A

KözHáló3 – Sulinet Program keretében

az Intézményi végpontok számára nyújtott

Internet

szolgáltatások ismertetése

2009. december 31.
V3.0

TARTALOM

1. Sulinet induló szolgáltatási csomag

Bevezetés

A Sulinet keretében a rendszerbe kapcsolt iskolák teljes körű, nagysebességű Internet hozzáféréshez és emelt szintű szolgáltatásokhoz jutnak. Ezek segítségével a pedagógusok és a diákok egyaránt gyorsan hozzájuthatnak az Internet világában található tengernyi információhoz, elsajátíthatják az Internet használatának eszközrendszerét, az ehhez kapcsolódó kommunikációs alapelveket, jártasságot szerezhetnek az Internet gyakorlati alkalmazásában, akár mint felhasználó, akár mint alkalmazásfejlesztő. A Sulinet rendszer keretében az alábbi szolgáltatásokat juttatjuk el az intézmények részére:

Alapszolgáltatások

- Nagysebességű Internet kapcsolat a magyarországi Internet felhasználókkal a Budapest Internet eXchange (BIX) adatcsere központon keresztül (www.bix.hu).
- Nagysebességű nemzetközi Internet kapcsolat az Internetezők milliárdos nemzetközi táborához.
- A Sulinet rendszer és az Internet eléréséhez szükséges helyi hálózati infrastruktúra és szélessávú távközlései kapcsolat
- Névfeloldó szolgáltatások az Internet világban alkalmazott úgynevezett Internet Protokoll (IP) által értelmezett címek és a hozzájuk rendelt nevek – weblapok, levelezési címek, keresők, multimédia szervizek, stb – összerendelésére.
- Hálózati időszinkronizáció a lokális PC-k és szerverek pontos idő szolgáltatásához
- Az iskolai rendszereket üzemeltető rendszergazdák, adminisztrátorok számára zártkörű levelező rendszer , az úgynevezett @adminmail.sulinet.hu szolgáltatás a gyors és zavarmentes információáramlást elősegítendő
- Webes felület az ügyfélszolgálat eléréséhez. Ezen a felületen keresztül minden intézmény a fax, telefon vagy email helyett egy szabványos formanyomtatvány rendszerrel regisztrálhatja kéréseit a Sulinet ügyfélszolgálata felé, és folyamatosan nyomon követheti az ezzel kapcsolatos intézkedéseket.
- Egyedi weblapos Internetes jelenlét www.iskola.sulinet.hu formában.

- Levéltovábbító **MailRelay szolgáltatás** olyan intézményeknek, amelyek saját maguk rendelkeznek levelező szerverrel, de annak rendelkezésre állása nem kielégítő, illetve annak vírus és spam (kéretlen reklámlevél) elleni védelmét ezzel a szolgáltatással szeretnék biztosítani.
- **Adminisztrátori postafiók** opció az iskolai rendszereket üzemeltető rendszergazdák, adminisztrátorok számára a zártkörű levelezőrendszerben (@adminmail.sulinet.hu)
- Azon intézményeknek, amelyek nem kívánnak saját levelező szervert üzemeltetni, **központi levelezési szolgáltatás** delegált adminisztrációval: az iskolai rendszergazda – aki egyben az adminisztrátori @adminmail.sulinet.hu csoport tagja - az erre dedikált admin@iskola.sulinet.hu postafiók tulajdonosaként egy speciális felületen az @iskola.sulinet.hu domainben létrehozott postafiókokat maga adminisztrálja. A szolgáltatással kötelezően vírusszűrés is jár.
- Azon iskoláknak, amelyek el akarják készíteni saját www.iskola.sulinet.hu weblapjukat és ehhez rendelkeznek programozói kapacitással, olyan **osztott Home Page üzemeltetői**

rendszer, amelyre akár Microsoft akár Linux alapokon dolgozva az egyéni honlap elkészíthető és WebDAV vagy SFTP felületen karbantartható.

1.1. Sulinet Internet elérési szolgáltatás

Az elérési szolgáltatással kapcsolatos további információk az alábbi oldalon érhetőek el:

http://www.kozhaloportal.hu/

Belépéshez a név formátum Txxxxxx, ahol a x-ek helyére a végpont Közháló azonosító kódja kerül, elölről 0 számjegyekkel kiegészítve hat számjegyűre. Az alapértelmezett jelszó az átadáskor kapott „Üzemeltetési paraméterek" dokumentumban található.

1.1.1. A szolgáltatás ismertetése

Az intézmény az elérési szolgáltatás keretében az alábbi al-szolgáltatásokat kapja:

- Távközlési kapcsolat, routerrel, switch-el
- Megfelelő sávszélességű, időben és havi forgalomban nem korlátozott Internet (IP) elérés
- 10/100 Mbps Ethernet switch 25 darab szabadon felhasználható interfésszel, DHCP támogatással, lokális hálózat kialakításhoz
- Tűzfal védelem, több különféle védelmi szintű szegmens kialakítási lehetőséggel (pl. nyilvános szerverek, munkaállomások)
- 5 regisztrált (publikus) IP cím Internet szerverek üzemeltetésére és egy privát IP címtartomány az intézmény gépei számára, amelyeket központilag adminisztrálunk
- NTP time szerverek idő szinkronizációhoz
- Falra szerelhető és zárható szekrényben elhelyezett eszközök
- 24 órás ügyfélszolgálat

1.1.2. A szolgáltatás igénybe vétele

A Sulinet Internet elérési szolgáltatás keretében az intézmény zárható és falra szerelt szekrényben elhelyezett 24+2 portos Ethernet switch-et, és tűzfal szolgáltatással integrált routert kap. A rack szekrényben kerülnek elhelyezésre továbbá a távközlési kapcsolatért felelős eszközök is (szolgáltatói végberendezés). Az intézmény által üzemeltetett hálózati eszközöket (PC munkaállomások, szerverek, nyomtatók, további intézményi switch) az intézmény saját UTP (Cat-5) patch kábelei segítségével a Sulinet Ethernet switch megfelelő portjaira kötheti be.

A switch-re 10Base-T vagy 10/100Base-TX interfésszel rendelkező eszközök kapcsolhatók. A két további Gigabit Ethernet port 10/100/1000Base-TX eszközöket is fogadhat. Minden switch interfész automatikusan felismeri a rá kapcsolt eszköz által támogatott sebességet és duplexitást. Ha mégsem sikerülne felismerni az eszköz oldali beállításokat, eltérő módba kerülhet a switch és a rá kapcsolt eszköz interfésze, ami drasztikus sebesség csökkenést, esetleg teljes kapcsolat szakadást eredményez. Ennek kiküszöbölésére a port szám

