|  |
| --- |
| ***Network Bilgisi*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Penetration testlerinde öncelikle temel network bilgisine ihtiyaç duyulmaktadır.Bu sebeple yaptığım araştırmaları sizler ile paylaşmak istiyorum. |

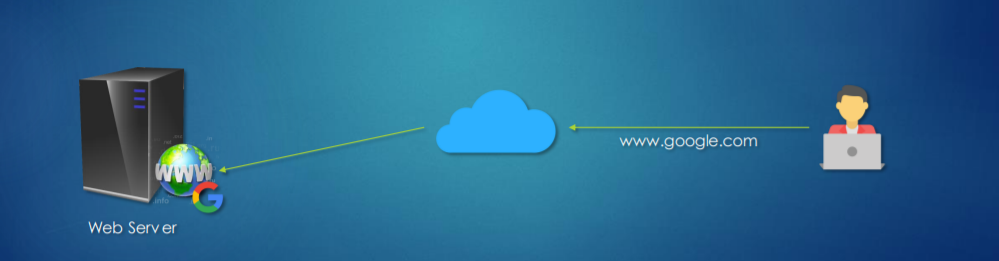
**26.11.2021**

***Ağ Nedir?***

-Birbirleri ile belirli kurallar çerçevesinde,iletişim kurabilen cihazların oluşturduğu yapıdır.

-Dosya,Program ve Donanım paylaşımına olanak sağlar.

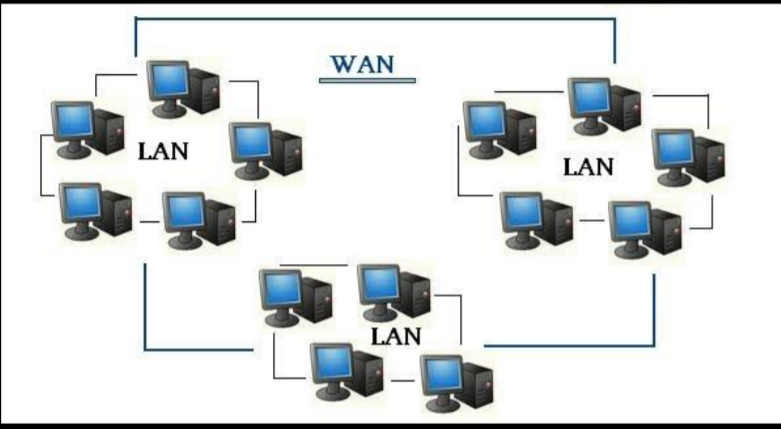
-Ayrıca bu karmaşık yapıyı güvenilir ve merkezi yönetim ile erişim sağlamamızı sağlar.



***Başlıca Ağ Donanımları***



***Network Mimarisi***

******

***1-)LAN(Local Area Network):***

-LAN’lar yüksek hızlı, güvenilir ve küçük bir alana yayılmış olan lokal (yerel) ağlardır.

Örn; bir şirketin veya bir evin içindeki ağdır.

“İç ağ” da denir.

***2-)WAN(Wide Area Network):***

-Coğrafi olarak birbirinden uzak LAN’ların birleştirilmesiyle oluşan ağdır.

Örn; internet ağı

“Dış ağ” da denir.

***Network Protokolü***

-Ağda çalşan cihazların iletişim kurabilmeleri için gerekli kurallar bütünüdür.

-Günümüzde en yaygın kullanılan protokol TCP/IP protokolüdür.TCP/IP her türlü ağda kullanılabilen esnek,gelişmiş ve hızlı bir protokoldür.

-Kullanılmak istenen protokolü,işletim sistemleri sağlar.

