Firewall-Regeln____old!!!! by EJ

Was wollen wir?

Firewall-Regeln erstellen, um unsere Subnetze gegeneinander abzusichern.

Warum wollen wir das?

Gäste in unserem Gast-Subnetz, USER aus anderen Subnetzen und/oder Geräte aus unserem IoT-Subnetz sollen nicht unberechtigte Zugriffe auf z.B. unser Admin-LAN oder auf Geräte in unserem NETZWERK erhalten. Die Kommunikation über Subnetz-Grenzen soll grundsätzlich verhindert, Ausnahmen jedoch ermöglicht werden.

Und wie geht das genau?

Im zugrundeliegenden Beispiel besteht unser Netzwerk aus drei Subnetzen;

LAN 1 (10.10.1.0/24) ist das Admin-LAN

LAN IoT (10.10.2.0/24) ist das LAN für das „Internet der Dinge“

LAN Gäste (10.10.3.0/24) ist das Gäste-LAN

WLAN-Netze besitzen eine Verbindung zu den zugehörigen LAN’s.

Deshalb werden die WLAN’s von den Firewall-Regeln mit erfasst.

Anzahl der Subnetze und die IP-Bereiche sind entsprechend eurer Situation vor Ort anzupassen.

Die hier beschriebenen Einstellungen sind im „Classic Mode“ durchzuführen, und beziehen sich auf die englische Controller-Oberfläche. Die Regeln werden als **Rules IPv4** definiert.

LOS GEHT's

Wir beginnen mit einer Firewall-Regel, die Datenpaketen, die zu bereits bestehenden (established) Verbindungen oder Datenpaketen die im Bezug (related) zu einer bestehenden Verbindung stehen, erlaubt die Regelprüfung zu umgehen.

Regel 1 „allow established/related sessions“:

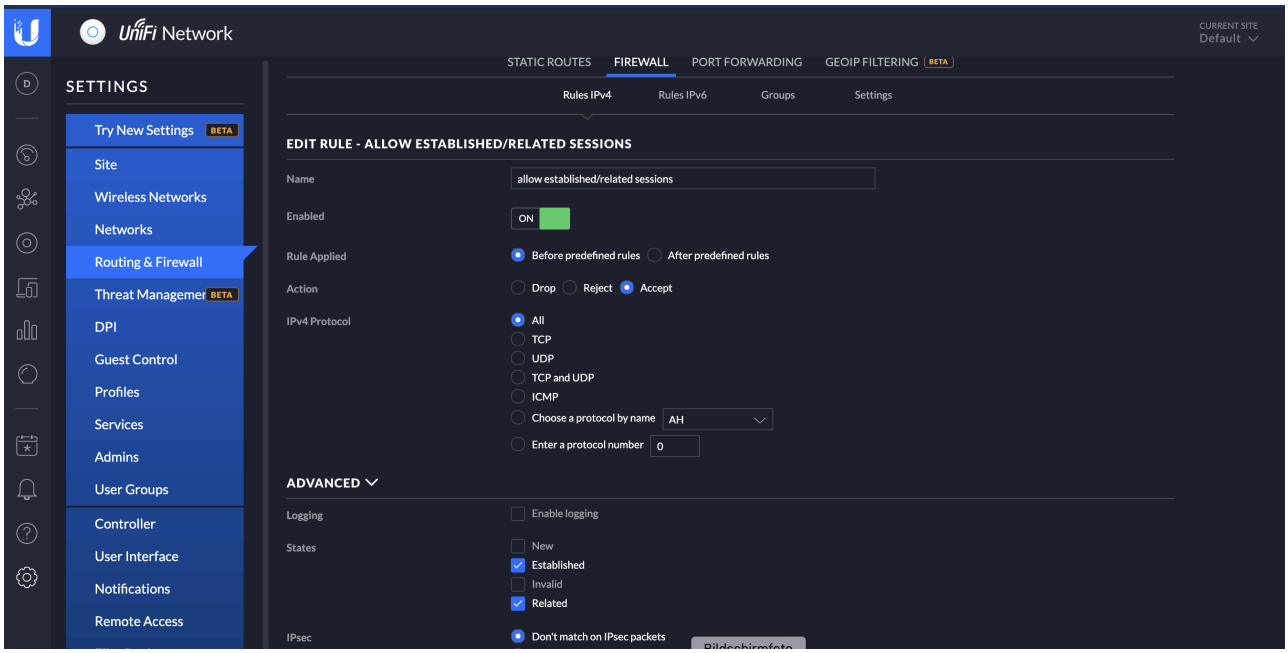
SETTINGS>Routing & Firewall>FIREWALL>LAN IN>CREATE NEW RULE

Name>>>allow established/related sessions

Action>>>Accept

States>>>Established, Related

>>mit Save abspeichern<<



Ohne einschränkende Firewall-Regeln kommunizieren die in unserem Netzwerk angelegten Subnetze untereinander.

USER die sich z.B. im LAN Gäste befinden, können auf die anderen Subnetze zugreifen und die dort eingebuchten Geräte ausfindig machen und im schlechtesten aller Fälle angreifen.

Diese Kommunikation zwischen allen Subnetzen wollen wir unterbinden.

Um uns das Erstellen von Firewall-Regeln zu erleichtern, benutzen wir zusätzlich Gruppen, auf die wir dann unsere Regeln anwenden können.

In der ersten Gruppe definieren wir die möglichen, privaten IP-Bereiche nach dem Standard RFC1918.

Private IP-Bereiche sollen ausnahmslos nach diesem Standard definiert sein:

192.168.0.0/16

172.16.0.0/12

10.0.0.0/8

Grundsätzlich reicht es hier die tatsächlich in unserem Netzwerk benutzten IP-Bereiche der Subnetze in die Gruppe einzutragen.

Um aber für die Zukunft flexibler zu sein, tragen wir vorsorglich alle drei IP-Bereiche ein.

Somit können wir später das Netzwerk um weitere IP-Adress-Bereiche erweitern, ohne diese Firewall-Regel anpassen zu müssen.

