

Otthoni hálózat és kiszolgáló rendszerek - rövid bemutató.

Az otthoni rendszerben a router feladatait egy pfSense (FreeBSD) rendszerű kiszolgáló látja el, amely az integrált Ethernet porton (amely a rendszer wan oldali interface, PoE kapcsolattal) kívül a következő Ethernet kártyákkal rendelkezik:

- 2 darab HP 331T 4x1 Gigabit switch kártya (bridge-be összevonva, a belső vezetékes kliensek számára)
- 1 darab Intel 82574L kártya (a Wifi AP kiszolgálására)
- 1 darab Dual-portos Intel 82576 hálókártya, amely a router oldali LAGG Interface (a hálózatot kiszolgáló szerver típusazonos Ethernet kártyával rendelkezik, párban bonding technológiával javítják a maximálisan elérhető adatátvitel sebességét)

System	pfSense Serial: CZC5361P4L Netgate Device ID: 3cb046be81bc5b1d9819
BIOS	Vendor: Hewlett-Packard Version: L01 v02.75 Release Date: Fri May 4 2018
Version	2.4.4-RELEASE-p3 (amd64) built on Wed May 15 18:53:44 EDT 2019 FreeBSD 11.2-RELEASE-p10 The system is on the latest version. Version information updated at Wed Sep 11 11:06:35 CEST 2019
CPU Type	Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz Current: 800 MHz, Max: 3301 MHz 4 CPUs: 1 package(s) x 4 core(s) AES-NI CPU Crypto: Yes (active)
Hardware crypto	AES-CBC,AES-XTS,AES-GCM,AES-ICM
Kernel PTI	Enabled
Uptime	9 Days 16 Hours 51 Minutes 55 Seconds
Current date/time	Wed Sep 11 11:07:09 CEST 2019

Interfaces			
WAN	↑	Uptime: 2d 16:51:20	185.62.129.146
SW01	✗	none	n/a
SW02	↑	100baseTX <full-duplex>	n/a
SW03	✗	none	n/a
SW04	✗	none	n/a
SW11	✗	none	n/a
SW12	↑	10baseT/UTP <full-duplex>	n/a
SW13	✗	none	n/a
SW14	✗	none	n/a
FEKLANDSERVER_PORT	↑	autoselect	n/a
LANALLPORT	↑		192.168.12.1
WIFI_LAP	↑	1000baseT <full-duplex>	n/a
WIFI_VENDEG	↑	1000baseT <full-duplex>	192.168.13.1

