macmon
nac intelligent einfach

MACMON NAC WHITEPAPER

Anbindung an Barracuda CloudGen Firewall

macmon
nac intelligent einfach

Inhaltsverzeichnis

Version: 2.8_de

Einleitung

Barracuda vereinfacht die IT-Infrastruktur durch Cloud-fähige Lösungen, die es Kunden ermöglichen, ihre Netzwerke, Applikationen und Daten standortunabhängig zu schützen. Über 150.000 Unternehmen und Organisationen weltweit vertrauen den leistungsstarken, benutzerfreundlichen und kostengünstigen Lösungen, die als physische oder virtuelle Appliance sowie als Cloud- oder hybride Lösungen verfügbar sind. Beim Geschäftsmodell von Barracuda steht die Kundenzufriedenheit im Mittelpunkt. Es setzt auf hochwertige IT-Lösungen auf Subskriptions-Basis, die das Netzwerk und die Daten der Kunden umfassend schützen. Scanner sorgen für das Aufspüren von Gefahren im Netzwerk und davon befallenen Geräten, die an macmon NAC übermittelt werden können. macmon NAC kann auf diesen Hinweis hin ein Gerät isolieren oder physikalisch vom Netzwerk trennen. Andersherum können auch neue Geräte an Barracuda CloudGen Firewall übermittelt werden, so dass diese dem Firewall-System sofort bekannt sind.

Anwendungsfälle

macmon NAC übermittelt neue vertrauenswürdige Geräte an Barracuda CloudGen Firewall

In einem Krankenhaus kann es sinnvoll sein, medizinische Geräte und Verwaltungscomputer durch Segmentierung des Netzwerks voneinander zu trennen. Dennoch ist es wünschenswert, dass nur wenige besonders geschützte und dadurch geeignete Computer auf die Ergebnisdatenbank eines medizinischen Geräts zugreifen können. Da macmon NAC den Zugriff für ein ganzes Netzwerksegment erlauben oder verbieten kann, bietet sich eine Schnittstelle zu einer Firewall an, die über bestimmte Richtlinien den Zugriff sehr feinkörnig steuern kann. Meldet sich ein Gerät im Netzwerk an, so bekommt es vom DHCP-Server eine IP-Adresse zugewiesen und hat fortan Zugriff zum Netzwerk. Wird dieses Gerät in macmon NAC einer Gruppe zugeordnet, die als vertrauenswürdig erachtet wird, so kann über die in diesem Dokument vorgestellte Schnittstelle die MAC-Adresse mit aktuell gültiger IP-Adresse an eine Barracuda CloudGen Firewall übermittelt werden. macmon NAC gewinnt so die Möglichkeit, exakt diesem Gerät den Zugriff in ein besonders geschütztes Netzwerksegment zu erlauben.

Barracuda CloudGen Firewall übermittelt von Schadsoftware befallene Geräte an macmon NAC

Im selben Netzwerk können Gefahren lauern. Ein Endgerät kann durch verschiedene Mechanismen von Schadsoftware infiziert werden und sich dadurch im Netzwerk auffällig verhalten. Barracuda CloudGen Firewall erkennt das schädliche Verhalten und kann den Netzwerkadministrator über den Fund informieren, der dann die nötigen Schritte zur Heilung einleiten kann. Mit der in diesem Dokument beschriebenen Schnittstelle kann die Reaktion auf die Entdeckung eines infizierten Endgeräts automatisiert werden. Nach der Entdeckung übermittelt Barracuda CloudGen Firewall die Identität dieses Geräts an macmon NAC, wo es gemäß voreingestellter oder selbst definierter Regeln isoliert oder anderweitig behandelt wird. Somit gewinnt Barracuda CloudGen Firewall die Möglichkeit, ein Gerät gezielt aus einem Netzwerksegment zu entfernen, um eine Heilung zu ermöglichen.

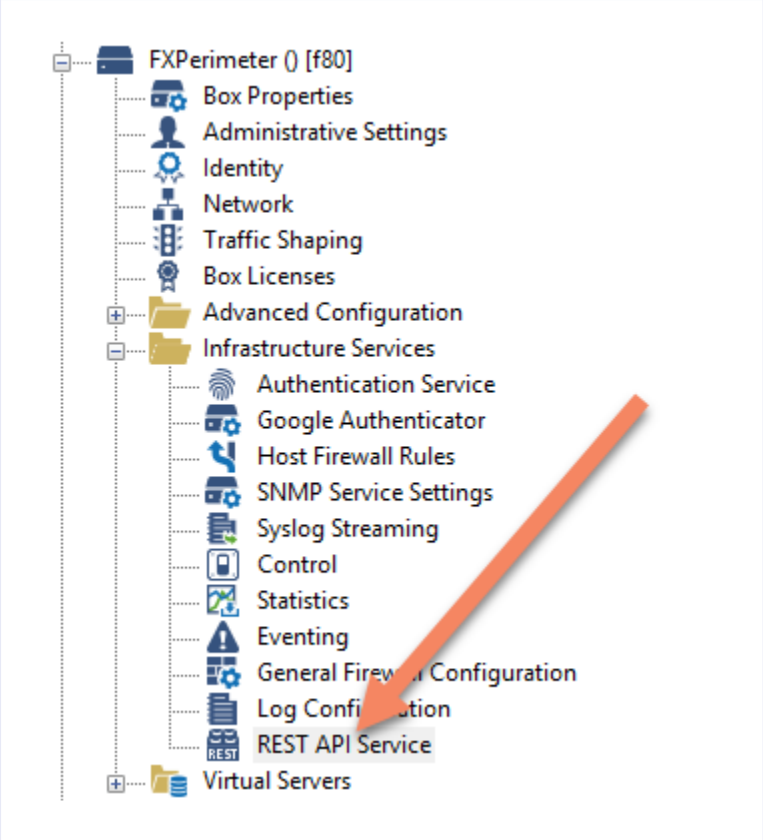
Voraussetzung

Für die Integration der Barracuda CloudGen Firewall in macmon NAC ist das macmon Premium Bundle nötig.