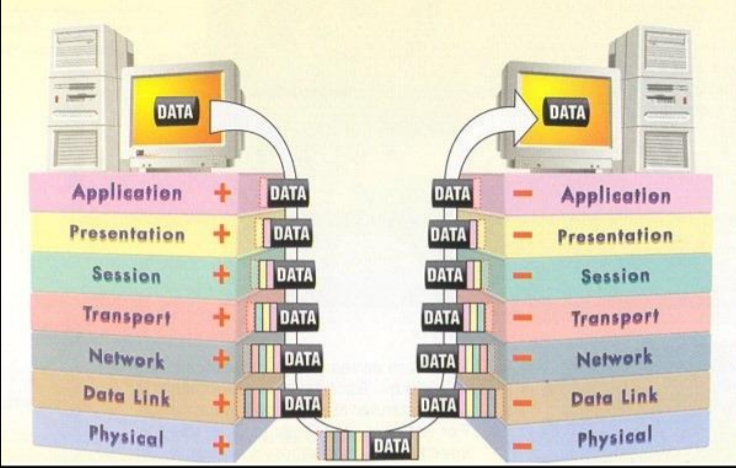
***OSI(Open System Interconnection) Referans Modeli***

-Network denince akla gelen 7 katmandan oluşan bir referans modelidir.

-Her bir katman,alt katmanından hizmet alırken üst katmanına hizmet verir.

-Gönderici her bir katmanda veriye(pakete) kendi bilgisini ekler.Alıcı da çıkarır.

-Bu katmanları şu görsel ile göstermek isterim.



***7-)Application Layer (Uygulama Katmanı):***

-E-posta,dosya transferi,web erişimi gibi ağ hizmetleri sağlayan servisleri denetler.

-Prensentation(Sunum) katmanında gelen paketi de uygulamada açıp kullanıcıya görüntüler.

-Kullanıcıya en yakın katmandır.

***6-)Presentation(Sunum) Katmanı:***

-APP katmanında gelen kullanıcının isteklerini yorumlayıp,alt katmanlara hazırlanması için işleme hazırlanır.

-Dönüştürme işlemlerini yapar.

-Şifreleme,çözme,sıkıştırma,karakter seti değişimi,grafik komutlarının yorumlanması gibi işler burada yapılır.

-Gelen paketlerin kullanıcıya aktarımı için de burada hazırlanılır.

***5-)SessionLayer(Oturum) Katmanı:***

-Diğer bilgisayarlar ile iletişim sağlandığında uygulamalar arasında oturum burada açılır.

-Karşılıklı iki uygulamanın birbirini bulduğu katmandır.

-Bu oturumun kopmaması, stabil olması, oturumda veri senkronizasyonu gibi görevleri vardır. Çakışmaları önler.

-İletişimde problem olması halinde gönderilen verinin baştan komple gönderilmemesi için veriye checkpoint’ler koyar.

Aksaklık halinde ne kadarı gönderilmediği tespit edilerek sadece o kısım gönderilir.

***4-)Transport Layer(Ulaşım) Katmanı:***

-Birincil görevi, paketin alıcıya ulaştığından emin olmaktır.

-Session katmanından gelen verileri, network katmanın daha iyi anlayabileceği şekilde küçük parçalara böler.

-Bu parçalara segment adı verilir. Segment’leme görevi buranındır.

-Alt ve üst katmanların eş zamanlı çalışabilmesini de sağlar.Bu işleme multiplexing adı verilir.

-Web’de gezerken aynı anda download yapılabilmesinden bu katman sorumludur.

-TCP (Transmission Control Protocol) ve UDP (User Datagram Protocol) bu katmanda işlenir.

***3-)Network Layer(Ağ) Katmanı :***

-En önemli katmandır.

-Paketlerin hangi route (rota) üzerinden gideceğini belirler.

-Paketin hedefe ulaşımında birden fazla rota varsa doğrusuna karar vermekle sorumludur.

-Bu yüzden IP adresi burada girilir.

-Verinin kalitesi (QoS – Quality of Service) de burada belirlenir.

-Segment boyutlarını, Data-Link katmanının daha iyi anlayabileceği daha küçük segmentlere böler.

