

# Több internet kapcsolat forgalom elosztással és hibatűréssel

Ezen dokumentum célja egy olyan LAN hálózat bemutatása, melyen több gateway is jelen van, ezáltal redundáns internet elérést használhatunk. Így ha az egyik internet elérés leáll, a másikon keresztül használhatjuk az internetet. Célunk eléréséhez a Zeroshell „Net Balancer” modulját használjuk. Végezetül megnézzük az aggregációs lehetőségeket (Bonding) VPN-en keresztül, mellyel reményeink szerint növelni tudjuk a távoli helyek közötti sávszélességet.

A leírást a következő részekre bontottuk:

- [Valóban lehetséges növelni az internetes kapcsolat sebességét?](#)
- [Több útválasztó beállítása](#)
- [Hibatűrés \(kezelés\) a kapcsolatok között Failover Monitor segítségével](#)
- [Forgalom elosztás manuálisan](#)
- [VPN csoportosítás és sávszélesség növelése 2-es „szinten”](#)

Gateway Description	IP Address	Interface	Weight	Status	Faults	UP
DEFAULT GATEWAY			1	Disabled	0	<input type="checkbox"/>
Infostrada ADSL	192.168.1.254		7	Active	0	<input checked="" type="checkbox"/>
TIM Mobile		ppp0	1	Disabled	1	<input type="checkbox"/>
WIND Mobile		ppp1	1	Active	1	<input checked="" type="checkbox"/>
TRE Mobile		ppp2	1	Active	1	<input checked="" type="checkbox"/>

Terhelés elosztás és átterhelés egy ADSL és 3 UMTS/HSDPA kapcsolat között.

## Valóban lehetséges növelni az internetes kapcsolat sebességét?

A válasz nem egyértelműen „igen”! A kérdés az, hogy mit értünk nagyobb sávszélesség alatt. Lényegében a Net Balancer a LAN-ból érkező kéréseket elosztja round-roubin (súlyozott) szabályok alapján az átjárók között. Más szóval, ha egyszerre csak egy felhasználó használja az internetet, egyetlen TCP kapcsolattal (pl egyetlen letöltést futtat a netről), egyetlen útválasztót használ, így neki nem származik lényegi haszna az elosztásból. Viszont, ha több felhasználónk használja a LAN-t, több párhuzamos kéréssel egy időben, az összes sávszélesség nagyobb lehet, mint egyetlen internet kapcsolatunk sebessége. Végül is megállapíthatjuk, hogy egy kapcsolat sosem lesz gyorsabb, mint egyetlen WAN kapcsolatunk, de ha sok kapcsolat megy a hálózaton, az összes sebesség nagyobb lesz. A kapcsolatok elosztódnak az útválasztók között.

