MACMON NAC WHITEPAPER

Connection with Barracuda CloudGen Firewall

Contents

Version: 1.6_en

Introduction

Barracuda simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications and data regardless of where they reside. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. It uses scanners to detect threats to the network and infected endpoint devices, that can be reported to macmon secure's NAC solution. As a reaction to this report, macmon NAC is able to isolate this very device and physically disconnect it from the network. On the other hand, macmon NAC can pass MAC addresses of new devices to Barracuda CloudGen Firewall so that they are immediately known to the firewall system.

Use Cases

macmon NAC passes new trustworthy endpoint devices to Barracuda CloudGen Firewall

In a hospital it might make sense to separate medical devices from management computers by segmenting the network. Nevertheless, a few specially protected and therefore suitable computers are supposed to be able to access the result database of a medical device. Since macmon NAC permits or denies access to an entire network segment, an interface to a firewall that can control access via certain policies is an ideal solution. Once an endpoint device connects to the network, it gets its IP address assigned by the DHCP server and has access to the network. If this endpoint device was assigned to a trusted devices group the MAC address with currently valid IP address can be passed to a Barracuda CloudGen Firewall via the interface presented in this document. macmon NAC gains the ability to grant exactly this device access to a specially protected network segment.

Barracuda CloudGen Firewall passes infected endpoint devices to macmon NAC

Threats could be lurking on the same network. An endpoint device can be infected by various mechanisms of malware and thus behave conspicuously on the network. Barracuda CloudGen Firewall detects the malicious behavior and can inform the network administrator about the discovered threat who in turn can take the necessary steps to remediation. The reaction to the discovery of an infected endpoint device can be automated with the interface presented in this document. After the discovery Barracuda CloudGen Firewall passed the identity of this device to macmon NAC, it gets treated or is isolated according to pre-defined or own policies. This gives Barracuda CloudGen Firewall the ability to selectively remove a device from a network segment for remediation.

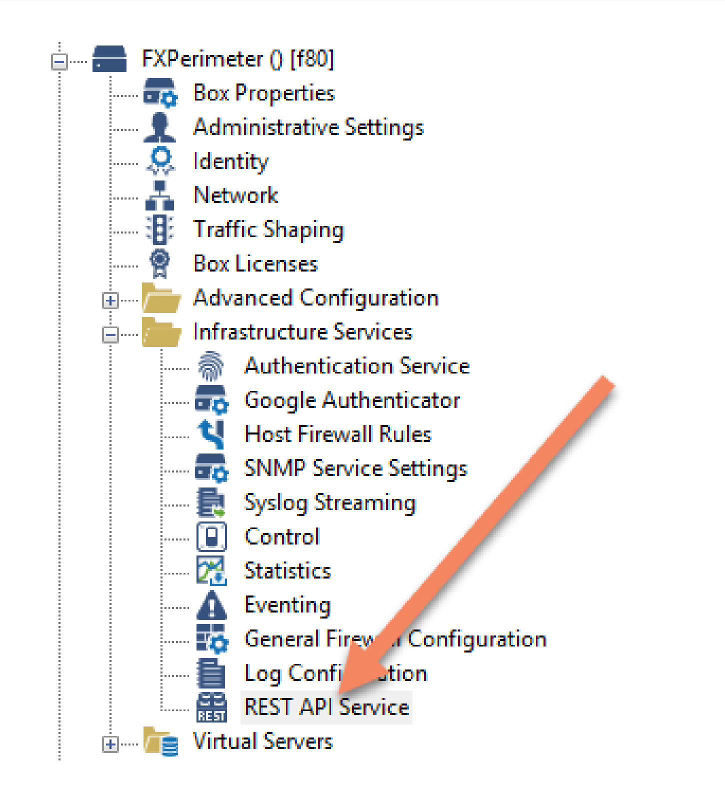
Requirements

In order to integrate the Barracuda CloudGen Firewall with macmon NAC the macmon premium bundle subscription is required.

Configuration of Barracuda CloudGen Firewall

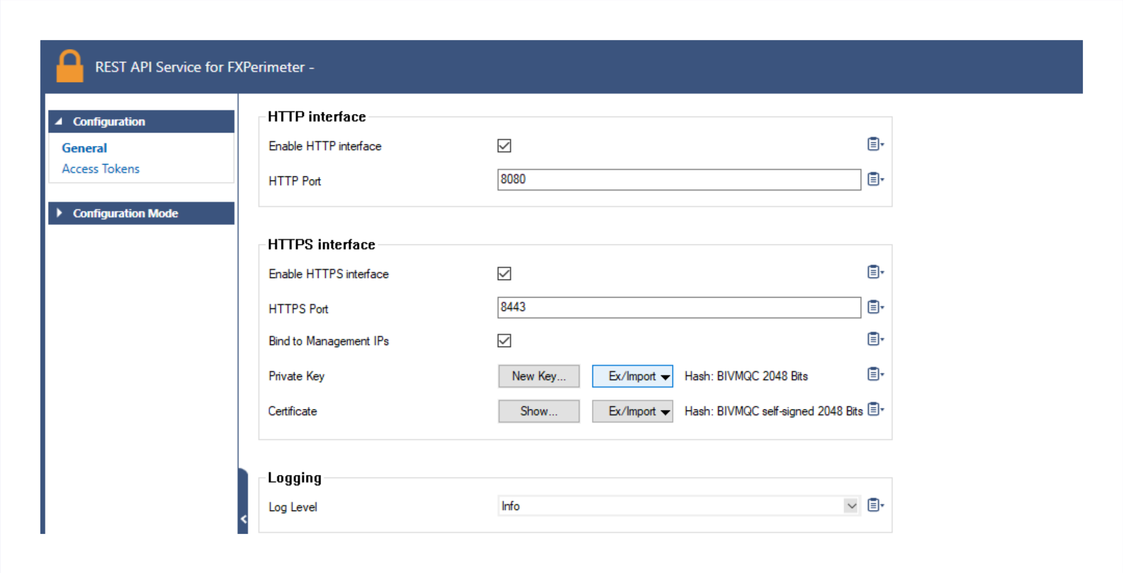
Preparation of the REST API service

Please start the application Firewall Admin and connect to your Barracuda CloudGen Firewall. In the configuration tree, please find the entry Infrastructure Services and the sub-entry REST API Service.



