Firewall-Regeln 2.0 by defcon

Was wollen wir?

Firewall-Regeln erstellen, um unsere Subnetze/Geräte gegeneinander abzusichern.

Warum wollen wir das?

selbsterklärend

Und wie geht das genau?

In meinem Beispiel besteht das Netzwerk aus fünf Subnetzen:

10.0.1.0/24 ist das 00-MGMT-LAN ohne VLAN

10.9.9.0/24 ist das 09-DNS LAN (VLAN 9) mit meinen DNS Servern (optional nur bei lokalen DNS Servern wie PiHole Adguard etc.pp.)

10.0.10.0/24 ist das 10-Home LAN (VLAN 10)

10.0.20.0/24 ist das 20-IoT-LAN (VLAN 20)

10.0.50.0/24 ist das 50-Guest-LAN (VLAN 50)

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 der IP-Bereiche sind entsprechend eurer Situation anzupassen.

Die hier beschriebenen Einstellungen sind auf Wunsch von vielen Usern mit der neuen GUI erstellt worden, und beziehen sich auf die englische Controller-Oberfläche. Die Regeln werden als Rules IPv4 definiert.

Bei Selbsterklärenden IP/Port Groups sind keine Screenshots angehängt!

Es kommt auch immer auf Einzelfälle an, deswegen werde ich das hier ziemlich allgemein halten.... ich habe bei mir 55 Regeln an der Zahl, ob alle bei euch zutreffen, keine Ahnung, deswegen werde ich nur auf die wichtigsten eingehen! Oft beziehen sich die Regeln auch auf gewisse VLANs, deswegen findet ihr in meinen IP/Port Groups auch führende Zahlen. den Aufbau muss jeder für sich selbst bestimmen!!!

Hier werden evtl. auch Regeln auftauchen, die euch gar nicht betreffen! Und ja, ihr werdet euren eigenen Hirnschmalz einfließen lassen müssen, Listen machen und euch einen Kopf drüber machen was zu euch passt oder nicht!

Los geht's!

Wir erstellen erst einmal die benötigten Port Gruppen, damit wir diese später mit den Firewall Regeln verheiraten können:

Settings -> Profiles -> Port and IP Groups ***(gilt ab jetzt für alle Port/IP Gruppen)***

00 | admin devices

IPv4 Address/Subnet

Hier kommen alle IPs eurer Geräte rein, welche ihr zum Administrieren eures Netzwerks benutzt – am besten benutzt ihr hierfür DHCP Reservierungen oder statische IPs

00 | all local Gateways

IPv4 Address/Subnet

Hier hinterlegt ihr alle Gateway Adressen eurer LANs/VLANs

00 | all local IP-Ranges

IPv4 Address/Subnet

Hier hinterlegt ihr alle lokalen IP-Adressen eurer Subnetze – in diesem Beispiel:

10.0.1.0/24

10.9.9.0/24

10.0.10.0/24

10.0.20.0/24

10.0.50.0/24

00 | local Gateways w/o MGMT

IPv4 Address/Subnet

Hier hinterlegt ihr alle Gateway Adressen eurer VLANs außer dem Management-LAN

09 | DNS-LAN to all Gateways

IPv4 Address/Subnet

Hier hinterlegt ihr alle lokalen IP-Adressen eurer Subnetze – außer das DNS VLAN:

10.0.1.0/24

10.0.10.0/24

10.0.20.0/24

10.0.50.0/24

09 | DNS Ports (nur erforderlich bei eigenem lokalen DNS Server)

Port Group

Hier hinterlegt ihr alle DNS Ports

53

443

853

09 | DNS Server

IPv4 Address/Subnet

Hier hinterlegt ihr die IP-Adressen eurer lokalen DNS Server (z.B. PiHole Adguard):

10.9.9.98

10.9.9.99

10 | Home LAN to all Gateways

Hier hinterlegt ihr alle lokalen IP-Adressen eurer Subnetze – außer das Home VLAN:

10.0.1.0/24

10.9.9.0/24

10.0.20.0/24

10.0.50.0/24

10 | iPhones (Sonderregle)

IPv4 Address/Subnet

Hier hinterlegt ihr die IP-Adresse eurer NAS

10 | NAS

IPv4 Address/Subnet

Hier hinterlegt ihr die IP-Adresse eures NAS

10 | NAS User

IPv4 Address/Subnet

Hier hinterlegt ihr die IP-Adressen eurer NAS-User

20 | Homeassistant

IPv4 Address/Subnet

Hier hinterlegt ihr die IP-Adressen eurer Smarthome Zentralen (in meinem Fall Homeassistant)

20 | IoT Devices

IPv4 Address/Subnet

Hier hinterlegt ihr die IP-Adressen eurer IoT Devices (Aktoren Lampen, Bridges etc.pp.)

20 | IoT LAN to all Gateways

Hier hinterlegt ihr alle lokalen IP-Adressen eurer Subnetze – außer das IoT VLAN:

10.0.1.0/24

10.9.9.0/24

10.0.10.0/24

10.0.50.0/24

50 | Guest LAN to All Gateways

Hier hinterlegt ihr alle lokalen IP-Adressen eurer Subnetze – außer das IoT VLAN:

10.0.1.0/24

10.9.9.0/24

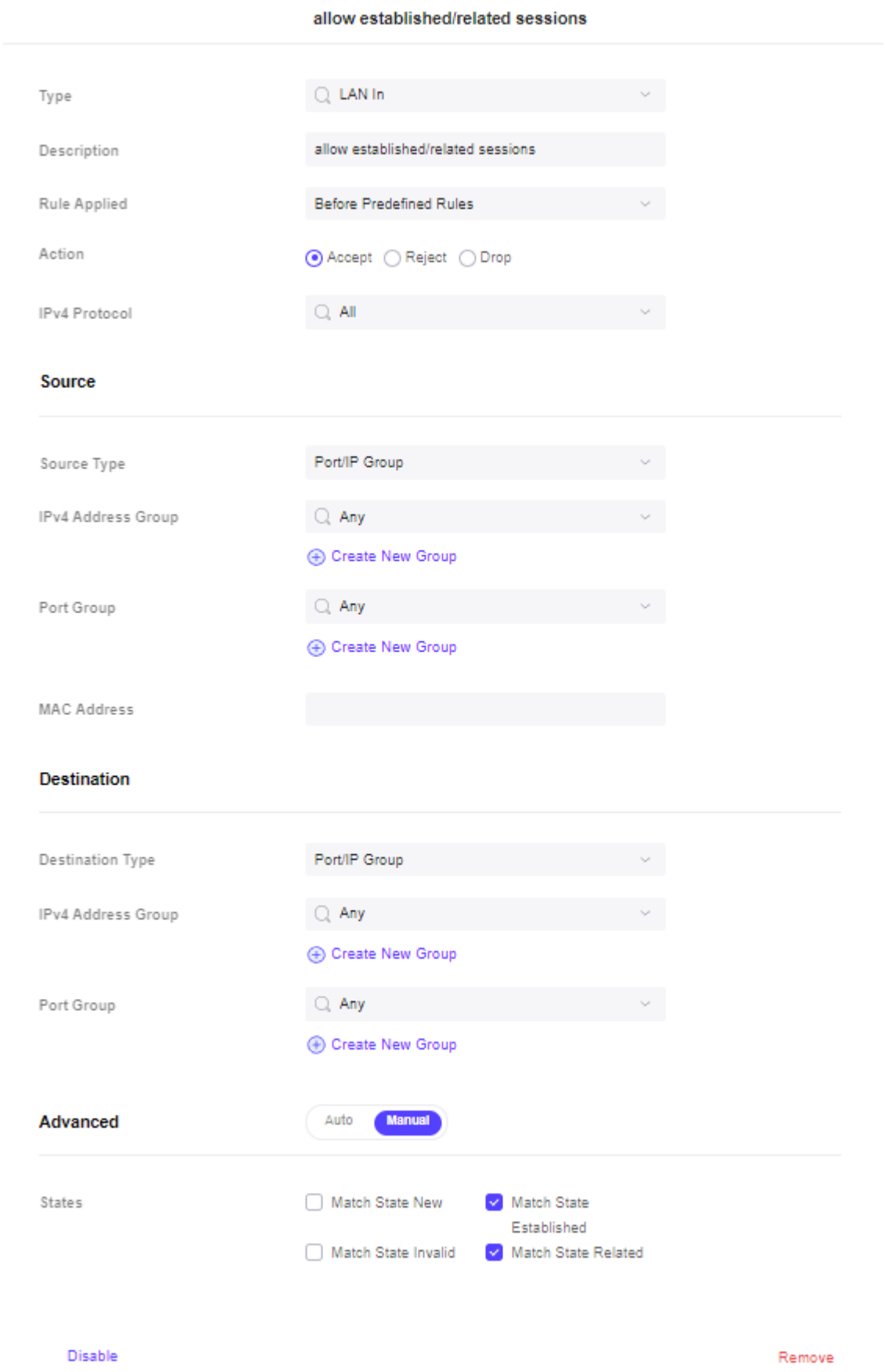
10.0.10.0/24

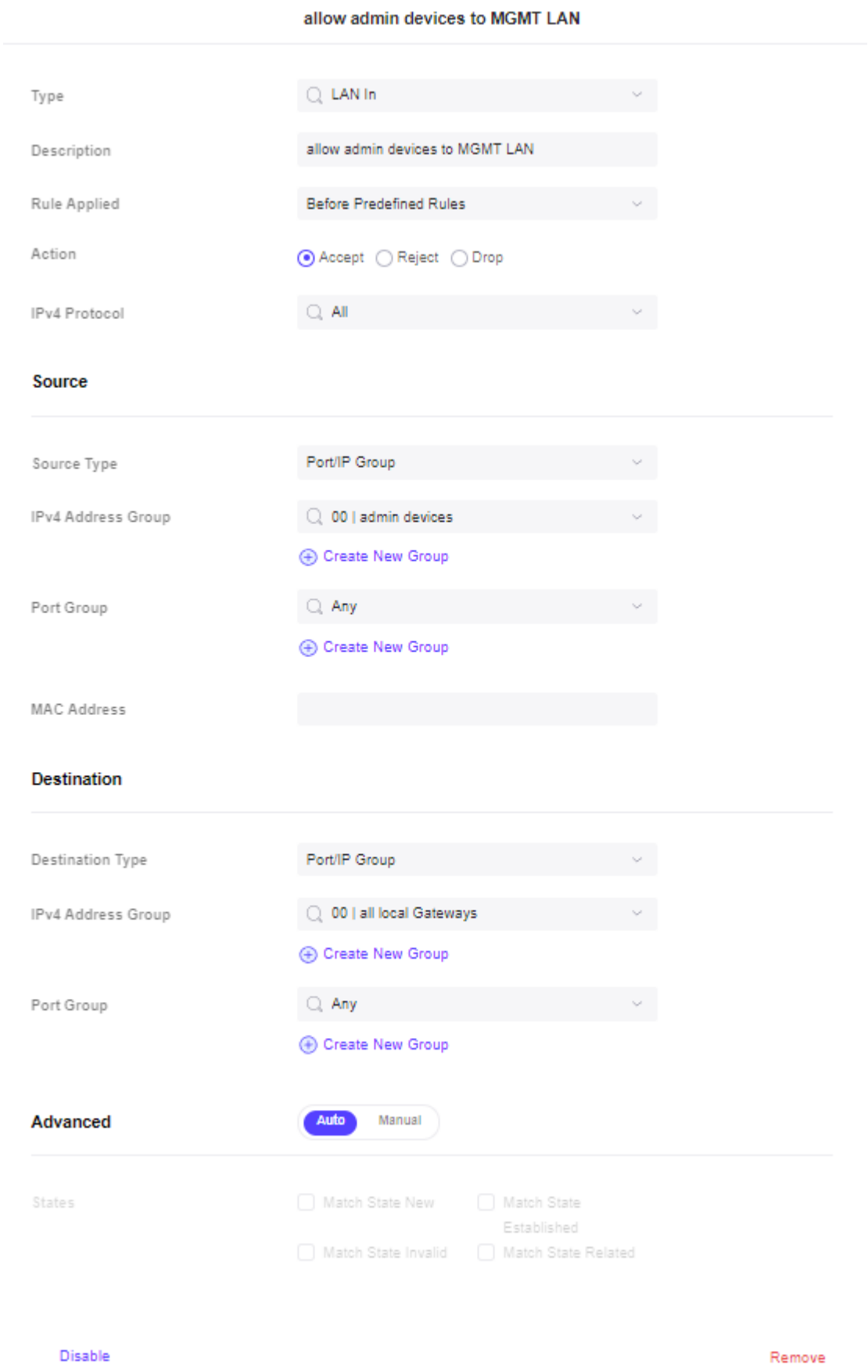
10.0.20.0/24

Jetzt sind wir endlich soweit, dass wir mit dem eigentlichen Firewalling anfangen können.

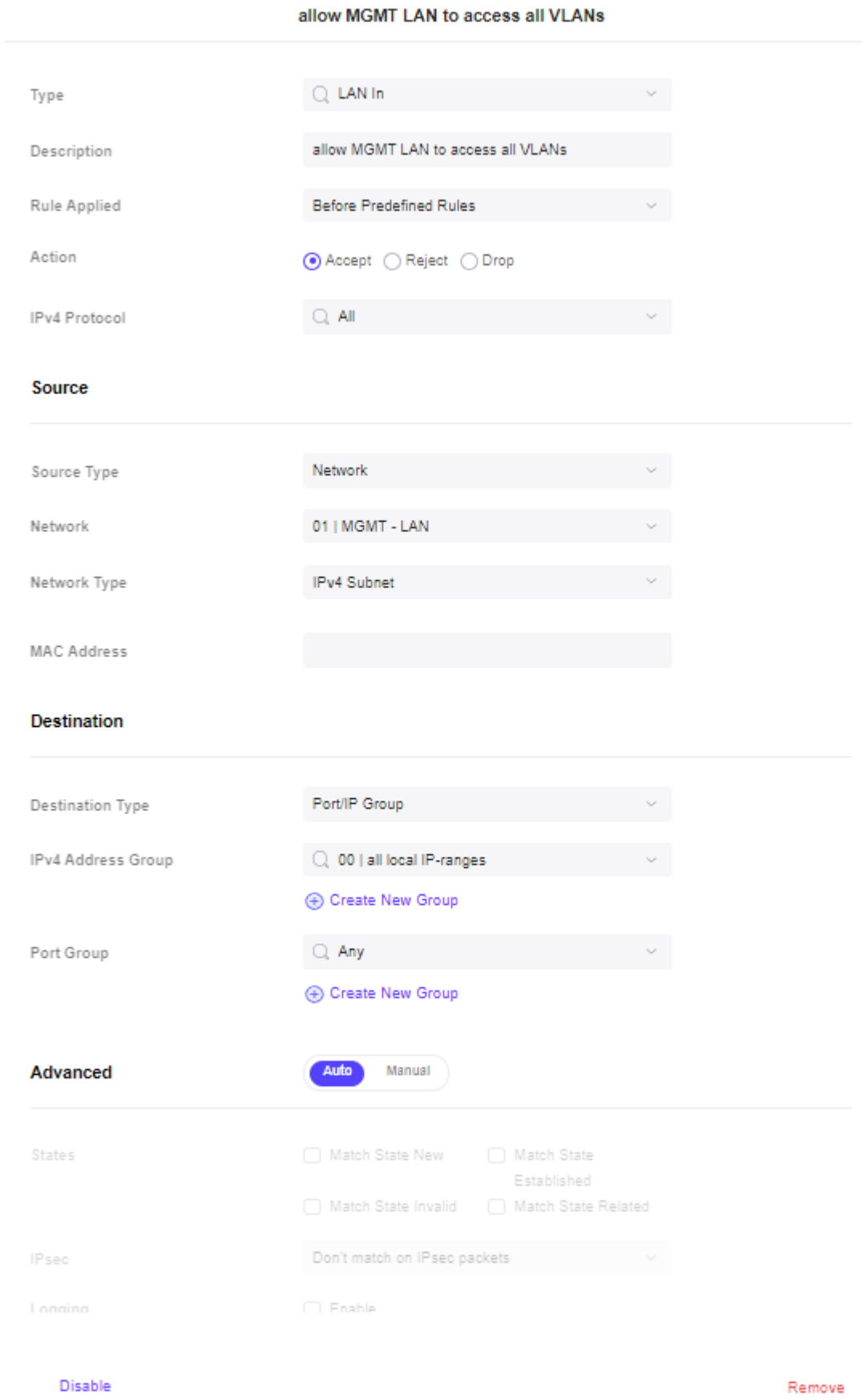
Ab jetzt gibt es nur noch Screenshots mit einer kurzen Beschreibung der Funktion wie/warum & wieso!

