Bilgi Güvenliği ve Kriptografi

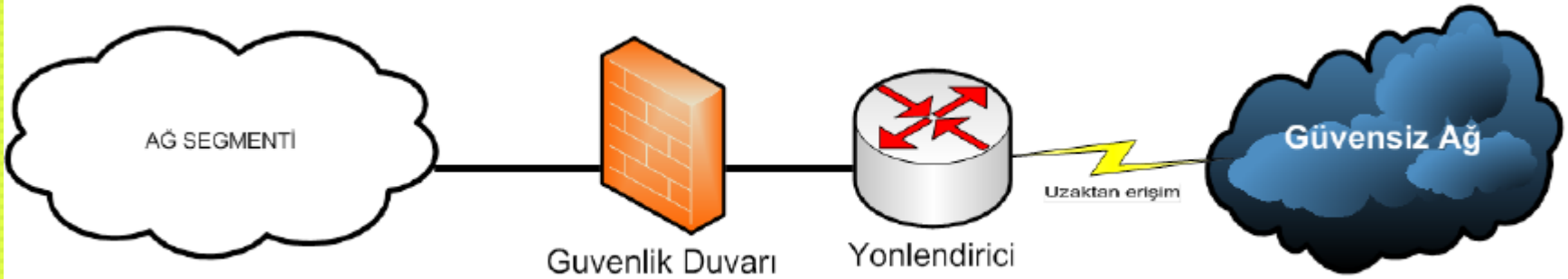
Temel Güvenlik Teknolojileri ve Güvenli Ağ Mimarileri

- Bu bölümde genel olarak ağ güvenliğini sağlamaya yönelik kullanılan araçlar ve protokoller ele alınacaktır.

- **GÜVENLİ AĞ MİMARİLERİ**

Tek Güvenlik Duvarı

- Tek güvenlik duvarı mimarisi tasarımı küçük veya orta büyüklükteki bilgisayar ağları veya içerisinde gizli bilgilerin bulunduğu ağlar için tasarlanmıştır. **Bu tip mimari tasarımlarda dış ağlara hizmet veren sunucu 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.



Tek Güvenlik Duvarı

Tek Güvenlik Duvarı

- Tek güvenlik duvarının kullanıldığı mimari topolojilerde ağ trafiği yüksek seviyelerde ise kullanılacak güvenlik duvarı durumsal güvenlik duvarı olarak seçilmelidir.

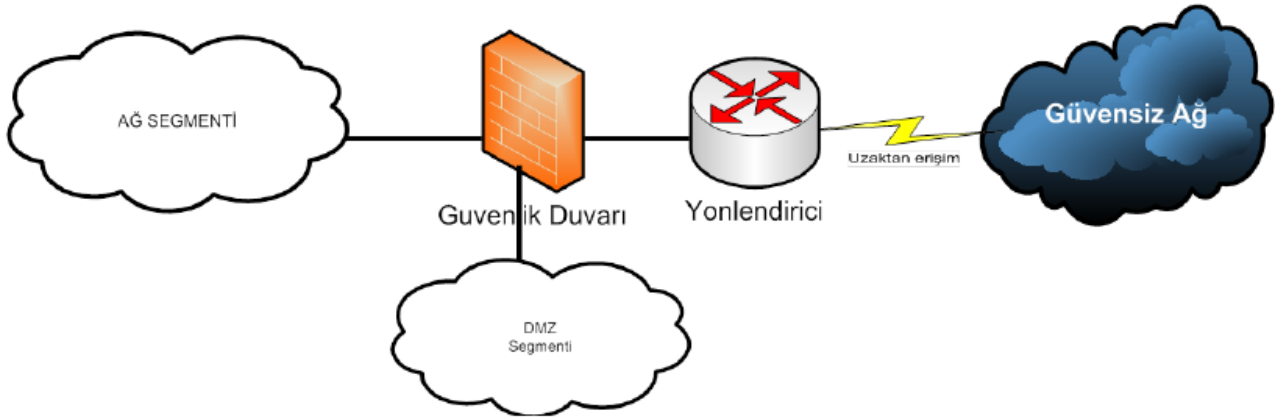
- Durumsal güvenlik duvarı OSI referans modelinin oturum katmanında hizmet verdiğinden uygulama seviyesinde güvenliğin sağlanması amacıyla eğer mümkünse güvenlik duvarı ile birlikte vekil sunucular da kullanılmalıdır.

Tek Güvenlik Duvarı ve DMZ

- Bu mimaride ağda bir yönlendirici ve bir güvenlik duvarı bulunmaktadır. Bu mimari dış dünyaya hizmet veren sunucuların bulunduğu ağlarda tercih edilmelidir. Kullanılan güvenlik duvarının üç tane ağ ara yüzü vardır. Bu ağ ara yüzleri 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 (internet) servis verilmez. Mimari topoloji içinde güvenlik derecesi en yüksek bölümdür. DMZ ağı, iç ağ bölümüne ve dış ağ bölümüne hizmet veren sunucuların oluşturduğu bölümdür. Güvenlik duvarı bu farklı güvenlik seviyesine sahip ağlar arasındaki trafiği düzenleyerek ağın güvenli ve yüksek performanslı olarak çalışmasını sağlar.

Tek Güvenlik Duvarı ve DMZ

- Arındırılmış Bölge" anlamına gelen **DMZ** (**DeMilitarized Zone**), internetten erişilmesini istediğiniz yerel bir bilgisayarınızın tüm portlarını açarak sınırsız erişilmesine izin verir Genellikle, dışarıdaki bir ağdan kullanıcılarına hizmet veren herhangi bir servis DMZ içerisine konumlandırılır. Bu servislerden en yaygını web sunucuları, posta sunucuları, FTP sunucuları, ve DNS sunucularıdır.



