Document de présentation des Réalisations professionnelles

Documentation détaillant lesRéalisations

BTS Service Informatique aux Organisation

Option Solution D'infrastructure, système et Réseaux

Akaki
Miminoshvili

I. Présentation

A- OpenVPN

OpenVPN peut être utilisé pour créer des réseaux VPN à la fois pour les entreprises et les particuliers. Il permet aux utilisateurs d'accéder à distance à des ressources réseau telles que des fichiers, des applications et des imprimantes, tout en garantissant la sécurité des données.

OpenVPN est un logiciel open-source qui permet de créer des connexions VPN (Virtual Private Network) sécurisées entre deux ou plusieurs ordinateurs via Internet. Il s'agit d'un protocole de VPN largement utilisé pour ses fonctionnalités de sécurité avancées et sa facilité d'utilisation.

OpenVPN utilise des certificats et des clés pour authentifier les utilisateurs et chiffre les données qui transitent sur le réseau VPN. Il prend en charge différents protocoles de chiffrement, tels que AES, Blowfish et DES, pour garantir une sécurité maximale. Il prend également en charge les protocoles de tunneling SSL/TLS et UDP pour une flexibilité et une compatibilité accrue avec les systèmes d'exploitation et les appareils réseau.

B- Veeam Backup

Veeam Backup est une solution de sauvegarde et de récupération de données pour les environnements virtuels et physiques. Elle est principalement utilisée par les entreprises pour protéger leurs données et garantir la continuité de leur activité en cas de perte de données ou d'interruption de service. Veeam Backup offre des fonctionnalités de sauvegarde et de récupération complètes pour les environnements VMware vSphere et Microsoft Hyper-V.

Veeam Backup offre également des fonctionnalités de restauration granulaire pour les machines virtuelles, les fichiers, les e-mails et les applications, ainsi que des fonctionnalités de réplication de données pour une protection contre les pannes et les catastrophes. Elle prend en charge la déduplication et la compression des données pour une utilisation efficace de l'espace de stockage.

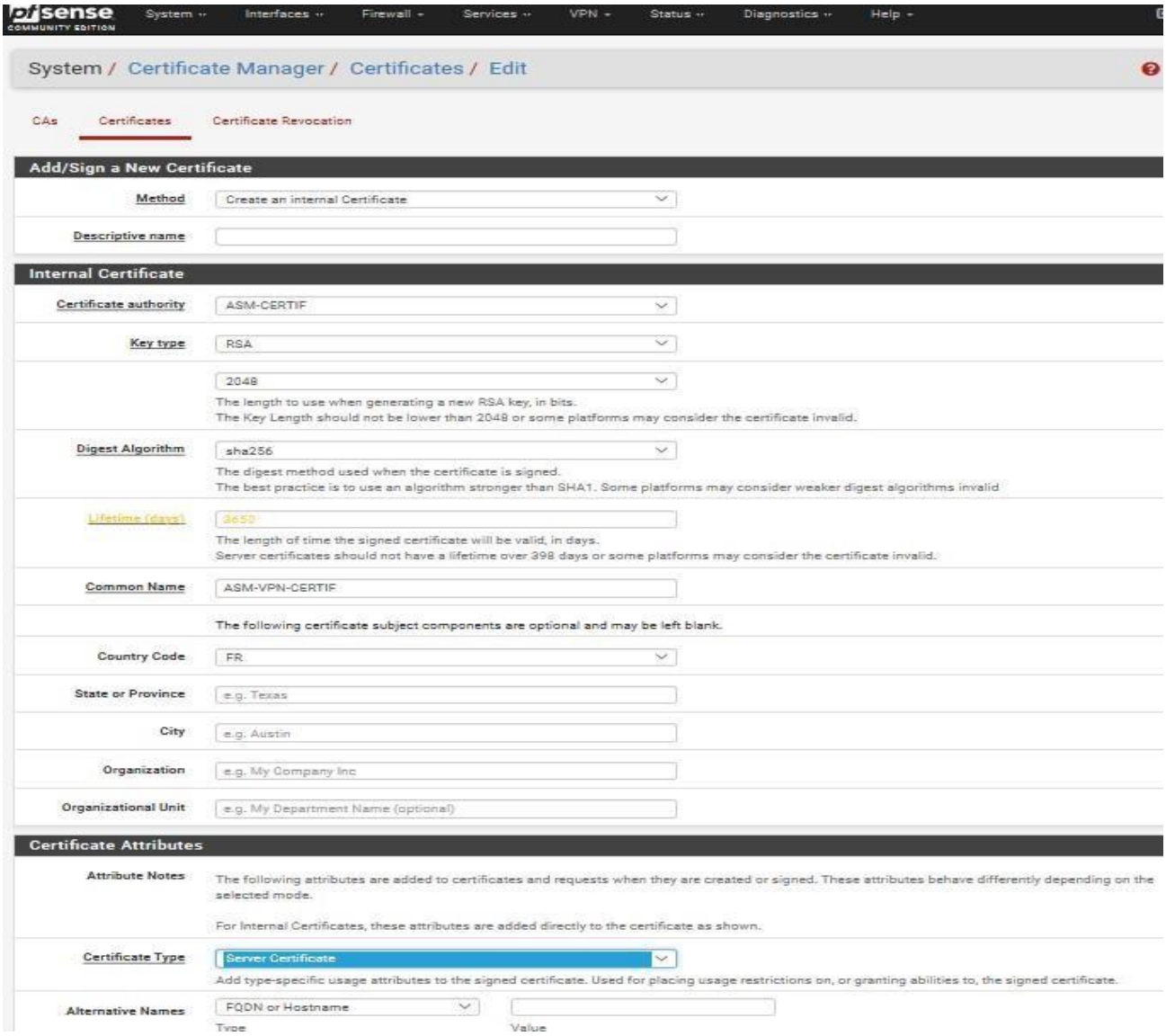
II. Procédure de configuration des équipements

