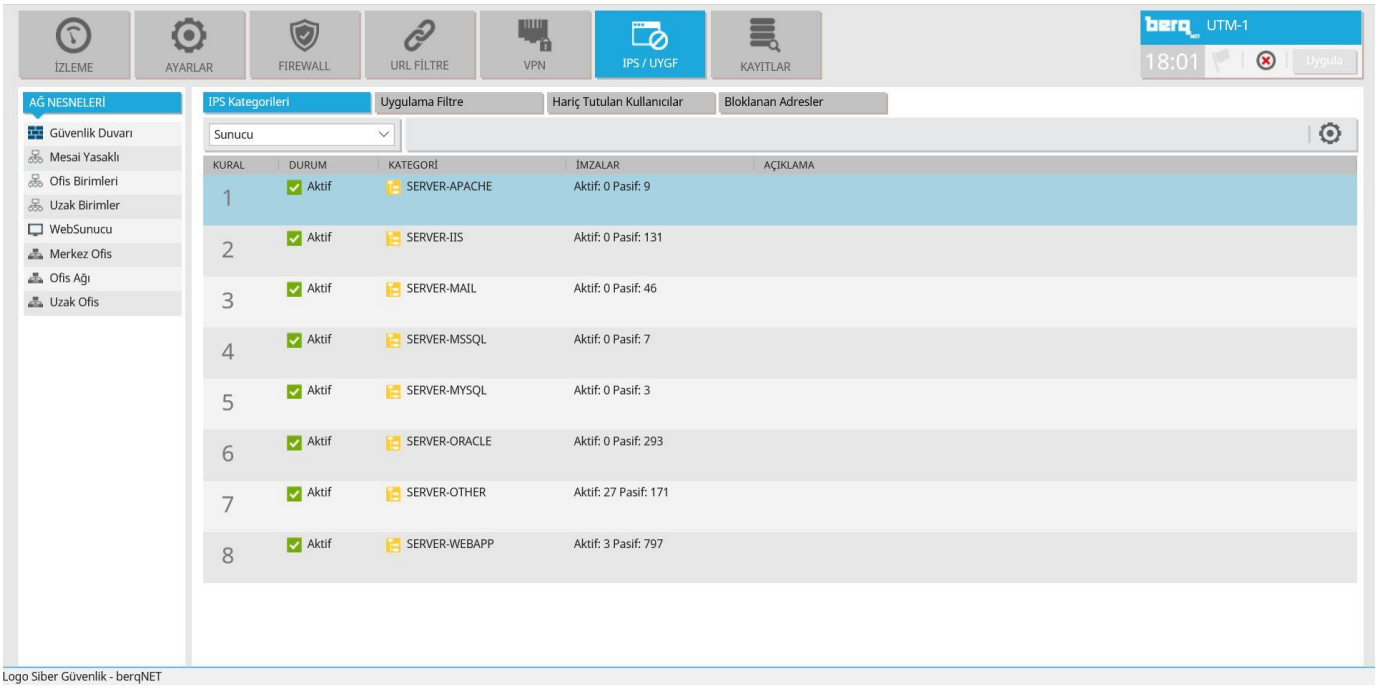
berqNET UTM

IPS (IPS/IDS)

