

Linux ile Ağ Yönetimi

Yavuz Selim Kömür - Can Uğur Ayfer

(komur@bilkent.edu.tr cayfer@bilkent.edu.tr)

XI. "Türkiye'de İnternet" Konferansı
21-23 Aralık 2006 TOBB Ekonomi ve Teknoloji Üniversitesi

Özet:

Bu yazıda Linux işletim sistemi ile donatılmış bilgisayarlar kullanarak büyük ölçekli TCP/IP ağlarının yönetimi konusundaki beş yıllık deneyimin aktarımı hedeflenmiştir. Bilkent Üniversitesi ağınının yönetiminden sorumlu olan yazarlar, beş yılı aşkın bir süredir üniversitenin ağında yönlendirici olarak sadece Linux tabanlı kişisel bilgisayarlar kullanmaktadır. Yaklaşık 8.000 bilgisayardan oluşan üniversite ağında her türlü yönlendirme, filtreleme, bant genişliği yönetimi, virüs ve solucanlarla mücadele, gözlem, raporlama Linux işletim sistemi altında açık kaynak yazılımlarla yapılmaktadır. Bu sayede, omurgadaki yönlendiriciler, virüs/solucan mücadelesi ve istenmeyen trafiğin önlenmesi için gereken yatırım; benzeri yapılanmaların yaklaşık onda birine yapılabilmektedir. Üstelik, benzeri yapılanmalara göre çok daha esnek, çok daha kolay kullanılan, yönetilen ve denetlenen bir omurga ortaya çıkmıştır.

Linux Yönlendiriciler

TCP/IP ağların birleştirilmesini; bir başka bakış açısından da ayrılmasını sağlayan yönlendiriciler, ağ yöneticileri için en önemli gözlem ve denetim noktalarıdır. Kaynakların paylaşılması açısından bakıldığında ağların birleştirilmesini sağlayan; ağ üzerindeki istenmeyen trafiğin yayılmasını önlemek açısından bakıldığında ise ağları birbirinden ayıran en önemli araçlar yönlendiricilerdir.

Yönlendiriciler, marka ve modeli ne olursa olsun üzerinde TCP/IP yönlendirme ile ilgili yazılım(lar) çalışan, birden fazla arabirim üzerinden aynı anda birden fazla ağa bağlı olan, bu ağlar arası trafiği düzenleyen birer bilgisayardır.

Bu yazıda vurgulamak istediğimiz en önemli nokta, özel olarak "yönlendirici" olarak üretilmiş ve tipik fiyatları on bin ABD dolarının katlarıyla ifade edilen cihazlar yerine, bin ABD dolarının oldukça altında satın alınabilecek kişisel bilgisayarların da Linux veya BSD işletim sistemi ile, yönlendirici olarak başarıyla kullanılabilirdir. Kaldı ki, piyasadaki tüm ticari yönlendiricilerin UNIX ya da türevi bir işletim sistemi kullanılarak geliştirilmiş olduğu bilinmektedir.

Linux işletim sistemi ile kurulmuş bir bilgisayarı kusursuz bir yönlendirici olarak kullanmak olasıdır. Linux yönlendiricilerin, ticari yönlendiricilere göre herhangi bir işlev eksikliği olmadığı gibi bir çok açıdan işlevsel üstünlükleri vardır. Beş yılı aşkın bir süredir Bilkent Üniversitesi'nde hiç bir ticari yönlendirici kullanılmamaktadır. Bunun nedeni ekonomik değil; Linux yönlendiricilerin daha kolay kurulmaları, yönetilmeleri, yedeklenebilmeleri ve gereksinimlerimize çok daha kolay uyarlanabilmeleri olmuştur.

Bilkent Üniversitesi'nin ağı; üç İnternet çıkışı olması nedeniyle bir otonom sistem (Autonomous system; AS) olarak işletilmektedir. Bu özellik, komşu otonom sistemlerle (UlakNet ve MeteksanNet) BGP-4 (Border Gate Protocol) ile yönlendirme bilgisi alışverişini gerektirmektedir. BGP sayesinde, bu üç hattımızdan

birinde sorun olduğunda, ağ yöneticilerinin müdahalesine gerek kalmadan trafik diğer iki hatta otomatik olarak kayabilmektedir. Sorun ortadan kalktığına ise tercih edilen arabirimler trafiği tekrar üstlenmektedir. Üniversitemizin üç bağlantısının toplandığı ana yönlendirici için yapılan yatırım 600 ABD Doları civarındadır. Söz konusu yönlendiricinin tıpatıp aynısını yedek olarak sistem odasında hazır bulundurmanın ek maliyeti de yine yalnızca 600 Dolar'dır.