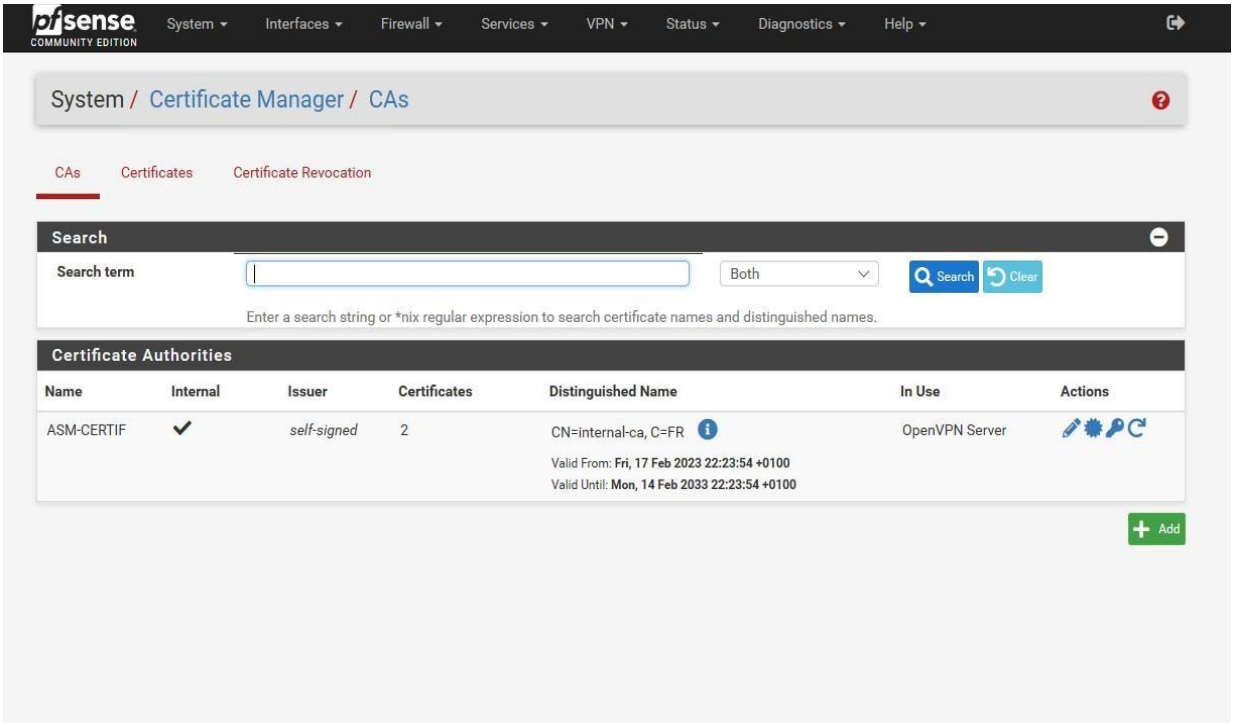
A- OpenVPN

Prérequis :

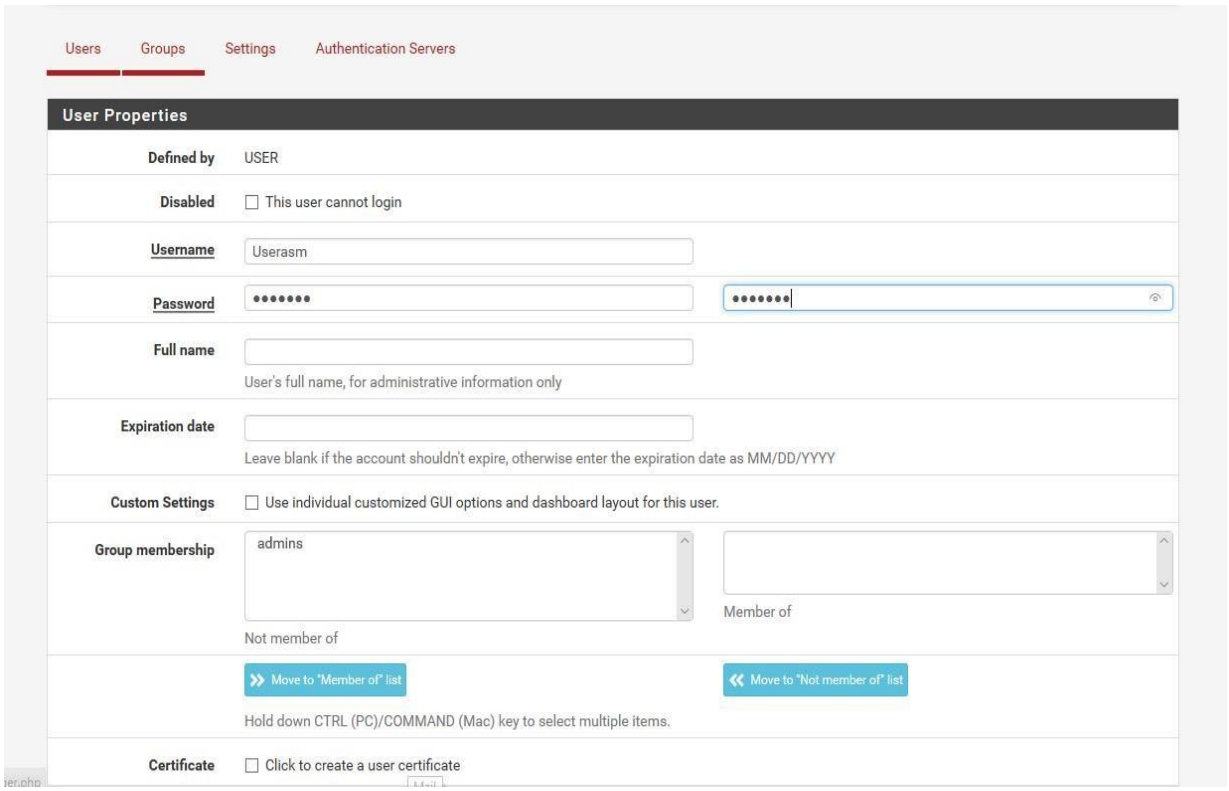
- Un pare-Feu Netgate sg-3100
- Un accès Internet Procédure *d'installation :*

1-Création des certificats d'autorités et de serveur.

