ADSL Router Seçimi & ADSL Router Firewall

Mustafa Serhat DÜNDAR, <serhat at serhatdundar dot com>,
01/11/2009

ADSL halen günümüzde en çok kullanılan internet bağlantı yöntemi. Bu yüzden ki piyasada bir çok adsl modem bulunmakta. Usb, ethernet, kablosuz gibi çeşitli özelliklerde modemler bulunmakta.

Kablolu bağlantı kullanan bir modem seçerken donanımsal tip olarak 2 adet seçeğimiz var; bunlar ethernet ve usb modemler. Usb modemler güvenlik yönünden oldukça zayıftır, sağladıkları avantaj yalnızca kolay bağlanabilmeleri ve fiyat yönünden daha uygun olmalarıyken bu tip modemler router özelliği barındırmadığından güvenlik için ciddi önem taşıyan portların bir çoğu açıktır.

Bir ADSL router seçerken dikkat etmemiz gereken hususları şimdi maddeler halinde inceleyelim :

Kullanici Arayüzü : Basit, anlaşılır, online yardım ve dökümentasyon hizmeti sunması, ayarlara dair açıklama ve bilgiler içermesi.

Ücret : Firewall tarafından korunabilecek host sayısı, fiyat/kalite oranı. Güncelleme ve teknik destek hizmeti.

Protokoller :

- Dinamik DNS yani DDNS.
- IP adres dönüştürme: gelen trafik için NAT ve SUA.
- Performans için DNS proxy.
- LAN yönlü adresleme için DHCP server.
- SMNP.

Güvenlik :

- Port filtreleme.
- Portların belirtilmesi ve IP adreslerinin listelenmesi.
- FTP gibi dinamil portları kullanana protokollerin merkezi filtrelenmesi.

o SYN flooding gibi DOS saldırılarına karşı koruma içerme.

o HTTP içerik filtreleme : Her bir site/domain/IP aralığı'na özel Javascript, active-x, VBScript, Java ve cookie filtreleme.

o E-mail içerik filtreleme : POP veya SMTP üzerinden tehlikeli dosya eklerinin filtrelenebilmesi.

o IPSec ve VPN desteği.

o DES, 3DES, AES gibi şifreleme seçekleri destekleyen PPTP protokolü.

o Mac adresi filtreleyebilme.

o DMZ.

SALDIRI TESPİTİ :

o Saldırı tespit ve uyarı yüzdesi.

o Bilindik trojan ve backdoor'ların tanınması, uyarı sistemi.

o Tehlikeli saldırılarda e-mail ile bildirim.

o Geçen ve engellenen paketler için local ve remote loglama.

o Uyarı sisteminin anlaşılabilirliği.

KARŞI KOYMA :

o Saldırganın kimliğinin tanımlanabilmesi.

o Düzenli olarak veya anında, tanımlanan saldırıların engellenmesi.

YÖNETİM ARAYÜZÜ :

o Serial, telnet, GUI, Web vb.

o Hata kurtarma özellikler.

o Şifre koruması, session (oturum) desteği.

o Güvenlik izinleri ve ayarları yedekleyebilme.

o Ayar değişikliklerinin loglanması.

o Fabrika ayarı olarak bütün yönetimsel servis ve portların filtrelenmiş olması.

ROUTER ARAŞTIRMASI (ZD-NET AUSTRALİA)

Yazılımsal firewall'lar hakkında oldukça çok araştırma mevcut. Arama motorlarından bir çok firewall karşılaştırması bulabilirsiniz. Fakat router'lar içerisinde dahili gelen firewall'lar hakkında hiç Türkçe araştırma bulunmamakta. Birazdan bahsedeceğim araştırma ve araştırma sonuçları ZD-Net Australia'a aittir.

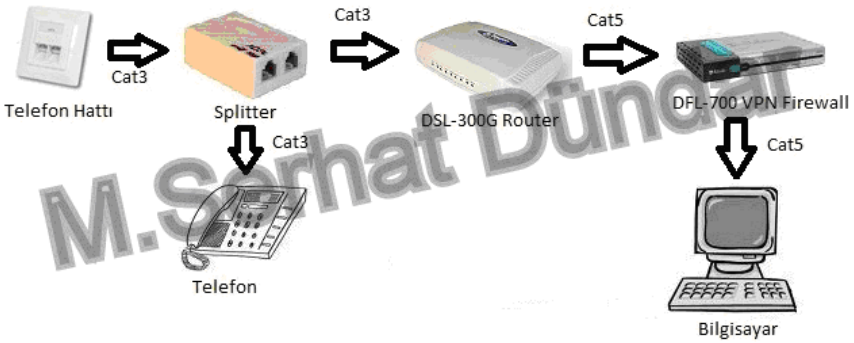
NMap yazılımı kullanılarak yapılmış olan bu araştırma da adsl router güvenlik duvarlarının hangi portları fabrika ayarı olarak "açık" bıraktığı test edilmiş.

