Elosztott tűzfal rendszer a Debreceni Egyetemen 2003-2004 években

Gál Zoltán, zgal@cis.unideb.hu
Karsai Andrea, kandrea@cis.unideb.hu
Balla Tamás, balla@cis.unideb.hu

Debreceni Egyetem, Informatikai Szolgáltató Központja

1. Bevezetés

Az egyetem HBONE/Internet kapcsolata az elmúlt évben 2,5 Gbps-re bővült. Mivel a városban az intézmény campusai között jelentősen megnőtt az adatforgalom, szükségessé vált a felhordó hálózat 100/155 Mbps átviteli sebességről a Gbps tartományba való emelése.

A sávszélesség bővülése, az utóbbi időben tapasztalt vírustámadások és betörési próbálkozások szükségessé tették az egész egyetemi hálózat számára védelmet nyújtó tűzfal felállítását. A HBONE router és az egyetemi MAN közé elhelyezett tűzfal egy IBM RS/6000 szerveren futó IBM Firewall szoftver. Habár a szerver gép gigabites interfészekkel rendelkezik, processzorának terheltsége és a bonyolult szabályrendszer miatt tapasztalatunk szerint meglehetősen leszűkült az intézmény Internet elérési sebessége.

Az cikk a Debreceni Egyetemen több mint egy tucat Gigabit/sec szintű Cisco L3 kapcsoló segítségével kialakított elosztott tűzfal rendszer gyakorlati tapasztalatait mutatja be. Jelen anyag az intézményi Gigabites felhordó hálózat védelmi rendszerrel kibővített bővítési filozófiáját és technikai megoldásait részletezi. A bemutatásra kerülő tapasztalatok lehetővé teszik, hogy más intézmények is a gerinchálózati eszközeik egyébként szükséges bővítésénél az Interneten jelenleg kritikus támadási problémakört hasonló módon hatékonyan lekezeljék.

2. A Debreceni Egyetem informatikai rendszerének rövid összefoglalása

A Debreceni Egyetem hallgatói, oktatói és dolgozói az intézmény hét nagy campusán, illetve telephelyén, az intézményi adatátviteli hálózatra kapcsolt számítógépekről férnek hozzá az informatikai rendszerekhez. A PC kliens gépek nagyobb része Microsoft Windows operációs rendszer működik, de egyre több esetben alkalmazzák a UNIX valamely ingyenes változatát (Linux, Solaris) is. Előbbiek az irodai jellegű elektronikus munkafelületet, utóbbiak inkább az alkalmazások szerver oldali funkcióját biztosítják. Az egyetem központi erőforrás gépei VAX, Sparc, Apha és Risc architektúrán VMS, illetve UNIX operációs rendszert futtatnak.

Az intézményi elektronikus szolgáltatások a következők: elektronikus levelezés, fájlszolgáltatás, szoftver lincensz és médiakezelés, web, cache, proxy, NAT, telefonos behívás (dial-up), vezeték nélküli adatkapcsolat, Internet cím-név összerendelés (DNS), nyilvános hallgatói terminálteremek, IP feletti telefon (VoIP), tűzfal, Névtár (LDAP), videokonferencia. Az egyetemi nagy elektronikus rendszerek az alábbiak:

- Könyvtári rendszer (Aleph),
- Gazdasági rendszer (EcoMed),
- Klinikai rendszerek (MedSol),
- Intézményi WWW rendszer,
- Intézményi számítógép hálózati rendszer (UDNet)

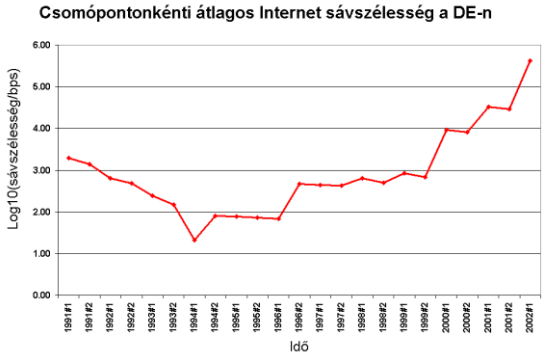
Ezen alkalmazások az alábbi hét campus számítógépiről érhetők el:

	Campus	**Cím**	**PC gépek száma**	**Szerver gépek száma**	**Hallgatók létszáma**
1.	Agrártudományi Centrum	Debrecen, Böszörményi út 138.	560	20	3340
2.	Bölcsészettudományi Kar, Természettudományi Kar,	Debrecen, Egyetem tér 1-2.	2600	60	9246

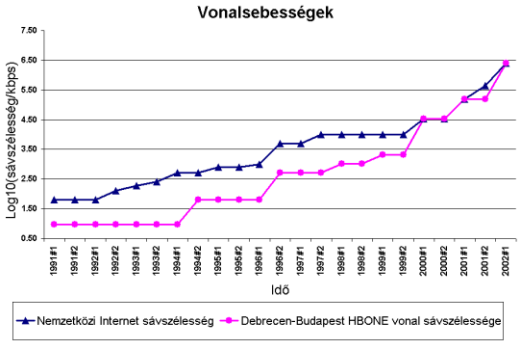
	Konzervatórium				
3.	Egészségügyi Főiskolai Kar	Nyíregyháza, Sóstói út 2.	120	10	2842
4.	Hajdúböszörményi Pedagógiai Főiskolai Kar	Hajdúböszörmény, Désány I. u. 1-9.	50	5	2587
5.	Közgazdaságtudományi Kar, Jogi és Államtudományi Intézet	Debrecen, Kassai út 26.	60	5	2527
6.	Műszaki Főiskolai Kar	Debrecen, Ótemető utca 2-4.	340	10	1972
7.	Orvos- és Egészségtudományi Centrum	Debrecen, Nagyerdei krt. 98.	2050	90	2199
		Összesen	5780	200	24713

Debrecenben az egyetemi felhasználók Internet hozzáférési sebessége az elmúlt tíz év alatt jelentősen megnőtt. Ezt mutatja az 1 és a 2. ábra is. Megfigyelhető, hogy a többi vidéki nagy egyetem viszonylatához hasonlóan a HBONE sávszélessége ma már megegyezik a nemzetközi vonalakéval.

Az intézmény különböző campusain az egyes épületek 10-, illetve 100 Megabit/sec sebességű Ethernet technológiával kapcsolódnak egymáshoz. Ezen átviteli sebességek a 2002. január óta Budapest-Debrecen között működő 2500 Megabit/sec-os értéknek csak 1/250-ed, illetve 1/25-öd részét képezik. Az egyetemnek épületei nem elegendő sávszélességgel kapcsolódnak az intézményi hálózatra. Emiatt az intézményi felhordó hálózat telítetté vált, miközben a rendelkezésre álló Internet hozzáférési kapacitás kihasználása nem éri el az optimális szintet. Jelenleg az egyetemi hálózatra kapcsolt 5800 gép közül mindegyik Internet hozzáféréssel rendelkezik.



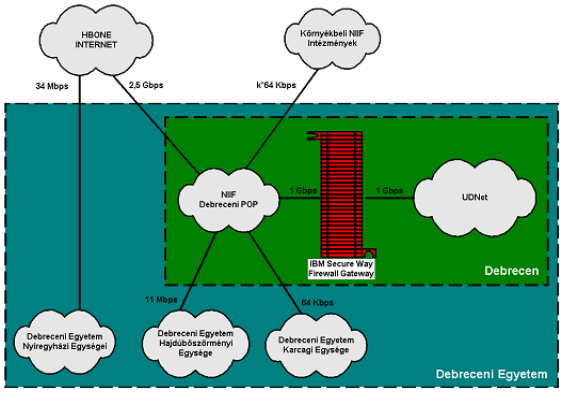
1. ábra. Csomópontonkénti sávszélesség



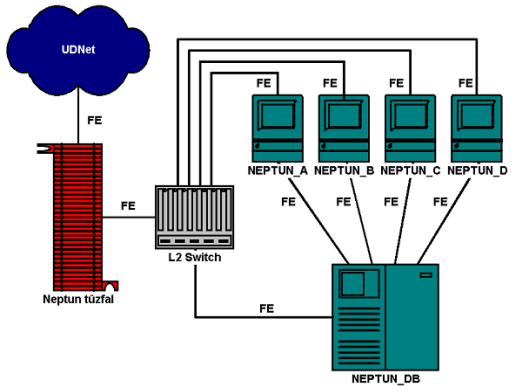
2. ábra. Vonalak sávszélessége

A megnőtt sávszélesség, az utóbbi időben tapasztalt vírustámadások és a betörési próbálkozások szükségessé tették egy olyan tűzfal rendszer felállítását, amely az egész egyetemi hálózat számára védelmet nyújt. A belső címtartomány kibővítése privát IP címekkel NAT technika útján történik és megoldja az egyetem számára egyre szűkebbé váló IP címtartomány problémáját is. A Neptun szerver gépeket ezen túlmenően egy további PC-s tűzfallal védjük, mivel az egyetemi belső hálózatról is tapasztalhatók vírus és féreg programok fertőzési kísérletéből származó támadások.

