Firewall-Regeln by Naichbindas

Was wollen wir?

Die Unifi Firewall mal ganz anders nutzen.

Warum wollen wir das?

Unifi hat seit geraumer Zeit neben der üblichen Firewall, noch etwas mehr zu bieten. Das wird angepriesen als Traffic-Regeln, und 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."

"Wie unterscheiden sich Traffic-Regeln von Firewall-Regeln?

Firewall-Regeln werden im Allgemeinen verwendet, um bestimmte Ports und IP-Adressen abzugleichen.

Traffic-Regeln können nach Kategorien wie einer App oder einer Domain abgeglichen werden und ermöglichen Ihnen, den Datenverkehr auf intuitive und optimierte Weise zu filtern."

Daher setzen wir uns hier damit mal auseinander.

Und wie geht das genau?

Wir kombinieren halt beides. Firewall- und Traffic Regeln. Ein mächtiges Werkzeug.

Ich habe halt im Internet mir diverse Webseiten und Videos angeschaut und bin da auf etwas gestoßen

was ich auch so umgesetzt habe und euch daran teil haben lassen möchte.

Darum möchte auch gerne mal meinen Senf dazu geben wie die Firewall und deren Einrichtung aussehen könnte.

Auch habe ich hier bewusst auf Pihole und andere Geschichten verzichtet oder weg gelassen.

Das sind alles weitere Sachen die aber erstmal mehr als das Grundprinzip hinaus gehen und Verwirrung stiften könnten,

wie jemanden der keinen hatt oder neu in der Materie Unifi und Netzwerke sowie Firewall und Co ist.

Fangen wir mal an.

Gehen wir mal davon aus, ganz klassisch das MGMT Lan 192.168.1.0/24 als Standard ist.

Dann legen wir mal als Beispiel folgende VLAN´s an.

1. Heimnetz 192.168.2.0/24

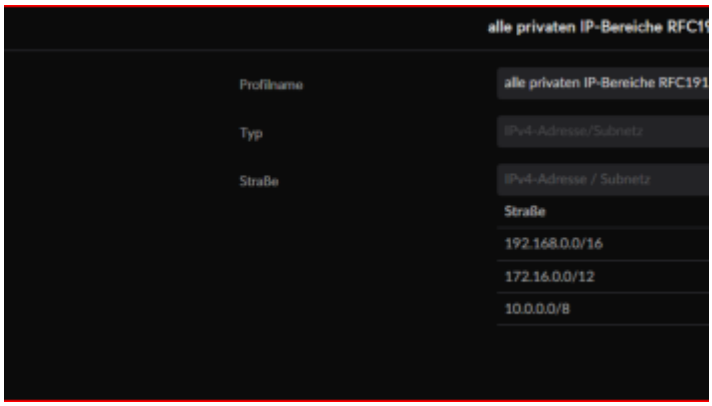
2. IOT 192.168.3.0/24

3. Gäste 192.168.8.0/24

Dazu habt ihr evtl. die entsprechenden WLAN´s dazu eingerichtet.

Jetzt legen wir unter "Einstellungen" - "Profile" - "IP-Gruppen", folgende Gruppen an:

(Hänge das als Bilder drann weil die sind ja selbst erklärend.)



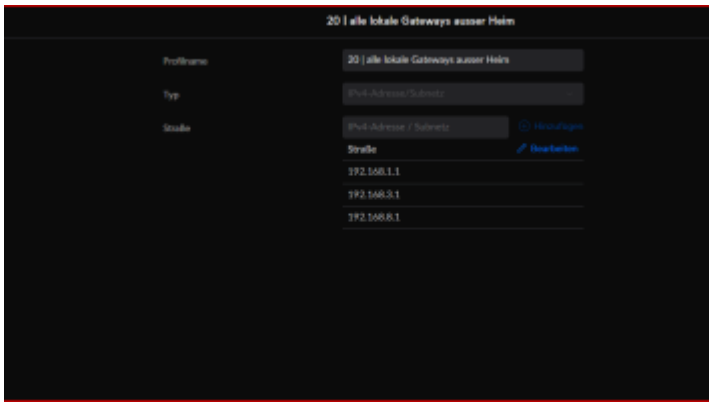
Diese IP Bereiche decken halt sämtliche privaten nutzbaren Adressen ab,

und erleichtert uns die Arbeit falls später weitere Netze / VLAN´s hinzukommen.

