SAKARYA ÜNİVERSİTESİ

SİBER GÜVENLİĞE GİRİŞ

AĞ MİMARİSİ CİHAZLARI VE AĞ TABANLI ÖNLEMLER

Prof. Dr. İbrahim ÖZÇELİK
Bilgisayar ve Bilişim Bilimleri Fakültesi

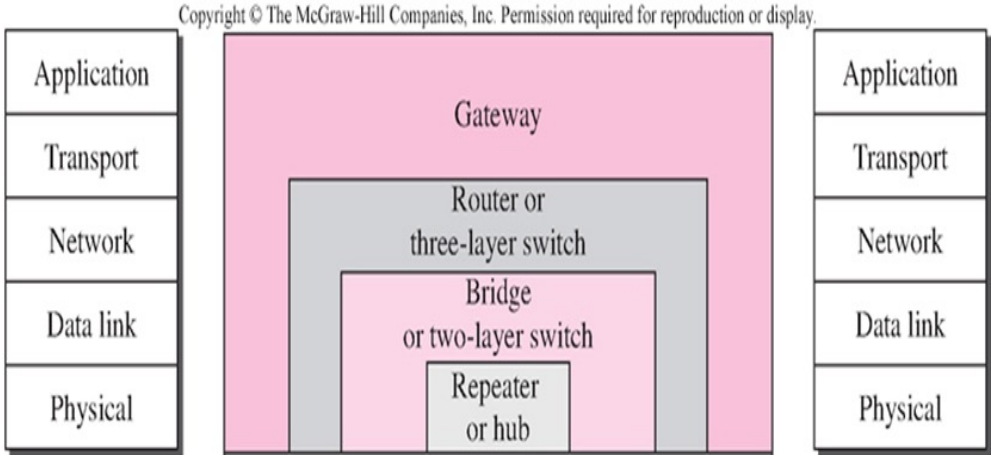
1

AĞ MİMARİSİ CİHAZLARI

- Tekrarlayıcı (Repeater)
- Hub
- Tap (Test Access Point)
- Köprü (Bridge)
- Anahtar (Switch)
- Yönlendirici (Router)
- Güvenlik Duvarı (Firewall)

2

Arabağlantı Cihazları



3

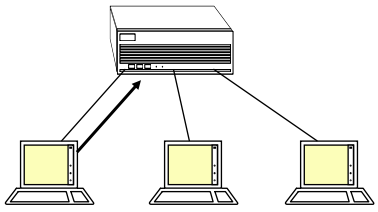
Tekrarlayıcı (Repeater) - Fiziksel Katman

- Veri, sinyal zayıflaması ve gürültü gibi etkenlerden dolayı ancak belirli mesafelere kadar uzaklığa gidebilir
- Bu ihtiyacı karşılamak için Tekrarlayıcı arabağlantı elemanı kullanılır
- Fiziksel segmenti iki katına çıkarmak için yada fiziksel segmentin izin verdiği istasyon sayısını artırmak gerektiğinde kullanılır
- Tekrarlayıcı, tekrar sinyal üretir ve verinin aktarımı ile ilgilenir, veri üzerinde bir yorumlama işlemi yapmaz
- Fiziksel katman birimi olarak çalışır
- Tekrarlayıcılar aynı ortam erişim protokolünü kullanan segmentleri birbirine bağlayabilirler (Ethernet-Ethernet, Token Ring-Token Ring, vb.)
- Tekrarlayıcılar, genelde Hub ve Kansantrator olarak isimlendirilen cihazlar olarak karşımıza çıkar – çok portlu tekrarlayıcı
- Dezavantajı:
  - Band genişliği problemi oluştururlar
  - Ağ trafiğini artırır

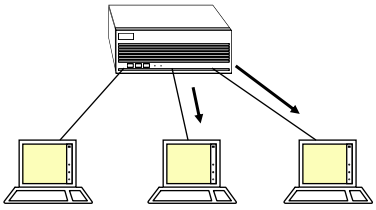
4

Hub (Çok Portlu Tekrarlayıcı) - Fiziksel Katman

- Bir portu üzerinden bir çerçeve alır ve aldığı çerçeveyi aldığı port haricindeki diğer tüm portlar üzerinden gönderir.
- Aldığı her şeyi tekrarladığı için çok portlu tekrarlayıcı olarak tanımlanır
- Çarpışma etki alanı (domain) azalmaz



