

Doküman Kodu: UEKAE BGT-2001

AĞ MİMARİSİ GÜVENLİĞİ KILAVUZU

SÜRÜM 1.00

29 ŞUBAT 2008

Hazırlayan: Fatih KOÇ

ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nün misyonu, "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaşılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı araştırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sağlanmaktadır.

Bu doküman "Ulusal Bilgi Sistemleri Güvenlik Projesi" kapsamında hazırlanmış olup ihtiyaç sahiplerini bilgi sistemleri güvenliği konusunda bilinçlendirmeyi hedeflemektedir. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

Bu dokümanda bahsi geçen belirli ticari marka isimleri kendi özgün sahiplerine aittir. Burada anlatılanlar tamamen tavsiye niteliğinde olup değişik ürünler/yapılandırmalar için farklılık gösterebilir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu değildir. Bu doküman UEKAE'nin izni olmadan değiştirilemez.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeđi geen Ađ Güvenliđi personeline ve dokümanı gözden geirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Mehmet KARA'ya ve Oktay ŞAHİN'e teşekkürü bor biliriz.

İÇİNDEKİLER

1. GİRİŞ.....	6
1.1 Amaç ve Kapsam.....	7
1.2 Hedeflenen Kitle.....	7
1.3 Kısaltmalar.....	7
1.4 , Dokümanda Kullanılan Semboller	9
2. GENEL AĞ MİMARİSİ ELEMANLARI	10
2.1 Anahtarlama Cihazı	10
2.1.1 VLAN	10
2.1.2 Anahtarlama Cihazlarında Kimlik Doğrulama	11
2.1.3 Anahtarlama Cihazlarında Erişim Kontrolü	11
2.1.4 Olay Kayıtları	12
2.1.5 Servis Güvenliği	12
2.1.6 Yedekli Yapıda Anahtarlama Cihazı Kullanımı	13
2.2 Yönlendiriciler.....	13
2.2.1 Yedekli Yapıda Yönlendirici Kullanımı	14
2.3 Güvenlik Duvarları	14
2.3.1 Yedekli/Kademeli Yapıda Güvenlik Duvarı Kullanımı	16
2.4 Saldırı Tespit Sistemleri	16
2.5 Saldırı Engelleme Sistemleri	17
2.6 VPN Cihazı (Virtual Private Network- Sanal Özel Ağ).....	18
2.7 İçerik Kontrolcülerini	19
2.8 Kablosuz Ağ Ürünleri.....	20
2.8.1 Erişim Noktaları (Access Point / Wireless Access Point)	21
2.9 Ağ Yönetim İzleme/Dinleme Ürünleri	22
2.10 Antivirüs Uygulamaları	23
2.11 Sunucu ve İstemciler	24
3. AĞ TASARIM PRENSİPLERİ	26

3.1 İhtiyaçların Belirlenmesi ve Amaca Yönelik Tasarım	26
3.2 Politikaların Belirlenmesi	26
3.2.1 Erişim Politikaları	26
3.2.2 Zamana Bağlı Kullanım Politikası	27
3.3 Büyüme Hızının Belirlenmesi	27
3.4 Maliyet Etkinlik Analizi	28
3.5 Çevrim Dışı Ağ Kullanımı	28
4. ÖRNEK AĞ MİMARİ MODELLERİ	29
4.1 Ağ Modellerinde Sanal Yerel Alan Ağ (VLAN) Kullanımı	29
4.2 Tek Yönlendirici ile Gerçeklenmiş Ağ Mimari Modeli	30
4.3 Tek Güvenlik Duvarı ile Gerçeklenmiş Ağ Mimari Modelleri	30
4.3.1 DMZ Olmaksızın Gerçeklenebilecek Ağ Mimari Modeli	30
4.3.2 İki veya Daha Fazla DMZ Bölgesine Ayrılmış Ağ Mimari Modeli	32
4.4 İki veya Daha Fazla Güvenlik Duvarı Kullanılarak Gerçeklenmiş Ağ Mimari Modeli.....	33
4.5 Saldırı Tespit Sistemlerinin Ağ Mimari Modellerinde Konumlandırılması.....	34
4.6 Saldırı Engelleme Sistemlerinin Ağ Mimari Modellerinde Konumlandırılması.....	36
4.7 Sanal Özel Ağ Cihazlarının Ağ Mimari Modellerinde Konumlandırılması.....	37
4.8 İçerik Kontrolcüsünün Ağ Mimari Modellerinde Konumlandırılması.....	38
4.9 Çok Sayıda Güvenlik Cihazı İçeren Bir Mimari Model.....	38

1. GİRİŞ

Günümüzde çok küçük işletmeler veya bilgisayar sistemleri dahi birçok saldırıya uğramaktadır. Maruz kalınan saldırıların kaynağı ve şekli incelendiğinde, zamana bağlı olarak saldırıların basitleştiği, başarılı saldırılar için kullanılan bilginin yaygınlığının arttığı gözlemlenmektedir. Birçok saldırı için ağ mimarisinde alınacak tedbirlerle başarılı saldırı sayısının düşürülebilmektedir. Bu sebeple birçok noktada ağın yapılandırmasında güvenlik, performansın da önüne geçmektedir. Özellikle dış dünyaya verilen hizmetlerde, elektronik ticarete, uzaktan eğitimde veya internet üzerinden kritik bilginin taşınmasında 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 yansımaktadır.

Bir bilgisayar ağı tasarlanırken dışarıya hizmet verecek servisler, dış dünyada kullanılacak servisler dikkatlice ele alınarak, bu servislerin güvenli çalışması için kullanılacak cihazlar ve bu cihazlar üzerinde alınacak önlemler belirlenmelidir. Dışarıya hizmet verecek servisler eğer mümkünse farklı güvenlik seviyesinde bir ağ segmentine konularak bunlara yapılan erişimler denetim altına alınmalıdır. Aynı şekilde iç ağa hizmet veren sunucular da mümkünse farklı güvenlik seviyesinde bir ağ segmentine taşınmalıdır. Eğer kaynaklar farklı segmentler kurulması için yeterli olmuyorsa ağ cihazları ve sunucular üzerinde gerekli güvenlik önlemleri alınarak risk seviyesi düşürülmeye çalışılmalıdır.

Ağa giren ve ağdan çıkan tüm trafiği izleyecek bir yapı oluşturulması olası saldırılarda veya bilgi ve kaynak kayıplarında sorunun kaynağının tespiti için büyük önem arz etmektedir. Herhangi bir kayıp olmaksızın dahi, düzenli kontrollerle sorun oluşmadan olası sorunun kaynağının tespiti ve gerekli önlemlerin alınması sağlanabilir (ör: ağda bulunan bir bilgisayarın amaçlanan hizmeti dışında bir portunun açık olduğunun tespiti).

1.1 Amaç ve Kapsam

Bu doküman, bir ağın tasarımı, iyileştirilmesi, genişletilmesi aşamalarında sistem ve güvenlik uzmanlarına rehberlik etmesi amacı ile hazırlanmıştır.

Bu dokümanda öncelikle ağ mimarisinde yaygın olarak kullanılan teknoloji ve bileşenlere değinilmiştir. Bu bileşenler özellikle güvenlik bakışı ile değerlendirilmiş ve detaylandırılmıştır. Üçüncü bölümde güvenli ağ tasarım prensipleri açıklanmış, dördüncü bölümde ise farklı amaçlar için gerçekleştirilebilecek ağ mimari modelleri örneklenmiştir.

1.2 Hedeflenen Kitle

Bu dokümandan ağ yöneticileri, ağ güvenlik yöneticileri, ağ tasarımcıları faydalanabilirler.

1.3 Kısaltmalar

AAA	: Authentication, Authorization, Accounting
ACL	: Access Control List
AES	: Advanced Encryption Standard
AH	: Authentication Header
BIOS	: Basic Input / Output System
CAST	: Bir blok şifreleme algoritması (block cipher), Kısaltma Carlisle Adams, Stafford Tavares in ilk harflerinden oluşmaktadır.
DES	: Data Encryption Standard
DHCP	: Dynamic Host Control Protocol
DMZ	: Demilitarized Zone / Demarcation Zone
DNS	: Domain Name Server
DoS	: Denial of Service
EAP-TLS	: Extensible Authentication Protocol -Transport Layer Security
ESP	: Encapsulating Security Payload
FTP	: File Transfer Protocol
GAŞ	: Geniş Alan Şebekesi

Gbps	: Giga bit per second
HTTP	: Hypertext Transfer Protocol
ICMP	: Internet Control Message Protocol
IDEA	: International Data Encryption Algorithm
IDS	: Intrusion Detection System
IEEE	: Institute of Electrical and Electronics Engineers
IKE	: Internet Key Exchange
IPS	: Intrusion Prevention System
IPSec	: Internet Prtocol Security
ISDN	: Integrated Services for Digital Networks
L2TP	: Layer 2 Tunneling Protocol
MAC	: Media Access Control
Mbps	: Mega bit per second
NTP	: Network Time Protocol
OSI	: Open System Interconnection
PEAP	: Protected Extensible Authentication Protocol
POP3	: Post Office Protocol 3
PPTP	: Point to Point Tunneling Protocol
RADIUS	: Remote Authentication Dial In User Service
SHA-1	: Secure Hash Algorithm 1
SMTP	: Sent Mail Transfer Protocol
SNMP	: Simple Network Management Protocol
SSH	: Secure Shell
SSL	: Secure Socket Layer
TCP	: Transport Control Protocol
TFTP	: Trivial File Transfer Protocol

TKIP	: Temporal Key Integrity Protocol
UDP	: User Datagram Protocol
UEKAE	: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
VLAN	: Virtual Local Area Network
WEP	: Wired Equivalent Privacy
WLAN	: Wireless Local Area Network
WMAN	: Wireless Metropolitan Area Network
WPA	: Wireless Protected Access
WPAN	: Wireless Personal Area Network
WPA-PSK	: Wireless Protected Access-PreShared Key

1.4 Dokümanda Kullanılan Semboller

Sembol	Açıklaması
koyu	İngilizce terimleri belirtmek içindir.
komut	Kod parçalarını ve betikleri belirtmek içindir.
<u>Koyu altı çizgili</u>	Vurgu yapmak içindir.

2. GENEL AĞ MİMARİSİ ELEMANLARI

2.1 Anahtarlama Cihazı

Anahtarlama cihazları, yerel alan ağlarında temel iletişimi sağlayan cihazlardır. Geleneksel anahtarlama cihazı tanımında OSI (Open System Interconnection) referans modelinde ikinci (veri iletim katmanı) katmanda çalışırlar. Günümüzde ikinci, üçüncü, dördüncü hatta uygulama katmanı olan yedinci katmana kadar çalışan anahtarlama cihazları mevcuttur.

Anahtarlama cihazları 10 Mbps-10 Gbps aralığında bir ara yüze sahip olabilirler. Günümüzde anahtarlama cihazları 10/100/1000 Mbps olanlar yaygın olarak kullanılmaktadır. 1000 Mbps ve 10 Gbps olanlar genellikle omurga bağlantılarında kullanılırlar. Bu arayüzlerden 1 Gbps'e kadar olanlar hem bakır hem fiber, 10 Gbps olanlar ise fiber olabilir. Bakır veya fiber olmasını etkileyen unsurlar; anahtarlama cihazları arası mesafe, ortam gürültüsü ve güvenlidir. Uzak mesafelere gidilmek istendiğinde fiber bağlantı zorunlu hale gelir. Bakır kabloya fiziksel müdahale edilerek üzerinden geçen trafiğin dinlenebilmesi fiber kabloya müdahale edilerek trafiğin dinlenmesinden daha kolaydır. Böyle bir olayın tespiti de çok daha zordur.

Ağın tamamı tek bir merkezden yönetilmek istendiğinde modüler anahtarlar alınarak istenilen sayıda kullanıcı desteklenebilir. Bu yapı izlenebilirlik, güvenlik, ölçeklenebilirlik ve yedeklilik sağlar.

Anahtarlama cihazları birçok güvenlik mekanizmasını da bünyesinde barındırmaktadır. Bunlardan en çok kullanılanlar: VLAN, kimlik doğrulama, port güvenliği, olay kayıtları, servis güvenliği, port yönlendirme, bazı servislere erişim denetimi ve güvenli yönetimidir.

2.1.1 VLAN

VLAN sanal yerel alan ağı (Virtual Local Area Network) olarak bilinir. İsminden de anlaşılacağı üzere 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. Sisteme yeni bir anahtarlama cihazı bağlandığı takdirde varsayılan VLAN da (VLAN1) çalışacaktır. Sistemde VLAN1 de çalışan bilgisayarlara erişimi mümkün olacaktır. Güvenliği artırılması için anahtar üzerinde kullanılan portlar başka bir VLAN yaratılarak onun üzerine alınmalıdır.

2.1.2 Anahtarlama Cihazlarında Kimlik Doğrulama

Bilgi sistemlerinde kimlik doğrulama, iddia edilen kimliĐin geçerli olup olmadıĐının doğrulanması veya test edilmesidir [3]. Anahtarlama cihazında kimlik doğrulama; cihaza yönetimsel veya denetimsel erişim söz konusu olduĐu zaman kişinin doğru kişi olup olmadıĐının kontrolüdür.

Anahtarlama cihazına yönetimsel bir bağlantı kurulmak istendiĐinde yönetim için parola ile bir yönetici kimlik doğrulaması gerçekleştirilir. Yönetim, cihaza fiziksel erişim ile (konsol bağlantısı ile) yapılabildiĐi gibi uzaktan da (telnet, web, ssl, ssh üzerinden, yönetim yazılımı veya snmp ile) yapılabilir. Bu noktada yönetimin nasıl gerçekleştirileceĐini kurum politikası belirler. Yani politika gereĐi uzaktan yönetim, yapılandırma ile engellenmiş olabilir. Tüm durumlarda yönetim için bir kimlik doğrulama işlemi gerçekleştirilmelidir. Yönetim parolaları cihaz üzerinde açık olarak saklanmamalı özet bilgileri saklanmalıdır (anahtarlama cihazı böyle bir özelliĐi destekliyorsa).