Settings -> Firewall & Security -> Create New Rule -> LAN IN ***(gilt ab jetzt für alle Rules)***

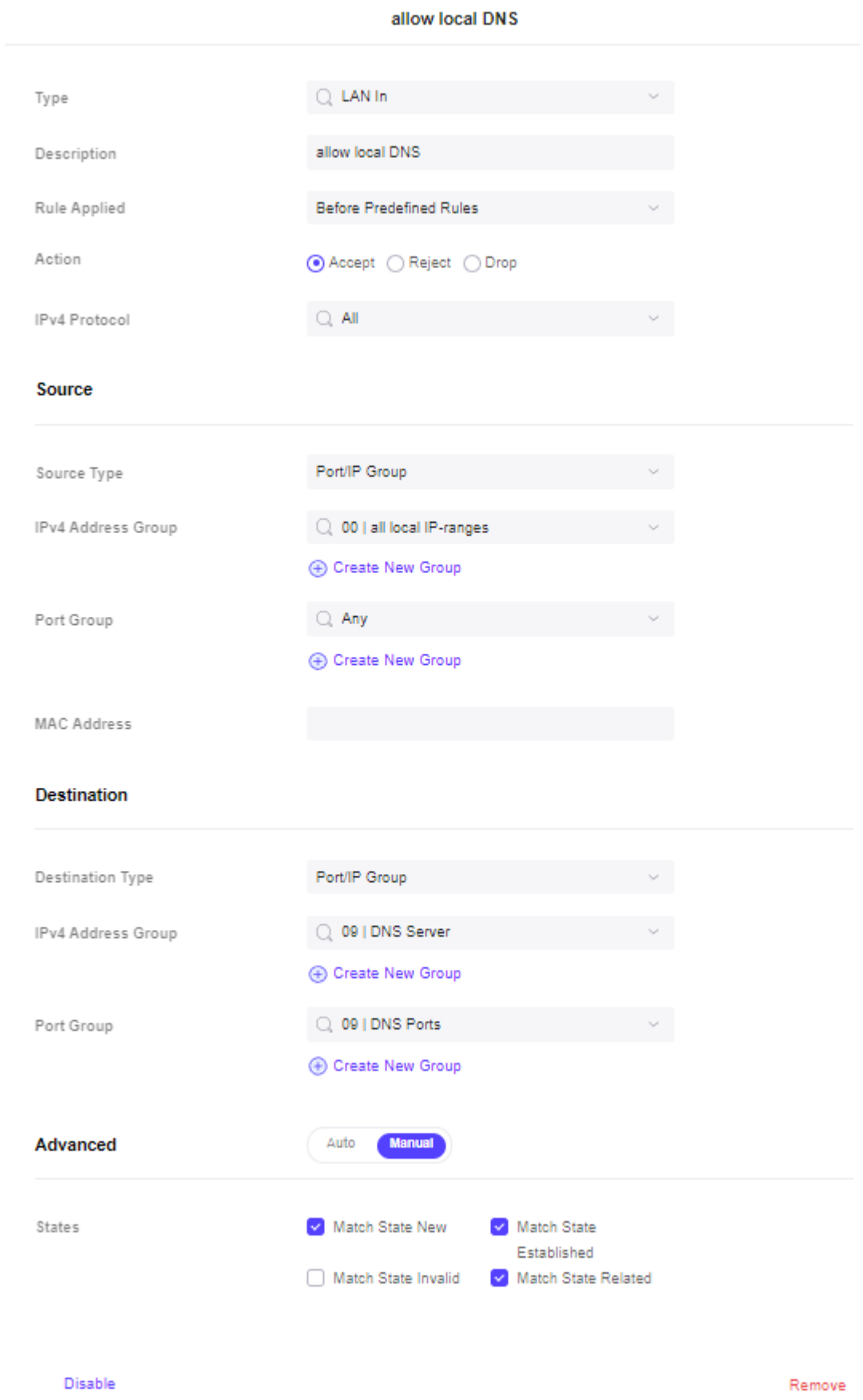

allow established/related sessions
Type
LAN In
Description
allow established/related sessions
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Port/IP Group
IPv4 Address Group
Any
Create New Group
Port Group
Any
Create New Group
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
Any
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
Disable
Remove


allow admin devices to MGMT LAN
Type
LAN In
Description
allow admin devices to MGMT LAN
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Port/IP Group
IPv4 Address Group
00 | admin devices
Create New Group
Port Group
Any
Create New Group
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
00 | all local Gateways
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
Disable
Remove

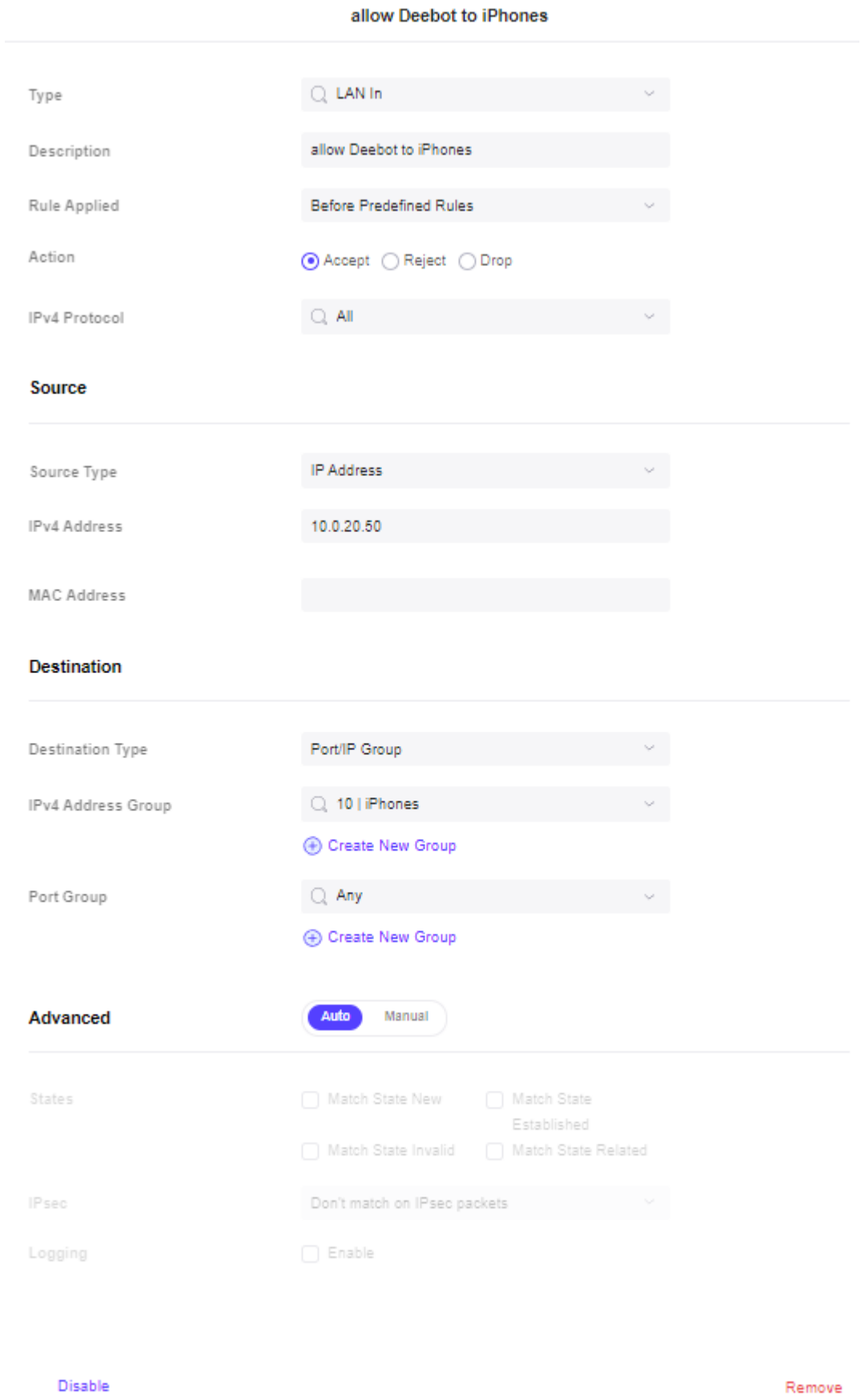
Hiermit sorgen wir dafür, dass unsere Admin Clients/devices auf das MGMT-LAN zugreifen können.


allow MGMT LAN to access all VLANs
Type
LAN In
Description
allow MGMT LAN to access all VLANs
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
01 | MGMT - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
00 | all local IP-ranges
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove

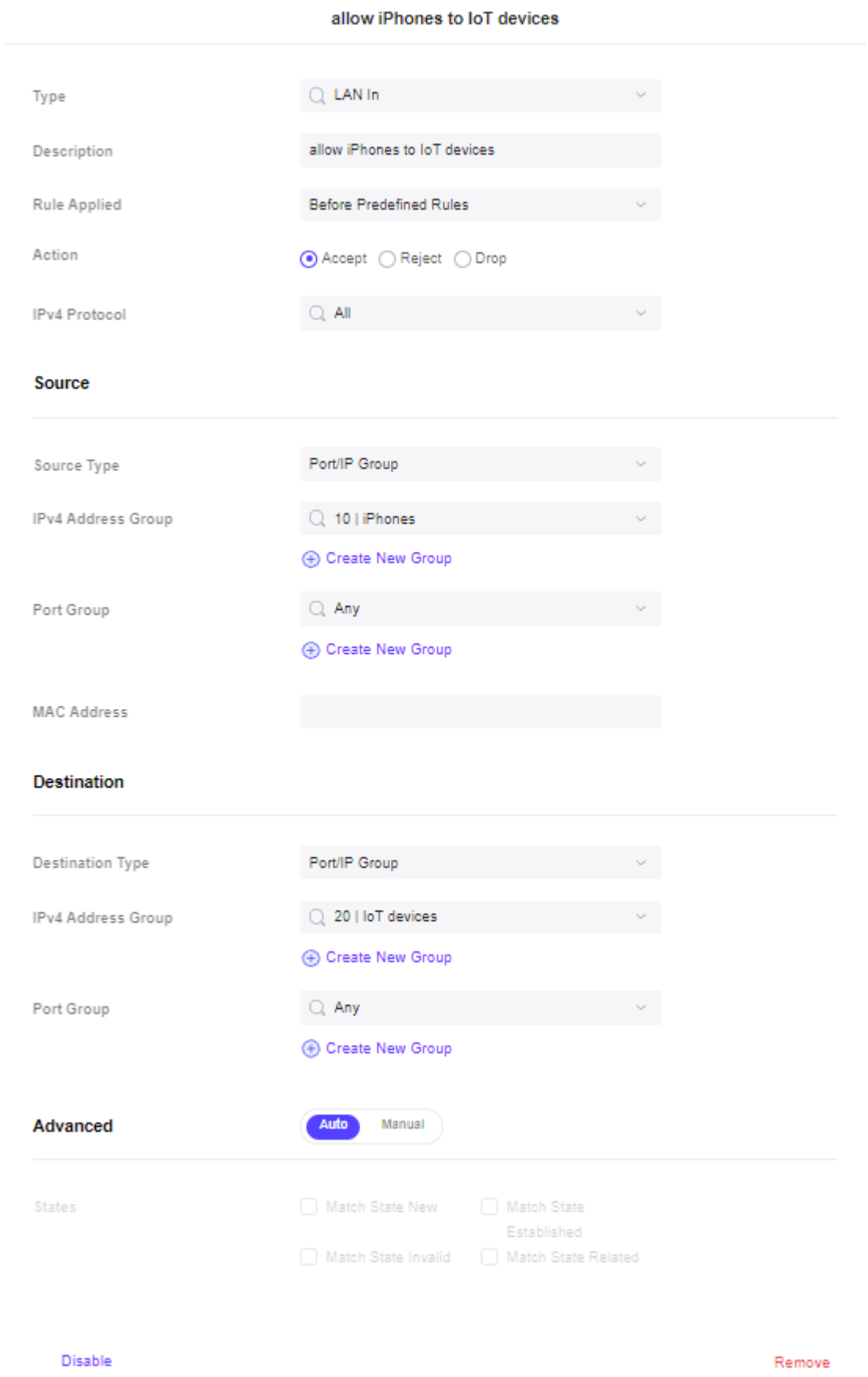
Hiermit sorgen wir dafür, dass unser MGMT-LAN sämtliche VLANs erreicht


allow local DNS
Type
LAN In
Description
allow local DNS
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Port/IP Group
IPv4 Address Group
00 | all local IP-ranges
Create New Group
Port Group
Any
Create New Group
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
09 | DNS Server
Create New Group
Port Group
09 | DNS Ports
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
Disable
Remove

