Bilgisayar Sistemleri Güvenliği

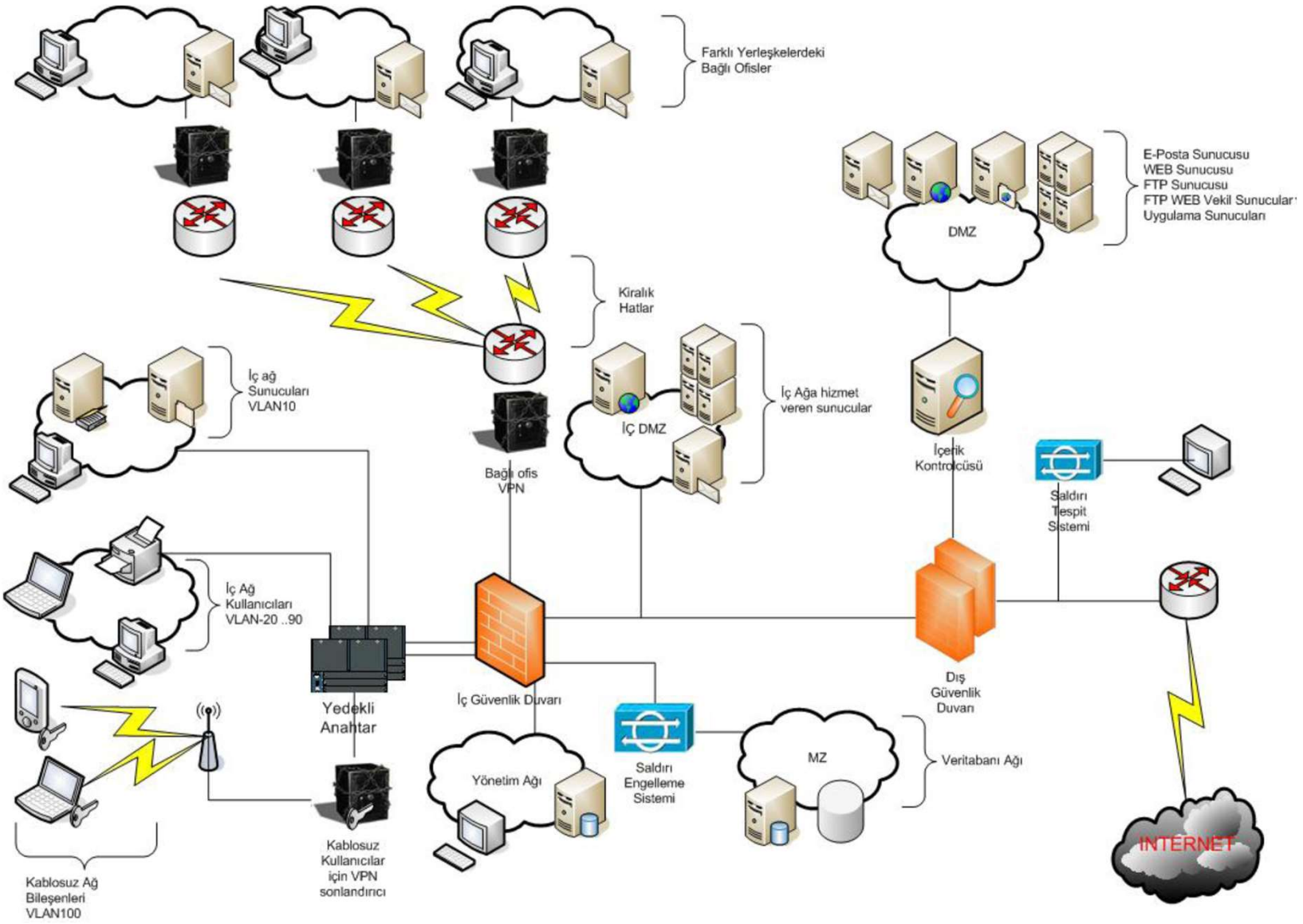
SİSTEM GÜVENLİĞİ

- Günümüzde , değişik boyutlardaki bilgisayar sistemleri birçok saldırıya uğramaktadır. Maruz kalınan saldırıların kaynağı ve şekli incelendiğinde, saldırıların basitleştiği, başarılı saldırılar için kullanılan bilginin yaygınlığının arttığı gözlemlenmektedir.

- Birçok saldırı için **ağ mimarisinde alınacak tedbirlerle başarılı saldırı sayısı azaltılabilmektedir.** Bu sebeple birçok noktada ağın yapılandırmasında güvenlik, performansın da önüne geçebilmektedir.

- Özellikle dış dünyaya verilen hizmetlerde, güvenli ağ tasarımının büyük önemi vardır. Çünkü bu tür bilgi paylaşımında bulunan bir ağın saldırganlar tarafından ele geçirilmesi, devre dışı bırakılması, ağdan bilgi çalınması veya ağın kaynaklarının kötüye kullanılması kurum ve/veya kuruluşlara para, itibar, iş ve zaman kaybı olarak yansıyacaktır.

Çok Sayıda Güvenlik Cihazı İçeren Bir Mimari Model



Bir bilgisayar ağ sisteminin güvenliğinden maksat, ağdaki aktif cihazların ve ağın bütnünün saldırılardan korunması anlamındadır.Bu güvenliğin sağlanabilmesi için

Güvenlik Duvarı(Firewall):Ag güvenlik duvarı , kurumun agı ile dıs aglar arasında bir geçit olarak görev yapan ve nternet baglantısında kurumun karsılasabilecegi sorunları çözmek üzere tasarlanan çözümlerdir.

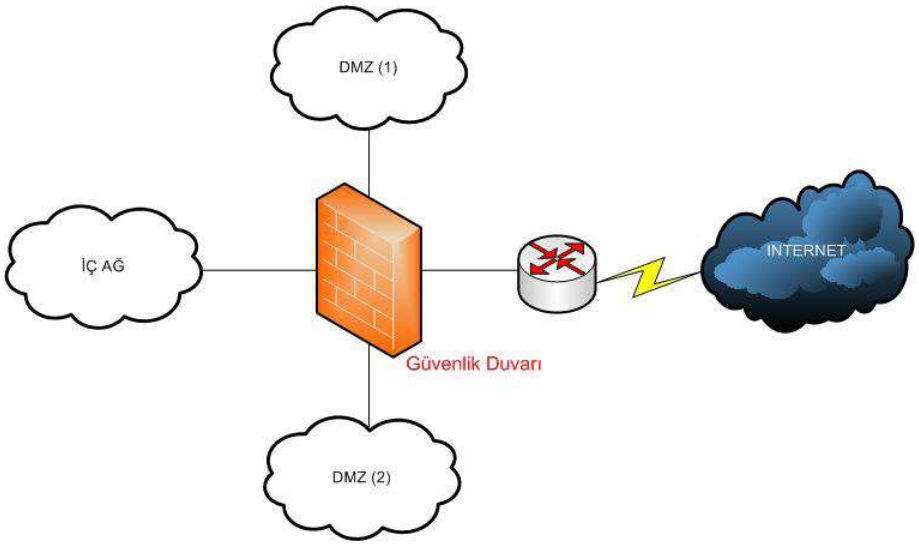
• ***Özel Sanal Aglar (Virtual Private Network-VPN):*** Ortak kullanıma açık veri agları üzerinden kurum agına baglantıların daha güvenilir olması için VPN kullanılmaktadır. İletilen bilgilerin sifrelenerek gönderilmesi, Genel/Özel (Public/Private) anahtar kullanımı ile saglanır. VPN kullanan birimler arttıkça daha sıkı politika tanımları gerekli hale gelmektedir.

• **(Saldırı)** ***Nüfuz Tespit Sistemleri (Intrusion Detection Systems-IDS):*** Süpheli olayları, nüfuz ve saldırıları tespit etmeyi hedefleyen bir sistemdir. IDS, süpheli durumlarda e-posta veya çagrı cihazı gibi yöntemlerle sistem yöneticisini uyarabilmektedir.

- ***Proxy:*** Proxy bir baglantı uygulamasında araya giren ve baglantıyı istemci (client) için kendisi gerçeklestiren bir hizmettir. Proxy'nin kullanımı, uygulama temelli (application-level) güvenlik duvarı olarak da adlandırılabilir. Bu tür bir uygulama aynı zamanda kimlerin bu hizmetleri kullanacagını belirlemek ve performans amaçlı olarak bant genisliginin daha etkin kullanılmasını saglamak için de kullanılır.
- • ***Anti-Virus Çözümleri:*** HTTP, FTP ve SMTP trafigini üzerinden geçirerek virüs taramasını yapmayı ve kullanıcıya gelmeden önce virüslerden temizlemeyi hedefleyen sistemlerdir.
- • **İ*çerik Süzme (content filtering):*** Çesitli yazılımlarla ulasılmak istenen web sayfalarını, gelen e-posta'ları süzmeye yarayan sistemlerdir.
- ***VLAN :*** Yerel ağların kendi içerisindeki performansı ve güvenliği arttırmak için, aynı switche bağlı bilgisayarların farklı şekilde guruplanmasıyla elde edilen sistemler.
- Bu servislerin hepsinin konfigürasyonu ve kullanacakları kuralların belirlenmesi, izlenecek güvenlik politikasına göre yapılmalıdır.

Güvenlik Duvarları

- Firewall'ler bir tür erişim denetleyicidirler. Kendi özel ağınız ile publik ağ arasında çalışarak iki yönlü bir şekilde trafiği denetlerler.Networke giriş bu nokta üzerinde yapılır.
- Temel olarak bir firewall, network üzerinde kendisine gelen paketleri, tanımlanan kurallar dogrultusunda geçirip geçirmeyecegine karar verir.
- Hardware veya software olarak gerçekleştirilebilir. Örnek olarak Firewall konfigirasyonuna izin verern Routerlar veya Pix veya ASA serisi kutu çözümleri donanımsal Firewallere örnek verilebilir.
- ipfw, ipchains, pf gibi yazılımsal çözümler ise Unix, Windows XP and Mac OS gibi işletim sistemleri üzerine kurulabilir.
- Güvenlik duvarı belirli bir makineyi denetlemek için o makine üzerine (host-based) kurulabileceği gibi, bir bilgisayar ağını denetlemek için de kurulabilir.



<u>Yarı Güvenli Bölge Yapısı (DMZ):</u> Eğer iç ağ farklı güvenlik seviyesine sahip bölgelere ayrılmışsa ve bu bölgeler arasında akan trafiğin güvenlik duvarı tarafından denetlenmesi isteniyorsa bu yapı kullanılmalıdır . DMZ'de genellikle işletmenin web, e-mail,ftp v.b dışa açık server'ları bulunur.

<u>Güvenli bölge:</u> Firewll'ın koruduğu ağ bölgesidir. Belirli politikalar dahilinde koruma sağlanan ağ bölgesidir. Örnek;İntranet

<u>Korumasız bölge:</u> Firewall'ın önündeki ağdır. Örnek İnternet

Bir güvenlik duvarı çeşitli işlevleri yerine getirebilir

- Ağ trafiğini Filtre ve kontrol eder.
- Olayların kaydını tutar (trafik).
- içerik taramayı gerçekleştirebilir. (virüs tarama motorları, içerik engelleme, url filtreleme , Protokol uygunluk test)
- Adres değişimi (Network Address Translation NAT fonksiyonu gerçekleştirmek) uygulayarak iç yapının dışarıdan gizlenmesini sağlar.
- Atakları belirlediğinde diğer güvenlik cihazlarına uyarılar gönderir.
- Bir sanal özel ağ (VPN) sunucusu olarak kullanılabilir.
- Yöneticilerin kimlik doğrulamasını yapar.

Firewall'ler değişik OSI katmanlarında trafiği kontrol edebilirler

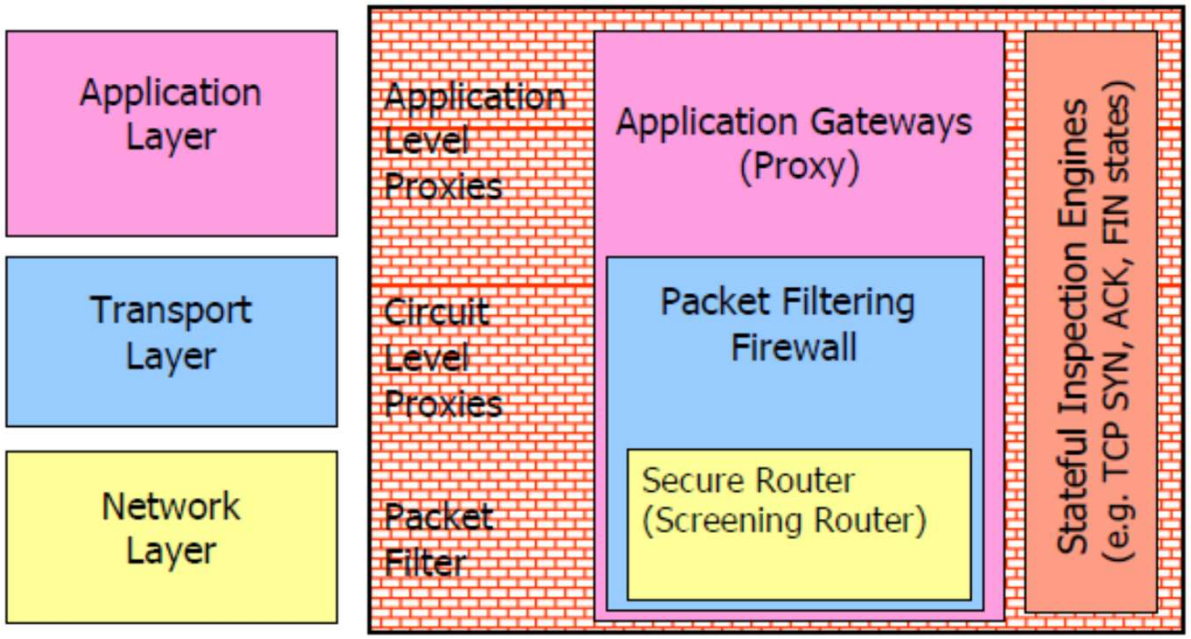
Ana güvenlik duvarı teknolojileri şunlardır:

-Paket filtreleme: Paketleri sadece başlık bilgilerine göre değerlendirir.

- Statik Paket Filtreleme
- Durum denetimli Paket Filtreleme (Stateful Inspection)

- İçerik Filtreleme (Deep packet İnspection): Paketlerin uygulama içeriğinede bakıldığı teknolojidir.

- Uygulama Seviyesi (Proxy özelliği): Bağlantıların sonlandırıldığı ve paketlerin içeriğinin denetlendiği teknolojidir.



Paket Filtreleme (Ağ Katmanı Firewalları)

- IP paketlerinin başlık alanı içindeki bilgilere bakılarak istenmeyen paketler karşı tarafa geçirilmez. Bu amaçla bir kurallar tablosu oluşturulur. Bu tabloda belirtilen kurallara uymayan paketler karşı tarafa geçirilmeyip süzülür. Bu tür firewall oluşturmanın en kolay yolu konfigüre edilebilir bir yönlendirici (router) kullanmaktır.
- IP başlığındaki kaynak adres, hedef adres ve port numarası bilgilerine bakılarak gelen veri analiz edilir ve ona göre geçirilir veya atılır; veya göndericiye bir mesaj gönderilir.

Filtre kurallarına bir örnek – Default Politika

• Hiçbir paketi reddetme

iptables –P INPUT ACCEPT
iptables –P FORWARD ACCEPT
iptables –P OUTPUT ACCEPT

• İzin verilmeyen herşeyi reddet.

iptables –P INPUT DROP
iptables –P FORWARD DROP
iptables –P OUTPUT DROP

Iptables, Linux işletim sisteminin varsayılan güvenlik duvarıdır. Bu güvenlik duvarı servislerin çalıştığı portlardan geçen trafiği engelleyebilir, başka bir porta yönlendirme yapabilir.

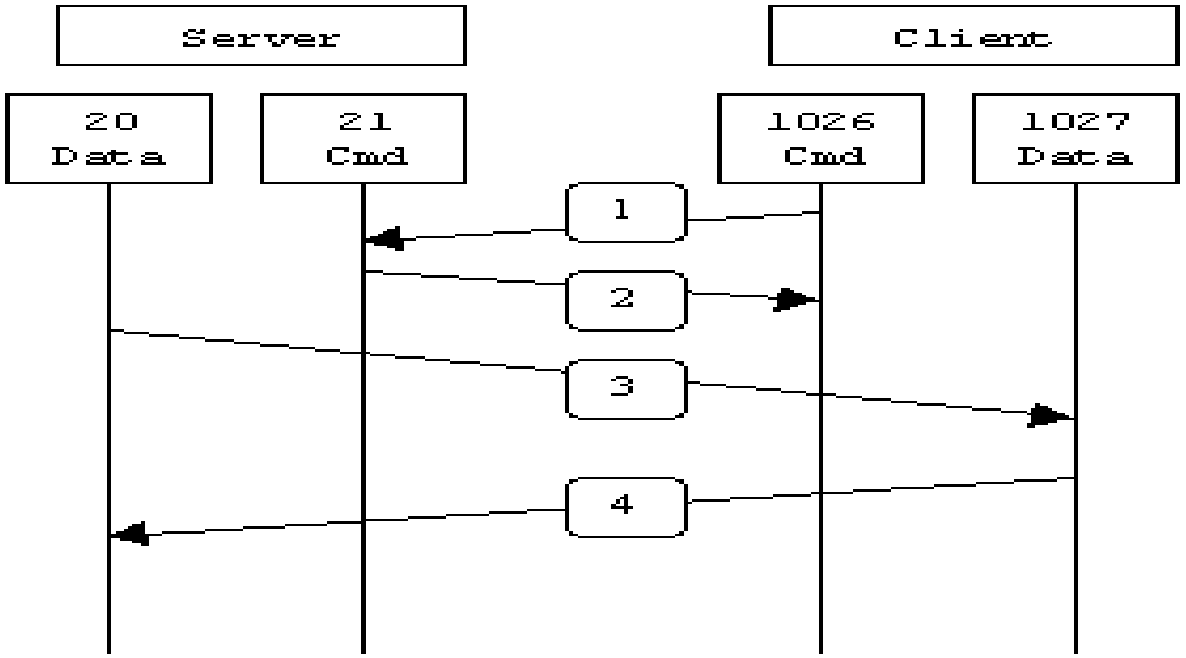
statik paket filtreleme teknolojisi

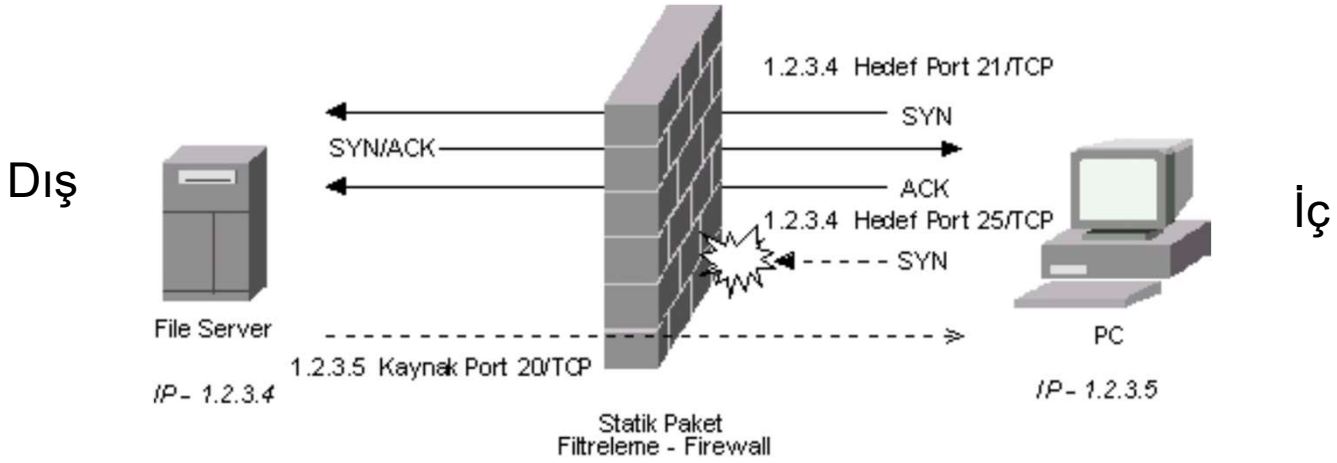
- Bu mimari halen Linux IPChains gibi bazı Firewall sistemlerinde kullanılan eski bir mimaridir. ***Gelen ve giden paketleri sadece geldiği yer ,erişmek istediği port numarası, protokolü gibi değerleri ile inceler*** ve bu değerlerden paketin erişimine izin olup olmadığının saptamasını yapar.

