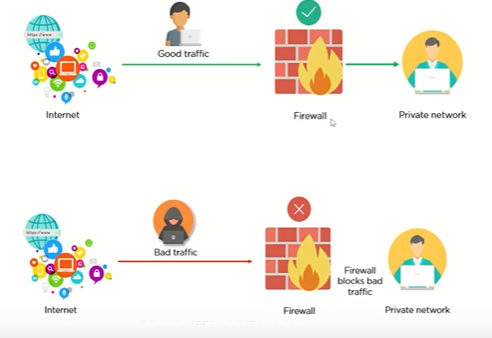
Güvenlik Duvarı (Firewall)

Güvenlik duvarı ağlar arasında veya çoğunlukla internet ve özel bir ağ arasında erişimi sınırlamak için tasarlanmış bir donanım ve yazılım bileşenleri sistemidir.

Güvenlik duvarları özel bir ağ içindeki ağ trafiğini filtreler .Bu dizi kurala göre hangi trafiğe izin verilmesi veya sınırlandırılması gerektiğini analiz eder.  
Güvenlik duvarı yalnızca kabul edecek şekilde yapılandırılmış gelen trafiği kabul eder. İyi ve kötü niyetli trafiği ayırt eder ve önceden belirlenmiş güvenlik kurallarında belirli veri paketlerine izin verir veya bunları engeller.  
Bu kurallar ,kayak, hedef ,içerik vb. gibi paket verileri tarafından belirtilen çeşitli yönlere dayanır. Siber saldırıları önlemek için şüpheli kaynaklardan gelen trafiği engellerler.  
  
**Yapısal Firewall Türleri**  
Yazılımsal güvenlik duvarları  
Donanımsal güvenlik duvarları  
**Mimarilerine göre Firewall Türleri**Paket filtreleme güvenlik duvarları: Bir ağ üzerinden gönderilen tüm bireysel veri paketlerini nereden geldiklerine ve nereye gitmeye çalıştıklarına bağlı olarak kontrol ederek temel filtreleme sunar   
Devre düzeyinde güvenlik duvarları : Denenen bir bağlantıda işlevsel paketleri kontrol eder.  
Uygulama seviyesinde güvenlik duvarları  
Yeni nesil güvenlik duvarları  
**Güvenlik Duvarı Kuralları ve Sıkılaştırma İşlemleri**



Firewall cihazlarının güvenlik seviyesini arttırarak ve olası saldırıya yönelik firewall ayarlarını ve düzenlemelerini kapsayan ,olası riskleri önlemeye çalışmak için yapılan düzenlemelere **Firewall sıkılaştırma işlemleri** denir  
**Güvenlik Duvarınızın İşletim Sistemlerini Güncel Tutun**Cihazlara erişim yönetim erişimi kazanmak   
Filtrelemeyi ve yetkisiz trafiği güvenlik duvarından geçirmek  
Güvenlik duvarını ve bir hizmet reddi durumunun oluşturulması (cihazlar üzerinde trafiğe izin verilmeyen yerlerde)  
**Güçlü ve varsayılan olmayan Parolaların yapılandırılması**Tüm varsayılan ve boş parolaların uygun şekilde güçlü şekilde değiştirildiğinden emin olmamız gerekiyor. Minimum olarak küçük ve büyük harfler sayılar ve özel karakterlerinin karışımını içeren en az 10 karakter uzunluğunda olması gerekmektedir.  
Uzaktan Yönetim Erişimini Yapılandırın  
Yönetim erişimini dahili/güvenilir ağ bölümlerini sınırlayarak ve daha geniş dahili ağdan veya internetten erişimi engelleyerek parola tahmin saldırılardan ve yönetim hizmetlerine potansiyel tehdidi büyük ölçüde azaltabilirsiniz.  
**Firewall Kuralları**  
Firewall Kuralları ayrı paketlerdeki kontrol bilgilerini inceler. Kurallar bu sayfalarda tanımlanan kurallara göre bu paketleri engeller veya bunlara izin verir. Firewall kuralları belirli aralıklarla gözden geçirilmeli ve optimize edilmeli.  
Her kuralın kural tabanında neden var olduğu kontrolü sağlanmalıdır.  
Güvenlik duvarının performansını etkileyen kural anormalliklerinin incelenmesi gerekmektedir.  
Belirli bağlantı hedef noktalarına giden trafiğe izin vermek için güvenlik duvarı kurallarını kısıtlayın.  
Dahili ortamınızda açık metin protokolleri kullanılmamalıdır. **Firewall Loglama İşlemleri**

Güvenlik duvarları güvenlik duvarının çeşitli trafik türlerini nasıl ele aldığını belgeleyen bir tür günlük kayıt özelliğine sahiptir. Bu günlükler kaynak, ve hedef IP adresleri ,bağlantı noktası numaraları ve protokoller gibi değerli bilgiler sağlayabilir.  
\*Firewalla yeni eklenen kuralların düzgün çalışıp çalışmadığını doğrulamak veya beklendiği gibi çalışmıyorlarsa hatalar var ise onları görmek için faydalı olur.  
\*Uygulama hatalarının nedeninin Windows firewall olup olmadığını belirlemek için  
\*Kötü amaçlı etkinliği tespit etmek ve yardımcı olmak için işimize yarar.  
\*Web sunucuları gibi dahili sunuculardan gelen giden bağlantılar veya saldırganın diğer ağlarda bulunan bilgisayarlara saldırı başlatmak için sisteminizi kullandığının bir göstergesi olabilir.  
**Log Dosyası nasıl oluşturulur?  
Win tuşu+R** tuşlarına basın . **wsf.msc** yazın Ve Enter’a basın