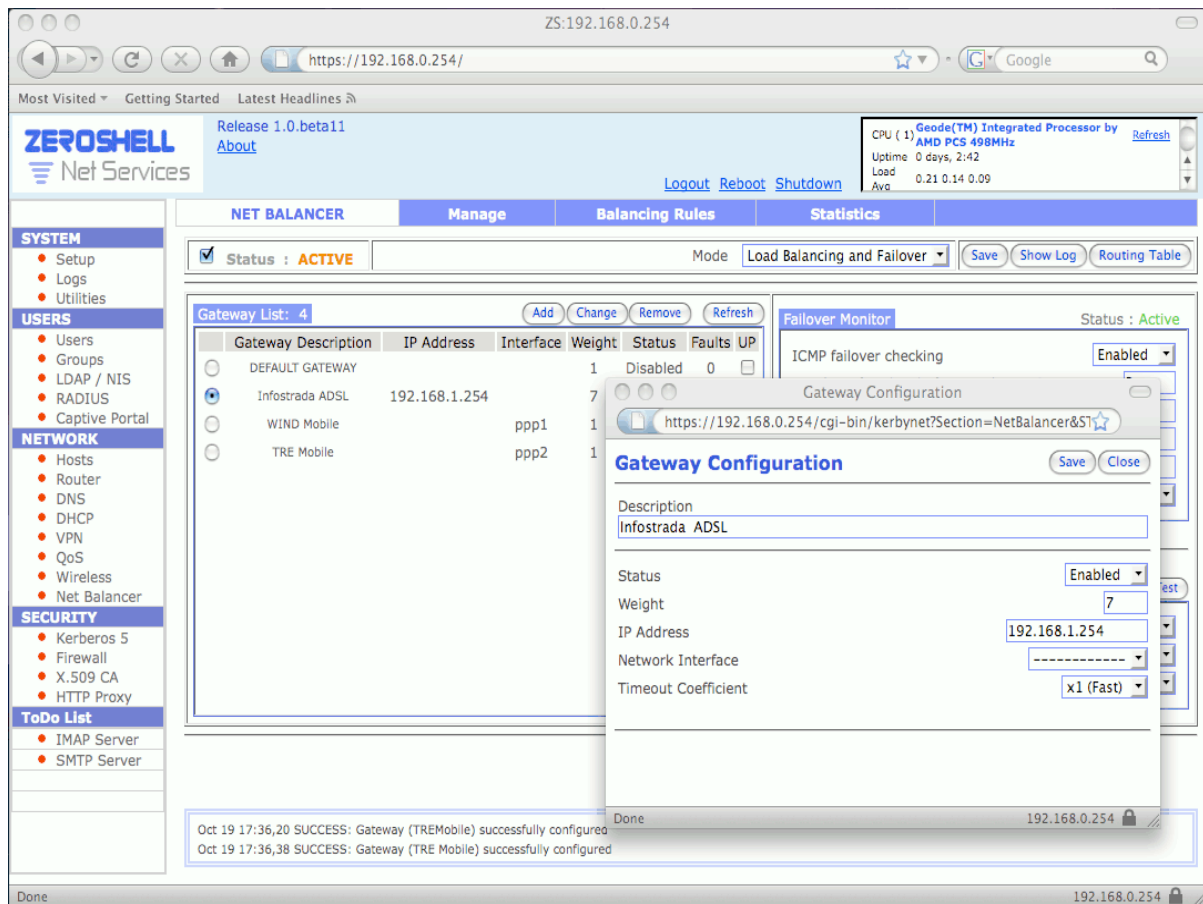
Másfelől a VPN aggregáció egy más történet. Ebben az esetben, az elosztott forgalom a „Layer 2” szinten történik, így némi sávszélesség növekedés elérhető egyszeres TCP/IP kapcsolathoz képest.

# Több útválasztó beállítása

Amire szükségünk lehet:

- Pl egy ADSL router. Ebben az esetben az IP címre hivatkozunk
- Egy modem, ami Point-to-Point kapcsolatot (ppp) hoz létre. Pl ADSL PPPoE vagy egy UMTS/HSDPA modem. Ebben az esetben nincs konkrét IP címünk, csak egy PPP interfészünk

Mielőtt beállítanánk az útválasztókat a Net Balancer –be, bizonyosodjunk meg róla, hogy fizikálisan és logikálisan csatlakoztatva vannak a Zeroshellhez. Ellenőrizzük, hogy ugyanazon az alhálózaton vagyunk-e. Másik lehetőség, ha a gateway egy modem, fizikálisan is csatlakoztassuk a Zeroshellhez PPPoE vagy USB segítségével 3G modem esetén. Ezeket előzőleg a [Setup][Network][New PPPoE] vagy [Setup][Network][New 3G Modem] útvonalon adhatjuk hozzá. Az eszközök automatikusan kapnak egy azonosítót, később ezekre hivatkozhatunk a Net Balancer felületén.



Útválasztók konfigurálása a Net Balancer modulban

Az [Add] gombra kattintva adhatunk hozzá új gatewayt vagy a [Change] gombra kattintva módosíthatunk egy korábban hozzáadottat. Az alábbi paraméterekkel találkozhatunk:

- **Description:** Szöveges leírás az útválasztóról. Pl megadhatjuk a szolgáltató nevét.
- **Status:** Ha „Enabled” akkor használhatjuk, egyébként nem. Ha pl egy kapcsolat túl sűrűn megszakad, de véstartaléknak meghagynánk, itt letilthatjuk.
- **Weight Value:** egy szám, fontosság megadása. Minél nagyobb számot adunk meg, az adott kapcsolaton annál több forgalom zajlik.
  - Ha a Net Balancert „Load Balancing and Failover” módban használjuk, a kimenő kapcsolatok a súlyozás szerint történnek. Nagyobb érték fontosabb kapcsolatot deklará. Ha egyforma kapcsolataink vannak, akkor mindenhova írjunk 1-et, és ugyanolyan arányban lesznek használva a kapcsolatok.

