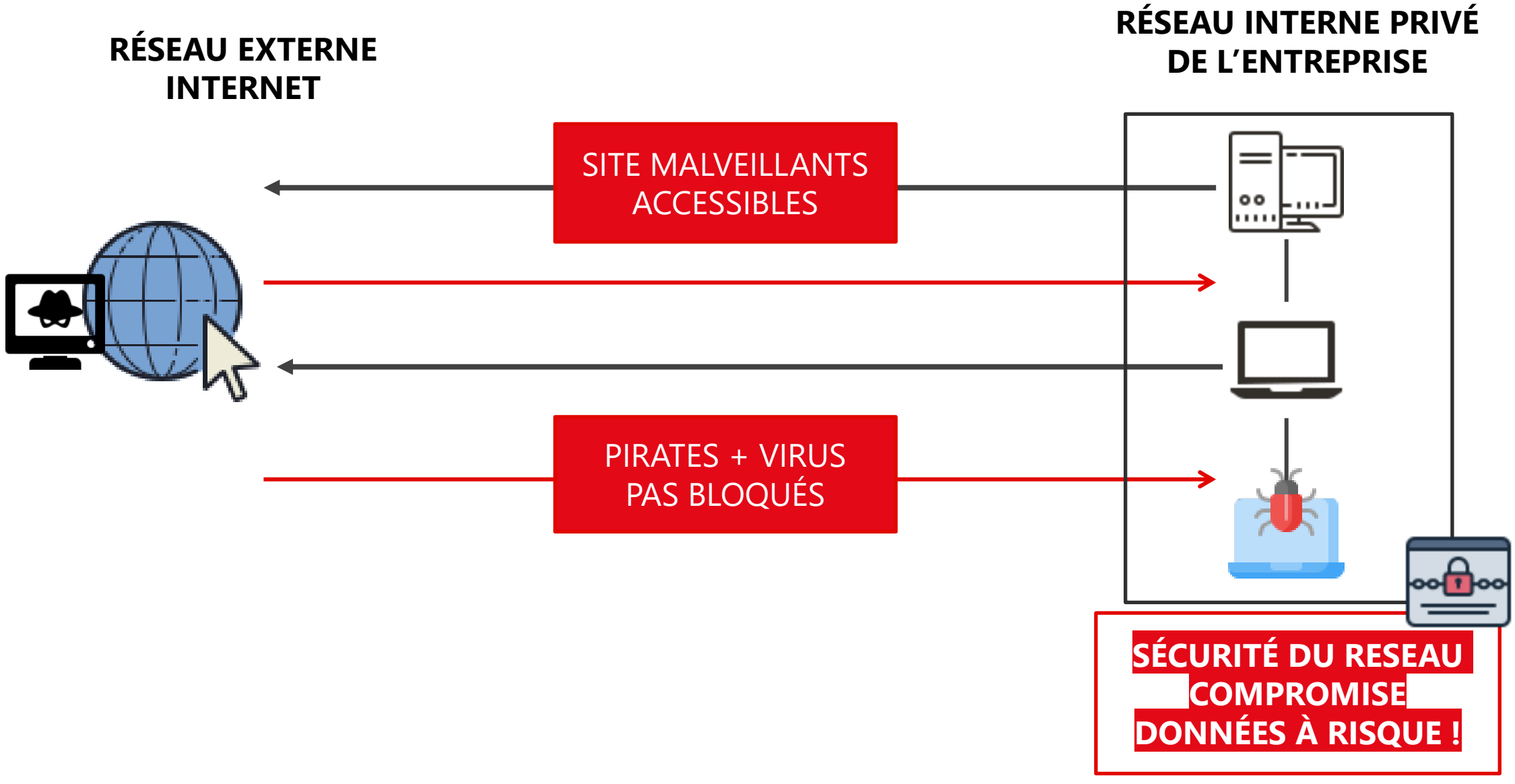


Antispam

Sauvegarde externalisée

SÉCURITÉ DU RÉSEAU FIREWALL

SANS FIREWALL, QUELS SONT LES IMPACTS ?

