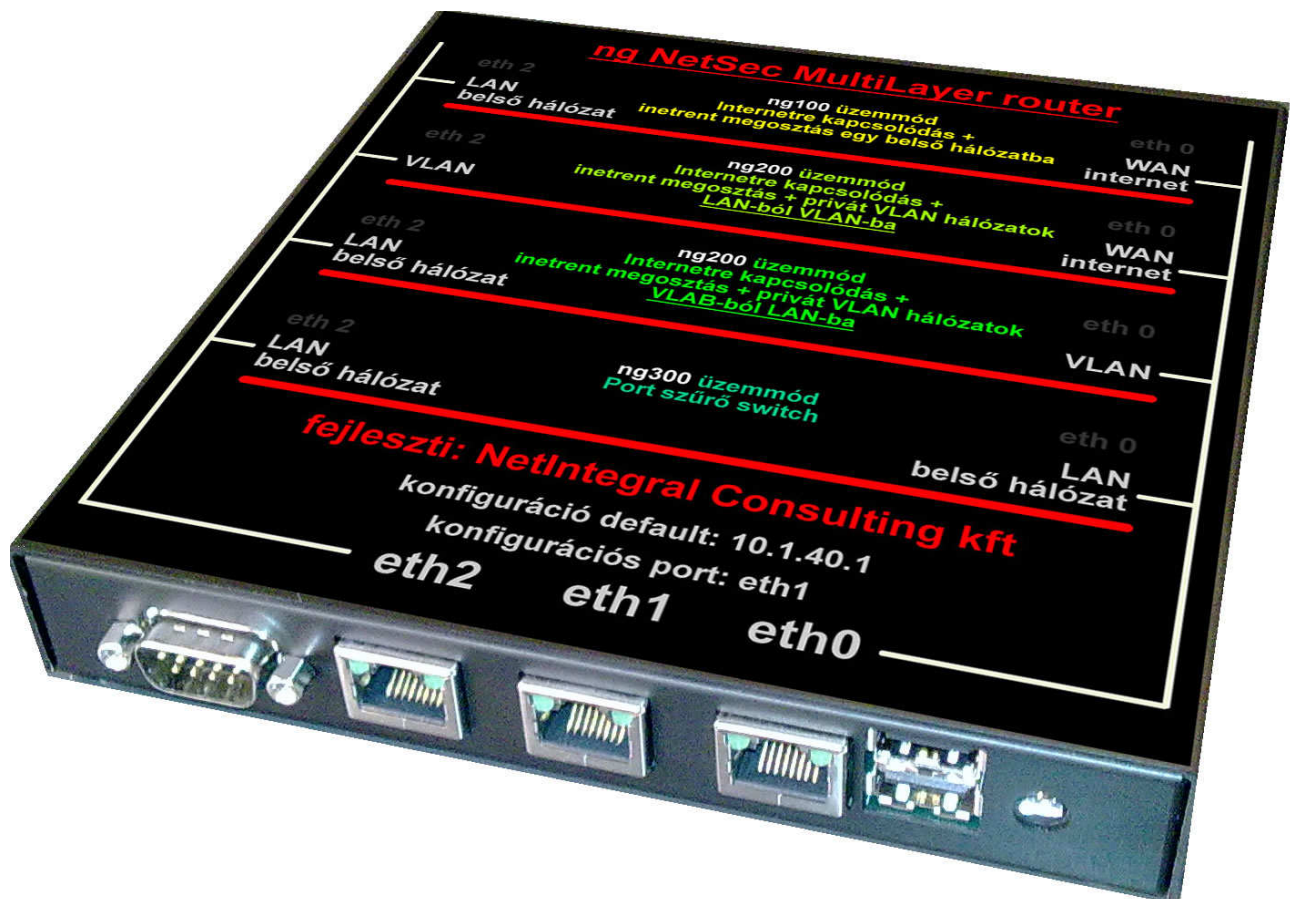


ngNetSec MultiLayer router

serial: ng100-300

Broadband Router 100 mbps vezetékcsatlakozási pontokkal.

Fejlesztő:
NetIntegral Consulting kft
www.netintegral.info

Tartalom:

Kezelési útmutató.....	1
Tartalom:.....	2
Tulajdonságok és lehetőségek.....	4
Csomag tartalma	4
ngNetSec MultiLayer router filozófia.....	4
Biztonságtechnikai megoldások az ngNetSec MultiLayer routerben	5
Kezdő lépések a használatbavételhez	9
Belépés	10
Reset.....	11
ng100 üzemmód: Internet megosztás egy belső hálózatba	11
Információk	11
<i>dsl kapcsolódás</i>	12
<i>lan / kábel tv</i>	13
<i>Belso hálózat</i>	15
<i>Port átirányítások</i>	17
<i>ng100 beállítás alapértelmezetté tétele/használat</i>	17
<i>Újraindítás</i>	17
ng300 üzemmód: Port szűrő switch	17
<i>switch paraméterezése</i>	17
<i>port szűrés</i>	19
<i>ng300 beállítás alapértelmezetté tétele/használat</i>	19
<i>újraindítás</i>	19
ng200 üzemmód: Internetre kapcsolódás internet megosztás privát VLAN hálózatokba	19
<i>Privát VLAN profil</i>	19
<i>Port szűrés</i>	20
<i>Port átirányítás</i>	20
<i>hozzáférési jog</i>	20
<i>LAN-ból VLAN-ba</i>	21
<i>VLAN-ból LAN-ba</i>	21
<i>Port átirányítás</i>	23
<i>ng200 beállítás alapértelmezetté tétele/használat</i>	23
<i>Újraindítás</i>	23
Alapadatok	23
<i>vpn beállítások</i>	26
<i>Adminisztrátori jelszó</i>	27
Statisztikák	28
<i>eszköz leltár</i>	28
<i>ethernet címek feloldása</i>	28
<i>hálózati térkép</i>	28
<i>Kockázat elemzés</i>	28
<i>Lehallgatás</i>	28
<i>Forgalom statisztika</i>	29
<i>NetStat</i>	29
Minta az ngNetSec MultiLayer router hálózati eszközzel elérhető hálózati variánsok egy összetett hálózatban	29
Minta az ngNetSec MultiLayer router ng100-as üzemmódban	30
Minta az ngNetSec MultiLayer router ng300-as üzemmódban	31

Minta az ngNetSec MultiLayer router ng200-as üzemmódban / LAN-ból VLAN-ba átalakítás	32
Minta az ngNetSec MultiLayer router ng200-as üzemmódban / VLAN-ból LAN átalakítás	33
Minta az ngNetSec MultiLayer router VPN kiszolgálója	34
Alkalmazott szabványok	35
Üzemeltetési körülmények.....	35
Garanciális feltételek.....	36
Jótállási jegy.....	38

Tulajdonságok és lehetőségek

- xDSL vagy kábeles modem segítségével internet csatlakozást biztosít.
- VLAN hálózatok létrehozása szerverként
- VLAN hálózatba kapcsolódás VLAN ID és ip cím alapján
- VLAN üzemmódban több ip cím és átjáró használata az internet irányába.
- Portsűrítő switch üzemmód, csatolónként beállítható hálózati áteresztő paraméterrel (path cost)
- VPN felhasználók létrehozása, hálózati korlátozása
- VPN szerveren keresztül, az engedélyezett alhálózatokhoz hozzáférés
- Új eszközök felderítése a hálózaton és erről http protokolon keresztül vagy e-mailben riasztás küldése.
- Lehallgató (promiscuous) üzemmódban működő eszközök keresése és riasztás http vagy e-mail formában
- Hálózaton lévő eszközök biztonsági kockázat elemzése, 3 szintű riasztás http vagy e-mail formában
- Visszacsatolt biztonsági ellenőrzés.
- 10 percenként frissülő grafikus hálózati topológia adatforgalomi kapcsolatok alapján
- Forgalom statisztika a router hálózati csatolóján.
- DHCP szerver, az IP címek és a DNS címek automatikus hozzárendeléséhez, mind LAN mind VLAN üzemmódokban
- Saját beépített DNS szerver mely opcionálisan használható
- címek (NAT) lefordítása a portok leképezésének támogatásával, a hálózaton belüli virtuális szerverek (webszerver, FTP, P2P hálózatok) használhatóságához
- (router-táblázat) beállításának lehetőségek
- kompatibilis az összes népszerű internetes alkalmazással.
- egyszerű beállítás internet böngésző segítségével a web interfészen keresztül.

Csomag tartalma

- 1 db ngNetSec MultiLayer router serial: ng100-300
- 1 db 18V 20Watt DC tápegység
- 1 db CD melyen kezelési útmutató található
- 1 db 512 MB pendrive karbantartási célokra.

ngNetSec MultiLayer router filozófia

Kapcsolatteremtés az internet zónával és hozzáférést biztosítani ngNetSec MultiLayer router-hez kapcsolódó hálózatoknak. Mind ezt oly módon, hogy a belső hálózaton lévő hálózati eszközök, folyamatos monitoring alatt állnak. Abban az esetben, ha a monitorozott eszközök bármilyen veszélyt jelentenek az gNetSec MultiLayer router által kiszolgált hálózatra vagy annak résztvevőire, azonnal riasztást indít a meghatározott protokollok szerint

Biztonságtechnikai megoldások az ngNetSec MultiLayer routerben

Eszközleltár

Rögzíti és folyamatosan keresi az új hálózati eszközöket az ngNetSec MultiLayer router-el azonos hálózatokban lévő címtartományokban. A leltározás után, ha új eszköz kerül az említett zónába, azonnal riasztást küld. Észlelési idő kb 1 perc

ip cím	ethernet cím	felderítés időpontja	csatoló	állapot
192.168.16.151	00:0c:6e:d8:42:65	2010-08-26 05:06:01	br0	új eszköz
192.168.16.165	00:11:d8:d3:0c:d9	2010-08-26 06:15:01	br0	új eszköz
192.168.16.7	00:1fc6:c0:5e:bd	2010-08-26 06:31:02	br0	új eszköz
192.168.16.1	6c:f0:49:00:28:17	2010-08-25 15:57:03	br0	leltárban
192.168.16.10	00:15:c5:a5:3b:62	2010-08-25 15:57:03	br0	leltárban
192.168.16.105	00:0d:60:06:6f:2f	2010-08-25 15:57:03	br0	leltárban
192.168.16.11	00:15:17:60:0b:fd	2010-08-25 15:57:03	br0	leltárban
192.168.16.12	00:18:f3:5e:b1:76	2010-08-25 15:57:02	br0	leltárban
192.168.16.131	00:a1:b0:09:01:df	2010-08-25 15:57:04	br0	leltárban
192.168.16.132	00:13:d4:40:5e:4f	2010-08-25 15:57:04	br0	leltárban
192.168.16.136	00:15:f2:86:8e:34	2010-08-25 15:57:04	br0	leltárban
192.168.16.159	00:19:66:59:98:47	2010-08-25 15:57:04	br0	leltárban
192.168.16.162	00:0a:e6:0b:8d:29	2010-08-25 15:57:05	br0	leltárban
192.168.16.171	00:1fc6:c0:32:8e	2010-08-25 15:57:03	br0	leltárban
192.168.16.177	00:16:ec:85:a9:0e	2010-08-25 15:57:04	br0	leltárban
192.168.16.18	00:00:85:43:93:64	2010-08-25 15:57:04	br0	leltárban
192.168.16.185	00:1fc6:c0:32:81	2010-08-25 15:57:04	br0	leltárban
192.168.16.19	00:00:85:00:00:00	2010-08-25 15:57:04	br0	leltárban

Kockázatelemzés:

Folyamatosan elemzi a hálózaton található eszközök állapotát. Naponta frissülő adatbázis alapján, képes eldönteni a hálózati eszközről, hogy az jelent-e veszélyt a hálózatra vagy nem, ha az eszközön akár csak jelszó nélkül felejtett szolgáltatás fut vagy olyan szolgáltatás, mely kihasználásával, súlyos következmények keletkezhetnek, ezeket megelőzve, a rendszer azonnal riaszt. Az eszközöket több tízezer kritérium alapján vizsgálja és 3 biztonsági rizikó faktorba sorolja azokat. Minden fenyegetettség feltárása után riasztást eszközöl az ngNetSec MultiLayer router. Jelen széria, 3-4 eszközt lépes ellenőrizni óránként, ez a szám lehet nagyobb illetve kisebb is, a hálózati eszközök szolgáltatásainak mennyiségi függvényében. Új hálózati eszközök ellenőrzési sorrendben az elsők, hálózati eszköz csatlakoztatását követően 2 és 17 percen belül elindul a vizsgálat.