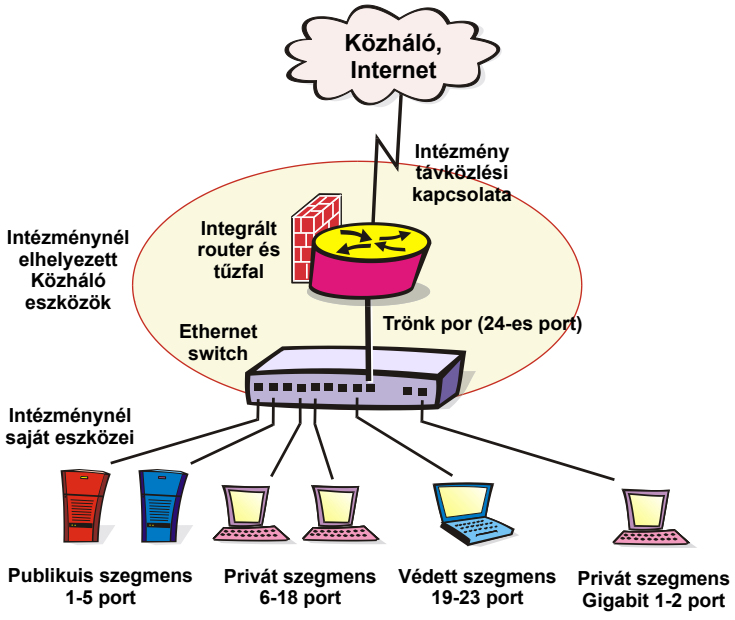
egyértelmű megjelölése mellett kérheti intézmény egyedi switch portokon az „auto negotiation” funkció kikapcsolását, és a port végleges beállítását 10-Half, 100-Half, vagy 100-Full módok egyikére.

További saját hub vagy switch összekapcsolása is megengedett Sulinet switch-el, ez esetben azonban un. fordítós patch kábelt kell alkalmazni, vagy a saját switch uplink (általában MDIX feliratú) interfészét kell használni.

Minden végponton három eltérő védelmet igénylő szegmens került kialakításra, mely szegmensek megfelelő switch portokon keresztül érhetők el:

- Publikus szegmens: ide célszerű elhelyezni a közvetlen nyilvános szolgáltatásokat nyújtó szervereket, mint pl. az intézményi web vagy levelező szervert.
- Privát szegmens: ez felhasználói munkaállomások, nyomtatók, belső intézményi szerverek (pl. file szerver) szegmense.
- Védett szegmens: olyan kiemelt munkaállomásokat célszerű ide helyezni, melyek a másik két szegmens felől is védelmet igényelnek. Szintén erről a szegmensről lehet a Tanár VPN központi szolgáltatásait is elérni.

Az átadások érvényes port kiosztást az alábbi ábra mutatja. Amennyiben ez nem megfelelő, vagyis valamelyik szegmensben több eszköz bekötése szükséges míg egy másikban kevesebb is elegendő, az intézmény kérheti egyes portok átkonfigurálását egyik szegmensből a másikba.



1. Ábra: Végpont fizikai kialakítása

A Privát és a Védett szegmensben a router DHCP (Dynamic Host Configuration Protocol) szolgáltatást nyújt, melyet javasolt igénybe venni. A DHCP segítségével a munkaállomások bekapcsoláskor automatikusan megkapják a hálózat eléréséhez szükséges beállításokat. A Publikus szegmensben DHCP szolgáltatást nem biztosítunk, mivel ide tipikusan fix hálózati

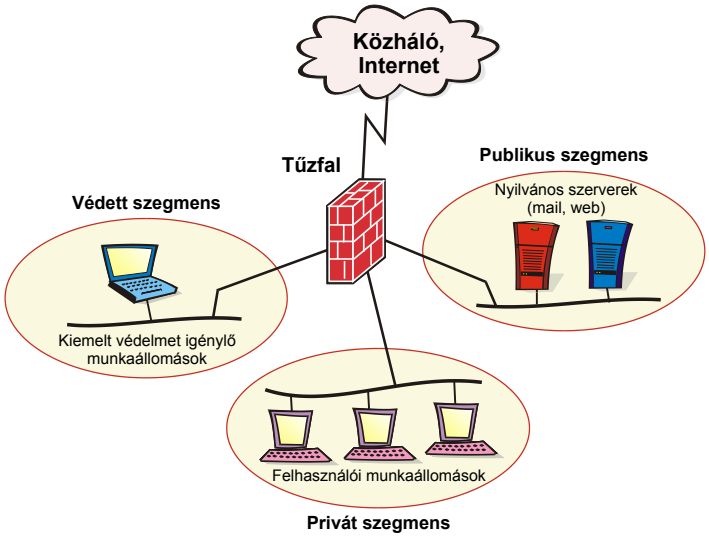
beállításokkal rendelkező szerverek kerülnek. A DHCP a Privát és Védett szegmenshez központilag rendelt teljes címtartományból oszt dinamikusan címeket. Ezen túl megadja a router IP címét, a két központi Sulinet DNS resolver szerver címét (195.199.255.4, 195.199.255.57), valamint az alapértelmezett intézményi domain nevet (intezmeny.sulinet.hu).

A DHCP szolgáltatás igénybe vételéhez a munkaállomásokat be kell állítani, hogy automatikusan állapítsák meg IP címüket, az alapértelmezett gateway címét, valamint a DNS szerverek címeit.

Az intézmény kérheti a DHCP szolgáltatás kikapcsolását az egyes szegmenseken, amennyiben a végpont telepítésekor már belső hálózatán rendelkezik DHCP szerverrel. Szintén ki kell kapcsoltatni a DHCP szolgáltatást és fix IP cím beállítást vagy saját DHCP szervert kell alkalmazni, ha

- az intézmény felváltva akar az egyik szegmensen dinamikus és fix beállítású (pl. nyomtatók, szerverek) eszközöket használni,
- az alapértelmezettől eltérő paramétereket (pl. saját DNS szerver használata) szeretne a munkaállomásokon beállítani,
- az alapértelmezetten túli paramétereket (pl. WINS szerver) szeretne a munkaállomásokon beállítani.

Az egy szegmensen belüli eszközök egymással szűrés nélkül kommunikálhatnak, míg a szegmensek közötti forgalom minden esetben a routerbe integrált tűzfalon folyik keresztül. A következő ábrán ez a logikai kapcsolat látszik.



2. Ábra: Végpont logikai kialakítása

Az egyes szegmensek tulajdonságait az alábbi pontokban foglalhatjuk össze.

Publikus szegmens

- Interneten regisztrált (publikus) címtartományt használ, mely segítségével legfeljebb 5 eszköz kaphat a teljes Interneten egyedi azonosításra alkalmas IP címet.

- Mind az Internet mind a másik két szegmens felé címfordítás nélkül kommunikálhat.
- Tetszőleges kapcsolatot építhet fel a Privát szegmens felé. A Védett szegmens felé minden kapcsolat tiltott.
- Az Internet felé néhány security jellegű tiltást leszámítva kezdeményezhet kapcsolatot. Ez alól kivétel a vírusok és backdoor programok által előszeretettel használt portok, valamint az SMTP port. Ez utóbbi bár tiltva van az Internet felé, a központi levelező szerverek felé nem, így azok használatát nem korlátozza. Ha pedig az intézmény saját relay szervert szeretne üzemeltetni, a megfelelő Open Relay tesztek sikeres lefutása után a Publikus szegmens ezen IP címére vonatkozóan az SMTP portot szabaddá lehet tenni az Internet felé és felől.
- Korlátozás nélkül elérhető a Védett és a Privát szegmens felől.
- Az Internet felől a kezdeti beállítások szerint nem lehet rá csatlakozni. Ez az egy tűzfal szabály azonban módosítható az Intézmény kérésére. Tipikusan intézményi WEB szerver vagy levelező szerver telepítésekor kell a megfelelő kapcsolatokat (portokat) a felkonfigurált szerver felé engedélyeztetni. Ezen túl lehetőség van további portok, vagy éppen tetszőleges forgalom beengedésére is. Azonban minden esetben, ha a tűzfal szabályok enyhítése történik, azt szolgáltatói hálózatbiztonsági tesztek előzik meg, hogy a végpont és a teljes Sulinet hálózat védelme megfelelő szinten tartható legyen. Ha a szolgáltató a módosítás előtti, vagy a később is rendszeresen futtatott tesztek során beállítási hibát érzékel (pl. Open Relay, Open Proxy), megtagadhatja a tűzfal szabályok módosítását, vagy visszavonhat régebbi módosításokat a hiba kijavításáig.

