

Firewall - Giriş

Lisans

Bu döküman **Fatih Özavcı** tarafından yazılmıştır. Amacı Firewall sistemlerini tanıtmak , mimarilerini ve örneklerle piyasadaki Firewall'ları incelemektir. Yazarın haklarına saygı duyarak her türlü kaynaktan yazılması ve yayınlanması serbesttir.

Firewall Nedir ?

Firewall ingilizceden ateş duvarı olarak çevrilmekte fakat pekte fazla anlam ifade etmemektedir. Aslında itfaiyecilerin kullandığı bir tabir olan Firewall kelimesinin nereden geldiğini anlatmak ne işe yaradığını daha iyi özetleyecektir. Binalarda yangın çıkması durumunda yanan bir odadaki alevlerin diğer odalara sıçramaması için özel oda duvarları yapılmıştır. Bu duvarlar ateşten etkilenmez ve ateşin yayılmasını büyük ölçüde önler. Bu duvarlara itfaiyecilerin verdiği isim ise Firewall'dur.

Peki günümüzdeki Firewall'larla ile ne ilgisi var ? İnternet güvensiz bir ağıdır , onu güvensiz kılan paylaşımın fazlalığı ve insanın doğal yoketme içgüdüsüdür. Yerel ağdaki özel bilgileri internetin getirdiği risklerden yalıtım isteniyorsa kullanılacak sistemlere de yukarıda anlatıldığı gibi Firewall denir. Kısaca amaç yanan internetin diğer ağları yakmasını engellemek denilebilir.

Birden fazla ağ parçası arasına kurulan Firewall sistemleri bu ağların yalıtılması işlemini gerçekleştirir. Bu ağlar internet , bayi ağı , müşteri ağı , hizmet alınan şirketlerin ağı yada yerel şirket ağı olabilir. Kullanım alanını sadece internet ile sınırlamak yanlıştır. Bu ağlar arası geçiş için çeşitli kural zincirleri ve erişim yetkileri belirlenir, böylece söz konusu ağlardaki kötü niyetli insanlardan etkilenme oranı büyük ölçüde düşer.

Ağlar arası yetkilendirme görüldüğü yada bahsedildiği kadarda basit bir kavram değildir. Bunun için çeşitli yöntemler uygulanmaktadır ve uygulanan yöntemler Firewall mimarilerininide çeşitlendirmektedir. Amacın sadece gelen paketi portuna, protokolüne veya geldiği yere bakarak filtrelemek olduğunu düşünmek bugün oldukça ilerlemiş olan Firewall sistemlerini yok saymak ile aynı düşüncedir. Çünkü bu sistemlerin farkları arasında statik olarak paket filtreleme , dinamik paket filtreleme (stateful inspection - stateful screening) ve uygulama proxy (vekil sunucu) gibi mimari farklılıkları , donanım veya yazılım çözümü olmaları , üzerinde çalıştıkları işletim sistemleri sayılabilir.

Firewall Nereelerde Gereklidir ?

Çeşitli ağ parçalarının birbirleriyle iletişim kurmalarını kısıtlamak ve bir ağı veya sunucuyu korumak amaçlı olarak Firewall kullanılabilir. Bugün Firewall ihtiyaç olarak düşünülmelidir , çünkü gelişen teknoloji ve saldırı teknikleri sahip olunan bilgileri yeterince büyük bir risk altında bırakmaktadır. Kaldı ki bireysel olarak internete bağlanan kullanıcılarda bile güvenlik sağlamak önemli olsaydı ticari kurumlarda güvenlik çok daha ileride olmak zorundadır. Bireysel kullanıcılara hergün çeşitli trojan saldırıları, DOS atakları gerçekleşirken kurumsal kullanıcılara da çok daha fazla saldırı gerçekleşmektedir.

Saldırıları engellemenin tabiki tek yolu Firewall değildir ve bunu düşünmekte bir hatadır. Ama güvenlik politikalarında önemli bir yeri olması gereken bileşenlerdendir. Ağda doğru şekilde düzenlenmiş bir Firewall gerek hız gerekse de güvenlik sağlayacaktır.

Tüm bahsi geçen saldırıları önlemek için öncelik Firewall sistemlerini düzenlemekten geçmektedir. Ağın dış dünyaya çeşitli kapılarla açıldığı unutulmamalıdır, eğer bu kapıların bazıları kapatılmazsa yada bu kapılardan gelen/giden paketler takip edilmezse davetsiz misafirleri ağda bulma olasılığı yükselir. Ağın ve bilgilerin mahremiyetini korumak için ilk ve en önemli bileşenlerden olan Firewall sistemleri saldırganları karşılayacak ilk sistem olması sebebiyle ciddi bir önem arz etmektedir.