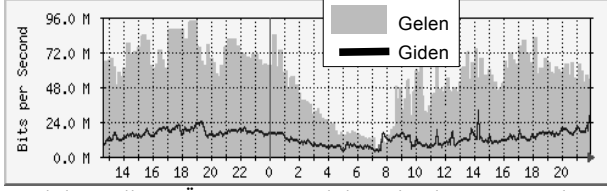
Ticari yönlendiricilerde BGP uygulamasına geçiş genellikle bellek arttırımı, denetim yazılımı değişikliği; hatta birçok durumda donanım değişikliği; kısaca, epeyce bir Amerikan Doları gerektirmektedir. Oysa, bir Linux yönlendirici kullanıldığında açık kaynak kodlu *quagga* [1] yazılımının kurulması yeterli olmaktadır.

Bu yazının yazıldığı tarihte Bilkent Üniversitesi'nde sekiz tane Linux yönlendirici kullanılmaktadır. Bunların tamamı, 1 ile 3 Ghz arasında Intel x86 serisi işlemciye sahip masaüstü kişisel bilgisayarlardır. Toplam parasal değerleri 5.000 ABD doları civarındadır. Bu yönlendiricilerde çalışan *quagga* yazılımı, yönlendiriciler arasında OSPF (Open Shortest Path First) protokolu ile yönlendirme tablolarını birbirlerine ileterek topoloji değişikliklerine tam otomatik uyum sağlamaktadır. Örneğin yönlendiriciler üzerinde yeni bir yerel ağ ekleyerek ya da çıkararak bir değişiklik yaptığımızda veya ağa yeni bir yönlendirici eklediğimizde diğer yönlendiricilerin kurulum ayarlarında hiç bir değişiklik yapmamız gerekmiyor.

Trafik Ölçme ve Gözleme

Bir ağda neler olup bittiğini anlamamın tek yolu, ağ üzerinde akan trafiği ve bileşenlerini kritik noktalarda sürekli olarak ölçmek ve ölçülen bu değerleri eskileriyle karşılaştırmaktır. Bu ölçümler yanlış giden bir şeylerin varlığı kadar kaynak gereksinimlerinin kaydığı ya da odaklandığı noktaların belirlenmesini de sağlar.

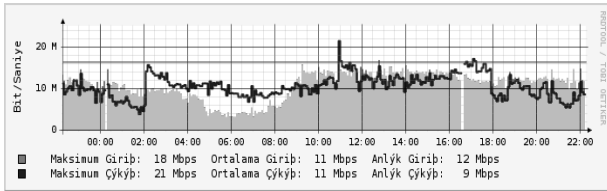
Bilkent Üniversitesi'nde iki trafik ölçme yazılımı kullanıyoruz. En çok işimize yarayan yazılım MRTG - Multi Router Traffic Grapher [2] isimli yazılımdır. Ağ üzerinde çeşitli noktalardaki aktif cihazlardan SNMP protokolü ile toplanan verileri grafik olarak sunan bu yazılım dünyada belki de en yaygın olarak kullanılan ağ performans gözlem yazılımıdır.



Şekil 1. Bilkent Üniversitesi-UlakNet bağlantısı veri akışı

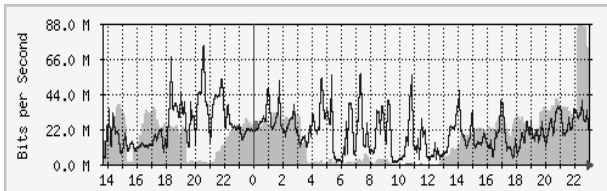
MRTG grafiklerine bakarak kısa ve uzun dönem trafik profili kolayca gözlenebilmektedir. Şekil-1'de Bilkent Üniversitesi'nin UlakNet bağlantısı üzerindeki gelen ve giden trafiği görülmektedir. Bu grafikleri günlük, haftalık aylık ve yıllık olarak gözleyerek ortaya çıkan anormalliklere hızla müdahale edebilmek olanağı buluyoruz.

Şekil-2'de ise bir başka üniversitenin UlakNet trafik akışı istatistikleri görülmektedir. Günün saatinden bağımsız olarak sürekli dışarı trafik oluşturan bu ağda çok sayıda P2P istemcisi çalıştığı ilk bakışta anlaşılmaktadır. Gece gündüz aralıksız devam eden P2P trafiği hat kapasitesinin neredeyse tamamını doldurmaktadır.



Şekil 2. Yoğun P2P trafiği gözlenen bir üniversitenin UlakNet trafiği

Şekil-3'deki grafik ise gece saat 22:00'de birden bire başlayan yüksek trafiğe dikkati çekmektedir. Ağ yöneticisi hemen bu trafiğin nedenini bulup, ters giden birşeyler olup olmadığını kontrol etmelidir.



Şekil 3. Saat 22:00'de bir şeylerin ters gitmeye başlamış olabileceğine işaret

İkinci en önemli ölçme aracımız NeTraMet [3] yazılımıdır. NeTraMet, ağ üzerindeki her bilgisayarın ölçüm noktasından geçen trafiğini çıkış ve varış noktaları itibarıyla paket sayısı ve toplam byte olarak ölçer. İnternet bağlantılarımızı sağlayan yönlendirici üzerinde çalıştırdığımız NeTraMet ile ağ içinde kimin ne kadar ve nereye İnternet trafiği oluşturduğunu gözleyebilmekteyiz.