Privát szegmens

- 253 munkaállomás csatlakoztatására alkalmas privát IP címtartománnyal rendelkezik. Mivel a privát címek sok más magánhálózaton is előfordulhatnak, ezen címek az Interneten nem jelenhetnek meg.
- Címfordítás nélkül kommunikálhat a Publikus és Védett szegmensekkel. Az Internet felé történő kommunikáció során címfordítás (NAT – Network Address Translation, vagy még pontosabban PAT – Port-Address Translation) történik, melynek során tetszőleges munkaállomásról indított kapcsolat esetében az intézményi router nyilvános címének (gw.intezmeny.kozhalo.hu mögötti cím) felhasználásával fog a kapcsolat felépülni.
- A Publikus szegmens felé tetszőleges kapcsolatot felépíthet. Az Internet felé néhány security jellegű tiltást leszámítva kezdeményezhet kapcsolatot. Ez alól kivétel a vírusok és backdoor programok által előszeretettel használt portok, valamint az SMTP port. Ez utóbbi bár tiltva van az Internet felé, a központi levelező szerverek felé nem, így azok használatát nem korlátozza. A Védett szegmens irányában minden tiltott.
- A Publikus és a Védett szegmens felől elérhető. Az Internet felől azonban nem lehet az itteni munkaállomások felé kapcsolatot felépíteni.

Védett szegmens

- 29 munkaállomás csatlakoztatására alkalmas privát IP címtartománnyal rendelkezik.
- Címfordítás nélkül kommunikálhat a Publikus és Privát szegmensekkel. Az Internet felé történő kommunikáció során címfordítás történik, melynek során tetszőleges munkaállomásról indított kapcsolat esetében az intézményi router nyilvános címének felhasználásával fog a kapcsolat felépülni.
- A Privát szegmens és a Publikus szegmens felé tetszőleges kapcsolatot felépíthet. Az Internet felé néhány security jellegű tiltást leszámítva kezdeményezhet kapcsolatot. Ez alól kivétel a vírusok és backdoor programok által előszeretettel használt portok, valamint az SMTP port. Ez utóbbi bár tiltva van az Internet felé, a központi levelező

szerverek felé nem, így azok használatát nem korlátozza.
- Egyik másik szegmens felől sem érhető el, vagyis nem kezdeményezhető rá befelé kapcsolat.
- Titkosított kapcsolaton korlátozás nélkül eléri a központi Tanár VPN szolgáltatásokat.

Bizonyos alkalmazások esetében (pl. FTP letöltés, Real Audio alapú rádióműsorok hallgatása) szükség lehet olyan kapcsolatok felépítésére, melyeket a fenti szabályok nem engednének át. Ez esetben a tűzfal a megfelelő vizsgálatok után külön beállítás nélkül is beengedi a jól definiált válasz kapcsolatokat.

A fenti szabályok kiegészítéseként, az Internet felé történő kilépési ponton további szűrések lépnek érvénybe, melyek egységesek minden intézményre, intézmény által nem módosíthatóak, de változhatnak az idők során a naprakész védelem érdekében. Ezek tipikusan:
- intézmény csak a számára regisztrált címekről küldhet ki csomagot,
- intézményi forrás címmel csomag nem jöhet be Internet felől,
- privát címekre szóló csomagok nem juthatnak ki az Internetre,
- privát címekről érkező csomagok nem juthatnak be intézményi szerverekre,

- Biztonsági problémát okozó portok (tipikusan az alap installációk után védtelenül maradó portok), és vírus fertőzések következményeként keletkezett backdoor (hátsó kiskapu) portok tiltva vannak Internet felé és felől. A Sulinet üzemeltetése során fenntartjuk a jogot arra, hogy vírusveszély vagy más aktuális támadási veszély felmerülése esetén azonnali szigorításokat vezethessünk be.

  A jelenlegi tiltólista:
  - tcp/udp/7 echo
  - tcp/udp/9 discard
  - tcp/udp/12 daytime
  - tcp/udp/19 chargen
  - tcp/23 telnet (csak befelé tiltott)
  - udp/69 tftp
  - tcp/udp/111 sunrpc
  - udp/161 snmp
  - tcp/135 dcom-rpc
  - udp/137 netbios-ns
  - tcp/udp/138 netbios-dgm
  - tcp/139 netbios-ssn
  - tcp/udp/369 rpc
  - tcp/445 smb-over-tcp
  - tcp/512 rexec
  - tcp/513 rlogin
  - tcp/udp/515 printer
  - tcp/593 http-rpc-epmap
  - tcp/udp/631 ipp
  - tcp/901 samba web admin
  - tcp/1080 socks
  - tcp/1433-1434 ms sql monitor
  - tcp/3127-3128 http proxy
  - tcp/3389 remote desktop *(csak befelé tiltott)*
  - tcp/4899 radmin

- tcp/5000 upnp
- tcp/6658 http proxy
- tcp/6660-6670 irc *(csak befelé tiltott)*
- tcp/6000-6063 xlogin *(csak befelé tiltott)*
- tcp/8000-8001 http proxy
- tcp/8080 http proxy
- tcp/8888 http proxy

Illetve a backdoor portok:

- tcp/4444 blaster worm
- tcp/6129 damware
- tcp/6777 bagle
- tcp/9898 crashcool
- tcp/10080 mydoom
- tcp/12345 netbus
- tcp/17300 kuang2
- tcp/20168 lovgate
- tcp/27374 subseven

Az Internet elérési szolgáltatás keretében lehetőség van a szerverek és munkaállomások óráinak pontos szinkronban tartására. Ez a szolgáltatás NTP (version 3) protokoll segítségével biztosított. A közháló NTP szervereinek elérhetősége:

ntp.sulinet.hu, ntp1.sulinet.hu és ntp2.sulinet.hu

NTP idő szinkronizációt közvetlenül támogatnak a Linux rendszerek, valamint a Windows XP munkaállomások. Windows XP esetében a fenti szerver neveket a jobb alsó sarokban található digitális órára kattintva lehet megadni. Linux rendszereken az ntpdate parancs rendszeres futtatásával. Ezen túl számos ingyenes (freeware) és fizetős (shareware) termék elérhető a legkülönfélébb operációs rendszerek idejének pontos beállítására.

1.2. Sulinet DNS alapszolgáltatások

1.2.1. A szolgáltatás ismertetése

A DNS rendszer az Internetben hasonló szerepet játszik, mint a telefonszámrendszer a telefonos kommunikációban.