- Örneğin bir http isteği geldiğinde, erişmek isteği portun 80, protokolün TCP ve geldiği yerin 1.2.3.4 IP'si olduğunu görür ve içerideki sunucuya ulaşmasına izin verilmişse, bu paketin içerideki sunucuya gitmesine izin verir. Basit bir mimaridir.

- ***En büyük zayıflığı paketleri ilk gönderen sistemi, yani oturumu ilk başlatan sistemi saptayamıyor olmasıdır.*** Bu durum ciddi riskler oluşturmaktadır, kaynak portu taramaları ve bağlantıları bu risklere örnektir.

- Bir örnek olarak; Ağdaki bir çalışanın FTP portundan bir servere iletişim kurabilmesi için izin verilmiştir. Oturumun işleyişi ise önce çalışanın 21/TCP portunu hedef port olarak belirleyerek bir sisteme dosya isteği göndermesi ile başlar. Hedef sistem, kaynak portu 20/TCP olan paketler ile çalışana dosya transferi yapar. Böyle bir durumda saldırgan ağa kaynak portu 20/TCP olan bir paket gönderdiğinde Firewall sistemi bu paketi görecek ve "içeriden bu pakete istek gelmeseydi bu paket gönderilmezdi" mantığına dayanacak ve paketin içeriye girmesine izin verecektir.





Şekilde statik paket filtrelemenin nasıl olduğu görülmektedir.

- PC, 1.2.3.4 IP'li dosya sunucusunun 21/TCP portuna bağlanırken Firewall izin veriyor. Ancak 25/TCP portuna bağlanmak istediğinde Firewall izin vermiyor.
- Dosya sunucusu ise isterse kaynak portunu 20/TCP yaparak PC'ye istediği porttan ulaşabilir. Çünkü Firewall PC'nin bir isteğinin karşılığında bu paketlerin gönderildiğini düşünür.
- Bu son durum, saldırgana; kaynak portunu 20/TCP yaparak, içerideki herhangibir bilgisayarın herhangibir portuna erişme imkanı verir. Çünkü Firewall 20/TCP'nin ağdan gelmiş bir isteğe FTP sunucusunun cevabı olduğunu zannetmektedir.
- Zaaf: statik paket filtreleme tekniğinin, oturumu ilk başlatan sistemi saptayamıyor olmasıdır.
- Firewall'un paketin hedef portuna bakmaması sebebiyle saldırgan kaynak portu 20/TCP olan paketlerle içerideki herhangi bir sistemin örneğin 139/TCP portuna ulaşabilecektir. Böylece Firewall üzerindeki erişim kontrol listeleri etkisiz kalacaktır.

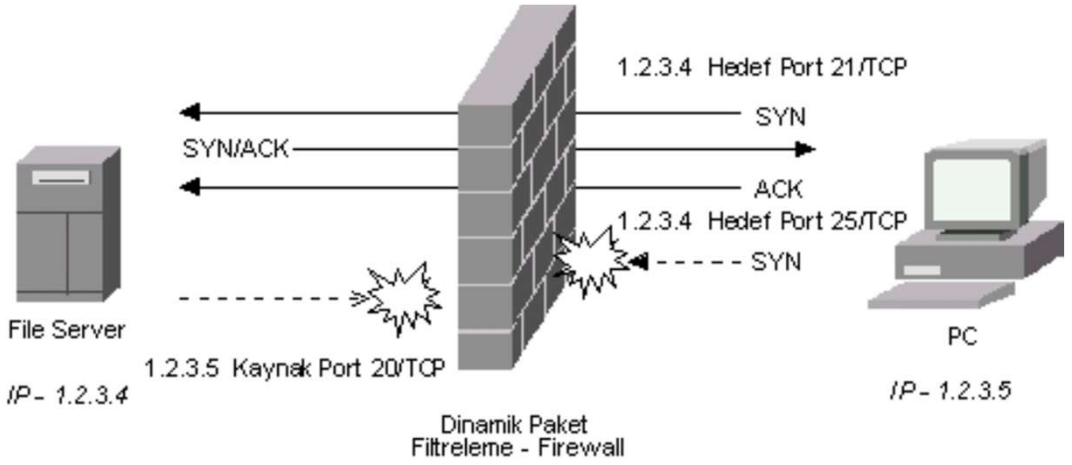
Dinamik paket filtreleme teknolojisi (Stateful İnspection)

- Dinamik paket filtrelemeli Firewall'ların,klasik paket filtrelemenin yanısıra oturumu takip etme özelliği de vardır.
- Checkpoint firmasının ürettiği bu teknoloji yine bu firmanın tescilli markası olan Stateful Inspection ismiyle anılmaktadır. Günümüz Firewall sistemleri genelde bu sistem ile çalışmaktadırlar.

- Temel olarak TCP oturumları bir başı , ortası ve sonu olan oturumlardır. Hiçbir oturum başından veya ortasından kurulamaz. Bu durumda Firewall'lar kuralları sadece SYN flag'ıyla gönderilen paketlere (nereden gönderildiği önemli değil) uygular ve geriye kalan paketler oturumun tutulduğu tabloya bakılarak takip edilir. Böylece örneğin FIN veya SYN/ACK flag'lı paketlerin bir oturumun devamı olmadığından geçişi engellenebilir. Oturumun SYN flag'lı paketler ile başlayacağını düşünerek tasarlanan bu sistemin kuralları bu paketlere uygulaması oldukça mantıklı ve güvenlidir. Ayrıca TCP için olan bu oturum izleme işlemi ICMP ve UDP paketlerine de uygulanabilir.

- Ancak bu teknolojinin zayıflıkları da vardır, paketlerin içeriğini kontrol etmemeleri bu zayıflıklarının başlıca sebebidir, ayrıca FTP protokolünün proxy özelliğini desteklemesi ve bunun kötüye kullanım oranın oldukça fazla olması Stateful Firewall sistemlerinin en büyük dezavantajlarındandır.

Dış



İç

- Şekilde, dinamik paket filtreleme sisteminin nasıl işlediği görülmektedir. PC'nin isteklerinde sonuç değişmezken dosya sunucusunun kaynak portu 20/TCP olan paketi ise engellenebilmektedir.
- Niye? Çünkü eğer server syn paketi ile oturum kurma isteğinde bulunmamışsa 20/TCP Firewall tarafından engellenebilir.

• İzin verilmeyen herşeyi iptal et.
iptables –P INPUT DROP
iptables –P FORWARD DROP
iptables –P OUTPUT DROP

• Dişarıdan firewall'e ssh ile login olunmasına izin ver.
iptables –A INPUT –i eth0 –p tcp -–dport ssh –j ACCEPT
iptables –A OUTPUT –o eth0 –p tcp -–sport ssh –j ACCEPT

• Bütün interface'lerden ping'e izin ver.
iptables –A INPUT –p icmp –-icmp-type echo-request –j ACCEPT
iptables –A OUTPUT –p icmp –-icmp-type echo-reply –j ACCEPT

• Drop any traffic coming from host 80.63.5.7'
iptables –I INPUT 1 –i eth0 –s 80.63.5.7 –j DROP

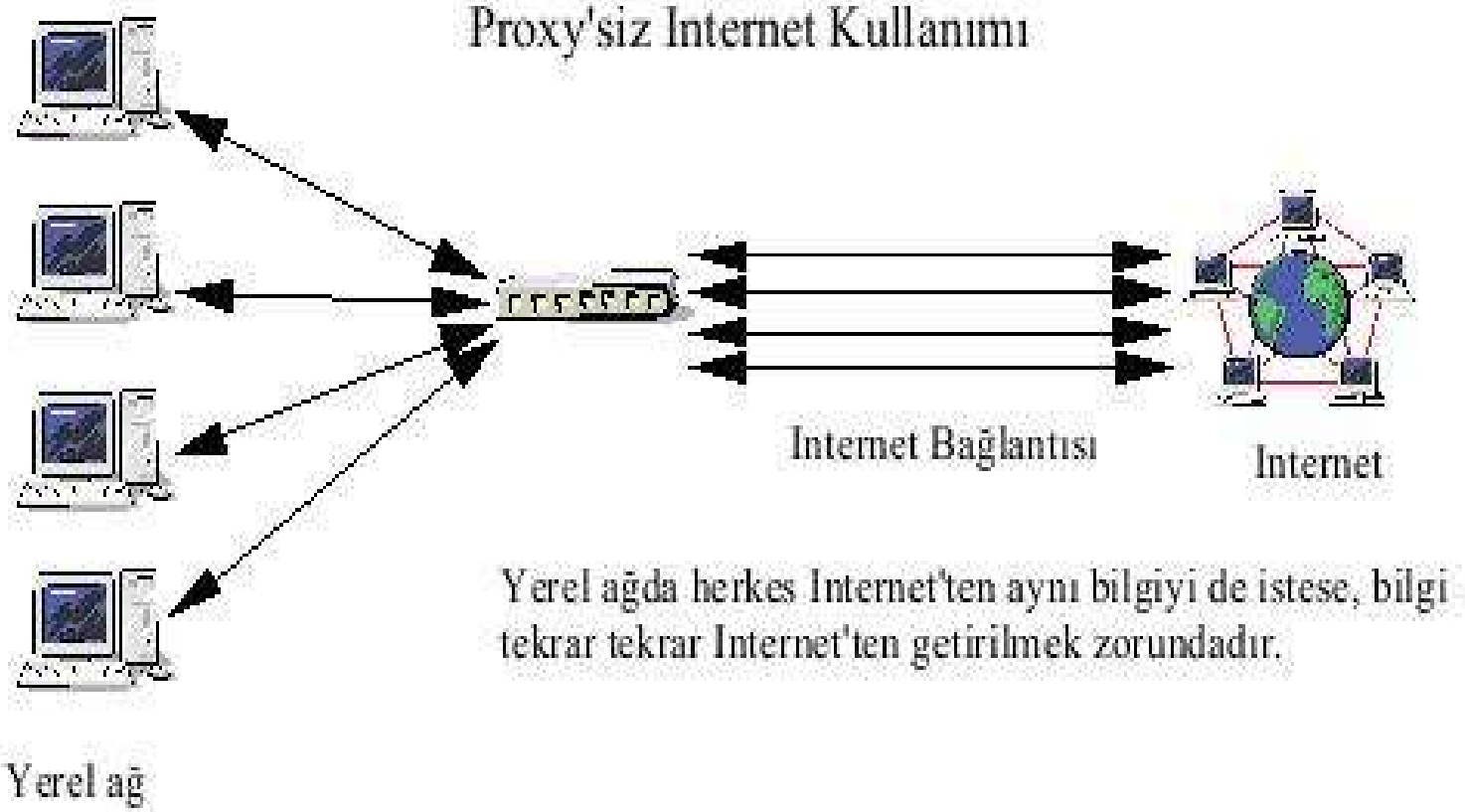
Uygulama Katmanı Firewalları

- Uygulama katmanı firewalları en sıkı koruma yapan firewall tekniğidir. Bu yöntemde ağın güvenliği için arada vekil (proxy) sistem kullanılır (Bu işlem, güçlü bir iş istasyonu üzerine yüklenen yazılımla gerçekleştirilebilir.)

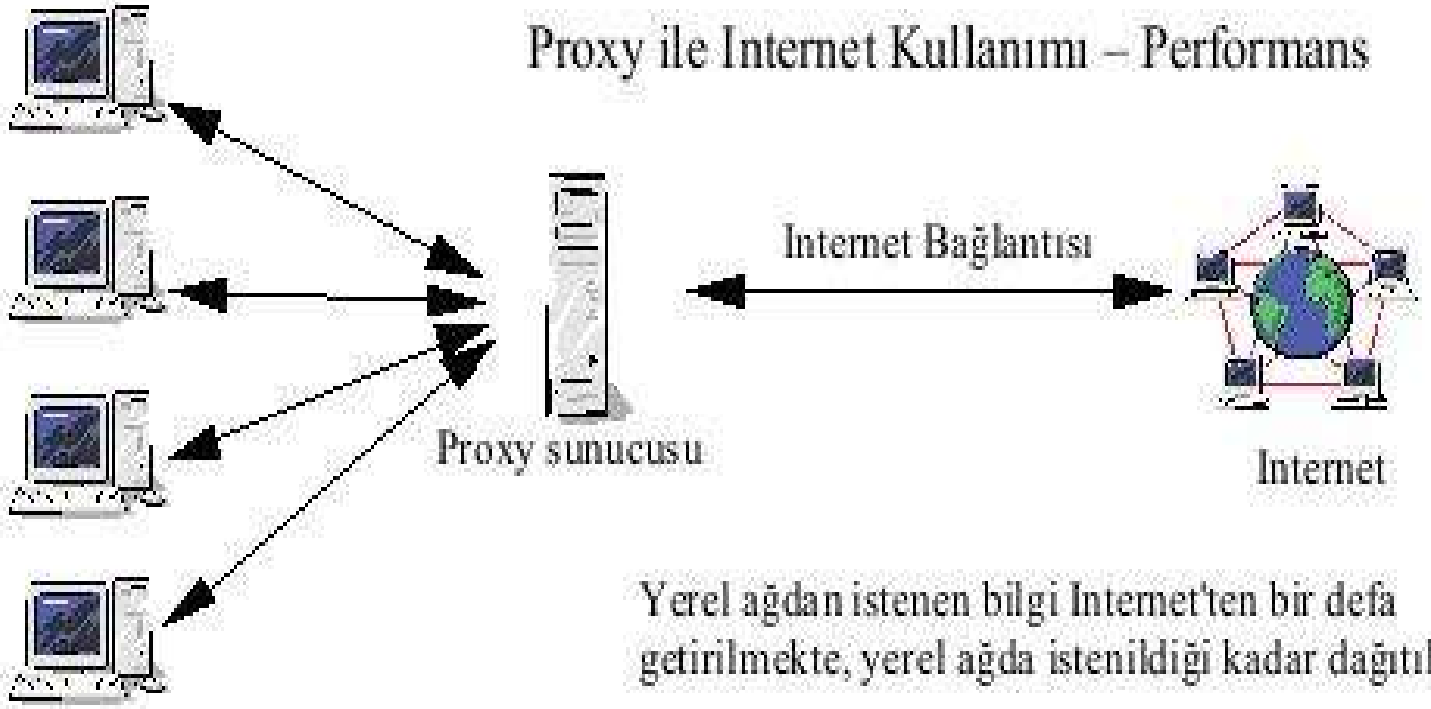
- Proxy mimarisini destekleyen Firewall'larda oturum başlatan ve hedef arasında gerçekleşmez. Oturum açmak isteyen taraf isteği Firewall'a gönderir ve Firewall bu paketi hedefe ulaştırır, hedeften cevap yine Firewall'a gelir ve Firewall tarafından oturumu açmak isteyen tarafa iletilir.
- Oturum açıldıktan sonrada aynı şekilde devam eder. Böylece 2 sistem arası tamamen yalıtılır ve Firewall paketlerin gerek içeriklerine, gerek hedef ve kaynak portlarına gerekse de gönderenin IP adresine müdahale edebilir.

- Paketlerin içeriğini kontrol edebilme Proxy Firewall'ların en büyük artılarındandır.
- Proxy, bir bağlantı uygulamasında araya giren ve bağlantıyı istemci (client) için kendisi gerçekleştiren bir servistir. Böylece aynı istekler bir defaya indirgenerek bağlantı sayısı azaltılmış ve band genişliğinin daha etkin kullanılması sağlanmış olur.