Örneğin Tablo-1'deki 139.179.14.xx IP adresli bilgisayarın üniversite dışına 6.34 GByte veri transfer etmiş olması doğal değildir. Ne bir web sunucusu, ne de ftp sunucusu olan bu bilgisayarın ayrıntılı trafik dağılımı incelendiğinde (Tablo-2) çok belirgin bir P2P veya torrent trafiği görülmektedir.

En yüksek 100 trafik kaynağı (6 Kasım 2006)			
İçeri Trafik		Dışarı Trafik	
IP Adresi	Toplam	IP Adresi	Toplam
139.179.159.xxx	4.38 GB	139.179.10.xx	13.69 GB
139.179.96.xxx	4.35 GB	139.179.14.xx	6.34 GB
139.179.210.xxx	3.92 GB	139.179.198.xx	1.07 GB
...

Tablo 1 : Üniversite ağında içeri ve dışarı yönlerde en yüksek trafik oluşturan bilgisayarlar

139.179.14.xx Trafik dağılımı(6 Kasım 2006)			
İçeri Trafik		Dışarı Trafik	
IP Adresi	Toplam	IP Adresi	Toplam
85.182.14.20	7.9 MB	82.21.160.24	332.5 MB
82.21.160.24	7 MB	85.182.14.204	326.3 MB
81.230.41.200	5.2 MB	81.230.41.200	207.6 MB
...

Tablo 2 : 139.179.14.xx IP adresli bilgisayarın trafik ayrıntıları

NeTraMet türü bir yazılımla kimin nereye ne kadar trafik oluşturduğunun ölçülmesi etik tartışmalara yol açabilir. Ancak, bir üniversitede veya iş yerinde İnternet alt yapısının kurulma ve işletilme amacı herhangi bir tartışmaya gerek olmayacak kadar açıktır.

Grafikler ve istatistikler normal olmayan bir trafiğe işaret ettiğinde arabirimler üzerindeki trafiği gerçekte çalıştırılacak *tcpdump* [4] komutuyla yayılmaya çalışan, ya da port taraması yapan yazılımların çalıştığı bilgisayar(lar) hemen görülebilmektedir. Örneğin, Şekil-4'deki *tcpdump* çıktısı 139.179.148.106 ve 139.179.148.140 IP adresli bilgisayarlarda çalışan solucan yazılımların, alıcı IP adreslerini sıradan artırarak 135 port açığı arayan trafiğine işaret etmektedir.

```
# tcpdump -ni any port 135 or 445

listening on any, link-type LINUX_SLL (Linux cooked), capture
size 96 bytes
22:19:11.504175 IP 139.179.148.106.4275 > 214.214.148.25.135
22:19:12.778009 IP 139.179.148.140.3217 > 60.171.173.185.135
22:19:12.778326 IP 139.179.148.140.3218 > 60.171.173.186.135
22:19:12.778427 IP 139.179.148.140.3219 > 60.171.173.187.135
22:19:12.779459 IP 139.179.148.140.3220 > 60.171.173.188.135
22:19:12.779695 IP 139.179.148.140.3221 > 60.171.173.189.135
22:19:12.780052 IP 139.179.148.140.3222 > 60.171.173.190.135
22:19:12.797236 IP 139.179.148.140.3233 > 60.171.173.201.135
22:19:12.797379 IP 139.179.148.140.3234 > 60.171.173.202.135
22:19:12.797478 IP 139.179.148.140.3235 > 60.171.173.203.135
22:19:12.801344 IP 139.179.148.140.3236 > 60.171.173.204.135
22:19:13.188870 IP 139.179.148.106.4295 > 214.214.148.45.135
```

Şekil 4: Solucan trafiği

Yönlendirici arabirimlerindeki trafikleri gerçek zamanda ölçmek için kullandığımız bir diğer önemli araç *iftop* [5] yazılımıdır.

Örneğin, yönlendiricinin *eth2* arabirimi üzerindeki trafiği oluşturan bilgisayarları gerçek zamanlı ve trafik yoğunluğuna göre sıralı olarak gözlemek için *iftop* komutunu kullandığımızda elde ettiğimiz tipik bir rapor Şekil-5'te gösterilmiştir.

IP	Direction	Rate	Count	Size
139.179.196.133	=>	87.248	197.26	98.8Kb
139.179.213.254	=>	139.179.193.170	68.0Kb	65.2Kb
139.179.194.189	=>	139.179.193.170	4.02Mb	4.02Mb
139.179.137.18	=>	193.239.89.16	76.1Kb	73.0Kb
139.179.213.217	=>	87.248.197.30	3.99Mb	3.80Mb
139.179.211.248	=>	139.179.286.212	35.3Kb	44.6Kb
139.179.204.230	=>	82.129.39.79	2.48Mb	2.91Mb
139.179.196.146	=>	139.179.198.173	30.3Kb	34.6Kb
139.179.204.220	=>	139.179.198.173	1.98Mb	2.26Mb
139.179.197.99	=>	139.179.198.173	28.3Kb	30.9Kb
139.179.216.244	=>	139.179.198.173	1.53Mb	1.70Mb
	=>	139.179.198.173	23.4Kb	23.1Kb
	=>	139.179.198.173	1.61Mb	1.58Mb
	=>	139.179.198.173	23.4Kb	23.0Kb
	=>	139.179.198.173	1.61Mb	1.57Mb
	=>	139.179.198.173	23.9Kb	23.0Kb
	=>	139.179.198.173	1.61Mb	1.54Mb