- A másik lehetőség, ha a Net Balancert „Failover” módban használjuk, egyszerre egy kapcsolat aktív. Alapértelmezésben azt használjuk, ez a legnagyobb súlyú. Ha meghibásodik, akkor a súlyozás szerinti sorrendben következő kapcsolatra terhelődik át a forgalom. A többi kapcsolat addig „Spare”, tehát tartalék üzemmódban vár az aktiválódásra.
- **IP Address:** IP cím, amennyiben az átjáró egy másik hálózati eszköz, pl router
- **Network Interface:** Point-to-Point interfész neve PPPoE (DSL vagy kábel) vagy egy 3G modem (UMTS vagy HSDPA).
- **Timeout Coefficient:** Átterhelés idejét állíthatjuk be. Egy nem terhelt, „jobb” kapcsolat esetén érdemes kisebb értéket megadni. Egy lassabb, terheltebb (pl GPRS) kapcsolat esetén, ahol nagyobbak a pingek, érdemes megnövelni ezt az értéket.

Ha végeztünk a beállításokkal, akkor aktiválni kell a Net Balancert. Ezzel egyből elindul a terhelés elosztásos hálózatunk.

## Hibatűrés (kezelés) a kapcsolatok között Failover Monitor segítségével

A Net Balancert a következő kétféle üzemmódban lehet használni, a helyes választás általában függ az adott internet kapcsolat paramétereitől.

- **Terhelés elosztás és átterhelés:** az internetes kapcsolat elosztása az útválasztók között automatikusan történik a megadott súlyozás (Weight) alapján. Ha az egyik útválasztó elérhetetlenné válik, a rendszer nem továbbít kéréseket felé. Az automatikus elosztást kézzel felül lehet bírálni a megadott kritériumok alapján (forrás IP, cél IP, TCP/UDP portok, stb)
- **Failover:** egyszerre csak egy (a legnagyobb súlyú, működő) útválasztón keresztül történik a forgalom. A többi tartalék üzemmódban működik, ha az aktív kapcsolat hibát jelez, automatikusan elindul a sorrendben következő legnagyobb súlyú kapcsolat. Ebben az esetben nincs automatikus terhelés elosztás, a forgalmat kézzel lehet szabályozni, ahogyan azt a későbbiekben be is mutatjuk.

Így tudjuk a hibatűrést garantálni, függetlenül a Net Balancer modul beállításaitól. Egy nem működő kapcsolat „Fault” jelzöt kap, két mechanizmus kezd el működni: az első ellenőrzi a fizikai kapcsolatot az útválasztóval (modem vagy router). A második mechanizmus (Failover Monitor) végrehajt egy alaposabb vizsgálatot, hogy felderítse a probléma okát. Mióta az első mechanizmus -ami irányítja a fizikai kapcsolatot a Net Balancerrel és automatikusan, konfigurálás nélkül aktiválódik- létezik, úgy gondoljuk, hogy nem lehet ehhez többet hozzáfűzni. Helyette inkább koncentrálnánk a „Failover Monitorra”, aminek egyértelműen aktívnak és konfigurálnak kell lennie. A hibatűrés menedzsment megbízhatósága nagyban függ ettől a komponenstől, mivel az adatsorozatok torlódásának a szintje által nagyon befolyásolt és következetesen függ a válaszidőktől. Ha a Failover Monitor hibásan van beállítva, hibát jelezhet akkor is, amikor a hálózat „csak” túlterhelt. Emiatt gyorsan megváltoztatharja egy kapcsolat állapotát aktívról hibásra és vissza, és ez a kapcsolat leállításával jár(hat). Ha megfelelően beállítottál mindent, és mégis hibákat tapasztalsz, néha jobb letiltani a Failover Monitort. Határozottan jobb egy nem létező felügyelet, mint egy hibásan, instabil rendszert eredményező. Most pedig nézzük a konfigurációs lehetőségeket:

- **ICMP failover checking:** ha az értéke *Enabled*, a Failover Monitor aktiválva van. Ahhoz, hogy az ellenőrzés valóban működjön, legalább egy ellenőrizendő IP címet meg kell adni és engedélyezni. Ezeknek „külső” IP címeknek kell lenniük, amit minden útválasztón keresztül el lehet érni.
- **Number of probes before marking DOWN:** megadható, hogy hány hibás ping után jelölje hibásnak a kapcsolatot.
- **Number of probes before marking UP:** megadható, hogy hány ping után jelölje ismét aktívnak a kapcsolatot.
- **Reply timeout (seconds):** megadható a maximum várakozási idő egy ICMP válaszra. Abban az esetben, ha a kapcsolat telítődik, ennek az értéknek a növelése segíthet. Tartsd észben, hogy az aktuális várakozási idő függhet a az előző bekezdés „Timeou Coefficient” részében tárgyaltaktól.
- **Pause before starting a new cycle (seconds):** megadható az ellenőrzések közötti várakozási idő