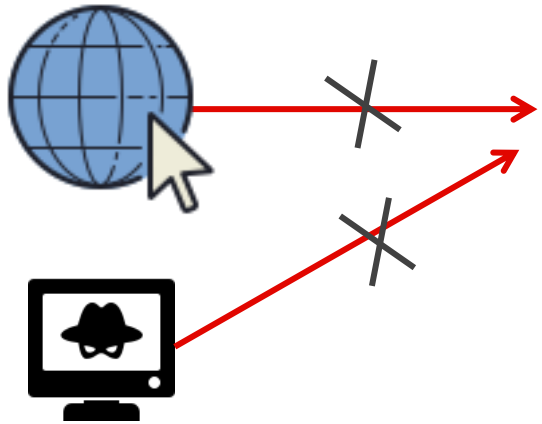


LE RÔLE DU FIREWALL

RÉSEAU EXTERNE INTERNET

Connexions entrantes bloquées

Bloque les tentatives de connexion d'Internet vers les ordinateurs du réseau local

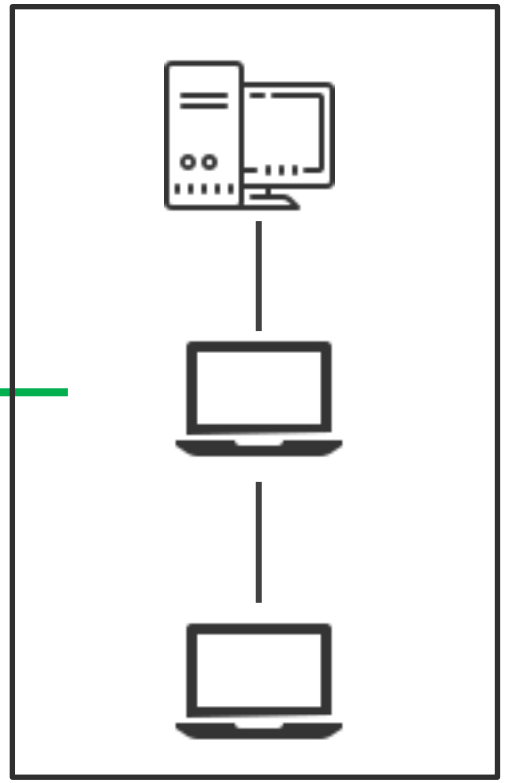


Connexions sortantes autorisées selon des règles

Autorise les ordinateurs du réseau à se connecter à Internet en toute sécurité

Listes noires X
Listes blanches ✓

RÉSEAU INTERNE PRIVÉ DE L'ENTREPRISE



FIREWALL
« MUR VIRTUEL »

RÉSEAU ET DONNÉES PROTÉGÉS !

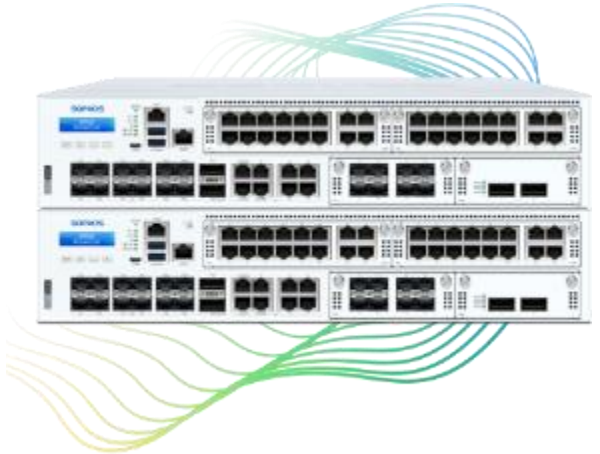
OFFRE PACKAGÉE, CLAIRE ET FACILE À CHIFFRER

Les menaces réseau sont complexes… mais protéger son entreprise ne doit pas l'être !