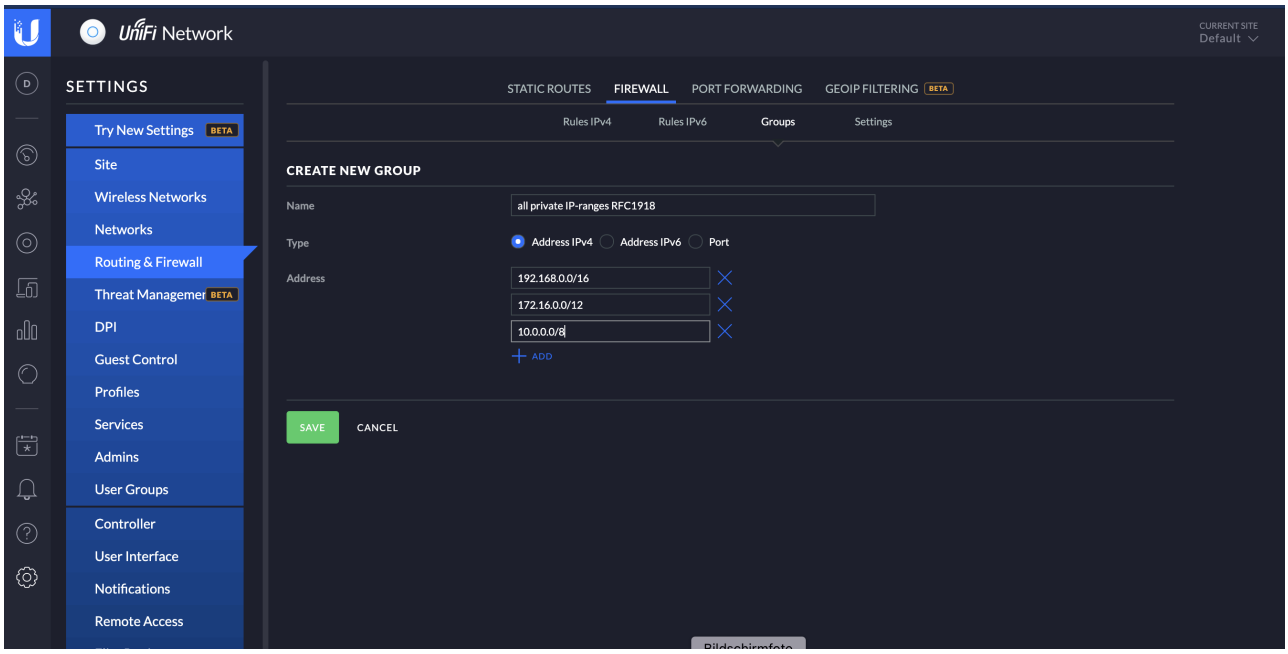
Gruppe 1 „all private IP-ranges RFC1918“

SETTINGS>Routing & Firewall>FIREWALL>Groups>CREATE NEW GROUP

Name>>>all private IP-ranges RFC1918

Address>>>192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8

>>mit Save abspeichern<<



Mit der nächsten Regel erlauben wir den Zugriff aus dem Administrator-LAN auf alle anderen Subnetze (VLAN's).