A Budapest-Debrecen közötti 2,5 Gigabit/sec-os HBONE vonal előnyeit csak úgy tudja az intézmény kihasználni, hogy egyrészt a campusok közötti kapcsolatokat, másrészt a campusokon belüli helyi hálózat gerincét Gigabit Ethernet technológiával biztosítja. Ezáltal a jelenlegi szűk keresztmetszetek megszűnnek és a hallgatók, oktatók, kutatók gyors Internet hozzáféréshez jutnak. Az STM-1/ATM átviteltechnikáról Gigabit Ethernetre történő migrációt az intézmény Informatikai Szolgáltató Központja (DISZK) két lépésben tervezi. Az első lépés a campusok közötti GbE kapcsolatokat kialakítása. Itt figyelembe kell venni, hogy az egyetemi informatikai központ és ezzel együtt az intézmény csillag/fa topológiájú hálózatának gyökere a jelenlegi templomépületből új épületbe költözik át. A második lépés, pedig a campusokon belüli felhordó hálózat átviteli sebességének egy-két nagyságrenddel való növelése.

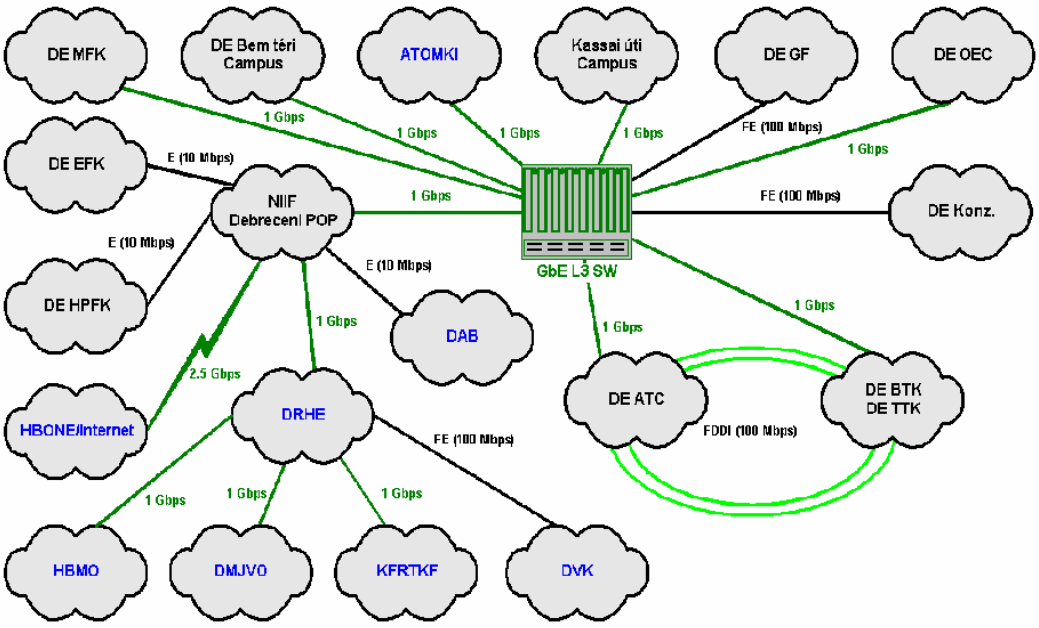


3. ábra. Az UDNet Internet kapcsolata

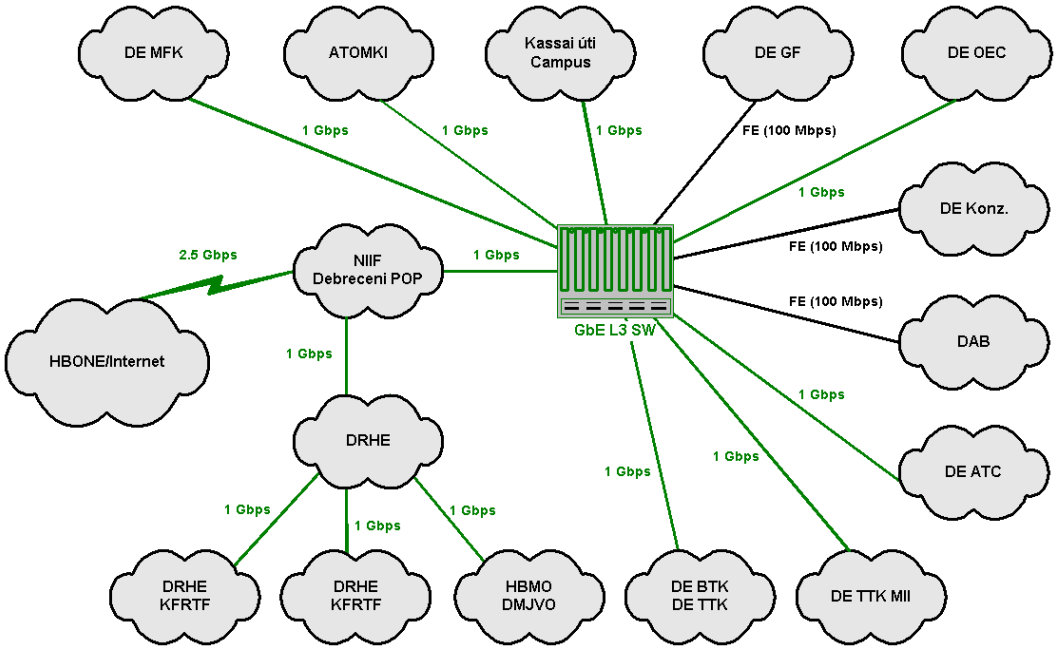


4. ábra. Az egyetem Neptun szerverei

Az intézményi számítógépes hálózat Internet kijárata mellé egy GbE L3 kapcsoló elhelyezése szükséges. Ez csillag topológiában tudja összefogni az egyes campusok GbE/FE L3 kapcsolóit. Az előbbinek csak SMF GbE interfészei lesznek, későbbi 10GbE bővítési lehetőséggel, míg az utóbbiak esetében szükségesek az MMF GbE és az MMF FE interfészek is. A jelenlegi csillag topológiájú ATM rendszert backup üzemmódban tervezzük megtartani, amely a GbE gerinccel párhuzamosan fog működni. Ennek kialakíthatósága nagymértékben függ az UDNet maradék, használatlan üvegszálainak darabszámától.