2.1.3 Anahtarlama Cihazlarında Erişim Kontrolü

Anahtarlama cihazı üzerine bağlanmış aĐ elemanlarının gerek aĐa gerekse anahtarlama cihazına erişimi denetlenebilir. Bunun için “Port GüvenliĐi” veya “Erişim Kontrol Listeleri (ACL-Access Control List)” kullanılmalıdır.

Erişim Kontrol Listeleri, bilgi teknolojilerinde belli kaynakların kullanımının yetkili kişilerle sınırlandırılması amacıyla kullanılan bir teknolojidir. Anahtarlama cihazlarında da belirlenen bir kaynak adresin bir hedef adrese erişimini kontrol etmek amacıyla erişim kontrol listeleri kullanılmaktadır.

Basit ve genişletilmiş olmak üzere iki tipte Erişim Kontrol Listesi mevcuttur. Basit Erişim Kontrol Listesinde sadece kaynak adres kullanılırken, genişletilmiş Erişim Kontrol Listesinde hem kaynak hem hedef adres kullanılmakta ayrıca protokol tipi (tcp, udp, icmp) ve port bilgisi hususunda kısıtlamalar yapılabilmektedir.

802.1x, IEEE (Institute of Electrical and Electronics Engineers) port tabanlı ağ erişim standardıdır. Bu standartta üç unsur vardır, istemci (supplicant), doğrulayıcı (authenticator) ve doğrulama sunucusu (Authentication Server/RADIUS- Remote Authentication Dial In User Service). Doğrulayıcının görevi bir portu için 802.1x uygulanacaksa o portta bir erişim isteği sezince istemciden alacağı paketi sunucuya iletmek, sunucudan gelecek cevap doğrultusunda erişime izin vermek veya erişimi engellemek olacaktır. Bu yapıda anahtarlama cihazının rolü doğrulayıcıdır (authenticator).

Anahtarlama cihazının marka ve modeline göre değişmekle birlikte, genel olarak; ağ cihazlarının fiziksel adresleri (MAC-Media Access Control) temel alınarak anahtarlama cihazının bir portundan paketin geçmesine izin verilir veya verilmez. Anahtarlama cihazının bir portunda “MAC kilitleme”(MAC Locking) ile sadece istenilen MAC adreslerine sahip cihazlarının erişimine müsaade edilebilir.

2.1.4 Olay Kayıtları

İzlenebilirliğin temel taşı olan olay kayıtları, anahtarlama cihazı tarafından oluşturulan, gerek kendi üzerinde kaydedilen gerekse başka bir noktaya gönderilen önceden tanımlı olayların meydana gelmesi durumunda oluşturulan verilerdir. Olay kaydı tutan veya gönderen bir anahtarlama cihaz için geçmişe yönelik izlenebilirlik söz konusudur.

Burada kritik olan nokta cihaz kayıt kapasitesidir, uygulamada genellikle anahtarlama cihazının olay kayıtlarını başka bir cihaza (bir kayıt sunucusu gibi) göndermesi beklenir. Olay kayıtlarının başka bir kayıt sunucusunda tutulması cihazın bir şekilde deve dışı kalması, ele geçirilmesi ya da kilitlenmesi durumunda sonradan olayların izlenebilmesini sağlamaktır.

İzlenebilirliğin sağlıklı ve tutarlı bir şekilde sağlanabilmesi için cihaz saatinin doğru olması beklenir. Bazı cihazlarda tarih/saat bilgisi cihaz üzerinde tanımlı saat aracılığı ile yapılırken bazı cihazlar da ise NTP (Network Time Protocol) ile tarih saat bilgisi merkezi bir sunucudan alınır. Bu da sistemdeki tüm cihazların saat bilgilerinin aynı olmasını ve onlardan gelen kayıtların doğru bir şekilde değerlendirilmesini sağlar.

2.1.5 Servis Güvenliği

Anahtarlama cihazı üzerinde kullanılmayan servislerin kapatılması gereklidir. Saldırgan açısından güvenli konfigüre edilmemiş bir servis açık bir kapı olabilir. Örneğin: yönetim için web tabanlı bir arayüz kullanılmayacaksa anahtarlama cihazında bu servis (http servisi) kapatılmalıdır. Var olan ağda disksiz iş istasyonları kullanılmıyorsa veya DHCP aktarımı

(DHCP relay) söz konusu değilse bootp servisi de kapatılmalıdır. Anahtarlama cihazı tarih saat bilgisi elle girilmiş ve başka kişiler ve cihazlar tarafından değiştirilmemesi isteniyorsa NTP servisi de kapatılmalıdır. Anahtarlama cihazı üzerinden etki alanı isim servisi (DNS-Domain Name Service) verilmeyecekse bu servis de kapatılmalıdır. Genel kural olarak şu düşünülebilir; kullanılmayan servis kontrol dışıdır, yönetimde gözden kaçabilir, bu sebeple kullanılmayan servisler kapatılmalıdır. Bir servis kullanılıyorsa güvenliği sağlanmalı (http yerine https, telnet yerine SSH kullanımı gibi), güvenliği sağlanamıyorsa (kullanılan cihazın desteklemediği durumlarla karşılaşılabılır) bu eksikliğin farkındalığı sağlanmalıdır.

2.1.6 Yedekli Yapıda Anahtarlama Cihazı Kullanımı

Gerek performans gerekse güvenlik açısından anahtarlama cihazları yedekli yapıda çalışabilmektedir. En temel anlamda anahtarlama cihazları Aktif-Aktif (aynı anda her iki anahtarlama cihazının çalışması, yükün paylaşımı) veya Aktif-Pasif (aynı anda sadece bir anahtarlama cihazının çalışması diğerinin beklemede kaldığı çalışma şekli) olarak çalışırlar. Burada anahtarlama cihazının yedekli yapıda çalışması erişebilirlik/kullanılabilirlik anlamında bir güvenlik önlemi olarak değerlendirilmelidir. Hem Aktif-Aktif hem de Aktif-Pasif çalışma şeklinde bir cihaz çalışmaz hale gelmesi durumunda çalışır durumdaki cihaz tüm trafik yükünü kendi üzerine alır.

2.2 Yönlendiriciler

Yönlendirici, iletişim altyapısı güvenliği mimarisinin en dışında bulunan varlıktır. Bu yüzden saldırıya uğrama olasılığı en fazla olan iletişim altyapısı güvenliği elemanıdır. Yönlendirici öncelikle kendini, daha sonra da ağ servislerini korumalıdır. Bir yönlendirici üzerinde aşağıdaki güvenlik önlemleri alınmalıdır.

Kimlik doğrulaması yönlendiriciye yapılan erişimleri kontrol altına almayı amaçlamaktadır. Bu mekanizma ile sadece yetkili kişiler yönlendiriciye erişebilirler.

Yönlendiricilerin üzerinde yetkilendirme mekanizması bulunmaktadır. Genellikle birden çok kullanıcı profili tanımlanarak bunların her birine değişik yetkiler verilebilir. Bu kullanıcılara üçüncü parti bir AAA sunucu üzerinde de yetkilendirme yapılabilir. Erişim kontrolü yönlendiriciye ya da ağa yapılan erişimlerin filtrelenerek kontrol altına alınmasını sağlamaktadır. Erişim kontrol listeleri ile yönlendirici üzerindeki servislere yapılan erişimler de kontrol altına alınabilir. Bu da yönlendiricinin sadece önceden belirlenmiş kişiler tarafından yönetilmesini sağlar.

Yönlendiriciler uzaktan yönetim servislerini desteklemektedir. Telnet, SSH, SNMP gibi yönetim ve uzaktan erişim mekanizmaları ile yönlendiriciye erişilerek yönetim işlemleri yapılmaktadır. Bu yönetimlerde erişim kontrol listeleri ya da AAA sunumcularla güvenlik sağlanmaktadır. Yönlendiriciler kendi üzerinde çalışan telnet, HTTP, DNS, TFTP, finger vb... servisleri de kontrol edebilirler.

Yönlendiriciler, üzerindeki önemli olayların kayıtlarını kendi üzerlerinde ya da sistemde bulunan bir kayıt sunucuda tutabilir. Bu güvenlik mekanizması ile yönlendirici üzerinde meydana gelen önemli olayların nedenleri ve kim tarafından yapıldığı tespit edilebilir.

Yönlendiriciler temel güvenlik kontrolleri dışında üzerlerine ilave edilen yazılımlarla güvenlik duvarı ya da saldırı tespit sistemi gibi gelişmiş güvenlik özelliklerini de kendi bünyelerinde barındırabilirler. Bu ek güvenlik özellikleri yönlendiriciye sınırlı güvenlik özellikleri kazandırmakla birlikte performansın önemli oranda düşmesine sebep olmaktadır.

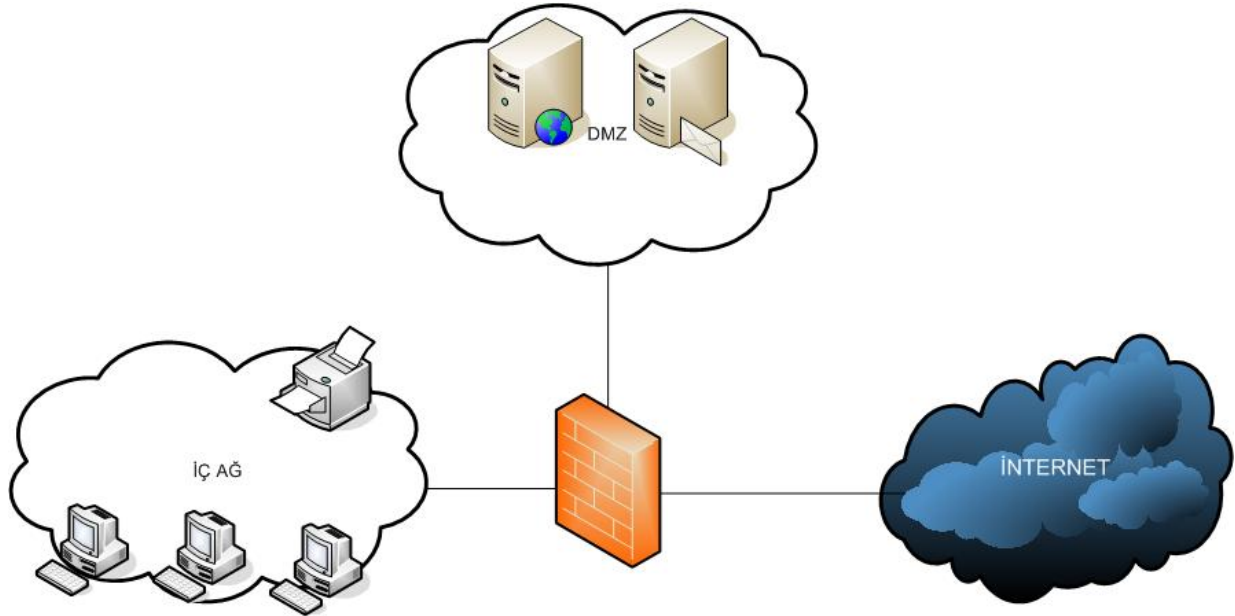
Yönlendirici güvenliği ile ilgili daha detaylı bilgi için UEKAE BGT-2003 Yönlendirici Güvenliği Kılavuzu Dokümanı incelenebilir.

2.2.1 Yedekli Yapıda Yönlendirici Kullanımı

Anahtarlama cihazlarında olduğu gibi yönlendiricilerde de yedekli yapı söz konusudur, özellikle servis kesintisinin çok kritik olarak değerlendirildiği sistemlerde farklı servis sağlayıcılardan kimi zaman farklı teknolojiler kullanılarak (ISDN, Frame Relay, Kablosuz iletişim) dış dünyaya bağlantı kesinti riski minimize edilebilir. Gerçek anlamda yedeklilik için üçüncü parti donanım ve yazılımlar gereklidir. Bunun yanında yük paylaşımı manüel olarak farklı yönlendiricilere verilebilir ve olası bir kesinti durumunda yine manüel olarak aktif olan yönlendirici kullanılacak şekilde yapılandırma yapılabilir.

2.3 Güvenlik Duvarları

Güvenlik duvarının temel görevi ağ trafiğini kontrol altına almaktır. Bu noktada bazı tanımlamalar yapmakta fayda var. Basit anlamda aşağıdaki şekil iç ağ, DMZ (Demilitarized Zone / Demarcation Zone) ağı ve dış ağ kavramlarını özetlemektedir.



Şekil 2-1 Basit anlamda iç ağ, DMZ ve dış ağ gösterimi

İç ağ diğer bir deyişle güvenli ağ, güvenliği sağlanması gereken, dışarıya (internete veya dış intranete) bir servis sunmayı hedeflemeyen cihazların bulunduğu ağdır.

DMZ ağı veya yarı güvenli ağ, gerek iç ağa gerekse dış dünyaya servis vermesi hedeflenen sunucuların konumlandırıldığı, güvenlik önlemleri iç ağa nazaran daha az olan bölgedir. Genellikle bu bölgede web sunucusu, uygulama sunucusu, e-posta sunucusu gibi sunucular konumlandırılır.

Dış ağ veya güvensiz ağ, tamamen kontrolsüz bölge olarak tanımlanabilir, genellikle internet veya sistem yöneticisi kontrolünde olmayan ağ segmenti olarak karşımıza çıkar.