Tek güvenlik duvarı ve tek DMZ'den oluşan mimari

Tek Güvenlik Duvarı ve DMZ

- Bilgisayar güvenliği'nde, bir **DMZ** veya **sivil bölge** bir kuruluşun dış servislerini içeren ve bu servisleri daha büyük güvensiz bir ağa (genellikle internet) maruz bırakan fiziksel veya mantıksal bir alt ağdır. . Bir DMZ'nin amacı bir kuruluşun Yerel Alan Ağı (LAN)'a ek bir güvenlik katmanı eklemektir; dışarıdaki bir saldırganın ağın herhangi başka bir bölümünden ziyade yalnızca DMZ içindeki ekipmana erişimi vardır.
  - Web sunucuları, bazı uzman servisler sağlamak için içerideki bir veritabanıyla iletişim kurmaya ihtiyaç duyabilir. Veritabanı sunucusu alenen erişilemez ve hassas bilgi içerebildiğinden dolayı DMZ içinde olmamalıdır. Genellikle, web sunucusunun içerideki veritabanı sunucusuyla doğrudan iletişim kurmasına müsaade edilmesi iyi bir fikir değildir. Bunun yerine, veritabanı sunucusu ve web sunucusu arasındaki iletişimde bir vasıta görevi gören bir uygulama güvenlik duvarı kullanılabilir.
  - E-postanın gizli doğasından dolayı, DMZ içerisinde e-posta saklamak kötü bir fikirdir, ve ayrıca orada kullanıcı veritabanı saklamak da kötü bir fikirdir. Onun yerine, DMZ içindeki gizli bir alanda (internetten erişimi olmayan ama e-posta sunucusundan erişim yapılabilen bir alan) bulunan içerideki bir e-posta sunucusunda e-posta saklanmalıdır.

