DrayTek

Firewall

Object Based

Firewall Cases

In deze handleiding gaan we een voorbeeld geven hoe u een bepaalde situatie kunt oplossen doormiddel van een aantal Firewall >> Filter Rules.

Situatie: Bedrijf

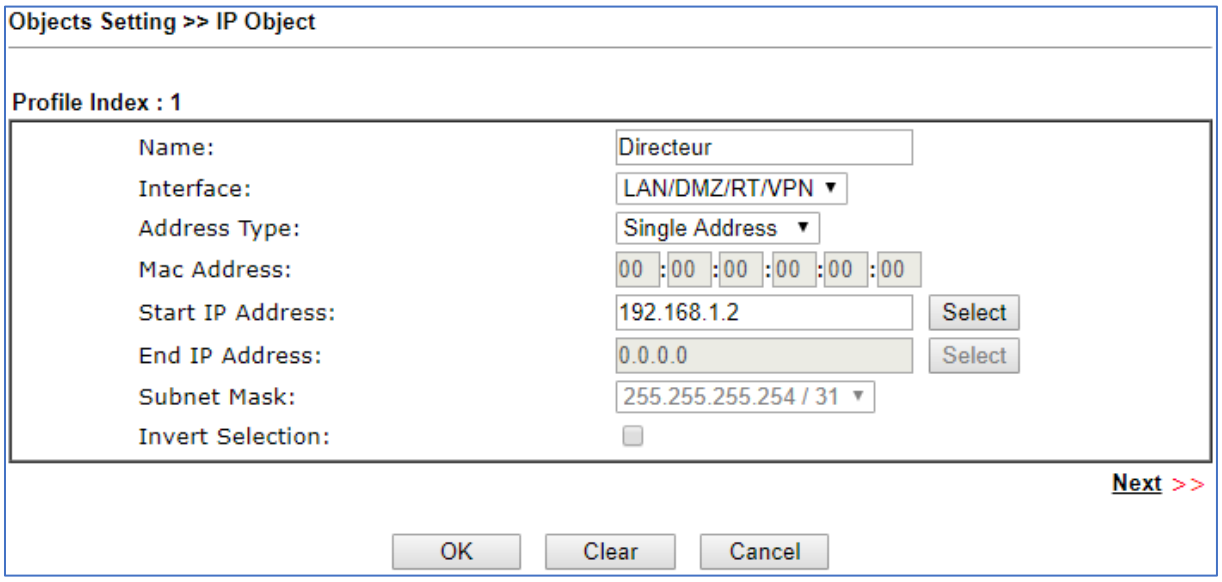
U heeft van de directeur een opdracht gekregen om voor zijn bedrijf enkele firewall regels aan te maken. Het bedrijf bestaat uit 2 afdelingen; een verkoop afdeling en een support afdeling. Tevens heeft elke afdeling een afdelingshoofd. Voor de volgende groepen moet u regels aanmaken:

- **Directeur:** 192.168.1.2
- **Hoofd afdeling Verkoop:** 192.168.1.20
- **Afdeling Verkoop:** 192.168.1.21 t/m 192.168.1.39
- **Hoofd afdeling Support:** 192.168.1.40
- **Afdeling Support:** 192.168.1.41 t/m 192.168.1.45

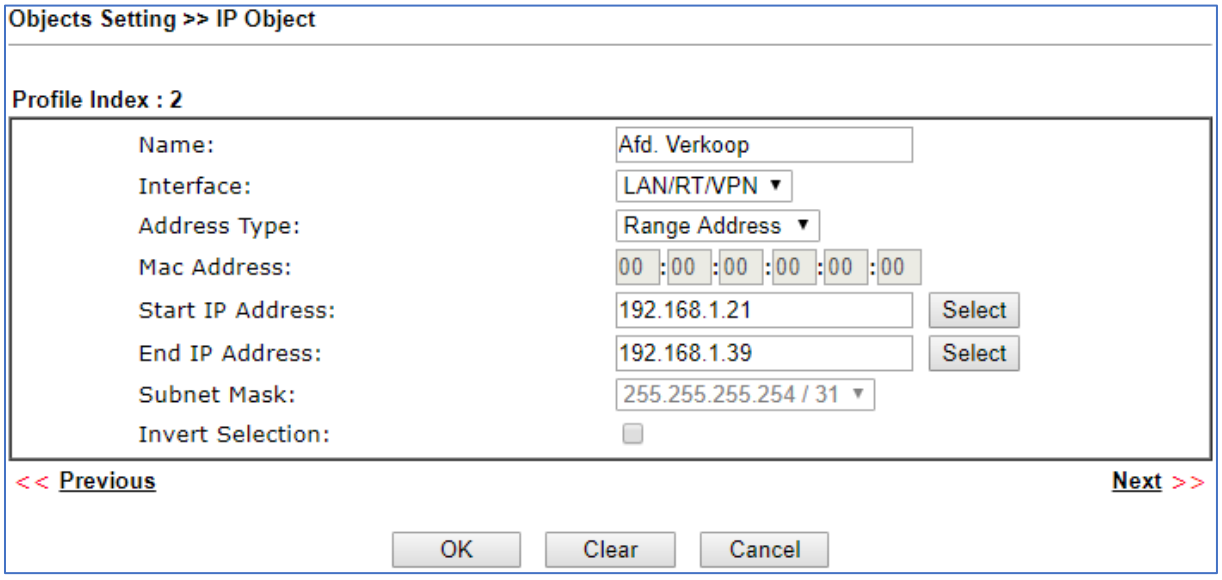
De directeur wil dat de afdeling verkoop en support alleen gebruik mogen maken van poort 80. Hij wil voor zijn afdelingshoofden en zichzelf volledig toegang.

U begint met het aanmaken van verschillende IP-Objecten voor de verschillende afdelingen, dit kunt u doen bij ‘Objects Settings >> IP-Objects’. U maakt een nieuw object aan door op een bepaald nummer te klikken.