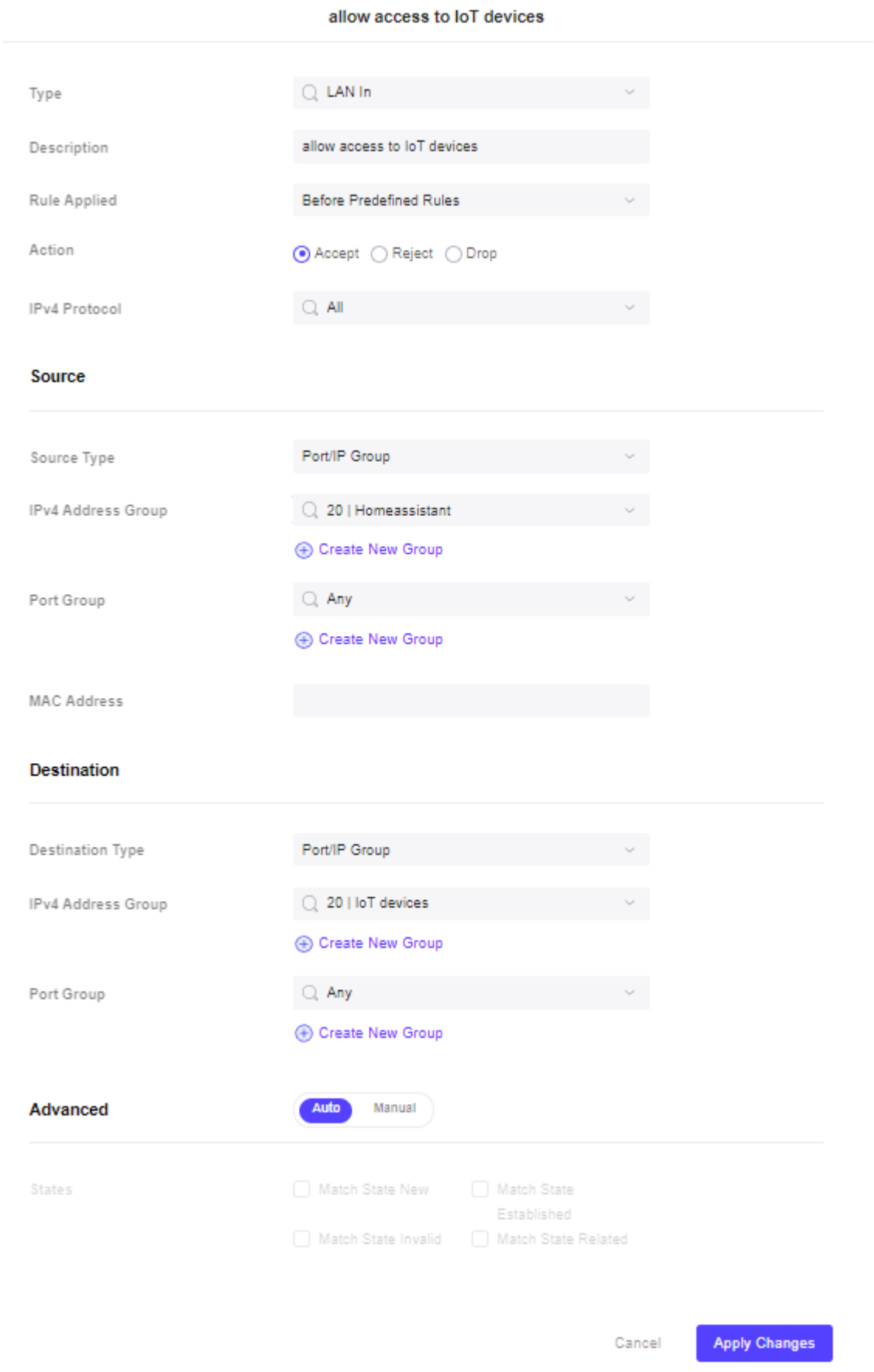
Hiermit sorgen wir dafür, dass unsere VLANs auf unseren lokalen DNS Server zugreifen können.


allow Deebot to iPhones
Type
LAN In
Description
allow Deebot to iPhones
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
IP Address
IPv4 Address
10.0.20.50
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
10 | iPhones
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove

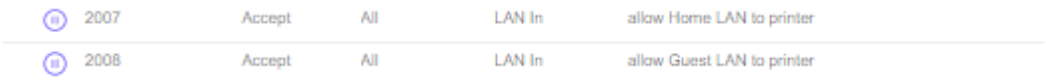
Ich hatte Probleme mit meinem Saugroboter, dafür war eine extra Regel beidseitig nötig


allow iPhones to IoT devices
Type
LAN In
Description
allow iPhones to IoT devices
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Port/IP Group
IPv4 Address Group
10 | iPhones
Create New Group
Port Group
Any
Create New Group
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
20 | IoT devices
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
Disable
Remove

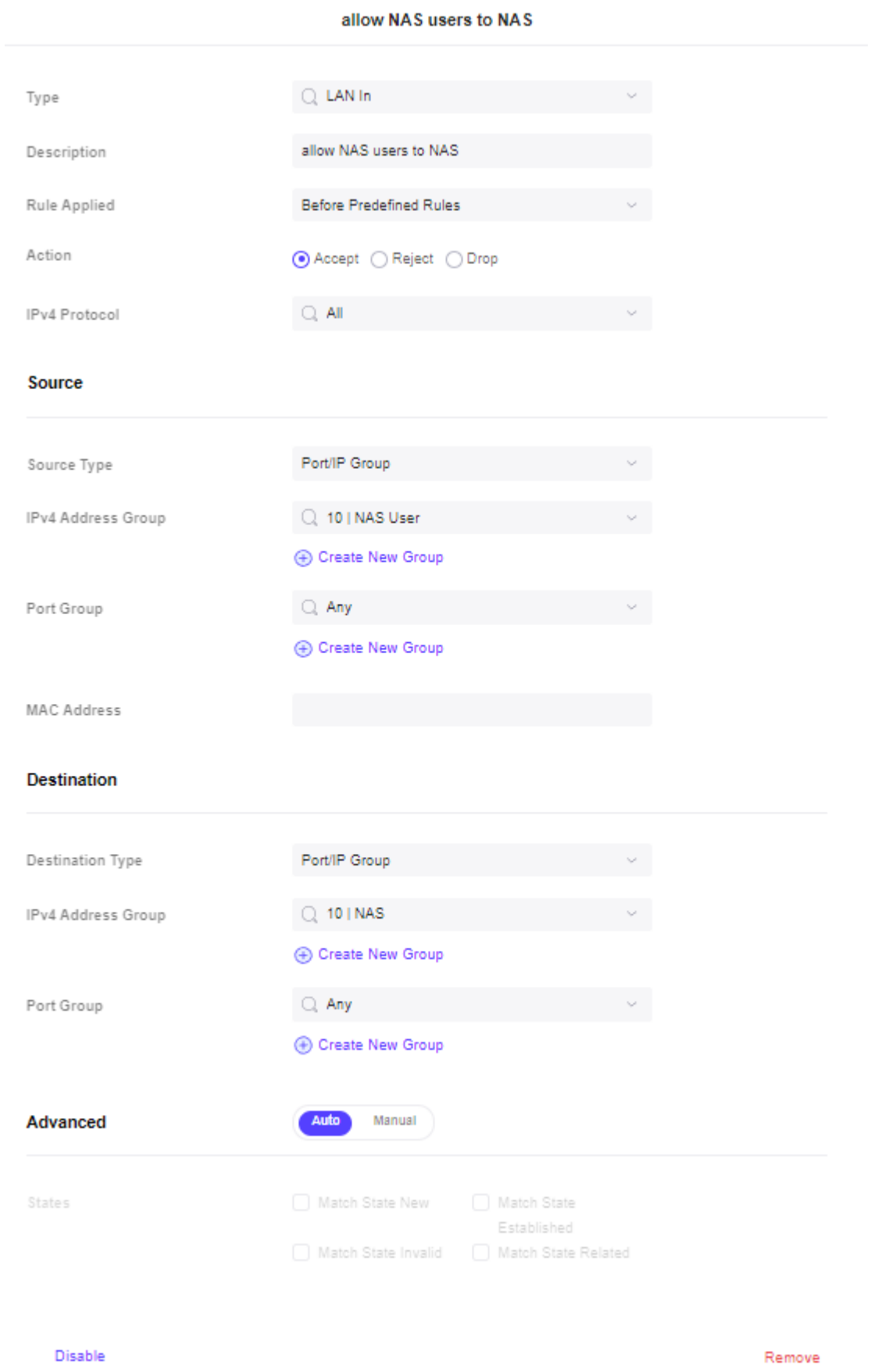
Ich möchte mit meinen iPhones auf sämtlich IoT devices zugreifen... autarkes Web IF von Lampen/Aktoren etc.pp


allow access to IoT devices
Type
LAN In
Description
allow access to IoT devices
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Port/IP Group
IPv4 Address Group
20 | Homeassistant
Create New Group
Port Group
Any
Create New Group
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
20 | IoT devices
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
Cancel
Apply Changes

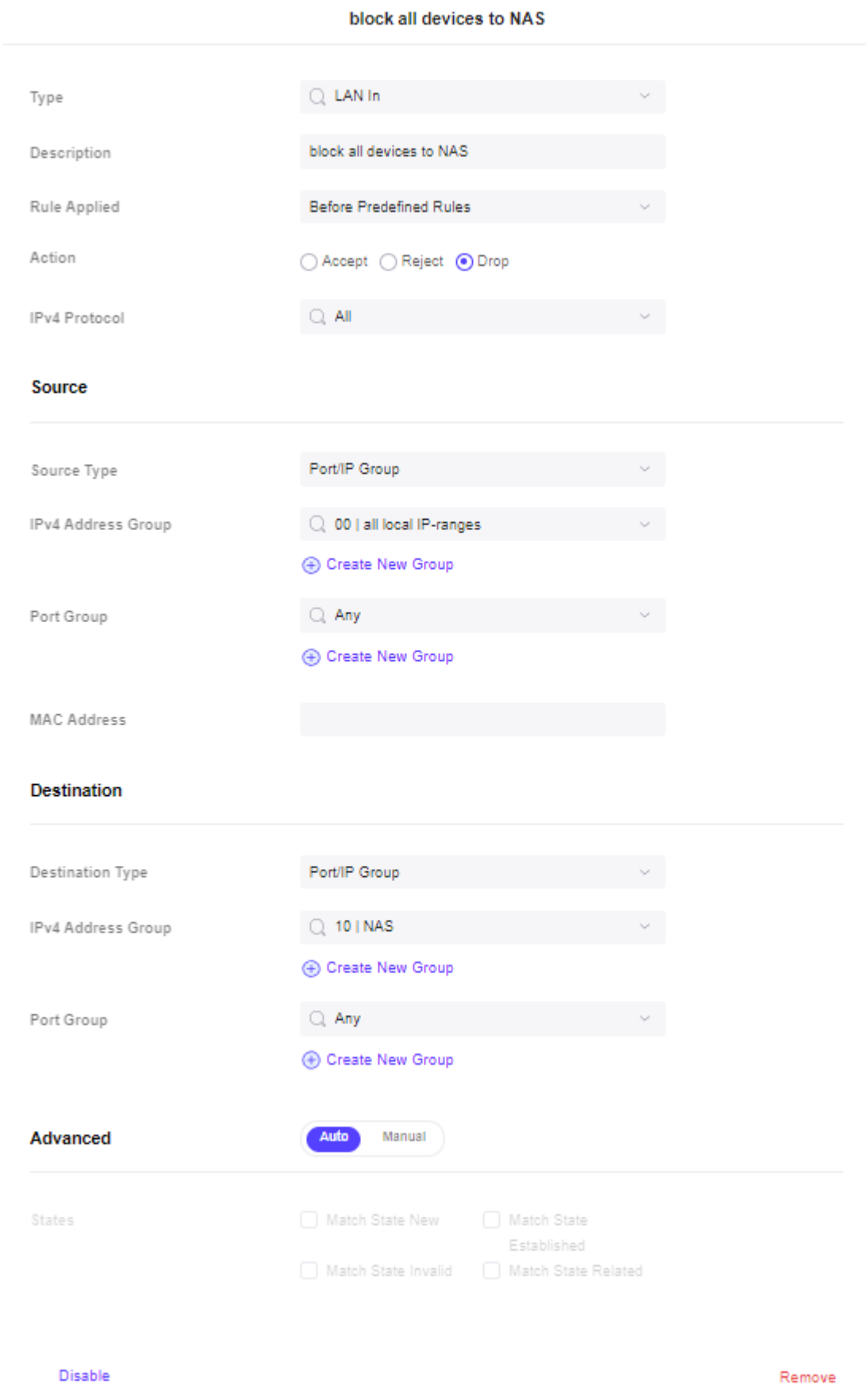
Der Homeassistant aka Smarthome Zentrale will natürlich auch auf alle IoT Devices zugreifen!



Auf diese Regeln werde ich nicht genauer eingehen, da es selbsterklärend ist!

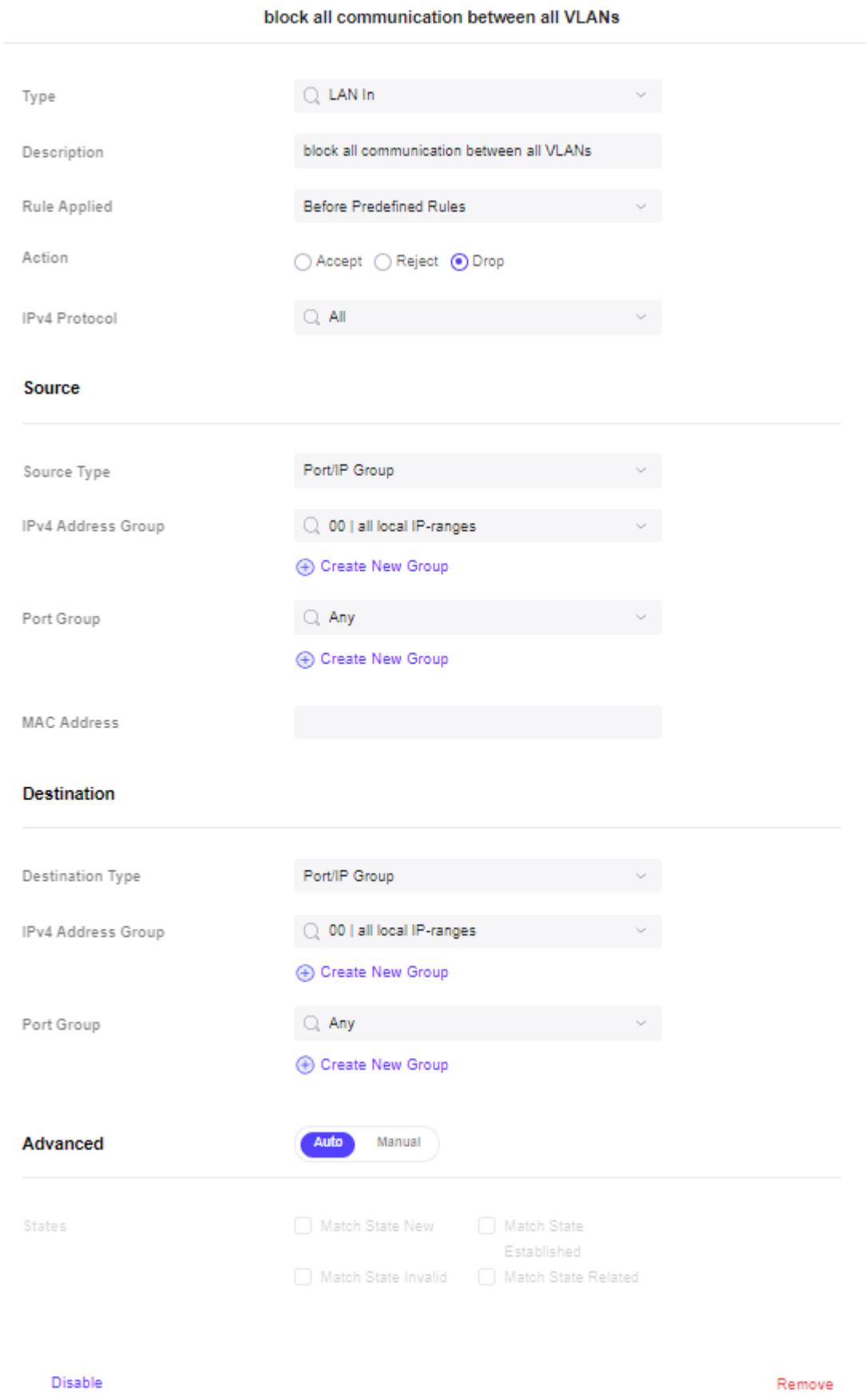

allow NAS users to NAS
Type
LAN In
Description
allow NAS users to NAS
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Port/IP Group
IPv4 Address Group
10 | NAS User
Create New Group
Port Group
Any
Create New Group
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
10 | NAS
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
Disable
Remove