Bu çerçevede güvenlik duvarı, iç ağdan dış ağa giden ya da dış ağdan iç ağa gelen trafiği kontrol ederek istenmeyen paketlerin ağa girmesini ve ağdan çıkmasını engeller. Ağ üzerinde ve kendi üzerinde çalışan servisleri kontrol eder. Güvenlik duvarına takılmış olan Ethernet kartları üzerinde farklı güvenlik özelliklerini etkinleştirerek farklı güvenlik seviyesine sahip ağlar oluşturur. Ağda bulunan cihazlar ve kendisinin yönetimi için gerekli erişim kontrolünü sağlayarak ağın güvenli bir şekilde erişim ve yönetimini sağlar. Kural tablosu ve servislere ilişkin önemli olayların kayıtlarını kendi üzerinde ya da kayıt sunucuda tutarak ağa ait önemli olayların sonradan incelenebilmesini sağlar. Ayrıca birçok ağ tabanlı saldırıyı engellerler, örneğin: bozuk paket saldırıları, sıfır boyutlu paket saldırıları, standart dışı uzunluktaki paketlerle yapılabilecek servis sonlandırma saldırıları güvenlik duvarında engellenebilir.

Güvenlik duvarı güvenliği ile ilgili daha detaylı bilgi için UEKAE BGT-2002 Güvenlik Duvarı Güvenliği Kılavuzu Dokümanı incelenebilir.

2.3.1 Yedekli/Kademeli Yapıda Güvenlik Duvarı Kullanımı

Güvenlik duvarlarındaki yedeklilik sürekliliği sağlamak ve performansı arttırmak için kullanılır. Aktif-Aktif ve Aktif-Pasif olmak üzere iki tür yedeklilik söz konusudur. Aktif-Aktif çalışmada güvenlik duvarlarının her ikisi de aynı anda aktif olurlar ve ağdaki trafiği paylaşarak hem performansı artırırılar hem de sürekliliği sağlarlar. Aktif-Pasif yapılandırmada ise güvenlik duvarlarından biri çalışırken diğeri beklemede kalmaktadır. Beklemede kalan güvenlik duvarı çalışan güvenlik duvarında sürekli olarak durum tablolarını ve geçerli oturum bilgilerini almaktadır. Çalışan güvenlik duvarında olası arayüz sorunları veya servisinin sonlanması durumunda beklemede bulunan güvenlik duvarı yükü üzerine alarak servis vermeye devam edecektir. Bu durumda herhangi bir oturum kaybı olmaması beklenir. Aktif-Pasif yapı daha çok sürekliliği sağlamak için kullanılır.

Güvenlik ve güvenilirliği artırıcı önlem olarak birden fazla güvenlik duvarı art arda (kademeli olarak) bağlamak daha iyi bir yöntem olarak değerlendirilmektedir. Art arda bağlanan güvenlik duvarlarının farklı marka ve modellerde olması tavsiye edilmektedir. Her bir üründe o ürüne özgü olası açıklığın/zayıflığın diğerk güvenlik duvarında bulunması ihtimali düşük olan ürünler seçilmesinde fayda vardır. Örneğin işletim sistemi farklı olan iki güvenlik duvarları tercihi işletim sistemine bağlı doğabilecek zayıflıklar açısından kademeli bir mimariye artı bir güç kazandıracaktır.

2.4 Saldırı Tespit Sistemleri

Saldırı tespit sistemlerinin temel amacı ağa yapılan saldırıları tespit edip kayıt altına almak ve sistem yöneticisine gerekli uyarılarda bulunarak saldırıya karşı zamanında gerekli önlemlerin alınmasını ve ağda meydana gelen olayların geriye doğru izinin sürülmesini sağlamaktır.. Bu uyarma mekanizması olay kayıtları tutma, e-posta gönderme, çağrı bırakma, belli programları çalıştırma veya diğerk şekillerde olabilir. Saldırı tespit sistemleri en çok ağ tabanlı ve sunucu tabanlı olarak karşımıza çıkmaktadır.

Ağ tabanlı saldırı tespit sistemleri ağa giren veya ağdan çıkan trafiği dinleyerek bir saldırı veya sızma olup olmadığını tespit eder. Ağa bir hub, anahtarlama cihazı (port mirroring yapılandırması gereklidir) veya ağ “tap” cihazı ile bağlanabilirler. Ağda en iyi konumlandırılacağı yer ağa ait tüm trafiğin geçtiği yönlendirici ve güvenlik duvarının arasındır. Böyle bir konumlandırılmayla ağa giren ve ağdan çıkan tüm trafik taranabilecektir. Genellikle bu cihazların bir IP adresi yoktur veya bu şekilde yapılandırılması tavsiye edilir. Bu sayede saldırılara hedef olma riski azalacaktır.

Sunucu tabanlı saldırı tespit sistemleri ise ilgili sunucu üzerinde sitsem çağrılarını, uygulama kayıtlarını (log dosyaları), dosya sistem değişiklikleri ile saldırıları tespit edebilirler. Bu tipteki saldırı tespit sistemleri genellikle sunucu üzerine kurulu bir ajan yazılımı ile gerçekleştirilmektedir.

Saldırı tespit sistemleri sadece kendi veri tabanlarında kayıtlı olan davranışları saldırı olarak değerlendirebilirler. Bir saldırı tespit sisteminin veri tabanının güncel olmaması yeni saldırıları tespit edememesi anlamına gelecektir. Mümkünse çevrim içi olarak saldırı imzalarının güncel tutulması değilse saldırı imzalarının sıklıkla kontrol edilip elle güncellenmesi gereklidir. Güvenlik forumları, üretici firma e-posta listeleri yeni saldırılardan ve saldırı imzalarından haberdar olmak için en iyi yöntemlerdendir.

2.5 Saldırı Engelleme Sistemleri

Gelişen teknoloji ile saldırıları tespit sistemlerinin saldırıyı veya sızmayı tespit etme yetenekleri ve güvenlik duvarlarının gerçek zamanlı erişim kontrol yetenekleri birleştirildi ve 1990'ların sonlarında uygulama seviyesinde saldırı tespit ve bu saldırıyı önleme kapasitesinde ürünler üretilmeye başlandı.

Çalışma mantığı bu iki teknolojinin birleşimi şeklindedir. Şöyle ki; saldırı veri tabanında bulunan imzalar yardımı ile tespit edilir, akabinde güvenlik politikasına bağlı olarak oturum sonlandırılabilir, ilgili paket düşürülebilir veya herhangi bir engelleme yapmaksızın haberleşmeye izin verilebilir. Saldırı tespit sistemleri pasif, saldırı engelleme sistemleri ise aktif koruma sağlarlar.

Saldırı Engelleme Sisteminin ağda konumlandırıldığı yerin tayini önem arz etmektedir. Saldırı engelleme sistemleri istenilen amaca göre ağda konumlandırılmalıdırlar. Yönlendirici ile güvenlik duvarı arasına konumlandırılacak bir saldırı engelleme sistemi Güvenlik Duvarının maruz kaldığı ve Güvenlik Duvarının engelleyebildiği saldırıları da (saldırıların veritabanında var olduğu varsayılmıştır) engelleyecektir. Bu noktada Saldırı Engelleme Sistemi ve Güvenlik Duvarı performansı karşılaştırılmalıdır. Aynı saldırıyı her iki cihazda engelleyebiliyorsa ve ağın performansı iyileştirilmek amacıyla hızlı çalışan cihaz daha dışa konumlandırılmalıdır.

2.6 VPN Cihazı (Virtual Private Network- Sanal Özel Ağ)

VPN cihazları güvensiz ağlar üzerinde güvenli olarak haberleşmek için kullanılır. Bu çerçevede VPN cihazları veriler üzerinde gizlilik, bütünlük, kimlik doğrulama ve inkar edememe güvenlik hizmetlerini sağlar. Bu işlemlerde IPSec (Internet Protocol Security), PPTP (Point-to-Point Tunneling Protocol), L2TP(Layer 2 Tunneling Protocol) gibi güvenlik protokollerini kullanır. Şifreleme için DES, 3DES, IDEA, CAST-128, Blowfish, AES gibi algoritmaları, bütünlük kontrolü için de MD-5, SHA-1 gibi özetleme algoritmalarını kullanır. VPN cihazları hem yazılım hem de donanım tabanlı olabilir.

VPN cihazlarında PPTP, L2TP veya IPSec protokolleri kullanılmaktadır. VPN cihazları çoğunlukla IPSec protokol ailesini kullanır [4]. IPSec, Intranet/Internet üzerinde güvenli haberleşmeyi sağlamak için IETF (Internet Engineering Task Force) tarafından geliştirilmiş bir ağ güvenliği standardıdır.

IPSec protokolü tünel mod ve transport mod olmak üzere iki farklı modda çalışabilmektedir. Her iki modun da kendine ait özellikleri ve avantajları bulunmaktadır. Tünel modda hem IP başlığı hem de veri kısmı şifrelenir. Şifreli paketin kaynak ve hedef adresi, tünel başlangıç ve bitiş noktaları olarak verilir. Genellikle VPN cihazından VPN cihazına gerçekleştirilen iletişimlerde kullanılır.

Transport modda ise sadece paketin veri kısmı şifrelenir. Orijinal paketin kaynak ve hedef adresleri korunur. Genellikle istemci ile VPN arasında gerçekleştirilen iletişimlerde kullanılır ve tünel moda göre paket işleme daha hızlıdır.

IPSec protokol ailesinde AH (Authentication Header), ESP (Encapsulation Security Payload) ve IKE (Internet Key Exchange) protokolleri kullanılır.

AH: Kimlik doğrulama, bütünlük kontrolü, inkâr edememe ve tekrarlama ataklarını önleme işlemlerini sağlar. Ancak, gizliliği yerine getirememektedir. AH protokolü, ESP protokolü tarafından desteklenmeyen IP başlığını doğrulama işlemini de yerine getirmektedir.

ESP: ESP protokolü kimlik doğrulama, bütünlük kontrolü ve gizlilik işlemlerinin tamamını yerine getirebilmektedir.

IKE: IKE protokolü IPsec protokol ailesinde kullanılan ve temel olarak Diffie-Hellman değişim mekanizmasını kullanan bir protokoldür. IKE protokolünün 3 temel amacı vardır:

- Uç noktalar arası anahtar değişimi için bir çözüm sağlamak,
- Yeni güvenlik birliklerinin kurulmasını sağlamak,

- Önceden oluşturulmuş olan bağlantıları yönetmek

VPN cihazları ile ilgili daha detaylı bilgi için UEKAE BGT-2004 VPN Güvenliği Kılavuzu Dokümanı incelenebilir.

2.7 İçerik Kontrolcileri

Dışarıdan ağa gelen saldırıların çoğu belli uygulamaların verileri içerisinde gelmektedir. İçerik kontrolcüsü, verilerin içerisinde gelen bu zararlı içerikleri tespit ederek bu içeriklerin ağa girmesini engellemektedir.

Zararlı içeriklerin engellenmesi yanında gelen verilerin içerisinde belli başlıkları, belli kelimeleri veya konuları tespit ederek bu tür verilerin ağa girmesi engellenebilmektedir. Bu verileri filtreleme işlemini doğal olarak belli protokoller için yapmaktadır. Bu protokoller HTTP, FTP, SMTP ve POP3'tür. Bu protokollere ait veriler ya ağın tamamında ya da yukarıda belirtilen sunucular üzerinde yapılabilir.

Ağ tabanlı bir içerik kontrolcüsü kullanımı, zararlı içeriğin hedeflenen bilgisayara ulaşmadan tespitini ve gerekli müdahalenin yapılmasını sağlaması sebebiyle sunucular üzerinde alınacak önlemlerden daha fazla bir güvenlik sağlarlar. Bunun yanında tüm trafiğin üzerinden geçtiği düşünülürse yüksek performans sağlaması gereken cihazlardır. Yapılandırmasında her türlü kontrolün (anti virüs, http filtreleme, ftp filtreleme, sıkıştırılmış dosyaların incelenmesi vs.) yapılması istendiğinde performans iyice düşecektir. İçerik kontrolcü üzerinde yürütülecek politika belirlenirken tüm ağ elemanları değerlendirilerek politikanın belirlenmesinde fayda vardır. Örneğin e-posta sunucusu üzerinde kurulacak aynı marka model anti virüs yazılımı varsa, aynı virüs tanımlamaları ile içerik kontrolcüsü üzerinde SMTP için virüs kontrolü yapmanın bir anlamı olmayacaktır. Aynı e-postanın aynı kriterlerle iki defa kontrol edilmesi mantıklı değildir.

Günümüzde özellikle web sunucularındaki yükü azaltmak ve kullanıcıların bekleme süresini düşürmek için web tasarımcıları tarafından aktif içerik konsepti geliştirilmiştir. Bu sayede kullanıcıların bilgisayarlarına dinamik içerikli dosyalar (Java Applet ler, ActiveX kontroller) indirilmektedir. Sıklıkla kullanılan dinamik içerikler birçok saldırının kaynağı olmaktadır. Bu içeriklerin içerik kontrolcüsü tarafından filtrelenmesi mümkündür.

İçerik kontrolcülerini ağa bağlanma şekilleri ürünün ürüne farklılık gösterebilmektedir. Köprü (bridge) modda bağlanacak bir cihaz için üzerinden geçmeyecek trafik söz konusu değildir. Bununla birlikte güvenlik duvarı duvarının bir bacağına bağlanacak içerik kontrolcüsü için güvenlik duvarında bir yönlendirme gereklidir. Dolayısıyla güvenlik duvarı üzerinde yapılabilecek yapılandırma değişikliği ile içerik kontrolcüsü üzerinden geçmeyen trafikten söz edilebilir.

Özellikle web sayfalarının içeriği kontrol edilerek, içerik kontrolcüsü ile kurum politikasına uymayan (finans siteleri, oyun ve kumar siteleri,) içerikte hizmet veren web sayfasına erişim kısıtlanabilmektedir.

