

Iptables

Deniz Özibrişim

Eylül, 2012

Bu yazı içerik filtreleme (Dansguardian) hakkında olacaktı; fakat bu yolda ilerlerken kullanacağımız iptables'ı anlatmadan geçmenin doğru olmayacağını düşündüm. Evet belki sadece birkaç yönlendirme komutu işimizi görecekti, ama açıkçası içime sinmedi. Bu yüzden ağırdan alıp kullanacaklarımıza (iptables, squid, dansguardian, webmin v.b) tek tek göz attıktan sonra, sonunda sadece bir dansguardian anlatımına nazaran konuya çok daha fazla hakim olacağımızı düşünüyorum. 222233334566778997711rrqwqqqqereewawwwwwwrrrrsadcvs

Iptables çok kuvvetlidir, detaylı anlatımı tabii ki bu yazıya sığmayacaktır, fakat buradan yola çıkarak ilerideki kullanım tecrübelerinizle emin olun birçok ücretli ürünün yaptığından daha fazlasını yapabileceğini göreceksiniz.

Iptables Nedir?

Linux, daha doğrusu *NIX ve *BSD sistemler üzerinde çalışan, zamanında görevini ipchain'den devralmış (hatırlayanlar vardır), üzerinden geçen trafiği verilen kurallara göre yorumlayan açık kaynak güvenlik/ateş duvarı (Firewall) yazılımıdır. Linux çekirdeği ile gelen (2.3 ve daha yeni) Netfilter'ı yönetmemizi sağlar.

Bu konuyu okumaya karar vermiş, içerik filtreleme, ya da vekil sunucu kullanmayı düşünen kişiler zaten güvenlik duvarının aşağı yukarı ne olduğunu bildikleri için lafı uzatmadan anlatıma geçiyorum.

Iptables, sizin verdiğiniz kurallar zincirine göre hareket eder, gelen veya giden ya da yönlendirilen bütün paketler bu kurallara uyar.

Kurallar zincirlerini siz oluşturabildiğiniz gibi aşağıda standart gelen zincirler mevcuttur.

INPUT : Gelen paketler için kurallar zinciri.

OUTPUT : Giden paketler için kurallar zinciri.

FORWARD : Yönlendirilen paketler için kurallar zinciri.

NAT tarafı için,

PREROUTING : Gelen paketlerin değiştirilmesi/yönlendirilmesi için.

POSTROUTING : Giden paketlerin değiştirilmesi/yönlendirilmesi için.

NAT kuralları da önemlidir, zira ağ geçidi olarak kullanmayı düşündüğünüz Linux bilgisayarınız ile NAT kullanmak zorundasınız. Hatta olaya şu açıdan bakabilirsiniz; bugün evimizde kullandığımız neredeyse bütün ADSL modemler NAT yapıyor.

Bu kurallar zincirini yönetmek için belirli parametreler vardır ki kural ekleme, çıkarma vb. durumları belirtir,

- **-A (append)** :
Belirtilen zincire kural ekler.
- **-D (delete)** :
Belirtilen kural zincirin