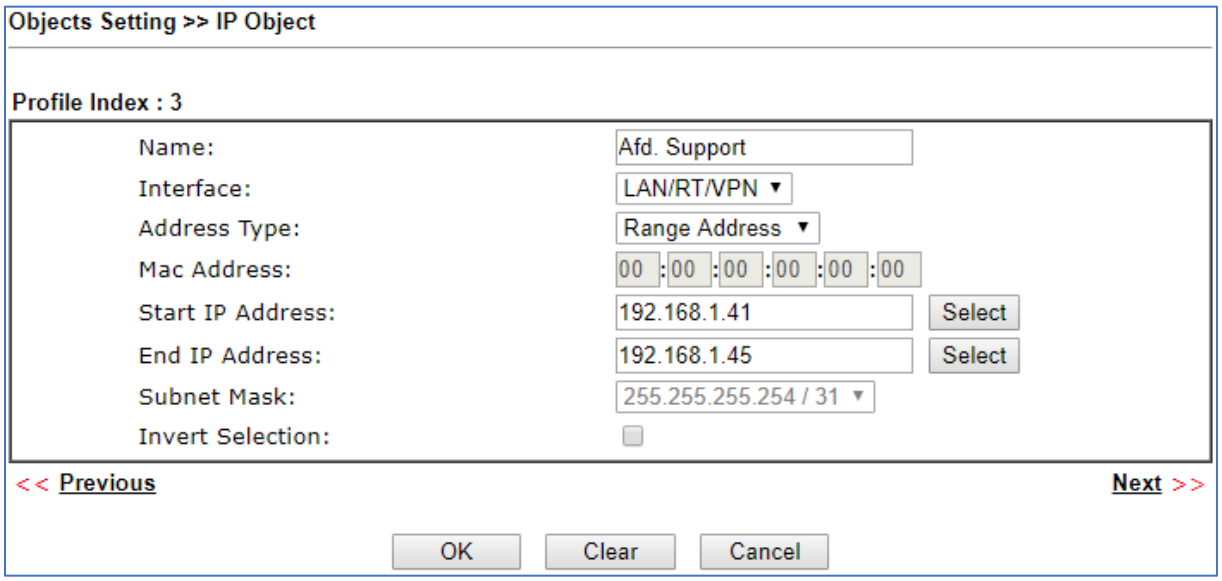
Als eerste maakt u een IP-Object aan voor de directeur, zoals u ziet op onderstaande afbeelding. Hiervoor maakt u gebruik van de LAN interface, en bij Address type selecteert u ‘Single Address’.



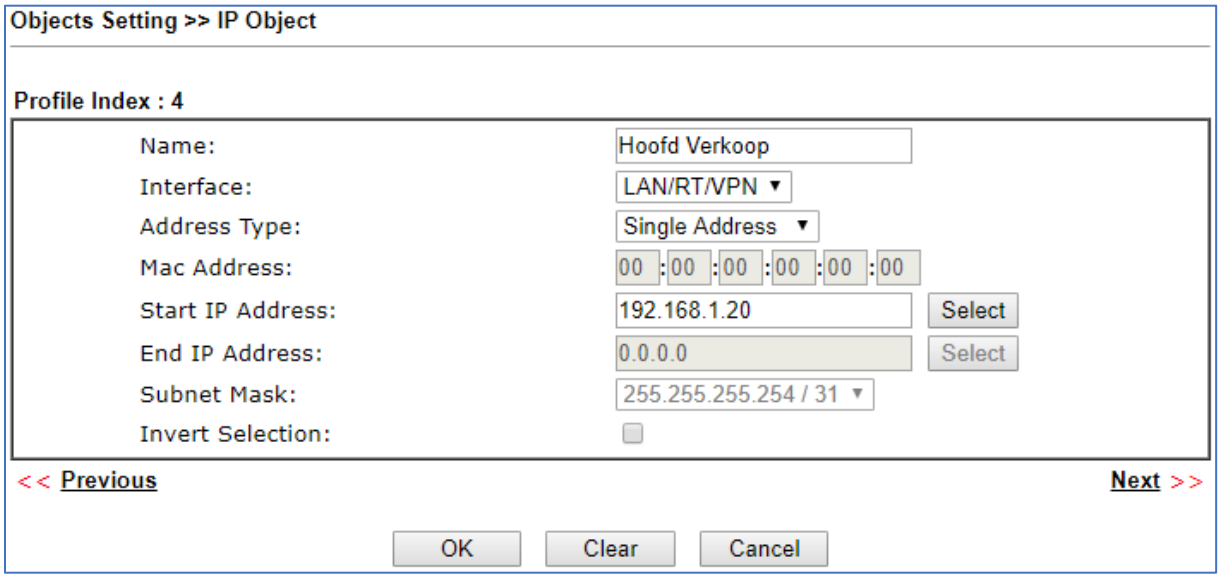
Vervolgens gaat u een IP-Object aanmaken voor de verkoop afdeling, hierbij maakt u gebruik van een reeks IP-adressen. Bij Interface selecteert u wederom de LAN kant, aangezien de verkoop afdeling aangesloten is op het interne netwerk.

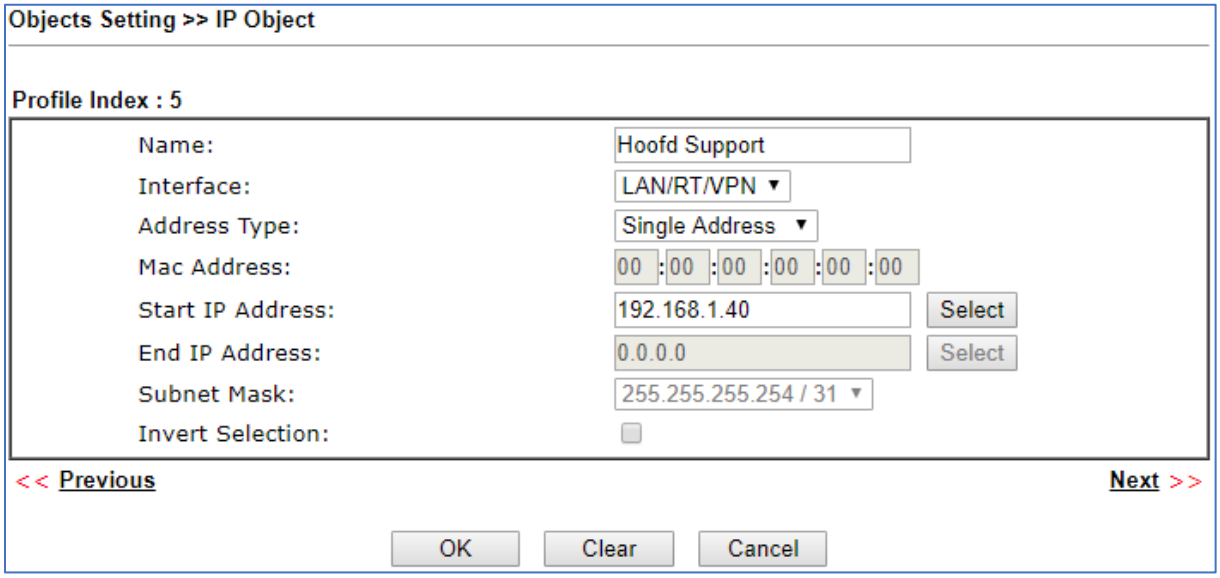


Hetzelfde doet u voor de support afdeling, hierbij gebruikt u ook de LAN interface.

