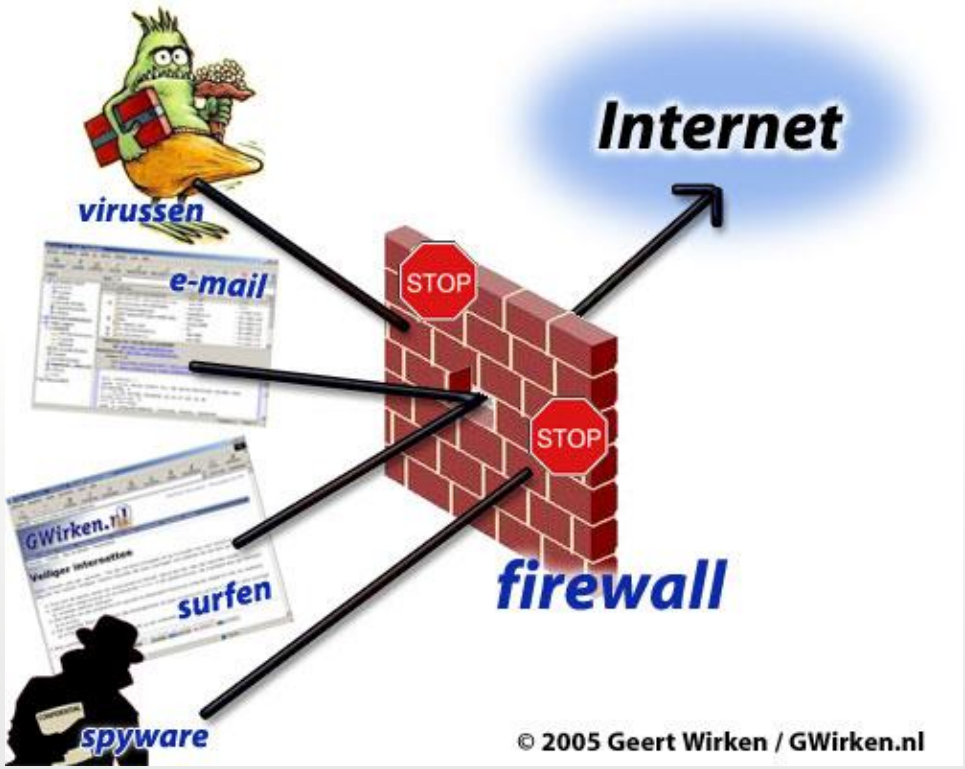
FİREWALL
IP TABLES
NAT

YUSUF SAVAŞLI

MÜCAHİT KARADAŞ

FİREWALL NEDİR?

- **Güvenlik duvarı** , güvenlik duvarı yazılımı, bir kural kümesi temelinde ağa gelen giden paket trafiğini kontrol eden donanım tabanlı ağ güvenliği sistemidir. Birçok farklı filtreleme özelliği ile bilgisayar ve ağın gelen ve giden paketler olmak üzere İnternet trafiğini kontrol altında tutar. İP filtreleme, Port filtreleme, Web filtreleme, içerik filtreleme bunlardan birkaçıdır.
- İnternet küresel kullanım ve bağlantı açısından oldukça yeni bir teknoloji iken Firewall teknolojisi 1980'lerin sonunda ortaya çıkmıştır.


Internet
virussen
e-mail
STOP
STOP
GWirken.nl
surfen
firewall
spyware
© 2005 Geert Wirken / GWirken.nl

GÜVENLİK DUVARININ TÜRLERİ

- Paket filtrelemeli güvenlik duvarları (*Packet Filters Firewall*)
- Durumlu denetim güvenlik duvarları (*Stateful Inspection Firewall*)
- Uygulama katmanı güvenlik duvarları (*Application Layer Firewall*)

PAKET FİLTRELEMELİ GÜVENLİK DUVARI

- Paket filtreleri, Internet üzerindeki bilgisayarlar arasında transfer edilen paket başlıklarını inceleyerek hareket eder.Bir paket güvenlik duvarından geçtiği sırada eğer başlık bilgisi, güvenlik duvarı üzerinde daha önceden tanımlanmış olan, "güvenlik duvarı paket filtresi" ile eşleşirse, ya paket atılır ya da reddedilerek kaynağa hata mesajları gönderilir.
- Bu tür paket filtreleme, paketin mevcut ağ akışının bir parçası olup olmadığına bakmaz.
- Paket filtrelemeli güvenlik duvarı OSI Modeli'nin ilk 3 katmanında çalışır. Paket başlığındaki bilgilerin hepsini baz alarak filtreleme işlemi gerçekleştirilebilir.

