

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.

The screenshot shows the berqNET UTM-1 web interface. The top navigation bar includes icons for İZLEME, AYARLAR, FIREWALL, URL FİLTRE, VPN, IPS / UYGF (selected), and KAYITLAR. The main content area is titled 'IPS Kategorileri' and features a table with the following data:

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 management interface of a berq UTM-1 device. The top navigation bar includes icons for Izleme, Ayarlar, Firewall, URL Filtre, VPN, IPS / UYGF, and Kayıtlar. The main content area is titled "IPS Kategorileri" and shows a list of rules with columns for KURAL, DURUM, KATEGORİ, İMZALAR, and AÇIKLAMA. A modal window titled "SEÇENEKLER" is open, allowing configuration of the IPS service. The modal contains the following options:

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

Below these options, there is a section for "Dinlemek istediğiniz arayüzü seçiniz." with two checkboxes:

- em0:192.168.23.10
- em1:192.168.12.1

The modal has "Tamam" and "İptal" buttons at the bottom. The background interface shows a table of rules, with rule 4 selected. The table has 8 rows and 5 columns. The status of all rules is "Aktif". The categories are SERVER-APACHE, SERVER-IIS, SERVER-MAIL, SERVER-MSSQL, SERVER-MYSQL, SERVER-ORACLE, SERVER-OTHER, and SERVER-WEBAPP. The total number of active rules is 3, and the pass count is 797.

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.

berq UTM-1
17:06 Uygula

İZLEME AYARLAR FIREWALL URL FİLTRE VPN IPS / UYGF KAYITLAR

AĞ NESNELERİ

Güvenlik Duvarı
Mesai Yasaklı
Ofis Birimleri
Uzak Birimler
WebSunucu
Merkez Ofis
Ofis Ağı
Uzak Ofis

IPS Kategorileri

Sınıucu
Protokol
Politika
İşletim Sistemi
Zararlı Yazılım
Gösterge
Dosya
Tarayıcı
Diğer

Uygulama Filtre

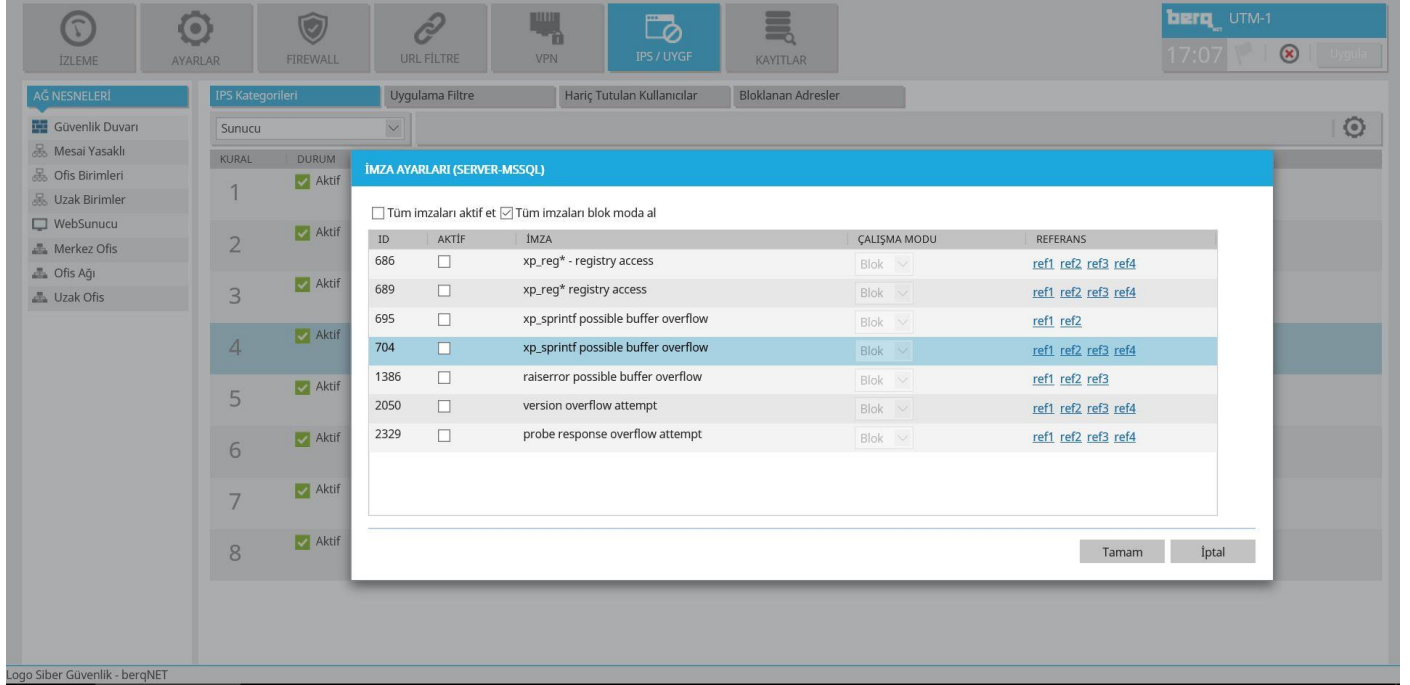
Hariç Tutulan Kullanıcılar

Bloklanmış Adresler

KATEGORİ	İMZALAR	AÇIKLAMA
SERVER-APACHE	Aktif: 0 Pasif: 9	
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	

..logo Siber Güvenlik - berqNET

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



The screenshot displays the BERQ UTM-1 web interface. The top navigation bar includes icons for 'İZLEME', 'AYARLAR', 'FIREWALL', 'URL FİLTRE', 'VPN', 'IPS / UYGF', and 'KAYITLAR'. The main area shows a list of rules under the 'IPS Kategorileri' tab. A modal window titled 'İMZA AYARLARI (SERVER-MSSQL)' is open, showing a table of signatures and their settings.

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 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 Izleme, Ayarlar, Firewall, URL Filtre, VPN, IPS / UYGF, and Kayıtlar. The main content area is divided into several sections:

- AG NESNELERİ**: A sidebar menu with options like Güvenlik Duvarı, Mesaj Yasaklı, Ofis Birimleri, Uzak Birimler, WebSunucu, Merkez Ofis, Ofis Ağı, and Uzak Ofis.
- IPS Kategorileri**: A dropdown menu currently set to 'Hariç Tutulan Kullanıcılar'.
- Uygulama Filtre**: A section for application filtering.
- Hariç Tutulan Kullanıcılar**: The active section showing a table of excluded users.
- Bloklanan Adresler**: A section for blocked addresses.

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

Logo Siber Güvenlik - berqNET