- **Immediately restart PPPoE and 3G Mobile:** ha ezt engedélyezed, Point-to-Point kapcsolat hibája esetén újracsatlakozás történik. Ez gyors megoldás lehet a problémára, ugyanakkor új IP címet eredményezhet, ha dinamikus címkiosztás van.

Valószínűleg többszöri próbálkozás szükséges, mire megtaláljuk az optimális beállításokat. Hiba esetén meg kell oldani a gyors beavatkozást, kizárni a hibás kapcsolatot, ugyanakkor nem szabad kizárni olyan kapcsolatot, ami egyszerűen „csak” túlterhelt.

## Forgalom elosztás manuálisan

Bizonyos esetekben elképzelhető, hogy nem szeretnénk automatikus terhelés elosztást. Más szóval a speciális kapcsolatoknak korlátozva kell lenniük egy bizonyos átjáró felé. Ehhez menjünk a [Net Balancer][Balancing Rules] oldalra, ahol a tűzfal és QoS osztályozóhoz hasonló felületet találunk. A kiválasztott szabályok alapján eldönthetjük, hogy a kapcsolatot mely útválasztó felé továbbítjuk.

The screenshot shows the 'Firewall Rule config' window. At the top, the browser address bar shows a URL: `https://192.168.0.254/cgi-bin/kerbynet?Section=FW&STk=d894551bcb6a71436a7282f97c66b3dadcaf3a4b&Action=AddRule&Chain=NetBal`. The main configuration area is titled 'NetBalancer' and includes a 'Sequence' field set to '1'. Below this is a table for 'Packet Matching' with columns for 'Description', 'Value', and 'Not'. The 'Value' column contains dropdown menus for 'Input', 'Output', 'Source IP (\*)' (set to '192.168.0.20'), 'Destination IP', 'Fragments' (with a checkbox for 'match only second and further fragments'), 'Packet Length', and 'Source MAC'. Below the table are sections for 'Protocol Matching' (set to 'TCP'), 'Connection State' (checkboxes for NEW, ESTABLISHED, RELATED, INVALID, UNTRACKED), 'Time Matching' (From, to, and day selection), 'Peer-to-Peer' (checkboxes for eMule, EDonkey, Kademia, KaZaA, FastTrack, Gnutella, BITTorrent, Direct Connect), 'Layer 7 Filter' (Protocol Description), 'Connection Limits' (Parallel connections per IP, Traffic per connection), and 'TARGET GATEWAY' (set to 'Optical Fiber Cable (192.168.1.250)'). At the bottom, there are 'NOTES' and a status bar showing 'Done' and the IP '192.168.0.254'.