- FXPerimeter () [f80]
  - Box Properties
  - Administrative Settings
  - Identity
  - Network
  - Traffic Shaping
  - Box Licenses
  - Advanced Configuration
  - Infrastructure Services
    - Authentication Service
    - Google Authenticator
    - Host Firewall Rules
    - SNMP Service Settings
    - Syslog Streaming
    - Control
    - Statistics
    - Eventing
    - General Firewall Configuration
    - Log Configuration
    - REST API Service
  - Virtual Servers

In the new dialog, please activate the option *Enable HTTPS interface*. Please set the value of the parameter *HTTPS Port* to *8443*.



REST API Service for FXPerimeter -

HTTP interface

Enable HTTP interface ☑

HTTP Port 8080

HTTPS interface

Enable HTTPS interface ☑

HTTPS Port 8443

Bind to Management IPs ☑

Private Key [New Key...] [Ex/Import] Hash: BIVMQC 2048 Bits

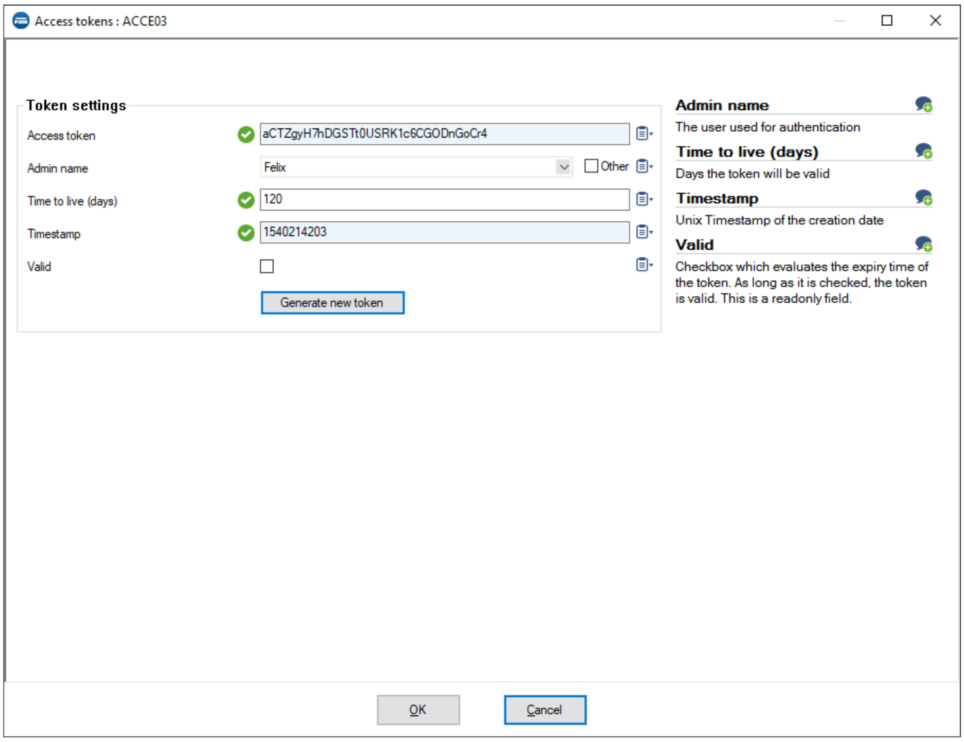
Certificate [Show...] [Ex/Import] Hash: BIVMQC self-signed 2048 Bits

Logging

Log Level Info

Please generate an *Access Token* to enable macmon NAC authenticating at the CloudGen Firewall.

Please make sure to choose a reasonable *Time to live* for the access token because its expiration prevents macmon NAC from authenticating at the firewall. Once your token is expired, please generate a new one and use the new value in the configuration file.



Access tokens : ACCE03

Token settings

Access token: aCTZgyH7hDGSTt0USRK1c6CGODnGoCr4

Admin name: Felix □ Other

Time to live (days): 120

Timestamp: 1540214203

Valid: □

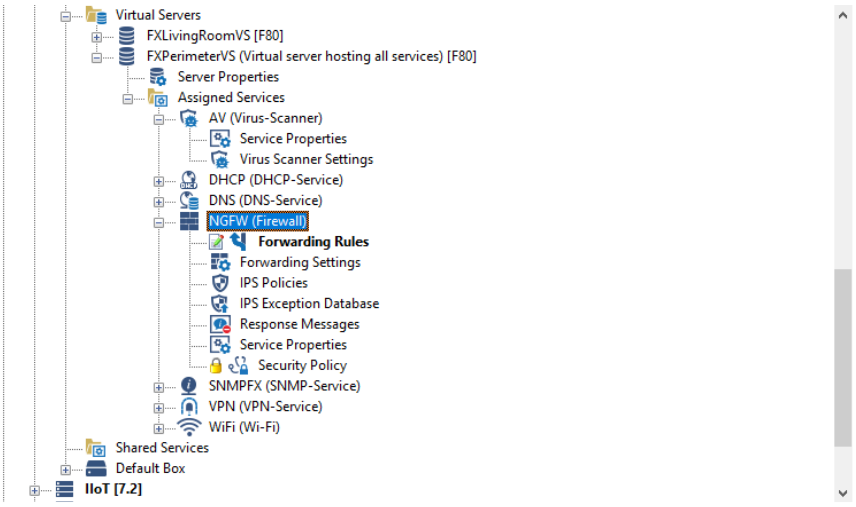
Admin name
The user used for authentication