***2-)Data-Link(Veri) Katmanı:***

-Gönderilen verilerin elektrik sinyallerine dönüştürülüp kabloya iletilmesini ve tersi yöndeki işlemi gerçekleştiren katmandır.

-MAC bilgisi burada girilir.

-Network katmanından gelen segment’leri,Physical katmanda yola çıkabilecek şekilde frame’lere böler.

-Frame tipi gibi bilgiler burada eklenir.Yolda bozulabilecek frame’leri tespit etmek için frame’lere

-CRC (Cyclic Redundancy Check) bilgileri ekler.

-Karşı bilgisayarda CRC bilgisi doğru okunuyorsa frame bozulmamıştır.

***1)Physical Layer(Fiziksel) Katman:***

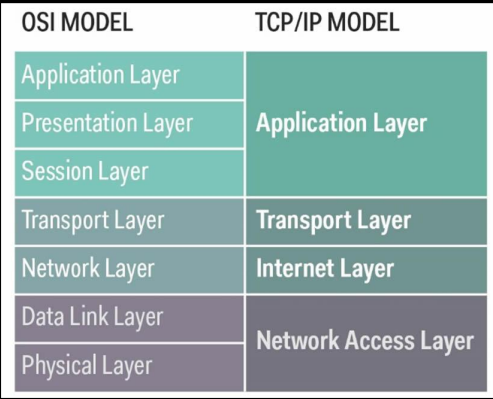
-Elektriksel, optik veya kablosuz sinyalleri A noktasından B noktasına iletmekle sorumludur.

-Sadece bit’lerin bir bilgisayardan diğerine ulaşmasıyla ilgilenir.

-Paketi teslim etmekle sorumludur, içeriğiyle ilgilenmez.

-Bu katmanda pakete, paketin hangi sinyalle taşınacağı,bit’lerin ne şekilde dizileceği, konnektörlerdeki kaç pin ile çalışılacağı, adaptörün ne zaman veri gönderip alacağı,teslimatın başarı durumu gibi detaylar tanımlanır, pakete yazılır.

***TCP/IP Modeli***

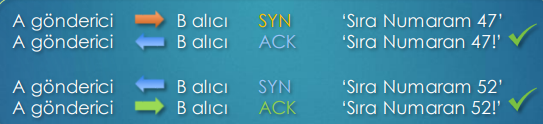


***TCP(Transmission Control Protocol)***

-Bağlantı temelli, güvenilir bir iletim protokolüdür.

- Veri iletimine başlamadan önce gönderici ve alıcı arasında anlaşma sağlar.

- Alıcıya ulaşmayan veriyi tekrar yollar.



***UDP(User Datagram Protocol)***

-Bağlantı temelli değildir ve kontrol mekanizmaları içermez.

- Kontroller yapmadığı için TCP’den hızlıdır.

- Hızın, güvenirlikten önemli olduğu bağlantılarda kullanılır.

***Portlar(Ports)***

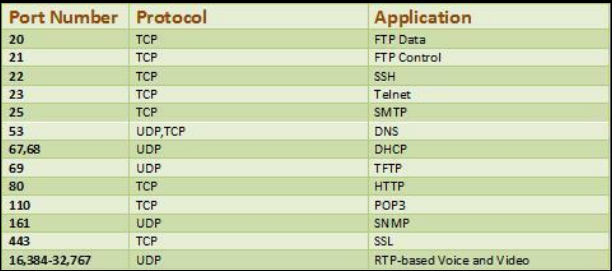
-Portlar, bilgisayarların giriş kapılarıdırlar.

- TCP ve UDP bağlantılar, veriyi üst katmanlara taşımak veya uygulamaya iletmek için port numaraları kulanırlar.

- Port numaraları, aynı anda yapılan farklı iletişimleri ayırt etmek için kullanılırlar.