Az Internet világában az eszközöket a telefonhoz hasonlóan egy egyedi számmal, az úgynevezett Internet Protokoll (IPv4) címmel azonosítják. Az IPv4 protokoll cím formailag négy, egyenként 0 és 255 között értékek között értelmezett mezőből áll, amelyeket pontokkal választunk el egymástól, például az Index.hu internetes újság IP címe, amelyre a www.index.hu névvel szoktunk hivatkozni a 212.20.131.2.

Egyszerű analógiával arra gondolhatunk, hogy a telefonszámok világában használatos nemzetközi, ország és körzetszám után található meg a helyi számon a megadott néven regisztrált előfizető. Nos, a DNS ehhez nagyon hasonlóan működik. És ahogyan a mobiltelefonnál megszokott a ROAMing, úgy a DNS szerviz is hatékonyan és gyorsan követi

a címek változásait.

Könnyen kiszámíthatjuk, hogy összesen 256 a negyedik hatványon, azaz 4294967296 lehetséges Internet cím létezik. A valóságban azonban a ténylegesen használható címek száma ennél kevesebb, kétmilliárd körül van. Ez a szám az Internet kialakításának kezdetén elegendőnek tűnt – mára azonban, a számítógépek rohamos elterjedése következtében kevésnek bizonyul. Spórolnunk kell vele, mint minden természeti kinccsel. Ezért a Sulinetben is az egyes intézmények részére egységesen 5 IP cím használata engedélyezett.

Az IP címzéseknél megszokott, hogy több címet a megfelelő cím helyi értékek X-el történő helyettesítésével jelölünk. Igy pl. a 212.20.131.XXX összesen 256 címet jelöl, amelyek közös tulajdonsága, hogy mindannyian a 212.20.131 számsorozattal kezdődnek. Ezt a címtartományt C osztálynak, az első három címjegyek hálózati, az utolsó címjegyet pedig lokális címnek szokásos nevezni.

A Sulinet a teljes 195.199.xxx.xxx címtartományt jelenti, összesen mintegy 64 ezer címmel.

Az Interneten rendkívüli dinamikával, percről percre változik az IP címek kiosztása. A DNS rendszer az a telefonkönyv rendszer, amely ezt követni és elosztani képes. A rendszer folyamatos összerendelést végez a nevek és az IP címek között. Ha egy név mögötti IP címre vagyunk kíváncsiak, akkor címlekérdezést, ha az IP címen lévő névre (vagy nevekre) vagyunk kíváncsiak, akkor reverse (fordított) lekérdezést kell végrehajtani.

A DNS működését tekintve tehát egy online adatbázis, mely egy adminisztrációs (autoritativ) és egy lekérdező (resolver) részből áll.

a. Autoritatív (felelős) DNS szolgáltatás

Ezt elsősorban az internetes domain regisztrációt intéző ISP munkatársai adminisztrálják, de lehetőség van arra is, hogy az iskola informatikáért felelős személye(i) is hozzáférést kapjanak, és igényeiknek megfelelően alakítsák az intézmény domain adatait.

Az ADNS szervereket praktikusan csak a Sulineten kívüli szerverek keresik meg, hogy a Sulinetes címeket lekérdezzék.

b. Resolver DNS névfeloldás

A számítógépek kommunikáció közben ezeket a szervereket használják internetes dns név feloldáskor. A Sulinetes felhasználóknak is ezekkel a szerverekkel kell dolgozniuk, mivel ezek a szerverek képesek rekurzióra, azaz a világhálón lévő DNS adatbázis lekérdezésére egy ismeretlen név megtalálása érdekében.

1.2.2. A szolgáltatás igénybevétele

a. Resolver DNS (saját intézményi számítógépen)

.Windows munkaállomások esetében a
„ számítógép hálózati beállítások -> TCP/IP -> DNS beállítások”

alatt lehet megadni a használni kívánt dns szervereket.

Elsődlegesen használt resolvernek az alábbi listából mindig a DNS1 címet, másodlagos resolvernek a DNS2 és DNS3 közül az egyiket kell beállítani:

DNS1: 195.199.255.4
DNS2: 195.199.255.57
DNS3: 195.199.255.58

A DNS resolver szervert az iskolai NAT mögötti szegmensekben alkalmazott DHCP szerver automatikusan beállítja.

b. Autoritatív DNS (intézményi domain-ek, hoszt-nevek, web lapok elérhetősége a világban)

A Sulinet ADNS szerveri az **ns.sulinet.hu** és **ns1.sulinet.hu** néven elérhetőek.
Ezzel a felhasználónak elvben semmi teendője nincs, csak akkor, ha a zónába bejegyzést akar eszközölni.

A webes adminisztrációs felülethez a hozzáférést előzetesen igényelni kell, az http://igenyles.sulinet.hu címe.

Web admin (ZonaTool) címe: http://webdns.sulinet.hu. Ha az ügyfélszolgálat a hozzáférést engedélyezte, a 2.7. fejeztében leírt felületen és korlátozások mellet a zóna adminisztrálható.

Rendszer adminisztrátoroknak:

Alapértelmezett zóna tartalom:

Minden (régi és újonnan bekötött) intézmény fix, egységesen előre definiált zónát kap induláskor. Ennek tartalma:

SOA rekord:
Admin mail: ISP admin postafiókra mutat
Serial: ISP által elfogadott módon, tipikusan a létrehozás/módosítás dátumából lehet származtatni
Timer változók:
3600 ; Refresh
3600 ; Retry
2592000 ; Expire
3600 ; Minimum

NS rekordok:
két Közháló Sulinet DNS szerverre mutatnak
MX rekord:

@ 10 → szerver1
* 10 → szerver1

A rekordok:
szerver1→ IP1
szerver2→ IP2
szerver3→ IP3
szerver4→ IP4
szerver5→ IP5
gw → IP6
@ → 195.199.255.66 ; alapszintű www szolgáltatás címei
@ → 195.199.255.67 ; alapszintű www szolgáltatás címei

CNAME rekordok:
www → Alapszintű WEB jelenlét szolgáltatás szerverre
ftp → szerver1
mail → szerver1

Valamint az intézményi címeket magába foglaló reverse zónába kerülő PTR bejegyzések:
IP1 → szerver1.intezmeny.sulinet.hu
IP2 → szerver2.intezmeny.sulinet.hu
IP3 → szerver3.intezmeny.sulinet.hu
IP4 → szerver4.intezmeny.sulinet.hu
IP5 → szerver5.intezmeny.sulinet.hu
IP6 → gw.intezmeny.sulinet.hu

1.3. Sulinet Adminisztrátori postafiók szolgáltatás

1.3.1. A szolgáltatás ismertetése

Internetes postafiók elsősorban az intézmény rendszergazdája és/vagy informatikai rendszert karbantartó személy(ek) részére. A postafiók tetszés szerint elérhető SuliNet-en belül, de biztonságtechnikai okok miatt más adminok postafiókjába csak admin e-mail címről és smtp-n keresztül csak hálózaton belülről írhat az intézményi rendszergazda. Természetesen webmail-en keresztül ez a postafiók bármely Internettel rendelkező helyről elérhető így naprakészen nyomon követhetőek az iskola rendszerével kapcsolatos események.

A rendszer csak 20Mbyte mérethatárnál kisebb leveleket továbbít.