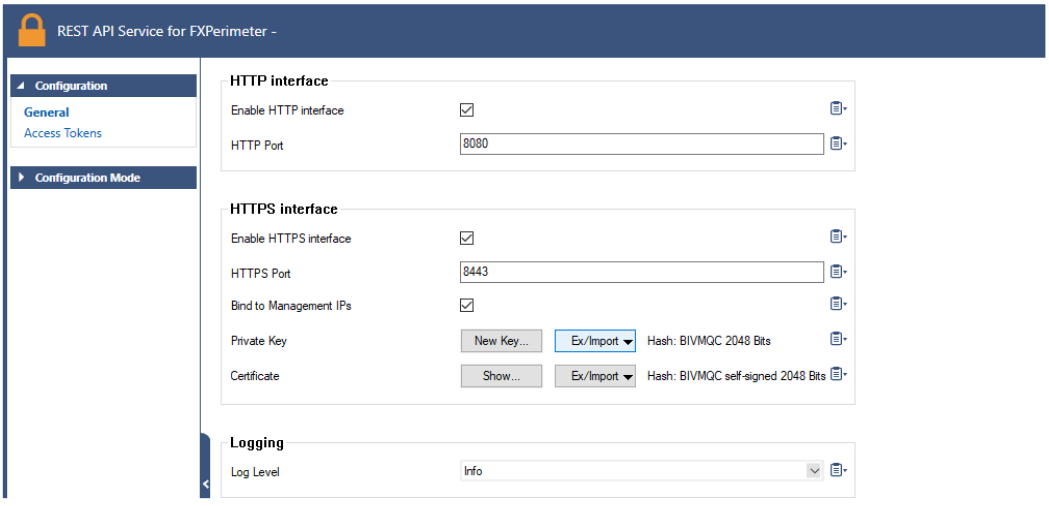
Konfiguration von Barracuda CloudGen Firewall

Vorbereitung der REST-Schnittstelle

Starten Sie bitte die Anwendung *Firewall Admin* und verbinden Sie sich mit Ihrer Barracuda CloudGen Firewall. Im Konfigurationsbaum finden Sie unter dem Punkt *Infrastructure Services* den Eintrag *REST API Service*.

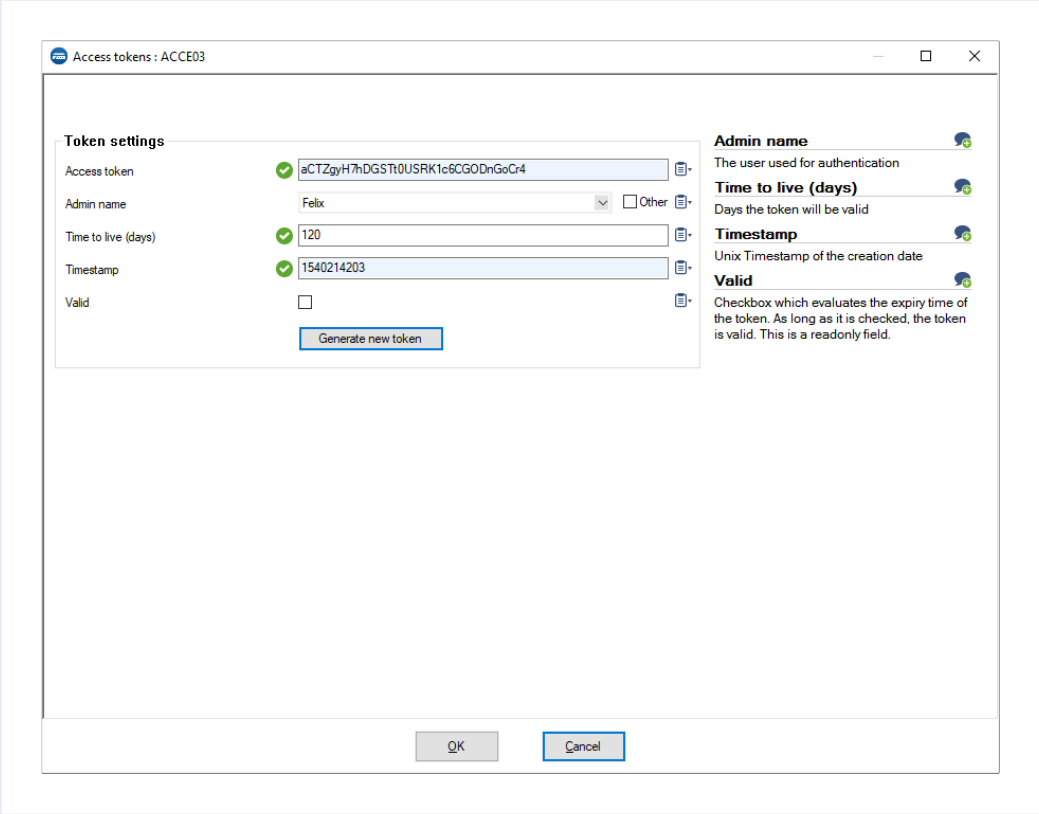


Im danach erscheinenden Dialog aktivieren Sie bitte die Option *Enable HTTPS interface* durch Setzen des Hakens. Den *HTTPS Port* setzen Sie bitte auf den Wert *8443*.