1. ábra Router Dashboard

```

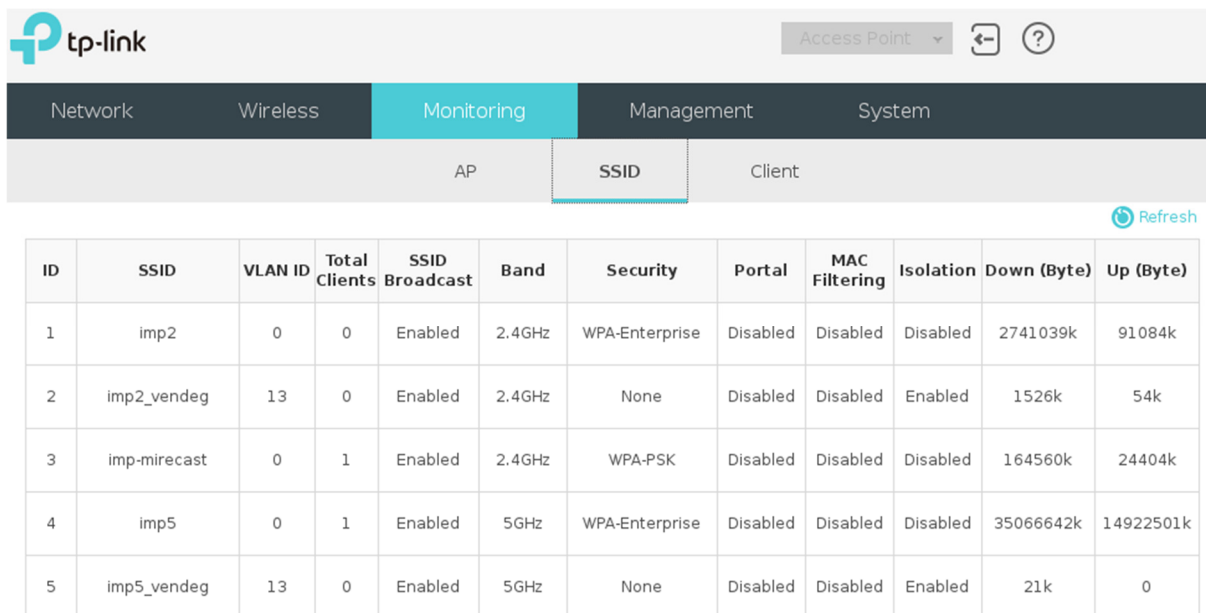
[REDACTED] fekc@fekland: ~ 237x68

syncpeer: 224.0.0.240 maxupd: 128 defer: on
syncok: 1
lagg0: flags=8043<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=8000b<VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWMCSUM,VLAN_HWTSO>
ether 6c:1b:31:1b:f7:d2
inet6 fe80::da9d:67ff:fe2d:1ea1%lagg0 prefixlen 64 scopeid 0x11
nd6 options=21<PERFFORMED, AUTO_LINKLOCAL>
media: Ethernet autoselect
status: active
groups: active
groups: lagg sw local
laggproto lacp lagghash 12,13,14
laggport: 1gb0 flags=3<ACTIVE, COLLECTING, DISTRIBUTING>
laggport: 1gb1 flags=3<ACTIVE, COLLECTING, DISTRIBUTING>
eml13: flags=8043<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
ether 00:1b:23:a9:1c
inet6 fe80::21b:21ff:fe63:a91c%eml13 prefixlen 64 scopeid 0x12
inet 192.168.13.1 netmask 0xfffff0 broadcast 192.168.13.31
nd6 options=21<PERFFORMED, AUTO_LINKLOCAL>
media: Ethernet autoselect (100baseT <full-duplex>)
status: active
vlan: 13 vlancpp: 0 parent interface: eml
groups: vlan
pppoe0: flags=80d1<UP,POINTOPOINT,RUNNING,NOARP,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1492
inet 185.62.129.146 -> 10.0.0.1 netmask 0xfffff0
inet6 fe80::da9d:67ff:fe2d:1ea1%pppoe0 prefixlen 64 scopeid 0x13
inet6 fe80::21b:21ff:fe63:a91c%pppoe0 prefixlen 64 scopeid 0x13
nd6 options=21<PERFFORMED, AUTO_LINKLOCAL>
bridgel: flags=8043<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
ether 02:58:b7:99:ad:01
inet 192.168.12.1 netmask 0xfffff0 broadcast 192.168.12.127
nd6 options=1<PERFORMED>
groups: bridge sw local
id 00:00:00:00:00:00 priority 32768 hellotime 2 fwdldelay 15
maxage 20 holdcnt 0 proto rstp maxaddr 2000 timeout 1200
root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
member: eml flags=143<LEARNING,DISCOVER,AUTOEDGE,AUTOPT>
ifmaxaddr 0 port 6 priority 128 path cost 55
member: lagg0 flags=143<LEARNING,DISCOVER,AUTOEDGE,AUTOPT>
ifmaxaddr 0 port 17 priority 128 path cost 2000000
member: bge7 flags=143<LEARNING,DISCOVER,AUTOEDGE,AUTOPT>
ifmaxaddr 0 port 12 priority 128 path cost 55
member: bge6 flags=143<LEARNING,DISCOVER,AUTOEDGE,AUTOPT>
ifmaxaddr 0 port 11 priority 128 path cost 55
member: bge5 flags=143<LEARNING,DISCOVER,AUTOEDGE,AUTOPT>
ifmaxaddr 0 port 10 priority 128 path cost 55
member: bge4 flags=143<LEARNING,DISCOVER,AUTOEDGE,AUTOPT>
ifmaxaddr 0 port 9 priority 128 path cost 55
member: bge3 flags=143<LEARNING,DISCOVER,AUTOEDGE,AUTOPT>
ifmaxaddr 0 port 4 priority 128 path cost 55
member: bge2 flags=143<LEARNING,DISCOVER,AUTOEDGE,AUTOPT>
ifmaxaddr 0 port 3 priority 128 path cost 55
member: bge1 flags=143<LEARNING,DISCOVER,AUTOEDGE,AUTOPT>
ifmaxaddr 0 port 2 priority 128 path cost 55
member: bge0 flags=143<LEARNING,DISCOVER,AUTOEDGE,AUTOPT>
ifmaxaddr 0 port 1 priority 128 path cost 55
ovpn1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu 1500
options=80000<LINKSTATE>
inet6 fe80::da9d:67ff:fe2d:1ea1%ovpn1 prefixlen 64 scopeid 0x15
inet 192.168.14.1 -> 192.168.14.2 netmask 0xfffff0
nd6 options=21<PERFORMED, AUTO_LINKLOCAL>
groups: tun openvpn
opened by PID 41060
ovpn2: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu 1500
options=80000<LINKSTATE>
inet6 fe80::da9d:67ff:fe2d:1ea1%ovpn2 prefixlen 64 scopeid 0x16
nd6 options=21<PERFORMED, AUTO_LINKLOCAL>
groups: tun openvpn
[2.4.4-RELEASE-p3] [root@fekland:~]