RX: cumm: 321MB peak: 7.22Mb rates: 3.77Mb 3.93Mb 4.83Mb
 BX: 2.04GB 50.4Mb 46.3Mb 46.9Mb 43.0Mb
 TOTAL: 2.36GB 54.4Mb 50.1Mb 50.9Mb 47.8Mb

Şekil 5 - Örnek *iftop* raporu

Trafik Denetimi

TCP/IP ağlarda trafik denetiminin yapılması için en uygun noktalar yönlendiricilerdir. Bilkent Üniversitesi'nde trafik denetimi için kullandığımız yazılım, Linux çekirdeğinin bir parçası olarak çalışan *netfilter* ve bu yazılımın yönetim arayüzü olan *iptables* [6] yazılımlarıdır. *netfilter/iptables* ile güvenlik duvarı (*firewall*), yük dengeleme (*load balancing*) ve trafik şekillendirme (*traffic shaping, QoS*) gibi işlevleri kolaylıkla ve etkin olarak yerine getirebilmekteyiz.

Güvenlik Duvarı (Firewall) İşlevleri

“Güvenlik duvarı” ya da “*firewall*” yazılımları tehlikeli ya da istenmeyen trafiğin bir bilgisayar ağına girmesini ya da çıkmasını önleyen denetim yazılımlarıdır. Son yıllarda bu amaca yönelik özel amaçlı donanımlar üretilmekte ve satılmakta ise de, bu işlev Linux yönlendiricilerin doğal bir özelliğidir.

Piyasadaki yönlendiricilerin yazılım ve donanım kısıtlamaları ve belki de daha önemlisi, fiyatlandırma politikaları nedeniyle, kurumlar ağlarını istenmeyen trafiğe karşı korumak için özel “*firewall*” donanımı satın almak zorunda kalmaktadır. Bu tür alımların ardından ağ yöneticileri yepyeni bir denetim yazılımını kullanmayı öğrenmek zorunda kalmakta; ilk yatırımın ardından da bakım ücreti adı altında hiç de küçümsenemeyecek yıllık/aylık ödemelerin yükü altına girmektedir. Oysa Linux işletim sistemi altında çalışan yönlendiriciler için, her Linux dağıtımı ile birlikte gelen, mükemmele yakın performans gösteren güvenlik duvarı yazılımı kullanıma hazırdır: *netfilter/iptables*.

netfilter/iptables basit bir paket filtreleme yazılımı değildir. Bir paketin ne yapılacağına karar vermeden önce o paketin ait olduğu TCP/IP seansına ilişkin

eski paketlerin de dikkate alınmasına olanak sağlar. “Bağlantı izleme” (*connection tracking*) adı verilen bu özellik sayesinde basit paket filtresi olarak eski güvenlik duvarı yazılımlarına (*ipchains* gibi) göre çok büyük üstünlük sağlamaktadır.

iptables ile gelen ve giden paketlerin kaderine karar verirken çıkış ve varış IP adresleri, port adresleri yanısıra paketlerin varış/çıkış sıklıkları, içerikleri, hatta günün tarih ve saati bile dikkate alınabilmektedir. Örneğin deneme yanılmayla şifre kırma çabasının işareti olan, bir IP adresinden beş saniye içinde üçten fazla *ftp* ya da *ssh* bağlantı isteği geldiğinde, bu paketleri reddetmek ya da daha iyisi, görmezlikten gelmek olasıdır. Gene günümüzün sıkça kullanılan saldırı yöntemlerinden biri, *http, smtp* gibi servisleri aşırı yükleyerek sunucuları yanıt veremez hale getirmeye yönelik DoS (*Denial of Service*) saldırılarıdır. Bu saldırılarda, sunucu yazılımının yanıt veremeyeceği sıklıkta bağlantı isteği (SYN) gönderilir. *iptables* ile, gelen SYN paketlerinin sıklığını denetlemek, aşırı yük yaratacak sıklıktaki paketleri durdurmak olasıdır.

Yük Dengeleme / Sunucu Yedekleme

Yoğun kullanılan web uygulama sunucularında, SMTP sunucularında zaman zaman ya da sürekli performans sorunu yaşanabilmektedir. Sunucular zorlandığında genellikle ilk akla gelen donanımı daha yüksek performanslı bir bilgisayarla değiştirmek olmaktadır. Oysa çoğu zaman ek sunucularla çok daha ucuz çözümler elde edilebilmektedir. Darboğaz hat hızında veya disk erişimlerinde olmadığıda sunucu eklemek, ekonomik olarak daha elverişli olmanın yanısıra yedek donanımla çalışma olanağını da beraberinde getirmektedir.