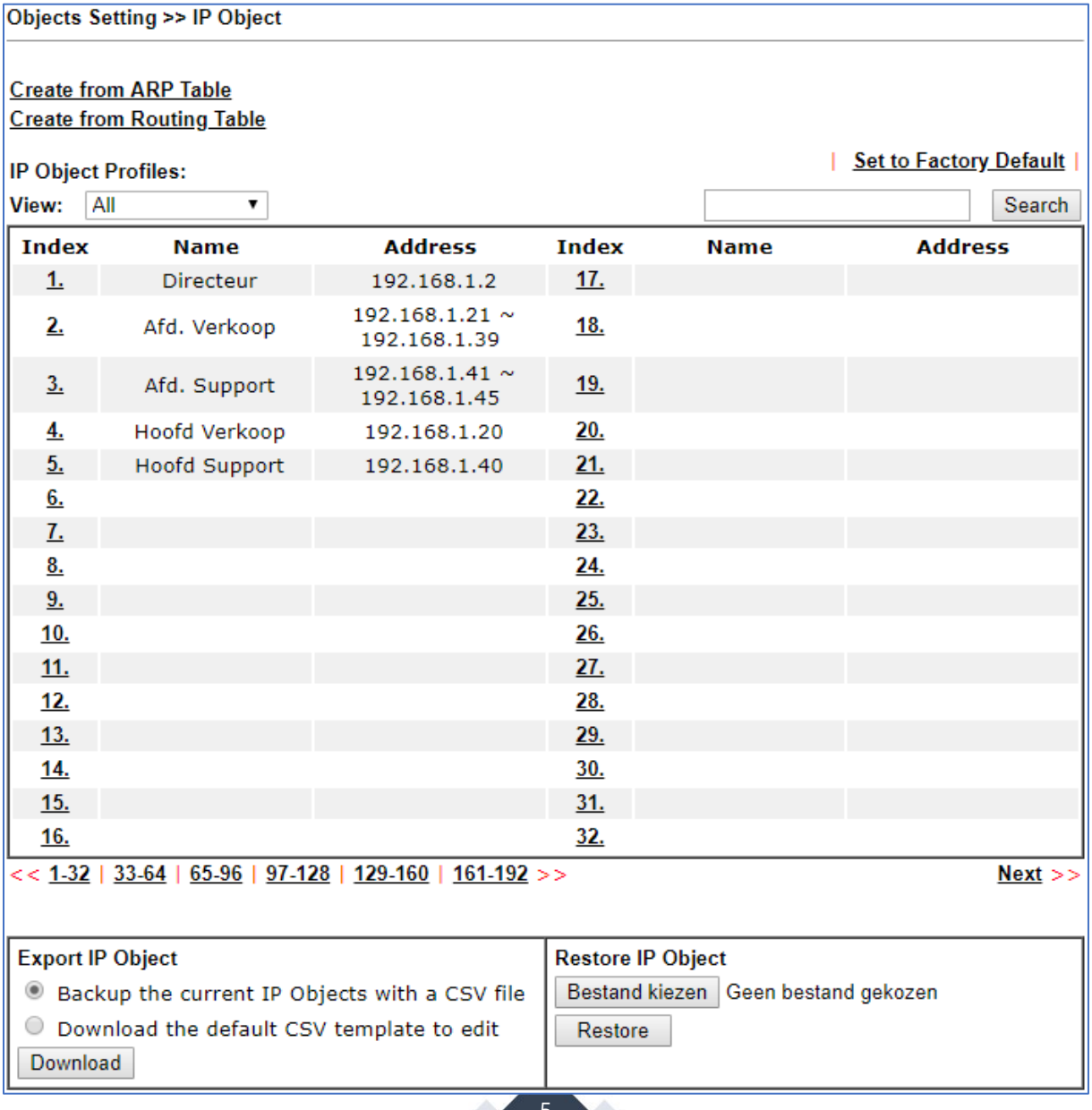


U moet nu alleen nog twee IP-Objecten aanmaken voor de afdelingshoofden, zoals u ziet op onderstaande afbeeldingen. Hierbij maakt u gebruik van een Single Address.

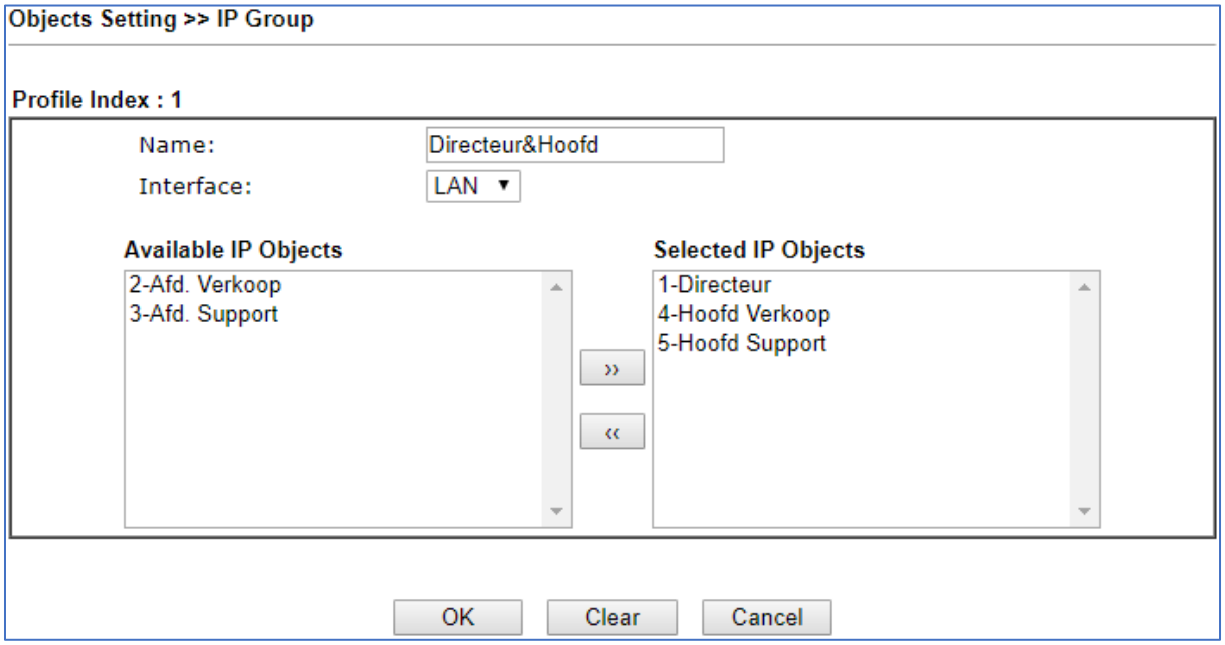




Op de onderstaande afbeelding ziet u de zojuist aangemaakte IP-Objecten:

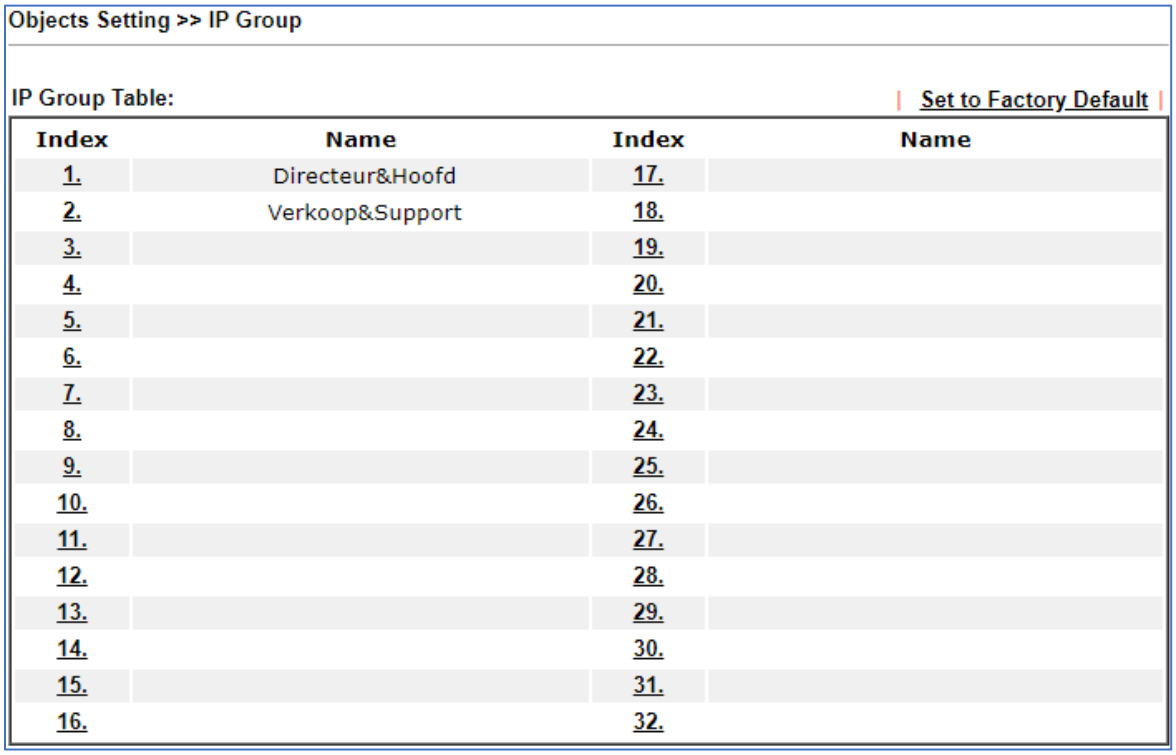


Nu we alle IP-Objecten hebben aangemaakt moeten we deze nog verdelen in een tweetal IP-Groups. De afdeling verkoop en support moeten in 1 IP-Group komen, en de directeur en de 2 afdelingshoofden ook. Navigeer naar 'Object Setting >> IP Group' en klik op een Index nummer.

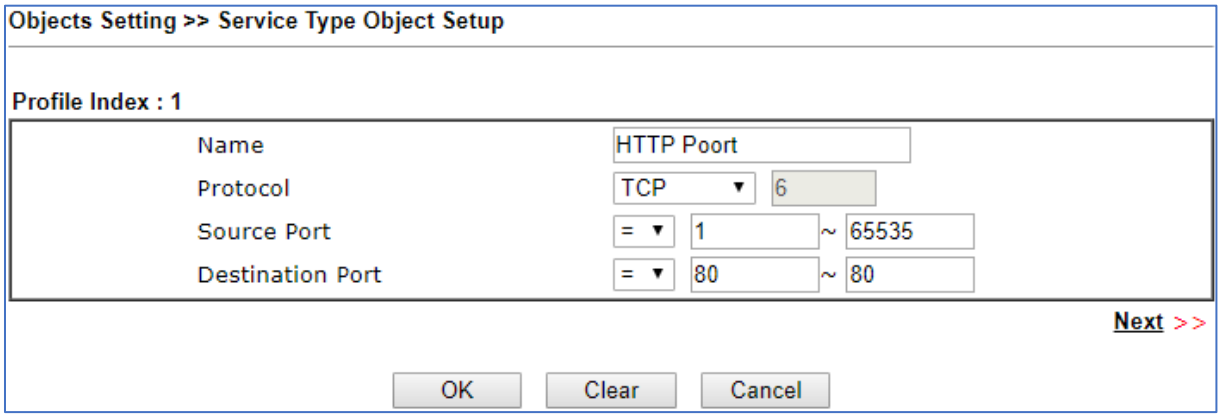


Wanneer u de IP-Objecten correct hebt aangemaakt krijgt u bij 'Available IP Objects' een 5 tal IP-objecten te zien. Deze 5 IP-objecten gaat u verdelen in 2 groepen, een voor de directeur en de twee afdelingshoofden en een voor de twee afdelingen. U vult bij 'Name' de bijbehorende naam in en geeft bij 'Interface' de LAN interface op. Vervolgens selecteert u de juiste IP-Objecten en klikt op onderstaande afbeelding om ze in een groep te plaatsen.

Zoals u in onderstaande afbeelding ziet hebben we 2 IP-Groups aangemaakt. Natuurlijk heeft u de mogelijkheid om meerdere IP-Objecten en/of IP-Groupen aan te maken.

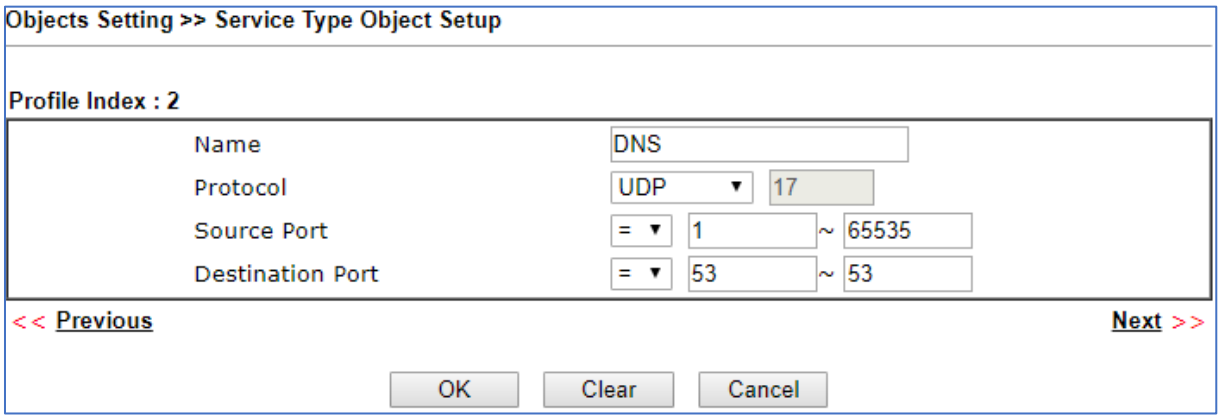


Bij 'Objects Settings' heeft u ook de keuze om een 'Service Type Object' en 'Service Type Group' aan te maken. U kiest voor een Service Type Object. Hierin gaat u een object aanmaken voor poort 80.