Eğer bir sunucu için yerel ağın erişim yetkileri düzenlemek isteniyorsa , güvenilmeyen ağların veya kişilerin ağa girişleri kontrol altına alınmak isteniyorsa ve çalışanların çeşitli ağlara erişimleri kısıtlanmak isteniyorsa Firewall bu amaçlar için ciddi bir gereklilik teşkil etmektedir.

Firewall Mimarileri ve Farkları

Günümüzde Firewall sistemleri genel olarak 3 ayrı yapı ile birbirlerinden ayrılmaktadırlar. Bu yapılar Firewall'lara çeşitli artılar ve eksiler kazandırmaktadır. Bu bölümde 3 yapı hakkında çeşitli bilgiler verilerek ve karşılaştırmalar yapılarak Firewall'lar arasındaki farklar incelenecektir.

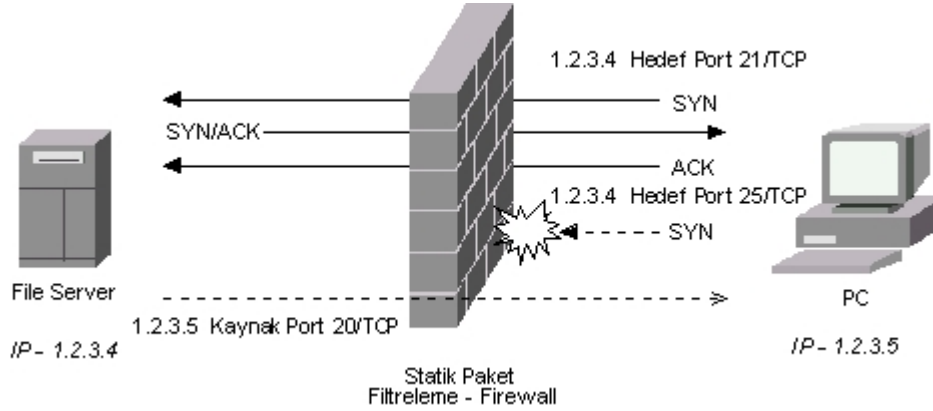
İlk mimari, statik paket filtreleme teknolojisidir. Bu mimari eskimiş olmasına rağmen halen Linux IPChains gibi bazı Firewall sistemlerinde kullanılmaktadır. Gelen ve giden paketleri sadece geldiği yer , erişmek istediği port numarası , protokolü gibi değerleri ile inceler ve bu değerlerden paketin erişimine izin olup olmadığını saptamasını yapar. Örneğin bir http isteği eline geldiğinde erişmek istediği portun 80, protokolün TCP ve geldiği yerin 1.2.3.4 IP'si olduğunu görür ve içerideki sunucuya ulaşmasına izin verilmişse, bu paketin içerideki sunucuya gitmesine izin verir. Basit bir mimaridir. Günümüzde ticari Firewall sistemlerinde kullanılmamaktadır. En büyük zayıflığı paketleri ilk gönderen sistemi yani oturumu ilk başlatan sistemi saptayamıyor olmasıdır. Bu durum ciddi riskler oluşturmaktadır, kaynak portu taramaları ve bağlantıları bu risklere örnektir. Bir örnek ile incelemek gerekirse ağdaki bir çalışanın FTP portundan iletişim kurabilmesi için izin verilmiştir. Oturumun işleyişi ise önce çalışanın 21/TCP portunu hedef port olarak belirleyerek bir sisteme dosya isteği göndermesi ile başlar, hedef sistem, kaynağı portu 20/TCP olan paketler ile çalışana dosya transferi yapar. Böyle bir durumda saldırgan ağa kaynak portu 20/TCP olan bir paket gönderdiğinde Firewall sistemi bu paketi görecektir ve içeriden bu pakete istek gelmeseydi bu paket gönderilmezdi mantığına dayanacak ve paketin içeriye girmesine izin verecektir. Firewall'un paketin hedef portuna bakmaması sebebiyle saldırgan kaynak portu 20/TCP olan paketlerle içerideki herhangi bir sistemin örneğin 139/TCP portuna ulaşabilecektir. Böylece Firewall üzerindeki erişim kontrol listeleri etkisiz kalacaktır. Bu sebeple oturumun baştan sona takip edilmesi , kimin ne istediği ve kimin ne gönderdiği bir tabloda tutulacak ve karşılaştırılacak bir sistem yaratılmıştır ; dinamik paket filtreleme sistemi - stateful inspection.

