Advanced routing beállítása - Policy-based routing

2022. július 28.

Egy vállalat működésében az adatforgalom tervezett és tudatos irányítása, az adatok rendeltetési helyének, csoportosításának meghatározása a cég hálózati biztonságának növelését és a terheléselosztását teszi lehetővé.

Az alábbi esettanulmányban azt szeretnénk bemutatni, hogy az advanced routing használatával, hogyan tudjuk a különféle adatforgalmakat igényeinknek megfelelően, eltérő útvonalakra irányítani. Ezzel lehetőségünk nyílik az erőforrások optimálisabb kihasználásra.

Tartalom

1. A probléma bemutatása

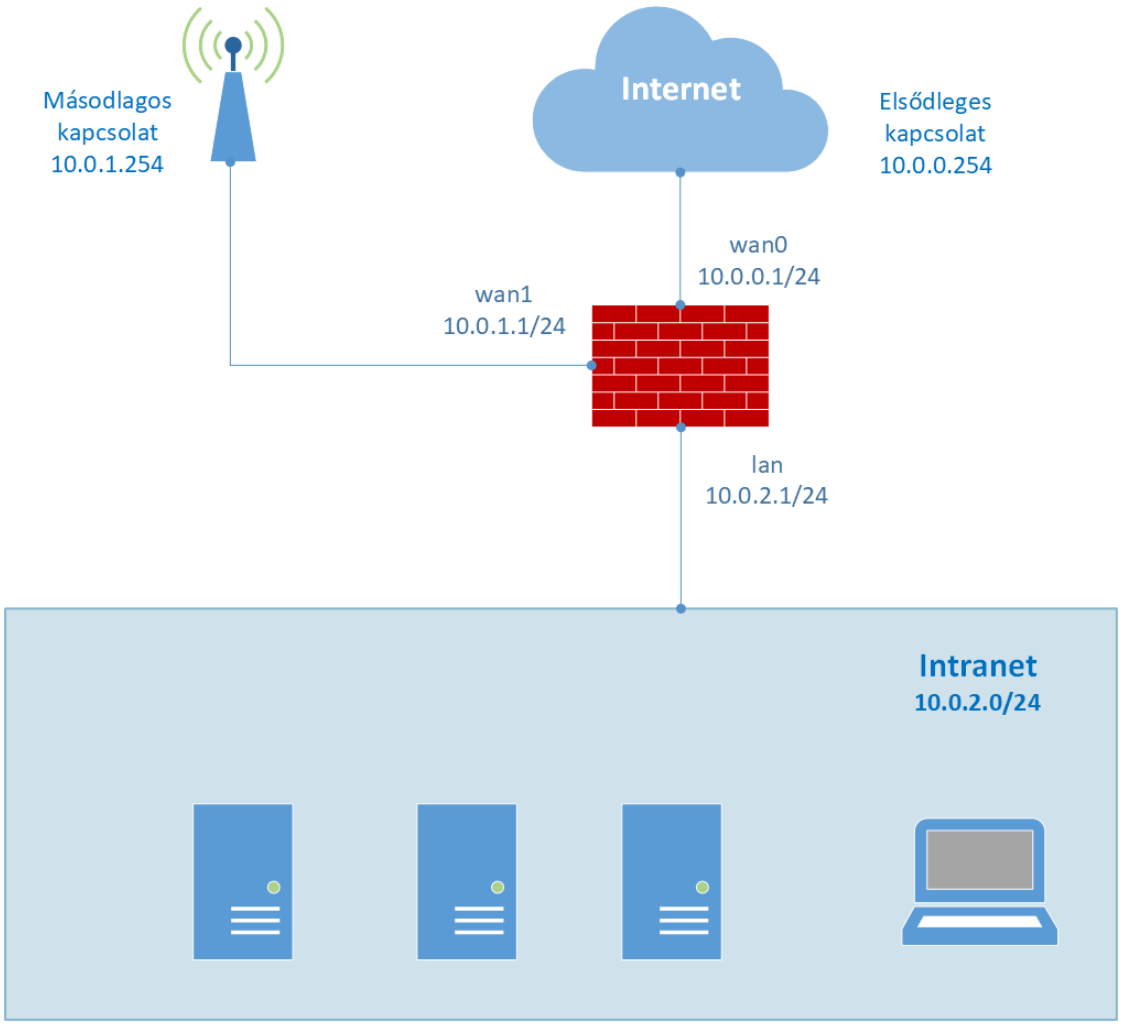
Hagyományos statikus routing alkalmazásával a csomagok cél IP címe alapján történik az útválasztás. Ebből adódóan, nincs lehetőség a különböző adatforgalmak elkülönítésére, különböző útvonalakon, hálózati kapcsolaton történő továbbítására. Erre kínál megoldást az advanced routing használata, mely során a kapcsolat számos paramétere alapján tudunk routing döntést hozni és az adatforgalmakat különböző hálózati interfészeken továbbítani.

