Targitas SASE Çözüm Dokümanı

1. Önsöz

1.1 Tanıtım

Geleneksel ağ güvenliği ve erişim çözümleri, günümüzün dinamik iş ortamına ve artan uzaktan çalışma gereksinimlerine etkili bir şekilde yanıt verememekte. Bu bağlamda, SASE teknolojisi değer yaratataktadır. SASE, ağ güvenliği ve erişimi entegre ederek, kullanıcıların her konumdan güvenli ve yüksek hızlı bir şekilde bağlanmasını sağlayan modern bir yaklaşım sunmaktadır. Bu dokümanda, SASE'nin temel prensipleri ve sunduğu avantajlar daha yakından incelenecektir.

Teknik detaylara inildiğinde, SASE'nin temel amacı, kullanıcıların ağa erişimini bir dizi güvenlik hizmetiyle birleştirerek tek bir platformda sunmaktır. Bu hizmetler arasında veri şifrelemesi, tehdit tespiti ve engelleme, kimlik doğrulama ve yetkilendirme bulunur. SASE, bulut tabanlı veya on-premise bir modelle çalışarak ağ erişimini geniş coğrafi bölgelere dağıtarak performansı artırırken, aynı zamanda güvenliği merkezi bir şekilde yönetebilme yeteneği sunar. Bu sayede işletmeler, ağ güvenliğini daha etkili bir şekilde yönetirken kullanıcı deneyimini de iyileştirebilirler.

1.2 Amaç

ISP olarak SASE kullanmanın amacı, güvenli ve ölçeklenebilir bir ağ altyapısıyla daha etkili hizmet sunmaktır. Bu yaklaşım sayesinde, ağımızı merkezileştirerek güvenlik, hız ve esneklik sağlayabiliriz. Maliyet-etkinlik açısından, SD-WAN sayesinde geniş bant ve ucuz İnternet bağlantılarını kullanarak tasarruf edebiliriz. Aynı zamanda, servis esnekliği, güvenlik ve uyum, servis güvenilirliği ve yüksek kullanılabilirlik gibi gereksinimleri karşılamak için tasarlanmış bir çözüm sunar. Şifreleme ve veri güvenliği ile DPI (Derin Paket İncelemesi) gibi güvenlik önlemleri sağlayarak ağ trafiğini korunur. Erişim kontrolü ve ağ segmentasyonu ile güvenliği artırırken, loglama ve denetleme ile olayları merkezi olarak izlenebilir. Sonuç olarak, SASE kullanımı, tek bir merkezden tüm bu özellikleri yönetebilme yeteneği ile bize eksiksiz bir çözüm sunar, iş süreçlerini iyileştirir ve müşterilerimize güvenli, hızlı ve güvenilir bir ağ deneyimi sunmamızı sağlar.

2. İş Gereksinimleri

SASE çözüm tasarımının değerlendirilmesinde kullanılabilecek gereksinimler ile ilgili örnekler aşağıda belirtilmiştir. Bu gereksinimler ISP'nin ve müşterinin ihtiyaçlarına göre uyarlanmalıdır.

- *Ölçeklenebilirlik:*
  SASE yaklaşımı, ISP'nin büyüyen müşteri tabanını desteklemeli ve yeni müşteriler katıldıkça kolayca ölçeklenebilir olmalıdır. Büyük sayıda şube konumunu yönetebilme yeteneğine sahip olmalı ve gelecekteki genişlemeleri karşılamak üzere esneklik sağlamalıdır. SASE yaklaşımı ile, bu tür ölçeklenme ve genişleme ihtiyaçları daha etkin bir şekilde karşılanabilir.
- *Maliyet:*
  SASE (Secure Access Service Edge) yaklaşımı, maliyet-etkinlik açısından değerlendirildiğinde, hem kısa hem de uzun vadeli avantajlar sunar. Bu çözüm, geleneksel ağ güvenliği ve erişim altyapılarını merkezi bir hizmet olarak sunarak, fiziksel donanım maliyetlerini azaltır ve bu da daha düşük başlangıç yatırımları anlamına gelir. Ayrıca, SASE'nin bulut tabanlı doğası, donanım, bakım ve güncelleme masraflarını azaltarak işletme maliyetlerini düşürmeye yardımcı olur. Tek bir merkezi kontrol noktası, ağ güvenliği politikalarını tutarlı bir şekilde uygulayarak yönetimi kolaylaştırır ve operasyonel verimliliği artırır. Bu kapsamlı avantajlar, SASE'nin maliyet-etkin bir güvenlik ve ağ erişim çözümü olarak öne çıkmasını sağlar.
- *Servis Esnekliği:*
  SASE yaklaşımı, hizmet farklılaştırması yönünden de önemli avantajlar sunar. Bu çözüm, ISP'nin müşterilere özelleştirilmiş yönetilen güvenlik hizmetleri sunmasını sağlar. İleri düzey tehdit koruması, güvenli uzaktan erişim, uygulama düzeyinde görünürlük ve kontrol, ayrıca müşteri gereksinimlerine özel olarak tasarlanmış ayrıntılı güvenlik politikaları gibi özellikler sunarak, ISP'nin müşterilere daha iyi bir deneyim sunmasını ve hizmetlerini farklılaştırmasını destekler
- *Güvenlik ve Uyum:*
  SASE yaklaşımı, güvenlik ve uyum açısından da önemli bir avantaj sunar. Bu çözüm, endüstri güvenlik standartlarına ve düzenlemelere uyum sağlamak için entegre edilmiş güvenlik özellikleri sunar. Şifreleme, güvenli kimlik doğrulama ve ağ erişim kontrolü gibi güçlü güvenlik mekanizmaları, kullanıcıların ve cihazların güvenli bir şekilde ağa erişimini sağlar. Ayrıca, merkezi politika yönetimi ile güvenlik politikaları tutarlı bir şekilde uygulanabilir ve denetlenebilir. Bu sayede işletmeler, hem güvenlik gereksinimlerini karşılayabilir hem de düzenlemelere uyum sağlayabilir.
- *Servis Güvenilirliği ve High Availability:*
  SASE yaklaşımı, müşterilere yüksek ağ kullanılabilirliği ve güvenilirliği sağlamak için entegre yedekleme ve bağlantı yedekliliği yetenekleri sunar. Bu sayede ağ arızaları durumunda dahi hizmet kesintileri minimum seviyeye çekilir ve iş sürekliliği sağlanır. İşletmeler, güvenilir bir ağ altyapısı ile operasyonel etkinliği artırabilir ve müşterilere kesintisiz hizmet sunabilirler.
- *Performans Optimizasyonu:*
  SASE yaklaşımı, uygulama performansını optimize etmeli ve trafik yönlendirmesini uygulama öncelikleri ve ağ koşullarına göre dinamik olarak ayarlayarak gerçekleştirmelidir. İş kritik uygulamaları önceliklendirmeli, düşük gecikme süresini sağlamalı ve optimize edilmiş performans için Hizmet Kalitesi (QoS) mekanizmaları sunmalıdır. Merkezi yönetim, ağ trafiğini etkili bir şekilde yönlendirebilme yeteneği ile uygulama performansını en üst düzeye çıkarırken, veri aktarımını en iyi duruma getirir.
- *Merkezi yönetim ve izlenebilirlik:*
  SASE yaklaşımı, ISP için ağ işlemlerini basitleştirmek amacıyla merkezi yönetim ve izleme yetenekleri sunmalıdır. Birleşik bir gösterge paneli sağlamalıdır; yapılandırma, izleme ve raporlama işlemleri için, etkili hizmet sağlama, sorun giderme ve performans analizi yapma imkanı sunarak, ağ operasyonlarını kolaylaştırmalıdır.

