Portail captif sur Fortigate :

Dans le cadre de cette mise en place, je vais travailler sur un environnement virtualisé ou deux machines virtuelles sont utilisées :

- **Un client Windows qui servira de poste client pour tester la connexion au portail captif**
- **Pare-feu Fortigate qui sera configuré pour gérer l'accès réseau et rediriger les utilisateurs vers la page d'authentification.**

  Cette architecture permet de simuler un réseau d'entreprise offrant un environnement réaliste pour tester et valider la configuration du portail captif avant un possible déploiement en production.

Dans un réseau informatique, e contrôle et la gestion des accès sont essentiels pour garantir la sécurité et la bonne utilisation des ressources. Un portail captif permet d'intercepter les connexions des utilisateurs et de les rediriger vers une page d'authentification avant qu'ils ne puissent accéder à Internet ou au réseau interne.

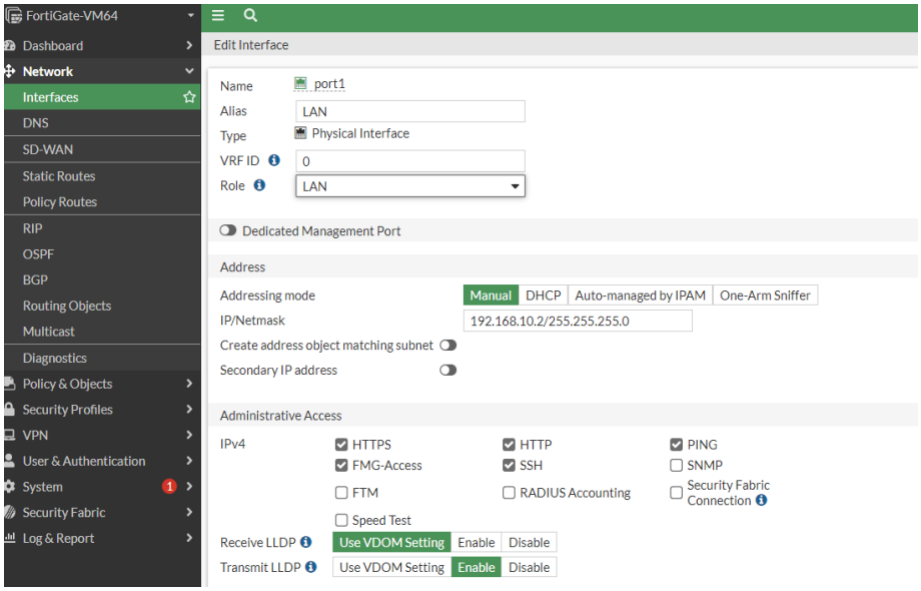
Je vais donc détailler étape par étape la configuration d'un portail captif sur un pare-feu Fortigate avec une page d'authentification modifiée en HTML pour une expérience utilisateur personnalisé.

Voici les objectifs que je souhaiterais atteindre dans cet exercice :

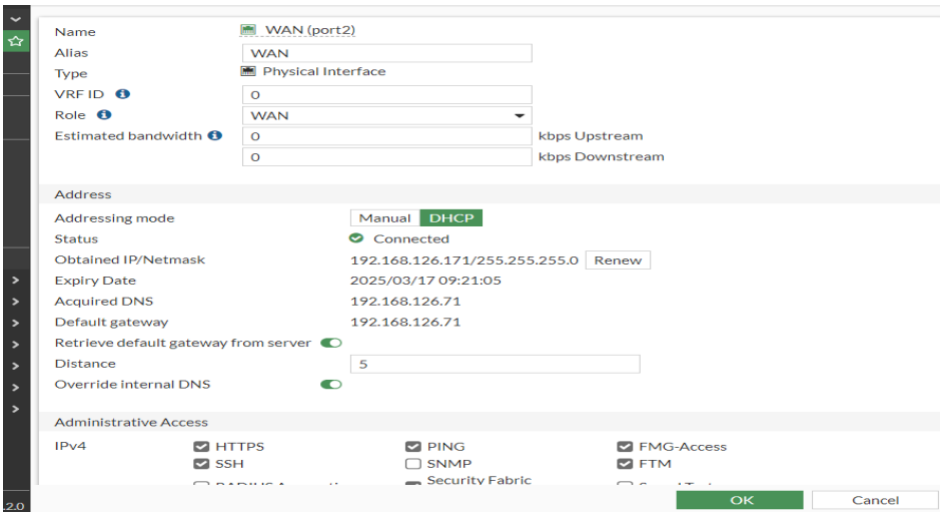
- **Comprendre le fonctionnement du portail captif sur Fortigate**
- **Configurer les interfaces réseaux et les règles d'accès**
- **Mettre en place un portail captif et personnaliser la page d'authentification en HTML**
- **Tester et valider la mise en place**