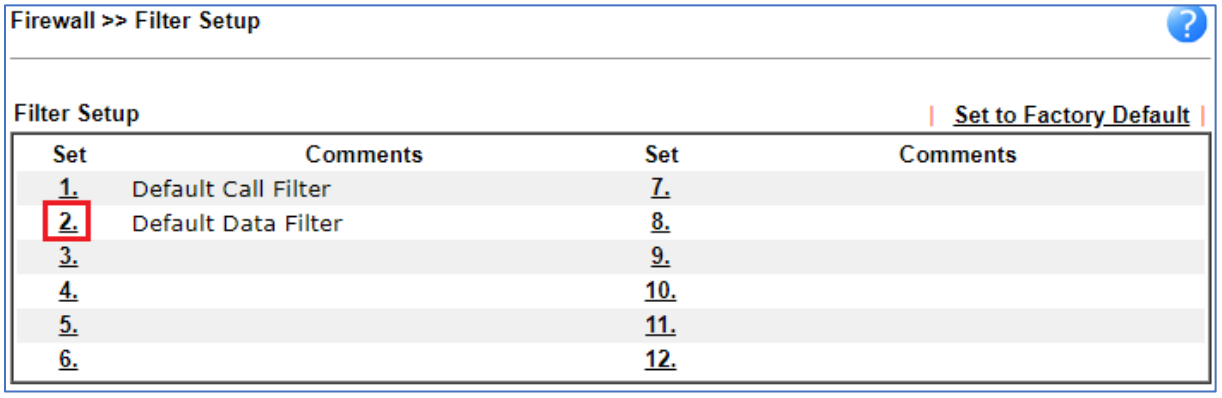


Belangrijk: De Source port is een Pseudo poort, deze wordt door de DrayTek gebruikt voor inkomende en uitgaande sessie's. Advies is deze altijd op 1 t/m 65535 te laten staan.

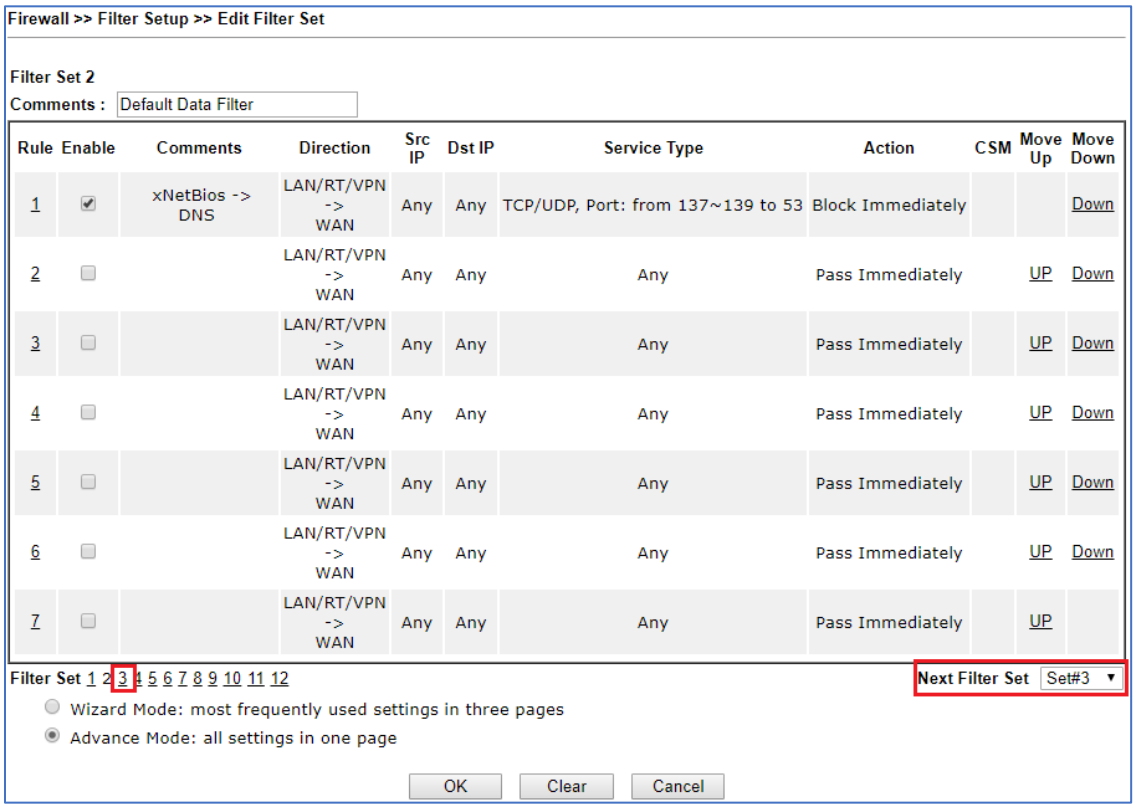
We maken hierna nog een Service Type object aan voor DNS verkeer.



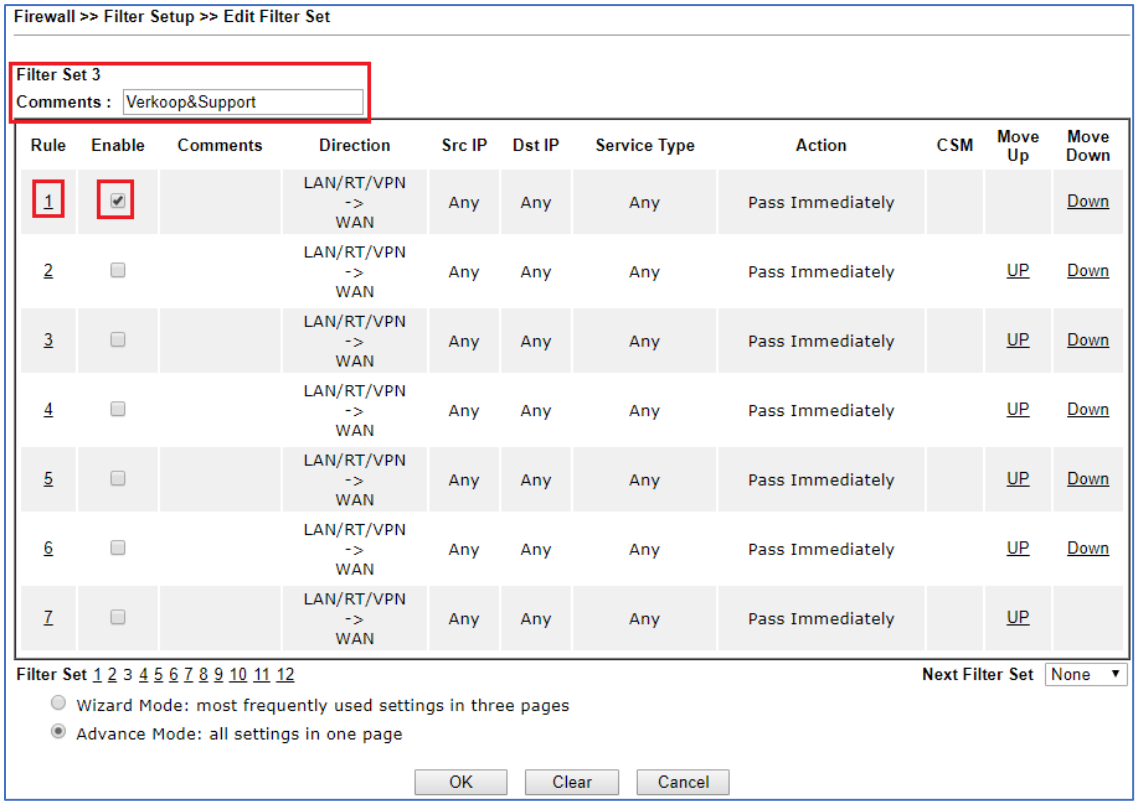
Navigeer vervolgens naar 'Firewall >> Filter Setup' en klik op Filter Set 2 (Default Data Filter).



