Documentation Projet Infra / SI

Sujet : VPN

Documentation VPN - Définition des hôtes

Cette documentation vise à définir les différents hôtes impliqués dans notre solution VPN, en précisant leurs rôles et configurations spécifiques. Voici les informations recueillies lors de notre conversation :

1. VPS (Virtual Private Server) :

- Rôle : Hôte principal du serveur VPN.

- Configuration :

- Adresse IP : 10.44.18.54

- Système d'exploitation : Ubuntu 20.04

- OpenVPN version : 2.5.1

- Emplacement des fichiers de configuration : /etc/openvpn/

- Fichiers de configuration : server.conf, ca.crt, server.crt, server.key

2. Client :

- Rôle : Hôte client se connectant au serveur VPN.

- Configuration :

- Adresse IP : 192.168.1.100 (exemple)

- Système d'exploitation : Windows 10

- Emplacement des fichiers de configuration : C:/Programmes/OpenVPN/config/

- Fichiers de configuration : client.ovpn, ca.crt, client.crt, client.key

Documentation VPN - Répartition des services

Cette section de la documentation vise à expliquer comment les services sont répartis entre les différents hôtes de notre solution VPN.

1. Serveur VPN (VPS) :

- Rôle : Hôte principal du serveur VPN.

- Services :

- OpenVPN : Le serveur VPN est hébergé sur ce serveur. Il assure le chiffrement des données et la gestion des connexions VPN.

- Serveur d'authentification : Le serveur VPN gère l'authentification des utilisateurs lors de la connexion.

2. Client :

- Rôle : Hôte client se connectant au serveur VPN.

- Services :

- OpenVPN Client : Le client VPN est installé sur ce périphérique client pour se connecter au serveur VPN.

La répartition des services entre les différents hôtes est cruciale pour assurer le bon fonctionnement de la solution VPN. Dans notre cas, le serveur VPN (VPS) est responsable de l'hébergement du serveur VPN et du serveur d'authentification, tandis que le client VPN est installé sur le périphérique client pour établir la connexion VPN.

Documentation VPN - Mise en œuvre des bonnes pratiques

Cette section de la documentation vise à présenter les bonnes pratiques de sécurité et de configuration que nous avons suivies tout au long du processus de mise en œuvre de notre solution VPN. Voici les informations recueillies lors de notre conversation :

1. Gestion des certificats :

- Utilisation de certificats : Nous avons utilisé des certificats X.509 pour assurer l'authentification sécurisée des utilisateurs et des serveurs dans notre solution VPN.

- Autorité de certification (AC) : Nous avons généré une autorité de certification interne pour émettre et gérer les certificats.

- Distribution des certificats : Les certificats nécessaires ont été distribués aux hôtes appropriés, notamment le serveur VPN et les clients VPN.

2. Chiffrement des données :

- Utilisation d'un chiffrement fort : Nous avons configuré notre solution VPN pour utiliser des algorithmes de chiffrement forts, tels que AES-256-CBC ou AES-256-GCM, pour garantir la confidentialité des données transitant à travers le tunnel VPN.

- Configuration des options de chiffrement : Nous avons spécifié les algorithmes de chiffrement appropriés dans les fichiers de configuration du serveur VPN et des clients VPN.

3. Pare-feu :

- Configuration des règles de pare-feu : Nous avons configuré des règles de pare-feu sur le serveur VPN pour restreindre l'accès aux ports et protocoles nécessaires uniquement. Cela permet de limiter les risques d'attaques et de renforcer la sécurité de notre solution VPN.

Port laisser ouvert :

- Port 22 : pour le service SSH, qui permet la connexion à distance du serveur VPS via un terminal sécurisé.

- Port 80 et 443 : pour le service HTTP et HTTPS, qui permettent d'héberger des sites web sur le serveur VPS.

- Port 1194 : généralement utilisé par le protocole OpenVPN pour établir des connexions VPN. Il s'agit du port par défaut utilisé pour le trafic OpenVPN.