Regel 2 „allow admin LAN to access all VLANs“

SETTINGS>Routing & Firewall>FIREWALL>LAN IN>CREATE NEW RULE

Name>>>allow admin LAN to access all VLANs

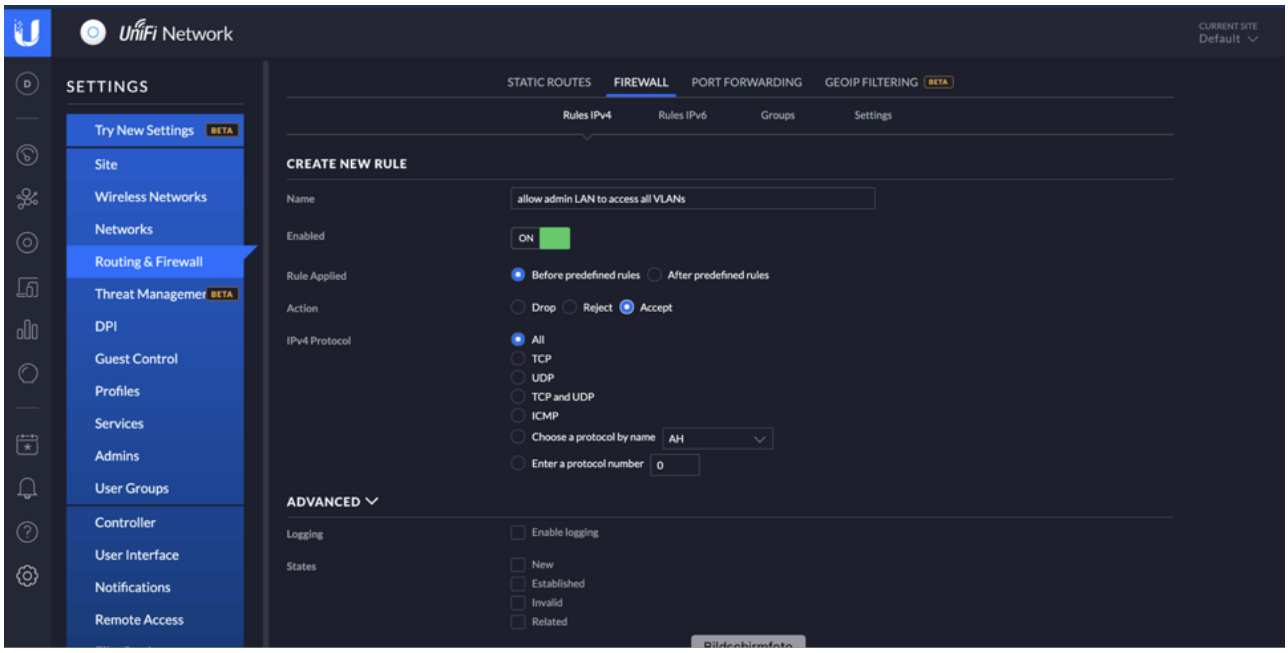
Action>>>Accept

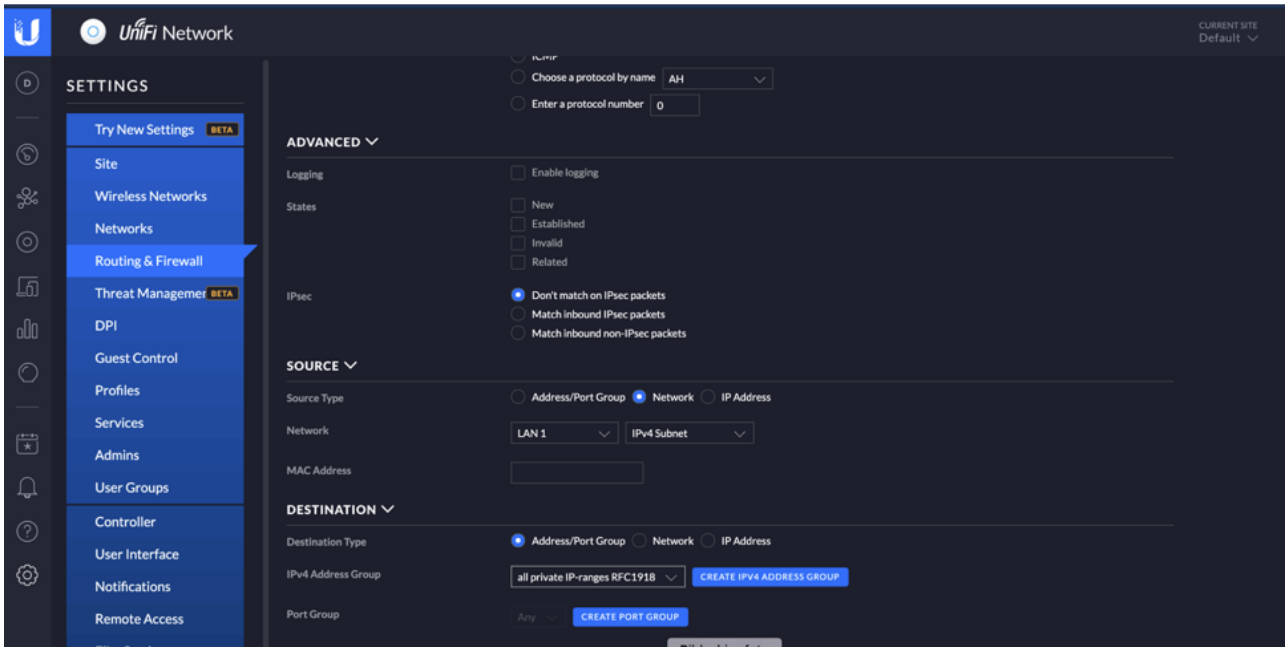
Source Type>>>Network

Network>>>LAN 1 (siehe Beispiel oben, hier ist der Name des Admin-LAN’s anzugeben)

IPv4 Address Group>>>all private IP-ranges RFC1918

>>mit Save abspeichern<<





Die nachfolgende Regel unterbindet die Kommunikation zwischen den Subnetzen (VLAN'S).

