Firewall von Unifi - Die Funktionsweise

Was wollen wir?

Wir wolllen uns mal die Funktionsweise vor Augen halten.

Warum wollen wir das?

Damit wir verstehen wie alles funktioniert, brauchen wir

zuerst den Baustein auf dem sich alles aufbaut.

Das Grundprinzip sollte verinnerlicht werden, um damit dann

vernünftige und sinnvolle Firewallregeln zu erstellen und anwenden zu können.

Und wie geht das genau?

Hier klären wir, was passiert eigentlich und mit diesem Wissen können wir arbeiten.

Das soll helfen ein Verständniss dafür zu bekommen, um dann weitere im Wiki erklärte Firewallregeln zu verstehen und um zu setzen.

Die Firewall von Unifi ist ein wenig anders.

Die meisten sind es vlt. gewohnt das Firewall´s erstmal alles blocken und man jedes einzelne erst freigeben muss.

Bei Unifi ist es genau anders herum. Da darf erstmal jeder mit jedem und allem kommunizieren.

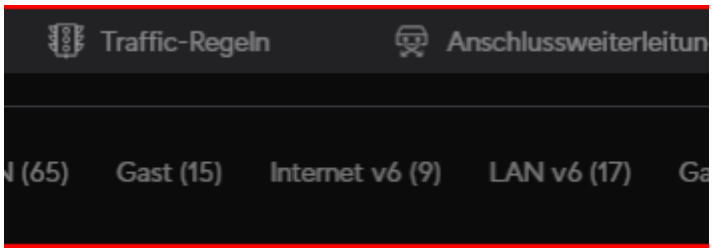
Lege ich also VLAN´s an sind die auch untereinander erstmal sehr auskunftsfreudig und unterhaltsam.

Schauen wir uns das mal genauer an.

Die Firewall ist zu erreichen unter Einstellungen - Anwendungsfirewall - Firewall-Regeln.

Zuerst ist die Firewall aufgeteilt in :

Alle, Internet, LAN, Gast, Internet v6, LAN v6 und Gast v6.



Die Aufteilung lautet wie folgt:

Alle : Alle Firewallregeln aufgelistet für IPv4 und IPv6,

Internet : Hier werden die Internetregeln für IPv4 erstellt,

LAN : Hier wird der LAN Verkehr der einzelnen VLAN´s geregelt für IPv4,

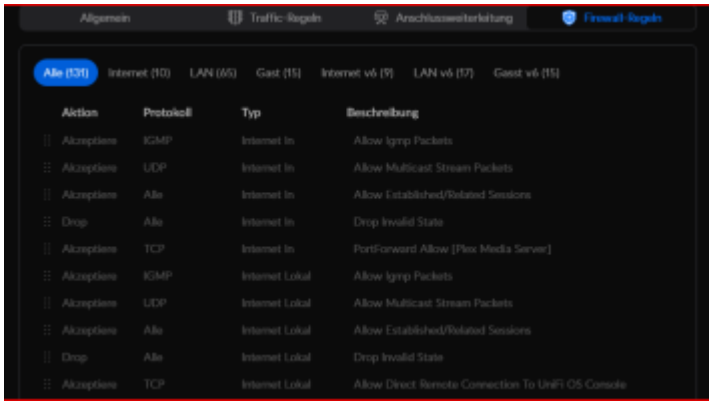
Gast : Hier werden die Regeln für die Gastnetzwerke für IPv4 gelistet.

Internet v6, LAN v6 und Gast v6 : Hier gelten dann die gleichen Bestimmungen,

wie bei IPv4 aber halt das ganze nur für IPv6.

Unifi bringt von Haus aus schon ein paar unveränderliche, vorkonfigurierte Firewallregeln mit,

die für den Betrieb der Unifi Produkte, Vorraussetzung sind.



Um das ganze noch ein wenig zu verfeinern sind die jeweiligen Punkte, Internet, Lan und Gast für IPv4 und IPv6 jeweils in drei Kategorien unterteilt.

Diese da nennen sich, "IN", "Out" und "Lokal".

Die Regeln werden entsprechen dann angewendet für:

In : Betrifft den Datenverkehr der aus dem Netzwerk kommt und über diese Schnittstelle für andere Netzwerke bestimmt ist,

Out : Betrifft den Datenverkehr der aus andere Netzwerken stammt und über diese Schnittstelle für dieses Netzwerk bestimmt ist,

Lokal : Betrifft den Datenverkehr der UDM / USG selbst.

