AD Blocker / Werbeblocker / Content blocker für UnifiOs - HOW IT WORKS

Was wollen wir?

Die DNS Basierten Block Funktion kennen lernen die unter UnifiOs zur Verfügung stehen

Warum wollen wir das?

Mit UniFi OS 3.x und Network 7.3.69 is ein DNS basierter Werbeblocker dazu gekommen.

schon länger existiert ein DNS basierter "Content Filtering" mit den Optionen „Family" und „Work"

Hier wird die Funktion erklärt und auf die Fallstricke hingewiesen die von dem aktivierten Blocker

ausgehen.

Und wie geht das genau?

Vorweg:

UnifiOs 3.x und Network ab 7.3.69 ist noch EalryAccess und grade UnifiOS 3.x nicht für alle Geräte Verfügbar.

getestet und beschrieben auf einer UDM-PRO-SE.

Unbestätigt: Die CloudKey Controller haben trotz UnifiOS 3.x KEINEN AD Blocker da mit ihnen

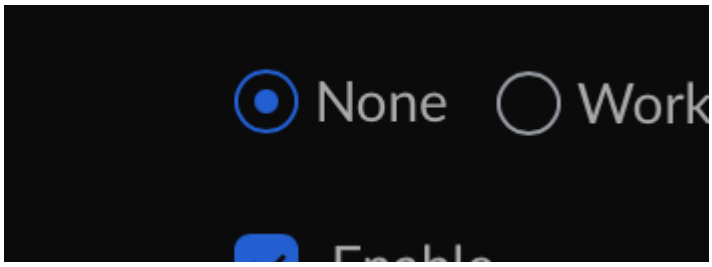
nur die „alten“ USG gesteuert werden können diese eine andere Basis haben.

Wie an und Aus:

Content Filtering:

Neue GUI -> Settings -> Networks -> auf das jeweilige VLAN

AUS, WORK, Family sind die einzigen Optionen.



AD Block:

Neue GUI -> Settings -> Traffic Management:

hat nun unter den statischen Routen einen "AD Blockig" Schalter.

Neben AN uns AUS ist die einzige Einstellung für welche VLANs der AD Blocker tätig sein soll.

Mehr Konfiguration Möglichkeiten gibt es nicht bisher.

?thumbnail=1 Image not found or type unknown

Was tut es:

Mit dem einschalten wird eine (interne nicht über die GUI einsebare) Firewall Regel für das jeweilige VLAN Netz hinzugefügt.

Diese biegt den DNS Traffic an eine 203.0.113.0/24 IP um unabhängig was ihr ggf. am Client direkt oder per DHCP

eingestellt habt. Sprich sobald ein DNS Packet in dem aktivierten VLAN auf die UDM oder an ihr vorbei will, wird umgebogen.

Beispiel für zwei VLANs:

Code

```
# iptables -v -t nat -L DNSFILTER
Chain DNSFILTER (1 references)
pkts bytes target prot opt in out source destination
0 0 DNAT tcp -- any any 10.0.20.0/24 anywhere tcp dpt:domain to:203.0.113.3:53
0 0 DNAT udp -- any any 10.0.20.0/24 anywhere udp dpt:domain to:203.0.113.3:53
0 0 DNAT tcp -- any any 192.168.1.0/24 anywhere tcp dpt:domain to:203.0.113.2:53
0 0 DNAT udp -- any any 192.168.1.0/24 anywhere udp dpt:domain to:203.0.113.2:53
```

Diese IP ist Local!

203.0.113.0/24 is das TEST-NET-3 und eigentlich für Dokumentation gedacht. Keine Ahnung was Ubiquiti da geritten hat

genau diesen Bereich zu nutzen. UI kann sich aber wohl sicher sein das den kein anderer irgendwie nutzt.

Wie man sehen kann bekommt jedes VLAN Netz seine eigene Zieladresse, auf den der DNS Verkehr umgeleitet wird.

Jede Zieladresse ist dabei in einem eignen Netzwerk Namespace, eine Technik wie sie beim betreiben von Container

Anwendung findet um eigne Interfaces/Ip/Routing/Firewall Tabellen zu nutzen die sich gegenseitig nicht beeinflussen.

Als Routing Brücke zum „default“ Netzwerk dient dabei die "203.0.113.1/24“.

Das is mehr oder minder elegant, Netzwerk Basierte Namensräume sind eine mächtige Waffe, macht es aber nicht

unbedingt leichter, da sich die settings hier „tiefer“ verstecken.

Am ende des Tages läuft dann für jedes VLAN eine eigne DNSMasq Instanz.