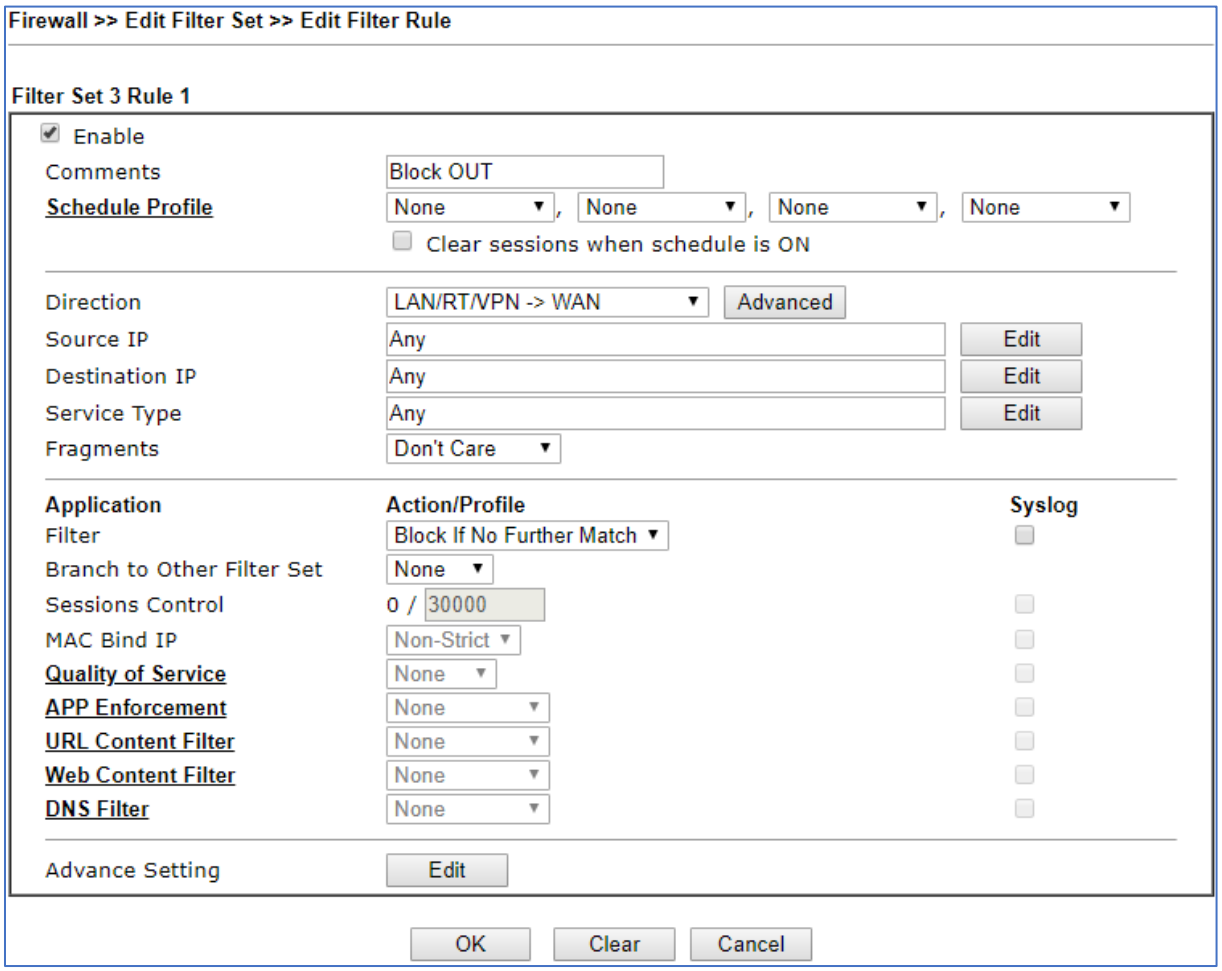
Vervolgens zet u rechts onderin de Next Filter Set op Set#3 en klikt u links onderin op Filter Set 3 om een hier een nieuwe firewall regel aan te maken.