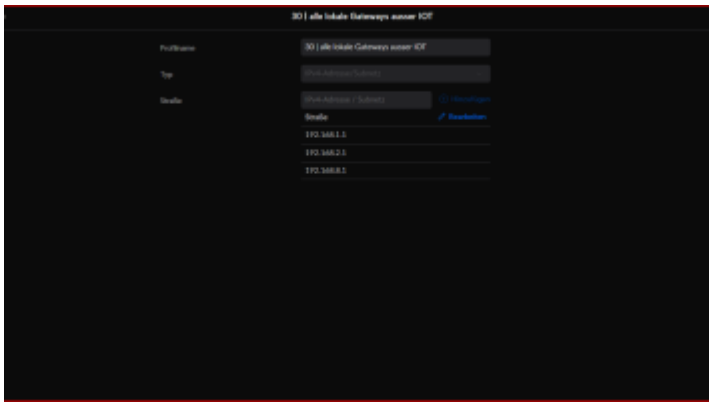
Somit haben wir das schonmal abgedeckt und müssen später auch nicht nachbessern,

mit weiteren Netzwerk- und oder Gateway Adressen.

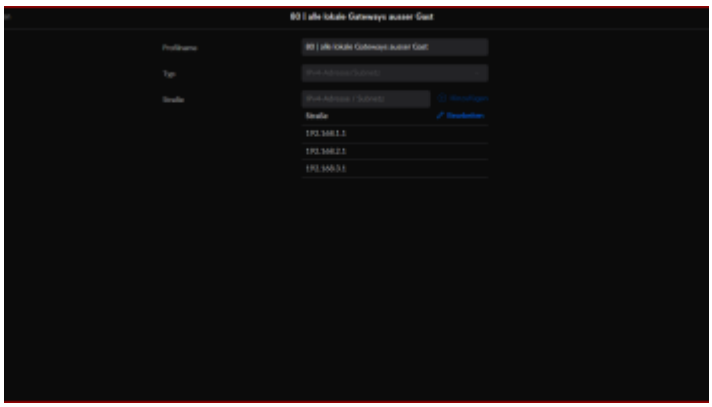
Dann ist es halt einfacher und schon alles vorbereitet.



Hier kommen alles ausser Heimnetz rein.

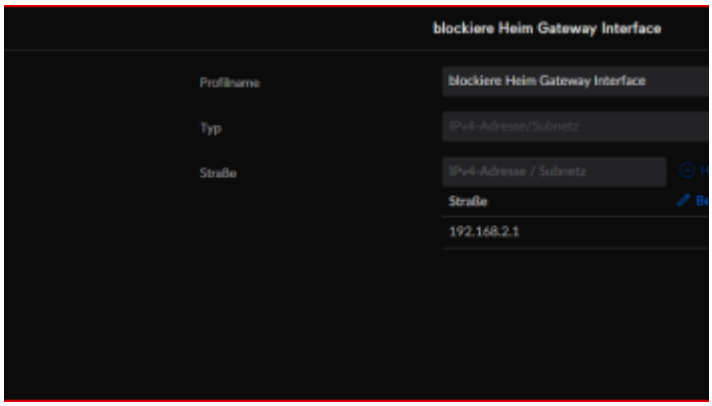


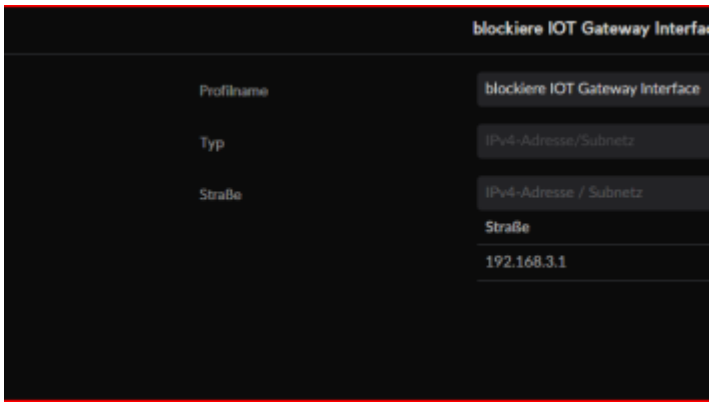
Hier kommen alle ausser IOT rein.