```

2. ábra Router oldali interface lista

A vezeték nélküli klienseket egy TP-Link EAP245 típusú Acces Point szolgálja ki:



The screenshot shows the TP-Link web interface for an Access Point. The 'Monitoring' tab is selected, and the 'SSID' sub-tab is active. A table lists the configured SSIDs with their respective settings.

ID	SSID	VLAN ID	Total Clients	SSID Broadcast	Band	Security	Portal	MAC Filtering	Isolation	Down (Byte)	Up (Byte)
1	imp2	0	0	Enabled	2.4GHz	WPA-Enterprise	Disabled	Disabled	Disabled	2741039k	91084k
2	imp2_vendeg	13	0	Enabled	2.4GHz	None	Disabled	Disabled	Enabled	1526k	54k
3	imp-mirecast	0	1	Enabled	2.4GHz	WPA-PSK	Disabled	Disabled	Disabled	164560k	24404k
4	imp5	0	1	Enabled	5GHz	WPA-Enterprise	Disabled	Disabled	Disabled	35066642k	14922501k
5	imp5_vendeg	13	0	Enabled	5GHz	None	Disabled	Disabled	Enabled	21k	0

3. ábra AP SSID List

A belső felhasználók wifi elérése FreeRadius segítségével, a központi Ldap kiszolgálón felvett felhasználói adatok és a meghatározott csoport tagság alapján történik:



The screenshot shows the 'View FreeRADIUS Configuration Files' interface. The 'ldap' configuration file is selected, displaying the following configuration:

```

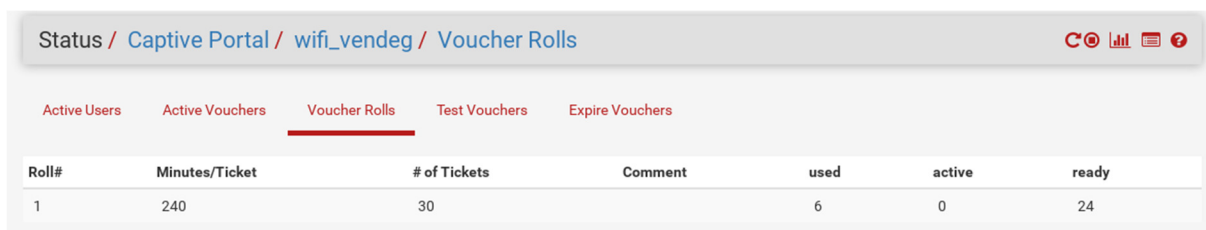
/usr/local/etc/raddb/mods-enabled/ldap
ldap {
    server = "ldap.fekland.dlinkddns.com"
    port = "389"
    identity = "cn=,dc=ldap,dc=fekland,dc=dlinkddns,dc=com"
    password = ' '
    base_dn = "ou=People,dc=ldap,dc=fekland,dc=dlinkddns,dc=com"

    user {
        base_dn = "${..base_dn}"
        filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
        ### access_attr = "dialupAccess" ###
    }
    group {
        base_dn = "${..base_dn}"
        filter = '(objectClass=posixGroup)'
        name_attribute = cn
        membership_filter = "ou=group,dc=ldap,dc=fekland,dc=dlinkddns,dc=com"
        membership_attribute = wifi
        compare_check_items = yes
        do_xlat = yes
        access_attr_used_for_allow = yes
    }
    profile {

