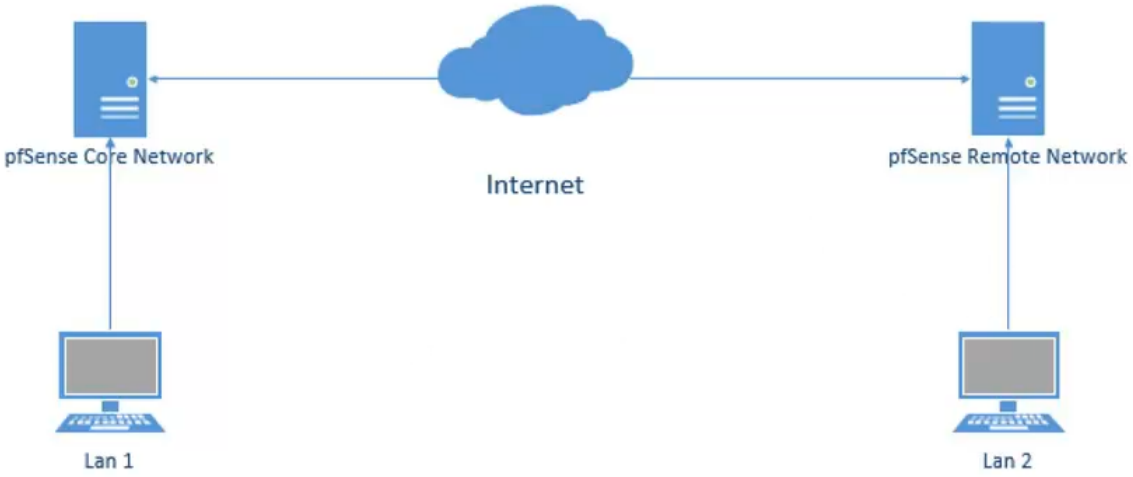
Pfsense : Mise en place de VPN

I. VPN IPSEC site to site



Le but est de configurer un VPN site 2 site à l'aide de pfsense. Pour cela, nous allons créer l'architecture suivante :

- 2 routeurs pfsense virtuels
- 2 LAN Segments (Lan 1 et Lan 2) avec l'adressage 192.168.10.0/24 et 192.168.20.0/24
- Un réseau publique simulé par le bridge
- 2 clients dans les LAN partageant des ressources (un dossier par exemple)

1. Mettez en place cette architecture, et effectuez la configuration IP nécessaire

La connexion VPN IPSEC va se dérouler en 2 temps : le premier effectuant la négociation des paramètres de sécurité, et le second sera relatif à l'échange des données.

La première phase concerne donc la partie IKE (P1 = Phase one)

2. Ajouter la phase P1
3. Configurez votre IKE en spécifiant la version 2 et en indiquant l'ip de la machine distante (Remote Gateway). Donnez une description explicite

L'idéal au niveau sécurité est l'authentification par certificat. Pour le moment, dans ce TP nous n'allons effectuer une authentification via mot de passe (Pré Shared Key)

4. Paramétrez les données d'authentification

   On choisira un hash en SHA256 (SHA1 étant sensible aux attaques). Les clés symétriques seront en 2048 bits

5. Expliquez les options suivantes :

- Disable rekey

- Responder only
- Dead Peer Detection

6. Validez votre phase 1

7. Créez la phase 2 et indiquez les paramètres nécessaires :
- IP du réseau distant
- Description
- Protocole ESP (AH ne chiffre pas les données)
- Chiffrement AES / SHA 256

8. Créez la règle de firewall autorisant le trafic entre les 2 réseaux VPN

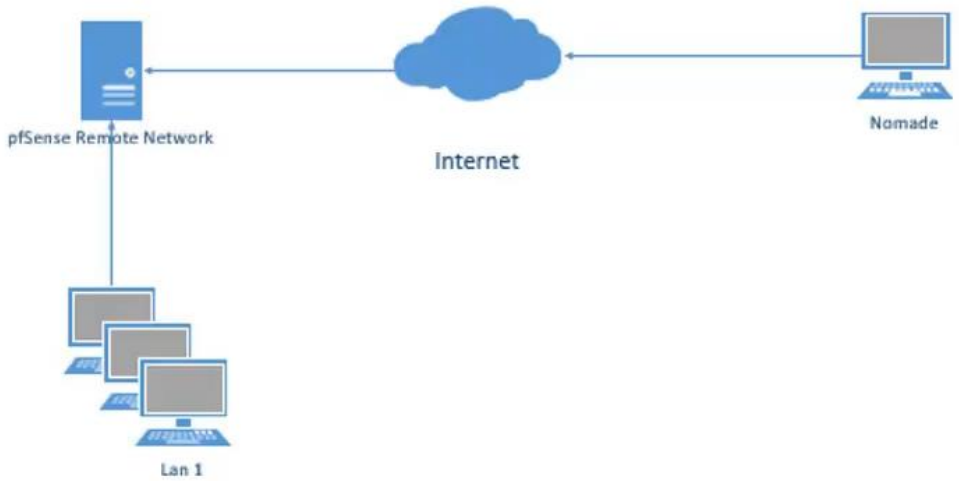
9. Définissez vos passerelles VPN

10. Effectuez la configuration du second serveur

11. Connectez vos routeurs VPN

12. Notez vos configurations IP des machines du LAN et tentez d'accéder mutuellement aux ressources partagées de chaque côté du VPN

II. VPN d'accès OpenVPN



Dans ce cas, l'utilisateur nomade va se connecter depuis internet sur le pfsense selon le protocole openvpn afin d'accéder aux ressources partagées du réseau local. Openvpn est une solution libre de VPN basée sur la cryptographie et les certificats.

1. Mettez en place la configuration précédente, le réseau LAN aura pour IP 192.168.10.0/24, et le réseau public sera simulé par le réseau NAT de Workstation

2. Utilisez le Wizzard afin de configurer votre connexion openvpn

   Décrivez en une phrase chaque étape de configuration

3. Terminez la configuration

4. Ajoutez le package openvpn-client-export

5. Créez un utilisateur nommé vpnuser

Openvpn requiert un logiciel client pour pouvoir se connecter à distance. L'outil vpn intégré dans Windows ne fonctionne pas avec openvpn

6. Téléchargez le logiciel client .exe à partir du Windows 10 sur le pfsense

7. Installez le et testez votre connexion en tant que vpnuser

8. Vérifiez que vous avez accès aux ressources partagées du LAN

9. Vérifiez le log de votre connexion sur pfsense

10. Ajoutez une supervision des connexions vpn sur le dashboard de pfsense