Statistikák, elemzések				
Statistikák, elemzések		Eth cím	Dátum	IP cím
eszköz leltár	részletek	00:00:8d:cb:5c:ae	2010-09-06 13:11:46	192.168.16.23
hálózati térkép	részletek	00:24:1d:10:79:31	2010-09-06 13:02:16	192.168.16.21
Kockázat elemzés	részletek	00:15:17:26:bd:63	2010-09-06 12:54:42	192.168.16.20
Lehallgatás	részletek	00:00:85:0c:9b:ae	2010-09-06 12:43:22	192.168.16.19
Forgalom statisztika	részletek	00:00:85:43:93:64	2010-09-06 12:23:19	192.168.16.18
NetStat	részletek	00:18:f3:5e:b1:76	2010-09-06 12:11:01	192.168.16.12
	részletek	00:15:17:60:0b:fd	2010-09-06 11:50:23	192.168.16.11
	részletek	00:15:c5:a5:3b:62	2010-09-06 11:17:52	192.168.16.10
	részletek	00:80:87:7b:81:04	2010-09-06 10:58:22	192.168.16.9
	részletek	00:1fc6:c0:5e:bd	2010-09-06 10:54:58	192.168.16.7
	részletek	00:1a:4b:1af7:64	2010-09-07 10:43:04	192.168.16.3
	részletek	00:1fd0:0e:6b:d6	2010-10-07 10:35:46	192.168.16.2
	részletek	6c:f0:49:00:28:17	2010-09-06 0:24:00	192.168.16.1
	részletek	00:40:f6:f4:a3:a0	2010-09-07 9:10:52	192.168.16.254
	részletek	00:a0:d1:ca:67:8b	2010-09-06 8:40:54	192.168.16.208

A fehér színnel jelölt eszközökön kívül az összes többivel probléma van.

Piros: Kritikus hibák, bárki számára hozzáférhető adatok.

Sárga: Inkább programozási tudással, a teljes számítógép felett a hatalom átvehető.

Zöld: Nagy valószínűséggel, több órai munkával olyan információk kérhetők le a számítógépből, melyek kritikusak.

Statisztikák, elemzések

Ip cím: 192.168.16.10 Arp cím: 00:15:c5:a5:3b:62 Dátum: 2010-09-06 11:17:52

Port protocol	Port id	Service name	Severity	Data
tcp	21	ftp	Security Warning	<p>Microsoft IIS FTPd stack overflow</p> <p>The Microsoft IIS FTPd service may be vulnerable to a stack overflow via the NLST command. On Microsoft IIS 5.x this vulnerability can be used to gain remote SYSTEM level access, whilst on IIS 6.x it has been reported to result in a denial of service. Whilst it can be triggered by authenticated users with write access to the FTP server, this check determines whether anonymous users have the write access necessary to trigger it without authentication.</p> <p>On the following platforms, we recommend you mitigate in the described manner: Microsoft IIS 5.x Microsoft IIS 6.x</p> <p>We recommend you mitigate in the following manner: Filter inbound traffic to 21/tcp to only known</p>

Statisztikák, elemzések

- eszköz leltár
- hálózati térkép
- Kockázat elemzés
- Lehallgatás
- Forgalom statisztika
- NetStat

Az adott problémák és a megoldási javaslatok hozzá!

Statisztikák, elemzések

tcp	443	https	Security Note	<p>Synopsis :</p> <p>The remote web server is vulnerable to a URL injection vulnerability.</p> <p>Description :</p> <p>The remote host is running Microsoft Outlook Web Access 2003.</p> <p>Due to a lack of sanitization of the user input, the remote version of this software is vulnerable to URL injection which can be exploited to redirect a user to a different, unauthorized web server after authenticating to OWA. This unauthorized site could be used to capture sensitive information by appearing to be part of the web application.</p> <p>See also:</p>
-----	-----	-------	---------------	---

Statisztikák, elemzések

- eszköz leltár
- hálózati térkép
- Kockázat elemzés
- Lehallgatás
- Forgalom statisztika
- NetStat

Az adott problémák és a megoldási javaslatok hozzá!

Visszacsatolt biztonsági ellenőrzés:

Beállítható a ngNetSec MultiLayer routerbe, hogy jelentkezzen be a NetIntegral Consulting kft biztonságtechnikai szerverére és kérjen revíziót a hálózati szegmens internetes oldalára. A vizsgálat azonnal elindul, végeztével a központi szerver jelentést küld az ngNetSec MultiLayer router adminisztrátorának. Az ellenőrzés opcionálisan választható gyakoriságú.

Lehallgatás:

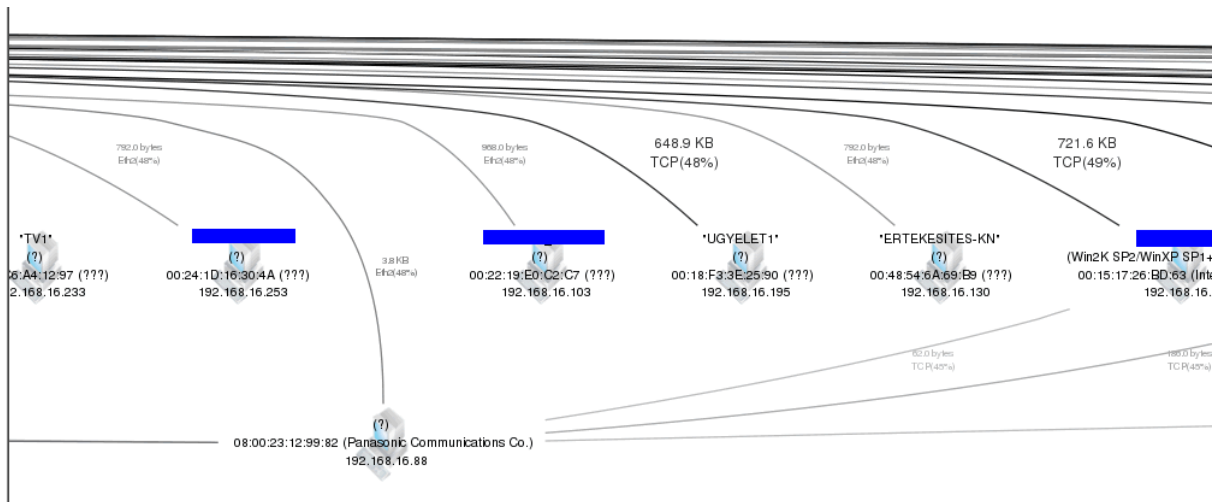
ngNetSec MultiLayer router a kockázatelemzések folyamán megvizsgálja az adott hálózati eszközön, hogy a kommunikációja rejt-e olyan jegyeket, mely arra enged következtetni, hogy a hálózati eszköz lehallgató üzemmódban van. Amennyiben talál ilyen eszközöket, úgy azonnal riaszt. A piros csillaggal jelölt eszközök viselkedése megegyezik a (promiscuous) üzemmódba állított eszközök viselkedésével.

Jelen széria, 3-4 hálózati eszközt képes ellenőrizni óránként. Új hálózati eszközök ellenőrzési sorrendben az elsők.

Statisztikák, elemzések					
Statisztikák, elemzések	riport	eth cím	ip cím	észlelés időponja	lahallgató üzemmód
eszköz leltár	részletek	00:12:17:49:59:d4	192.168.16.74	2010-08-26 7:33:19	*****
	részletek	00:00:85:43:93:64	192.168.16.18	2010-08-26 5:13:13	*****
hálózati térkép	részletek	00:00:85:0c:9b:ae	192.168.16.19	2010-08-26 4:32:45	*****
Kockázat elemzés	részletek	00:80:87:db:3f:67	192.168.16.205	2010-08-26 10:53:19	*****
Lehallgatás	részletek	00:24:1d:16:45:23	192.168.16.251	2010-08-26 9:47:14	*****
	részletek	00:16:ec:85:a9:0e	192.168.16.177	2010-08-26 9:26:03	*****
Forgalom statisztika	részletek	00:14:2ab7:26:fa	192.168.16.81	2010-08-26 9:19:26	*****
NetStat	részletek	00:1fc6:c0:32:81	192.168.16.185	2010-08-26 8:59:02	*****
	részletek	00:15f2:86:8e:34	192.168.16.136	2010-08-26 8:31:39	*****
	részletek	00:a0:d1:ca:67:8b	192.168.16.208	2010-08-26 8:20:59	*****
	részletek	00:24:1d:15:8f:23	192.168.16.31	2010-08-26 8:10:55	*****
	részletek	00:1a:92:4e:e4:82	192.168.16.213	2010-08-26 7:53:20	*****
	részletek	00:24:1d:12:ca:07	192.168.16.57	2010-08-26 6:22:49	*****
	részletek	00:15f2:ef:7d:2d	192.168.16.25	2010-08-26 6:04:09	*****
	részletek	00:1fd0:90:35:2c	192.168.16.249	2010-08-26 5:49:00	*****
	részletek	00:19:66:59:98:47	192.168.16.159	2010-08-26 5:04:59	*****
	részletek	00:40:f4:bc:39:05	192.168.16.192	2010-08-26 4:47:07	*****
	részletek	00:24:1d:14:20:fc	192.168.16.194	2010-08-26 4:10:28	*****

Hálózati térkép:

Hálózati topográfia készítés az adatforgalmak alapján. Képes a teljes hálózati eszközparkról vizuális térképet készíteni, függetlenül attól, hogy az eszközök milyen hálózati tartományban vannak elhelyezve. Hálózati térkép 10 percenként frissül.



