Açık Kaynak ile Güvenlik Duvarı

Kerem ERZURUMLU

Bu belge açık kaynak ile güvenlik duvarı (AKGD) kullanmayı düşünen kişilere yardımcı olması amacı ile hazırlanmıştır. Okunurluğu ve anlaşılırlığı artırmak amacı ile bilgiler soru/cevap şeklinde verilecektir.

S: AKGD'lerin avantajları ve dezavantajları nelerdir?

C: AKGD'ler x86 mimarisine sahip herhangi bir bilgisayar üzerinde çalışabilir. Çalışması için özel bir donanım gerektirmemesi ilk kurulum ve işletimi sırasındaki maliyetlerin hemen hemen tüm hazır güvenlik duvarından daha az olmasını sağlamaktadır. Benzer şekilde donanım üzerinde yaşanabilecek bir arıza sonucunda sistemin tamiri çok daha hızlı ve ucuz olarak sağlanabilmektedir.

AKGD'lerde lisans sınırlaması mevcut değildir. Kurulmuş olan bir AKGD işlemcisi ve belleği yettiği sürece/kişiye hizmet verir.

AKGD'lerin x86 tabanlı olması nedeni ile bir çok arabirim kartı (metro ethernet gibi) takılabilir ve bu arabirimler bu cihaz üzerinde sonlandırılabilir.

Bir AKGD ile diğer güvenlik duvarı çözümlerinde ayrıca satılan modülleri elde etmiş olursunuz.

AKGD olarak kurulmuş olan donanım, eğer arzu edilirse web sunucu, posta sunucusu, kurum mesajlaşma/takvim sistemi olarak da kullanılabilir.

Bunların yanı sıra AKGD'lerin düzenli olarak izlenmesi ve takip edilmesi gerekmektedir.

S: AKGD'ler hangi işleri yapabilmektedir?

C: AKGD'ler genel olarak "akla gelen her işi" yapabilir. Fakat en bilindik çözümler aşağıda listelenmiştir;

a. Yönlendirici (router)
b. Güvenlik Duvarı (Erişim Denetim Listeleri)
c. DHCP Sunucu
d. HTTP Vekil Sunucu (proxy)
e. Ağ Adres/Kapı Dönüştürme (NAT/PAT)
f. VPN
g. Web İçerik Denetleyici (Content managment)
h. Saldırı Tespit ve Önleme Sistemi (IDS/IPS)
i. İstenmeyen Trafik Önleyici
j. Posta Sunucusu için SPAM ve Anti-Virüs
k. Arzu edilen diğer internet sunucuları

S: VPN nasıl çalışıyor? Bazı VPN'lerin çalışması için istemci tarafında gerçek bir IP'ye ihtiyacı olduğunu duydum.

C: Açık kaynak VPN yazılımı 2 farklı ortam için çalışabilmektedir. İlki ağdan ağa, diğer ise personelden ağa.

Ağdan ağa bağlantılarda 2 ağ arasındaki tüm veri trafiği şifrelenir ve üçüncü şahısların dinlemesi önlenir.

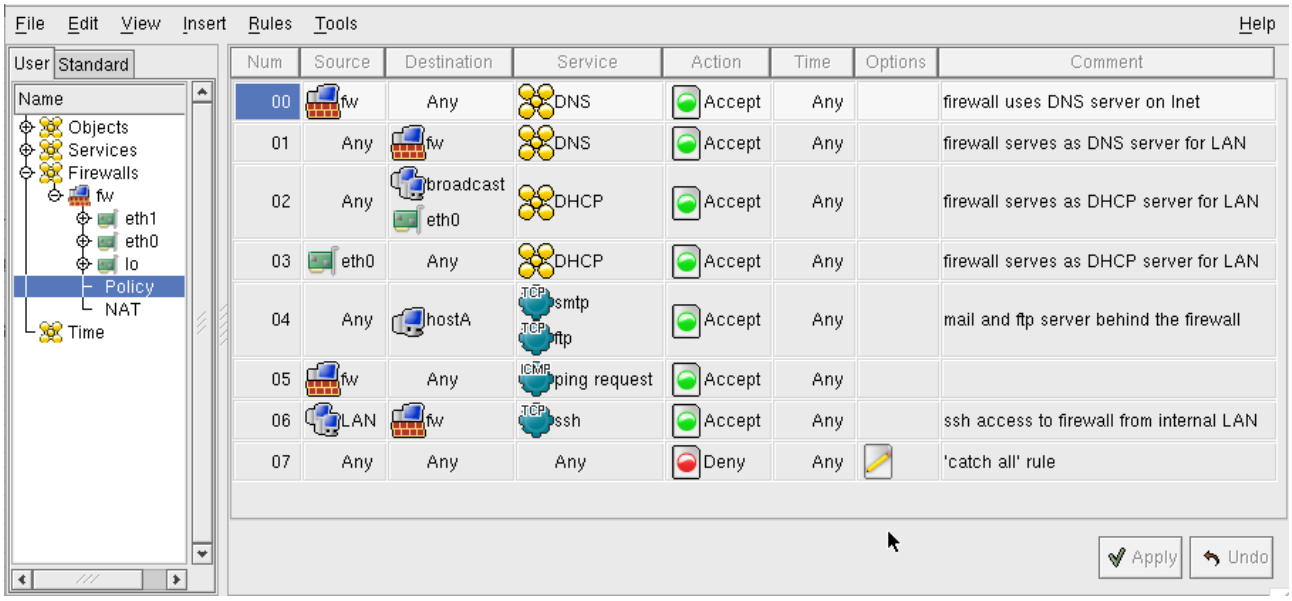
Personelden ağa kısmında ise yukarıda bahsedildiği gibi bir kısıtlama mevcut değildir. İstemci nerede olursa olsun, internet bağlantısına sahipse, IP'sinden bağımsız olarak VPN sunucusuna bağlanır ve yanlızca kurum yerel ağına gönderdiği istemler şifrelenir, internet'e yaptığı rutin istemler şifrelenmez. Bu hem performans hemde başarım artışı sağlar.