- *Hizmet Seviyesi Anlaşmaları (SLAs):*
  SASE çözümü, ISP'nin müşterilere SLA'lar sunma kapasitesini desteklemelidir. Gerekli görünürlığı sağlamalı ve SLA taahhütlerine uyumun izlenebilir olmasını sağlamalıdır
- *Mevcut Sistemle Entegrasyon:*
  SASE çözümü, İSP'nin mevcut ağ altyapısı ve yönetim sistemleriyle sorunsuz bir şekilde entegre olmalıdır. Geleneksel ağ cihazları, güvenlik duvarları, güvenlik sistemleri ve raporlama araçları ile uyumlu olmalıdır; böylece kesintiyi en aza indirirken, sorunsuz bir geçişi sağlayabilir.

3. Güvenlik Durumu

- *Şifreleme ve Veri Güvenliği:*
  SASE teknolojisi kapsamında, SD-WAN çözümü, evrilen siber tehditlere karşı ağı ve müşteri verilerini korumak adına gelişmiş tehdit önleme mekanizmalarını bünyesinde barındırmalıdır. Bu kapsamda, tehlikeleri tespit edip anında engellemek için sızma tespit ve önleme sistemleri (IDS, IPS), antivirüs, webfilter özelliklerin uygulanması gerekmektedir.
- *DPI (Derin Paket İncelemesi):*
  SASE, derin paket inceleme (DPI) filtrelemeleri ile güvenliği sağlamada kritik bir rol üstlenir. DPI, ağ trafiğini OSI katman 7 düzeyinde analiz ederek zararlı içerikleri tespit etmeye yardımcı olur. SASE, bu mekanizmayı kullanarak ağ trafiğini gerçek zamanlı olarak denetler ve kötü niyetli aktiviteleri tespit edip engeller. Bu sayede, gelişmiş tehditlere karşı daha etkin bir koruma sağlanır ve ağa erişim güvenliği sağlamak için gereken adımlar atılmış olur.
- *Erişim Kontrol:*
  SASE altyapısı ve müşteri ağlarına izinsiz erişimi engellemek için sağlam erişim kontrol mekanizmalarının uygulanması gerekmektedir. Bu, çok faktörlü kimlik doğrulama (MFA), rol tabanlı erişim kontrolü (RBAC) ve kritik kaynaklara ve yapılandırma değişikliklerine sadece yetkilendirilmiş personelin erişebilmesini sağlamak için detaylı erişim politikalarını içermektedir. SASE yaklaşımıyla, bu önlemler ağ güvenliğini daha da güçlendirir ve yetkisiz erişimlerin önlenmesine önemli katkıda bulunur.
- *Ağ Segmentasyonu:*
  Ağ segmentasyonu, müşteri ağlarını ve uygulamalarını izole ederek tehditlerin yayılmasını engellemek ve güvenlik ihlallerinin etkisini minimize etmek için elzemdir. SASE çözümü,

güvenli ağ segmentasyonunu desteklemeli ve sanal ağlar veya VLAN'lar (Sanal Yerel Ağ Ağları) oluşturarak müşteri trafiğini izole etmeyi ve segmentler arasında güvenlik politikalarını uygulamayı sağlamalıdır. Bu yaklaşım, SASE'nin temel özelliklerinden biri olarak ağ güvenliğini daha da güçlendirir.

- *Loglama ve Denetleme:*
  Kapsamlı kayıt ve denetim mekanizmaları, güvenlik olaylarını, ağ aktivitesini ve politika ihlallerini yakalayarak analiz etmek için uygulanmalıdır. Güvenlik günlükleri analiz amacıyla merkezi bir şekilde toplanmalı ve proaktif tehdit tespiti, olay yanıtı ve düzenleyici gereksinimlere uyumu desteklemelidir. SASE yaklaşımı ile birlikte, bu tür mekanizmalar ağ güvenliğini artırmanın yanı sıra olaylara etkili ve hızlı bir yanıt verilmesine olanak tanır.
- *Tek Merkezden İzleme ve Yönetme:*
  SASE yaklaşımı, İnternet Hizmet Sağlayıcıları için merkezi yönetim ve izleme yetenekleri sunarak, ağ operasyonlarını kolaylaştırır. Birleşik bir gösterge paneli aracılığıyla yapılandırma, izleme ve raporlama işlevlerini merkezi bir noktada birleştirerek, ağ operasyonlarını daha verimli hale getirir, hızlı yanıt verme sağlar, hata ayıklama süreçlerini hızlandırır ve kolaylaştırır.