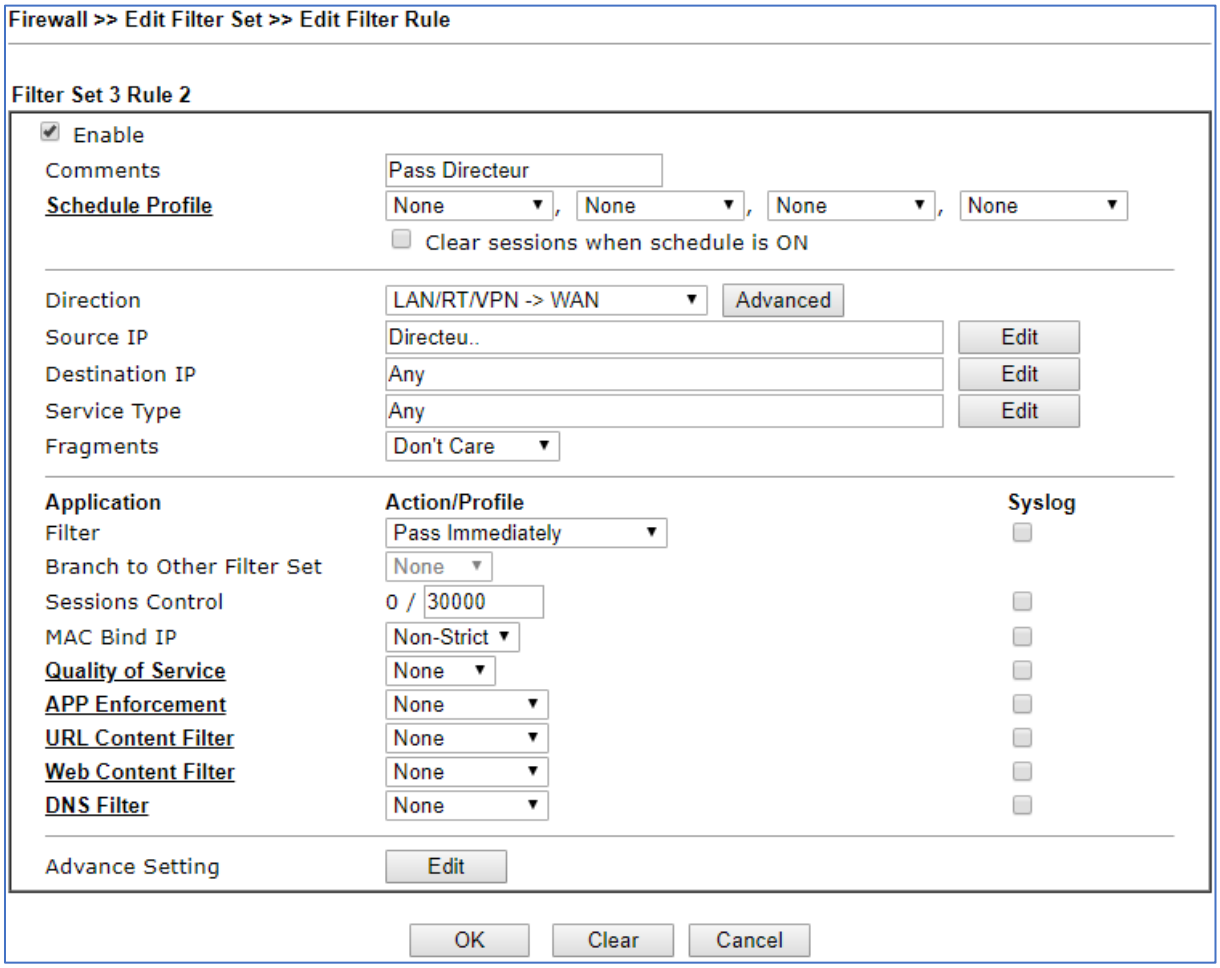
Geef de firewall regel een naam en zet een vinkje bij Enable. Klik vervolgens op Rule 1.



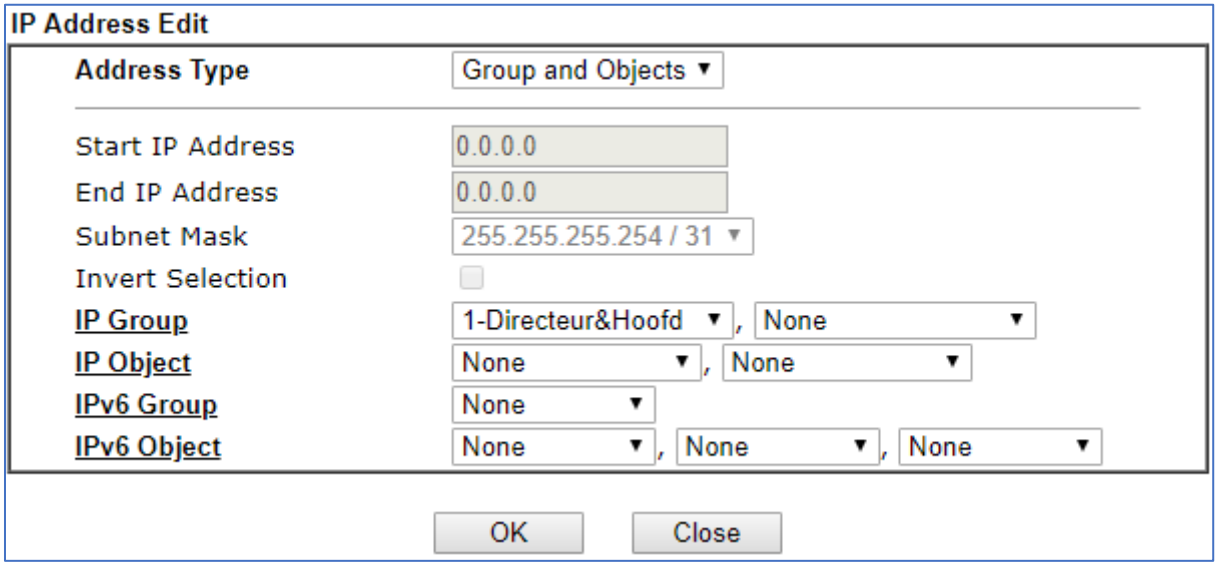
We creëren een Block if No Further Match regel, hierin blokkeren we al het verkeer van binnen (LAN) naar buiten (WAN). Wanneer u dan op OK klikt zult u merken dat u geen toegang meer hebt tot het internet (WAN).



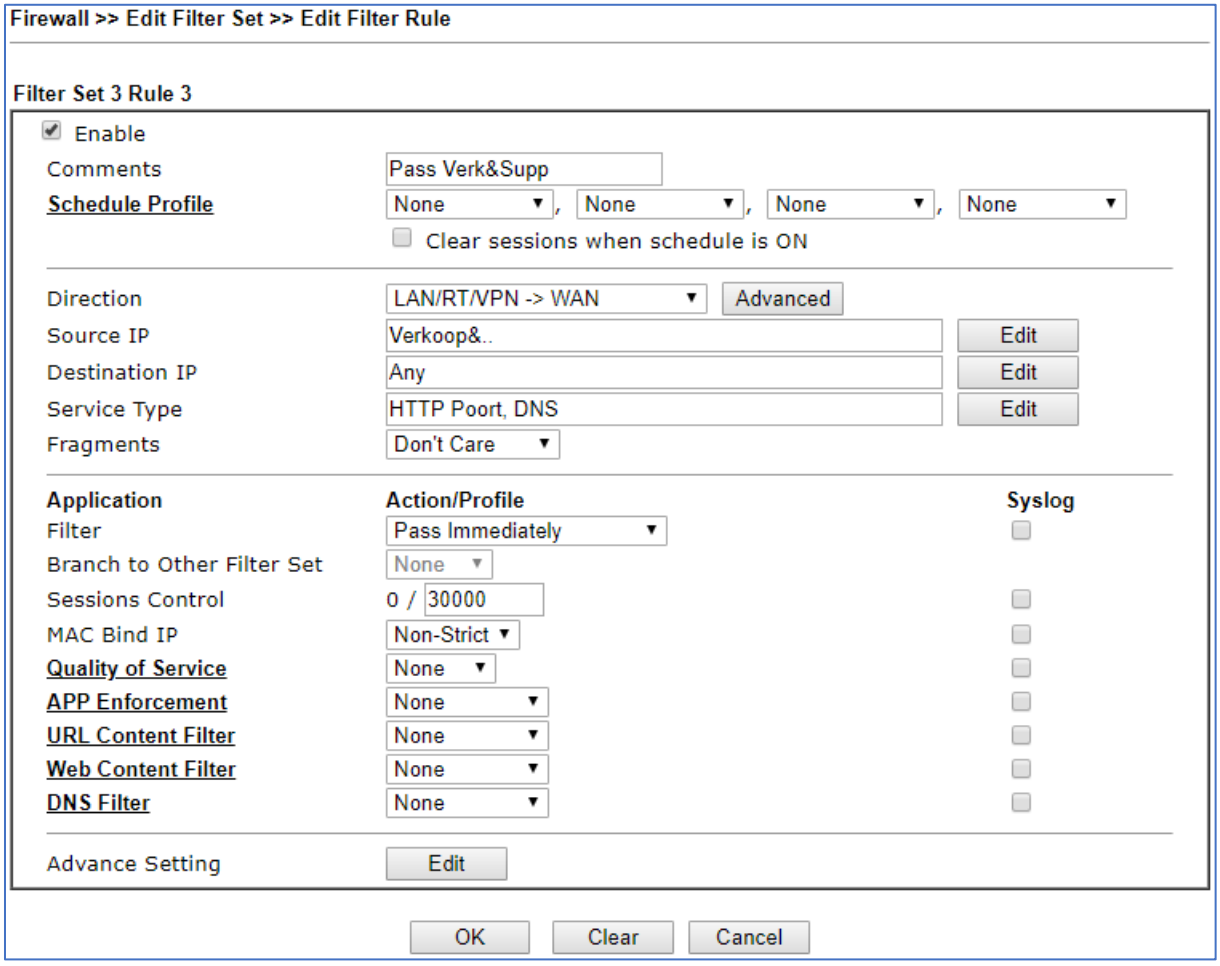
U maakt voor de directeur en zijn afdelingshoofden een nieuwe regel aan, waarin wordt vermeld dat ze een Pass Immediately krijgen op al het LAN => WAN verkeer.