2.8 Kablosuz Ağ Ürünleri

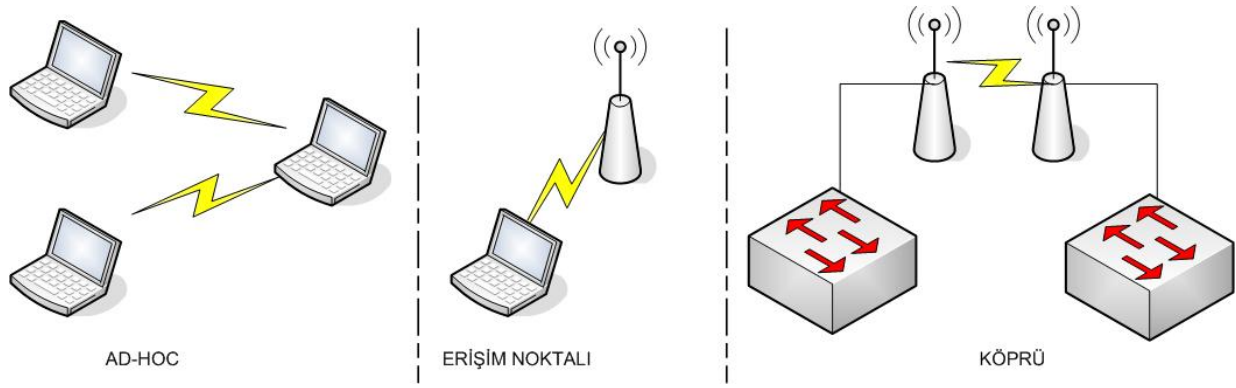
Günümüzde popülerliği giderek artan kablosuz ağ ürünleri, gerek ilk kurulum maliyeti (para ve zaman) açısından, gerekse esnekliği ve çalışan kişilere getirdiği hareket özgürlüğü açısından sıklıkla tercih edilmektedir. Veri aktarım ortamının hava olması sebebiyle, bu ortama fiziksel bir erişim kontrolü mümkün değildir. Dolayısıyla hattın dinlenilmesinin engellenmesi kriptografik önlemlerle sağlanmaktadır. Kablosuz yerel alan ağları (802.11a/b/g veya WLAN-Wireless Local Area Network) ülkemizde yaygınca kullanılmaktadır. Bunun dışındaki kablosuz kişisel alan ağları (WPAN-Wireless Personal Area Network veya 802.15, bluetooth, ZigBee vs.), kablosuz kampus ağları (WMAN-Wireless Metropolitan Area Network veya 802.16, WiMax) konuları kapsam dışında tutulmuştur.

Kablosuz Yerel Alan Ağları, kullanıcı açısından iki, erişim noktası açısından da iki farklı tip göstermektedir.

Kullanıcı açısından tasarsız (ad-hoc) ve erişim noktalı (tasarlı - infrastructure) olmak üzere iki tipte kablosuz yerel alan ağı mevcuttur. Ad-hoc tipinde, bilgisayarlar bir erişim noktasına ihtiyaç duymaksızın bir ağ oluşturabilmektedirler. Erişim noktalı ağlarda ise her bir bilgisayar erişim noktası ile haberleşmektedir.

Erişim noktası açısından, bilgisayarların faydalanacağı erişim noktalı (infrastructure) tipte ve köprü (bridge) tipinde olmak üzere iki tip ağ mevcuttur. Burada diğerlerinden farklı olarak köprü tipinde erişim noktası başka bir erişim noktası ile haberleşmekte bir bilgisayara hizmet vermemektedir.

Bu dokümanda tasarlı tipinde gerçekleştirilmiş bir yerel alan ağı için tavsiyelere yer verilmiştir. Aşağıda üç farklı tipte gerçekleştirilmiş kablosuz ağ teknolojileri şekil olarak ifade edilmiştir.



Şekil 2-2 Kablosuz Ağ Teknolojileri

Kablosuz ağlarda güvenliği üç ana başlık altında sınıflandıra biliriz; erişim kontrolü, şifreleme ve gözlemleme. 1999 yılından bu yana gelişen kablosuz yerel alan ağı (WLAN- iee 802.11) şu an WEP, WPA, WPA2 gibi farklı şifreleme ve kimlik doğrulama yöntemleri sunmaktadır. Kablosuz yerel alan ağları ile ilgili olarak daha detaylı bilgi için Kablosuz Ağ Güvenliği Dokümanı incelenebilir.

2.8.1 Erişim Noktaları (Access Point / Wireless Access Point)

Bilgisayar ağlarında erişim noktaları, kablosuz haberleşme cihazlarının birbiriyle ve bağlı olduğu kablolu ağ ile haberleşmesini sağlamak amacıyla kablosuz bir ağ kuran cihazlardır.

Gerek köprü tipinde gerekse erişim noktası ile kurulmuş kablosuz ağ tipinde gizliliğin sağlanması için kullanılacak teknolojiler WEP, WPA-PSK, WPA ve WPA2 olarak sıralanabilir.

Kablosuz yerel alan ağlarında veri iletişim ortamı hava olması sebebiyle, veri iletim ortamına erişim kontrolünün fiziksel önlemlerle alınması mümkün değildir. RADIUS kullanılarak kimlik doğrulama yapılması mümkünse sertifika kullanılması tavsiye edilen erişim kontrolü /kimlik doğrulama yöntemidir.

Şifreleme için gerek RC-4 zayıflıkları gerekse IV (başlangıç vektörü) boyunun kısa olması sebebiyle WEP kullanımı tavsiye edilmez. Şifreleme algoritması olarak AES (Advanced Encryption Standard) kullanılması tavsiye edilmektedir.

Bir kablosuz erişim noktası için tavsiye edilen şifreleme ve kimlik doğrulama yöntemleri aşağıda verilmiştir.

- WPA2/AES ve EAP-TLS
- WPA2/AES ve PEAP-MS-CHAP v2

- WPA/TKIP ve EAP-TLS
- WPA/TKIP ve PEAP-MS-CHAP v2

Bu teknolojilerin kullanmadığı durumlarda kullanılacak diğer yöntemlerin (WEP, WPA-PSK) kablosuz trafik dinlenerek kırılacağı, transfer edilen bilginin gizliliğinin tehlikede olduğu unutulmamalıdır.

Gerek ağa saldırının tespiti gerekse var olan politika dışında davranan kurum çalışanlarının tespiti için gerçek zamanlı kablosuz ağ dinleme ve kontrol yazılımı/sistemi kullanılması tavsiye edilmektedir.

Bilginin gizliliğinin ve bütünlüğünün korunması dışında servisin sürdürülebilirliği, kablosuz alan ağlarında sağlanması zor hizmetlerden biridir. Özellikle servis sonlandırma (DoS: Denial of Service) tipindeki saldırılara karşı koruma sağlamak hayli güçtür. Bu hususta piyasada bulunan, ürüne özgü koruma yöntemleri mevcuttur.

Erişim noktasının fiziksel konumu ve sinyal gücü de önemli güvenlik parametreleri arasında sayılabilir. Erişim noktasının olası fiziksel müdahalelere karşı korunması varsayılan ayarlarına döndürülememesi konsol bağlantısı ile konfigürasyonunun değiştirilmemesi için kolay ulaşılamayacak bir yere monte edilmesi, mümkünse erişim noktası ile antenin ayrılması tavsiye edilmektedir. Kapsama alanının istenen/hedeflenen bölgenin dışına çıkması istenmeyen bir durumdur, kullanılan şifreleme yöntemine göre zayıflıkların sezilmesi ihtimalini arttıracaktır.

2.9 Ağ Yönetim İzleme/Dinleme Ürünleri

Yönetilen, işletilen bir ağda uygulanan güvenlik politikası dışında davranışların sezilmesi, kullanılan ürünlerin açıklıklarının veya güvensiz yapılandırmalarının tespit edilmesi ve bunun gibi birçok sebepten kurumsal bir ağda bir ağ yönetim ve izleme ürünü kullanılmasında büyük fayda vardır.

Ağ yönetim ve izleme yazılımları;

- Kurum içinde ve kurum dışında kullanılan bilgisayarların değişen yapılandırması ile olabilecek güvenlik açıklıkları veya istenmeyen servislerin tespiti
- Kurum bünyesinde bulunan bilgisayarların açık servislerinin tespiti
- Ağa dâhil olmayan makinelerin tespiti
- Yapılandırma hatalarının tespiti ve incelenmesi

- Ürün yama eksikliklerinin tespiti

gibi özellikler sağlarlar.

Bu tip yazılım veya sistem çözümleri kurumsal bir ağda özellikle sistem ve güvenlik yöneticilerinin olası bir probleme müdahale süresini kısaltır, sorunun karmaşıklığını azaltır. Hiçbir sorunla karşılaşmadığı durumlarda da sistemin gerçekten sorunsuz çalıştığından emin olunmasını sağlar.

Bir ağ yönetim yazılımı, ağ üzerinde birçok cihazı yönetebileceği ve yapılandırmasını değiştirebileceği için ağda en güvenli (en iyi korunan) bölgede yer almalıdır. Bu bölge için güvenlik duvarı kuralları sadece yönetim yapılabilecek kadar sıkı olması tavsiye edilmektedir.

Ağ izleme/dinleme yazılımı ise genellikle taşınabilir bir bilgisayarla kullanılması, sorun oluşması halinde ilgili ağ segmentine taşınması ve kullanılması tavsiye edilmektedir.

2.10 Antivirüs Uygulamaları

Kurumlarda bilgi teknolojileri ortamından kaynaklanan hizmet kesintilerinin, veri kayıplarının, gizli bilgilerin istenmeyen kişilerin eline geçmesinin vb. durumların ana sebeplerinden bir sistemlere bulaşan zararlı yazılımlardır. Bilinen ve sıklıkla karşımıza çıkan virüsler bu zararlı yazılımların başını çekmektedir.

Ağın ve diğer ağ unsurlarının (sunucular ve istemcilerin) bu zararlı yazılımlara karşı korunması antivirüs diye bilinen ürünlerle sağlanabilmektedir.

Ağın dolayısıyla ağda bulunan tüm istemci ve sunucuların virüslere karşı korunması için ağ tabanlı antivirüs cihazları kullanılabilir. Bu cihazlar dış dünyadan, özellikle güvensiz olarak kabul ettiğimiz internetten, e-posta, http ve ftp yolu ile bilgisayarlara geçecek virüslerin girişini engellemek amacıyla kullanılabilirler.

İnternetten gelebilecek virüsler dışında kullanıcıların kullandıkları taşınabilir medyalar da sistemlere virüs girişi mümkündür. Bunun önüne geçilmesi için ise sunucu ve istemcilerde antivirüs programları bulunması gerekmektedir.

Gerek ağ tabanlı antivirüs sistemlerinde gerekse istemci ve sunucularda kullanılan antivirüs yazılımlarında en önemli nokta virüs tanımlamaları ve bu tanımlamaların güncelliğidir. Virüs veritabanı güncel tutulmayan bir sistemin yeni geliştirilmiş virüslere karşı zaafiyet taşıdığı aşikârdır. Bu zayıflığın önüne geçmek için özellikle çok kullanıcıli kurumsal ağlarda merkezi antivirüs yönetimi kullanılması gereklidir. Özellikle kullanıcıların sistemlerine yüklenmiş antivirüs yazılımlarına erişmeleri ve bu yazılımlara müdahale etmeleri grup politikaları ile engellenmelidir. Merkezi antivirüs yönetim yazılımı ile tüm ağda kullanılan antivirüs sistemlerine antivirüs politikası yüklenmesi, sunucu ve istemci bilgisayarlarında bulunan ajan yazılımlarının kontrolleri, ağ tabanlı antivirüsün güncel durumunun izlenmesi politika değişikliği yapılabilir.

Ağ tabanlı antivirüs sistemi kullanımının sunucu ve istemcilerde antivirüs kullanımına göre avantajı, virüslü dosyanın hedeflenen bilgisayara gitmeden müdahale edilmesinin mümkün olmasıdır. Bununla birlikte Ağ tabanlı antivirüs sisteminin gelen tüm paketleri OSI referans modeline göre yedinci katmana kadar çıkarması, incelemesi sıkıştırılmış (ZIP RAR vs formatındaki dosyalar) paketleri açması, incelemesi sonra ilgili sisteme göndermesi gerekmektedir. Dolayısı ile ağa giren ve çıkan tüm trafiğin (smtp, http, ftp) virüs açısından incelenmesi ciddi bir performans kaybına yol açmaktadır. Kurum için bir ağ tabanlı antivirüs sistemi seçilirken mevcut ve planlanan bant genişliği göz önünde bulundurularak uygun hızda çalışabilecek bir sistem seçilmesi gereklidir.

2.11 Sunucu ve İstemciler

Bu noktaya kadar ağda kullanılan/kullanılacak olan güvenlik sistemlerinden (güvenlik duvarı, saldırı tespit/önleme sistemi, antivirüs sistemleri, VPN gibi) veya ağ sistemlerinin (anahtarlama cihazı, yönlendirici gibi) nasıl güvenli olarak kullanılacağından bahsedildi. Bununla birlikte asıl korunmak istenen varlıkları barındıran, işleyen sistemler (sunucular ve istemci bilgisayarları) ve bunların güvenli ve güvenilir kullanımı da ciddi önem arz etmektedir.

Gerek sunucularda gerekse istemcilerde ilk kurulumunda birçok iş ve hizmet için kullanılması öngörülerek kimi servisleri açık kimi servisleri kapalı olarak dağıtılmaktadır. Sunucu ve istemcilerde istenmeyen/amaçlanmayan servisleri kötüye kullanımı engellemek maksadıyla kapatılmalıdır.

