Ağ Güvenliği ve Güvenlik Duvarları Nedir?

Çalışma Kağıdı

Ağ güvenliği, bilgisayar ağlarının bütünlüğünü, gizliliğini ve erişilebilirliğini sağlamak için alınan önlemler bütünüdür. Güvenlik duvarları ise bu önlemlerin başında gelen, ağ trafiğini izleyerek ve kontrol ederek belirlenen güvenlik kurallarına göre izin verilen veya reddedilen paketleri belirleyen donanımsal veya yazılımsal sistemlerdir.

Sorular

1. Aşağıdakilerden hangisi güvenlik duvarının temel işlevlerinden biri DEĞİLDİR?

A) Ağ trafiğini izlemek ve kontrol etmek
B) Yetkisiz erişimi engellemek
C) Ağ performansını artırmak
D) Zararlı yazılımların yayılmasını önlemek

2. Hangi güvenlik duvarı türü, ağ bağlantısının durumunu (state) takip ederek daha akıllı kararlar verebilir?

A) Statik Paket Filtreleme
B) Proxy Güvenlik Duvarı
C) Durumsal İnceleme (Stateful Inspection)
D) Uygulama Katmanı Güvenlik Duvarı

3. Bir şirketin dış ağ (internet) ile iç ağı arasına yerleştirilen güvenlik duvarı neyi korumayı hedefler?

A) Yalnızca şirket içi sunucuları
B) Tüm iç ağı ve bağlı cihazları
C) Sadece yöneticilerin bilgisayarlarını
D) Misafir Wi-Fi ağını

4. Bir şirketin iç ağı ile internet arasındaki güvenlik duvarının temel görevi nedir?

5. Ev kullanıcıları için güvenlik duvarı nasıl bir rol oynar?

6. Proxy güvenlik duvarı ile paket filtreleme güvenlik duvarı arasındaki temel fark nedir?

7. Tanımla: Ağ Güvenliği Nedir?

8. Tanımla: Güvenlik Duvarı (Firewall) Nedir?

9. Tanımla: Temel Güvenlik Duvarı Türleri Nelerdir?

Cevap Anahtarı

1. C) Ağ performansını artırmak — Güvenlik duvarının birincil amacı güvenliktir; ağ performansını artırmak doğrudan görevi değildir, ancak bazen optimizasyonlar içerebilir.

2. C) Durumsal İnceleme (Stateful Inspection) — Durumsal inceleme (stateful inspection) güvenlik duvarları, önceki paketlerle olan bağlantı durumunu takip ederek daha dinamik ve güvenli kararlar alır.

3. B) Tüm iç ağı ve bağlı cihazları — Genellikle dış ağ ile iç ağ arasına yerleştirilen güvenlik duvarı, tüm iç ağı ve bu ağa bağlı tüm cihazları dış tehditlere karşı korur.

4. 1. Gelen ve giden tüm ağ trafiğini denetler. 2. Önceden tanımlanmış güvenlik politikalarına göre paketleri inceler. 3. Yetkisiz erişim girişimlerini engeller ve zararlı yazılımların ağa sızmasını önler. 4. Yalnızca izin verilen bağlantıların geçişine izin verir.

5. 1. Modem veya router üzerindeki yerleşik güvenlik duvarı, ev ağını dış tehditlere karşı korur. 2. Bilgisayarlardaki yazılım tabanlı güvenlik duvarları, uygulamaların ağ erişimini kontrol eder. 3. Zararlı web sitelerine veya dosyalara karşı birincil savunma hattını oluşturur.

6. 1. Paket filtreleme, paket başlıklarını (kaynak/hedef IP, port) inceler ve kurallara göre geçirir. 2. Proxy güvenlik duvarı, istemci ile sunucu arasında bir vekil görevi görür, trafiği sonlandırır ve yeniden başlatır, daha derinlemesine inceleme yapabilir.

7. Ağların yetkisiz erişim, saldırı ve zararlı yazılımlardan korunmasıdır.

8. Ağ trafiğini denetleyerek güvenlik kurallarına göre izin verilen veya reddedilen paketleri belirleyen sistemdir.

9. Paket Filtreleme, Durumsal İnceleme (Stateful Inspection), Proxy ve Uygulama Katmanı Güvenlik Duvarları.