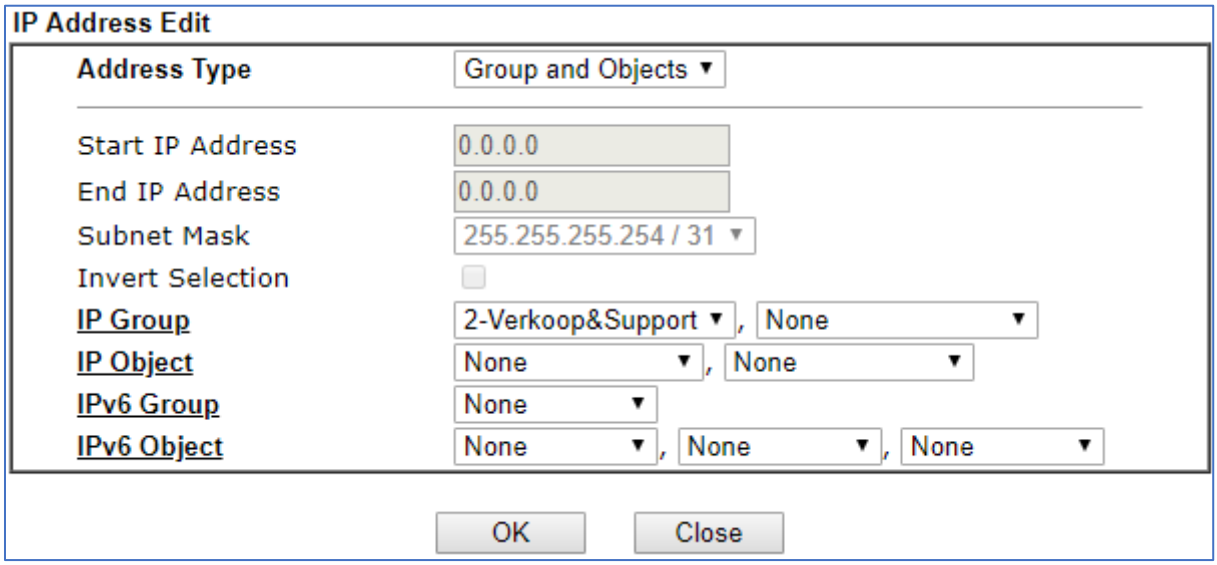
U maakt een nieuwe regel aan die u eerst activeert, vervolgens geeft u de juiste beschrijving op en verandert u de Direction in LAN/RT/VPN => WAN. Deze regel heeft betrekking op de directeur en zijn afdelingshoofden, zij hebben geen restricties op het LAN => WAN verkeer, dus wordt er hier gewerkt met een 'Pass Immediately'. Vervolgens klikt u bij Source IP op 'Edit', hier heeft u de mogelijkheid om bij Address Type voor 'Group and Objects' te kiezen.



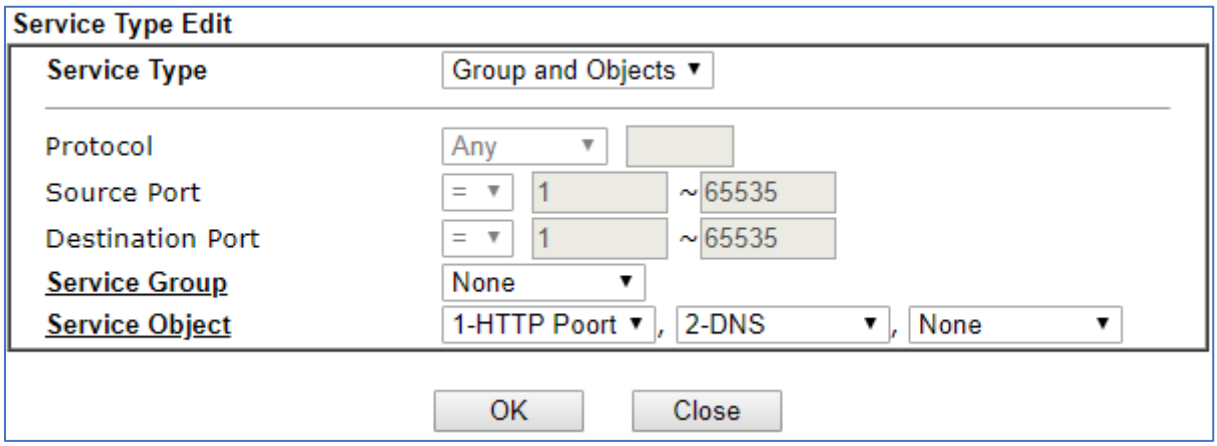
Nu hoeft u alleen nog maar een regel aan te maken voor de Verkoop & Support afdeling. Deze 2 afdelingen hebben alleen toegang tot poort 80. U geeft bij Source IP de IP Group op waarin u deze 2 afdelingen heeft geplaatst.



Bij Source IP geeft u de IP Group Verkoop & Support op.



Vervolgens selecteert u bij Service Object de aangemaakte Service Type Objects. Aangezien de twee afdelingen alleen toegang tot HTTP en DNS mogen hebben.



Voorbehoud
We behouden ons het recht voor om deze en andere documentatie te wijzigen zonder de verplichting gebruikers hiervan op de hoogte te stellen. Afbeeldingen en screenshots kunnen afwijken.