2. A megoldás bemutatása

A belső hálózatból érkező forgalom alapesetben a *wan0* interfészen keresztül jut el az Internetre. A tűzfalon ehhez az interfészhez van beállítva az alapértelmezett átjáró, így minden forgalom, amelyre nincs külön definiált routing szabály, ezen az interfészen keresztül kerül továbbításra.

Példánkban a tűzfalon áthaladó HTTP és DNS forgalmakat egy másodlagos átjáró felé fogjuk továbbítani. A tűzfal működési módjainak megfelelően két különböző technikai megoldást szeretnénk bemutatni erre:

- *Packet filtering* (OSI layer 4): A csomagszintű vizsgálatot a tűzfal PFService szolgáltatása végzi. Itt csak a csomagok layer 3 és layer 4 szintű fejléc ellenőrzésére van lehetőség.
- *Alkalmazás proxy* (OSI layer 7): A kliens és a szerver között nincs közvetlen kapcsolat. A tűzfal külön-külön kapcsolatot tart fenn a kliens- és a szerveroldalon. Az adatforgalom ellenőrzése, alkalmazás protokoll szinten történik.



1. ábra - Hálózati topológia

3. Technikai megvalósítás

3.1. Routing tábla beállítása

A tűzfal parancssorából, az alábbi parancs segítségével vegyen fel egy új routing táblát:

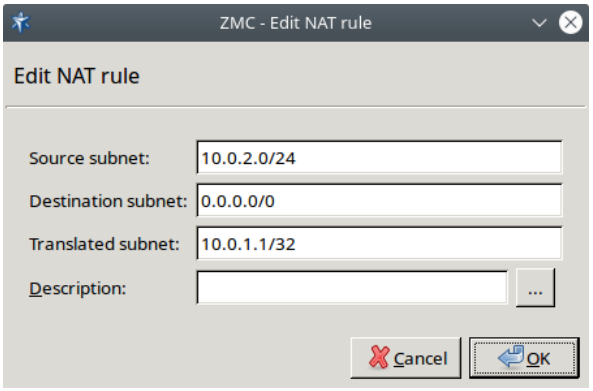
```
$ echo "200 wan1table" >> /etc/iproute2/rt_tables
$ cat /etc/iproute2/rt_tables
#
# reserved values
#
255     local
254     main
253     default
0       unspec
#
# local
#
#1      inr.ruhep
200     wan1table
```

3.2. Az alkalmazás proxy beállítása

Amennyiben a beérkező forgalom esetén alkalmazás proxy indul a protokoll elemzésére, a tűzfal az alapértelmezett átjárót tartalmazó interfészen nyitná meg a szerveroldali kapcsolatot. Ez úgy változtatható meg, hogy a service-hez létrehozunk és hozzárendelünk egy SNAT policy-t a másodlagos interfész címével. Ezután advanced routing segítségével az új NAT-olt forráscím alapján a fent létrehozott wan1table nevű routing táblába irányítjuk a forgalmat. A táblába felveszünk egy új szabályt a másodlagos kapcsolat alapértelmezett átjárójára. A service-hez tartozó forgalom ezután a másodlagos útvonalra lesz irányítva.