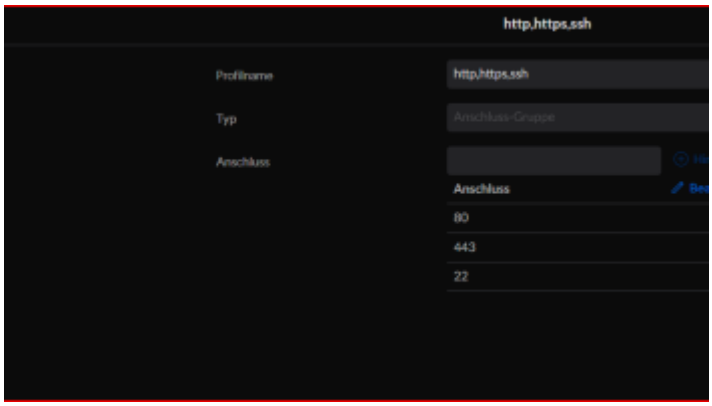
und hier kommen alle ausser Gast rein.

Dann brauchen wir noch:





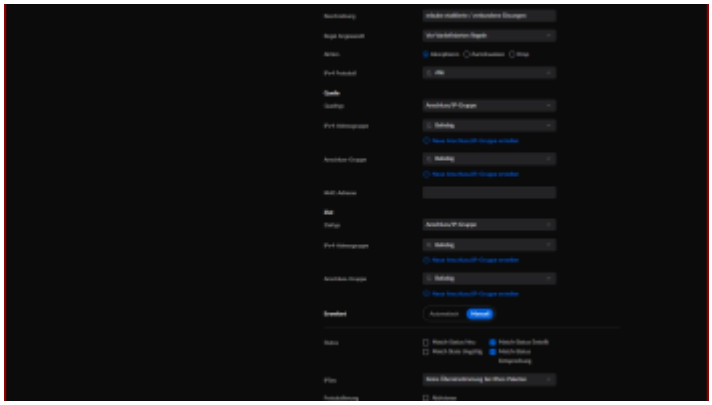
Zu guter letzt legen wir noch eine Gruppe an.....:

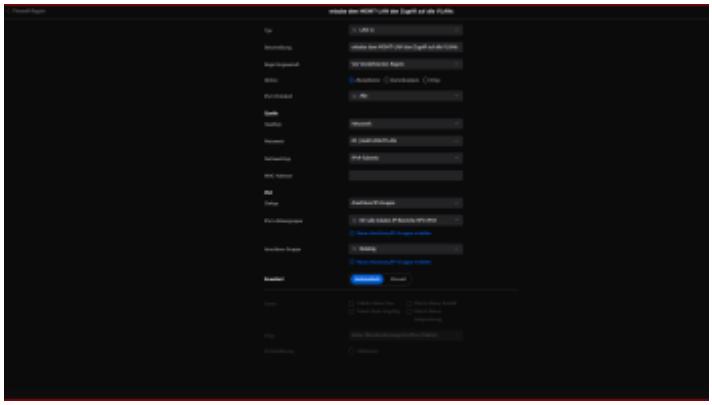


Damit können wir dann arbeiten und unser System sicher machen.

