Traffic - Regeln by Naichbindas

Was wollen wir?

Die Unifi Firewall ergänzen bzw verfeinern oder auch präzisieren.

Warum wollen wir das?

Damit erleichtern wir uns die tägliche Arbeit mit unserem Unifi System.

Abläufe sollen rund laufen und korrekt gesteuert werden.

Kurz gesagt soll in unserer Routine ein wenig professionalität rein kommen.

Wir sparen uns viele einzelne Firewallregeln ein. Das geht jetzt kompakter.

Und wir brauchen nicht mehr mit IP-Gruppen arbeiten.

All das können wir direkt mit ein arbeiten, beim erstellen der Regeln.

Und wie geht das genau?

Mit Traffic-Regeln, wie ich finde ein Fluch und Segen zugleich.

Eigene Regeln mit erstellen mit wenigen Mausklicks.

Hallo

Ich knüpfe hier an folgenden zuvor eingerichteten Firewallregeln an:

Firewall-Regeln by Naichbindas

Wir haben uns schon gefragt wozu diese Traffic-Regeln gedacht und gut sind.

Unifi kündigt seine zuvor genannten "Traffic-Rules" mit folgender Botschaft an,

ich zitiere:

"Verwenden Sie Traffic Rules als Firewall der nächsten Generation,

die über erweiterte Sicherheitsfilterung verfügt,

um bestimmten Datenverkehr zu blockieren,

zuzulassen oder die Geschwindigkeit zu begrenzen."

Ich versuche hier ein wenig Licht ins Dunkel zu bringen und

aufzuzeigen das es doch einen Haken gibt aber auch Vorteile.

Zu den Vorteilen komme ich gleich:

Wir brauchen keine Reihenfolge mehr einhalten, "Zulassen vor Blockieren" entfällt,

Mehrfachauswahl ist möglich, wie "Geräte", "Apps" und "App-Gruppen", oder "Netzwerke".

Das erleichtert uns mehreres in einer Regel zusammen zu fassen und nicht alles einzeln.

Ich brauche keine IP-Gruppen, Port-Gruppen (Profile) mehr anlegen.

Das passiert gleich in der Config dann mit. Nennt sich aber "Anschluss", nicht "Port".

und zu den Nachteilen komme ich später:

Fangen wir mal an:

Viele erinnern sich vlt. noch das mann unter "Firewall", diese Regeln angelegt hatt.

Akzeptieren - Alle - LAN In - erlaube etablierte / verbundene Sitzungen

Drop - Alle - LAN In - alle ungültigen Zustände löschen

Akzeptieren - Alle - LAN In - erlaube dem MGMT-LAN den Zugriff auf alle VLANs

Akzeptieren - Alle - LAN In - erlaube lokales DNS

Drop - Alle - LAN In - blockiere Heim LAN den Zugriff auf MGMT Lan

Drop - Alle - LAN In - blockiere IoT LAN den Zugriff auf MGMT Lan

Drop - Alle - LAN In - blockiere Gast LAN den Zugriff auf MGMT Lan

Drop - Alle - LAN In - blockiert die gesamte Kommunikation zwischen VLANs

und vlt auch diese dann noch:

Drop - Alle - LAN In - blockiere Heim LAN den Zugriff auf IoT Lan

Drop - Alle - LAN In - blockiere Heim LAN den Zugriff auf CAM Lan

Drop - Alle - LAN In - blockiere IOT LAN den Zugriff auf Heim Lan

Drop - Alle - LAN In - blockiere IOT LAN den Zugriff auf CAM Lan

Drop - Alle - LAN In - blockiere Gast LAN den Zugriff auf Heim Lan

Drop - Alle - LAN In - blockiere Gast LAN den Zugriff auf IOT Lan

Wenn dann mehrere Netzwerke und evtl. verschiedene Endgeräte noch ins Spiel kommen,