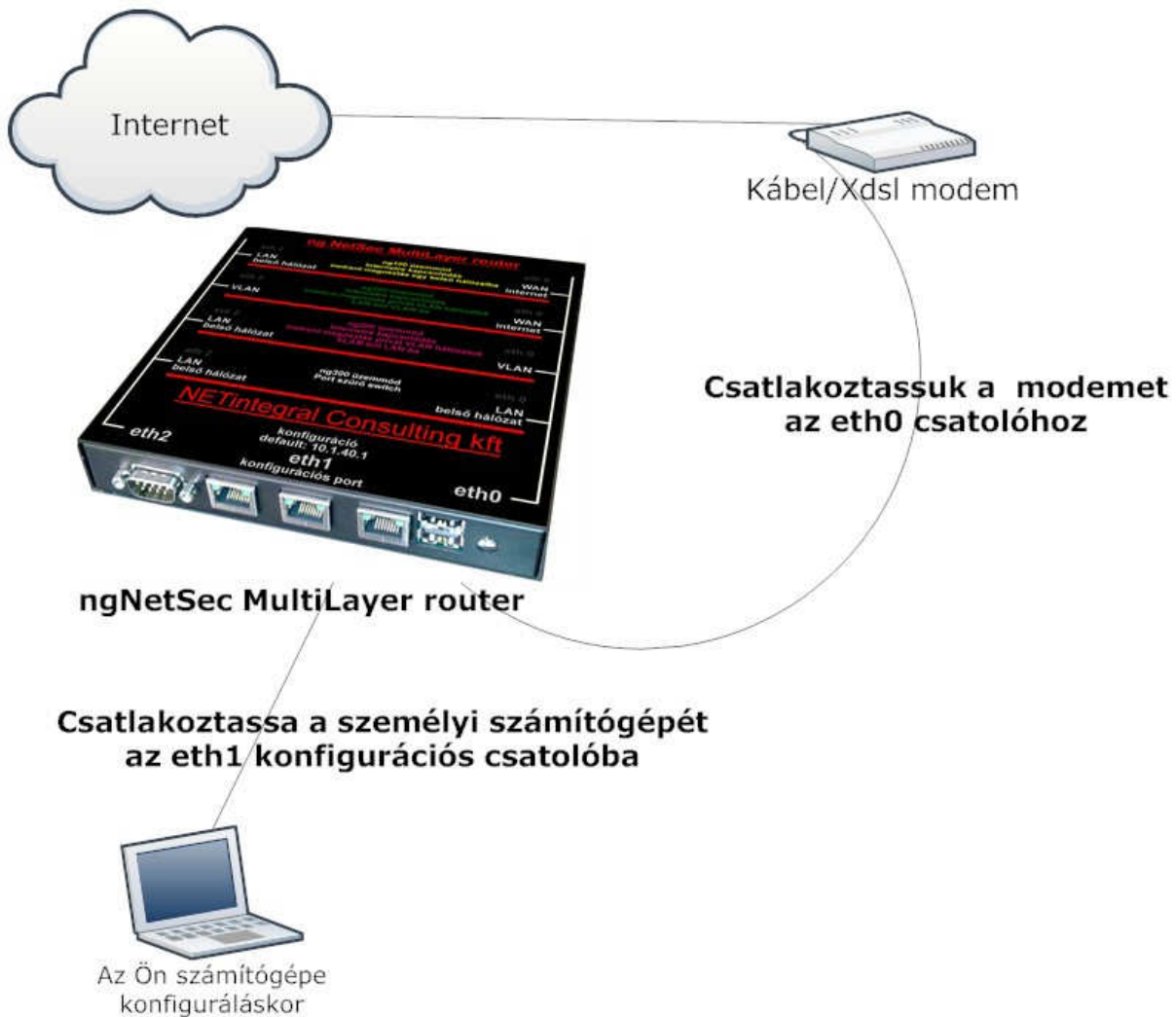
Kezdő lépések a használatbavételhez

Szüksége lesz egy szélessávú internet csatlakozásra

Tájékozódjon internet szolgáltatójánál az ADSL , ethernet kábel, kábelmodem, telepítésről.

Csatlakoztassa ng100-300 router WAN/internet eth0 portjához a modemhez.

Csatlakoztassa személyi számítógépét az eth1 konfigurációs porthoz.



ngNetSec MultiLayer router az **eth1** konfigurációs porton, DHCP segítségével kioszt Önnek egy 10.1.40.41 és 10.1.40.45 közötti címet.

Egy internet böngészőben nyissuk meg a következő címet:
<http://10.1.40.1> Itt az ngNetSec MultiLayer router kezelőfelülete fogad minket.

Megjegyzés: Ha az Ön számítógépe, melyről a konfigurálást végzi, nem tud DHCP-t fogadni, kérem olvassa el az 1. számú mellékletet, hogy a módosításokat el tudja végezni a konfigurációs számítógépen:

Belépés

Belépéskor alapértelmezett felhasználói név: admin

Belépéskor alapértelmezett jelszó név:

Csak abban az esetben tudunk a konfigurációs menübe jutni, ha a jelszót, mely minimum 12 karakteres szám és betű, be lett állítva

Reset

Resztelés: Szükségünk lesz egy pendrivera.

1. Áramtalanítsuk a készüléket.
2. A pendriveon hozzunk létre egy reset_ng_router.txt nevű üres állományt.
3. Helyezzük be az ngNetSec MultiLayer router serial: ng100-300 egyik usb csatolójába.
4. Majd helyezzük elektromos áram alá, az eszközt.
5. Kb 10-15 másodperc elteltével zero konfigurációval ismét elérhető lesz az eth1-es csatolón a 10.1.40.1 netmask 255.255.255.0 címen. Reset alatt az eth0 és az eth2 lekapcsolt állapotban van.
6. Miután konfiguráltuk az eszközt, vegyük ki a pendriveot és szabályosan indítsuk újra az adminisztrátori felületről.

ng100 üzemmód: Internet megosztás egy belső hálózatba

Információk

Általános információkat kaphatunk az ng100 üzemmódból:
hálózati csatolók eth0, eth1, eth2 eszközök állapotáról kapunk információkat

```

hálózati csatolók

eth0      Link encap:Ethernet  HWaddr [redacted]
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:10

          Link detected: no

eth1      Link encap:Ethernet  HWaddr [redacted]
          inet addr:10.1.40.1 Bcast:10.1.40.255 Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:11 Base address:0x4000

          Link detected: no

```

routing információk: A router útválasztásait láthatjuk

```

routing információk:

Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
-----
[redacted]        0.0.0.0         255.255.255.255 UH      0      0      0 tun0
[redacted]        0.0.0.0         255.255.255.0  U       0      0      0 eth1
[redacted]        0.0.0.0         255.255.255.0  U       0      0      0 br0
[redacted]        [redacted]      255.255.255.0  UG      0      0      0 tun0
0.0.0.0          [redacted]      0.0.0.0         UG      0      0      0 br0

```

dns: Névkiszolgáló szerver ip címe a router számára.

```
dns:  
,,127.0.0.1
```

dátum és idő: Router rendszerideje

```
dátum és idő:  
Tue Sep 7 15:11:35 CEST 2010
```

dsl kapcsolódás

Csatlakoztassuk a modemből érkező utp kábelt a routerünk eth0 hálózati csatlakoztatójába.

```
profil neve  
_____  
felhasználói név  
_____  
jelszó  
_____
```

profil neve: Adjuk meg a profil nevét, több profil is létrehozható, a profil név alapján tehetjük majd alapértelmezett kapcsolattá a az internet kapcsolatunkat. Az alapértelmezett kapcsolatot fogja használni internetszolgáltatónkhoz történő kapcsolódáshoz

felhasználói név: Adjuk meg dsl szolgáltatóunktól kapott felhasználói nevet

jelszó: Adjuk meg dsl szolgáltatóunktól kapott jelszavunkat



haladó beállítások: Az itt található rekordokat ne módosítsuk, ha egyértelműen nem tudjuk, hogy mit szeretnénk változtatni. A haladó beállítások különleges beállítások, melyek használatát az átlagos internetszolgáltatók nem módosítatják.

Rögzít: Rögzítsük az általunk megadott adatok alapján a profilt



Létrehozott profilok:

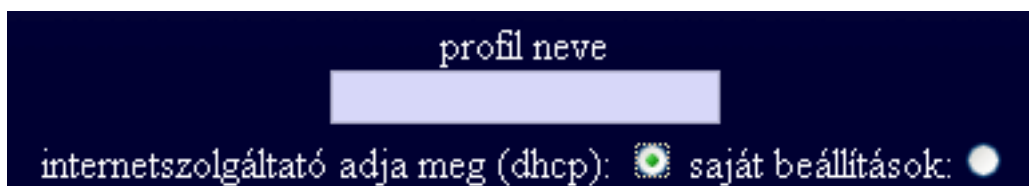
Itt gyűlnek a létrehozott profilok, melyekből a későbbiek folyamán választani lehet

Szerkesztés: Lehetőségünk van a profil szerkesztésre. Jelöljük ki a profilt majd nyomjunk a szerkesztés gombra. Végezzük el a szerkesztést, majd ismét nyomjunk a rögzít gombra.

Törlés: Ha nem kívánjuk a profilt megtartani, törölhetjük.

lan / kábel tv

Csatlakoztassuk a modemből érkező utp kábelt a routerünk eth0 hálózati csatlakoztatójába.



profil neve: Adjuk meg a profil nevét, több profil is létrehozható, a profil név alapján tehetjük majd alapértelmezett kapcsolattá a az internet kapcsolatunkat. Az alapértelmezett kapcsolatot fogja használni internetszolgáltatónkhoz történő kapcsolódáshoz

dhcp: ha internetszolgáltatónk dhcp-n keresztül osztja ki a kapcsolódáshoz szükséges információt, jelöljük be a dhcp beállítások jelölőgombot.

dhcp: Ha fix ip címmel rendelkezünk az internetszolgáltatónál, úgy a következőket kell megadni: jelöljük be a saját beállítások jelölőgombot.

ip cím: adjuk meg azt az ip címet, amit az internetszolgáltatónk adott meg, ez lesz az Ön ip címe azaz ezen a címen lesz elérhető a routere.

internetszolgáltató adja meg (dhcp): saját beállítások:

ip cím

alhálózati maszk

átjáró

MTU

névszerver:

névszerver:

rögzít

alhálózati maszk: Adjuk meg az alhálózati maszkot, melyet szintén az internetszolgáltatónk ad meg.

Átjáró: Adjuk meg az alapértelmezett átjárót, erről szintén az internetszolgáltató tájékoztatatta Önt

MTU: Adjuk meg a maximálisan feladható csomagméret számot, ezt szintén az internetszolgáltató adja meg (alapértelmezett érték: 1500)

névszerver: Adjuk meg a névszervereket, melyeket az internetszolgáltatónk adott meg.

Létrehozott profilok

[Dropdown menu]

Szerkesztés

Törlés

Létrehozott profilok:

Itt gyűlnek a létrehozott profilok, melyekből a későbbiek folyamán választani lehet

Szerkesztés: Lehetőségünk van a profil szerkesztésre. Jelöljük ki a profilt majd nyomjunk a szerkesztés gombra. Végezzük el a szerkesztést, majd ismét nyomjunk a rögzít gombra.

Törlés: Ha nem kívánjuk a profilt megtartani, törölhetjük.

Belso hálózat

Csatlakoztassuk a belsőhálózatunkat összekötő eszközből (switch, személyi számítógép) érkező hálózati csatlakoztatót a ngNetSec MultiLayer router eth2 hálózati csatlakoztatójába.

profil neve: Adjuk meg a profil nevét, több profil is létrehozható, a profil név alapján tehetjük majd alapértelmezett hálózattá a beállításokat. Az alapértelmezett kapcsolatot fogja használni hálózatunk automatikus elkészítésénél a router

router ip címe az alhálózat számára:

Határozzunk meg egy belsőhálózati ip címet: pl: 10.1.1.1 Ezen a címen lesz elérhető a routerünk a belsőhálózatban elhelyezett hálózati eszközök számára

alhálózati perfix: Az alhálózatban maximálisan elhelyezhető számítógépek száma:

24: 255 hálózati eszköz

18: 16,384 hálózati eszköz

16: 65, 536 hálózati eszköz

a továbbiakat a rendszer számítja ki: A router automatikusan a kapott információk alapján létrehozza a hálózatot melyhez a kliensek dhcp vagy direkt beállításokon keresztül csatlakozhatnak.

(Az alapbeállításokban engedélyezni vagy tiltani kell a dhcp automatikus kiszolgálását a kliens hálózat irányába)

saját beállítások:

kezdő ip cím:
 záró ip cím:
 átjáró
 névszerver:
 névszerver:
 WINS szerver
 rögzít

kezdő ip cím: Ha dhcp-n keresztül szolgáljuk ki a klienseket, úgy adjuk meg, hogy honnan induljon a dhcp címkiszolgálás. Pl: 10.1.1.100

záró ip cím: Ha dhcp-n keresztül szolgáljuk ki a klienseket, úgy adjuk meg, mekkora tartományig szolgáljon ki a dhcp szerver a kliensek felé Pl: 10.1.1.200

Tehát a kliensek ip címei 10.1.1.100 és 10.1.1.200 közé esnek majd.