4. SASE Çözümü

SASE, ağ güvenliğini ve ağ erişimini bir araya getiren yenilikçi bir yaklaşımdır. Bu konsepte göre, güvenlik ve ağ erişimi bulut tabanlı bir hizmet olarak sunulur. SASE, kullanıcıların ve cihazların her yerden güvenli bir şekilde ağa erişmesini sağlamak için verileri merkezi olarak korurken, gelişmiş güvenlik önlemleri ile ağ trafiğini korur. Bu yaklaşım, ağ sınırlarını ve geleneksel güvenlik altyapısını aşarak, hızlı ve esnek bir şekilde ölçeklenebilir, tehditlere karşı daha dirençli ve düzenlemelere uygun bir güvenlik çerçevesi sunar.

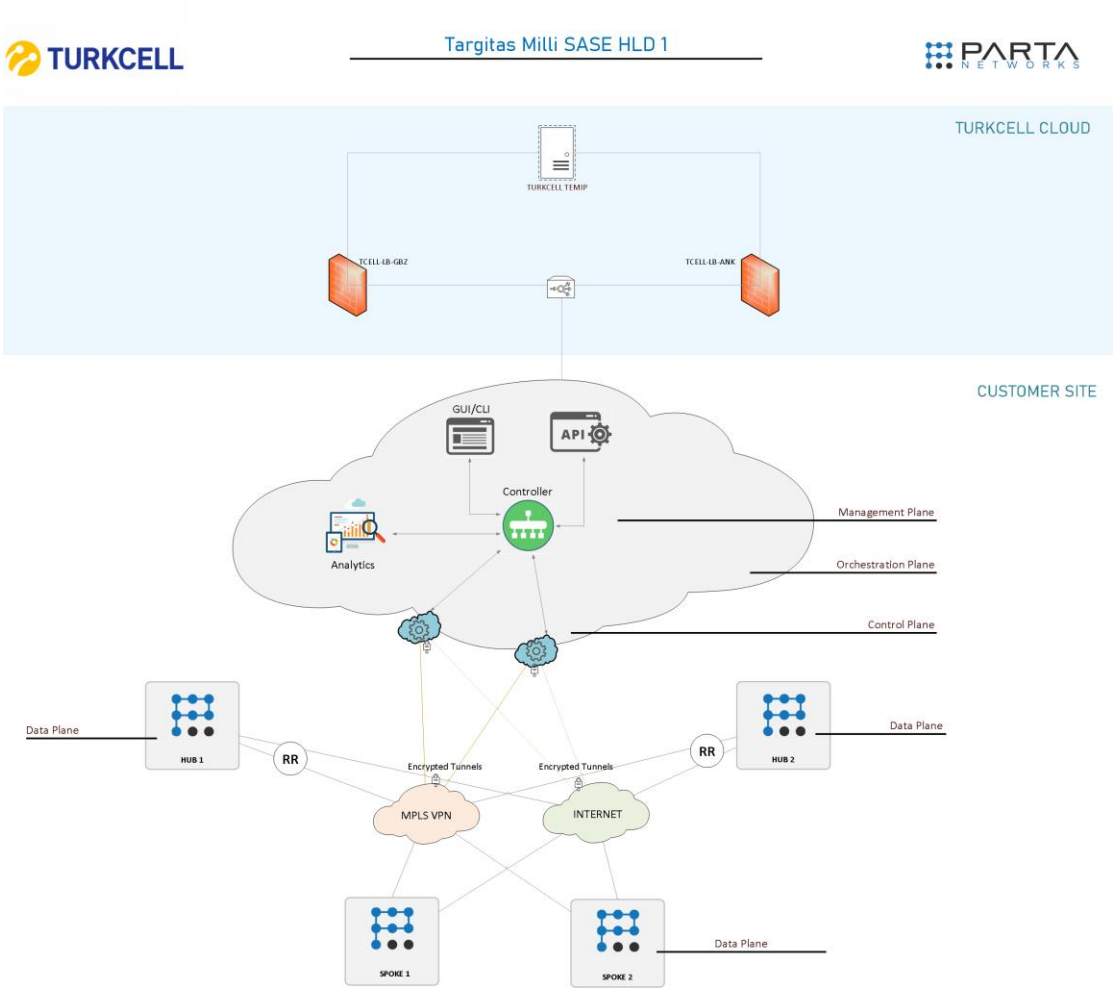
- *Spoke Cihaz:*
  Bu cihazlar, müşteri şube konumları için giriş noktaları olarak işlev görerek ağın kenarında bağlantı ve güvenlik denetimi sağlarlar. MPLS, geniş bant ve hücresel bağlantılar dahil olmak üzere çeşitli bağlantı seçeneklerini desteklerler, bu da esnek ve maliyet-etkin ağ dağıtımlarına olanak tanır. SASE yaklaşımı ile bu cihazlar, ağ erişimi ve güvenliği konularında güçlü bir entegrasyon sağlar.
- *Hub Cihaz:*
  Hub Cihaz, bağlı bulunduğu Spoke cihazlar için Route Reflector görevini üstlenir ve ağ yapısında Spoke cihazların birbirleri ile iletişim kurabilmesi için güvenilir ve verimli bir ortam sağlar. Ek olarak DIA özelliği sayesinde Spoke cihazlarda oluşan istenilen trafiğin Hub cihaz üzerinden internete çıkartılması sağlanır.
- *Controller:*
  SASE Controller cihaz kendisine bağlı uç cihazların tek bir arayüz üzerinden izlenebilmesini ve konfigürasyon gerçekleştirilebilmesini sağlar. Controller, uç cihazlara ait 5651 logları ve konfigürasyon yedeklerini saklama görevini üstlenebilir.
- *Analytics:*
  Uç cihazlardaki trafiğe ait 5651 logları merkezde toplanabilir. Bu verilere ait analiz ve inceleme gerçekleştirilebilir.
- *Turkcell TEMIP:*
  SASE topolojisinde Controller'a ulaşan alarmlar merkezi Turkcell TEMIP'e yönlendirilir.

