



## Berqnet UTM (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.

KURAL	DURUM	KATEGORI	İMZALAR	AÇIKLAMA
1	Aktif	SERVER-APACHE	Aktif: 0 Pasif: 9	
2	Aktif	SERVER-IIS	Aktif: 0 Pasif: 131	
3	Aktif	SERVER-MAIL	Aktif: 0 Pasif: 46	
4	Aktif	SERVER-MSSQL	Aktif: 0 Pasif: 7	
5	Aktif	SERVER-MYSQL	Aktif: 0 Pasif: 3	
6	Aktif	SERVER-ORACLE	Aktif: 0 Pasif: 293	
7	Aktif	SERVER-OTHER	Aktif: 27 Pasif: 171	
8	Aktif	SERVER-WEBAPP	Aktif: 3 Pasif: 797	

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.

The screenshot displays the configuration interface for the IPS service in the berq UTM-1. The main window shows a table of active rules (KURAL) with columns for KURAL, DURUM, KATEGORİ, İMZALAR, and AÇIKLAMA. The rules are listed as follows:

KURAL	DURUM	KATEGORİ	İMZALAR	AÇIKLAMA
1	Aktif	SERVER-APACHE		
2	Aktif	SERVER-IIS		
3	Aktif	SERVER-MAIL		
4	Aktif	SERVER-MSSQL		
5	Aktif	SERVER-MYSQL		
6	Aktif	SERVER-ORACLE		
7	Aktif	SERVER-OTHER		
8	Aktif	SERVER-WEBAPP		

The modal window 'SEÇENEKLER' contains the following options:

- Uygulama filtreyi aktive etmek istiyorum.
- IPS(Saldırı önleme) Aktif
- IDS(Saldırı tespit) Aktif
- IPS/IDS Kapalı

Dinlemek istediğiniz arayüzü seçiniz.

- em0:192.168.23.10
- em1:192.168.12.1

Buttons: Tamam, İptal

Footer: Logo Siber Güvenlik - berqNET

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

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

The screenshot shows the management interface for the berq UTM-1 device. The top navigation bar includes icons for İZLEME, AYARLAR, FIREWALL, URL FİLTRE, VPN, IPS / UYGF, and KAYITLAR. The main content area is titled 'AG NESNELERİ' and contains a sidebar with various security settings. The 'IPS Kategorileri' section is active, displaying a table of server categories. A dropdown menu is open over the 'Sunucu' category, showing options like 'Sunucu', 'Protokol', 'Politika', 'İşletim Sistemi', 'Zararlı Yazılım', 'Gösterge', 'Dosya', 'Tarayıcı', and 'Diğer'. The main table lists categories such as SERVER-APACHE, SERVER-IIS, SERVER-MAIL, SERVER-MSSQL, SERVER-MYSQL, SERVER-ORACLE, SERVER-OTHER, and SERVER-WEBAPP, each with a status indicator (Aktif) and a count of active and passive signatures.

KATEGORİ	İMZALAR	AÇIKLAMA
SERVER-APACHE	Aktif: 0 Pasif: 9	
SERVER-IIS	Aktif: 0 Pasif: 131	
SERVER-MAIL	Aktif: 0 Pasif: 46	
SERVER-MSSQL	Aktif: 0 Pasif: 7	
SERVER-MYSQL	Aktif: 0 Pasif: 3	
SERVER-ORACLE	Aktif: 0 Pasif: 293	
SERVER-OTHER	Aktif: 27 Pasif: 171	
SERVER-WEBAPP	Aktif: 3 Pasif: 797	

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

The screenshot shows the BERQ UTM-1 management interface. The top navigation bar includes icons for İzleme, Ayarlar, Firewall, URL Filtre, VPN, IPS / UYGF, and Kayıtlar. The main content area is divided into sections: Ağ Nesneleri, IPS Kategorileri, Uygulama Filtre, Hariç Tutulan Kullanıcılar, and Bloklanmış Adresler. The 'IPS Kategorileri' section is active, showing a list of rules (KURAL) and their status (DURUM). A modal window titled 'IMZA AYARLARI (SERVER-MSSQL)' is open, displaying a table of signatures. The table has columns for ID, Aktif, İmza, Çalışma Modu, and Referans. The 'Aktif' column has checkboxes, and the 'Çalışma Modu' column has dropdown menus. The 'Referans' column contains links like ref1, ref2, ref3, and ref4. The 'Aktif' checkbox for ID 704 is checked, and the 'Çalışma Modu' dropdown is set to 'Blok'. The 'Tüm imzaları aktif et' checkbox is also checked. The 'Tüm imzaları blok moda al' checkbox is unchecked. The 'Tamam' and 'İptal' buttons are at the bottom right of the modal window.

ID	AKTİF	İMZA	ÇALIŞMA MODU	REFERANS
686	<input type="checkbox"/>	xp_reg* - registry access	Blok	ref1 ref2 ref3 ref4
689	<input type="checkbox"/>	xp_reg* registry access	Blok	ref1 ref2 ref3 ref4
695	<input type="checkbox"/>	xp_sprintf possible buffer overflow	Blok	ref1 ref2
704	<input checked="" type="checkbox"/>	xp_sprintf possible buffer overflow	Blok	ref1 ref2 ref3 ref4
1386	<input type="checkbox"/>	raiserror possible buffer overflow	Blok	ref1 ref2 ref3
2050	<input type="checkbox"/>	version overflow attempt	Blok	ref1 ref2 ref3 ref4
2329	<input type="checkbox"/>	probe response overflow attempt	Blok	ref1 ref2 ref3 ref4

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.

The screenshot displays the management interface for the berq UTM-1 device. The top navigation bar includes icons for İzleme, Ayarlar, Firewall, URL Filtre, VPN, IPS / UYGF, and Kayıtlar. The main content area is divided into several sections: AĞ NESNELERİ (Network Objects), IPS Kategorileri (IPS Categories), Uygulama Filtre (Application Filter), Hariç Tutulan Kullanıcılar (Excluded Users), and Bloklanan Adresler (Blocked Addresses). The 'Hariç Tutulan Kullanıcılar' section is active, showing a table with the following data:

KURAL	DURUM	KULLANICI	AÇIKLAMA
1	<input checked="" type="checkbox"/> Pasif	Herhangi	Bu kural ips dışı kullanıcıları tanımlamak için kullanılır.