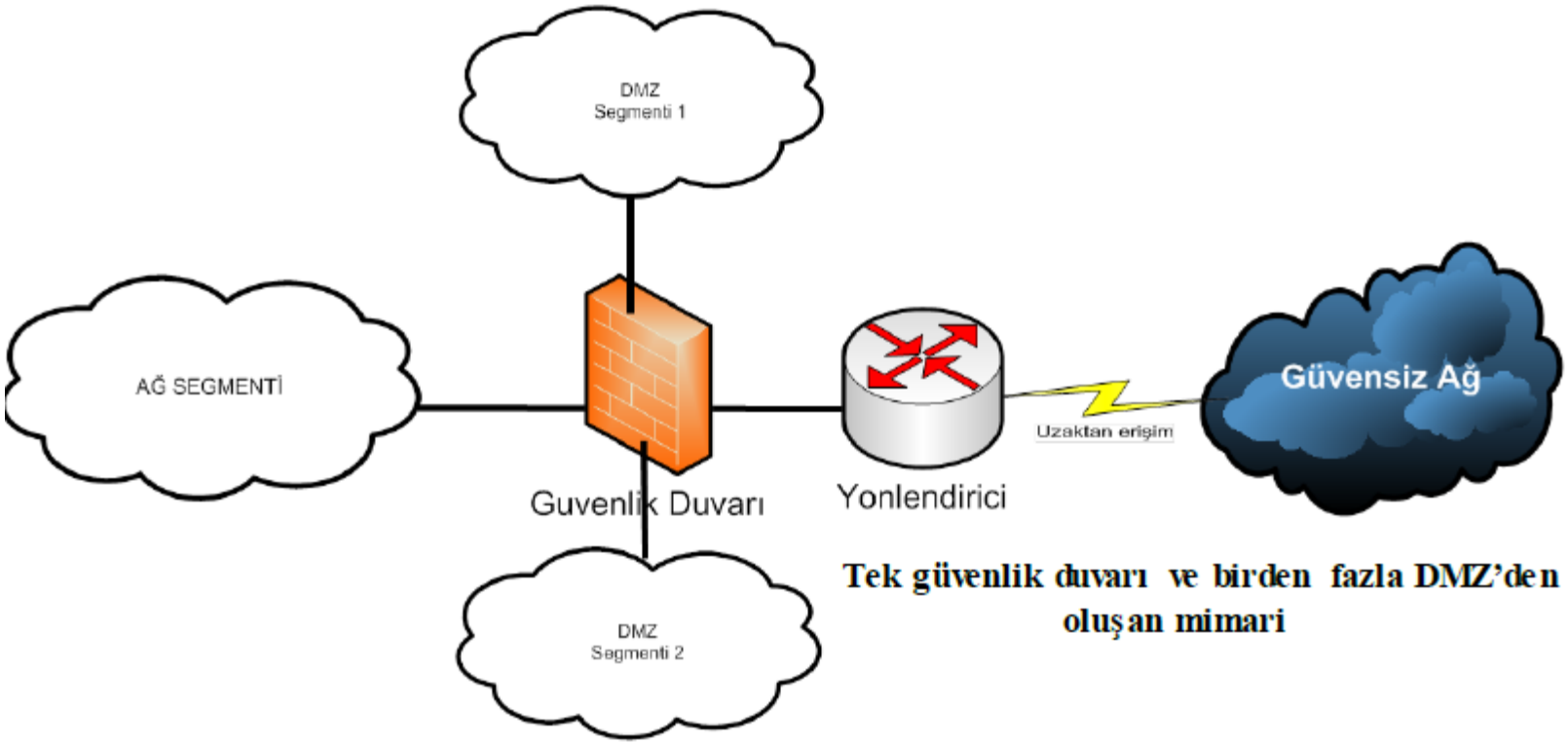
Tek Güvenlik Duvarı ve DMZ

- Bir iş ortamında; güvenlik, yasal uyum ve gerekçe takibi yapabilmek için DMZ içerisinde bir vekil sunucu da kurulması önerilir. Bunu yapmanın aşağıdaki yararları vardır:
  - İçerideki kullanıcıların (genellikle işçilerin), internet erişimi yapmaları için bu vekil sunucuyu kullanmalarını mecbur kılar. Kullanıcıların, doğrudan internette gezinmelerine ve DMZ korumalarını atlatmalarına izin verilmemiş olur.
  - Şirketin, internet bant genişliğinden tasarruf etmesine imkân sağlar çünkü web içeriğinin bir kısmı vekil sunucu tarafından önbelleğe alınmış olabilir.
  - Kullanıcı aktivitelerini izlemek ve kaydetmek için ve yasal olmayan içeriğin işçiler tarafından download veya upload edilmediğinden emin olmak için sistem yöneticisine imkân sağlar. Örneğin birçok Avrupa Birliği ülkesinde bir şirket yöneticisi, işçilerinin aktivitelerine karşı sorumludur.

Tek Güvenlik Duvarı ve Birden Fazla DMZ

- Bu mimaride ağda bir yönlendirici ve bir güvenlik duvarı bulunmaktadır. Bu mimari farklı güvenlik seviyesine sahip birçok ağın olduğu durumlarda uygulanır. Bu mimaride iç ağ segmenti ağ kullanıcılarına hizmet vermektedir. Gerek iç ağ kullanıcıları için gerekse dış ağdan gelecek bağlantı istekleri için farklı güvenlik seviyesine sahip iki adet DMZ ağı oluşturulmuştur. Örneğin bu topolojide *DMZ segment 1* sadece iç ağ kullanıcılarına hizmet veren sunucuların bulunduğu bir ağ, *DMZ segment 2* ise dış ağ kullanıcılarına hizmet veren sunucuların bulunduğu bir ağ olabilir.

Tek Güvenlik Duvarı ve Birden Fazla DMZ



Tek güvenlik duvarı ve birden fazla DMZ'den oluşan mimari

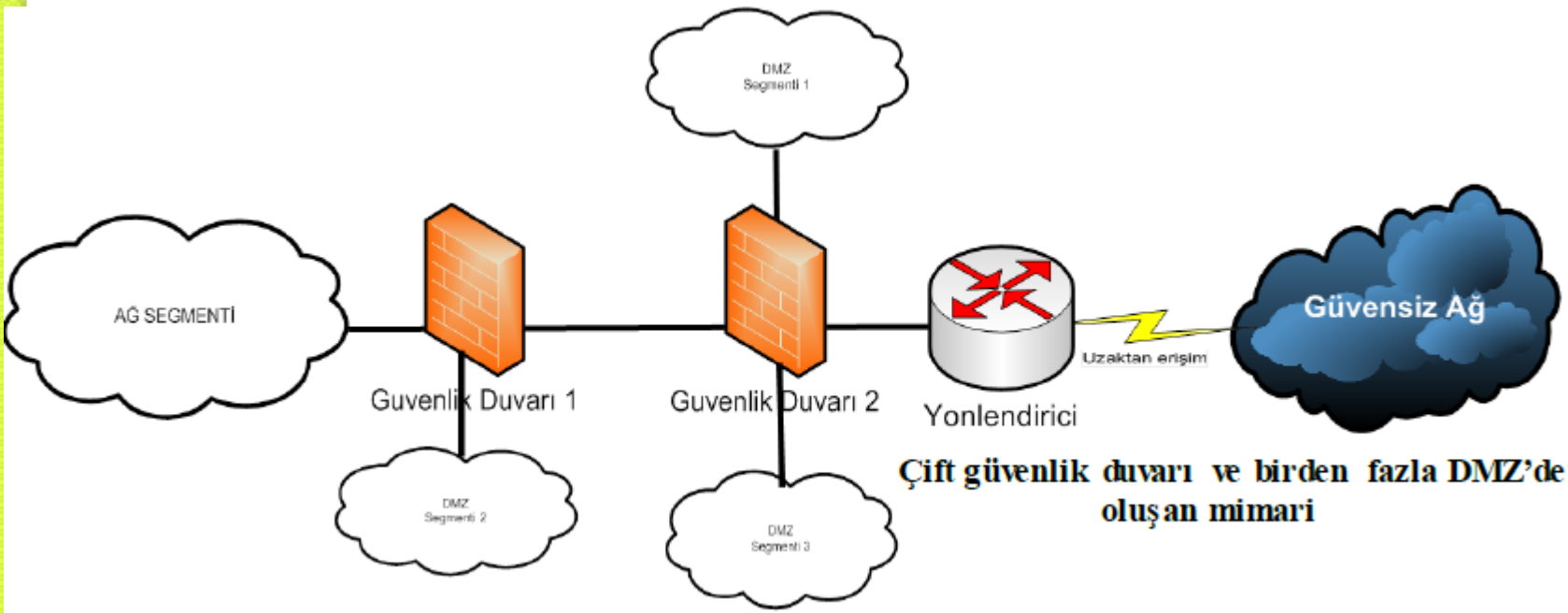
Tek Güvenlik Duvarı ve Birden Fazla DMZ

- Bu mimaride genellikle iç ağda, kullanıcı bilgisayarları, dosya sunucu ve etki alanı sunucusu bulunur. İç ağ kullanıcıları birbirleriyle haberleşir ve dosya paylaşımlarını bu ağ içerisinde yaparlar. İç ağ kullanıcı bilgisayarlarının kontrollü olarak erişmesi gereken ve iç ağa hizmet veren veritabanı, e-posta, web sunucuları *DMZ segment 1*'de konumlandırılmalıdır. Dış ağ kullanıcılarına hizmet veren veritabanı, e-posta, web vb... sunucular *DMZ segment 2*'de yer alırlar. Bu üç ayrı ağ segmentinin her birinin güvenlik seviyesi farklı olur. Böylece farklı güvenlik seviyesine sahip ağlar oluşturulur.