3.2.1. NAT policy létrehozása

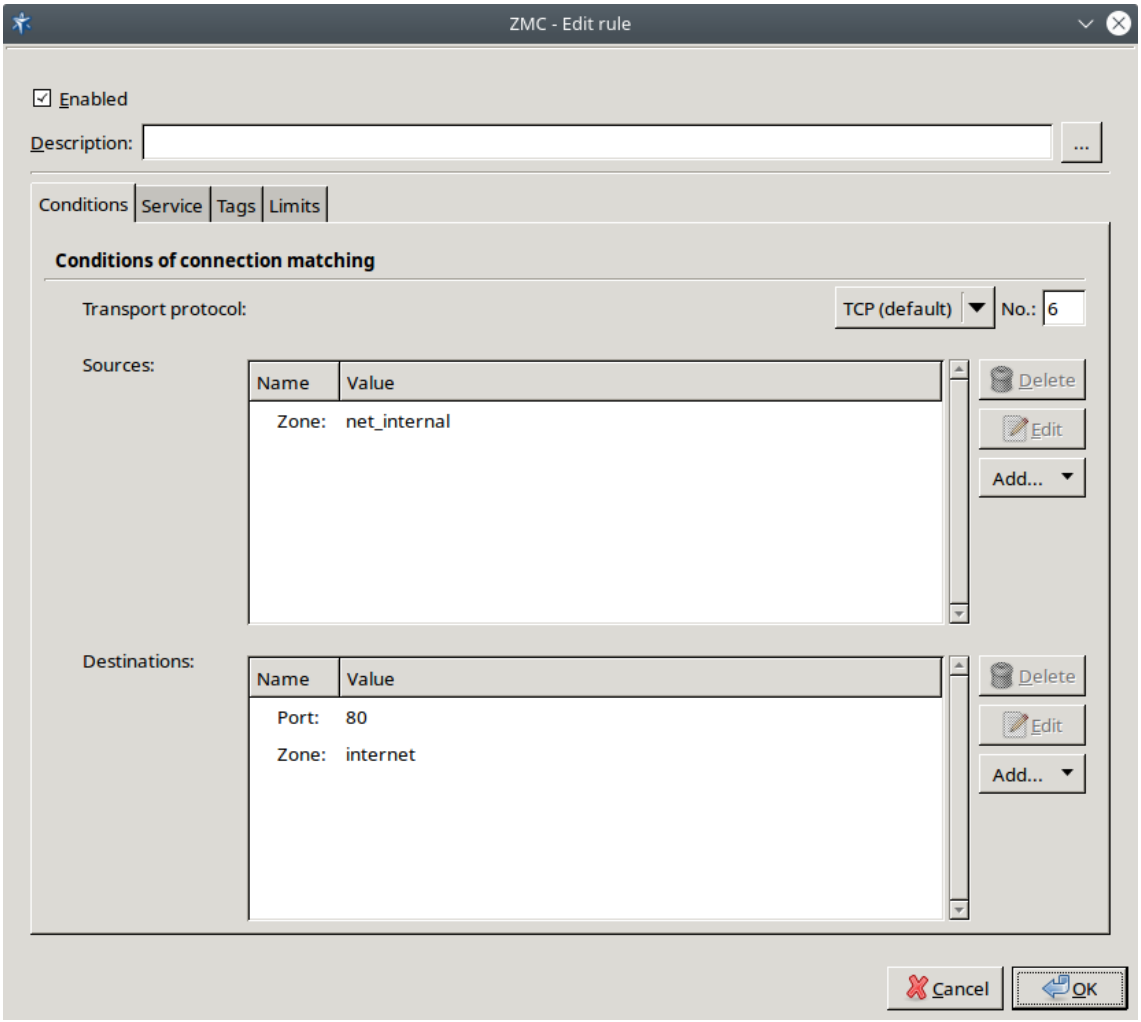
1. Válassza ki a Zorp Gateway komponenst, majd kattintson a **Policy** fülre.
2. Kattintson a **New** gombra, majd válassza ki a policy típusát (NAT Policy) és adjon meg egy nevet (MySNAT) a policy számára.
3. Válassza ki a **GeneralNAT** osztályt a **class** mezőben, majd a **New** gombra kattintva hozzon létre egy NAT szabályt.
4. Adja meg a belső LAN hálózat címét (10.0.2.0/24) a **Source subnet** mezőben, a célhálózat címét (0.0.0.0/0), a **Destination subnet** mezőben, és a *wan1* interfész IP címét (10.0.1.1/32), a **Translated subnet** mezőben.
5. Kattintson az **OK** gombra és mentse el a NAT szabályt.