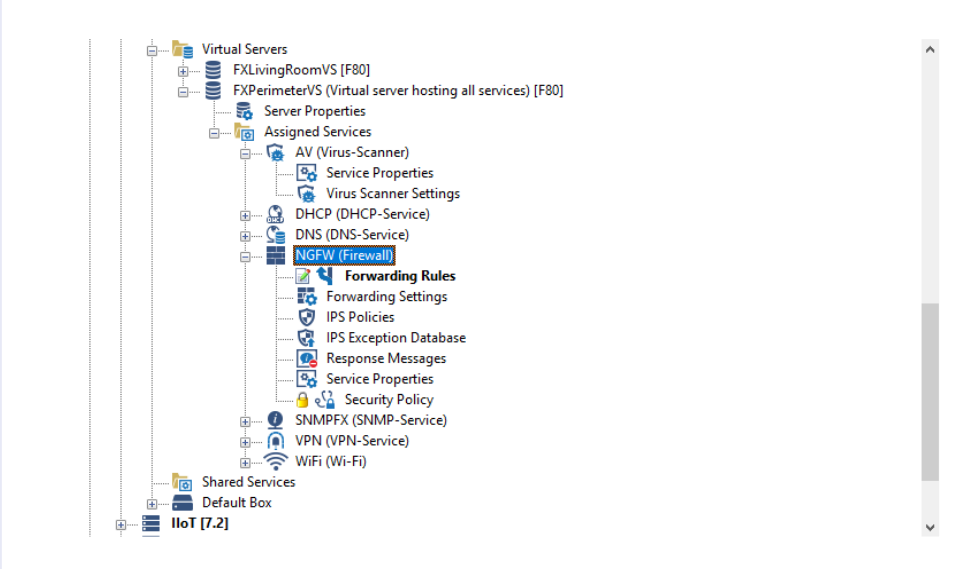


Generieren Sie bitte einen *Access Token* mit dem sich macmon NAC an der CloudGen Firewall authentifizieren kann.

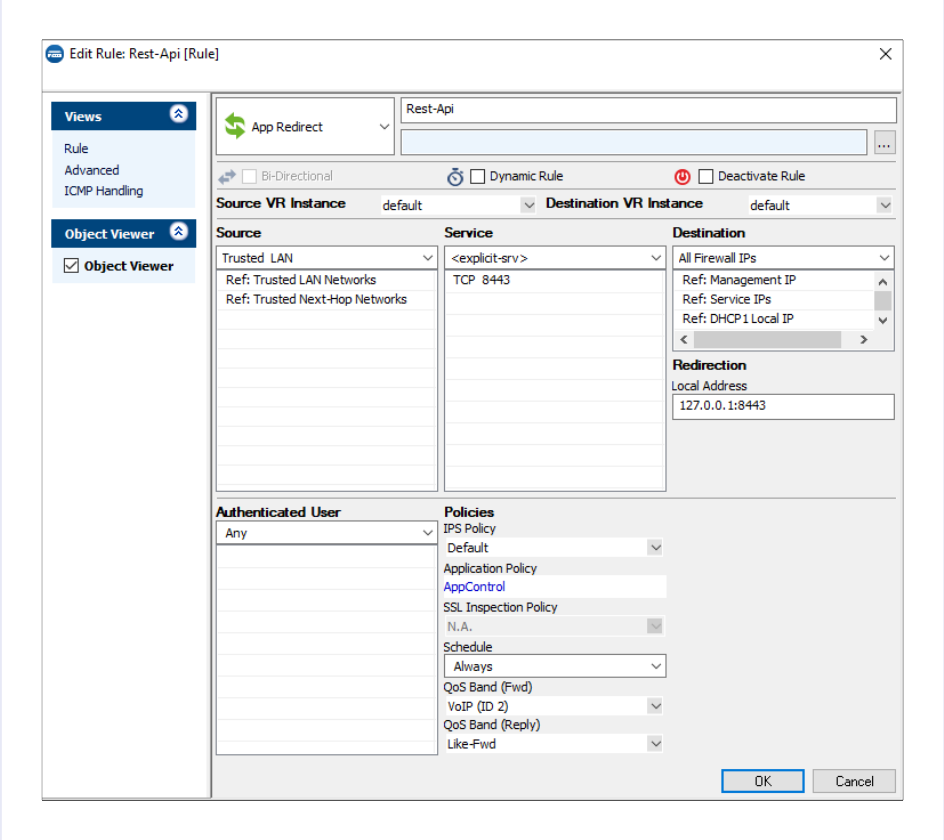
Achten Sie bitte darauf, die Gültigkeitsdauer (*Time to live*) nicht zu kurz zu wählen, da die Kommunikation zwischen Ihrem macmon NAC und Ihrer CloudGen Firewall sonst nicht mehr funktionieren wird. Sollte Ihr Token abgelaufen sein, generieren Sie bitte einen neuen und hinterlegen Sie den geänderten Wert einfach in der entsprechenden CloudGen-Firewall-Konfiguration in macmon NAC.



Im nächsten Schritt definieren Sie eine Firewall-Regel, die eingehende Verbindungen auf Port 8443 zum REST-API Service umleitet.



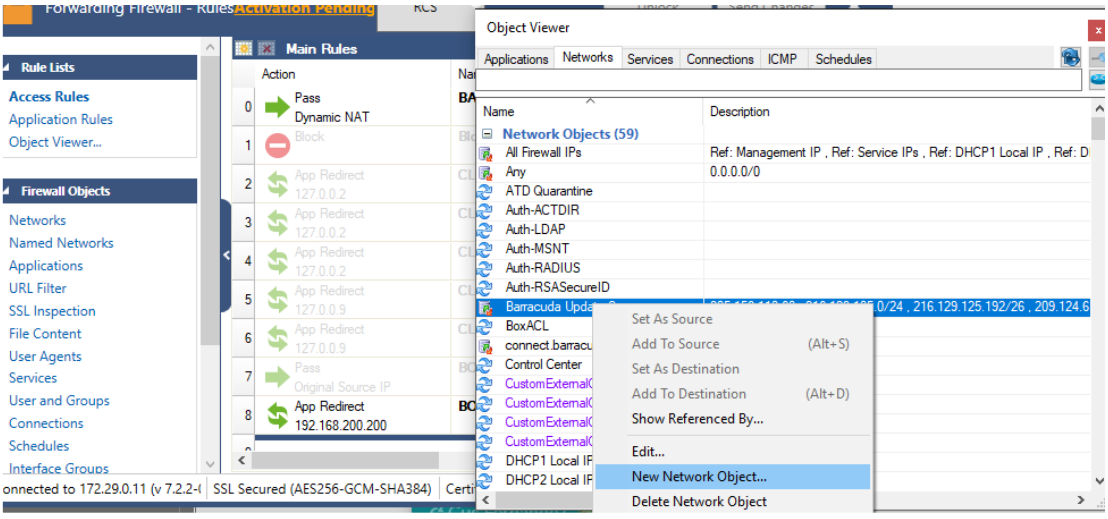
Passen Sie die Regel für die REST-API bitte wie folgt an:



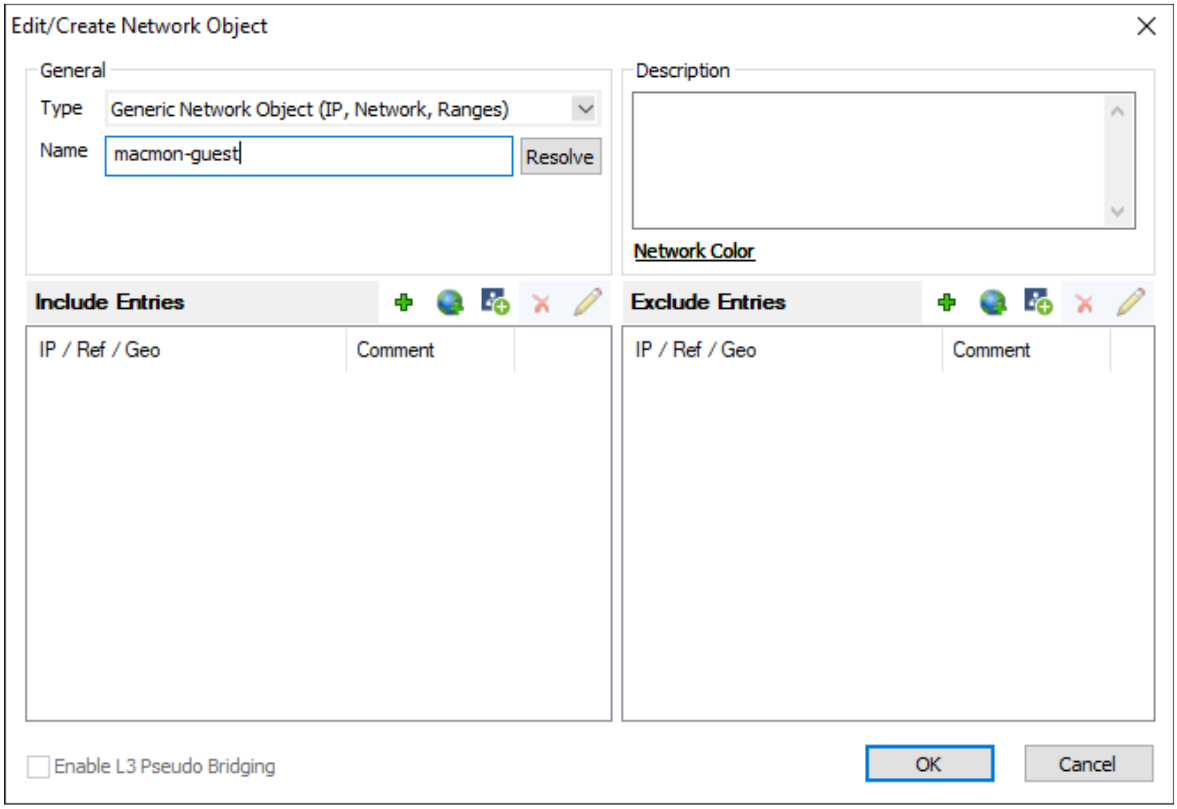
Erstellen eines Objekts für vertrauenswürdige Geräte

Dieses Objekt wird herangezogen, um die von macmon NAC übermittelten vertrauenswürdigen Geräte zu identifizieren. Für dieses müssen auch noch die entsprechenden Firewall-Regeln gesetzt werden. Das hier angelegte Objekt ermöglicht macmon NAC die Übertragung der IP-Adressen der entsprechenden Endgeräte. Ist das Objekt angelegt, so kann es frei in verschiedenen Firewall-Regeln verwenden werden.

Bitte machen Sie einen Rechtsklick im *Object Viewer* und klicken Sie auf *New Network Object*.



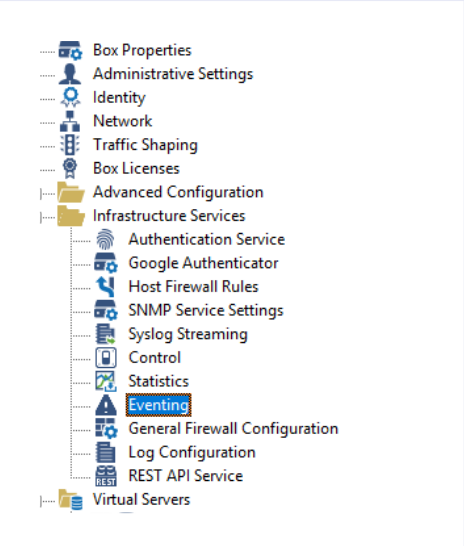
Im folgenden Fenster legen Sie ein neues Objekt an. Den Namen können Sie frei wählen. Wir empfehlen Ihnen einen Namen wie beispielsweise *macmon-guest* oder *macmon-group*.