Átjáró: Ha dhcp-n keresztül szolgáljuk ki a klienseket, adjuk meg, mely alapértelmezett átjárón keresztül használják az internetet. Ha a routerünket szeretnénk használni az internetre történő csatlakozásra, úgy adjuk meg a fentebb már beírt „router ip címe”-t a példánál maradva ez 10.1.1.1 lesz

névszerver: Adjuk meg, hogy a domain neveket mely névszerveren keresztül kívánjuk feloldani (dns) az alapbeállítások menüpontban lehetőség van a router saját dns szerverét igénybe venni, a példánál maradva ez: 10.1.1.1 lesz, de lehetőségünk van beállítani azt is, hogy az internetszolgáltató által biztosított névszervereket használjuk.

WINS szerver: Windows tallózó szerver ip címe

Létrehozott profilok

Szerkesztés Törlés

Létrehozott profilok:

Itt gyűlnek a létrehozott profilok, melyekből a későbbiek folyamán választani lehet

Szerkesztés: Lehetőségünk van a profil szerkesztésre. Jelöljük ki a profilt majd nyomjunk a szerkesztés gombra. Végezzük el a szerkesztést, majd ismét nyomjunk a rögzít gombra.

Törlés: Ha nem kívánjuk a profilt megtartani, törölhetjük.

Port átirányítások

Lehetőségünk van az internet irányából érkező adatforgalmak átirányítására egy belső hálózaton elhelyezett számítógépre.

inetren port: Internetes ip címünk mely portjára érkező forgalmat szeretnénk átirányítani: pl: 25

ip címre: Mely belsőhálózati ip címre szeretnénk a forgalmat átirányítani: pl 10.1.1.20

portra: A megadott ip cím hányas portjára szeretnénk átirányítani a forgalmat: pl 25

Ekkor az internetről érkező 25-ös portra azaz a levelezés a belsőhálózati 10.1.1.20-as számítógép smtp portára érkezik be.

ng100 beállítás alapértelmezetté tétele/használat

A már megadott profilokból tudjuk kiválasztani, hogy melyeket szeretnénk használni az internet és a belsőhálózat kialakítására.

Újraindítás

A módosítások csak akkor lépnek életbe, ha szabályosan újraindul routerünk, tehát erősítsük meg az újraindítási szándékunkat. A router 15-40 másodperc között ismét elérhető és megkezdí a szolgáltatását.

ng300 üzemmód: Port szűrő switch

1. Csatlakoztassuk az egyik belsőhálózatunkat összekötő eszközből (switch, személyi számítógép) érkező hálózati csatlakoztatót a ngNetSec MultiLayer router eth2 hálózati csatlakoztatójába.
2. Csatlakoztassuk a másik belsőhálózatunkat összekötő eszközből (switch, személyi számítógép) érkező hálózati csatlakoztatót a ngNetSec MultiLayer router eth0 hálózati csatlakoztatójába.

switch paraméterezése

The image shows a vertical list of configuration fields on a dark blue background. Each field consists of a label and a light blue input box. At the bottom is a 'rögzít' (save) button.

- profil neve
- ip cím
- alhálózati maszk
- átjáró
- MTU
- névszerver:
- névszerver:
- cost eth0:
- cost eth2:
- rögzít

profil neve: Adjuk meg a profil nevét, több profil is létrehozható, a profil név alapján tehetjük majd alapértelmezetté beállításokat.

ip cím: A switch ip címen, ezen keresztül kommunikál a hálózat többi résztvevőjével fontos, hogy ugyan abba az ip címtartományban, hálózatban legyen az eszköz melyeket kiszolgál.

alhálózati maszk: adjuk meg ugyan azt az alhálózati maszkot, ami a kiszolgált hálózatnál be lett állítva

átjáró: adjuk meg ugyan azt az alapértelmezett átjárót, ami a kiszolgált hálózatnál be lett állítva.

MTU: Adjuk meg a maximálisan feladható csomagméret számot (alapértelmezett érték: 1500)

névszerver: adjuk meg ugyan azt a névszerveret, ami a kiszolgált hálózatnál be lett állítva.

cost eth0- cost eth2: Az adott hálózati eszköz információszolgáltatása a hálózat többi résztvevője felé, oly módon, hogy a hálózat tagjaival elhitegeti magáról, hogy az adott hálózati csatoló a következő paraméterek szerinti. Ezzel a beállítással lehet forgalmat irányítani a hálózati eszközöket útválasztás nélkül. Minél nagyobb az áteresztőképesség, annál inkább emelkedik a forgalom.

Áteresztőképesség: path cost érték

4 Mbps: 250

10 Mbps: 100

16	Mbps: 62
45	Mbps: 39
100	Mbps: 19
155	Mbps: 14
622	Mbps: 6
1	Gbps: 4
10	Gbps: 2



Létrehozott profilok:

Itt gyűlnek a létrehozott profilok, melyekből a későbbiek folyamán választani lehet

Szerkesztés: Lehetőségünk van a profil szerkesztésre. Jelöljük ki a profilt majd nyomjunk a szerkesztés gombra. Végezzük el a szerkesztést, majd ismét nyomjunk a rögzít gombra.

Törlés: Ha nem kívánjuk a profilt megtartani, törölhetjük.

port szűrés

eth0 és eth2 között azok a portok nem kommunikálhatnak, melyeket itt rögzítünk.

ng300 beállítás alapértelmezetté tétele/használat

A megadott profil tudjuk kiválasztani melyet a router használni fog az újraindítást követően.

újraindítás

A módosítások csak akkor lépnek életbe, ha szabályosan újraindul routerünk, tehát erősítsük meg az újraindítási szándékunkat. A router 15-40 másodperc között ismét elérhető és megkezd a szolgáltatását.

ng200 üzemmód: Internetre kapcsolódás internet megosztás privát VLAN hálózatokba

VLAN átalakításokat csak fix ip címmel lehet végezni, azaz vagy egy másik ngNetSec MultiLayer router szükséges az internet csatlakozáshoz vagy egyéb router vagy pedig fix ip cím az internetszolgáltatótól.

Csatlakoztassuk az internet irányából érkező hálózati kábelt az eth0 hálózati csatlóba, míg belső hálózatra szánt kábelt az eth2 csatlóba

Privát VLAN profil

profil neve: Adjuk meg a profil nevét, több profil is létrehozható, a profil név alapján tehetjük majd alapértelmezetté beállításokat.

VLAN cím: VLAN ID-ben közlekedő tartományok belső átjáró címe, mely összeköti a hálózatokat egymással illetve az internettel. Ide olyan privát hálózati címet adjunk meg, ami nincs használatban. Pl: 10.99.99.1

Hálózati prefix(opcionális): alhálózati perfix: Az alhálózatban maximálisan elhelyezhető számítógépek száma:

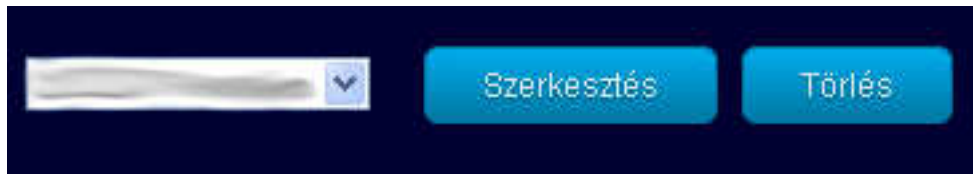
24: 255 hálózati eszköz

18: 16,384 hálózati eszköz

16: 65, 536 hálózati eszköz

VLAN ID: 2-4095 közötti azonosítót adjunk meg. A VLAN ID-k teszik lehetővé, hogy fizikailag ugyan azon a kábelén több „virtuális kábel” elkülönül

Mentés: mentsük el a profilt, később ebből kell kijelölnünk az alapértelmezett üzemmód használatot.



Szerkesztés: Lehetőségünk van a profil szerkesztésre. Jelöljük ki a profilt majd nyomjunk a szerkesztés gombra. Végezzük el a szerkesztést, majd ismét nyomjunk a mentés gombra.

Port szűrés

Meghatározhatjuk, hogy adott VLAN ID-ban milyen portokat blokkolunk a továbbjutásban.

Port átirányítás

Meghatározhatjuk, hogy egy adott internetes hálózatból érkező forgalom portjait átirányítsuk egy VLAN ID-ban szereplő ip címre illetve a kiszolgált hálózati eszköz portjára.

hozzáférési jog

Amennyiben használjuk, úgy csak azok a VLAN kliensek tudnak az ID-ba belépni, akiknek a hálózati csatoló címük (mac address) szerepel a listában.

LAN-ból VLAN-ba

Itt rendelkezhetjük össze, hogy mely internetes ip címek tartozzanak a VLAN ID-hez, egy ip cím több VLAN ID-hoz is tartozhat.

Példa:

lan / kábel tv ip cím: 84.112.25.9

VLAN ID: 5

VLAN cím: 10.99.99.1 prefix:24

Hálózati cím: 00:0D:B9:1C:E4:3C

Ekkor a kliens oldalon a következők a beállítások:

VLAN ID: 5

Kliens ip címe: 10.99.99.2- től 10.99.99.254 ig

Netmaszk: 255.255.255.0

Alapértelmezett átjáró: 10.99.99.1

Dns: 10.99.99.1, ha be lett kapcsolva a saját dns kiszolgáló használata, egyéb esetben az internetszolgáltató dns szerver címe.

Hálózati cím: 00:0D:B9:1C:E4:3C

VLAN-ból LAN-ba

Beléphetünk az ngNetSec MultiLayer router által létrehozott VLAN egyik ID-jába.

Vlan ID

Vlan átjáró IP címe

Vlan IP címe

profil neve

router ip címe az alhálózat számára:

VLAN ID: adjuk meg azt az azonosítót, melyet a ngNetSec MultiLayer router LAN-ból VLAN funkciójában megadtunk és amit ezen az eszközön szeretnénk üzemeltetni.

Pl: 5

VLAN átjáró IP címe: Adjuk meg a kiválasztott VLAN ID ip címét amit a másik ngNetSec MultiLayer router LAN-ból VLAN funkciójában megadtunk

Pl: 10.99.99.1

Vlan IP címe: Ide adjunk meg egy a VLAN átjáró IP cím tartományban szereplő szabad ip címet
 Pl: 10.99.99.254

profil neve: Adjuk meg a profil nevét, több profil is létrehozható, a profil név alapján tehetjük majd alapértelmezetté beállításokat.

A következőkben állítsuk be a VLAN-ból érkező adatforgalom kiosztását a belső hálózatunkra

router ip címe az alhálózat számára: ez lesz az alapértelmezett átjáró a kliensek számára.
 Pl: 192.168.1.1

kezdő ip cím: Ha dhcp-n keresztül szolgáljuk ki a klienseket, úgy adjuk meg, hogy honnan induljon a dhcp címkiszolgálás. Pl: 192.168.1.100

záró ip cím: Ha dhcp-n keresztül szolgáljuk ki a klienseket, úgy adjuk meg, mekkora tartományig szolgáljon ki a dhcp szerver a kliensek felé Pl: 192.168.1.200

Tehát a kliensek ip címei 192.168.1.100 és 192.168.1.200 közé esnek majd.

Átjáró: Ha dhcp-n keresztül szolgáljuk ki a klienseket, adjuk meg, mely alapértelmezett átjárón keresztül használják az internetet. Ha a routerünket szeretnénk használni az internetre történő csatlakozásra, úgy adjuk meg a fentebb már beírt „router ip címe”-t a példánál maradva ez 192.168.1.1 lesz

névszerver: Adjuk meg, hogy a domain neveket mely névszerveren keresztül kívánjuk feloldani (dns) az alapbeállítások menüpontban lehetőség van a router saját dns szerverét igénybe venni, a

példánál maradva ez: 192.168.1.1 lesz, de lehetőségünk van beállítani azt is, hogy az internetszolgáltató által biztosított névszervereket használjuk.