2. ábra - NAT szabály létrehozása

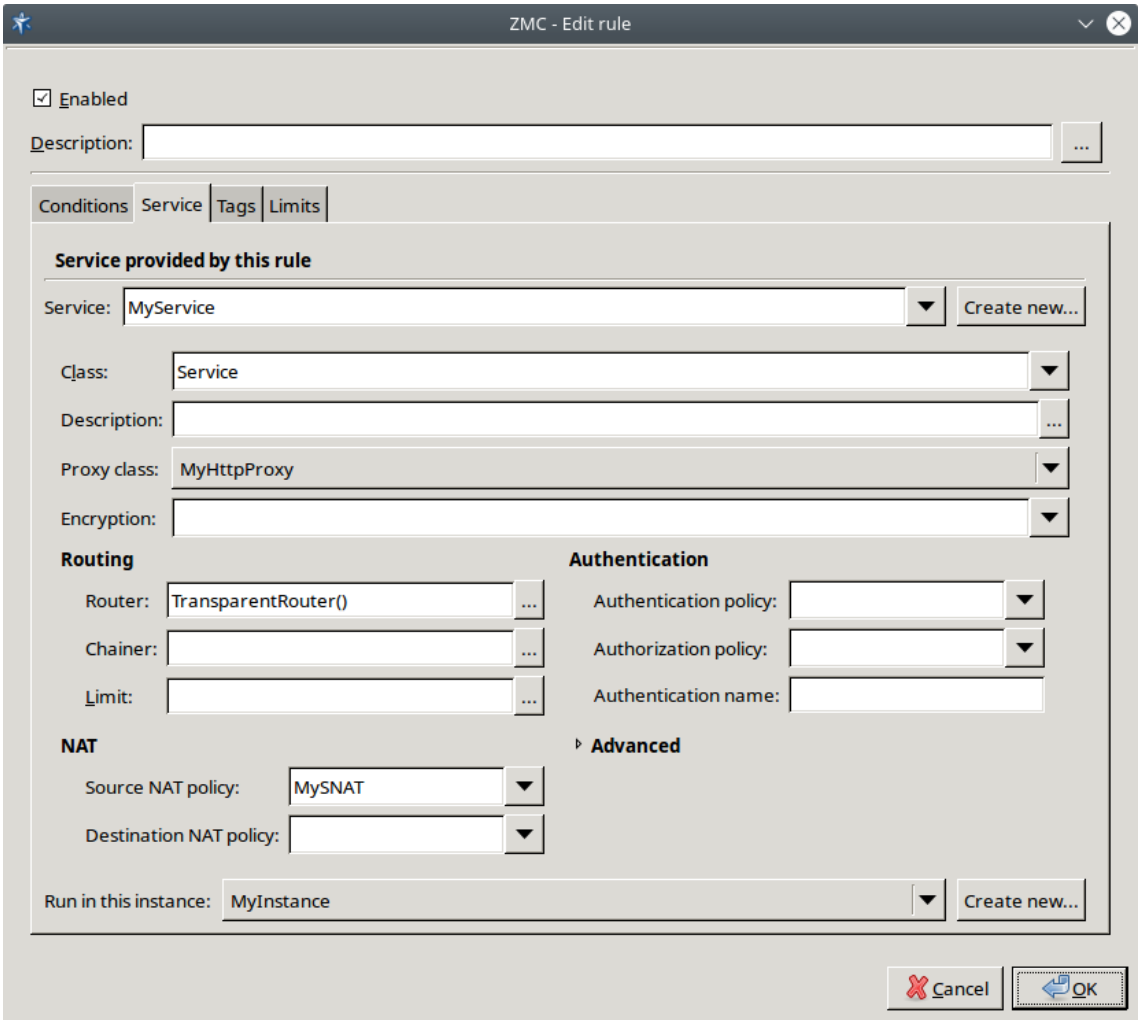
3.2.2. Tűzfalszabály létrehozása

1. Válassza ki a *Zorp Gateway* komponenst, majd kattintson a **Firewall rules** fülre. Kattintson a **New** gombra.



3. ábra - Tűzfalszabály létrehozása

2. Adja meg a kapcsolat protokollját, forrás- és célparamétereit az ablak **Condition** fülén. Ezen a fülön adhatóak meg a tűzfalszabály paraméterei. Ezen paraméterek alapján történik a kapcsolat illeszkedésének kiértékelése.
3. Kattintson a **Service** fülre, majd a **Create new...** gombra. Adjon meg egy nevet (MyService) az új service számára.
4. A **Class** mezőben válassza ki a **Service** típust.
5. A **Source NAT policy** mezőben válassz ki a korábban létrehozott NAT policyt (MySNAT).