wie "NAS" und "Pihole", da kommen schnell ein paar Regeln zusammen

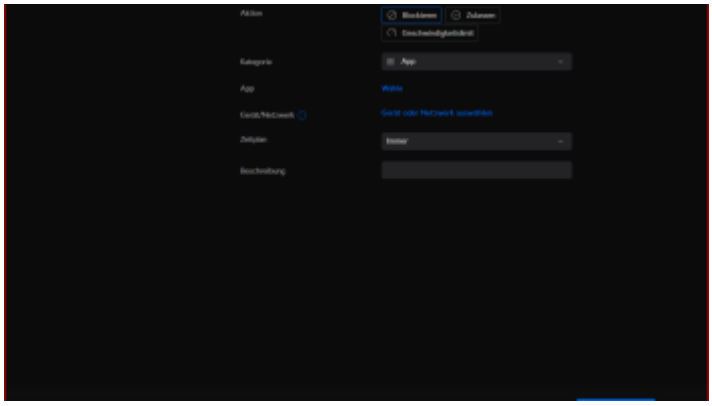
und verliert auch schon mal den Überblick.

Jetzt kommen die "Traffic-Regeln" zum Einsatz:

Wir gehen dazu auf Einstellungen, - Sicherheit, - Traffic Regeln.

Dort gehen wir dann auf erstellen und finden eine Eingabemaske vor.

Die sieht folgendermaßen aus:



Unter Aktion haben wir folgende drei Möglichkeiten:

Blockieren :

Wie der Name schon sagt, hier blockieren oder verbieten wir etwas,

Zulassen :

Hier gestatten oder besser gesagt erlauben wir etwas,

Geschwindigkeit :

Hier können wir etwas an der Geschwindigkeit bzw. Bandbreite drehen im Down und Upload.

Bei der Kategorie können wir dan folgendes auswählen:

App :

Hier kann dann einzelne oder mehrere Apps aus einer Liste auswählt und

mit den zuvor genannten "Actionen" verknüpft werden.

App Gruppe :

Hier kann ich gleich ganze Gruppen von Apps auswählen die zu einem Thema gehören.

(Sozial Media, Online Spiele und so weiter)

Domain-Name :

Damit sind Domain Namen gemeint, aus denen also eine Web-URL besteht.

(z. Bsp. rtl.de, google.de)

IP Adressen :

Dort trage ich dann IP Adressen ein aus dem lokalem Netzwerk um dann wie

bei den Aktionen eingestellt, zu verfahren.

Region :

Um Ländergrenzen einzustellen wohin ich Zugrifff haben darf oder nicht,

sowie was umgekehrt auch wieder rein kommt oder geblockt wird.

Internet :

Hier kann ich regeln, wie mit dem Internet verfahren werden soll.

Sperre ich ein LAN oder ein Gerät aus dem Internet aus? Hier geht das.

Lokales Netzwerk :

Auch hier gibt es nette Spielereien seine Netzwerke / Vlans zu beregeln,

dort habe ich dann noch drei weitere Unterkategorien.

- "Traffic zu und von allen lokalen Netzwerken"
- "Traffic von allen lokalen Netzwerken"
- "Traffic zu allen lokalen Netzwerken"

Zur letzteren gehe ich zuerst näher drauf ein.

Um nicht diese ganzen Firewallregeln so aufwändig zu gestalten,

ist hier in "Traffic-Regeln" der Punkt "Lokales Netzwerk" ein guter Helfer.

Achtung: Hier bitte keinen, (oder noch nicht), DNS Server eintragen unter Netzwerke.

Da sollten die DNS Server von Unifi drinnen sein.

Sonst geht erst mal nur das Internet nicht mehr, weil dann euer DNS-Server nicht mehr erreichbar ist.

Das ist aber nur dann der Fall, wenn Ihr schon einen DNS Server im Netzerk habt,

und meine Einstellungen nachvollzieht !!!

(Der Grund wird weiter unten beim Eintragen eines DNS-Server´s erläutert)

Oben nehmen wir blockieren, weil wir die Netze abschotten wollen.

