Institut Universitaire de Technologie
Aix*Marseille Université

HARIBO

Institut Universitaire de Technologie,
Aix-Marseille Université

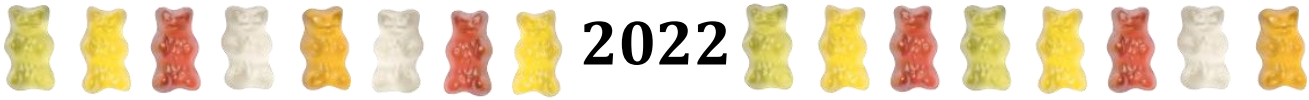
RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Sécurisation et déploiement du nouveau logiciel de VPN

Adam BERENGUER
HARIBO RICQLÈS-ZAN

Responsable entreprise : Laurence TELLO

Responsable académique : Anouch HOVSEPIAN



2022

Table des matières

Introduction

Dans le cadre de mon Diplôme Universitaire de Technologie (**DUT***) Réseaux et Télécommunications à l'**IUT*** (Institut universitaire de Technologie) d'Aix Marseille, j'ai effectué un stage de dix semaines, afin de mettre en pratique mes connaissances acquises lors de ma formation.

J'ai réalisé mon stage de fin d'étude dans le service informatique de l'entreprise Haribo Ricqlès-Zan, sous la tutelle de Laurence Tello, Manager Informatiques Systèmes & Réseaux.

Dans une entreprise aussi grande et importante que représente l'entreprise Haribo, il est fondamental d'assurer une sécurité stricte et efficace pour maintenir l'activité de production.

La mission qui m'a été confiée, a été de sécuriser les flux provenant des connexions **VPN*** (Virtual Private Network) utilisateurs et de déployer le nouveau client d'accès à distance.

La crise sanitaire ayant précipité la transition numérique, la mise en œuvre de VPN est devenue indispensable pour permettre le télétravail.
Néanmoins, sans sécurisation, cette solution peut représenter un danger.
Depuis plusieurs années, les cyberattaques sont devenues une préoccupation majeure pour la plupart des entreprises. Celles n'ayant pas suffisamment sécurisé leurs accès ont subi majoritairement des attaques du type **ransomware***.

J'ai commencé par l'étude d'un cluster de Fortigate pour comprendre sa configuration et être plus à l'aise dans mon projet. Par la suite, je me suis concentré sur l'analyse et la création de règles **firewall***, que j'ai appliquées puis testées. Enfin, j'ai contribué au déploiement du VPN dans l'entreprise.

Les mots en gras étoilés sont expliqués dans le glossaire page 21

1 L'entreprise et son organisation

1.1 Présentation de l'entreprise

Haribo est une entreprise familiale allemande de confiserie fondée en 1920 par le confiseur Hans Riegel originaire de Bonn. Le choix du nom « Haribo » est composé des deux premières lettres de son inventeur et de sa ville d'origine : **HA**ns **RI**egel **BO**nn.

Son implantation en France date de 1967, où l'enseigne a acquis les parts de l'usine Lorette à Marseille et est devenue « Haribo France S.A ». Elle fusionnera par la suite avec Ricqlès-Zan (composé de Zan et Ricqlès unifié en 1920) en 1987 situé à Uzès pour donner « Haribo Ricqlès-Zan ».

Haribo est un des leaders du secteur de la confiserie. Possédant une part de marché de 41% en France et 60 % en Allemagne, il s'impose comme le numéro 1 de la confiserie.

1.2 Localisation

Haribo Ricqlès-Zan se concentre sur trois principaux sites :

- Le site de Gèze, le siège social
- Le site **TLM*** (Tour la Marseillaise)
- Le site d'Uzès

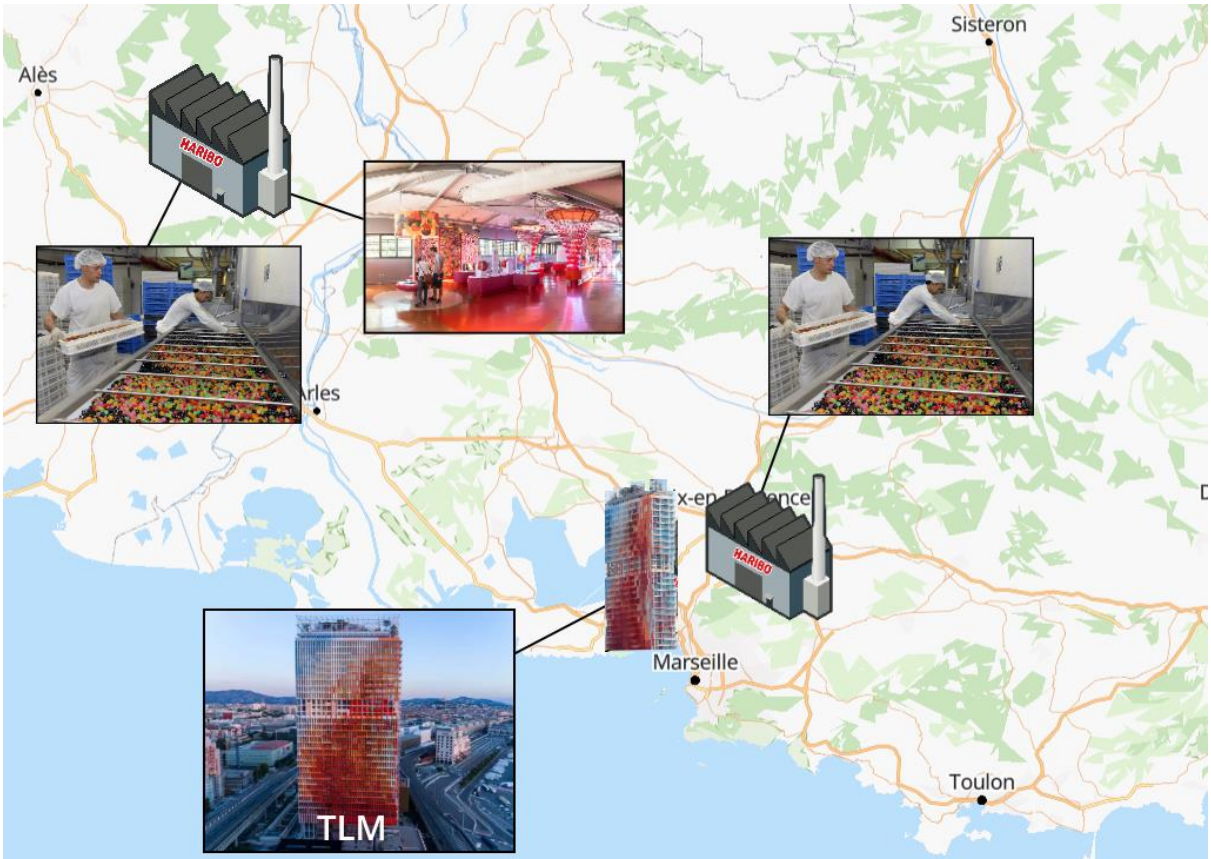


Figure 1 : Schéma des principaux sites d'Haribo Ricqlès-Zan

1.3 Organisation

Durant mon stage, j'ai pu travailler sur les trois différents sites, dans le service Informatique. Principalement basé à Gèze, j'intervenais une fois par semaine à la TLM, un lieu plus propice au support utilisateurs. J'ai visité également le site d'Uzès pendant une journée, ce qui m'a permis de rencontrer l'ensemble de l'équipe.

L'entreprise est actuellement dans une phase de transition numérique, pour donner suite à la récente uniformisation en groupe d'Haribo.

Actuellement, chaque pays dispose de son Active Directory (**AD***).

Dans le cadre de cette transition, l'objectif du groupe est de regrouper les Active Directory entre les différents pays et d'harmoniser le système d'information.

Un Active Directory est un annuaire chargé de répertorier tous les équipements du réseau (comptes des utilisateurs, comptes des ordinateurs et des serveurs, les imprimantes…).
Les administrateurs de celui-ci contrôlent l'accès et l'utilisation des ressources.

