1. Bilgi Güvenliği Yazılımları: Çeşitli donanım ve yazılımlar kullanılır. Bilgi teknolojileri yöneticiler, ihtiyaca bağlı bilgi güvenliği araçlarını temin etmek ve sistem üzerinde sürekliliğini ve güncelliğini sağlamak durumundadır. Bu araçlar birbiri yerine kullanılamazlar, birbirini tamamlayabilirler. Gereksinime göre hibrit olarak kullanılabilirler.
2. Güvenlik Duvarları(firewall): Temel ağ güvenliği sistemlerindendir. Statik izleme kabiliyetine sahiptir, üzerinden geçen trafik için belirlenen kurallara göre erişim denetimi yapmak amacıyla kullanılır. Kural tablosuna sahiptirler ve istenmeyen verileri engelleyebilirler. Dış dünya ile bağlantıyı sağlarlar. Verinin gizliliğini korurlar.
3. Saldırı Tespit ve Engelleme Sistemleri (STS): STS’ler saldırıları trafik üzerinde önceden belirlenmiş saldırı imzalarına uyan trafiği raporlayarak, kritik durumlarda sistem yöneticisini uyarabilir. Ağ trafiğine müdahale etme özellikleri yoktur. Korunmak istenen ağ seğmenlerinin bağlantıları üstüne konularak zararlı trafiğin kesilmesini sağlar. Saldırı engelleme sistemleri, trafik üzerinde önceden belirlenmiş saldırı imzalarına uyan trafiği ararlar ve bulduklarında, paket düşürme, TCP bağlantısını sonlandırma gibi eylemlerde bulunabilirler. Bu özelliklere ek olarak servis dışı bırakma saldırılarına karşı (DoS, DDoS), istatistiksel ve manuel verilmiş sınırları işleterek koruma sağlayabilirler.
4. Web Uygulama Güvenlik Duvarı: Web hizmetlerinin çok yaygın kullanılması sebebi ile üretilen bu sistemler, web hizmetlerine ve web sunucularına gelebilecek saldırıları önleyecek trafik imzaları bulundururlar.
5. Veri Tabanı Güvenlik Duvarı: Veri tabanlarına gelen sorguların incelenmesi ve olası kötücül faaliyetlerin önlemlerinin alınması gerekmektedir. Veri tabanı güvenlik duvarlı bu amaçla kullanılmaktadır. Veri sabanı güvenlik duvarları, kullanıcıların genel davranışlarını öğrenerek bunların dışına çıkılması halinde uyarı verebilen sistemlerdir. Veri tabanı güvenlik duvarı ile web güvenlik duvarlarının birlikte kullanılması sayesinde sistem kullanıcılarının web üzerinde gerçekleştirdiği eylemlerin izdüşümleri takip edilebilmektedir.
6. E-posta Güvenliği: Kurum ve kuruluşların sistemlerine dışarıdan gelebilecek SPAM ve zararlı kod içeren e postaları engellenmesi amacıyla kullanılırlar. E-posta güvenliği (gateway), ağ üzerinde Internet erişimi olan bir mail sunucu (Mail Transfer Agent, MTA) görevi ile de kullanılabilmektedir.
7. Yük Dengeleyici: Bilişim sistemlerinde işlem hacmi oldukça kritik seviyelere ulaşabilmektedir. Yük dengeleyiciler, artan trafiği, yoğun istek gelen sunucular arasında yükü paylaştırarak rahatlatırlar. Örneğin söz konusu bir web sunucu ise yük dengeleyiciler, SSL'i kendi üzerinde sonlandırır ve diğer sunuculan şifreleme yükünden kurtarıp performans artışı sağlayabilmektedir.
8. URL Filtresi ve Anti Virüs: Bilgisayar ağlarında çalışan istemci makinelerin İnternet erişimlerinin düzenlenmesi için kullanılmaktadırlar. Kurum politikaları gereği erişim yasağı bulunan sitelerin engellenmesi gibi kritik işlemleri gerçekleştiren yapılardır. Bu eylemlerin yanı sıra bu yazılımlar eğer vekil sunucu olarak çalışıyorlarsa ağ üzerindeki gelen trafiği kontrol edip zararlı yazılım analizi de yapabilmektedirler.