Çift Güvenlik Duvarı ve Birden Fazla DMZ

- 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 yazılımın 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 arttırmanın yanında çok sayıda DMZ bölgesi oluşturma ve her birinde farklı güvenlik seviyesi elde etmeyi sağlamaktadır.

Çift Güvenlik Duvarı ve Birden Fazla DMZ



Çift güvenlik duvarı ve birden fazla DMZ'den oluşan mimari

Çift Güvenlik Duvarı ve Birden Fazla DMZ

- 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.

Yedekli Yapıda Güvenlik Duvarından Oluşan Mimariler

- Ağ bilgi akışı sürekliliğinin ya da performansın önemli olduğu durumlarda yedekli yapıda güvenlik duvarı kullanılır. Bu yapıdaki güvenlik duvarları aktif-pasif ya da aktif-aktif çalışabilirler.

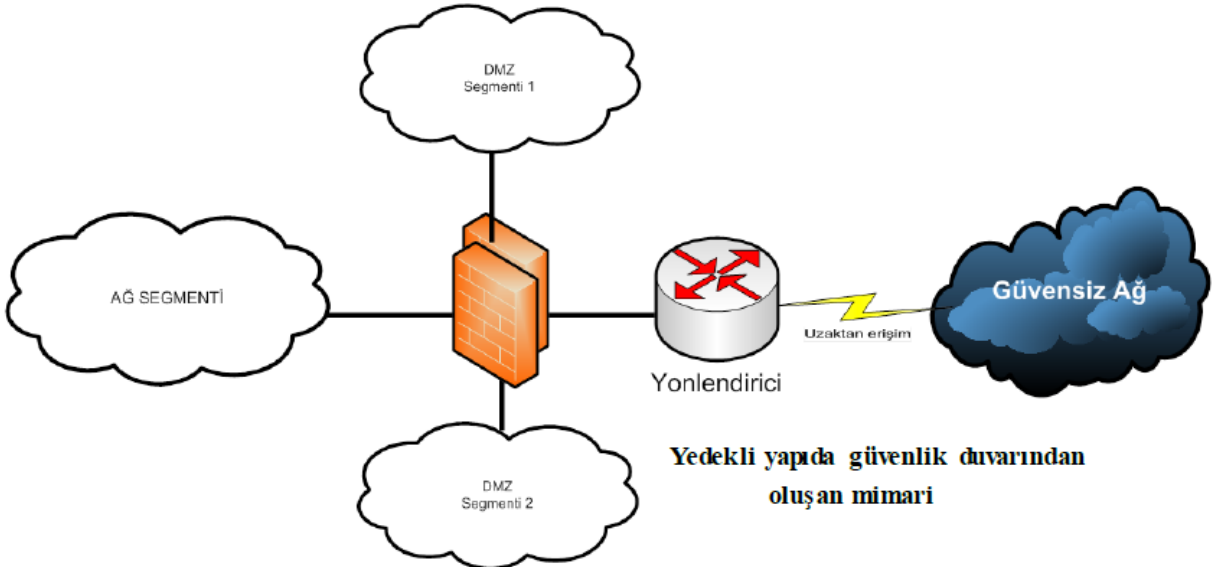
- Aktif-pasif yapıda herhangi bir anda güvenlik duvarlarından sadece bir tanesi çalışır. Çalışmayan güvenlik duvarı diğerini sürekli kontrol eder ve çalışmadığını anladığında kendisi otomatik olarak devreye girer ve ağda oluşacak muhtemel kesintiyi engeller.
- Aktif-aktif çalışmada ise güvenlik duvarlarının her ikisi birden devrede olur ve hem yük paylaşımını sağlarlar hem de güvenlik duvarlarından biri devre dışı kaldığında diğeri ağ iletişimini sağlar.

Yedekli Yapıda Güvenlik Duvarından Oluşan Mimariler

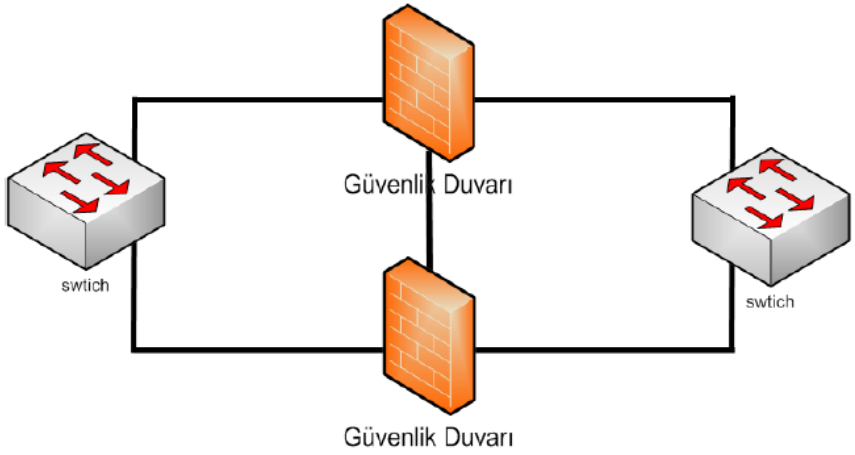
- Aktif-pasif yedekli yapıda güvenlik duvarlarından bir tanesi *master* diğeri ise *slave* olarak ayarlanır. Güvenlik duvarları arasında senkronizasyonu sağlayan bir bağlantı bulunur. Bu bağlantı aracılığı ile *slave* olan güvenlik duvarı *master* olanı sürekli dinler. *Master* olan güvenlik duvarı herhangi bir nedenle servis veremez hale geldiğinde *slave* güvenlik duvarı tüm bağlantıları kendi üzerinden yapar ve ağ iletişimini sağlar. Bu yapıya *failover* mimari de denir.

