Açık Kaynak Güvenlik Duvarı Sistemi

Erkan Esmer

Nisan, 2016

İçindekiler

1 Unified Threat Management (UTM) Firewall - Birleştirilmiş Tehdit Yönetim Sistemleri -1

Bu yazımızda donanımsal olarak kullanılan açık kaynak Güvenlik Duvarı sistemlerini inceleyeceğiz.
Güvenlik Duvarı sistemlerine geçiş yapmadan önce

1. Güvenlik Duvarı tanımı
2. Güvenlik Duvarı gerekliliği
3. UTM Güvenlik Duvarı

maddelerini açıklamaya çalışacağız.

Yazımızı iki bölüm hâlinde sunmayı düşündük. Giriş ve tanımlama niteliği taşıyan birinci bölüme bu ay, Güvenlik Duvarı çözümlerine yer vereceğimiz ikinci bölüme ise önümüzdeki ay yer vereceğiz.

2 Güvenlik Duvarı Tanımı

Modemlerden yapılan bağlantılar, İnternet çıkışları, uzak bir sisteme bağlanma veya uzak bir sistemden bağlantı kabul etme gibi işlemler, sistemler arası bir trafik oluşturur. Bununla beraber bir tehdit de oluşmuş olmaktadır. Yapılan icraatın tehditlere açık olması sebebiyle izlenmesi ve emniyetinin sağlanması çok önemlidir.

Bu emniyeti sağlamada Güvenlik Duvarı sistemleri kullanılır. Temel olarak yerelden dışarıya yapılan çıkışlar veya dışarıdan sistemimize yapılan girişler, güvenlik duvarından geçer. Böylece trafik denetlenebilir, kısıtlama veya engelleme uygulanabilir.

Sistemlerde bu görevi icra eden cihazlara Güvenlik Duvarı denir. Güvenlik Duvarı, sistemin sağlıklı çalışması için en önemli güvenlik objelerinden biridir.

Şekil 1:

3 Güvenlik Duvarı Özelliklerinin Gelişimi

Güvenlik Duvarı ssistemleri, ilk üretiminden itibaren temel bir bakışla günümüze kadar aşağıda değineceğimiz özellikleri edinerek gelişmeler göstermiştir. Şimdi bunlara ve amaçlarına bir bakalım:

1) Paket Filtreleme

Paket filtreleme, gelen paketin yazılan kurala göre denetlemesi işlemini yapar. IP iletişim kuralını,IP adresini ve port numarasını güvenlik duvarına yazdığımız kurala göre denetler. Girilen kural yapılacak eylemde kesin belirleyicidir. Her gelen talepte veya pakette kurala tekrar bakılır ve kurala uygun olarak işlem yapılır. Bu yolla hizmet veren noktalara yapılan erişimlerin iyi niyetli veya kötü niyetli olduğu tespit edilemez. Paket filtreleme ile salt olarak trafik engelleme işlemi yapılabilir. Paket filtreleme, yeni nesil güvenlik duvarlarında artık bir modüldür.

2) Durum Denetleme (Stateful)

Durum denetleme ile paket filtreleme özelliği daha akıllı ve etkin şekilde kullanılır olmuştur diyebiliriz. Durum denetleme gelen talebin doğru bir talep olup olmadığına ve izin verilen yerden gelip gelmediğine bakabilir. IP, iletişim kuralı ve portlara bakarak saldırı niyetli bir talebi belirleyebilir. Durum denetleme, yapılan erişimler için kullanılan iletişim protokolünün prensiplerini de aktif şekilde kullanır. Gelen talepten aldığı pakete cevaben karşı tarafa bir paket gönderir ve tekrar bir paket alınca bağlantıyı kurar. (TCP-üçlü el sıkışma)

3) IDS -Intrusion Detection System-Saldırı Tespit Sistemi

IDS ile trafik sürekli olarak izlenir. IDS, şüpheli paketleri tespit eder ve gerekli bildirimi yapar.

4) IPS -Intrusion Prevention System-Saldırı Önleme Sistemi

IDS'ten farklı olarak şüpheli paketleri tespit eder ve ilgili trafiği kapatmaya varana kadar önlemler alabilir.