WINS szerver: Windows tallózó szerver ip címe



Szerkesztés: Lehetőségünk van a profil szerkesztésre. Jelöljük ki a profilt majd nyomjunk a szerkesztés gombra. Végezzük el a szerkesztést, majd ismét nyomjunk a rögzít gombra

Törlés: Ha nem kívánjuk a profilt megtartani, törölhetjük.

Port átirányítás

Lehetőségünk van a belépett VLAN ID irányából érkező adatforgalmak átirányítására egy belső hálózaton elhelyezett számítógépre.

VLAN ID ip címére érkező port: Pl: 10.99.99.254

VLAN ID ip címünk mely portájára érkező forgalmat szeretnénk átirányítani: pl: 25
ip címre: Mely belsőhálózati ip címre szeretnénk a forgalmat átirányítani: pl 192.168.1.30
portra: A megadott ip cím hányas portjára szeretnénk átirányítani a forgalmat: pl 25

Ekkor VLAN ID ip címére érkező 25-ös portra azaz a levelezés a belsőhálózati 192.168.1.30-as számítógép smtp portára érkezik be.

ng200 beállítás alapértelmezetté tétele/használat

Válasszuk ki, hogy mely üzemmódot szeretnénk használni.

Újraindítás

A módosítások csak akkor lépnek életbe, ha szabályosan újraindul routerünk, tehát erősítsük meg az újraindítási szándékunkat. A router 15-40 másodperc között ismét elérhető és megkezdi a szolgáltatását.

Alapadatok



Profil használata:

Kiválaszthatjuk, hogy mely üzemmódban szeretnénk használni a ngNetSec MultiLayer router serial: ng100-300 eszközt, kiválasztás után az üzemmód konfigurálhatóvá válik.

Router azonosító:

Szerződés szerinti azonosító, ez elsősorban a visszacsatolt biztonsági ellenőrzésekhez szükséges, ez alapján történik az azonosítás.

Host name:

Adminisztrátor e-mail címe:

SMTP szerver

Felhasználó név

Jelszó

Ez a mail cím jelenik meg küldőként

Teszt

Adminisztrátor e-mail címe: Erre az email címre küldi a router a különböző riasztásokat, figyelmeztetéseket. Pontosvesszővel elválasztva, több e-mail cím is megadható.

SMTP szerver: Levél küldéshez szükséges az smtp szerver ip címének vagy hoszt nevének megadása

Felhasználó név: Ha az smtp szerver, azonosítást kér, itt adhatjuk meg a felhasználói nevet

Jelszó: Ha az smtp szerver, azonosítást kér, itt adhatjuk meg a jelszót

Ez az e-mail cím jelenik meg küldőként: A riasztásoknál ez az email cím kerül a levél feladó részébe.

Teszt gomb: Az e-mail riasztás lehetőségének tesztelése.

Visszacsatolt biztonsági ellenőrzés kérés használata

Hálózati felderítés bekapcsolása

Eredmény POST-olása a következő http címre:

Internet oldaláról rendellenes hálózati forgalom tiltása

Hálózati eszközök kockázat elemzése

Eredmény POST-olása a következő http címre:

Visszacsatolt biztonsági ellenőrzés kérés használata: Bejelentkeztetés a biztonságtechnikai szerverre és önrevíziót kérése a hálózati szegmens internetes oldalára

Hálózati felderítés bekapcsolása: Új hálózati eszközöket keres az ngNetSec MultiLayer router serial: ng100-300 által kiszolgált hálózatban.

Eredmény POST-olása a következő http címre: A tesztelési eredmények elküldése http-n keresztül a mellékelt példa alapján, adjuk meg azt az url-t, ahol a postolási eredményeket fogadni tudjuk.

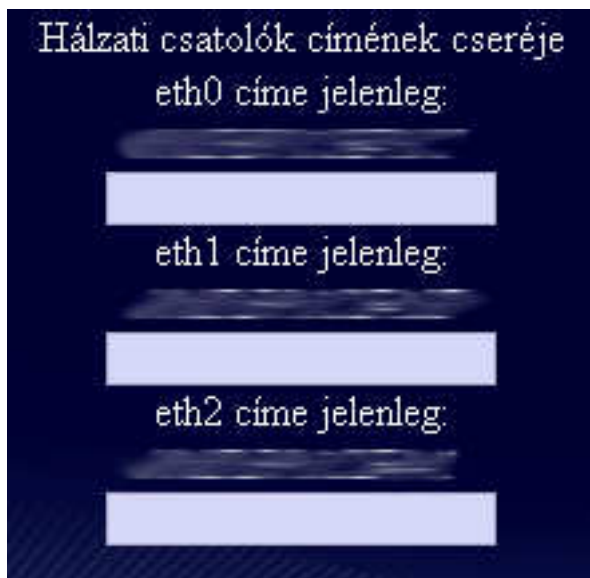
Internet oldaláról rendellenes hálózati forgalom tiltása: Olyan szabály együttes, melyek megakadályozzák az internetről érkező terheléses támadásokat (D.O.S)

Hálózati eszközök kockázat elemzése:

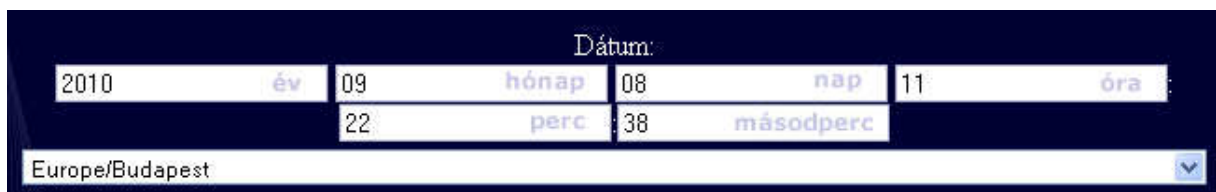
Hibákat, hátsó kapukat keres a már felderített hálózati eszközökön.

Eredmény POST-olása a következő http címre:

A tesztelési eredmények elküldése http-n keresztül a mellékelt példa alapján, adjuk meg azt az url-t, ahol a postolási eredményeket fogadni tudjuk, minta kódot a kezelőfelületen tudunk letölteni.



Hálózati csatolók címének cseréje: Lehetőségünk van megadni saját hálózati csatoló címet azaz Media Access Control address (MAC address)



Dátum: dátum és idő beállítása

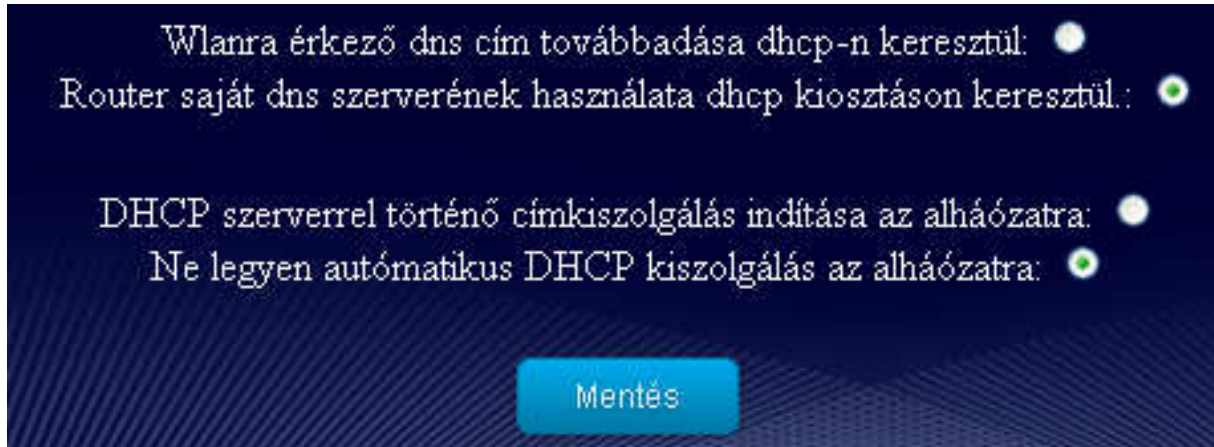
Wlanra érkező dns cím továbbadása dhcp-n keresztül: Az internetszolgáltató által megadott dns cím átadása a dhcp szerver részére.

Router saját dns szerverének használata dhcp kiosztáson keresztül:

Az ngNetSec MultiLayer router serial: ng100-300 saját dns szerverének indítása majd az elérhetőségének továbbítása a dhcp szerver által kiszolgált kliensek részére

DHCP szerverrel történő cím kiosztás indítása az alhálózatra: Automatikusan indítja a dhcp szervert.

Ne legyen automatikus DHCP kiosztás az alhálózatra: Nem indít dhcp szervert.



Mentés gomb. A beállítások alkalmazása

vpn beállítások

VPN által létrehozott magánhálózat: hálózati cím:10.222.111.0 netmaszk: 255.255.255.0:
A vpn kliensek részére 10.222.111.0/24-es hálózatból kerül kiosztásra ip cím.

Rendszer VPN kulcsok felülírása, most feltöltött VPN kulcsok használata:

Feltölthetjük saját vpn kulcsainkat, vpn kulcsok generálásáról a <http://openvpn.net/> címen tájékozódhatunk.

Ha az alapbeállítást szeretnénk használni, töltsük le a kliensek kapcsolódásához szükséges konfigurációs fájlokat http://router_admin_cime/router/alapadatok/hasznalható_minta.zip helyről, melyeket be kell másolni az OpenVPN Config könyvtárba, majd az ng_serias.ovpn fájlban a kapcsolódáshoz szükséges ip címet le kell cserélni.

Hálózatok, melyekbe lehetséges a VPN útválasztás: Azok a hálózatok, melyek a VPN szerver számára elérhetőek lehetnek. A VPN szerver automatikusan indul, ha)

Hálózat felvétele a VPN routingba

hálózat:

netmaszk:

felvétel

törlés 10.222.111.0 / 255.255.255.0

Hálózat felvétele a VPN routingba:

Adjuk hozzá azokat a hálózatokat, melyeket a VPN szerver elérhet.

(A VPN szerver automatikusan elindul, ha talál hálózati bejegyzést, melyet elérhet)

hálózat: Adjuk meg a hálózatot: pl: 10.222.111.0

netmaszk: adjuk meg a hálózati maszkot, pl: 255.255.255.0

felvétel: alkalmazzuk a beállításokat.

Felhasználói név:

Jelszó:

Tiltott hálózatok a kliens számára, egy sor/hálózat:

pl: 192.168.1.0 255.255.255.0

felvétel

Felhasználói név: Adjuk meg a vpn felhasználói nevet:
speciális karakterek és szóköz nélkül.

Jelszó: Adjuk meg a minimum 12 számból és betű karakterekből álló jelszót.

Tiltott hálózatok a kliens számára, egy sor/hálózat: Ha nem szeretnénk, hogy az összes a vpn szerver által elérhető hálózatba be tudjon lépni a kliens, úgy tiltsuk le azokat a hálózatokat, melyekbe a belépés nem engedélyezett

Adjuk meg a minimum 12 számból és betű karakterekből álló jelszót.

Statisztikák

eszköz leltár

Ha a beállításokban engedélyezve lett a hálózati felderítés, úgy ezen a felületen találhatjuk meg azokat az eszközöket, melyeket az ngNetSec MultiLayer router serial: ng100-300 eszköz megtalált.

ethernet címek feloldása

Mivel az ip címek változhatnak, így az ethernet csatolók címe alapján végzi a rendszer a felderítést, az ethernet címek feloldásával láthatóvá válik, hogy mely hálózati csatolónak mi a jelenlegi ip címe.

hálózati térkép

Grafikus megjelenítésű hálózati térkép, mely a hálózati forgalmak alapján jeleníti meg az eszközök kapcsolatát.

Kockázat elemzés

Az ngNetSec MultiLayer router serial: ng100-300 eszköz által kockázatosnak ítélt hálózati eszközök listája.