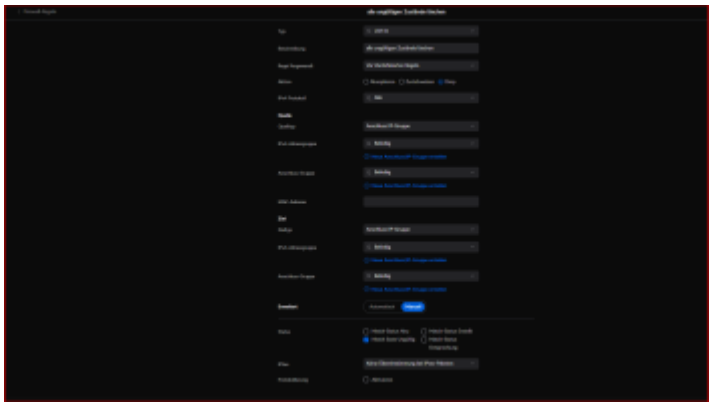
Unter Einstellungen - Anwendungs-Firewall - Firewall-Regeln, wählen wir den Reiter LAN aus.

Dann unten auf "Eintrag erstellen" gehen und folgende Regel´n in "LAN In" erstellen:


und abspeichern. Das ist die Regel "erlaube etablierte / verbundene Sitzungen".

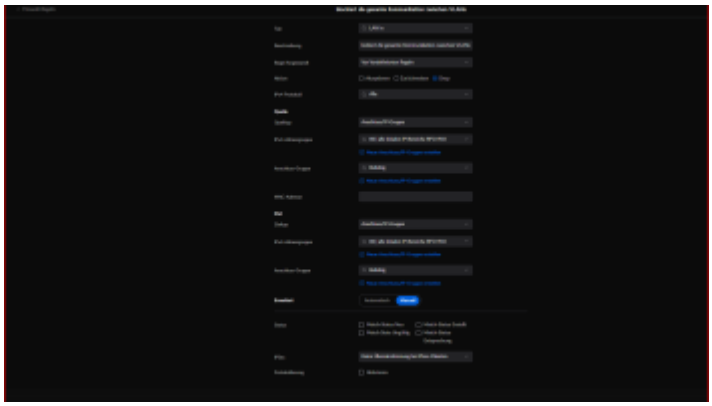


auch abspeichern. Das ist die Regel "erlaube dem MGMT-LAN den Zugriff auf alle VLANs".



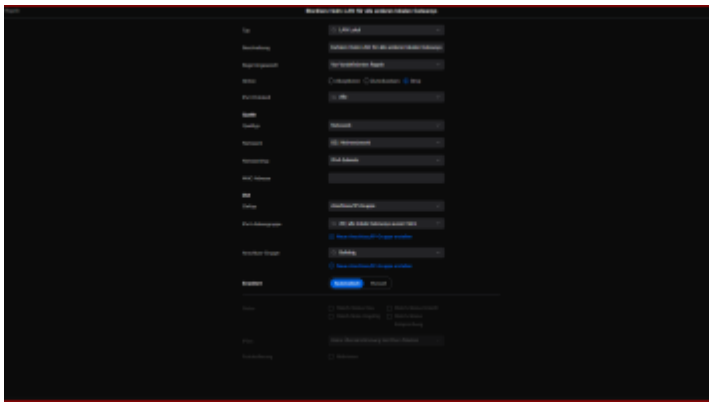
das speichern nicht vergessen. Das ist eine neue Regel für "alle ungültigen Zustände löschen".

Damit wird alles was nicht mehr gültig ist terminiert, also getrennt.



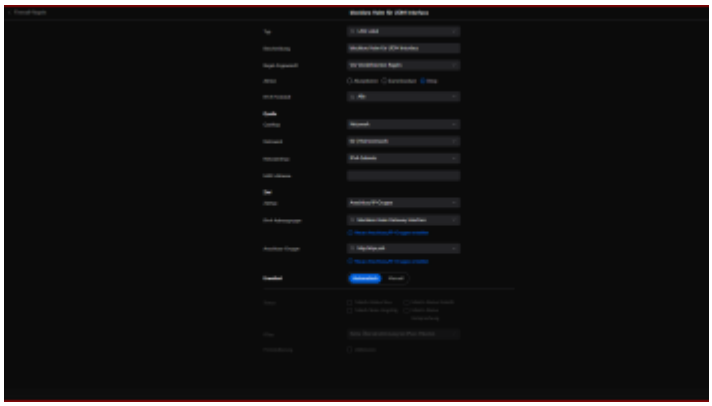
und zum Schluss wieder speichern. Das ist die Regel "blockiert die gesamte Kommunikation zwischen VLANs".