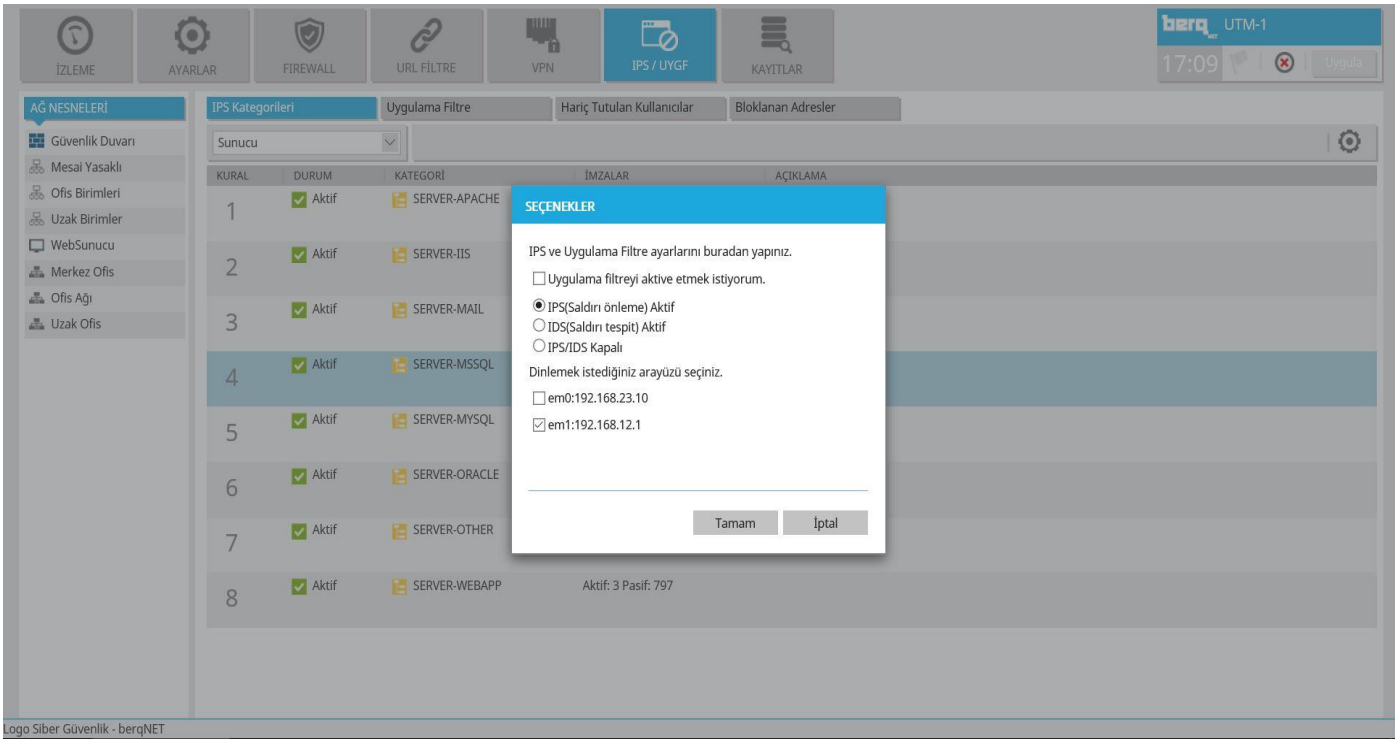
IDS, Saldırı tespit sistemidir. Teknolojik olarak dünya üzerinde bilinen ve daha önceden kaydedilmiş saldırı tipleri saldırı veritabanlarında toplanır. Kullandığımız IPS/IDS sistemleri bu veritabanlarını sürekli olarak güncel tutar ve berqNET UTM ürünlerinize gelecek saldırıları sürekli izleyebilmenizi sağlar. IDS sadece analiz ve izleme sistemleridir. Herhangi bir engelleme özellikleri bulunmamaktadır.

IDS sistemleri ile aynı teknolojiyle çalışan IPS sistemlerinde ek olarak engelleme özelliği de bulunmaktadır. Bu özellik sayesinde ek bir cihaza gerek duymadan berqNET UTM ile saldırı engelleme yapılabilir.

IPS ayarlaması için öncelikle aşağıdaki resimde de görüleceği gibi IPS / UYGF sekmesinin tıklanması gerekmektedir.

