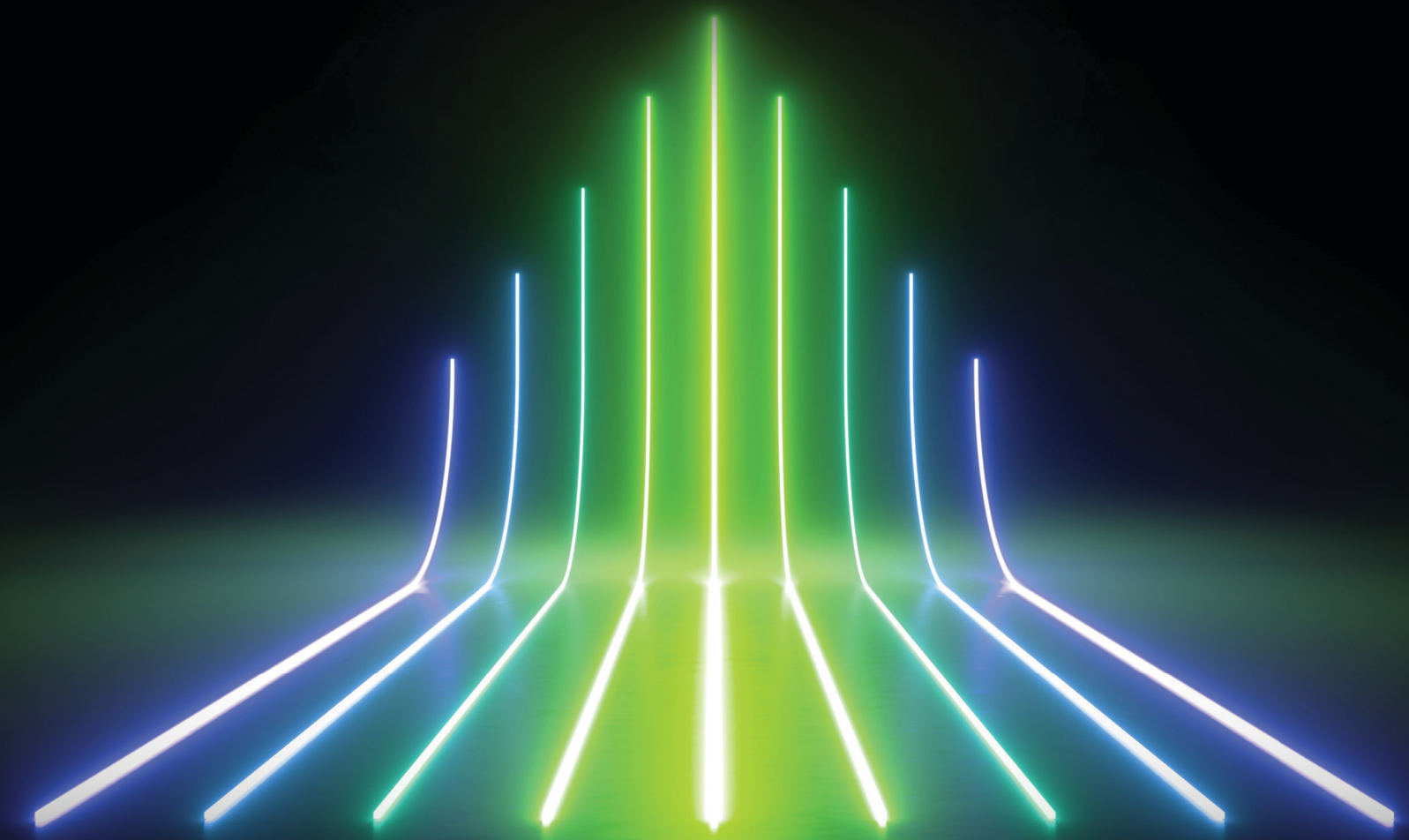
Ağ Uç Katmanını Yönetin

Ağ Güvenliği Ağın Uç Katmanında Başlar

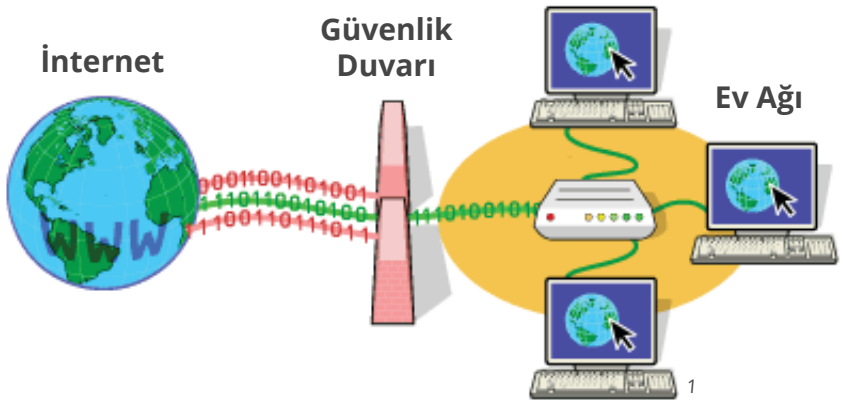


OTD BİLİŞİM
GLOBAL VAD

GARLAND TECHNOLOGY

Kurumsal Ağ Güvenliğinin Evrimi

1990'ların başında güvenlik duvarlarının ilk kez devreye alınmaya başladığı dönemde sektörde bulunan ağ uzmanları için, siber güvenliğin çok daha basit olduğu günler olduğu konusunda genel bir kabul vardır. Nitekim o dönemde ağ güvenliği mühendisi sayısı oldukça azdı; bugünkü anlamda güvenlik mimarları ise neredeyse hiç yoktu.



1

1990'lı yıllarda ağ güvenliği mühendisleri için tehditler yeterince zayıf, trafik yükleri ise yeterince düşük olduğundan, sorun gidermek amacıyla ağı tamamen kapatmak ve fişi çekmek oldukça sıradan bir yöntemdi. O dönemde ağ uzmanlarının odağı, paket iletimini iyileştirmek amacıyla ağ çekirdeğini güçlendirmekti — ağın uç katmanını yönetmek ise henüz gündemde bile değildi.

> Yeni ağ gerçekliği, hem kurum içi iş uygulamalarını hem de bulut tabanlı çözümleri destekleyen hibrit bir yapıdır — üstelik bu çözümlerin tamamı ağın uç katmanında çalışır.

Siber saldırganların giderek daha sofistike hâle gelmesiyle birlikte, güvenlik mimarları ağın uç katmanındaki savunmayı inline güvenlik cihazlarıyla güçlendirmekle görevlendirilmiştir.

How Stuff Works tarafından sağlanan görsel

Güvenlik duvarlarının ilk sürümleri, trafik verilerini yakalamak amacıyla doğrudan canlı hattın üzerine yerleştiriliyordu; ancak günümüz ağları artık yalnızca birincil bağlantı ve gerektiğinde devreye girecek ikincil bir bağlantıdan ibaret değil. Bunun yerine güvenlik mimarları, birden fazla bağlantıyla başa çıkmak ve buna bağlı olarak yük dengelemesi yapmak zorundadır. Ağın uç katmanında bu kadar çok bağlantının bulunması, bugün karşılaşılan siber güvenlik zorluklarının temel nedenlerinden biridir ve bu durum
güvenlik mimarlarını şu kritik sorularla karşı karşıya bırakmaktadır:

- **Uç katmanda birden fazla aracı nasıl bağlarım?**
- **Uç katmandaki verilere nasıl erişirim?**
- **Inline ve out-of-band bağlantıları nasıl ayırt ederim?**
- **Günlük trafiği nasıl yönetirim?**
- **Birden fazla cihazı nasıl kurar ve her birini ayrı ayrı nasıl yönetirim?**

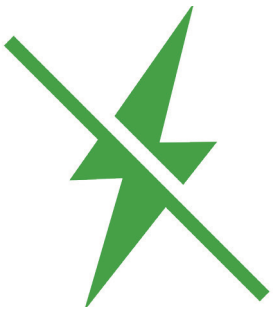
Modern ağ güvenliğinin bu engellerine ek olarak, güvenlik mimarlarının ağ sürekliliğinden ödün vermeden koruma sağlaması gerekir. Ponemon Institute tarafından yayınlanan güncel araştırmalara göre, plansız bir veri merkezi kesintisinin ortalama maliyeti dakikada yaklaşık 9.000 ABD dolarıdır. Ağın %100 erişilebilir olması beklentisini karşılamak için güvenlik mimarları, inline cihazlarını yönetmede bypass network TAP'lerine yönelmektedir. Bu yaklaşım, aktif bir inline cihazı bakım veya sorun giderme amacıyla tek bir anahtar hareketiyle out-of-band moda alma olanağı sunarken, aynı zamanda ağın %100 çalışma süresini korur.

Bu yöntem 1 veya 2 bağlantı tap edilirken oldukça etkili bir stratejidir; ancak güvenlik mimarlarının kendi ortamlarının gereksinimlerini doğru şekilde karşılayabilmesi için anlaması gereken birden fazla TAP senaryosu bulunmaktadır.

Çok Sayıda Inline Güvenlik Cihazı Dağıtırken Karşılaşılan Zorluklar

Ağ güvenliği, şirketlerin artık yalnızca temel güvenlik duvarlarının ötesine geçen, belirli bir standart haline gelmiş inline güvenlik cihazı setlerini kullanacak kadar gelişmiştir. Bu cihazlar; Yeni Nesil Güvenlik Duvarları (NGFW), Dağıtık Hizmet Engelleme koruması (DDoS), veri sızıntısı önleme (DLP), saldırı önleme sistemleri (IPS), uyumluluk çözümleri, web uygulama güvenlik duvarları (WAF), SSL çözme, ağ izleme, adli analiz (forensics) ve daha birçok bileşeni içerir.

Bu inline güvenlik cihazları koruma için neredeyse vazgeçilmez hâle gelmiş olsa da, güvenlik mimarlarının tüm bu yığını (full stack) dağıtma konusunda hâlâ çekinceleri bulunmaktadır. Güvenlik mimarlarının çok sayıda inline güvenlik cihazı dağıtmasını zorlaştıran en kritik sorunlardan bazıları şunlardır:

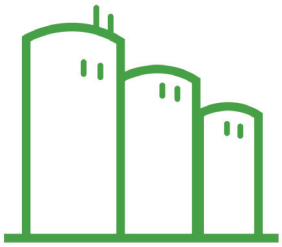


Ağ Kesintisi Olasılığı

Güvenlik mimarları, iki farklı açıdan zorluklarla karşı karşıyadır. Bir yandan, gerekli inline güvenlik cihazı setinin dağıtılmaması veri ihlallerine bağlı ağ kesintilerine yol açabilir. Öte yandan, doğru şekilde konumlandırılmadığında inline güvenlik cihazları ağ içerisinde çok hızlı bir şekilde tek hata noktası (Single Point of Failure – SPOF) hâline gelebilir. Ağ çalışma süresine verilen yüksek önem nedeniyle, ağ kesintisi endişeleri çoğu zaman aşılması güç bir engel olarak görünmektedir.

Dağıtım Karmaşıklığı

Güvenlik mimarlarının yıllar önce tasarlanmış bir kurumsal ağa inline güvenlik cihazları yerleştirmesi gerektiğinde, doğru ve verimli konumlandırmayı belirlemek oldukça zor olabilir. Ayrıca eski altyapılar, modern güvenlik araçlarıyla uyumsuzluklara da neden olabilir.



Silo Problemi

Günümüz ağ trendleri, verimliliği artırmak için siloları ortadan kaldırmaya odaklanmıştır; ancak inline güvenlik cihazları dağıtıldıkça, bu cihazların kendileri birer silo hâline gelebilir. Bağlantıların belirli cihazlara yönlendirilmesi, yanlış yapılan bir dağıtımla birlikte güvenlik katmanlarının birbirinden kopmasına ve bütünleşik güvenlik yapısının parçalanmasına yol açabilir.

Inline Güvenlik Cihazları Çok Sayıda Porta İhtiyaç Duyar

Birçok güvenlik mimarı, out-of-band çalışan güvenlik cihazlarını bağlamak için SPAN portlarına yönelmektedir. Ancak bağlantı için kullanılabilecek SPAN portlarının sayısı sınırlıdır ve trafik yükü arttıkça bu portlar kolayca kapasitesini aşabilir. Bir ağ TAP destek sistemi olmadan, tüm güvenlik cihazlarının görünürlük ihtiyaçlarını karşılamak neredeyse imkânsızdır.

Tüm bu zorluklar, tek bir kurumsal ağın kontrol edilen ortamı içinde ortaya çıkmaktadır. Ancak büyük ölçekli işletmeler için yeni gerçeklik, giderek artan sayıda şube ofisi ve uzak lokasyondur.

> Her yıl katlanarak artan siber saldırı sayısıyla birlikte güvenlik mimarlarının, bu inline güvenlik cihazlarını hem yerelde hem de uzaktan etkili bir şekilde dağıtmanın ve ağın uç katmanını yönetmenin bir yolunu bulması gerekmektedir.

Inline Bypass TAPs Kullanmanın Faydaları

Günümüz güvenlik ortamında, üretim trafiği üzerinde inline çalışan araçlar genellikle cihaz arızalandığında fail-to-wire modunda çalışabilme yeteneğine sahiptir. Ancak bu durum bypass TAP ihtiyacını ortadan kaldırmaz. Bypass TAP'lerin, TAP'in bypass işlevinin uzaktan yönetilebilmesi özelliğiyle birlikte kullanılması, ağ yöneticilerine ağ üzerinde önemli ölçüde kontrol sağlar. Bypass kullanımının başlıca faydaları şunlardır:

1 Bypass TAP üzerinde “zorunlu bypass modu”nu (forced bypass mode) etkinleştirerek ağ sorunlarının olası nedenlerini hızlı bir şekilde eleyebilirsiniz. Bu işlem, inline güvenlik cihazını üretim ağındaki akıştan etkili şekilde çıkarır. Sorun buna rağmen devam ediyorsa, ilgili güvenlik cihazının sorunun kaynağı olmadığı anında doğrulanmış olur.

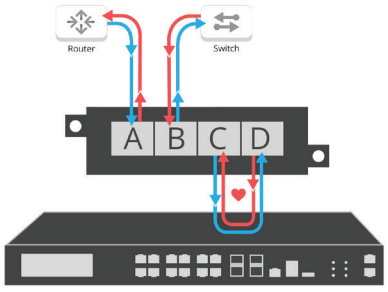
Bu süreç boyunca bypass edilen güvenlik cihazı paketleri almaya devam eder; dolayısıyla cihaz, hiçbir kesinti veya senkron kaybı yaşamadan yeniden inline hâle getirilebilir.

2 Zaman içinde herhangi bir güvenlik cihazının donanım yazılımı (firmware) güncellemesine ihtiyaç duyacağı kaçınılmazdır. Bir cihazın güncellenme süreci genellikle ağın değişikliklerden etkilendiği bir bakım penceresi gerektirir. “Zorunlu bypass modu” özelliğinden yararlanılarak, inline güvenlik cihazı bakıma alınırken ağın kesintisiz çalışması sağlanabilir.

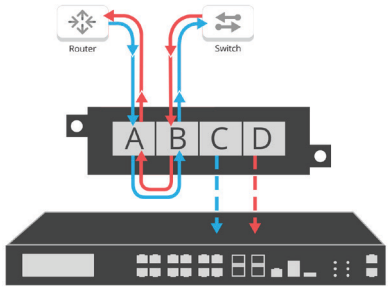
Eğer yedekli güvenlik cihazları varsa, bypass modunun etkinleştirilmesi yüksek erişilebilirlik (HA) modundaki yedek cihazın devreye girmesini sağlar. Bakım bir cihazda tamamlandığında, bu cihaz yeniden inline duruma getirilebilir ve ardından yedek cihaz kendi bakım süreci için devre dışı bırakılabilir.

3 Yeni bir uzak lokasyon kurarken veya ağa yeni bir inline güvenlik cihazı eklerken, bypass TAP kullanmak süreci minimum kesintiyle hızlandırabilir. Zaman planlamak, kabloları söküp yeni cihazı takmak ve temel yapılandırmaları tamamlamak yerine, ağda önceden konumlandırılmış bir bypass TAP bulunması, yeni cihazın yapılandırılmasına ve yapılandırma doğrulandıktan sonra sorunsuzca ağa dahil edilmesine olanak tanır.

Bu işlem yine “zorunlu bypass modu” kullanılarak gerçekleştirilebilir; çünkü canlı ağ trafiğinin kopyaları yeni cihaza aktarılmaya devam eder, ancak yeni cihazın üretim trafiğini etkileme imkânı olmaz. Böylece cihazı gerçek trafikle güvenle yapılandırabilirsiniz.



Diyagram 1. Bypass modu, aktif inline



Diyagram 2. Bypass modu, çevrim dışı (off-line)

Günümüz Ağ Görünürlüğünün Nasıl Olması Gerekiyor

Önceki beyaz bültenlerde ve makalelerde, ağ görünürlüğü ve güvenlik cihazı bağlantıları için SPAN portlarının verimsizlikleri tartışılmıştır; ancak güvenlik mimarlarının, ağ uç katmanı yönetimine ilişkin sorulara daha somut ve uygulanabilir yanıtlara ihtiyacı vardır.

Inline güvenlik cihazları ve ağ uç katmanı yönetimiyle ilgili belirgin zorlukların üstesinden gelmek için güvenlik mimarlarının doğru dağıtım amacıyla "zincirleme" (chaining) yaklaşımına yönelmesi gerekir. Zincirleme (daisy-chaining olarak da bilinir), birden fazla cihazın ardışık olarak birbirine bağlandığı basit bir kablolama şemasıdır. Güvenlik cihazlarının ağın uç katmanında ardışık şekilde zincirlenmiş olması, trafiğin ağa giriş veya çıkış yapmadan önce mutlaka denetlenmesini ve temizlenmesini sağlar. Zincirleme yöntemi ağ güvenliğini artırsa da, aynı zamanda bir trafik akışı darboğazı oluşturur: zincirdeki herhangi bir güvenlik cihazı arızalanırsa, tüm ağ devre dışı kalır.

Bir Ağ Uç Katmanı görünürlük altyapısı oluşturulurken, Network Packet Broker'ların (NPB) mutlaka dikkate alınması gerekir; çünkü NPB'ler, ağa ek bir hata noktası oluşturmadan güvenlik cihazlarının zincirlenmesini sağlayan mekanizmayı sunar. Ayrıca NPB'ler, zincire bağlı tüm güvenlik cihazları arasında tek ve bütünleşik bir görünürlük katmanı oluşturur.

NPB'ler; ağ hızı, port sayısı ve desteklenen optik türleri gibi çeşitli teknik özelliklerle donatılmıştır. Bir NPB'yi tanımlayan temel unsur ise, birden fazla inline veya out-of-band cihazı bağlayabilmesi ve bu cihazlara hizmet ederken trafiği birleştirme, filtreleme, yeniden üretme (regenerate) ve yük dengeleme işlevlerini yerine getirebilmesidir. Ağın uç katmanındaki inline cihazların yönetimi söz konusu olduğunda, NPB'lerin aktif inline cihazların sağlık durumunu izleyebilmesi ve bir inline cihaz arızalandığında ağ bağlantısının bütünlüğünü önceliklendirmesi kritik önem taşır.

Bu katmanın, gerçek inline cihazlar ile ağ trafiğinin akışı arasında aracı görevi görmesi sayesinde güvenlik mimarları, tek hata noktası (SPOF) oluşması veya port yönetiminde hata yapılması endişesi taşımadan gerekli uç katman korumasını ve yönetimini sağlayabilir. Kurum içi iş uygulamalarını ve bulut çözümlerini destekleyen modern hibrit ağ yapılarında, uç katmanın zincirlenmesiyle elde edilen ağ görünürlüğü tam olarak şu şekilde çalışmalıdır:

1. Trafik, internetten iç ağa doğru akar ve burada Network Packet Broker (NPB)
2. tarafından kopyalanır.
3. NPB daha sonra paketleri inline güvenlik cihazları zincirine yönlendirir. Güvenlik cihazları verilerin tamamını — bit bit, bayt bayt ve paket paket — görebilir.
4. Inline güvenlik araçlarının her biri görevini tamamladıktan sonra trafik NPB'ye geri döner ve ağ çekirdeğine doğru akışına devam eder.
5. Ağ trafiğinin kopyaları, iletim sürecinin herhangi bir noktasında NPB tarafından alınabilir. Bu kopyalanan trafik, analiz ve adli bilişim işlemleri için bağlı out-of-band izleme çözümlerine iletilir. Ayrıca belirli araçların yalnızca ihtiyaç duyduğu paketleri görmesini sağlamak amacıyla kural tabanlı filtreler uygulanabilir.
6. Inline cihazlardan önce ve sonra akan trafiğin görünür olması, güvenlik mimarlarının her iki uçtaki paketleri karşılaştırarak temel davranıştan sapmaları tespit etmesini sağlar.

Inline güvenlik cihazlarını canlı hat üzerinden ayıran bir görünürlük katmanına sahip olmak, güvenlik mimarlarının performans sorunlarını tespit edebilmesine ve trafik akışını kesintiye uğratmadan sorun giderebilmesine olanak tanır. Modern işletmeler için çalışma süresi bu kadar kritik bir öneme sahipken, zincirleme yaklaşımı güvenlik mimarisinde verimlilik ve cihaz etkinliği açısından vazgeçilmezdir.

Her ölçekten şirkette güvenlik mimarları benzer inline güvenlik cihazı zorluklarıyla karşılaşsa da, görünürlük için gerekli olan NPB'lerin uygulanmasında tek bir standart çözüm olduğu anlamına gelmez. Her ağın kendine özgü teknik gereksinimleri olduğundan, ağ uç katmanını yönetmek için çeşitli farklı çözümler bulunmaktadır.

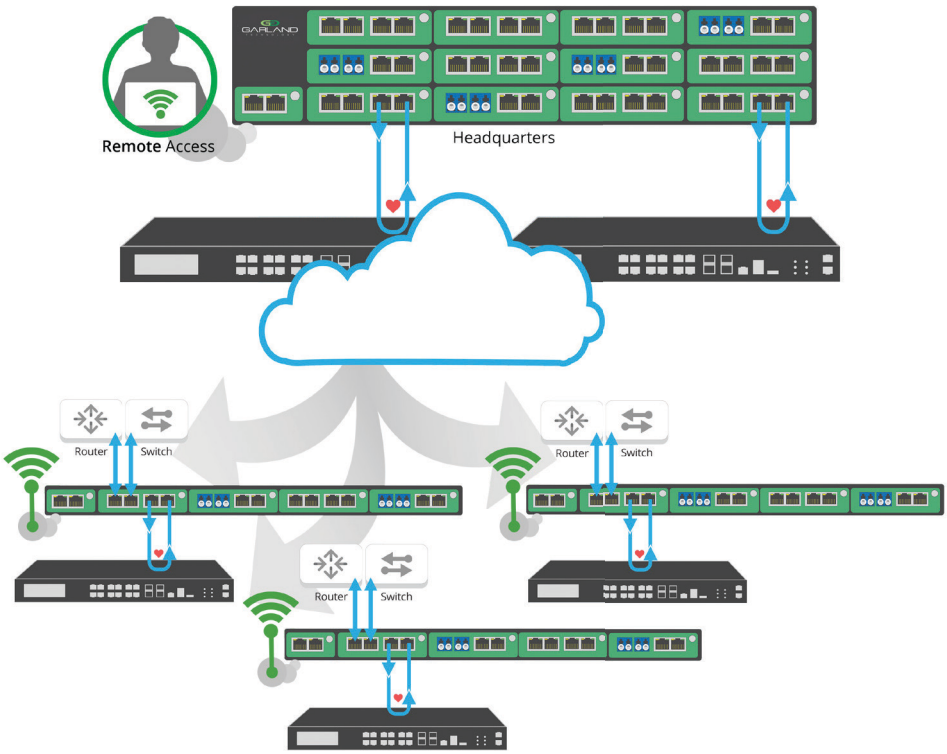
Dört Yaygın Inline Güvenlik Cihazı TAP Senaryosu

Inline güvenlik cihazı bağlantı ihtiyaçlarının geniş bir yelpazesi için mevcut NPB çözümleri bulunmaktadır. Ortam, bir veya iki inline cihaza sahip küçük bir işletme de olabilir, gelişmiş ağ hızlarında çalışan büyük bir kurumsal yapı da olabilir; her iki durumda da güvenlik mimarlarının hem bugünün hem de geleceğin ağ ihtiyaçlarına uygun bir yaklaşım seçmesi gerekir.

Dört yaygın senaryo şunlardır:

- Uzaktan Site Yönetimi ile 1G Veri Merkezi Çözümü
- Yüksek Erişilebilirlik (HA) Çözümü
- Ortam Dönüşümü ile 10G Uç Katman Zincirleme Çözümü
- The EdgeLens® -Gelişmiş Uç Katman Yönetimi

Uzaktan Site Yönetimi ile 1G Veri Merkezi Çözümü

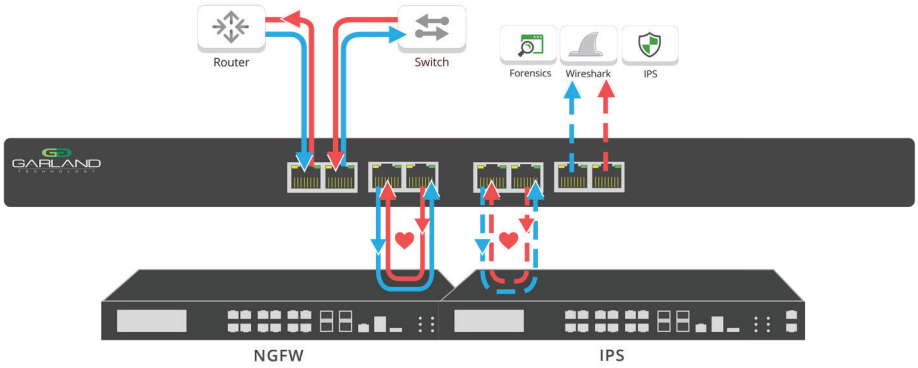


Bu çözüm, birden fazla uzak lokasyona sahip olan ve bu lokasyonlarda yerinde (on-site) yönetici bulundurmayan şirketler (perakende zincirleri, banka şubeleri vb.) için yaygın şekilde kullanılmaktadır. Bu tür yapılarda ana merkez, birden fazla inline güvenlik cihazı içeren güçlü bir güvenlik mimarisine sahip olabilir. Uzak lokasyonlardaki güvenlik yapısı ise çoğu zaman yalnızca birkaç inline güvenlik cihazının bulunduğu oldukça sınırlı bir düzey-dedir. Yerinde BT kaynağının olmaması nedeniyle, inline cihazların hem aktif hem de düzgün çalışır durumda olmasını sağlamak zorlayıcı hâle gelebilir. Uzaktan yönetim yetenekleriyle birlikte kullanılan inline bypass TAP'ler, hem ağ bağlantısının sürekliliğini sağlamak hem de uzak ofiste fiziksel olarak bulunmaya gerek kalmadan cihazlarda hızlı sorun giderme yapmak için etkili bir çözüm sunar.

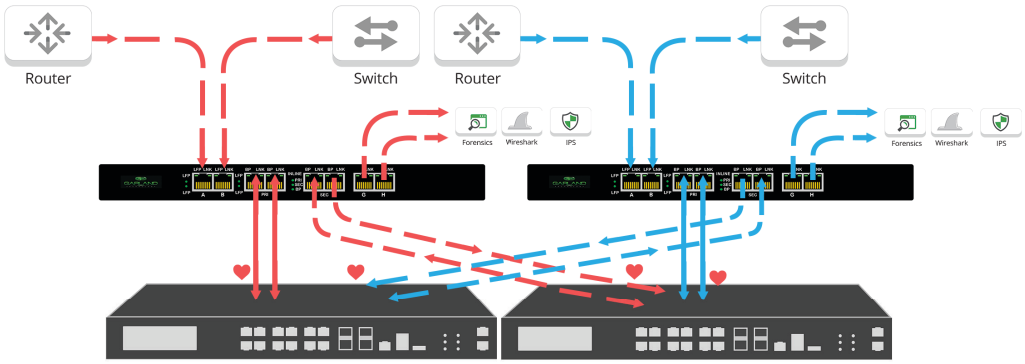
Bu çözümün sağladığı faydalar şunlardır:

- Ölçeklenebilirlik – Gerektiğinde modüler TAP'ler eklenebilir
- 1G Ortam Dönüşümü – fiberden bakıra dönüşüm
- GUI veya CLI üzerinden uzaktan yönetim

Yüksek Erişilebilirlik (HA) Çözümleri



Diyagram 2. Aktif/Pasif için Yüksek Erişilebilirlik (HA) çözümü; birincil cihazdan yedek cihaza otomatik geçiş (failover) sağlar

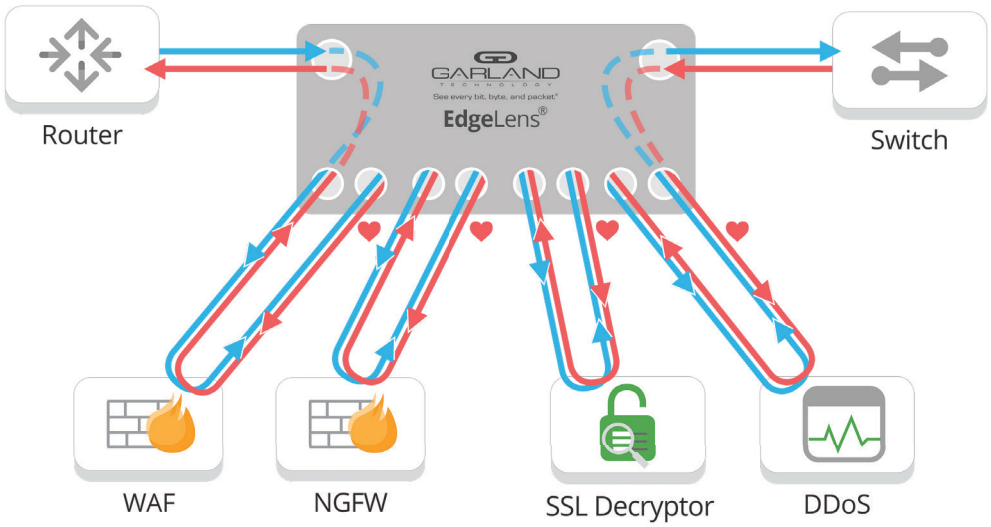


Diyagram 3. Aktif/Aktif için Yüksek Erişilebilirlik (HA) çözümü; aktif cihazlardan herhangi biri arızalandığında otomatik geçiş (failover) sağlar

Bu çözümde, özel olarak tasarlanmış bir inline TAP, tek bir ağ bağlantısını TAP ederek trafiği iki farklı inline cihaza dağıtabilir. Inline bağlantıların yanı sıra, trafik kopyaları out-of-band çalışan araçlara da gönderilebilir.
Bu tür bir TAP, İnternet Servis Sağlayıcı (ISP) bağlantılarının pahalı ve sağlayıcı seçeneklerinin sınırlı olduğu dönemde geliştirilmiştir. Bu TAP modeli, tek bir bağlantı üzerinde iki güvenlik cihazı kullanarak ağ güvenliğinin yüksek erişilebilirlikte olmasını sağlamıştır. Bir güvenlik cihazı arızalandığında, ikinci cihaz hazır durumda devralmak için bekliyor olurdu.

Günümüzde internet bağlantı maliyetleri önemli ölçüde düşmüş ve birden fazla ISP'den alınan yedekli bağlantılar failover için standart hâline gelmiştir. Güvenlik cihazları da bir arada çalışabilmekte ve herhangi bir cihaz arızasında kesintisiz bir şekilde failover gerçekleştirebilmektedir. Bu tür bir inline TAP tasarımının, ikinci bir güvenlik cihazını içerecek şekilde uyarlanması sayesinde, yedekli internet bağlantılarına ve HA modunda çalışan güvenlik cihazlarına sahip ortamlarda inline TAP'in sağladığı ek dayanıklılık katmanından yararlanılmaya devam edilebilir.

Uç Katmanı Zincirleme
4 Adede Kadar Aktif 10G Inline Cihaz Desteği

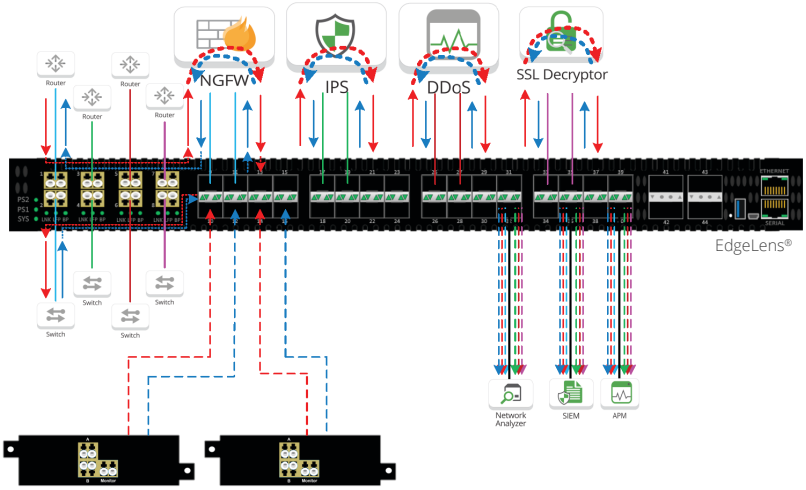


Bu çözüm, yüksek trafik hacmine sahip organizasyonları (örneğin perakende veya finansal hizmet şirketleri) desteklemek zorunda olan güvenlik mimarlarına yöneliktir. Çözüm, dört adede kadar inline güvenlik cihazını izleyebilir ve büyük ölçekli işletmelerin ihtiyaç duyduğu failover güvencesini sağlar.

Esnek 1U tasarımı sayesinde güvenlik mimarları fiber bağlantıları karıştırıp eşleştirebilir ve dört adede kadar bypass TAP konuşlandırabilir.

Bu çözümler, güvenlik mimarlarının ihtiyaç duyduğu işlevsellik ve esnekliği sunsa da, giderek büyüyen inline güvenlik cihazı zincirinden geçen trafiği daha verimli şekilde yönlendirecek çözümlere olan ihtiyaç devam etmektedir. İşte bu noktada EdgeLens®, paket broker yetenekleriyle birleştirilmiş hibrit bir bypass TAP çözümü olarak kurumsal güvenlik mimarlarının ihtiyaçlarını karşılamak üzere devreye girer.

Güvenlik Mimarlarının Gelişmiş Uç Katman Yönetimi Gereksinimlerini Karşılaması



EdgeLens®, birden fazla inline güvenlik cihazını yönetmek ve artan bant genişliği gereksinimlerini desteklemek için yük dengelemesi yapmakla sorumlu güvenlik mimarları için tasarlanmış bir çözümdür. Hibrit bir bypass TAP ve paket broker olarak EdgeLens; 8 adet dahili failsafe ağ portu ile birlikte dört entegre 10G TAP, ayrıca 32 SFP+ ve 4 QSFP+ izleme portu sunar.
Bu yapı, güvenlik mimarlarının inline veri akışını filtrelemesine, birleştirmesine ve güvenlik ile izleme çözümleri arasında yük dengelemesi yapmasına olanak tanır.

EdgeLens ile güvenlik mimarları, 10G'lik bir devreyi TAP ederek trafiği ayrı 1G cihazlar için filtreleme özgürlüğüne sahiptir. Bu yaklaşım, tek bir network TAP üzerinden birden fazla cihazı bağlamanın maliyet açısından verimli bir yoludur ve tümü 1U bir şaside sunularak veri merkezi verimliliği sağlar.

Bu örnekte, dört (4) adede kadar inline cihazın yönetilmesi vurgulanırken, aynı zamanda trafiğin tüm out-of-band araçlar için çoğaltılabileceği gösterilmektedir. EdgeLens'in dört adet 1G/10G TAP'i bulunur ve bunlar dört 1G/10G inline güvenlik cihazı için inline bypass yetenekleri sağlayabilir.

EdgeLens ile Zincirleme Yapmanın Faydaları:
- Akıllı ve optimize edilmiş paket görünürlüğü elde etme
- Hem inline hem de out-of-band güvenlik/izleme araçlarına erişim sağlama
- Ağı etkilemeden gerçek zamanlı güvenlik kavram kanıtı (PoC) değerlendirmeleri gerçekleştirme
- İzleme cihazlarını siber saldırganlara karşı koruma
- Inline ve out-of-band araçların verimliliğini artırma

Sonuç

Güvenlik mimarları, artan siber tehditlere karşı ağın değerli çekirdeğini korumak ve ağın uç katmanını yönetmek konusunda yoğun bir baskı altındadır. Daha yaygın TAP senaryoları esneklik sunsa da, EdgeLens; etkili bir zincirleme yaklaşımı uygulamak isteyen güvenlik mimarları için hepsi bir arada bir çözümdür.

Ağın uç katmanını EdgeLens® Inline Security Packet Broker veya EdgeSafe™ Bypass TAP çözümleriyle nasıl yönetebileceğiniz hakkında daha fazla bilgi edinmek isterseniz, ihtiyaçlarınıza özel güvenlik mimarisi tasarımı için Garland Technology ile iletişime geçerek bir Design-IT danışmanlığı talep edebilirsiniz.

Güvenlikte Başarı için Doğru Zemini Hazırlamak

Ağ güvenliği en iyi uygulamalarını hayata geçirmenize nasıl yardımcı olabileceğimizi öğrenmek ister misiniz?
Ücretsiz bir Design-IT danışmanlığı randevusu oluşturun; mühendislerimizden biri, ağ bağlantı stratejinizi tasarlama sürecinde sizinle birebir çalışacaktır.