

Quantum Spark 1535 Appliance

- Firewall
 - Service/Applikation hinzufügen
 - Eingehende/Ausgehende Regeln definieren

Firewall

Service/Applikation hinzufügen

Beschreibung:

In der Quantum werden Regeln über Services / Applikationen gesteuert.

Ein Service definiert Port(s).

Das schöne ist, braucht eine Applikation mehrere ports, sind diese hier zusammen gefasst unter einen Namen.

In Unserem beispiel wollen wir Wireguard UDP Rausgehend erlauben. Der Port ist 51820/UDP
Dazu legen wir folgende Applikation an.

Durchführung:

Auf users & Objects klicken.

Dann Services -> New

The screenshot displays a network management interface. On the left sidebar, the 'Users and Objects' icon is highlighted with a blue box. The main menu on the left shows 'Network Resources' expanded, with 'Services' highlighted in blue. A red arrow points from the 'Services' menu item to the 'New' button in the right pane. The right pane is titled 'Services' and contains a list of service names: Any_TCP, Any_UDP, AOL, AP-Defender, archie, AT-Defender, BGP, biff, and Blubster. The 'New' button is highlighted with a blue box.

Nun ausfüllen was die Applikation braucht.



New Service

Service	Advanced
Name:	<input type="text" value="wireguard_51820_UDP"/>
Type:	<input type="text" value="TCP"/>
Protocol type:	<input type="text" value="None"/>
Ports:	<input type="text" value="51820"/> <small>Enter port number or port range. For example: 5-8</small>
Comments:	<input type="text" value="Wireguard Standard Port 51820 UDP"/>

Cancel

Save

Nun haben wir einen neuen Service angelegt.

Diesen können wir [hier](#) benutzen.

Eingehende/Ausgehende Regeln definieren

Beschreibung:

Hier kann man zusätzliche regeln definieren, die erlaubt oder geblockt.

Die Ports die geblockt werden sollen müssen vorher als Services/Appliaktionen angelegt werden.

Siehe [hier](#).

Nun kann man diese dann benutzen.

Durchführung:

Auf Access Policy klicken -> policy -> Dann entweder bei Ausgehende oder Eingehende Regel auf New klicken, je nach dem was man will.

Firewall Access Policy

Outgoing Internet Access - 3 rules, 1 block actions, 2 accept actions

New Edit Delete More

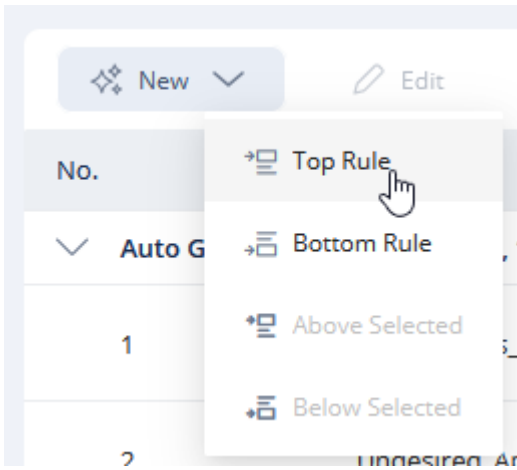
No.	Name	Sources
Auto Generated Rules - 3 rules, 1 block actions, 2 accept actions		
1	CP_Products_Bypass_Rule	* Any
2	Undesired_Apps_Rule	* Any
3	Cleanup_Rule	* Any

Incoming, Internal and VPN Traffic - 5 rules, 1 block actions, 4 accept actions

New Edit Delete More

No.	Name	Sources
Auto Generated Rules - 5 rules, 1 block actions, 4 accept actions		
1	Server_Rule_wireguard	* Any
2	Remote_Access_Rule	VPN Remote Access
3	VPN_Rule	VPN Sites
4	Local_Network_Rule	LAN networks
5	Cleanup_Rule	* Any

Nun Auswählen ob Top rule oder Bottom Rule (Sprich an erster Stelle oder letzte)
wir nehmen Top rule als Beispiel



Nun Namen vergeben.

Dann auf Das Plus bei Application and Services

Dann auf den Register Services

In den Filter unseren Namen des Services/Applikation

Gewünschter eintrag anhaken und auf select klicken.

Add Rule: Outgoing Internet Access

nun Auf action (Auf Block klicken, dann gibts die Liste) was wir wollen.

cih möchte in unserem beispiel ACCEPT

Add Rule: Outgoing Internet Access

Name	Sources	Destinations	Applications and Services	Action	Log
wireguard_standard	* Any	+ Internet	+ wireguard_518...	Block	Log

Write a comment...

Apply only during this time: 09:00 AM > 09:00 AM

Limit download traffic of applications to: 1000 Kbps

Limit upload traffic of applications to: 100 Kbps

Cancel **Save**

Jetzt kann man wenn man möchte noch ne Zeit definieren, wann die Regel greifen soll.
Ein QOS hinzufügen.
Das brauchen wir in unserem Beispiel nicht deswegen lass ich die haken weg.
Dann nur noch speichern, fertig.

Add Rule: Outgoing Internet Access

Name	Sources	Destinations	Applications and Services	Action	Log
wireguard_standard	* Any	+ Internet	+ wireguard_518...	Accept	Log

Write a comment...

Apply only during this time: 09:00 AM > 09:00 AM

Limit download traffic of applications to: 1000 Kbps

Limit upload traffic of applications to: 100 Kbps

Cancel **Save**

Die Liste, unter manuelle regeln zu finden:

Outgoing Internet Access - 4 rules, 1 block actions, 3 accept actions

No.	Name	Sources	Destinations	Applications and Services	Action	Log
Manual Rules - 1 rules, wireguard_standard accept actions						
1	wireguard_standard	* Any	Internet	wireguard_51820_UDP	Accept	Log
Auto Generated Rules - 3 rules, 1 block actions, 2 accept actions						
2	CP_Products_Bypass_Rule	* Any	Internet	Bypass_Predefined_Appi	Accept	Log
3	Undesired_Apps_Rule	* Any	Internet	Undesired applications	Block	Log
4	Cleanup_Rule	* Any	Internet	* Any	Accept	Log