

## Cisco IOS Firewall

Son Güncelleme Pazartesi, 03 Kasım 2008

Firewall yapılarında 3 tane teknoloji kullanılabılır. Packet filtering, application gateway(layer 7 de çalışır), stateful packet filtering(layer 7 de çalışır). Cisco IOS Router üzerinde kuruludur, hem router hem de firewall olarak çalışabilir, üzerinde acl ler yapılabılır, DOS ve DDOS atakları önlenabilir.

Yapıdır ve en basitten adsl modemlerde de olabilir. Kullandığımız yapıda DMZ yoksa da oluşturalabiliriz. Inside ve outside lar paketleri filtreleme yaparlar. DMZ yapısı aslında layer 4 e kadar çıkar. DMZ portu olmayan bir porta dmz yapabilmek bir nevi acl yazmaktır. Inside dan DMZ e girip her zaman serbesttir, fakat DMZ ten inside a girip te yasakla karşılaşırız. DMZ arındırılmıyıp bölge dir. Genellikle PIX ve ASA nın bir sürü DMZ portu vardır. Web ve ftp gibi serv lar DMZ te bulundurulurlar. Cisco IOS IPS: SDF denen bir yapı ile çalışır. IPS, üzerinde olan imzaların sayesinde saldırıları önler. IDS, 700 den fazla atak çepidine karşı önlem alır. Dört act vardır; Alarm Drop Reset Block IDS olup olmadığının denetlerler. CISCO IOS FIREWALL WORKS 1 nci Aşama firewall u etkinleştirir. İP INSPECT NAME komutunu biz router a verdigimiz zaman aslında router a bundan sonra firewall gibi çalışıp tcp ye bakıcağın demiş oluruz. Örnek : ip inspect name FWRULE tcp 2 nci Aşama: Access-list yazarız. (Firewall creates a dynamic acl allowing return traffic back through the firewall) Access-list 102 permit tcp host 172.30.1.50 eq 23 host 10.0.0.3 eq 2447 Desteklediği Protocoller; TCP (Single channel) UDP (Single channel) RPCFTP/FTPSTFTPTELNET/SSHSMTPICMPSNMPKAZAASQL NETTACACS+RADYUSBGPSIP Router(config)#ip inspect audit-trail (bu komutla syslog server kullanıcağımızyı belirtiriz. Router(config)#no ip inspect alert-off (normalde alert kapalıdır ve bu komutla açarız) Router(config)#logging on (syslog server kullanılmayı için gereken komut) Router(config)#logging host 10.0.0.3 (syslog server ıp si) IDS (Detected System) IDS ler sadece gelip giden paketleri izler, bu paketleri açar ve bakarlar, gene IPS ler gibi üzerindeki imzalar (signature) sayesinde önlemleri yaparlar. Çalışma şekilleri; Signature-based Policy-based Anomaly-based (trafiği izler, trafikteki alçalmalara ve yükselmelere göre önlemler alınır) IDS leri istersek host-based istersek network based olarak çalıştırabiliriz. IDS leri atak tiplerine, servislere, işletim sistemlerine ve network protokollerine göre yapabiliriz. Signature ları üç katmana göre yapabiliriz; Application Layer Transport Layer Network Layer SDF location ın nerde olduğunu göstermek için kullanılan komut ; İp inspect location dir. Normalde signature ler çok azdır ve sdf gibi uygulamalar ile bunu Cisco da 1200 imzaya standart tada 1500 imzaya çıkartabiliriz.