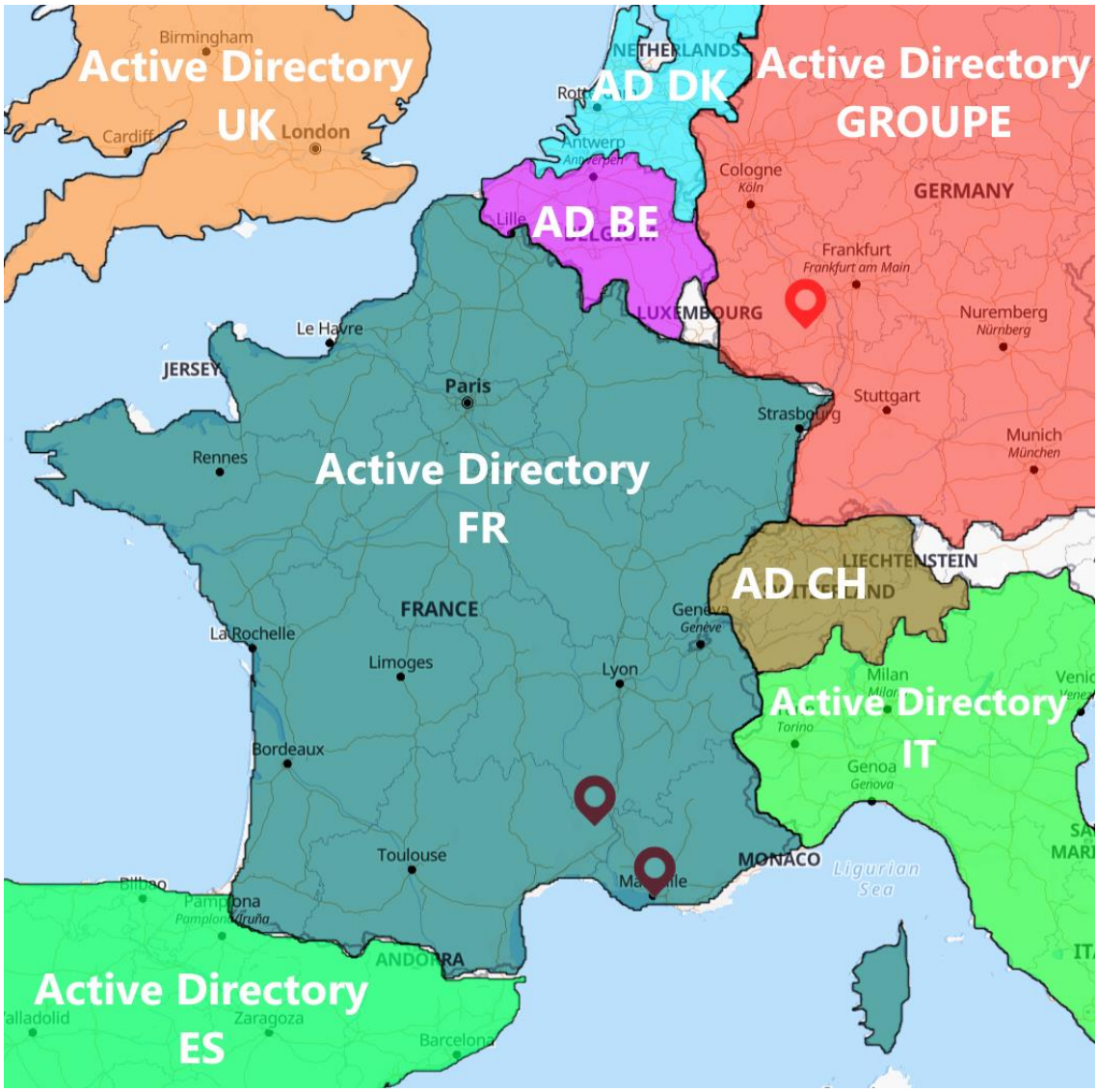


Figure 2 : Schéma de l'organisation de L'Active Directory

1.4 Organigramme

Ci-dessous l'organigramme du service Informatique :

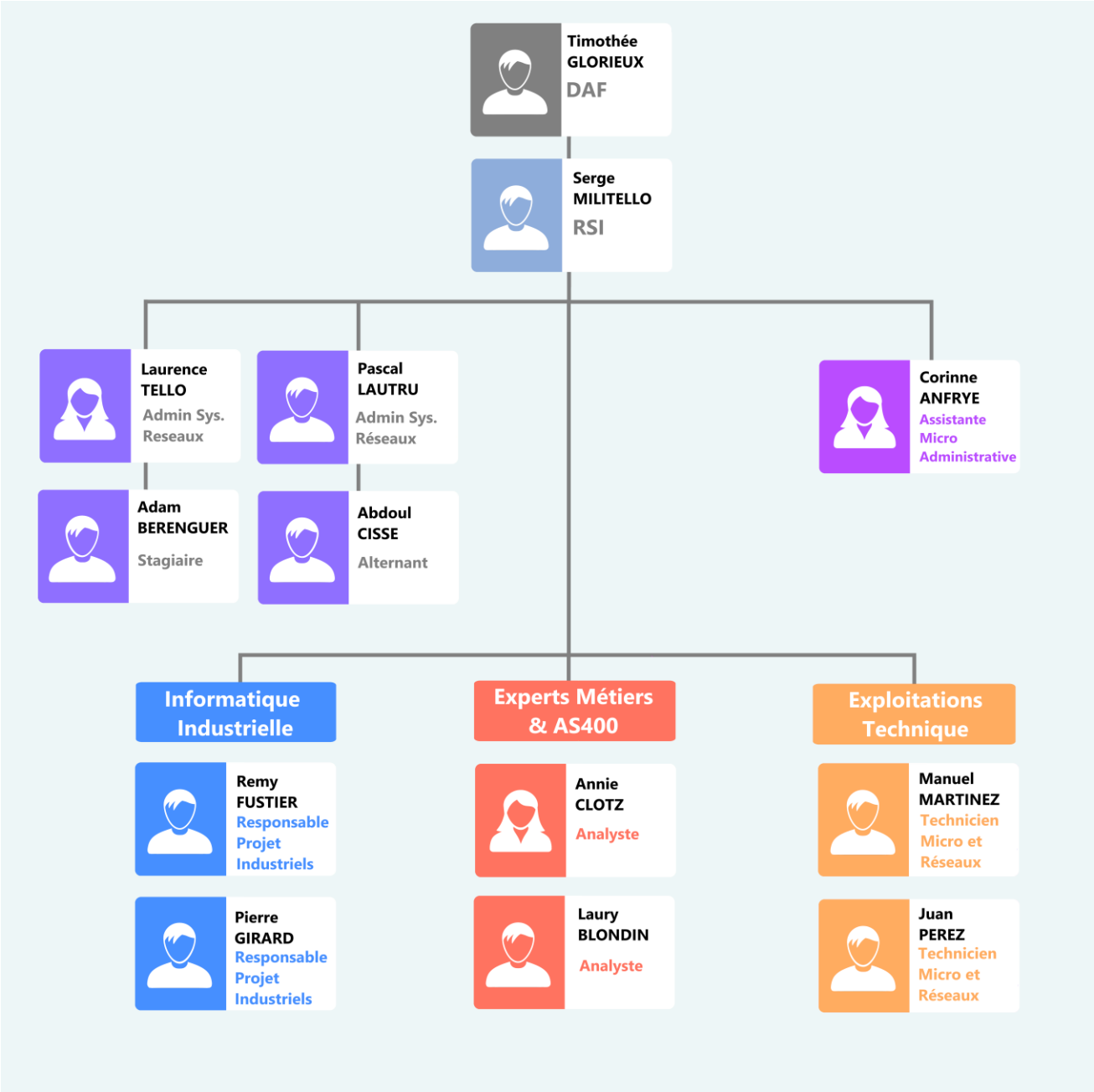


Figure 3 : Organigramme du service Informatique

2 Projet : Changement du client VPN

Les étapes du projet sont les suivantes :

- Analyse des règles existantes concernant l'actuel VPN
- Analyse et mise en œuvre des nouvelles règles firewall pour sécuriser les flux provenant des futures connexions **VPN*** (nouveau client)
- Élaboration d'un dossier de tests
- Création d'une documentation pour les utilisateurs et les informaticiens
- Installation et tests avec des bêta-testeurs
- Élaboration de la procédure pour déployer de manière industrielle le nouveau client VPN (**GPO***)

Qu'est qu'un VPN ?

Un réseau privé virtuel (VPN) est une connexion sécurisée et chiffrée entre deux réseaux.
Dans le cas d'Haribo, il s'agit d'une connexion entre un utilisateur distant (depuis son domicile par exemple) et le réseau interne (intranet) d'Haribo.

L'utilisateur peut ainsi accéder à des informations confidentielles de l'entreprise de manière sécurisée.

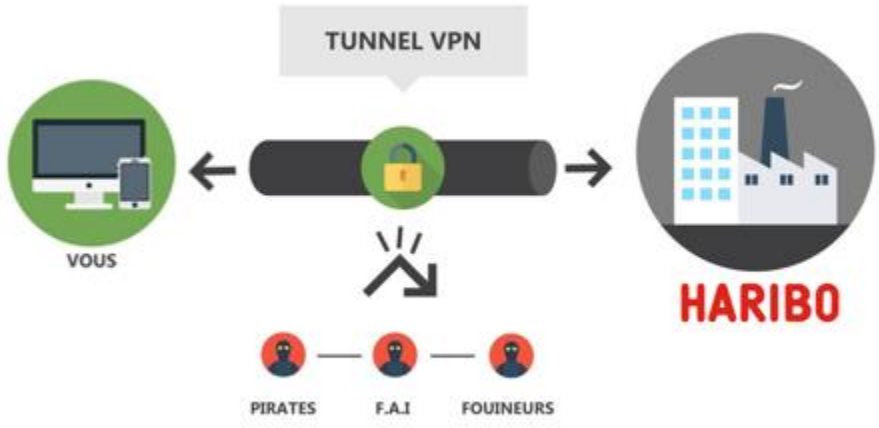


Figure 4 : Schéma du fonctionnement d'un VPN

Pourquoi changer de VPN ?

L'ancien VPN n'est plus maintenu par le constructeur, il est donc obsolète.

De plus, en raison de la récente uniformisation du groupe Haribo, chaque pays doit utiliser la solution VPN préconisée par le groupe.