- Aktif-aktif yedekli yapıda ise güvenlik duvarlarının arasında yine senkronizasyonu sağlayan bağlantı bulunur. Fakat bu yapıda güvenlik duvarlarının her ikisi de sürekli olarak aktiftir. Güvenlik duvarlarından bir tanesi herhangi bir sebepten devre dışı kalırsa diğeri otomatik olarak tüm bağlantıları üzerine alıp ağ iletişimini sürdürür.

Yedekli Yapıda Güvenlik Duvarından Oluşan Mimariler



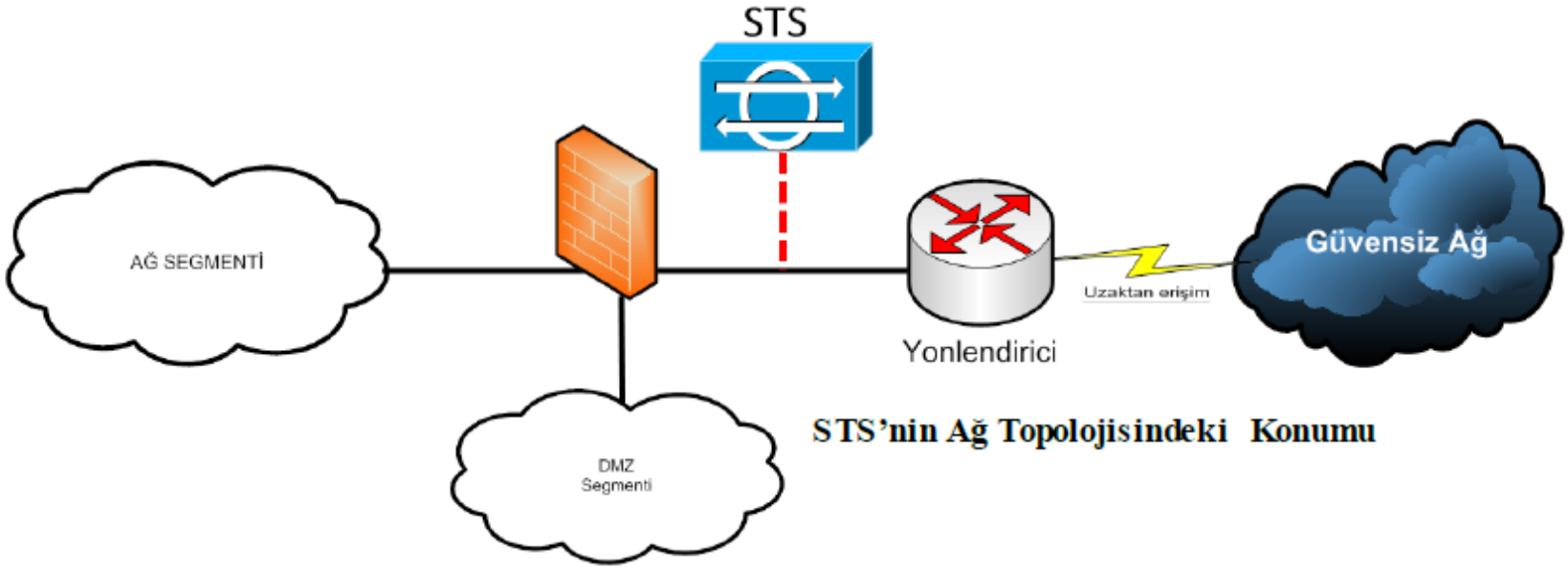
Yedekli yapıda güvenlik duvarından oluşan mimari