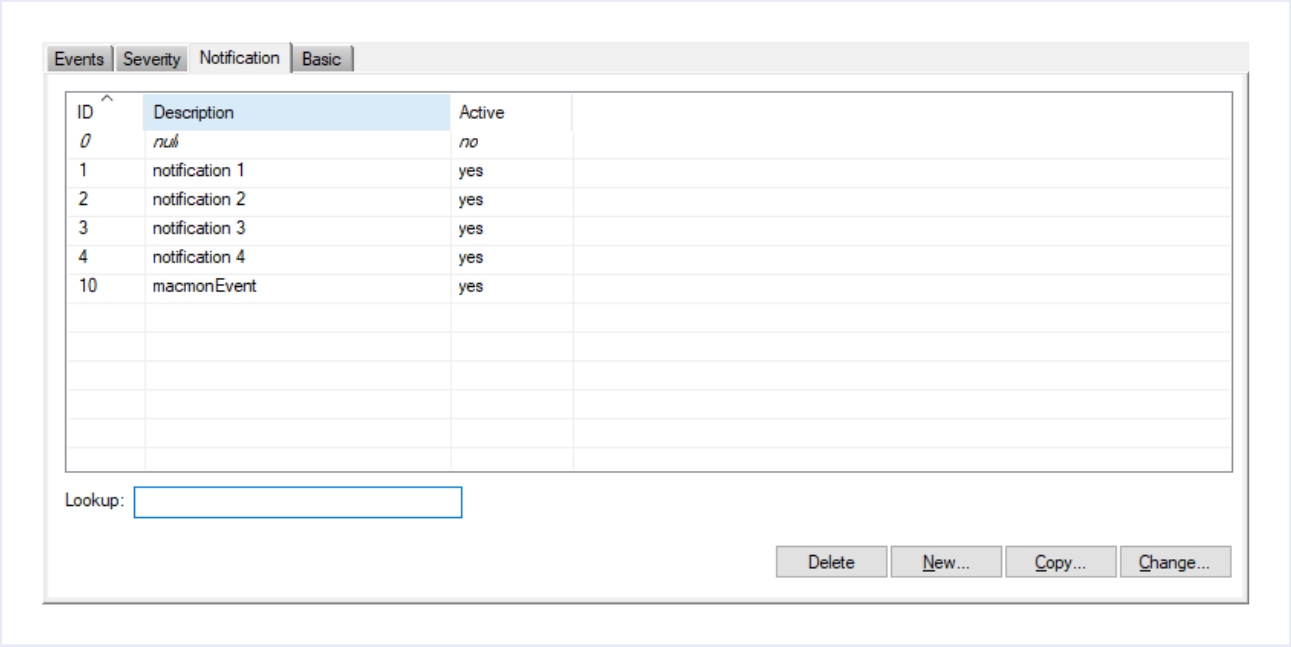
Regeln für Outbound-Kommunikation

Mit dieser Konfiguration werden die Regeln erstellt, die die MAC-Adresse eines infizierten Devices via Script an macmon NAC übermitteln und somit den Compliance-Status setzen.

Im Konfigurationsbaum Ihrer Barracuda CloudGen Firewall finden Sie den Menüeintrag *Infrastructure Services* und dort den Eintrag *Eventing*.



Im nachfolgenden Dialog wählen Sie bitte das Tab *Notification* aus. Dort legen Sie über einen Klick auf den Button *New* eine neue Benachrichtigung an.

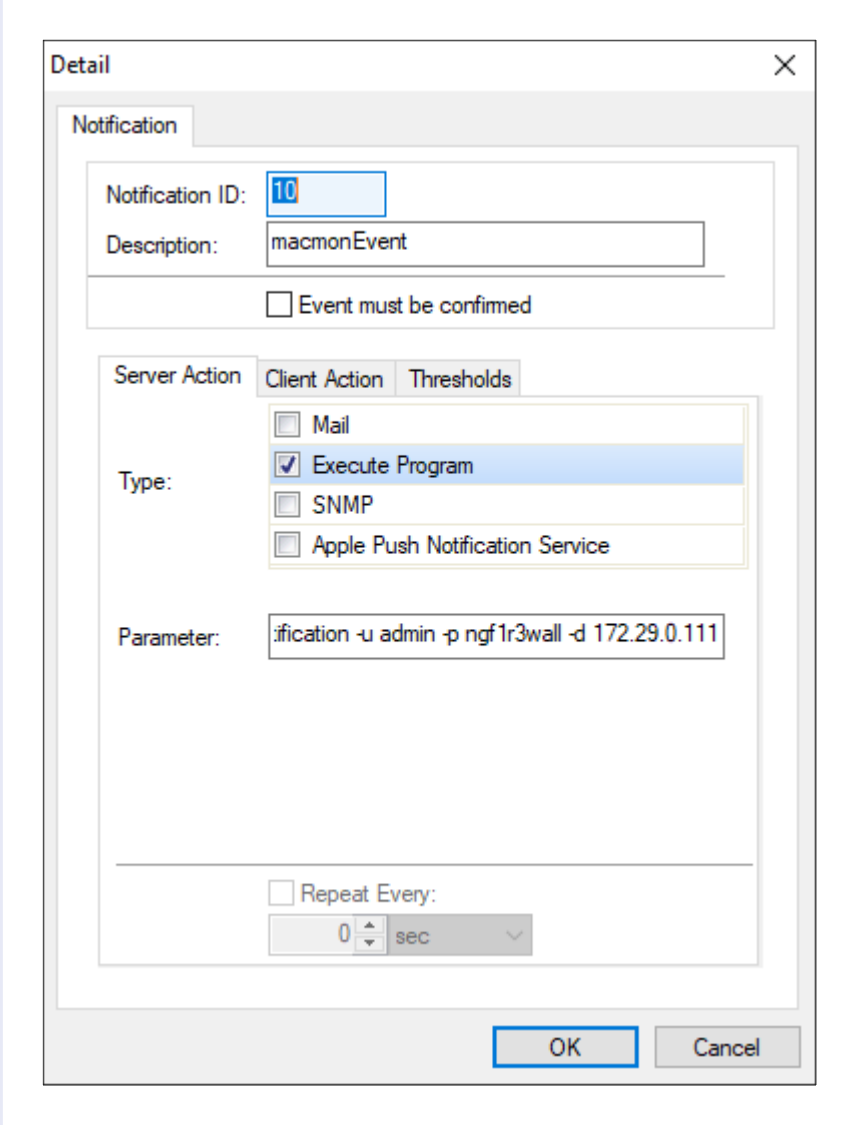


Im Tab *Server Action* wählen Sie beim Eintrag *Type* bitte die Option *Execute Program* aus. Tragen Sie danach im Textfeld *Parameter* folgendes ein:

