Opensense Firewall

Beitrag von „ozw00d“ vom 14. Juli 2021, 13:11

firewalls werden immer nach dem selben prinzip konfiguriert.

Erst mal immer ein Deny auf alles und dann pö a pö ein permit auf das was du freigeben möchtest.

Die meisten Firewalls bringen aber ein gutes ruleset mit, welches für den Hausgebrauch ausreicht.

zum beispiel das hier sind rulesets welche man übernehmen kann.

Da OPNSense auch APP based fungieren kann, schaut man sich halt immer am besten die entsprechende Application an und welche Ports verwendet werden.

Ist bei allen anderen Firewalls auch nicht anders 

Ich konfiguriere FWs immer wie folgt:

-> haupt konfiguration -> standard ports zur kommunikation nach außen (Web, Mail)

-> Anwendungsbasierte Konfiguration -> Themen wie Filesharing (SMB, ZIFS, NFS etc.)

-> App Konfiguration -> welche APP darf was (bspw. ist das Messaging via Whatsapp, Social Media wie Facebook etc, bei mir komplett geblockt)

-> Interne Kommunikation ist separat zu betrachten, die regeln sollten hier so konfiguriert werden das eine Interne Kommunikation nicht geblockt (deny) wird.

Daran kann man sich super langhangeln. Wichtig ist das man Rulesets sichert, um bei einem Problem schnell auf eine funktionierende zurück zu kehren.

Hinzu kommt das man nicht mehr als 30 -50 Regeln nutzen sollte, fehler lassen sich dort eher finden als wenn man 300+ Regeln konfiguriert hat.

Hier habe ich noch einen Cheatsheet an dem du dich orientieren kannst.