Time to live (days)
Days the token will be valid

Timestamp
Unix Timestamp of the creation date

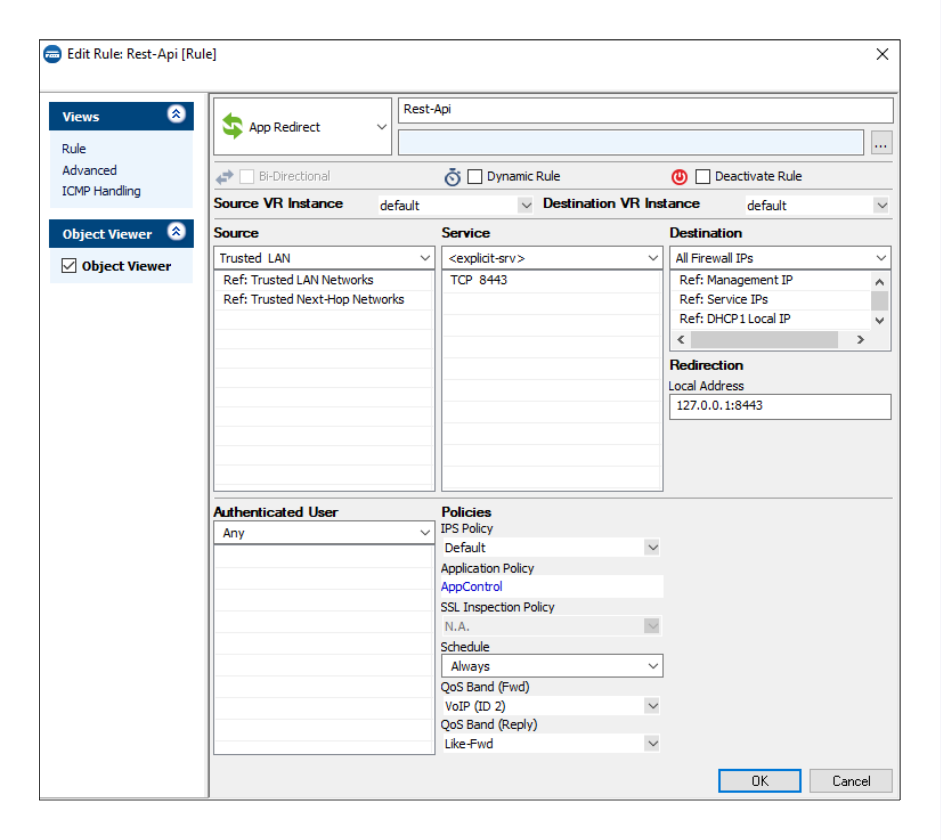
Valid
Checkbox which evaluates the expiry time of the token. As long as it is checked, the token is valid. This is a readonly field.

In the next step you will define a firewall rule that forwards incoming connection on port 8443 to the REST API service.



```
Virtual Servers
  FXLivingRoomVS [F80]
  FXPerimeterVS (Virtual server hosting all services) [F80]
    Server Properties
    Assigned Services
      AV (Virus-Scanner)
        Service Properties
        Virus Scanner Settings
      DHCP (DHCP-Service)
      DNS (DNS-Service)
      NGFW (Firewall)
        Forwarding Rules
        Forwarding Settings
        IPS Policies
        IPS Exception Database
        Response Messages
        Service Properties
        Security Policy
      SNMPFX (SNMP-Service)
      VPN (VPN-Service)
      WiFi (Wi-Fi)
Shared Services
Default Box
IIoT [7.2]
```

Please adapt the rule for the REST API as follows:



Edit Rule: Rest-Api [Rule]

Views: Rule, Advanced, ICMP Handling

Object Viewer: ☑ Object Viewer

App Redirect — Rest-Api

□ Bi-Directional □ Dynamic Rule □ Deactivate Rule

Source VR Instance: default — Destination VR Instance: default

Source: Trusted LAN
- Ref: Trusted LAN Networks
- Ref: Trusted Next-Hop Networks

Service: <explicit-srv>
- TCP 8443

Destination: All Firewall IPs
- Ref: Management IP
- Ref: Service IPs
- Ref: DHCP1 Local IP

Redirection
Local Address: 127.0.0.1:8443

Authenticated User: Any

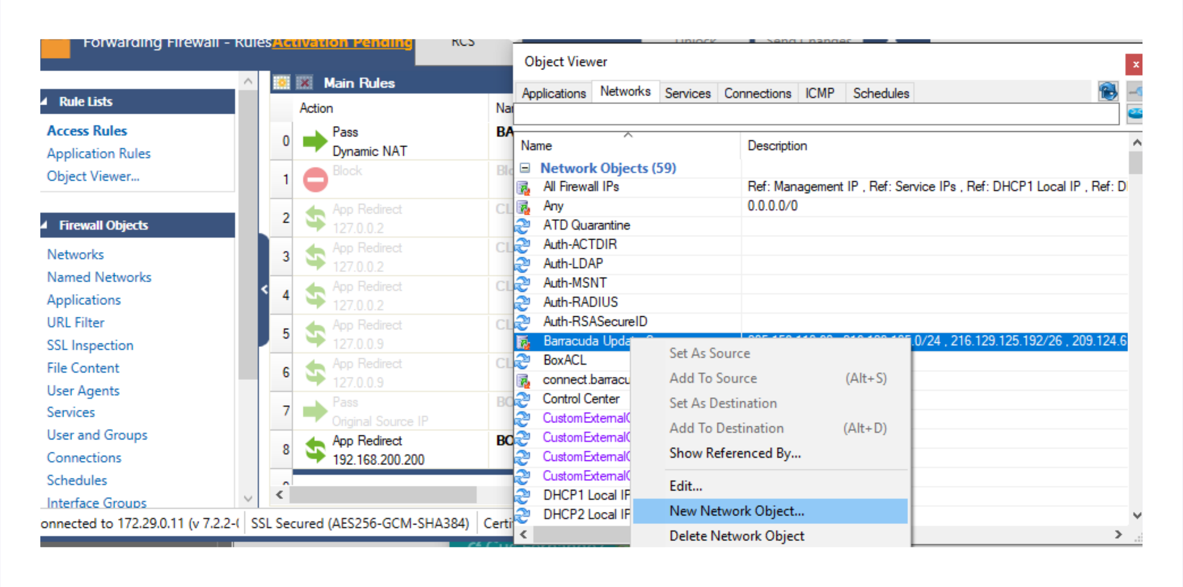
Policies
IPS Policy: Default
Application Policy: AppControl
SSL Inspection Policy: N.A.
Schedule: Always
QoS Band (Fwd): VoIP (ID 2)
QoS Band (Reply): Like-Fwd

OK Cancel

Create an object for trustworthy endpoint devices

This object will be used to identify trustworthy endpoint devices passed by macmon NAC. To use this object, corresponding firewall rules must be set.