- **Yetersiz olduğu noktalara gelince araya girmesi ve paketleri kendisinin iletmesinin doğal sonucu olan yavaşlık ortaya çıkmaktadır. Ciddi bir yavaşlık olmamasına rağmen artan bağlantı sayısı ve yoğun ağlardaki veri trafiği hızı olumsuz yönde etkilemektedir.**

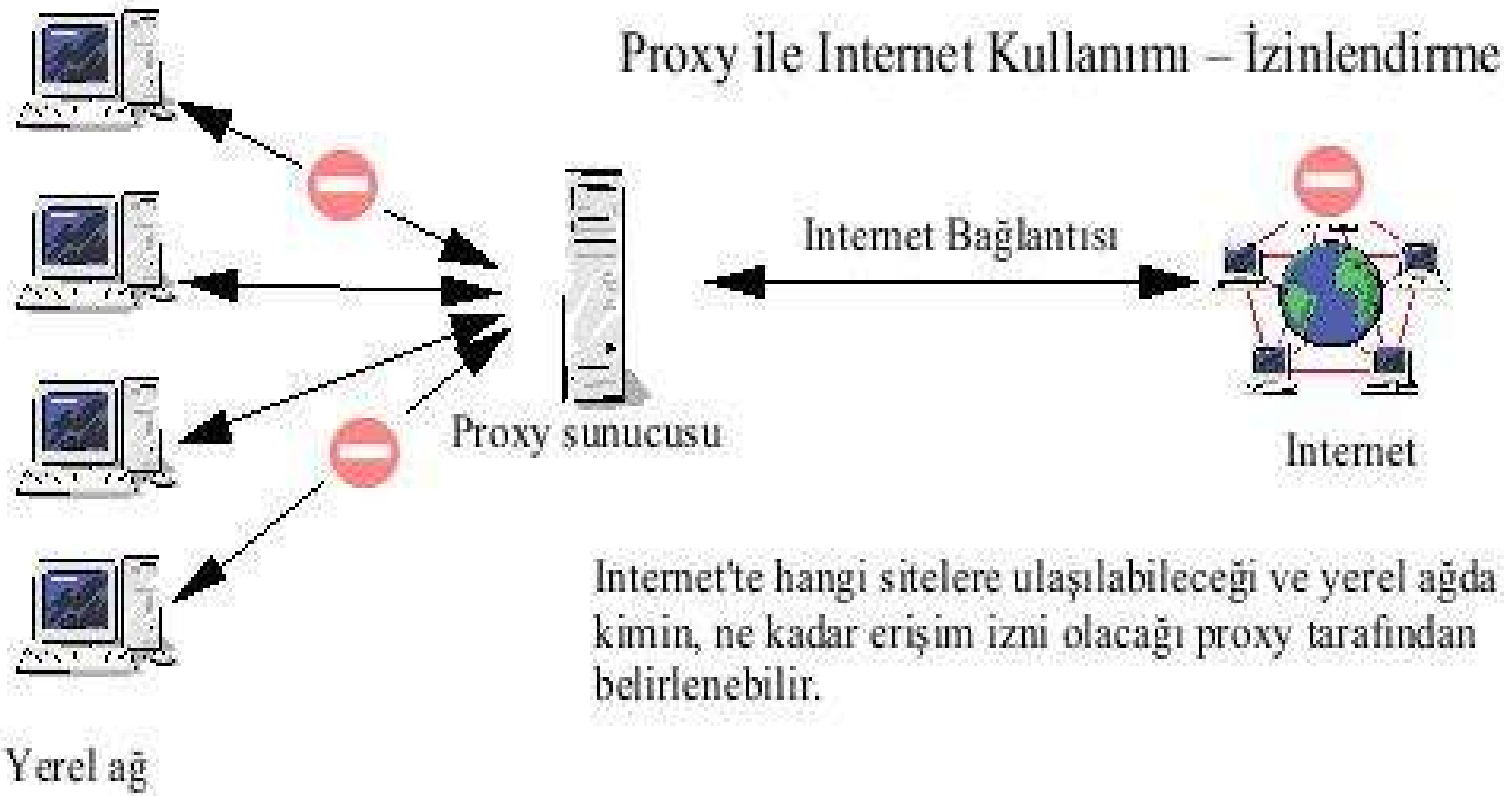

Proxy'siz Internet Kullanımı
Internet Bağlantısı
Internet
Yerel ağda herkes Internet'ten aynı bilgiyi de istese, bilgi tekrar tekrar Internet'ten getirilmek zorundadır.
Yerel ağ

Proxy ile Internet Kullanımı – Performans



Yerel ağdan istenen bilgi Internet'ten bir defa getirilmekte, yerel ağda istenildiği kadar dağıtılmaktadır.

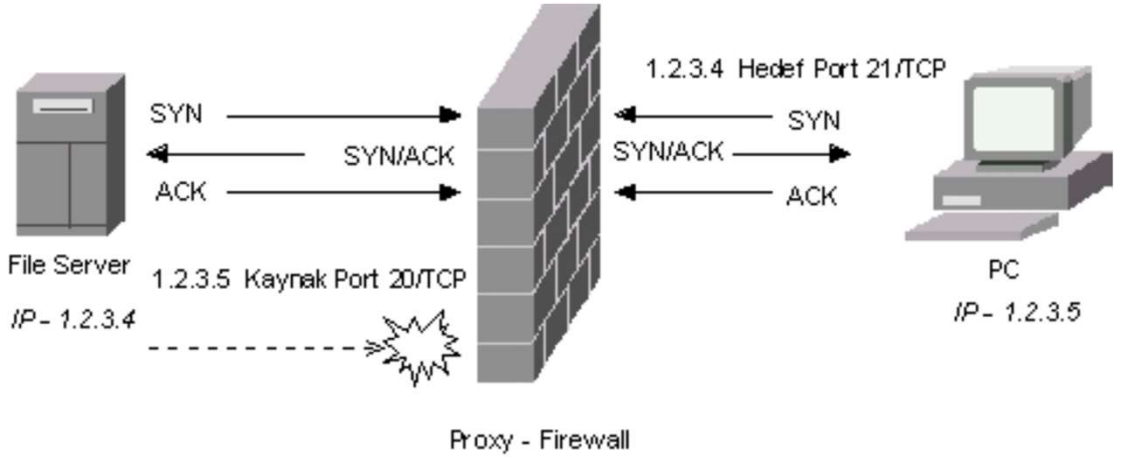
Proxy ile Internet Kullanımı – İzinlendirme



Internet'te hangi sitelere ulaşılabileceği ve yerel ağda kimin, ne kadar erişim izni olacağı proxy tarafından belirlenebilir.

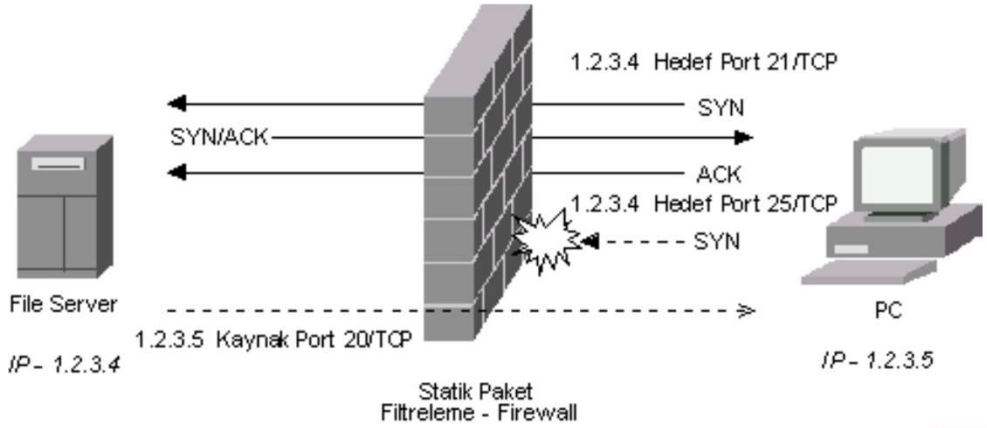
Ağ Katmanı ve Uygulama Katmanı Firewallarının Karşılaştırılması

- Ağ katmanı firewallarında kuralları aşmak uygulama katmanı firewallarına göre kuralları aşmaktan kolaydır.
- Uygulama katmanı firewallarında; ağ katmanı firewallarına göre daha iyi kayıtlama (log) ve etkinlik raporları tutmak mümkündür.
- Uygulama katmanı firewallarında sunucu makine işlemlerle ilgilendiği için saldırılara açık haldedir.
- Ağ katmanı firewalları daha kolay konfigüre edilir. Uygulama katmanı firewallarında ise ağ yöneticisine büyük bir sorumluluk düşer; gerekli olan konfigürasyonu kendisi yapmalıdır.

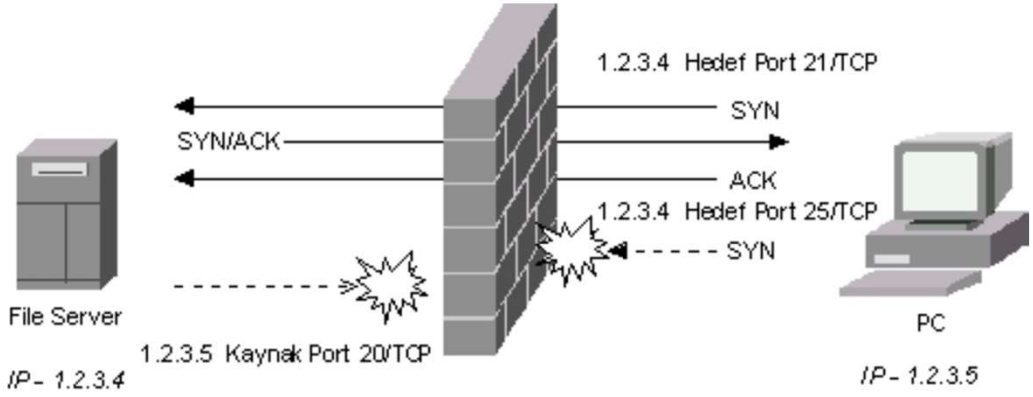


Şekilde, proxy mimarisinin işleyişi görülmektedir. PC'nin istekleri Firewall'a gelmekte ve Firewall üzerinden dosya sunucusuna ulaşmaktadır, cevaplar ise yine Firewall üzerinden PC'ye ulaşmaktadır.

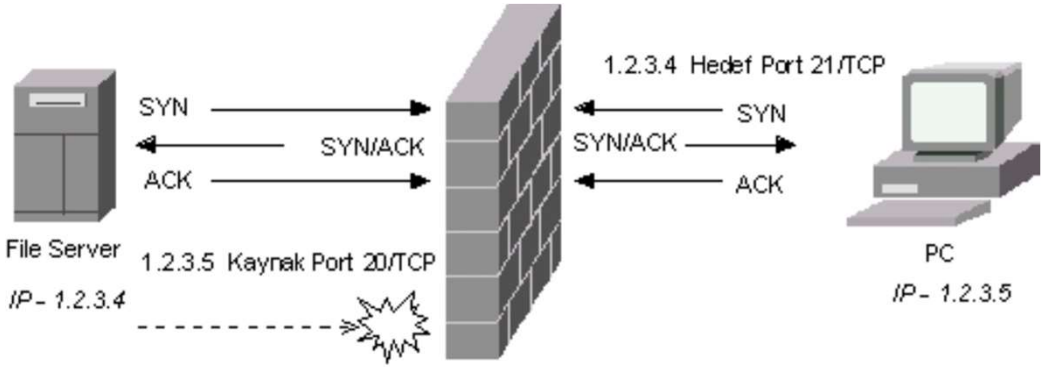
Kaynak portu 20/TCP olan paketler için yine engelleme söz konusudur.



Statik Paket
Filtreleme - Firewall



Dinamik Paket
Filtreleme - Firewall



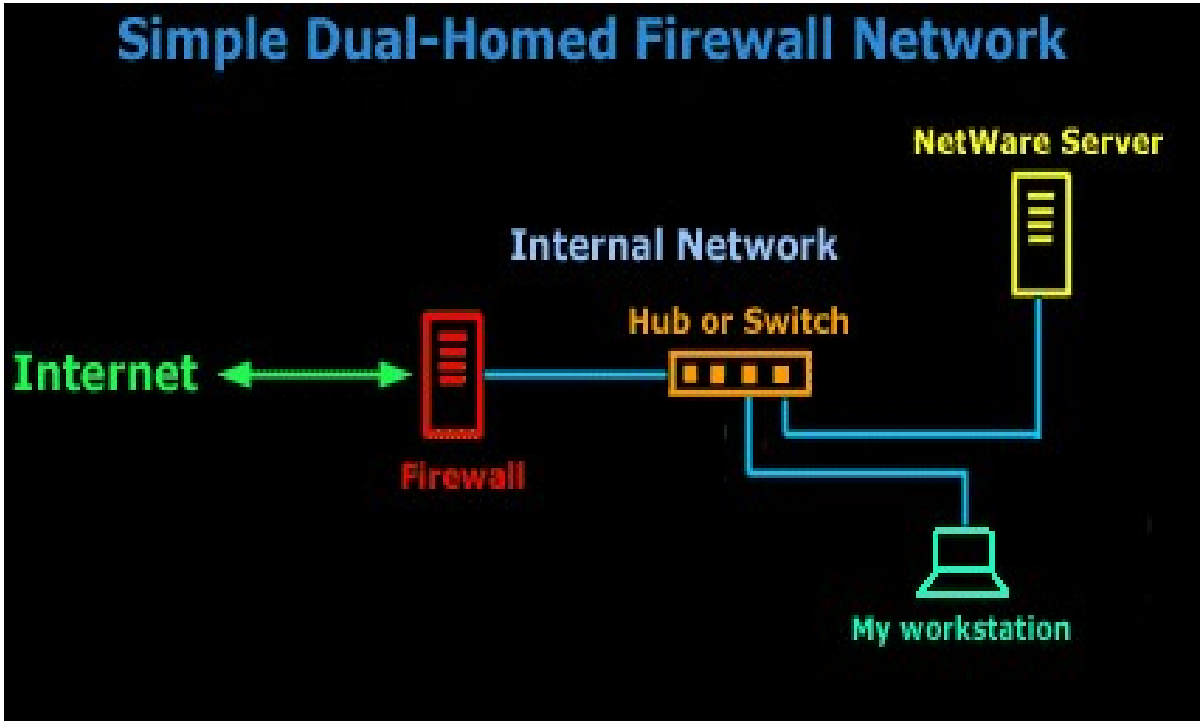
Proxy - Firewall

FİREWALL TOPOLOJİLERİ

- Bir firewall değişik yollar ile kurulabilmektedir. İhtiyaçlara bağlı olarak küçük bir network yada kişisel bir bilgisayar için yeterli korumayı sağlayan basit bir firewall de kullanılabilir;
- yada daha fazla koruma ve güvenlik sağlayan daha komplike bir firewall seçilebilir.

Basit Dual-Homed Firewall

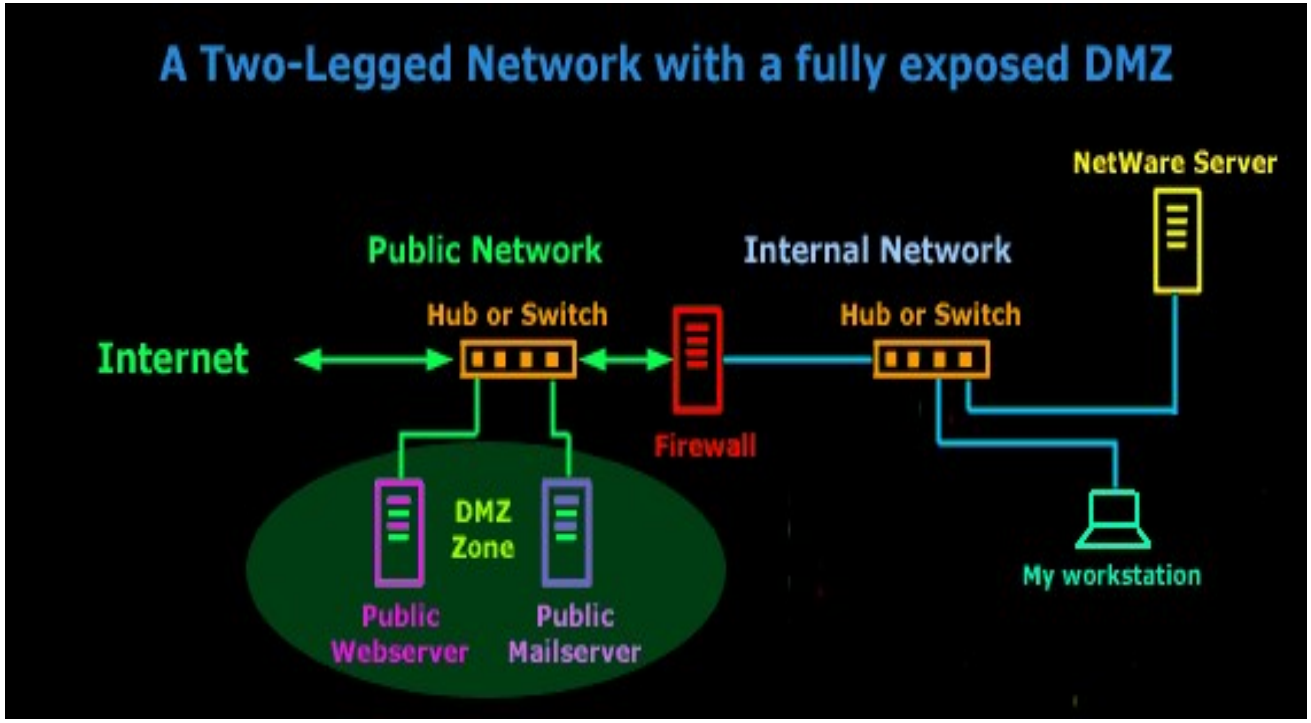
- Dual-homed firewall bir firewall kullanmanın en basit ve en genel yoludur. Internet, direk dial-up modem yada ISDN gibi diğer bağlantı tipleri üzerinden firewall'e girer. Bu konfigürasyon tipinde DMZ (De-Militarized Zone) bulunamaz. Firewall, üzerinde bulundurduğu filtreleme kurallarıyla yerel ağ ile internet arasındaki paket geçişini kontrol eder.



- Burada firewall'in bir yüzü ile yerel ağın dışına, bir yüzü ile de yerel ağın içine bağlanıldığı için dual-homed olarak isimlendirilmiştir.
- Bu yöntemin kolaylık avantajı bulunmaktadır. Eğer internet bağlantısı bir modem üzerinden ise ve sadece bir IP adresi varsa bu yöntem kullanılabilir.