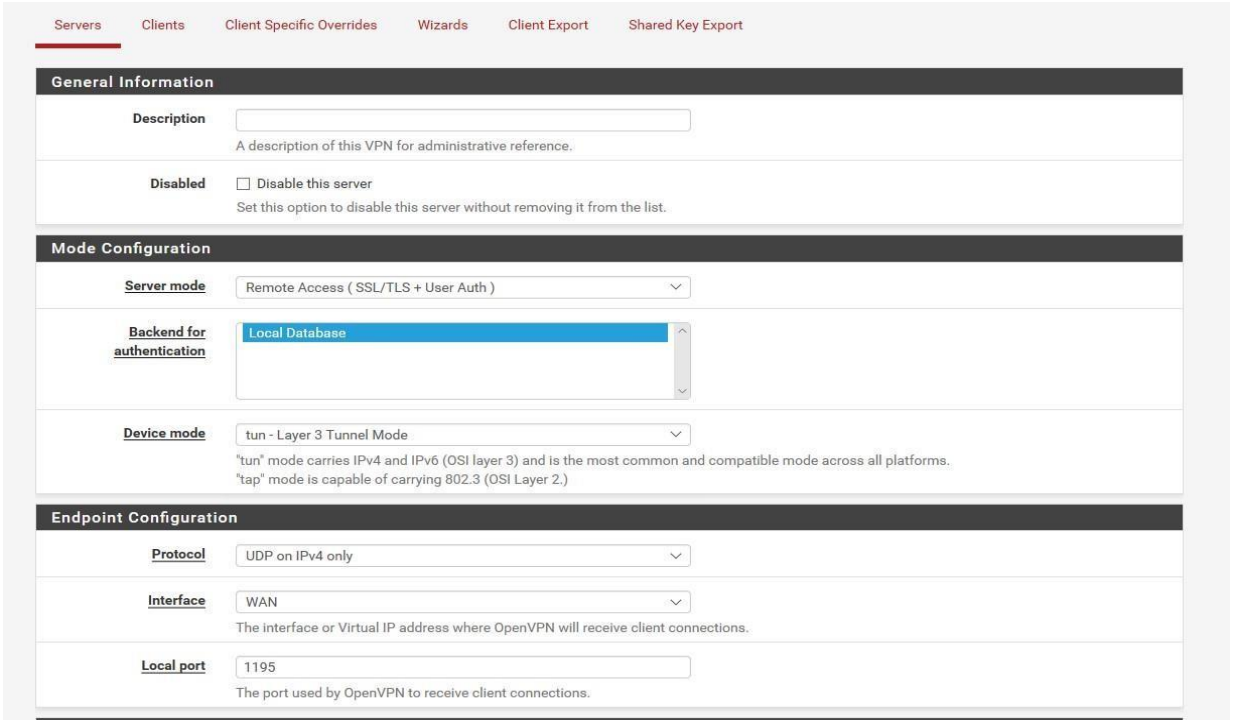


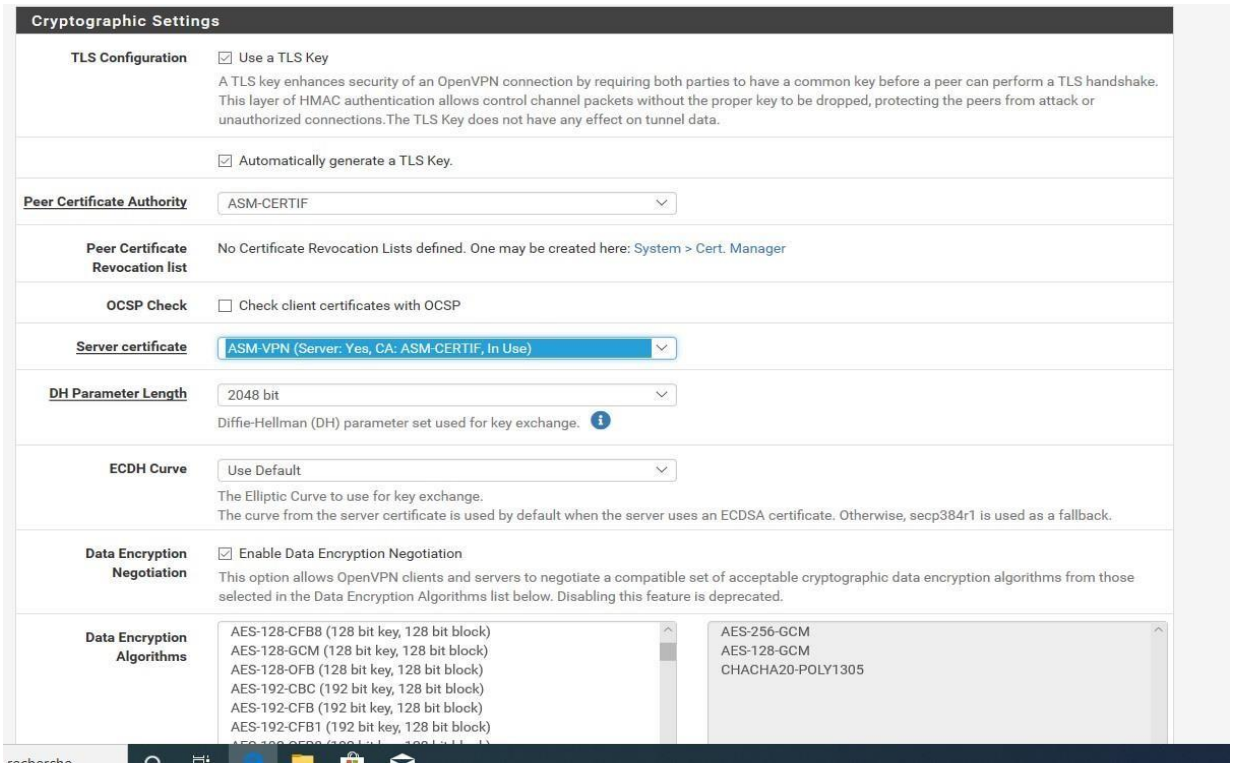


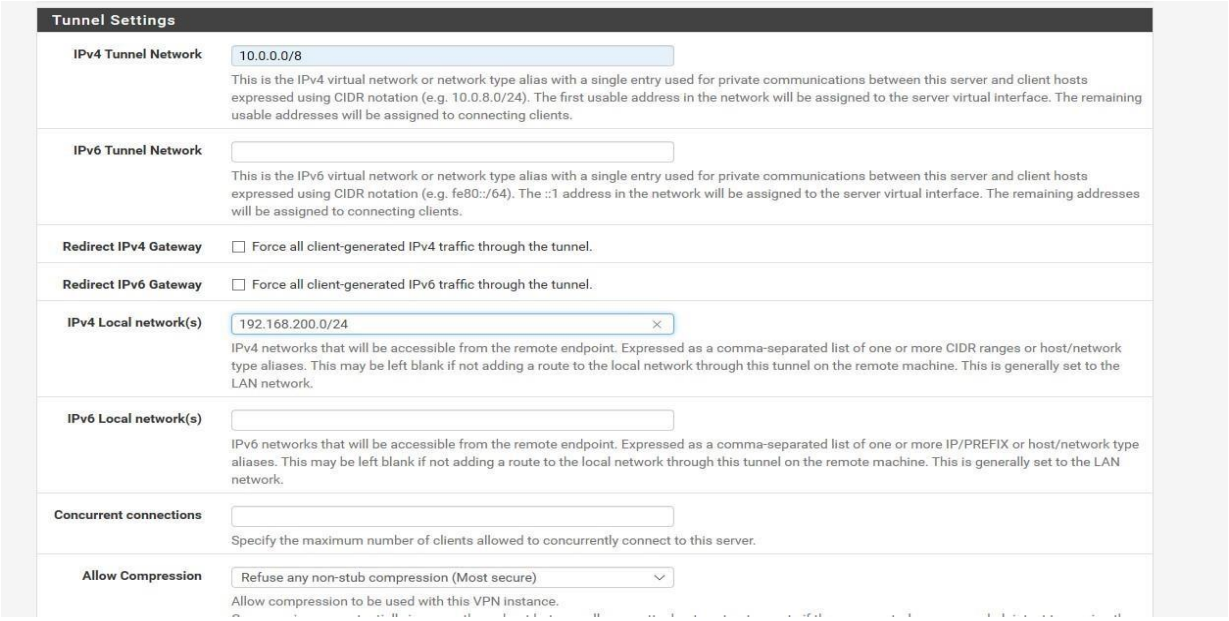
2-Création d'un utilisateur avec son certificat