1.3.2. A szolgáltatás igénybevétele

Igénybe vehető postafiókok száma: 2 db. (max)

Megjegyzés: ha további postafiókokra van szükség, akkor ezzel kapcsolatosan a SuliNet WebMail menüpont alatt találhatnak hasznos információkat.

Az admin postafiókot Web böngészővel és levelező kliens-el lehet elérni

Admin WebMail:

- URL: http://adminmail.sulinet.hu/
- URL2 (biztoságos): https://adminmail.sulinet.hu/

Levelező kliens beállítások:

- Név: [használó neve] vagy [intézmény neve]
- Email cím: s[végponti azonosító]@adminmail.sulinet.hu
- Felhasználónév: s[végponti azonosító]@adminmail.sulinet.hu
- Jelszó: [jelszó]
- Bejövő levelek kiszolgálója portoktól függetlenül az adminmail.sulinet.hu szerver:
  - Pop3: adminmail.sulinet.hu
  - Pop3s (biztonságos): adminmail.sulinet.hu
  - Imap: adminmail.sulinet.hu
  - Imaps (biztonságos): adminmail.sulinet.hu
- Kimenő levelek kiszolgálója (smtp): emailsmtp.sulinet.hu

Imap/Imaps alapú kapcsolódás esetén a levelek a szerveren maradnak, így bárhonnan könnyen elérhetőek leveleink és levelezési mappáink.

Megj: időszakosan javasolt az így tárolt leveleinket, illetve régi (1-2 hónapos) leveleinket helyi mappákba lementeni (archiválni).

Az admin postafiókok zárt levelezésként működnek. Ez azt jelenti, hogy ebbe a postafiókba csak más intézmény adminjai és a szolgáltatásban résztvevők írhatnak levelet. Webes bejelentkezés esetén további adminisztratív funkciók is elérhetők: jelszómódosítás, vakáció üzenet, naptár (ezzel kapcsolatosan részletesebb információk a SuliNet WebMail fejezetben találhatók). A zárt rendszer minden kívülről érkező levelet elutasít, kivéve az alábbi, a Sulinet részének is tekintett domaineket:

@.sulinet.hu
*@sulinet.hu

*@netvisor.hu

uszi@kozhaloportal.hu [Közháló Ügyfélszolgálat]

1.4. Webes ügyfélszolgálati felület

Ezen a felületen az intézményi adminisztrátorok kapcsolatot tarthatnak az ügyfélszolgálattal.

1.4.1. A felhasználók bejelentkezése

A **http:// forms.sulinet.hu** felületen be kell jelentkezni a rendszer használathoz. A bejelentkezéshez az adminisztrációs postafiók címét és a hozzá tartozó jelszót kell használni.
Az iskolák felhasználóinak autentikációs adatait LDAP-ból veszi a rendszer

1.4.2. Az iskolák felhasználóinak felülete

Az iskolák felhasználói bejelentkezés után listázhatják régebbi kéréseiket, a kérés típusától függően, a megfelelő menüpontra kattintva. Itt megnézhetik, hogy a feldolgozás mely szakaszában tart. Illetve esetlegesen kiegészíthetik extra információkkal, amennyiben az adminisztrátorok ezt kérték. Az iskolák felhasználói itt még megtekinthetik egy összesített listában az összes kérésüket. (*Kérelmek* menüpont) Új kérelem felvétele után a *Kérelmez* gombra kattintva kerül át a kérelem a Közháló Ügyfélszolgálathoz. Ezután az iskola a kérelmet már nem tudja módosítani.

1.5. Sulinet Mail Relay szolgáltatás

1.5.1. A szolgáltatás ismertetése

A Mail Relay szolgáltatás egy olyan átmeneti levéltárolási funkció amely a hagyományos értelemben a postán maradó (Poste Restante) levélküldésnek felel meg, de ennél jóval többet tud. A Mail Relay jelentősége abban áll, hogy az általa kiszolgált levelező szervereket védi a támadásoktól, és egyben tehermentesíti a forgalomtól. Használata mellett a relay ügyfelek szerverei kevésbé védett konfigurációban, kisebb hardver teljesítménnyel, gyenge rendelkezésre állás mellett is képesek levelező felhasználóik hatékony kiszolgálására. A Mail Relay főbb funkciói:

Levélfogadás

- A nagyvilágból beérkező leveleket fogadja, és ha lehet, azonnal továbbítja a cél felé. Ha valamilyen okból – ami lehet átmeneti túlterhelés, karbantartás vagy éppen áramkimaradás is – a címzett számítógép nem elérhető, a relay rendszer átveszi és meghatározott ideig – általában maximum 3 napig - tárolja az érkező leveleket mindaddig, amíg a címzett újra működőképes nem lesz, és ilyenkor a levelet azonnal kézbesíti felé. Ha a címzett folyamatosan elérhetetlen, visszajelez a feladó részére a problémáról.

- A beérkező leveleket a rendszer vírusmentesíti, illetve amennyiben ezt nem képes megtenni, törli.
- Az ismert reklámforrások felől érkező kéretlen leveleket kiszűri.
- A mögötte levő szervereket megvédi a biztonsági réseket kihasználó támadások ellen

Levélküldés

- A kézbesítendő levelet azonnal átveszi, és gondoskodik annak célba juttatásáról. Ezzel tehermentesíti a küldőt a célállomás elérhetetlensége vagy a sok címzettel rendelkező körlevelek ismétlődő kiküldése okozta forgalmi terheléstől.
- A kézbesítendő leveleket vírusmentesíti.
- Visszajelzés ad, ha egy küldeményt a megadott időn belül nem képes kézbesíteni.

A levélfogadást a DNS rendszer MX rekordja segítségével lehet átirányítani a központi Mail Relay rendszerre, ugyanis a zóna MX rekordja adja meg a külvilág számára az alkalmazott levelezőszerver nevét. A levélküldést a Mail Relay szerver levelezésre használt úgynevezett smtp portjaira kell beállítani. Mind az MX mind az smtp funkcióban redundáns szerverkapacitás áll rendelkezésre, ami azt jelenti, hogy a DNS-ben két IP címmel lehet a szolgáltatásokat elérni.

A rendszer csak a 20Mbyte méretkorlátnál kisebb leveleket továbbítja.

1.5.2. A szolgáltatás igénybevétele

A Szolgáltatás igénybevételének szándékát az ügyfélszolgálaton kell jelezni Mail Relay igénylési formanyomtatványon. Az egyetlen szükséges paraméter az intézményi levelező szerver címének és nevének megadása. A szolgáltatás védelmi jellegéből adódóan vírusszűrést végez, tehát a szolgáltatás igénylés során jelezni kell, ha az igénylő vírusvédelmet nem kér. Ennek jelzésére a szolgáltatásigénylő lapon biztosítunk lehetőséget.