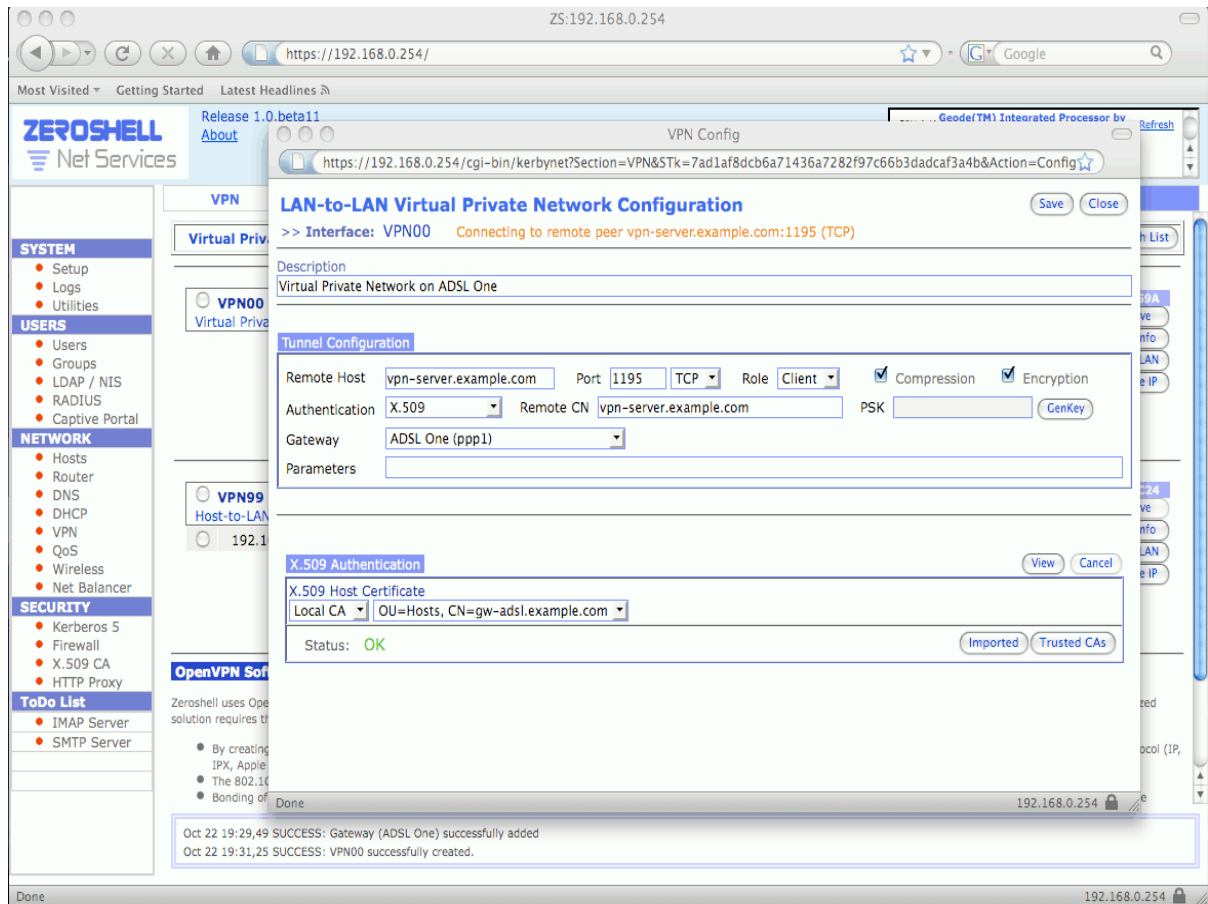
Szabály az SMTP forgalom kézi irányításához.

A fenti példában 192.168.0.20 –as IP-ről érkező SMTP forgalmat (25-ös TCP port) mindig a 192.168.1.250 –es útválasztón keresztül továbbítjuk, ami egy optikai kapcsolat.

## VPN csoportosítás és sávszélesség növelése 2-es „szinten”

A Zeroshellben beállíthatunk LAN-to-LAN VPN kapcsolatot, ami elérhető OpenVPN használatával, vagy TAP virtuális csatlón keresztül. Ez utóbbi teljesen úgy működik, mint egy valódi Ethernet eszköz, és mint olyan, így lehetőségünk van „összefűzni” több kapcsolatot (Bonding). Ez a lehetőség a Zeroshell első kiadása óta elérhető. Meglehető, a VPN bonding azt indokolja, hogy minden egyes VPN alagútnak ami a bondhoz tartozik külön internet kapcsolat szükséges. Mielőtt a Net Balancert bemutatták, ez a módszer működött olyan statikus utakon keresztül, amik legalább egy féltől megkövetelték, hogy legyen két nyilvános IP címe. A Net Balancernek köszönhetően viszont, a site-to-site VPN konfiguráció lehetőséget nyújt arra, hogy kiválasz egy

átjárót, amin keresztül történhet a titkosított kapcsolat. Ez nagyban megkönnyíti a konfigurációt azáltal, hogy már nem igényel statikus utakat és két nyilvános IP-címet.



Átjáró választása a VPN csatlakozáshoz.

VPN létrehozását és egy megadott átjáró hozzárendelését, és így egy bond interfész létrehozását az alábbi ábra szemlélteti:

Bond interfész létrehozása 2 VPN kapcsolat összefűzésével.

A létrejött BOND00 eszköz úgy működik, mint egy Ethernet kártya: lehet IP címe, hozzáadhatjuk VLAN –hoz, vagy hozzárendelhetjük egy bridge –hez. Ahogy az elején említettük, minden TCP/IP kapcsolat megnövekedett sebességet érhet el, köszönhetően a többszörös kapcsolatnak.