


TCPdump auf der STARFACE aktivieren


Mit dem Linux-Kommandozeilenbefehl "tcpdump" kann der gesamte Datenverkehr von und zu der STARFACE überwacht und mitgeschnitten werden. Der Dump kann entweder direkt auf dem Monitor ausgegeben werden oder auch in eine Dumpdatei geschrieben werden. Diese Dumpdatei kann mit dem Programm "Wireshark" nachträglich analysiert werden ([Download des Wireshark](#)).

Es gibt auch ein Video, das die grundlegende Erstellung und Speicherung eines TCPdumps erklärt ([Link zum Video](#)).

**Hinweis:** Es ist auch möglich einen TCPdump über die Weboberfläche der STARFACE zu aktivieren. Siehe dazu den [Punkt "Diagnose" im Systemstatus](#).

Um auf der STARFACE einen TCPdump durchzuführen, müssen die folgenden Schritte durchgeführt werden:

- 1. Verbindung via ssh zu der Appliance herstellen
- 2. Login mit dem root-User durchführen (siehe auch ["Passwort für den root-User"](#))
- 3. TCPdump-Befehl eingeben und mit der Enter-Taste bestätigen
- 4. Aufzeichnung des Fehlerfalls abwarten
- 5. TCPdump beenden

**Hinweis:** In vielen Fehlerszenarien (z.B. bei Audioproblemen) kann über den Befehl "nohup tcpdump -w dump.pcap -s0 -vv -C50M -Zroot &" (ohne Anführungszeichen) der zur Analyse notwendige Datenstrom aufgezeichnet und in eine Datei geschrieben werden.

Die folgenden Parameter erlauben es den TCPdump-Befehl weiter zu spezifizieren:

Parameter	Beschreibung
-i <Interfacena me>	Angabe des Interfaces, für das die Datenpakete protokolliert werden sollen.
-s0	Angabe, dass die Datenpakete in vollständiger Länge protokolliert werden.
-w Dateiname. pcap	Schreibt den TCPdump in eine lokale Datei mit dem Namen "Dateiname.pcap"
-C50M	Gibt die Maximalgröße einer Dumpdatei an (z.B. 50MB), bevor begonnen wird in eine neue Dump-Datei zu schreiben. Die neue Datei wird dabei mit einer fortlaufenden Nummer gekennzeichnet.
host IP- Adresse	Angabe einer einzelnen IP-Adresse
port Portnummer	Angabe eines einzelnen Ports
-Zroot	Angabe des Benutzers

Einige Beispiele für TCPdump-Befehle:

Befehl	Beschreibung
tcpdump	Alle Datenpakete von und zur STARFACE werden direkt auf dem Monitor ausgegeben.
tcpdump -i eth0	Alle Datenpakete von und zur der ersten Netzwerkkarte (eth0) der STARFACE werden auf dem Monitor ausgegeben.
tcpdump -i any	Alle Datenpakete von und zur jedem Interface der STARFACE werden auf dem Monitor ausgegeben.
tcpdump port 5060	Alle Datenpakete von und zu dem Port 5060 werden auf dem Monitor ausgegeben.
tcpdump host 192.168.1.100	Alle Datenpakete von und zu der IP-Adresse "192.168.1.100" werden auf dem Monitor ausgegeben.
tcpdump -s0 port 5060 -w test.pcap	Alle Datenpakete von und zu dem Port 5060 werden vollständig in eine lokale Datei mit dem Namen "test.pcap" geschrieben.
tcpdump -s0 host 192.168.2.200 -w 1234.pcap	Alle Datenpakete von und zu der IP-Adresse "192.168.2.200" werden vollständig in eine lokale Datei mit dem Namen "1234.pcap" geschrieben.

nohup tcpdump -w dump.pcap - s0 -vv -C50M - Zroot -W 10 - G -C &	Alle Datenpakete von und zur STARFACE werden vollständig in eine lokale Datei mit dem Namen "dump.pcap" geschrieben. Wenn die Dump-Datei eine Größe von 50MB erreicht, wird begonnen in eine neue Datei zu schreiben, die mit einer fortlaufenden Nummer gekennzeichnet ist. Es werden insgesamt 10 Dateien a 50 MB geschrieben und die 11te Datei überschreibt die erste angelegte Datei wieder. Der Prozess wird dabei in den Hintergrund verschoben, so dass der ssh-Zugriff beendet werden kann ohne dass der Prozess abbricht.
nohup tcpdump -s0 - w abcd.pcap &	Alle Datenpakete von und zur STARFACE werden vollständig in eine lokale Datei mit dem Namen "abcd.pcap" geschrieben. Der Prozess wird dabei in den Hintergrund verschoben, so dass der ssh-Zugriff beendet werden kann ohne dass der Prozess abbricht.
nohup tcpdump -s0 - w dump.pcap - C50M -Zroot &	Alle Datenpakete von und zur STARFACE werden vollständig in eine lokale Datei mit dem Namen "dump.pcap" geschrieben. Wenn die Dump-Datei eine Größe von 50MB erreicht, wird begonnen in eine neue Datei zu schreiben, die mit einer fortlaufenden Nummer gekennzeichnet ist. Der Prozess wird dabei in den Hintergrund verschoben, so dass der ssh-Zugriff beendet werden kann ohne dass der Prozess abbricht.

Die Ausgabe des TCPdumps am Monitor bzw. ein nicht in den Hintergrund verschobener TCPdump-Prozess kann mit der Tastenkombination "STRG + C" beendet werden. Ein TCPdump, der im Hintergrund läuft, kann über den folgenden Befehl beendet werden:

```
killall tcpdump
```

Zur Analyse der erstellten Dump-Dateien wird empfohlen selbige via sFTP auf einen lokalen Rechner zu kopieren und dort mit dem Programm "Wireshark" zu öffnen.



Hinweis: Ein Server- oder Diensteneustart der STARFACE beendet ebenfalls alle in den Hintergrund verschobenen TCPdump-Prozesse.