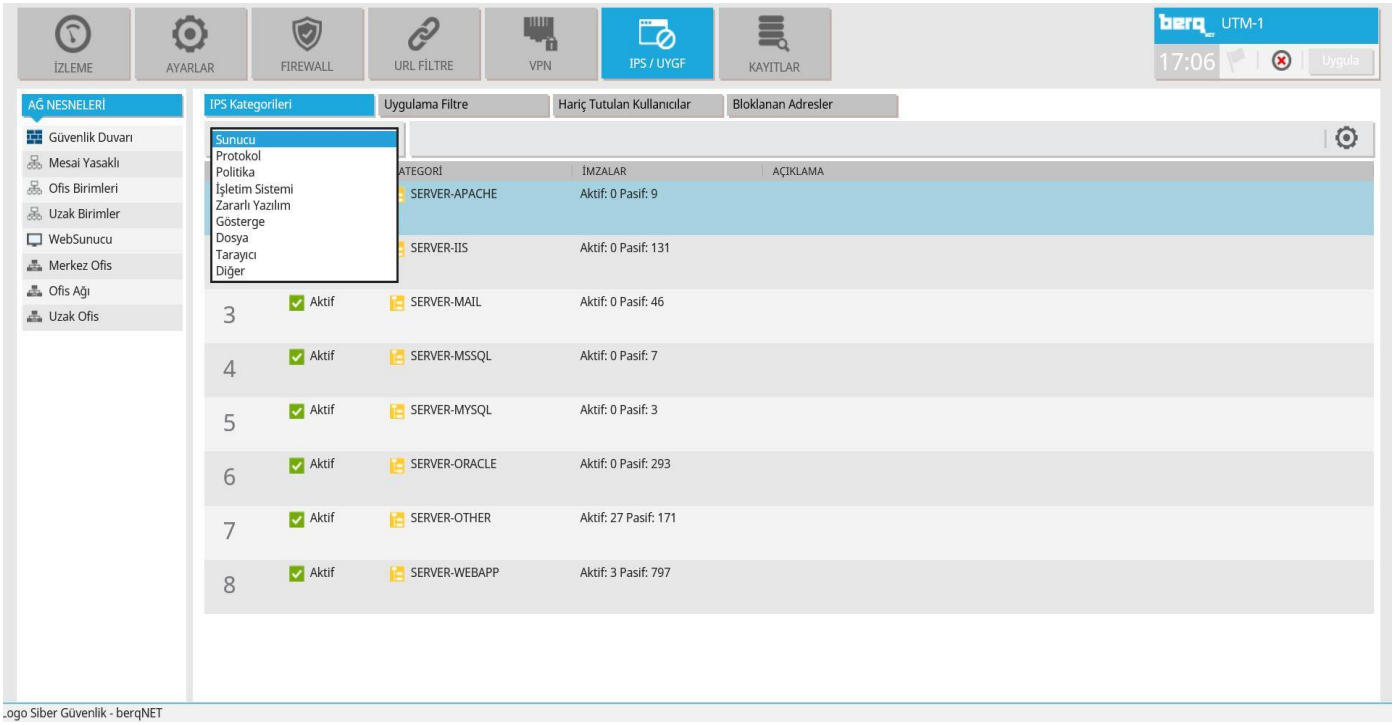


IPS Servisini aktif hale getirmek için sağ köşede bulunan çark şeklindeki butonu tıklamanız yeterli olacaktır. Ardından karşınıza aşağıdaki resimde de görüleceği gibi Seçenekler bölümü açılacaktır. Bu bölümde ‘’IPS (Saldırı önleme) Aktif’’ seçeneğini işaretleyerek IPS servisini aktif hale getirdikten sonra alt kısımda ‘’Dinlemek istediğiniz arayüzü seçiniz.’’ bölümünden IPS servisinin hangi arayüzlerde çalışacağını seçebilirsiniz. Hemen altında ise ‘’IDS (Saldırı Tespit)’’ seçeneğinde ise sadece saldırıların tespiti ve raporlaması için bu seçeneğini aktif hale getirebilirsiniz.Son olarakta tamam butonunu tıkladıktan sonra sağ üst köşede bulunan Uygula butonunu tıklamanız gerekmektedir.