Linux yönlendirici üzerinde çalışan *netfilter/iptables* yazılımı, bağlantıları da izleyerek, istemcilerden gelen paketleri birden fazla sunucu arasında sırayla dağıtabilir. Örneğin bir web sitesini dört web sunucu üzerinde işletmek mümkündür. Dışarıdaki bir istemciden *http* bağlantı isteği geldiğinde, bu paket ve bu bağlantı ile ardından gelen ilgili tüm paketler, belirlenen kriterlere göre seçilecek bir sunucuya yönlendirilebilir. *netfilter/iptables* yük dengeleme işlevini yerine getirirken gelen paketleri, gidebilecekleri sunuculara *round robin* algoritmasına göre; bir diğer deyişle sırayla, yükü eşit dağıtacak şekilde yönlendirir.

Bir servisi birden fazla sunucu ile vermenin nedeni yük dengeleme değil de yedekleme olduğu zaman *netfilter* yazılımının sırayla sunucu seçip paketleri ona yönlendirmesi amaca tam olarak hizmet etmemektedir. Sunucu yedekleme gerektiğinde kullanılabilen *keepalived* [7] yazılımı hem ilgili sunucuları sürekli izlemekte, hem de bunlardan birinde bir aksaklık olduğunda yükü diğer sunucular arasında önceden belirlenmiş oranlarla paylaşabilmektedir. Bir Linux PC ve *keepalived* yazılımının maliyeti tipik olarak 500 ABD Doları iken, “en ucuz” olduğu sloganıyla satılan bir yük dengeleyici “cihaz” 5.000 ABD Dolarına satılmaktadır. Üstelik o cihazın içinde aslında bir Linux ya da BSD PC var iken...

NAT

ADSL ve kablosuz ağ hizmetleri yaygınlaştıkça, NAT (*Network Address Translation*); bir diğer deyişle, tek ya da az sayıda gerçek IP adresiyle çok sayıda bilgisayara ağ hizmeti verme gereksinimi de artmaktadır. NAT kullanmanın tek amacı IP adresinden tasarruf etmek değildir. Güvenlik amacıyla, kritik sunucuları ağ içinde özel IP adresleri ile gizleyerek dışarıdan gelebilecek saldırılara karşı korumak da yaygın olarak kullanılan bir NAT uygulamasıdır.

netfilter/iptables yazılımı kaynak adres dönüşümü (SNAT : *Source Network Address Translation*) ve alıcı adres dönüşümü (DNAT: *Destination Network Address Translation*) işlevlerini kusursuz ve etkin bir şekilde yapabilecek şekilde geliştirilmiştir. Bilkent Üniversitesi'nde, *netfilter/iptables* yazılımının adres dönüştürme yeteneklerini, hem yük dağılımı yapmak hem de gelen tüm elektronik postaların önce bir virüs tarayıcı bilgisayardan geçirilmesini sağlamak amacıyla kullanıyoruz.

P2P ile Mücadele

Masaüstü bilgisayarların iyi denetlenemediği ağlarda P2P (Peer-to-peer) trafik çok ciddi bir sorun olmaktadır. Serbest bırakıldığında hat kapasitesinin tamamını tüketme eğilimindeki bu uygulamayı kontrol altına almak için *ipp2p* [14] isimli *iptables* modülünden yararlanıyoruz. *ipp2p* ile Kazaa, Ares, e-Donkey, emule ve DC trafiklerini denetim altına alabiliyoruz. *iptables* ile *ipp2p* filtrelerine takılan bu P2P paketlerini tamamen durdurabildiğimiz gibi yavaşlatma olanağımız da oluyor.

Trafik Şekillendirme

P2P dosya paylaşım yazılımları (BitTorrent gibi), web tabanlı dosya paylaşım servisleri (RapidShare gibi), video paylaşım siteleri (uTube gibi) band genişliğini hızla eriten uygulamalardır. Bunlar, özellikle üniversitelerde laboratuvar kaynaklarının gereksiz yere tüketilmesine yol açmaktadır. Hele yurtlarda ve ofislerde; günlerce, haftalarca aralıksız tam kapasite dosya indiren kullanıcılar başkalarının çalışmalarını aksatacak boyutlara varan trafik yaratmaktadır.

Band genişliğini adil bir şekilde paylaşmak; bazı bilgisayarlara veya servislere öncelik vermek ya da tam tersine önceliklerini düşürmek olasıdır.

tc [13] (*traffic control*) yazılımı ile yönlendiriciler üzerinde değişik kapasitelerde birkaç band tanımlamak olasıdır. Örneğin 100 Mbit bir hat üzerinde 60, 30 ve 10 Mbit'lik 3 band tanımladıktan sonra BitTorrent kullanan, paylaşım sitelerinden dosya indiren kullanıcıların trafiğini 10 Mbit'lik banda; FTP, SMTP gibi zaman açısından fazla önemli olmayan trafiği 30 Mbit'lik banda kaydırabiliyoruz.

