FIREWALL

Firewall Nedir?

Güvenlik duvarı (firewall), bir ağdaki kaynakların, diğer ağlardan gelen kötü amaçlı veya yetkisiz erişimden korunmasına yardımcı olan bir güvenlik cihazıdır. Güvenlik duvarları, gelen ve giden ağ trafiğini filtreleyerek çalışır ve bu trafiği belirli kurallara göre denetler.

Güvenlik duvarı ne işe yarar?

Güvenlik duvarları, ağ güvenliğini sağlamanın en önemli araçlarından biridir. Aşağıdakiler de dahil olmak üzere çeşitli tehditlere karşı koruma sağlayabilir:

* **İnternet korsanları:** Güvenlik duvarları, internet korsanlarının ağlara yetkisiz erişimini engellemeye yardımcı olabilir.
* **Virüsler ve diğer kötü amaçlı yazılımlar:** Güvenlik duvarları, ağlara yayılan virüsleri ve diğer kötü amaçlı yazılımları engellemeye yardımcı olabilir.
* **DoS (Denial-of-Service) saldırıları:** Güvenlik duvarları, ağları DoS saldırılarından korumaya yardımcı olabilir.
* **İç tehditler:** Güvenlik duvarları, ağlara iç tehditler oluşturan kullanıcıları veya uygulamaları engellemeye yardımcı olabilir.

Firewall tipleri nelerdir?

Güvenlik duvarları, işleyişlerine göre iki ana kategoriye ayrılır:

* Donanımsal güvenlik duvarları: Bu güvenlik duvarları, özel donanım cihazlarıdır. Genellikle yönlendiriciler veya ağ geçitleri ile birlikte gelirler.
* Yazılımsal güvenlik duvarları: Bu güvenlik duvarları, bilgisayarlarda veya sunucularda çalışan yazılımlardır.

Güvenlik duvarları, filtreleme düzeylerine göre de sınıflandırılabilir:

* Paket filtreleme güvenlik duvarları: Bu güvenlik duvarları, paketlerin IP adresleri, portları ve protokolleri gibi özelliklerini kullanarak filtreleme yapar.
* Devre düzeyi güvenlik duvarları: Bu güvenlik duvarları, bir bağlantının tüm oturumunu kontrol eder.
* Uygulama düzeyi güvenlik duvarları: Bu güvenlik duvarları, belirli uygulamaları veya hizmetleri filtrelemek için kullanılır.

Güvenlik duvarı kuralları nasıl oluşturulmalıdır?

Güvenlik duvarı kuralları, ağ trafiğini filtrelemek ve koruma sağlamak için kullanılır. Bir güvenlik duvarı kuralını oluştururken, aşağıdakileri göz önünde bulundurmanız gerekir:

* İzin verilen trafik: Hangi tür trafiğin ağınıza girmesine izin vermek istediğinizi belirleyin.
* Yasaklanan trafik: Hangi tür trafiğin ağınıza girmesini engellemek istediğinizi belirleyin.
* Öncelik: Kuralların uygulanma sırasını belirleyin.

Güvenlik duvarı kuralları oluşturmak için çeşitli yöntemler kullanılabilir. Bazı güvenlik duvarları, yerleşik bir kural düzenleyicisi içerir. Diğer güvenlik duvarları için ise üçüncü taraf bir kural düzenleyicisi kullanmanız gerekebilir.

Günümüzdeki güvenlik duvarı özellikleri nelerdir?

Günümüzdeki güvenlik duvarları, aşağıdaki gibi çeşitli özellikleri destekleyebilir:

* İç tehdit koruması: Bu özellik, ağlara iç tehditler oluşturan kullanıcıları veya uygulamaları engellemeyi sağlar.
* Uygulama denetimi: Bu özellik, belirli uygulamaları veya hizmetleri filtrelemek için kullanılır.
* Kurumsal ağ güvenliği: Bu özellik, çok lokasyonlu ağların güvenliğini sağlamak için kullanılır.
* Bulut tabanlı güvenlik: Bu özellik, bulut tabanlı ortamları korumak için kullanılır.
* Yapay zeka (AI): Bu özellik, güvenlik duvarlarının daha iyi karar vermesine yardımcı olmak için kullanılır.

Güvenlik duvarları, ağ güvenliğini sağlamanın en önemli araçlarından biridir. Ağınızı kötü amaçlı veya yetkisiz erişimden korumak için bir güvenlik duvarı kullanılmalıdır.