- ✓ *Boîtier Firewall*
- ✓ *Mise à jour du boîtier*
- ✓ *Maintenance*
- ✓ *Gestion des firewalls par XEFI*

	Sécurité Firewall Protection Standard	Sécurité Firewall Protection XSTREAM	
	Par boîter • Protection du réseau • Filtrage des URL • Accès à distance (VPN)	*1er boîtier sur site* + Ouverture et exécution de fichiers inconnus hors du réseau	*Cluster* *(2nd boîtier sur site)* Second boîtier (haute disponibilité du réseau)
Maximum 5 utilisateurs *(limité à 500 Mbits/sec)*	49 €	59 €	39 €
Maximum 15 utilisateurs	79 €	89 €	59 €
Maximum 35 utilisateurs	109 €	119 €	79 €
Maximum 50 utilisateurs	169 €	179 €	99 €
Maximum 100 utilisateurs	229 €	239 €	129 €
Frais de mise en service		**790 €**	

1 PROTECTION STANDARD



➔ **Protége le réseau des intrusions et menaces**

Contrôle des connexions entrantes et sortantes

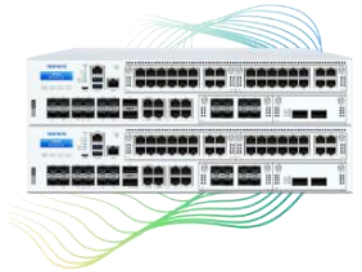
➔ **Contrôle les accès Web et les applications :**

- *Définition de listes blanches et noires*
- *Attribution de règles de navigation par réseau et/ou par groupes d'utilisateurs*

➔**Permet d'accéder au réseau depuis l'extérieur de manière sécurisée**

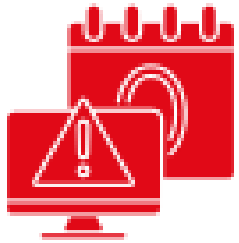
- *Accès à distance sécurisé (VPN)*

2 PROTECTION XSTREAM



➔ Toutes les fonctionnalités de la Protection Standard

\+ **Couche de <u>protection supplémentaire</u> contre les nouvelles vulnérabilités non connues**
➔ protection zero day !



Détecte et bloque les nouvelles menaces <u>encore inconnues</u>

➔ avant qu'elles n'atteignent le réseau

➔ avant qu'elles ne causent des dommages !

1. Téléchargement de fichiers provenant d'Internet <u>hors du réseau de l'entreprise</u>	2. **Analyse comportementale** des fichiers dans un cloud Sophos isolé et sécurité	3. Téléchargement du fichier sur le **<u>réseau du client</u> si inoffensif !**

STOCKAGE ET REPORTING DES LOG

- **La CNIL** recommande de conserver les logs de connexion **entre 6 et 12 mois**
- La loi impose aux entreprises qui proposent un **WIFI public** de conserver les logs pendant **12 mois.**

ALERTER LE CLIENT :

La <u>responsabilité légale du dirigeant peut être mise en cause</u> concernant les connexions internet de ses collaborateurs !

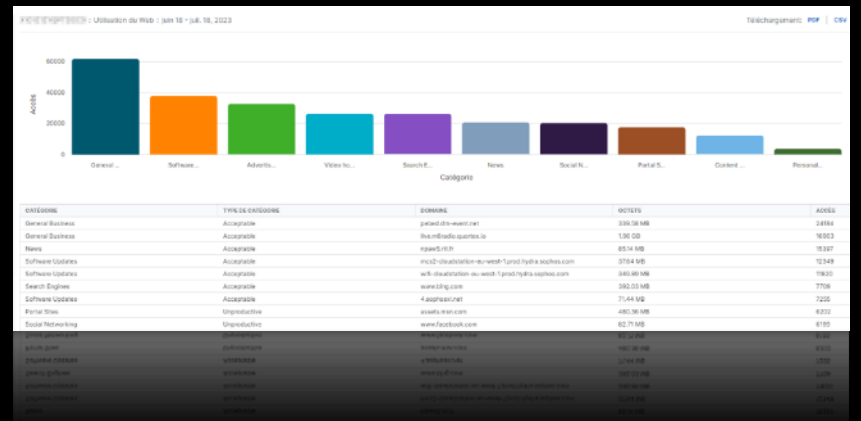
EXPLIQUER L'INTÉRET AU CLIENT :