Bütünüyle Serbest Olan DMZ İçeren İki-bacaklı Network

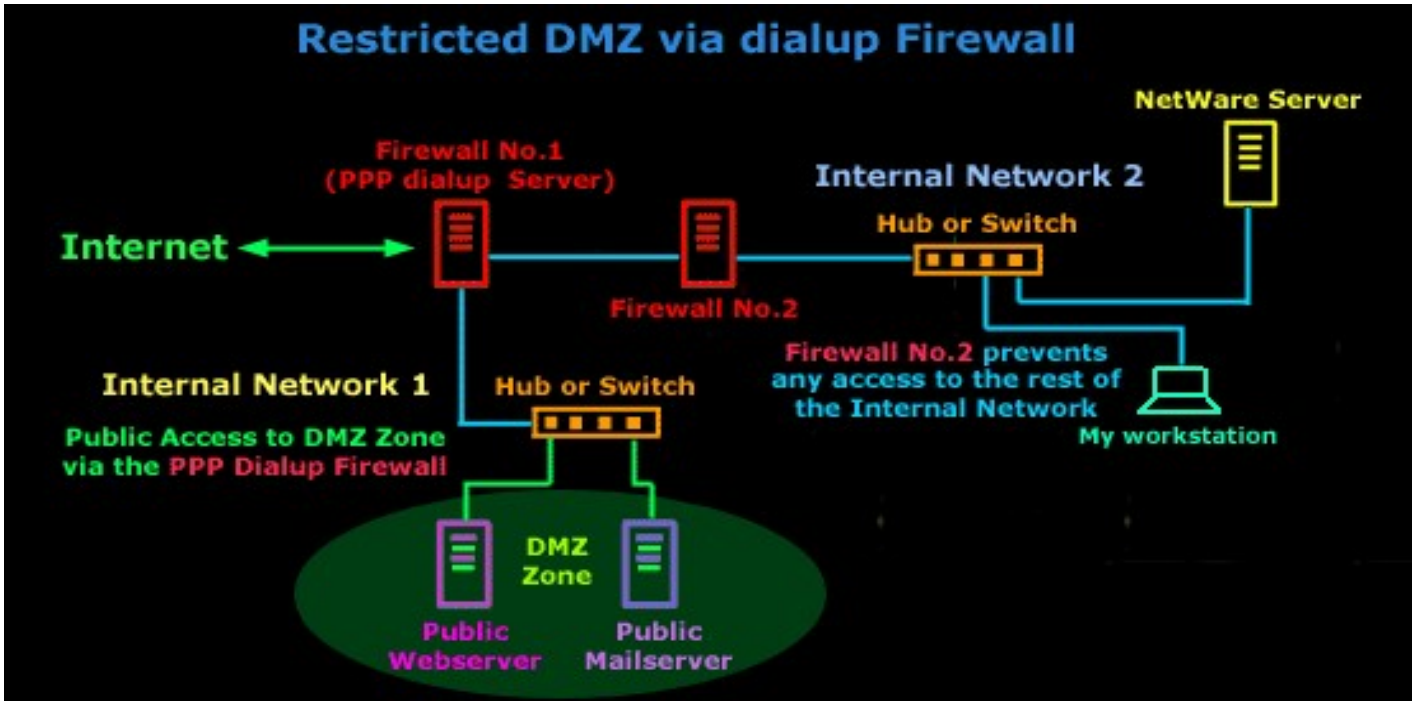
- Daha avantajlı olan bu konfigürasyonda, dışarıya çıkmayı sağlayan router dışarıda bir hub veya switch'e bağlıdır. Firewall ile filtrelenmeden dış dünyaya direk ulaşmak isteyen makineler bu hub'a bağlanır. Ayrıca firewall'in dışa açılan yüzü bu hub'a bağlıdır. Firewall'in diğer yüzü ise iç ağda bulunan hub'a bağlıdır.Firewall tarafından korunma ihtiyacı duyan makineler iç ağdaki hub'a bağlanırlar. İç ağdaki hub yerine switch kullanmak ek güvenlik ve hız avantajı getirir.



Bir önceki şekildeki gibi; DMZ bölgesi korumasız olarak internete açık durumdadır. Bu durum firewall'in konfigürasyonunu kolaylaştırmaktadır.

Eğer DMZ bölgesi için de sınırlı bir koruma sağlamak gerekirse iç ağı koruyan firewall'den tamamen ayrılmış olarak bir filtreleme gerçekleştirilebilir. ***DMZ bölgesi için sınırlı bir koruma, harici bir router ve çoklu IP adresleri kavramlarına bağlı olarak gerçekleştirilir.***

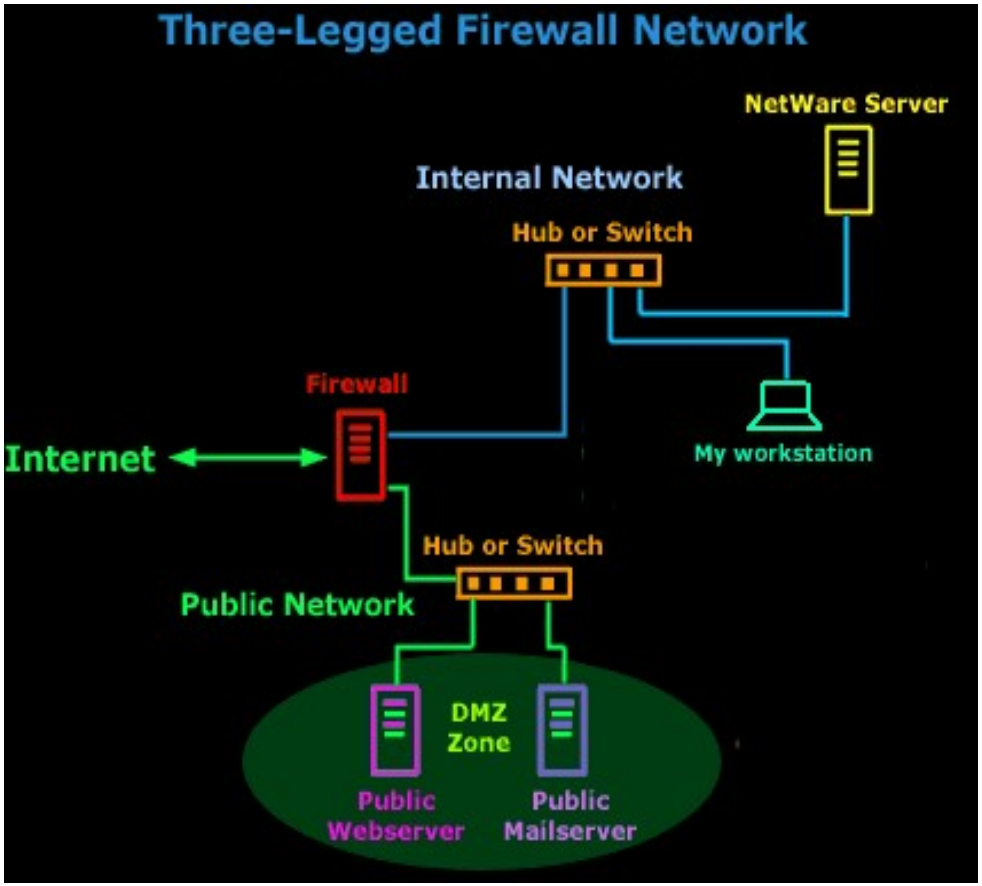
DMZ bölgesi için sınırlı koruma sağlamak üzere iki çözüm mevcuttur. Birinci çözüm; ikinci bir router/firewall kurmak.



Eğer PPP üzerinden bağlanılıyorsa bu faydalıdır.
Burada bir makine dış router/firewall (Firewall No.1) dır. Bu makine PPP bağlantısını oluşturmak ve DMZ bölgesine olan ulaşımları kontrol etmekten sorumludur.
Diğer firewall (Firewall No.2) standart dual-homed firewall'dir ve görevi iç ağı korumaktır.

ÜÇ BACAKLI FİREWALL

DMZ bölgesi için sınırlı koruma sağlamak üzere ikinci çözüm üç-bacaklı bir firewall oluşturmaktır. Bu, firewall kutusunda DMZ için ek bir ağ bağdaştırıcısına gerek duyulması anlamına gelir. Firewall, dış dünya ile DMZ arasındaki paket yönlendirmeyi;dış dünya ile iç ağ arasındakinden farklı yapacak şekilde konfigüre edilir.



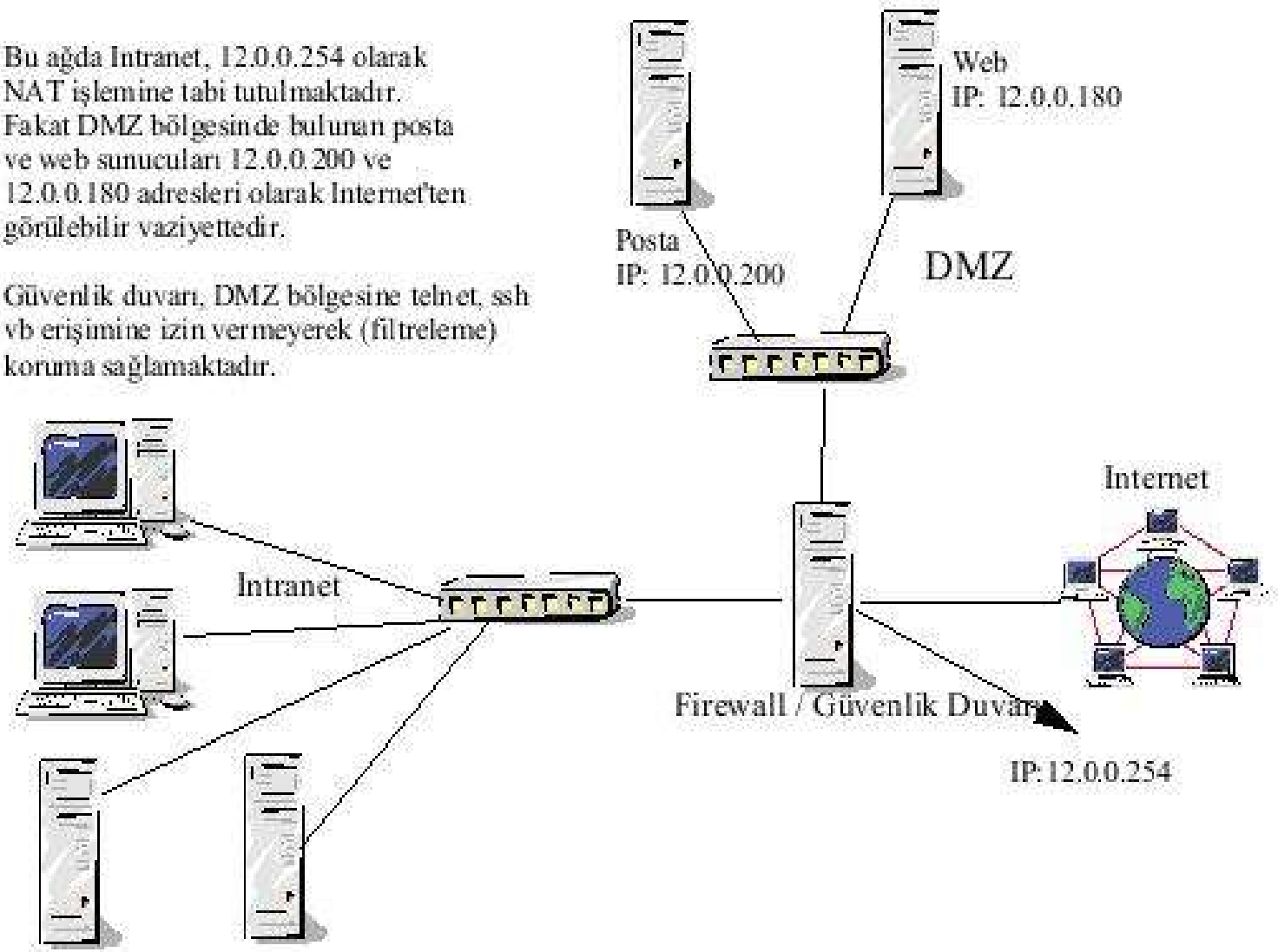
Üç-bacaklı firewall'un dezavantajı ek olarak gelen karmaşıklıktır. DMZ bölgesine olan giriş/çıkış ve iç ağa olan giriş/çıkış tek bir geniş kurallar kümesi tarafından kontrol edilir. Dikkatli olunmazsa bu kurallar yanlış oluşturulabilir.

DMZ BÖLGESİ

- DMZ, firewall tarafından daha az korunan, daha fazla erişime izin verilen bir bölgedir. Firewall'a üçüncü bir ağ çıkışı eklenmesi ve Internet'e servis verecek olan makinelerin(DNS, mail relaying, FTP gibi WEB servisleri) buraya konulması ile oluşturulur. Örneğin DMZ'deki makinelere NAT uygulanmayabilir, tahsisli IP numaralarına sahip olabilirler.

Bu ağda Intranet, 12.0.0.254 olarak NAT işlemine tabi tutulmaktadır. Fakat DMZ bölgesinde bulunan posta ve web sunucuları 12.0.0.200 ve 12.0.0.180 adresleri olarak Internet'ten görülebilir vaziyettedir.

Güvenlik duvarı, DMZ bölgesine telnet, ssh vb erişimine izin vermeyerek (filtreleme) koruma sağlamaktadır.



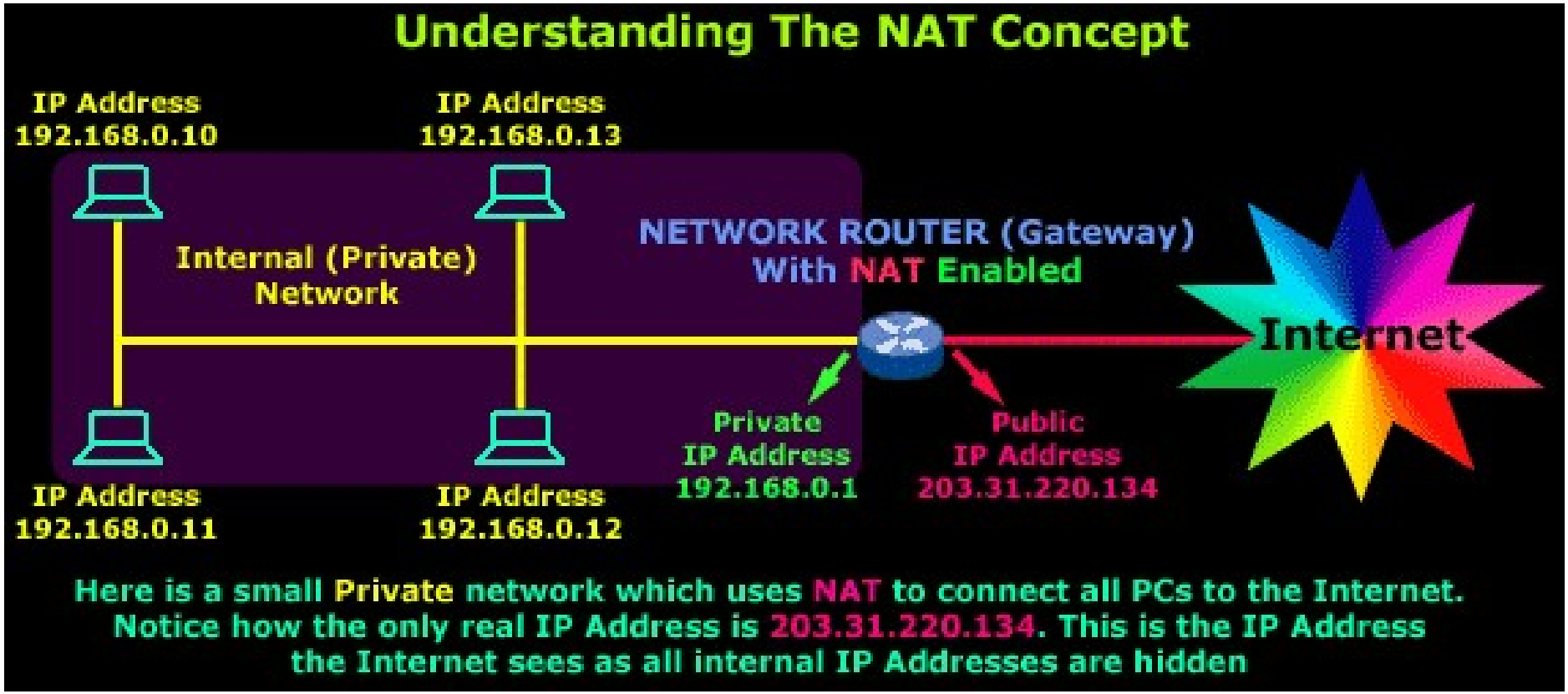
NAT(Network Adress Translation)

- NAT, RFC 1613 ile tanımlanıp, hemen hemen bütün işletim sistemleri, firewall cihazları ve uygulamalarca desteklenen güncel ağlarda çok popüler bir uygulamadır.

- NAT hızla tükenen gerçek IP adreslerine bir çözüm olarak doğmuştur. Başka bir deyişle gerçek IP adresiyle sadece internete çıkmak için geliştirilmiştir.

- NAT internete bağlı bir cihaz üzerinde çalışır ve, iç ağdaki IP adreslerini dış ağdan gizleyerek , ağınızı herkese açık olan ağdan (internetten) gizler.

- NAT ağınızı şeffaflaştırır; yani dahili ağınızdaki cihazların tümünü internet bağlantısı için konfigüre etmeniz gerekmez. Gateway konumundaki NAT cihazının bunları tanıması ve izin vermesi yeterlidir.



4 bilgisayar ve bir routerdan oluşan bu ağ internete bağlanmıştır. Ağdaki bütün hostlar C sınıfı özel bir IP adresine sahiptir.

Router da 'özel ağ' arayüzünde 192.168.0.1, internete bağlandığı 'açık ağ' arayüzünde ise 203.31.220.134 gerçek IP adresine sahiptir.

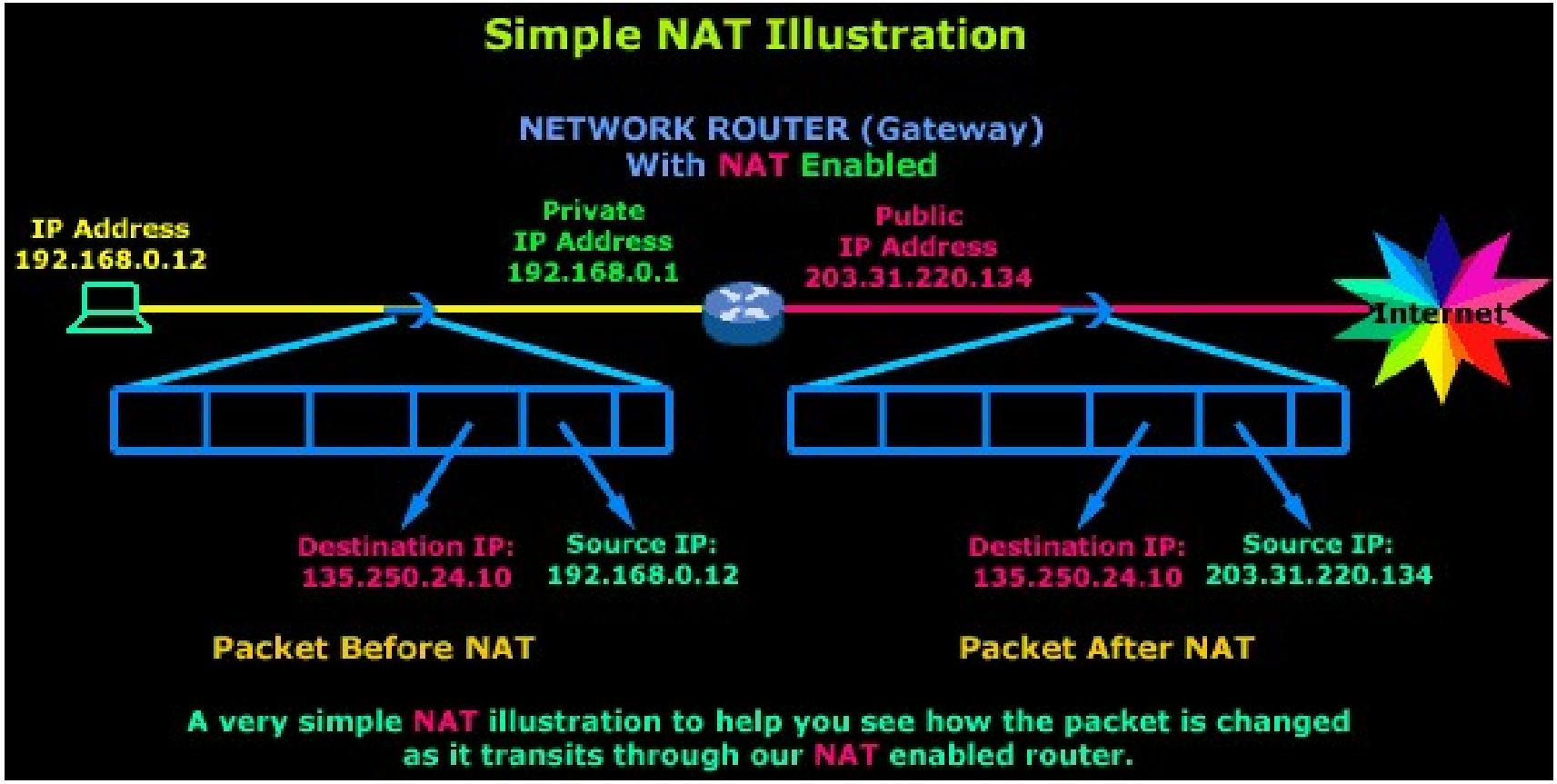
NAT NASIL ÇALIŞIR

NAT'ın çalışması için 3 farklı yol vardır, ancak temel prensip her üçünde de aynıdır.