Fentiek alapján az Internet szolgáltató elvégzi az alábbi műveleteket:

- Beállítja, hogy az Intézmény részére érkező leveleket a Relay rendszer fogadja és továbbítsa
- Beállítja a kézbesítési gondok esetén a maximális levél tárolási időt 3 napra.
- Beállítja a spam (kéretlen reklámlevél) szűrést
- Letiltja a vírusszűrést, amennyiben ezt az igénylő nem kéri
- Amennyiben az intézményi levelező szerver zónájában karbantartási joggal rendelkezik, beállítja a zóna MX rekordját: **két azonos súlyú MX rekordot vesz fel a relay1.sulinet.hu és relay2.sulinethu nevekkel**

A megrendelő egyetlen feladata, hogy a saját levelező rendszerében a levélküldés kimenő irányát meghatározó úgynevezett Smart Host (Esetleg SMTP vagy Mail Gateway) néven ismert funkciót beállítsa a Mail Relay rendszerre. Itt a beállításnál az **smtp.sulinet.hu** nevet kell beállítani, amit a DNS rendszer redundánsan két IP címre, a **195.199.255.35** és **195.199.255.36** címekre fog feloldani. Ha a rendszer olyan, hogy nevet nem, de IP címeket elfogad, akkor ezt a két IP-t kell beállítani (ha csak egy cím megadására van

lehetőség, akkor mindegy, melyik címet választjuk).

Ha az intézmény a zónáját maga adminisztrálja, akkor természetesen a megfelelő MX rekordokat (relay1.sulinet.hu és relay2.sulinethu) szigorúan azonos súlyozással fel kell vegye a zónában.

A zónatartalmak módosítását követően legkésőbb három napon belül érdemes a levélfogadást az intézményi szerveren a **relay1.sulinet.hu és relay2.sulinet.hu** felől érkező SMTP kérésekre korlátozni, ezek a **195.199.255.33** és **195.199.255.34** címeket jelentik. Amennyiben ugyanis az intézményi szerveren ezt a korlátozást nem teszik meg, bárki megkísérelheti a szerverre való közvetlen levélküldést és ezzel pl. vírust juttathat a rendszerbe. Az intézményi szerver védelme tehát csak akkor biztosított, ha ezt a szűrést a szerveren vagy az előtte lévő router eszközön beállítják. Ezt a „tűzfal hangolási" műveletet a szolgáltatás beállítását és tesztelését követően az ügyfélszolgálat automatikusan elindítja.

Hosszabb üzemszünet esetén az ügyfélszolgálatnál kérhető a levelek relay szerveren történő hosszabb idejű tárolása. Ennek ideje maximum 2 hét. A szolgáltató a relay szervert ebben az esetben úgy állítja be, hogy az úgynevezett SMTP 505 hibajelzést ad a feladónak – ezzel jelzi, hogy a kézbesítéssel tartósan gondok vannak, de átveszi a levelet. A központi vírusvédelem kikapcsolását akkor sem javasoljuk, ha iskola belső levelező szerverén is használ vírusvédelmet, mert a kétféle szűrés csak erősíti a védekezés hatékonyságát.

FONTOS: A megrendeléssel egy időben az intézményi címek és az Internet SMTP forgalma (TCP/25) tűzfal szinten tiltásra kerül, csak ISP Relay szerver felé megengedett az SMTP. Ugyancsak tiltásra kerül az Internet felől érkező SMTP forgalom, és csak az ISP Relay szerver oldali kapcsolat lesz beengedve az SMTP (TCP/25) portra.

1.6. Mail Relay vírusszűrés szolgáltatás

1.6.1. A szolgáltatás ismertetése

A vírusszűrés alaphelyzetben a Mail Relay szolgáltatás részeként kerül beállításra.
A vírusszűrő rendszer a DialogueScience Dr. Web nevű terméke a levelező rendszerrel integráltan működik, ezért sebességre optimalizált. A vírusadatbázis frissítése a gyártó által mellékelt program segítségével naponta történik.

A vírusirtó rendszer képes tömörített (ZIP, RAR, ARJ, TAR, GZIP, CAB) fájlok többszintű ellenőrzésére, természetesen a támadások kivédése érdekében megadott korlátok betartásával (maximális fájlméret, tömörítési mélység, tömörítési arány).

Vírusos levél észlelésekor a rendszer először a vírusmentesítést hajtja végre (ekkor is keletkezik opcionális figyelmezető üzenet), ha ez nem sikeres, akkor figyelmeztető értesítést küld a címzettnek.

Alaphelyzetben a feladó illetve a rendszeradminisztráció felé semmiféle automatikus

figyelmeztetést (Non Delivery Record, NDR, ami jelzi, hogy a levelet nem kézbesítették, és megadja az okot is) nem generál a rendszer. A vírusokat ugyanis manapság leginkább robotok terjesztik, amelyek a feladót meghamisítják. Ha a hamisított feladó valós személy, a vírusriport csak megzavarja, hiszen ő nem küldött ilyen levelet. Ha viszont nem valóságos feladót hamisítanak, az a rendszereket túlterheli, mivel az NDR-t nincs kinek kézbesíteni, ami újabb hibaüzeneteket generál ezúttal a postamasterek felé. Mindez egy levél esetén nem nagy gond, de a vírus viharok esetében órák alatt levelek millióiról van szó, ami visszajelzés lavinát generálhat megbénítva a hálózatot, a szervereket és az üzemeltetőket is.

1.6.2. A szolgáltatás igénybevétele

A víruskeresést a rendszer a levéltovábbítással egyidejűleg végzi el. Ezzel a felhasználó automatikusan szűrt leveleket kap, illetve a Relay rendszeren keresztül kimenő levelei is szűrésre kerülnek (smarthost). Ha a rendszer vírust talál, és azt képes kiszűrni, a szűrt levelet továbbítja kiegészítve a vírusra vonatkozó információval – például vírusos csatolás eltávolítása. A kiirthatatlan vírust tartalmazó levelet a rendszer törli és értesítést küld a címzettnek. A címzett az értesítés alapján megkeresheti a feladót, figyelmezteti és levélismétlésre kéri. Ismeretlen, feltehetően hamis feladóval nem érdemes, nem szabad foglalkozni.

A vírusszűrő rendszer technikailag képes arra, hogy a vírusos leveleket ne dobja el, hanem az intézmény kérésére megadott címre továbbítsa. Erre jelentős diszkkapacitás szükségeltetik, és sok értelme nincs, hiszen a milliónyi levél gyakorlatilag kiértékelhetetlen. Amennyiben ilyen igény van, az ügyfélszolgálat felé jelezni kell a „vírusgyűjtő" levélcím megadásával egyetemben

Titkosított, kódolt levelekben, illetve jelszóval védett, és így nem olvasható csatolt állományokban víruskeresés nem lehetséges. Ezeket a rendszer nem képes vizsgálni, de ezek feltehetően nem vírusosak, mivel megbízható helyről érkeztek. – ezért a rendszer az ilyen leveleket továbbítja a címzettnek, mivel esetleges figyelmeztetésekkel erősen zavarna egy PGP kódol levelezést. Amennyiben valakitől részben (csatolás) vagy egészben titkosított levelet kapunk, és a jelszó a levél üzenetben vagy külön levélben megküldi a feladó, ne bízzunk benne! Mielőtt a kérdéses levelet dekódolnánk, kérdezzük ré a feladóra, valóban küldött-e részünkre ilyen emailt.

Amennyiben a védelem ellenére valaki vírusos levelet kapott, a levél minden paraméterét (fejléc, azonosító, érkezés dátuma, stb.) levélben jelenteni kell az ügyfélszolgálton.