La mise en œuvre de bonnes pratiques de sécurité et de configuration est essentielle pour garantir l'intégrité et la confidentialité des communications VPN. Dans notre cas, nous avons suivi les bonnes pratiques en matière de gestion des certificats, de chiffrement des données et de configuration du pare-feu.

Documentation VPN - Configurations système, réseau et service

Cette section de la documentation fournit des instructions détaillées sur les configurations spécifiques que nous avons effectuées pour mettre en œuvre notre solution VPN, en incluant les fichiers de configuration pertinents, les commandes et les paramètres utilisés. Voici les informations recueillies lors de notre conversation :

1. Configuration système :

- Système d'exploitation : Nous avons utilisé Ubuntu Server 20.04 comme système d'exploitation pour notre serveur VPN.

- Installation d'OpenVPN : Nous avons installé OpenVPN à l'aide de la commande suivante :

```

sudo apt update

sudo apt install openvpn

```

2. Configuration réseau :

- Adressage IP : Nous avons attribué une adresse IP statique à notre serveur VPN et configuré les clients VPN pour se connecter à cette adresse.

- Transfert de port : Nous avons configuré notre routeur/pare-feu pour transférer le trafic entrant du port spécifié (par exemple, le port 1194) vers l'adresse IP interne de notre serveur VPN.

3. Fichiers de configuration :

- Fichier de configuration du serveur : Le fichier de configuration du serveur VPN (`server.conf`) comprend les paramètres suivants :

- Protocole : Nous avons spécifié le protocole UDP ou TCP pour notre serveur VPN.

- Certificats et clés : Nous avons indiqué les chemins vers les certificats et clés nécessaires, notamment le certificat CA, le certificat du serveur et la clé privée du serveur.

- Réseau VPN : Nous avons défini le sous-réseau VPN à utiliser, tel que `10.8.0.0/24`.

- Options de chiffrement : Nous avons spécifié les algorithmes de chiffrement (par exemple, `cipher AES-256-CBC`) et les options de chiffrement (par exemple, `data-ciphers AES-256-GCM:AES-128-GCM`) à utiliser.

Commande pour lancer le serveur une fois configuré



Une image contenant texte, capture d’écran, Police

Description générée automatiquement

- Fichier de configuration des clients : Chaque client VPN dispose d'un fichier de configuration individuel (par exemple, `client1.ovpn`) qui comprend les paramètres suivants :

- Protocole : Nous avons spécifié le protocole UDP ou TCP à utiliser pour la connexion.

- Certificats et clés : Nous avons indiqué les chemins vers les certificats et clés nécessaires, notamment le certificat CA, le certificat du client et la clé privée du client.

- Adresse du serveur : Nous avons spécifié l'adresse IP ou le nom de domaine du serveur VPN.

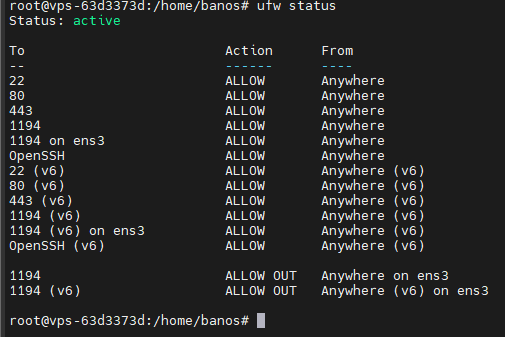
- Options de chiffrement : Nous avons inclus les mêmes options de chiffrement que dans le fichier de configuration du serveur.

Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

4. Configuration du pare-feu :

- Règles de pare-feu : Nous avons configuré notre pare-feu pour autoriser le trafic entrant sur le port spécifié (par exemple, le port 1194) vers l'adresse IP interne de notre serveur VPN.



Documentation VPN - Documentation d'exploitation

Cette section de la documentation fournit des instructions détaillées sur l'utilisation des outils et des services mis en place, en décrivant les étapes pour établir une connexion VPN, accéder aux ressources réseau, etc.