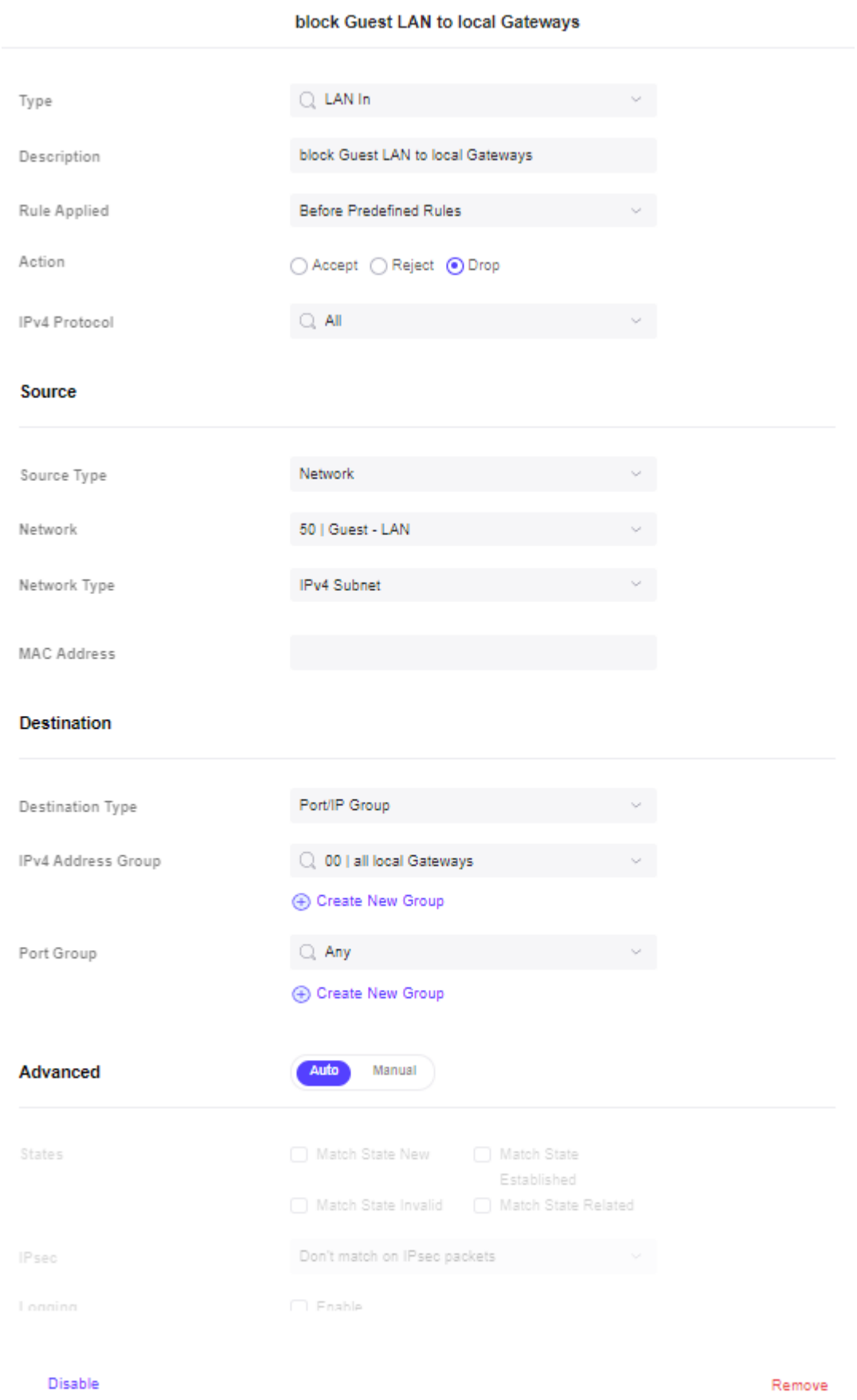
Hier erlauben wir, welche User auf das NAS zugreifen dürfen

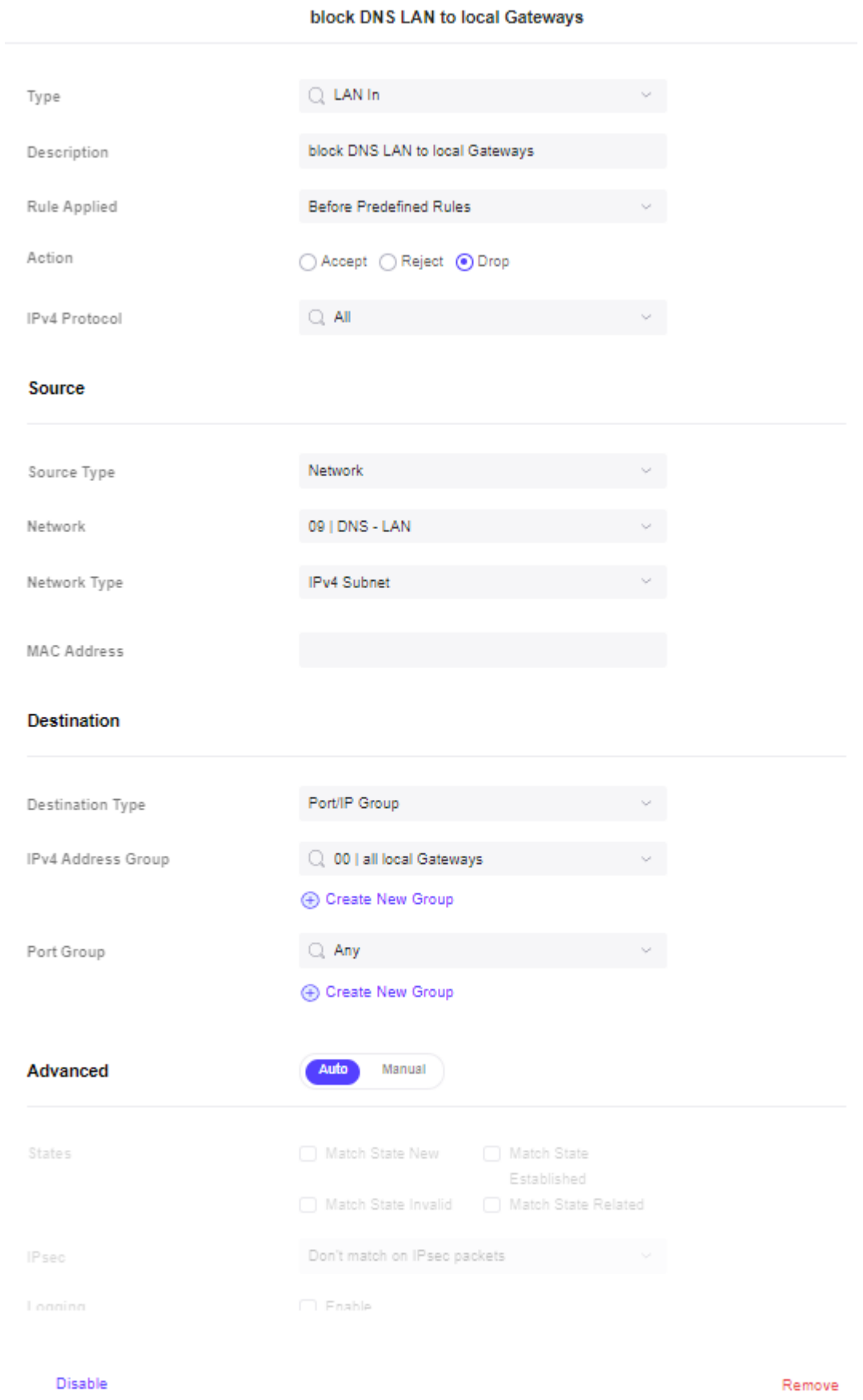

block all devices to NAS
Type
LAN In
Description
block all devices to NAS
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Port/IP Group
IPv4 Address Group
00 | all local IP-ranges
Create New Group
Port Group
Any
Create New Group
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
10 | NAS
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
Disable
Remove

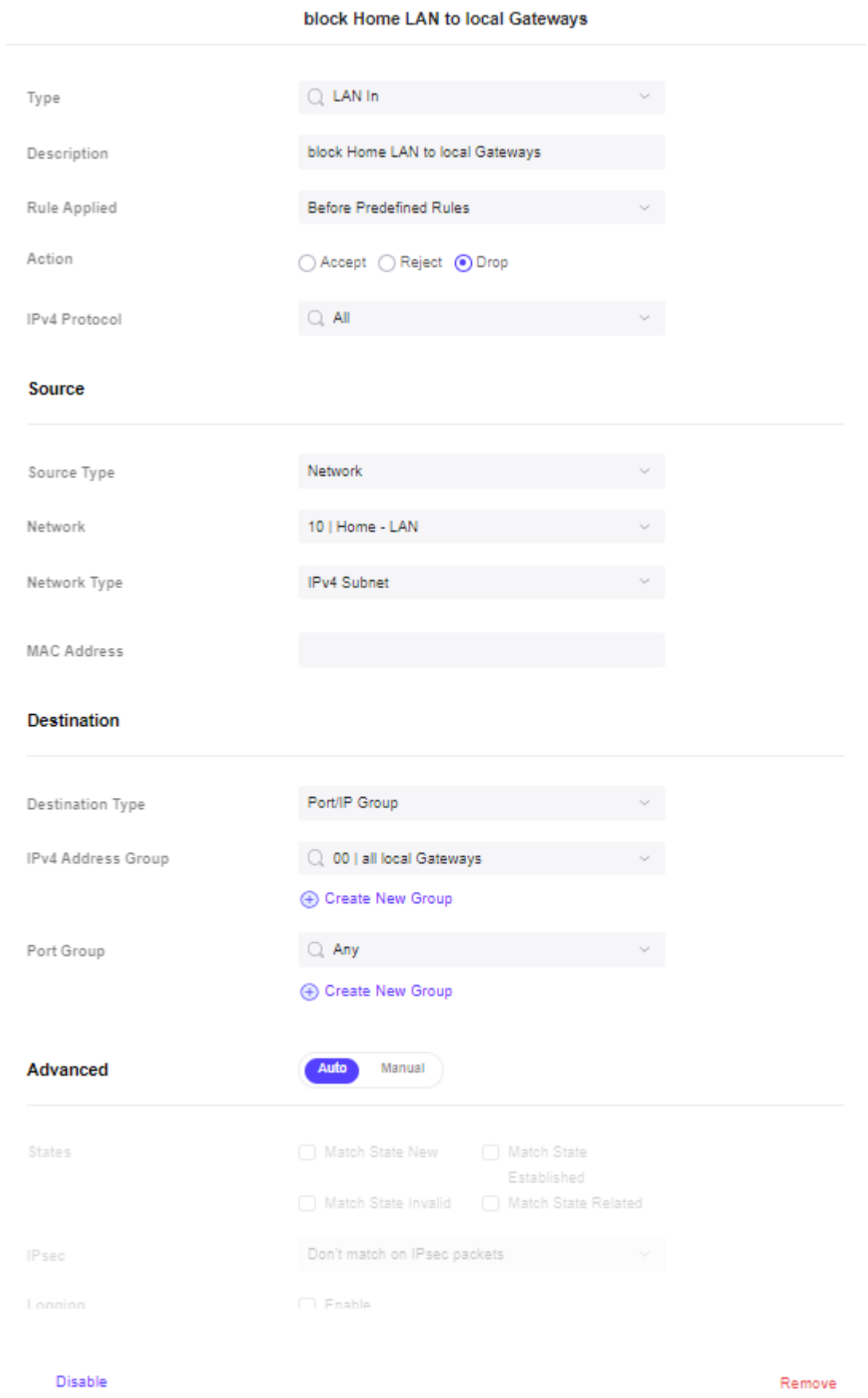
Hier blocken wir sämtliche andere Kommunikation zum NAS