Kablosuz Ağ Yönetimi

Hızla yaygınlaşan dizüstü bilgisayarlar kablosuz erişim isteklerini de beraberinde getirmektedir. Kablosuz erişim noktaları arttıkça yönettiğiniz ağa giren bilgisayarlar üzerinde denetiminiz de azalıyor. Pek çok denetimsiz dizüstü bilgisayarın ağa girip çıkması

virüs ve solucanların yayılmasını hızlandırmakta; ele geçirilmiş bilgisayarlar birer kablosuz Truva atı olarak ağda cirit atabilmektedir. Bilkent Üniversitesi'nde kablosuz bağlantı yapan kullanıcıları VPN (Virtual Private Network) [8] kullanmaya zorluyoruz. Kablosuz ağa bağlandıktan sonra geçerli bir kullanıcı kodu ve şifre vermeden kimse yönlendiricilerden geçemiyor. Bu sayede virüs ve solucan yayan, ele geçirildiği için SPAM yollamaya çalışan bilgisayarların sahiplerinin kullandığı hesapları gerektiğinde bloke ederek denetim sağlıyoruz. VPN bağlantıları için sunucu tarafında kullandığımız yazılım, Linux'un standard servislerinden olan *pptpd* [9] yazılımıdır.

Virüslerle Savaş

Virüsler ne yazık ki ağ yöneticilerinin birlikte yaşamayı ve baş etmeyi öğrenmesi gereken önlenemez gerçeklerden biridir. Gözlemlerimize göre bir çok ağ yöneticisi, ticari antivirüs ürünlerinin kurumsal lisanslarını satın alarak dertlerine çare aramaktadır. Eğer antivirüs yazılımları bir çare olsaydı, aynı çiçek hastalığı virüsü gibi bilgisayar virüslerinin de şimdiye kadar soyu tükenmiş olmalıydı. Oysa, azalmak yerine virüs tehditleri artarak ağ yöneticilerinin başını ağrıtmayı sürdürmektedir.

E-posta ile yayılan virüsleri önleme konusunda açık kaynak kodlu yazılımlarla yüzde yüze yakın başarı elde ettik. Bilkent Üniversitesi'nde çeşitli fakülte, birim ve kullanıcı grubuna hizmet veren sekiz e-posta sunucusu bulunmaktadır. Bu sunuculara yönelik SMTP bağlantıları, güvenlik duvarındaki *keepalived* ile yük dengelemesi yapılarak virüs taraması için iki ara sunucuya yönlendirilmektedir. Bu iki Linux sunucusu üzerinde, açık kaynak kodlu *clamav* [10] yazılımı ile tüm e-posta mesajları üzerinde virüs taraması yapılmakta; temiz olan mesajlar ilgili fakülte veya birimin e-posta sunucusuna yönlendirilmektedir. *clamav* yazılımı saat başlarında virüs veri tabanına bir ekleme olup olmadığını kontrol etmekte; varsa yeni virüs veri tabanını indirmektedir. *clamav* kullanılmaya başlandığından beri, yaklaşık üç yıldır, Bilkent Üniversitesi'ne e-posta ile virüs girmesi sorunu kökünden hallolmuştur.

Masa üstünde MS-Windows işletim sisteminin ezici yaygınlığı ve bu işletim sistemi ailesinin güvenlik sorunlarının büyüklüğü yadsınamaz bir gerçektir. Windows bilgisayarlarını kötü adamlara karşı korumak için çok sayıda ürün satılmasına, kullanılmasına rağmen ne yazık ki sorunlar ortadan kaldırılabilmiş değildir. Belki de bunun en önemli nedeni kullanıcıların umarsızlığıdır.

Deneyimlerimize göre ağ yöneticilerinin güvenlikle ilgili literatürü iyi izlemesi; ağ üzerindeki trafiği dikkatle ölçüp değerlendirerek gereken önlemleri alması, çeşitli ticari ürünlerin kurum lisanslarını satın alıp tüm kullanıcı bilgisayarlarına kurmaktan daha etkin olmaktadır. Örneğin virüs ve solucan bulaşması sonucu ağ üzerinde sorun yaratan bilgisayarların internet erişimini kesmek üniversite ortamında çok etkili olmuş, bu uygulama başladıktan sonra kullanıcılar kendi Windows bilgisayarlarını koruma konusunda çok daha hassas davranmaya başlamışlardır.

Solucanlarla Savaş

Solucan adı verilen yazılımların neredeyse tamamı Microsoft işletim sistemleri altında sunulan servislerin zayıflıklarından yararlanarak yayılmaktadır. Bu servislerin kullandığı iletişim kapılarına (*port*) yönelik trafiği *iptables* ile denetim altına alarak solucan yayılımını önlemek çok kolaydır. İyi bir güvenlik duvarı kurulumunda bilinen port adresleri dışında trafiğe izin verilmez. Örneğin 135-139 ve 445 numaralı portlar üzerindeki trafiğe denetimsiz olarak izin vermek kelimenin tek anlamıyla intihardır. Güvenlik duvarlarının politikası "herşey kapalı, gerekli olanlar açık" olmalıdır. *iptables* ile bu tür politikaları uygulamak son derece kolaydır.