9. Web Cache Vekil Sunucu: URL filtreleri ile birlikte kullanılabildikleri gibi tek başlarına da kullanılabilmektedir. İnternet üzerinden aynı dosyanın birden çok kez indirilmesi durumunun önüne geçilmesi amacıyla kullanılmaktadır. Web Cache vekil sunucuları, indirilen dosyalan kendi üzerlerinde tutarak Internet bant genişliği açısından tasarruf sağlamış olurlar.
10. Transparan İçerik Yönlendiriciler: Transparan içerik yönlendiriciler, kompleks ağ yapılarında ağa bağlı istemcilerin URL filtrelemesi gibi trafik yönlendirmesi gerektiği durumlarda, kullanıcı tarafında herhangi bir ayarlama yapılmadan işlemin gerçekleştirilmesini sağlayabilirler. Böylece kullanım kolaylığı sağlanmış ve ayarların eksik yapılması durumu ortadan kalkmış olur. Ayrıca kullanıcıların istenilen vekil sunucuları kullanması garanti edilmiş olur.
11. Zafiyet Tarama Sistemleri: Bu yazılımlar, sistem üzerindeki açıklıkların tespit edilmesi amacıyla kullanılan yapılardır. Zafiyet tarayıcı sistemler, işletim sistemlerindeki ve işletim sistemi üzerinde çalışan uygulamalar içindeki açıklıkları otomatik taramalar ile bulabilmektedir. Bu sistemler ayrıca yama eksiklikleri ve kurum/kuruluş güvenlik politikalarına aykırı durumları tespit edebilme yeteneğine de sahiptirler.
12. Risk Analiz Yönetim Sistemleri: Ağ üzerinde bulunan zafiyet tarama sistemlerinden sistem açıklıklarını, güvenlik duvarı, anahtar ve yönlendirici gibi ağ aktif cihazlarımdan da yapılandırma ayarlarını toplayıp bir ağ modeli oluşturabilen yapılardır. Oluşturulan bu ağ modeli ile risk analizleri gerçekleştirilir ve bu riskler önceliklerine göre derecelendirilir. Böylece sınırlı iş gücü kaynaklarının nerede ve hangi durumda ilk önce kullanılması gerektiği ve en çok riske sahip olan sistemler gibi kritik bilgiler elde edilebilmektedir.
13. Kayıt Toplama ve Korelasyon Sistemi: Ağ üzerinde birçok cihaz ve sistem kendi üzerinde meydana gelen aktiviteleri barındıran olay kayıtlarını tutmaktadır. Bu kayıtlar, her sistem üzerinde ayrı ayrı formatlarda bulunabildiğinden bunların ilişkilendirilmesi çok zor olmaktadır. SIEM (Security Information and Event Management) adı verilen bu kayıt toplama ve korelasyon sistemleri sayesinde dağıtık halde bulunan bu kayıtlar, merkezi bir yerde toplanıp ilişkili hale getirilebilmektedir. Yazılan mantıksal kurallar sayesinde gerçek zamanlı korelasyon yapılabilir ve böylece normalde tespit edilemeyen güvenlik olayları tespit edilebilir.
14. Ağ Erişim Kontrolü: Ağ erişim kontrolü sistemleri, kurum politikalarına uymayan sistemlerin ağa dâhil olmalarını engellemek amacı ile kullanılır. Bu sayede yabancı sistemlerin ve güvenlik durumu uygun olmayan sistemlerin iç ağı tehdit etmesi önlenir.
