

MACMON NAC WHITEPAPER Anbindung an Barracuda CloudGen Firewall

ANBINDUNG AN BARRACUDA CLOUDGEN FIREWALL



Inhaltsverzeichnis

Einleitung	3
Anwendungsfälle	3
macmon NAC übermittelt neue vertrauenswürdige Geräte an Barracuda CloudGen Firewall	3
Barracuda CloudGen Firewall übermittelt von Schadsoftware befallene Geräte an macmon NAC	3
Voraussetzung	3
Konfiguration von Barracuda CloudGen Firewall	4
Vorbereitung der REST-Schnittstelle	4
Erstellen eines Objekts für vertrauenswürdige Geräte	7
Regeln für Outbound-Kommunikation	8
Konfiguration von macmon NAC	12
Barracuda	12
macmon NAC	14
Konfiguration des Regelwerks	15
Weitergehende Anwendungsfälle	15
Kontakt bei Barracuda	16
Varcian: 2.8 da	



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*.

figuration	HTTP interface		
al	Enable HTTP interface		
Tokens	HTTP Port	8080	I -
iguration Mode			
	HTTPS interface		
	Enable HTTPS interface		.
	HTTPS Port	8443	۲
	Bind to Management IPs		
	Private Key	New Key Ex/Import - Hash: BIVMQC 2048 Bits	.
	Certificate	Show Ex/Import Hash: BIVMQC self-signed 20	48 Bits 🗐 *
	Logging		
	Log Level	Info	✓ ■•



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.

						-
oken settings					Admin name	
locess token	0	aCTZgyH7hDGSTt0USRK1c6CGODnGoCr4		•	The user used for authentication	
dmin name		Felix	✓ Othe	er 🗐 -	Days the token will be valid	20
ìme to live (davs)	0	120		-	Timestamp	5
		1540314202			Unix Timestamp of the creation date	
imestamp	v	1340214203		U EI*	Valid	5
alid		Generate new token		.	Checkbox which evaluates the expiry tin the token. As long as it is checked, the to is valid. This is a readonly field.	ie of ken

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

l l 🗄 🖿 ura ura en	
	^
A P Course Departmenter S (Virtual server nosting all services) [Fo0]	
Server Properties	
- Vo Assigned Services	
AV (Virus-Scanner)	
Service Properties	
🦾 Virus Scanner Settings	
🗈 🔛 DHCP (DHCP-Service)	
🕀 🦕 DNS (DNS-Service)	
🖨 🚔 NGFW (Firewall)	
IPS Policies	
🚱 IPS Exception Database	
👧 Response Messages	
Service Properties	
🔤 🖓 Security Policy	
🛓 👥 SNMPFX (SNMP-Service)	
🔬 🚺 VPN (VPN-Service)	
wiFi (Wi-Fi)	
😥 🚍 Default Box	
🖶 🔚 🔚 [I-T [7.2]	~
	4



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

/iews 🔕	App Redirect	Rest-	Арі			
tule						
Advanced	Bi-Directional		ै 🗌 Dynamic Rule	0	Deactivate Rule	
CMP Handling	Source VR Instance	default	✓ Destination	on VR Instance	default	-
bject Viewer 🛛 🔕	Source		Service	Destina	ation	
Object Viewer	Trusted LAN	~	<explicit-srv></explicit-srv>	✓ All Fire	wall IPs	
Object viewer	Ref: Trusted LAN Netwo	rks	TCP 8443	Ref: N	lanagement IP	
	Ref: Trusted Next-Hop N	letworks		Ref: S	ervice IPs	_
				Ref: D	HCP1 Local IP	
				<		>
				Redire	ction	
				Local Ad	dress	
				127.0.	0.1:8443	
	Authenticated User		Policies			
	Any	~	Default	~		
			Application Delicy	~		
			Application Policy			
			SSL Inspection Policy			
			N.A.	\sim		
			Schedule			
			Always	~		
			OoS Band (Fwd)			
			VoIP (ID 2)	\sim		
			QoS Band (Reply)			
			Like Fund	~		

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.