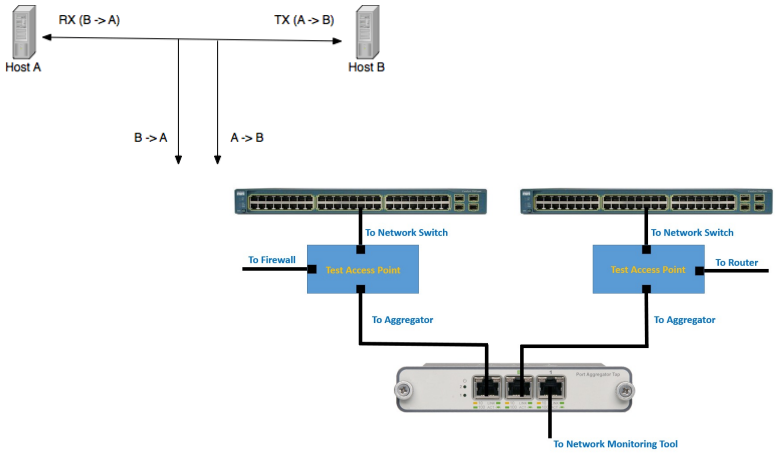
İstasyon Hub'a paket gönderiyor



Hub, gönderen hariç tüm istasyonlara yayınlıyor

5

TAP (Test Access Point) - Fiziksel Katman

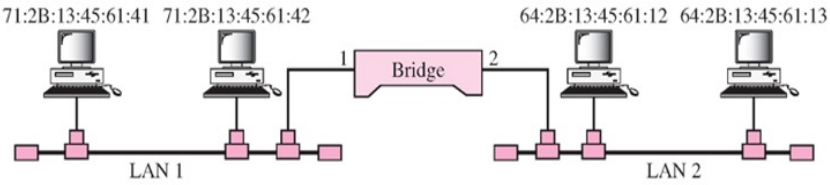


6

Köprü/Anahtar – Veri Bağı Katmanı

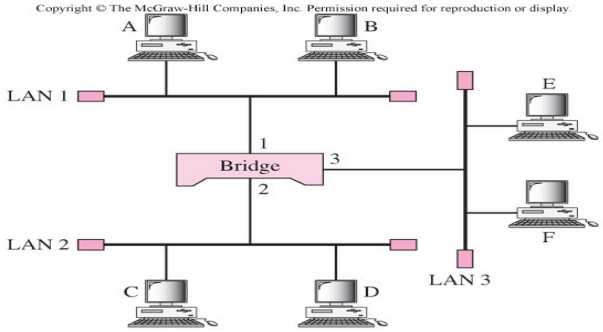
Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	1
64:2B:13:45:61:12	2
64:2B:13:45:61:13	2

Bridge Table



7

Köprü/Anahtar – Veri Bağı Katmanı



Address	Port

a. Original

Address	Port
A	1

b. After A sends a frame to D

Address	Port
A	1
E	3

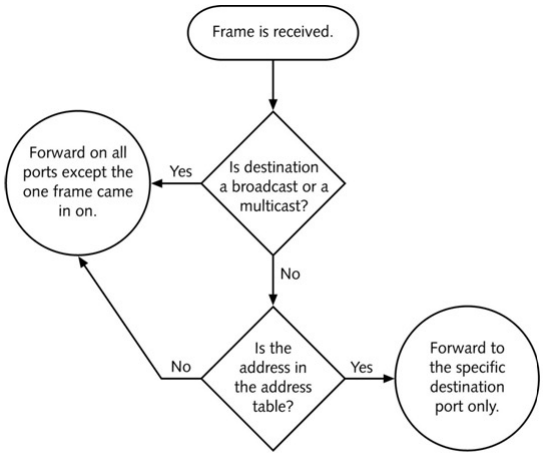
c. After E sends a frame to A

Address	Port
A	1
E	3
B	1

d. After B sends a frame to C

8

Anahtar Cihazında İletim (Forward)