Folyamatosan elemzi a hálózaton található eszközök állapotát. Naponta frissülő adatbázis alapján, képes eldönteni a hálózati eszközről, hogy az jelent-e veszélyt a hálózatra vagy nem, ha az eszközön akár csak jelszó nélkül felejtett szolgáltatás fut vagy olyan szolgáltatás, mely kihasználásával, súlyos következmények keletkezhetnek, ezeket megelőzve, a rendszer azonnal riaszt. Az eszközöket több tízezer kritérium alapján vizsgálja és 3 biztonsági rizikó faktorba sorolja azokat. Minden fenyegetettség feltárása után riasztást eszközöl az ngNetSec MultiLayer router. Jelen széria, 3-4 eszközt lépés ellenőrizni óránként, ez a szám lehet nagyobb illetve kisebb is, a hálózati eszközök szolgáltatásainak mennyiségi függvényében. Új hálózati eszközök ellenőrzési sorrendben az elsők, hálózati eszköz csatlakoztatását követően 2 és 17 percen belül elindul a vizsgálat.

Fehér: Nincs hiba, biztonságos eszköz

Piros: Kritikus hibák, bárki számára hozzáférhető adatok.

Sárga: Inkább programozási tudással, a teljes számítógép felett a hatalom átvehető.

Zöld: Nagy valószínűséggel, több órai munkával olyan információk kérhetők le a számítógépből, melyek kritikusak.

Lehallgatás

Az ngNetSec MultiLayer router serial: ng100-300 a kockázatelemzések folyamán megvizsgálja az adott hálózati eszközön, hogy a kommunikációja rejt-e olyan jegyeket, mely arra enged következtetni, hogy a hálózati eszköz lehallgató üzemmódban van. Amennyiben talál ilyen

eszközöket, úgy azonnal riaszt. A piros csillaggal jelölt eszközök viselkedése megegyezik a (promiscuous) üzemmódba állított eszközök viselkedésével.

Bizonyos típusú eszközök, pl egyes Cisco routerek, switch-ek ellenőrzésekor, hasonló eredmények jöhetnek ki, mint a lehallgató üzemmódba helyezett számítógépeknél

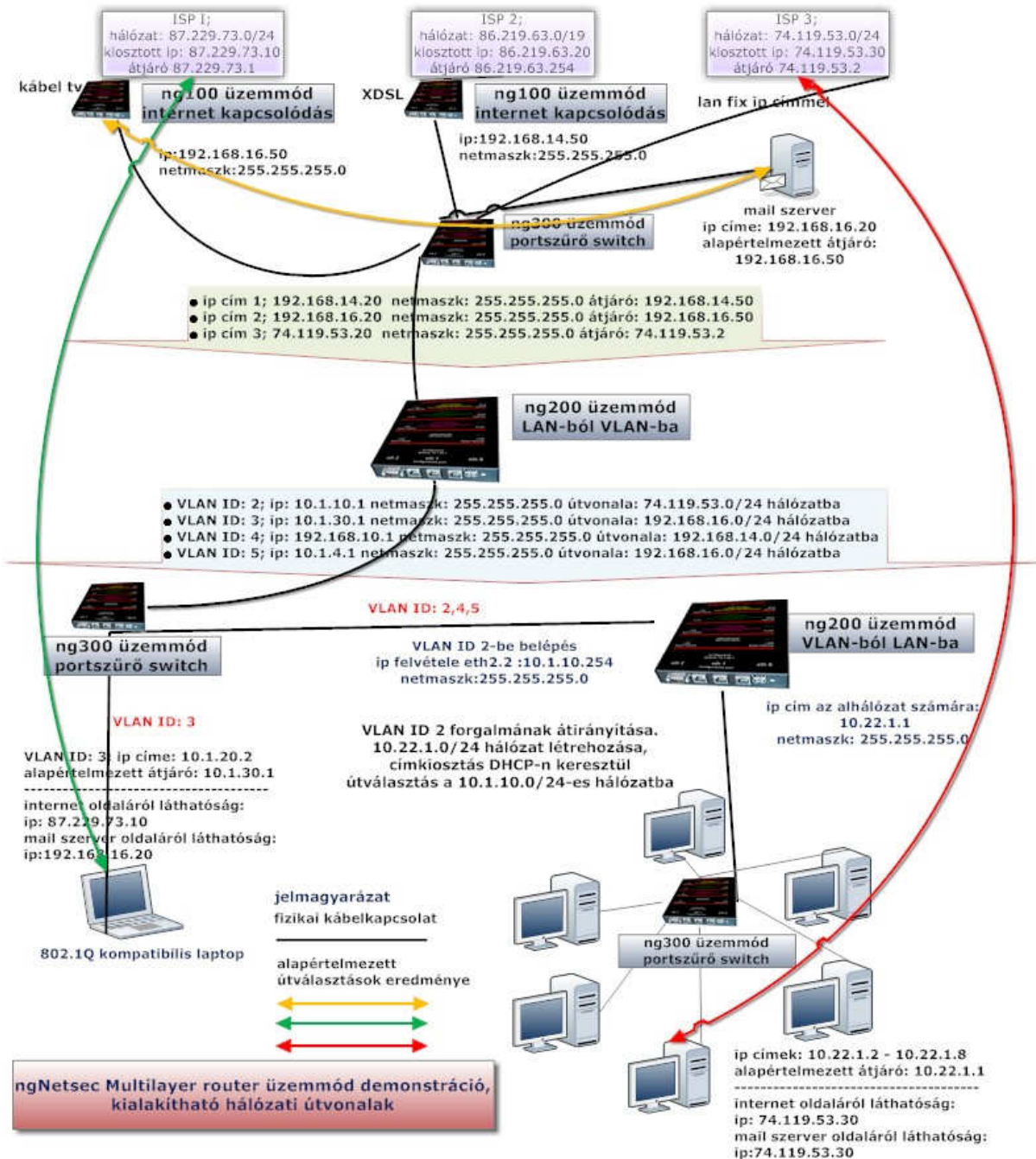
Forgalom statisztika

Hálózati csatolók adatforgalmi statisztikái.

NetStat

Az ngNetSec MultiLayer router serial: ng100-300 eszköz hálózati kezdeményezései.

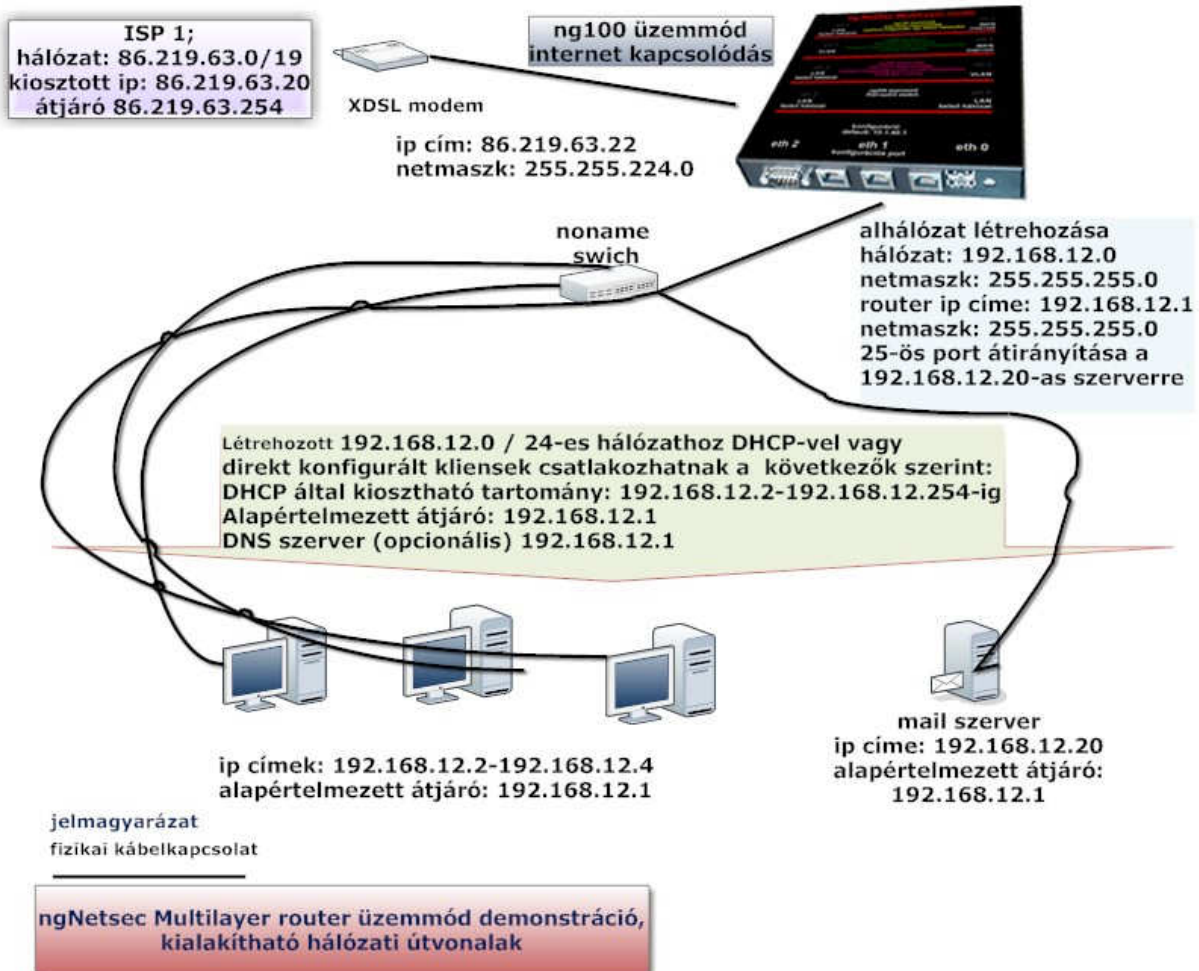
Minta az ngNetSec MultiLayer router hálózati eszközzel elérhető hálózati variánsok egy összetett hálózatban



Minta az ngNetSec MultiLayer router ng100-as üzemmódban

Internetre kapcsolódás, intrnet megosztás egy belső hálózatba

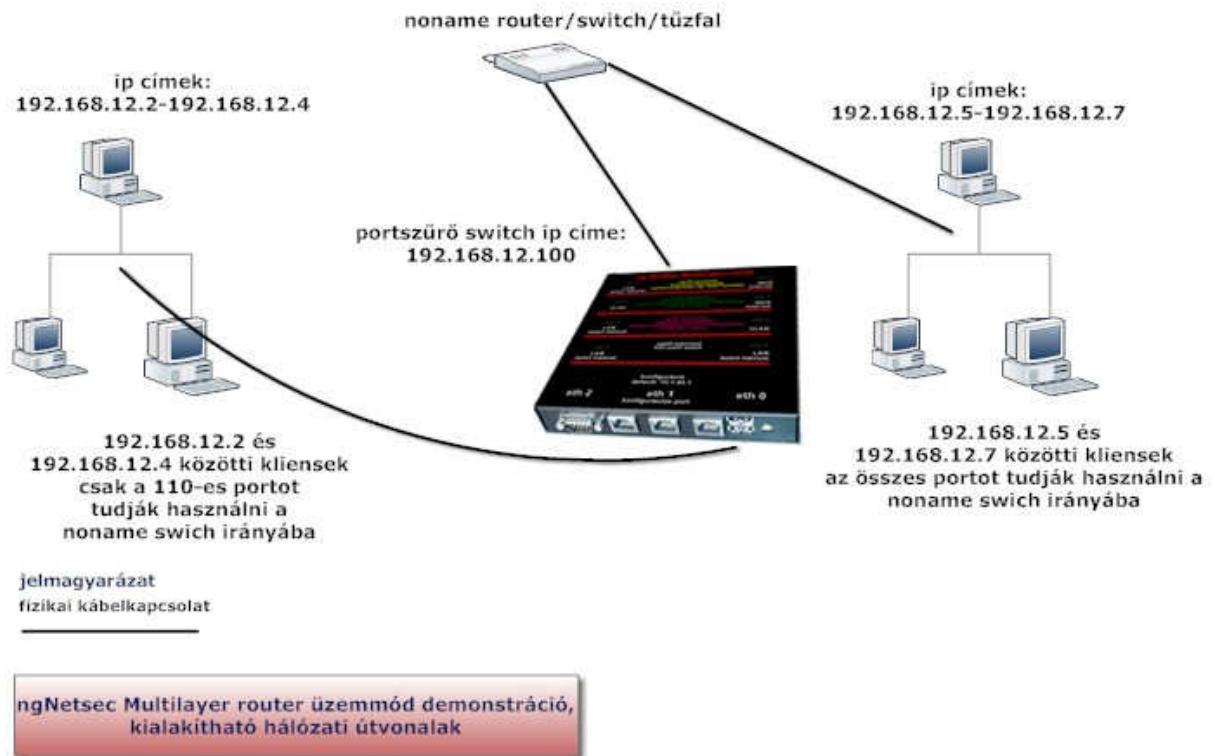
A következő ábra egy internet kapcsolódást mutat be kábel tv vagy xDSL (pl adsl) modemen keresztül, majd létrehozza a kívánt alhálózatot s egyben a létrehozott hálózat számára címfordításon keresztül internet kapcsolatot biztosít illetve a bejövő leveleket a 25-ös porton keresztül a belső hálózatban található levelezőszerver felé továbbítja