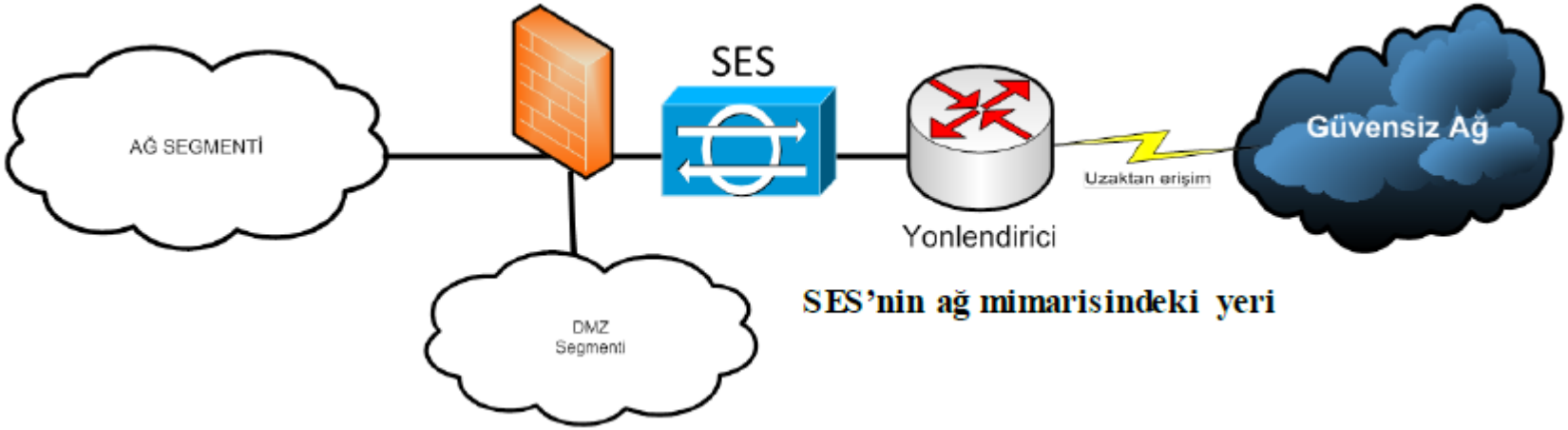
STS ve SES'in Ağ Topolojisindeki Konumu

- Ağa yapılan saldırıların anlaşılabilmesi için saldırı tespit sistemi, yönlendirici ve güvenlik duvarı arasında konumlandırılır. Yönlendirici ve güvenlik duvarı arasındaki bağlantı iki şekilde yapılabilir. Birincisinde güvenlik duvarı ile yönlendirici arasına bir HUB yerleştirilir ve STS de bu HUB'a bağlanır. HUB, herhangi bir portuna gelen bilgiyi diğer portlarına genel yayınla 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.
- Sunucular üzerine kurulmuş olan saldırı tespit sistemi ise sadece o sunucuya yapılan saldırıları algılar ve gerekli uyarı mesajlarını oluşturur.

STS ve SES'in Ağ Topolojisindeki Konumu



STS'nin Ağ Topolojisindeki Konumu



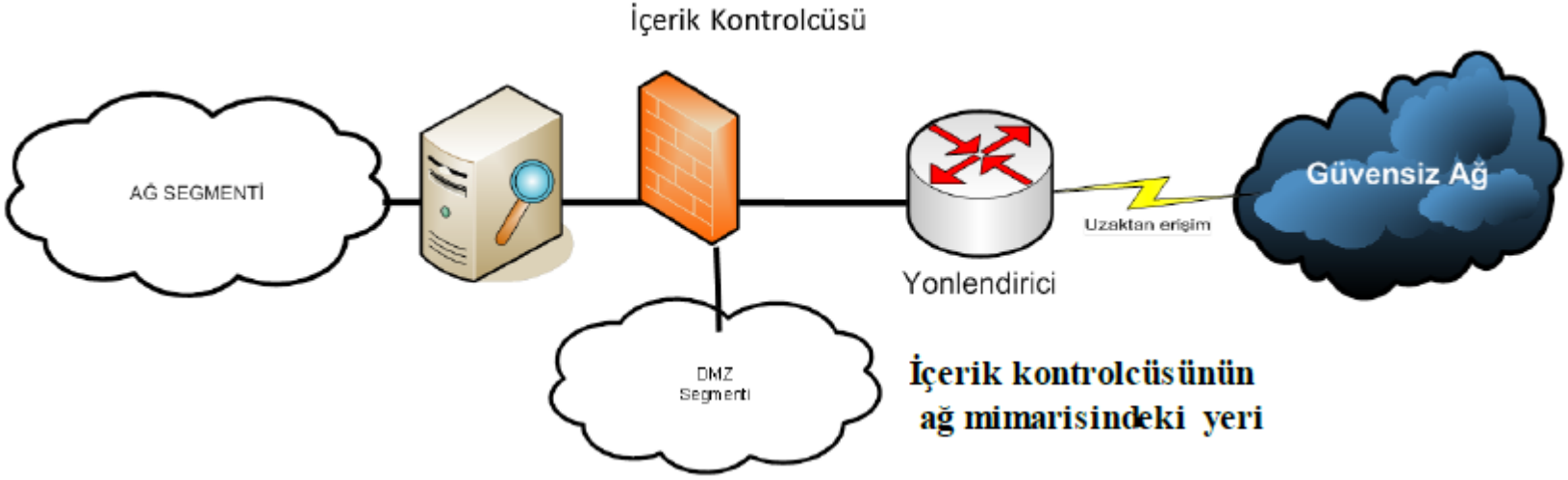
SES'nin ağ mimarisindeki yeri

STS ve SES'in Ağ Topolojisindeki Konumu

- Alternatif 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 durdurmamasıdır. Bu yapı daha çok saldırı engelleme cihazlarında görülür.