SPAM ile Savaş

2006 yılının sonlarına doğru artık dayanılmaz boyutlara varan istenmeyen e-posta trafiği ile savaşta en önemli ve etkin silahlarımız gene açık kaynak kodlu yazılımlardır. Bilkent Üniversitesi'nde bu amaçla *spamassassin* [11] açık kaynak kodlu yazılımı yanı sıra kara liste servislerinden de yararlanılmaktadır. *spamassassin*, gelen e-posta mesajlarının içerdikleri anahtar sözcükler yanı sıra mesajın görsel düzenleme karakteristiklerini (çok renkli yazı tipleri kullanılmış olması, "listeden çıkmak için şunu yapın" benzeri ifadeler içermesi gibi) değerlendirerek puanlama yapmakta; belirli bir puanı geçen mesajların SPAM olarak işaretlenmesini sağlamaktadır. DNSBL (DNS kara liste) [12] servislerinden yararlanarak da, mesajı gönderen SMTP sunucunun şöhreti kontrol edilebilmektedir. *postfix*, *qmail*, *sendmail* gibi yaygın olarak kullanılan Linux e-posta sunucu yazılımlarına kolaylıkla entegre edilebilen *spamassassin*, yüzde yüz olmasa da, SPAM mesajların yakalanmasında çok başarılıdır.

SPAM savaşındaki bir diğer önemli silahımız da *SQLgrey* [13] isimli *grey listing* yazılımıdır. SPAM gönderen yazılımlar mesajları mümkün olduğunca hızlı göndermeye çalışırlar. Bunun belki de en önemli nedeni, SPAM filtreleri yeni dalgaya göre düzenlenmeden olabildiğince çok mesaj göndermektir. Bu nedenle, gönderemedikleri mesajları bir süre sonra tekrar göndermeyi denemezler. *SQLgrey* yazılımı, herhangi bir IP adresinden herhangi bir kullanıcıya ilk kez gelen e-posta mesajına ilişkin SMTP bağlantısını beş dakikalığına reddetmemizi sağlamaktadır. Eğer gönderici SMTP protokolunu kurallarına göre oynayan bir bilgisayarsa, kısa bir süre sonra tekrar deneyecektir. *Greylisting* sayesinde üniversitemize gelen SPAM mesajların sayısında yüzde doksan oranında azalma sağlanmıştır. Bu çözümün geçici olduğunu, *greylisting* uygulamasının yaygınlaşmasıyla SPAM yazılımlarının da gönderemedikleri mesajlar için yeniden deneme yapmaya başlayacaklarını biliyoruz; ancak şimdilik *greylisting* işe yaramaktadır.

SPAM ile savaş tek yönlü değildir. Gelen SPAM'i önlemenin yanı sıra, giden SPAM'in önlenmesi de kurumların kara listelere alınmaması açısından çok önemlidir. Ne yazık ki, çok çeşitli yöntemlerle kullanıcı bilgisayarları ele geçirilmekte ve uzaktan yönetilerek

SPAM göndermek amacıyla kullanılabilir. Her ne kadar kuşkuyla karşılanan bir oran olsa da, dünyada Windows işletim sistemi ile çalışan ev bilgisayarlarının yüzde 70'inin ele geçirilmiş olduğu tahmin edilmektedir. Oran ne olursa olsun, ele geçirilmiş bilgisayar sayısı hepimizi rahatsız etmeye yetecek kadar çoktur ve ne yazık ki artış eğilimindedir.

Alınan tüm önlemlere rağmen, 29 Ekim - 6 Kasım 2006 tarihleri arasındaki bir haftalık dönemde, Bilkent Üniversitesi'ndeki ele geçirilmiş bilgisayarlardan 1.300.000 den fazla e-posta gönderme girişimi *iptables* filtrelerine takıldı. Bu elektronik postaları, gene *netfilter/iptables* ile sahte bir SMTP sunucusuna yönlendirip topladık. Ortaya çıkan manzarada iki tip ele geçirilmiş bilgisayar profili gördük:

1. SPAM göndermek için uzaktan yönetilen, *zombie*'ye dönüşmüş, yani ele geçirilmiş bilgisayarlar ve
2. kullanıcısının klavyede bastığı tüm tuşları, Windows ve MSN, ICQ gibi uygulama programları tarafından kaydedilen tüm kullanıcı kodu ve şifreleri bir yerlere e-posta ile yollayan bilgisayarlar.

Bu bilgisayarların kullanıcıları ile yapılan görüşmelerde bilgisayarların tamamında ticari birer antivirüs ve İnternet güvenlik yazılımının kurulu, aktif ve güncel olduğunu öğrendik. Sorunlu bilgisayarları kullananların neredeyse tamamı, sohbet sitelerinde bir arkadaşları tarafından kendilerine tavsiye edilen ya da gönderilen bir programı kurduklarını veya "hoş" bir resim dosyasını açtıklarını söylediler. Kullanıcıların kendi elleriyle, "yalnızca bir kerecik" yüklediği; üstelik "böyle şeyler yapmayacak bir arkadaşından gelen" bir yazılım nedeniyle bilgisayarının başkalarının denetimine geçmesinin olası sonuçları hakkında bilgilendirilmesi elbette ağ yöneticilerinin görevidir. Ancak bu konuda pek başarılı olabildiğimiz söylenemez.