Packet forwarding decisions made by a switch

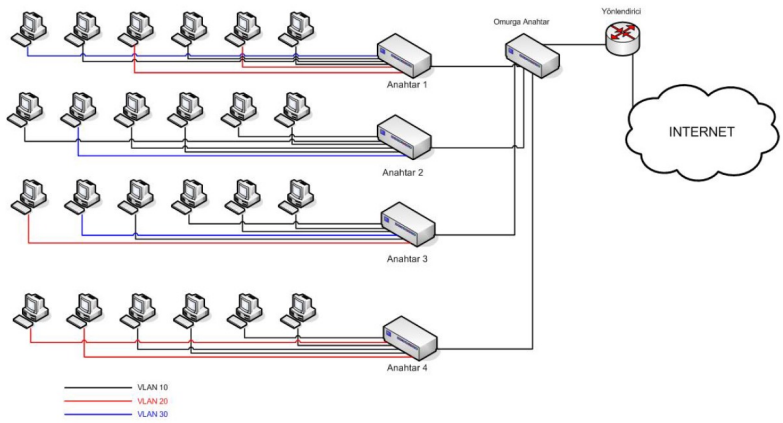
9

Anahtar Cihazı - VLAN

- VLAN sanal yerel alan ağı (Virtual Local Area Network) olarak bilinir.
- Fiziksel olarak aynı anahtarlama cihazına bağlı olmasına rağmen iki veya daha fazla ağın birbirinden yalıtımı için geliştirilmiş bir yapıdır.
- Farklı VLAN'larda bulunan ağlar birbirleri ile ancak bir yönlendirme ile haberleşebilirler.
- Anahtar ilk alındığında üzerinde VLAN1 bulunur ve anahtar üzerindeki tüm portlar bu VLAN'a üyedir.
- Güvenliğin artırılması için anahtar üzerinde kullanılan portlar başka bir VLAN oluşturularak onun üzerine alınmalıdır.

10

Anahtar Cihazı – VLAN Kullanımı



11

Anahtar Cihazı – Diğer Özellikler

- Kimlik doğrulama
  - cihaza yönetimsel veya denetimsel erişim
  - fiziksel erişim (konsol bağlantısı ile)
  - uzaktan erişim (telnet, web, ssl, ssh üzerinden, yönetim yazılımı veya snmp ile)
- Erişim Kontrolü
  - “Port Güvenliği”
  - “Erişim Kontrol Listeleri (ACL-Access Control List)”
- Olay Kayıtları
- Servis Güvenliği
- Yedekli Yapıda Kullanım

12

Veri İzlemede Kullanılan Cihazlar

- Hub kullanarak
- TAP kullanarak
- SPAN portu kullanarak
- Inline cihaz kullanarak

13

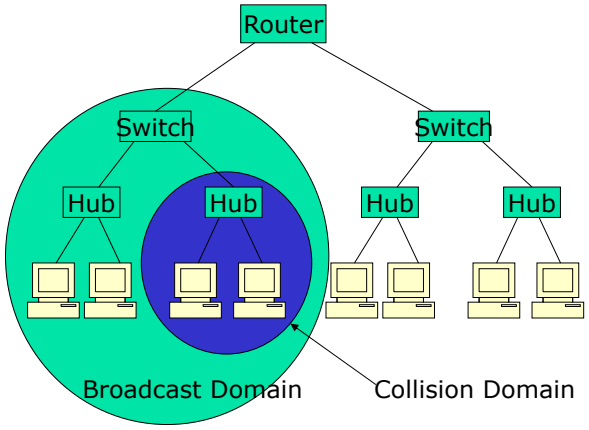
Yönlendirici

- Yönlendirici, iletişim altyapısı güvenliği mimarisinin en dışında bulunan varlıktır.
- Saldırıya uğrama olasılığı en fazla olan iletişim altyapısı güvenliği elemanıdır.
- Yönlendirici öncelikle kendini, daha sonra da ağ servislerini korumalıdır.
  - Kimlik Doğrulaması
  - Yetkilendirme Mekanizması
  - Erişim Kontrol Listeleri (erişimi sağlayacak bilgisayar, erişilecek bilgisayar, erişim sağlanacak servisler)
  - Olay Kayıtları
  - Yedekli Yapıda Kullanım