İçerik Kontrolcüsünün Ağ Mimarisindeki Yeri

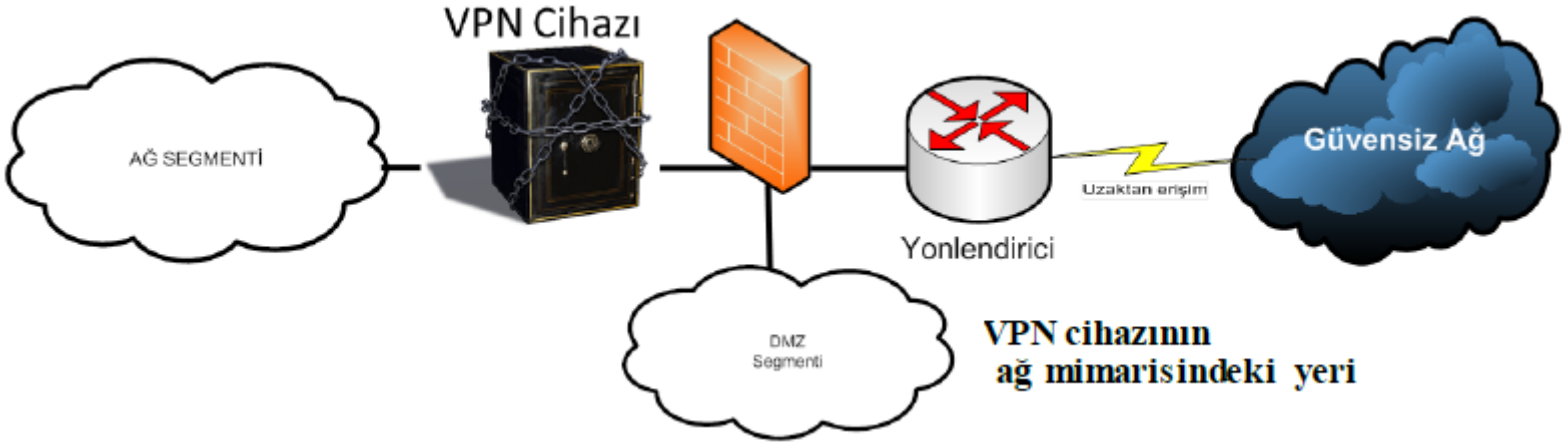
- İçerik kontrolcüsü ağa gönderilen zararlı içeriklerin engellenmesini amaçlamaktadır. Bu içerik kontrollerini http, ftp, smtp ve POP3 protokolleri için yapmaktadır. İçerik kontrolcüsü yazılım tabanlı veya donanım tabanlı olabilir. Yalnız başına ya da güvenlik duvarı ile entegre bir şekilde çalışabilir.



İçerik kontrolcüsünün ağ mimarisindeki yeri

VPN cihazının ağ mimarisindeki yeri

- VPN (Virtual Private Network) cihazları genellikle güvenlik duvarı ve iç ağ arasında yer alır. Bunun yanında ağda ayrı bir VPN cihazı bulundurulması maliyet açışından önemli bir yük getireceği için güvenlik duvarı ve yönlendirici de VPN cihazlarının yaptığı gizlilik, bütünlük, kimlik doğrulama ve inkar edememe fonksiyonlarını yerine getirmektedir. VPN cihazları veriler üzerinde güvenlik sağlamasına karşın kendisini TCP/IP saldırılarına karşı koruyamaz, bu yüzden de güvenlik duvarının arkasında konumlandırılır.
- VPN internete başka bir IP adresi üzerinden bağlanmanızı sağlayan hizmettir. **VPN**, bağlantınızı güvenli hale getirir ve herhangi bir ağa bağlanırken sizin bağlantınızı şifreler ve kimliğinizin bulunamamasını sağlar.



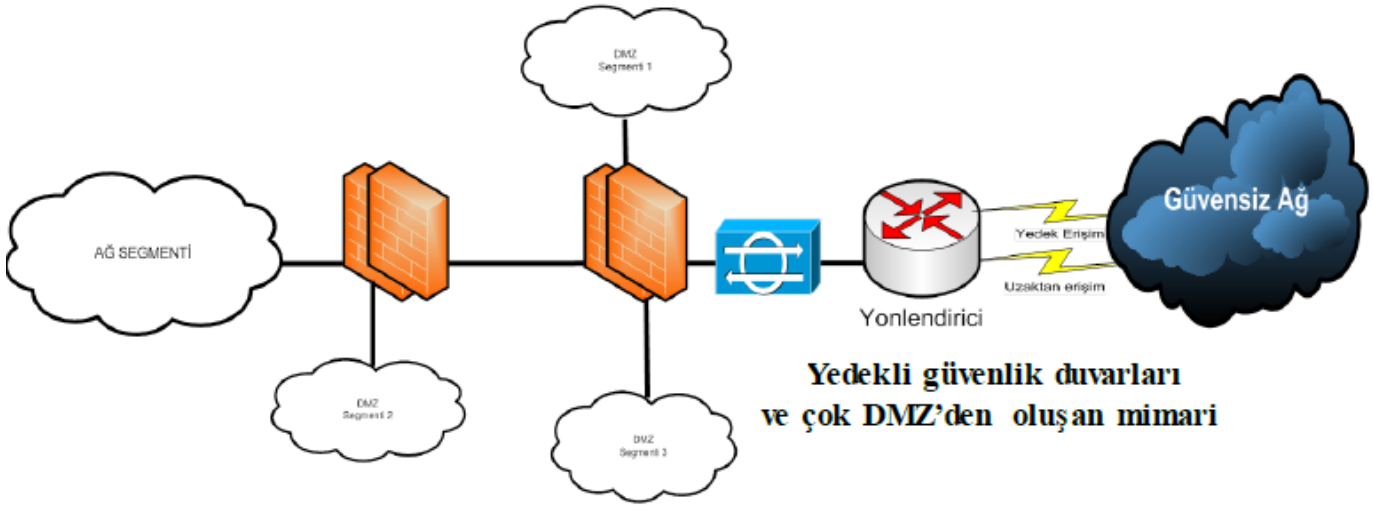
VPN cihazının ağ mimarisindeki yeri

- Eğer ağda çok sayıda VPN bağlantısı oluyorsa özellikle merkezde özel donanımsal VPN konsantratörler (*VPN concentrator*) kullanılır. Bunun yanında performans için özel sunuculara yüklenen VPN yazılımları da mevcuttur. Merkezlerde VPN konsantratör kullanılmasına karşın uzak uçlarda VPN istemci kullanılır.

- VPN cihazları ağdaki tüm trafiği ele alacağı için kullanılacak şifreleme ve özetleme algoritması dikkatlice seçilmelidir.