5. ábra. Az UDNet gerinchálózata (2003. március 18.)



6. ábra. Az UDNet gerinchálózata (2004. február 15.)

3. Az intézményi elosztott tűzfal rendszer struktúrája

A belső gerinchálózat forgalmát a központban elhelyezett Cisco Catalyst 6506 router, illetve a campusokon elhelyezett Cisco Catalyst 3550, gigabit interfészekkel rendelkező, L3 switchek biztosítják. A debreceni campusok közötti gigabites kapcsolatokat több mint egy tucat L4 szinten szűrési lehetőséggel rendelkező kapcsoló biztosítja. Ezen eszközök terheltsége – tapasztaltunk szerint - a megnőtt forgalom ellenére is alacsony. Ez lehetővé tette, hogy a tűzfal funkció számára szükséges védelmi rendszert a célhálózatokhoz közelebb helyezzük, azaz a szűréseket a campusok kapcsolódását biztosító switchek végezzék. Ezáltal az így kialakított tűzfal rendszer nem egyetlen ponton védi az UDNet hálózatot az Internet felől érzékelt támadásokkal szemben, hanem elosztott formában campusonként fejti ki hatását.

Ez jelentősen csökkentette az intézmény korábbi egyetlen tűzfal szerverének terheltségét, mivel ez csak az intézmény gerinchálózati eszközeit védi. Ezáltal a szerver gép áteresztő képessége lényegesen javul és lehetővé teszi a regionális HBONE router közel 1 Gbps sebességű elérését. Ezen túlmenően az elosztott tűzfal rendszer a campusok számára is nagyobb biztonságot nyújt, mivel nem csak az Internet felől biztosít számukra védelmet, hanem a többi campus irányából esetlegesen kezdeményezett támadásokat is kiszűri.