Regel 3 „block all communication between VLANs“

SETTINGS>Routing & Firewall>FIREWALL>LAN IN>CREATE NEW RULE

Name>>>block all communication between VLANs

Action>>>Drop

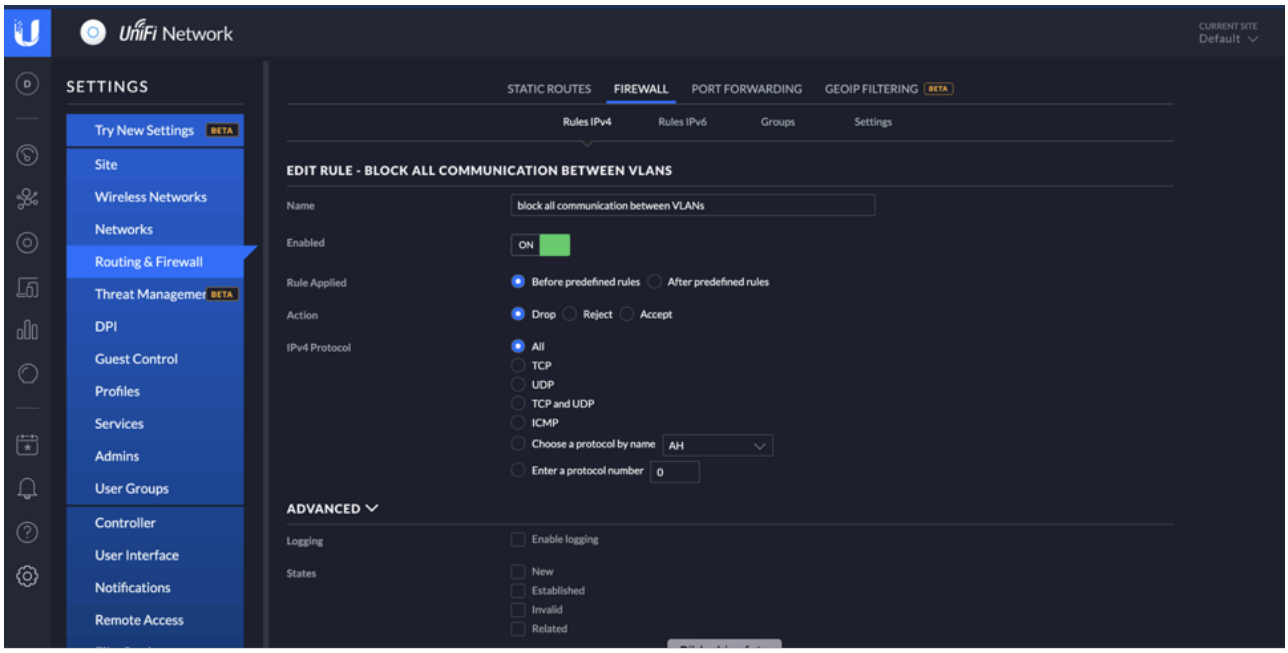
Source Typ>>>Address/Port Group

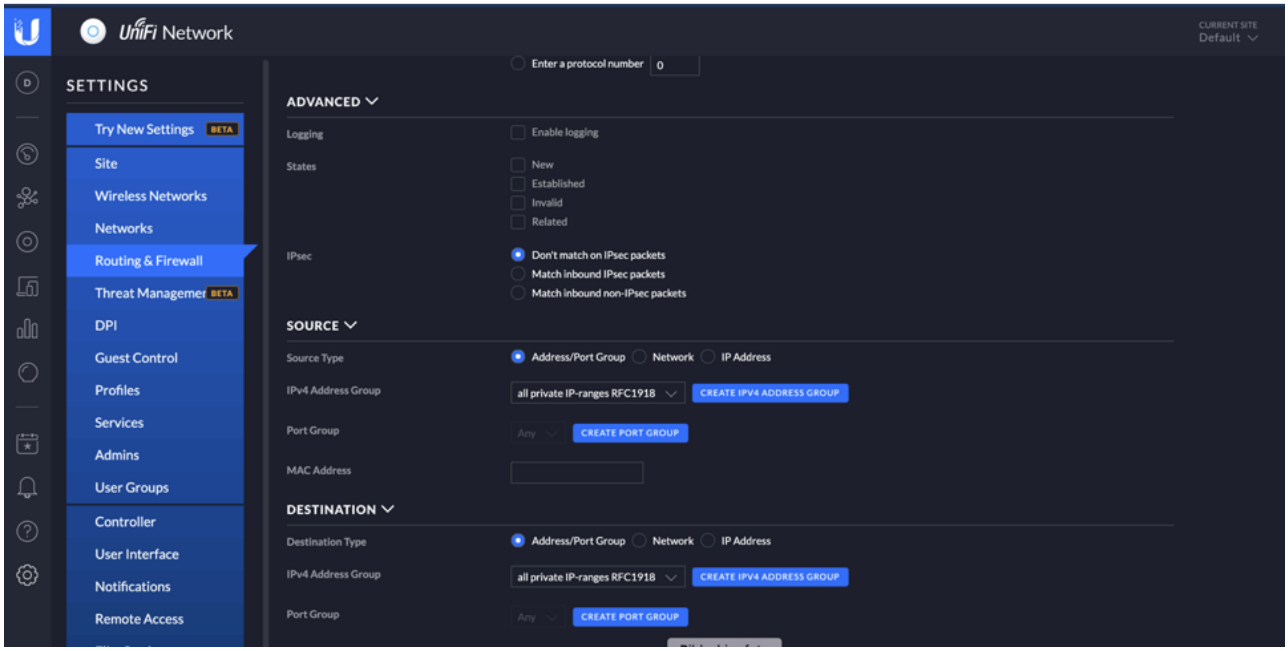
IPv4 Address Group>>>all private IP-ranges RFC1918

Destination Type>>>Address/Port Group

IPv4 Adress Group>>>all private IP-ranges RFC1918

>>mit Save abspeichern<<





Wir haben mit Regel 3 die Kommunikation der Subnetze untereinander eingeschränkt. Geräte können sich über die Subnetz-Grenzen nicht sehen und auch nicht erreichen.

Die Gateways der Subnetze sind jedoch noch aus den anderen Subnetze erreichbar.

Beispiel: Von einem Gerät im LAN IoT (10.10.2.x) ist das Gateway des LAN 1 -Admin-LAN- (10.10.1.1) erreichbar. Somit auch USG oder UDM.

Das wollen wir im nächsten Schritt unterbinden.

Dazu definieren wir weitere Gruppen.