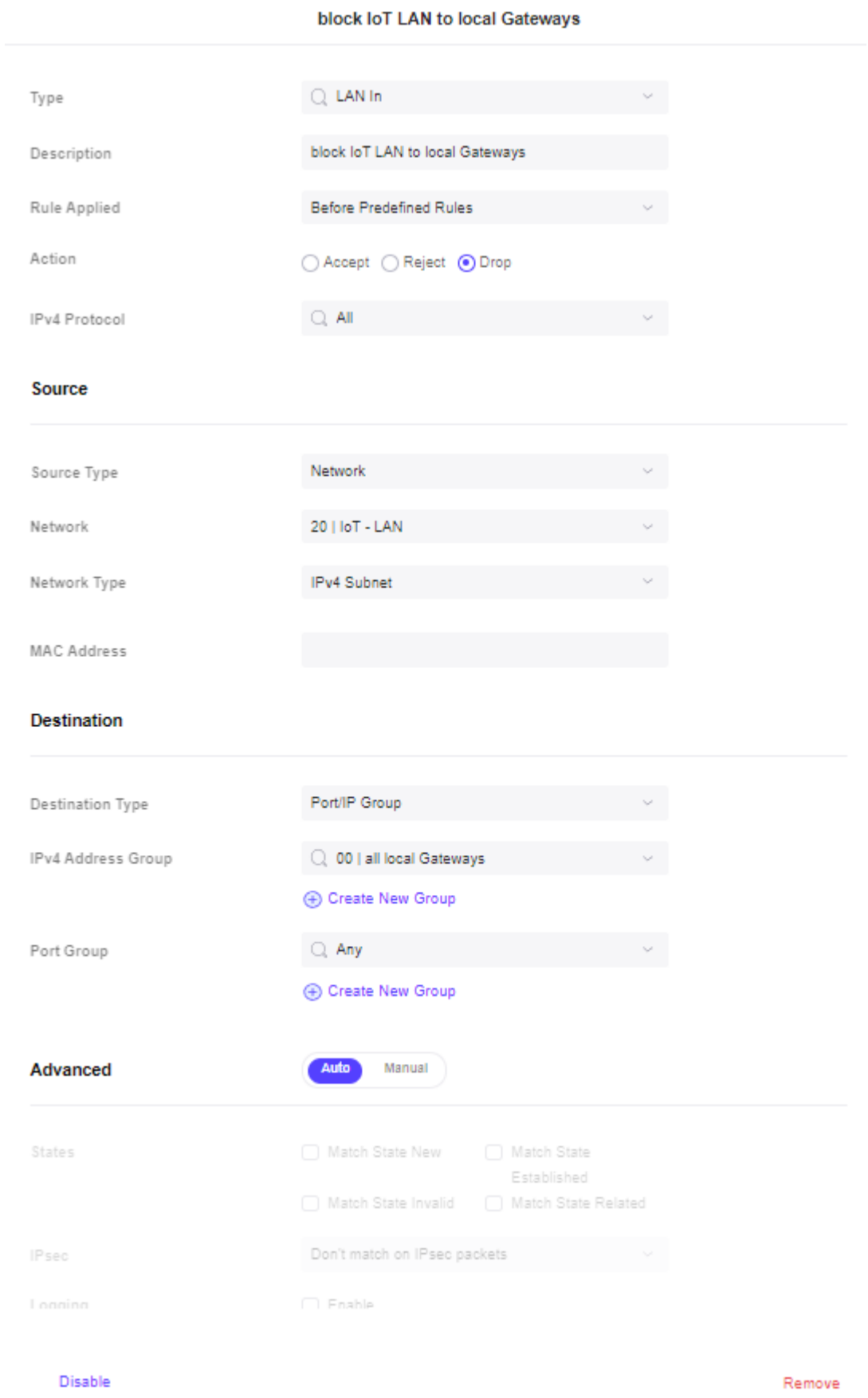
Jetzt wird's spannend! Wir blocken die komplette VLAN Kommunikation gegeneinander


block all communication between all VLANs
Type
LAN In
Description
block all communication between all VLANs
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Port/IP Group
IPv4 Address Group
00 | all local IP-ranges
Create New Group
Port Group
Any
Create New Group
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
00 | all local IP-ranges
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
Disable
Remove

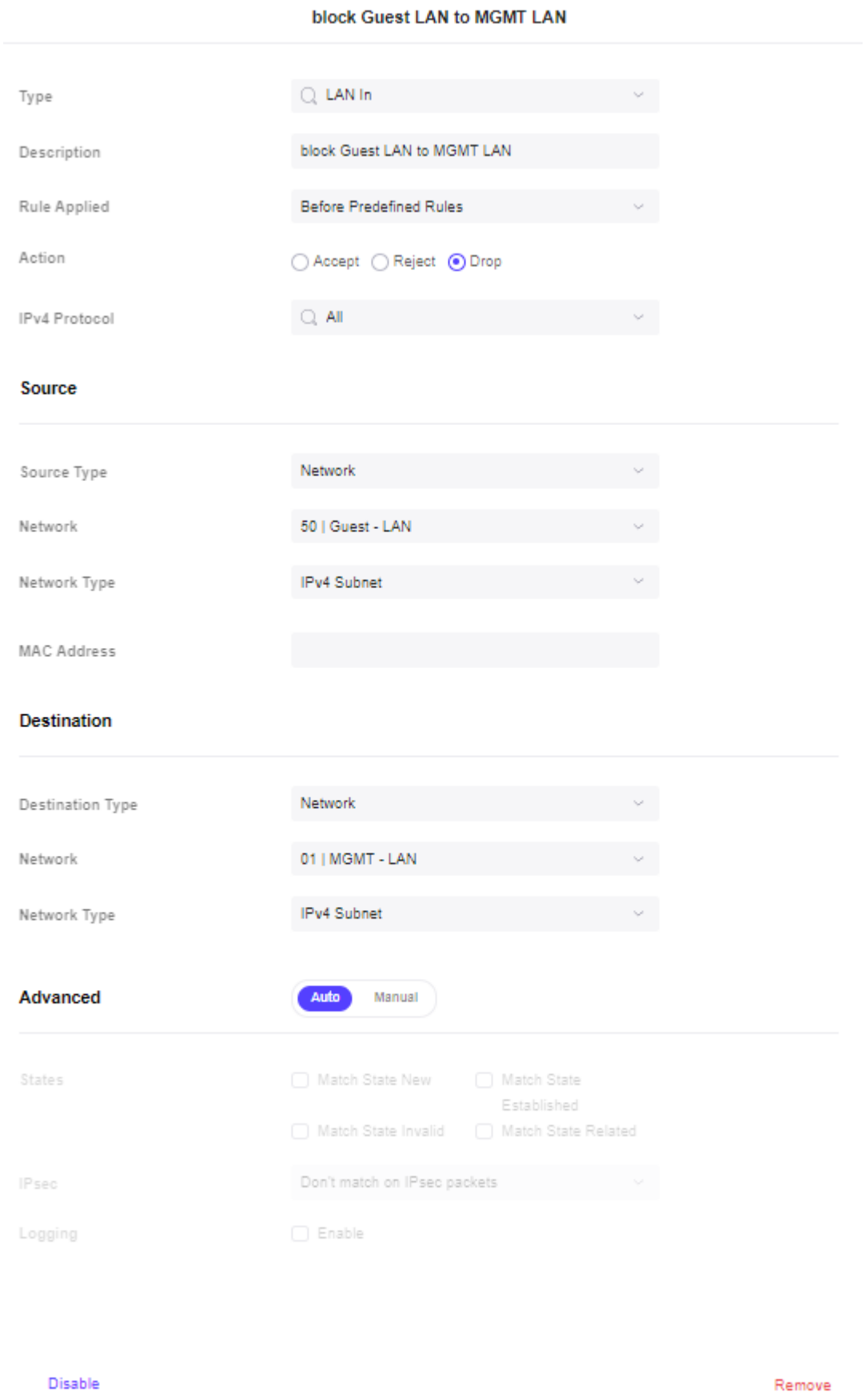

block Guest LAN to local Gateways
Type
LAN In
Description
block Guest LAN to local Gateways
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
50 | Guest - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
00 | all local Gateways
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove

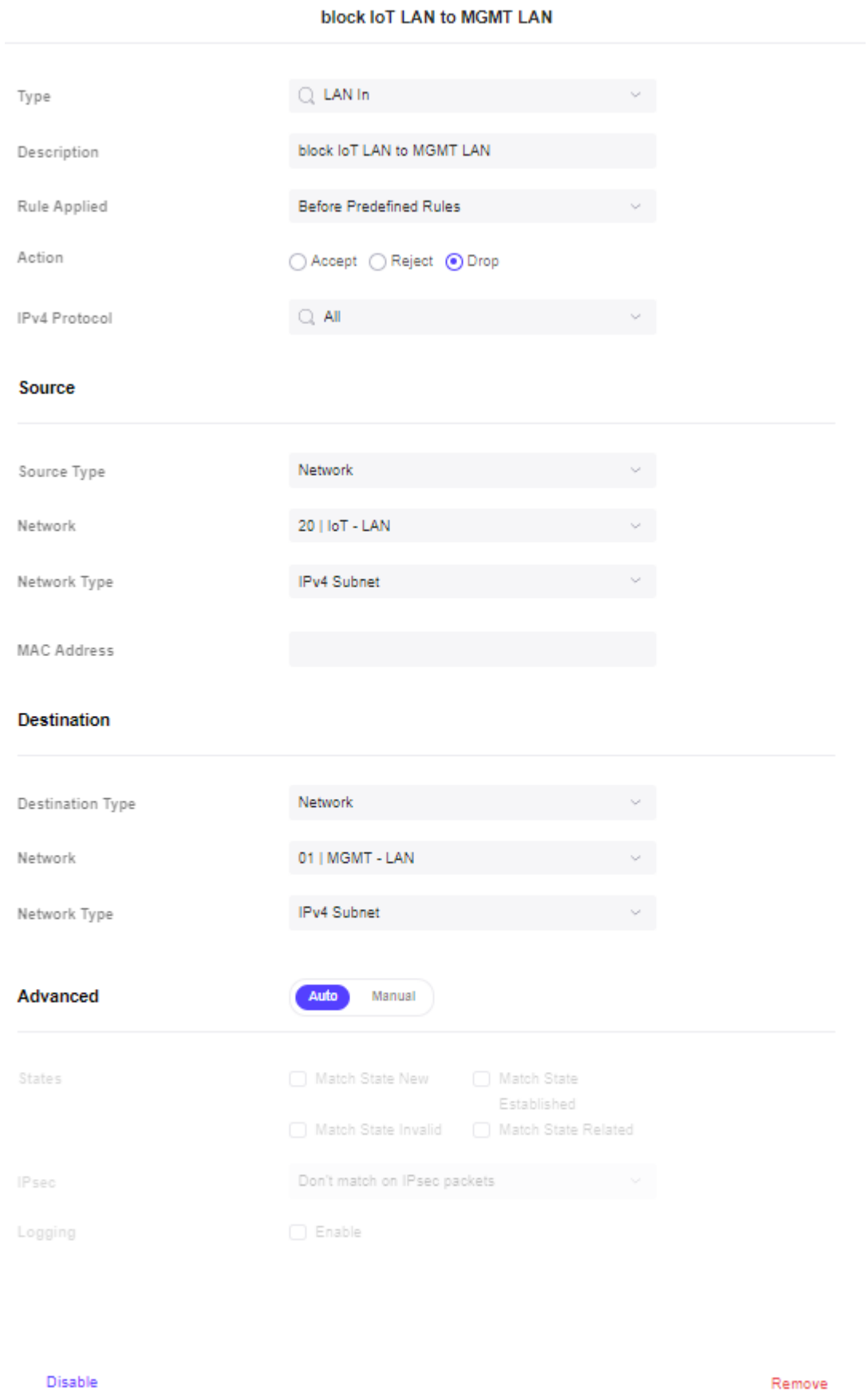

block DNS LAN to local Gateways
Type
LAN In
Description
block DNS LAN to local Gateways
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
09 | DNS - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
00 | all local Gateways
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove

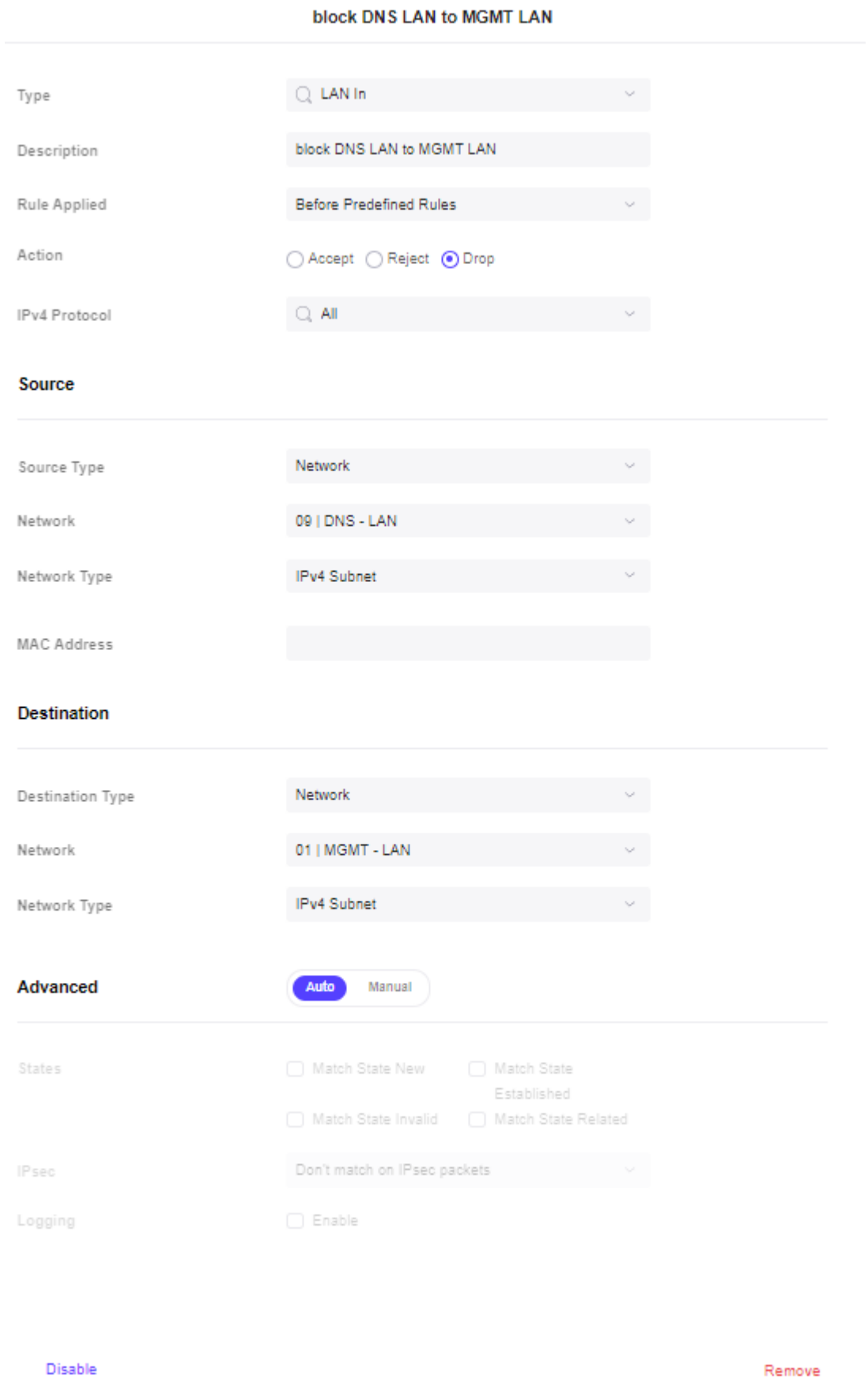

block Home LAN to local Gateways
Type
LAN In
Description
block Home LAN to local Gateways
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
10 | Home - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
00 | all local Gateways
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove

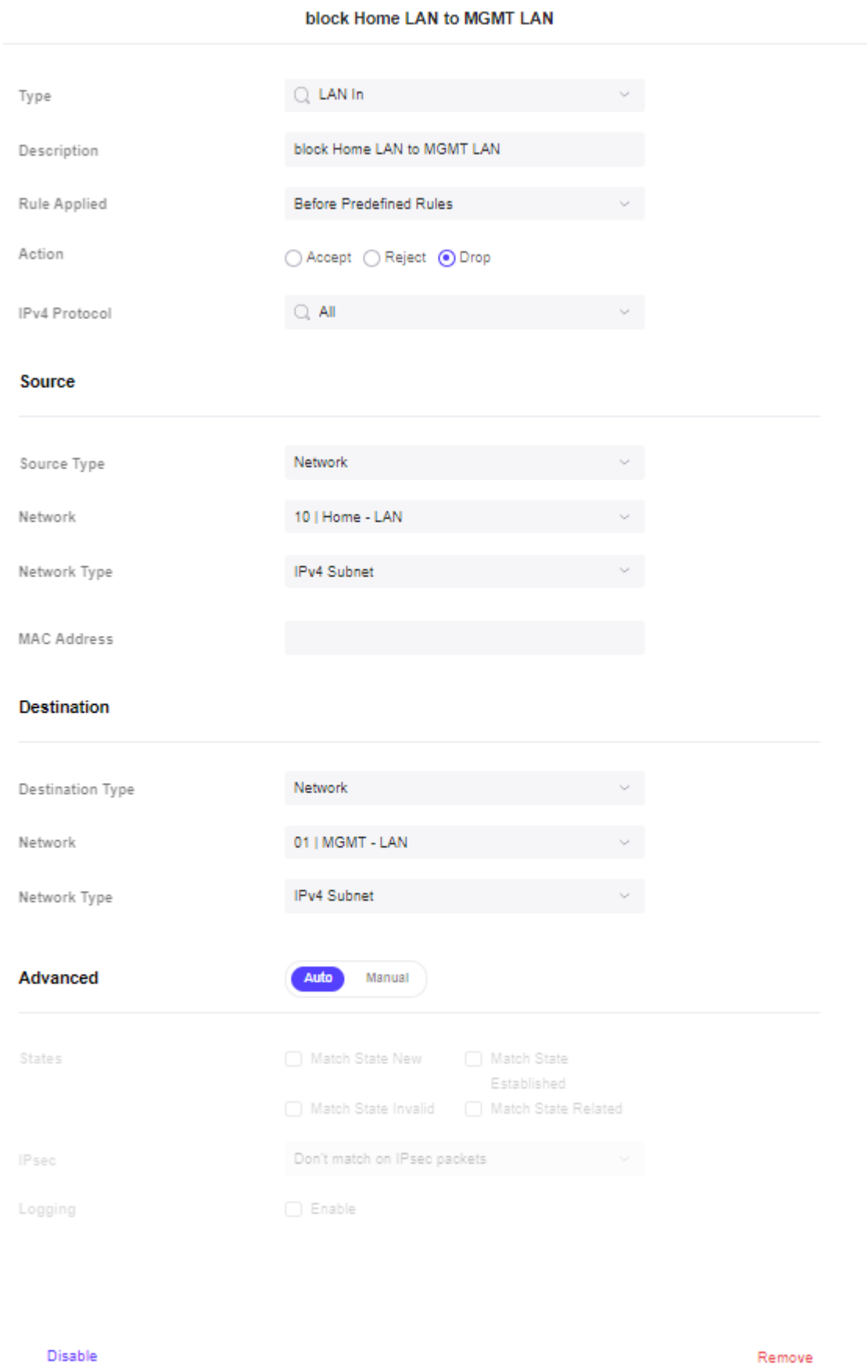

block IoT LAN to local Gateways
Type
LAN In
Description
block IoT LAN to local Gateways
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
20 | IoT - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
00 | all local Gateways
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove

Und es wird noch spannender! Wir blocken die gesamte Gateway Kommunikation in Richtung MGMT-LAN (dafür brauchen wir aber established&related)


block Guest LAN to MGMT LAN
Type
LAN In
Description
block Guest LAN to MGMT LAN
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
50 | Guest - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Network
Network
01 | MGMT - LAN
Network Type
IPv4 Subnet
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove


block IoT LAN to MGMT LAN
Type
LAN In
Description
block IoT LAN to MGMT LAN
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
20 | IoT - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Network
Network
01 | MGMT - LAN
Network Type
IPv4 Subnet
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove

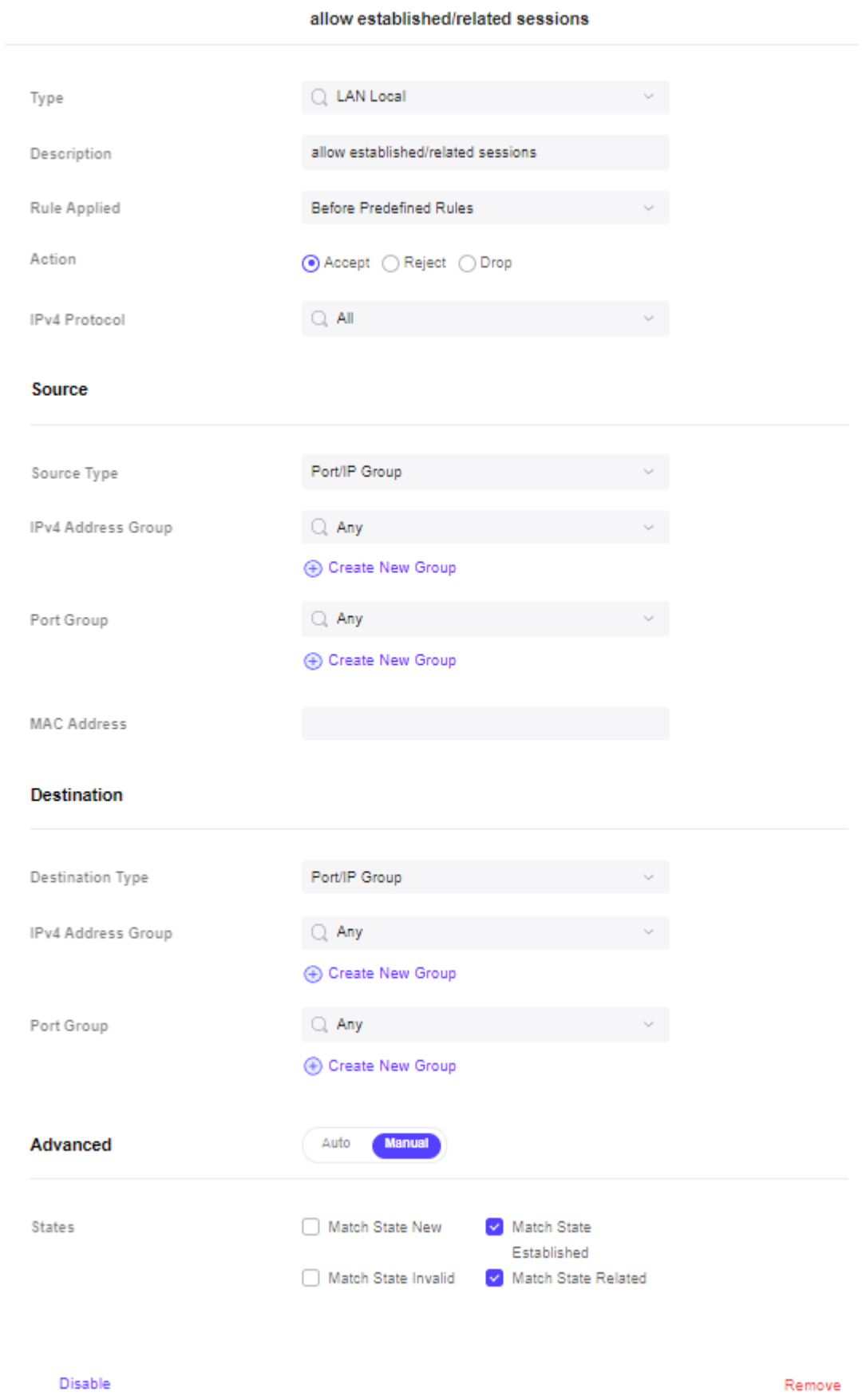

block DNS LAN to MGMT LAN
Type
LAN In
Description
block DNS LAN to MGMT LAN
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
09 | DNS - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Network
Network
01 | MGMT - LAN
Network Type
IPv4 Subnet
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove

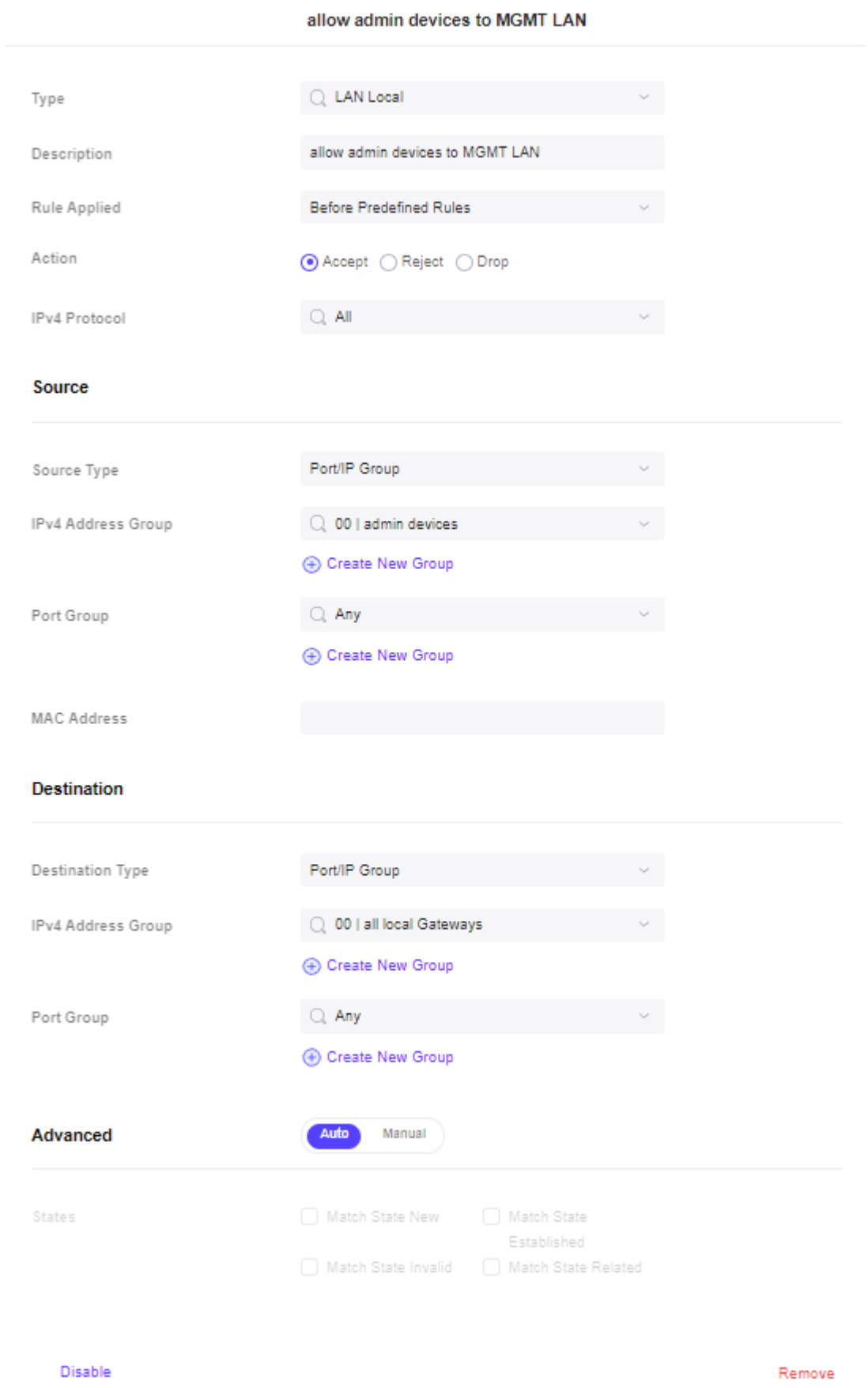

block Home LAN to MGMT LAN
Type
LAN In
Description
block Home LAN to MGMT LAN
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
10 | Home - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Network
Network
01 | MGMT - LAN
Network Type
IPv4 Subnet
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove

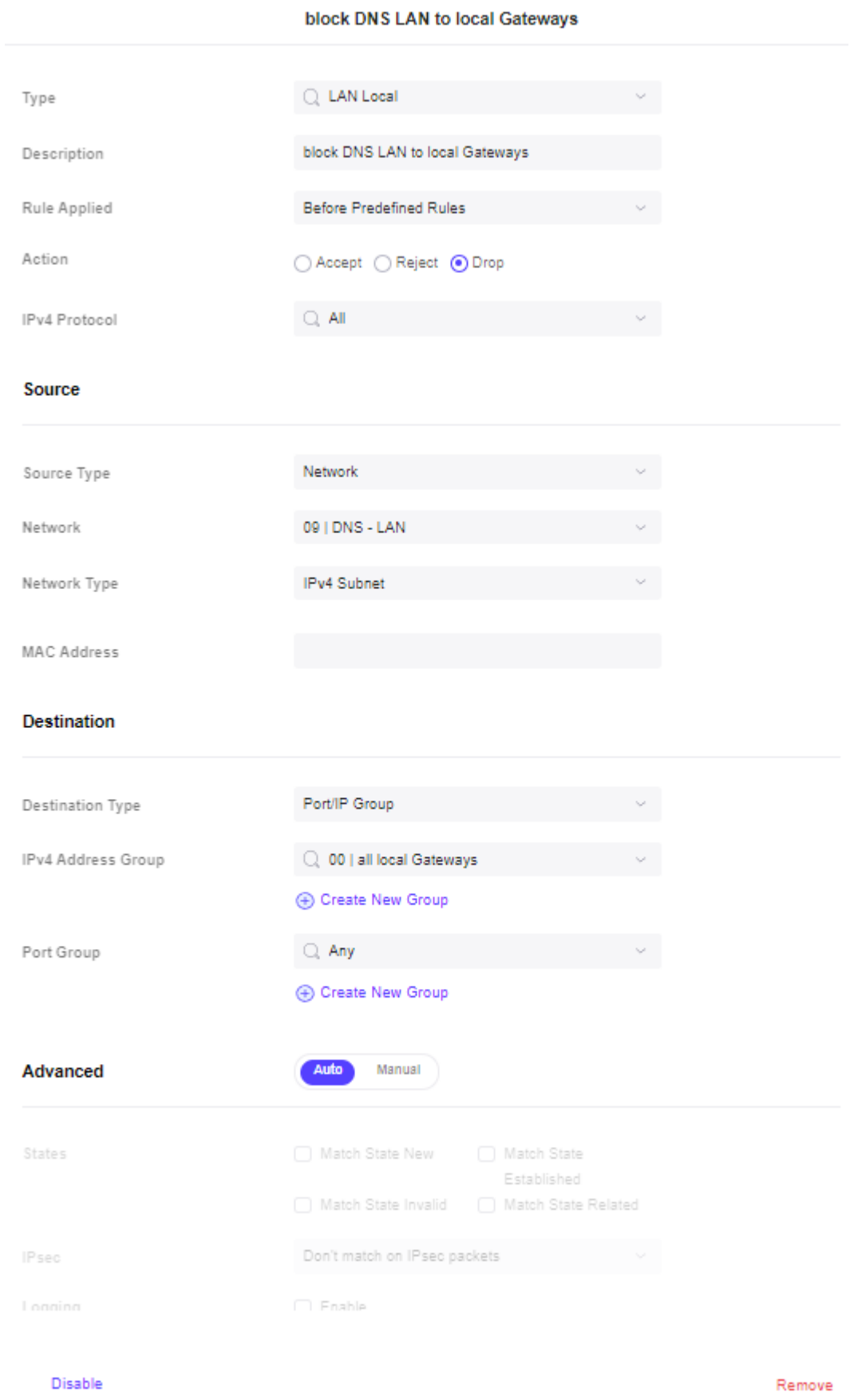
Ihr seid jetzt schon wirklich gut abgesichert! aber wir treiben es noch etwas weiter!

