



NetWyl Informatik
IT-Security Experts

Checkpoint Access Control Policy

Version 1.0

Dokument Name: Checkpoint_Acess Controll Policy

Dokumentenkontrolle

Version	Datum	Änderungsnotiz	Betroffene Seiten	Status	Author
1.0	10.07.2024				

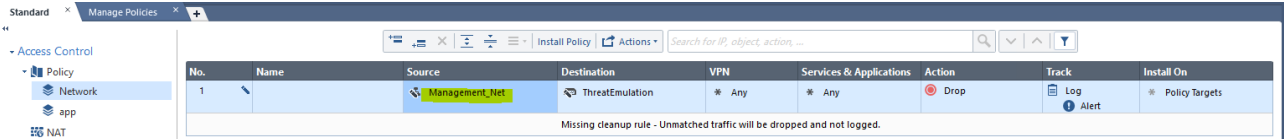
Copyright 2024 NetWyl Informatik

NetWyl Informatik GmbH
Täschmattstrasse 19
6015 Luzern
info@netwyl-informatik.ch
Phone: +41 41 520 73 90

First, we need to create mandatory rules to harden our security policy.

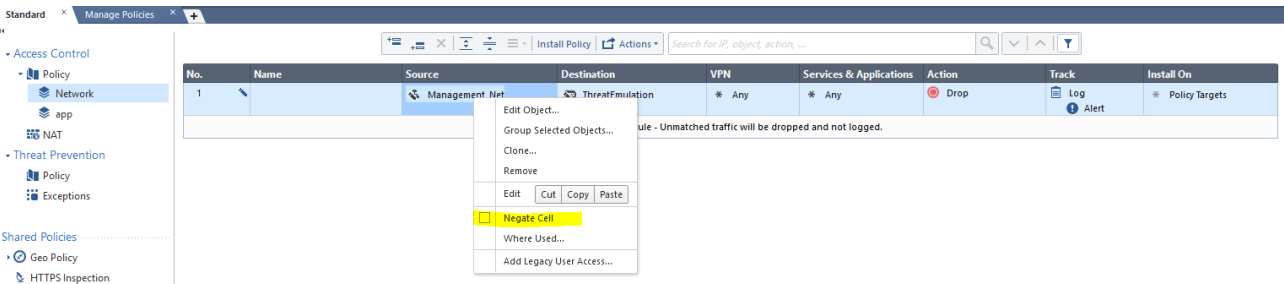
Stealth Rule

To do so, we need to create a **Stealth rule**. (All traffic that is not from your internal network will be dropped and your admins will be alerted)

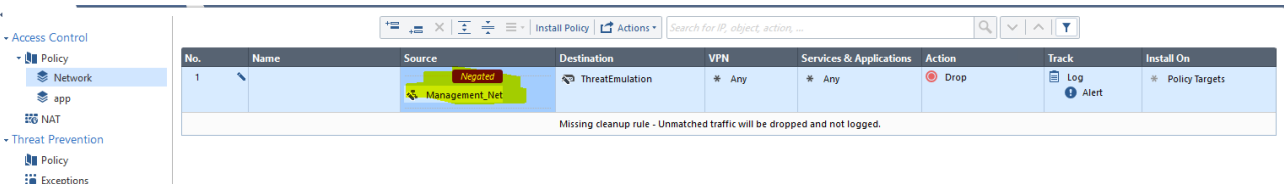


Management_Net – 172.16.10.0 /24 (Internal Net from which I manage my Firewall)

Then right-click Management_Net -> **Negate**



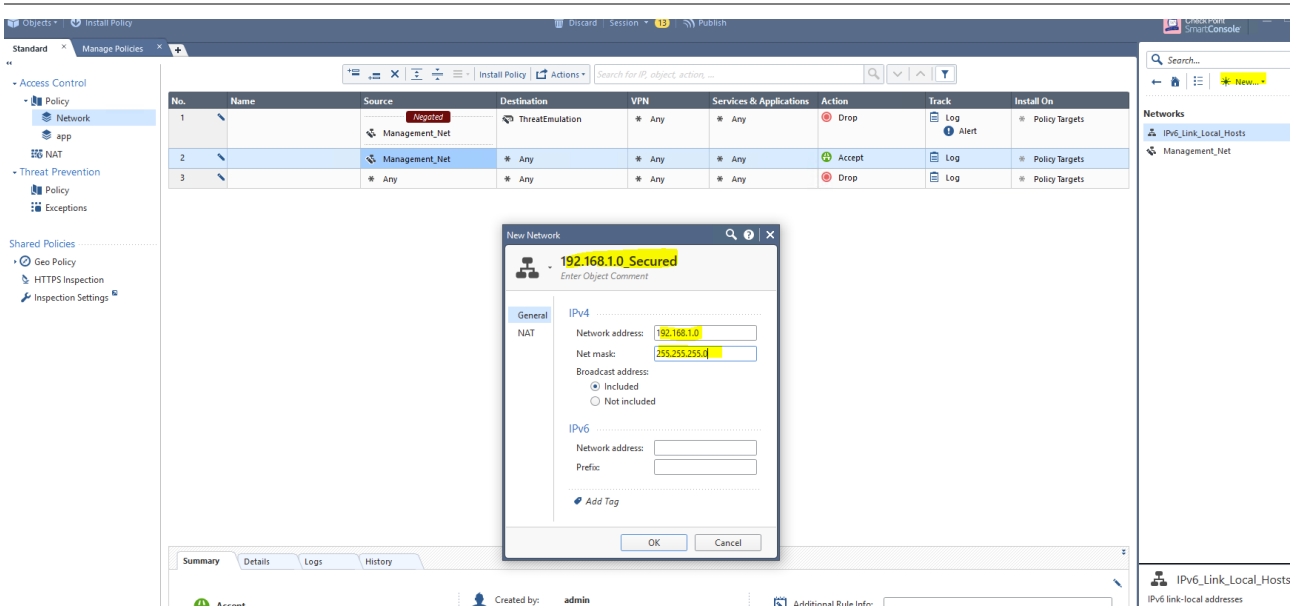
->



Once it's negated, everything else will be dropped trying to connect to our Gateway, except for Management_Net.

Cleanup Rule

Cleanup Rule – drops all traffic that wasn't matched with other rules. Cleanup rule always placed last in the security policy.



The screenshot shows the Palo Alto Networks SmartConsole interface. A table lists three policy rules:

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1		Management_Net	ThreatEmulation	* Any	* Any	Drop	Alert	* Policy Targets
2		Management_Net	* Any	* Any	* Any	Accept	Log	* Policy Targets
3		* Any	* Any	* Any	* Any	Drop	Log	* Policy Targets

A 'New Network' dialog box is open, showing the configuration for a new network object named '192.168.1.0_Secured'. The 'General' tab is selected, and the 'IPv4' section is active. The 'Network address' is set to '192.168.1.0' and the 'Net mask' is '255.255.255.0'. The 'Broadcast address' is empty. Under the 'NAT' section, the 'Included' radio button is selected. The 'IPv6' section is currently empty.

Then, we add that object to rule 2

Then fill the policy with the rules needed for your environment.