5. Çözüm Taslağı

5.1 Çözüm Topolojisi

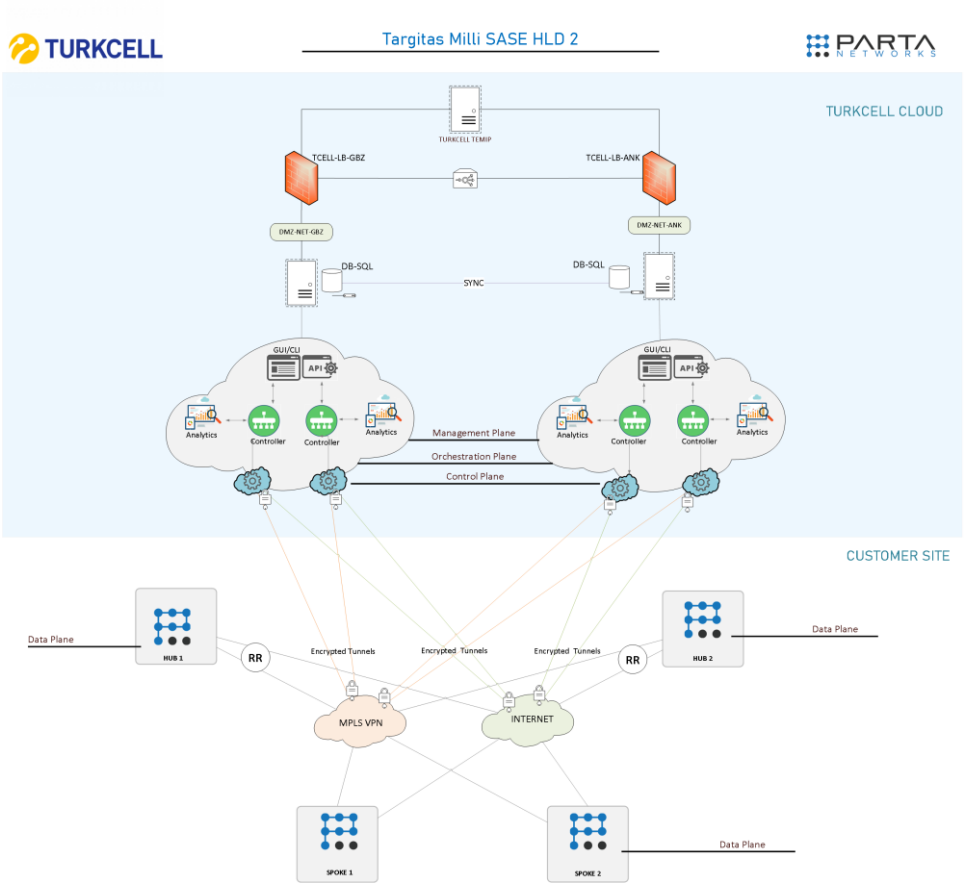
5.1.1 Management Plane Müşteri Yönetiminde

Müşteri, Controller yönetim yetkisine sahiptir. Control, Orchestration ve Management Plane müşteri altyapısında yer almaktadır. Alarmlar Turkcell TEMIP'e iletilmektedir.



5.1.2 Management Plane Turkcell Cloud Yönetiminde

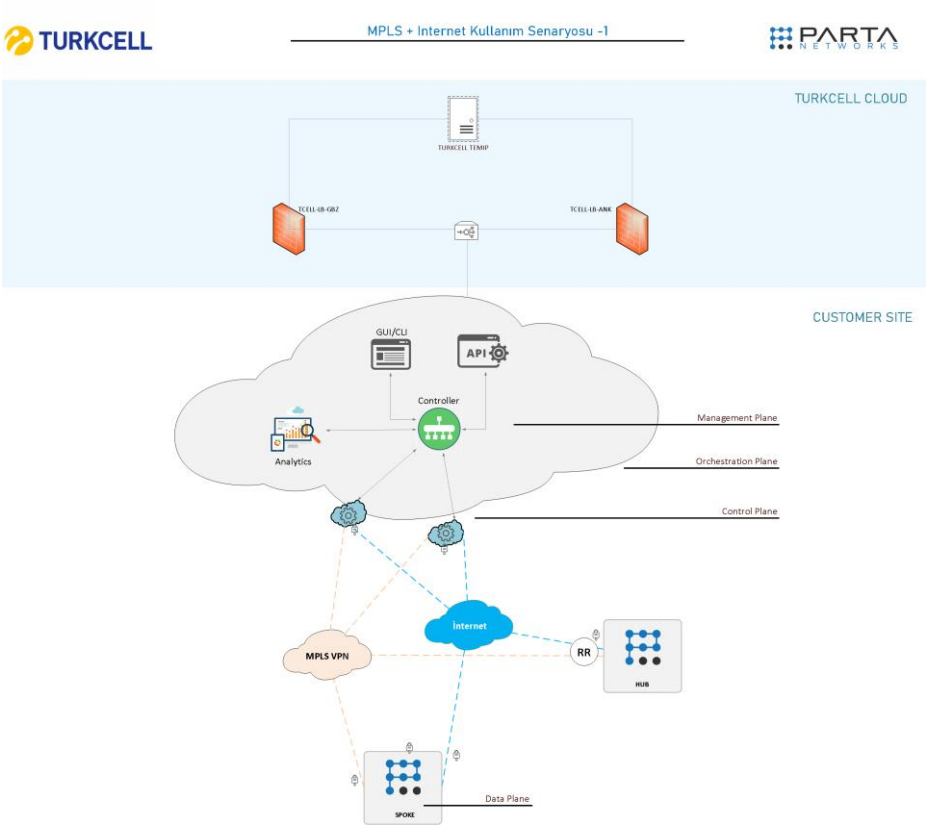
Control, Orchestration ve Management Plane yönetim yetkisi Turcell Cloud tarafında bulunmaktadır.