Die weiteren Einträge werden jetzt unter "LAN Lokal" eingetragen:



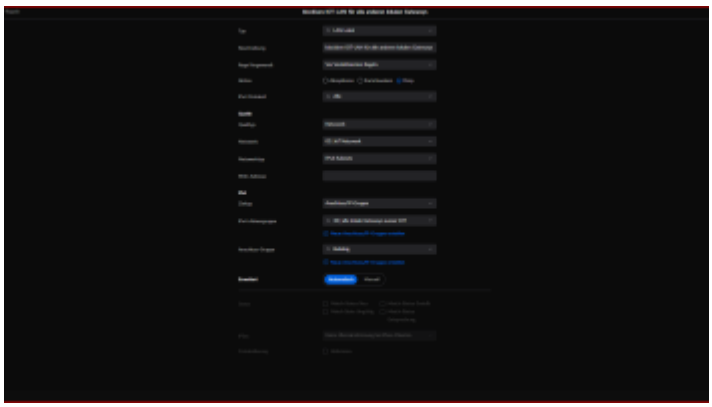
Hier blockieren wir das Heimnetzwerk für alle anderen Gateway´s.

Aber da fehlt ja noch etwas, das machen wir jetzt mit der nächsten Regel.

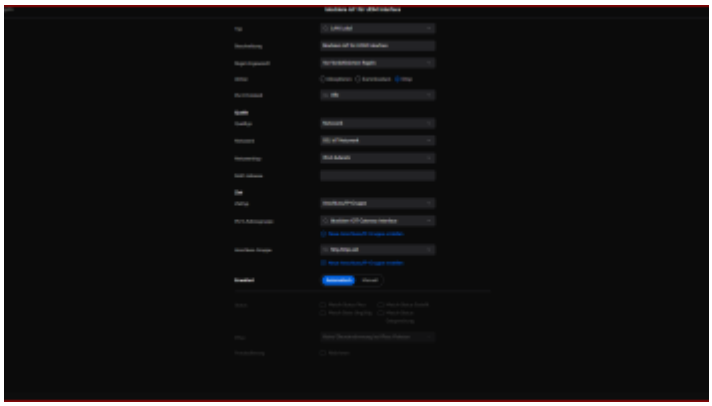


Damit blockieren wir den Endgeräten aus diesem Netzwerk / VLAN den Zugriff auf das eigene Gateway.

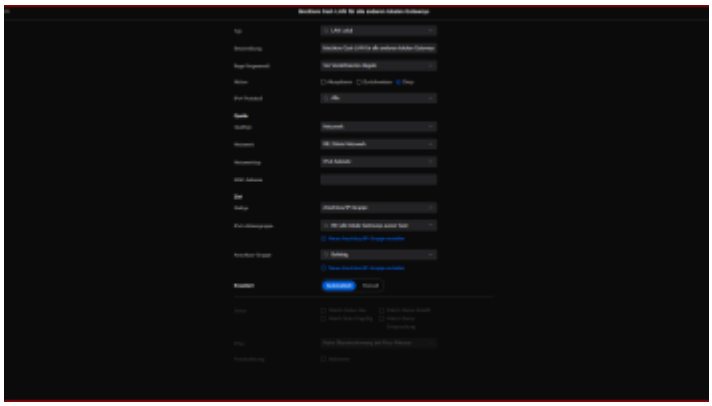
Das gleiche machen wir jetzt noch mit IOT und Gast.