- Her application katmanı servisi, belirli bir port’tan sunulur.

- Bir bilgisayarda 65535 adet port vardır. 1024 tanesi iyi bilinendir.



***TCP Bağlantı Başarım Protokolleri***

***ARP(Address Resolution Protocol):***

-Ağ cihazlarının 2 adresi vardır.

a-)***MAC:*** -Fiziksel adresidir.

-Ağ kartlarının ROM belleğine üreticisi tarafından yazılır.

-48 bit’lik hexadecimal (on altılık) bir sayıdır.

-Örn; 4F-00-1C-25-1B-4B

b-)***IP:*** -Mantıksal adresidir.

-Cihazlara yöneticiler tarafından yazılır.

-32 bit’lik binary (ikilik) bir sayıdır.

-Örn; 11000000.10101000.00000001.00001010

-Böyle bir sayıyı hatırlamak ve yazmak zor olduğu için her 8’li grup (4’lü parça) decimal’e (ondalık) çevrilmiştir. Sayı artık 192.168.1.10’dur.

-Verinin gönderilebilmesi için her iki adresin de bilinmesi gerekir. Bilinmiyorsa ARP Request mesajı yayınlayıp öğrenebilinir.

***ICMP(Internet Control Message Protocol):***

-Sorun gidermek ve hata tespiti için kullanılır.

a-)***Ping:*** -Kaynaktan hedefin IP’sine gönderilen küçük bir mesajdır (Echo Request).

-Mesajı alan bilgisayar cevap verir (Echo Reply).

-Mesajın hedefe ulaşması zamanlarını da gösterir (Rount Trip Time).

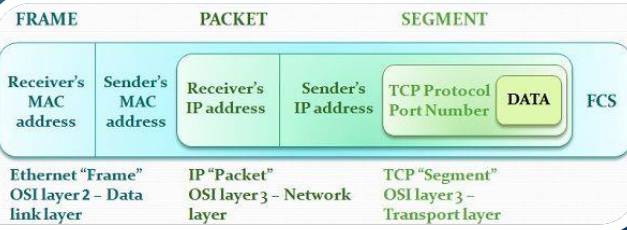
b-)***Tracert:*** Kaynaktan hedef IP’ye giderken geçilen IP ve cevap verme sürelerini gösterir.

***TCP/IP Paketleri***

- Bir ağın en küçük yapı taşlarıdır. İletişimdeki temel bilgi birimleridir.

- Kaynak, hedef, tip, metot, yaşam süresi, iletim doğruluk hesaplaması gibi bilgiler içerirler.

- Yola çıkmaya hazırlanırken her katmanda pakete bir bilgi eklenir.



- Data eklendikçe, sırasıyla Segment >>> Packet >>> Frame oluşur.

***RFC(Request For Comments)***

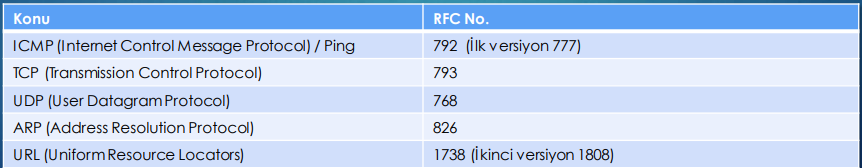
- Tüm internet standartları ve protokolleri için tanımlayıcı kurallardır.

- DNS, URL, WEB, DHCP, ICMP, HTTP gibi tüm kuralların tanımlarını içerir.

- Farklı yıllar ve çeşitli kişilerce ortaya atılmış önergelerin testi ve kabul görmesiyle oluşturulur.

- IETF (Internet Engineering Task Force) otoritesi tarafından yönetilirler.

- Tüm RFC’lere “https://tools.ietf.org/rfc/index” adresinden ulaşılabilir.



***IANA(Internet Assigned Numbers Authority)***

- IP adresleri, DNS adları, protokol atamaları, zaman senkronu gibi görevlerden sorumludur.

