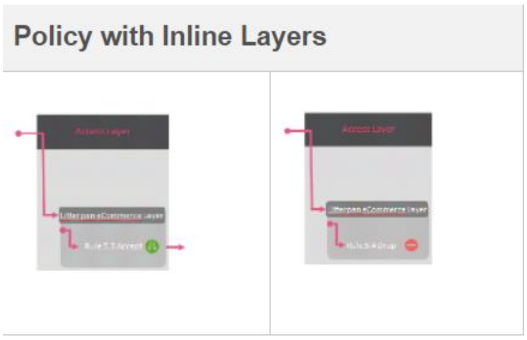
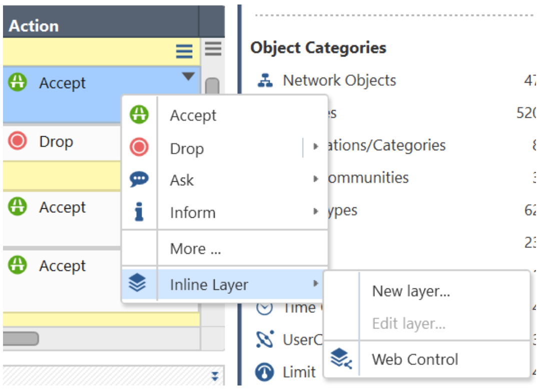
Inline Layer Policy Best Practice

In **Inline Layers** only traffic *matched/accepted* on the parent rule will reach and be inspected by the inside layer rules.

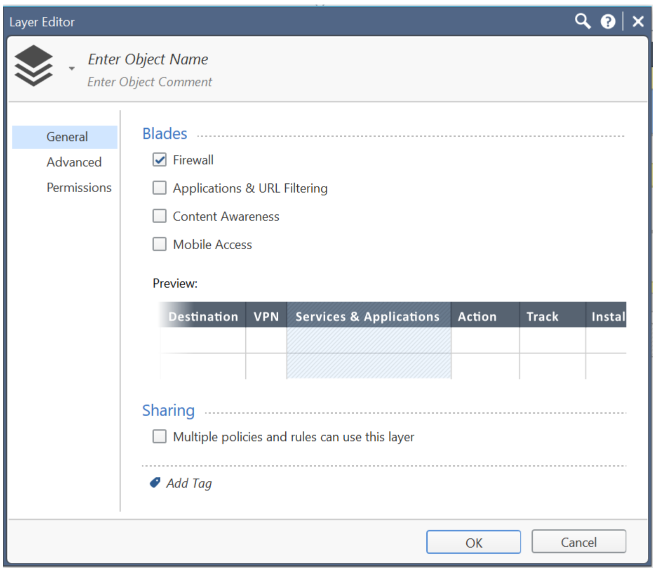
Example of traffic matching using Inline Layers


Policy with Inline Layers
Access Layer
Litterpanta eCommerce Layer
Rule 5.3 Accept
Access Layer
Litterpanta eCommerce Layer
Rule 5.4 Drop

Creating Inline Layers in a Policy for Access Control



- Right Click “Action” column then place cursor over “Inline Layer”
- Select New layer



Enter Object Name

Enter Object Comment

Blades

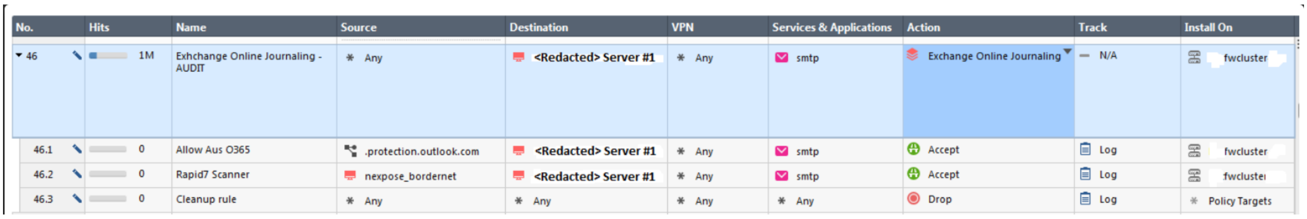
- ☑ Firewall
- ☐ Applications & URL Filtering
- ☐ Content Awareness
- ☐ Mobile Access

Sharing

- ☐ Multiple policies and rules can use this layer

- Enter desired Object name followed by selecting which blade you wish to apply then hit OK.

Example of an Inline Layer Parent Rule with inside sub-rules:



No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
46	1M	Exhchange Online Journaling - AUDIT	Any	<Redacted> Server #1	Any	smtp	Exchange Online Journaling	N/A	fwcluster
46.1	0	Allow Aus O365	.protection.outlook.com	<Redacted> Server #1	Any	smtp	Accept	Log	fwcluster
46.2	0	Rapid7 Scanner	nexpose_bordernet	<Redacted> Server #1	Any	smtp	Accept	Log	fwclustei
46.3	0	Cleanup rule	Any	Any	Any	Any	Drop	Log	Policy Targets

- It is also best practice to add a cleanup rule at the end of each inside rules for logging purposes.

Build xx rules with Inline Layers for efficiency. Below are a list of Parent Inline Layer Rules to create in your Policy.

- **Firewall Management Rules**
  - Allow traffic between your Management Server(s) and gateway(s)
  - Allow traffic from a specific terminal server to manage gateway(s) and/or Management Server(s)
- **Stealth Rule**
  - Deny unwanted traffic going to your gateways
- **Outbound Rules**
  - Allow access to internet based on your companies rules and regulation
- **Inbound Rules**
  - Allow incoming traffic to your environment (branch office, Data center, etc.). This traffic can be from the internet, another office, an external partner, customer, etc.
- **DMZ to DMZ Rules**
  - Traffic that is allowed within your environment for organization systems and resource.
- **Cleanup Rule**
  - Create Any Any with Drop action to log denied traffic

Having Inline Layers creates operational efficiency by having a packet be first matched through the list of Parent Rules instead of going through hundreds of access control rules.