İşletim sistemlerinin tespit edilen açıklıkları için sürekli yamaları, güncellemeleri yayımlanmaktadır. Bu yamaların yüklenmemesi halinde kritik güvenlik açıklıkları ile karşılaşılabilir. Birçok virüs ve zararlı yazılım aslında işletim sistemlerinin bu açıklıklarını kullanarak yayılır ve hedef sisteme zarar verir. Özellikle yama yönetimi için geliştirilmiş ürünler kullanılması, bu iş için ayrılacak iş gücünün minimumda tutulmasını sağlayacaktır.

Kurumlarda değerli ve kritik bilgiler çoğunlukla sunucularda tutulmaktadır. Bununla birlikte birçok durumda iş ihtiyacı gereği bu veriler kişisel bilgisayarlara kopyalanabilmekte ve çalışanların bu veriler üzerinde çalışması sağlanmaktadır. Bu sebeple kişisel bilgisayarlarda da bazı güvenlik önlemleri alınması gerekmektedir. Çalışanların yetkisi dışında iş yapmalarının önüne geçmek için yetkilerinin kullanıcı seviyesinde olması yönetici yetkisinin verilmemesi gereklidir.

Kullanıcı bilgisayarları ve sunucularda BIOS (Basic Input Output System) parolası uygulanması yetkisiz kişilerin BIOS a müdahale etmesini engelleyecektir.

İşletim sisteminin sağladığı durumlarda kişisel güvenlik duvarları açık olmalı, kullanıcı eylemleri için log tutulmalıdır.

Özellikle kullanıcı bilgisayarları (Windows sistemleri için) etki alanı altında bulunmalı ve grup politikası uygulanmalıdır. Bu hem güvenliği arttırıcı bir önlem hem de yönetim için gerekli iş gücünün verimli kullanılmasını sağlayacaktır.

Günümüzde gittikçe yaygınlaşan, bir çok kurumda da kullanımı artan açık anahtar altyapısı ile gerek kullanılan dokümanların, gerekse yapılan mesajlaşmaların (e-posta) gizliliği bütünlüğü, inkar edemezliği sağlanabilmektedir. Ayrıca kimi uygulama yazılımları içinde de kullanım artmaktadır.

3. AĞ TASARIM PRENSİPLERİ

3.1 İhtiyaçların Belirlenmesi ve Amaca Yönelik Tasarım

Ağ tasarımının uygun olarak yapılması, gerek performans gerekse maliyet açısından oldukça önemlidir. Bunun için ilk önce ihtiyaçlar belirlenmelidir. İhtiyaçlar çerçevesinde hangi protokol veya protokollerin kullanılacağı, bu protokol veya protokollerin bir bağlantı esnasında ne kadar bant genişliği gerektireceği ve ağdaki toplam trafik yükünün ne olacağı hesaplanmalıdır.

Ağda kullanılan teknolojilerin dar boğazları göz önüne alınarak tasarım yapılmalıdır. Örneğin çevirmeli ağ bağlantısı ucuna 10/100/1000 Mbps'lik bir bağlantı yerine kolayca 10/100 Mbps hızında çalışan bir bağlantı yapılabilir.

3.2 Politikaların Belirlenmesi

Bir kurumda mutlaka bir bilgi güvenliği politikasının olması, yoksa belirlenmesi ve uygulanması tavsiye edilmektedir. Bilgi güvenliği politikası kapsamında oluşturulacak diğer politikalarla, bilginin ne şekilde oluşturulacağı veya kabul edileceği, ne şekilde işleneceği, ne şekil ve şartlar altında transfer edileceği ve ne şekilde değersiz kılınacağı veya yok edileceği belirlenmelidir. Bu kapsamda bir bilgi sistem yöneticisi veya güvenlik yöneticisi bilgi sistem cihazlarının ne şekilde kullanılması ve yapılandırılması gerektiğini belirleyecektir.

Erişim politikaları veya erişim kontrol politikaları, hangi bilgi veya bilgilere kimlerin nasıl erişebileceğini, hangi sistem kaynaklarını kimlerin nasıl kullanacağını belirlediği politikalardır.

Erişim politikalarının dışında veri yedekleme ile ilgili politikalar, kullanıcıların bilgi sistemini kullanımı ile ilgili politikalar, iş sürekliliği ile ilgili politikalar, felaket kurtarımı ile ilgili politikalar ağ mimarisi güvenliği kapsamı dışında tutulmuştur.

3.2.1 Erişim Politikaları

Bir ağ tasarımı esnasında uygulanacak politikalara bağlı olarak gerekli ağ bileşenleri belirlenmelidir. Var olan bir ağ iyileştirilmek istendiğinde veya güvenlik ve performansı sorgulanacağı zaman kullanılan ağ cihazları politikalar ile birlikte değerlendirilmelidir.

Kurum ağında erişim politikalarını güvenlik duvarları, anahtarlama cihazları, VPN cihazları gibi cihazlar uygularlar.

Güvenlik duvarları üzerinde bulunan güvenlik politikasına bağlı olarak, ağ adresi, IP adresi, port ve yeni nesil güvenlik duvarlarında uygulama seviyesine kadar trafiğin geçişine izin verilebilir veya trafik durdurulabilir.

Anahtarlama cihazlarında (ilgili port kilitleme özelliğine sahip anahtarlama cihazları için), cihazın portuna yabancı bir makinenin bağlanması halinde makinenin ağa erişimi engelleyecek mekanizmalar mevcuttur.

VPN cihazlarında ise yine üzerinde bulunan politikaya bağlı olarak üzerinden geçen trafiği şifreli veya şifresiz geçirebildiği gibi trafiği durdurma veya paketleri düşürme yetenekleri mevcuttur.

3.2.2 Zamana Bağlı Kullanım Politikası

Ağ üzerinde bulunan kaynakların kullanımı belli zaman aralıkları ile sınırlandırılması gerek erişim politikasının gerekse bilgi güvenliği politikasının bir parçası olduğu durumlarda, erişim kontrolü sağlayan cihazlarda politikalar zaman kriterine göre belirlenebilir. Örneğin; politikada kritiklik seviyesi yüksek olan bir veri tabanına sadece veri tabanı yöneticisinin kurumda olduğu zamanlarda -mesai saatleri içinde- erişime müsaade edilebilir. Trafik bazında ücretlendirme yapılan bir hattın kullanımı sadece iş için kullanılması maksadı ile mesai saatleri ile sınırlandırılabilir veya çalışan verimliliğinin düşmemesi için sohbet, finans amaçlı sitelere erişim sadece belli saatlerle sınırlandırılabilir.

Bu tipte zamana bağlı kullanımlar ağda güvenlik duvarları ve içerik kontrolcülerini aracılığı ile sağlanabilir.

3.3 Büyüme Hızının Belirlenmesi

Ağ tasarımında ileriki zamanlar da düşünülerek yatırım yapılmalıdır. Örneğin bir yıl sonra ağa eklenecek kullanıcı sayısı veya ağda çalıştırılacak yeni uygulamalar göz önüne alınarak tasarım yapılmalıdır.

Kurumun büyüme hızı sadece personel sayısı olarak düşünülmemelidir. Yeni teknolojilerin kullanımı da kurum için teknolojik olarak büyüme anlamına gelir. Gelişen bilgi sistem cihazları daha fazla bant genişliği, daha düşük hata toleransı beklentileri ile gelecektir. Bu sebeple yeni ağ cihazlarının temininde büyüme hızı ve şekli çok iyi değerlendirilmesi gereklidir. Örneğin; ağdaki hızı arttırmak maksadı ile 100Mbit hızında çalışan anahtarlama cihazları 1000Mbit hızında çalışan anahtarlama cihazları ile değiştirileceği bir durumda var olan teknolojinin incelenmesi tavsiye edilmektedir. Var olan servisler incelenip yakın gelecekte

kullanılması muhtemel teknolojiler kurumunun teknolojik büyüme planı içinde olup olmadığı sorgulanmalıdır. Anahtarlama cihazlarının temini sırasında IP telefon kullanılmadığı halde yakın gelecekte IP telefon kullanımı söz konusu ise bu servis için yüksek performans sağlayan cihazların maliyet etkinliği kontrol edilmelidir.

3.4 Maliyet Etkinlik Analizi

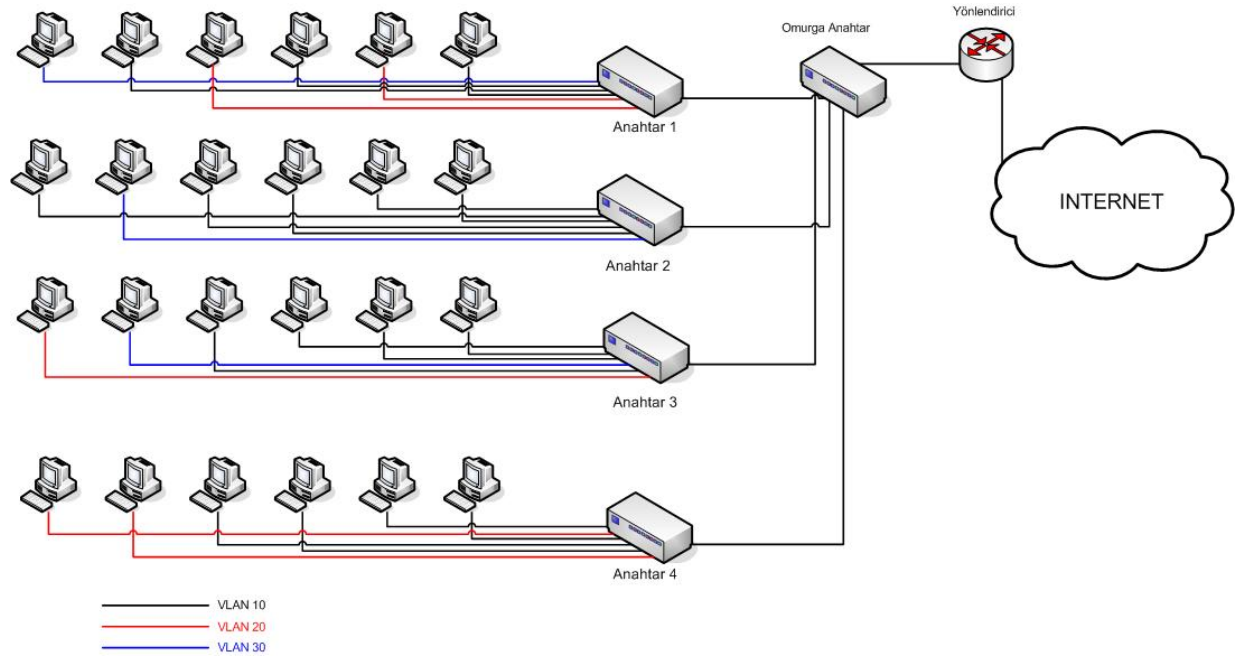
Tasarımlarda maliyet önemli unsurlardan bir tanesidir. Her zaman en pahalı olan çözüm kurum için en iyisi olmayabilir. Bu yüzden ihtiyaçlar etkin bir şekilde tanımlanarak en uygun maliyetli çözüm belirlenmelidir. Ağda performans problemlerinin ortaya çıkması durumunda hemen daha performanslı bir cihaz almak yerine mevcut cihazın etkin kullanımı, ağ trafiğinin incelenerek yeniden düzenlenmesi gibi maliyet getirmeyecek fakat düzenlemelerle performansı artıracak çözümler tercih edilmelidir.

3.5 Çevrim Dışı Ağ Kullanımı

Özellikle kurum için kritik görülen işler için kullanıcı makinelerinin bulunduğu ağ dışında, dış dünyaya kapalı ağlar kullanılmaktadır. Sadece iş maksatlı kurulan bu ağlarda da çevrim içi kullanımda alınan tedbirler alınabileceği gibi, ağ boyutu çok küçük ise sadece giriş çıkış arabirim kısıtlamaları, kullanıcı hak kısıtlamaları, anti virüs sistemleri ile güvenliği sağlanabilir. Örneğin sadece muhasebe ve finans işlerinin görüleceği beş kişinin kullanacağı bir oluşturulup bu ağın dış dünyaya bağlantısı kesilebilir veya çevrim içi ağda kullanılacak sayısal sertifikaların üretileceği makine veya makineler dış dünyadan izole edilebilir. Her iki örnekte de söz konusu sistemlerin amaçlanan işleri dış dünyaya bağlanmayı gerektirmiyorsa veya dış dünyaya bağlanmak, ciddi riskleri doğuracaksa bu sistemlerin çevrim dışı bir ağda konumlandırılması güvenlik açısından risk azaltıcı tedbir olarak değerlendirilmelidir.

4. ÖRNEK AĞ MİMARİ MODELLERİ

4.1 Ağ Modellerinde Sanal Yerel Alan Ağ (VLAN) Kullanımı

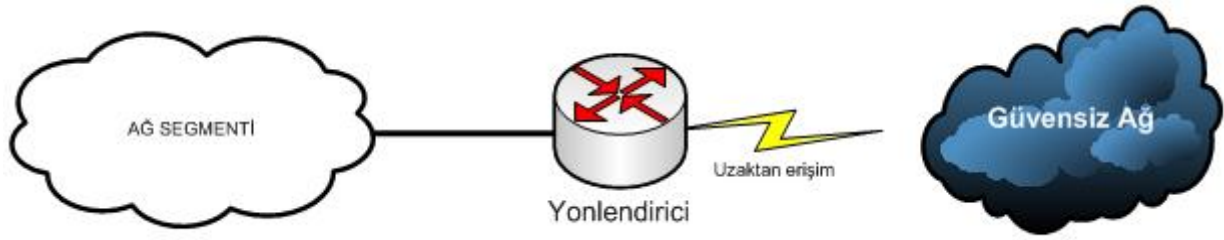


Şekil 4-1 VLAN kullanımı ile gerçekleştirilmiş ağ mimari modeli

Bir organizasyonda aynı yerde (büro, ofis, kat gibi) çalışmasına rağmen farklı görev ve işlerde çalışan personelin ağ trafiğini birbirinden izole etmek ve ağ performansını artırmak için sanal yerel alan ağları (VLAN) kullanılır. VLAN mekanizması olmasaydı, birbirinden izole etmek istediğimiz ağa trafikleri için ayrı ayrı anahtarlar ve yönlendiriciler kullanmak zorunda kalınacaktı. VLAN kullanımı ağ yöneticisine uygun cihazlar kullanımı halinde “Personel Dairesinde çalışanlar internete mesai saatleri dışında çıkabilsinler” şeklinde bir politikanın uygulamaya konmasını kolaylaştırır.

