

epati

1.04. Gösterge Paneli

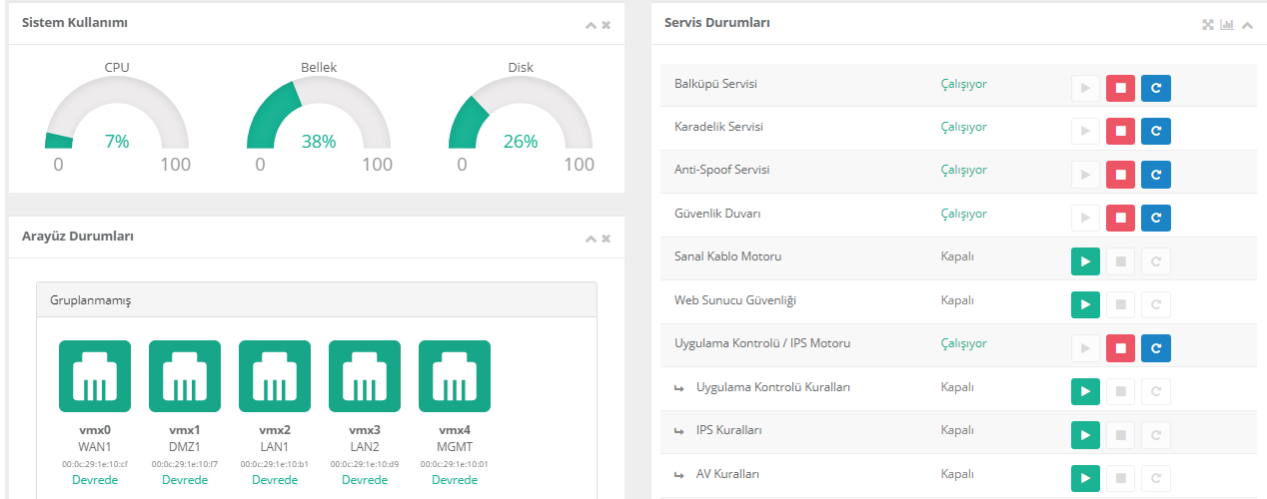
Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı
Kılavuzlar

1.04. Gösterge Paneli

Bu bölüm anlık olarak;

- sistem kullanımını,
- arayüz durumunu,
- durum (anlık oturum sayısı, sistemin çalışma süresi, vb..)
- ethernet bant genişliğini,
- network önbellek ve paket durumunu,
- bildirim geçmişini gösterir.

Aynı zamanda sayfanın sağ tarafında bulunan servis durumlarından Antikor servisleri başlatılıp durdurulabilmektedir.



Servis Durumları

- Balküüp Servisi

Balküüp, belirli konfigürasyonlar(portlar) pasif olsa da, bu konfigürasyonları aktif olarak gösterebilmektedir. Herhangi bir saldırgan bunu fark ederek bir erişim sağlamaya çalışır ise engellenecek ve logu tutulacaktır.

- Karadelik Servisi

Router tarafından iletilen DoS/DDoS saldırılarına yönelik paketlerin drop edilmesini sağlayan servistir. Servisin başlatılabilmesi için IP Havuzlarında birden fazla WAN IP adres bloğu olmalıdır.

- Anti-Spoof Servisi

Spoofing (Sahtecilik) saldırılarını önlemek amacıyla hazırlanmış yüksek teknolojiye sahip bir servistir.

- Güvenlik Duvarı

NATsız Bypass Geç, NATlı Bypass Geç, Normal Geç, Engelle, Reddet kurallarının filtrelenmesi için geliştirilmiş servistir.

- Sanal Kablo Motoru

Ağı yeniden tasarlamadan veya çevredeki ağ aygıtlarını yeniden yapılandırmadan varolan bir topolojiye ekleyebileceğiniz bir güvenlik duvarını yüklemeyi kolaylaştıran bir servistir.

- **Web Sunucu Güvenliği**

Web sunucularının güvenliğini sağlamak amacıyla geliştirilmiş bir servistir.

- **Uygulama Kontrolü / IPS Motoru**

İmza veritabanını kullanarak imza ile eşleşen uygulamaların filtrelenmesi için geliştirilmiş servistir.

- **Antivirüs Motoru**

Beyaz listedeki kaynaklar haricinde gelen datalar üzerinde antivirüs kontrolü yapmak için geliştirilmiş servistir.

- **Web Filtreleme Motoru**

Web sayfaları için belirlenmiş kuralların filtrelenmesi için geliştirilmiş servistir.

- **DNS Denetleme Motoru**

Web sayfalarının DNS üzerinden filtrelenmesi için geliştirilmiş servistir.

- **E-Posta Denetleme Motoru**

Gelen e-postaların içeriklerini denetlemek amacıyla geliştirilmiş bir servistir.