Bunu bir örnek üzerinde anlatalım; router (firewall veya normal bir PC) NAT desteğiyle direk internete bağlı olsun. Bütün hostlar internete router yoluyla bilgi göndereceklerdir.

Router NAT aracılığıyla bu paketleri işleyip hedef adreslerine gönderir.

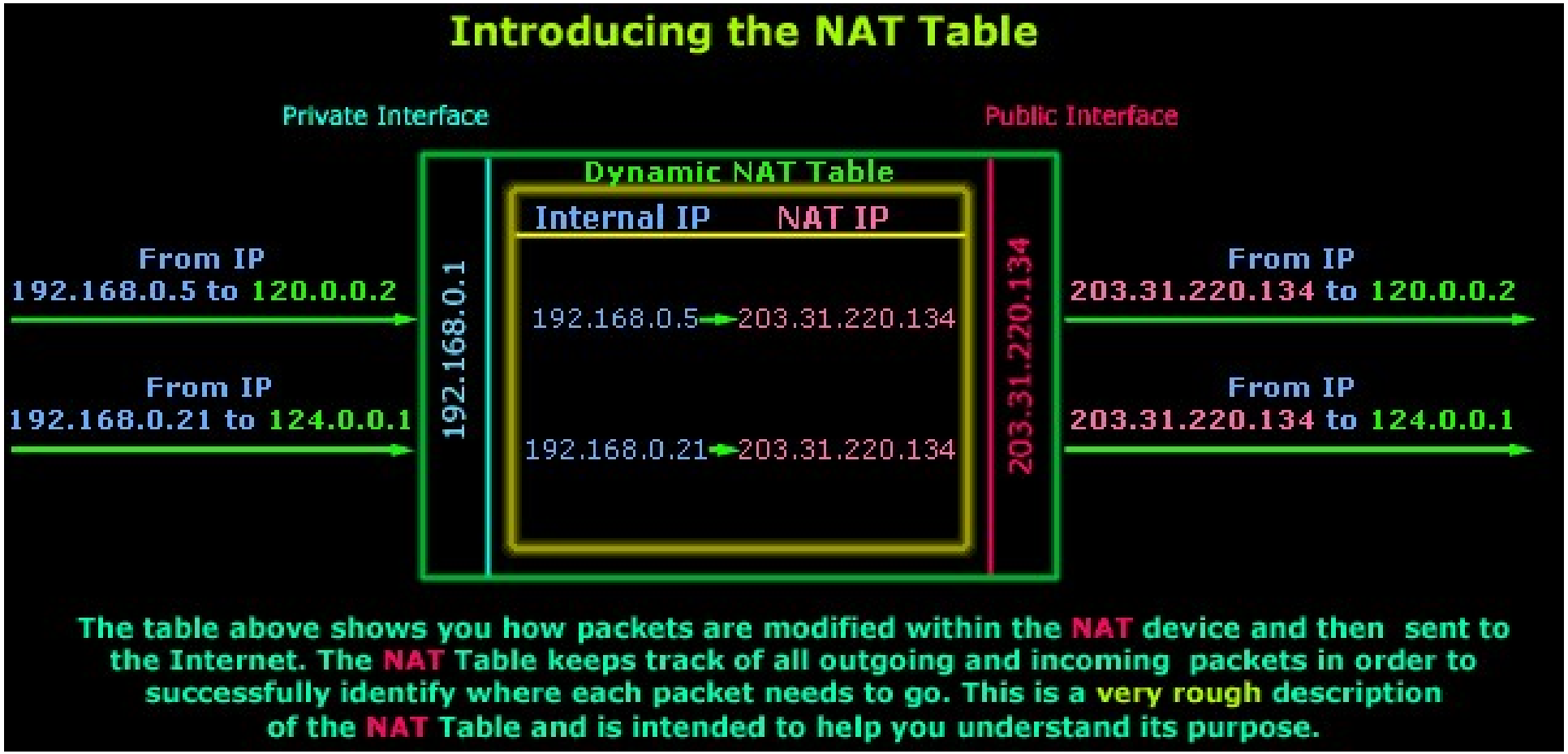
Her paket routerın 'özel ağ' arabiriminden alındığında router ağ katmanında o paketin kaynak IP adresini (192.168.0.10) çıkarır ve yerine gerçek IP adresini (203.31.220.134) yerleştirir ve o paketi yeni haliyle internete gönderir.



- Router içerisindeki NAT operasyonuna bakarsak; orjinal paketlerin kaynak adresleri değiştiriliyor ve bu bilgi router içerisindeki (NAT tablosu olarak bilinen) hafızanın belirli adreslerine yazılıyor. Bu tablo sayesinde bir cevap paketi alınırsa, router ağ içerisinde hangi hostun bu paketi beklediğini anlar ve ona gönderir.

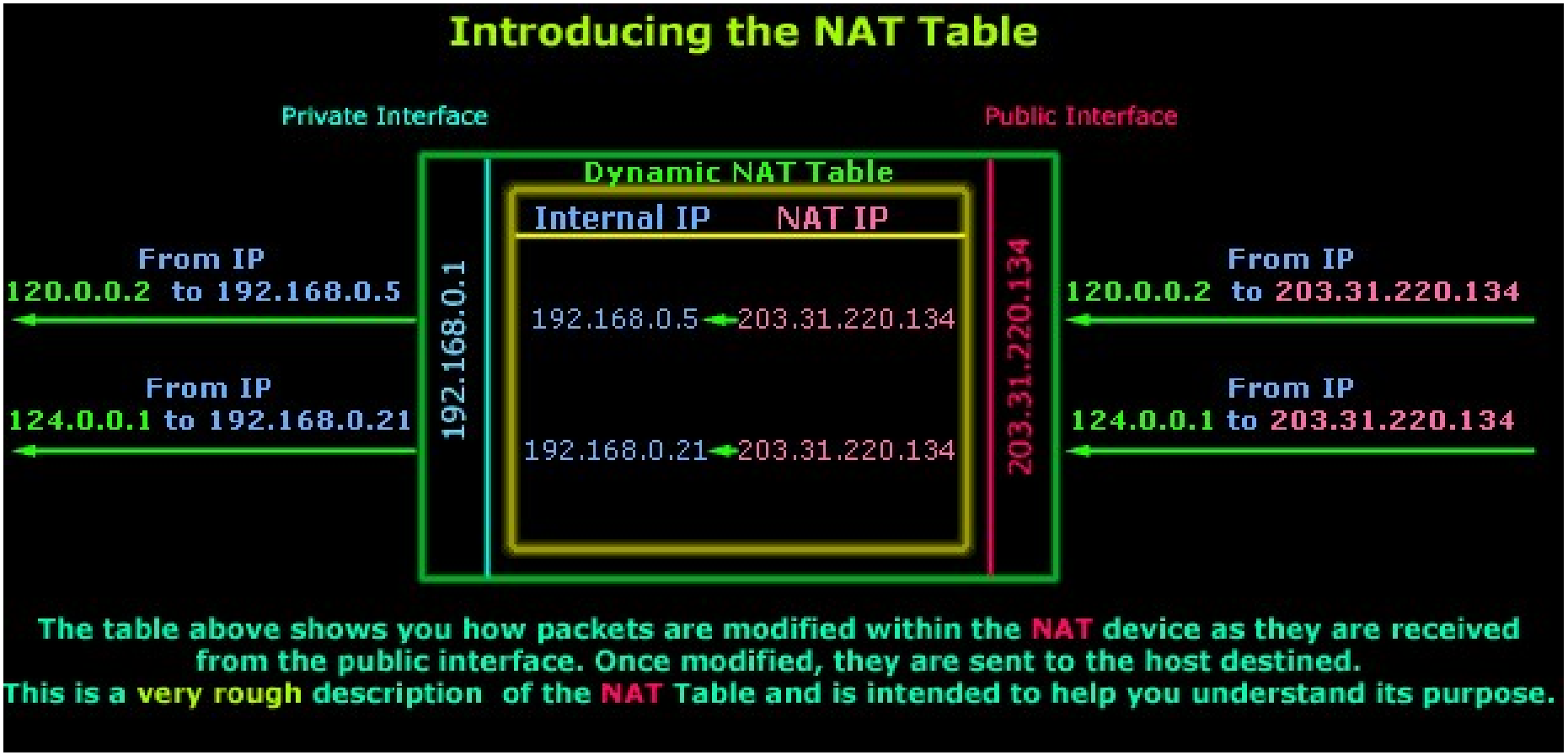
NAT TABLOSU

- NAT Tabloları, routerlar tarafından (veya başka NAT destekli cihazların) paketlerin alınıp, kendi arabirimlerine iletim işlevinde en önemli birimlerdir.
- Dahili ağdan harici ağa olan her türlü iletişim (veya ters yönü) izlenir ve tüm arabirimlerdeki paketlerin ne yapılacağı konusunda yardımcı olacak özel bir tablo oluşturulur.
- NAT tablosunun çok büyük olması (daha fazla hafıza gerektirdiği anlamına da gelir) çok daha fazla çift yönlü iletişimin izlenebilmesini sağlar.
- Büyük NAT tablosuna sahip NAT destekli cihazdan kasıt; dahili ağdaki daha fazla sayıda istemciye hizmet edebilmesi demektir.



- Burada, özel ağdaki 192.168.0.5 ve 192.168.0.21'in istekleri NAT destekli routerın 'özel ağ' arabiriminden alınır. Bu paketler; üzerlerinde küçük bir değişiklik yapılana kadar router üzerinde özel bir alanda geçici olarak tutulurlar. Bu örnekte yapılan değişiklik, kaynak IP adresleri yerine gerçek IP adresinin (203.31.220.134) yazılmasıdır.

- Router paketleri salmadan önce, NAT tablosunda her paket girişi için bir kayıt tutar. Bu kayıtlar, internetten cevap geldiği zaman routerın ne yapacağı konusunda uygun hareketin seçilmesini sağlar.



- Cevap alındığı zaman router NAT tablosuna bakar, uygun kaydı bulur ve yapması gereken diğer değişiklikleri yapar. Yani internetten gelen paketlerin hedef adreslerini 203.31.220.134'ten 192.168.0.5 ve 192.168.0.21 olarak değiştirir ve paketleri bu hostlara gönderip, NAT tabosundaki ilgili kaydı siler.

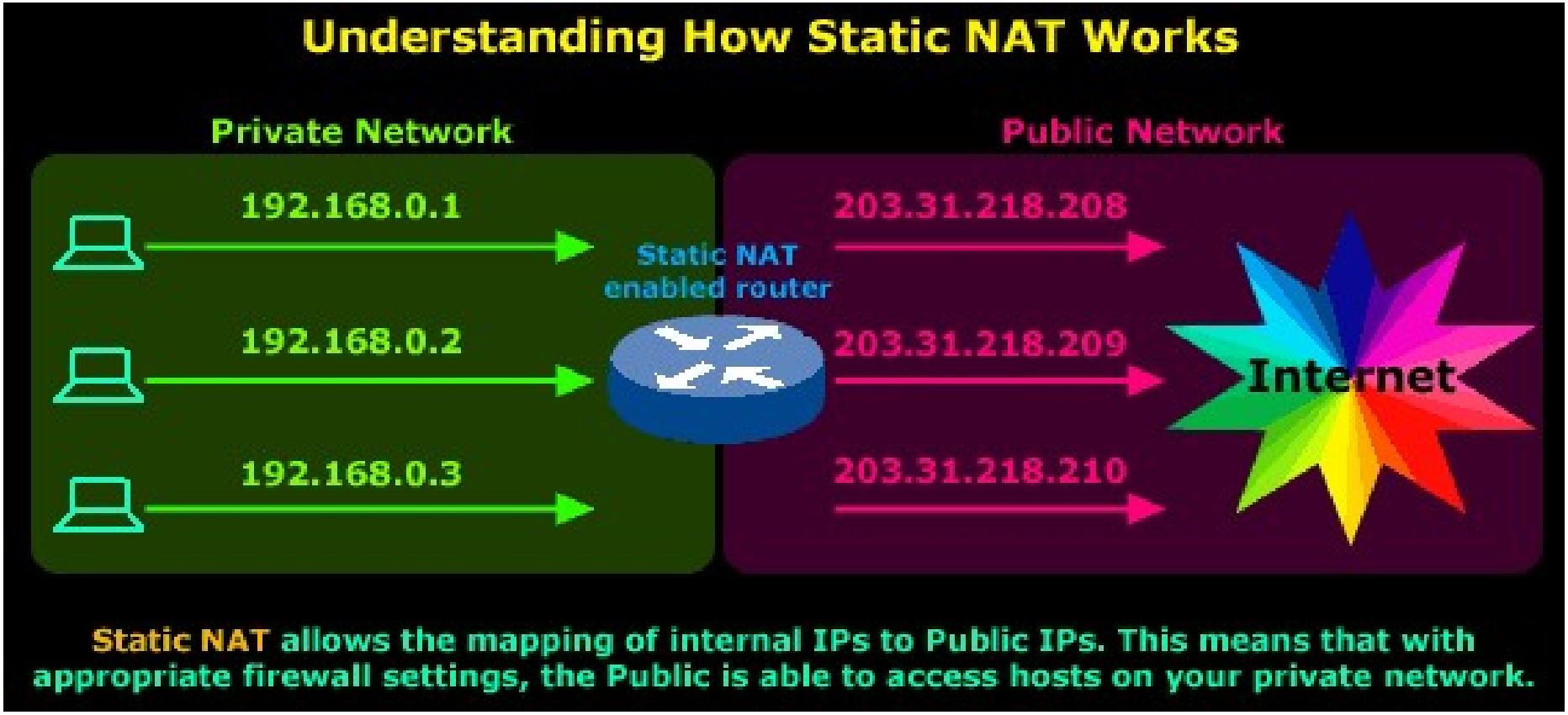
- Bir çok NAT cihazında NAT oturum limiti, mevcut hafıza boyutu ile sınırlıdır. Her bir dönüşüm cihaz hafızasında 160 byte'lık yer harcar. Sonuçta 10000 dönüşüm için 1.6 MB hafıza alanı gereklidir. Bunun için yönlendirme platformları daha fazla sayıda dönüşüme cevap verebilmek için yüksek hafızaya sahip olmalıdır. Ancak pratikte durum farklıdır.

- Küçük Cisco routerlar (700,800,1600 serisi gibi) NAT destekli IOS'lere sahiptirler. NAT oturum sayıları 2000 civarındadır. Fakat 3000-4000 oturum açılmak istendiği zaman çok büyük hafıza gereksinimi yanında CPU yönetimi problemi de ortaya çıkar. Bu durumda mesela ping cevapları çok uzun süre bekleyebilir ve ergeç paket ölümlerinde de exponansiyel bir artış olur.

- Gateway ve firewall özelliği ile beraber çok büyük router modelleri eş zamanlı olarak (8000-25000) oturum açabilir ve çok büyük şirketlerde ihtiyaçları gidermede kullanılır.

STATİK NAT

- Bir özel ağdaki tüm bilgisayarların internete kendi gerçek IP'si ile çıkmak istemesi durumudur. Çok küçük ağlarda bu durum görülebilir.

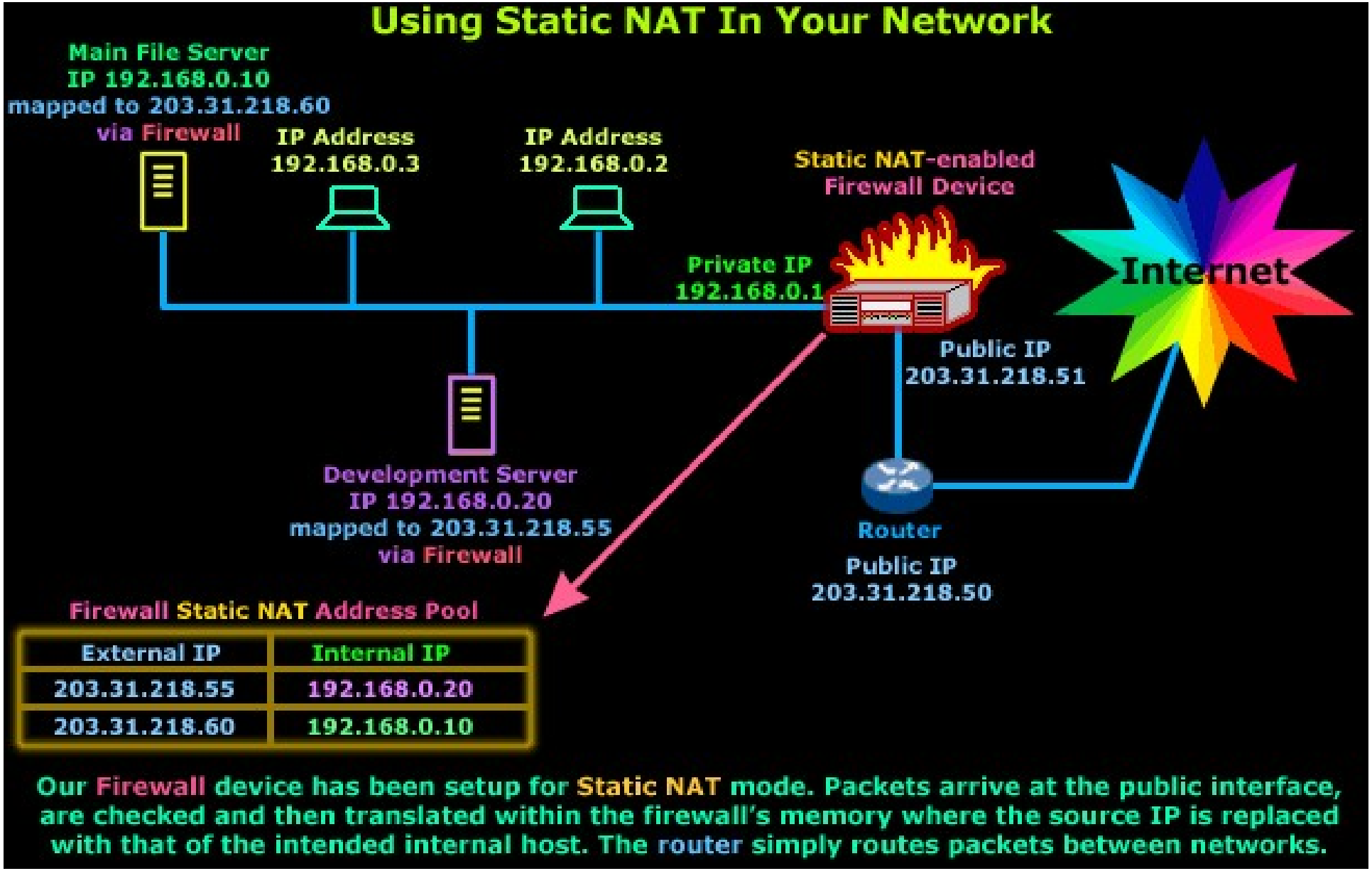


Bu diyagramda bizim özel ağımızın statik NAT modundaki router ile internet bağlantısı görülüyor

- Bu modd’a her bir host kendisiyle eşleşecek bir IP adresine sahiptir. Mesela 192.168.0.1 IP adresine sahip host 203.31.218.208 gerçek IP adresiyle eşleşir. Artık bu hosttan gelecek her bir paket direk kendine özgü gerçek IP adresiyle değiştirilecektir.

