Policies

01 | Local-in policy

Met de functie *Local in Policy* op een FortiGate apparaat kun je de toegang tot de administratieve interfaces van de firewall beheren. Deze policy maakt het mogelijk om specifieke toegangspaden voor beheerders te configureren, zodat je kunt bepalen welke IP-adressen of netwerken wel of niet toegang krijgen tot de beheermogelijkheden van het apparaat. Dit is een belangrijk hulpmiddel voor het versterken van de beveiliging, aangezien het het risico op ongeautoriseerde toegang tot de device instellingen vermindert.

```
config firewall local-in-policy
    edit 1
        set intf "<WAN interface>"
        set srcaddr "<Firewall address>"
        set dstaddr "all"
        set action accept
        set service "ALL_ICMP" "SNMP"
        set schedule "always"
    next
    edit 2
        set intf "<WAN interface>"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL"
        set schedule "always"
    next
end
```

Deze regels zorgen ervoor dat alleen verkeer voor ICMP (ping) en SNMP (voor netwerkbeheer) wordt toegestaan naar de firewall via de opgegeven WAN-interface, terwijl al het andere verkeer wordt geblokkeerd. De eerste regel staat specifiek ICMP en SNMP toe vanaf een bepaald IP-adres, terwijl de tweede regel alle andere diensten voor elke bron blokkeert.

02 | Negate Policy

Negate kun je gebruiken als omgekeerd policy object.
Geef je bijvoorbeeld aan dat je RFC1918 als destination Negate, dan word alles toegestaan behalve RFC1918.

Deze functie gebruik je bijvoorbeeld als je al het internet verkeer wil toestaan behalve bepaalde URL's, hiermee heb je dan maar 1 policy in plaats van 2.

In het voorbeeld hieronder kun je naar alle internet adressen toe, behalve 1.1.1.1

```
config firewall policy
    edit 0
        set srcintf "VLAN2001"
        set dstintf "wan1"
        set action accept
        set srcaddr "N-10.20.1.0/24"
        set dstaddr "H-1.1.1.1"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
        set dstaddr-negate enable
    next
end
```