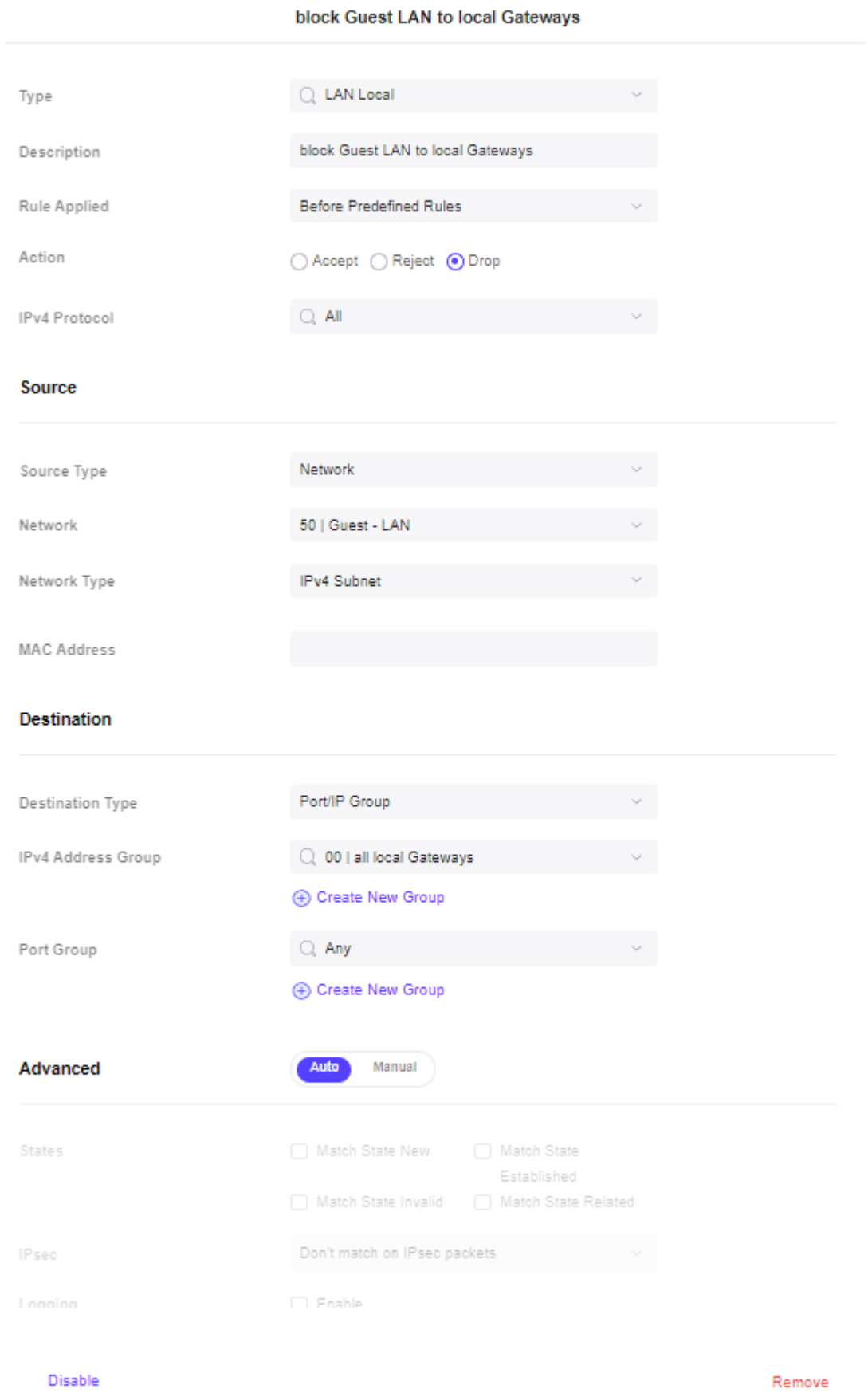
Wir werden jetzt noch den Traffic auf lokaler Gateway Ebene (UDM/UDMP/UDR/UXG etc.pp.) beschränken.

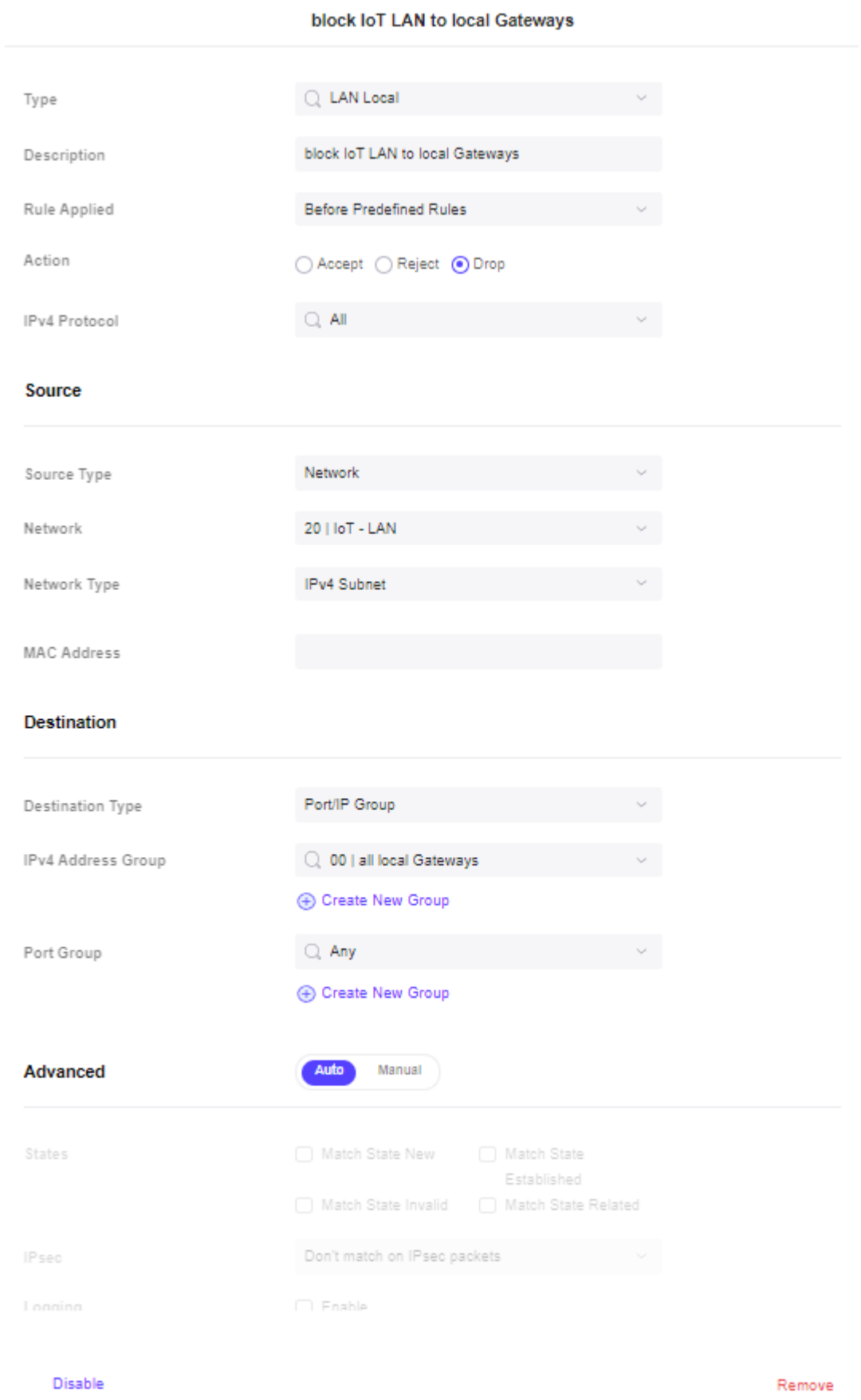
Settings -> Firewall & Security -> Create New Rule -> LAN Local ***(gilt ab jetzt für alle Rules)***

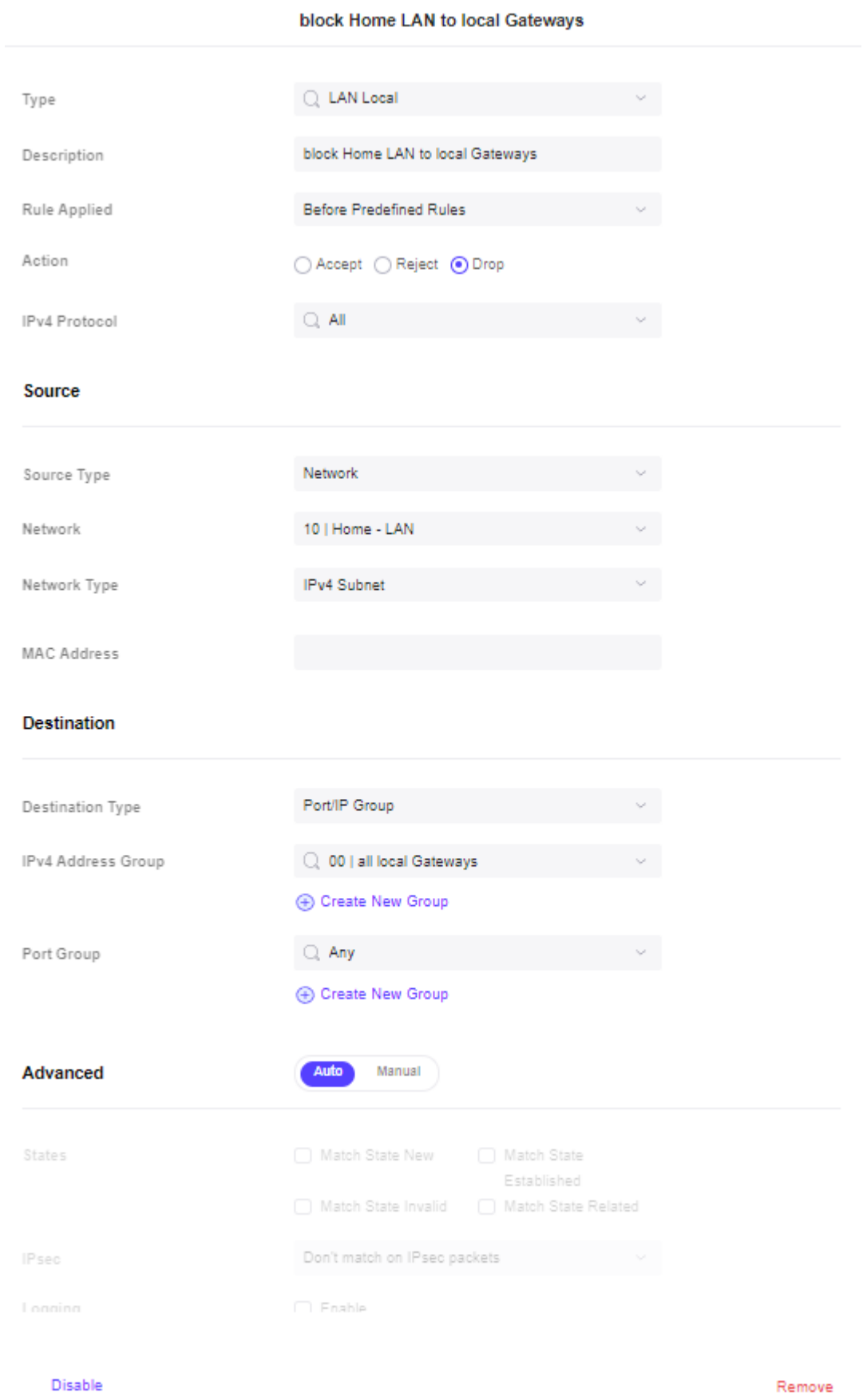

allow established/related sessions
Type
LAN Local
Description
allow established/related sessions
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Port/IP Group
IPv4 Address Group
Any
Create New Group
Port Group
Any
Create New Group
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
Any
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
Disable
Remove

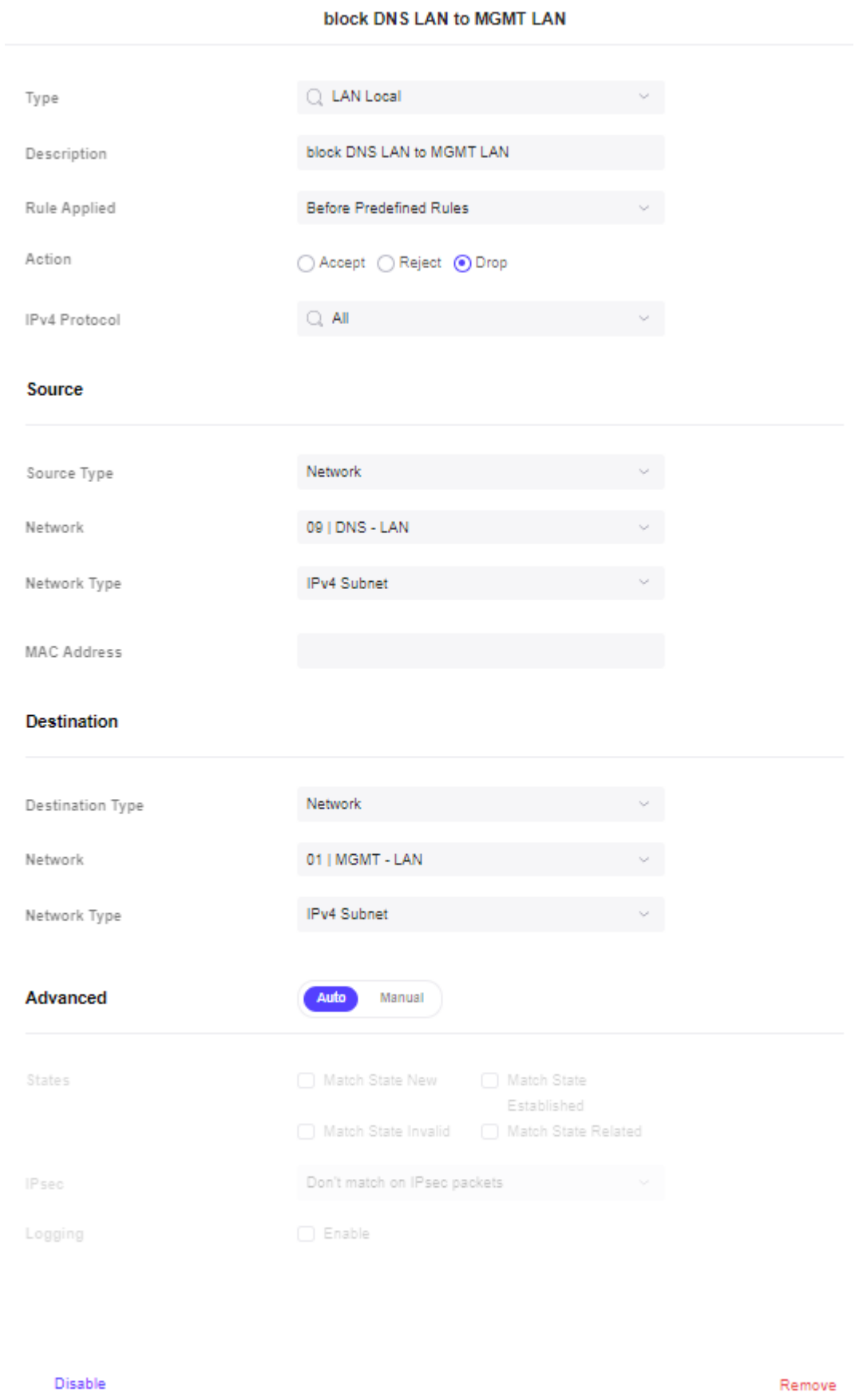

allow admin devices to MGMT LAN
Type
LAN Local
Description
allow admin devices to MGMT LAN
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Port/IP Group
IPv4 Address Group
00 | admin devices
Create New Group
Port Group
Any
Create New Group
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
00 | all local Gateways
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
Disable
Remove