- Tescil işlemlerini, üst kuruluşu olan ICANN (Internet Corporation for Assigned Names and Numbers) üzerinden yürütür.

- IETF (Internet Engineering Task Force) ile yakın koordineli olarak hareket eder.

- Bölgelere göre IP veritabanları vardır.

***IP(Internet Protocol) Adresleri***

- IP adresleri, cihazların hangi ağda olduğunu ve ağdaki kimliğini belirtir.

- IP adresleri 32 bit’lik, binary ve mantıksal bir sayıdır.

- Örn; 11000000101010000000000100001010

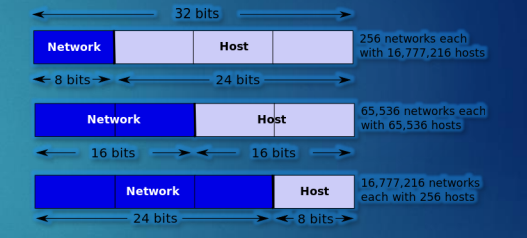
-Böyle bir sayıyı hatırlamak ve yazmak zor olduğu için önce 4 parçaya bölünür.

“11000000.10101000.00000001.00001010 “

-Her bir parçaya ‘oktet’ adı verilir. Her IP’de 4 oktet vardır.

-Her oktet de decimal’e (ondalık’a) çevrilir.

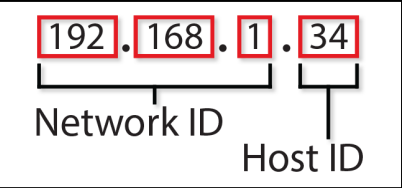
-IP, artık bizler için 192.168.1.10 şeklindedir.



-Bilgisayar için hala en başındaki gibi binary’dir (ikilik’tir.)

- Her oktet minimum 0; maksimum 255 değeri alabilir.

-Ip adresleri 2 kısımdan oluşur.



1-)***Network ID :*** Network'ün kendine ait ID'sidir. Bu ID, cihazların hangi ağda olduğunu belirtir.

-Aynı ağda olan cihazların Network ID’leri aynı olmak zorundadır.

2-)***Host ID:*** Cihazın, ağda kendisini tanımlayan ID’dir.

-Aynı ağda olan cihazların Host ID’leri farklı olmak zorundadır.

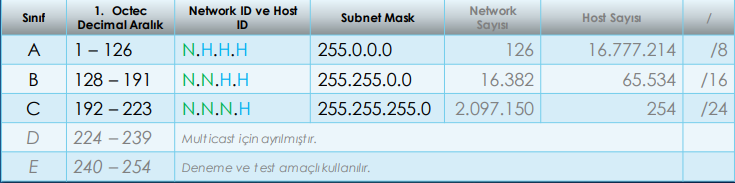
-0 değeri alamaz. Host ID’leri minimum 1; maksimum 254 olabilir.

***Subnet Mask***

-Ip adreslerinin Network ve Host ID'sini belireyen faktör Subnet Mask(Alt Ağ Maskesi)'dir.

-Subnet Mask'ı belirleyen de IP adresi sınıflarıdır.

-Her IP'nin Subnet Mask'ı ve sınıfı(class) vardır.



***İletim türleri ve teknikleri***

-Bir ağda 3 tür haberleşme vardır.

1-)***Unicast:*** Bir cihazdan sadece bir cihaza yapılan iletim.

2-)***Multicast :*** Bir cihazdan belirli bir grup cihaza yapılan iletim.

3-)***Broadcast :*** Bir cihazdan diğer tüm cihazlara yapılan iletim.

-Network'teki son host IPsi(.255),broadcast için kullanılır.

***Ağ servisleri***

-Ağ ortamında kullanıcılar ve bilgisayarlara hizmet etmesi gereken servisler vardır.

Örneğin;

DHCP,talep eden bilgisayarlara ağa katılması için IP dağıtır.