Yönetilebilen tüm anahtarlama cihazları VLAN desteği ile kullanılmaktadır. Anahtarlama cihazlarında her bir arayüz için varsayılan VLAN değeri VLAN1’dir. En azından basit saldırılara karşı koymak amacıyla organizasyon bünyesinde kullanılacak anahtarların tüm arayüzlerinin varsayılan VLAN dışına alınmasında fayda vardır.

4.2 Tek Yönlendirici ile Gerçeklenmiş Ağ Mimari Modeli



Şekil 4-2 Tek yönlendirici ile gerçekleştirilmiş bir ağ mimari modeli

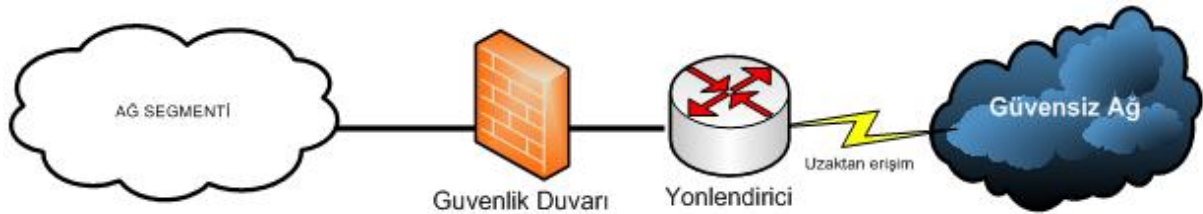
Tek yönlendirici ile gerçekleştirilmiş mimari modelinde şekilde de görüldüğü gibi dışa ağdan iç ağa erişim için sadece yönlendirici üzerinden geçilmesi gerekmektedir. Bir yönlendiricide alınabilecek güvenlik önlemleri çok kısıtlıdır. Böyle bir mimari kullanımı ticari veya kurumsal uygulamalarda ağ güvenliği açısından tavsiye edilmemektedir.

Yönlendirici üzerinde uygulanacak ağ erişim kuralları alınabilecek önlemlerden biridir. Fakat bu yönlendiricide performans kaybına sebep olacaktır. Bun dışında iç ağa yapılacak saldırılara karşı bir önlem bulunmamaktadır. Şekildeki mimaride kayıt mekanizması bulunmamaktadır bunun sonucunda yönlendirici üzerinde bulunan kısıtlı bir alan denetim kayıtları için kullanılacak, bu da etkin bir kayıt mekanizması olmayacaktır.

4.3 Tek Güvenlik Duvarı ile Gerçeklenmiş Ağ Mimari Modelleri

Genel mimaride DMZ'in var veya yok olma durumuna göre iki farklı mimari modeli sunulmuştur.

4.3.1 DMZ Olmaksızın Gerçeklenebilecek Ağ Mimari Modeli



Şekil 4-3 Tek güvenlik duvarı ile gerçekleştirilmiş bir ağ mimari modeli

Tek güvenlik duvarı mimarisi tasarımı küçük veya orta büyüklükteki bilgisayar ağları için tasarlanmıştır. Bu tip mimari tasarımlarda dış ağlara hizmet veren sunumcu sistemlerin olmaması gerekmektedir. Eğer dış ağa hizmet veren sunucular olursa bu sunucular iç ağda konumlandırılacağı için hem iç ağdan doğrudan saldırılar alabilir hem de dış ağdan bu sunuculara erişen kişiler iç ağa erişmiş olur.

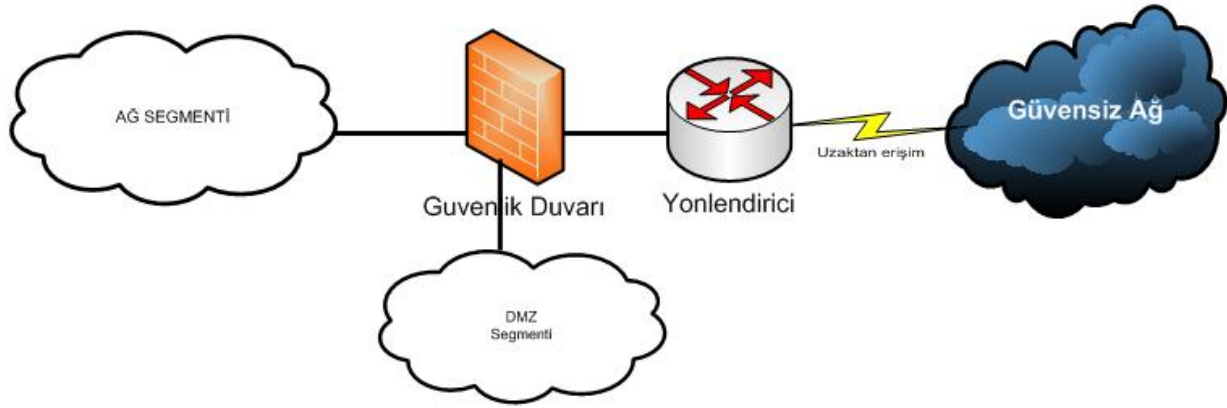
Ağa erişim denetimi güvenlik duvarı tarafından sağlanır. Güvenlik duvarı üzerinde iki adet ağ ara yüzü bulunmaktadır. Ağ ara yüzlerinden birisi dış ağlardan gelen istekleri iç ağa iletmekle, diğer ağ arayüzü ise iç ağdan giden istekleri dış ağlara aktarmakla görevlidir. Güvenlik duvarı bu iki ağ arayüzü arasındaki ağ trafiğinin akışını güvenlik ihtiyaçları doğrultusunda belirlenmiş olan güvenli ağ erişim kurallarına göre kontrol eder. Güvenlik duvarının kural tablosu güvenlik politikaları, yönergeler ve ihtiyaçları doğrultusunda belirlenmelidir. Dış ağdan iç ağa olan erişimler güvenlik duvarı tarafından kısıtlanmalı ve kontrol edilmelidir. Normal şartlarda bu tip mimari topolojilerde dış ağdan iç ağa olan erişimlere izin verilmemesi gerekmektedir.

Tek güvenlik duvarının kullanıldığı mimari topolojilerde ağ trafiği yüksek seviyelerde ise kullanılacak güvenlik duvarı durumsal güvenlik duvarı olarak seçilmelidir. Durumsal güvenlik duvarı OSI referans modelinin oturma katmanında hizmet verdiği için uygulama seviyesinde güvenliğin sağlanması amacıyla eğer mümkünse güvenlik duvarı ile birlikte vekil sunucular da kullanılmalıdır.

Tek güvenlik duvarı kullanılan mimari topolojilerde güvenlik duvarının yönetimi farklı şekillerde gerçekleştirilmektedir. Güvenlik duvarının iç ağ üzerinden veya dış ağda bulunan yönetim konsolu aracılığıyla da yönetimi yapılabilir. Güvenlik duvarının yönetiminde önemli olan güvenlik duvarının konfigürasyonunun yetkisiz olarak değiştirilememesi ilkesinin uygulanmasıdır. Eğer iç ağ gizlilik dereceli bilgiler içeriyorsa güvenlik duvarı iç ağdan yönetilmelidir. Güvenlik duvarı ile yönetici konsolu arasındaki iletişim şifreli olmalıdır. Güvenlik duvarı üzerinde yapılan tüm değişiklikler raporlanabilmelidir.

Tek güvenlik duvarının kullanıldığı mimari topolojilerde normal şartlarda iç ağda bulunan sunucuların dış ağdaki kullanıcılara servis vermemesi gerekmektedir. Bu durumun en önemli gerekçesi, iç ağdaki sunucudaki oluşan zafiyet veya açıklık durumlarında dış ağdan iç ağdaki sunucuya bağlanan kötü niyetli kişilerin var olan açıklıkları ve zafiyetleri kullanarak sunucuyu ele geçirip iç ağa erişmeleridir. Fakat iç ağdaki sunucular dış ağda bulunan sunuculardan belirlenen güvenlik politikaları, yönergeler ve ihtiyaçlar doğrultusunda servis alabilirler.

4.3.2 İki veya Daha Fazla DMZ Bölgesine Ayrılmış Ağ Mimari Modeli



Şekil 4-4 Bir güvenlik duvarı ile iki ağ segmentine ayrılmış bir ağ mimari modeli

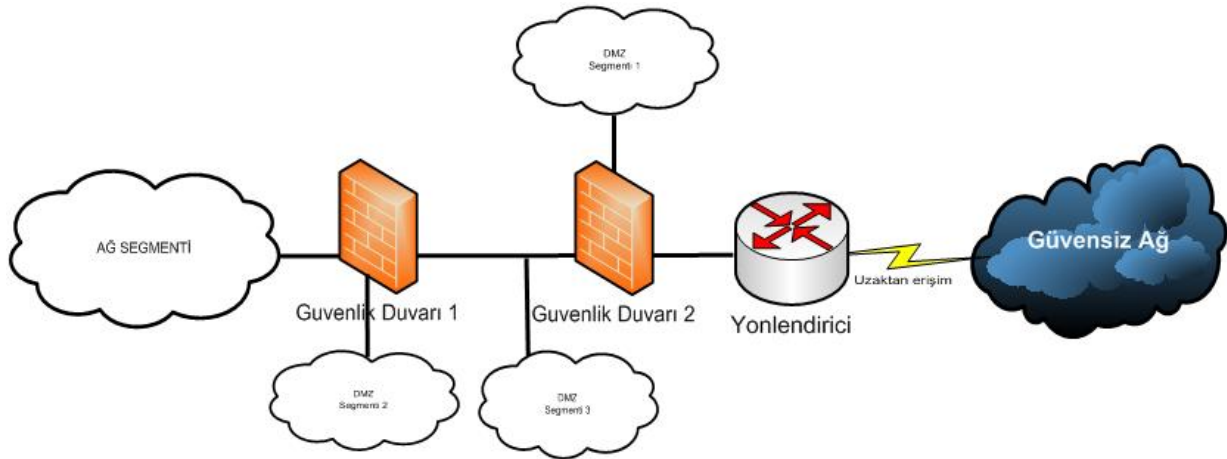
Bu mimaride ağda bir yönlendirici ve bir güvenlik duvarı bulunmaktadır. Bu mimari farklı güvenlik seviyesine sahip ağların bulunduğu durumlarda tercih edilmelidir. Kullanılan güvenlik duvarının üç tane ağ arayüzü vardır. Bu ağ arayüzleri geniş alan ağı (internet), iç ağ, DMZ ağlarını bağlamaktadır. İç ağ bölümünde kullanıcı bilgisayarları, alan adı, etki alanı, vekil, e-posta sunucuları gibi sunucular mevcuttur. İç ağ bölümünde bulunan sunucu veya kullanıcı bilgisayarlarından dış ağ bölümüne (GAŞ, internet) servis verilmez. Mimari topoloji içinde güvenlik derecesi en yüksek bölümdür. DMZ ağı, iç ağ bölümüne ve dış ağ bölümüne (GAŞ, internet) hizmet veren sunucuların oluşturduğu bölümdür. Güvenlik duvarı bu farklı güvenlik seviyesine sahip ağlar arasındaki trafiği düzenleyerek ağın güvenli ve yüksek performanslı olarak çalışmasını sağlar.

İç ağ, ağ kullanıcıları ve bu kullanıcılara hizmet veren sunuculardan oluşmaktadır. İç ağda bulunan sunucular sadece iç ağdaki kullanıcılara ve istemcilere hizmet veren sunuculardan oluşmalıdır. İç ağda bulunan sunucuların ve istemcilerin IP adresleri gerçek IP adresleri olmamalı, iç ağda kullanılan sanal IP adresleri olmalıdır. İç ağdaki herhangi bir bileşen geniş alan ağıyla haberleşmek istediğinde iç ağdaki IP adresleri güvenlik duvarı üzerinde adres dönüşümüne tabi tutularak dönüştürülmüş IP adresleri ile geniş alan ağına açılmalıdır. İç ağdan geniş alan ağına olan adres dönüşümü dinamik adres dönüşümü olmalı, bu sayede iç ağın IP adres bloğu gizlenebilmelidir.

Dış ağ bölümü DMZ bölümündeki sunuculardan servis alan kullanıcıların ve kullanıcı bilgisayarlarının bulunduğu bölüm veya iç ağ ve DMZ bölümündeki sistemlerin servis aldığı bölümdür.

Mimari topolojilerde bulunan DMZ bölümü ise iç ağ ve dış ağ kullanıcılarının hizmet aldığı sunuculardan oluşan ve iç ağdan farklı güvenlik seviyesine sahip bir bölüm olarak tarif edilebilir. Güvenlik duvarı üzerinde iç ve dış ağ bölümlerinden DMZ bölümüne erişim için sadece DMZ bölümündeki sunucuların sunduğu servislere ihtiyaç dahilinde ve güvenlik gereksinimleri göz önüne alınarak izin verilmelidir. E-posta, web, alan adı, vekil sunucuları genel olarak DMZ bölümünde bulunabilecek belli başlı sunuculardır. DMZ bölgesindeki sunucular için gerçek IP adresleri kullanılmamalıdır. DMZ bölümünde kullanılacak IP adresleri IETF'un tanımladığı rezerve edilmiş IP adresleri (10.0.0.0/24, 192.168.0.0/16, 172.16.0.0-172.31.255.255) olmalıdır. Bilindiği üzere rezerve edilmiş IP adresleri dış ağda yönlendirici tarafından yönlendirilmediği için bu bölümde bulunan sunucular için statik adres dönüşümü kuralları uygulanmalıdır. Ayrıca DMZ bölümünde bulunan tüm sunucular anahtarlama cihazlarına bağlanmalıdır. Anahtarlama cihazlarına bağlanan her bir sunumcunun MAC adresi anahtarın ilgili portuna kilitlemelidir.