14

Trafik Etki Alanları

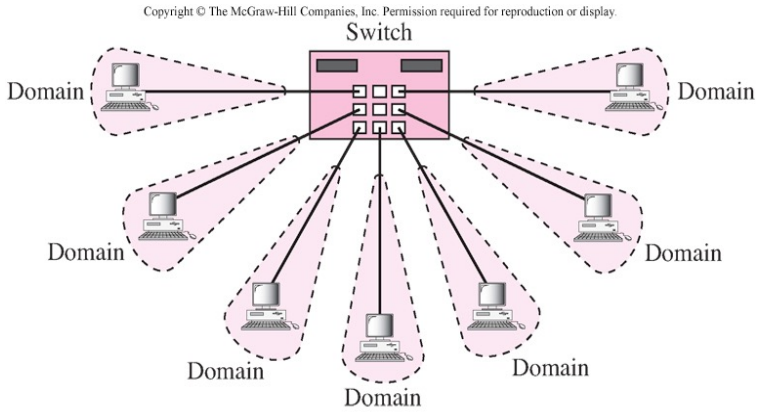
- Çarpışma etki alanlarını elimine etmek için Hub cihazının **kullanılmaması** gerekir
- Yayın çerçevelerinin önemli bir trafik olması durumunda, ağı yönlendiriciler kullanarak segmentlere ayırmak gerekir.



15

Anahtar Cihazında Çarpışma Etki Alanı

Anahtar cihazın her bir portu bir çarpışma etki alanına sahiptir



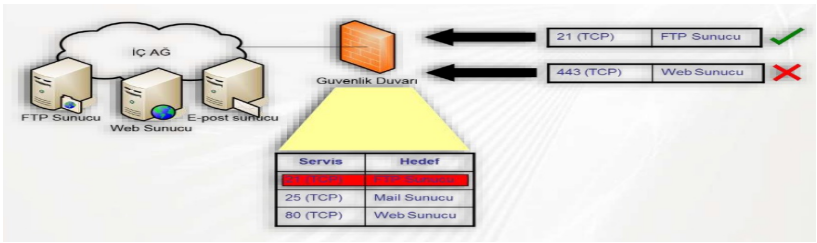
16

Güvenlik Duvarı

- Güvenlik duvarı ağ trafiğini kural tablosuna göre denetler.
- Güvenlik duvarının kural tablosu, önceden hazırlanmış bir erişim kontrolü politikası esas alınarak oluşturulmalıdır.
- Kural tablosunda sadece ihtiyaç duyulan ağ trafiğine izin verilmeli, bunun dışında kalan tüm ağ trafiğinin geçişi engellenmelidir.
- Kurla tablosunda aşağıdaki alanlar bulunur:
  - Kaynak IP: Erişimi başlatan bilgisayarın IP adresi (örneğin bir ftp istemcisi)
  - Hedef IP: Erişim sağlanacak bilgisayarın IP adresi (örneğin bir ftp sunucusu)
  - Servis: Erişim sağlanacak servis (örneğin ftp servisi)
  - Zaman: Erişim sağlanacak zaman aralığı (örneğin mesai saatleri)
  - Davranış: Söz konusu erişime izin verilip verilmeyeceği bilgisi (örneğin geçir veya düşür)
  - Kayıt: Söz konusu erişimle ilgili kayıt tutulup tutulmayacağı bilgisi (örneğin kayıt tut veya e-posta gönder)

17

Paket Filtreleme - Yorumlama



18

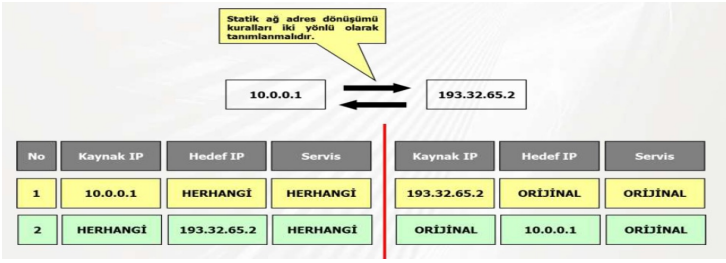
Ağ Adres Dönüşümü

- Özel IP adresleri, gerçek IP adreslerine dönüştürülür.
- Dış dünyadaki bilgisayarlar iç ağdaki bilgisayarların orijinal IP adreslerini bilemez.
- 3 farklı adres dönüşümü vardır:
  - Statik Ağ Adres Dönüşümü
  - Dinamik Ağ Adres Dönüşümü
  - Port Yönlendirme
- Güvenlik duvarı gelen ve giden ağ trafiği için öncelikle ağ adres çevrimi kurallarını uygulamakta, daha sonra kural tablosuna bakmaktadır.