Please right-click in the *Object Viewer* and click on *New Network Object*.

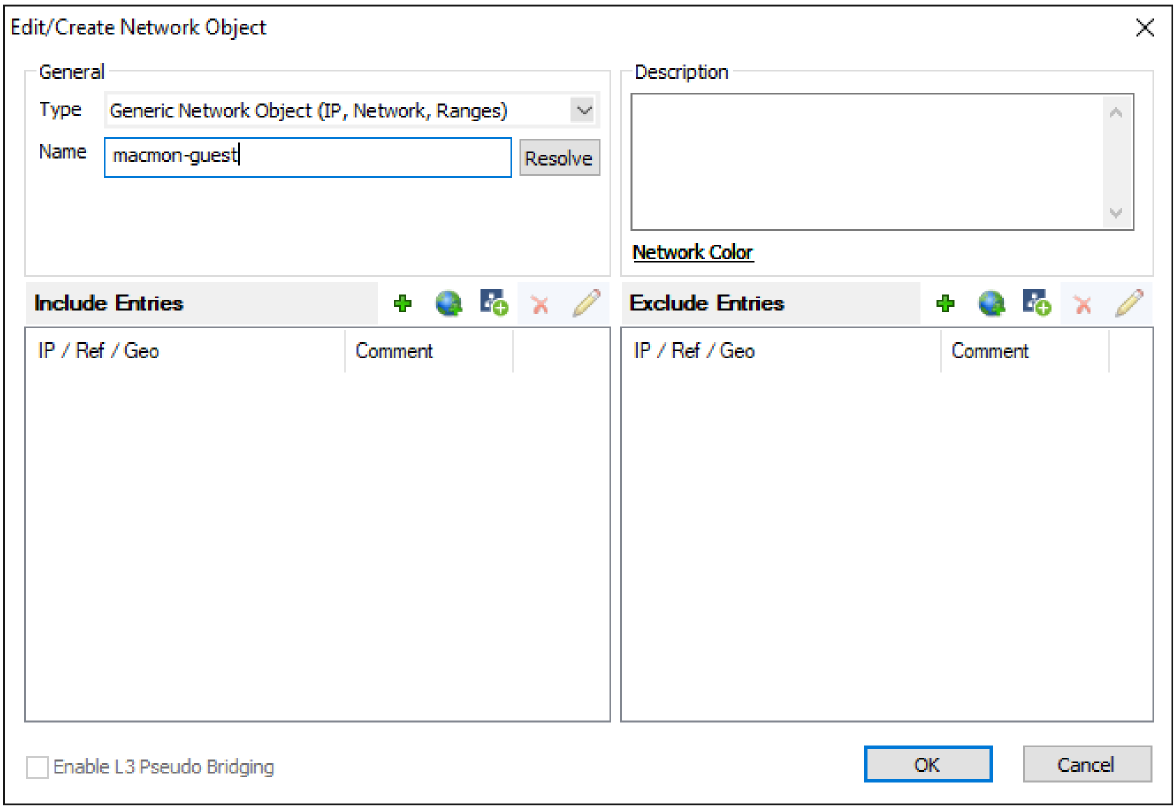


	Action
0	Pass Dynamic NAT
1	Block
2	App Redirect 127.0.0.2
3	App Redirect 127.0.0.2
4	App Redirect 127.0.0.2
5	App Redirect 127.0.0.9
6	App Redirect 127.0.0.9
7	Pass Original Source IP
8	App Redirect 192.168.200.200

Name	Description
Network Objects (59)	
All Firewall IPs	Ref: Management IP , Ref: Service IPs , Ref: DHCP1 Local IP , Ref: D
Any	0.0.0.0/0
ATD Quarantine	
Auth-ACTDIR	
Auth-LDAP	
Auth-MSNT	
Auth-RADIUS	
Auth-RSASecureID	
Barracuda Upda	0/24 , 216.129.125.192/26 , 209.124.6
BoxACL	
connect.barracu	
Control Center	
CustomExternal(	
CustomExternal(	
CustomExternal(	
CustomExternal(	
DHCP1 Local IF	
DHCP2 Local IF	

onnected to 172.29.0.11 (v 7.2.2-(SSL Secured (AES256-GCM-SHA384) Certi

In the appearing windows you will set up a new object. Please choose a name. We recommend a name like *macmon-guest* or *macmon-group*.