DNS, isimleri çözmelerine yardımcı olur.

NAT ise IP çevrimleri yaparak bilgisayarların dış dünyaya açılmasını sağlar.

***DNS(Domain Name System)***

-Bilgisayarlar birbirleri ile sadece rakamlarla (IP) ile haberleşirler,harflerle değil.

-Hedefe ulaşmak isteyen kaynağın,IP adresine ihtiyacı vardır.(LAN-WAN)

-Bu ismlerin IP karşılıkları gerekmektedir.İsim çözümlemesi yapılmalıdır.Bunları DNS sunucuları yapar.

-DNS sunucusuna, 'www.google.com' kimdir,IP'si nedir?' denir.O da geri dönüş yapar.

***DHCP(Dynmamic Host Configuration Protocol)***

-Client'ler IP adresini otomatik olarak alabilmek için ortamdaki DHCP sunucunu bilmelidirler.

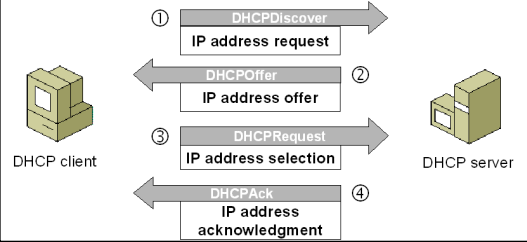
-Bunu,ağa broadcast yayını yaparak öğrenirler.Süreç şöyledir:

-***DHCP Discover (DHCP Keşfi):*** İlk kez IP alacak olan client, broadcast yayını yapar. Bu yayına DHCPDISCOVER adı verilir. Bu yayının içine MAC adresini de ekler.

-***DHCP Offer (DHCP Teklifi):*** Yayını alan DHCP sunucusu ağa DHCPOFFER mesajı yayınlar. Bu mesaj boroadcast’tir; tüm client’lara gider fakat içinde MAC bilgisi olduğu için sadece ilgilisi alır.

-***DHCP Request (DHCP İsteği):*** Client, DHCP’den gelen teklifi kabul ederse DHCPREQUEST yayını ile cevap verir. Bu mesaj da broadcast’tir.

-***DHCP Acknowledgement (DHCP Onayı):*** DHCP, isteği kabul ettiğini DHCPACK broadcast yayınıyla duyurur ve client, IP adresi edinmiş olur.



***APIPA(Automatic Private IP Addressing):***

- DISCOVERY yayınına bir DHCP’den cevap alamayan client, ağ IP’si alamaz.

- Fakat kendine bir IP atar. Buna APIPA (Automatic Private IP Addressing) denir.

- APIPA IP’si 169.254.x.x şeklindedir; subnet’i ise 255.255.0.0’dır.

- APIPA IP’si almış diğer client’lar ile görüşebilir.

***NAT(Network Address Translation)***

-Bir network için geçerli 2 tür IP vardır:

1) ***Private IP***: Lokal network’te (LAN’da) kullanılan IP’lerdir. Lokal network’e aittirler. İç IP’lerdir.

2) ***Public IP***: Dış network’te (WAN’da) kullanılan IP’lerdir. İnternet’e aittirler. Dış IP’lerdir.

- NAT, bu ağlar arasında IP çevirme işini yapar.

- Public (WAN) ve Private (LAN) ağlarının birbiriyle haberleşebilmelerini sağlar.

- Bilgisayarınızın IP’si Private IP’dir.

- Evinizin IP’si Public IP’dir.

- Modeminizin eve bakan bacağında Private IP; internete bakan bacağında Public IP vardır.