Dinamik paket filtreleme mimarisindeki Firewall'larda yukarıdaki örnekte anlatıldığı gibi klasik paket filtrelemenin yanısıra oturumu takip etme özelliğide vardır. Checkpoint firmasının ürettiği bu teknoloji yine bu firmanın tescilli markası olan Stateful Inspection ismiyle anılmaktadır. Günümüz Firewall sistemleri genelde bu sistem ile çalışmaktadırlar. Temel olarak TCP oturumları bir başı , ortası ve sonu olan oturumlardır. Hiçbir oturum başından veya ortasından kurulamaz. Bu durumda Firewall'lar kuralları sadece SYN flag'ıyla gönderilen paketlere (nereden gönderildiği önemli değil) uygular ve geriye kalan paketler oturumun tutulduğu tabloya bakılarak takip edilir. Böylece örneğin FIN veya SYN/ACK flag'lı paketlerin bir oturumun devamı olmadığından geçişi engellenebilir. Oturumun SYN flag'lı paketler ile başlayacağını düşünerek tasarlanan bu sistemin kuralları bu paketlere uygulaması oldukça mantıklı ve güvenlidir. Ayrıca TCP için olan bu oturum izleme işlemi ICMP ve UDP paketlerine de uygulanabilmektedir. Kaynak port taraması ile ilgili daha fazla bilgiye *Firewall Penetration Testleri ve Ağ Haritalama Teknikleri* isimli dökümanlarından ulaşılabilir. Ticari olmayan ürünlerden IPFilter (*BSD) , ticari ürünlerden Checkpoint FW-1 , Netscreen , Cisco PIX gibi birçok Firewall bu teknolojiye dayanır. Ancak bu teknolojinin zayıflıkları da vardır, paketlerin içeriğini kontrol etmemeleri bu zayıflıklarının başlıca sebebidir, ayrıca FTP protokolünün proxy özelliğini desteklemesi ve bunun kötüye kullanım oranını oldukça fazla olması Stateful Firewall sistemlerinin en büyük dezavantajlarından biridir.

Proxy mimarisini destekleyen Firewall'larda ise oturum başlatan ve hedef arasında gerçekleşmez. Oturum açmak isteyen taraf isteği Firewall'a gönderir ve Firewall bu paketi hedefe ulaştırır, hedeften cevap yine Firewall'a gelir ve Firewall tarafından oturumu açmak isteyen tarafa iletilir. Oturum açıldıktan sonrada aynı şekilde devam eder. Böylece 2 sistem arası tamamen yalıtılır ve Firewall paketlerin gerek içeriklerine , gerek hedef ve kaynak portlarına gerekse de gönderenin IP adresine müdahale edebilir. Paketlerin içeriğini kontrol edebilme Proxy Firewall'ların en büyük artılarından, böylece istenmeyen komutlar (HTTP paketlerinde POST komutunun kullanılmaması gibi) veya içerik (Java , ActiveX gibi) filtrelenebilir. Özellikle FTP Protokolü kesinlikle proxy olarak hizmet vermelidir, aksi taktirde FTP prtokolünün pasif FTP seçeneği ile saldırgan FTP sunucusundan içerideki sistemlere ulaşabilir, FTP Proxy kullanımı bu tür isteklerin Firewall tarafından filtrelenmesini sağlamaktadır. Stateful Firewall'lar gibi oturumu takip etmek zorunda değildir ; çünkü oturum zaten kendisi tarafından devam ettirilmektedir. Bu proxy'ler transparan (görünmeyen) proxy'ler olabileceği gibi normal proxy'lerde olabilmektedir. Yetersiz olduğu noktalara gelince araya girmesi ve paketleri kendisinin iletmesinin doğal sonucu olan yavaşlık ortaya çıkmaktadır. Ciddi bir yavaşlık olmamasına rağmen artan bağlantı sayısı ve yoğun ağlardaki veri trafiği , hızı olumsuz yönde etkilemektedir.

