

# VPN\_SSL PLUS

Création d'un VPN SSL pour vous connecter au réseau d'entreprise de votre data center virtuel (VDC)



**nxs\_advanced**

Pour utiliser le service **VPN SSL** d'une passerelle EDGE , vous devez avoir une passerelle NSX EDGE ADVANCED

Avec un réseau privé, les utilisateurs distants peuvent accéder aux serveurs et applications des réseaux privés.



**network\_fw**

La passerelle VPN SSL requiert que le port 443 soit accessible à partir des réseaux externes et le client VPN SSL impose que l'adresse IP et le port 443 de la passerelle NSX Edge soient accessibles depuis le système client pour cette configuration.

Se connecter sur la passerelle et configurer les services

## Dans l'onglet **VPN-Plus SSL** :

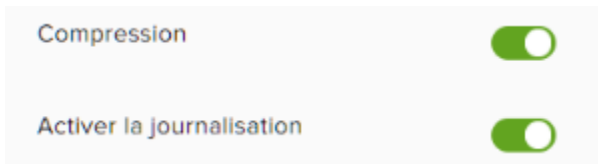
The screenshot shows the configuration page for a VPN-Plus SSL service on a GwEdge gateway. The page title is "Passerelle Edge - GwEdge". The navigation menu includes: Pare-feu, DHCP, NAT, Routage, Load Balancer, VPN, **VPN-Plus SSL** (selected), Certificats, Regroupement d'objets, Statistiques, Paramètres Edge. The sub-menu includes: Paramètres généraux (selected), Configuration du client, Utilisateurs, Pools d'adresses IP, Modules d'installation, Réseaux privés, Paramètres du serveur, Authentication.

**Paramètres généraux de SSL VPN-Plus**

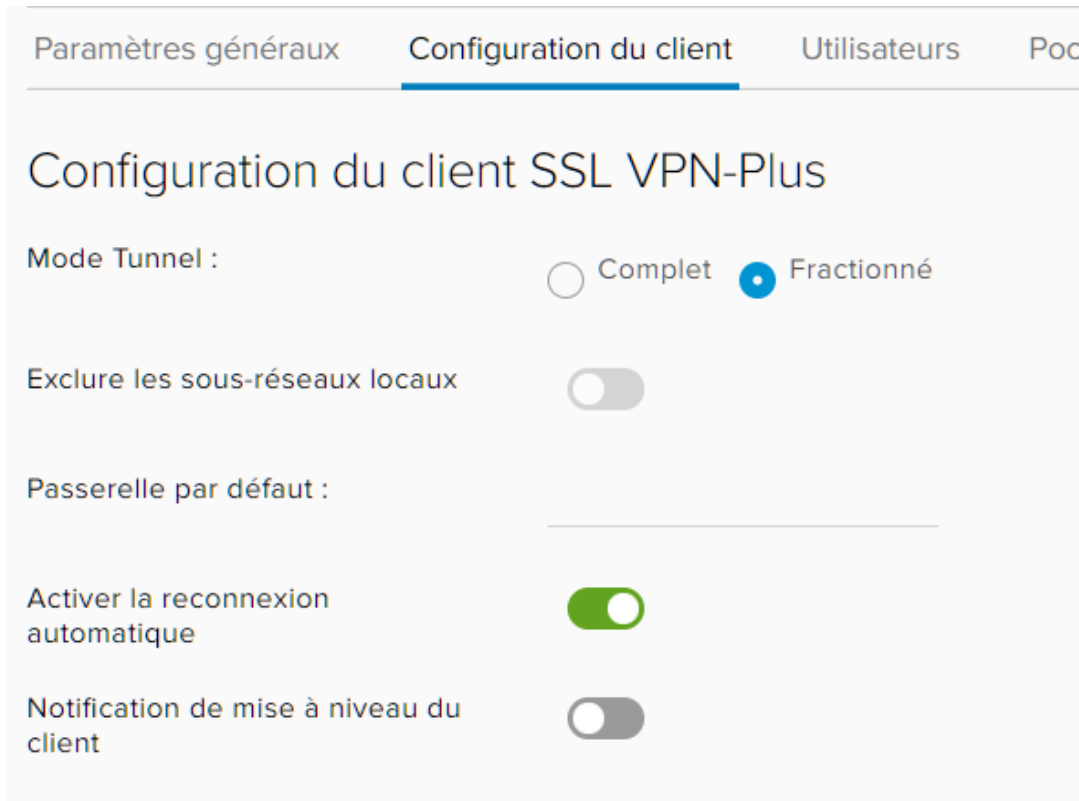
- Empêcher les connexions multiples avec le même nom d'utilisateur:
- Compression:
- Activer la journalisation:
- Forcer le clavier virtuel:
- Randomiser les touches du clavier virtuel:
- Délai d'inactivité de la session \*: 10 Min(s)
- Notification utilisateur:
- Activer l'accès aux URL publiques:
- Activer le délai d'expiration forcé:

Dans cet onglet, vous pouvez modifier les paramètres de base pour le fonctionnement de votre **VPN**.

Vous pouvez par exemple, **activer la compression** et la **journalisation**



Dans l'onglet **Configuration du client** :



Vous pouvez configurer ici à quels réseaux de votre **VDC** vos utilisateurs vont pouvoir se connecter.

Complet: l'ensemble des réseaux du

**VDC**

Fractionné: un certain type de réseau, que vous définissiez depuis l'onglet

**Réseau privés**

Dans l'onglet **Utilisateurs** :

# Passerelle Edge - GwEdge

Pare-feu DHCP NAT Routage Load Balancer VPN **VPN-Plus SSL**

Paramètres généraux Configuration du client **Utilisateurs** Pools d'adresses IP

## Utilisateurs SSL VPN-Plus



ID utilisateur

Vous pouvez gérer les utilisateurs autorisé à utiliser le réseau privé.

### authentication\_idap

Vous pouvez également configurer une méthode d'authentification externe (AD, LDAP, Radius ou RSA) depuis l'onglet **Authentification**  
**Attention:** si vous choisissez une authentification externe, le délai d'authentification maximal via VPN SSL est de 3 minutes. Si votre processus d'authentification prends plus de temps, vous ne serez pas authentifié.

Pour ajouter un utilisateur, cliquer sur



Créer un utilisateur



ID utilisateur \*

Mot de passe \*

Confirmer le mot de passe \*

Prénom

Nom

Description

Activé

Détails du mot de passe  
Le mot de passe n'expire jamais

Autoriser la modification du mot de passe

Modifier le mot de passe à la prochaine connexion

IGNORER

CONSERVER

Sélectionner les options que vous souhaitez appliquer et cliquer sur **CONSERVER** pour sauvegarder

## Dans l'onglet **Pools d'adresses IP**

# Passerelle Edge - GwEdge

Pare-feu DHCP NAT Routage Load Balancer VPN VPN-Plus SSL

Paramètres généraux Configuration du client Utilisateurs Pools d'adresses IP

## Pools d'adresses IP de SSL VPN-Plus



Plage IP

Dans cet onglet, vous allez pouvoir définir l'adressage utilisé pour ce réseau privé. Un utilisateur connecté à ce réseau recevra une adresse IPv4 de ce pool.

Pour ajouter un pool d'adresse, cliquer sur



Modifier un pool d'adresses IP

×

Plage IP \* 192.168.10.1-192.168.10.5C

Masque réseau \* 255.255.255.0

Passerelle \* 192.168.10.254

Cela ajoutera une adresse IP à l'interface na0

Description

VPN SSL PLUS

État



Avancé

DNS primaire

DNS secondaire

Suffixe DNS

Exemple : eng.vmware.com

Serveur WINS

IGNORER

CONSERVER

Indiquer une plage IP utilisé par les clients, **un adressage en dehors des réseaux domestiques privés standard est conseillé (autre autre que 192.168.0.x et 192.168.1.x)**

Idéalement, vous pouvez avoir sur votre réseau privé, un serveur DNS (privé) et vous pourriez remplir un **Suffixe DNS**, par exemple.

Configurer votre pool et cliquer **CONSERVER** pour sauvegarder.

Dans l'onglet **Module d'installation:**

# Passerelle Edge - GwEdge

Pare-feu DHCP NAT Routage Load Balancer VPN **VPN-Plus SSL** Certificats Regroupement  
Paramètres généraux Configuration du client Utilisateurs Pools d'adresses IP **Modules d'installation** Rés

## Modules d'installation de SSL VPN-Plus

### Nom de profil

Aucun module d'installation défini.