Hier wähle ich dann unter "lokales Netzwerk" - Heimnetz aus,

unter "Traffic Richtung" gehe ich auf - Traffic zu und von allen lokalen Netzwerken,

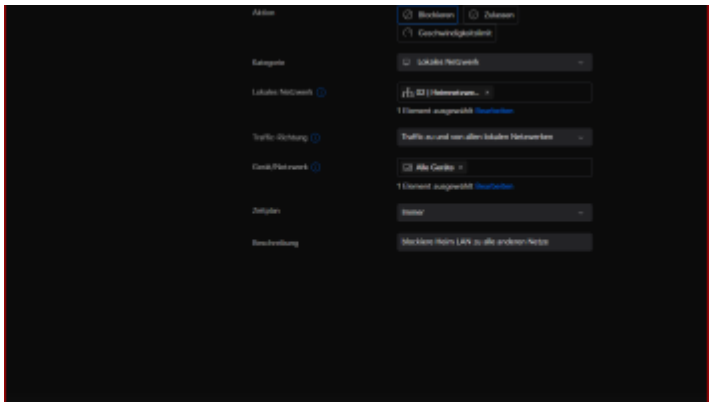
dann unter "Gerät / Netzwerk" wählen wir - alle Geräte aus,

"Zeitplan" steht auf - Immer und zum Schluss geben wir dem Kind noch einen Namen

unter dem Punkt "Beschreibung" - blockiere Heim LAN zu alle anderen Netze.

Dann noch Regel hinzufügen also speichern.

Hier ein Beispiel wie es bei euch aussehen könnte:



Genauso macht ihr das dann mit euren weiteren Netzwerken.

Ihr wiederholt einfach die zuvor genannten Schritte, müsst dann nur

anstatt "Heimnetzwerk", das "IOT", und "GAST" und so weiter auswählen.

Kommt drauf an wie viele Netzwerke ihr habt.

Der Vorteil hierbei ist das ich mit einer Regel gleich sagen könnt, das wie im meinem Beispiel

das "Heimnetz" nur mit sich selber reden darf und nicht mit anderen Netzen inklusive dem MGMT LAN.

Somit muss ich nicht jede einzelne Regel in der Firewall erstellen, so wie am Anfang erwähnt.

Im nächsten Schritt erfahren wir wie Geräten, der Zugriff auf andere erlaubt werden darf:

Zuerst nehmen wir diesmal "Zulassen",

Ich wähle in diesem Falle die Kategorie "IP Adresse" aus,

bei IP Adresse, trage ich das Objeckt der Begierde - die IP ein im meinem Fall,

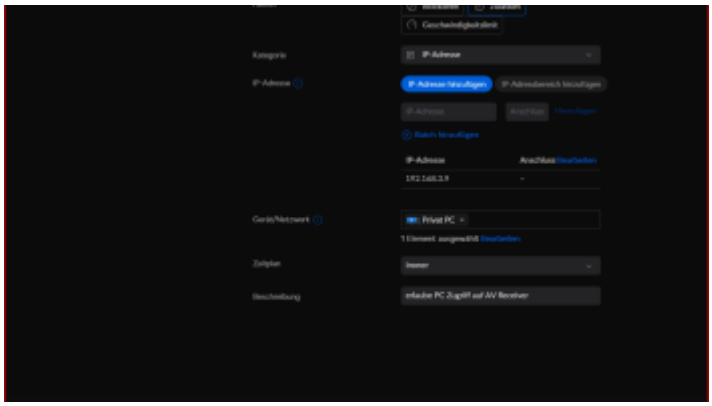
nehme ich mal einen "AV Receiver".

Unter "Gerät / Netzwerk" suche ich mir ein Gerät aus wer der Glückliche sein darf, bei mir mal der PC.

"Zeitplan" steht auch hier wieder auf - immer.

Und als "Beschreibung" kommt dann rein was ich da angestellt habe.

So würde das dann aussehen:



Speichern nicht vergessen und dann sollte der Zugriff auf das Gerät möglich sein.

Hier kann man nach belieben verfahren, blockieren, erlauben oder beschränken.

