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.

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 zincirinden belirtilen numaradaki kuralı siler.
- **-E (rename) :**
  Belirtilen zinciri yeniden adlandırır.
- **-L (list) :**
  Kuralları gösterir, listeler. Zincir belirtilirse, sadece o zincirin kurallarını listeler.
- **-I (insert) :**
  Belirtilen zincirde, belirtilen kural sıralamasında araya bir kural eklemek için kullanılır. (Daha önceden girdiğimiz bir kuralın, söz konusu paket için farklı kural uygulamaması adına, kuralı araya girebilmemiz için gerekebilir.)
- **-R (replace) :**
  Zincirde belirtilen numarada ki alana başka kural koyar.
- **-P (policy) :**
  Herhangi bir kurala uymayan paketlerin başına ne geleceğini belirtir. :)

- **-N (new) :**
  Yeni bir zincir oluşturur.
- **-X (delete) :**
  Oluşturduğumuz kural zincirini siler.
- **-F (flush) :**
  Zincirdeki kuralların tümünü siler.

Yukarıda verdiğimiz kurallar zincirleri ile paketler değerlendirilecek, değerlendirme sonunda bir de pakete uygulanması için verdiğimiz son karar olması lazım ki şöyle:

ACCEPT : Paketlerin geçişine izin verilir.

DROP : Paketlerin geçişine izin verilmez. [Paket düşürülür, hedefe hiç ulaşmamış gibi. Mantıklı gözükse de bazı güvenlik açıklarını doğurabilir. Özellikle DDOS (Önceki sayılarda kısaca bahsetmiştik.) için korunmayan bir yapıda, yönlendirici arkasında paketleri 'DROP'lamak 'router'ın yönlendirici tablosunu aşırı yüklemeden cevap veremez hâle getirebilir.]

REJECT : Paketlerin erişimi reddedilir ve gönderen bilgilendirilir. (DROP yerine REJECT kullanımını öneririm.) Paketin neden geri çevrildiğine ilişkin bilgi eklenebilir.

RETURN : Zincirin sonuna gönderilir.

QUEUE : Paketler kullanıcı alanına gönderilir.

Seçenekler	Açıklama
-s	(source) Kaynak adresini belirtir.
–sport	(source port) Kaynak portu belirtir.
-d	(destination) Hedef adresidir.
–dport	(destination port) Hedef portudur.
-p	Protokolü belirtir, TCP ya da UDP gibi. ALL hepsi için kullanılır.
-i	(interface) Ara birim belirtir, eth0 gibi.
-o	Çıkan veya yönlendirilen kural zincirinde kullanılır. (-o eth1 gibi)
-t	Tabloyu belirtir, nat tablosu için -t nat şeklinde kullanılır.
-m	Kullanılacak modülü belirtir, -m limit gibi.
-j	Belirtilen kural zincirine uygulanacak seçim, -j ACCEPT gibi..
!	Yazılan kuralı tersine çevirir. (Neredeyse bütün seçenekler ile kullanılabilir.)
–tcp-flags	TCP flag'leri. (ACK, FIN, RST, URG, SYN, PS veya ALL.)
–syn	SYN paketlerini kontrol etmek için kullanılır.
–state	State (durum) modülü içindir. ESTABLISHED ve RELATED gibi. (Bağlı olan bağlantıların kayıtlarını tutar vb.)
–limit	Saniye saniye eşleşme hızını kontrol etmek için kullanılır.
–mac-source	Belirtilen mac adresi için işlem yapılır.

NAT (Network Address Translation) Seçenekleri : NAT yapacaklar için, yönlendirici vb. durumlarda kullanacaklar için,

DNAT – PREROUTING : (Destination NAT) Hedef NAT, Size gelen isteği yerel ağınızdaki bir bilgisayara yönlendirmek için kullanılır. Gelen paketin başlığına (Header) hedef adresi değiştirip yazar. Örnek olarak, içeride web sunucusu olarak

hizmet veren bir sunucu varsa, 80 portuna gelen istekleri içerideki web sunucunuza yönlendirebilirsiniz. Uzak masaüstü vb. birçok durum için geçerli.

SNAT - POSTROUTING : (Source NAT) Kaynak NAT, DNAT'ın tersine, paket başlığındaki kaynak adresi değiştirip yazar.

MASQUERADE : Bir SNAT türü, pakete maskeleme yapar, paketin kaynak adresi ve kaynak portu, sunucu adresiyle ve boş bir portla eşleşerek hedefe gider. Örnek olarak, ağdaki bütün istemciler aynı IP adresinden dışarı çıkar.

REDIRECT : (Yeniden yönlendirme) Gelen paketi direkt olarak başka bir portla ilişkilendirir/yönlendirir.

Yukarıda bahsi geçen "durum" (–state), derin bir mevzu olmamakla birlikte, biraz açmamız kullanım açısından iyi olacaktır.

State kullanabileceğimiz durumlar aşağıdaki gibidir:

NEW : SYN isteği doğrultusunda NEW state alırız, yeni bir bağlantı vardır, birkaç şekilde kullanılır ama örnek verme açısından; sisteme girişte yeni bir bağlantı açılır "NEW", gelen paket içerisinde SYN açık ACK boşsa, bu tür paketleri düşürmek saldırı durumunda avantaj olacaktır. Zira normalde "header" içi bu şekilde boş olmaz.

ESTABLISHED : Açık olan bağlantılara ait paketler. Paketler karşılıklı gidip gelip, bilgisayarlar arası sohbet başladığı zaman, bağlantı "NEW" durumundan "ESTABLISHED" durumuna geçer.

RELATED : An itibarıyla sistemde "ESTABLISHED" bağlantı varsa, aynı yerden aynı konu ile ilgili benzer istek geldiği zaman, durumu fark edip "hımm bunlar aynı konu üzerinde konuşuyor" diyerek bu bağlantıyı "RELATED" olarak işaretler. "RELATED" bağlantı gördüğümüzde böyle bir durum olduğunu anlarız.

INVALID : Diğer durumlara "state" uymayan durumlardır. Genelde bu paketler düşürülür. (Hata mesajı döndüren paketler vb.)

Bir sonraki yazıda, burada gördüğümüz teorik durumu pratiğe dökerek değişik senaryolar yaratıp, örnek oluşturup, üzerinde kendinize göre değişiklik yapacağınız ve geliştirebileceğiniz iptables "firewall" uygulamaları yer alacaktır.

Görüşmek üzere…