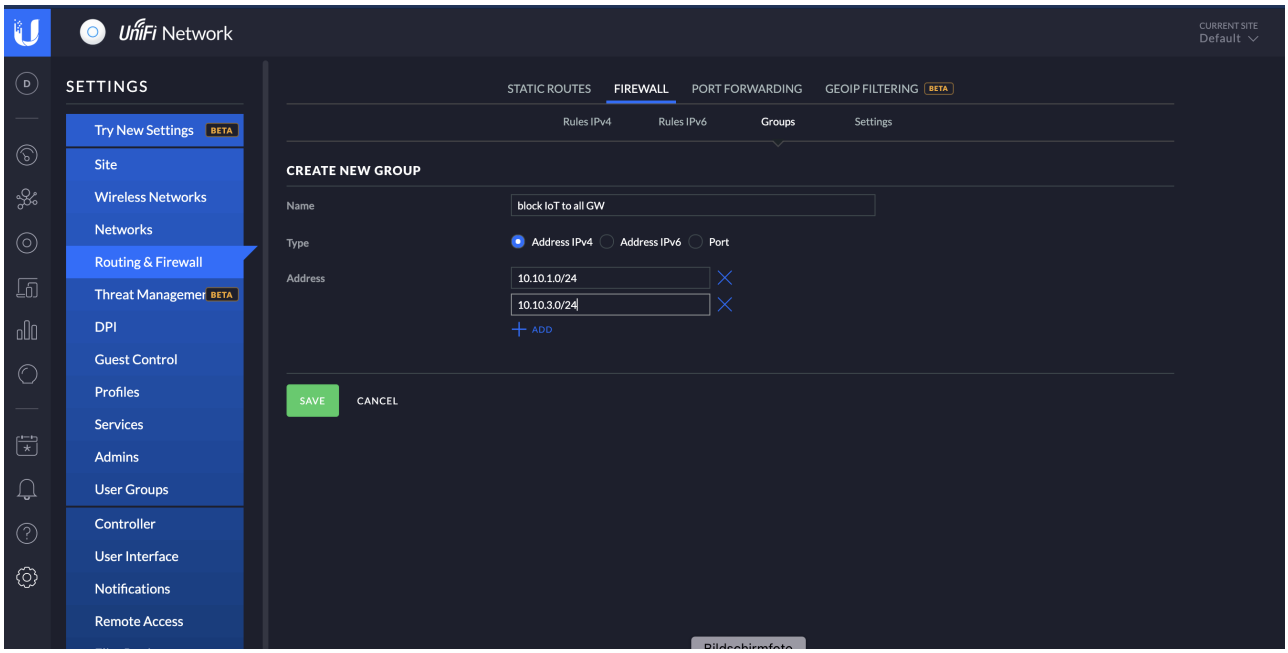
Gruppe 2 „block IoT to all GW“

SETTINGS>Routing & Firewall>FIREWALL>Groups>CREATE NEW GROUP

Name>>>block IoT to all GW

Address>>>10.10.1.0/24, 10.10.3.0/24

>>mit Save abspeichern<<



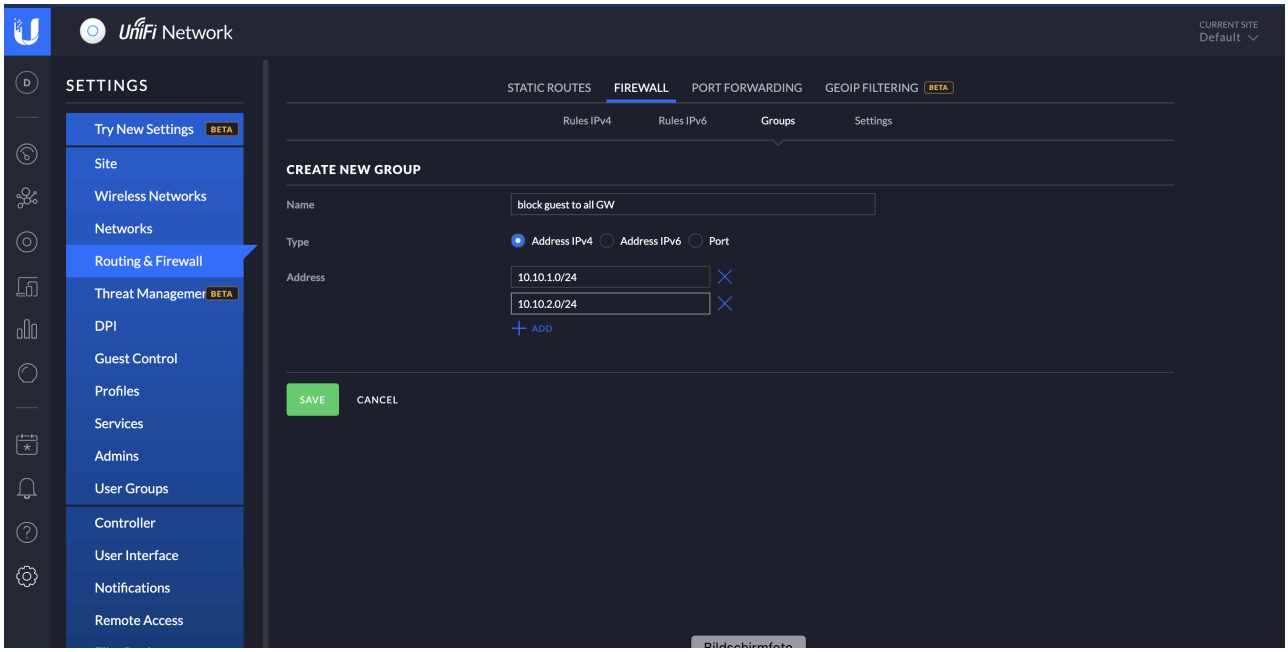
Gruppe 3 „block guest to all GW“

SETTINGS>Routing & Firewall>FIREWALL>Groups>CREATE NEW GROUP

Name>>>block guest to all GW

Address>>>10.10.1.0/24, 10.10.2.0/24

>>mit Save abspeichern<<



Wer genau hinsieht, erkennt leicht das Prinzip.

Die Gruppen werden so definiert, dass die jeweils anderen Subnetze eingetragen werden.

Nachdem die Gruppen definiert wurden, folgen jetzt die notwendigen Regeln.