A cela s'ajoute l'avantage d'un renforcement de la sécurité par l'utilisation du **MFA*** (Multi Factor Authentication)

2.1 Etude du firewall Fortigate

La première mission qui m'a été confiée par ma tutrice a été l'étude et la configuration d'un cluster de Fortigate, afin de m'initier aux commandes et à l'interface.

2.1.1 Équipement

Tout d'abord, ma tutrice et moi sommes allés récupérer des anciens firewalls dans la boutique Haribo, située en face de l'usine. Ce sont des Fortigate 600D, sortis en 2018, qui offrent des capacités de pare-feu parfaites, pour des entreprises de taille moyenne à grande.

Quel est le rôle du firewall ?

Le rôle d'un firewall est de protéger la totalité du trafic réseau. L'objectif est de créer les règles qui permettront de contrôler les accès au réseau et de sécuriser au maximum, en ne filtrant que l'essentiel. Les firewalls ont la capacité d'identifier et de bloquer le trafic indésirable.

Dans le cadre de mon projet, celui-ci sécurisa l'accès à distance.

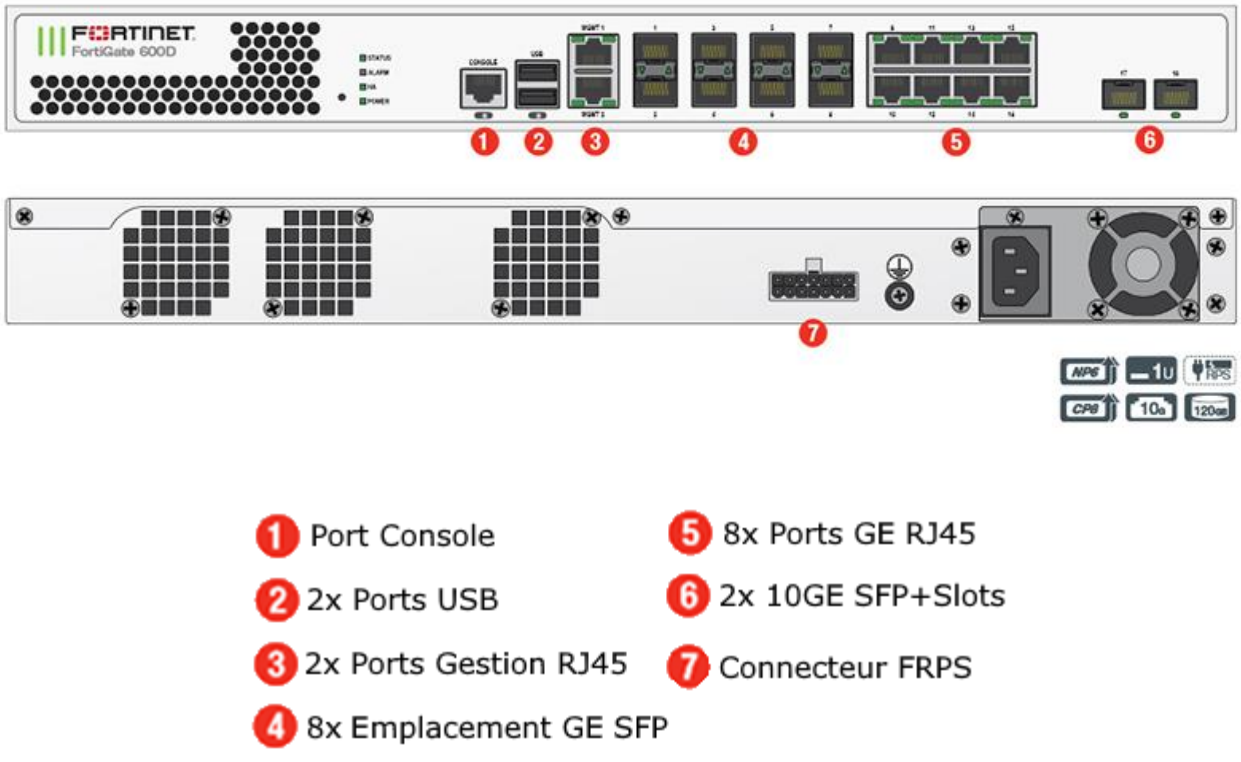


Figure 5 : Schéma et ports avant/arrière du Fortigate 600D

2.1.2 Mise en place

La première étape a été de réinitialiser les deux firewalls à l'aide de la commande :

```
FR-MRS-FW-AD1#execute factoryreset
```

J'utilise deux firewalls afin de créer un cluster, ce qui autorise le mécanisme de redondance de Fortinet, le FGCP (FortiGate Cluster Protocol).
Les boitiers communiquent via un lien **HA*** (High Availability) dédié, qui a pour objectif de synchroniser les tables de sessions et permet une reprise sans coupure du traitement des flux. Ceci s'explique par les signaux de Heartbeat envoyés par les firewalls toutes les x millisecondes.

Dans la photo ci-dessous, on peut observer les branchements que j'ai effectués :

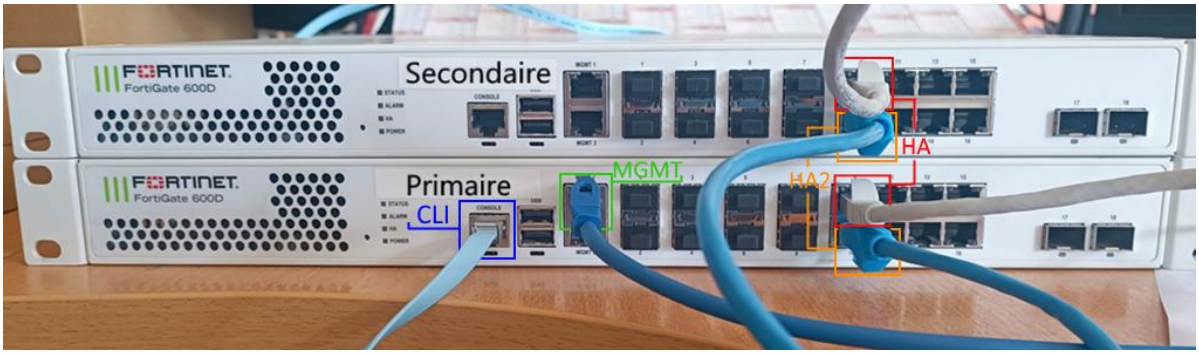


Figure 6: Photo du cluster Fortigate 600D

- Il s'agit du câble console qui permet d'accéder au CLI avec PuTTY
- Il s'agit du câble management permettant d'accéder à l'interface web en précisant l'adresse IP dans le navigateur
- Il s'agit du HA principal et des interfaces de heartbeat principales
- Il s'agit du HA secondaire et des interfaces de heartbeat secondaires

Lorsque l'on configure un firewall FortiGate, on a le choix entre deux interfaces :

- **CLI***, interface classique par commande qui nécessite une connexion par câble console et par PuTTY

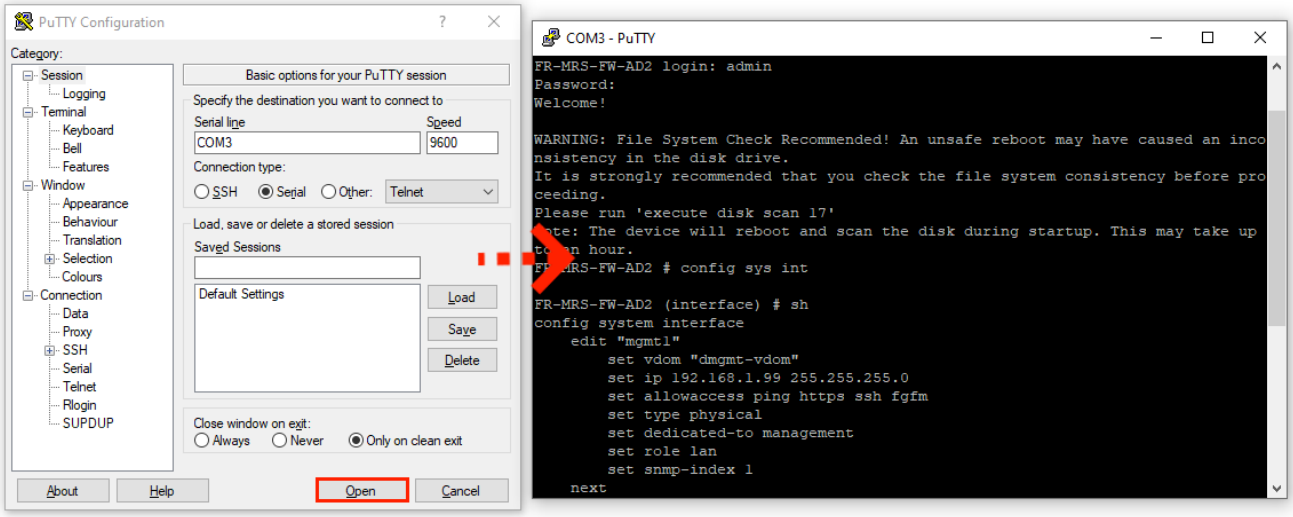


Figure 7 : Capture d'écran d'une connexion par PuTTY

- **GUI***, interface web disponible en précisant l'adresse IP du firewall, dans un navigateur