So könnt Ihr mit dem Rest auch verfügen, mit "App", "App-Gruppe", "Domain-Name", "Region" und "Internet"

Hier kommt dann allerdings der zuvor besagte "Haken"

Die letzteren funktionieren leider nur mit "UNIFI DNS".

Wer einen "Pihole oder Adgard und Co" benutzt wird mit diesen Regeln leider nix erreichen.

Lokales Netzwerk und IP Adresse funktionieren aber.

Machen wir mit einem Eintrag aus "IP-Adresse" und "Port" weiter:

Hierzu gehen wir wieder auf "Eintrag erstellen", auf "Zulassen" klicken,

wählen unter "Kategorie" den Reiter "IP-Adresse" aus,

trage die IP Adresse des Pihole ein, und unter Anschluß kommt der "Port 53" rein.

Mit dieser Einstellung kann ich gewährleisten das die Clients mit "DNS" arbeiten können,

aber nicht auf die Weboberfläche meines "DNS Server´s" wie "Pihole, Adguard" dürfen.

Bei Gerät / Netzwerk nehmen wir dann alle Geräte oder nur einzelne Netzwerke oder

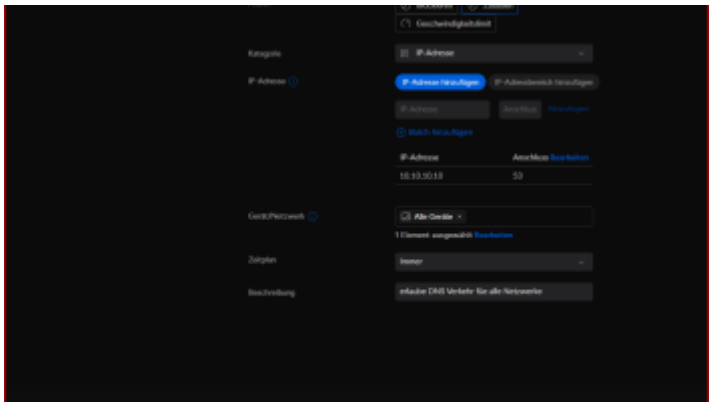
einzelne bzw. mehrere Geräte, das könnt Ihr euch aussuchen.

Beim "Zeitplan" - Immer einstellen.

Beschreibung zum Beispiel "erlaube DNS Verkehr für alle Netzwerke"

Speichern fertig.

Das müsste dann so aussehen, wie hier im Beispiel.



Wenn Ihr aber auch wollt das ein "Admin-PC" auf die Weboberfläche darf,

Dann erstellt noch eine weitere Regel die fast mit der voran gegangenen

identisch ist. Last nur den Port unter "Anschluss" weg.

Bei Gerät / Netzwerk nur den Admin-PC auswählen und Beschreibung einfügen.

Nur noch speichern und der PC darf als Admin Gerät dann auch auf die Weboberfläche.

Erst dann in den Netzwerken unter "DNS" die IP Adresse eintragen.

Sonst haben die Netze vorher kein Internet mehr, wenn man die DNS Server vorher drinn hatt,

und aber schon meine hier beschrieben "Traffic-Regeln" umgesetzt hatt.

So viel Spaß damit, ich hoffe das hilft ein wenig weiter.

Disclaimer: Alle Anleitungen/Tutorials sind nach bestem Wissen und Gewissen verfasst, gehen immer von den definierten Software/Firmware-Versionen aus und sind auf das englische GUI ausgelegt.

Es gibt keine Garantien auf Erfolg. Im Falle eines Misserfolges hilft aber sicherlich die Community hier immer weiter.

Keiner der Autoren oder der Betreiber des Forums ist für die aus der Nutzung resultierenden Probleme/Herausforderungen verantwortlich.

Jegliche hier beschriebenen Schritte erfolgen ausnahmslos in eigener Verantwortung des Durchführenden. Eltern haften für ihre Kinder.

Auswählen:

Gültige Software-Version Keine Firmware-Relevanz!