Edit/Create Network Object

General

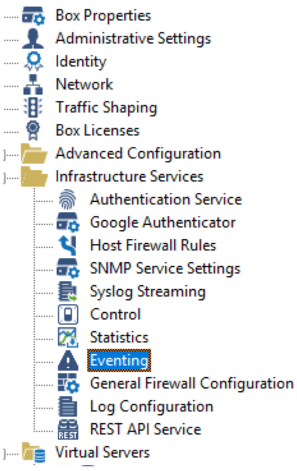
Type: Generic Network Object (IP, Network, Ranges)

Name: macmon-guest

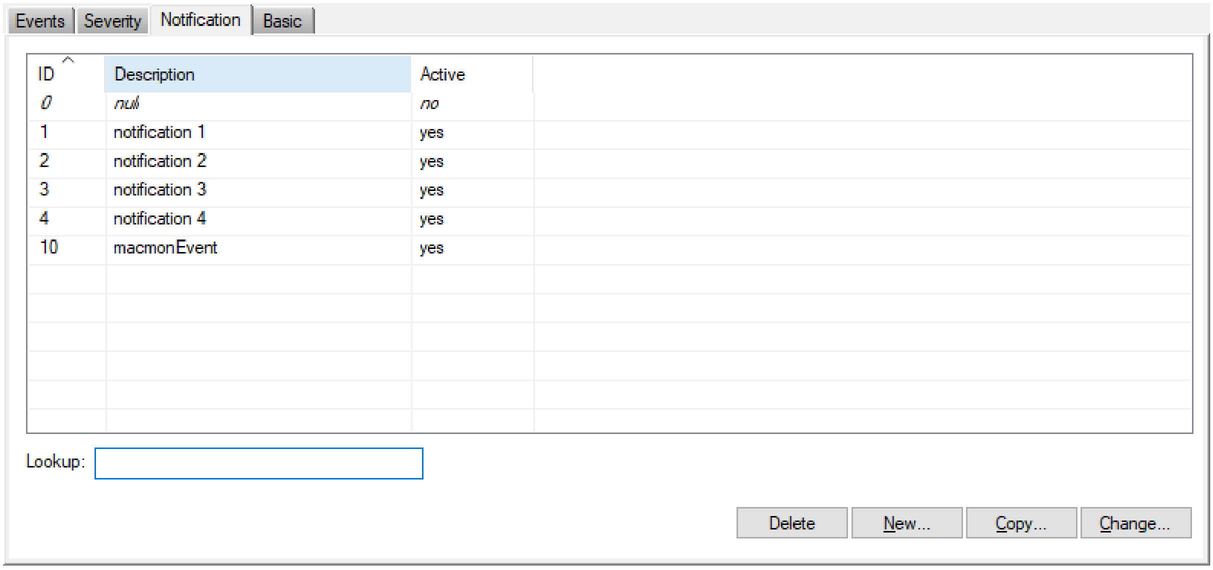
Rules for outbound communication

With this configuration you will set up rules that enable Barracuda CloudGen Firewall to pass the MAC address of an infected device automatically to macmon NAC and set the corresponding compliance status.

In the configuration tree of your Barracuda CloudGen Firewall, please find the entry *Infrastructure Services* and the sub-entry *Eventing*.



In the following dialog please click on the tab *Notification*. To create a new notification, please click on the button *New*.



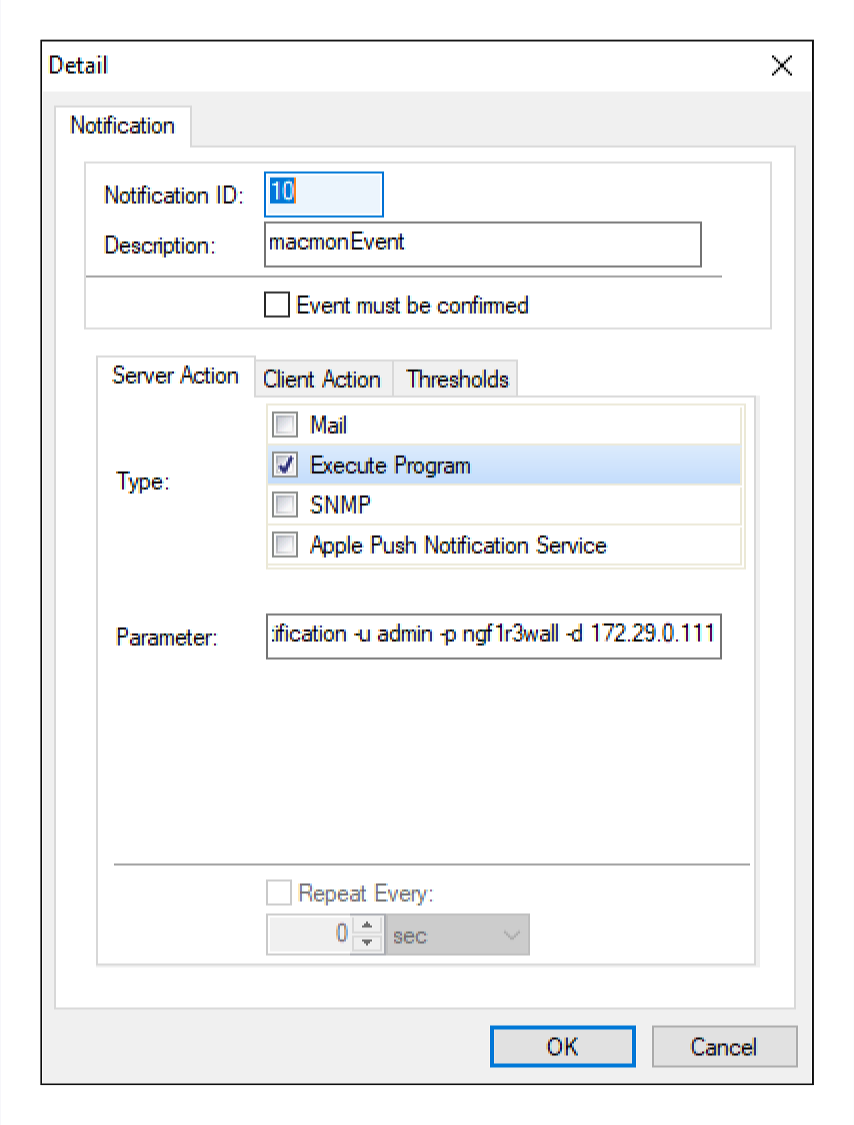
ID	Description	Active
0	*null*	*no*
1	notification 1	yes
2	notification 2	yes
3	notification 3	yes
4	notification 4	yes
10	macmonEvent	yes

