

ÖN BİLGİ

Bu belge

- <https://www.bgasecurity.com/makale/ddos-engelleme-urunleri/>

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Ddos%20Engelleme%20%C3%9Cr%C3%BCnleri.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

DDOS Engelleme Ürünleri

- IPS Ürünleri
- Firewall Ürünleri
- Tek işi DDOS Olan Ürünler

(Page 2)

2)

Bazı Firewall'lar

- Fortinet
- Netscreen

(Page 5-6)

3)

Güvenlik duvarları DDOS saldırılarını engelleme amaçlı düşünülmemiştir. İstisnalar elbette mevcuttur: Örn; Packet Filter gibi...

(Page 10)

4)

CheckPoint

CheckPoint en fazla tercih edilen güvenlik duvarı yazılımıdır. Donanım versiyonları da vardır.

Benim NOT: Hatırlarsan Barikat A.Ş'ye mülakata gittiğinde sınav olurken karşında Check Point cihazının kutusunu görmüştün. Üzerinde Check Point yazıyordu. Demek ki o firewall'mış.

(Page 13)

5)

Fortinet

Fortinet donanımsal güvenlik duvarlarından (firewall'lardan) biridir.

(Page 21)

6)

DDOS konusunda özellik bakımından en gerçekçi savunmayı IPS sağlar. DDOS özelliklerinin çoğu istatistiksel bilgiye dayanır. IPS bu istatistiksel veriye göre iyi ayarlanmazsa false positive (yanlış alarm) olayı ciddi miktarda olup rahatsızlık verebilir.