Détails du module d'installation pour « »

### Détails de connexion

Passerelle

### Modules d'installation activés pour

Description

### Paramètres d'installation pour Windows

Démarrer le client lors de la connexion  
Autoriser la mémorisation du mot de passe  
Activer l'installation en mode silencieux  
Masquer l'adaptateur réseau du client SSL

Cet onglet vous permet de créer un installeur qui s'occupera de configurer vos postes client suivant la configuration que vous souhaitez mettre en place par défaut.

Vous pouvez créer un module d'installation pour simplifier vos déploiements et configurations du réseau privé.

Cliquer sur  pour ajouter un nouveau profil.

## Ajouter le module d'installation

Nom de profil \*

VPN\_DEFAULT

+

x

Passerelle	Port
vpn-ssl.yulpa.io	443

Créer des modules d'installation pour

Windows

Linux

Mac

Description

VPN SSL DEFAULT

La **passerelle** correspond au nom ou à l'IP publique utilisée par le **client VPN SSL** pour joindre votre **passerelle EDGE** qui fournit le service **VPN SSL**. Le module d'installation est créé pour le système d'exploitation Windows par défaut. Sélectionnez Linux ou Mac pour créer un module d'installation pour les systèmes d'exploitation Linux ou Mac

Activé



## Paramètres d'installation pour Windows

Démarrer le client lors de la connexion

Masquer l'icône de la barre d'état système du client

Autoriser la mémorisation du mot de passe

Créer une icône de bureau

Activer l'installation en mode silencieux

Activer l'opération en mode silencieux

Masquer l'adaptateur réseau du client SSL

Validation du certificat de sécurité du serveur

Vous pouvez configurer les comportements de l'installateur en cochant les options que vous souhaitez utiliser.  
 Si vous n'avez pas de certificat valide, nous vous recommandons dans un premier temps de mettre à jour votre certificat.  
 Si vous utilisez un certificat auto-signé, **considéré comme non valide et non recommandé**, vous devez décocher la case : **Validation du certificat de sécurité du serveur**

Cliquer sur **CONSERVER** pour sauvegarder le profil d'installation.

### Passerelle Edge - GwEdge

Pare-feu DHCP NAT Routage Load Balancer VPN **VPN-Plus SSL** Certificats Regroupement d'objets Statistiques

Paramètres généraux Configuration du client Utilisateurs Pools d'adresses IP **Modules d'installation** Réseaux privés Paramètres

#### Modules d'installation de SSL VPN-Plus

+ [ ] [ ] [ ]

Nom de profil	État
VPN_DEFAULT	Activé

Détails du module d'installation pour « VPN\_DEFAULT »

#### Détails de connexion

Passerelle	Port
vpn-ssl.yulpa.io	443

Modules d'installation activés pour Windows  
 Description VPN SSL DEFAULT

#### Paramètres d'installation pour Windows

Démarrer le client lors de la connexion	Désactivé	Masquer l'icône de la barre d'état système du client	Désactivé
Autoriser la mémorisation du mot de passe	Désactivé	Créer une icône de bureau	Activé
Activer l'installation en mode silencieux	Désactivé	Activer l'opération en mode silencieux	Désactivé
Masquer l'adaptateur réseau du client SSL	Désactivé	Validation du certificat de sécurité du serveur	Activé

## Dans l'onglet **Réseau privés**:

### Passerelle Edge - GwEdge

Pare-feu DHCP NAT Routage Load Balancer VPN **VPN-Plus SSL** Certificats Regroupement d'objets Statistiques

Paramètres généraux Configuration du client Utilisateurs Pools d'adresses IP Modules d'installation **Réseaux privés** Paramètres

#### Réseaux privés SSL VPN-Plus

+ [ ] [ ] [ ] [ ] [ ]

Réseau	Ports	Transmettre par tunnel	Optimiser le trafic	État

Détails du réseau privé :

Transmettre par tunnel	
Optimiser le trafic	
Description	
Ports	

Vous pouvez gérer ici les réseaux privés de votre VDC qui seront accessibles depuis le VPN SSL

Cliquer sur  pour ajouter un réseau

## Ajouter un réseau privé

Réseau \*

Le réseau doit être entré au format CIDR, par exemple : 192.169.1.0/24

Description

Accès a mon réseau local BACKEND

Envoyer le trafic

Activer l'optimisation TCP

Ports

État

IGNORER

CONSERVER

Le réseau correspond à un réseau privé existant dans votre VDC. Ici le réseau **192.168.100.0/24** représente un réseau disponible dans le VDC qui sera accessible aux clients du VPN SSL


Envoyer le trafic, **Par tunnel**. Dans ce cas là, cocher également **Activer l'optimisation TCP**

Port, peut rester vide. Si aucun port n'est spécifié, **tout** le trafic sera optimisé (donc plus de ressources utilisé) version une liste de ports ou l'optimisation sera sélective.