Regel 4 „block IoT to all GW“

SETTINGS>Routing & Firewall>FIREWALL>LAN LOCAL>CREATE NEW RULE

Name>>>block IoT to all GW

Action>>>Drop

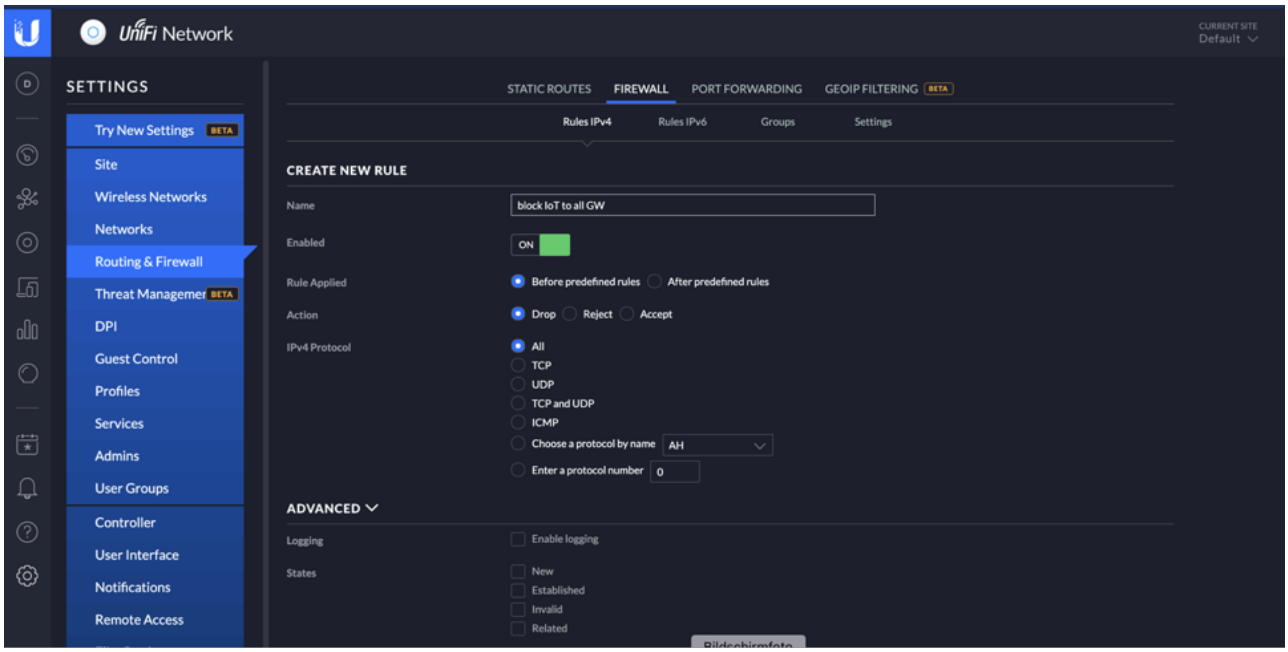
Source Typ>>>Network

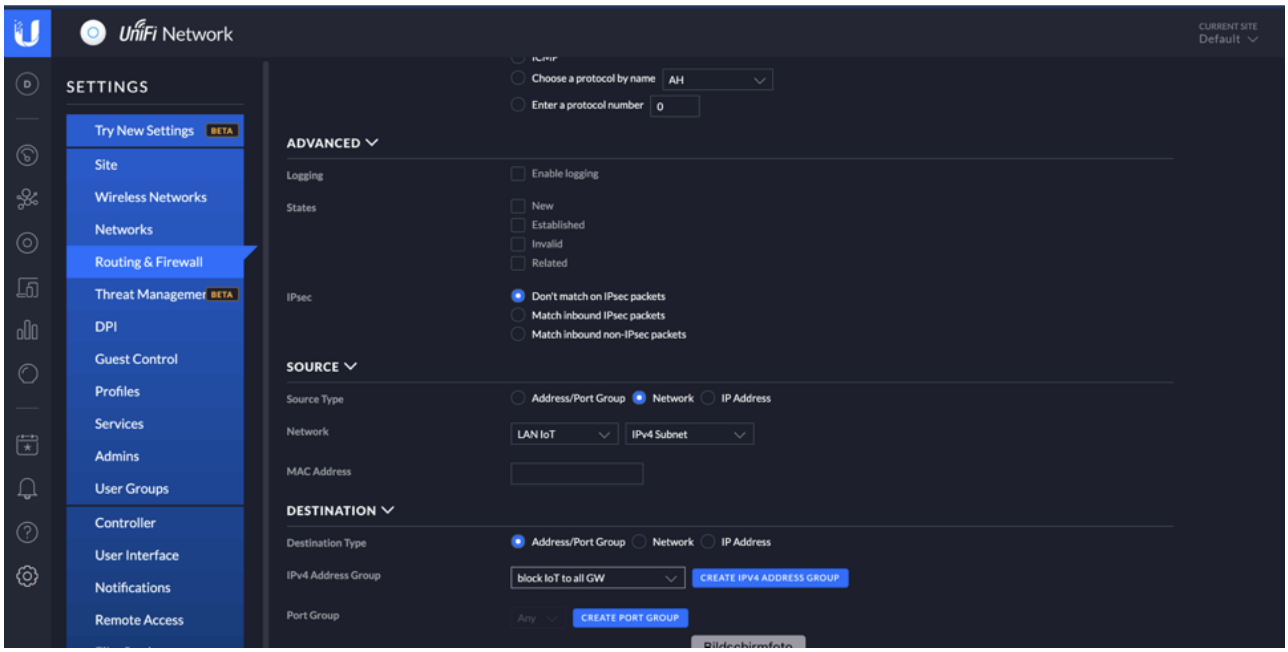
Network>>>LAN IoT

Destination Type>>>Address/Port Group

IPv4 Address Group>>>block IoT to all GW

>>mit Save abspeichern<<





Regel 5 „block guest to all GW“

SETTINGS>Routing & Firewall>FIREWALL>LAN LOCAL>CREATE NEW RULE

Name>>>block guest to all GW

Action>>>Drop

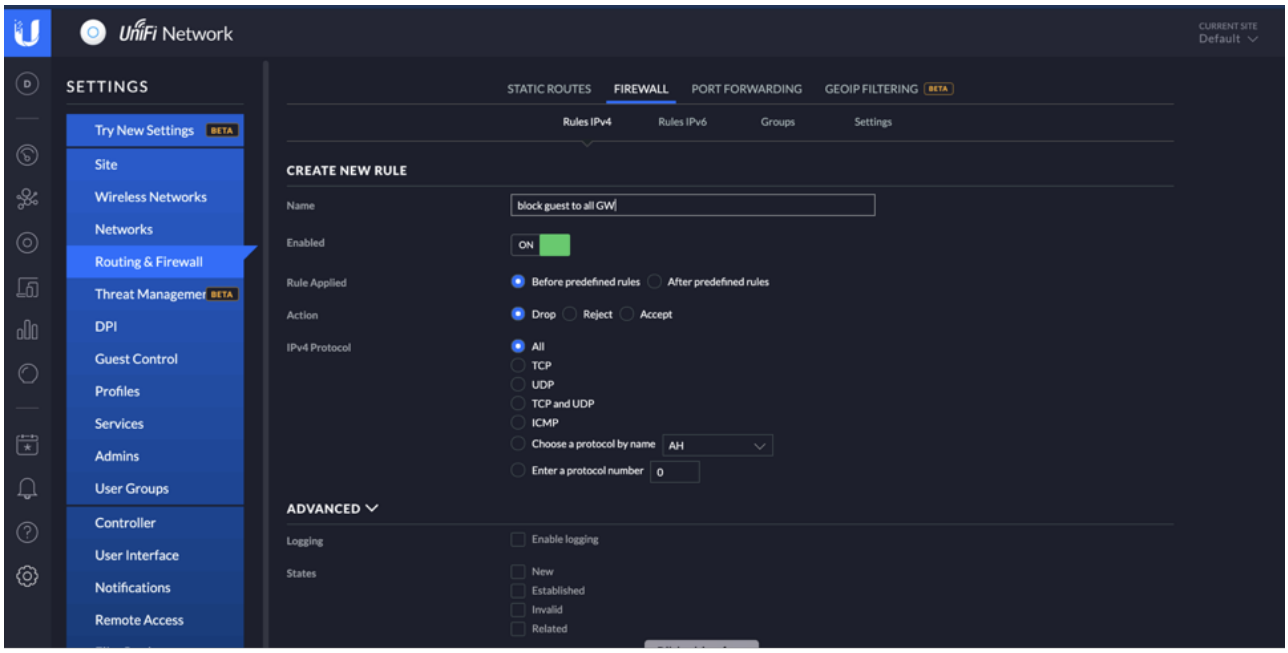
Source Typ>>>Network

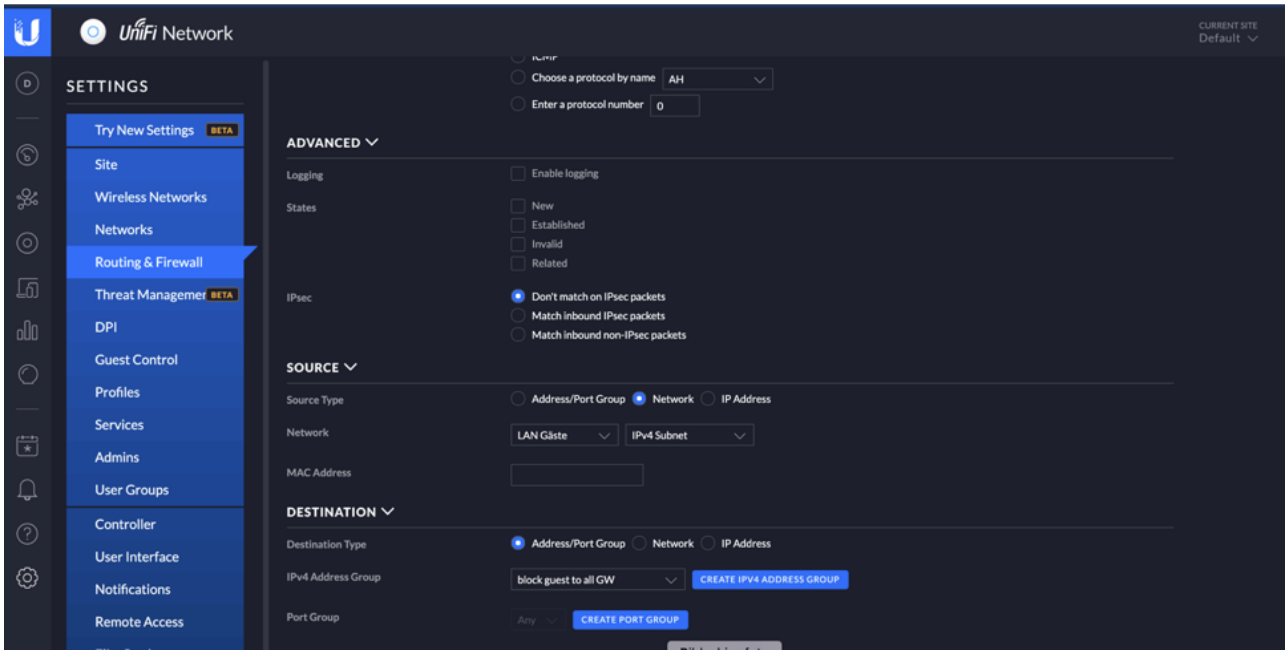
Network>>>LAN Gäste

Destination Type>>>Address/Port Group

IPv4 Address Group>>>block guest to all GW

>>mit Save abspeichern<<





Soweit so gut!

Unser Subnetze sind nun gegeneinander abgesichert.

Das bedeutet jedoch auch, dass ein Gast aus dem LAN Gäste nicht auf den Drucker im LAN IoT (10.10.2.10) zugreifen kann.

Um dies zu ermöglichen, ist eine weitere Regel erforderlich.

Und damit uns die Erweiterung der Zugriffsrechte auf weitere Geräte im LAN IoT leichter fällt, erstellen wir auch eine weitere Gruppe!

Gruppe 4 „allow access to IoT devices“

SETTINGS>Routing & Firewall>FIREWALL>Groups>CREATE NEW GROUP

Name>>>allow access to IoT devices

Address>>>10.10.2.10

>>mit Save abspeichern<<

Sollen später weitere Devices im LAN IoT erreichbar sein, könnt ihr die Gruppe um die IP’s der Geräte erweitern.

Aber bitte beachten, die Geräte müssen eine feste IP zugewiesen bekommen haben.

Nun zur notwendigen Regel.