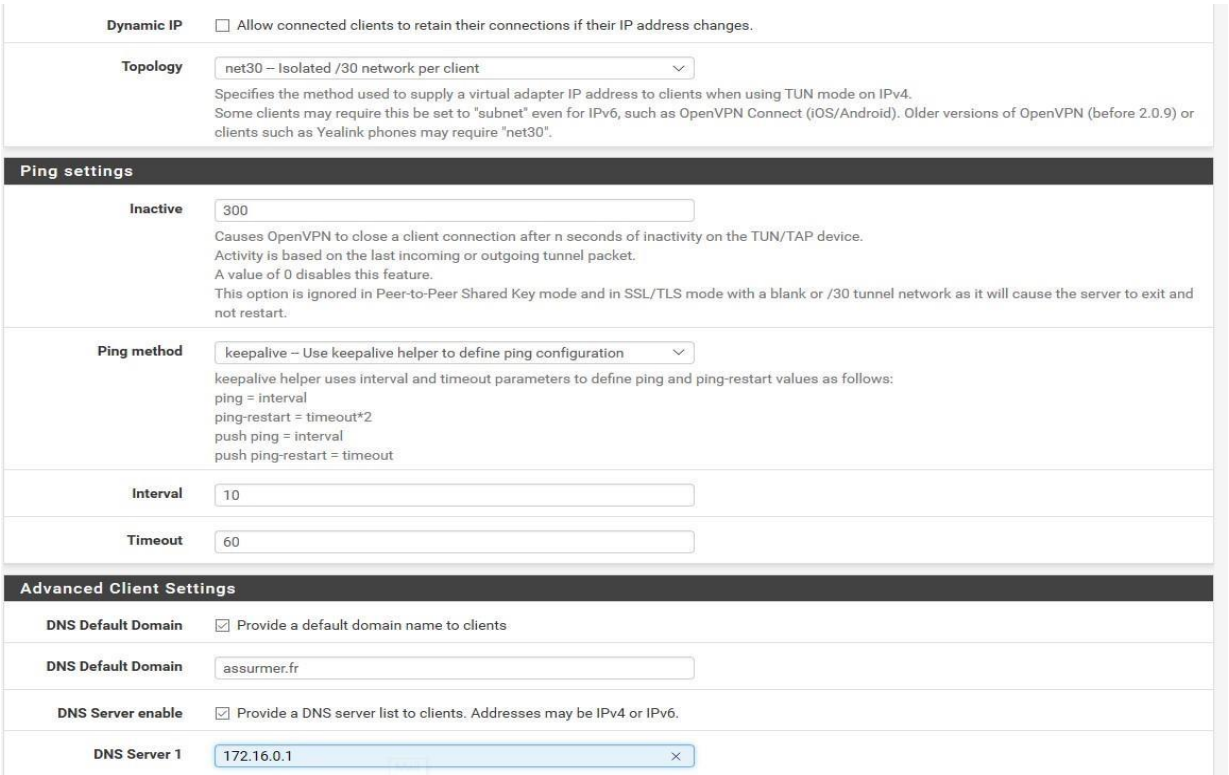


3-Création d'un serveur OpenVPN

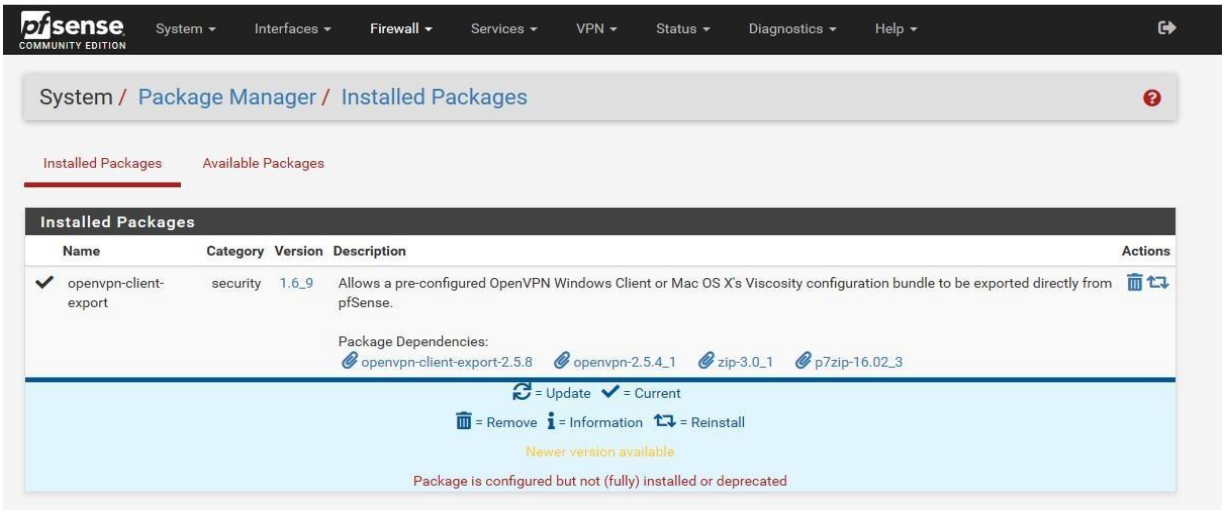




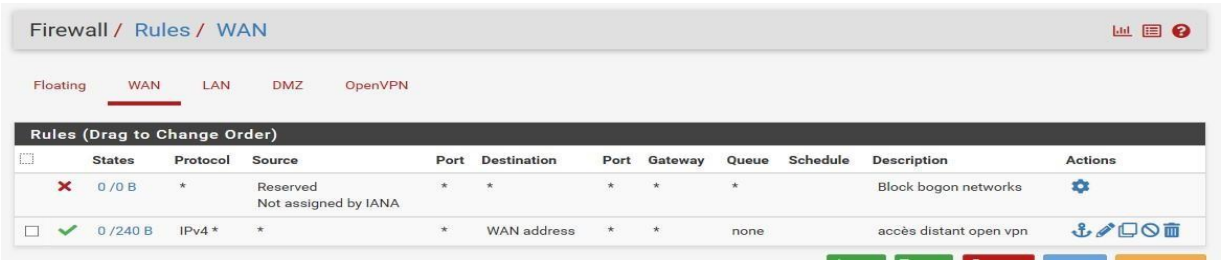

Tunnel Settings
IPv4 Tunnel Network
10.0.0.0/8
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
IPv6 Tunnel Network
This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
Redirect IPv4 Gateway
Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway
Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)
192.168.200.0/24
IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
IPv6 Local network(s)
IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent connections
Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression
Refuse any non-stub compression (Most secure)
Allow compression to be used with this VPN instance.


Dynamic IP
Allow connected clients to retain their connections if their IP address changes.
Topology
net30 – Isolated /30 network per client
Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4.
Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".
Ping settings
Inactive
300
Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device.
Activity is based on the last incoming or outgoing tunnel packet.
A value of 0 disables this feature.
This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.
Ping method
keepalive – Use keepalive helper to define ping configuration
keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows:
ping = interval
ping-restart = timeout*2
push ping = interval
push ping-restart = timeout
Interval
10
Timeout
60
Advanced Client Settings
DNS Default Domain
Provide a default domain name to clients
DNS Default Domain
assurmer.fr
DNS Server enable
Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1
172.16.0.1

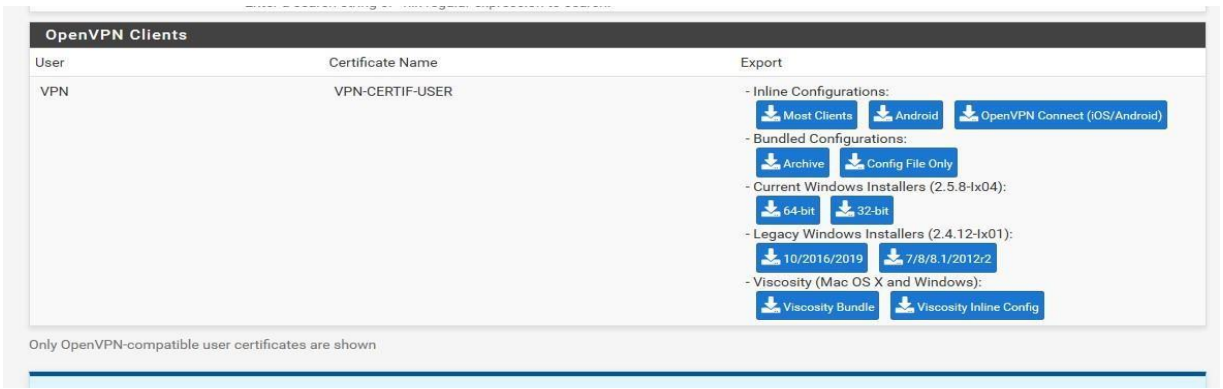
4-Installation du package « openvpn-client-export »

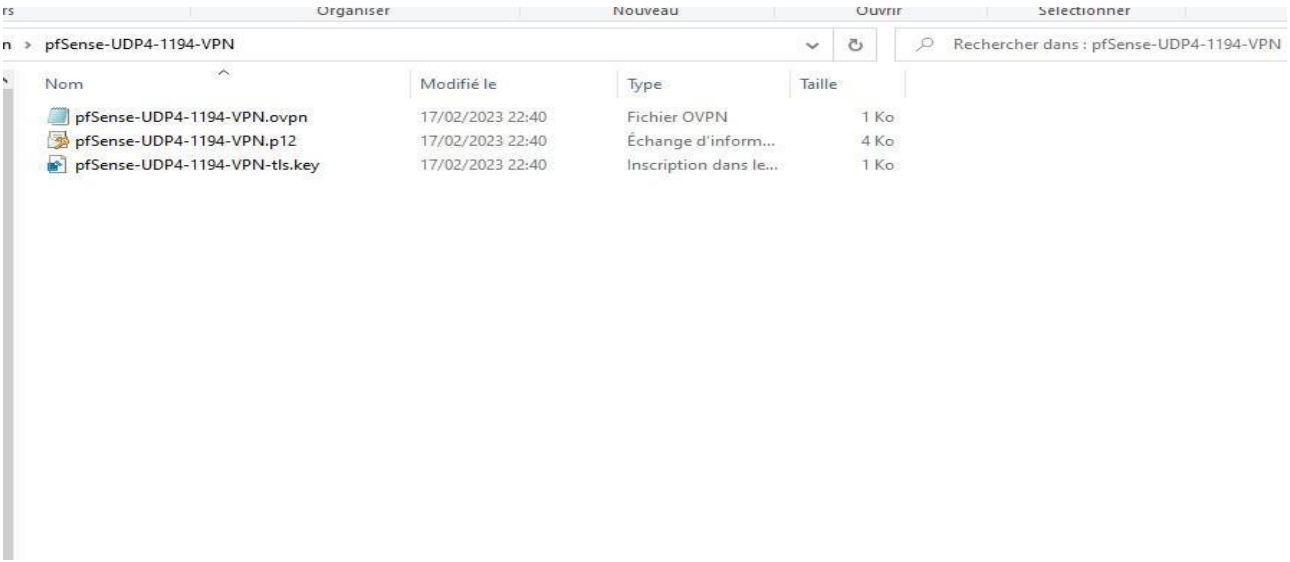


5-Mise en place des règles de pare-feu, afin d'accéder à la DMZ depuis le VPN



6-Exportation et installation du client sur l'utilisateur distant.