```

4. ábra FreeRadius – Ldap

A vendég felhasználók a vezeték nélküli hálózatot az előre generált Voucher kóddal használhatják a hálózatba való bejelentkezés után (elszeparált Vlan-ba érkeznek, a belső szolgáltatásokat és egymást ezek a kliensek nem érik el)





The screenshot shows the 'Voucher Rolls' section of the web interface. It displays a table with voucher roll information.

Roll#	Minutes/Ticket	# of Tickets	Comment	used	active	ready
1	240	30		6	0	24

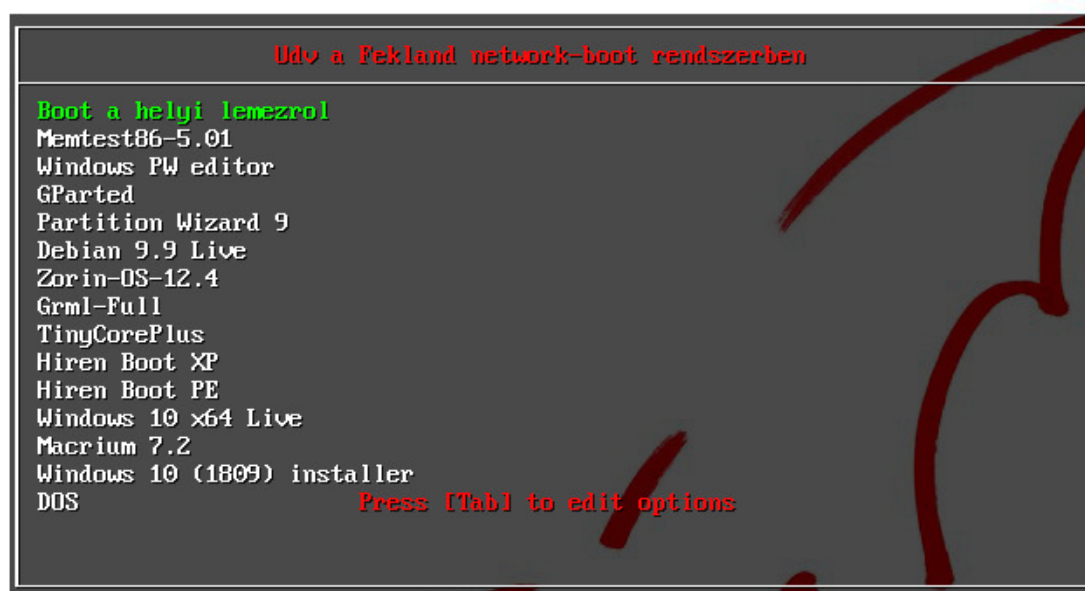
5. ábra guest wifi - voucher

A hálózat külső elérése OpenVPN használatával valósítható meg, amely az előre generált tanúsítványon kívül a felhasználó azonosítását is megköveteli (Ldap-ban rögzített felhasználói név és jelszó, valamint megfelelő csoport tagság szükséges):

VPN / OpenVPN / Servers					
Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export					
OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
WAN	UDP4 / 1194	192.168.14.0/27	Crypto: AES-256-CBC/SHA256 D-H Params: 2048 bits	Fekland VPN (tun)	 

6. ábra OpenVPN

A router ezen kívül PXE kiszolgálóként is működik a lokális hálózaton:



Automatikus indulás 25 másodperc múlva...