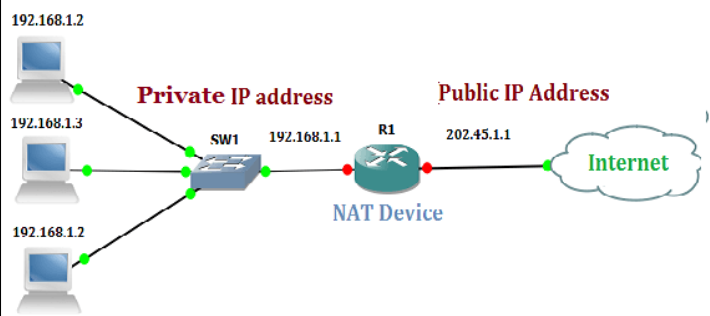
Örneğin; 192.168.2.1 (Private IP) (İç IP)

88.249.51.113 (Public IP) (Dış IP)

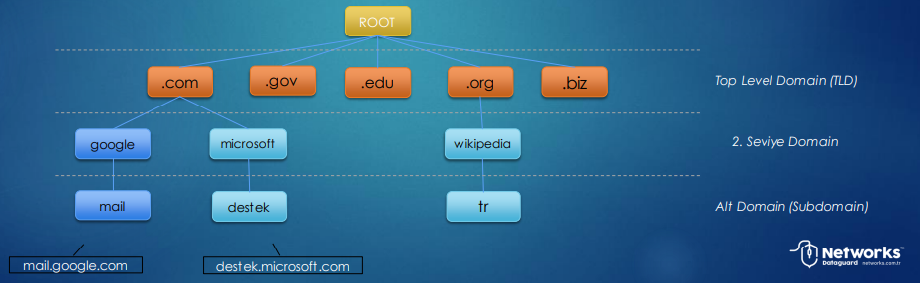
-Client’ın 192.168.2.10 Private IP’si, 3000 portu ile, Server’ın 85.74.114.25 Public IP’sinin 80 portu ile haberleşemez. -Çünkü farklı network’teler. Network ID’leri, subnet’leri farklı araya NAT girerse haberleşebilirler.

-Modem’de, İnternet Hizmet Sağlayıcı (ISP) tarafından atanan bir Public IP vardır.

-NAT, client’ın Private IP’sini, modemin Public IP’si ile değiştirerek hedefe gönderir ve böylelikle haberleşebilirler.Bu işlem ters yönde de gerçekleşir.



***Domain,DNS Hiyerarşisi ve FQDN Kavramları***



İnternet’teki DNS’ler hiyerarşik bir isimlendirme metodu kullanırlar. Bu isimlendirmelere domain adı verilir.

-Ağaç şeklinde domain grup’ları ve bu domain grup’larının alt grupları şeklindedir.

-Bütün domain’ler Root (kök) adı verilen tek bir domain’de birleşirler.

-Tüm domain’ler Root domain’in üyesidir. Bu yapıya DNS Hiyerarşisi (DNS Hierarchy) denir.