4. ábra - Tűzfalszabályhoz tartó Service beállítása

3.2.3. Advanced routing beállítása

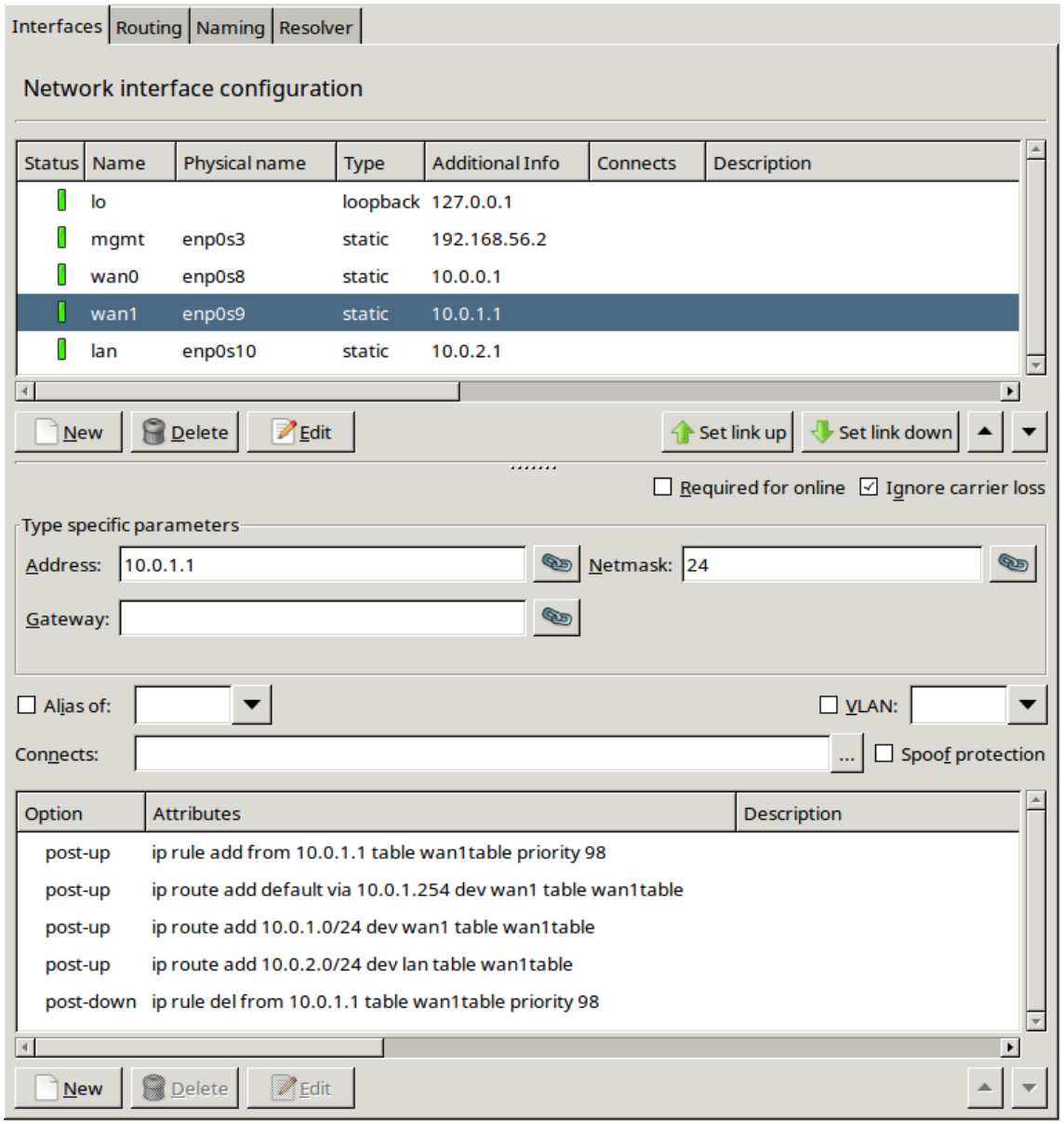
A *wan1* interfészhez létrehozott routing táblába még fel kell venni az alapértelmezett átjáróra vonatkozó szabályt, valamint a *connected route* szabályokat. Ezeket a Networking komponensen belül adhatja hozzá a *wan1* interfész post-up és post-down paramétereként. Jelölje ki *wan1* hálózati interfészt, majd az ablak alján lévő **New** gombra kattintva vegye fel az alábbi route szabályokat:

Post-up paraméterek:

```
ip rule add from 10.0.1.1 table wan1table priority 98
ip route add default via 10.0.1.254 dev wan1 table wan1table
ip route add 10.0.2.0/0 via dev lan table wan1table
```

Post-down paraméterek:

```
 ip rule del from 10.0.1.1 table wan1table priority 98
```