En cas <u>d'incident</u>, <u>d'intrusion</u>, ou de <u>détournement d'usage</u>, les logs sont un **outil efficace d'investigation et donc de protection**

TABLEAU DE BORD PRATIQUE ET INTELLIGENT

Visualisez :

1. L'état et l'utilisation des firewalls
2. Les **menaces bloquées** et les **alertes** de sécurité
3. Les violations de **politiques** de **sécurité** et les applications à risque

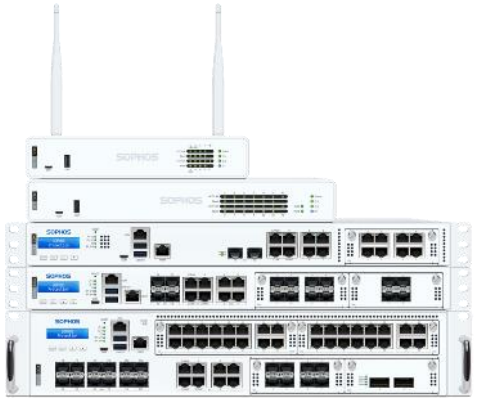


UN BOITIER ADAPTÉ

COMBIEN DE PERSONNES SE CONNECTENT AU RÉSEAU ?

- Prendre en compte tous les équipements périphériques :
  ordinateurs, téléphones portables, tablettes, utilisateurs connectés en Wifi et ceux à distance

- Demander au client l'usage qu'il a de ses équipements :
  Par exemple : tablette à prendre en compte si utilisée pour lecture de grosses vidéos ou téléchargement de gros fichiers



CIBLE DU BOITIER 5 UTILISATEURS :

très petites entreprises, artisans, médecins … (débit internet limité !)

› **Ne proposez pas le 5 utilisateurs alors que vous pourriez vendre le 15 !**

› Pas de boitier 5 utilisateurs dans les offres Cloud

Un boitier bien dimensionné vous permettra d'éviter les surcharges et des soucis avec votre client !

OBJECTION SUR LE CONTRAT DE SÉCURITÉ :

« CA ME COUTE TROP CHER JE PREFERE L'ACHETER »

Notre solution n'est pas uniquement un firewall mais surtout sa mise à jour et sa supervision par une équipe de professionnels.
Un firewall non mise à jour est une faille de sécurité.

Si achat sec + maintenance, les pièces ne sont pas incluses et au final ce n'est pas rentable à terme. Votre budget ne sera pas maitrisé.

LE CLIENT DOIT PRENDRE CONSCIENCE DE LA VALEUR DU SERVICE

OBJECTION SUR LE CONTRAT DE SÉCURITÉ :

« J'AI DÉJÀ UN FIREWALL ET JE N'AI JAMAIS EU DE PROBLEME »

Tant mieux, mais cela ne veut pas dire que vous en aurez jamais.
Les virus et méthodes d'attaques évoluent en permanence.
Pourriez-vous me confirmer que votre firewall est maintenu en temps réel par un spécialiste ?
Est-ce que depuis son installation il a été contrôlé, testé, vérifié, mise à jour ?

Un firewall n'est pas seulement un outil, c'est avant tout un logiciel qui doit être tenu à jour et supervisé.
C'est pour cela que nos intégrons notre firewall avec 100% de services (supervision, maintenance, mise a jour et remplacement)

Avez-vous des fonctionnalités de filtrage d'URL ? Afin de contrôler notamment l'usage d'Internet par vos collaborateurs

OBJECTION SUR LE CONTRAT DE SÉCURITÉ :

« POURQUOI FACTUREZ-VOUS DES FAS J'AI DÉJÀ LA MAINTENANCE CHEZ VOUS »

Le contrat de maintenance comme son nom l'indique a pour but de maintenir votre matériel, cependant la mise en place d'un firewall n'est pas de la maintenance de poste ou serveur.