Ayrıca VPN istemciler arzu edilirse windows tabanlı işletim sistemleri ile de çalışabilmektedir.

Resim1: Windows ile VPN (En sol ikon)

S: Güvenlik Duvarında kuralları nasıl yönetiliyor ve kuralları zaman tabanlı yazmak mümkün mü?

C: Erişim Denetim Listelerini yönetmek için "fwbuilder" isimli uygulama kullanılmaktadır. Bu uygulama hem linux altında hemde windows altında çalışabilmektedir. Kuralların zaman tabanlı yazılabilmesi mümkündür. Resim 2'de ilgili programın örnek bir ekran görüntüsü yer almaktadır.



Resim 2: fwbuilder örnek ekran görüntüsü

S: Web İçerik Denetleyici ne demek?

C: Web içerik deneyleyici istemcilerin firma politikaları ile belirlenmiş web sayfalarına erişiminin engellenmesi demekdir. Örneğin firma kural olarak zararlı olabileceğini düşündüğü için warez, crack türü siteleri, personellerinin performansını düşürdüğü için oyun sitelerini yasaklarsa istemciler bu sitelere bağlanamayacaktır.

Web içerik denetleyicisi kendilerini sürekli olarak internet üzerinden güncelleyecek ve engellenen siteler listesini güncel tutarak en üstün başarımı sağlayacaktır.

S: Peki ya P2P (eDonkey, bittorrent vb) gibi programlar?

C: İstenmeyen trafik önleyici bu tür programların internete erişmesini engellemektedir. Bu engelleme işlemini ise standart güvenlik duvarları gibi kapı numaraları ile değil, paket içeriklerine göre yapar. Paket içeriğine göre engelleme yapan bir sistemin kandırılması çok zordur.

S: Peki MSN gibi sohbet programları da engellenebilir mi?

C: İstenmeyen trafik önleyici her türlü istenmeyen trafiği engelleyebilir.

S: Açık Kaynak sistemlerin yönetiminin zor olduğunu duydum. Doğru mu?

C: Kısmen evet. Açık kaynak kodlu sistemler birçok bileşenden oluştuğu için merkezi bir yönetim arayüzü mevcut değildir. Her bileşenin tek tek ayrı arayüzler aracılığı ile yönetilmesi gerekir.

S: Peki nasıl bir donanıma ihtiyaç duyacağım?

C: Sorunun cevabı firmanın kendi ihtiyaçlarında gizlidir. Öncelikle donanımın türüne karar verilmelidir. Sunucu Tabanlı mı, PC tabanlı mı?

PC tabanlı bilgisayarlar standart masaüstünde kullanılan bilgisayarlardır. Yedekli güç kaynağı, çift işlemci ve ECC bellek gibi bileşenler içermezler. Tamirleri daha kolay ve ucuzdur.

Sunucu Tabanlı bilgisayarlar 24 saat çalışmak üzere tasarlanmış bilgisayarlardır. Arzu edilmesi halinde yedekli güç kaynaklı, çift işlemcili, ECC bellekli olabilirler. Fakat bu bilgisayarların yedek parçaları daha pahalıdır.

AKGD için çoğu zaman tek işlemci tek başına yeterlidir. Fakat bazı uç noktalarda tek işlemci yeterli olmayabilir.

Eğer AKGD aynı zamanda posta sunucusu, dosya sunucusu, web sunucusu gibi ek işler de yerine getirecek ise çift işlemcili bir sunucu kaçınılmazdır.

Diğer durumlarda ise AMD Athlon64 3500+ işlemciye sahip 1G bellekli bir AKGD aynı anda 500 kullanıcının erişimini sağlayıp, web vekil sunucu olarak çalışıp, 10 civarı VPN bağlantısını yürütüp, istenmeyen trafiği engelleyebilir.

Eğer biraz daha esneklik istenirse AMD Athlon64 4200+ DualCore işlemli ve 2G bellekli bir sunucu ile 1000 kullanıcının internet erişimini sağlayıp, web vekil sunucu olarak çalışıp, 15 civarı VPN bağlantısını yürütüp, istenmeyen trafiği engelleyebilir.