- Herkesin ağ ihtiyaçları farklı olup, bu tip bir bağlantıyı kullanmak; internetten özel ağının görünmesini ve erişimin kolay olmasını isteyen bazı şirketler için ihtiyaç olabilir.

1. örnek

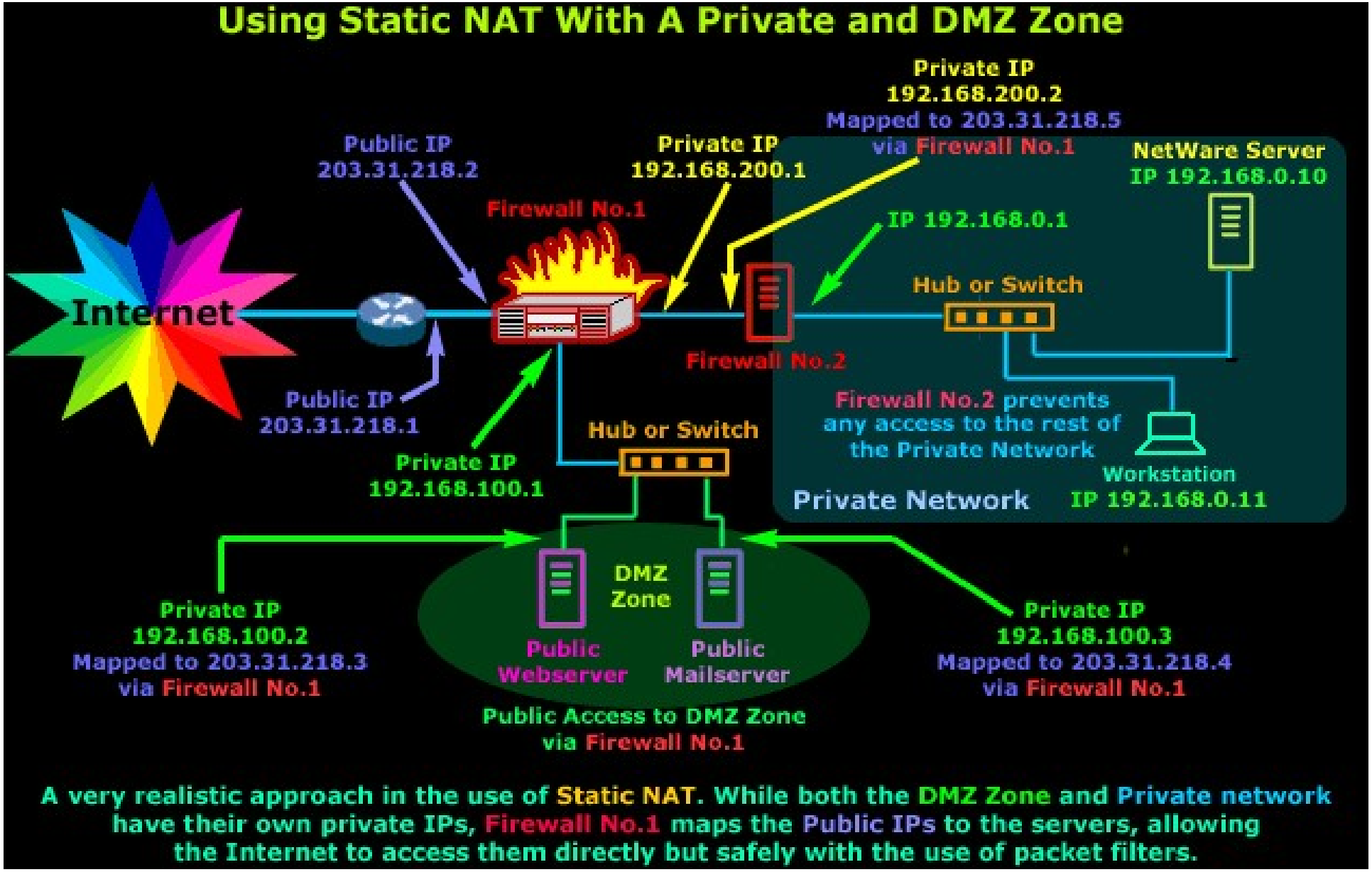

Using Static NAT In Your Network
Main File Server
IP 192.168.0.10
mapped to 203.31.218.60
via Firewall
IP Address
192.168.0.3
IP Address
192.168.0.2
Static NAT-enabled
Firewall Device
Private IP
192.168.0.1
Internet
Public IP
203.31.218.51
Development Server
IP 192.168.0.20
mapped to 203.31.218.55
via Firewall
Router
Public IP
203.31.218.50
Firewall Static NAT Address Pool
External IP
Internal IP
203.31.218.55
192.168.0.20
203.31.218.60
192.168.0.10
Our Firewall device has been setup for Static NAT mode. Packets arrive at the public interface, are checked and then translated within the firewall's memory where the source IP is replaced with that of the intended internal host. The router simply routes packets between networks.

- Bu örnekte 192.168.0.20 adresine sahip bir geliştirme serverı bulunmaktadır. Bu serverın çok fazla güvenlik ihtiyacı olmakla beraber bazı emin müşteriler tarafından değişik servislerine erişmek için kullanılmaktadır. Aynı zamanda ana file serverımızda (192.168.0.10) müşterilerimizin erişebileceği özel bir veritabanı bulunmaktadır.

- Bu seçenekte statik NAT'ın ancak kompleks filtreler ile tek bir IP adresi üzerinden güvenliği sağlanmıştır.

- Eğer sadece bir servis (sadece http gibi) kullandırmak amacıyla benzer bir kurulum arıyorsanız, bundan daha güvenli ve daha kısıtlayıcı olması yönünden mutlaka farklı NAT modlarını kullanmalısınız.

2. örnek


Using Static NAT With A Private and DMZ Zone
Private IP
192.168.200.2
Mapped to 203.31.218.5
via Firewall No.1
Public IP
203.31.218.2
Private IP
192.168.200.1
NetWare Server
IP 192.168.0.10
Firewall No.1
IP 192.168.0.1
Internet
Hub or Switch
Firewall No.2
Public IP
203.31.218.1
Firewall No.2 prevents
any access to the rest of
the Private Network
Hub or Switch
Private IP
192.168.100.1
Workstation
IP 192.168.0.11
Private Network
DMZ
Zone
Private IP
192.168.100.2
Mapped to 203.31.218.3
via Firewall No.1
Public
Webserver
Public
Mailserver
Private IP
192.168.100.3
Mapped to 203.31.218.4
via Firewall No.1
Public Access to DMZ Zone
via Firewall No.1
A very realistic approach in the use of Static NAT. While both the DMZ Zone and Private network
have their own private IPs, Firewall No.1 maps the Public IPs to the servers, allowing
the Internet to access them directly but safely with the use of packet filters.

- Statik NAT için diğer bir örnek DMZ alanlarının kullanılmasıdır. DMZ alanları; bazı gerekli makinelar (webserver, e-mail server gibi) internete direk erişebilip, aynı zamanda bütün datanın saklanması ve özel ağın internet bağlantısına da engel olmaması gereken alanlardır.

- Bu diyagramda 1.firewall'a 3 ağ bağlıdır;

a- internet (203.31.218.X),

b- DMZ alanı (192.168.100.X)

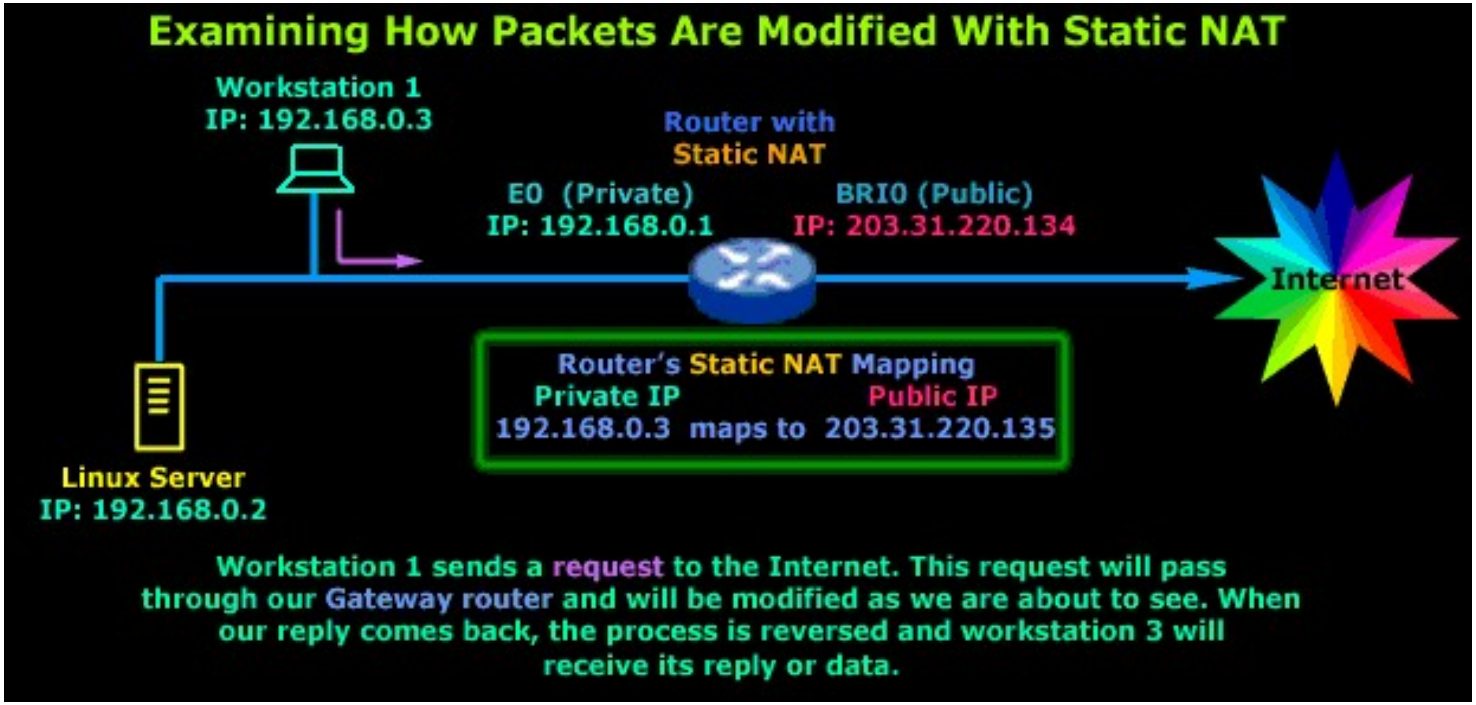
c- iki firewall arasındaki küçük özel ağ (192.168.200.X).

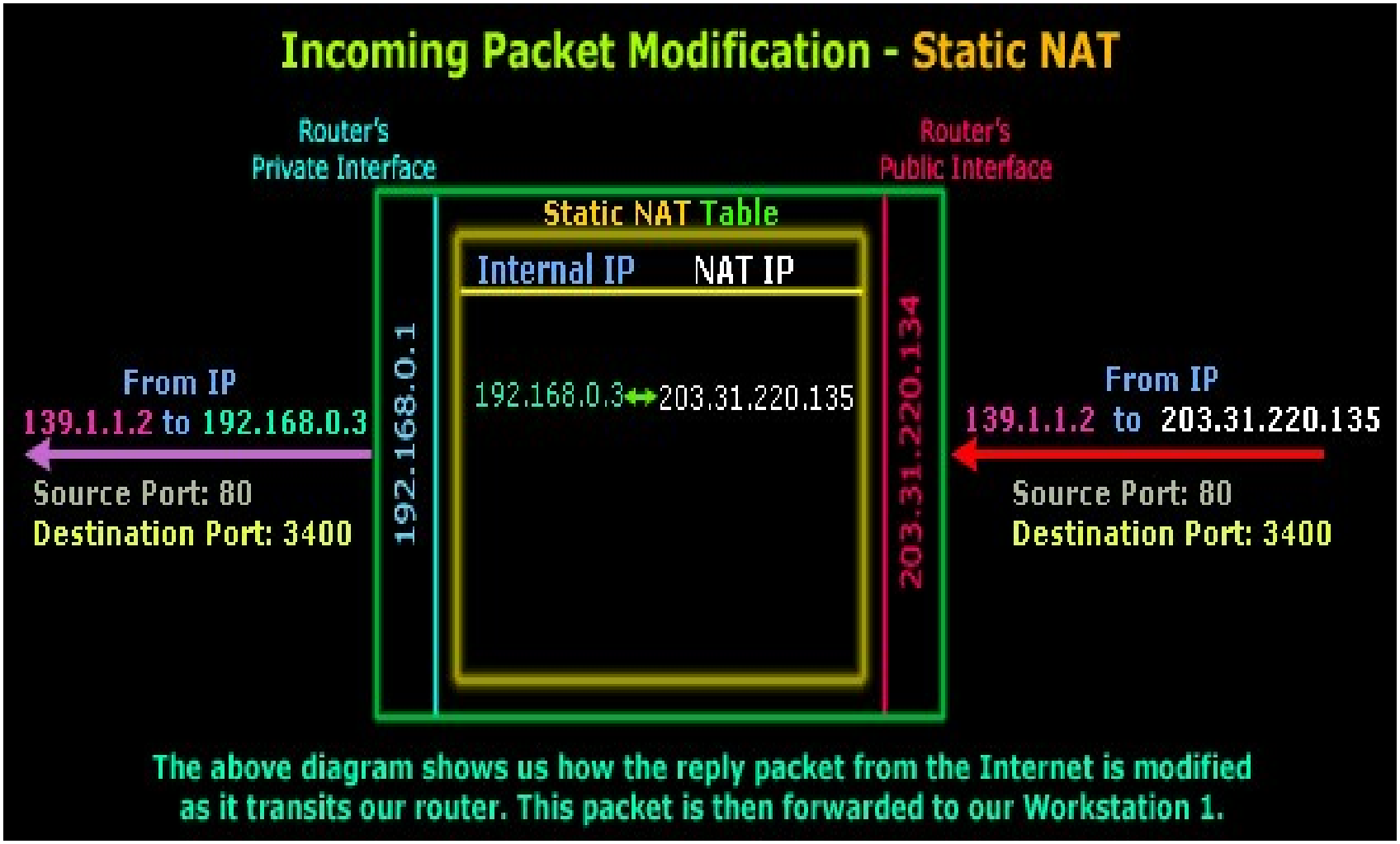
1.Firewall 3 farklı host için statik NAT olarak konfigure edilebilir, bunlardan ikisi DMZ'deki serverlar, diğeri ise 2. firewall.

- Firewall'deki her bir arabirim, aralarında yönlendirme yapılabilmesi için farklı ağların bir parçası olmalıdır. Bu sebeple diyagram IP adresleri yönünden karışık görünmekte fakat bunlar gerekli olmaktadır.

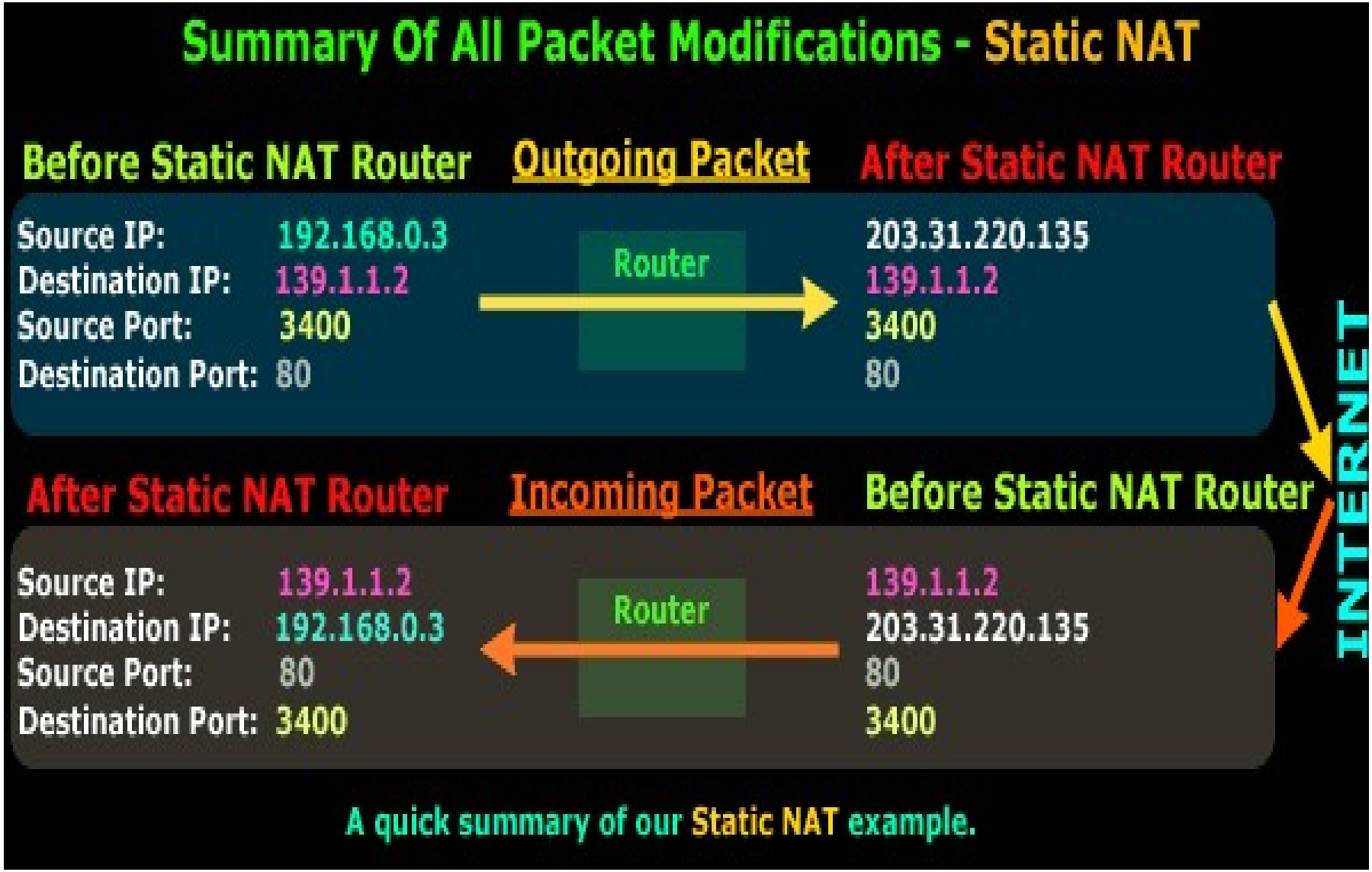
NAT adres dönüşümü nasıl meydana gelir?