Nous facturons des frais d'accès car nos techniciens ont été formés, et certifiés sur la mise en place de ce matériel. La mise en service de cet équipement implique une installation équivalente à une journée technique (préparation atelier, intégration sur site avec déploiement des stratégies de sécurité)

LE CLIENT DOIT PRENDRE CONSCIENCE DE LA VALEUR DU SERVICE

OBJECTION SUR LE CONTRAT DE SÉCURITÉ :

« J'AI DÉJÀ UN FIREWALL INCLUS DANS MA BOX OPÉRATEUR »

Avec une box tous les ports sont ouverts, il n'y a pas de règles ; il n'y a pas de possibilité de gérer des accès à distance sécurisés, de contrôler les accès et log de connexion des utilisateurs.

Avec un opérateur, la maintenance peut être très compliquée et le délai de réponse téléphonique et celui d'intervention d'un technicien sont souvent longs.

L'important n'est pas le firewall en soit, mais les mises à jour et la supervision quotidienne par des professionnels !

OBJECTION SUR LE CONTRAT DE SÉCURITÉ :

« JE N'AI PAS BESOIN D'UN FIREWALL, J'AI DÉJÀ UN ANTIVIRUS ET UN ANTISPAM »

L'antivirus et l'antispam protège un poste et non pas un réseau.
Exemple de la douane (firewall) et de la police (antivirus/antispam)

Toute entreprise a besoin de protéger son réseau et ses données des attaques malveillantes.

Tout chef d'entreprise est responsable de ce qui se passe sur son réseau, en cas de problème il doit pouvoir fournir les logs de connexions

Si l'on vous bloque l'accès à vos fichiers, quelle incidence il y aura sur votre activité ?

LE CLIENT DOIT PRENDRE CONSCIENCE DU RISQUE

OBJECTION SUR LE CONTRAT DE SÉCURITÉ :

« J'AI DÉJÀ UN FIREWALL AVEC WINDOWS »

Le firewall de Windows ne protège que le poste, pas tout le réseau.
Il faut être vigilants avec les paramétrages.

Ce firewall permet juste d'ouvrir ou fermer les ports
Il n'y a pas de filtrage web, pas de prévention d'intrusion, pas de VPN
Ce qui est gratuit ne peut pas avoir les mêmes fonctionnalités et les mêmes performances que des outils professionnels adaptés.

OBJECTION SUR LE CONTRAT DE SÉCURITÉ :