B- Veeam Backup

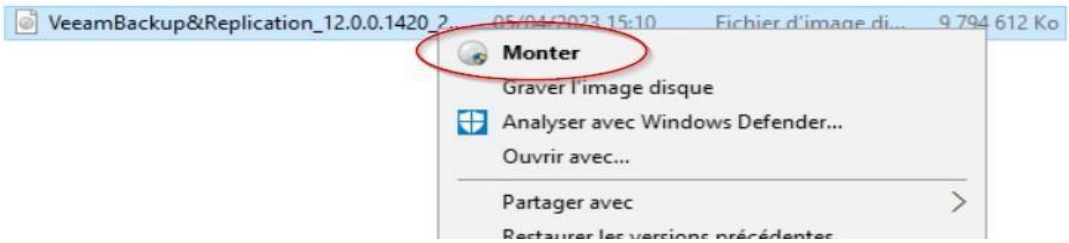
Prérequis :

- Nombre de mémoire RAM conséquent pour assurer les sauvegardes : 8Go
- Un disque dur possédant l'espace nécessaire afin d'accueillir les sauvegardes des différentes VM

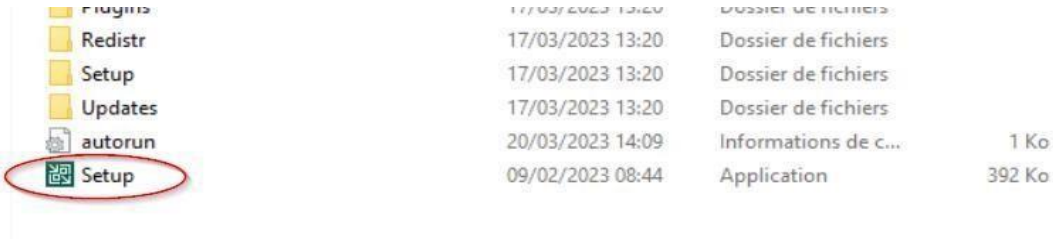
- L'ISO d'installation de Veeam Backup & Réplication (https://www.veeam.com/fr/virtual-machine-backup-solution-free.html)

Procédure d'installation :

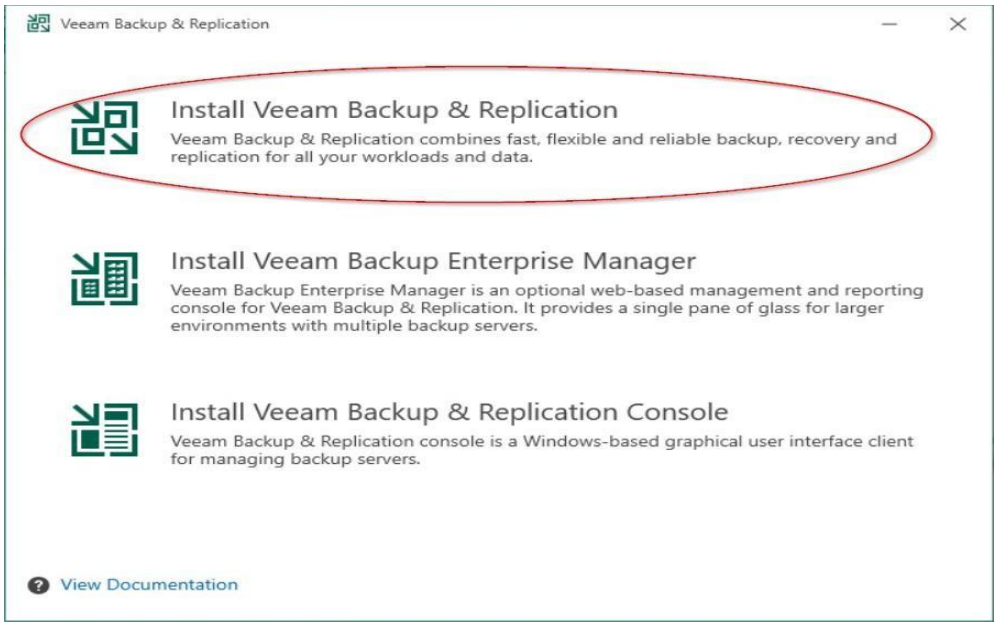
1. Après avoir installé le fichier ISO de Veeam Backup & Réplication, il suffit de faire un clic-droit, et sélectionner l'option « Monter ».



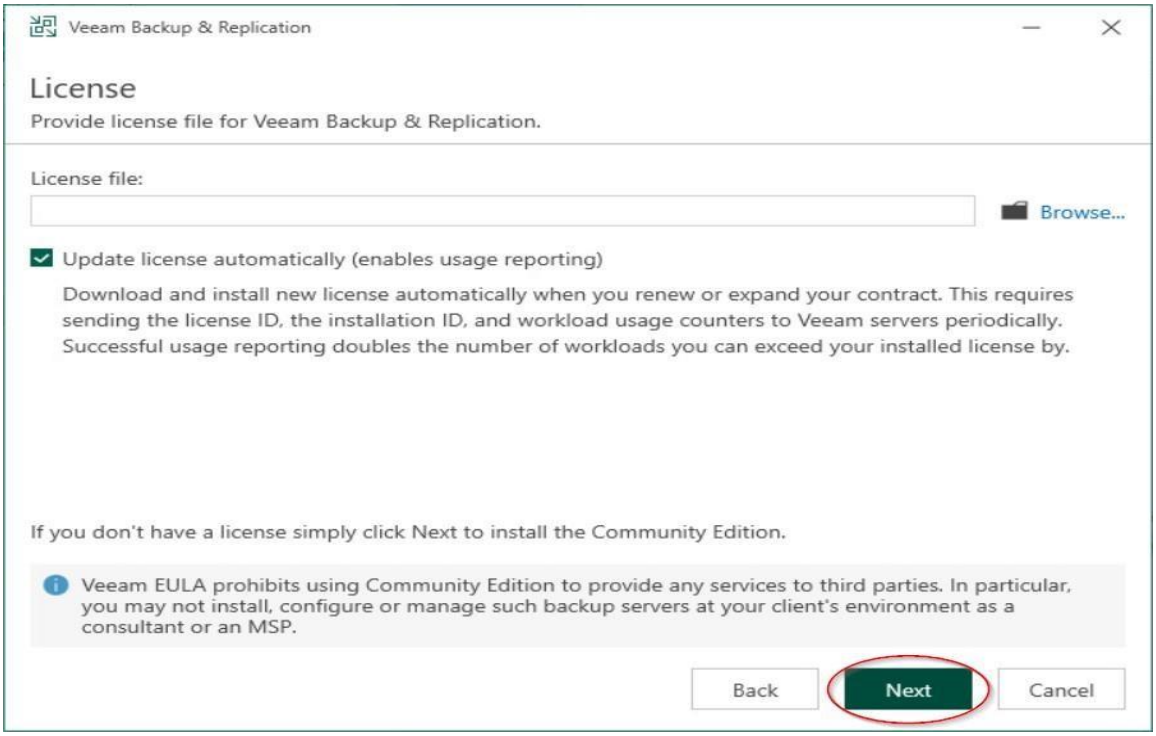
2. Ouvrez ensuite le fichier exécutable « setup ».