7. ábra PXE Menu

A hálózati szolgáltatásokat nyújtó szerver Debian 9.11 (stretch) operációs rendszert futtat, amely a routerrel az 1 darab Dual-port Intel 82576 Gigabit Ethernet hálókártyával kommunikál, mint a server oldali LAGG Interface része:

```

root@fekeland: /home/fekc 237x68

Bonding Mode: IEEE 802.3ad Dynamic link aggregation
Transmit Hash Policy: layer2 (0)
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 200
Down Delay (ms): 200

802.3ad info
LACP rate: slow
Min Links: 0
Aggregator selection policy (ad_select): stable
System priority: 65535
System MAC address: 6c:b3:11:1b:ff:54
Active Aggregator Info:
  Aggregator ID: 1
  Number of ports: 2
  Actor Key: 9
  Partner Key: 555
  Partner Mac Address: 6c:b3:11:1b:f7:d2

Slave Interface: enp3s0f0
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 6c:b3:11:1b:ff:54
Slave queue ID: 0
Aggregator ID: 1
Actor Churn State: none
Partner Churn State: none
Actor Churned Count: 0
Partner Churned Count: 0
details actor lacp pdu:
  system priority: 65535
  system mac address: 6c:b3:11:1b:ff:54
  port key: 9
  port priority: 255
  port number: 1
  port state: 61
details partner lacp pdu:
  system priority: 32768
  system mac address: 6c:b3:11:1b:f7:d2
  oper key: 555
  port priority: 32768
  port number: 8
  port state: 61

Slave Interface: enp3s0f1
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 6c:b3:11:1b:ff:55
Slave queue ID: 0
Aggregator ID: 1
Actor Churn State: none
Partner Churn State: none
Actor Churned Count: 0
Partner Churned Count: 0
details actor lacp pdu:
  system priority: 65535
  system mac address: 6c:b3:11:1b:ff:54
  port key: 9
  port priority: 255
  port number: 2
  port state: 61
details partner lacp pdu:

```

8. ábra server Bond interface

Szerveren futó szolgáltatások összesítése:

- Apache2 a webes eléréshez (a belső rendszereket Reverse Proxy segítségével szolgálja ki)
- APCu (User Cache) + Redis a webes elérések gyorsítására
- Levelező kiszolgáló (Postfix) valamit természetesen SSH szerver is elérhető
- Samba a helyi file megosztás kiszolgálására, OwnCloudX, a webes tárhely kiszolgálására
- Transmission, WordPress blog kiszolgáló
- 1 darab virtualizációban futó Debian 9.11, amely Ldap címtár szolgáltat
- 1 darab virtualizációban futó Ubuntu 16.04, amely a Zimbra levelező rendszert szolgáltatja
- MiniDNLA a helyi hálózat média állományok megosztására