Performans Değerlendirmeleri / GigaBit Linux Yönlendiriciler

Özel yönlendirici donanımlarının performansı; özellikle de ana kart arabirim performansları (*backplane performance*) etkileyici düzeydedir. Bunların tipik performansları birkaç yüz Gigabit/sn veri akış hızına kadar çıkabilmektedir. x86 ailesinden bir merkezi işlem birimine sahip kişisel bilgisayar donanımıyla bu hızların küçük kesirlerine dahi yaklaşmak olası değildir. Ancak, en azından üniversite ortamında, önümüzdeki 3-5 yıl içinde departmanlar arasında yüzlerce GigaBit/sn yönlendirme kapasitesine gereksinim duyulmayacağı da bir gerçektir.

Bilkent Üniversitesi'nde Mühendislik Fakültesi ile Fen Fakültesi arasındaki trafik ortalama birkaç Megabit/sn düzeyinde oluşmaktadır. Gene Mühendislik Fakültesi ile Bilgisayar Merkezi arasındaki trafik 70-80 Megabit/sn'yi pek geçmiyor. Oysa her iki fakültenin de kendi içlerindeki trafik doğal olarak çok daha yüksek. Ancak bu iç trafikler yerel ağ Ethernet anahtarları üzerinde kalıyor ve yönlendiricilerimize ulaşmıyor. GigaBit Ethernet arabirimleri-

nin zamanla masaüstü bilgisayarlarda yaygınlaşmasıyla trafik gereksinimleri artabilir ancak bu olasılığa karşı onbinlerce dolarlık yönlendiricilere şimdiden yatırım yapmak ne derece mantıklı?

2006 Aralık ayında Bilkent Üniversitesi'nde Debian Linux, Pentium 4 serisi 3 Ghz'lik kişisel bilgisayarlar ve yüksek tampon bellekli, PCI-Express arabirimli, SM optik kablo arabirimi olan dörder adet Ethernet arabirimi kullanarak GigaBit yönlendiriciler kuruyoruz. Yaptığımız performans ölçümlerinde, her arabirime aynı anda 1 GigaBit trafik basmaya çalıştığımızda 941 MegaBit/sn ile yönlendirme yapabildiğimizi gördük. Seçtiğimiz yüksek performanslı Ethernet kartlarının ve ana kartın fiyatlarının oldukça yüksek olmasına rağmen, söz konusu bilgisayarların, daha doğrusu yönlendiricilerin, her birinin maliyeti 2.000 ABD Doları'nın altında kaldı. Bu yönlendiricilerde sabit disk yerine USB bellek kullandık; böylece arıza olasılığını da azalttık. 2007 yılının ilk gün-

lerinde bu yönlendiricilerimizi devreye almış olacağız. Önceki deneyimlerimize dayanarak hiçbir sorunla karşılaşmayacağımıza eminiz.

Genel Değerlendirme

Linux işletim sistemi kullanarak kişisel bilgisayar donanımları üzerinde kurulan IP yönlendiriciler çok başarılı olmaktadır. Deneyimlerimiz ve gözlemlerimiz genel amaçlı, sıradan bir masaüstü bir bilgisayar ve Linux işletim sistemi kullanarak kurulan yönlendiricilerin büyük avantajları olduğunu; her düzeyde dokümantasyon ve destek bulmanın son derece kolay olduğunu gösterdi. Öte yandan birden fazla marka/model yönlendiricinin yönetim yazılımını öğrenme gereksinimi ortadan kalktı. Değişen koşullara, gelişen ağ topolojisine, ortaya çıkan yeni İnternet zararlılarına hızla ve kolaylıkla uyum ve tepki gösterebildik. Tasarruf ettiğimiz birkaç yüzbin YTL de yanımıza kâr kaldı.

Referanslar	URL
[1] The <i>quagga</i> suite	www.quagga.net
[2] The Multi Router Traffic Grapher	oss.oetiker.ch/mrtg
[3] NeTraMet, Network Traffic Flow Measurement Tool	www.caida.org/tools/measurement/netramet
[4] tcpdump, paket izleme yazılımı	en.wikipedia.org/wiki/Tcpdump
[5] iftop, arabirim trafik izleme yazılımı	freshmeat.net/projects/iftop
[6] iptables/netfilter, güvenlik duvarı yazılımı	www.netfilter.org
[7] keepalived, yük dağıtma yazılımı	www.keepalived.org
[8] VPN	linas.org/linux/vpn.html
[9] pptpd	poptop.sourceforge.net/dox/debian-howto.phtml
[10] clamav	www.clamav.net
[11] spamassassin	spamassassin.apache.org
[12] DNSBL	en.wikipedia.org/wiki/DNSBL
[13] Linux Advanced Routing & Traffic Control	lartc.org
[14] ipp2p	www.ipp2p.org