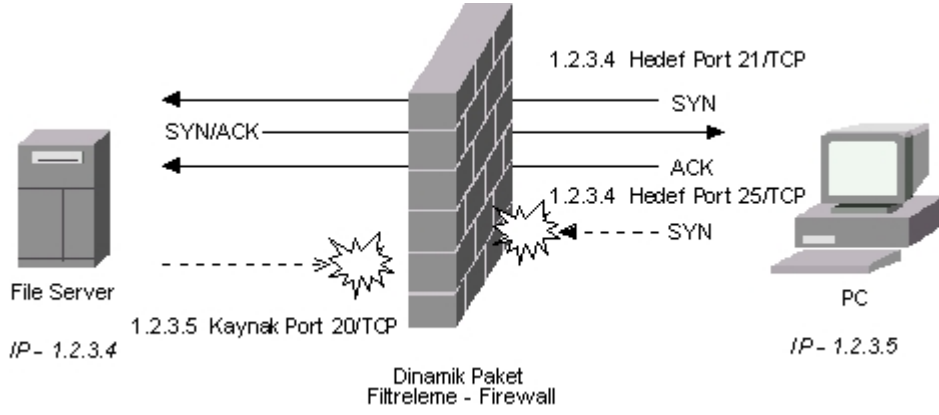
Bu mimarilerin 2 veya daha fazlasını barındıran Firewall sistemleride bulunmaktadır, bu sistemlere Hybrid sistemler denir. Bazı protokoller için proxy (Örneğin FTP, SMTP,HTTP) diğer protokoller için ise Stateful çalışabilen yada sürekli Stateful çalışabilen gereğinde proxy kullanılacak sistemlerdir. Yoğun ağlarda Stateful Firewall'lar , daha az yoğun yada güvenliğin önemli olduğu noktalarda Proxy Firewall'lar tercih edilmektedir.

Örnek şekiller ile bu mimarilerdeki farklılıklar aşağıda gösterilmiştir.



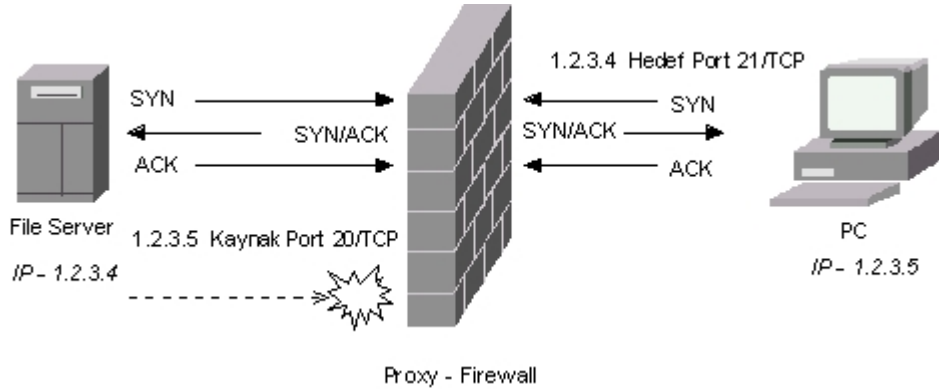
Şekil 1

İlk şekilde statik paket filtrelemenin nasıl olduğu görülmektedir. PC 1.2.3.4 IP'li dosya sunucusunun 21/TCP portuna bağlanırken Firewall izin veriyor. Ancak 25/TCP portuna bağlanmak istediğinde Firewall izin vermiyor. Dosya sunucusu ise isterse kaynak portunu 20/TCP yaparak PC'ye istediği porttan ulaşabilir. Çünkü Firewall PC'nin bir isteğinin karşılığında bu paketlerin gönderildiğini düşünür.



Şekil 2

İkinci şekilde ise dinamik paket filtreleme sisteminin nasıl işlediği görülmektedir. PC'nin isteklerinde sonuç değişmezken dosya sunucusunun kaynak portu 20/TCP olan paketi ise engellenmektedir.



Şekil 3

Son şekilde ise proxy mimarisinin işleyişi görülmektedir. PC'nin istekleri Firewall'a gelmekte ve Firewall üzerinden dosya sunucusuna ulaşmaktadır, cevaplar ise yine Firewall üzerinden PC'ye ulaşmaktadır. Kaynak portu 20/TCP olan paketler için yine engelleme söz konusudur.

Firewall Ürünleri

Piyasada yukarıdaki farklı mimari çeşitlerini kullanabilen , ticari yada açık kodlu , donanım yada yazılım olarak Firewall çözümleri mevcuttur. Bu ürünlerden bazıları aşağıda tanıtılmaya çalışılmıştır ; ancak aşağıda anlatılanlardan çok daha fazla çözüm piyasada bulunduğu için içerinde elemeler yapılarak anlatılmıştır.