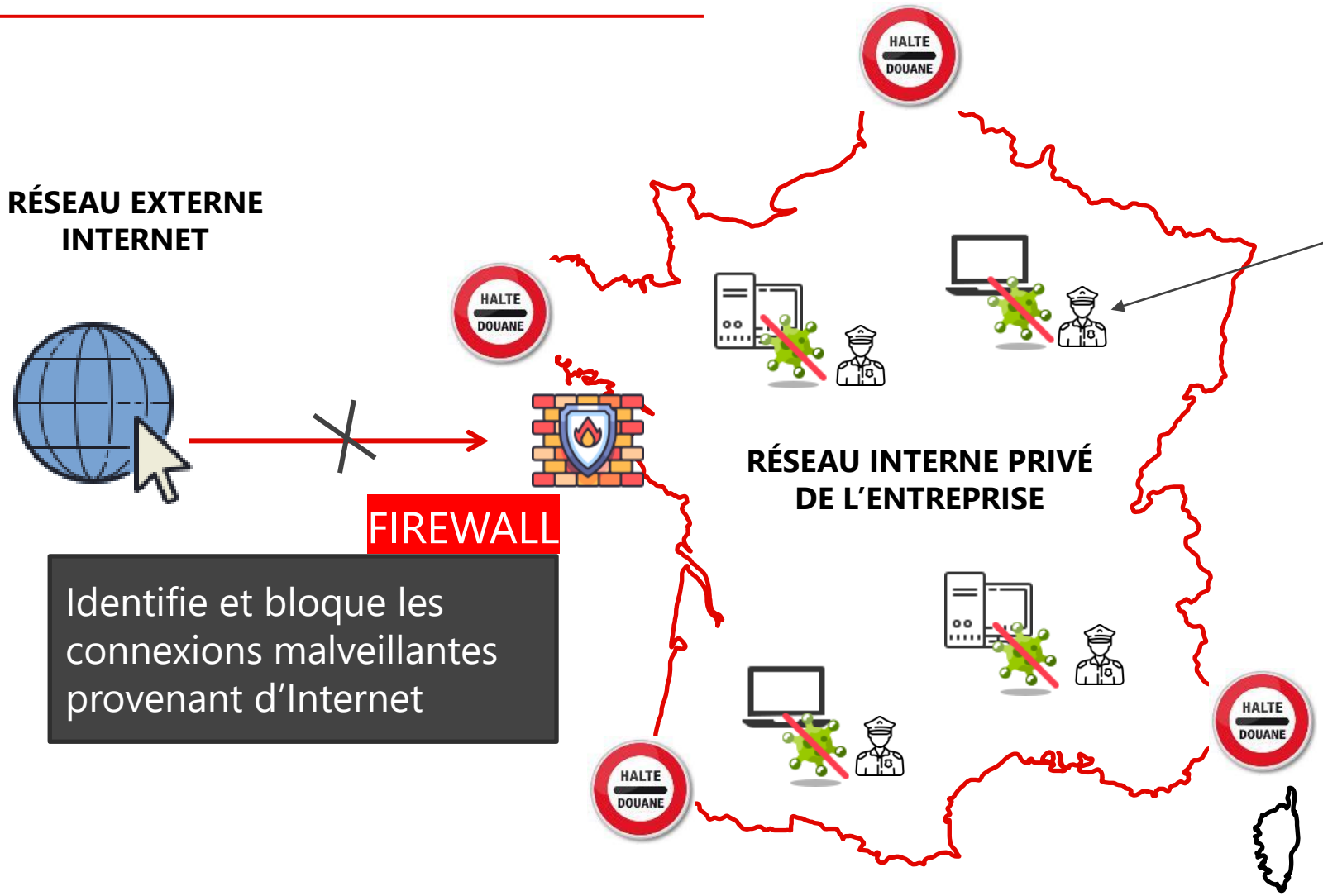
« NOUS SOMMES 20, LE BOITIER 15 UTILISATEURS ME SUFFIRA »

Les équipements périphériques supplémentaires tels que les téléphones portables et autres utilisateurs connectés en wifi sont considérés également comme 1 utilisateur.

Le nombre de périphériques de votre entreprise est plutôt évalué à 30 qu'à 20. Un boitier bien dimensionné vous permettra d'éviter les surcharges. De plus si votre équipe s'agrandit, pas besoin de changer de boitier pour contrôler toutes les connexions.

SÉCURITÉ DES POSTES

FIREWALL VS. ANTIVIRUS



FIREWALL

Identifie et bloque les connexions malveillantes provenant d'Internet

ANTIVIRUS

Détecte et neutralise les menaces externes (virus et ransomwares) qui arrivent sur <u>le poste via :</u>

- serveur partagé
- périphériques externes
- connexion hors réseau

L'OFFRE CRYPTOPROTECT

POURQUOI LE CLIENT DOIT SE PROTÉGER

➔ EN CAS D'ATTAQUE PAR RANSOMWARE :

- Prise en **otage des données** contre une **demande de rançon**
- Exploitation des **données personnelles avec risques de publication**
- **Dysfonctionnement** du matériel et systèmes, **jusqu'à l'arrêt total**

UNE PROTECTION ANTIVIRUS SEULE NE SUFFIT PLUS

NOTRE SOLUTION :

DOUBLE PROTECTION

Antivirus
+ ANTI-RANSOMWARE

AMÉLIORATION CONSTANTE

MAJ automatique grâce à l'intelligence artificielle

CONTINUITÉ D'ACTIVITÉ

Pas de perturbation pour l'utilisateur

*Un **prix unique,** serveur ou poste (3,40€)*