In the tab *Server Action* please select *Execute Program* in the *Type* select box. Afterwards, please enter the following in the input field *Parameter*:

```
/opt/phion/bin/macmonEventNotification -u [username] -p [passwort] -d [ip-adresse]
```

Parameter overview:
-u passes the username of your macmon NAC installation
-p passes the password of the corresponding user.
-d passes the FQDN/the IP address of your macmon NAC installation

This would be an example call: `/opt/phion/bin/macmonEventNotification -u admin -p ngf1r3wall -d 172.29.0.111`



Notification ID: 10

Description: macmonEvent

☐ Event must be confirmed

Type:

☐ Mail
☑ Execute Program
☐ SNMP
☐ Apple Push Notification Service

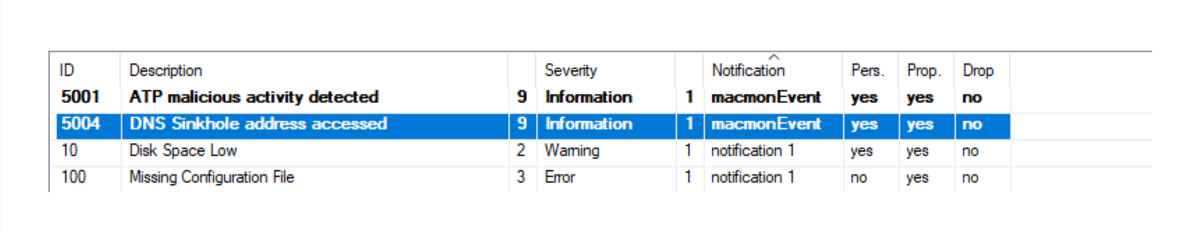
Parameter: :fication -u admin -p ngf1r3wall -d 172.29.0.111

☐ Repeat Every:

0 sec

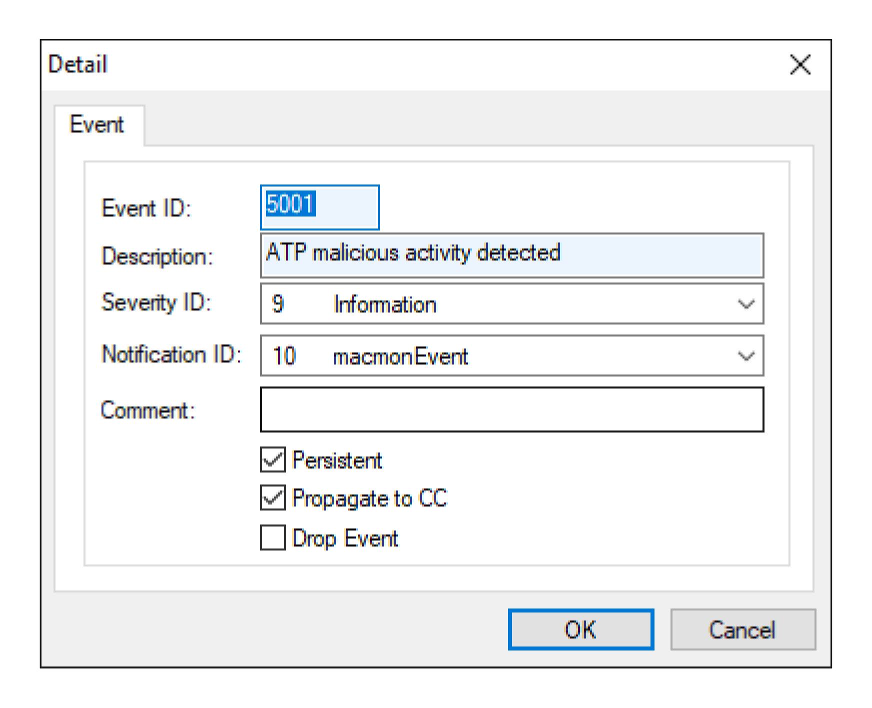
Please make sure to remember the *Notification ID* that is automatically assigned. You can see this ID in the upper third of the Detail window. (In the screenshot, the ID is 10.)

You now bind the new notification to the events with the IDs 5001 and 5004. For this, please click on the tab *Events* in the menu *Eventing*. Afterwards please double-click on the entry with the ID 5001.



ID	Description		Severity		Notification	Pers.	Prop.	Drop
5001	**ATP malicious activity detected**	**9**	**Information**	**1**	**macmonEvent**	**yes**	**yes**	**no**
5004	**DNS Sinkhole address accessed**	**9**	**Information**	**1**	**macmonEvent**	**yes**	**yes**	**no**
10	Disk Space Low	2	Warning	1	notification 1	yes	yes	no
100	Missing Configuration File	3	Error	1	notification 1	no	yes	no

Please select the *Notification ID* of the previous step in the dropdown menu with the same name. This is to bind the event 5001 on the notification.