19

Statik Ağ Adres Dönüşümü – Statik NAT

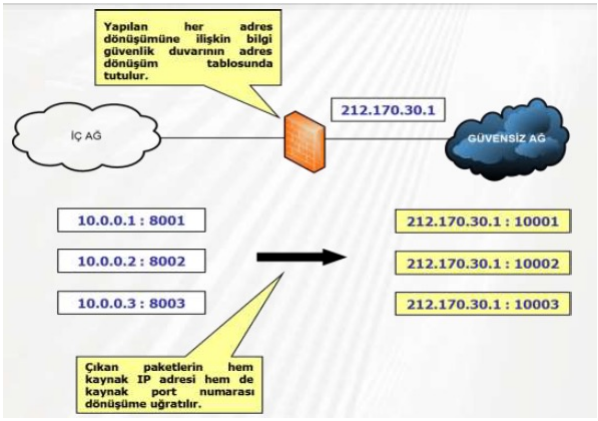
- Belirli sayıdaki bilgisayarlar için statik ağ adres çevriminin yapılması daha uygun olmaktadır.
- Statik ağ adres çevrimi iki yönlü olarak yapılmaktadır.
- Bazı durumlarda güvenlik açısından dış dünyanın iç ağa erişmemesi istenebilir. Bu durumda statik ağ adres çevrimi yerine dinamik ağ adres çevrimi kullanılmalıdır.



20

Dinamik Ağ Adres Dönüşümü – Dinamik NAT

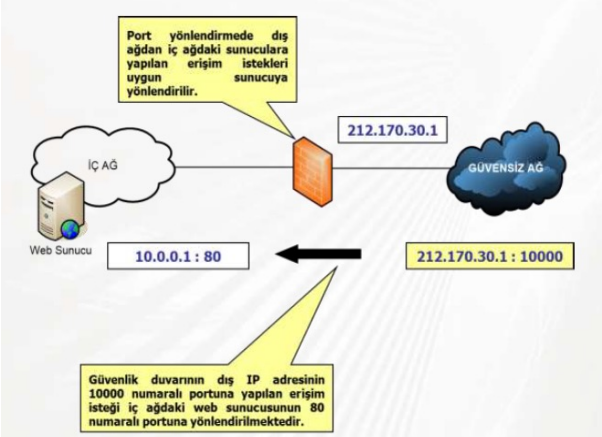
- İç ağdaki IP adresleri tek bir gerçek IP adresine dönüştürülmektedir.
- Tek yönlü olarak çalışmaktadır.
- Sadece iç ağdaki bilgisayarlar bağlantıyı başlatan taraf olabilir.
- İç ağdaki bilgisayarlar aynı IP adresi ile fakat farklı bir port numarası kullanarak dışarı çıkmaktadır.



21

Port Yönlendirme (PAT)

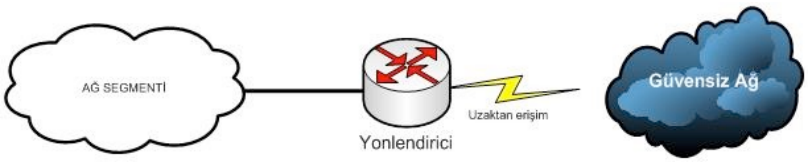
- Statik ağ adres çevriminin özelleşmiş bir halidir.
- Dış dünyadan iç ağdaki web, ftp, e-posta gibi sunuculara erişim sağlanması amacıyla kullanılır.



22

AĞ TABANLI ÖNLEMLER – Tek Yönlendirici

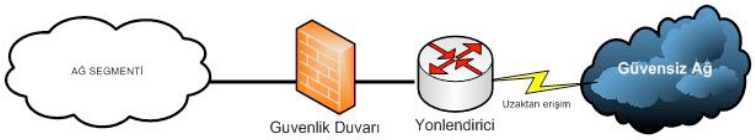
- Tek yönlendirici ile gerçeklenmiş ağ modeli – DMZ yok
- Yönlendiricide alınacak güvenlik önlemleri oldukça kısıtlıdır. Ağ erişim kuralları alınabilecek önlemlerden biridir. Fakat,
  - Performans kaybı
  - Sınır güvenliği yok, iç ağa yapılacak saldırılara karşı bir önlem bulunmamakta
  - Kayıt mekanizması bulunmamaktadır