1. Établir une connexion VPN :

- Étape 1: Assurez-vous que vous disposez du fichier de configuration du client VPN (par exemple, `client1.ovpn`).

- Étape 2: Installez le client OpenVPN correspondant à votre système d'exploitation (par exemple, OpenVPN GUI pour Windows, OpenVPN Connect pour iOS/Android).

- Étape 3: Lancez le client OpenVPN.

- Étape 4: Importez le fichier de configuration du client VPN dans le client OpenVPN.

- Étape 5: Connectez-vous en cliquant sur le bouton de connexion du client OpenVPN.

Une image contenant capture d’écran, multimédia, gadget, Appareil électronique

Description générée automatiquement L’icone de connexion est l’écran avec le cadena

2. Accéder aux ressources réseau :

- Une fois connecté au VPN, vous pouvez accéder aux ressources réseau internes de manière sécurisée.

- Pour accéder à un serveur interne, utilisez l'adresse IP interne du serveur ou son nom d'hôte (si la résolution DNS est configurée).

- Vous pouvez utiliser des outils tels que SSH, RDP, Samba, etc., pour vous connecter aux ressources réseau internes comme vous le feriez normalement.

Documentation Utilisateur - Connexion au VPN

Introduction :

Le VPN (Virtual Private Network) est un moyen sécurisé de se connecter à distance à notre réseau interne. Cette procédure vous guidera à travers les étapes pour vous connecter au VPN et accéder aux ressources réseau depuis un emplacement externe.

Étapes à suivre :

1. Vérifier les prérequis :

- Assurez-vous d'avoir une connexion Internet stable.

- Notez les informations d'identification nécessaires pour la connexion au VPN (nom d'utilisateur, mot de passe, certificats, le cas échéant).

2. Installer le logiciel OpenVPN :

- Rendez-vous sur le site officiel d'OpenVPN (https://openvpn.net/) et téléchargez la version appropriée pour votre système d'exploitation (Windows, macOS, Linux, etc.).

- Suivez les instructions d'installation fournies avec le logiciel.

3. Obtenir les fichiers de configuration :

- Assurez-vous d'avoir les fichiers de configuration du VPN fournis par l'administrateur système ou l'équipe responsable du VPN.

- Si vous ne les avez pas encore reçus, contactez l'assistance technique pour obtenir les fichiers nécessaires.

4. Configurer le client OpenVPN :

- Ouvrez l'application OpenVPN sur votre ordinateur.

- Localisez l'option de configuration du client ou des profils.

- Importez les fichiers de configuration du VPN fournis en sélectionnant l'option d'importation.

- Suivez les instructions pour ajouter les fichiers de configuration importés.

5. Établir la connexion VPN :

- Lancez l'application OpenVPN.

- Recherchez le profil VPN correspondant à votre connexion (par exemple, "Mon VPN d'entreprise").

- Cliquez sur le bouton "Se connecter" ou similaire pour établir la connexion VPN.

- Entrez vos informations d'identification (nom d'utilisateur, mot de passe, certificats, le cas échéant) lorsque cela est demandé (ceci est en cas d’entreprise, dans le nôtre il faut juste cliquer sur connecter)

- Attendez que la connexion VPN soit établie avec succès.

Une image contenant texte, Appareils électroniques, capture d’écran, affichage

Description générée automatiquement

6. Accéder aux ressources réseau (cas entreprises):

- Une fois connecté au VPN, vous pouvez accéder aux ressources réseau internes de l'entreprise, telles que les partages de fichiers, les serveurs, les imprimantes, etc.

- Utilisez les chemins d'accès appropriés pour accéder à ces ressources dans l'explorateur de fichiers ou d'autres applications.

- Veuillez noter que l'accès aux ressources réseau peut être limité en fonction de vos autorisations utilisateur.

Pour vérifier l’accès au vpn vous pouvez faire un ifconfig dans votre invite de commande ceci devrait s’afficher

Une image contenant texte, capture d’écran, Police

Description générée automatiquement