Activer le TCPdump sur la STARFACE

La commande Linux « tcpdump » peut être utilisée pour surveiller et enregistrer tout le trafic de données à destination et en provenance de la STARFACE. Le dump peut être affiché directement sur l'écran ou écrit dans un fichier dump. Ce fichier de vidage peut être analysé par la suite avec le programme « Wireshark » (Télécharger le Wireshark).

> **Remarque :** Il est également possible d'activer un TCPdump via l'interface web de STARFACE. Voir en plus État du système de STARFACE.

Pour effectuer un dump TCP sur la STARFACE, les étapes suivantes doivent être effectuées :

1. Se connecter à l'Appliance via ssh
2. Effectuer la connexion avec l'utilisateur root (voir aussi « Mot de passe pour le root-User »)
3. Entrer la commande TCPdump et confirmer avec la touche Entrée
4. Attendre l'enregistrement du cas de défaut.
5. Mettre fin au TCPdump

> **Remarque :** Dans de nombreux scénarios d'erreur (par exemple des problèmes audio), la commande **nohup tcpdump -w dump.pcap -s0 -vv -C50M -Zroot &** peut être utilisée pour enregistrer le flux de données nécessaire à l'analyse et l'écrire dans un fichier.

Les paramètres suivants permettent de préciser davantage la commande TCPdump :

Paramètres	Description
-i **Nom de l'interface**	Spécifie l'interface pour laquelle les paquets de données doivent être enregistrés.
-s0	Spécifie que les paquets de données sont enregistrés dans toute leur longueur.
-w **Nom du fichier**.pcap	Écrit le TCPdump dans un fichier local nommé « **Nom du fichier**.pcap »
-C50M	Spécifie la taille maximale d'un fichier de vidage (par exemple 50 Mo) avant de commencer à écrire dans un nouveau fichier de dump. Le nouveau dossier est identifié par un numéro consécutif.
host **Adresse IP**	Spécification d'une adresse IP unique
port **Numéro de port**	Spécification d'un port unique
-Z**root**	Spécification de l'utilisateur

Quelques exemples de commandes TCPdump :

Commande	Description
tcpdump	Tous les paquets de données en provenance et à destination de STARFACE sont affichés sur le moniteur.
tcpdump -i eth0	Tous les paquets de données en provenance et à destination de la première carte réseau (eth0) de la STARFACE sont affichés sur le moniteur.
tcpdump -i any	Tous les paquets de données en provenance et à destination de chaque interface de STARFACE sont affichés sur le moniteur.
tcpdump port 5060	Tous les paquets de données en provenance et à destination du port 5060 sont affichés sur le moniteur.
tcpdump host 192.168.1.100	Tous les paquets de données à destination et en provenance de l'adresse IP « 192.168.1.100 » sont affichés sur le moniteur.
tcpdump -s0 port 5060 -w test.pcap	Tous les paquets de données à destination et en provenance du port 5060 sont écrits intégralement dans un fichier local appelé « test.pcap ».
tcpdump -s0 host 192.168.2.200 -w 1234.pcap	Tous les paquets de données à destination et en provenance de l'adresse IP « 192.168.2.200 » sont entièrement écrits dans un fichier local appelé « 1234.pcap ».

nohup tcpdump -w dump.pcap -s0 -vv -C50M -Zroot -W 10 -G -C &	Tous les paquets de données en provenance et à destination de STARFACE sont entièrement écrits dans un fichier local appelé « dump.pcap ». Lorsque le fichier de vidage atteint une taille de 50 Mo, l'écriture dans un nouveau fichier marqué d'un numéro séquentiel est lancée. Au total, 10 fichiers de 50 Mo chacun sont écrits et le 11e fichier écrase le premier fichier créé. Le processus est déplacé en arrière-plan, de sorte que l'accès ssh peut être interrompu sans que le processus ne soit interrompu.
nohup tcpdump -s0 -w abcd.pcap &	Tous les paquets de données à destination et en provenance de STARFACE sont entièrement écrits dans un fichier local appelé « abcd.pcap ». Le processus est déplacé en arrière-plan afin que l'accès à ssh puisse être interrompu sans que le processus ne prenne fin.
nohup tcpdump -s0 -w dump.pcap -C50M -Zroot &	Tous les paquets de données en provenance et à destination de STARFACE sont entièrement écrits dans un fichier local appelé « dump.pcap ». Lorsque le fichier de vidage atteint une taille de 50 Mo, l'écriture dans un nouveau fichier marqué d'un numéro séquentiel est lancée. Le processus est déplacé en arrière-plan afin que l'accès à ssh puisse être interrompu sans que le processus ne prenne fin.

La sortie du dump TCP sur le moniteur ou un processus de dump TCP qui n'a pas été déplacé en arrière-plan peut être terminé avec la combinaison de touches **« CTRL + C »**. Un TCPdump s'exécutant en arrière-plan peut être terminé avec la commande suivante :

killall tcpdump

Pour analyser les fichiers dump créés, il est recommandé de les copier via sFTP sur un ordinateur local et de les y ouvrir avec le programme « Wireshark ».

Remarque : Le redémarrage d'un serveur ou d'un service de la STARFACE met également fin à tous les processus de vidage de TCP qui ont été déplacés en arrière-plan.