Güvenlik Duvarları
ve
Duvardaki Paketler

Burak DAYIOĞLU ve Burç YILDIRIM
{bd,by}@dikey8.com

İçerik

- Güvenlik duvarı nedir, ne işe yarar?
- Güvenlik duvarı mimarileri
  - Paket filtreleme, devre düzeyi vekil, uygulama düzeyi vekil
- İlave Özellikler
- Yapılandırma
- Kayıtlar ve İncelenmesi
- Özgür Güvenlik Duvarı Yazılımları

Güvenlik Duvarı

- Güvenlik duvarı, bir ya da daha fazla ağ bölümü arasında duran ve bu ağlar arasındaki geçişleri denetleyen sistem ya da sistemler bütünüdür
  - Seçici geçirgenlik sağlamak ve yetkisiz erişimleri engellemek (Bekçilik yapmak)
  - Bağlantı kayıtları üretmek

Güvenlik Duvarı Mimarileri

- Paket Filtreleme
  - *(ing. Packet Filtering)*
- Durum Korumalı Paket Filtreleme
  - *(ing. Stateful Packet Filtering)*
- Devre Düzeyi Vekil
  - *(ing. Circuit Level Proxy)*
- Uygulama Düzeyi Vekil
  - *(ing. Application Level Proxy)*

Paket Filtreleme

- İletim (ing. transport) katmanında çalışır
- Paketin
  - Protokolüne (TCP, UDP, ICMP ...)
  - Kaynak ve hedef IP adreslerine
  - Kaynak ve hedef TCP/UDP port numaralarına
  - ...

  bakarak erişim denetimi kararı verilebildiği durumlarda
- En temel güvenlik duvarı uygulamasıdır
- Hemen tüm ağ aktif cihazları tarafından gerçekleştirilebilir

Paket Filtreleme - 2

- Paket filtreleme yapabilmek için aygıtın “durum bilgisi” saklaması gerekmez
  - Hangi iletişimin ne durumda olduğu bilinmek zorunda değil
  - TCP/UDP/ICMP’nin nasıl çalıştığı bilinmek zorunda değil
  - İletişim başlamış, sürüyor ya da bitmiş olabilir
  - Her paket için bağımsız olarak karar verilir
- Daha hızlı paket filtreleme
  - TCP temelli bağlantılarda yalnızca üçlü el-sıkışma (ing. three way handshake) paketlerini denetle
  - TCP bağlantılarında diğer tüm paketleri geçir
  - **Tehlike:** Başlamış bir iletişim varmışçasına gönderilen paketler güvenlik duvarını geçecektir

Durum Korumalı P. Filtreleme

- Paket filtreleme yeteneklerinin hepsini taşır
- TCP, UDP ve ICMP'nin nasıl çalıştığını bilir
- Bağlantılara ilişkin durum bilgisinin saklanacağı bir "durum tablosu" tutulur ve kullanılır
- Yeni paket geldiğinde
  - 1. Gelen paket mevcut bir iletişim ile "ilişkili mi"?
  - 2. İlişkili ise geçmesine müsaade et
  - 3. İlişkili değil ise
    - A. Yeni bir iletişim isteği ise kurallar ile karşılaştır
    - B. Kurallara uygun ise durum tablosuna kaydet
    - C. Kurallara uygun değil ise paketi durdur

İlişkili Olma Tanımı

- TCP bağlantıları için
  - Kaynak ve hedef IP adresleri
  - Kaynak ve hedef port numaraları
  - IP ve TCP sıra numaraları
  - TCP bayrakları

  kontrol edilir ve tüm bu alanları uygun olan paketlerin mevcut bir bağlantı ile ilişkili olduğu varsayılır
- UDP ve ICMP iletişimleri için
  - Bağlantılıymış gibi ele alınır
  - Giden bir UDP/ICMP paketinden sonra “bir süre” ilişkili yanıt paketini bekle

Devre Seviyesi Vekil (Proxy)

- İstemci ve sunumcu arasındaki veri akışını oturum (ing. session) katmanında kontrol eder
  - İstemci, vekil sunucuyla iletişim kurar, vekil sunucu tanımlanmış güvenlik politikasını temel alarak istemcinin hizmet alıp alamayacağına karar verir
  - İstemci, talep ettiği hizmeti ve hedef sunucuyu vekil sunucuya bildirir
  - Vekil sunucu, iki nokta arasında kendi üzerinde oturum bazında sanal bir devre oluşturur, ve iletişim başlar
  - Vekil sunucu uygulama protokolünü bilmez (konuşmaları anlamaz)
- Tüm iletişim süresince vekil sunucu arada durur
  - İstemci ve sunucu birbirinden izole edilir
  - IP, TCP/UDP/ICMP protokollerinin zaafiyetleri engellenebilir