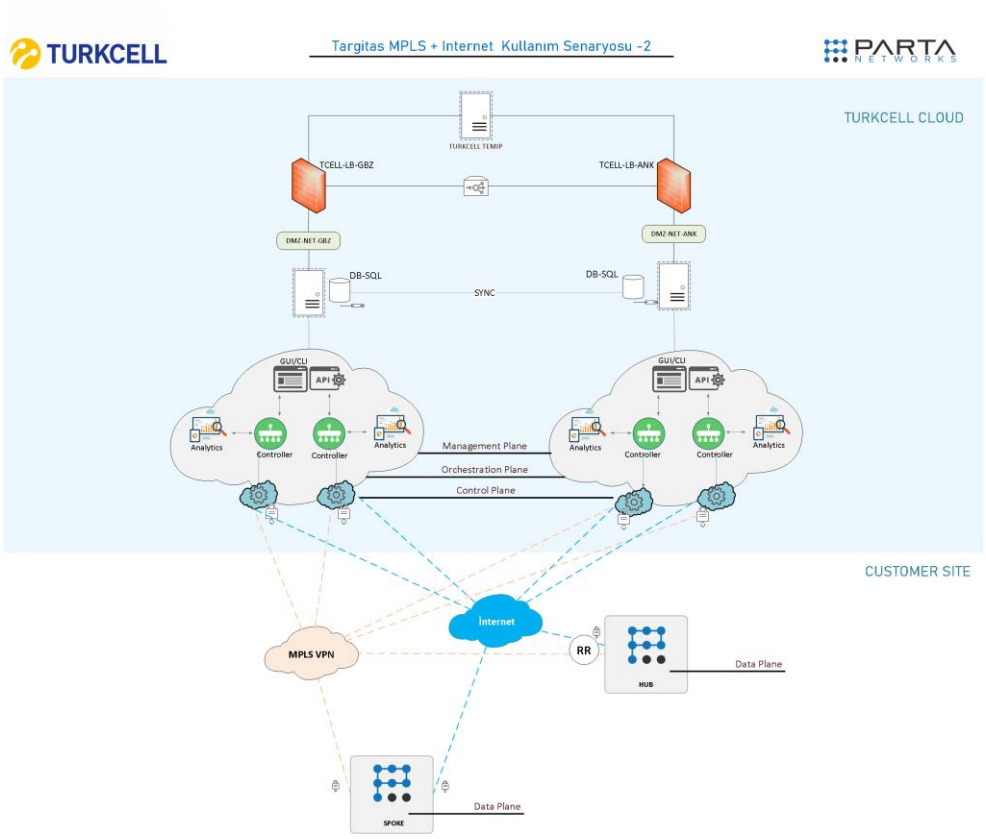
5.2 Kayıt ve Alarm Yönetimi Entegrasyonu

6. Kullanım Senaryoları

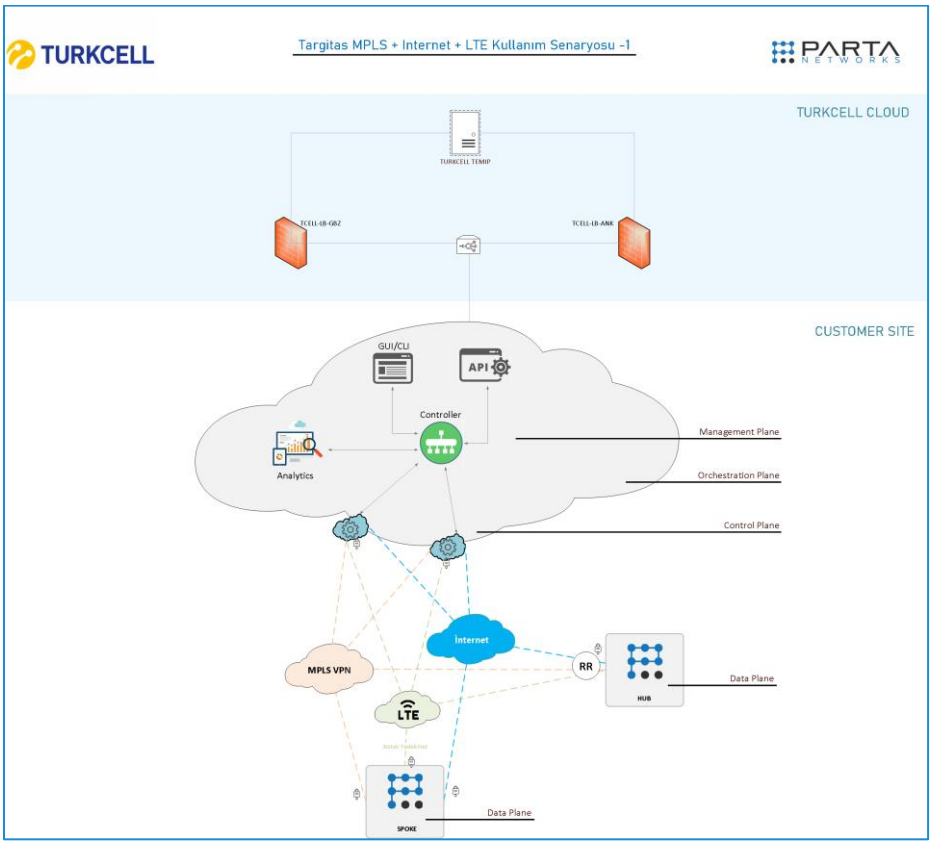
6.1) MPLS + İnternet



- Uç cihazlar arasındaki yerel ağ iletişimi şifreli tüneller üzerinden gerçekleştirilir.
- Her uç cihaz Turkcell MPLS hattına ve bir adet herhangi bir Internet hattına bağlıdır.
- Farklı sağlayıcı ve tür WAN hattı kullanımı destekler.
- Uç cihazlarda birden fazla WAN hattı bulunması durumunda Hub yerel ağına erişimde Load Balance gerçekleştirilebilir.
- Belirli uygulama veya web kategori trafiği belirli WAN hattı ve tünel üzerinden yönlendirilebilir.
- Uç cihazlar Controller tarafından izlenebilir ve yönetilebilir. Controller yönetimi Turkcell Cloud ekibinde veya müşteride olabilir. İki durumda da alarmlar Turkcell TEMIP'e yönlendirilir.