État, **activé**

Cliquer sur **CONSERVER** pour sauvegarder ce réseau privé.

## Réseaux privés SSL VPN-Plus

 Certaines modifications n'ont pas été enregistrées.

[Enregistrer les modifications](#)

[Ignorer les modifications](#)

Réseau	Ports	Transmettre par tu...	Optimiser le trafic	État
192.168.100.0/24	-	Activé	Activé	Activé

### Détails du réseau privé : 192.168.100.0/24

Transmettre par tunnel	Activé
Optimiser le trafic	Activé
Description	Accès a mon réseau local BACKEND
Ports	

Ici vous devez également cliquer sur **Enregistrer les modifications** pour valider la configuration.



## Dans l'onglet **Paramètres du serveur**:

Passerelle Edge - GwEdge

Pare-feu DHCP NAT Routage Load Balancer VPN **VPN-Plus SSL** Certificats Regroupement d'objets Statistiques Paramètres Edge

Paramètres généraux Configuration du client Utilisateurs Pools d'adresses IP Modules d'installation Réseaux privés **Paramètres du serveur** Aut

### Paramètres du serveur

Les paramètres du serveur représentent les configurations associées au serveur SSL VPN comme l'adresse IP et le port d'écoute, la liste de chiffrement et le certificat du ser

Activé

Adresse IPv4 ip\_publique\_de\_votre\_passerelle

Port 443

Liste des chiffrements

AES128-SHA	<input type="checkbox"/>
AES256-SHA	<input checked="" type="checkbox"/>
DES-CBC3-SHA	<input type="checkbox"/>

Stratégie de journalisation

Activer la journalisation Activé


Niveau de consignation Avis

[MODIFIER LE CERTIFICAT DU SERVEUR](#)


Ici vous pouvez configurer votre serveur VPN SSL .

Vous devez **Activer** le serveur

Sélectionner l'IPv4 Publique pour laquelle le serveur répondra aux clients essayant de se connecter

 **fw\_vpn**

Assurez vous que pare-feu est bien ouvert pour cette IP publique et sur le port que vous avez configuré le VPN SSL

2 	sslvpn	Interne élev Tous	IPv4 Publique	tcp:443:any	Accepter
---	--------	-------------------	---------------	-------------	----------

La liste des chiffrements correspond au chiffrement utilisé pour les communications.

Vous devez vous assurer que vos clients sont compatibles avec ce type de chiffrements.

La configuration de la journalisation par défaut est **activée**

Vous pouvez cliquer ensuite sur **Enregistrer les modifications** pour valider la configuration du serveur VPN

Vous pouvez maintenant vous connecter au réseau VPN SSL depuis votre navigateur : [https://ip\\_ou\\_nom\\_de\\_votre\\_passerelle](https://ip_ou_nom_de_votre_passerelle)

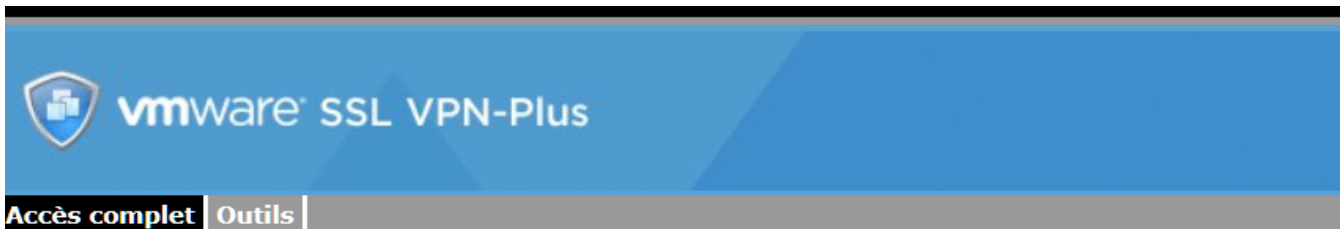


### Connexion au portail

Entrez ici vos informations d'identification de connexion

Nom d'utilisateur   
Mot de passe

Indiquer un nom d'utilisateur et son mot de passe puis cliquer sur **Connexion**  
Une fois connecté, vous pouvez télécharger le module d'installation pour installer votre client VPN



### Accès complet

Clients de l'extension réseau disponibles.