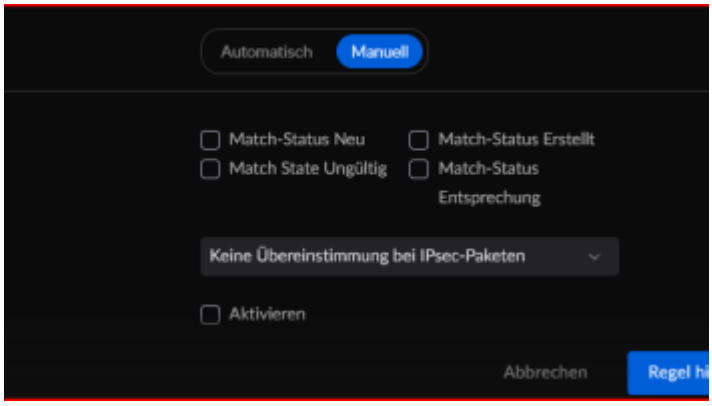
Dieses gibt es jeweils für Internet, LAN und Gast im IPv4 und IPv6 Bereich.

Das wird uns klar, sobald wir auf Eintrag erstellen gehen und dann werden wir gleich ganz oben unter "Typ", danach gefragt.

Hier können wir dann wählen für Internet, LAN, Gast - In, Out oder Lokal.

Weiterhin können wir wenn gebraucht der Firewallregel, einen Status zuordnen.

Das wären dann, "Neu", "Etabliert", "Verwandt" und "Ungültig".



(Die Übersetzung in der Oberfläche von Unifi lässt noch ein wenig zu wünschen übrig)

Neu : steht für den Datenverkehr aus einer neuen Verbindung,

Etabliert : betrifft den Datenverkehr aus bereits bestehenden oder bekannten Verbindungen,

Verwandt : betrifft den neuen Verkehr einer bereits bestehen oder bekannten Verbindung,

Ungültig : trifft dann zu, wenn keiner der zuvor Genannten Zustände zutrifft.

Mit diesem Grundwissen können wir dann die Unifi Firewallregeln verstehen und aufbauen.

Diese werden auch sehr anschaulich im Wiki erklärt.

Was bleibt noch zu sagen?

Die Unifi Firewallregeln könnt ihr gut mit Traffic Regeln kombinieren, um eine geziehlte Wirkung zu erreichen.

Informiert euch auch noch über das Thema, "Gruppen".

Das vereinfacht einem das erstellen, sowie das spätere arbeiten mit den Firewallregeln.

Wenn ihr Firewallregeln anlegt, ist noch zu beachten, das erlauben Regeln vor den blockieren Regeln sein müssen.

Dieses könnt ihr erreichen, in dem man die Regeln an die richtige Position verschiebt.

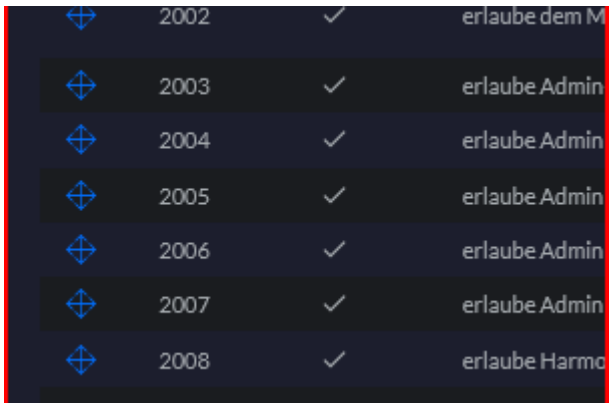
Die Firewallregeln bei Unifi werden der Reihe nach abgearbeitet.

Soll heissen, wenn ich vorher alles blockiere kann danach nix mehr erlaubt werden.

Nachtrag: Das mit der Reihenfolge betrifft auch die Regeln untereinander. Also die erlauben Regeln werden auch der Reihe nach abgearbeitet und genauso die blokieren Regeln.

Unifi spricht da von einem Indexing. Desto geringer der Wert um so eher wird diese Regel angewandt.

Man kann das heute aber nur noch über die alte Oberfläche erkennen. In der neuen leider nicht mehr.



Also auch innerhalb der Regeln die Reihenfolge beachten. Nicht erst alle VLAN´s untereinander blockieren und dann erst die Gateway´s und so weiter.

Wenn ich schon vorher die Regel "blockiert die gesamte Kommunikation zwischen VLANs" anwende, kommen die nachfolgenden Regeln garnicht mehr zur Anwendung.

Nein zuerst die normalen Regeln, dann Gateway´s und zum Schluss, wenn keine der Regeln zutrifft, dann alles sperren.

Beim erlauben Regeln verhält sich genauso.

Nun viel Erfolg und wünsche euch viel Spaß, bei der täglichen Arbeit in der Unifiumgebung.

Auswählen:

Gültige Software-Version Keine Firmware-Relevanz!