- **FTP Kontrol Servisi**

Antikor'da bulunan FTP sunucusuna bağlanabilmek için geliştirilmiş servistir.

- **SSH Denetleme Motoru**

ssh bağlantı isteklerini denetlemek amacıyla geliştirilmiş bir servistir.

- **DHCPv4 Servisi**

Dynamic Host Configuration Protocol (v4), Türkçe karşılığı Dinamik Bilgisayar Yapılandırma Protokolüdür. Yerel ağda bulunan ve internete çıkabilecek olan cihazların IP, subnet, gateway vb. adres yapılandırmalarının otomatik olarak verilmesini sağlayan bir protokoldür.

- **DHCPv6 Servisi**

Dynamic Host Configuration Protocol (v6), Türkçe karşılığı Dinamik Bilgisayar Yapılandırma Protokolüdür. Yerel ağda bulunan ve internete çıkabilecek olan cihazların IP, subnet, gateway vb. adres yapılandırmalarının otomatik olarak verilmesini sağlayan bir protokoldür. DHCPv4'ten farklı olarak NDP(Komşu Saptama İletişim Kuralı) gibi özellikleri kullanmaktadır.

- **DHCPv4 Relay Servisi**

DHCPv4 paketlerini belirlenen bir routerdan geçerek DHCPv4 sunuculara iletebilmesi için geliştirilmiş bir servistir.

- **DHCPv6 Relay Servisi**

DHCPv6 paketlerini belirlenen bir routerdan geçerek DHCPv6 sunuculara iletebilmesi için geliştirilmiş bir servistir.

- **MAC-IP Eşleştirme Servisi**

Ağa dahil olan istemcilerin MAC ve IP bilgilerinin eşleştirilmesini sağlayan servistir.

- QoS - Etkin Bant Genişliği Yönetimi

Quality of Service Türkçe karşılığı Hizmet Kalitesidir. Bu modül ile trafik akışları önceliklendirilebilir, bant genişliği rezervasyonu yapılabilir ve bant genişliği limiti belirlenebilir.

- Hotspot Servisi

Hotspot servisi, kamusal alanlarda (üniversiteler, belediyeler vb.) internet erişiminin güvenli olmasını sağlar. Her kullanıcıya özel kayıt alınarak ve logları tutularak gerekli güvenlik önlemleri sağlanmış olur.

- Bant Genişliği Monitörü

Hat üzerindeki toplam trafiğin anlık bant genişliğini monitörize eder.

- Kayıt Servisi

Antikor, internete çıkmak isteyen her istemciden kayıt olmasını isteyebilmektedir. Servis aktif edildikten sonra kayıtsız istemciler internete çıkamayacaklardır.

- Duyuru Servisi

Yerel Ağ ya da VLAN'lar için duyuru yapılabilir. İstemci internete erişmeye çalıştığında duyuru görüntülenir ve okudum tuşuna basılmadığı sürece gezintiye devam edilemez.

- Netflow Servisi

Trafiğin data başlıklarını toplayabilir ve belirlenen bir collectora (toplayıcıya) gönderilebilir. Bu sayede internet trafiğini analiz etmek kolaylaşır. Aynı zamanda QoS servisinin uygulanması için gerekli olan veya DoS saldırılarına ait IP bloklarının tespit edilmesini kolaylaştırır.

- Trafik Loglama

Güvenlik duvarı üzerinden geçen trafiğin loglanması amacıyla geliştirilmiş bir servistir.

- IPSec VPN Servisi

Merkez ve merkeze ait olan uç noktaları doğrulama ve şifreleme kullanarak birbirlerine bağlayan bir protokoldür. İçinde barındırdığı protokoller ile karşılıklı doğrulama ve anahtar değişim yetkisine sahiptir.

- SSL VPN Servisi

SSL VPN (Secure Sockets Layer Virtual Private Network) Türkçe karşılığı Güvenli Yuva Katmanı Tabanlı Sanal Özel Ağ'dır. Herhangi bir ağa uzaktan güvenli bir şekilde erişmek için kullanılır. SSL VPN sayesinde SSL Sertifikalı şifreli bir iletişim sağlanır.

- Site to Site VPN Servisi

Site to site VPN, kurumların uzak lokasyondaki ofisleri için veya herhangi bir kuruluş ile aralarında güvenli bir iletişimin sağlanması için kullanılan ortak bir ağıdır.

- RADIUS Servisi

RADIUS (Remote Authentication Dial In User Service) ağlara erişim sağlayan kullanıcıların AAA (authentication, authorization, accounting) yani kimlik denetimi, yetkilendirme ve kayıt altına alma işlemleri yapmak üzere geliştirilmiş bir servistir.

- HTTP(s) Sunucu Yönlendirme Servisi

Yerel Ağda bulunan HTTP/HTTPS sunucularının port yönlendirmeye ihtiyaç duyulmadan internete çıkarılması için geliştirilmiş bir servistir.