Minta az ngNetSec MultiLayer router ng300-as üzemmódban

Port szűrő switch (ng300)

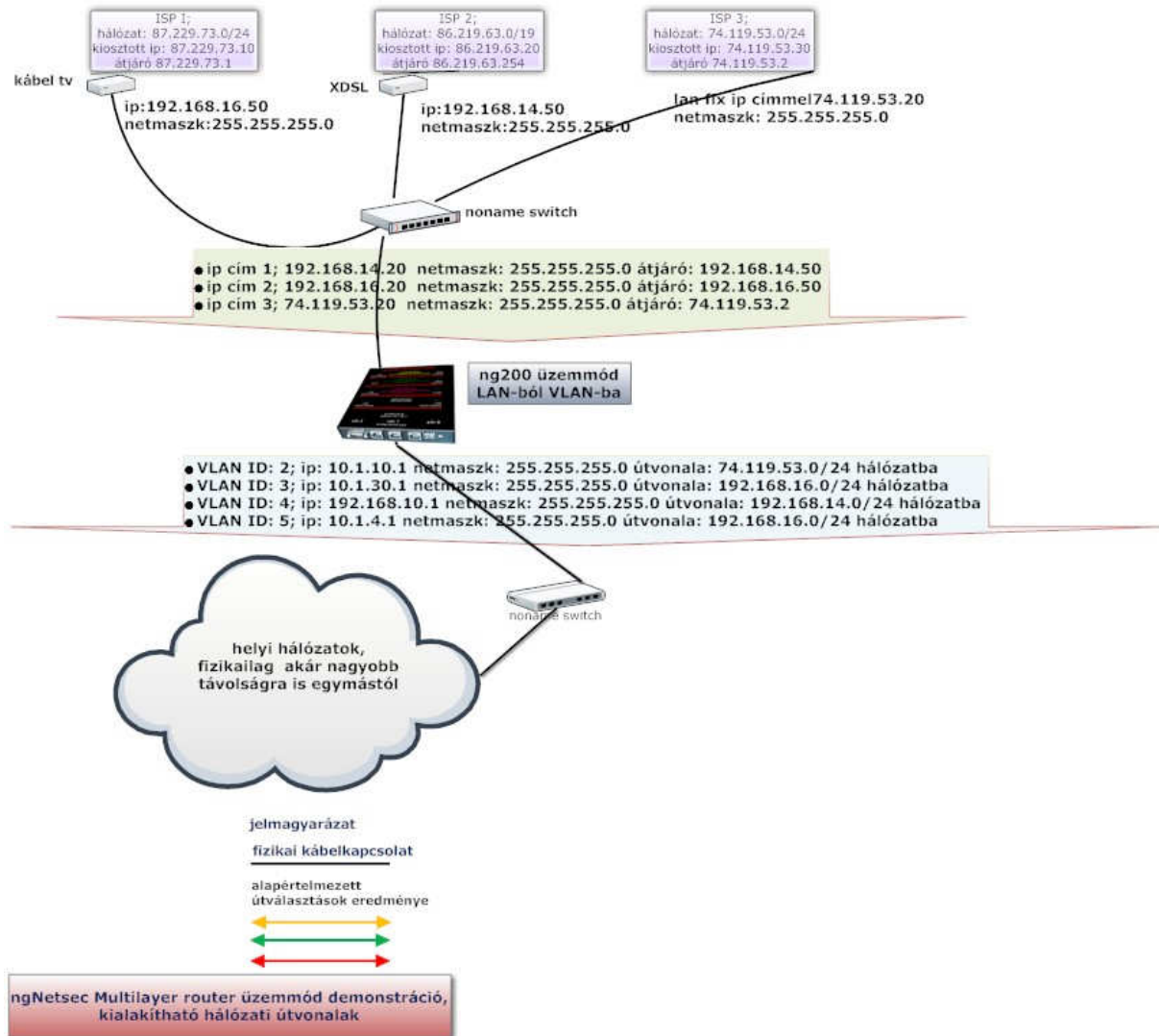
Lehetőségünk van portszűrő switch-ként üzemeltetni a routert, ezzel megoldható egy alhálózaton belül bizonyos hálózati szegmensek korlátozása.



Minta az ngNetSec MultiLayer router ng200-as üzemmódban / LAN-ból VLAN-ba átalakítás

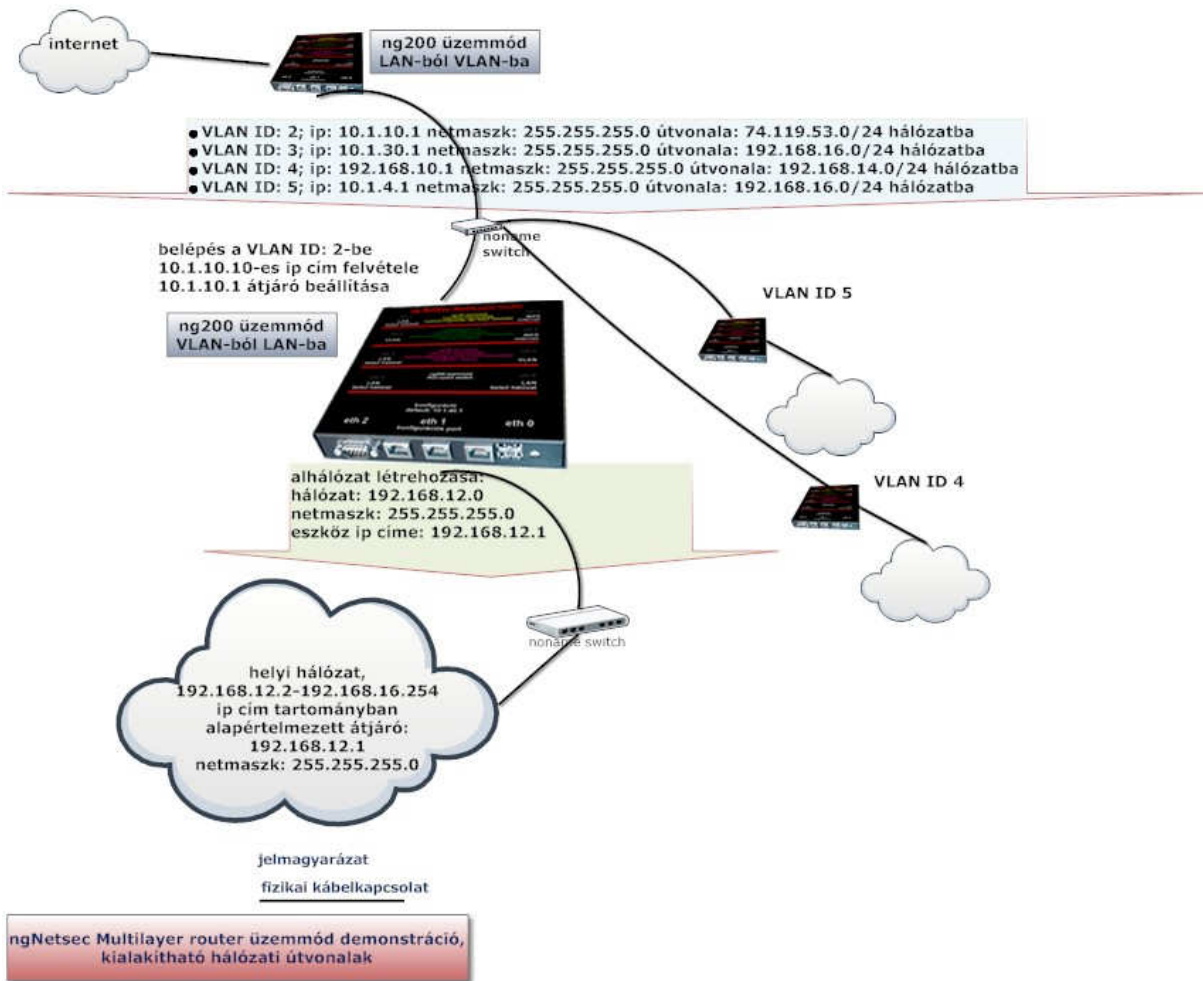
ngNetSec MultiLayer router több ip címet képes felvenni az eth0 lábon, így akár több internet szolgáltatóhoz is képes kapcsolódni, a router mindig azt az átjárót használja a kommunikációhoz ami az ip címhez hozzá lett rendelve.

VLAN-ok létrehozásakor az eszköz képes arra, hogy egy felvett ip címet akár több VLAN-hoz is hozzárendelje, ebben az esetben az összerendelt VLAN-IP –k az ip címhez rendelt átjárót fogják használni. Lehetőség van arra is, hogy mindegyik VLAN-t külön külső ip címmel illetve a hozzá tartozó átjáróhoz rendeljük:



Minta az ngNetSec MultiLayer router ng200-as üzemmódban / VLAN-ból LAN átalakítás