DURUMLU DENETİM GÜVENLİK DUVARI

- Veriyi kaynağından hedefine kadar takip eder. Uygulama tabakası güvenlik duvarı ise yalnızca gelen ve giden verinin başlık kısımlarını kontrol eder ve uygulama katmanındaki protokolleri kısıtlayarak güvenliği sağlar. Örneğin HTTP protokolü üzerinden bir Web sitesinin erişiminin engellenmesi buna örnek olarak verilebilir. Daha gelişmiş olanı durumlu denetim özellikte olanlar olup daha çok büyük ağlarınİnternet ve iç ağdaki trafiklerini kontrol eder.

UYGULAMA KATMANI GÜVENLİK DUVARI

- OSI Modelinde uygulama katmanı düzeyinde çalışır. En sık kullanılan güvenlik duvarı tekniğidir. Uygulama katmanındaki güvenlik duvarı, gelen paketin veri kısmına kadar olan tüm paket başlıklarını açıp kontrol edebilir ve filtreliyebilir.
- Uygulama katmanında filtreleme yapmanın en önemli avantajı bazı uygulamalar ve protokollerin anlaşılır olmasıdır (FTP, DNS, HTTP gibi).
- Günümüzdeki güvenlik duvarları da sadece port kapamak amaçlı kullanılmıyor. Yeni nesil güvenlik duvarları da U.T.M. (Unified Threat Management) (güvenlik duvarı, antivirüs, antispam, IDS/IPS, VPN, yönlendirici (router) gibi özellikleri olan) tümleşik cihazlardır. Her ne kadar bir dönem bilinen ateş duvarı markaları U.T.M. cihazlarının hantal ve başarız olduğunu iddia etse de günümüzde tüm ateş duvarı üreticileri U.T.M. cihazlarını üretmektedir.

GÜVENLİK DUVARININ FAYDALARI

- Güvenlik duvarı, yetkisiz kullanıcıların korunan ağın dışına çıkmasını önleyen, potansiyel güvenlik zayıflıkları olan servislerin ağa girmesini ve çıkmasını önleyen ve değişik IP aldatması veya yönlendirme saldırılarını kısıtlayan tek bir tıkama noktası oluşturur. Tek bir tıkama noktasının kullanılması güvenlik yönetimini kolaylaştırır.

GÜVENLİK DUVARININ ZARARLARI

- Güvenlik duvarı kendisine uğramadan geçen saldırılara karşı koruma yapamaz. İç sistem bir ISP'ye bağlantı için çevirmeli hat kullanabilir veya modem havuzu bulunabilir. Bu tür bağlantılar güvenlik duvarını devre dışı bırakabilir.
- Güvenlik duvarı dış saldırgan ile işbirliği yapan iç tehditlere karşı koruma sağlayamaz.
- Güvenlik duvarı virüs bulaşmış olan dosya ve programların iletilmesine karşı koruma sağlayamaz. Değişik işletim sistemi ve desteklenen yazılım çeşitliliği nedeniyle bütün dosyaların virüs testine tabi tutulması pratik değil hatta imkânsızdır.

IP TABLES

- Iptables Linux ve Unix yada BSD tabanlı sunucularımız üzerinden geçen trafiğin erişim denetimini sağlayan kural tabanlı bir uygulamadır. Iptables günümüzde birçok firewall yazılımının entegresi olarak kullanılmakta olan kural tabanlı bir erişim denetleyicisi olarak adlandırılabilir. Iptables ile erişim denetimi dışında birçok işlem yapılabilmektedir.
- Iptables kural tabanlı işlem denetimi yapar. Bu işlemler genellikle işlem, prosedür, protokol, hedef, kaynak, denetim şeklinde sıralı olarak gider.

İŞLEM

- A :Yeni kural eklemek
- I :Aralıklara kural eklemek
- L : Kuralları Listelemek
- N : İşlem eklemek
- X : İşlem silmek
- D : Kural Silmek
- F :Tüm kuralları silmek
- Z : Sayaçları sıfırlamak
- R : Kuralı Değiştirmek

PROSEDÜR

- İşlem sırasındaki bir sonraki parametre yapılacak işlemin prosedürünü belirtir. Sadece üç adet prosedür mevcuttur.

- INPUT : Dışarıdan gelen paketler.
- OUTPUT : Dışarıya çıkan paketler.
- FORWARD: Dışarıdan gelen ve bizim üzerimizden geçip çıkan paketler.