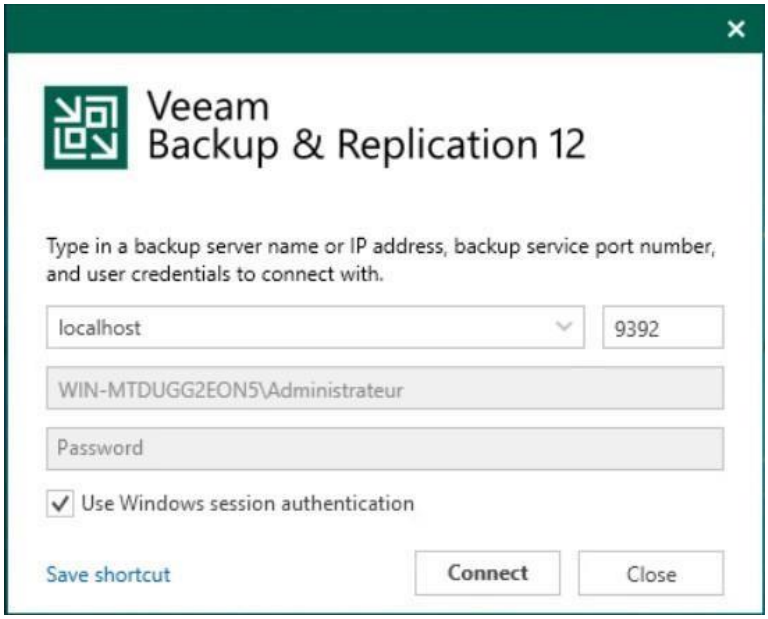
3. Vous pourrez alors procéder à l'installation de l'utilitaire Veeam ; sélectionnez « Install Veeam Backup & Réplication »



4. Il nous sera alors demandé de sélectionner une licence. Dans notre cas nous utilisons la version Gratuite, on cliquera alors simplement sur « Next ».

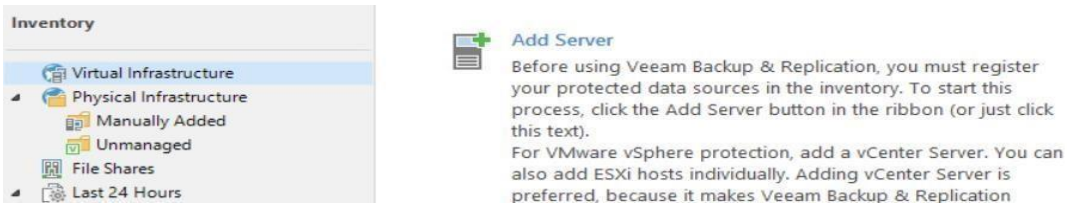


5. À la suite de l'installation, vous devrez lancer « Veeam Backup & Réplication Console ».

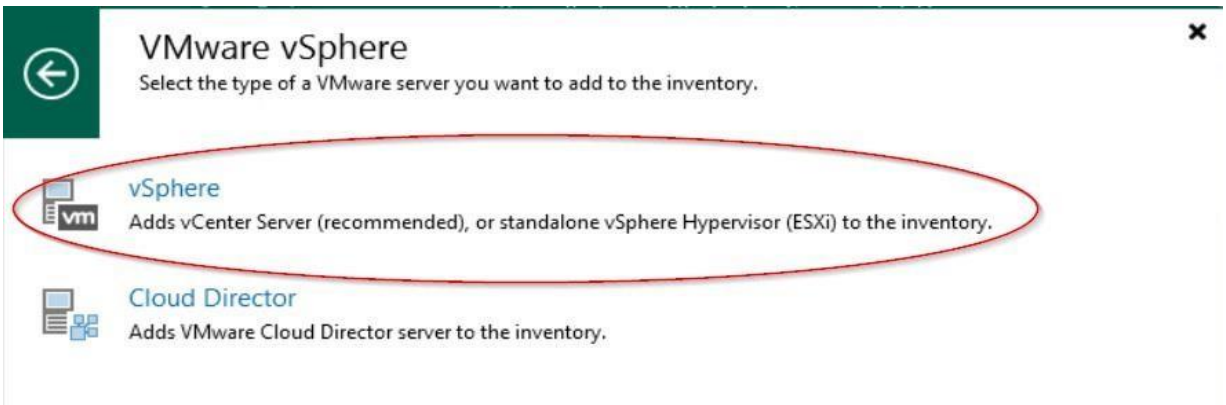


7. Après vous être authentifié, vous aurez accès à l'interface de Veeam. Pour lier notre serveur de sauvegarde à l'hyperviseur que l'on souhaite backuper, on doit se rendre dans « inventory » puis « Virtual infrastructure ».