A Sulinet minden levelező szervere automatikus vírusmentesítést végez.

1.7. Sulinet WebMail szolgáltatás delegált adminisztrációval

1.7.1. A szolgáltatás ismertetése

Dedikált központi levelező postafiókok intézmények részére. Ez a szolgáltatás elsősorban

olyan intézmények részére lett összeállítva, ahol nincs lehetőség/igény helyi levelező szerver használatára. A dedikált levelező szolgáltatás keretében minden intézmény a saját internetes domain-je alatt hozhatja létre postafiókjait, ugyanúgy, mintha helyi szervert üzemeltetne.

A rendszer csak a 20Mbyte méretkorlátnál kisebb leveleket továbbítja.

1.7.2. A szolgáltatás igénybevétele

Igénybe vehető postafiókok száma: 200 db. (további mailboxokat igényelni kell)
Max levelezési tárhely: 1 Gb/intézmény

Az admin postafiókokhoz hasonlóan ez is Web böngészővel és levelező kliens-el érhető el:

WebMail:

- URL: **http://httpmail.sulinet.hu/**
- URL2 (biztoságos): **https://httpsmail.sulinet.hu/**

Levelező kliens beállítások:

- Név: [használó neve] vagy [intézmény neve]
- Email cím: [fióknév]@[inézményi_domain].sulinet.hu
- Felhasználónév: [fióknév]@[intézményi_domain].sulinet.hu
- Jelszó: [jelszó]
- Bejövő levelek kiszolgálója:
    - Pop3: pop.sulinet.hu
    - Pop3s (biztonságos): pops.sulinet.hu
    - Imap: imap.sulinet.hu
    - Imaps (biztonságos): imaps.sulinet.hu
- Kimenő levelek kiszolgálója (smtp): emailsmtp.sulinet.hu

Imap/Imaps alapú kapcsolódás esetén a levelek a szerveren maradnak, így bárhonnan könnyen elérhetőek leveleink és levelezési mappáink. A kimenő SMTP levelezés a Sulinet hálózatból szabadon megengedett, de Sulineten kívüli címről a rendszer kéri a feladó postafiók nevét és jelszavát, ami nélkül nem enged levelet feladni.

Megj: időszakosan javasolt az így tárolt leveleinket, illetve régi (1-2 hónapos) leveleinket helyi mappákba lementeni (archiválni).

Ezekről a postafiókokból nincs lehetőség levél írására az admin posta rendszerbe, így ha oda szeretnénk levelet eljuttatni, akkor azt továbbítsuk hálózati rendszergazdán részére, és ő tudja azt továbbítani.

Az intézmény részére allokált 1Gb levelezési tárhelyet az intézményi rendszergazda tetszés szerint osztja meg az általa létrehozott postafiókok részére. Ez a folyamat a delegált domain adminisztrációs felületen történik. Ezen beállításokat (maibox méret, új mailbox, mailbox törlés, stb.) a külön e célra kialakított adminisztrációs webfelületen állíthatók be, amelynek használatát külön felhasználói utasítás tartalmazza. A domain adminisztrátor maga is rendelkezik postafiókkal az általa adminisztrált domainben, tehát oda mint közönséges webuser is bejelentkezhet. Ha azonban az adminisztrációs felületet szeretné használni, akkor a **https://httpsmail.sulinet.hu:9010/Admin/[intézményi_domain]** címet kell használnia.

A központi szerveren lévő postafiókok vírusszűrtek, esetleges vírusnak tűnő levél esetén kérjük küldjék meg a levelet + teljes levél fejlécet az ügyfélszolgálat részére.
Ha a használat során kevésnek bizonyul a postafiók maximális tárhely / maximális mailbox mennyiség, úgy további kapacitás igénylésére– megfelelő indokolással – a Közháló Ügyfélszolgálaton van lehetőség. Az igény elbírálásáról a Közháló Ügyfélszolgálat és az ISP együttesen dönt.

1.8. Intézményi Home Page üzemeltetése (Weblap Szolgáltatás)

1.8.1. A szolgáltatás ismertetése

Intézményi Weblap szolgáltatást minden intézmény megrendelheti, amennyiben egyedi, saját web oldalakkal szeretne megjelenni a világhálón.

Az alapesetnek megfelelően az ISP ebben az esetben is létrehozza a http://www.iskola.sulinet.hu weboldalt egy osztott szerverfarmon, amelyen az intézmény fontosabb adatai – név, cím, elérhetőség és kapcsolatfelvétel – lesznek feltüntetve.

Ezek után az Intézmény saját fejlesztésű oldalai kerülhetnek erre a tárhelyre elhelyezésre, az Intézmény erre a célra kijelölt alkalmazottai által szabadon frissíthető módon (új állományok feltöltése, meglévők módosítása, törlése). A feltöltött oldalak tartalmáért, aktualitásáért ezt követően az Intézmény felelős.

Az intézmény számára 200Mbyte tárhely áll rendelkezésre, ezt a rendszer nem engedi túllépni. További tárhely a Közháló Ügyfélszolgálaton – megfelelő indokolással – igényelhető. Az igény elbírálásáról a Közháló Ügyfélszolgálat és az ISP együttesen dönt.

1.8.2. A szolgáltatás igénybevétele

A Szolgáltatás igénybevételének szándékát az ügyfélszolgálaton kell jelezni Emelt szintű Intézményi Home Page igénylési formanyomtatványon. Tartalmat a szolgáltatás beüzemelésekor létrejött felhasználói fiókkal lehet feltölteni az alábbi titkosított protokollok használatával, login/password autentikációval:

- WebDAV
- SFTP

WebDAV-os feltöltés elérhetősége: **https://webdav.sulinet.hu/username** (ahol

username a felhasználói fiók).

SFTP feltöltés elérhetősége: **sftp.sulinet.hu** (itt a bejelentkezés után rögtön a megfelelő könyvtárba irányítódik át a felhasználó).

Mindkét típusú webszolgáltatás esetén (Linux, Windows) lehetőség nyílik úgy statikus mint dinamikus tartalom megjelenítésére.

Statikus tartalom esetén feltölthető fájlok lehetnek *.htm és *.html kiterjesztésűek.

A Webszerver farmok a következő dinamikus weboldal megjelenítő technológiák futtatását teszik lehetővé:

- Microsoft oldalon:
  - ASP, feltölthető fájlnevek: *.asp
  - ASP.NET (1.1-es .NET Framework), feltölthető fájlnevek: *.aspx; *.asmx
- Linux oldalon:
  - PHP (4.x), feltölthető fájlnevek: *.php
  - PERL (5.6), feltölthető fájlnevek: *.pl

A szerverek által támogatott képformátumok: GIF (*.gif); JPEG (*.jpg; *.jpeg); PNG (*.png).

Minden feltöltött website-hoz alapkövetelmény egy kezdő oldal megléte. A webszerverek a következő neveket fogadják el (és jelenítik meg) mint kezdő lapot:

- index.htm (és .html; .php; .asp; .aspx)
- default.htm (és .html; .php; .asp; .aspx)

A webszerverek adatbázisszerverekhez (MySQL, MSSQL) nem férnek hozzá.