5) DPI -Deep Packet Inspection-Derin Paket İnceleme

DPI, IDS ve IPS'ten farklı olarak gelen paketin amacını algılamaya çalışan bir sistemdir. DPI, sadece kaynak IP, hedef IP ve port numarasına bakmaz. Trafiğin gelişimine göre alınacak önlemi veya verilecek izni belirler. Bu özelliği ile esnek bir kullanım ve duruma göre reaksiyon için daha isabetli bir ortam oluşturulmuş olur. Yani sistem daha esnek ve akıllı müdahalelerde bulunur. Örnek verecek olursak 100 numaralı portu kullanan bir uygulamanın bant genişliğini fazla işgal ettiği için bir kural yazarak alışverişini kesebiliriz. Fakat program 200 nolu portu kullanmaya başlarsa alınan önlem boşa gider. Ya da 100 numaralı port, başka uygulamalar için gerekli ise yaptığımız işlem başka uygulamaları etkiler.

DPI daha kolay bir tarif ile pakete derin bir bakış atarak ne işlem yapacağını, yani amacını belirlemeye çalışır ve paketin yapacağı işe göre bir filtreleme uygular.

Değindiğimiz bu birkaç nokta, Güvenlik Duvarı sistemlerinin gelişimi üzerine varılan en temel ve somut gelişmedir. Bahsettiğimiz bu sistemler tabii ki daha birçok özellik taşır. Biz sadece Güvenlik Duvarı sisteminin, niteliklerini belirleyici birkaç önemli noktaya dikkat çektik. Şimdi yazımızın başında belirttiğimiz maddelere devam edelim.

4 Güvenlik Duvarı Neden Gereklidir?

Gerek iş gerekse kişisel ihtiyaçlar için kullandığımız İnternet veya İnternet tabanlı hizmetlerde güvenliği sağlamanın gerekliliği artık günümüzde kaçınılmazdır.

Güvenliği sağlamak derken web dolaşımı, e-posta alışverişi, güvenli web sitelerine erişim, saldırıları tespit ve önlem alma gibi maddelerden bahsediyoruz.

Artık sistemlerin hizmet yelpazeleri genişledikçe kontrollü ve kararlı bir şekilde çalışması hem zorunlu olmakta hem de bunu sağlamak kolay olmamaktadır.

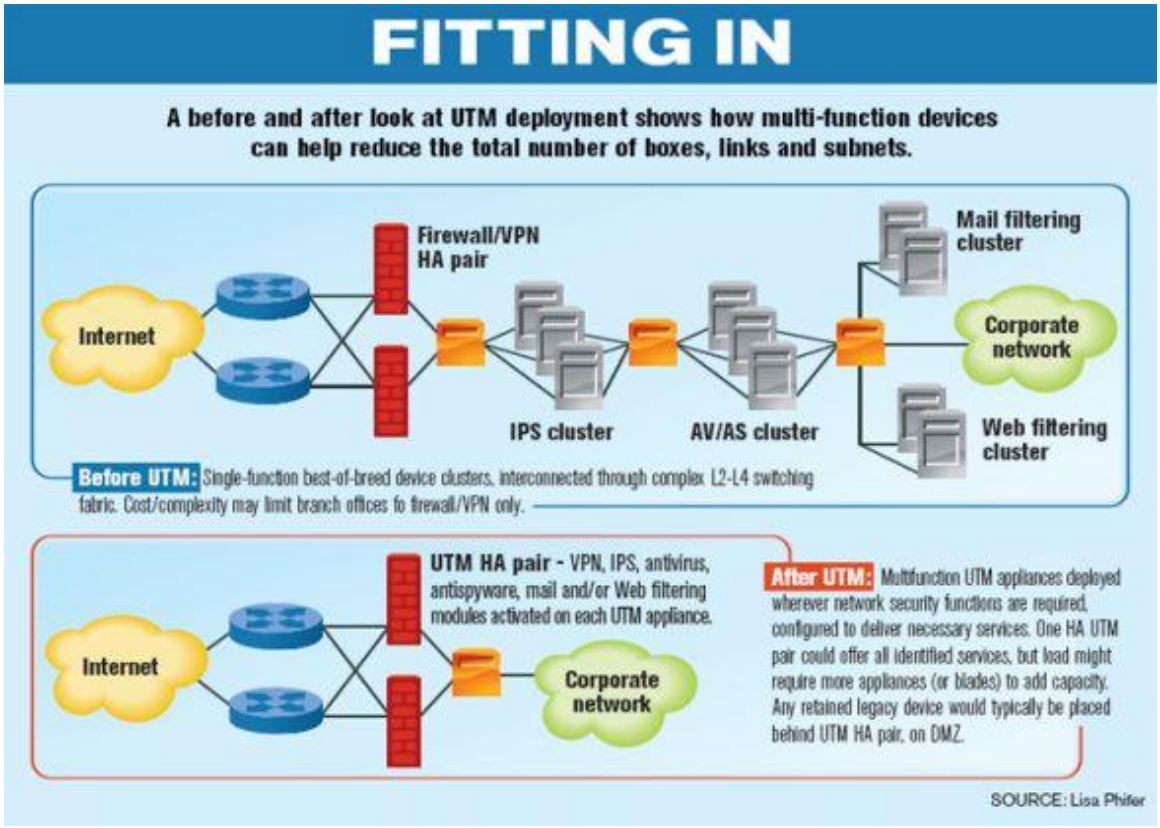
Ve üstelik artık günümüzde hedef, İnternet üzerinden yapacağımız bir işlemin sadece tamamlanması değildir. İşlemin güvenli bir şekilde tamamlanması büyük önem arz etmektedir. İnsanların aldıkları hizmette yaptıkları işlemlerde güvenli bir bölgede olmaları, özellikle iş dünyasında önemli bir sorumluluktur.

