Bir Firewall Olarak İsa Server 2004®

Bir "Firewall" olarak ISA Server 2004®
Internet gibi public network'lere erişim (bilgi alışverişi), kullanıcılara ve a şirketlere ait verilerin güvenliğini tehdit etmektedir. Internet'e bağlı olan kullanıcıların ve şirketlerin bu tehlikenin bilincince olmaları gerekir. İşte firewall'lar, kullanıcı ve şirketlerin verilerinin Internet gibi dış network'ler ya da iç network üzerinden gelen risklere karşı korumayı sağlar.
Bir firewall, donanım ya da yazılım olarak yapılandırılabilir. Her iki durumda da genellikle iç (internal) ve dış (external) olmak üzere iki interface (network arayüzü) vardır. Birisinin korunması, diğerinin de erişilir olması gerekir; Firewall, iki network (private network ile public network) arasında bir gateway olarak yapılandırılır ve üzerinde geçen trafiğin kontrolünü yapar.

Bir firewall Ne Yapar?
Bir firewall iki network arasındaki trafiği inceler. Firewall lar kaynak adresi, hedef adresi, port adresi ve kullanılan protokole göre filtreleme yapar. Diğer bir deyişle, belli bir pakete izin verir (allow) ya da engeller (deny).
Firewall'lar OSI katmanlarına göre; üçüncü ve daha üst katmanlarda çalışırlar. Üçüncü katman network katmanıdır. TCP/IP protokolünde Internet Protokol'ü katmanı olan bu katmanda paketler hedeflerine yönlendirilir. Bu katmanda firewall'lar paketlerin güvenilir olup olmadığını ve doğru kaynaktan gelip gelmediğini kontrol ederler. Bu işleme filtreleme (filtering) denir. Paket filtreleme paketin adresinin kontrol edilir, ancak paketin içeriğine bakılmaz. Daha üst katmanlarda çalışan Firewall'lar ise application katmanında da çalışır ve paketin içeriğini de kontrol eder.

Firewall Olarak ISA Server
Firewall şirket network ünü Internet ten korumak ya da şirket network'ünün belli bölümlerini korumak için kullanılır. Genellikle perimeter network'te (ayrı bir network segmenti) oluşturulan firewall ların ana amacı Internet gibi public bir network'ten şirket network üne erişimin engellenmesidir. Örneğin şirketin bir Web server'ı olabilir ve kullanıcılar Internet üzerinden bu server'a erişmek isterler. Firewall, trafiği yalnızca Internet Web server'a erişmek üzere kısıtlayabilir.
ISA Server, firewall fonksiyonu ile varsayım olarak bağlı olduğu network (iç network, perimeter network) ile Internet arasındaki trafiği bloklar. ISA Server network trafiğini bloklamak ya da izin vermek için üç tür filtreleme yapar: paket filtreleme, stateful filtreleme ve application-katmanı filtreleme.

Paket Filtreleme
Bir firewall'un ana görevi, izin verilmeyen network trafiğinin internal (iç) network'e girmesini engellemektir. Bu işlem öncelikle paket filtrelemeyle (packet filtering) sağlanır.
Paket filtreleme firewall'a gelen bütün paketlerin başlık bilgisinin incelenmesidir. Paket filtreleme yalnızca network ve transport katmanı başlıklarını inceler.
ISA Server, network interface'i üzerinden gelen paketin başlığını açar ve kaynak adresi, hedef adresi ve port numarası gibi bilgileri oluşturulan kurallara (rules) göre kontrol eder ve gerekli işlemi (allow ya da deny) yapar.

Statefull Filtreleme
Stateful filtreleme network paketlerinin yönlendirilmesi kararının daha ayrıntılı verilmesidir. ISA Server bu ayrıntılı incelemede (stateful inspection) Internet Protocol (IP) ve Transmission Control Protocol (TCP) başlığını inceleyerek paketin durumunu; daha önce işlediği paketlerle (TCP oturumu içinde) karşılaştırır. Örneğin kullanıcının başlattığı bir Web isteği trafiğinin yanıtı geldiğinde, ISA Server bu paketin aktif oturumun parçası olup olmadığını kontrol eder.

Uygulama Katmanı Filtreleme
ISA Server ayrıca uygulama katmanı (application-layer) filtreleme ile paketlerin yönlendirilmesi kararını verir. Application-layer filtreleme paketin içeriğini inceleyerek gönderilen verileri kontrol eder. HTTP trafiğinin kontrolü için kullanılan bir HTTP filtresi, HTTP isteğindeki komutları ve verileri inceler. Böylece Web server'ların doğru isteklere yanıt vermesi sağlanır.

Intrusion Detection
Intrusion detection network yapılan (girişimde bulunulan ya da gerçekleşen) atakların (saldırıların) belirlenmesidir. Bir intrusion (izinsiz giriş) yeterince erken anlaşılırsa önlenmesi de o kadar kolay olacaktır. Bu nedenle, izinsiz bir giriş algılandığında hemen gerekli uyarılar (alerts) verilmelidir.

Intrusion Detection'ın önemli olması, intrusion-detection sistemlerinin (IDS) geliştirilmesine neden olmuştur. IDS'ler network'ün ucuna (edge) yerleştirilir ve gelen ve giden bütün network trafiğini inceleyerek atakları belirlemeye çalışır. Bir IDS, genellikle tipik atakları bilir ve network'e yapılan bu atakları anlar. Birçok katmanda çalışan IDS'ler elde ettikleri bilgileri toplam olarak verebilir .

ISA Server ve Intrusion Detection
ISA Server intrusion-detection işlevi görür ve birçok (bilinen) atağı izler. Network katmanında ve application katmanı düzeyindeki izinsiz girişleri (intrusion) izyelen ISA Server, sistem yöneticilerinin gerekli önlemleri almasını sağlar.

Sonuç
Şirketlerde çok sayıda kullanıcının network'e erişmesi, Internet gibi public network'lere sürekli bağlı kalınması şirketlerin özel bilgilerinin güvenliğini tehdit eder. Bu nedenle şirket network'lerinin Internet gibi public network'lere bağlanmasında güvenliği sağlaması bakımından firewall'lar geliştirilmiştir.
Bir firewall iki network arasındaki trafiği inceler. Firewall'lar kaynak adresi, hedef adresi, port adresi ve kullanılan protokole göre filtreleme yapar. ISA Server, firewall fonksiyonu ile varsayım olarak bağlı olduğu network (iç network, perimeter network) ile Internet arasındaki trafiği bloklar. ISA Server network trafiğini bloklamak ya da izin vermek için üç tür filtreleme yapar: paket filtreleme, stateful filtreleme ve application-katmanı filtreleme. Paket filtreleme firewall'a gelen bütün paketlerin başlık bilgisinin incelenmesidir. Stateful filtreleme ise network paketlerinin yönlendirilmesi kararının daha ayrıntılı verilmesidir. ISA Server, Internet Protocol (IP) ve Transmission Control Protocol (TCP) başlığını inceleyerek paketin durumunu; daha önce işlenen paketlerle (TCP oturumu içinde) karşılaştırır. Application-layer filtrelemede paketin içeriğini incelenerek gönderilen verileri kontrol edilir.

Faruk Cubukcu, 23.03.2006