A szolgáltatás megszüntetését szintén az Ügyfélszolgálat végzi, az Intézmény kapcsolattartójától kapott írásos kérelem alapján. Ilyenkor a felhasználói fiók és a webtárhely zárolásra kerül, majd egy hét türelmi idő után automatikusan törlődik. Ezalatt az idő alatt az Intézmény írásban visszavonhatja megszüntetési kérelmét és lehetőség nyílik a teljes tartalom visszaállítására, a szolgáltatás ismételt beüzemelésére.

Amennyiben az egy hét türelmi idő alatt nem érkezik visszavonó kérelem, a feltöltött adatok és a felhasználói fiók véglegesen törlődnek, visszaállítási lehetőség nélkül!

1.9. Sulinet DNS kiegészítő szolgáltatás (második sublevel domain rendelése) és saját Domain adminisztráció

1.9.1. A szolgáltatás ismertetése

A Sulinet ISP szolgáltató biztosítja az intézmények részére egy második aldomain regisztrálásának lehetőségét a sulinet.hu tartományban.

Az Sulinet ISP rendszere a teljes körű regisztrációra (mindkét zóna szervert Sulinet ISP biztosítja), másodlagos szerver biztosítására (elsődleges szervert iskola üzemelteti, másodlagos szervert Sulinet ISP biztosítja), valamint csak regisztráció igénybe vételére (elsődleges és másodlagos zóna szervert intézmény üzemelteti) egyaránt alkalmas. Az Sulinet ISP által üzemeltetett két központi DNS szerver az intézményi zónára vonatkoztatva mindenképpen jogosult (authoritative) szerverként üzemel.

1.9.2. A szolgáltatás igénybevétele

A szolgáltatást az ügyfélszolgálatnál illetve a regisztrációs form rendszerben lehet igényelni. Az igénylésnél pontosan meg kell adni a zóna nevét név.sulinet.hu formában, ahol a név célszerűen utal a zóna tulajdonosára és vagy a zóna funkciójára.

A zóna letöltést Sulinet ISP szabályozza. Engedélyezi a zóna letöltést a hozzá tartozó intézmény felől, a másodlagos szerverek felől, és a NIC teszt szerverei felől. Egyébhelyekről az intézményi zónák tartalmához nem lehet listázással hozzáférni. Nem letöltés alapú kéréseket, vagyis az intézményi zóna tartalmán belüli rekordra mutató DNS kéréseket az Internet közösség számára természetesen korlátlanul szolgálja ki mindkét DNS szerver.

Mindkét szerver a Bind 9.2.1 verziót használja, amely a reverse zónákat is szolgáltatja igény szerint az RFC2317 szerint is. Az Sulinet ISP gondoskodik a szoftver folyamatos frissítéséről, karbantartásáról.

Az DNS adminisztrátor rendszer a zóna adatokat adatbázisban tárolja. A DNS adatokat az intézményi delegált adminisztrátorok grafikus felületen, vagy az ügyfélszolgálaton keresztül (elektronikus on-line web-form oldalon, vagy letölthető és kinyomtatható formanyomtatvány kitöltésével és elküldésével) módosíthatják.
On-line módon a delegált adminisztrátor „A", CNAME, és PTR rekordok létrehozását, törlését és módosítását végezheti. „A" rekord csak az intézményhez rendelt domain zónából, és csak az intézményhez rendelt címtartományba mutathat. PTR rekord csak az intézményhez rendelt címtartományból és csak az intézményhez rendelt domain zónába mutathat. CNAME rekord az intézményhez rendelt domain zónán belül bárhova mutathat. Ezeket a korlátozásokat a rendszer automatikusan az adminisztrátorokra kényszeríti. „A" rekord létrehozásakor, módosításakor vagy törlésekor a rendszer automatikusan javasolja a hozzá tartozó PTR rekord létrehozását, törlését, vagy módosítását. A grafikus felület védelmet biztosít az ismertebb DNS beállítási hibák elkövetése ellen.

A grafikus felületen történt szintaktikailag és szemantikailag helyes módosítások automatikusan bekerülnek az aktuális DNS adatbázisba. Mentés előtt van visszalépési lehetőség. A mentés során a zónák széria számának módosítását automatikusan kezeli a rendszer. A szoftver a DNS szervert a konfiguráció frissítés szükségességéről 15 percenként értesíti a megváltozott zónák nevének pontos megadásával. A DNS szerver az érintett zónákat reloaddal újraindítja

Más típusú rekordok, vagy a fenti szabályoknak nem megfelelő A és PTR rekordok adminisztrálása csak az ügyfélszolgálaton keresztül, formanyomtatványok segítségével lehetséges.

A domain adminisztrációhoz a **https://webdns.sulinet.hu** címen kell az adminisztrátori postafiók login nevével és jelszavával az intézményi adminisztrátornak bejelentkeznie.

FONTOS: az admin eszköz használata feltételezi a DNS rendszer zóna rekord rendszerének szakmai ismeretét, enélkül ne próbálkozzon senki a zóna szerkesztésével.

A felületen kizárólag az intézmény saját zónáiba és IP tartományába mutató rekordok vehetőek fel. Minden más igény esetén forduljon a HelpDesk munkatársaihoz.

A zóna (domain) kiválasztása

A bejelentkezést követően megjelenített lapon a bal oldali menüsávban láthatóak az intézményhez tartozó zónák. Ezekre klikkelve a jobb oldali keretben megjelenik a zóna tartalma, és az ahhoz kapcsolódó beállítási lehetőségek.

Új bejegyzés létrehozása, meglévő bejegyzés módosítása

Klikkeljen az 'új bejegyzés' menüpontra, vagy amennyiben meglevő rekordot kíván módosítani, az illető rekord melletti 'változtat' linkre. A megjelenő formot az alábbiak szerint töltse ki:

host:
forward zóna esetén a hostnév (pl.: server) kerül ide, reverse zóna esetén az IP cím utolsó oktetje (pl.: 195.199.2.26 -> 26)

típus:
rekord típus. Forward zóna esetén ez vagy 'A', vagy 'CNAME' rekord lehet, reverse zóna esetén kizárólag 'PTR'.

költség:
egyedül 'MX' rekordnál értelmezett, egyébként hagyja üresen.

paraméter:

- 'A' rekord esetén a paraméter az IP cím (pl.: 195.199.2.26).
- 'CNAME' esetén az a hostnév, amelyre a CNAME mutat (pl.: www IN CNAME server)
- 'PTR' rekord esetén a hostnév mellett az intézmény teljes domain nevét ki kell írni. (pl.: server.intezmeny9465.sulinet.hu.)

FONTOS: CNAME és PTR rekordnál a paraméter végére tett pont jelenti azt, hogy az a domain nevet is tartalmazza. Amennyiben a terminálló pont hiányzik, a rendszer feltételezi, hogy relatív rekordról van szó, és a művelet az adott domainen belülre mutató rekordot eredményez.

Automatikus reverse beállítás

'A' rekordok létrehozása, változtatása, illetve törlése esetén a rendszer gondoskodik a reverse zóna beállításáról. Új bejegyzést azonban csak abban az esetben hoz létre, ha az adott IP címhez még nem tartozik reverse bejegyzés, vagy bekapcsolja a 'reverse beállítás mindenképpen' kapcsolót.

Bejegyzés törlése

A megfelelő bejegyzés melletti 'töröl' linkre klikkelve eltávolíthatja a rekordot.