Uygulama Seviyesi Vekil

- İstemci ve sunumcu arasındaki veri akışını uygulama katmanında denetler
  - Paketlerin içindeki “bilgilerin” denetimi
- İstemci ve sunucu arasında durarak tam bir yalıtım sağlar
- Uygulama protokolünü bilmesi (konuşmaları anlayabilmesi) gereklidir
- Web, ftp, e-posta hizmetleri için vekil sunucular yaygındır
- İçerik filtrelemeyi mümkün kılmaktadır

Doğru Mimarinin Seçimi

- Pek çok durumda durum korumalı paket filtreleme yeterli olacaktır
- Durum korumalı paket filtreleme en yaygın yöntemdir
- Güvenlik ihtiyacı/hassasiyeti yüksek ise durum korumalı paket filtreleme ve uygulama düzeyi vekiller bir arada kullanılabilir
- Uygulama düzeyi vekiller, paket filtreleme düzeneklerine göre daha karmaşıktırlar
  - Daha çok donanım kaynağı gereksinimi
  - Daha güç yönetim

İlave Özellikler

- Ağ Adres Dönüşümü (NAT)
- Kimlik doğrulama hizmetleri
- VPN sonlandırıcısı
- URL filtreleme
- İçerik filtreleme (virüs, truva atı, spam)

Paket Filtreleme Kuralları

- Mümkün ise yalnızca nelere izin verildiği belirtilmeli, izin verilmeyen her iletişim yasaklanmalıdır
- Kurallar olabildiğince detaylı bir biçimde belgelenmelidir
  - Hangi kuralların neden seçildiği anlatılmalı
  - Geriye dönük tüm eski kural kümeleri saklanmalı
- Kural sayısı çok arttığında güvenlik duvarı "bölünmelidir"
  - İki-üç A4 sayfası dolusu kural fazlası ile karmaşıktır
  - Yeni kural eklenmesi/çıkartılması esnasında hata yapma ihtimali çok ciddi bir biçimde artar

Kural Grupları

- Sınır Filtrelemesi
  - Giriş Filtreleme (ing. Ingress Filtering)
  - Çıkış Filtreleme (ing. Egress Filtering)
- Ağ hizmetlerine göre filtreleme

Giriş Filtreleme (Ingress)

- Ağınıza aşağıdaki IP adres bloklarından gelen paketleri sokmamalısınız:
  - 0.0.0.0/8 – default gw
  - 127.0.0.0/8 – loopback
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 255.255.255.255/32
  - 169.254.0.0/16 DHCP'den IP adresi alamayanlar
  - 224.0.0.0/4 Multicast grubu (RFC 1166)
  - 240.0.0.0/5 Rezerve (RFC 1166)
  - IANA rezerve IP adres aralıkları
    (http://www.iana.org/assignments/ipv4-address-space)
  - Güvenlik duvarının ardında kullanılan kuruma ait IP adres aralığı

Giriş Filtreleme - Devam

- Ağınıza aşağıdaki IP adres bloklarından gelen paketleri sokmamalısınız (devam):
  - ICMP redirect
  - ICMP broadcast, (RFC 2644)
  - UDP echo,
  - Güvenlik duvarının IP adresine gelen direkt bağlantı talepleri

Çıkış Filtreleme (Egress)

- Giriş filtrelemesinde, “bu IP adreslerinden gelen paketlere izin vermeyin” denilen IP adreslerinden dışarı doğru paketlerin gidişine izin verilmemelidir
  - 0.0.0.0/8 – default gw
  - 127.0.0.0/8 – loopback
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 255.255.255.255/32
  - 169.254.0.0/16 DHCP’den IP adresi alamayanlar
  - 224.0.0.0/4 Multicast grubu (RFC 1166)
  - 240.0.0.0/5 Rezerve (RFC 1166)
  - ...
  - Yalnızca kurum tarafından kullanılan IP adres aralığından dışarı paket çıkmasına izin verilmeli

Hizmete Özel Kurallar

- Hizmet kuralları belirlenirken minimalist yaklaşım sergilenmelidir
  - Olabildiğince az yetkili erişime izin verilmelidir
  - Bir bilgisayarın diğerine her türlü bağlantıyı gerçekleştirebileceği açık-uçlu kurallar tanımlanmamalıdır
  - İzin verilmeyen tüm işlemler yasaklanmalıdır
- Güvenlik duvarı kurma ve ayarlama çabasına girilmeden mutlaka ama mutlaka kurum güvenlik politikası belirlenmiş olmalıdır
  - Güvenlik duvarı, yalnızca belirlenen bir politikayı uygulamak için kullanılabilir