5. ábra - Routing szabályok beállítása

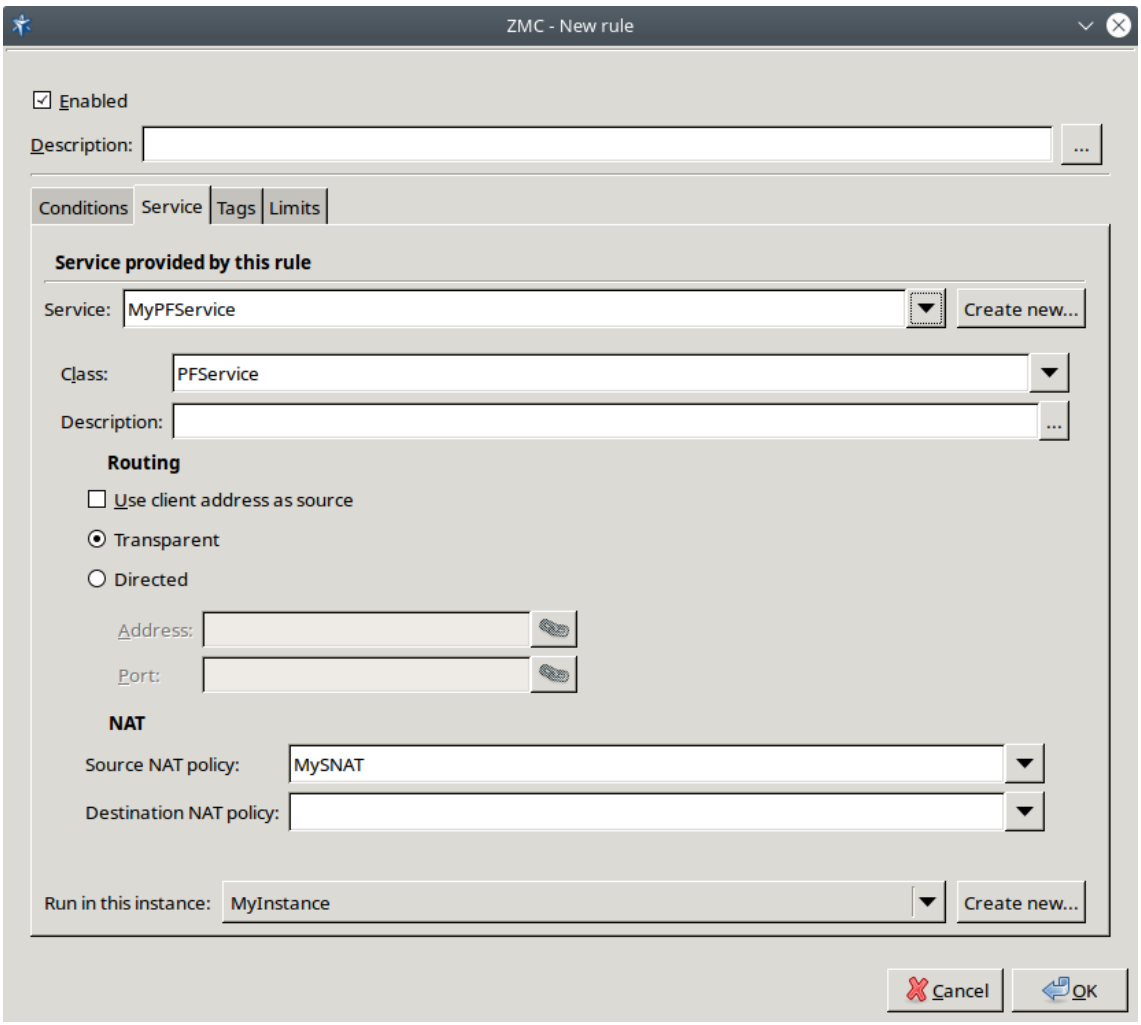
3.3. PFService alkalmazása

Packet Filter Service (PFService) használata esetén az advanced routing nem végezhető el a korábban ismertetett módon, a forgalom forráscíme alapján, mivel a routing döntés még a source NAT elvégzése előtt megszületik. Az advanced routing szabályokban viszont nem csak a csomagok forráscímére, hanem egyéb jellemzőikre is hivatkozhatunk. A következő példában a kapcsolathoz tartozó csomagokat megjelöljük az *iptables MARK* extension segítségével, majd a kapcsolat csomagjain lévő *mark* alapján történik meg a routing döntés.

3.3.1. Tűzfalszabály létrehozása PFService esetén

Hozzon létre tűzfal szabályt, ami illeszkedik a szabályozni kívánt forgalomra.

1. Válassza ki a Zorp Gateway komponenst, majd kattintson a **Firewall rules** fülre. Kattintson a **New** gombra.
2. Adja meg a tűzfalszabály paramétereit, amely alapján a kapcsolat illeszkedésének kiértékelése történik, az új ablakban a **Condition** fülön. Adja meg a kapcsolat protokollját, forrás- és célparamétereit.
3. Kattintson a **Service** fülre, majd a **Create new…** gombra. Adjon meg egy nevet (MyPFService) az új **PFService** számára.
4. Válassza ki a **PFService** típust a **Class** mezőben.
5. Válassza ki a **Source NAT policy** mezőben a korábban létrehozott NAT policy-t (MySNAT), majd állítson be egy Zorp instance-t.



6. ábra - PFService létrehozása

3.3.2. Packet Filter szabályok beállítása

3.3.2.1. NAT packet mark szabály

Az alábbiak a kapcsolat első csomagjának megjelölésére szolgálnak.