Un portail captif est une solution de contrôle d'accès permettant de rediriger les utilisateurs vers une page d'authentification avant qu'ils ne puissent accéder à Internet ou aux ressources du réseau. Il est couramment utilisé dans les environnements professionnels, les établissements scolaires=, les hôtels et les espaces publics pour sécuriser l'accès et appliquer des politiques d'utilisation. Dans ce guide, je vais détailler la mise en place d'un portail captif sur le pare-feu Fortigate, en configurant les interfaces réseau, les règles de sécurité et en personnalisant la page d'authentification pour offrir une expérience utilisateur adaptée aux besoins de l'organisation.

Voici la configuration de l'interface LAN :

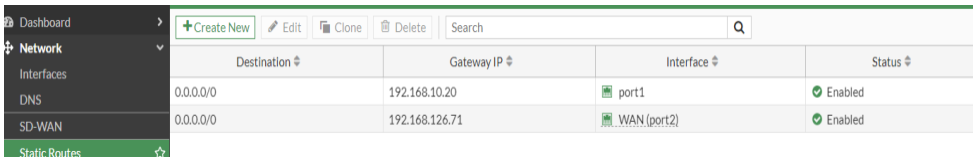


Voici la configuration de l'interface WAN :



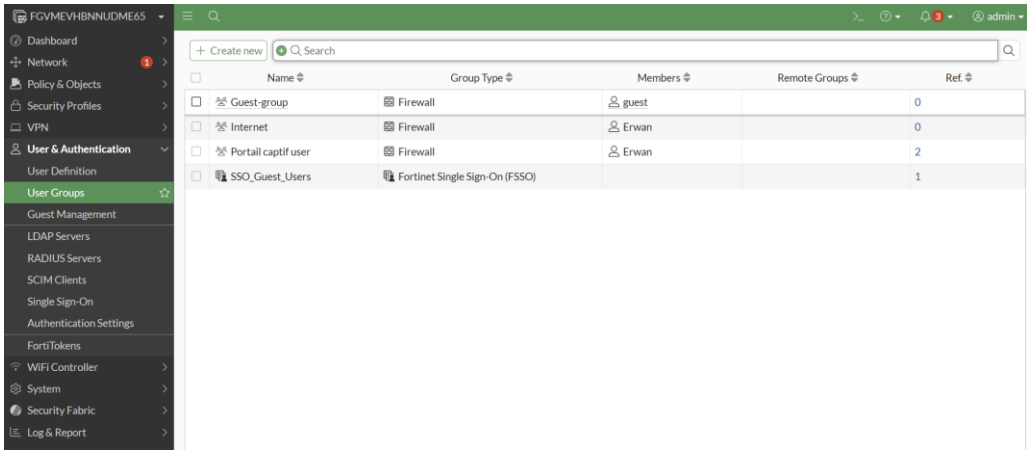
Voici les routes que j'ai créé :

- **La première route est définie vers la destination 0.0.0.0/0, ce qui signifie que c'est une route par défaut utiliser pour diriger tout traffic qui ne correspond à une aucune route spécifique. Elle utilise la passerelle à l'adresse IP 192.168.10.20 et passe par l'interface réseau LAN qui est le port 1.**
- **Pour la deuxième route, elle utilise également une route par défaut mais elle emprunte une interface différente sur l'adresse IP 192.168.126.71 et passe par l'interface réseau WAN qui est à l'occurrence le port 2.**