Güvenlik Duvarı Kayıtları

- Kayıtların amacı
  - Güvenlik ihlallerinin
  - Artan/azalan tehditin
  - Yapılan başarılı bağlantıların

  izlenebilmesi için zemin hazırlamaktır
- Mümkün olduğunca fazla kayıt üretilmesi sağlanmalıdır
  - Her kayıt işlemi güvenlik duvarını yavaşlatacaktır
  - Kayıt miktarı ve performans arasında bir denge noktası belirlenmelidir
- Kayıtlar için zaman senkronizasyonu şarttır

IPF Kayıt Formatı

May 14 18:04:08 arthur ipmon[26647]: 18:04:07.369711 dc0

Kayıt zamanı	Bilgisayar	Kayıt Süreci	Olay Zamanı	Arayüz

@0:12 b a.b.c.d,3965 -> w.x.y.z,113 PR tcp len 20 60 -S IN

Grup/Kural No	Eylem	Kaynak IP/Port	Hedef IP/Port	Protokol	Paket Boyu	Bayraklar/Yön

Örnek Kayıtlar

- May 11 11:49:37 Dikey8 ipmon[26647]: 11:49:36.878436 dc0 @0:12 b S1.SALDIR.COM,38392 -> Z1.ZAVALLI.NET,8080 PR tcp len 20 40 -S IN
  - Açık proxy taraması / verilmeyen hizmete bağlantı
- May 11 11:49:37 Dikey8 ipmon[26647]: 11:49:36.884593 dc0 @0:12 b S1.SALDIR.COM,38392 -> Z1.ZAVALLI.NET,110 PR tcp len 20 40 -FUP IN
  - Muhtemel port taraması

Örnek Kayıtlar (Devam)

- May 11 17:19:35 Dikey8 ipmon[26647]: 17:19:35.051015 dc0 @0:12 b 213.194.XX.XX,2044 -> 213.74.YY.YY,113 PR tcp len 20 60 -S IN
  - 213.74.YY.YY'nin bağlantı istemi sonucunda oluşmuş bir kimlik tanımlama (IDENT) isteği
- May 12 22:56:44 Dikey8 ipmon[15593]: 22:56:43.858374 dc0 @0:1 b 213.153.XX.XX,137 -> 195.155.YY.YY,137 PR udp len 20 78 IN
  - Kurum dışından SMB bağlantı isteği

Örnek Kayıtlar (Devam)

- May 10 02:39:06 Dikey8 ipmon[15593]: 02:39:06.024797 rl0 @0:1 b 212.211.XX.XX,23 -> 195.155.YY.YY,23 PR tcp len 20 40 -SF IN
  - Port taraması (Kaynak ve hedef port numaraları aynı)
- May 8 22:56:44 Dikey8 ipmon[15593]: 22:56:43.858543 rl0 @0:1 b 10.10.10.100,137 -> 195.155.YY.YY,137 PR udp len 20 78 IN
  - Müşterilerini birbirinden izole etmeyen İSS

Özgür Güvenlik Duvarları

- Netfilter/IPTables (D.K. Paket Filtresi)
  - http://www.netfilter.org
- IPF (D.K. Paket Filtresi)
  - http://coombs.anu.edu.au/ipfilter/
  - Yerel yansı: http://www.enderunix.org/ipfilter
- PF (D.K. Paket Filtresi)
  - http://www.benzedrine.cx/pf.html
- Delegate (Uygulama Düzeyi Vekil)
  - http://www.delegate.org/
- Dante (SOCKS uyumlu)
  - http://www.inet.no/dante/

Özet ve Sonuç

- Güvenlik duvarı planlama ve gerçekleştiriminden önce güvenlik politikası belirlenmelidir
  - Güvenlik politikasını belirlemeden uygulayamazsınız
- Güvenlik duvarları ağ güvenliği için “çözüm” değildir
- Güvenlik duvarının ayarlanması çok kısa sürede gerçekleştirilebilecek “basit” bir işlem değildir
- Sınırda giriş/çıkış filtrelemesi, kurumunuzu korumak için şarttır
- Güvenlik tek seferlik bir çalışma değil bir süreç işidir; metodolojik çalışma zorunludur

Gelecek Neler Getirecek?

- Geleneksel güvenlik duvarı teknolojisinin zaafiyetleri
  - Denetimi merkezileştirme çabası
  - Topoloji değişikliklerinin zorlanması
  - Ağ üzerinde darboğazlar
  - Tek hata noktası
  - Kural kümelerini makul ölçülerde tutulmasının güçlüğü
- Dağıtık güvenlik duvarları
  - Tüm uç sistemler üzerinde çalışan güvenlik duvarı “motorları”
  - Merkezi yönetim, dağıtık denetim