23

Tek Güvenlik Duvarından Oluşan Mimari

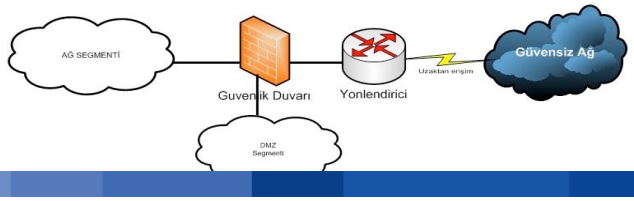
- DMZ yok
- Sunuculara erişim iç ağa erişim anlamına gelir
- Ağa erişim denetimi güvenlik duvarı tarafından sağlanır. Güvenlik duvarı ki ağ arayüzü arasındaki ağ trafiğinin akışını güvenlik ihtiyaçları doğrultusunda belirlenmiş olan güvenli ağ erişim kurallarına göre kontrol eder.
- Normal şartlarda bu tip mimari topolojilerde dış ağdan iç ağa olan erişimlere izin verilmemesi gerekmektedir.



24

Tek Güvenlik Duvarı ve Tek Dmz'den Oluşan Mimari

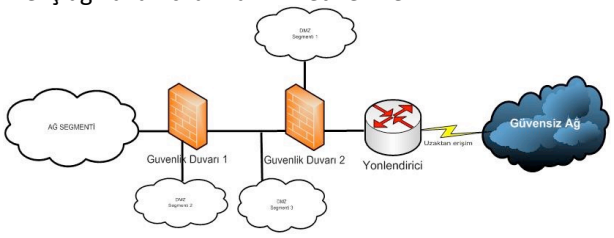
- İç ağ, ağ kullanıcıları ve bu kullanıcılara hizmet veren sunuculardan oluşmaktadır.
  - İç ağda bulunan sunucuların ve istemcilerin IP adresleri gerçek IP adresleri olmamalı, iç ağda kullanılan sanal IP adresleri olmalıdır.
- Dış ağ bölümü DMZ bölümündeki sunuculardan servis alan kullanıcıların ve kullanıcı bilgisayarlarının bulunduğu bölüm veya iç ağ ve DMZ bölümündeki sistemlerin servis aldığı bölümdür.
  - DMZ bölgesindeki sunucular için sanal IP adresleri kullanılmalıdır (10.0.0.0/24, 192.168.0.0/16, 172.16.0.0-172.31.255.255). Bu bölümde bulunan sunucular için statik adres dönüşümü kuralları uygulanmalıdır.
  - DMZ bölümünde bulunan tüm sunucular anahtarlama cihazlarına bağlanmalıdır. Anahtarlama cihazlarına bağlanan her bir sunumcunun MAC adresi anahtarın ilgili portuna kilitlenmelidir.



25

Birden Fazla Güvenlik Duvarından Oluşan Mimari

- Ağ erişimini sıkı bir şekilde denetlemek için iki güvenlik duvarı ardışık olarak kullanılır.
- Ardışık iki güvenlik duvarının bağlanması güvenliği arttırmanın yanında çok sayıda DMZ bölgesi oluşturma ve her birinde farklı güvenlik seviyesi elde etmeyi sağlamaktadır.
- Güvenlik Duvarı 2 üzerinde oluşturulan DMZ bölgelerinde genellikle dış ağ kullanıcılarına hizmet veren sunucular bulunur.
- Güvenlik Duvarı 1 ise iç ağ, iç ağ sunucuları, veritabanı ve DMZ bölümleri arasındaki mantıksal bilgi akışını yönetir ve genellikle iç ağ kullanıcılarına hizmet verirler.

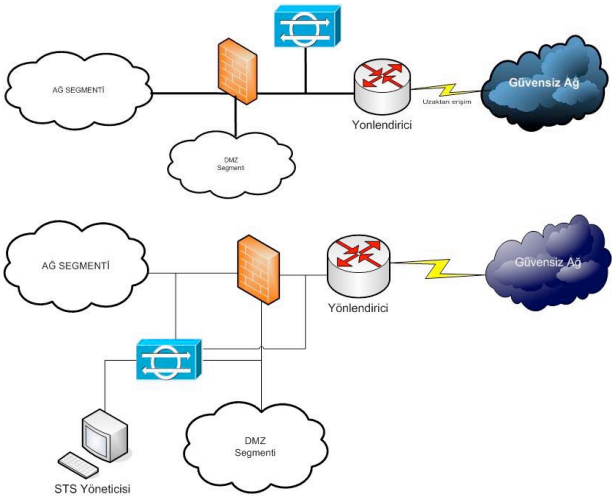


26

Saldırı Tespit Sistemi

Farklı şekillerde konumlandırılabilir.