Liste	Description
VPN_DEFAULT	Télécharger le client d'accès complet (client PHAT)

Cliquer sur le profil en question **VPN\_DEFAULT**



Page de téléchargement de VMware Full Access Client (PHAT)

Nom du profil : VPN\_DEFAULT  
Version : v6.4.0

Si l'installation ne commence pas dans 60 secondes ou si votre navigateur ne prend pas en charge ActiveX,  
Veuillez [cliquer ici](#) pour démarrer l'installation.

Utilisateurs de Windows XP SP2 et versions ultérieures : recherchez la barre d'informations d'Internet Explorer en haut du navigateur Web. Selon les paramètres de sécurité de votre machine, une fenêtre d'avertissement de sécurité peut s'afficher. Veuillez à cliquer sur « Installer » (ou sur « Oui » pour les autres versions de Windows)

Durant l'installation du client VMware VPN-Plus SSL, une fenêtre de signature de pilote peut s'afficher. Veuillez à cliquer sur « Continuer quand même » (ou sur « Oui » pour Windows 2000)

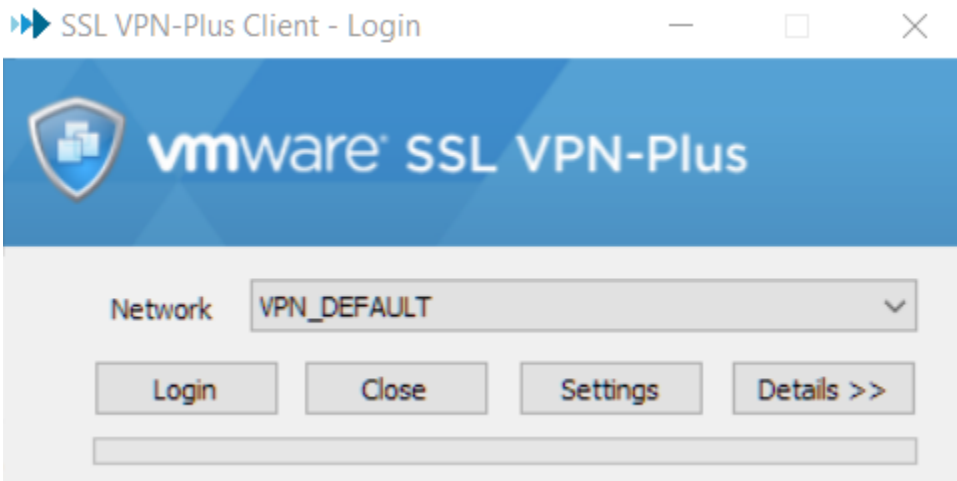
Le téléchargement doit se faire automatiquement ou vous pouvez cliquer sur le lien indiqué pour "**démarrer l'installation**"

L'archive ZIP contient l'installer que vous avez configuré et que vous pouvez maintenant installer après avoir extrait le contenu de l'archive :

Nom

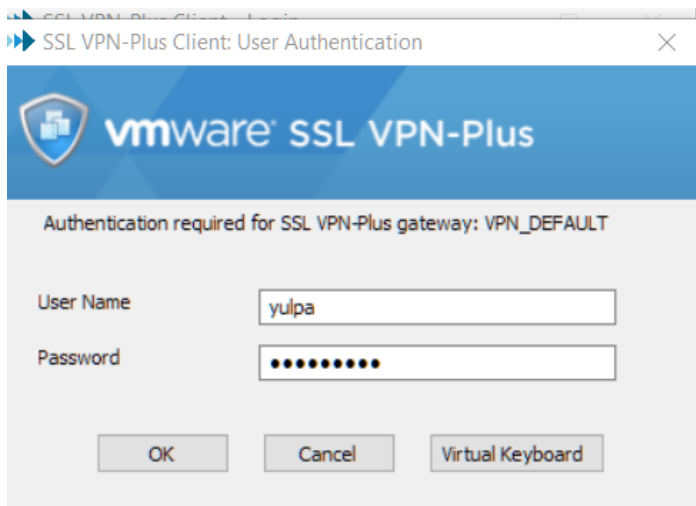
- connected.ico
- desktopconnected.ico
- disconnected.ico
- errorconnected.ico
- Installer.exe**
- InstallerRes\_040c.dll
- InstallerRes\_0407.dll
- InstallerRes\_0409.dll
- InstallerRes\_0411.dll
- InstallerRes\_0412.dll
- InstallerRes\_0804.dll
- naconf.cfg
- nafiles.exe
- nainstaller.exe
- phat\_banner.bmp
- upgrade.exe