Checkpoint firması ticari ürünleri FW-1 ile pazar lideri konumundadır. Solaris , AIX , Linux ve Windows gibi işletim sistemleri üzerinde çalışmaktadır. Donanım çözümlerinde Nokia firmasının donanımlarını yine bu işletim sistemleri ile beraber sunmaktadırlar. Stateful Inspection (Dinamik Paket Filtreleme) mimarisinde çalışmaktadır.

Gauntlet NAI firmasının Firewall çözümüdür. Proxy mimarisi ile Stateful Inspection mimarisini destekler. Windows 2000 için Firewall geliştirmeyeceğini açıklayan NAI, Solaris üzerinde yoluna devam etmektedir. Donanım çözümlerinde arasında Netscreen'inde bulunduğu farklı firmalardan donanımlar sağlayarak işletim sistemini ve Firewall'u yine bu donanıma kurmaktadır.

Cisco ise PIX ile piyasada Checkpoint'in en yakın rakibidir. Cisco IOS üzerinde çalışmaktadırlar. Donanım çözümü Cisco'nun Routerlarında kullandığı donanımlar gibidir. Stateful Inspection mimarisinde çalışmaktadır.

CyberGuard firması aynı isimdeki Firewall'u ile proxy mimarisini sunmaktadır. Aynı zamanda Stateful Inspection mimarisi ilede çalışır. Split DNS yapısı bir diğer artısıdır, amacı bağımsız iki ayrı DNS sistemi çalıştırarak ağda DNS'ten kaynaklanabilecek tehlikeleri gidermek ve DNS için ayrıca bir sunucu bulundurulmasını engellemektir. Donanım çözümlerini yine kendisi sağlamaktadır. Windows ve Unixware üzerinde çalışmaktadır. Donanım çözümleri özel olarak dizayn edilmiş , kernel'ı ve yapısı tamamıyla tekrar yazılmış bir Unixware ile sunulmaktadır. Tarantella ile uzaktan X erişimi , SSH sunucusu Unix sürümünün artılarındanadır.

Netscreen firması adıyla aynı ürününü Stateful Screening (Stateful Inspection ile aynıdır.) mimarisi ile sunmaktadır. Donanım çözümü olarak ve NetScreen'in kendi işletim sistemi ile gelmektedir. Donanımlar yine kendileri tarafından üretilmektedir. Transparan modunda çalışabilme artısına sahiptir, yani reel IP'lerin bulunduğu bir ağ üzerinden kendisini göstermeden yani trace çekildiğinde görünmeyerek gizlenmektedir. Hızı oldukça yüksektir , ssh sunucusuyla gelmektedir. VPN çözümü donanıma dahil olarak gelebilmektedir.

*BSD işletim sistemleri üzerindeki Ipfilter'ın ticari olmayan en güçlü Firewall olduğu söylenebilir. Kodu açık olmasına rağmen güvenliğini oldukça üst düzeyde korumaktadır. Stateful Inspection desteği mevcuttur. Proxy eklenebilmektedir. BSD Unix'in gücü ile birleştiğinde kararlılığı ve güvenliği üst düzeydir. Kullanımı konsol üzerinde yapılmaktadır. Donanım ihtiyacı oldukça düşüktür.

Linux ve Ipchains bir açık kodlu diğer alternatiftir. Statik paket filtreleme yapabilmektedir. Basit çözümler için tercih edilmektedir.

Sonuç

Firewall'un gerekliliği konusunun yeterince açık olduğu görülmektedir. Bugün ücretli veya ücretsiz çeşitli Firewall çözümlerinin mevcut olduğu da görülmektedir. Bu durum maliyeti yüksek denilerek güvenliğin önemsenmemesi gibi bir bahaneyi önlemektedir. Ücretsiz IPFilter'da ticari ürünler kadar kalitelidir. Ancak sonuçta ihtiyaçlar , genişleyebilirlik, vpn , anti-virüs, içerik kontrol gibi yazılımların kullanılabilirliği ve kullanılacak Firewall sistemlerinin örneklenen yada örneklenmeyen diğer sistemler ile uyumlu olması seçimi etkileyecektir. Güvenlik süreci düşüncede başlar , tasarım ile devam eder , kullanılacak ürünler ve sistemler ile biter. Gerisi tamamen yöneticilerin bu sistemleri yönetim gücüne kalır. Firewall seçimi konusunda daha sonra hazırlanacak yazı ile alınacak Firewall sistemi konusunda da yol gösterilmeye çalışılacaktır.

Referanslar

Checkpoint Inc.
Cisco Systems
Network Associates
CyberGuard Corp.
Netscreen
OpenBSD
FreeBSD
Linux