Media library

Audio files	5632
Video files	4529
Image files	12376

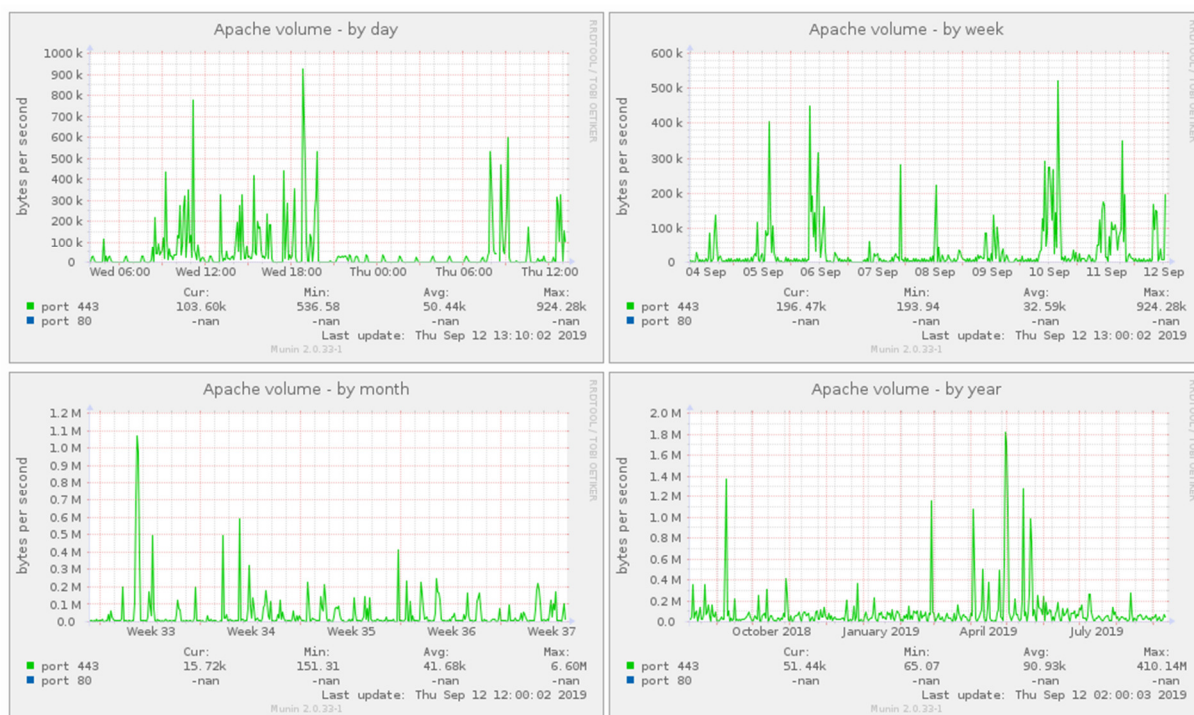
Connected clients

ID	Type	IP Address	HW Address	Connections
0	Generic UPnP 1.0	192.168.12.22	00:24:8C:94:7A:86	0
1	Generic UPnP 1.0	192.168.12.65	00:1C:C0:A3:25:5E	0
2	BubbleUPnP	192.168.12.26	1C:CB:99:EC:FA:2E	0
3	Unknown	127.0.0.1	FF:FF:FF:FF:FF:FF	0