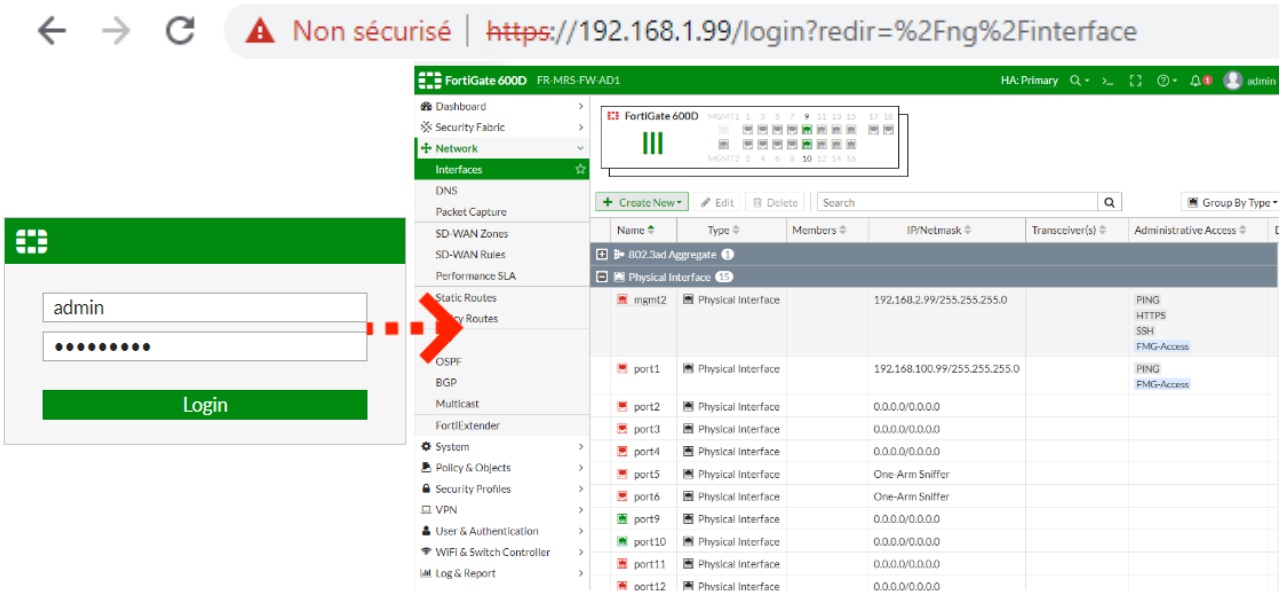


Figure 8 : Capture d'écran d'une connexion interface Web

Lorsque l'on réinitialise le firewall, l'adresse IP par défaut pour accéder à celui-ci sur le web est **192.168.1.99**

Il faut par la suite configurer un compte admin afin de pouvoir gérer le firewall.

Pour qu'un HA fonctionne correctement, nous devons :

- Entrer dans la configuration du HA :
```
FR-MRS-FW-AD1#config system ha
```

- Définir le mode, ici « active-passive » (si le firewall actif tombe le passif devient l'actif) :
```
FR-MRS-FW-AD1#set mode a-p
```

- Définir le « group-name » qui doit être identique sur les deux firewalls :
```
FR-MRS-FW-AD1#set group-name FR-MRS-FW-HA
```

- Définir le mode de passe du groupe HA qui doit être identique sur les deux firewalls :
```
FR-MRS-FW-AD1#set password MDP_Très_Compliqué
```

- Sélectionner les interfaces de Heartbeat qui correspondent aux ports qui relient les deux firewalls :
```
FR-MRS-FW-AD1#set hbdev <port> <priority>
```

- Définir la priorité pour identifier le firewall nominal du firewall esclave (la priorité la plus haute définit le nominal) :
```
FR-MRS-FW-AD1#set priority <priority>
```

- Activer « session-pickup » pour indiquer que les sessions ne sont pas perdues en cas de basculement entre les firewalls :
```
FR-MRS-FW-AD1#set session-pickup enable
```

Si les paramètres sont corrects, le statut du HA changera et passera du mode « out-of-sync » à « in-sync » (avec la commande : `get system ha status`)

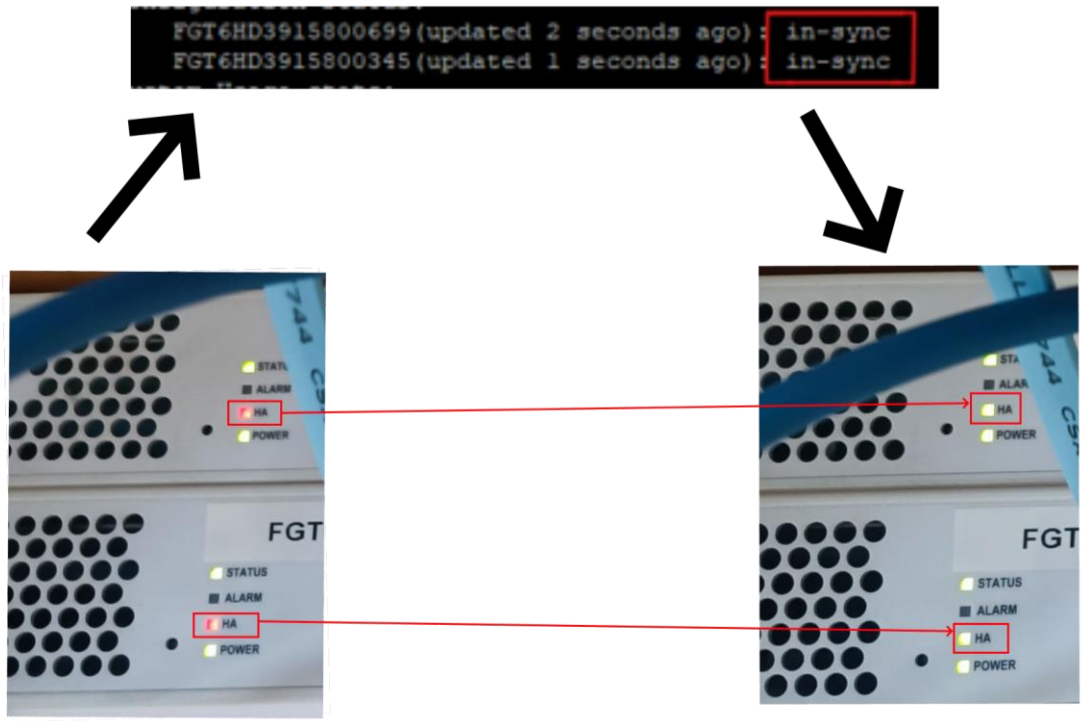


Figure 9 : Représentation de la synchronisation du HA

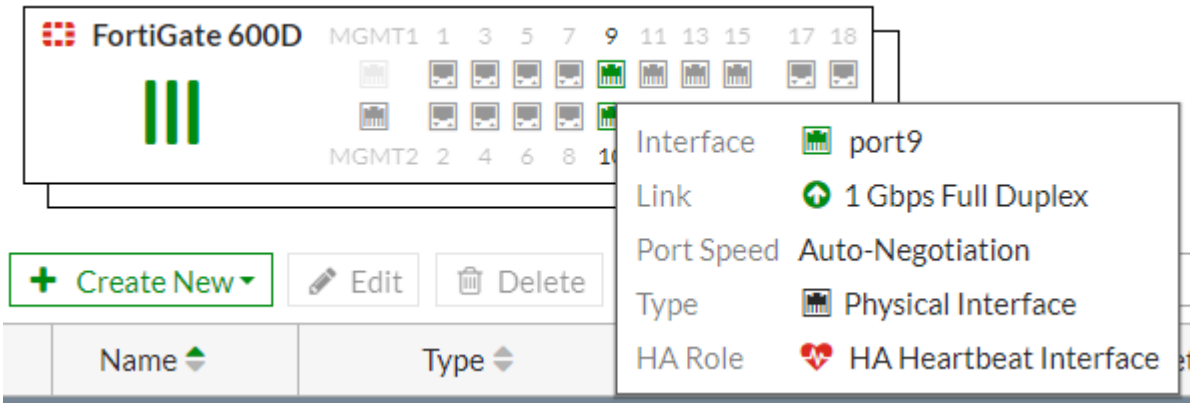


Figure 10 : Capture d'écran de l'interface Heartbeat HA

Dans la suite de mes travaux, j'ai eu à faire en sorte que les deux firewalls soient accessibles par GUI avec une adresse IP individuelle.

En effet, lorsqu'un HA est effectué, le firewall secondaire n'est pas accessible, l'adresse **192.168.1.99** étant associée au cluster.

Pour simplifier la configuration et gérer chaque firewall, il est fortement conseillé de leur configurer une adresse IP.

Sites	Nom	IP de Management dédié	Passerelle
FRMRS-FW-AD	FRMRS-FW-AD1	192.168.1.99	192.168.1.100
	FRMRS-FW-AD2	192.168.1.98	

Figure 11 : Tableau des adresses IP

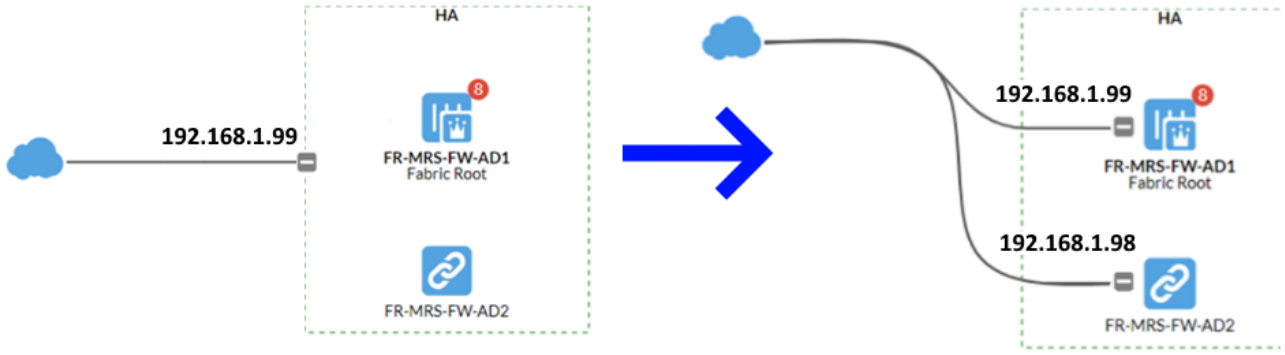


Figure 12 : Schéma du changement de topologie logique du HA

Il est maintenant possible de se connecter à l'interface Web de chaque firewall du cluster sans passer par le câble console ou par la commande : `execute ha mange <ID> admin`

Cette commande permet de se connecter au CLI de toute unité du cluster.

Cette étude a été très importante pour la suite de mon projet car elle m'a permis de découvrir certaines notions importantes, comme la nomenclature et surtout l'interface web du Fortigate.

2.2 Analyse et Création de règles

Après avoir configuré mon premier cluster, j'ai dû créer mes premières règles firewall pour comprendre comment cela fonctionnait.

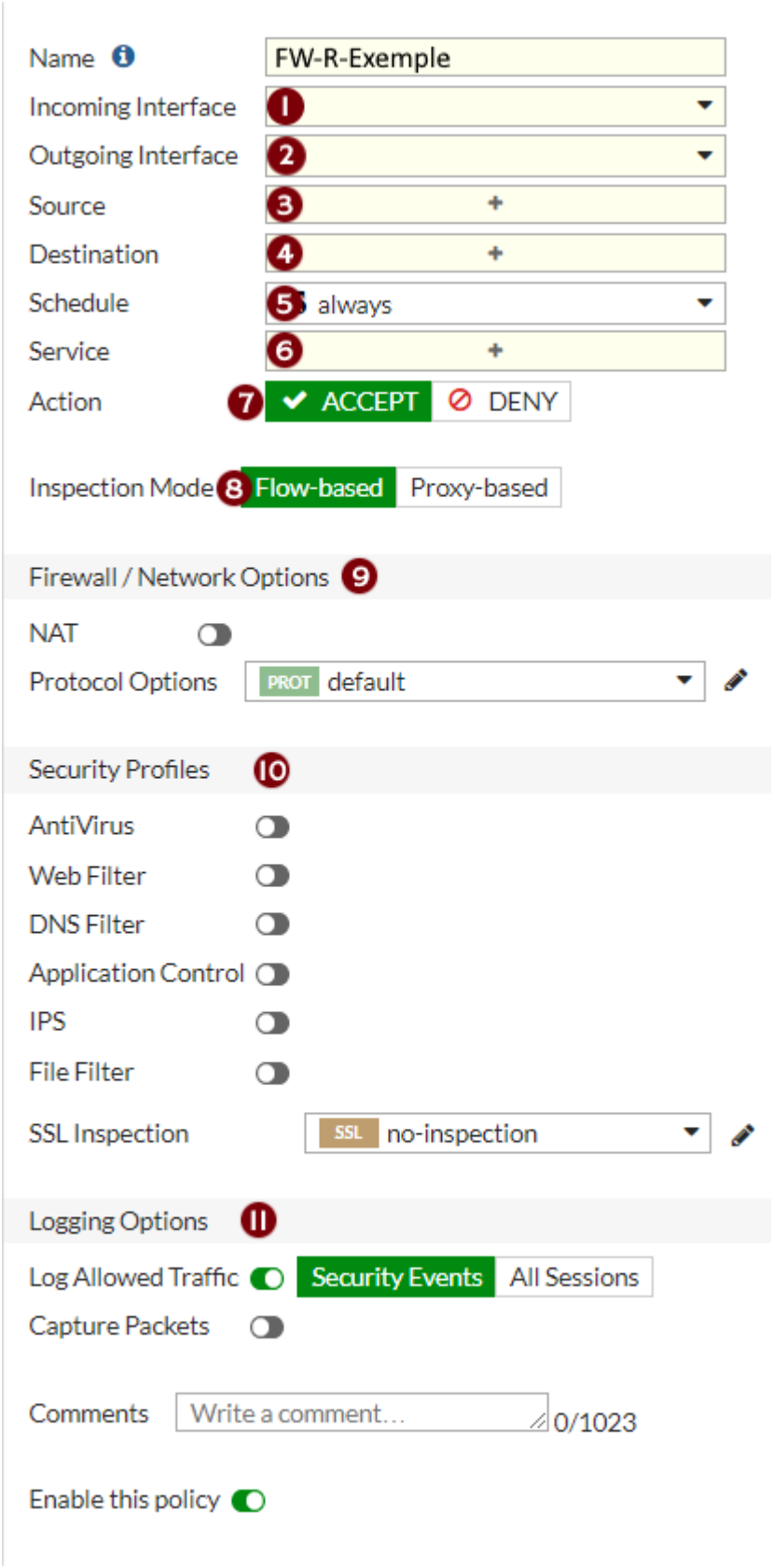
L'objectif de ces règles est de limiter au maximum les différents protocoles et connexions.

Les règles d'un firewall se lisent de haut en bas et finissent toujours par une règle implicite « **deny deny all** » qui interdira tout ce que l'on n'a pas autorisé.

Figure 13 : Capture d'écran de la règle implicite placé à la fin du Fortigate 600D

Comment créer une règle firewall ?

La première façon, la plus classique, nécessite une connexion par CLI ou par interface Web. J'ai utilisé l'interface Web, plus compréhensible et ergonomique.



1) Il s'agit de l'interface d'où le trafic provient.

2) C'est l'interface où le trafic est envoyé.

3) La source du trafic est un objet (adresse IP, plage d'adresse IP, objet du type **FQDN***) ou un groupe regroupant les différents types d'objet.

4) Il s'agit également d'un objet ou d'un groupe où le trafic va s'acheminer.

5) Il est possible de programmer l'horaire où la règle est appliquée.

6) Les services regroupent les protocoles à autoriser.

7) L'action sera soit d'accepter (ACCEPT) le trafic, soit de l'interdire (DENY).

8) Établi par défaut sur les flux, le mode d'inspection permet d'affiner son contrôle sur les trafics basés sur le proxy.

9) Cette partie concerne la translation d'adresse et les redirections de ports.

10) Cette section touche à la sécurité. On peut activer des filtres (Antivirus, Web, **DNS***, Fichier, **IPS***), du contrôle Applicatif et faire de l'inspection **SSL***.

11) La dernière partie permet d'autoriser les logs et d'activer la règle.

Figure 14 : Description de l'interface GUI pour la création de règle

2.2.1 Avec Active Directory

L'utilisation des groupes ou des comptes (utilisateurs ou ordinateurs) de l'Active Directory est beaucoup plus intéressante car elle permet une meilleure granularité, au niveau des règles.
Au lieu de choisir un objet manuellement créé sur le firewall, il faut choisir une personne ou un groupe d'utilisateur de l'AD.