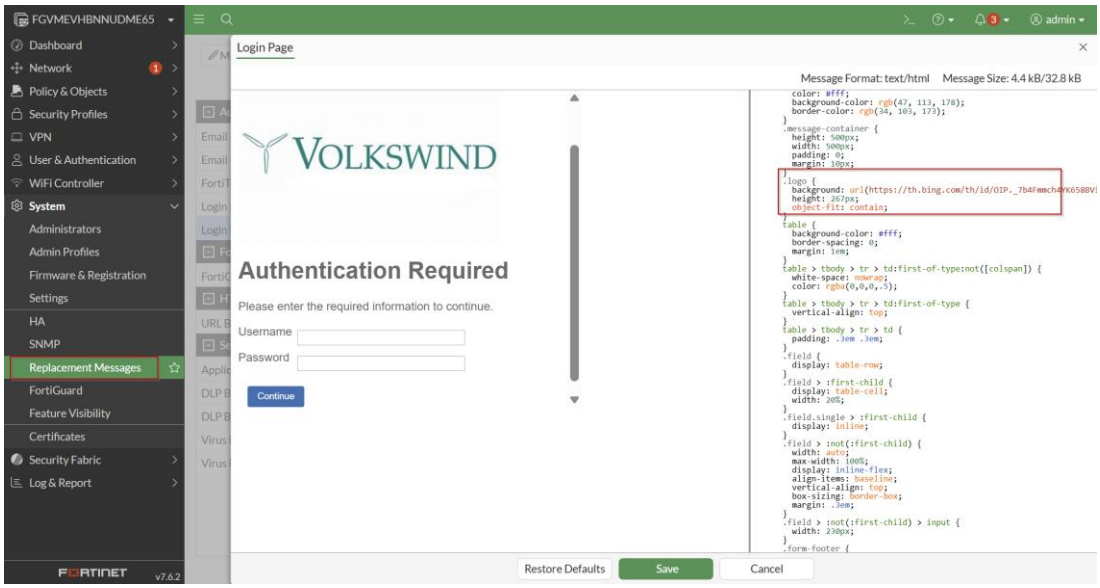


Ensuite, j'ai créé un utilisateur « Erwan » et je l'ai ajouter dans le groupe « Portail captif User » pour qu'il puisse accéder aux ressources interne.

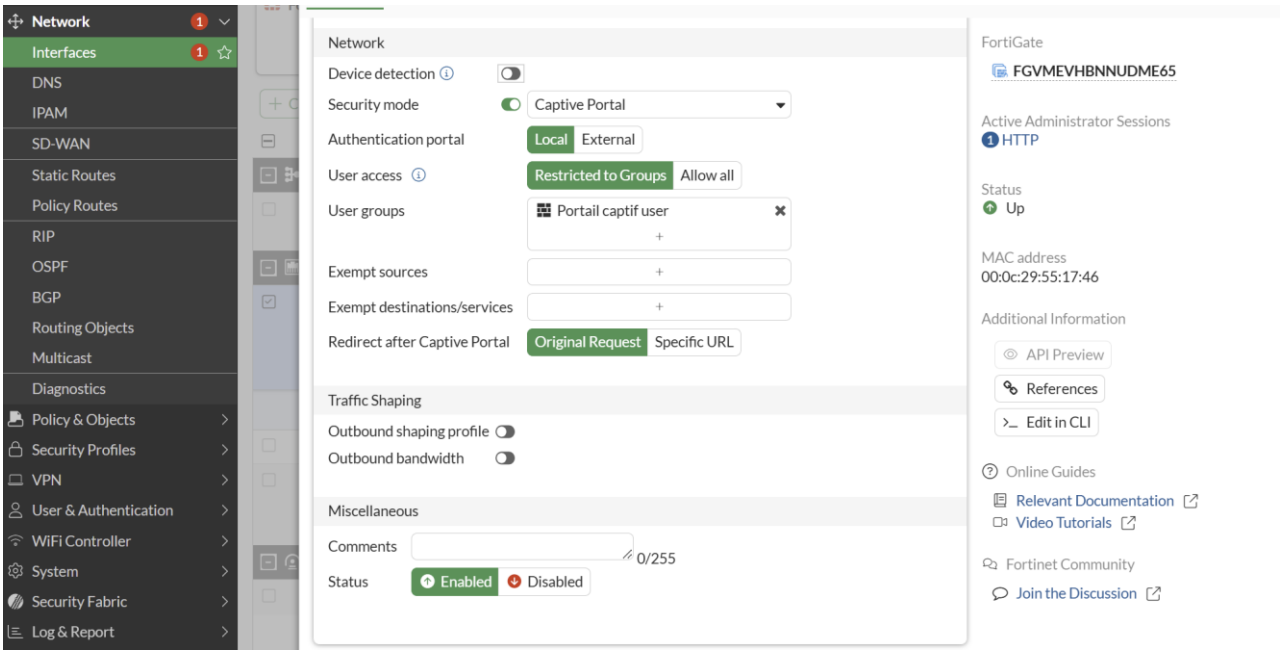
Cette configuration se fera dans le port 1 pour autoriser seulement le groupe à accéder aux ressources juste après.