Yedekli güvenlik duvarları ve çok DMZ'den oluşan mimari

- Bu mimaride yedekli yapıda çalışan güvenlik duvarlarından oluşan ve çok sayıda farklı güvenlik seviyesinde ağ barındıran bir mimari görülmektedir. Bu mimaride ardı ardına iki güvenlik duvarı kullanılarak tek üreticinin sağladığı güvenlik arttırılmış olup ağın dinlenme riski azaltılmıştır. Yönlendirici iki farklı bağlantı ile geniş alan ağına bağlanarak bir bağlantı koptuğunda diğer bağlantı üzerinden iletişimi sürdürecek şekilde yapılandırılmıştır. Güvenlik duvarları kendi aralarında yedekli yapıda olup biri devre dışı kaldığında diğeri ağın iletişimini sürdürecektir.

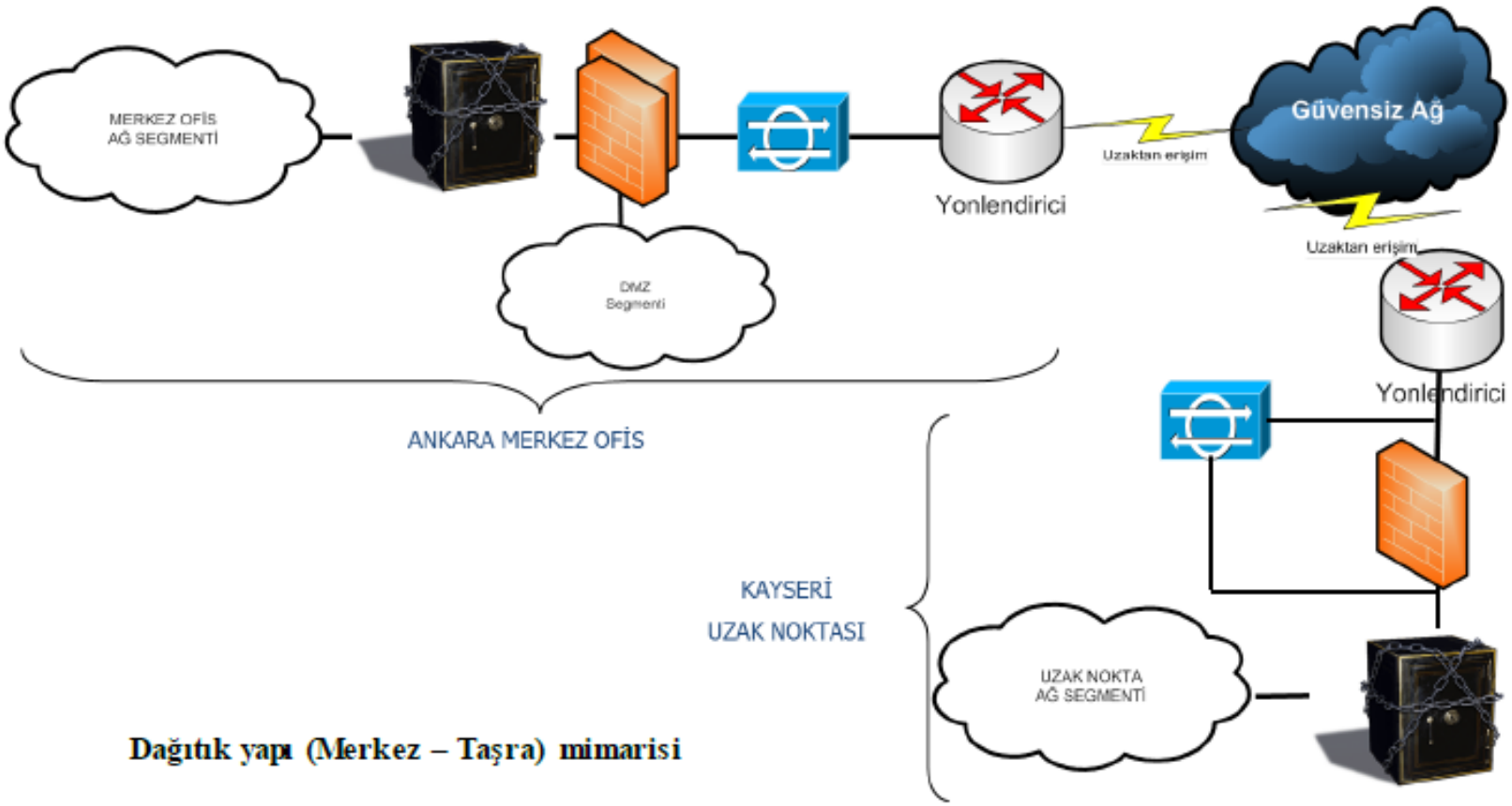


Yedekli güvenlik duvarları ve çok DMZ'den oluşan mimari

Dağıtık yapı (Merkez – Taşra) mimarisi

- Bu mimaride merkez ofis ve bu ofisle birlikte çalışan "uzak nokta" olarak adlandırdığımız bağlı ofis ve bu ofislere ait ağ bileşenleri ve segmentleri görülmektedir. Bundan önceki yansılardan farklı olarak bu yansıda uzak noktada bulunan saldır tespit sisteminin güvenlik duvarının her iki arayüzünü de dinlediği görülmektedir. Dolayısıyla güvenlik duvarının engellediği veya geçirdiği saldırıların izlenebilme şansı doğmaktadır. Merkez ofisle uzak nokta arasında sanal özel ağ kurmak maksadıyla her iki lokasyona da VPN cihazı konulmuş ve üzerindeki politika doğrultusunda merkez ofis segmenti ile uzak nokta segmenti arasında şifreli haberleşmeyi sağlamaktadır. Uzak nokta ile DNZ segmentleri arasındaki trafik şifreli gerçekleşemez.

Dağıtık yapı (Merkez – Taşra) mimarisi



Dağıtık yapı (Merkez – Taşra) mimarisi