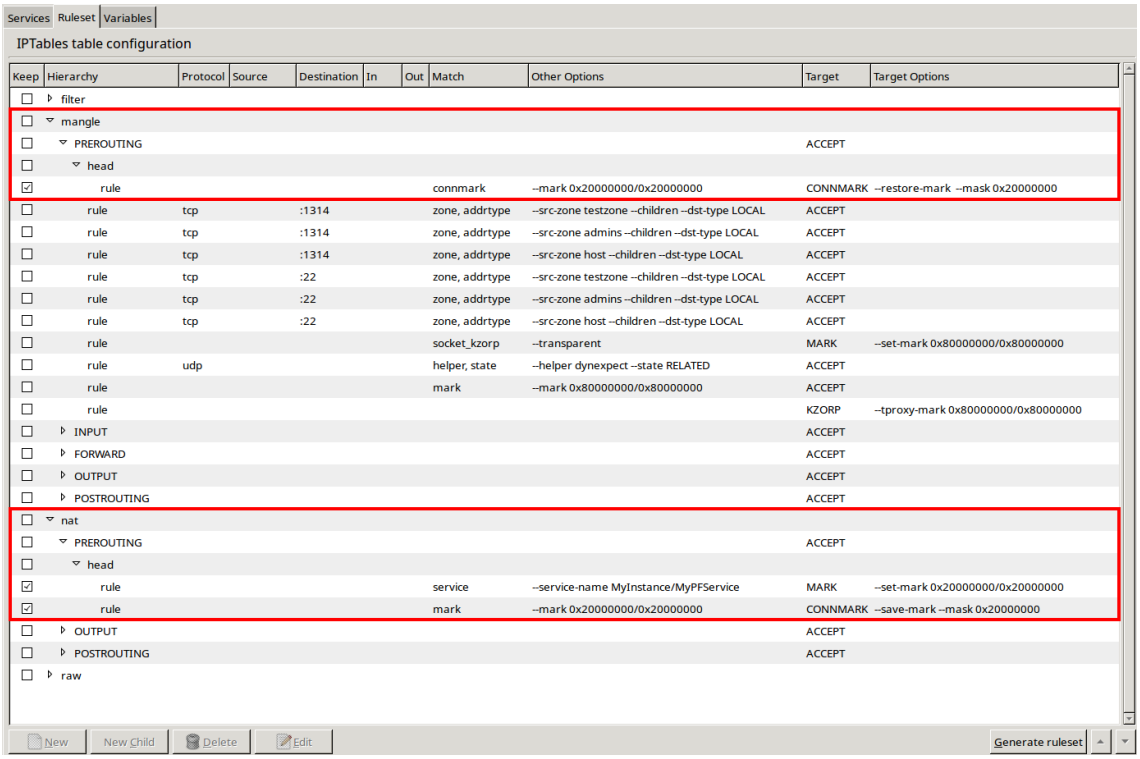
1. Válassza ki a **Packet Filter** komponenst a **ZMC** komponens fa ablakban, majd kattintson a **Ruleset** fülre.
2. Nyissa meg a **NAT** táblát a táblázat **Hierarchy** oszlopában, majd válassza ki a *PREROUTING* lánc **head** csoportját.
3. Kattintson a **New Child** gombra, majd válassza ki a **MARK** targetet. A **New** gombra kattintva adja hozzá a paraméterlistához a **MARK** paramétert és állítsa be hozzá a *0x20000000/0x20000000* értéket.
4. Keresse ki a **service** modul **service name** paraméterét az **Advanced options** fülön és dupla kattintással helyezze át a jobb oldali paraméter listára.
5. Adja meg a korábban létrehozott service nevét az instance nevével együtt (MyInstance/MyPFService) az ablak jobb alsó részén. A **Set** gombra kattintva állítsa be az megadott értéket.

3.3.2.2. NAT connection mark szabály

1. Kattintson a **New Child** gombra, majd válassza ki a **CONNMARK** targetet. A **New** gombra kattintva adja hozzá a paraméterlistához a *save-mark* paramétert és állítsa be hozzá a *–mask 0x20000000* értéket.
2. Keresse ki a **mark** modul *set-mark* paramétert az **Advanced options** fülön és dupla kattintással helyezze át a jobb oldali paraméterlistára.
3. Adja meg a *0x20000000/0x20000000* értéket az ablak alatt, majd a **Set** gombra kattintva állítsa be az megadott értéket.

3.3.2.3. Mangle connection restore mark szabály

1. Válassza ki a **Packet Filter** komponenst a *ZMC* komponens fa ablakban, majd kattintson a **Ruleset** fülre.
2. A táblázat **Hierarchy** oszlopában nyissa meg a **mangle** táblát, majd válassza ki a **PREROUTING** lánc **head** csoportját.
3. Kattintson a **New Child** gombra, majd válassza ki a **CONNMARK** targetet. A **New** gombra kattintva adja hozzá a paraméter listához a **restore-mark** paramétert, valamint állítsa be hozzá a *0x20000000/0x20000000* értéket.
4. Keresse ki a **service** modul *service name* paraméterét az **Advanced options** fülön és dupla kattintással helyezze át a jobb oldali paraméter listára.
5. Adja meg a korábban létrehozott **service** nevét az **instance** nevével együtt (MyInstance/MyPFService) az ablak alatt. A **Set** gombra kattintva állítsa be az megadott értéket.
6. Végül az **OK** gombbal mentse el a tűzfalszabályt.



7. ábra - Packet Filter - csomagok megjelölése

Figyelem
A *Zorp Gateway* tűzfal belső működése során a *0x40000000* és *0x80000000* markot használja. Ezeket az értékeket semmilyen körülmények között ne írja felül. Mindig használja a maszk paramétert a beállíás során!