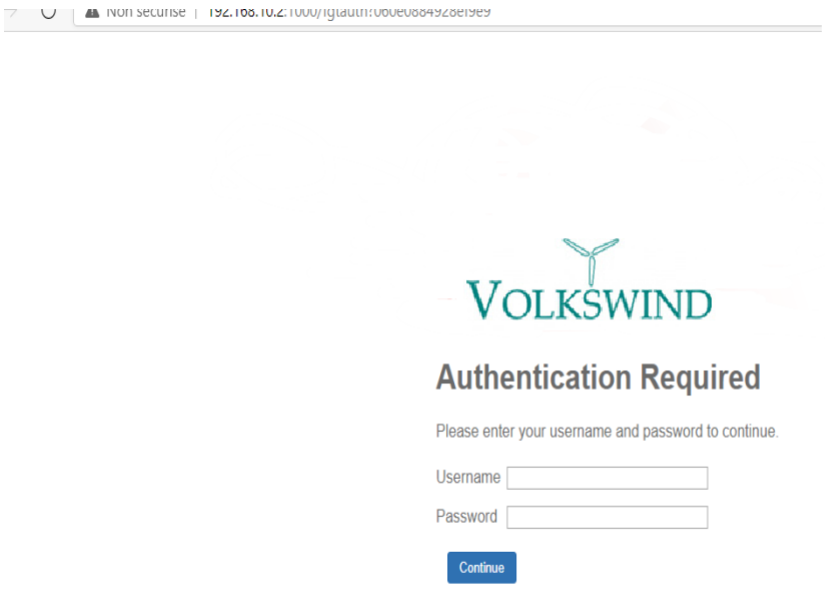
J'ai modifié la page HTML avec le logo de mon entreprise afin de personnaliser le portail captif. On peut le voir sur la section « logo » encadré dans le code HTML.



On procède à l'activation du portail captif sur l'interface réseau correspondant au port 1 de l'équipement Fortigate, afin d'obliger les utilisateurs du groupe « Portail captif user » à s'authentifier avant d'accéder aux ressources réseaux.



Voici le résultat depuis mon client Windows 10 :



Pour conclure, la mise en place d'un portail captif sur Fortigate permet de sécuriser et de contrôler l'accès à un réseau en imposant une authentification préalable aux utilisateurs. Grâce à cette configuration, il est possible de gérer les connexions, d'appliquer des politiques d'utilisation et de personnaliser l'expérience utilisateur avec une page de connexion adaptée. En utilisant un environnement virtualisé avec une

machine Windows et un pare-feu Fortigate, nous avons pu tester et valider l'ensemble des étapes nécessaires à son déploiement. Cette solution est idéale pour les entreprises, les établissements scolaires et les lieux publics souhaitent offrir un accès Internet tout en garantissant une meilleure gestion et sécurité réseau.