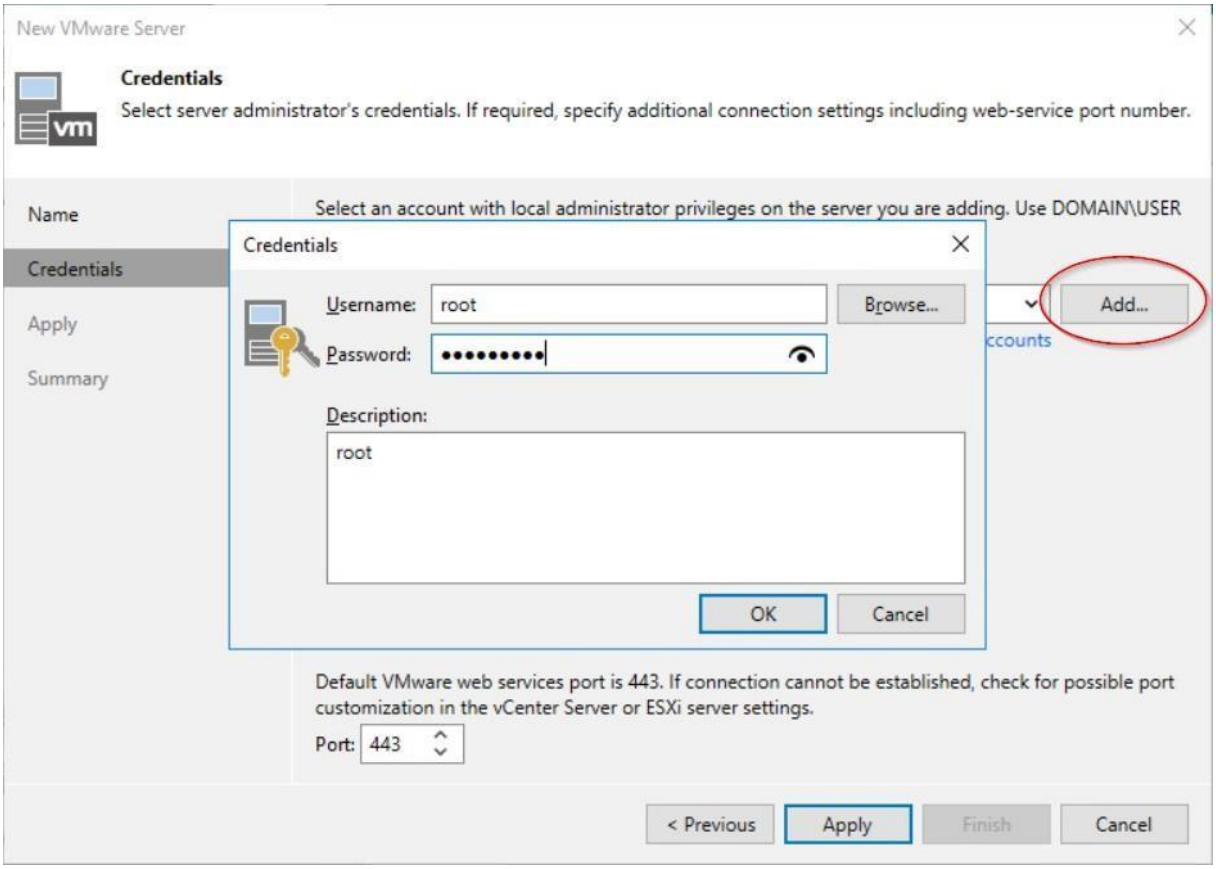
8. On se rendra alors dans « Add-Server »



Dans notre cas, on choisit de backuper un ESXI, on se rendra donc dans « Vmware VSphere », puis VSphere.

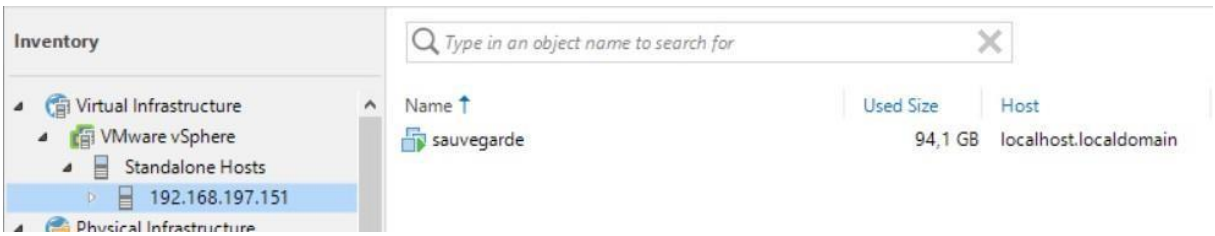


Après avoir renseigné l'adresse IP de notre hôte ESXI, on passera à l'étape suivante pour ajouter les identifiants servant à établir une connexion à l'ESXI, dans notre cas on utilise le compte root. (Si le port d'accès à l'hôte est autre que le port https par défaut, vous devrez le modifier dans cette même rubrique.)



À la suite de cela, vous pourrez cliquer sur « Apply », il vous sera alors demandé d'accepter le certificat auto-généré de l'ESXI lors de la première connexion, puis si vos identifiants sont corrects, Veeam récupérera les informations propres à l'ESXI.

Vous pourrez désormais consulter la liste des machines virtuelles dans la rubrique « Virtual infrastructure » en cliquant sur l'IP ou le nom de votre Hyperviseur.



Afin de connaître comment créer ou restaurer des backups de machines virtuelles, merci de vous rendre sur la procédure dédiée.

III. Quelles sont les impacts

A- OpenVPN

Avec la multiplication des équipements mobile et le développement du télétravail depuis 2020, il nécessaire de disposer d'outils et service sécurisé, afin d'accéder aux ressources de l'entreprise à distance. Il est nécessaire de disposer d'un VPN. En effet, il permet d'accéder au SI depuis un site distant et de disposer d'un canal sécurisé depuis l'extérieur de l'entreprise.

Dans une entreprise, quelle que soit sa taille, les aspects liés à la sécurité informatique sont fondamentaux. L'entreprise doit pouvoir échanger des données sensibles avec ses filiales ou partenaires, en toute sérénité. De plus, les processus d'interconnexion répondent parfaitement aux nouveaux usages, comme la mobilité, le multi-site ou encore le télétravail.

La mise en place d'un VPN pour l'accès distant est recommandée par la CNIL avec une solution de chiffrement suffisante. De plus le logiciel OpenVPN est certifié par l'ANSSI.

B- Veeam Backup

Les solutions de sauvegarde permettent de sauver de manière intègre les données (fichiers, logiciels, systèmes d'information) de l'entreprise pour assurer une reprise d'activité rapide notamment après une attaque de type ransomware ou un sinistre. Ces sauvegardes proposent en effet une restauration facilitée des données devenues inaccessibles. Elles peuvent être faites localement sur les infrastructures d'une organisation.

Les sauvegardes maîtrisées et protégées, associées à un plan de reprise d'activité, constituent un élément essentiel face aux menaces telles que les ransomware ou autres sinistres. Il est nécessaire de définir un plan de sauvegarde (types de sauvegardes, fréquence, espace de stockage, etc.) Ainsi que de réaliser des tests d'intégrité des sauvegardes et des tests de restauration réguliers.

Il est important de suivre les recommandations de la CNIL, prévoir des sauvegardes incrémentales quotidiennes et des sauvegardes complètes à intervalles réguliers. Et ne pas conserver les sauvegardes de donnée au même endroit que les machines les hébergeant.

Le serveur Veeam Backup & Réplication permet de sauvegarder et de restaurer des serveurs critiques tel que l'Active Directory, Mail et de stockage.