Bu test için 6 adet router kullanıldı. Bunlar Cisco/Linksys, Netgear, Nortel, Allied Telesyn, Dynalink, ve D-Link markalarına ait routerlar.

1.A- D-LİNK DSL-300G VE D-LİNK DFL-700 KOMBİNASYONU

D-Link firmasının bu iki ürünlerinden DSL-300G bizim routerimiz, DFL-700 ise firewall donanımı. Dsl-300G modemimizi telefon hattımıza bağlayıp, adsl yazılımını kurduktan sonra modemimiz kullanıma hazır fakat bizim istediğimiz bağlantıyı DFL-700 ile birlikte kurmak olduğu için modemin bilgisayarla bağlantısını kestikten sonra DSL-300G modemimizi bir ethernet (Cat5 kablosu) kablosu ile DFL-700'ün WLAN portuna bağlıyoruz. Sıra geldi DFL-700 firewall'umuzu bilgisayara bağlamaya. DFL-700'ün LAN portundan yine bir cat5 kablosu ile bilgisayarımıza bağlantı kurduktan sonra modem konfigürasyonuna hazırız.

Yaptığımız işlemin net olarak anlaşılması için şematik olarak göstermekte fayda var.



Bu ikili güvenlik yöntemi, teste katacağımız diğer cihazlardan kurulumu daha zor ve genel olarak daha karmaşık görünse de aslında göründüğü kadar da karmaşık ve kötü değil.

Firewall donanımını daha dikkatli incelediğimizde sadece firewall güvenlik yazılımı değil, aynı zamanda VPN desteği, içerik filtreleme ve bandwidth yönetimi, loglama ve raporlama gibi özellikler taşıdığınıda görüyoruz.

1.B- Dynalink RTA770

Dynalink çok fazla özellik içermiyor ancak diğer çözümlere göre fiyat avantajı var. "Gelişmiş" menüsünde IP paketlerini filtrelemenizi sağlayan bir firewall özelliği mevcut. Uzaktan yönetim özelliği de bulunmakta. Sistem logları ve trafik istatistikleri yalnızca temel düzeyde raporlama içeriyor.

1.C- Netgear DG834

Netgear Adsl router'ı ücret/başarı yönünden testimizde ki en iyi router çözümlerinden. Kurulumu Dynalink kadar olmasa da oldukça basit. Fiziksel olarak ilk incelediğimiz ürün olan D-Link ile kurulumu aynı. Kullanıcı arayüzünün oldukça basit olmasının yanında site engelleme, belirli trafiğe izin verme, trafik filtreleme gibi olduıkça hoş özelliklere sahip. Ayrıca kendisine ait görev yöneticisi içermekte ve istediğiniz takdirde sistem loglarını mail adresinize yollayabilmekte.

1.D- Nortel Contivity 251

Nortel testimiz içerisinde ki ciddi önem taşıyan router'lardan. Kurulumu, kurulum yardımcısı ile oldukça basit. Kurulum aşamasında karşımıza gelen sayfada ISP parametrelerimizi belirlememiz ve sonrasında adsl kullanıcı adı ve şifremizi girmemiz gerekirken biz bu sayfayı pas geçtik. Yükleme programı çalıştırdığı program ile Lan ve Wan bağlantılarımızı test etti, eğer testlerden geçeli sonuç aldıysanız bilin ki şuan internete bağlısınız.

Nortel sadece firewall güvenliği yönünden değil, aynı zamanda gelen/giden trafik kontrolü, kelime bazında web sayfası engelleme, içerik filtreleme gibi özelliklere de sahip. Ayrıca DES, 3DES, AES şifrelemelerini kullanan VPN'ler de oluşturabiliyor. Sistem günlükleri yöneticiye belirlenen gün ve saatlerde yollanabilmekte.

1.E- LİNKSYS WAG54G

Linksys testimiz içerisinde kablosuz bağlantı sunan tek router. A ve G wireless modlarının her ikisinde desteklemekte. Kurulum aşaması kullanıcıyı zorlayacak düzeyde değil, sadece encepsulation ve adsl giriş bilgilerinizi tanımlamanız yetecektir. Kablosuz menüsünden WEP ve WPA gibi şifrelemeleri seçebilirsiniz.

Güvenlik menüsü altından Java appletleri, çerezleri, active-x nesnelerini ve proxileri filtreleyebilirsiniz. Fabrika ayarlarında anonymous bağlantı talepleri engelli şekilde geliyor. Testimizi sürdürebilmek için bu özelliği devre dışı bırakıyoruz çünkü bu özellik bilgisayarımız üzerinden router'ı ping etmemizi engelliyor.