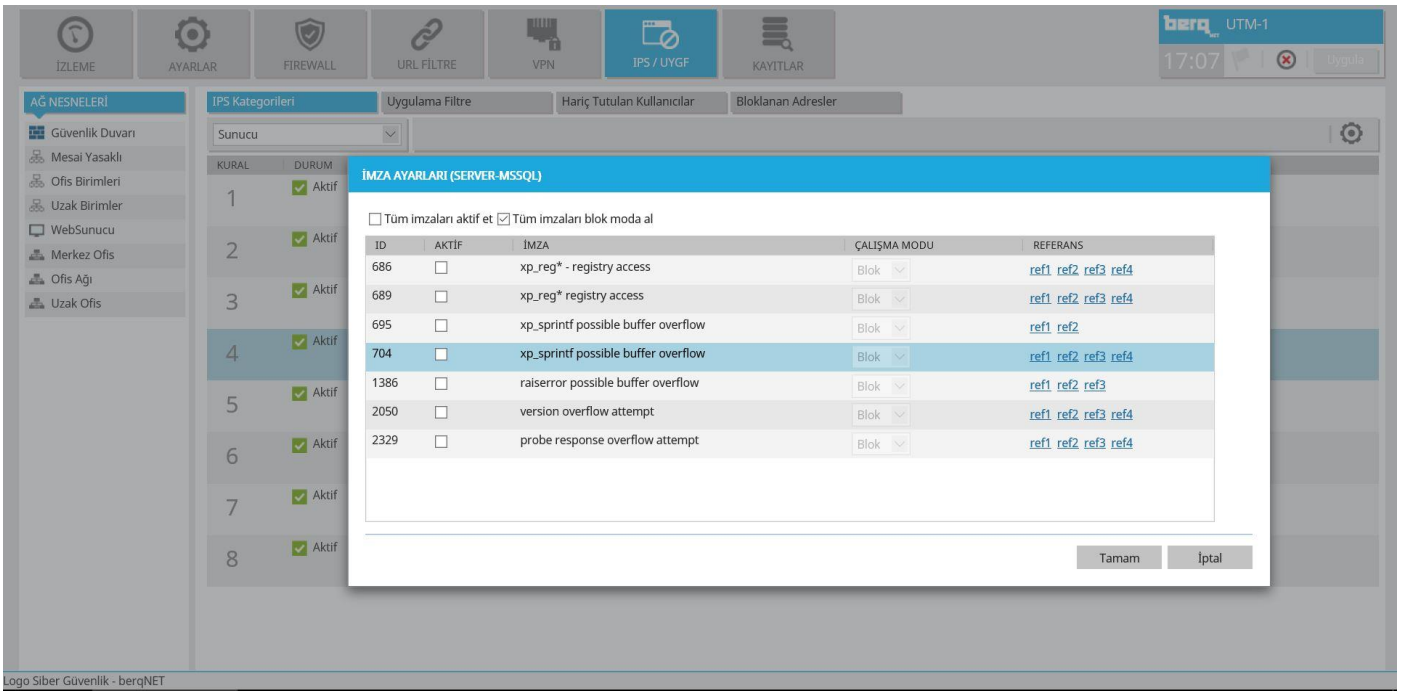


IPS servisini aktif hale getirdikten sonra saldırı tespit ve engelleme sistemi varsayılan politaka ve imzalar ile aktif hale gelecektir.

Özelleştirilmiş politika ve imza ayarlarınız için ise aşağıdaki resimde görüleceği gibi kategoriler seçeneği ile ayarlamalarınızı yapabilirsiniz.



Bu ayarlamalarınızı ise aşağıdaki resimde de görüldüğü gibi öncelikle bölümünü ardından da kategorisini tıklamanız gerekmektedir.



Örneğin yukarıdaki resimde ‘’SERVER- MSSQL’’ Microsoft SQL Server ile ilgili olarak yer alan güncel 7 adet imza bulunduğunu bunları referansları ile kontrol ederek açabilir veya üst tarafta yer alan ‘’Tüm imzaları aktif et’’ seçeneğini işaretliyerek tüm imzaları aktif hale getirebilirsiniz.

IPS Servisindeki ayarlamaların ardından belirli kullanıcı veya kullanıcı gruplarını hariç tutmak isterseniz aşağıdaki resimde yer alan ‘’Hariç Tutulan Kullanıcılar’’ sekmesinden IPS servisinden hariç tutmak istediğiniz kullanıcı veya kullanıcı gruplarınızı Kullanıcı bölümüne sürekleyip bırakmanız yeterli olacaktır.