Bütün bunlarla beraber, güvenlik şartı teknik olarak gerekli olduğu kadar kanun olarak da bir şart olmuştur. Şöyleki İnternet erişimi sağlayan kurumlar 5651 yasası gereği İnternet giriş/çıkışlarını kayıt altına almak ve belli bir süre saklamak durumundadır.

5 UTM Güvenlik Duvarı -Birleştirilmiş Tehdit Yönetimi

Güvenlik Duvarı çözümleri, ihtiyaçlara göre gelişme sağlarken, birbirinden ayrı olan çözümleri (paket filtreleme,IDS/IPS) zamanla bir arada toplayarak birleştirilmiş bir tehdit yönetimi uygulaması hâline gelmiştir.

Üzerinde güvenlik duvarı, antivirüs, antispam, VPN, IDS/IPS gibi servisleri barındıran Güvenlik Duvarı Yönetim Sistemlerine UTM -Birleştirilmiş Güvenlik Yönetimi Sistemi denir.



Şekil 2:

Bu resmin, üstteki bölümünde UTM olmayan bir güvenlik çözümünü görüyorsunuz. E-posta filtreleme ve web filtreleme ayrı ayrı cihazlarla yapılmakta. Böyle bir düzeni kurmaktan ziyade yönetmek daha güç olsa gerek. Altta ise VPN, e-posta, web filter modüllerinin bir arada uygulanışını, aynı cihaz üzerinden yönetimini görebilirsiniz.

Böylece şunu söyleyebiliriz ki UTM cihazlarla beraber yönetim ve uygulama kolay hâle gelmiş olup bu tür ihtiyaçlarda başarılı çözümler bizlere sunulmuştur.

İlk bölümümüzü UTM cihazların bir arada bulundurduğu güvenlik duvarı özelliklerini toparlayarak tamamlayalım.

- İnternet üzerinde çok yaygın olarak kullanılan web dolaşımı, e-posta alışverişi, dosya transferi gibi işlemler için antivirüs hizmeti verir.
- İnternet üzerindeki uygunsuz içerikli sitelere erişimin engellenmesi veya kontrolü için içerik filtreleme hizmeti sunar.

- Kurulu olduğu sistem içinde tüm İnternet erişimini kendi üzerinden sağlayarak tüm trafiği yönetmemize imkân verir.
- Üzerinden geçirdiği bütün trafiğin kaydını tutar. Bu kayıtları da raporlar ile incelememize olanak sağlar.
- Önbellek özelliği ile İnternet erişiminde performans sağlar. Yapılan erişimler önbellekte tutulur ve tekrar erişim istendiğinde önbellekten erişim sağlanır. Bu da sistemin performansı için önemlidir.
- İnternet üzerinde kullanılacak programlar ve servisler kontrol edilebilr. Örnek olarak belli programların kullanılması veya belli dosya türlerinin (müzik, video dosyaları) indirilmesi engellenebilir.
- Saldırı tespit etme ve engelleme özelliği sayesinde sisteme izinsiz girme teşebbüslerini bildirir ve engeller.
- Yerel ağımıza aldığımız e-postaları, antivirüs ve antispam taramasından geçirerek e-posta alışverişimizin daha güvenli ve konforlu şekilde yapılmasını sağlar.
- Tüm bu aktiviteler izlenebilir ve raporlanabilir.

Güvenlik Duvarı sistemlerine giriş yaparak gelişimini anlatmaya ve son hali ile ilgili bilgiler vermeye çalıştık. Güvenlik ve güvenlik ekipmanları konusundan ne kadar bahsedersek bahsedelim yine de işin tümüne değinmiş olamayız. Özet bir yazı yazmaya çalışıp önemli noktaları ifade etmeye çalıştık.

Önümüzdeki sayıda, 2.bölüm yazımızla, açık kaynak UTM Güvenlik Duvarı uygulamalarından bahsedeceğiz.