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

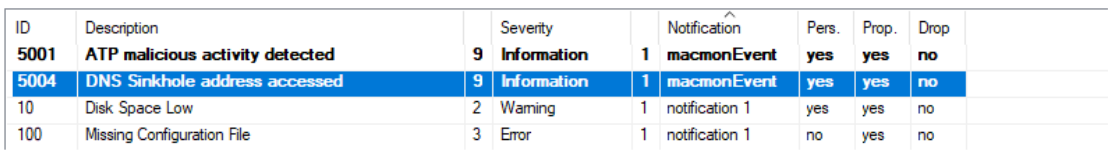
Übersicht der Parameter:
-u gibt den Benutzernamen Ihrer macmon NAC-Installation an
-p gibt das Passwort des zugehörigen Benutzers an
-d gibt den FQDN/die IP-Adresse Ihrer macmon NAC-Installation an

Ein beispielhafter Aufruf könnte also so aussehen: `/opt/phion/bin/macmonEventNotification -u admin -p ngf1r3wall -d 172.29.0.111`



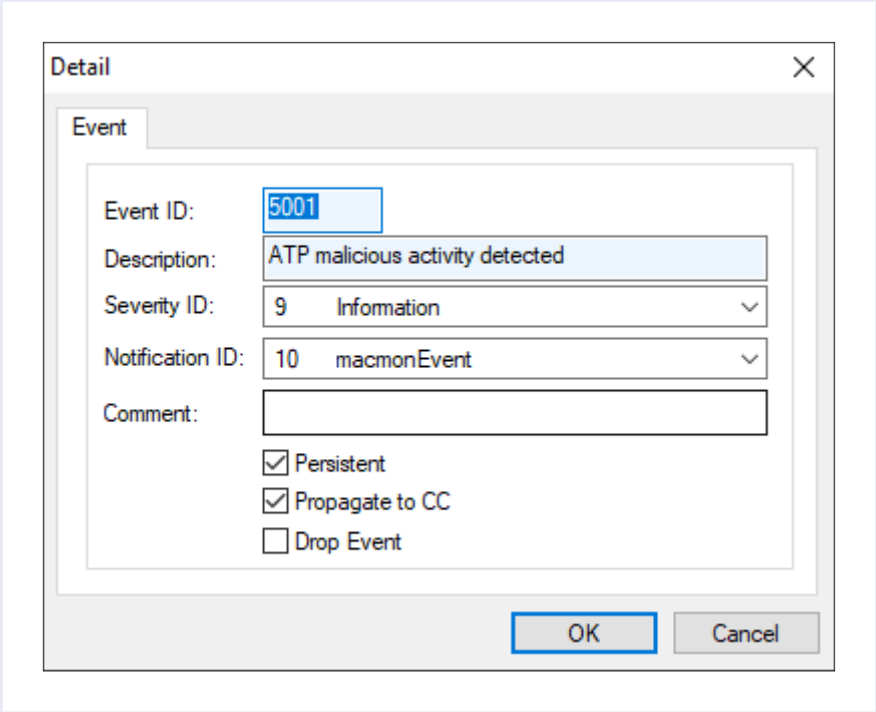
Notieren Sie sich bitte die *Notification ID*, die hier automatisch vergeben wird und bereits im oberen Drittel der Detailansicht zu sehen ist. (Im Screenshot hier ist die ID 10.)

Die nun angelegte Notification binden Sie bitte an die beiden Events mit den IDs 5001 und 5004. Klicken Sie dazu zunächst im Menü *Eventing* auf das Tab *Events*. Dort wählen Sie durch einen Doppelklick den Eintrag mit der ID 5001 aus.