- LLDP Servisi

LLDP; kullanılan ağ cihazlarının markasından bağımsız olarak çalışmakta, ağ topolojileri ve ağ cihazlarını keşif protokolü olarak kullanılmaktadır. Bu servis kullanılacaksa gereken **LLDP ayarları** yapıldıktan sonra bu servis başlatılmalıdır.

- **SNMP Servisi**

Simple Network Management Protocol, Türkçe karşılığı Kolay Ağ Yönetim Protokolüdür. Layer 7(Application Layer-Uygulama Katmanı) katmanında çalışır. Ağ cihazlarının daha rahat yönetilebilmesini ve izlenebilmesini sağlayan servistir.

- **Dinamik Yönlendirme Motoru**

Dinamik yönlendirme, ağ üzerinde kullanılan routerların yönlendirme tablolarını birbiriyle paylaşmasıdır.

- **Yönlendirme - Kural Tabanlı Yönlendirme**

Kural Tabanlı Yönlendirme servisi, istenilen protokol, kaynak/hedef adres, port bilgilerine göre paketleri istenilen routera yönlendirir.

- **Yönlendirme - Multicast Yönlendirme Servisi**

Ağ üzerindeki multicast trafiğini izlemek, denetlemek ve yönlendirmek için geliştirilmiş bir servistir.

- **NAT64 Servisi**

IPv6 ağlarında bulunan cihazların IPv4 kaynaklarına erişimini sağlamak için kullanılan bir dönüşüm ve güvenlik hizmetidir. Bu servis, ağ yöneticilerine IPv6 geçiş sürecinde güvenli ve etkin bir çözüm sunmak amacıyla geliştirilmiştir.

- **MAC Karantina Servisi**

Karantinada bulunan MAC adreslerinin erişimlerinin kesilmesini sağlayan servistir.

- **Statik ARP Servisi**

Antikorum, LAN tarafında kayıtlı istemciler dışında hiçbir MAC ve IP adresi ile muhatap olmamasını sağlayan servistir. Yeni IP ve MAC adresi öğrenemeyecektir. Bu servis açık olduğu sürece Kayıt Servisi çalışmayacaktır.

- **Yerleşke Bilgi Servisi**

Sistemde bulunan çıkış etherneti ile dış kampüslerin RRD grafiklerini çizerek, oluşturulan linklerden bu RRD grafiklerin alınmasını sağlar. Aynı zamanda Aktif Cihaz sayılarını da anlık olarak verir. Oluşturulan linklerin ULAKBİM uç istatistiklerinde ilgili alanlara kopyalanması yeterlidir.

ALAN	AÇIKLAMA
	Servisi başlatmak için butona tıklanır.
	Servisi durdurmak için butona tıklanır.
	Servisi yeniden başlatmak için butona tıklanır.

ALAN	AÇIKLAMA
Kapalı	Servisin kapalı olduğunu gösterir.
Çalışıyor	Servisin çalışır durumda olduğunu gösterir.
ByPass	Alt servisin ByPass'da olduğunu gösterir. Bu sembol ana servis açılrsa dahi alt servisin başlamayacağına işaret eder.
ByPass II	Alt servisin ByPass'da olduğunu gösterir. Bu sembol ana servis açılırsa alt servisin de başlayacağına işaret eder.
Yapılandırılmadı	Servis ile ilgili herhangi bir yapılandırmanın yapılmadığını gösterir. Servisi başlatmak için arayüzde ilgili servis ile ilgili ayarlamaların yapılması gerekmektedir.
Başlatılmadı	Servis ile ilgili yapılandırmalar yapılmış fakat sonrasında hiçbir ayar girilmeden başlatılmışsa kullanıcı bu sembol ile karşılaşacaktır. (Örneğin güvenlik kurallarının boş olması durumunda Güvenlik Duvarı başlatılamayacaktır.)
Durdurulmadı	Servisin arka planda hala çalışmakta olduğunu ve durdurulmadığını göstermektedir. (Girilen herhangi bir ayar varsa Pasif'e almanız gerekmektedir.)

Gösterge Panelinde Sayfa Arama, Web SSH Servisi ve Lisans Sürüm Listesi

Sayfa aramanın nereden yapılacağı, Web SSH Servisi ve [Lisans Sürüm Listesi](#) ne nasıl gidileceği üstteki şekilde verilmektedir.

Ayrıca, sistem adı sol menüde sürekli görüntülenmektedir.

ePati Siber Güvenlik Teknolojileri A.Ş.
Mersin Üniversitesi Çiftlikköy Kampüsü
Teknopark İdari Binası Kat: 4 No: 411
Posta Kodu: 33343 Yenişehir / MERSİN

www.epati.com.tr
bilgi@epati.com.tr
+90 324 361 02 33
+90 324 361 02 39