15. Sıfır Gün Zararlı Yazılım Tespit Sistemi: Kötüye kullanım tespiti mantığı ile çalışan imza tabanlı saldırı tespit sistemleri (anti virüs vb.), kendi imza veri tabanlarında olmayan zararlı yazılımları yakalayamamaktadır. Bu durum, özellikle günümüzde artan bir hacme sahip kötücül yazılımların varlığı düşünüldüğünde oldukça kötü sonuçlar doğurabilmektedir. Bugün ortaya çıkartılan yeni bir kötücül yazılımın, ilgili tespit sisteminin imza veri tabanında yer alması uzun süreler alabilmektedir. Arada geçen süre zarfında sistemler yeni çıkartılan kötücül yazılımlara karşı savunmasız kalmaktadır. Sıfırıncı gün zararlı yazılım tespit sistemi, şüpheli gördüğü yazılımları ağ seviyesinde yakalayıp test sistemlerinde çalıştırırlar. Bu testler sonucunda imzasız olarak zararlı olduğu tespit edilen yazılımların engellenmesi sağlanmaktadır.
16. Ağ İzleme ve Performans Analiz Sistemi: Ağ üzerinde ağ trafiğini izleyip, uygulamalar ve ağ performansı hakkında bilgi toplayan yapılardır. Ağ izleme ve performans analiz sistemlerinin kullanım amacı, performans kaybı durumlarında sistem yöneticisini bilgilendirmek ve sorunun kaynağı hakkında detaylı bir raporlama sağlamaktır.
17. Veri Kaçakları Önleme Sistemi: Kurumsal açıdan önem arz eden hassas verilerin izinsiz olarak kurum dışına çıkartılmasına engel olan sistemlerdir. İstemci ve ağ düzeyinde çalışan farklı modelleri mevcuttur. İstemci üzerinde çalışan sistemlerde, taşınabilir cihazlardan oluşabilecek veri kaçaklarının önlenmesi için aygıtsal kontrol yapan bileşenler bulunmaktadır.
18. Ağ Tabanı Adli Bilişim Sistemi: Bu sistemler pasif olarak ağ trafiğini yakalayarak trafik üzerinde derin paket incelemesi yapabilme imkânı sağlarlar. Bu sistemler, bilişim sistemlerindeki bilgilerin mahkemede suçluluğun veya suçsuzluğun ispatında kullanılmak üzere incelenmesini sağlamaktadır. Ağ tabanlı adli bilişim sistemleri, sayısal verilerin elde edilmesi, korunması ve analiz edilmesi işlemlerinin kanıtın gereklerine uygun olarak adli makamlara sunulması aşamasına kadar uygulanması sürecini yönetir.
19. Tek Yönlü Veri Transfer Cihazları: Internet erişimi olmayan ağlara veri transferi yapıldığı zaman dış dünyaya veri sızmasını engellemek amacı ile kullanılan cihazlardır. Donanım tabanlı tek yönlü veri transfer cihazları, kullanılan protokolü her iki tarafa da çalışırmış gibi gösterip donanım üzerinde bir yön dışında ters tarafa veri iletişimini fiziksel olarak engelleyen yapılardır.
20. İstemci Güvenlik Ürünleri: İstemci tarafında çalışan güvenlik ürünleri, ağ seviyesinde çalışan araçlara destek niteliğindeki yapılar olup ek bir katman gibi görev yaparlar, İstemci güvenlik ürünlerine örnek olarak, anti virüs, saldırı engelleme sistemleri, veri kaçakları önleme yazılımları ve disk şifreleme yazılımları örnek olarak verilebilir.
21. Saldırı Tespit Sistemleri: Saldırılar, sezgisel olarak bir bilgi sistemi içerisinde, sistemin güvenlik politikalarını ihlal eden etkinliklerdir. Saldırı tespiti ise saldırıların türünü, şiddetini, ihlal ettiği zafiyet vb. durumları tespit etmeye, tanımlamaya yönelik olarak geliştirilen işlemlerdir. Saldırı tespit sistemleri ise, saldırıları tespit etmeye yönelik olarak geliştirilen işlemleri bünyesinde barındıran yazılımsal veya donanımsal çözümlerdir.