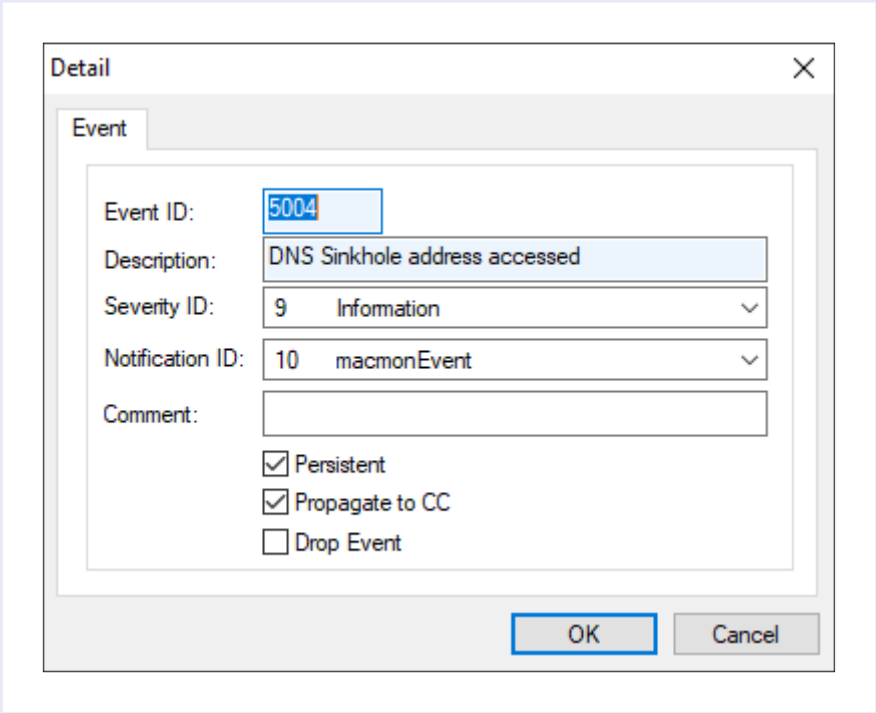


ID	Description		Severity		Notification	Pers.	Prop.	Drop
5001	**ATP malicious activity detected**	**9**	**Information**	**1**	**macmonEvent**	**yes**	**yes**	**no**
5004	**DNS Sinkhole address accessed**	**9**	**Information**	**1**	**macmonEvent**	**yes**	**yes**	**no**
10	Disk Space Low	2	Warning	1	notification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

In der folgenden Detailansicht wählen Sie bitte im Dropdown-Menü *Notification ID* die zuvor notierte ID aus, um das Ereignis 5001 an diese Benachrichtigung zu binden.



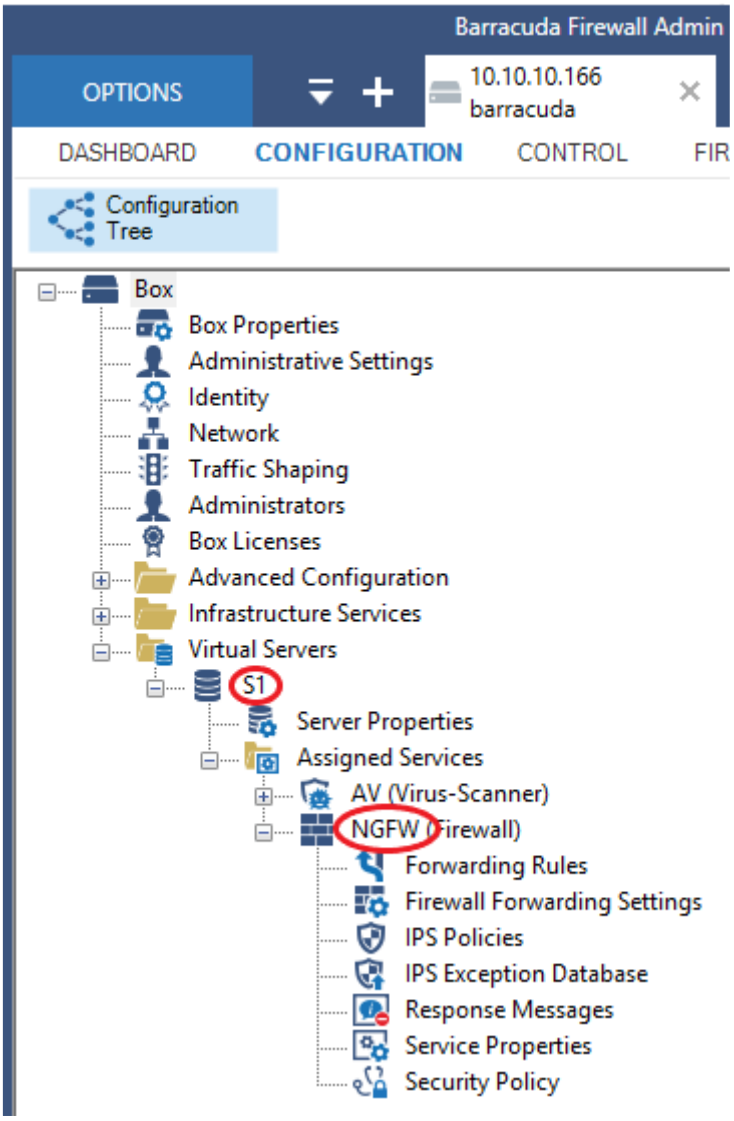
Analog dazu gehen Sie bitte für das Event mit der ID 5004 vor. Dazu wählen Sie durch einen Doppelklick den Eintrag mit der ID 5004 aus. In der folgenden Detailansicht wählen Sie bitte im Dropdown-Menü *Notification ID* die zuvor notierte ID aus, um das Ereignis 5004 an diese Benachrichtigung zu binden.



Konfiguration von macmon NAC

Barracuda

Bitte notieren Sie sich die folgenden Informationen bezüglich apikey, server und service:
In einem vorherigen Schritt haben Sie einen API-Schlüssel erzeugt. Dieser Wert wird nun für *apikey* verwendet. Die Werte für *server* und *service* entnehmen Sie bitte Ihrer Firewall-Konfiguration. Die Werte können Sie im Programm Firewall Admin ablesen.



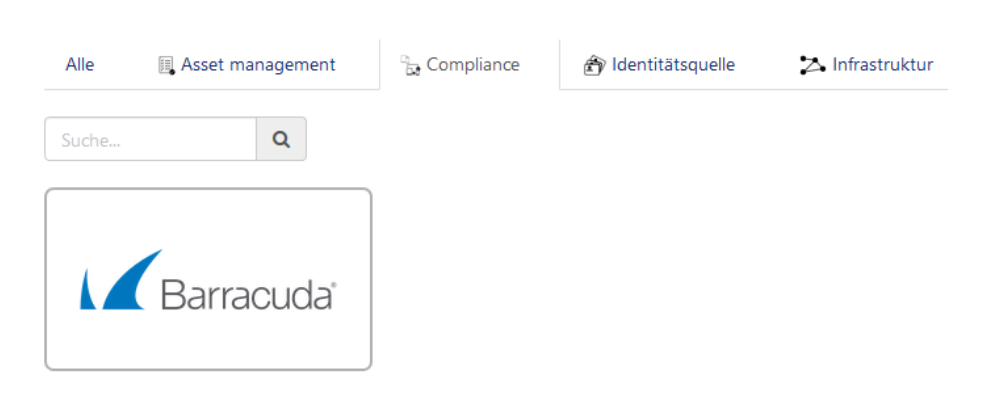
Der Wert für *name* richtet sich nach dem Objekt-Namen, den Sie zuvor für das Firewall-Objekt vergeben haben.