- Statik NAT dönüşümü işlemi bunu destekleyen tüm cihazlarda aynıdır, değişmez. Yani bir router veya firewall kullanırsak her ikiside statik NAT'ın kullanılmasında aynı özelliklere sahip olacaktır.
- Burada hosttan gelen paketin routerda nasıl değiştiği görülüyor. Sadece 192.168.0.3 olan kaynak IP adresi 203.31.220.135 gerçek IP adresi ile değiştiriliyor. Hedef IP adresi, kaynak portu veya hedef portu değiştirilmiyor.
- Paketin, gönderildiği hedef tarafından alındığını ve cevap gönderildiğini farzedelim; alınan cevap veya bu hotsa gelen diğer paketler bu modifikasyonda aynı sıraya girerek alınmalı ve ilgili host'a teslim edilmelidir.



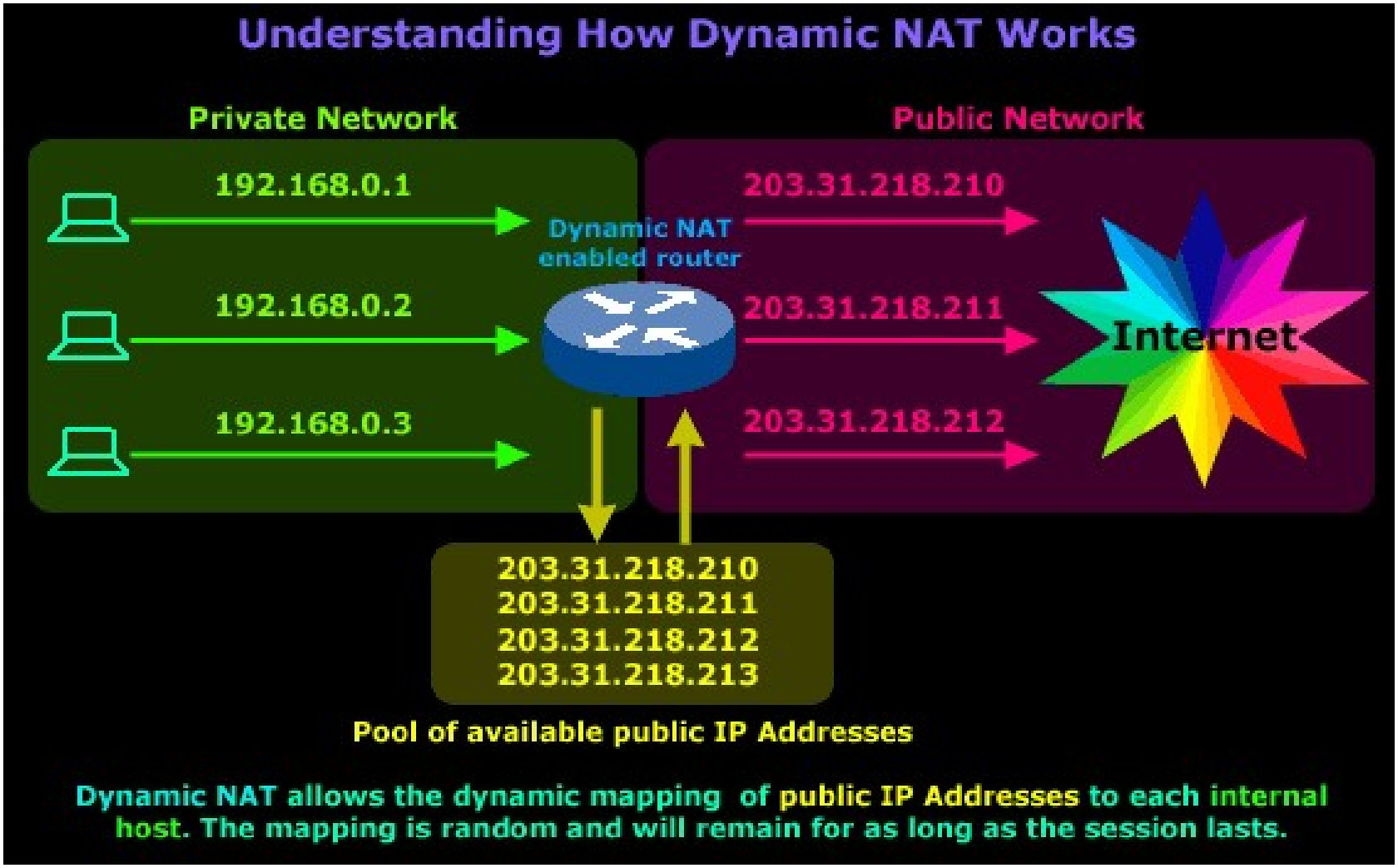


- Bu diyagram gelen paketlerin router içerisinde uğradığı değişikliği gösteriyor.


Summary Of All Packet Modifications - Static NAT
Before Static NAT Router
Outgoing Packet
After Static NAT Router
Source IP: 192.168.0.3
Destination IP: 139.1.1.2
Source Port: 3400
Destination Port: 80
Router
203.31.220.135
139.1.1.2
3400
80
INTERNET
After Static NAT Router
Incoming Packet
Before Static NAT Router
Source IP: 139.1.1.2
Destination IP: 192.168.0.3
Source Port: 80
Destination Port: 3400
Router
139.1.1.2
203.31.220.135
80
3400
A quick summary of our Static NAT example.

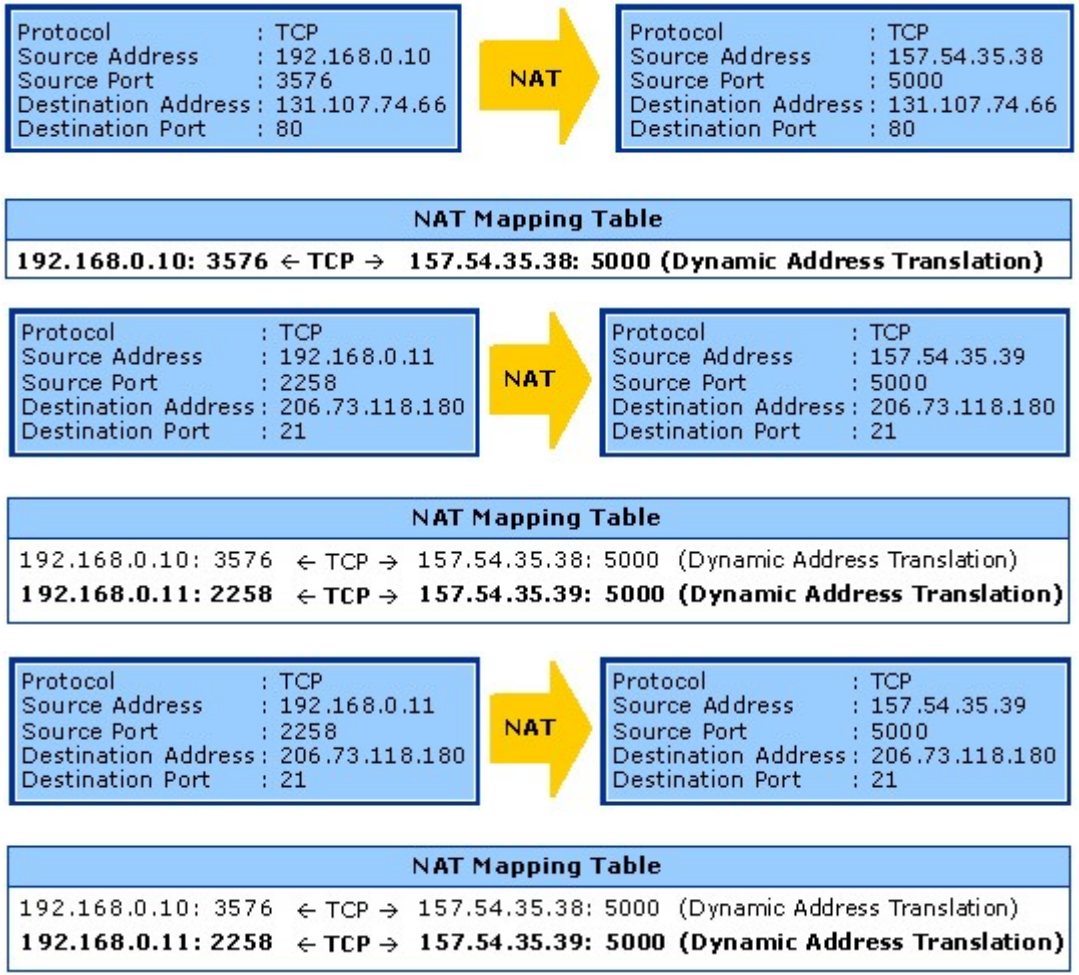
DİNAMİK NAT

- Dinamik NAT ile özel IP adreslerimizi gerçek IP adreslerine –statik olmayan bir yolla dönüştürürüz. Yani dahili hostların internet ile iletişim kurduğu her bir oturum için, onların gerçek IP adresleri aynı kalsa da (muhtemelen değişebilir) Bu IP adresleri ISS tarafından bizim özel ağımıza tahsis edilmiş olan IP havuzundan çekilirler.
- Dinamik NAT'ta, router IP dönüşümü için gerekli trafik bilgisini almadan NAT tablosu üzerinde dönüşüm gerçekleşmez.
- Dinamik dönüşümler NAT tablosundan silindikten sonra ağdaki diğer hostlar tarafından kullanılmak için bir timeout periyodu tutarlar.



- Bu örnekte, bizim router ile dahili hostları ayarlayabilmemiz için ISS'den 4 gerçek IP adresi isteğimiz vardır(203.31.218.210'dan 203.31.218.213' kadar).
- 192.168.0.1 özel IP adresine sahip host, internete bir istek gönderirken kurulan küçük oturumda, bu host'a 203.31.218.210 gerçek IP adresi tahsis ediliyor ve bu tahsis oturum sonlandırılana kadar devam ediyor.

Varsayınız Firewall'un public ağa bağlanmak için 157.54.35.38 ve 157.54.35.39 gibi iki tane resmi IP adresi vardır.



Linux Netfilter ile NAT örnekleri

• Maskeleme (dynamic IP addresses)
**iptables -t nat -A POSTROUTING -o eth0 -s 10.1.0.0/16 **
-j MASQUERADE

• Source NAT (static IP addresses)
**iptables -t nat -A POSTROUTING -o eth0 -s 10.1.0.0/16 **
-j SNAT --to 1.2.3.4-1.2.3.6

• Destination NAT (with static IP addresses)
**iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 **
-j DNAT --to 10.1.0.7:8080

Port Yönlendirme

• Statik ağ adres çevriminin özelleşmiş bir halidir. Dış dünyadan iç ağdaki web, ftp, e-posta gibi sunuculara erişim sağlanması amacıyla kullanılır.

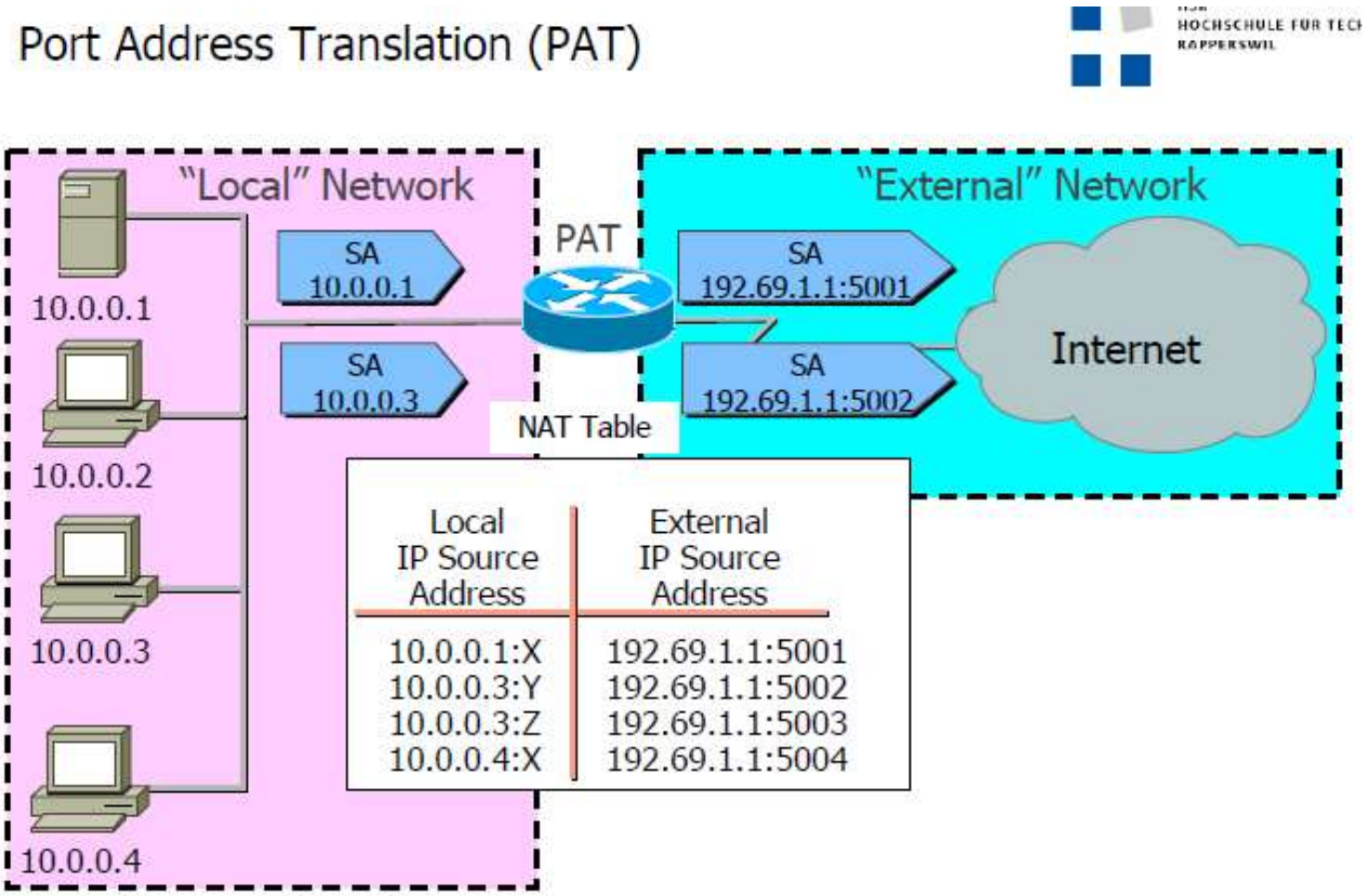
• Port yönlendirmede erişim sağlanmak istenen sunucuya ilişkin gerçek IP adresi, güvenlik duvarının dış dünyaya açılan IP adresi olarak belirlenir.

•Dış dünyadaki herhangi bir kullanıcı söz konusu sunucuya ulaşmak için aslında güvenlik duvarının gerçek IP adresine erişim sağlar.

•Daha sonra güvenlik duvarı gelen bağlantı isteğini inceleyip kendisi için olup olmadığına bakar. Sonuç olarak bağlantı isteği eğer güvenlik duvarı için değilse ilgili sunucuya yönlendirilir.

• Böylelikle iç ağdaki sunucuya dış ağdan erişim sağlanmış olur. Bu tür erişimler için statik ağ adres çevrimi yerine port yönlendirmenin kullanılması daha güvenli olmaktadır.

Port yönlendirme



SALDIRI ÖNLEME MEKANİZMASI

• son zamanlarda saldırı önleme özelliği güvenlik duvarlarında da bir özellik haline gelmeye başlamıştır.

• Normalde saldırı tespit ve engelleme sistemlerine ait olan bu güvenlik özelliği, güvenlik duvarlarına da kısıtlı olarak entegre edilmeye başlanmıştır.

•Bu özellik genellikle uygulama tabanlı güvenlik duvarlarında bulunmaktadır. Bu tip güvenlik duvarları gelen paketlerin içeriğini kontrol edebilmektedir. Böylelikle zararlı içerik taşıyan paketler tespit edilip engellenebilmektedir.

• Ayrıca tespit edilip engellenen saldırılara ilişkin kayıtlar tutulabilmektedir. Daha sonradan bu kayıtlar incelenip saldırıların niteliği hakkında fikir edinilebilir.

Örneğin saldırıyı yapan bilgisayarın IP adresi tespit edilip bu IP adresinden bundan sonra gelen bütün paketlerin bloklanması sağlanabilir. TCP – SYN seli gibi birçok servis dışı bırakma saldırısı engellenebilir.

Ancak güvelik duvarlarındaki bu özellik sınırlıdır ve sadece saldırı imzaları dâhilindeki saldırılar tespit edilip durdurulabilmektedir. Bu nedenle iç ağa gelen saldırıların tespit edilmesi ve engellenmesi için sadece bu amaç için özelleşmiş olan saldırı tespit ve engelleme sistemleri kullanılmalıdır.