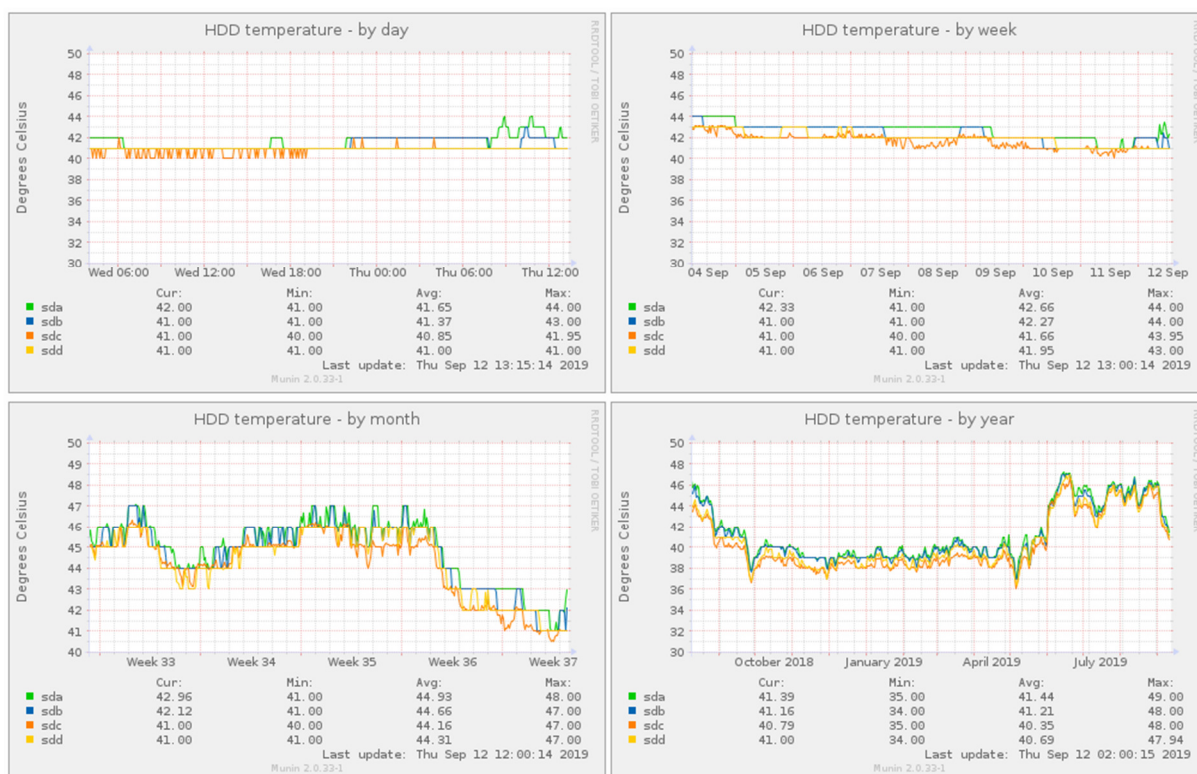
0 connections currently open

9. ábra MiniDNLA státusz

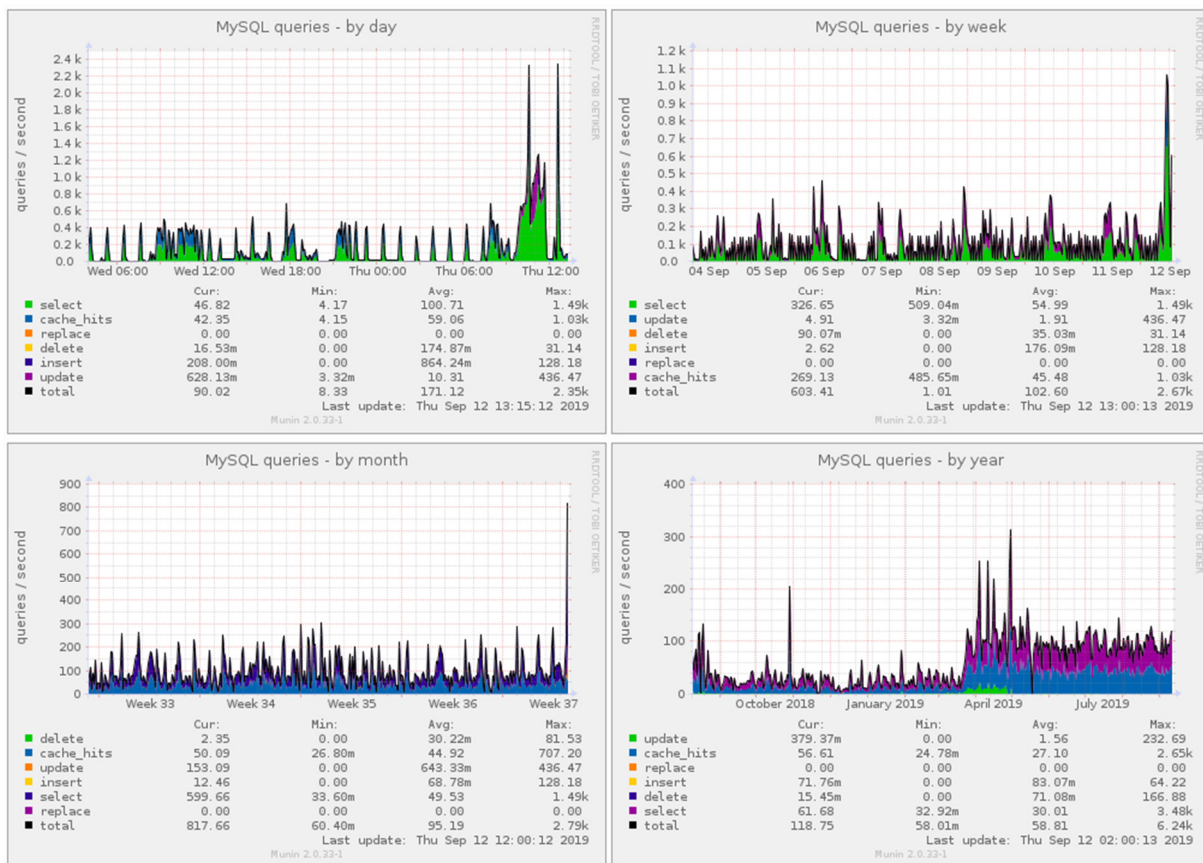
A rendszer monitorozását és a riasztások kezelését Munin felügyeleti szoftver szolgáltatja:



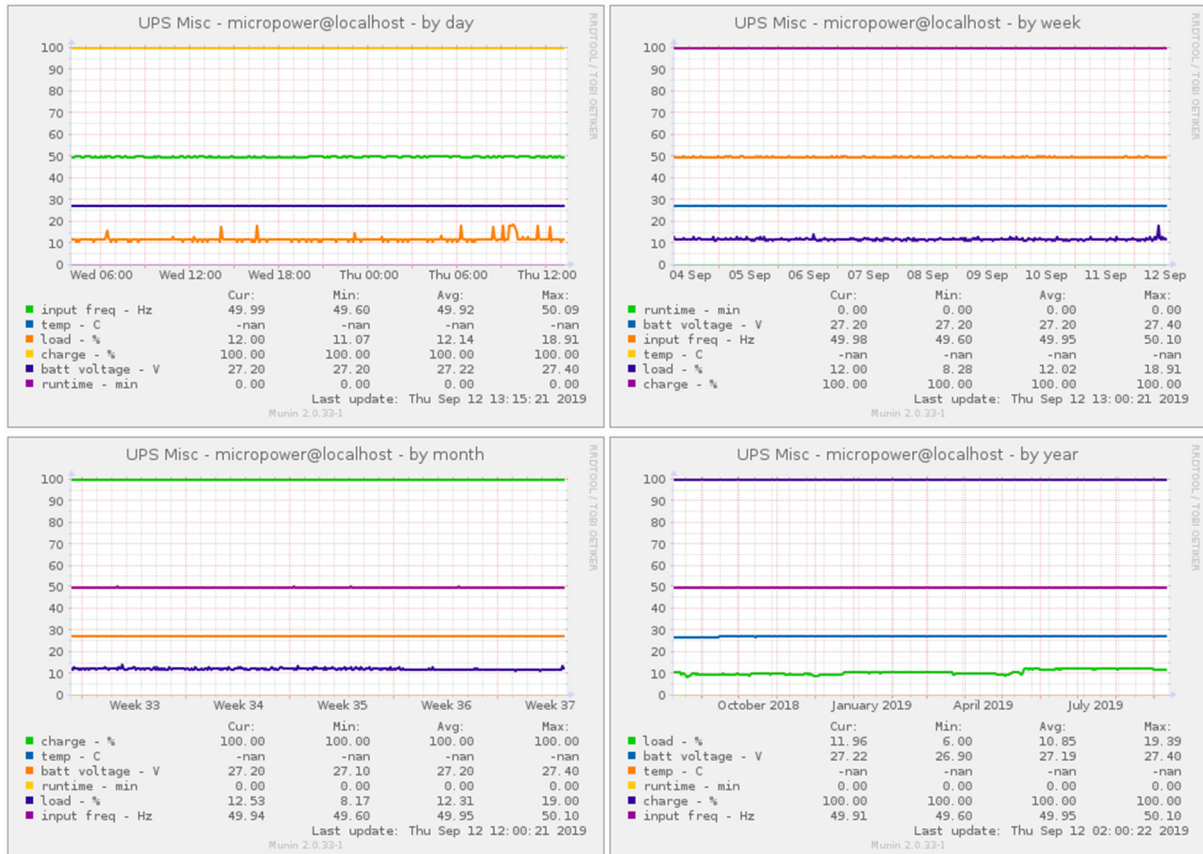
10. ábra Monitor – Apache



11. ábra Monitor - HDD temp



12. ábra Monitor – MySQL



13. ábra Monitor – UPS