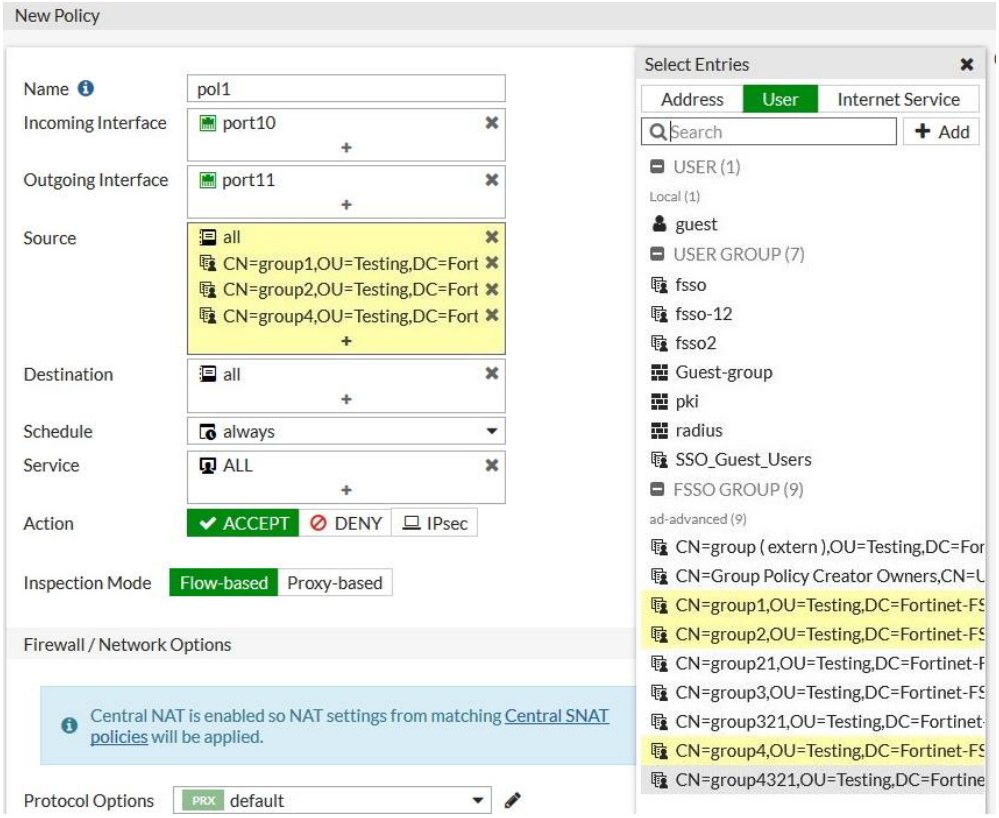


Figure 15 : Exemple de l'interface GUI pour la création de règle avec AD

Il n'est pas forcément judicieux de connecter la majorité des équipements avec l'Active Directory (**SSO***), car si une personne malveillante pénètre la sécurité de celle-ci, elle pourra accéder à tous les équipements et applications connectés.

C'est pourquoi il est important de mettre en place des solutions de type MFA.
À chaque connexion, l'utilisateur doit insérer un code provenant de l'application d'authentification installée sur son smartphone (équivalente à une **clé OTP***).
Ce code se renouvèle toutes les 60 secondes.

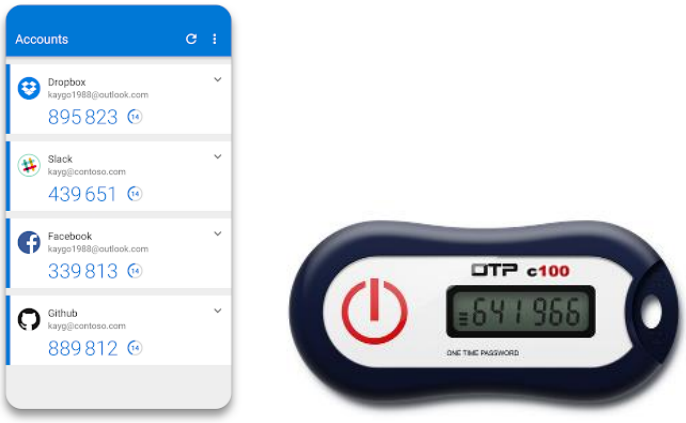


Figure 16 : Microsoft Authenticator et clé OTP

Après cette étude, j'ai finalement choisi la méthode avec Active directory.
Malgré ses failles, elle bénéficie d'une meilleure granularité, à condition que l'administrateur se connecte sur le firewall par le MFA (hors SMS).

Par exemple, en connectant le firewall à l'Active Directory, il est possible de créer des règles par application.

Prenons une application comme WebVideo qui permet la diffusion de contenu sur les écrans :

- Le groupe **FW-WebVideo_Fortinet_VPN_Users** est créé dans l'Active Directory
- Une règle **FW-WebVideo_Fortinet_VPN_Users** est créé sur le firewall en utilisant le groupe ajouté ci-dessus

Il suffit d'ajouter une personne dans le groupe **FW-WebVideo_Fortinet_VPN_Users** qui aura ensuite accès à l'application WebVideo via le VPN.

Figure 17 : Exemple d'une règle créé sur le Firewall avec l'AD (modifié en raison de la confidentialité)

2.2.2 Analyse

Dans le cadre de la mise en place des nouvelles règles, j'ai dû analyser celles du précédent VPN.

Pour m'aider dans cette démarche, j'avais également accès à un outil très pratique : le « FortiAnalyzer ».
Celui-ci est connecté à tous les firewalls FortiGate. Il permet d'enregistrer tous les logs de connexion.

À la suite de cette analyse, j'ai préparé toutes les nouvelles règles dans un fichier Excel (voir Annexe 1), en utilisant la nouvelle nomenclature du groupe et les différents protocoles utilisés.

J'ai ensuite collaboré avec mes collègues allemands par Teams et par courriel afin de créer ensemble les règles sur le firewall et les groupes dans l'Active Directory.
Je leur ai transmis mon analyse Excel et après quelques corrections, les règles ont été créées.
Évidemment, tout n'était pas fonctionnel pour un déploiement complet. C'est la raison pour laquelle j'ai commencé à entreprendre une phase de tests.

2.3 Test et Résolution

Pour la phase de tests, j'ai réalisé une fiche de tests (voir Annexe 2) indiquant toutes les applications qui seront accessibles par le VPN.

Ensuite, je me suis connecté au FortiClient VPN, en simulant une connexion distante à l'aide d'un point d'accès Wi-Fi grâce au smartphone.

Puis, j'ai débuté une série de tests sur chaque application en notant les liens, fichiers, et commandes afin de vérifier le bon fonctionnement de chacune des règles.

Pour conclure, j'ai validé les applications qui fonctionnaient et celles qui présentaient des erreurs sur la fiche de test. Cela permet de garder un fil conducteur et également d'investiguer plus facilement les problèmes.

2.4 Déploiement du client VPN

2.4.1 Déploiement par installation manuelle (Bêta-Testeur)

Avant de déployer le VPN sur les 3 sites d'Haribo, j'ai contacté différents collaborateurs des sites d'Uzès et de la TLM.

Pour leur installer le nouveau client VPN, j'ai conversé avec eux afin de convenir d'une date de mise en œuvre. Lorsque la date était fixée, j'ai réalisé une enquête auprès de ces utilisateurs.
Je leur ai envoyé un formulaire à cocher avec les différents logiciels utilisés pour que je puisse ensuite les ajouter dans les groupes dédiés de l'Active Directory.

☒	Accès VPN à l'ERP
☒	Accès VPN au logiciel GMAO
☐	Accès VPN au NeoScreen (publication sur écran)
☐	Accès VPN au logiciel Lims
☐	Accès VPN au site web de qualité alimentaire
☐	Accès VPN au serveur de fichiers de Marseille
☐	Accès VPN au serveur de fichiers d'Uzès
☐	Accès VPN au serveur GED
☐	Accès VPN au logiciel de compatibilité
☒	Accès VPN au logiciel de production (Marseille)
☒	Accès VPN au logiciel de production (Uzès)
☐	Accès VPN au logiciel BI
☐	Accès VPN au logiciel comptabilité 2
☐	Accès VPN au logiciel de production 2
☐	Accès VPN au logiciel de finance
☐	Accès VPN au logiciel RH
☐	Accès VPN au site de sécurité
☐	Accès VPN au contrôle d'accès

Figure 16 : Formulaire de vérification d'accès (modifié en raison de la confidentialité)

Afin d'expliquer parfaitement le fonctionnement du nouveau VPN aux utilisateurs et surtout la nouvelle politique de MFA, j'ai préparé une documentation/tuto (voir Annexe 3) qui décrit étape par étape la méthode d'installation du logiciel.

Cette documentation est divisée en deux parties : l'une pour les utilisateurs et la seconde pour mes collègues du service informatique. Cela permettra de faciliter le déploiement du VPN lorsque j'aurai terminé mon stage.

L'étape des tests avec les utilisateurs s'est révélée très importante car grâce à elle, j'ai pu observer un problème lié au MFA. En effet, le FortiClient VPN ne demandait plus de code aux utilisateurs et j'ai fait remonter cette faille cruciale à mon collègue en Allemagne.

2.4.2 Déploiement Industriel (Par GPO)

Mon stage arrivant bientôt à sa fin je ne pourrai malheureusement pas assister au déploiement du nouveau client VPN, sur tous les ordinateurs des utilisateurs. Néanmoins, j'ai eu à réfléchir sur une solution de déploiement en masse.

Ma réflexion m'a conduit à un déploiement par GPO, une solution pratique et qui évite de se compliquer la tâche. L'autre solution, le logiciel **SCCM*** de Microsoft, est un très bon logiciel de déploiement, connecté à l'Active Directory.
SCCM pourra être utilisé par la France une fois qu'ils auront migré leur infrastructure dans le Groupe.

La création d'une GPO de déploiement de logiciel .msi se fait en plusieurs étapes :

- Création d'un répertoire partagé pour y stocker notre logiciel (FortiClient VPN)
- Création d'un groupe **FortiClientVPN_User** ayant comme droit de modifier le contenu du dossier partagé de notre application
- Dans la Gestion des stratégies de groupes de l'AD, Clic droit sur Configuration ordinateur>Stratégies>Paramètres du logiciel>Installation de logiciel
- Nouveau package puis on indique le dossier partagé qui contient notre exécutable msi
- Cocher « Attribué » et valider la règle
- Modifier la zone pour que la règle ne s'applique que pour le groupe **FortiClientVPN_User**
- Il faut ensuite redémarrer l'ordinateur, après effectué sur PowerShell la commande :

```
PS C:\Windows\system32>Gpupdate /force
```

3 Travail Annexe

En dehors de mon projet principal, j'ai réalisé de nombreuses missions annexes.

3.1 Support Utilisateur

Au cours de mon stage j'ai pu de multiples fois intervenir auprès des utilisateurs pour différentes demandes.

- Tout d'abord en sécurité, avec par exemple la création de règles pour autoriser une personne à se connecter à des applications ou l'ajout d'adresses MAC dans la liste blanche des serveurs DHCP pour autoriser une personne à se connecter au réseau Wi-Fi.

- D'autre part, j'ai effectué des analyses de protocoles pour optimiser certaines règles sur les firewalls qui étaient trop permissives.

- La mise en place de matériel informatique a fait partie de l'une de mes missions, notamment par la préparation des ordinateurs par le logiciel **MDT***.

- Enfin, j'ai pu expérimenter la préparation et l'enrôlement d'IPhone et d'IPad via l'application **MDM*** (Mobile Device Management) de MobileIron.

3.2 Campagne de sensibilisation

J'ai eu la chance de réaliser deux campagnes de sensibilisation sur la sécurité informatique, auprès des utilisateurs.
Sachant que la plupart des attaques proviennent de l'intérieur (80 %), il est très important de sensibiliser et de former les personnes à une utilisation sécurisée.
Ces bonnes pratiques peuvent également leur servir dans leur vie personnelle.

J'ai donc téléchargé plusieurs vidéos courtes et simples à comprendre pour les utilisateurs.
Le site gouvernementale ***Cybermalveillance.gouv.fr*** est une mine d'or.

Ensuite, j'ai réalisé plusieurs flyers digitaux résumant les points importants de la sécurité informatique sur le phishing, les mots de passe et les clé USB.
Ils ont été envoyés à intervalle réguliers en tant que **Newsletter*** (voir Annexe 4) avec la possibilité de cliquer sur les flyers pour voir les vidéos.

De plus, les flyers et les vidéos ont été diffusés en complément sur les écrans Néoscreen (Accueil, salle de restauration, usines) des différents sites de l'entreprise.

4 Conclusion

Au cours de mon stage chez Haribo Ricqlès-Zan, j'ai pu expérimenter la vie en entreprise, réaliser un projet concret et endosser des responsabilités.

J'ai apprécié de travailler en équipe et de découvrir toutes les activités et les métiers de l'entreprise.

Je suis très fier d'avoir réalisé ce projet et d'avoir ainsi pu acquérir des compétences indispensables pour mon avenir professionnel.
J'ai développé des qualités essentielles dans le domaine de l'informatique, comme la proactivité et l'autonomie. Mais surtout, j'ai réalisé l'importance de mener une veille technologique.

Quand on observe ces 2 dernières années on remarque qu'avec la crise sanitaire, l'informatique et le numérique ont fait un bon technologique de 10 ans. Il faut donc continuellement s'informer tout au long de sa carrière notamment dans le secteur de la cybersécurité.

L'entreprise Haribo m'a proposé un poste d'alternant pour 3 ans, dans le cadre de mon diplôme d'ingénieur Systèmes et réseaux à l'école des Mines d'Alès. J'aurai donc l'opportunité de contribuer, dès septembre, au déploiement du nouveau logiciel VPN.

En outre, j'ai participé à plusieurs réunions sur des solutions de sécurités informatiques telles que CryptoSpike et sur les projets planifiés en septembre, sur lesquels je devrai intervenir lors de mon alternance.

Ce stage a été une réussite. Il m'a permis de confirmer ma volonté de me diriger dans le domaine de la Cybersécurité.

5 Remerciements

Tout d'abord, je tiens à remercier **Eric MAZZOLI** qui a transmis ma candidature de stage à cette merveilleuse équipe informatique.

Je souhaite ensuite adresser mes remerciements à ma tutrice de stage **Laurence TELLO**, Manager Informatiques Systèmes & Réseaux pour m'avoir accepté en stage, pour sa disponibilité et le partage de son expertise. Elle a su me familiariser avec les enjeux de ma mission et de mon sujet de stage, de manière intéressante et pédagogique.

Mes remerciements vont également à toute l'équipe informatique pour l'accueil et la bienveillance que ses membres m'ont réservé, et surtout pour toutes les connaissances qu'ils m'ont transmises.

Enfin, je remercie **Serge MILITELLO** et **Frédérique HENRY**, responsables Système d'Information, ainsi que **Timothée GLORIEUX,** Directeur Administratif et financier, Membre du Directoire, de me faire confiance dans le cadre de mon futur contrat d'alternant de 3 ans.

6 Glossaire

DUT, Diplôme Universitaire de Technologie

IUT, Institut Universitaire de Technologie

VPN, Virtual Private Network, est un type de réseau informatique qui permet la création de liens directs entre des ordinateurs distants.

Ransomware : c'est un type de malware qui empêche les utilisateurs d'accéder à leur système ou à leurs fichiers personnels et exige le paiement d'une rançon en échange du rétablissement de l'accès.

Firewall ou pare-feu, est un outil qui permet d'assurer la sécurité du réseau, il se présente comme une barrière de sécurité empêchant certains trafics d'entrer ou sortir d'un réseau.

TLM, Tour La Marseillaise

AD, Active Directory, est un annuaire chargé de répertorier tout ce qui touche au réseau (comptes des utilisateurs, comptes des ordinateurs et des serveurs, les imprimantes…), les administrateurs de celui-ci, contrôle l'accès et utilisation des ressources.

GPO, Group Policy Object, une stratégie de groupe est un ensemble d'outils intégrés à Windows Server qui permet au service informatique de centraliser la gestion de l'environnement utilisateur et la configuration des machines grâce à l'application de politiques.

MFA, Multi Factor Authentification, consiste à demander un second facteur d'authentification et donc à prouver la propriété légitime grâce à quelque chose que l'on possède (SMS, application d'authentification, clé OTP…)

HA, Hight Availability**,** est la capacité d'un système à fonctionner en continu sans défaillance pendant une période donnée.

CLI, Command Line Interface, designee n français l'interface de ligne de commande.

GUI, Graphical User Interface, désigne en français l'interface graphique.

FQDN, Fully Qualified Domain Name, désigne l'adresse complète et unique d'un site Internet.

SSO, Single Sign-On, est une technologie d'authentification unique permettant de se connecter avec un seul identifiant à de multiples applications

Clé OTP : c'est un outil d'authentification forte qui permet l'accès aux applications de gestion.

DNS, Domain Name System, est un service informatique distribué utilisé qui traduit les noms de domaine Internet en adresse IP ou autres enregistrements.

IPS, Intrusion Prevention Systems, est une forme de sécurité de réseau qui sert à détecter et prévenir les menaces identifiées.

SSL, Secure Socket Layer, est un protocole de sécurité qui permet de sécuriser les échanges d'informations entre des appareils reliés à un réseau interne ou à Internet.

SCCM, System Center Configuration Manager, est un logiciel de gestion de systèmes édité par Microsoft. Il est destiné à gérer de grands parcs d'ordinateurs sur systèmes Windows.

MDT, Microsoft Deployment Toolkit, est une solution de déploiement créé par Microsoft.

MDM, Mobile device management, est une application permettant la gestion d'un parc d'appareils mobiles (smartphone, tablette).

Newsletter : c'est une lettre d'information envoyée régulièrement par e-mail à une liste de diffusion, c'est-à-dire à des abonnés

7 Bibliographie

Empson, S. (April 17, 2005). *CCNA Command Quick Reference (Cisco Networking Academy Program) .*

Haribo, (https://fr.wikipedia.org/wiki/Haribo)

Fortigate 600D, (http://fortinet.globalgate.com.ar/pdfs/FortiGate/FortiGate-600D.pdf)

Fortigate Active Directory, (https://docs.fortinet.com/document/fortigate/6.4.5/administration-guide/795593/use-active-directory-objects-directly-in-policies)

Institut Universitaire de Technologie,
Aix-Marseille Université

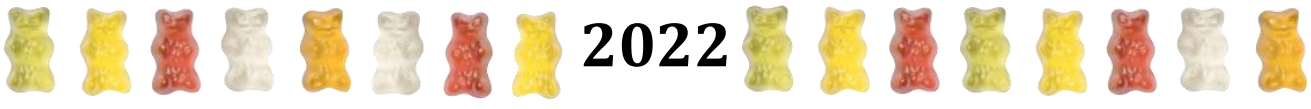
ANNEXES
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Sécurisation et déploiement du nouveau logiciel de VPN

Adam BERENGUER
HARIBO RICQLÈS-ZAN

Responsable entreprise : Laurence TELLO

Responsable académique : Anouch HOVSEPIAN



Annexe 1 :