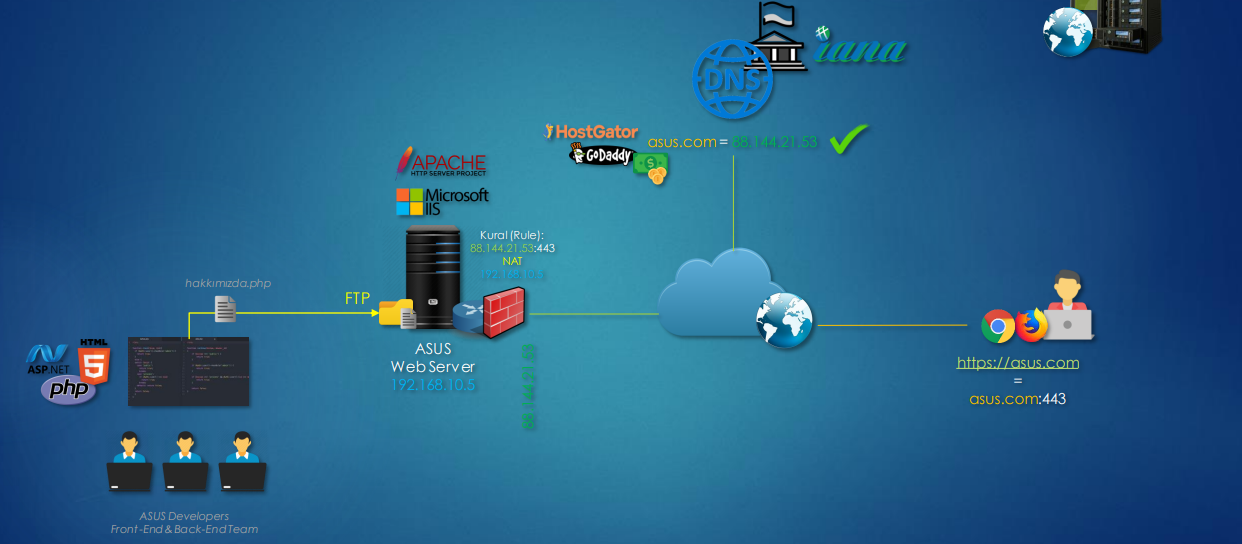
***FQDN(Full Qualified Domain Name):***

-DNS hiyerarşisinde bir bilgisayarın tam adresini belirten tamamlanmış addır. “mail.google.com” bir FQDN'dir.

-Domainler,bir nesneler topluluğunu temsil etmek ve bunların merkezi yönetilebilirliği amacıyla şirket içlerinde de uygulanabilirler.Örn;pepsi.local

-Burada da server05.pepsi.local veya muhasebe03.pepsi.local bir FQDN’dir.

***Web Hosting Süreçleri***



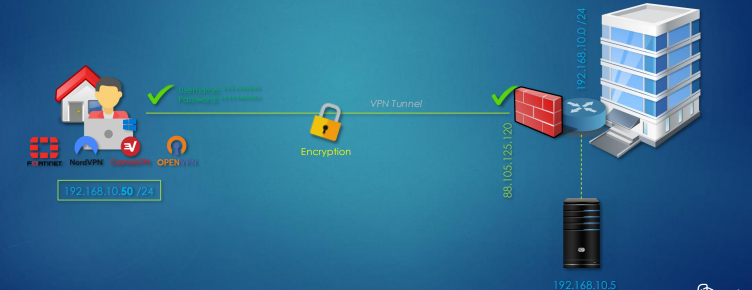
***VPN Kavramı ve türleri***

-VPN (Virtual Private Network), şifrelendirilmiş bir iletimle, private (özel) ağa bağlanma metodudur.

-İletim şifreleme sürecinde SHA, AES, 3DES, RSA gibi encryption metotları kullanılır.

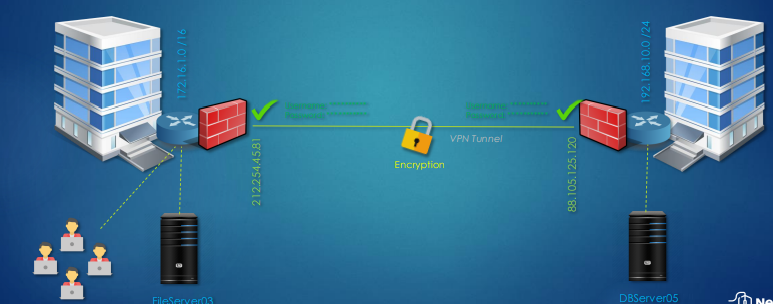
İki tip VPN türü vardır:

***1)Client-to-Site (C2S) VPN:***



- Kişilerin uygulamalar aracılığıyla belirli bir cihaza veya sunucuya bağlanarak şirket özel ağına katılmalarıdır.

***2) Site-to-Site (S2S) VPN:***



-Şirketlerin kendi aralarında cihaz veya sunucuya bağlanarak özel ağlarını paylaşmalarıdır.