4.4 İki veya Daha Fazla Güvenlik Duvarı Kullanılarak Gerçekleşmiş Ağ Mimari Modeli



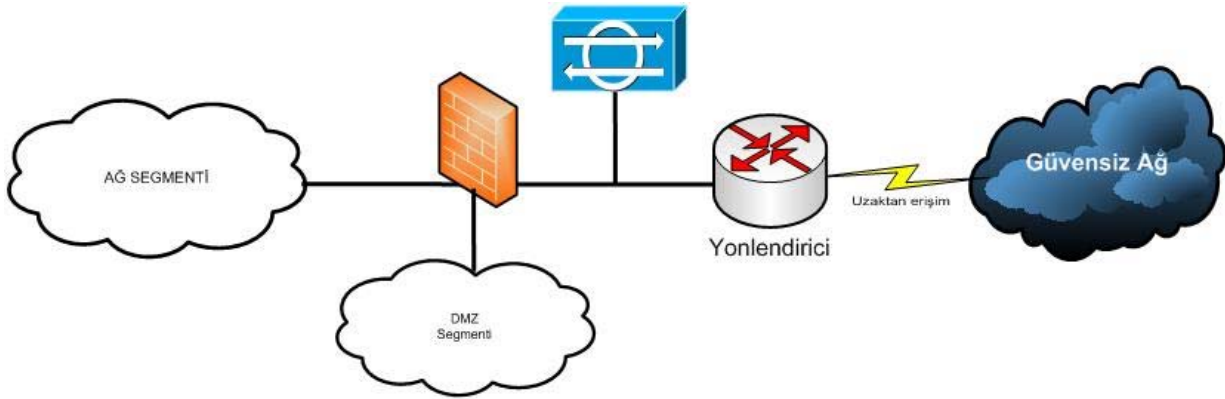
Şekil 4-5 Ardışık bağlı iki güvenlik duvarı ile gerçekleştirilmiş bir ağ mimari modeli

Mimari topolojide ağ erişimini sıkı bir şekilde denetlemek için iki güvenlik duvarı ardışık olarak kullanılır. Bu topoloji genellikle sıkı güvenlik istenen sistemlerde kullanılır. Çünkü herhangi bir sebepten dolayı yetkisiz bir kullanıcının güvenlik duvarlarının birinden geçmesi durumunda diğer güvenlik duvarının yetkisiz kullanıcıyı durdurması hedeflenir. Güvenlik duvarları içerisine yerleştirilmiş bir arka kapı, ajan yazılımının veya güvenlik açıklığının tüm sistemi etkileme riski azaltılır. Bu yapıda güvenliğin maksimize edilmesi için ağda kullanılan güvenlik duvarlarının farklı üreticilerden seçilmesine ve birbirini tamamlayıcı nitelikte olmasına dikkat edilmelidir.

Ardışık iki güvenlik duvarının bağlanması güvenliği artırmanın yanında çok sayıda DMZ bölgesi oluşturma ve her birinde farklı güvenlik seviyesi elde etmeyi sağlamaktadır.

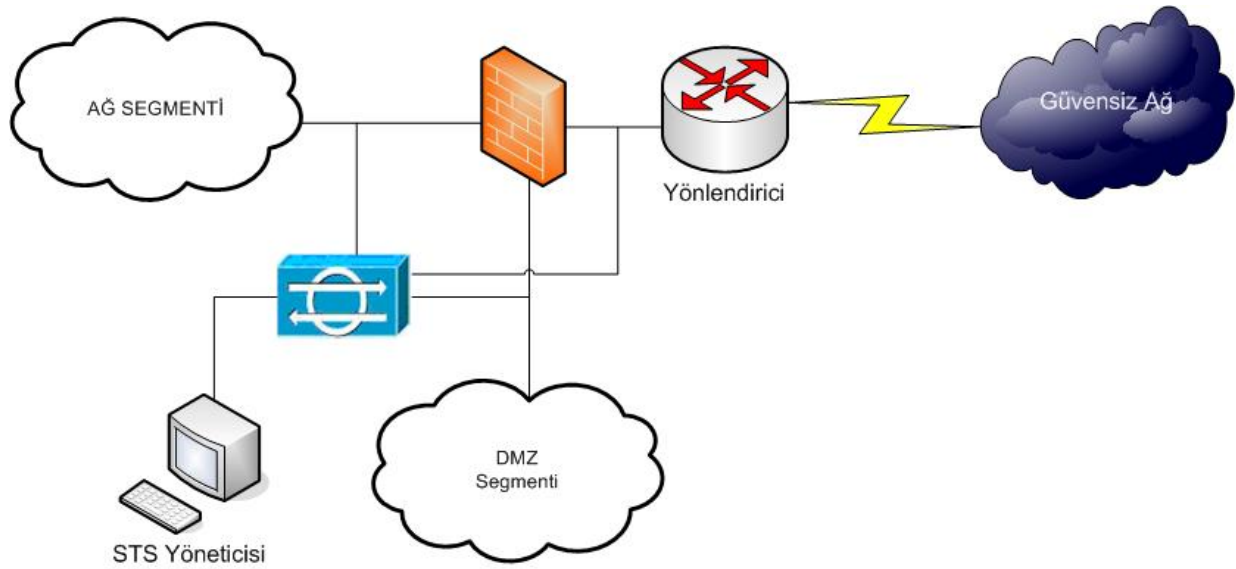
Mimari topolojinin geniş alan ağına bakan tarafındaki güvenlik duvarı geniş alan ağı, DMZ 1, DMZ 3 ve Güvenlik Duvarı 1 arasındaki mantıksal bilgi akışını kontrol eder. Bu kısımda kullanılan güvenlik duvarı türünün durumsal filtreleyici olması yeterlidir. Güvenlik Duvarı 2 üzerinde oluşturulan DMZ bölgelerinde genellikle dış ağ kullanıcılarına hizmet veren sunucular bulunur. Arka kısımda bulunan Güvenlik Duvarı 1 ise iç ağ, iç ağ sunucuları, veritabanı ve DMZ bölümleri arasındaki mantıksal bilgi akışını yönetir. Güvenlik Duvarı 1'e bağlı DMZ'lerde bulunan sunucular genellikle iç ağ kullanıcılarına hizmet verirler. Bu kısımda kullanılacak güvenlik duvarlarının gerektiğinde OSI referans modelinin 4-7 katmanlarında hizmet verebiliyor olması gerekmektedir.

4.5 Saldırı Tespit Sistemlerinin Ağ Mimari Modellerinde Konumlandırılması



Şekil 4-6 Saldırı tespit sisteminin ağ mimarisindeki yeri

Ağa yapılan saldırıların anlaşılabilmesi için saldırı tespit sistemi değişik şekillerde konumlandırılabilir. Bunlarda yaygın olarak kullanılanları: yönlendirici ve güvenlik duvarı arasında konumlandırma, güvenlik duvarı ile iç ağ arasında konumlandırma, veya birden çok arayüzü dinleyecek şekilde konumlandırma olabilir.. Yönlendirici ve güvenlik duvarı arasındaki bağlantı iki şekilde yapılabilir. Birincisinde güvenlik duvarı ile yönlendirici arasında bir HUB yerleştirilir ve STS de bu HUB'a bağlanır. HUB, herhangi bir portuna gelen bilgiyi diğer portlarına genel yayımla gönderdiği için STS ağa giren ve ağdan çıkan tüm bilgileri dinleyebilir. İkincisinde ise araya bir anahtarlama cihazı yerleştirilir. Yönlendirici, güvenlik duvarı ve STS bu anahtara bağlanır. Yönlendiriciden güvenlik duvarına bilgi aktaran port STS'ye aynalanır (*mirroring*). Bu şekilde yönlendiriciden çıkan tüm bilgiler STS'ye gönderilmiş olur. STS de gelen paketleri inceleyerek bir saldırı varsa gerekli uyarıları yapar.



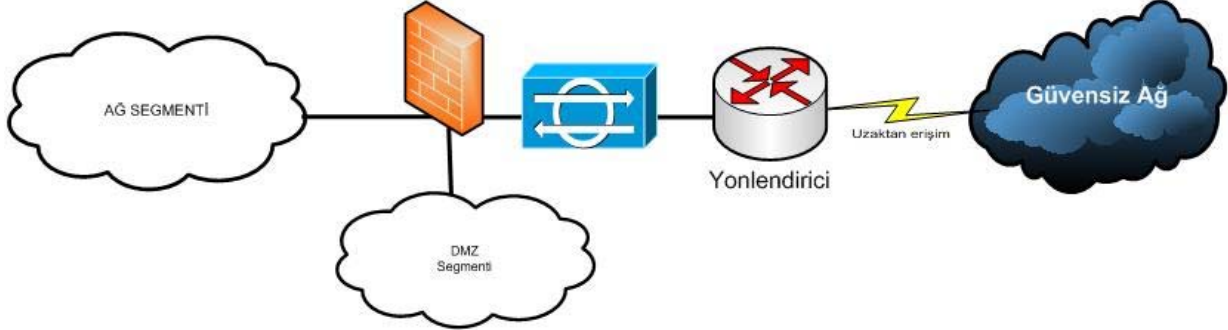
Şekil 4-7 Çok noktadan dinleme yapan bir saldırı tespit sistemi kullanımı

Özellikle hassas bilgi işleyen, saklayan bilgi sistem organizasyonlarında gerek iç ağın gerekse DMZ ağ segmentinin maruz kalacağı saldırıların tespiti önem kazanmaktadır. Bu durumda her bir ağ segmentine ya da kritik olarak önceliklendirilmiş ağ segmentlerine yapılacak saldırıların tespiti gereklidir. Bazı ağ tabanlı saldırı tespit cihazları birden fazla arayüze sahiptirler. Bu türde saldırı tespit sistemleri birden fazla ağa bağlanıp geçen trafik incelenebilmektedir. Aynı iş birden fazla tek arayüze sahip saldırı tespit sistemleri ile de gerçekleştirilebilir. Birden fazla saldırı tespit sistemi kullanmak daha spesifik imzalar kullanılması sebebiyle “false pozitive” log sayısını da azaltacaktır. Örneğin MZ bölgesinde bulunan veri tabanı sunucularının işletim sistemine ve ilgili veritabanı tipine uygun imzalar seçilmesi ile gereksiz log fazlalıkları engellenebilir. Güvenlik duvarının arkasında bulunan bir ağa bağlanan arayüzü (ör: DMZ ağı) sadece ilgili ağa gelen saldırıları tespit edebilmektedir. Birden fazla ağ segmentine kurulacak saldırı tespit sistemleri olası iç saldırılara (bilinçli/ bilinçsiz) karşı farkındalık sağlayacaktır. Örneğin iç ağda bulunan bir PC ye bulaşmış bir “worm” DMZ de bulunan sunuculara sürekli port taraması yapmakta olduğunu düşünelim. Bu durumda sadece güvenlik duvarının dışına bağlanacak saldırı tespit sistemi iç ağ kaynaklı gerçekleşebilecek saldırıları tespit edemeyecektir. Güvenlik duvarının iç ağa veya DMZ ağına bakan arayüzüne bağlanmış bir saldırı tespit sistemi ile bu tür istenmeyen durumların tespiti sağlanabilir.

Saldırı tespit sistemi yönetimi münferit bir bilgisayarla yapılabileceği gibi bir güvenli yönetim ağı oluşturulup, bu ağda konumlandırılan bir bilgisayarla da yapılabilir. Burada amaç yönetim işlevlerinin güvenliğini sağlamak olmalıdır.

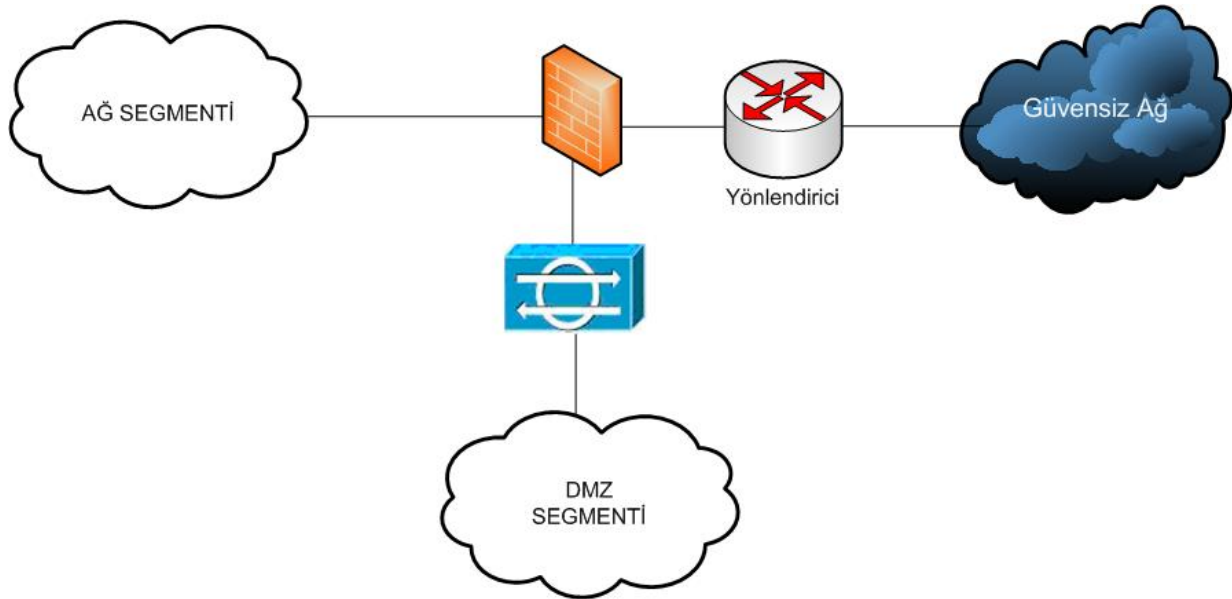
Sunucular üzerine kurulmuş olan saldırı tespit sistemi ise sadece o sunucuya yapılan saldırıları algılar ve gerekli uyarı mesajlarını oluşturur.