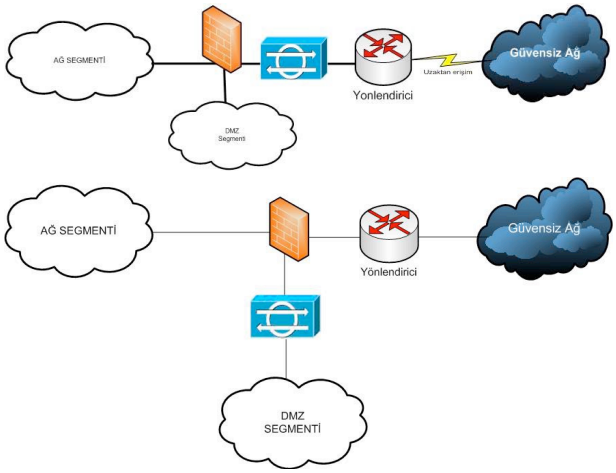
- Yönlendirici ve güvenlik duvarı arasında konumlandırma (Hub ya da anahtar- mirroring),
- Güvenlik duvarı ile iç ağ arasında konumladırma,
- Birden çok arayüzü dinleyecek şekilde konumlandırma olabilir.



27

Saldırı Engelleme Sistemi

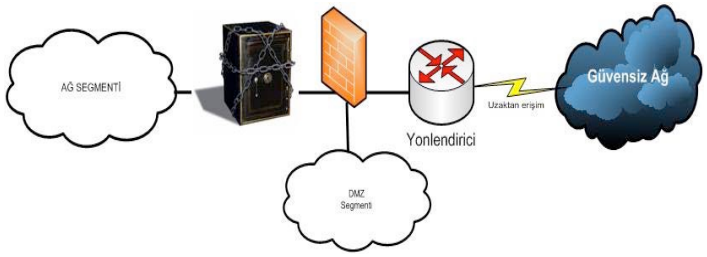
- Saldırı engelleme sistemleri köprü (*bridge*) modunda çalışır.
- Herhangi bir şekilde elektrik kesilmesi ya da arızalanması durumunda girişini ve çıkışını kısa devre ederek ağın iletişimini durdurmaz.



28

VPN Kullanımı

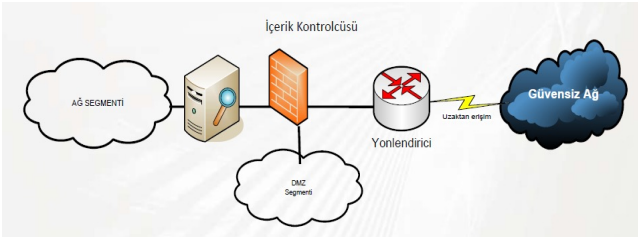
- VPN cihazları genellikle güvenlik duvarı ve iç ağ arasında yer alır.
- VPN cihazları veriler üzerinde güvenlik sağlamasına karşın kendisini TCP/IP saldırılarına karşı koruyamaz, bu yüzden de güvenlik duvarının arkasında konumlandırılır.
- DMZ segmenti ile güvensiz ağ arasında gerçekleşecek trafik VPN cihazı kontrolünde değildir.



29

İçerik Kontrolçüsü

- İçerik kontrolcüsü http, ftp, smtp ve pop3 protokoller üzerinden ağa gelen saldırıları, zararlı içerikleri, belli başlıkları, belli kelimeleri, vb. tespit ederek bu tür içeriklerin ağa girmesini engeller.
- Web sayfalarının içeriği kontrol edilerek, içerik kontrolcüsü ile kurum politikasına uymayan (finans siteleri, oyun ve kumar siteleri,) içerikte hizmet veren web sayfalarına erişim kısıtlanabilmektedir.
- Yapılandırmasına dikkat edilmelidir. Performans kayıpları oluşabilir



30

Kaynaklar

- Ağ Mimarisi Güvenliği Kılavuzu, Tübitak-UEKAE, Doküman Kodu: UEKAE BGT-2001