_			_	-	0	Object Viewer						
Rule Lists			Action	Na	A	pplications Networks	Services	Connection	ns ICMP	Schedules		8
Access Rules		0	Pass Dynamic NAT	BA	N	ame		Descri	ption			
bject Viewer		1	Block		5	All Firewall IPs	(59)	Ref: M	anagemen	t IP , Ref: Servic	e IPs , Ref: DHCP1 Local IP ,	, Ref:
Firewall Objects		2	App Redirect 127.0.0.2		2	Any ATD Quarantine		0.0.0.0)/0			
etworks		3	App Redirect 127.0.0.2		22	Auth-ACTDIR Auth-LDAP						
pplications		۲ <mark>4</mark>	App Redirect 127.0.0.2		27 C	Auth-MSNT Auth-RADIUS						
RL Filter IL Inspection		5	App Redirect 127.0.09			Auth-RSASecureID Barracuda Upda	S-1-4-5	005.4		<u>010 100 105</u> .0/	24 , 216.129.125.192/26 , 20	9.124
e Content		6	App Redirect 127.0.09		2	BoxACL connect.barracu	Add To	ource Source		(Alt+S)		
rvices		7	Pass Original Source IP		22	Control Center CustomExternal	Set As D	estination		(0.14.17)		
er and Groups nnections		8	App Redirect 192.168.200.200	BC	22	CustomExternal CustomExternal	Show Re	eferenced E	y	(AILTD)		
hedules orface Groups	~	< <			22	CustomExternal DHCP1 Local IF	Edit					
nected to 172.29.0.11 (v 7	.2.2-(SS	L Sec	ured (AES256-GCM-SHA384) Certi	æ	DHCP2 Local IF	New Ne	twork Obje	ct			



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*.

Genera				Description	
Туре	Generic Network Object (IP	, Network, Ranges)	\sim		~
Name	macmon-guest		Resolve		
				Network Color	~
Include	e Entries	+ 🧕 🌆	× 🦉	Exclude Entries	🕂 🐥 🔕 🕹 🗙
IF / Kel	r / Geo	Comment		IP / Her / Geo	Comment
					0% C 1

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.

D^	Description	Active				
0	nuli	no				
	notification 1	yes				
2	notification 2	yes				
	notification 3	yes				
ŀ	notification 4	yes				
0	macmonEvent	yes				
okup:	:					
			Delete	New	Copy	Change

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 [ipadresse]

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 ngflr3wall -d 172.29.0.111



Detail		\times
Notification		
Notification ID: Description:	IO macmonEvent Event must be confirmed	
Server Action	Client Action Thresholds	
Туре:	 Mail Execute Program SNMP Apple Push Notification Service 	
Parameter:	ification -u admin -p ngf1r3wall -d 172.29.0.111	
	Repeat Every: 0 <mark>↓</mark> sec ∨	
	OK Cance	!

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.

Detail		×
Event		
Event ID: Description:	5001 ATP malicious activity detected	
Notification ID:	10 macmonEvent	
	Persistent Propagate to CC Drop Event	
	OK Cancel	

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.

ail	
vent	
Event ID:	5004
Description:	DNS Sinkhole address accessed
Severity ID:	9 Information ~
Notification ID:	10 macmonEvent ~
Comment:	
	✓ Persistent
	Propagate to CC
	Drop Event
	OK Cancel



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".

Beschreibu	ng			
Konfiguratio	ı			
URL *				
https://10.10	.10.123:8443			
URL zu Barracuda	(z. B. 'https://172	2.23.27.96:9090/')		
API Schlüssel *				
•••••	•••••			
API Schlüssel				
API Version *				
v1				
Version der API (z	. B. 'v1')			
Server *				
S1				
Name des Server				
Dienst *				
NGFW				
Dienst				
Name des Firev	vall Objekts *			
macmon-tru	sted-devices			
Name des Objekt	s in der Firewall			
🖌 Aktiv				



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.

• Regel hinzu	fügen				
Aktionen	Status	Name	Ereignis	Beschreibung	Ergebnis
♦	aktiv	[BARRACUDA_FIREWALL] Delete endpoint rule	arp_offline	Created from Barracuda Firewall i	1 Reaktion(en)
♦ Ø ∅	aktiv	[BARRACUDA_FIREWALL] Create endpoint rule	arp_online	Created from Barracuda Firewall i	1 Reaktion(en)

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