Après l'installation, vous pouvez exécuter **VMwareTray** pour lancer le client et vous connecter

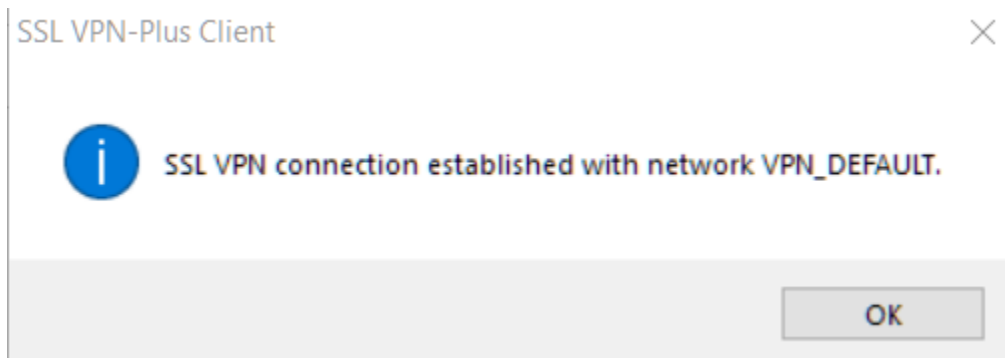


Cliquer sur **Login**

La connexion se fait directement à votre passerelle edge pour accéder au service VPN SSL



Indiquer votre nom d'utilisateur et votre mot de passe et cliquer sur **OK**

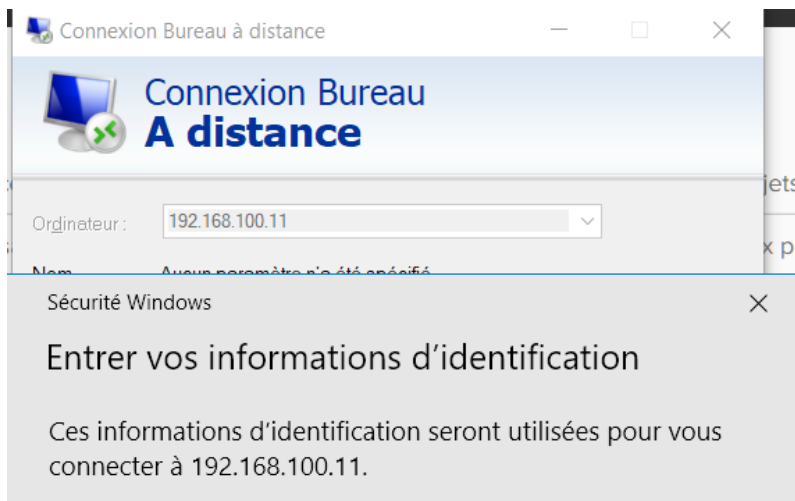


**La connexion est établie !**

Vous pouvez maintenant accéder aux services présents dans votre VDC , autorisé par la configuration .

Ici , nous avons autorisé le réseau **192.168.100.0/24**

Un serveur Windows autorisant les connexions RDP écoute sur son IP privée : **192.168.100.11** , il est maintenant possible de se connecter en VPN et de se connecter en RDP via son ip privée



Cette documentation vous permet d'avoir un réseau privé VPN SSL fonctionnel en quelques minutes.  
Les options et les configurations sont complètes au niveau de la passerelle, nous vous invitons à regarder en détail le fonctionnement du VPN SSL PLUS sur les documentation officiel de VMware pour ajuster les configurations et la sécurité suivant vos besoins.