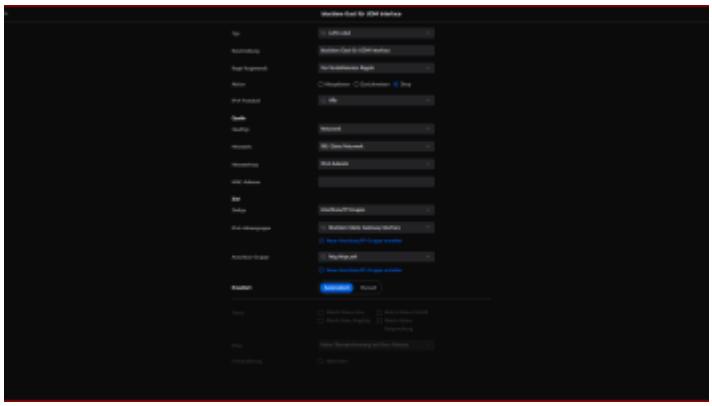
Gesperrt wird wieder der Zugriff auf die anderen Gateway´s.



Damit blockieren wir den Endgeräten aus diesem Netzwerk / VLAN den Zugriff auf das eigene Gateway.



Wieder der Zugriff auf die anderen Gateway´s gesperrt.



Damit blockieren wir den Endgeräten aus diesem Netzwerk / VLAN den Zugriff auf das eigene Gateway.

Somit haben wir das Grundgerüst erstellt und einsatzbereit.

Wir haben die VLAN´s untereinander abgeschottet und die Gateway´s gegen Zugriff der Endgeräte verhindert.

Den Rest kann man etwas anders einrichten, als wie wir das bisher gewohnt waren.

Das ganze machen wir jetzt "Traffic-Regeln":

Dort greifen wir sensibler in die Materie ein um gezielter blockieren,

zulassen oder sogar die Geschwindigkeit zu steuern.

Hier können wir für einzelne Geräte oder ganze Netzwerk-Regeln erstellen,

ob ich Zugriff auf eine Resource habe oder nicht.

Es können geregelt werden, welche Geräte mit einander reden dürfen oder auch nicht,

welche App´s erlaubt sind oder nicht,

ob Internet erlaubt ist oder nicht und so weiter, aber das wird ein weiterer Wiki Eintrag werden.

Jedenfalls soll uns das ganze dabei helfen weitere Regeln mit wenigen Klick´s zu erstellen, zum täglichen Gebrauch.

Sonst haben wir das ja immer direkt in den Firewallregeln unter "LAN In", aufwändiger gemacht.

Hier geht es dann weiter wie versprochen : Traffic - Regeln by Naichbindas

Ich hoffe euch damit weiter helfen zu können.

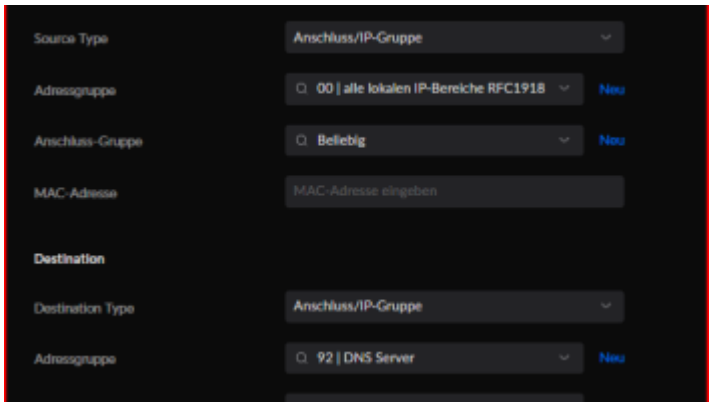
nun viel Spaß beim Networken... 

PS: Weil gewünscht füge ich hier doch noch eine Regel hinzu um einen Pihole zu betreiben.

Mache aber ebend nur einen Screenshot, denn ich denke das sollte als Erklärung reichen.

Vorher bitte noch unter Profile eine Gruppe anlegen die sich da DNS Server

nennt und eine wo die DNS Ports reinkommen.



Achtung wer dann noch mit Traffic-Regeln arbeitet muss unter Umständen

dann dort noch eine weitere Regel für den DNS Traffic einstellen.

Ist aber im dortigen tread erklärt.

Mfg

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!