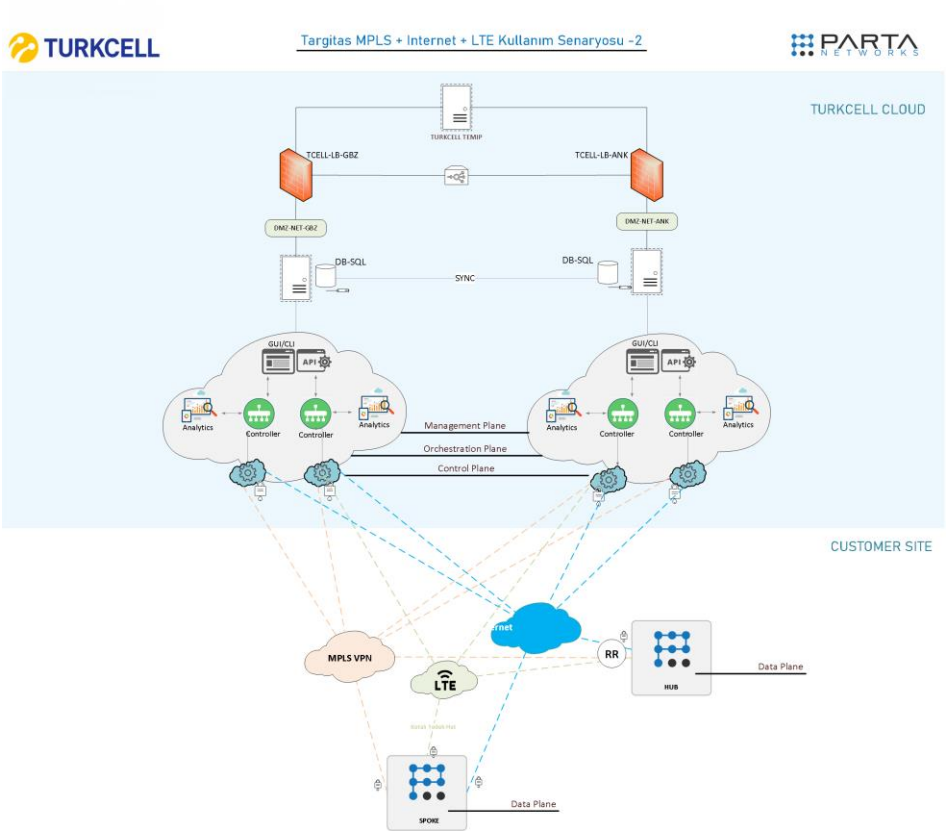


6.2) MPLS + İnternet ve LTE

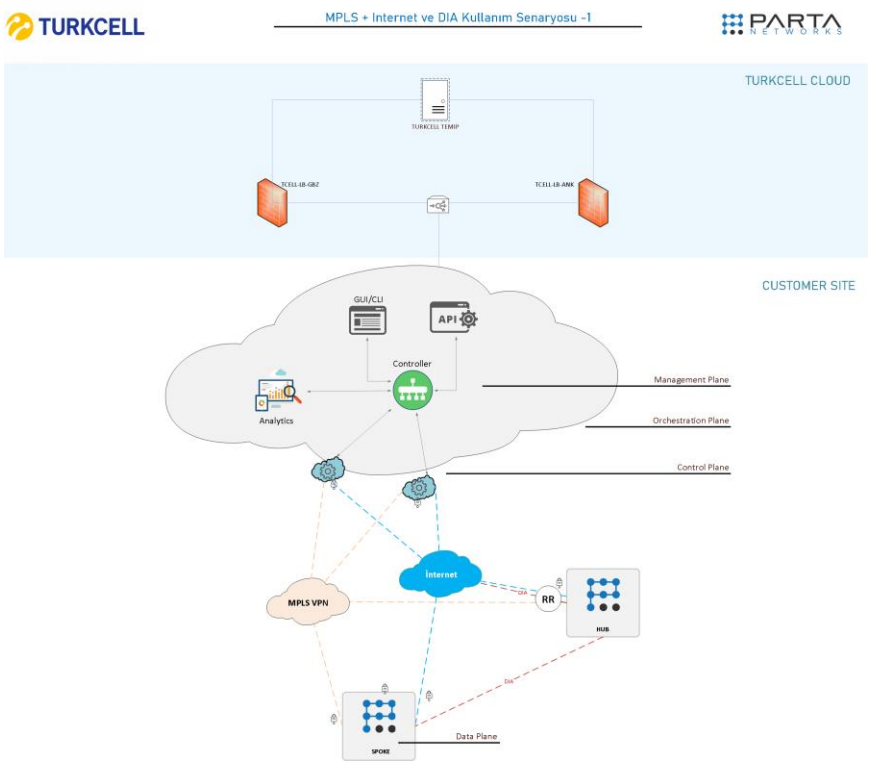


- Uç cihazlar arasındaki yerel ağ iletişimi şifreli tüneller üzerinden gerçekleştirilir.

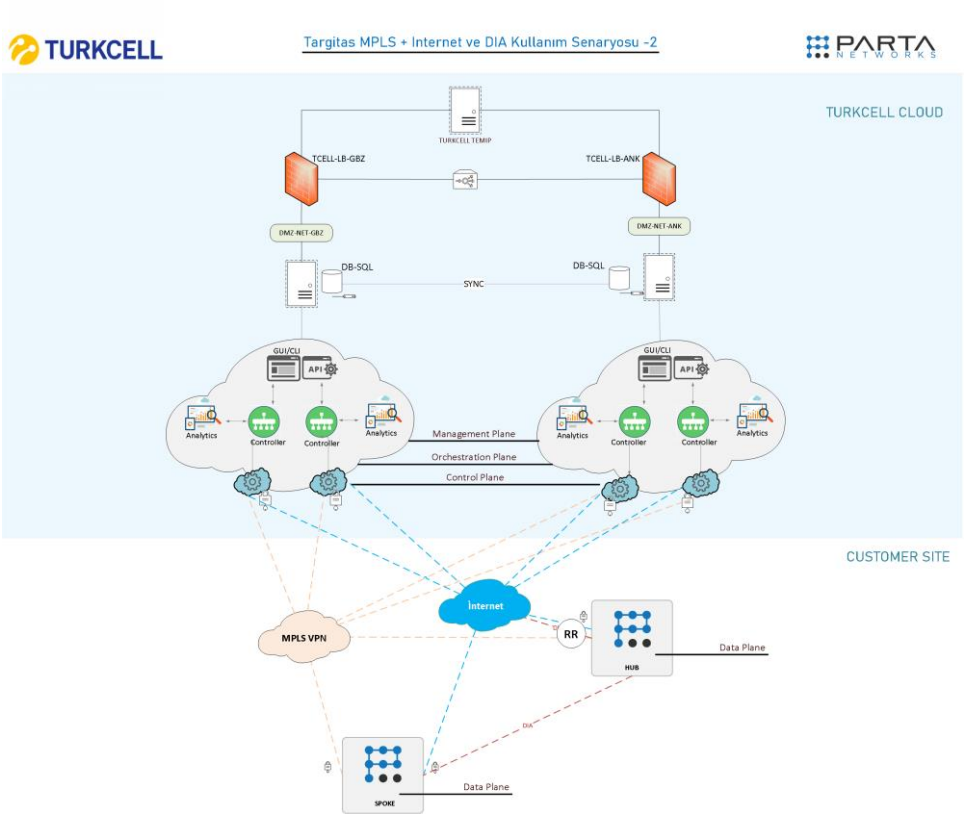
- Farklı sağlayıcı ve tür WAN hattı kullanımı destekler.
- Uç cihazlarda birden fazla WAN hattı bulunması durumunda Hub yerel ağına erişimde Load Balance gerçekleştirilebilir.
- Belirli uygulama veya web kategori trafiği belirli WAN hattı ve tünel üzerinden yönlendirilebilir.
- Uç cihaz, Data veya Management Plane için kotalı LTE yedek hat kullanabilir.
- Tanımlanan SLA sayesinde kota dolumu durumunda LTE hat yenilenme tarihine kadar pasifleşir.
- Uç cihazlar Controller tarafından izlenebilir ve yönetilebilir. Controller yönetimi Turkcell Cloud ekibinde veya müşteride olabilir. İki durumda da alarmlar Turkcell TEMIP'e yönlendirilir.



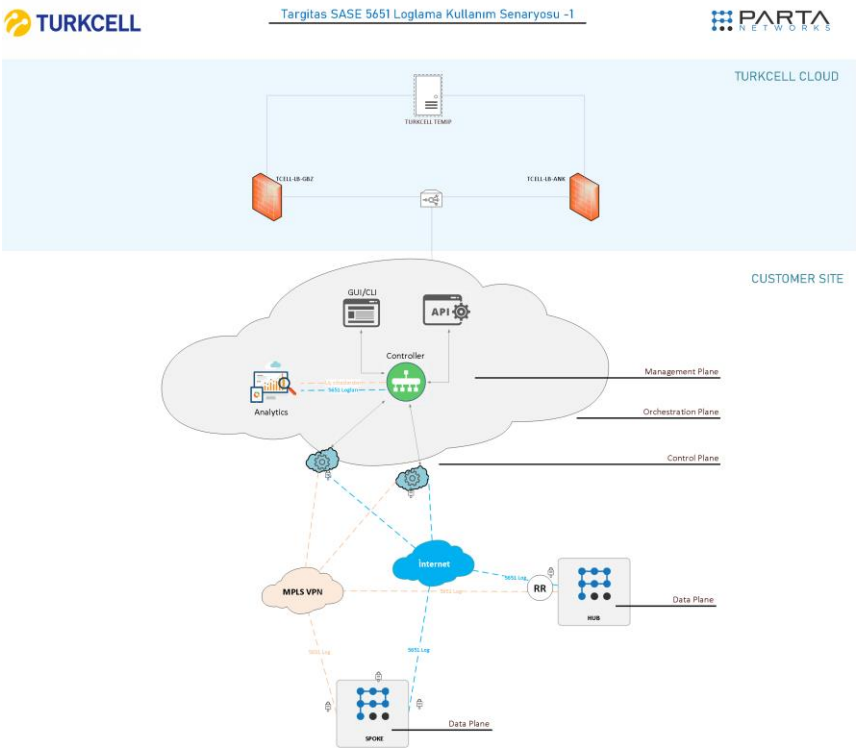
6.3) MPLS + İnternet ve DIA



- Uç cihazlar arasındaki yerel ağ iletişimi şifreli tüneller üzerinden gerçekleştirilir.
- Her uç cihaz Turkcell MPLS hattına ve bir adet herhangi bir Internet hattına bağlıdır.
- Farklı sağlayıcı ve tür WAN hattı kullanımı destekler.
- Uç cihazlarda birden fazla WAN hattı bulunması durumunda Hub yerel ağına erişimde Load Balance gerçekleştirilebilir.
- Belirli uygulama veya web kategori trafiği belirli WAN hattı ve tünel üzerinden yönlendirilebilir.
- Spoke cihazların internet erişimi Hub cihaz üzerinden sağlanabilir.
- Spoke cihazda belirli uygulama ve web kategori trafiği Hub cihaza uğramadan direkt Spoke üzerinden internete çıkartılabilir.
- Uç cihazlar Controller tarafından izlenebilir ve yönetilebilir. Controller yönetimi Turkcell Cloud ekibinde veya müşteride olabilir. İki durumda da alarmlar Turkcell TEMIP'e yönlendirilir.

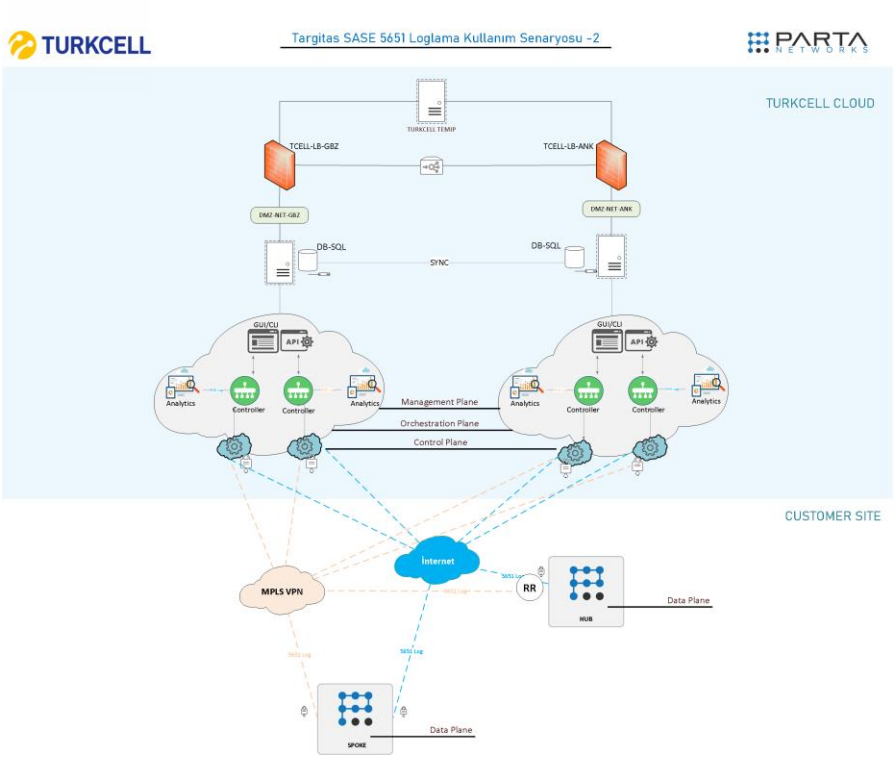


6.4) 5651 Loglama gerçekleştiren SASE çözümü

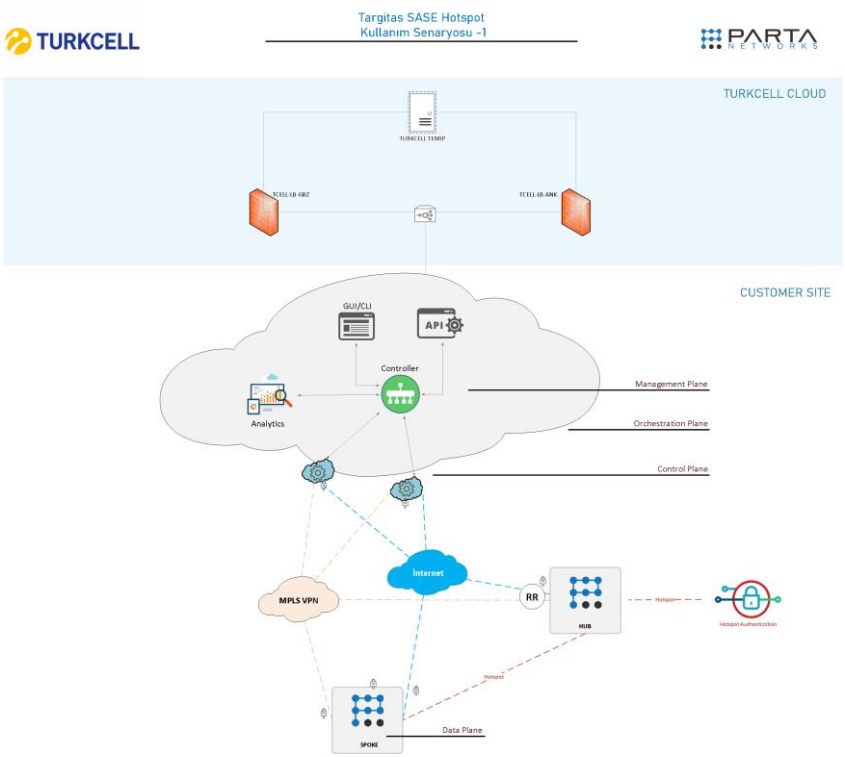


- Uç cihazlarda meydana gelen trafik, 5651 sayılı kanuna uygun olarak loglanmaktadır.
- Uç cihazlar arasındaki yerel ağ iletişimi şifreli tüneller üzerinden gerçekleştirilir.
- Her uç cihaz Turkcell MPLS hattına ve bir adet herhangi bir Internet hattına bağlıdır.

- Farklı sağlayıcı ve tür WAN hattı kullanımı destekler.
- Uç cihazlarda birden fazla WAN hattı bulunması durumunda Hub yerel ağına erişimde Load Balance gerçekleştirilebilir.
- Belirli uygulama veya web kategori trafiği belirli WAN hattı ve tünel üzerinden yönlendirilebilir.
- Uç cihazlar Controller tarafından izlenebilir ve yönetilebilir. Controller yönetimi Turkcell Cloud ekibinde veya müşteride olabilir. İki durumda da alarmlar Turkcell TEMIP'e yönlendirilir.



6.5) Hotspot + 5651 loglama gerçekleştiren SASE Çözümü



- Uç cihazların arkasında yer alan kullanıcılar Hotspot doğrulaması ardından internete erişim sağlar.
- Uç cihazlarda meydana gelen trafik, 5651 sayılı kanuna uygun olarak loglanmaktadır.
- Uç cihazlar arasındaki yerel ağ iletişimi şifreli tüneller üzerinden gerçekleştirilir.
- Her uç cihaz Turkcell MPLS hattına ve bir adet herhangi bir Internet hattına bağlıdır.
- Farklı sağlayıcı ve tür WAN hattı kullanımı destekler.
- Uç cihazlarda birden fazla WAN hattı bulunması durumunda Hub yerel ağına erişimde Load Balance gerçekleştirilebilir.
- Belirli uygulama veya web kategori trafiği belirli WAN hattı ve tünel üzerinden yönlendirilebilir.
- Uç cihazlar Controller tarafından izlenebilir ve yönetilebilir. Controller yönetimi Turkcell Cloud ekibinde veya müşteride olabilir. İki durumda da alarmlar Turkcell TEMIP'e yönlendirilir.

TURKCELL

Targitas SASE Hotspot Kullanım Senaryosu -2

PARTA NETWORKS