Somit ergibt sich folgende beispielhafte Konfiguration:
URL: `https://10.10.10.123:8443`
API Schlüssel: `example-api-key`
API Version: `v1`
Server: `S1`
Dienst: `NGFW`

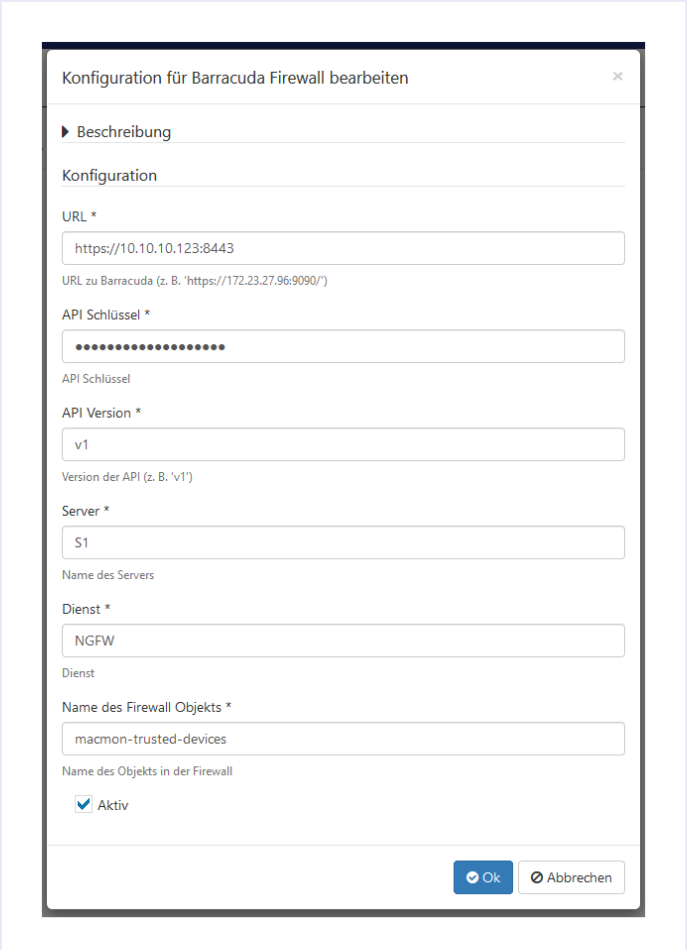
Name des Firewall Objekts: `macmon-trusted-devices`

macmon NAC

Die Konfiguration erfolgt über das Web-GUI. Bitte tippen Sie auf *Einstellungen* und *Drittanbieter-Integrationen*, danach auf *Compliance*.

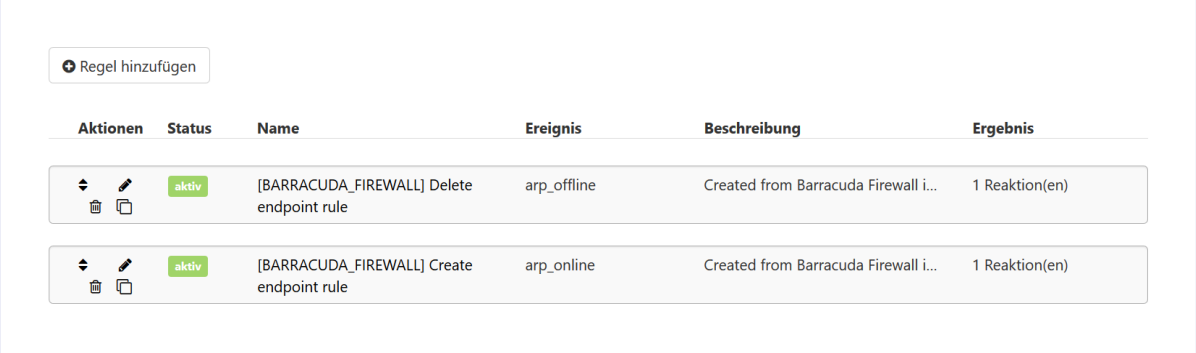


Wenn der Rahmen der Barracuda-Kachel grau erscheint, ist die Integration noch nicht aktiviert. Bitte tippen Sie auf die Kachel, um den Konfigurationsdialog zu öffnen und geben Sie die Zugangsdaten ein, die Sie in Ihrer Barracuda CloudGen Firewall vorbereitet haben. Bitte setzen Sie den Haken bei „Aktiv" und bestätigen Sie mit "Ok".



Konfiguration des Regelwerks

Sobald die Integration von Barracuda CloudGen Firewall aktiviert wird, werden alle notwendigen Regeln automatisch eingerichtet. Beide Regeln erscheinen in Richtlinien – Ereignisse. Wenn Sie die Regeln anpassen wollen, tippen Sie bitte auf das Stift-Symbol.



Weitergehende Anwendungsfälle

Ohne weiteres lässt sich der Anwendungsfall von vertrauenswürdigen Endgeräten auch auf Gastgeräte übertragen. Dazu kann in der Firewall von Barracuda ein Objekt für das Gästeportal angelegt (beispielsweise macmon-guest-portal) und die auslösende Regel so angepasst werden, dass sie beim Anmelden eines neuen Gastgeräts auslöst. Dies versetzt die Barracuda CloudGen Firewall in die Lage, das Routing für neue Gastgeräte vollautomatisch zu übernehmen.

Kontakt bei Barracuda

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

Kontakt

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