Opensense Firewall

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

Gibt es empfehlenswerte FAQ / Anleitungen zur Firewall / Konfiguration?

Die Masse an Treffern dazu erschlägt mich, wenn ihr etwas empfehlen könntet wäre das super.

Beitrag von „maybeageek“ vom 14. Juli 2021, 11:42

Wäre die Frage: Was genau willst Du wissen?

Ich setze seit Jahren pfSense und OpnSense ein, und finde das Handbuch eigentlich aussagekräftig genug falls ich was nachlesen will.

DocumentationWiki

Beitrag von „Canyonwalker“ vom 14. Juli 2021, 12:11

Aktuell sehe ich den Wald vor lauter Bäumen nicht.

Gestern habe ich das System installiert und es läuft, wenn auch aktuell nur mit einer Schnittstelle. Dazu gibt es einen sep. Beitrag.

Es soll zunächst als vernünftige Firewall laufen.

Aktuell habe ich einen PI-Hole im Netz.

Obwohl ich nur eine Schnittstelle am Opensense habe, habe ich Zugriff ins Internet. Schön für den Augenblick,(

aber da ist die Konfiguration für Gateway, DHCP und DNS aktuell falsch, werde ich irgendwie hinbekommen wenn die 2. Schnittstelle erkannt ist.

Wie aber konfiguriere ich die Firewall richtig?

Was macht darüberhinaus Sinn?

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.

Beitrag von „roqueeee“ vom 14. Juli 2021, 23:08

Von mir auch ein +1 für das offizielle Wiki. Damit sollten sich eigtl. alle Standardfragen beantworten lassen.

Wie ozw00d schon geschrieben hat blockiert OPNsense grundsätzlich erstmal jeden Traffic außer du erlaubst es. Eine Ausnahme sind hier allerdings die Default Rules am LAN interface.

Bei mir ersetzt OPNsense z.B. Pihole. Dafür benutze ich Unbound + Blacklist, allerdings muss man dann auf das schöne Dashboard von Pihole verzichten.

Traffic Shaping mit FQCoDel kann auch sinnvoll sein. Noch schöner wäre cake, das existiert aber leider nicht bei FreeBSD.

Grundsätzlich gibt es unzählige Möglichkeiten OPNsense sinnvoll einzusetzen. Das hängt letzten Endes davon ab, was du mit einer Firewall erreichen willst.

Beitrag von „Canyonwalker“ vom 19. Juli 2021, 17:08

Irgendetwas lief bei mir falsch, entweder war es ein Gateway oder ein Verweis darauf oder DNS oder DHCP, nun läuft es, hoffe das bleibt auch so.

Thema Firewall Regel schaue ich mir gleich noch mal an,)

Eine Sicherung hab ich erstellt, denn……..

Morgen gibt es dann den POE AP und einen passenden Switch, dann kann ich WLAN der FB deaktivieren und ggfls auch DHCP, falls es dort aktiv ist?
Wenn das läuft soll es mit weiteren Modulen weitergehen.

Antivirusprogramm und eine geographische Anzeige der IP wären schön, aber nur wenn sowas ohne x Datenbanken und 1000 andere Sachen geht. Gibt es etwas „einfach“ zu aktivierendes?

Was ich damit machen will, gute Frage ich habe ja keine Ahnung was da alles geht. Bin kein Netzwerkprofi, viele Begriffe sagen mir aktuell noch nichts. Die Firewall läuft, wo ich nun welche Daten angezeigt bekomme und welche für mich interessant/wichtig sind/sein könnten ist mir noch ein Rätsel.

Ist einfach verdammt viel neuer Input/Daten.

Woran erkenne ich denn das Wichtige, bzw. Wie finde ich es und wo?

Beitrag von „Canyonwalker“ vom 27. Juli 2021, 23:52

Nachdem ich mich nun schon seit ein paar Tagen mit der OpnSense beschäftige kann ich sagen, es ist eigentlich gar nicht so schwer.

Heute habe ich es auf einer neuen Hardware, Marke AWOW (<200 Euro) mit zwei onboard Netzwerkschnittstellen installiert. In weniger als einer Stunde lief das System mit den Defaulteinstellungen. Also nur Mut, ist gut zu schaffen,))

Lediglich der Lüfter nervt etwas, da er aus welchem Grund auch immer, immer wieder kurz anläuft. CPU Usage ist so bei ca. 35 %, warum auch immer. Eigentlich läuft gerade fast nichts?

Mal schauen was da für ein billiger Lüfter verbaut ist, den kann man mit Sicherheit tauschen;)

Da ein Bild mehr als 1000 Worte sagt, hier mal ein Snapshot des Web Interface der OPNsense.

Beitrag von „apfel-baum“ vom 28. Juli 2021, 15:54

das ist klasse,- und wie schaut es mit der fritte und deren diensten aus?  ist die nun im modem-only-modus?

Beitrag von „Canyonwalker“ vom 28. Juli 2021, 16:07

Die FB hat jetzt nur noch Dect und ist in einem AVM Mode der ähnliches bewirken soll, wo genau der Unterschied liegt, frag mich nicht.

Um das zu verstehen fehlt mir aktuell das nötige Knowhow.

Für mich ist/war wichtig es geht.

Wlan ist auf der FB deaktiviert und läuft über einen AP der via Switch an der Firewall hängt.

Das Dashboard zu Opnsense ist super, man kann sich die gewünschten Dinge einfach so reinziehen,))

Beitrag von „apfel-baum“ vom 28. Juli 2021, 16:11

dankesehr dafür  , hm vielleicht hier auch irgendwann in der art  mal gucken