Detail

Event

Event ID: 5001

Description: ATP malicious activity detected

Severity ID: 9 Information

Notification ID: 10 macmonEvent

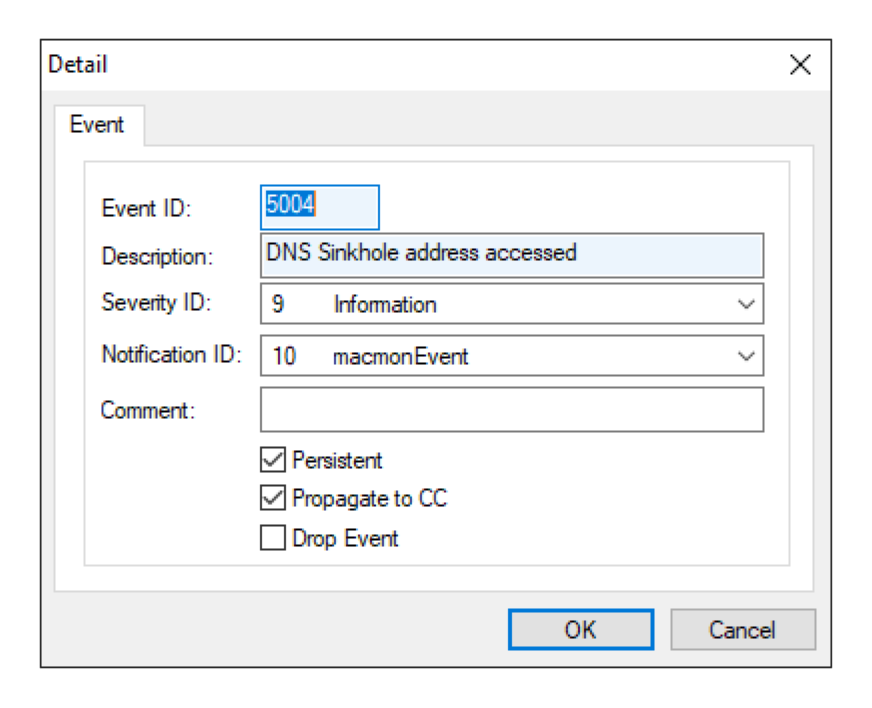
Comment:

☑ Persistent

☑ Propagate to CC

□ Drop Event

Please proceed in the same way with the event 5004. Please double-click on the entry with the ID 5004. Please select the *Notification ID* of the previous step in the dropdown menu with the same name. This is to bind the event 5004 on the notification.



Detail

Event

Event ID: 5004

Description: DNS Sinkhole address accessed

Severity ID: 9 Information

Notification ID: 10 macmonEvent

Comment:

☑ Persistent

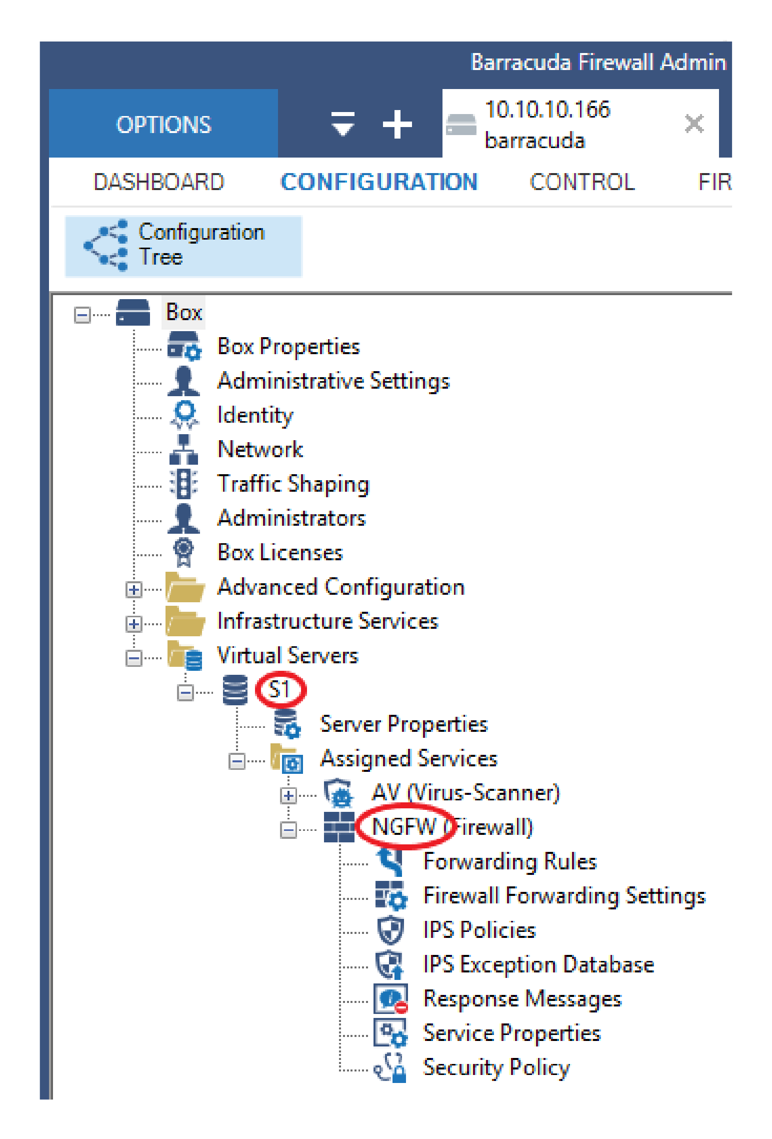
☑ Propagate to CC

□ Drop Event

Configuration of macmon NAC

Barracuda

Please note the following data regarding *apikey*, *server* and *service*:
You have already set up the API key in a previous step. This value is now used as *apikey*. You can find the values for *server* and *service* in the Firewall Admin application.



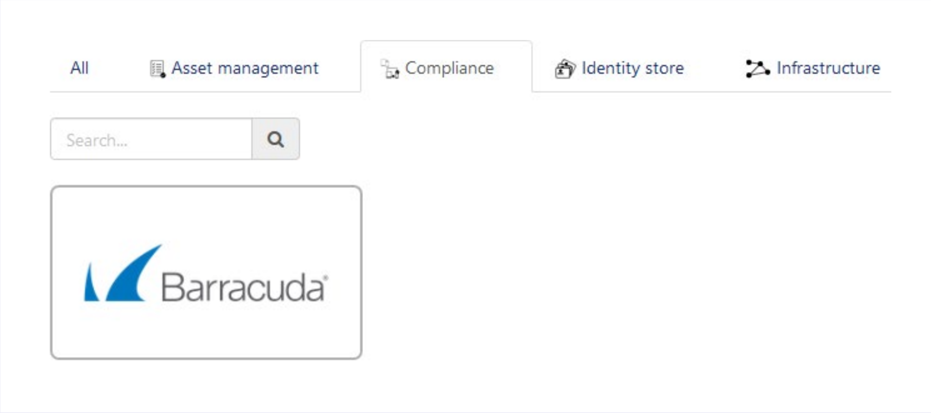
The value *name of the firewall object* refers to the object name you have chosen for the firewall object in a previous step.