4.6 Saldırı Engelleme Sistemlerinin Ağ Mimari Modellerinde Konumlandırılması



Şekil 4-8 Saldırı engelleme sisteminin ağ mimarisindeki yeri -1

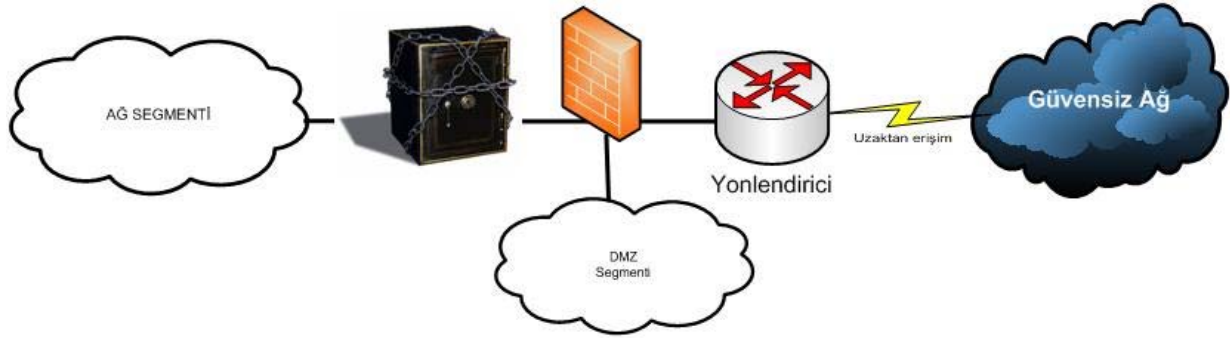
Bu mimari daha çok saldırı engelleme sistemleri için uygulanır. Saldırı engelleme sistemleri köprü (*bridge*) modunda çalışır. Saldırı tespit/engelleme sistemi kendisine gelen paketleri inceleyerek saldırı varsa tespit eder ve gerekli uyarıları verir. Bu tür çalışan cihazların önemli bir özelliği herhangi bir şekilde elektrik kesilmesi ya da arızalanması durumunda girişini ve çıkışını kısa devre ederek ağın iletişimini durdurulmamasıdır. Saldırı Engelleme Sistemi Güvenlik duvarı ile yönlendirici arasında konumlandırılabilir (Şekil 4-8) dışarıdan bakıldığında güvenlik duvarından sonrada konumlandırılabilir (Şekil 4-9).



Şekil 4-9 Saldırı engelleme sisteminin ağ mimarisindeki yeri -2

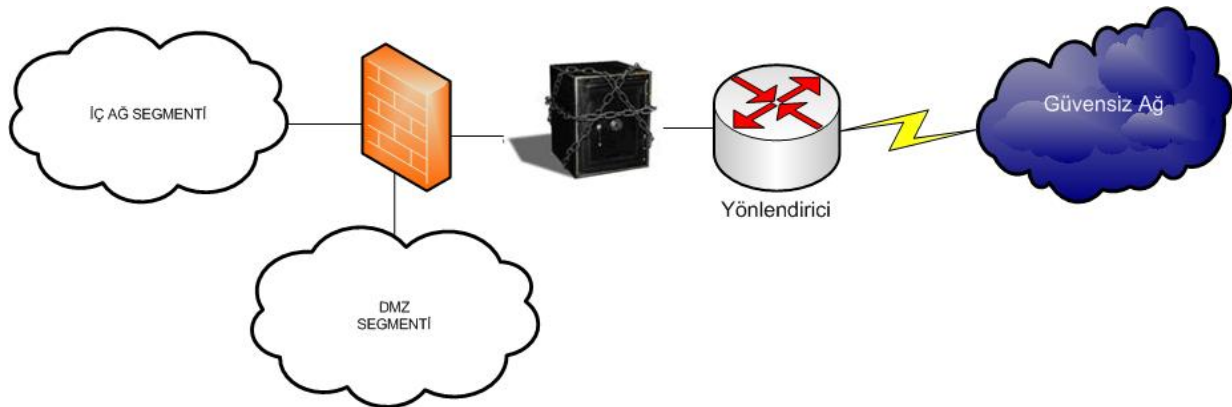
Saldırı Engelleme Sisteminin güvenlik duvarının arkasında konumlandırılması Saldırı Engelleme Sisteminin bazı saldırılara karşı güvenlik duvarı tarafından korunmasını sağlayacaktır. Bununla birlikte önüne konulduğu ağ segmenti (Şekil 4-9 de DMZ olarak görünmektedir) dışında kalan ağ segmentlerinin (Şekil 4-9 de AĞ SEGMENTİ olarak görünmektedir) saldırı engelleme sistemi tarafından korunması mümkün olmayacaktır.

4.7 Sanal Özel Ağ Cihazlarının Ağ Mimari Modellerinde Konumlandırılması



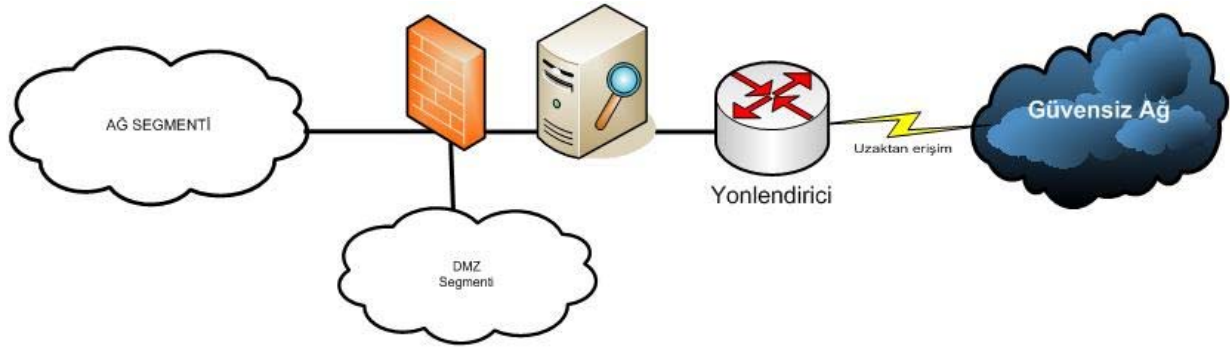
Şekil 4-10 VPN cihazının iç ağ segmentinde kullanımı

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. Bununla birlikte DMZ segmenti ile güvensiz ağ arasında gerçekleşecek trafik VPN cihazı kontrolünde değildir. Tüm ağ segmentlerine ait trafiğin VPN tarafından kontrol edilmesi, politika gereğince gerekli gizlilik kimlik doğrulama işlemlerinin yapılması gerekli olduğu durumlarda Şekil 4-11 daki bir mimari tercih edilebilir.



Şekil 4-11 VPN cihazının güvenlik duvarı dışında kullanımı

4.8 İçerik Kontrolcüsünün Ağ Mimari Modellerinde Konumlandırılması



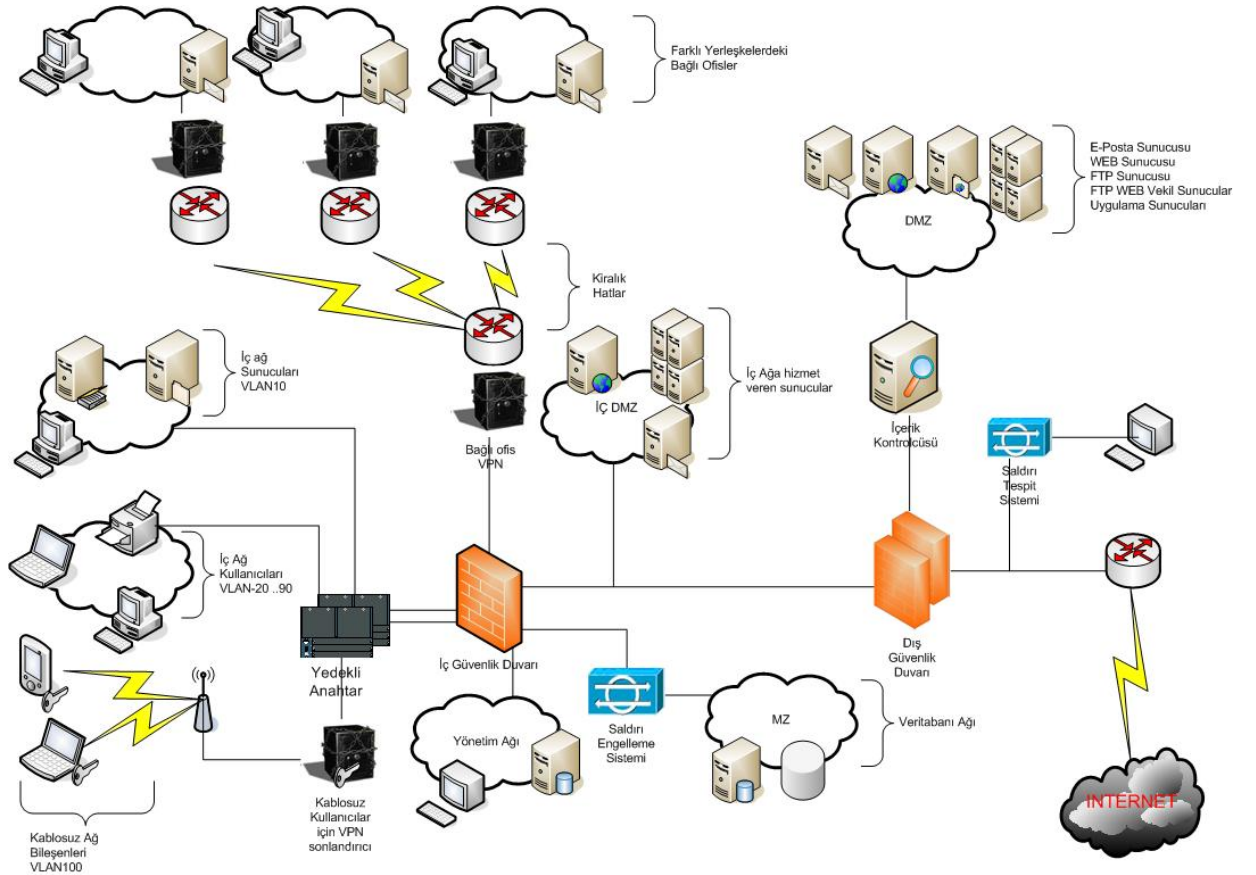
Şekil 4-12 İçerik kontrolcüsünün ağ mimarisindeki yeri

İçerik kontrolcüsü ağa gönderilen zararlı içeriklerin engellenmesini amaçlamaktadır. Bu içerik kontrollerini http, ftp, smtp ve POP3 protokolleri için yapmaktadır. İçerik kontrolcüsü yazılım tabanlı veya donanım tabanlı olabilir. Yalnız başına ya da güvenlik duvarı ile entegre bir şekilde çalışabilir.

4.9 Çok Sayıda Güvenlik Cihazı İçeren Bir Mimari Model

Bundan önceki kısımlarda her bir güvenlik ürünü için ayrı ayrı mimari modeli verilmiş bu modeller üzerinde açıklamalar yapılmıştır. Aşağıdaki mimari modelinde de kurumsal bir ağ için birçok güvenlik önleminin bir arada kullanıldığı bir model örnek olarak verilmiştir. Bu mimari modeli ve diğer mimari modelleri tavsiye niteliğindedir. Her organizasyon kullandığı teknolojiye, kullandığı yazılım, donanım envanterine, işlediği bilgi hassasiyet seviyesine ve iş hedeflerine bağlı olarak kendisi için en uygun mimari modelini kendisi belirlemelidir.

Organizasyonda bilgi güvenliği için yapılacak risk analizi çalışmaları, organizasyonun o anki durumunu sergileyecektir. Bazı durumlarda organizasyonda yapılan işin sürekliliği için belirlenen risklerde, bazı durumlarda ise bilginin gizliliği için tespit edilen risklerde kabul edilebilir seviyenin üzerinde sonuçlarla karşılaşılacaktır. Erişilebilirlik /kullanılabilirlik ile ilgili yapılacak iyileştirmelerde yedekli yapıdaki sistemler kullanılması, gizlilik ve bütünlükle ilgili alınması gereken önlemlerde ise kriptografik önlemler alınması tavsiye edilmektedir.



Şekil 4-13 Çok Sayıda Güvenlik Cihazı İçeren Bir Mimari Model

KAYNAKÇA

- [1] Mark Levitt and Brian E. Burke, *Choosing the Best Technology To Fight Spam*, IDC, April 2004
- [2] <http://www.commtouch.com/documents/040429_IDC_Choosing%20the%20Best%20AS_Technology.pdf>
- [3] *CISSP: Certified Information Systems Security Professional Study Guide 2nd Eddition*, Ed Tittel, James Michael Stewart, MikeChapple
- [4] Joseph Steinberg, *SSL VPN Security*, Whale Communications, 16 Mayıs 2003