PROTOKOL

- Protokol denetimin yapılacağı yeri göstermektedir. Bu protokoller "TCP, UDP, SSH, RDP, HTTP, IMAP, POP3" olarak örneklendirilebilir. Protokolleri kullanabilmek için "-p" parametresi kullanılmalıdır.

HEDEF

- Hedef yapılacak denetim işleminin hedefini belirtmemiz gerekir hedef içinde "-d" parametresini kullanıyoruz .
- Hedef portu da "–dport" parametresi ile belirtiliyor.

- –d 10.0.0.2 --dport 80

KAYNAK

- Yapılacak işin kaynağı "–s" parametresi ile belirtilir. Kullanımı aynı Hedef işlemi gibidir.

- Port belirtmek içinde "–sport" parametresi kullanılır.

DENETİM

- Yapılacak işin denetimi belirtilmesi gerekir. Yani eklenmek istenen kuralın asıl amacı budur. Denetim yapmak için kullanılan betiklerin bazılarının anlamları şunlardır;

- DROP : Yasaklamak
- ACCEPT : İzin vermek
- REJECT : Yasaklamak ve yasak cevabı göndermek
- LOG : İşlemlerimizin kaydını tutmak

NAT

- **Network Address Translation** (**NAT**), TCP/IP ağındaki bir bilgisayarın yönlendirme cihazı ile başka bir ağa çıkarken adres uzayındaki bir IP ile yeniden haritalandırma yaparak IP paket başlığındaki ağ adres bilgisini değiştirme sürecidir.
- NAT, Ağ maskelemeyle (ya da IP maskelemeyle) birlikte, bir adres uzayını gizlemek için kullanılan teknik bir terimdir. Çoğu kez private network adreslerinden ibarettir .
- NAT'ın ciddi sonuçları vardır. İnternet kalitesine, bağlantısına ve uygulama detaylarına dikkat etmeyi gerektirir. Sonuç olarak, birçok yöntem gibi sorunlarla karşılaşılmış ve hafifletmek için icat edilmiştir.

NAT

- IP adres uzayı gün geçtikçe azalmaktadır. Bu azalmanın hızını yavaşlatmak için bazı yöntemler denenmiştir. IPv4'ün sayısının muhtemel yetersizliğini engellemek içinde kurumlar, ev kullanıcıları vs. için NAT, servis sağlayıcılar ve yönlendirmede kullananlar içinde CIDR gibi teknolojiler geliştirilmiştir.
- NAT özel bir IP adresi kullanarak yüzlerce cihazın internet ortamında haberleşmesini sağlar. Böylece IP adresi sıkıntısı kısmen önlenmiş olur.

NAT AVANTAJLARI

- Az sayıda IP kullanarak birçok istemciyi internete çıkarabilirsiniz. Hem parasal olarak kazanç sağlar hem de IP adresi azalmasını yavaşlatmış olur.
- Yerel ağımızı istediğimiz gibi tasarlamanıza da olanak sağlar. Yeni istemciler ekleyebilir. Adreslerini değiştirebiliriz veya yeni yerel ağlar ekleyebiliriz. Tek değiştirmeniz gereken NAT ayarlarıdır.
- Güvenlik sağlar. Yerel ağınızla internet arasında bir çeşit firewall gibi durur. Dışarıdan gelenler siz izin vermediğiniz sürece içeriye erişemezler.
- NAT'ın tek dezavantajı , bazı uygulamalarda sıkıntı yaşamasıdır.(FTP , IPSec gibi…)

NAT TÜRLERİ

- **Basit NAT (Basic NAT)**
- Bu sadece IP adres çevirimini sağlar,port haritalamayı sağlamaz. Sabit NAT da denir.
- **Değişken NAT (Dynamic NAT)**
- İnternet Servis Sağlayıcısından satın alınan 5 adet Ip adresini düşündüğümüzde, LAN üzerindeki bilgisayarlardan biri internete çıkmak istediğinde bu 5 Ip adresinden biri boşta ise o Ip adresini kullanarak internete çıkar.

PORT ADRES ÇEVİRİMİ

- Diğer adı Overloading (Aşırı Yükleme)'dir.
- Yalnızca tek bir genel Ip adresi ile LAN üzerindeki tüm bilgisayarları internette çıkarmakta kullanılır.
- Yerel port numaraları kullanılır.Bunlar; 1024-65535 aralığındadır.
- Bu işlemin tek farkı Ip adresi dönüşüme uğrarken eklenmesi ve çıktığı durumda ise port numarasının farklı olmasıdır.