Regel 6 „allow access to IoT devices“

SETTINGS>Routing & Firewall>FIREWALL>LAN IN>CREATE NEW RULE

Name>>>allow access to IoT devices

Action>>>Accept

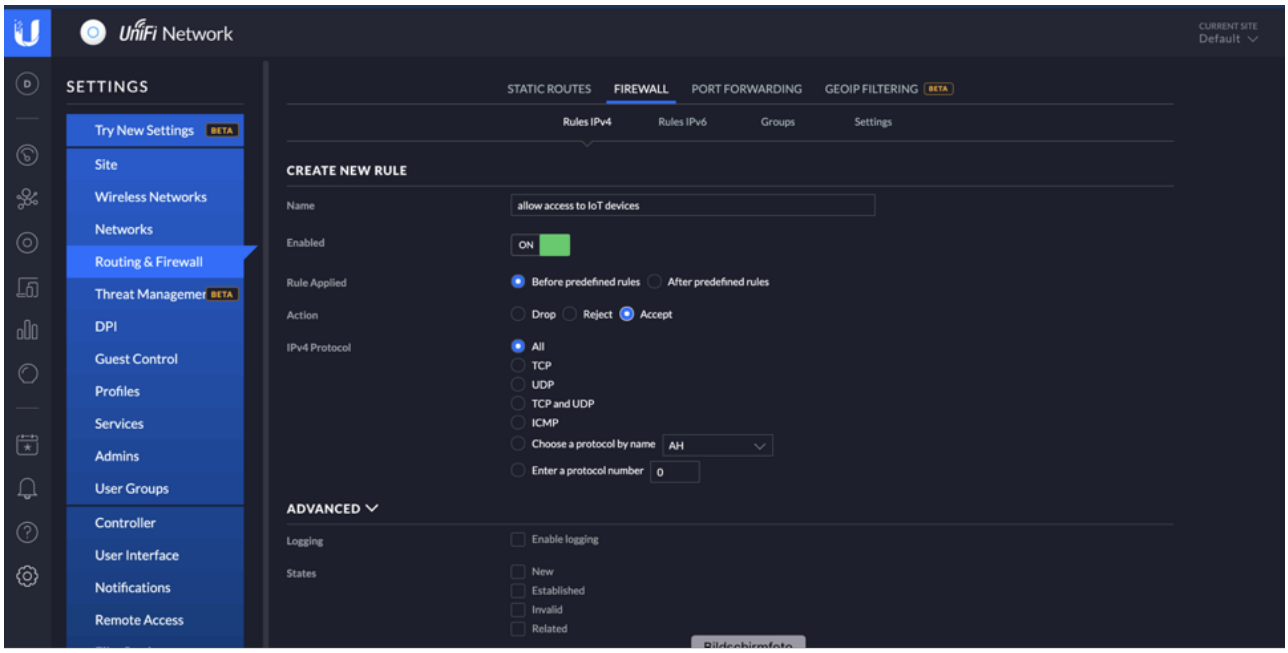
Source Typ>>>Network

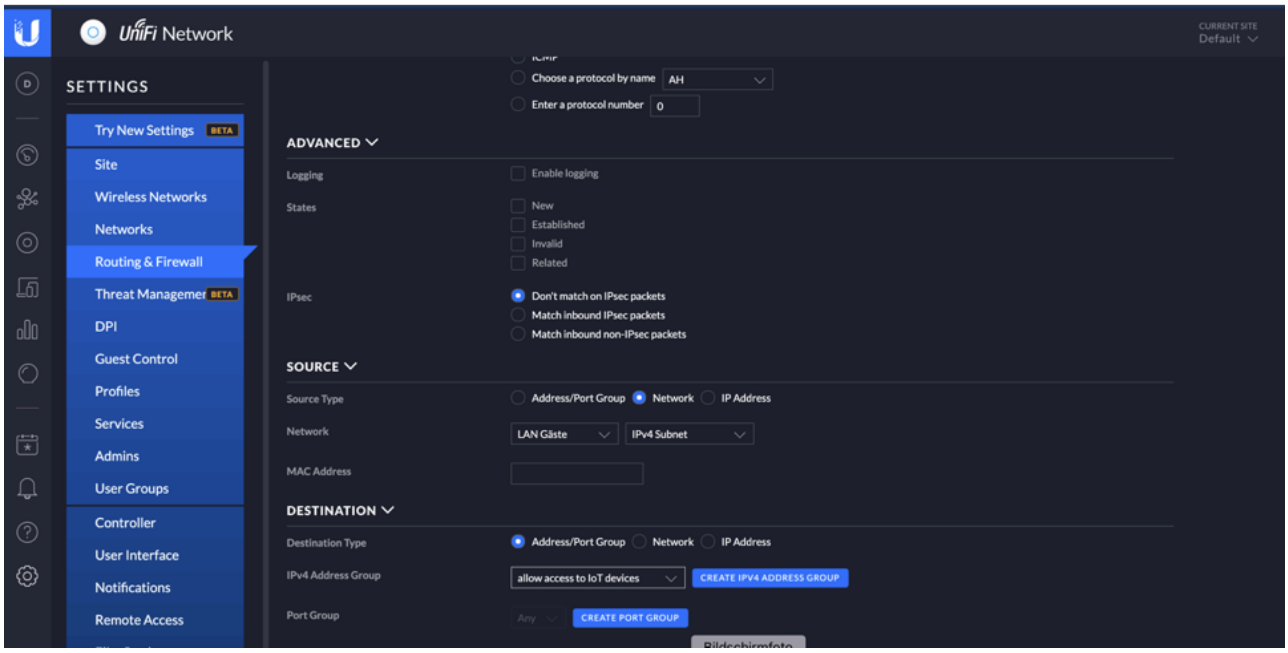
Network>>>LAN Gäste

Destination Type>>>Address/Port Group

IPv4 Address Group>>>allow access to IoT devices

>>mit Save abspeichern<<

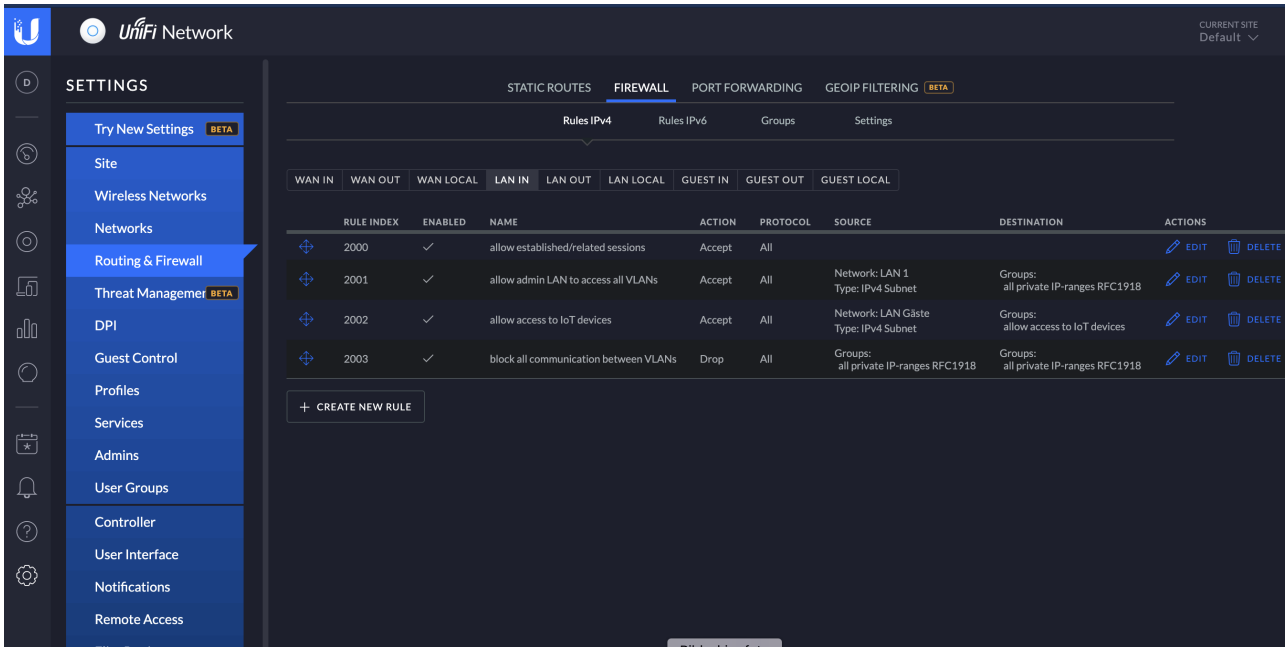




WICHTIGE AKTION!

Die Regel „allow access to IoT devices“ muss nun unbedingt vor die Regel „block all communication between VLANs“ verschoben werden.

Die Regeln werden von oben nach unten abgearbeitet. Also muss die Regel für den Drucker-Zugriff vor der Regel stehen, die alle Kommunikation zwischen den Subnetzen verbietet.



Viel Spaß!

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 Firmware-Versionen	Keine Firmware-Relevanz!
Gültige Software-Version	Keine Firmware-Relevanz!