3.3.3. Routing szabályok hozzáadása

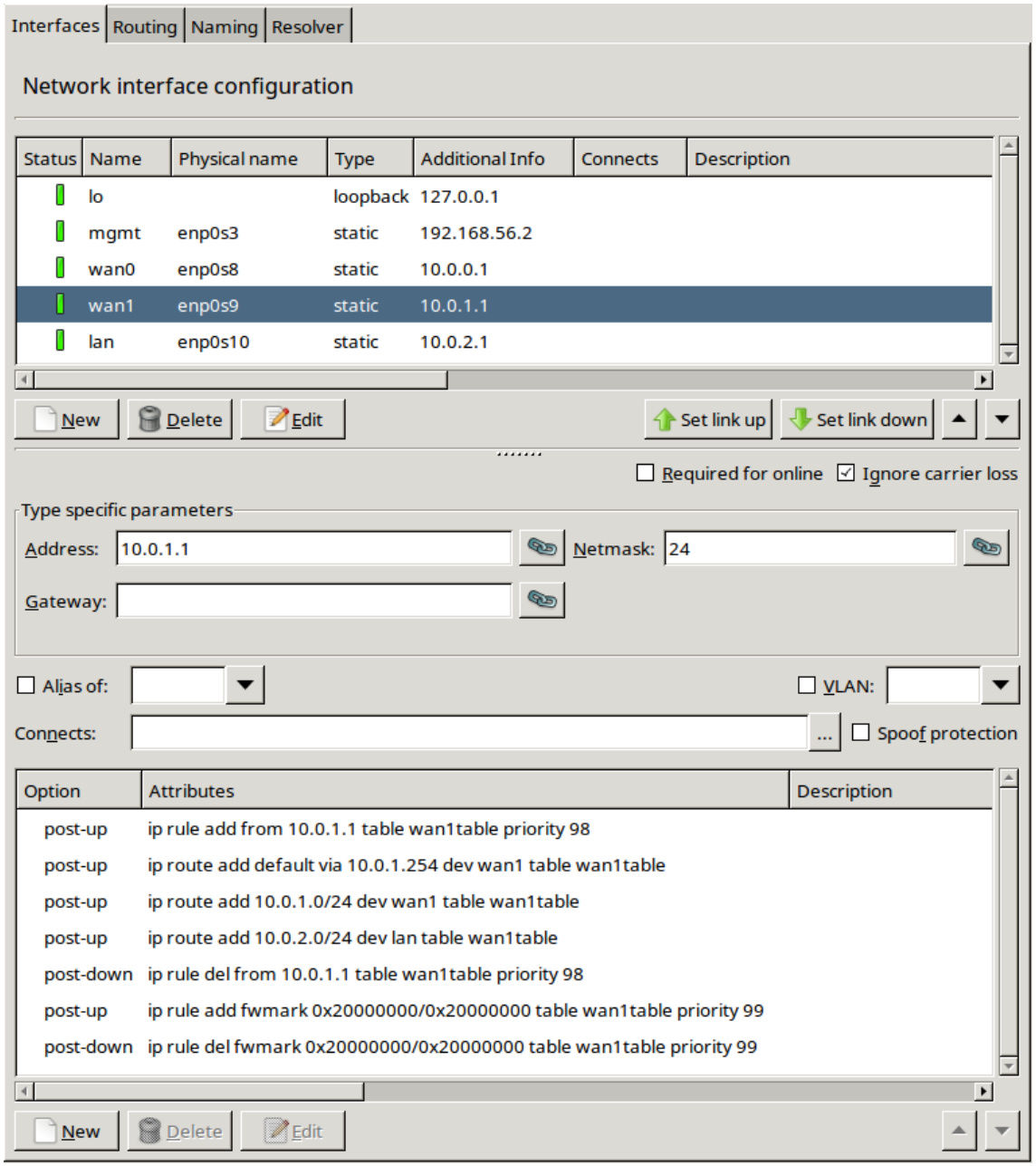
A fenti példához hasonlóan vegye fel az „ip rule” szabályt a *wan1* interfészhez a **Networking** komponensen belül, hogy az tartósan megmaradjon.

Post-up paraméterek:

```
ip rule add fwmark 0x20000000/0x20000000 table wan1table priority 99
ip route add default via 10.0.1.254 dev wan1 table wan1table
ip route add 10.0.2.0/0 via dev lan table wan1table
```

Post-down paraméterek

```
 ip rule del fwmark 0x20000000/0x20000000 table wan1table priority 99
```



8. ábra - Routing szabályok beállítása

4. Konklúzió

A fenti leírás alapján a hálózati forgalom az igényeknek megfelelően irányítható a különböző hálózati útvonalak között, figyelembe véve a hálózati linkek, illetve protokollok sajátosságait. Például, az interaktív, alacsony késleltetést igénylő protokollok számára ezáltal biztosítható a megfelelő útvonal, míg a hibatűrőbb protokollok számára egyéb útvonal jelölhető ki.