Getway

Pour configurer une gateway sous Linux sans interface graphique, nous pouvons utiliser la commande **ip** qui nous permet de configurer les paramètres réseau de notre système. Voici les étapes à suivre :

1. Vérifiez notre configuration réseau actuelle en utilisant la commande **ip a**. Cela nous donnera une liste de toutes les interfaces réseau de notre système, ainsi que leur adresse IP et leur masque de sous-réseau.
2. Définissez l'adresse IP de notre interface réseau en utilisant la commande **ip a add <adresse IP>/<masque de sous-réseau> dev <interface>**. Pour définir, notre l'adresse IP 10.0.0.1 sur l'interface enp0s3 avec un masque de sous-réseau de 24 bits, nous pouvons utiliser la commande suivante : **ip a add 10.0.0.1/24 dev enp0s3**.
3. Définissez la passerelle par défaut en utilisant la commande **ip route add default via adresse IP de la passerelle**. Par exemple, pour définir la passerelle 10.0.0.1 comme passerelle par défaut, nous devons utiliser la commande suivante : **ip route add default via 10.0.0.1**.
4. Vérifiez que notre configuration est correcte en utilisant la commande **ip route**. Cela devrait afficher nos passerelles par défaut ainsi que toutes les routes actuellement définies sur notre système.

Pour protéger notre gateway avec un pare-feu qui respecte les règles de notre entreprise, nous pouvons utiliser **iptables**, qui est un utilitaire de pare-feu intégré à la plupart des distributions Linux. Voici comment configurer un pare-feu avec **iptables** :

1. Faudrait vider les règles existantes du pare-feu en utilisant la commande **iptables -F**.
2. Autoriser les connexions entrantes et sortantes établies et récentes en utilisant les commandes suivantes :

iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

3. Autoriser les connexions entrantes sur les ports ouverts de votre entreprise en utilisant la commande **iptables -A INPUT -p tcp --dport 80 -j ACCEPT**. Par exemple, pour autoriser les connexions entrantes sur le port 80 (HTTP), vous pouvez utiliser la commande `iptables -A INPUT-p tcp --dport 80 -j ACCEPT`. Répétez cette étape pour chaque port ouvert de votre entreprise.
4. Bloquer toutes les autres connexions entrantes en utilisant la commande **iptables -A INPUT -j DROP**.
5. Enregistrer la configuration en utilisant la commande **iptables-save**. Cela enregistrera notre configuration dans un fichier de configuration qui pourra être chargé automatiquement au démarrage de notre système.

Script pour le parfeu

Getway

```
#!/bin/bash #

iptables -F

# Autoriser les connexions entrantes et sortantes établies et récentes

iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

 iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

 # Autoriser les connexions entrantes sur les ports ouverts de l'entreprise

iptables -A INPUT -p tcp --dport 80 -j ACCEPT iptables -A INPUT -p tcp --dport 443 -j ACCEPT

# Bloquer toutes les autres connexions entrantes

 iptables -A INPUT -j DROP

 # Enregistrer la configuration

 iptables-save > /etc/iptables.conf
```

Pour exécuter ce script, on lui donne les droits d'exécution en utilisant la commande **chmod +x script.parfeu** et on l'exécute en utilisant la commande **./script.parfeu**.

Il est également important de s'assurer que les machines de notre réseau ne peuvent pas accéder à Internet s'ils ne sont pas connectés à la gateway.

Pour ce faire, nous pouvons configurer notre pare-feu pour bloquer toutes les connexions sortantes à l'exception de celles passant par la gateway. Nous pouvons utiliser la commande **iptables -A OUTPUT -d 10.0.2.15 -j ACCEPT** pour autoriser les connexions sortantes vers la gateway, et la commande **iptables -A OUTPUT -j DROP** pour bloquer toutes les autres connexions sortantes. On sauvegarde avec la commande

iptables-**save**.

Il est également recommandé de configurer un journal de pare-feu pour enregistrer les tentatives d'accès non autorisées à notre réseau. Nous pouvons utiliser la commande **iptables -A INPUT -j LOG** pour enregistrer les connexions entrantes non autorisées dans le journal de pare-feu. N'oubliez pas de spécifier une règle de pare-feu qui bloque réellement ces connexions, sinon elles seront simplement enregistrées dans le journal sans être bloquées.

Enfin, on n'oublie pas de tester notre pare-feu pour nous assurer qu'il fonctionne correctement et qu'il protège efficacement notre réseau. Nous pouvons utiliser des outils tels que **nmap** ou **hping3** pour tester votre pare-feu et nous assurer qu'il bloque les connexions non autorisées.