(Ausgabe der besseren Lesbarkeit gekürzt):

Code

```
# ps -ef | grep dnsfilter
nobody dnsmasq -r /run/dnsfilter/dns-192.168.1.1-resolv.conf -C /run/dnsfilter/dns-192.168.1.1-conf.conf
nobody dnsmasq -r /run/dnsfilter/dns-10.0.20.1-resolv.conf -C /run/dnsfilter/dns-10.0.20.1-c
```

Jede Instanz bekommt dabei über die jeweilige „resolve.conf“ einen DNS Server als Forwarder.

Sollte der Content Filter eingeschaltet sein sind das aktuell EXTERNE DNS Server

von cleanbrowsing.org. Diese stellen kostenlose DNS Filter zu Verfügung, die die auch

gerne beim PI-Hole benutzt werden.

DNS 185.228.168.10 für die „Work“ Einstellung -> Adult Filter bei cleanbrowsing.org

DNS 185.228.168.168 für die „Family“ Einstellung -> Family Filter cleanbrowsing.org

Beide blocken bekannte erwachsenden Seiten, Porno oder andere explizite Inhalte.

Sowie VPN, Proxy und so weiter. Der Work Filter ist dabei nicht ganz so erbarmungslos

und lässt auch Mixed content Seiten wie Reddit VPN zu.

In einer lokale "White List" sind die Lokalen DNS Eintrage (die eigenen und und die default wie „unifi")

als Verweis auf den normalen UDM DNS eingetragen.

Sollte nur der AD Block eingeschaltet sein wird nun zu dem normal UDM DNS zurückverwiesen

über die 203.0.113.1 der neben den evt. vorhandenen Lokalen Namen

(und die generischen wie „unifi“) seinerseits die im WAN interface konfigurierten DNS Server benutzt (Manuel gesetzten oder per PPP/DHCP zugewiesene)

Dazu gesellt sich dann ein Host file mit ca. 155000 Einträgen von bekannten Werbeservern die auf die 0.0.0.0 aufgelöst werden.

Aktualisiert wird das ganze so wie die IDS Rules einmal alle 24 stunden (/run/utm/ads.list) und wird vom UNIFI System dann

angepasst und für die einzelnen VLANs ausgerollt.

Damit sind bei Benutzung von Content Filter oder AD block die eigne DNS Einstellungen auf der Client Seite ausgehebelt.

Es wird alles auf die UDM umgebogen in dem aktiven VLAN, sobald ein DNS Paket vorbei kommt.

Das ganze funktioniert ganz anständig, es gibt auch eine minimale Statistik unter:

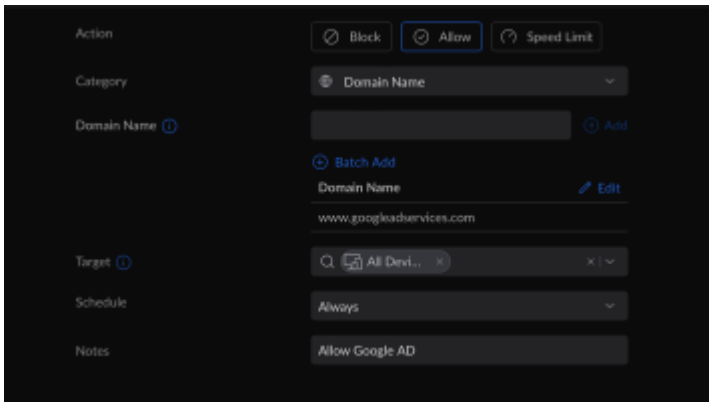
Neue GUI -> Security Insights, oben auf **Filtering Activity** klicken.

Unten in der Liste neben taucht ein „AD Blocks“ ein einfacher Zähler auf

Mit UnifiOS 3.0.16 und Network 7.4.x gibt es auch die Möglichkeit externe Domains

in die Whitelist aufzunehmen, das geschieht über eine Traffic Rule.

hier z.B für die beliebte „http://www.googleadservices.com"



Anmerkungen:

Die älteren USG unterstützen wohl den Content Filter da hier einfach nur ein Externer DNS als Forwarder eingetragen wird

(wohl auch der Grund warum bei den Release immer steht das service dns forwarding options in config.gateway.json

nicht mehr unterstützt werden). AD Block wird wohl nicht auf die alten USG kommen, da aktuell hier

ein lokaler DNS Server die Auflösung macht der „Dazwischen" geschaltet wird. das geht so nicht

mit den auf EDGEOs basierten Geräten.

Die Rule Basierten Regeln Traffic Management oder die DPI Filter in der alte UI.

Basieren auf die DPI Engine und Integration über IP Tables. und sind

von den DNS Filter bisher unabhängig.

Auswählen:

Gültige Software-Version	Keine Firmware-Relevanz!