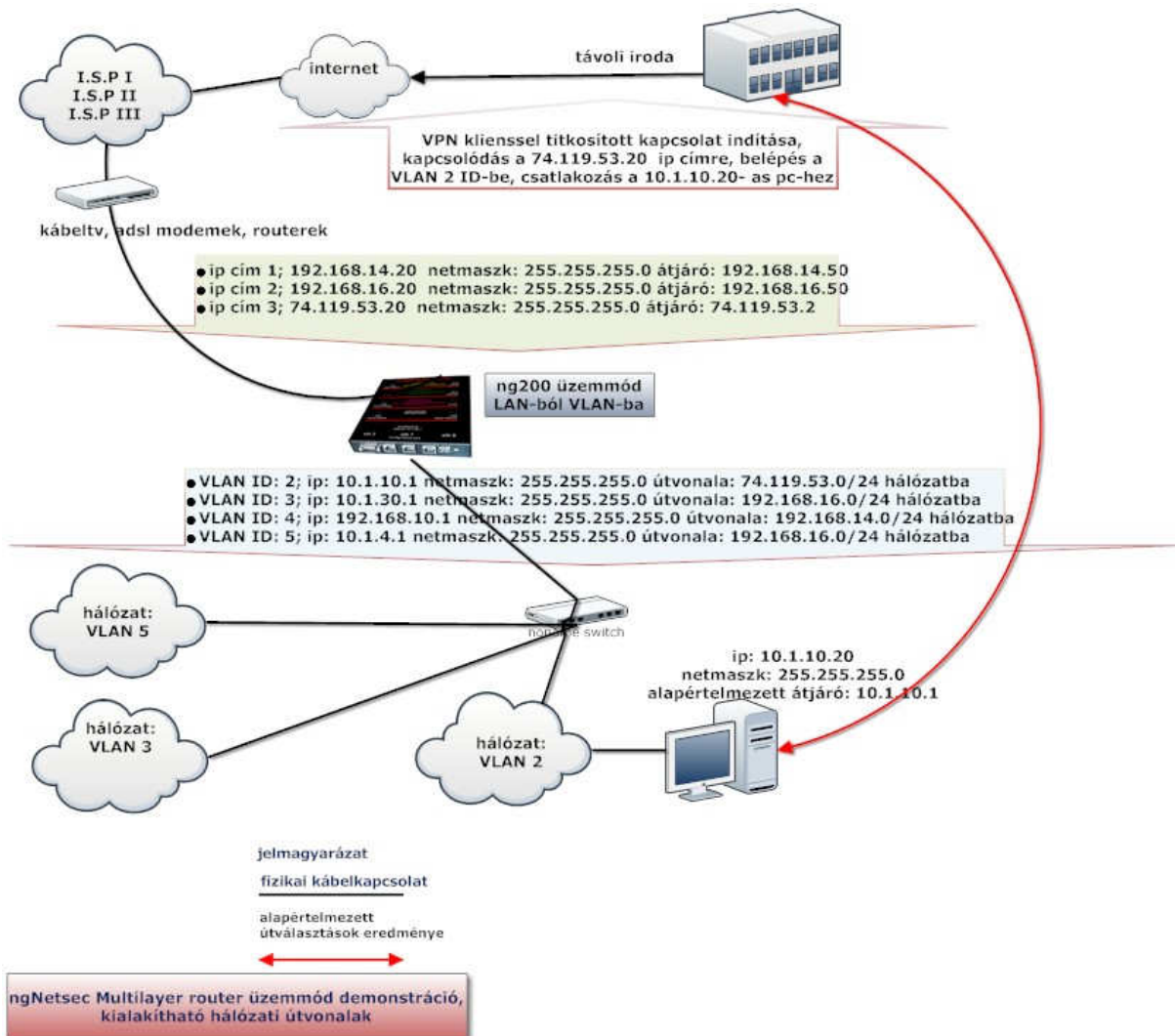
ngNetSec MultiLayer router belép egy VLAN hálózatba majd a két VLAN közötti ip címet használja natolt formában az adattovábbításra.



Minta az ngNetSec MultiLayer router VPN kiszolgálója

Lehetőség van korlátlan számban VPN felhasználókat létrehozni a ngNetSec MultiLayer router kezelőfelületén.

Meg kell határozni, hogy a VPN kiszolgáló mely hálózatokat érhet el.
Lehetőség van a kliensek hálózati korlátozására, ezekben az esetekben a tiltott hálózatokat nem tudják elérni.



Alkalmazott szabványok

Kompatibilis az IEEE802.3 és IEEE802.3u, IEEE 802.1Q szabványokkal,
Hálózati kábel: 100Base-TX UTP EIA/TIA-568 100Ω STP (maximum 100 méter)
Port számok: 3 / 10/100 Mbps auto-negotiation RJ45
Hálózati réteg: IPv4
IEV 195-06-08, IEC 61201, 3. érintésvédelmi osztály (törpefeszültség)

Üzemeltetési körülmények

Üzem típusa: beltéri használatra
Üzemi hőmérséklet: 0 és +40 C között.

Tárolási hőmérséklet: -40 és +70 C között.
Áramellátás: 18V 20Watt DC tápegységgel

Garanciális feltételek

A 49/2003. (VII.30.) GKM rendelet 4.§-ának (1) és (2) bekezdése szerint a garanciális javítási idő nem meghatározott, annak határidejéről tájékoztatni kell a fogyasztót és a forgalmazónak/szerviznek törekednie kell arra, hogy a kijavítást vagy kicserélést legfeljebb tizenöt napon belül elvégezze.

A 10.000.- Ft. azaz tízezer forint bruttó értéket meghaladó, általunk összeállított hardveres konfigurációra, valamint 2003. november 22-től az egyes tartós fogyasztási cikkekre vonatkozó 151/2003 (IX.22.) Kormányrendelet érvényes.

A 151/2003 (IX.22.) Kormányrendelet hatálya alá nem tartozó alkatrészekre és komponensekre az alábbi feltételek szerint vállalunk jótállást.

Általános feltételek:

- A jótállási igényt számlával lehet érvényesíteni a vásárlástól számított 12 hónapig. Kivételt képeznek a saját garanciajeggyel rendelkező, valamint a számlán emelt garanciális időtartammal feltüntetett termékek, amelyekre a garanciajegyen illetve a számlán megjelölt jótállási idő vonatkozik.
- Pénzvisszafizetési garancia időtartama a vásárlástól számított 3 nap.
- A garanciális javításra behozott alkatrészeket csak eredeti csomagolásban, tartozékaival együtt (pl.: driverek, kábelek) áll módunkban átvenni. Az egység azonosító címkéjének (sorozatszám és egyedi azonosító, valamint egyéb zárjegy és matrica) sérülésmentes állapotban kell lennie.
- Ha a vásárolt árucikk meghibásodik, és megfelel a garanciális feltételeknek, akkor azt a vásárló kívánságára azonos típusú új termékre cseréljük, vagy a vételár-különbözet elszámolása mellett más típusú terméket adunk helyette. Amennyiben a meghibásodott alkatrészt, részegységet szervizünk nem tudja ugyanolyanra, vagy korszerűbbre cserélni, abban az esetben vásárlónk élhet a vételár-visszafizetés igényével. Szervizünk nem köteles az eredeti alkatrésznél korszerűbbre, nagyobb teljesítményűre cserélni az alkatrészt, de egyedi elbírálás alapján, a disztribútor jóindulatú együttműködésével általában megoldható a korszerűbbre való csere.
- Konfiguráció esetén a garancia alkatrészenként, csak a hardver hibátlan működésére vonatkozik.
- A garanciajegy (számla) pótlása megoldható. Kivételt képez az a termék, amely külső szerviz által kiadott garancialevéllel volt ellátva. Ezt sajnos nincs módunkban pótolni. Bár a jótállási jegy szabálytalan kiállítás vagy a fogyasztó részére történő átadásának elmaradása nem érinti a jótállási kötelezettségvállalás érvényességét, mégis kérjük, hogy a garanciajegyen feltüntetett adatok meglétét és egyezőségét minden esetben ellenőrizze!
- Olyan termékeknél, melyek saját, gyártói garanciajeggyel rendelkeznek, mindenképp a gyártó által a garanciajegy hátulján megjelölt, a vásárló lakóhelyéhez legközelebb eső szervizben jelentse a meghibásodást.
- A javításra, cserére leadott winchestereken (adathordozókon) tárolt adatok sértetlenségéért és titkosságáért nem vállalunk garanciát.

Nem garanciális okok:

- A termék bárminemű szoftveres illetve hardveres környezetben való, inkompatibilitás (összeférhetetlenség) miatt adódó hibás működése.
- Ventilátorral szerelt alkatrészek (processzor, VGA kártya, stb...) működéséből adódó elhasználódása, porosodás okozta ventilátorhang, ventilátor leállás és ezen okból származó túlmelegedés és / vagy „fagyás”. Ezeknél a hibáknál a szerviz, ha a hiba tisztítással megszüntethető, bruttó 2500 Ft munkadíjat számíthat fel.
- A felhasználó által telepített operációs rendszer hibájából, vagy nem megfelelően végrehajtott telepítésből adódó problémák .
- Abban az esetben ha a garanciális javításra átvett termék a feltüntetett hibát nem produkálja, szervizünk bruttó 1000 Ft munkadíjat kérhet az ügyféltől.
- Jelentéktelen hibának minősül és nem garanciális esemény az észlelt elváltozás, ha a termék használati értékét jelentősen nem csökkenti, használhatóságát nem befolyásolja. Az ilyen esetekben cserére csak méltányosságból, a disztribútor jóindulatú együttműködésével van lehetőség.
- Konfiguráció esetén a garancia alkatrészenként, csak a hardver hibátlan működésére vonatkozik, így a felhasználó által telepített és karbantartott operációs rendszerek / szoftverek okozta hibák nem minősülnek garanciális hibának.

Garanciavesztés okai :

- A termék szállítása vagy üzembe helyezése közben bekövetkező sérülés, a nem megfelelő tárolás.
- A terméken bármilyen mechanikai sérülés (égés , roncsolódás , törés , repedés), akkor is, ha a hiba látszólag nem függ össze a sérüléssel.
- A terméken elemi kár okozta meghibásodás (villámkár , túlfeszültség)
- A terméken szereplő sorozatszám, egyedi azonosító címke, zárjegy, vagy egyéb matrica sérülése , hiánya.
- A termék nem rendeltetésszerű használatából eredő meghibásodások (pl.: az alkatrész gyári beállításainál nagyobb teljesítményen történő használat, helytelen BIOS-, vagy meghajtó program frissítés, szakszerűtlen szerelés, hibás kábelezés okozta meghibásodás. A termékeken illetéktelen és/vagy szakszerűtlen javítási, szerelési próbálkozásra utaló nyomok sérülések. (Javítási munkákat csak a forgalmazó által erre felhatalmazott szakszervizek, szakemberek végezhetnek, amit adott esetben számlával is igazoltatni kell.)

Feltételes garancia:

- A mechanikai sérülés miatt garanciáját veszített alkatrészt cégünk bizonyos esetekben a vásárló kifejezett kérésére visszaküldi felülbírálásra elsősorban a disztribútornak, vagy közvetlenül a gyártónak.
- Mivel a feltételes garanciára átvett termék cseréje/javítása teljes mértékben a disztribútor, ill. a gyártó jóindulatától függ, ezért időtartama előre nem meghatározható, de minimum 90 nap.
- Ha az ügyfél kéri a feltételes garancia ügyintézését, akkor egyben elfogadja a fent felsorolt feltételeket, valamint azt, hogy a disztribútor, vagy a gyártó visszautasíthatja a cserét, vagy javítást és hosszadalmas idő elteltével is csak a sérült terméket kapja vissza.

A jótállás a Ptk. 248. § (1) bekezdése szerint nem érinti a jogosultnak (vásárlónak) a törvényből eredő jogait.

A Fogyasztóvédelmi Főfelügyelőség elérhetősége: 1088 Budapest, József krt. 6. Tel: 06-1 / 459-4800.

A Fővárosi Fogyasztóvédelmi Felügyelőség elérhetősége: 1074 Budapest, Rákóczi út 54.. Tel: 06-1 / 461-0488.

Jótállási jegy

A **Netintegral Consulting Kft.** az általa forgalmazott ngNetSec MultiLayer router serial: ng100-300 hálózati eszközre **12 hónap** jótállást vállal.

Termékmegnevezése: ngNetSec MultiLayer router	Típusa: ng100- 300	Gyári száma:	Vásárlás időpontja, üzlet bélyegzője:
---	-----------------------	--------------	--

Szerviz: Előzetes telefonos vagy E-mail bejelentés után a 1086 Budapest, Dobozi utca 7-9. fsz 6. szám alatt

Jótállási szelvény:

A javítási igény bejelentésének időpontja: A javításra időpontja: A hiba: A javítás módja: A javítás (átadás) időpontja: A jótállás új határideje: Szerviz munkalap száma, aláírás:	A javítási igény bejelentésének időpontja: A javításra időpontja: A hiba: A javítás módja: A javítás (átadás) időpontja: A jótállás új határideje: Szerviz munkalap száma, aláírás:
A javítási igény bejelentésének időpontja: A javításra időpontja: A hiba: A javítás módja: A javítás (átadás) időpontja: A jótállás új határideje: Szerviz munkalap száma, aláírás:	A javítási igény bejelentésének időpontja: A javításra időpontja: A hiba: A javítás módja: A javítás (átadás) időpontja: A jótállás új határideje: Szerviz munkalap száma, aláírás:

