Network On-Prem Security
Genel Değerlendirme

1. Yönetici Özeti

Bu rapor ürün bağımsız olup, teknoloji odaklı bir rapordur.

Raporda yer alan adımlar ve öneriler güvenliğin en sıkı olduğu durumlara göre dizayn edilmektedir. Günümüzde bu metodolojiye “Zero Trust” olarak adlandırılmaktadır. Aslında bu bakış açısı yıllardır varolan bir yöntem olmakla beraber, marketing anlamında bu terimin son yıllarda daha çok kullanıldığını gözlenmektedir.

Güvenlik seviyeleri ölçülebilen kavramlar değildir. Daha doğrusu %90 güvenlidir diyebileceğimiz bir seviyeye, kurumlar çok kısa süre içinde gelebilse de kalan kısım belki de yıllar alabilir. Basit, yönetilebilir, güvenli yapılar oluşturmak zor olmasa da güvenliği çok sıkıp, yönetilemeyen bir yapı ile, basit tutup güvensiz bırakma arasında çok ince bir çizgi vardır.

Biz bu raporda bu ince çizgi hakkında detaylara gireceğiz.

Kurumlarda network üzerinden gelen tehditler genelde belli vektörlerde olur.

Bunlardan en çok maruz kalınan saldırılardan biri mail. Geleneksel mail gw’ler burada, belli kontrolleri yapsalar da, herhangi bir imzaya eşleşmeyen veya bir şekilde tespit edilemeyen zararlılar Sandbox cihazları tarafından analiz edilmesi kritikdir.

Mail üzerinden, son kullanıcıya gelen linklerden de zararlılar bulaşabilir. Bu durumda link’in url kategorisini mail gw’ler tespit edebilse de, normal bir kategoriye ait linkde (Google.com v.b.) uzantılı linklerde, içeriğin kontrolü de gerekmektedir. İçerik kontrolü, proxy, fw-urlfilter v.b. sistemler sayesinde yapılabilir.

Burada zero-trust mantığını biraz devreye soktuğumuzda, isolation teknolojisi devreye girmektedir. Özet olarak, bu teknoloji, sizin adınıza linke gider ve erişilecek, dosya, web sayfası v.b. içeriği size görüntü olarak aktarır. Dolayısıyla bilgisayarınızda hiçbir şey çalışmadığından risk de olmaz. Render mantığında çalışan bu teknolojinin handikapları olsa da belli yerlerde gereklidir.

Kullanıcının web erişimini sağlayan teknolojinin adı web proxy- forward proxy olarak geçer. Bazı kurumlar bu işlemi firewall üzerinde yapmayı tercih etse de, flow-base çalışan bir firewallda bu işlem güvenli değildir.

Diğer bir network koruma vektörü, dışarı hizmet veren sunuculara yöneliktir. Burada ips, waf, dos gibi teknolojiler yer alır. Bu teknolojilerin deployment metodlarına göre kabiliyetleri değişir. Hepsinin kendine göre avantajı ve dezavantajı bulunmaktadır.

SSL/TLS bu işin en kritik rolünü oynar. Birçok SSL çözme cihazı olsa da, bunların çalışma metodları, entegre olacakları cihazlarla uyumlulukları, desteklediği protokoller kilit rol oynar. Topolojik değişiklikler ile, bu cihazların da kullanılmasına göreceli olarak gerek kalmayabilir.

SSL/TLS web istekleri genel olarak load-balancer'larda (LTM) sonlanır. Bu cihazlar üzerinde WAF kontrolleri de yapılabilir ancak bu seferde performans sorunları ile karşılaşılır.

Bazı Firewall'lar birçok şeyi üzerinde yapabiliyor gözükse de bunu güvenlik bakış açısında bazı eksiklikler ile gerçekleştirebilir ve atlatılması çok da zor değildir.

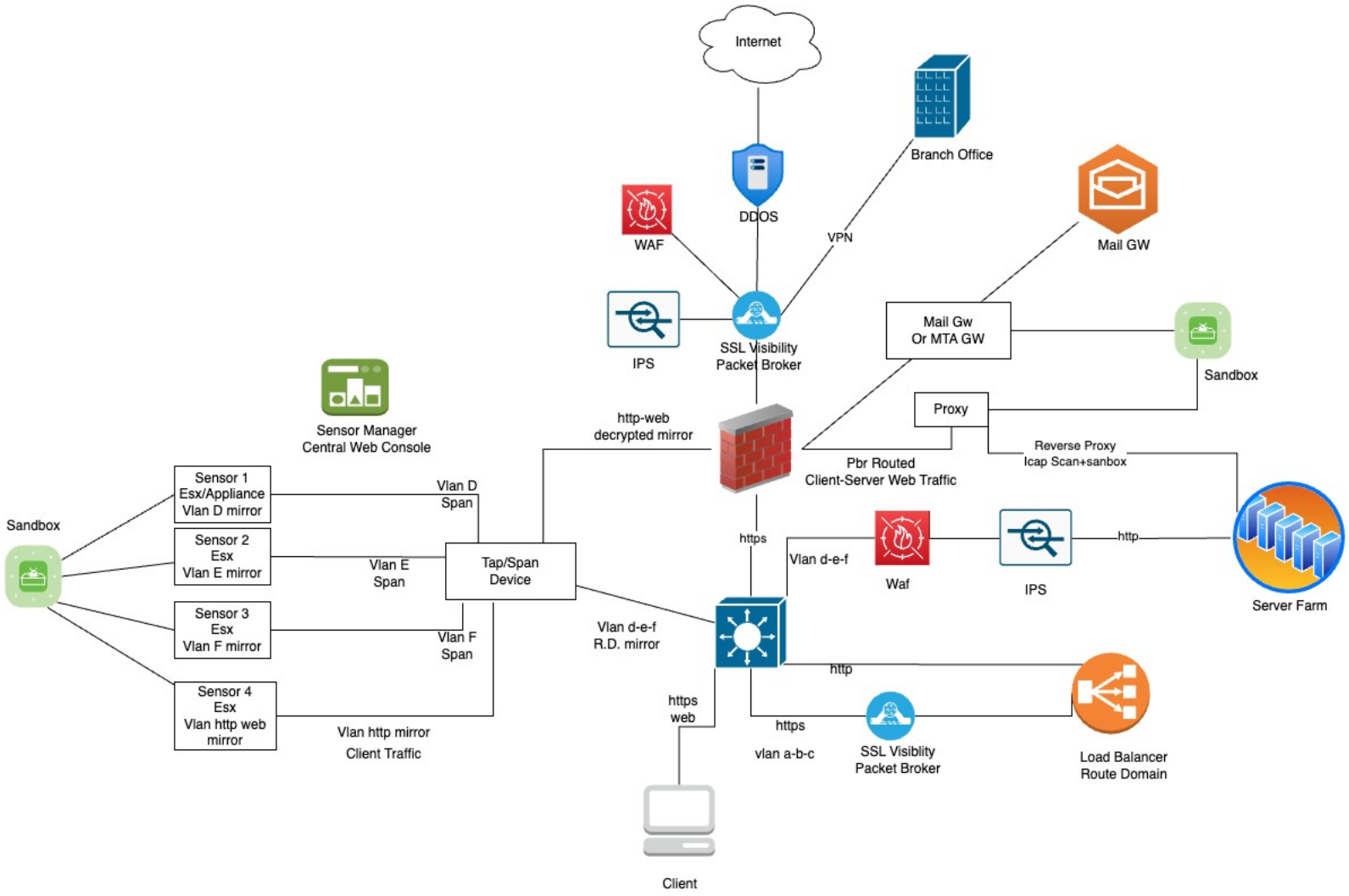
En önemli kritik bir nokta, ne kadar güvenli olursa olsun, network üzerinde her şeyin kaydedilmesi elzemdir. Herhangi bir ihlal durumunda, olayın ilk nereden başladığı ve hangi cihaz/sunucuların etkilendiği bu sistemler ile çok kısa sürede bulunabilir ki bu olmadığı durumda, analiz ve etklielşimli olan sistemlerin temizleme süreci hem uzun hem de maliyetli bir iştir. En kötüsü de kapatılamayacak bir sistem olması durumunda belki aylarca bu şekilde sistemin çalıştırılması gerekebilir.

Bu raporun bundan sonraki kısmında teknolojiler ile ilgili ayrıntılara yer verilecektir.

2. Önerilen Topoloji

Bir sonraki sayfada örnek bir network topolojisini bulabilirsiniz. Örnek topoloji oluşturulurken, genel olarak kurumlarda yaygın olarak kullanılan, yıllardır kendini ispatlamış, kabul görmüş teknolojilere değinilecektir.

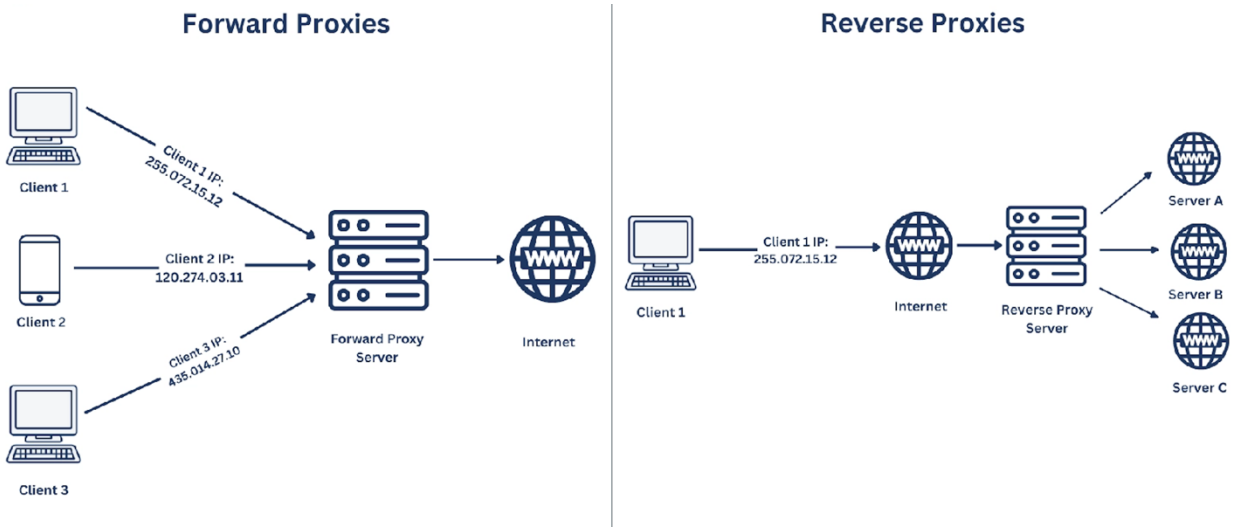
İlgili teknolojiler ve benzer türevleri farklı tip cihazlarda da olabilir. Bunların artıları ve eksileri, ilgili başlıklar altında ayrıntılı bir şekilde belirtilecektir.



Network Mantıksal Topoloji Önerisi

2.1. Proxy

Proxy teknolojisi basit olarak iki istemci arasında vekillik anlamına gelmektedir. Bu teknolojide hiçbir zaman iki istemci birbiri ile direk temas etmez, dolayısıyla bir izolasyon aracı olarak da düşünebiliriz.



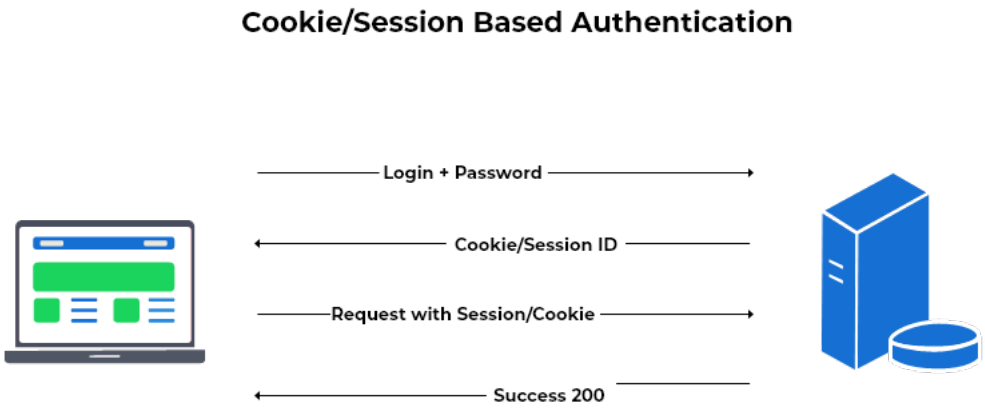
Web tarafı için 2 proxy metodu vardır. Bunlardan en bilineni forward proxy yani istemcilerin internete çıkarken uğradıkları proxy, bir diğeri de dünyadaki istemcilerin, hizmet verdiğiniz web sunuculara erişirken kullandığı teknoloji olan reverse proxy'dir. Her iki durumda da session, proxy üzerinde sonlanır ve client-server arasında ayrı sessionlar oluşturulur. Şimdi bu konuda kritik olan ayrıntılardan bahsedelim.

2.1.1. Forward Proxy

Forward Proxy, genel olarak url proxy olarak bilinir. Temel fonksiyonu, client'ın internet üzerinden eriştiği içerikleri kontrol ettiği gibi, eş zamanlı istemcisinden paylaştığı içerikleri de kontrol etmektir.

Neden proxy teknolojisi kullanılması gerektiğini bazı örnekler ile açıklamaya çalışacağız. Bakış açımız burada sadece güvenlik odaklıdır.

2.1.1.1. Session Authentication



Kullanıcı bilgisayarına bir zararlı bulaştığı veya isteğin direk olarak kullanıcı tarafından yapılmadığı durumda, proxy bu session a izin vermez. Bu da güvenlik kriteri olarak çok kritik bir durumdur. Flow base olarak çalışan sistemler veya ldap ile kullanıcıyı authanticate eden sistemlerde bu yapılamaz.

2.1.1.2. Gelişmiş SSL interception (Proxy)

SSL/TLS trafiği çözülmediği durumda, bu vektörden gelebilecek hiçbir tehdit veya yetkisiz paylaşımın kontrolü mümkün olmamaktadır.

Proxy, transparan ve explicit olarak genelde 2 şekilde konumlandırılabilir.

Transparan senaryoda, istemci bir internet sitesine eriştiğini düşünür ve session bu şekilde oluşur.

Explicit senaryoda ise istemci, bir proxy üzerinden internete eriştiğini bilir ve session bu şekilde oluşur.

Bu tarafta çok ayrıntıya girmekten ziyade, bir konuya açıklık getirmek için bu açıklamayı yaptık.

Eğer istemci transparan modda erişiyorsa, geniş bir cipher-suite/TLS versiyon desteğine sahip olmalıdır ki, session düzgün bir şekilde intercept edilebilsin. Özellikle flow modda url-filter'lık yapan firewall'lar, kısıtlı bir cipher süite desteğine sahiptir. Dolayısıyla intercept edemediği session'ı eğer düzgün ayarlanmadı ise bypass eder ve güvenlik açığına neden olur.

Bunun yanında, bankacılık v.b. kritik işlemlerde yüksek algoritma kullanılmaya zorlanması, ssl sertifikasının tarihi geçmişse yine de belli bir adrese giderken ssl sertifika doğrulaması yapmadan, ssl çözümlemesi yapılması gibi özellikler proxy cihazlarında mevcuttur.

Yine ssl üzerinden geçen dns isteklerini bu cihazlar tespit edebilir, engelleyebilir.

Protokol algılama özelliği sayesinde, http, dns, ftp v.b. dışında herhangi bir paketin geçmesini otomatik olarak engellenir. Tünelleme yaparak proxy atlatma teknikleri bu senaryoda çalışmayacaktır. Flow base çalışan firewall'larda deep packet inspection (DPI engine) mutlaka bu sebepten dolayı açık olmalıdır.

Çözülen ssl trafiğin bir kopyasının da adli amaçlar için kayıt edilmesi için, bu cihazlardan trafiğin çözülmüş bir kopyası da alınmak zorundadır.

Çözülemeyen, istemci tarafından gerçekleştirilmeyen her türlü trafik bloklanmalıdır, bu özellik mutlaka aktif olmalıdır.

2.1.1.3. Üçüncü parti servisler ile entegrasyon

Bazı proxy cihazları üzerinde antivirus bütünleşik gelirken, bazılarında ayrı gelmektedir. Proxy, session'ı sonlandırdığından, TCP/IP'ye kolay hükmeder. İndirilen bir dosya, analiz edilmeden, istemciye iletilmemelidir. Sisteme bulaşan bir ransomware, yatay da dakikalar mertebesinde tüm kuruma yayılma potansiyeline sahiptir.

Bunun yanında Sandbox cihazları da açık entegrasyon kullanabilir (ICAP veya API) veya kapalı entegrasyon kullanabilir. Açık entegrasyona sahip sistemler seçildiğinde, örneğin mail tarafından gelen zararlılar burada analiz edilebilir veya fileserver üzerindeki dosyalar, API ile bu cihaza yollanarak tarama yapılabilir.

Bir diğer önemli kısım DLP entegrasyonudur. ICAP olmadığı durumda açık entegrasyon yapılamaz.

Flow base çalışan bir firewall, trafik akarken tüm trafik ile işlem yaparken, web trafiğini genel olarak tutamaz, bu da ilk tehdidin içeri geçmesine neden olmakla beraber, DLP ve Sandbox tarafında da belirtilen durumlardan ötürü zayıf kalmakta veya bazı fonksiyonları yerine getirememektedir.

2.1.1.4. Dns Proxy-Dns Güvenliği

Proxy cihazları Dns istekleri için de vekillik yapmalıdır. Bu sayede, dns tünelleme başta olmak üzere, istenmeyen istekler engellenebilmelidir. Bu işlemde cihaz, dns trafiğini açıp, trafik içindeki dns ile alakalı olmayan tüm istekleri kesebildiği gibi, örneğin, istek zararlı bir domainden geliyorsa farklı cevaplar dönebilmeli veya istek istemciden geliyorsa, yazılan kurallar ile erişim yetkisi verilebilmelidir.

2.1.2. Reverse Proxy

Reverse Proxy dışardan gelen isteklerin karşılandığı yerdir. Genelde kurumlarda Load Balancer (LTM) cihazları bulunur. Bunların hepsi reverse proxy olarak çalışır. SSL/TLS server side session bu cihazda genelde bir sertifika ile sonlanır.

Session burada sonlandığında, içerik kontrolleri, WAF gibi özellikler de işletilebilir. Ayrıca L7 DOS atakları tarafında aksiyonlar yine burada alınabilir.

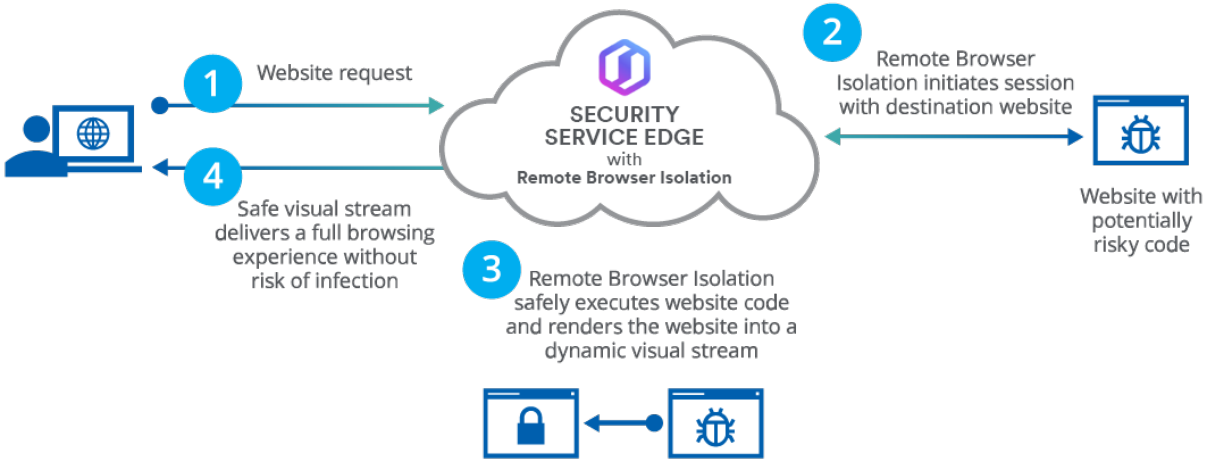
Reverse Proxy cihazları, sunuculara post edilen dosyaları zararlı, içerik taramasından geçirebildiği gibi, uzantı bağımsız, "apparent data type" tarafında analiz ve tespit operasyonlarını

yapabilmelidir. Doc uzantılı bir exe dosyası otomatik bloklanabilmeli veya executable olarak analiz edilebilmelidir.

LTM cihazlarında icap entegrasyonu olsa da genelde uzantıya bakar ve/veya dosya analiz boyutu ve sayısı çok sınırlıdır.

2.1.3. Web Isolation

Isolation teknolojisi, aslında bir proxy teknolojisinden farksızdır. Burada farklı olan kısım, kullanıcıya ulaşan kısmın tamamen görüntüden ibaret olmasıdır.



Genelde, bilinmeyen kategorilere olan erişimler, mail içinde gelen linklere erişim bu yöntem ile sağlanarak güvenlik seviyesi en üst noktaya çıkarılabilir.

Kısaca özetlemek gerekirse, session'ın bir cihaz üzerinde sonlanarak (proxy mode) alınabilen güvenlik önlemleri, flow modda çalışan (firewall v.b.) sistem üzerinden alınabilen güvenlik önlemlerinden farklıdır.

Her iki yöntemin kendine göre avantajı olsa da güvenlik ön planda olduğunda Proxy modun seçilmesi elzemdir.

2.2. Sandbox Sistemleri

Sandbox cihazlarının hepsi temel olarak aynı prensibe göre çalışır. Temel prensip, bir dosyanın hiçbir imza tarafından tetiklenmediği durumda, çalıştırıldığında bilgisayar üzerinde neleri değiştirdiği ve neler yapabildiğinin tespiti üzerinedir. Bu yüzden adı "zero day detection system" olarak da geçmektedir.

Farklılık çalışma metodlarında ortaya çıkar. Ancak buna değinmeden önce, gelişmiş sandbox cihazları bir dosyayı 30 ile 120 sn arasında analiz edebilir. Dosya analizi için üzerlerinde sanal işletim sistemleri barındırır ve bu sayı da genel olalrak büyük cihazlar için 50-100 dosya aralığındadır.

Sandbox sistemleri dosyaları farklı şekilde tarayabilse de (simulation, emulation, virtuluzation), en doğru sonuç sanallaştırma ile gelmektedir. Bu durumda sanal makine üzerinde çalışan dosyaların, burada yaptığı değişiklikleri izleyerek, dosyanın zararlı olup olmadığına karar verebilir.

Sandbox cihazları paralelde eş zamanlı çalıştırdığı sanal sistem sayısı kadar dosya tarayabilir. Bu bağlamda ortalama bir Sandbox cihazı 50-100 sanal sistem eş zamanlı çalıştırdığı durumda, bu da dakikada en fazla 75-150 dosya tarayabilmesine olanak sağlar.

Eğer bizim sistemimizden dakikada örneğin 2000 dosya geçiyorsa, bu tüm dosyaların sandox tarafından taranamaması ile sonuçlanır.

Hiçbir sandbox cihazı büyük network'lerde bu sebepten yeterli gelemez. Dolayısıyla farklı bir mekanizmaya ihtiyacımız otomatik olarak doğmaktadır.

Bu sebepten, statik kod analizi, antivirus, whitelist v.b. ön filtreleme yapılarak sandbox'a trafik gelmelidir, aksi halde topolojiksel olarak sandbox görevini yapmak için gereken süreyi elde edemez.

Sandbox ürünleri tercih edilirken aşağıdaki özelliklerin olması avantaj sağlar.

- Elle Pattern imza yazabilme
- İşletim sistemi özelleştirme
- Uzantı bağımsız analiz, tüm dosya tiplerini analiz edebilme
- Antivirüs ve Statik kod analizi entegrasyonlarına açık olması
- Aksiyon alabilmesi için plug-in desteği

Sandox cihazları, api(açık entegrasyon), icap(web entegrasyon) ve smtp(entegrasyon) ile çalışmalıdır. Aksi halde her vektör için ayrı sandbox kullanılması gerekir bu da maliyetleri artırır.

Flow base çalışan Sandbox'lar (Flow base firewall, inline network sandbox, span-mirror analiz) aktif olarak bloklama yapamaz. Bu da ilk tehditin içeri girmesine neden olur. ZeroDay koruması sağlamak için konumlandırılan bir ürünün, dosyayı geçirdikten sonra analiz etmesi mantıklı gözükmemektedir.

Session'a hükmedilmesi gerektiğinden proxy-base teknolojiler kullanılmalıdır. Aksi halde yukarıda belirtilen sebeplerden etkin bir koruma sağlamaktan söz edilemez.

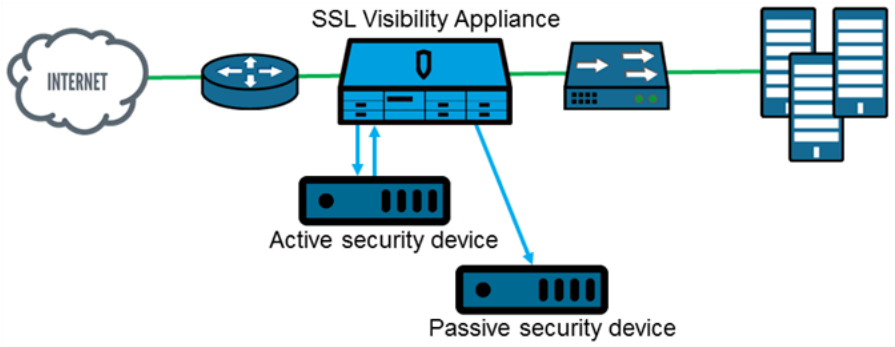
2.3. SSL Visibility Appliance ve Packet Broker

SSL Visibility appliance kısmına girmeden önce bir konuya tekrar değinelim. Güvenliğin tam olarak çözülmesi için SSL trafiğin açılması şart, 2 temel SSL trafik bulunuyor.

Bunlardan biri Forward SSL dediğimiz, istemcilerin veya sunucuların internet yönüne yaptığı trafik. Bu kontrolü zaten yukarıda anlatıldığı üzere Fwd Proxy ile yapılıyor.

Bu durumda Fwd SSL trafiği için SSL Visibility çok da mantıklı olmamakla birlikte. Ancak flow base bir sandbox kullanılıyorsa veya iç taraftaki kullanıcı trafiğini bir güvenlik cihazından geçirilmek isteniyorsa bu özellik yine de kullanılabilir.

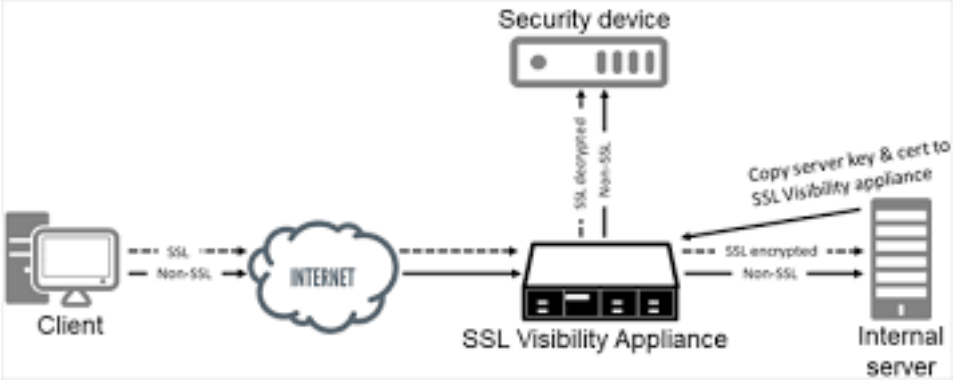
Forward SSL dışında bizim asıl ilgilendiren kısım, sunucularımıza dışarıdan gelen tehditlerin incelenmesi. Bu kısımda da daha önceki "Reverse Proxy" kısmında açıklandığı üzere inbound ssl trafiğinin çözülüp analiz edilmesi gerekiyor.



Bu analiz sonucunda temiz trafik yoluna devam ederken, kirli trafik daha network'umuze girmeden önce durduruluyor.

SSL Visibility Appliance'ın kullanılmasının diğer önemli avantajları ise sunucuya kadar trafiğin SSL gitmesi gerektiği durumlarda bu trafiğin ssl session bütünlüğü bozulmadan analiz edilebilmesin sağlanması. Bu işlemin gerçekleştirilebilmesi için ilgili SSL Visibilty cihazının Layer2 transparent çalışması gerekmektedir. L3 transparan durumlarda trafik bütünlüğü bozulacağından (Proxy route mode, proxy transparent mode v.b.) aslında bu cihazın da kullanılmasının anlamı çok da kalmamaktadır. İlerleyen bölümde LTM (Local Traffic Manager) kullanarak bunun nasıl sıfır maliyetle gerçekleştirilebileceği ayrıca anlatılmaktadır.

Layer2 transparent çalışan bir SSL Visibility cihazı, eş zamanlı olarak inbound yönünde flow modda çalışıyor diyebiliriz. Dolayısıyla ssl trafiğini çözdükten sonra, trafiğin doğası gereği L2 transparan-Virtual wire desteği olan bir cihaz tarafından analiz edilebilir.



Örneğin elimizde sadece bir ips var ise p.brocker da kullanmak zorunda değiliz. Ancak Packet Brocker'ın topolojilerde en çok kullanılmasının nedeni esneklik sağlamasıdır.

Elimizde, Network IPS, Firewall IPS, WAF, APT, Network DLP v.b. birçok cihaz olduğunu düşünelim. Normal şartlar altında tüm bu cihazları birbirine bağlamamız gerekecektir. Ancak herhangi bir sorun olduğunda bu işin t.shoot'u inanılmaz zor bir hal alabilir. Dolayısıyla network ve güvenlik yöneticileri, belli şartlarda sadece ilgili trafiğin bir cihaza uğramadan bypass etmek isteyebilir. İşte tam da bu durum için p.brocker'lar hayat kurtarır.

Yalnız bu yöntemin güvenlik bakış açısında bazı eksiklikleri bulunabilir. Örneğin L7 Ddos tarafında önlem alınamayabilir, url-re-write yapılamaz belki de http/2 desteği olmayabilir. Ürünlerin ve TCP/IP limitasyonlarına göre belli özellikler kullanılamaz.

Burada tekrar altını çizme gereği duyuyoruz. Layer2 transparent kullanmadığınız durumda eğer elinizde bir Load Balancer (LTM) cihazınız varsa, SSL Visibility Cihazına ihtiyacınız olmayabilir. LTM tarafında bu duruma ayrıca değineceğiz.

SSL için en kritik olan kısım data-integrity ve protocol detection'dır. Yani port tanımı yapmadan cihaz, SSL trafiğini cihaz dışına çıkarmadan tespit edip çözebilmeli, diğer trafikleri bloklayabilmelidir. 443 portundan http trafik geliyorsa veya 80 portundan https trafik geliyorsa tespit edebilmelidir.

2.4. LTM (Local Traffic Manager)

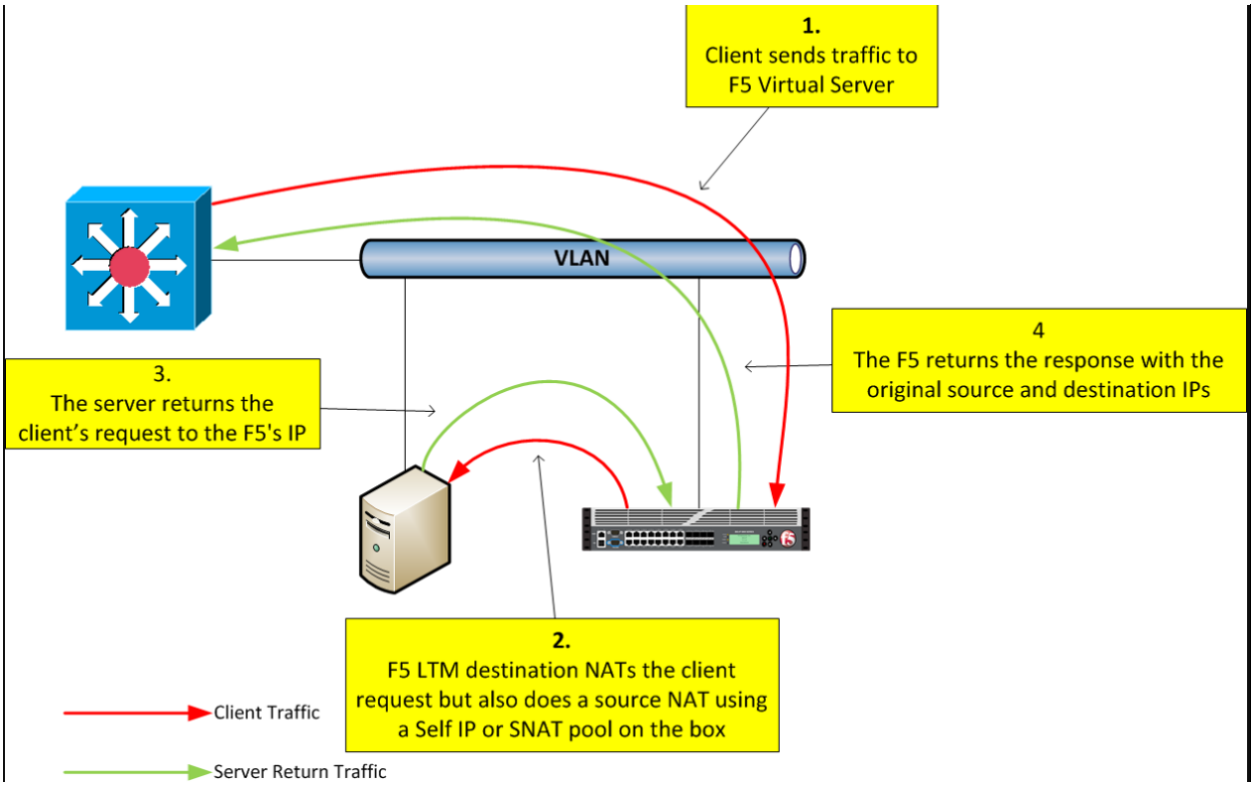
LTM neredeyse her yapıda olan bir cihazdır, burada tekrar hatırlatma gereği duyuyoruz, sadece güvenlik bakış açısı altında kritik noktalara değineceğiz.

LTM bir reverse proxy'dir. Genel kullanıcım amacı ise ssl sonlandırmak ve ilgili trafiği sunuculara paylaştırmaktır.

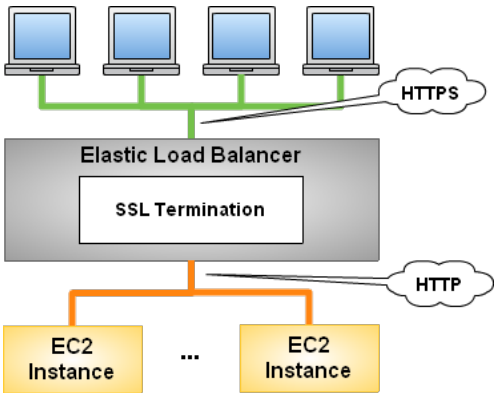
LTM cihazlarının deployment modellerine bu noktada değinmek zorunda kalacağız.

Temel 2 metod ile bu cihazlar kurulmaktadır.

Bunlardan en çok kullanılanı one arm metod olarak geçer.



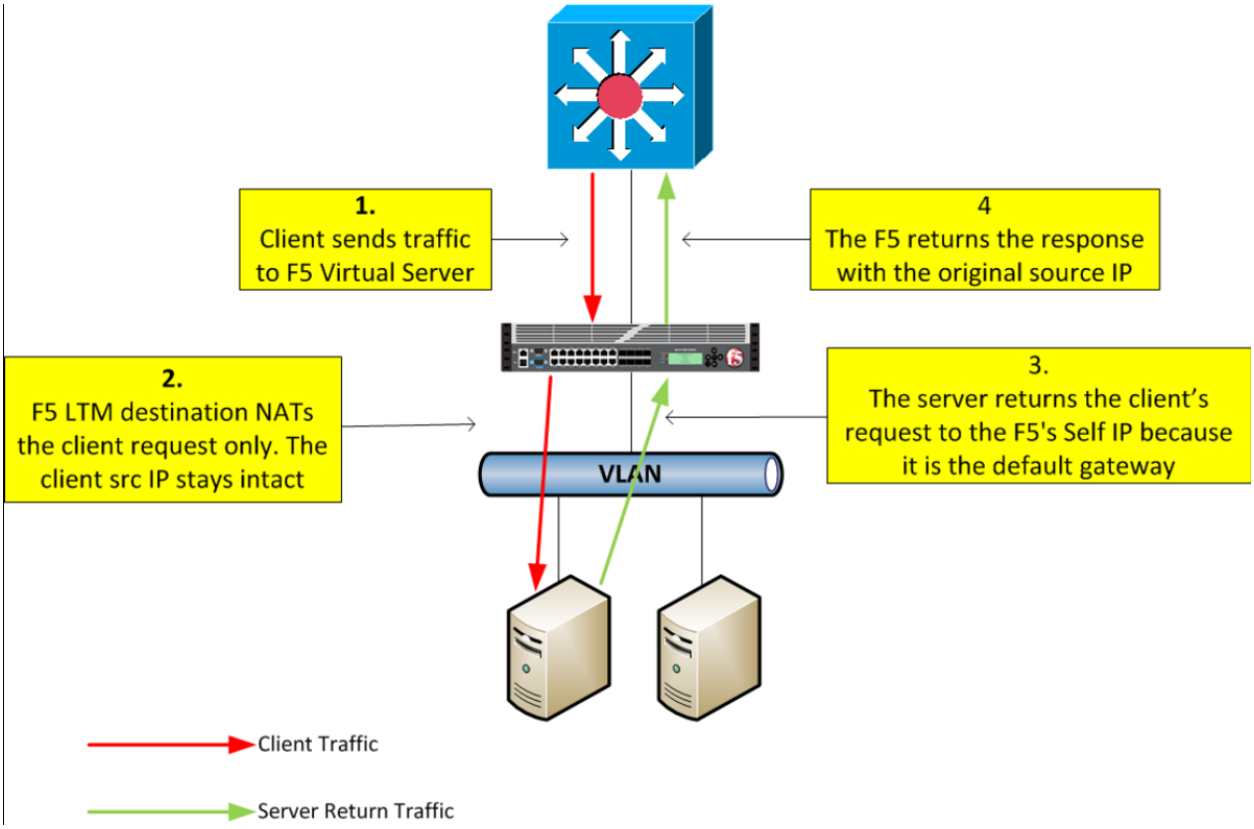
Bu durumda Load Balancer'da sonlanan session, Load Balancer Ip'si ile sunucuya doğru gider ve sunucu cevabı doğal olarak Load Balancer ip'sine döner. Bu senaryoda sunucunun default gw'i L3 firewall veya omurgadır. Topolojiksel değişiklik gerekmediğinden bu yöntem en çok seçilen yöntemdir. Ancak visibilite tamamen kaybolur. Sunucu tarafında client ip gözükmez.



Kolay yöntemi seçtiğimizi varsayalım. Source ip'yi de xff ile sağladık. Ancak bu durumda Load Balancer arkasında yer alan http trafiğinde source ip olarak load balancer ip'si

gözükeceğinden güvenlik cihazı, network monitoring, siem, kolerasyon v.b. birçok alanda çok fazla zorluk çekilir.

Bu sebepten zor olan route mod olarak konumlandırılmalıdır.



Bu senaryoda source ip kaybolmaz ancak her segment için route tanımlarının yapılması gerekir. Implemantasyonu zordur, sunucuların default gw'inin load balancer olması gerekir. Ancak sunucuya kadar trafik https gitmek zorunda değilse, ssl visibility cihazı kullanmadan, sunucuya erişmeden önce trafik istenilen network cihazı tarafından analiz edilebilir. Bu alanda istenirse sadece packet broker kullanılmaya devam edilebilir. Yine istenilen yapı oluşturulabilir.

One arm LTM kullanan bir kurum, SSL Visibility'yi inbound yönünde kullanmak istiyorsa, topolojiksel değişiklikle route mode olarak LTM'i konumlandırarak SSL Visibility kullanmasına gerek kalmayacaktır.

2.5. WAF (Web Application Firewall)

Waf'ın temel fonksiyonu Web uygulamalarınızı, bilinen ataklara veya olağan dışı durumlara doğru korur.

Waf cihazları L2 inline transparan, L3 inline proxy veya L3 one arm proxy olarak çalışmaktadır.

Ayrı cihazlar olabildikleri gibi LTM üzerinde bir modül olarak da çalışmakla birlikte, bu durum yüksek trafiğe sahip kurumlarda çok tavsiye edilmez. Ciddi performans sorunlarına neden olduğu gibi, gereksiz maliyet artışlarına da neden olur. Üstüne yönetimsel sorunlar da çıkarmaktadır.

Kullanılacak cihaza ve yapıya göre, cihazların konumlandırılması gerekir. Bazı cihazlar yukarıda anlatılan deployment metodlarından dolayı topolojik uyumsuzluk yaratabilir.

Waf cihazlarının kabiliyetleri değişkendir. Ancak güvenlik bakış açısında proxy modda konumlandırılması tavsiye edilmektedir. Yüksek ölçekli trafiklerde LTM ve WAF ayrılmalıdır.

LTM fiziksel, WAF sanal deployment metodları da vardır.
Topolojiksel analiz yapılarak, profesyonel olarak dizayn edilmesi gereken sistemlerdir.

2.6. IPS Cihazları

Ips cihazları bilinen imzası olan tüm atakları kesme üzerine dizayn edilse de belli başlı özellikler de üzerinde gelmektedir. Ip reputation, dos protection, karantina özellikleri her ips de olması gereken özelliklerdir.

Ips cihazlarının kapasiteleri datahseetlerine bakıldığında muazzam yüksek değerler olsa da, işin içine SSL girdiğinde direk olarak performans düşüklüğü yaşanır.

Bunun yanında yüksek algoritmaya sahip cipher suite/TLS versiyonları bu cihazları daha da yorar. Cipher suite desteği de çok limitli olduğundan, güvenlikten de ödün verilmesi gerekebilir. Hepsini geçtiğimizde, maliyetler gereksiz yükselir.

Bu yüzden SSL çözümleme işlemi SSL Visibility Appliance üzerinde yapılması tavsiye edilir.

Eğer route modda konumlandırılan bir LTM'e sahipseniz, LTM-Sunucu arasını http'ye çekip bu cihazı koyduğunuzda da benzer korumayı sağlamış olursunuz.

2.7. Network Forensic Cihazları

Alınan tüm network güvenlik önlemlerine rağmen, hesap edilmeyen senaryolar ile karşılaşılır. Bu işin doğasında vardır ve gayet normaldir.

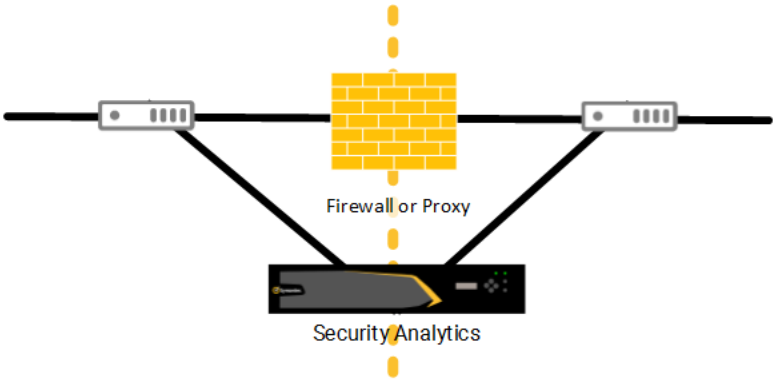
Böyle bir olay yaşandığında bunu tespit edip, önlem almak çok kritik bir süreçtir. Network forensic cihazları olmadığı durumda olayların tespiti çok uzun sürer (1-6 ay) ve çok maliyetli bir hal alır.

Network forensic cihazları aşağıdaki özelliklere sahiptir.

- Veri ihlal durumlarında hızlı aksiyon, enfekte olan sistemlerin nokta atış tespiti.
- Tanımlanabilecek harici IOC'ler ile (Usom, Sans v.b) ağ üzerinde zararlı aktivite tespiti.
- Ağ trafiği anomali tespiti
- Network performans durum analizleri
- Güvenlik bakış açısında, olmaması gereken durumların (basit şifre kullanımı, tünelleme trafikleri, zayıf algoritma erişimleri v.b.) sürekli tespiti
- Pivot Entegrasyonlar ile Api ve Icap ile Universal Sandbox entegrasyonu.

Bu cihazlar temel olarak ağ trafiğinin bir kopyasını kaydeder ve eş zamanlı analiz imkânı verir. Pasif bir cihazdır, aktif koruma sağlamasa da problemlerin hızlı çözümü için gereklidir.

Meta ve Raw olarak datayı 2 şekilde tutar. Meta kısmında, bir pcap dosyasından parse edilebilecek birçok veri vardır. Ve bu veriler uzun süreler tutulabilir (1-12 ay) ancak Raw data doğal olarak daha kısa süre tutulur (1-2 hafta) ideal değerlerdir.



Trafiğin analiz için bu cihazlara clear text (http, ftp, smb v.b) gelmesi gerekir. Eğer encrypted (https, ftps, smtps v.b.) gelirse analiz edilemez. Dolayısıyla doğru yerden trafiğin alınması önemli olmakla birlikte, network'de yer alan cihazların doğru konumlandırılması gerekmektedir.

Örneğin One arm konumlandırılan bir LTM cihazının arkasından alınan http trafiğinin bir kopyasında source ip olarak maalesef LTM ip'si gözükür. Xff üzerinde ilgili ip aranır ancak bu durumda bu bir saldırgan ise ve bu trafiğin analizi gerekiyorsa kolerasyon neredeyse imkansız hale gelir veya çok uzun süreç alır.

2.8. Mail Gw Sistemleri

Tehditlerin önemli bir kısmı mail body'sinde gelen linkler veya eklerinden meydana gelir. Kullanıcıya bu isteklerin iletilmeden önce tüm her şeyin analiz edilmesi kritikdir.

Linkler daha önce Proxy başlığı altındaki Web Isolation ile entegre edilerek erişim sağlanması en güvenli yoldur.

Eklerin ve linklerin analizi de cihazlar üzerinde yapılabilir veya eklerin ZeroDay analizleri için Sandbox cihazları kullanılır.

Sandbox tarafında bu kısma değinildiği için ayrıntısına girilmeyecektir. Web Proxy başlığı altında yazan aynı özellikler mail tarafı için de aynen geçerlidir.

Web ve Mail için ayrı sandbox cihazların kullanılmaması hem maliyet hem de güvenlik bakış açısında önemlidir. Örneğin flow modda çalışan bir web sandbox cihazına, mail sandbox cihazı entegre edilemeyebilir.

3. Sonuç

Sonuç olarak her kurumun dinamikleri ve uygulamak zorunda oldukları regülasyonlar farklıdır.

İhtiyaçlara göre network topolojisinin dizaynı, güvenliği doğrudan etkileyecek ölçektedir.

Çok büyük maliyetler ile yatırım yapmak yerine, doğru ve yönetilebilir çözümleri uygulamak önemlidir. Bazı durumlarda topolojik değişiklikler, en baştan dizayn etmekten çok daha fazla zaman alır.

Ürünlerin birbiri ile entegrasyonu, ihtiyaca göre kullanılacak metodlar tamamıyla farklıdır. Her ürünün çalışma mantalitesi farklı olduğundan uyum çok önemlidir.

Aksi halde çalışan bir yapıdaki Paket Broker+SSL+IPS+WAF topolojisi, farklı markalarla oluşturulduğunda çalışmayabilir veya çalışması için güvenlik tarafında feragat edilmesi gerekir.

Şartname ve topoloji danışmanlığı almak, bu ölçüde ilerde yaşanabilecek problemleri önlediği gibi, maliyetleri de büyük ölçüde kısabilir.

Daha fazla ayrıntı ve bilgi için https://zenithdefense.com/ adresinden firmamızla iletişime geçebilirsiniz.

Bu doküman versiyon 1.0 olarak yayınlanmıştır.