Guide complet : Installation et configuration d'OPNsense

1. Installation d'OPNsense

L'installation d'OPNsense commence par le téléchargement de son image ISO. Cette image doit être transférée sur une clé USB bootable à l'aide d'un outil tel que Rufus ou Etcher. Insérez ensuite la clé USB dans la machine destinée à héberger OPNsense et configurez le BIOS/UEFI pour démarrer sur la clé USB. Une fois démarré, suivez les instructions à l'écran pour lancer l'installation.
Configuration initiale :
Durant l'installation, plusieurs informations vous seront demandées, comme le disque où OPNsense sera installé. Une fois l'installation terminée, redémarrez la machine et retirez la clé USB.
2. Configuration des interfaces réseau
Lorsque le système redémarre, vous accédez à une interface en ligne de commande qui permet de configurer les interfaces réseau.

La première étape consiste à attribuer les interfaces réseau aux différents segments (LAN, DMZ, WAN) en utilisant la commande :
1) Assign interfaces

Identifiez chaque interface à l'aide des adresses MAC pour les associer aux réseaux LAN, DMZ et WAN. Si vous n'avez pas de correspondance précise, vous pouvez attribuer les interfaces au hasard, mais cela pourrait compliquer le dépannage.
Une fois les interfaces attribuées, configurez les adresses IP pour chaque interface via :
2) Set interface IP address

Sélectionnez une interface à configurer.
Indiquez si l'adresse IP doit être statique ou dynamique (choisissez "n" pour une IP statique). Entrez l'adresse IPv4 souhaitée (par exemple : 10.31.224.1 pour le LAN). Spécifiez le masque de sous-réseau en notation CIDR (Pour le lan 255.255.252.0). Fournissez l'adresse IP de la passerelle si nécessaire. Configurez un serveur DNS (10.31.232.53). Terminez en validant chaque étape avec la touche Entrée. Répétez cette opération pour les interfaces WAN et DMZ.

Après la configuration des interfaces, désactivez temporairement le pare-feu avec la commande : pfctl -d Vous pourrez le réactiver plus tard avec pfctl -e une fois la configuration terminée.

3. Accès à l'interface web d'OPNsense
Après avoir configuré les interfaces réseau, vous pouvez accéder à l'interface de gestion Web d'OPNsense depuis un navigateur web. Utilisez l'adresse IP attribuée à l'interface WAN.

Avant de commencer, pensez à autoriser les réseaux privés sur l'interface WAN pour sécuriser l'accès. Ensuite, créez une règle NAT qui permettra d'accéder à l'interface graphique d'OPNsense depuis le WAN, même si le pare-feu est activé.

4. Configuration des règles de pare-feu Les règles de pare-feu permettent de contrôler le trafic réseau entre les différentes interfaces et de sécuriser l'accès. Voici les configurations nécessaires pour chaque interface :

Règles pour le LAN Le réseau LAN doit permettre le trafic DNS vers des adresses spécifiques comme 10.31.232.53 et 10.31.232.54. En outre, autorisez les connexions nécessaires pour les mises à jour système via HTTP (port 80) et HTTPS (port 443).

Ajoutez également des règles pour :

Autoriser le trafic SSH (port 22) entre le LAN et la DMZ, si nécessaire pour des sauvegardes ou la gestion des serveurs. Autoriser les pings (ICMP) entre le LAN et la DMZ, ce qui est utile pour tester la connectivité réseau. Règles pour la DMZ Dans la DMZ, configurez des règles permettant :

Le trafic DNS vers des serveurs externes tels que 8.8.8.8 et 8.8.4.4. Les connexions HTTP et HTTPS vers Internet, indispensables pour les mises à jour système. Si des applications hébergées dans la DMZ nécessitent un accès à des services spécifiques, comme une base de données sur un réseau distinct ou un serveur DHCP, ajoutez des règles adaptées. Par exemple :

Une règle pour permettre les connexions de la DMZ vers une base de données sur le réseau interne (port 3306 pour MySQL). Une règle pour autoriser le relais DHCP vers un serveur dédié. Règles pour le WAN Sur l'interface WAN, configurez des règles pour autoriser l'accès aux services internes tout en maintenant un bon niveau de sécurité :

Autorisez les connexions HTTPS (port 443) vers des serveurs web publics et privés situés dans la DMZ. Ajoutez des règles pour permettre des services spécifiques tels que le FTP (port 21), le Samba pour les fichiers (port 445), ou encore les connexions de bureau à distance (RDP, port 3389). Autorisez les pings (ICMP) depuis le WAN vers les réseaux internes (LAN et DMZ) pour des besoins de diagnostic réseau. Par exemple :

Une règle permettant l'accès depuis un réseau externe à un serveur Proxmox interne via le port 8006. Une autre pour autoriser les connexions SSH vers les serveurs du LAN ou de la DMZ. 5. Test et validation Une fois toutes les règles de pare-feu configurées, effectuez les tests suivants :

Vérifiez que chaque interface réseau peut communiquer avec les segments qui lui sont attribués. Testez l'accès à Internet depuis les réseaux LAN et DMZ. Assurez-vous que les règles spécifiques (SSH, FTP, etc.) fonctionnent comme prévu. Validez l'accès à l'interface Web d'OPNsense via le WAN avec les règles NAT et de pare-feu actives.