This could be an example configuration:
URL: `https://10.10.10.123:8443`
API key: `example-api-key`
API version: `v1`
Server: `S1`
Service: `NGFW`

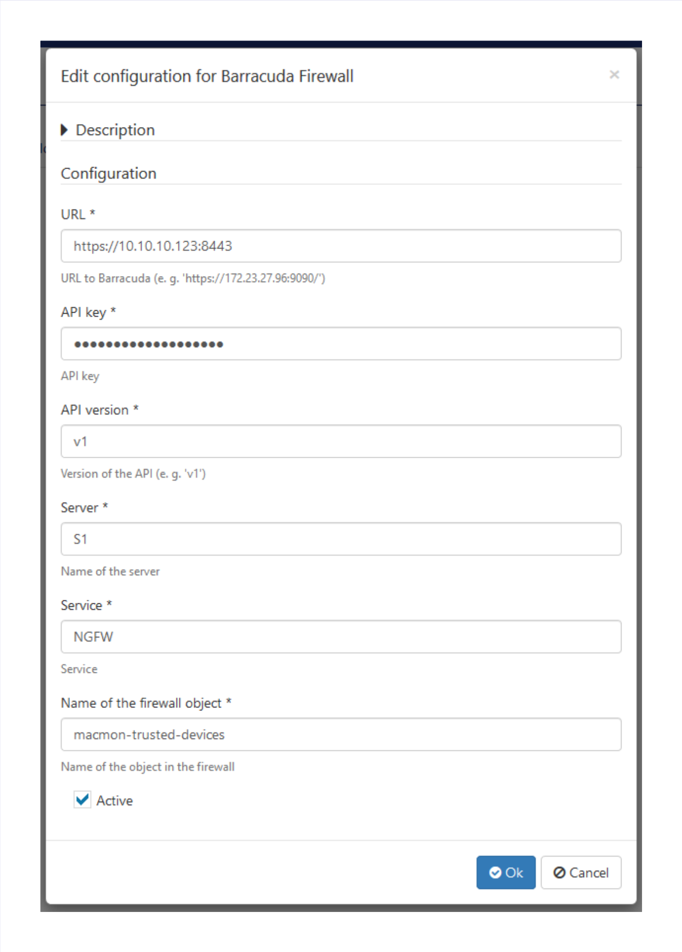
Name of the firewall object: `macmon-trusted-devices`

macmon NAC

The configuration is done via the web GUI. Please tap on *Settings* and *Third party integrations*, then on *Compliance*.



If the border of the Barracuda tile appears gray the integration is not yet activated. Please tap on the tile for the configuration dialog to be shown and enter the credentials you've set up on your Barracuda CloudGen Firewall instance. Please make sure to check the box with the label "Active" and confirm by tapping "Ok".



Edit configuration for Barracuda Firewall

Description

Configuration

URL *
https://10.10.10.123:8443
URL to Barracuda (e. g. 'https://172.23.27.96:9090/')

API key *
•••••••••••••••••••
API key

API version *
v1
Version of the API (e. g. 'v1')

Server *
S1
Name of the server

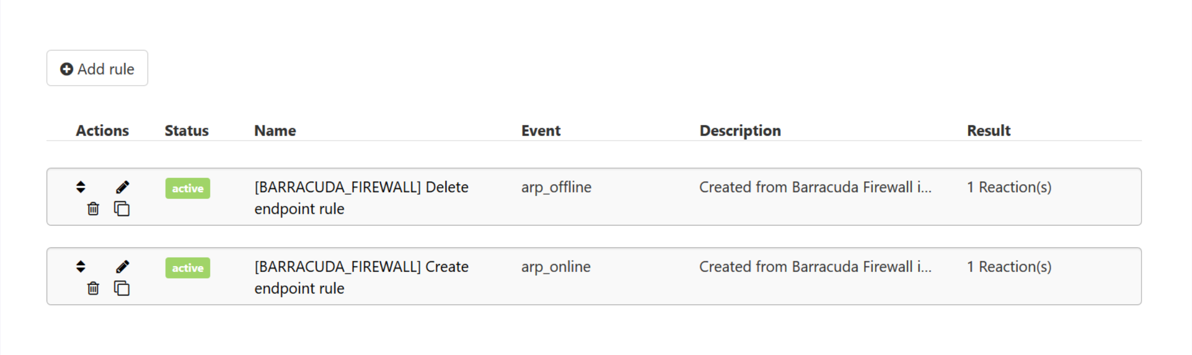
Service *
NGFW
Service

Name of the firewall object *
macmon-trusted-devices
Name of the object in the firewall

☑ Active

Policies configuration

When activating the Barracuda CloudGen Firewall integration, all necessary rules are set up automatically. Both rules will appear in *Policies – Events*. If you need to customize them, please tap on the pen icon.



Actions	Status	Name	Event	Description	Result
⬍ ✎ 🗑 ⧉	active	[BARRACUDA_FIREWALL] Delete endpoint rule	arp_offline	Created from Barracuda Firewall i...	1 Reaction(s)
⬍ ✎ 🗑 ⧉	active	[BARRACUDA_FIREWALL] Create endpoint rule	arp_online	Created from Barracuda Firewall i...	1 Reaction(s)

Further use cases

The use case of trustworthy endpoint devices can also be easily transferred to guest devices. For this purpose, an object for the guest portal can be created in Barracuda CloudGen Firewall (e.g., macmon-guest-portal) and the triggering policy rule can be adapted so that it triggers when a new guest device logs on. This enables Barracuda CloudGen Firewall to take over the routing for new guest devices automatically.

Contact at Barracuda

Technical Support
https://campus.barracuda.com
https://www.barracuda.com/support/index

Contact

macmon secure GmbH
Alte Jakobstrasse 79-80 | 10179 Berlin
Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu