



**NetWyl Informatik**  
IT-Security Experts

# Checkpoint Access Control Policy – URL filtering and App control

Version 1.0

Dokument Name: Checkpoint\_Access Control Policy  
– URL filtering and App control

---

## Dokumentenkontrolle

Version	Datum	Änderungsnotiz	Betroffene Seiten	Status	Author
1.0	10.07.2024				

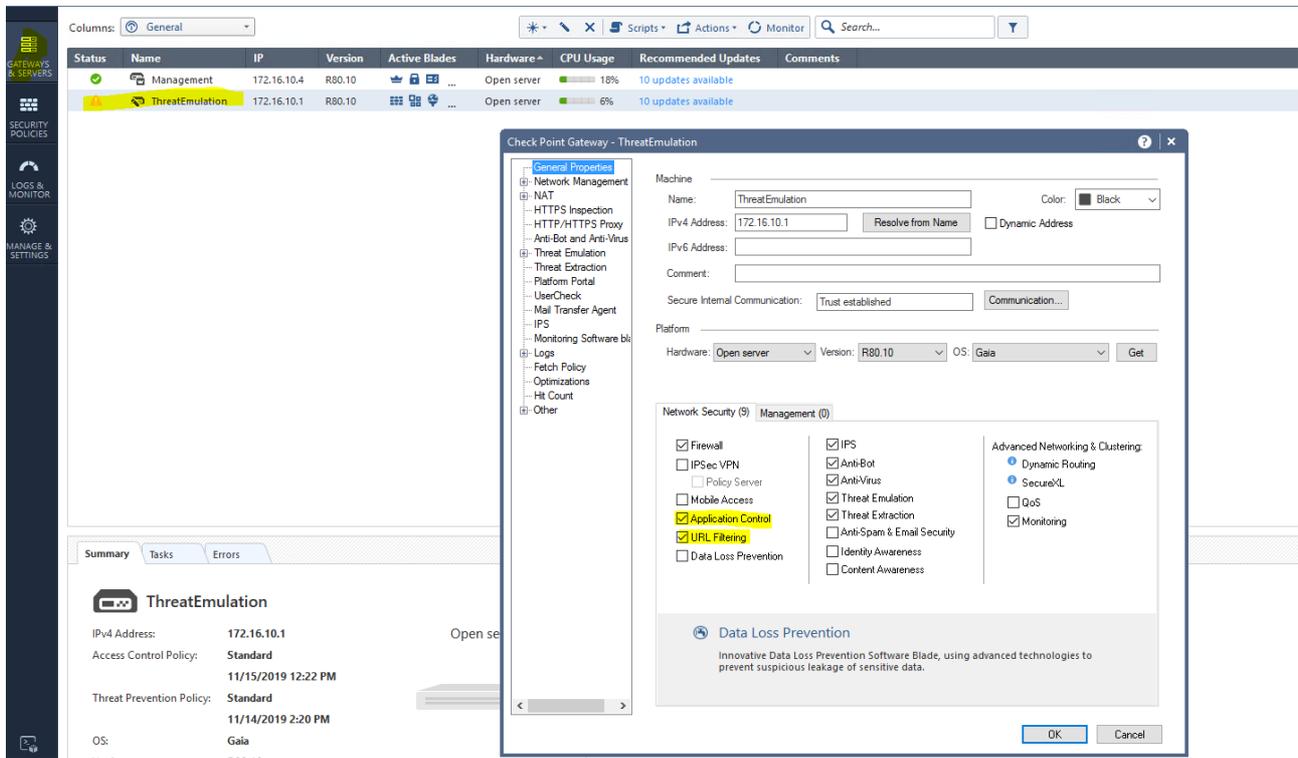
## Copyright 2024 NetWyl Informatik

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

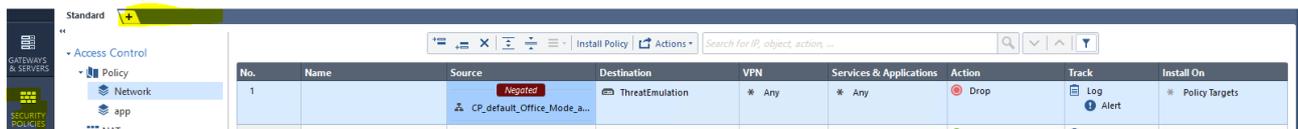


## Access Control Policy – URL filtering and APP control

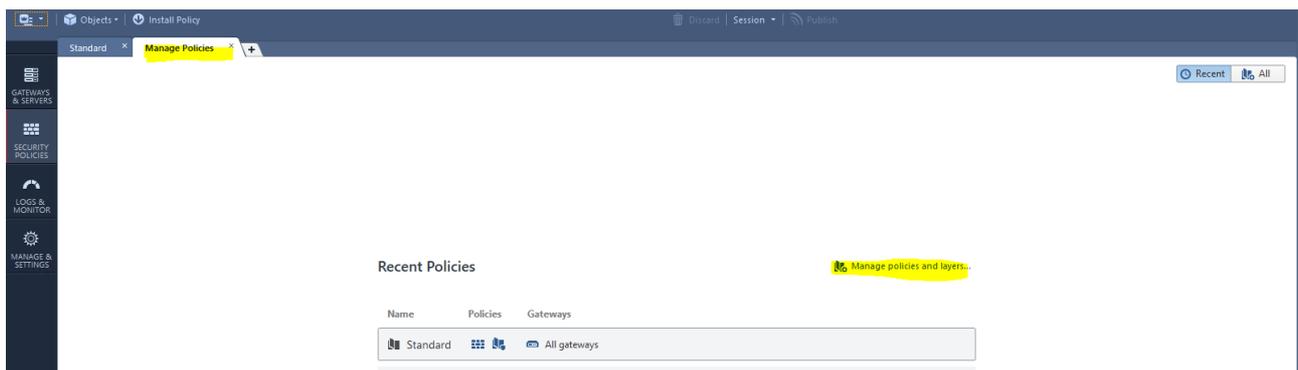
First, enable URL filtering and APP control in your Gateway properties

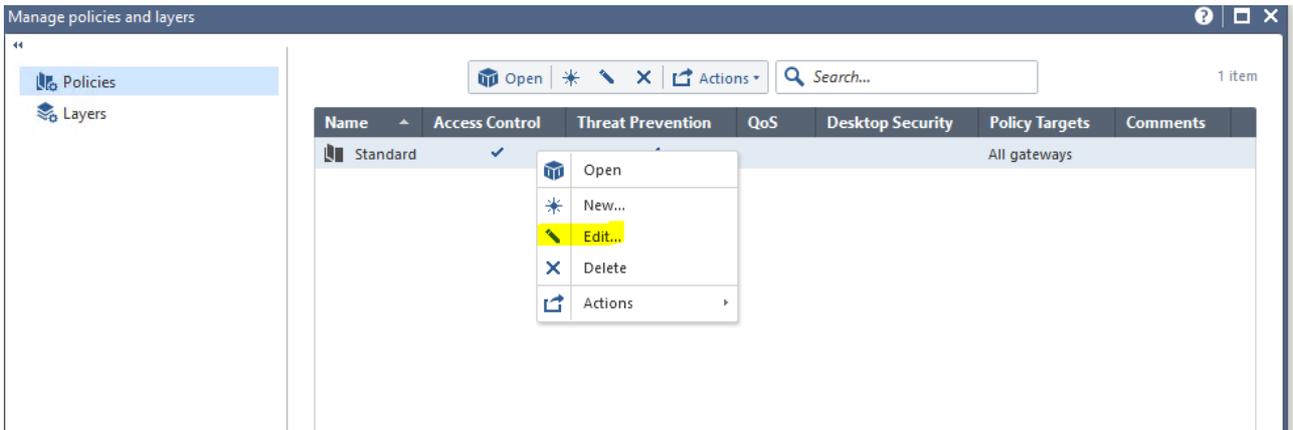


Inside the Security Policy click + sign

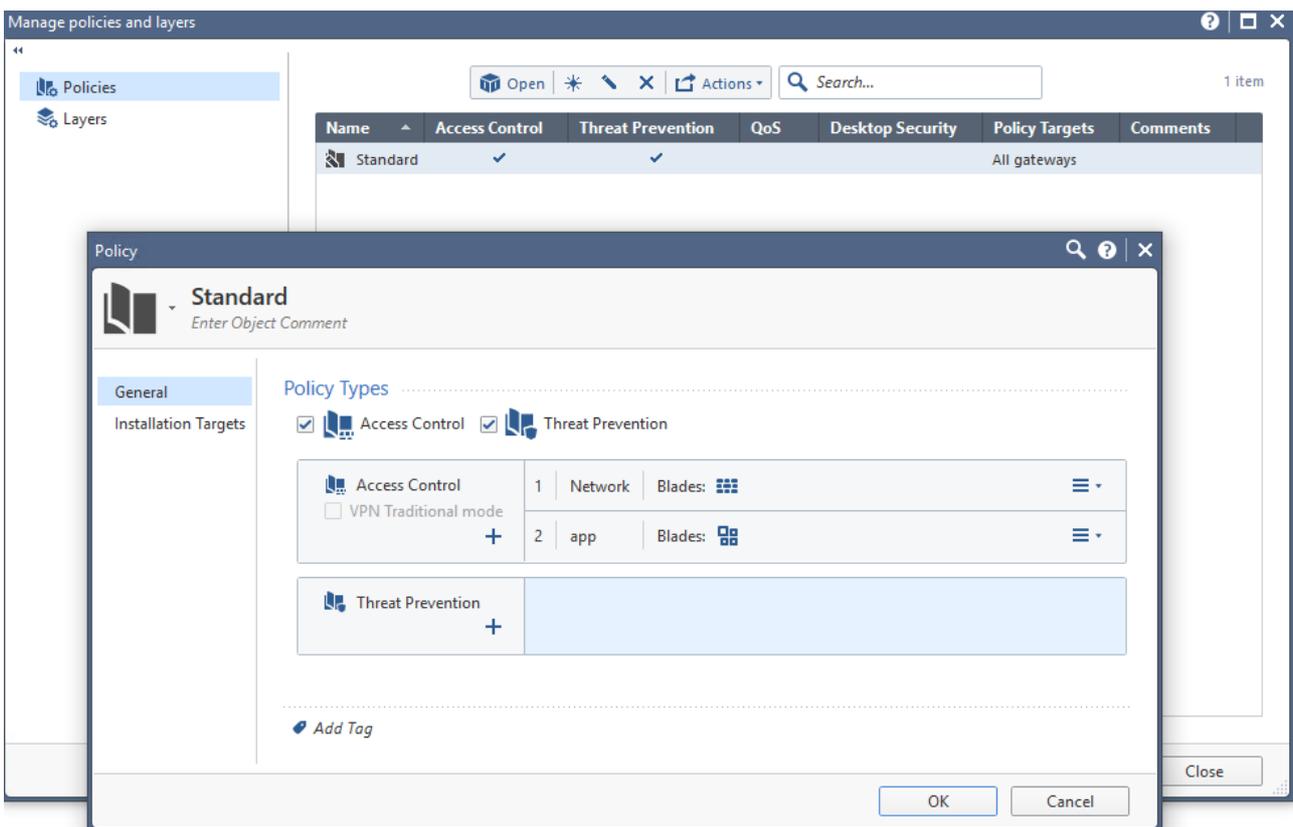


In R80.XX you can Manage Layers of your policies. We will configure that. Click Manage policies and layers.

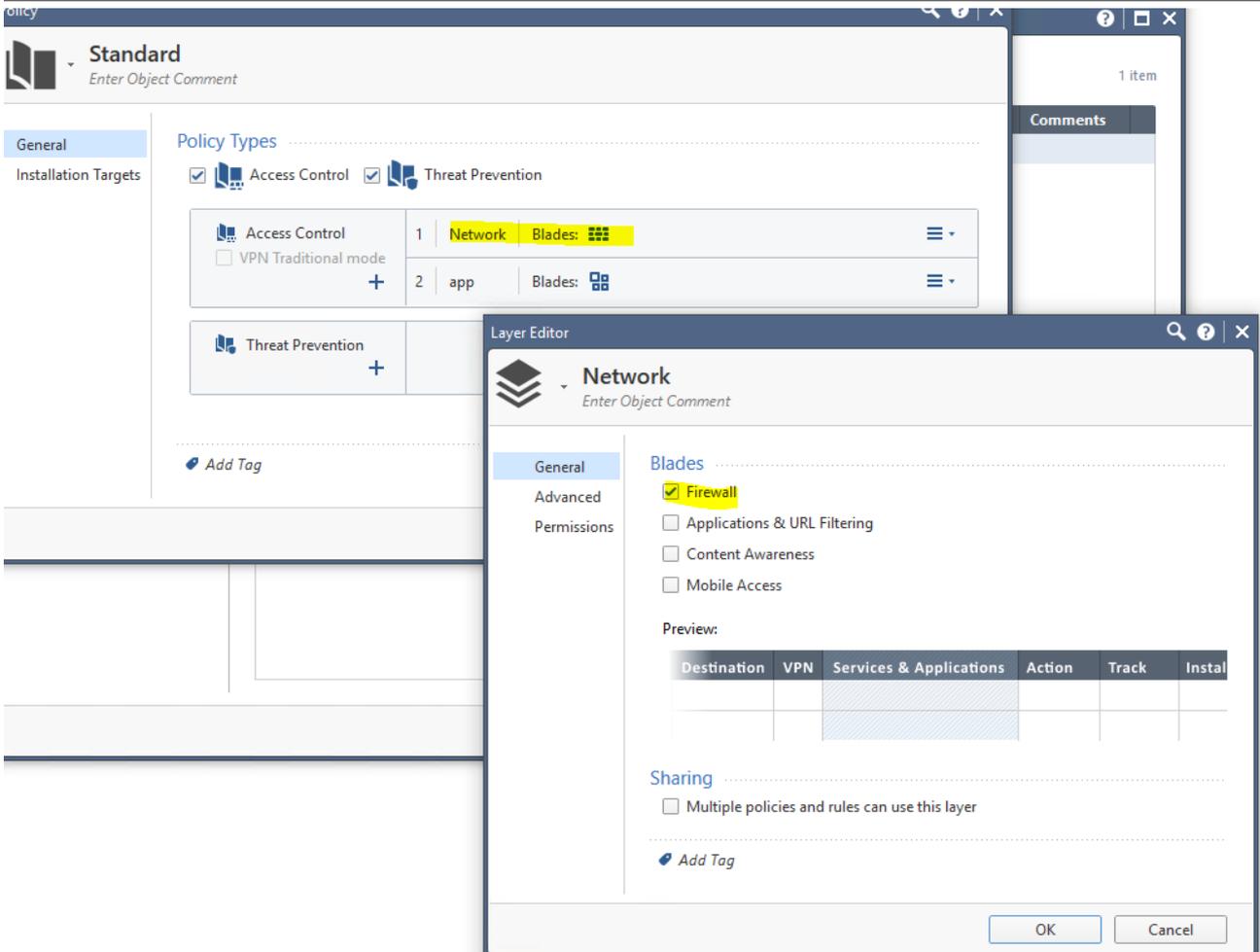




-> Select Access Control and Threat Prevention. However, for access control we are going to split (Firewall blade and app control/url filtering ones). That would be our policy package.



Double click Network and check only Firewall.



The screenshot displays the Checkpoint management console. The main window shows the configuration for a policy named "Standard". Under "Policy Types", both "Access Control" and "Threat Prevention" are selected. The "Access Control" section is expanded to show two layers:

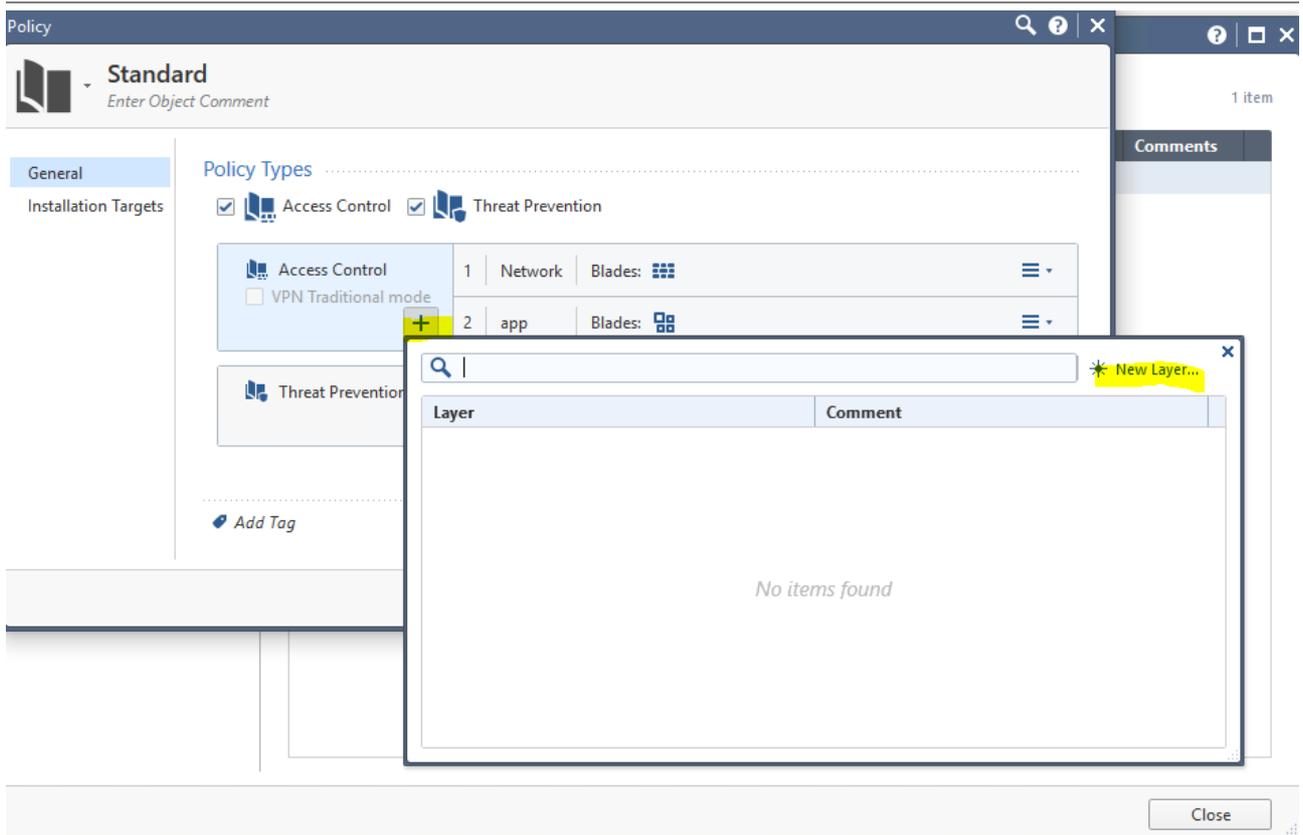
Layer ID	Name	Blades
1	Network	Blades: [Firewall]
2	app	Blades: [Applications & URL Filtering]

A "Layer Editor" dialog box is open for the "Network" layer. It shows the "Blades" section with "Firewall" selected. Below it is a "Preview" table:

Destination	VPN	Services & Applications	Action	Track	Instal

The dialog also includes a "Sharing" section with an unchecked checkbox for "Multiple policies and rules can use this layer".

Click + under Access control to create a new layer for app control/url filtering.



Select only Application and URL filtering

Layer Editor 🔍 ? | ✕

 **app**  
Enter Object Comment

**General**  
Advanced  
Permissions

**Blades** .....

- Firewall
- Applications & URL Filtering
- Content Awareness
- Mobile Access

**Preview:**

Destination	VPN	Services & Applications	Action	Track	Instal

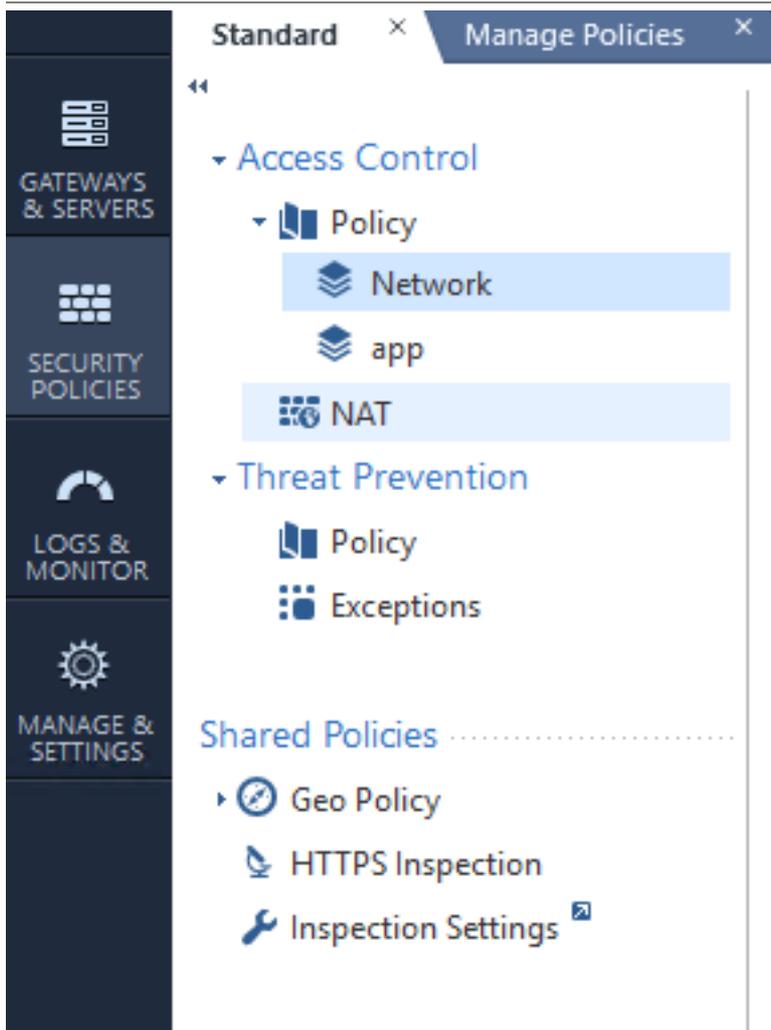
**Sharing** .....

- Multiple policies and rules can use this layer

 Add Tag

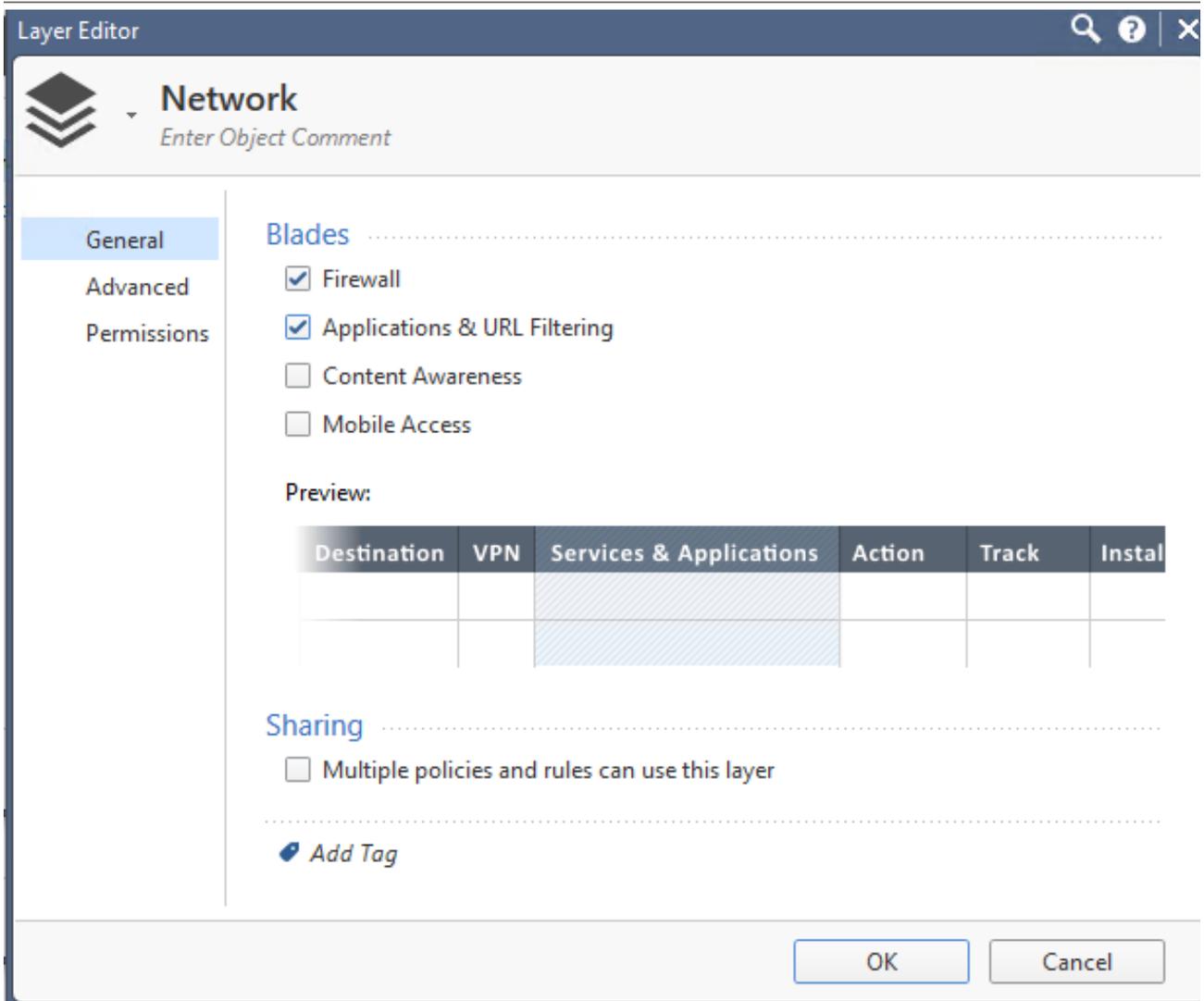
OK Cancel

Right after you click Ok, you will see your Policy Package as show on the screenshot.



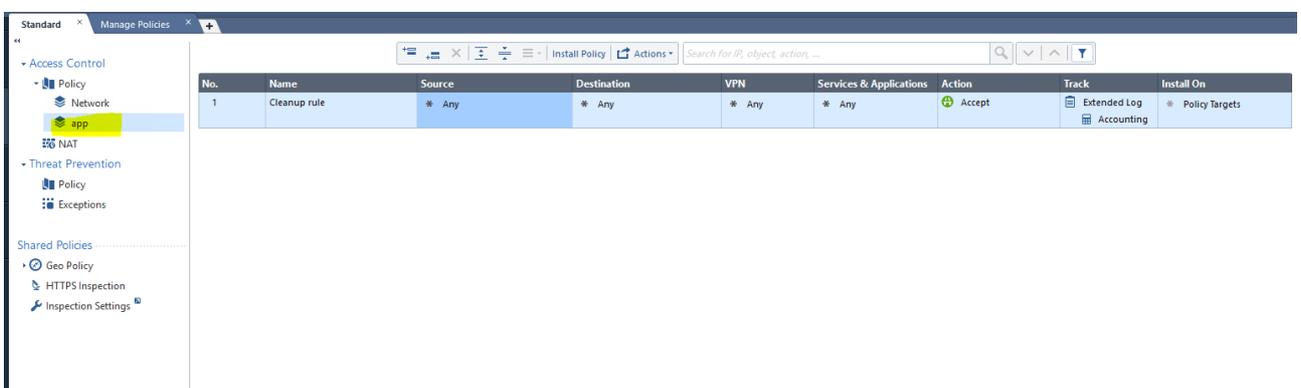
Your firewall policy is different from URL and App control. You can select both blades to be under one tab. But for the purposes of learning, we are splitting them.

Firewall and Application and Url filtering inside one layer



Creating Application Control and URL filtering rules.

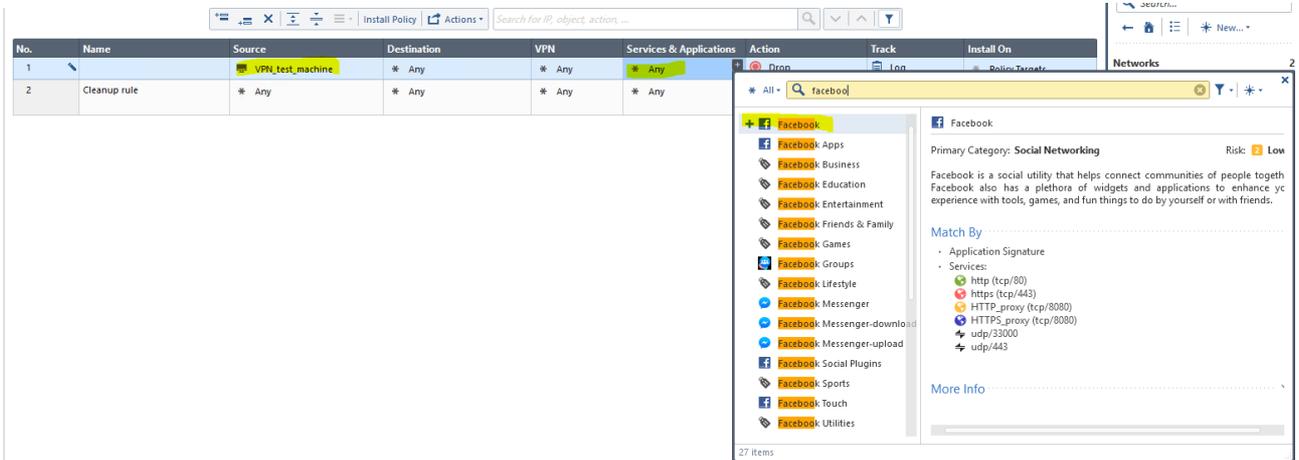
Click app layer, and create a rule as you would in a policy tab.



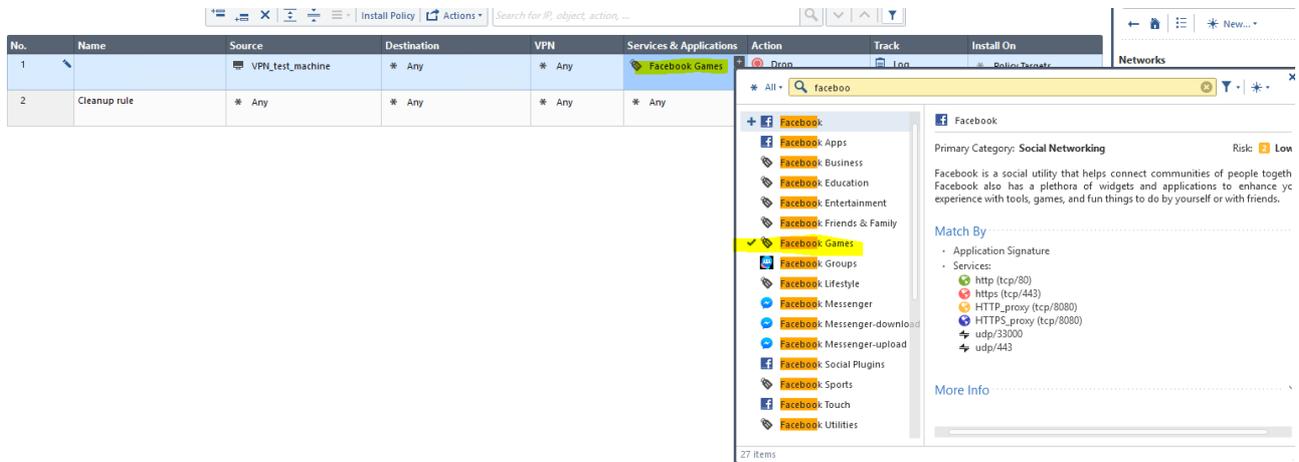
In URL/APP control it's recommended to use blacklist. Everything is allowed, unless specifically blocked.

As a cleanup rule we have “allow any any accept”.

You create a rule above your cleanup rule, and specify apps you want to block.

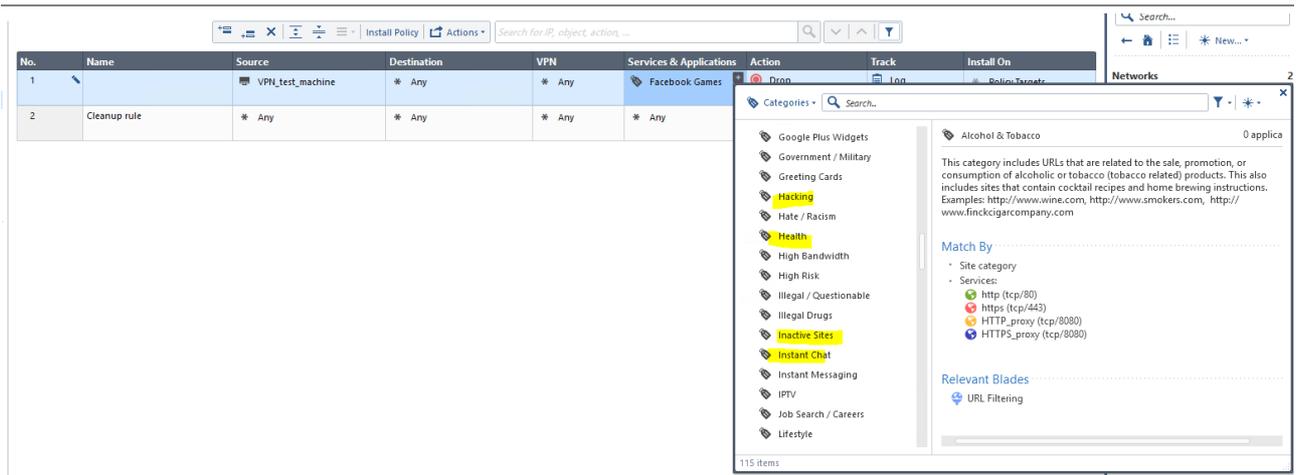


Apart from just blocking the whole “Facebook” related stuff, you can only block specific things related to Facebook. For example, Facebook Games, while leaving the access to Facebook.



You can select categories. Websites that fall under certain category will be blocked.





More in depth configuration can be found at Manage and settings -> Blades -> Application Control and URL Filtering -> Advanced Settings