Güvenlik duvarının saldırı önleme mekanizmasına ilişkin aşağıdaki adımlar gerçekleştirilmelidir:

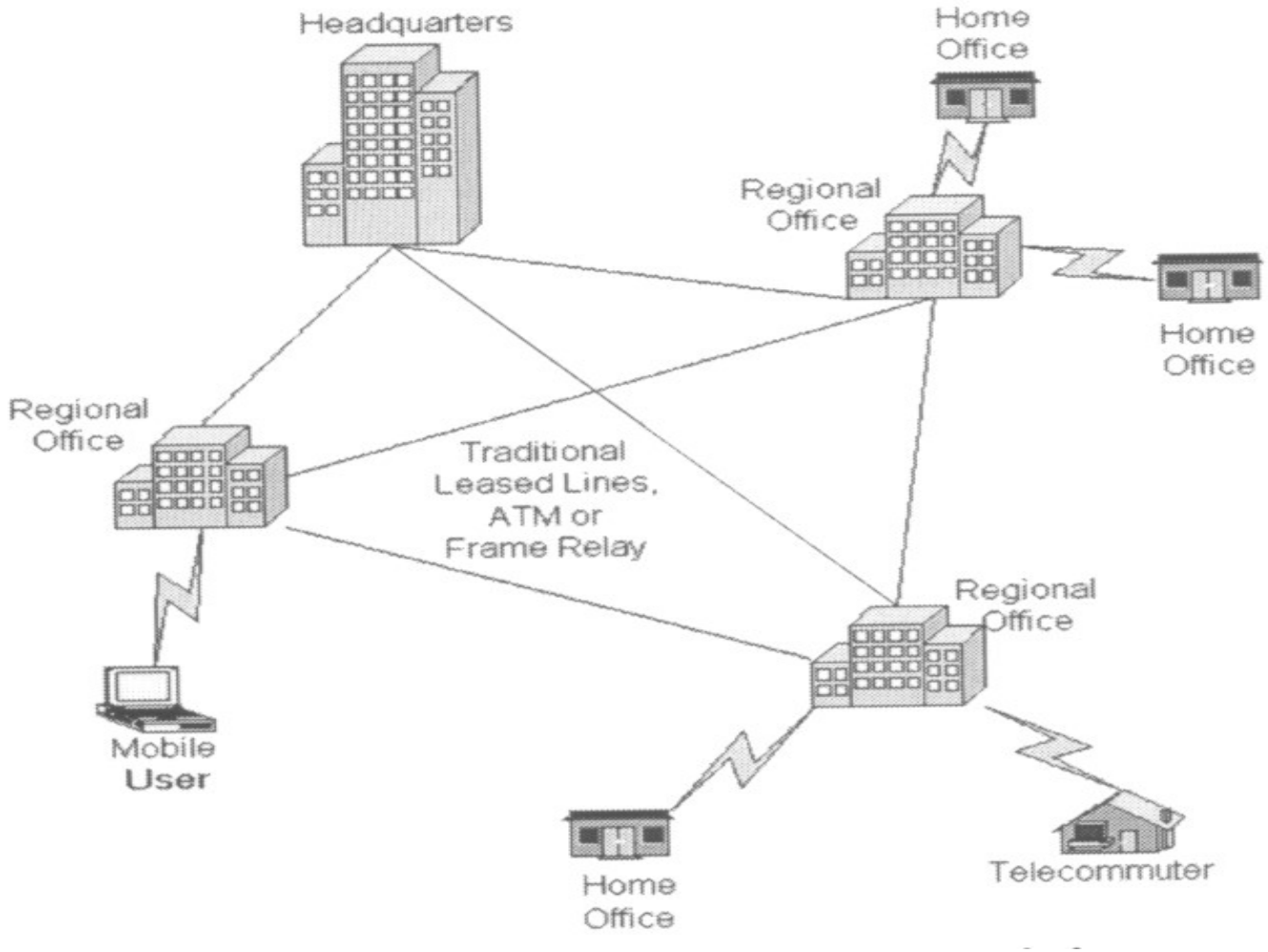
•En son çıkan güvenlik tehditlerine karşı koruma sağlanabilmesi açısından saldırı imzaları periyodik olarak güncellenmelidir.

• Hem güvenlik duvarının yükünü hafifletmek hem de yanlış alarmların **(false positive) sayısını azaltmak amacıyla gerek duyulmayan imzalar pasif hale getirilmelidir.**

• Denetlenebilirliğin arttırılması amacıyla kritik saldırılara ilişkin kayıtların tutulması sağlanmalıdır.

VIRTUAL PRIVATE NETWORKS (VPN)

Geleneksel Bağlantı



VPN nedir?

•VPN(Virtual Private Network/Sanal Özel Ag) internet üzerinden sifreli ve güvenli veri iletisimi saglamak için düsünülmüs bir teknolojidir.

• Kamusal bir iletişim ağı üzerinde, Kiralık hatlar(Lease-line) gibi daha güvenli, saglam çözümlerin yerine VPN kullanilmasinin temel nedeni, maliyet ve kolay yapılandırmadır.

•Tüm VPN çözümlerinde İnternet erişimi üzerinden kurulan güvenli tüneller söz konusudur. Güvenli tüneller, kriptolama teknikleri ile sağlanır.

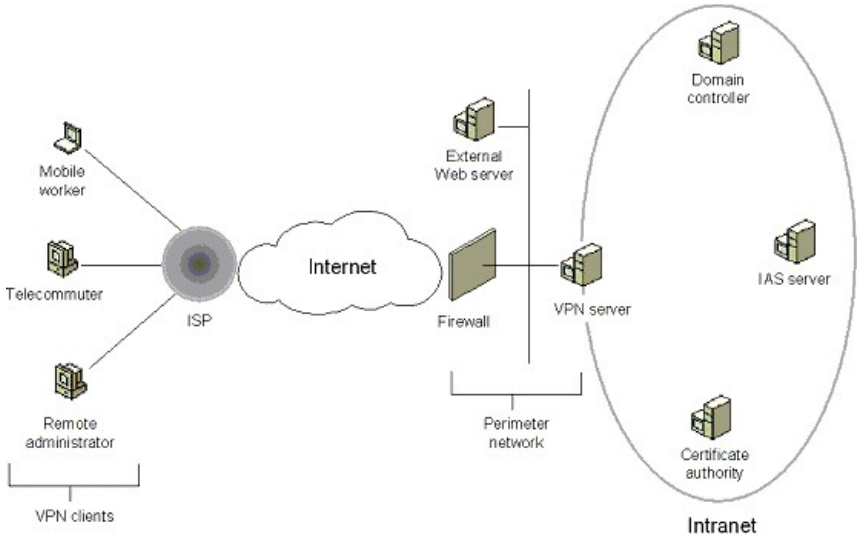
• Gartner Group; VPN'i, herkese açık bir iletişim altyapısı üzerinden, iki veya daha fazla doğrulanmış/onaylanmış taraflar arasında güvenli veri iletişimi sağlamak üzere oluşturulmuş sanal ağlar olarak tanımlar.

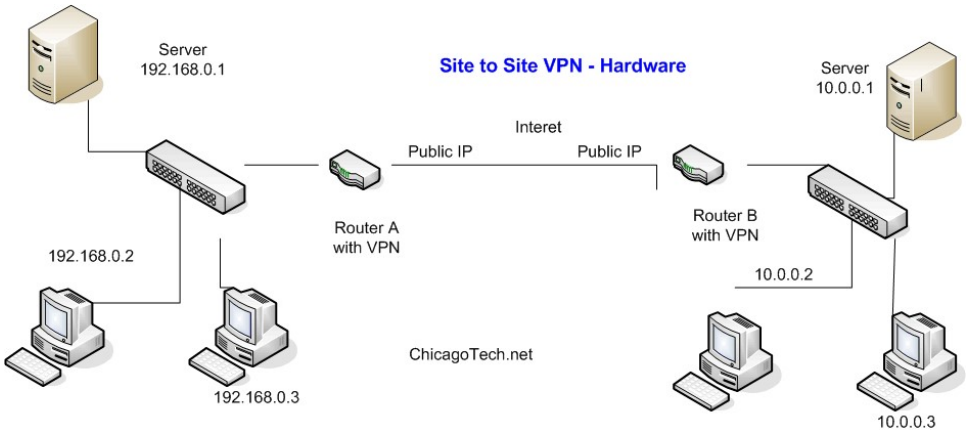
Virtual Private Networks

Temelde iki tip VPN teknolojisi vardır. Amacımıza gore bu iki VPNteknolojisinden birini seçebiliriz. Bu teknolojiler

1- Remote Access VPN (Uzak erişim VPN -)

2-Site-to-site VPN



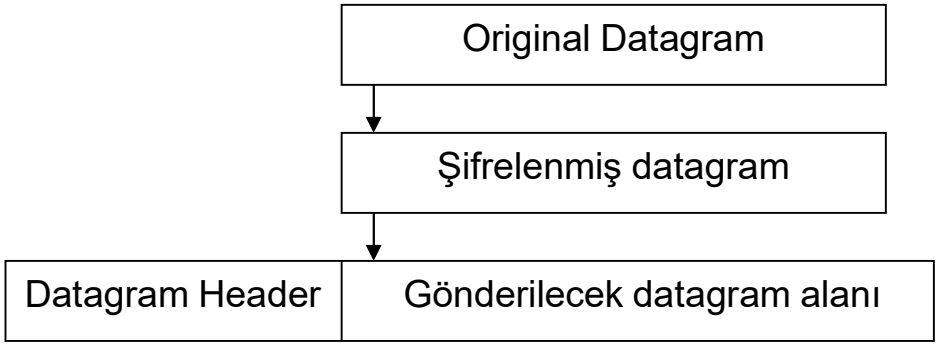


VPN 4 kritik Fonksiyonu yerine getirir

- Authentication – Veriyi gönderen, alanın doğru kişi olduğunu bilir.
- Access control – Yetkisiz kişiler VPN'i kullanamaz.
- Confidentiality – Veri gizliği garanti edilir.
- Data Integrity – Veri bütünlüğü garanti edilir.

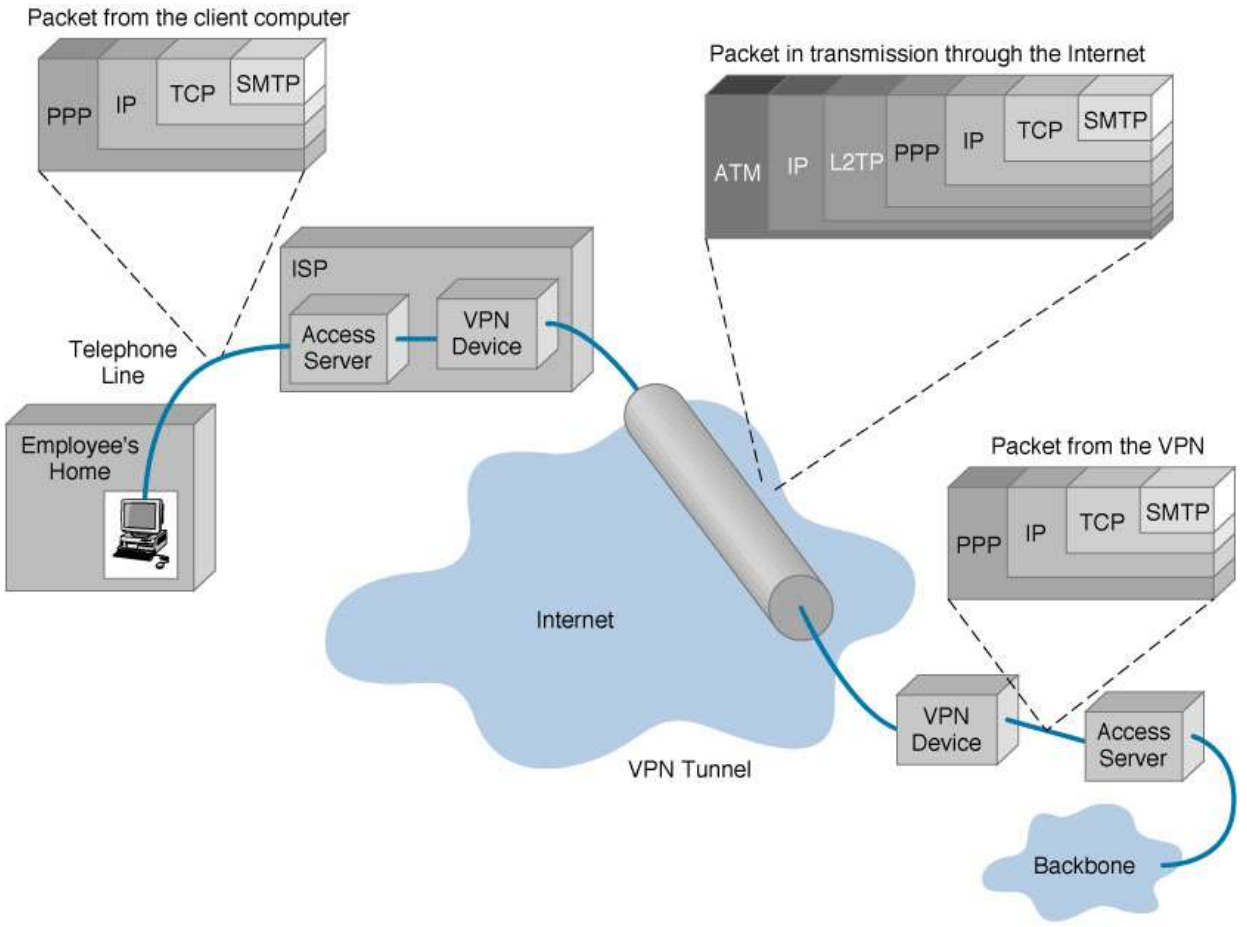
Tunelleme

- Bir genel ağ üzerinde sanal bir point-to point bağlantı oluşturmaktır. Tünel tekniğini 2 fazda anlatabiliriz:
- Faz1: İstemci VPN isteğini gönderir ve HA (Home Agent) sistemi bu istemcinin kimlik sorgulamasını yapar.
- Faz2: Tünel içinden veri transferi başlatılır.



Data kapsülleme

Paketlerin VPN kapsüllenmesi



Tünelleme protokolleri üç kategoride sınıflandırılabilir:

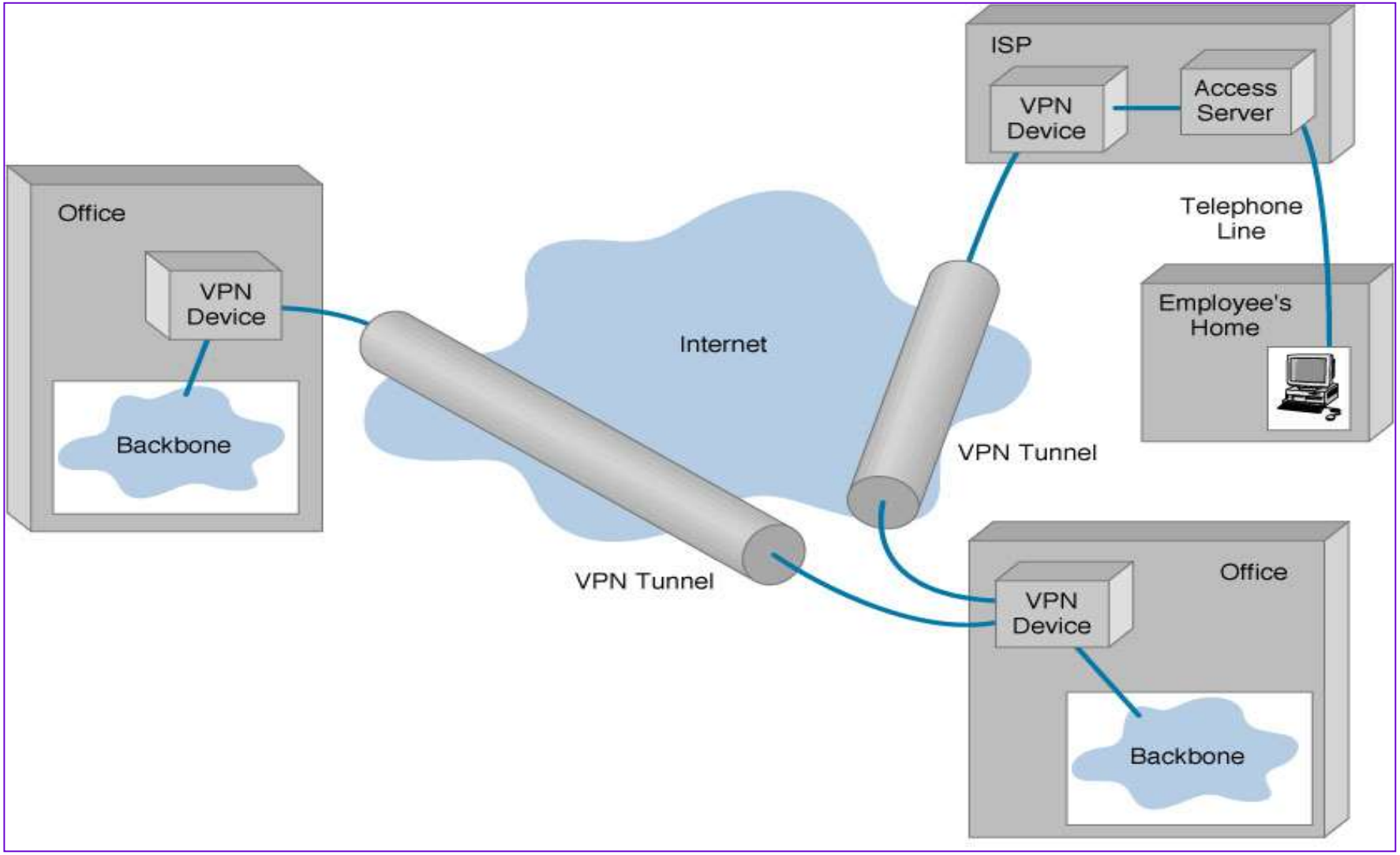
1. Taşıyıcı protokoller: Tünellenmiş paketlerin Internet üzerinden iletimini sağlamak için bu paketleri yönlendirir. Tünellenmiş paketler bu protokolün paketleri içine enkapsüle edilir.

2. Enkapsüle protokolleri: Pay-load paketin enkapsüle edilmesini sağlar. Bu protokol ile tünel kurulur ve sonlandırılır. Günümüzde en yaygın olan enkapsüle protokolleri PPTP, L2TP, ve IPSEC'dir.

3. İletim protokolleri: Tünel içinden iletilmesi amacıyla enkapsüle edilmesi gereken orijinal veriler için bu protokol devreye girer. En yaygın olan iletim protokolleri PPP ve SLIP (serial line internet protocol) protokolleridir.

Virtual Private Networks (VPN)

Basic Architecture



VPN gerçekleştirme tipleri

- 3 tip
  - Hardware
  - Firewall
  - Software

Device Types: Hardware

- Genellikle VPN desteği olan Routerlardır.

Device Types: Firewall

Hem Firewall, hem VPN? Oldukça pahalı bir çözüm.

Device Tipi: Software

- Aynı organizasyonun iki son noktası arasında kullanımı için uygundur.

En çok kullanılan yazılımlar

PPTP Çözümü : Poptop
Ipsec Çözümü : Linux OpenSWAN, OpenBSD Ipsec
SSL VPN Çözümü : SSLExplore, OpenVPN
L2TP Çözümü : OpenL2tp
Gerçek bir VPN Çözümü Olarak OpenVPN