NMap yazılımını çalıştırırken yaşadığımız sorunlar bu router'ın güvenliği açısından oldukça sevindirici çünkü bu hiçbir açık port exploit edemediğimiz anlamına geliyor. Fakat bu durum bize oldukça ilginç geldi ve firewall'ı kapattık, ancak halen NMap'i çalıştırırken sorun yaşamamız oldukça ilginçti. Maalesef bu durumun köküne inmek için daha fazla zaman harcamadık, zamanımızı NMap'i çalıştırmak için harcadık ve bunu güvenlik ayarlarını hassaslıktan uzaklaştırarak sağladık. Sonuç olarak herhangi bir açık port bulamadık.

Linksys ayrıca DES ve 3DES şifrelemelerini destekleyen dahili VPN server desteği sunmakta. Ayrıca Linksys uzaktan yönetim ve dahili şekilde gelen raporlama özellikleri içinde kurulabilir. Son olarak e-mail uyarı sisteminide bulunduğunu belirtmekte fayda var.

1.F- ALLİED TELESYN AR440S

Donanımı kurmak oldukça basit. DHCP özelliği fabrika ayarı olarak kapalı geliyor. El ile bilgisayarınıza IP adresi atamadığınız sürece router'e bağlanamıyorsunuz.

Kurulum aşamasının sonunda arayüzü; uzaktan atanmış adresler, firewall kurulumu, NAT, DHCP özelliğinin çalışabilirlik durumu ve trafik yönetimi için düzenledik. Bu sayede LAN'ın arka planını görebilecektik. Tüm bu işlemler yorucu, meşakkatli ve karmaşık görünebilir ancak bu işlemleri bir kereye mahsus yaptığınızı düşünürsek gözümüzde büyütmeye gerek yok.

AR44OS, trafik filtreleme özelliği ile gelmekte. VPN; AES, DES ve 3DES desteklemekte.

1.G- TEST SONUÇLARI

Şimdi tüm bu incelememizi tablo üzerinde görelim :

Ürün	Allied Telesyn AR440S	D-Link DSL-300G/ D-Link DFL-700	Dynalink RTA770	Linksys WAG54G	Netgear DG834	Yokrtel Contivity 251
Ethernet LAN	5-port 10/100Mbps LAN ve DMZ olarak kullanılabilir.	1-port 10/100Base-TX	4-port 10/100 Mbps	4-port 10/100Mbps	4-port 10/100Mbps	4-port 10/100 Mbps
Diğer Portlar (USB, Serial)	1 x Async. serial, 1 x PIC genişleme yuvası	WAN port (10/100), DMZ port (10/100) ve seri konsol portu	USB	~	~	RS232, DB-9f
URL/İçerik Filtreleme	URL filtreleme Firewall HTTP proxy kullanılarak gerçekleşiyor.	Var	Yok	Var	Var	ActiveX, Java appletleri ve çerezleri engelliyor ve web proxieleri kabul etmiyor.
Bandwidth yönetimi	LLQ, PQ, WRR, DWRR, PQ ile WRR/DWRR, 802.1P, IP TOS, IP DSCP, RSVP	Var	Yok	Var	~	Yok
DoS koruması	SYN ve FIN flood, Ping of death ve smurf saldırılarına karşı sezgi sistemi ve port taraması güvenliği.	Var	Yok	Var	Var	Paket inceleme, saldırı günlüğü ve e-mail uyarı sistemi
VPN server	Var	Var	Sadece pass-through	Var	Sadece pass-through	Var
Şifreleme seçenekleri	DES, 3DES, AES	AES, 3DES, DES, CAST128, Blowfish ve Twofish	NA	DES, 3DES	NA	DES, 3DES, AES

Router	Tespit edilen portlar	Isim	Zaaf Testi
Dlink	23	telnet	Kaldı
	80	http	Geçti
	113	auth	Geçti
	443	https	Geçti
Dynalink	80	http	Kaldı
	443	https	Geçti
Netgear	21	ftp	Kaldı
	22	ssh	Geçti
	80	http	Geçti
	256	FW1-secureremote	Geçti
	443	https	Geçti
	554	rtsp	Geçti
	636	ldapssl	Geçti
Nortel	80	http	Kaldı
	443	https	Geçti
Linksys		Did Not Run	Kaldı
Allied Telesyn	80	http	Kaldı
	113	auth	Geçti
	443	https	Geçti

ZDnet Editörünün Seçimi Nortel Contivity 251.

Nortel; bandwidth yönetimi haricinde diğer router'ların içerdiği bütün özellikleri içermekte. Kurulumu ve yönetimi basit, ve fiyatı özelliklerine göre oldukça normal.

M.SERHAT DÜNDAR