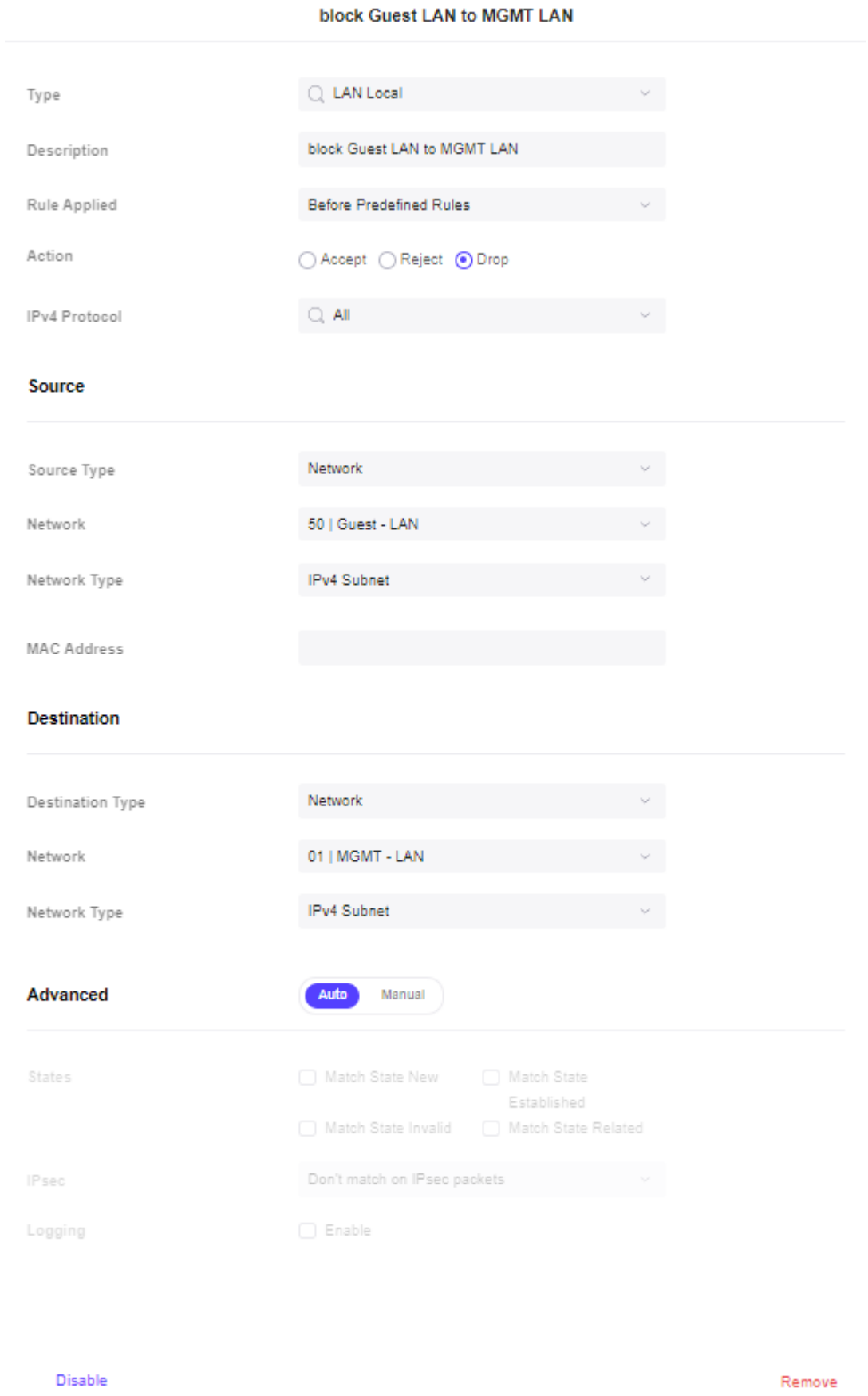

block DNS LAN to local Gateways
Type
LAN Local
Description
block DNS LAN to local Gateways
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
09 | DNS - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
00 | all local Gateways
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove

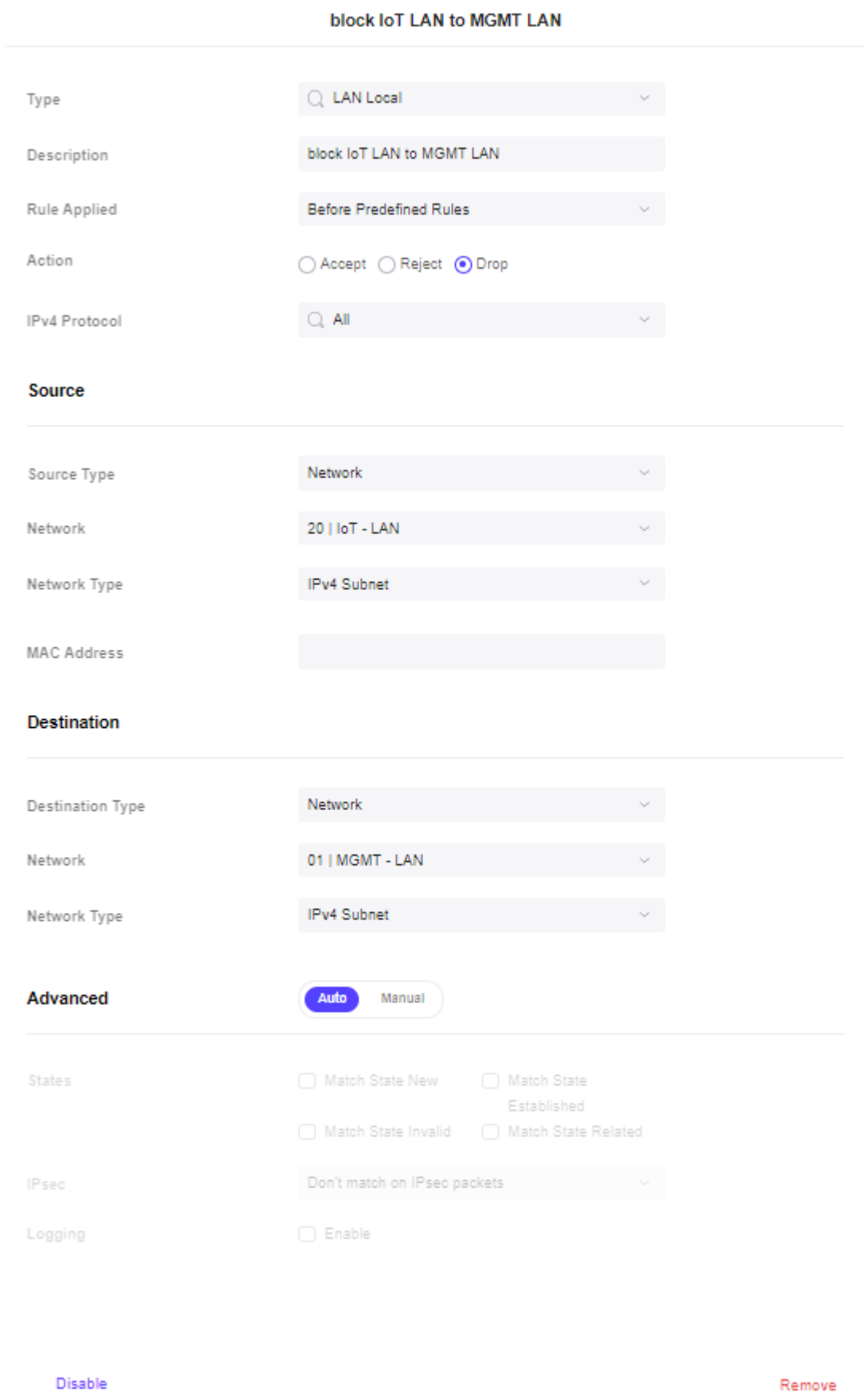

block Guest LAN to local Gateways
Type
LAN Local
Description
block Guest LAN to local Gateways
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
50 | Guest - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
00 | all local Gateways
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove

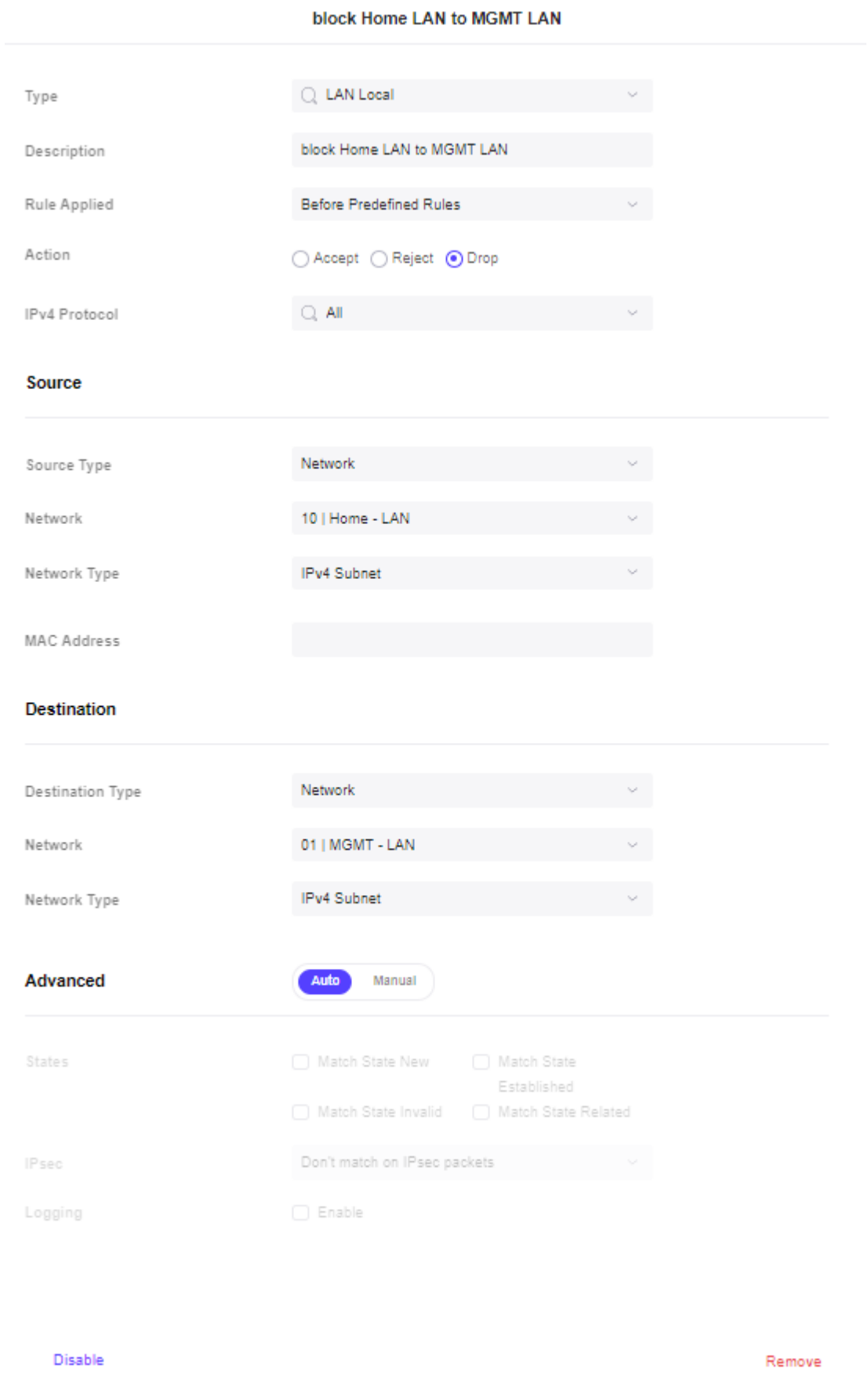

block IoT LAN to local Gateways
Type
LAN Local
Description
block IoT LAN to local Gateways
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
20 | IoT - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
00 | all local Gateways
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove


block Home LAN to local Gateways
Type
LAN Local
Description
block Home LAN to local Gateways
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
10 | Home - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Port/IP Group
IPv4 Address Group
00 | all local Gateways
Create New Group
Port Group
Any
Create New Group
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove


block DNS LAN to MGMT LAN
Type
LAN Local
Description
block DNS LAN to MGMT LAN
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
09 | DNS - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Network
Network
01 | MGMT - LAN
Network Type
IPv4 Subnet
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove


block Guest LAN to MGMT LAN
Type
LAN Local
Description
block Guest LAN to MGMT LAN
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
50 | Guest - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Network
Network
01 | MGMT - LAN
Network Type
IPv4 Subnet
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove


block IoT LAN to MGMT LAN
Type
LAN Local
Description
block IoT LAN to MGMT LAN
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
20 | IoT - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Network
Network
01 | MGMT - LAN
Network Type
IPv4 Subnet
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove


block Home LAN to MGMT LAN
Type
LAN Local
Description
block Home LAN to MGMT LAN
Rule Applied
Before Predefined Rules
Action
Accept
Reject
Drop
IPv4 Protocol
All
Source
Source Type
Network
Network
10 | Home - LAN
Network Type
IPv4 Subnet
MAC Address
Destination
Destination Type
Network
Network
01 | MGMT - LAN
Network Type
IPv4 Subnet
Advanced
Auto
Manual
States
Match State New
Match State Established
Match State Invalid
Match State Related
IPsec
Don't match on IPsec packets
Logging
Enable
Disable
Remove

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 Garantie auf Erfolg. Im Falle eines Misserfolges hilft aber die Community hier sicherlich 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!