Nr.	Source	ource-zor	destination	ination-descri	stination-zc	protocol (TCP)	protocol (UDP)
1	FW-ERP_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.1	confidentiel	LAN	8470-8476, 500, 400, 449, 445(SMB), HTTP(80), 23(Telnet)	
2	FW-GMAO_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.2	confidentiel	LAN	HTTPS,RDP	
3	FW-WebVideo_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.3	confidentiel	LAN	HTTPS	
4	FW-Lims_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.4	confidentiel	LAN	HTTPS	
5	FW-QA_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.5	confidentiel	LAN	8080(HTTP-Proxy)	
6	FW-OCS_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.6	confidentiel	LAN	HTTPS	
7	FW-AC_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.7	confidentiel	LAN	3389(RDP)	
9	FW-Compta_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.8	confidentiel	LAN	HTTPS, SMB, RDP	
10	FW-EDI_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.9	confidentiel	LAN	HTTPS	
11	FW-GED_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.10 172.16.100.11	confidentiel confidentiel	LAN	SMB,HTTPS	
12	FW-Plan_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.12 172.16.100.13	confidentiel confidentiel	LAN	HTTPS, RDP	
13	FW-Files_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.14	confidentiel	LAN	SMB	
14	FW-Prod_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.15	confidentiel	LAN	SMB, 111(rpcbind), 2638(SybaseAnywhere)	)S-NS), 2638(Sybase.
15	FW-BI_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.16	confidentiel	LAN	SMB, HTTPS, 9300, 5495, 5498, 19300, 19306	
16	FW-Finance_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.17	confidentiel	LAN	HTTPS, 8480(Talentia.s), 8380(Talentia.s), SMB	
17	FW-Compta2_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.18	confidentiel	LAN	6083, RDP	
18	FW-Prod2_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.19	confidentiel	LAN	RDP	
19	FW-RH_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.20	confidentiel	LAN	HTTPS, RDP, 9704(HRI_Talentia)	
20	FW-Secu_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.21	confidentiel	LAN	HTTPS	
21	FW-CA_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.22	confidentiel	LAN	HTTP, 49762, 135(DCE-RPC)	135(DCE-RPC)
22	FW-Backup_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.23	confidentiel	LAN	8400-8600,49152-6535, 8400-8403	

Annexe 2 :

Nr.	Source	ource-zor	destination	ination-descri	stination-zc	protocol (TCP)	protocol (UDP)	Description	Work?		
1	FW-ERP_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.1	confidentiel	LAN	8470-8476, 500, 400, 449, 445(SMB), HTTP(80), 23(Telnet)		ERP	✓		telnet 172.16.100.1 23
2	FW-GMAO_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.2	confidentiel	LAN	HTTPS,RDP		GMAO	✓		https://172.16.100.2
3	FW-WebVideo_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.3	confidentiel	LAN	HTTPS		WebVideo	✗		
4	FW-Lims_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.4	confidentiel	LAN	HTTPS		Lims	✓		https://172.16.100.4
5	FW-QA_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.5	confidentiel	LAN	8080(HTTP-Proxy)		Qualité Alimentaire	✓		http://172.16.100.5
6	FW-OCS_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.6	confidentiel	LAN	HTTPS		OCS	✓		https://172.16.100.6
7	FW-AC_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.7	confidentiel	LAN	3389(RDP)		Contrôle d'Accès	✗		https://172.16.100.7
9	FW-Compta_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.8	confidentiel	LAN	HTTPS, SMB, RDP		Comptabilité	✓		
10	FW-EDI_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.9	confidentiel	LAN	HTTPS		EDI	✓		https://172.16.100.9
11	FW-GED_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.10 172.16.100.11	confidentiel confidentiel	LAN	SMB,HTTPS		GED	✓		https://172.16.100.10 NO IPS
12	FW-Plan_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.12 172.16.100.13	confidentiel confidentiel	LAN	HTTPS, RDP		Planification	✗		https://172.16.100.12 https://172.16.100.13
13	FW-Files_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.14	confidentiel	LAN	SMB		Serveur de fichier	✓		Test des repertoires distants //Production/Prod
14	FW-Prod_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.15	confidentiel	LAN	SMB, 111(rpcbind), 2638(SybaseAnywhere)	)S-NS), 2638(Sybase	Production	✗		
15	FW-BI_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.16	confidentiel	LAN	SMB, HTTPS, 9300, 5495, 5498, 19300, 19306		BI	✗		
16	FW-Finance_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.17	confidentiel	LAN	HTTPS, 8480(Talentia.s), 8380(Talentia.s), SMB		Finance	✓		https://172.16.100.17
17	FW-Compta2_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.18	confidentiel	LAN	6083, RDP		Comptabilité	✗		
18	FW-Prod2_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.19	confidentiel	LAN	RDP		Production	✗		
19	FW-RH_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.20	confidentiel	LAN	HTTPS, RDP, 9704(HRI_Talentia)		RH	✗		
20	FW-Secu_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.21	confidentiel	LAN	HTTPS		Sécurité	✓		https://172.16.100.21
21	FW-CA_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.22	confidentiel	LAN	HTTP, 49762, 135(DCE-RPC)	135(DCE-RPC)	CA	✗		
22	FW-Backup_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.16.100.23	confidentiel	LAN	8400-8600,49152-6535, 8400-8403		Sauvegarde	✓		
	UZES								9 ✗ 12 ✓		
21	FWUZE-Prod_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.17.100.1	confidentiel	LAN	HTTP ,1433(MS-SQL), 4022(MS-SQL)	1434(MS-SQL)	Production Uzès	✗		
22			172.17.100.2	confidentiel					✗		
23			172.17.100.3	confidentiel					✗		
24			172.17.100.4	confidentiel					✗		
25			172.17.100.5	confidentiel					✗		
26			172.17.100.6	confidentiel					✗		
27	FWUZE-Files_Fortinet_VPN_Users + Subnet_VPN_User	WAN	172.17.100.7	confidentiel	LAN	SMB		Serveur de fichier Uzès	✓		Test des repertoires distants \\Uzes\General
28									6 ✗ 1 ✓		
29											

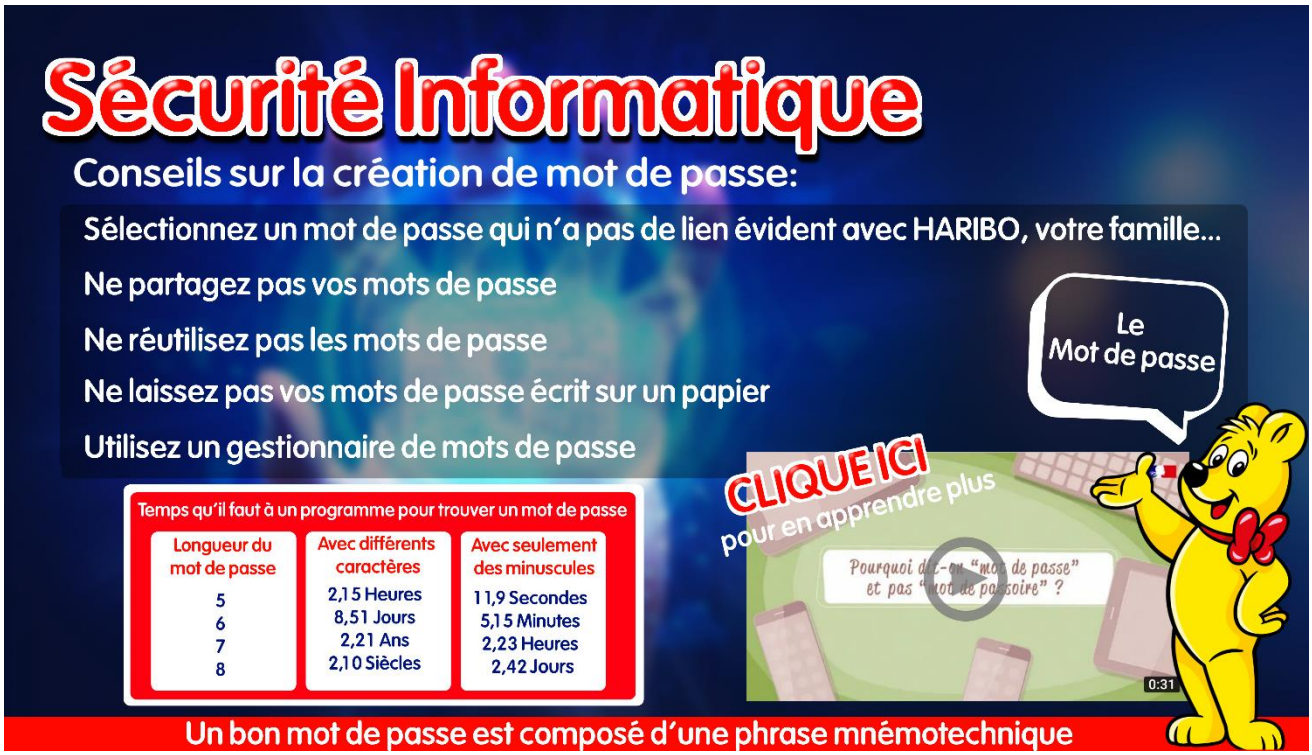
Annexe 3 :

FORTICLIENT_Annexe.pdf

Lien pour voir le PowerPoint : https://adamberenguer.fr/doc/FORTICLIENT_Annexe.pdf

Annexe 4 :

Lien de la vidéo Youtube en question : https://youtu.be/bSp6gSp5KT4



Lien de la vidéo Youtube en question : https://www.youtube.com/watch?v=kamD7Rw--Xw