



# ePati

## Bilişim Teknolojileri

### AntiKor® Güvenlik & Web Filtreleme Modelleri

Özellik	AKR-G100	AKR-S100	AKR-S200	AKR-P100	AKR-P200
Yönetim Arabirimi	Web	Web	Web	Web	Web
Maksimum Throughput	32 Mbps	100 Mbps	300 Mbps	900 Mbps	2 Gbps
Çalışma Modu	PPPoE	PPPoE	PPPoE + Routing + TransparP200	PPPoE + Routing + TransparP200	PPPoE + Routing + TransparP200
AntiKor İkizler - Cluster	Yok	Opsiyonel	Opsiyonel	Opsiyonel	Opsiyonel
AntiKor İkizler - Failover	Yok	Opsiyonel	Opsiyonel	Opsiyonel	Opsiyonel
AntiKor - Yedek Hat	Yok	Opsiyonel	Opsiyonel	Opsiyonel	Opsiyonel
AntiKor - Hotspot	Yok	Opsiyonel	Opsiyonel	Opsiyonel	Opsiyonel
Güvenlik Duvarı (Firewall)	Standart	Standart	Standart	Standart	Standart
VLAN Uygulaması	Yok	Yok	Opsiyonel	Opsiyonel	Standart
DMZ Uygulaması	Yok	Yok	Opsiyonel	Opsiyonel	Standart
HTTP Filtreleme	Standart	Standart	Standart	Standart	Standart
POP3 Virüs Filtreleme	Yok	Yok	Opsiyonel	Standart	Standart
SMTP Virüs Filtreleme	Yok	Yok	Opsiyonel	Standart	Standart
POP3 Spam Filtreleme	Yok	Yok	Opsiyonel	Standart	Standart
Saldırı Tespit ve Önleme	Yok	Yok	Standart	Standart	Standart
URL Filtreleme ve Blacklist	Sadece TK Veritabanı	Sadece TK veritabanı	TK + Esnek Yapılandırma	TK + Esnek Yapılandırma	TK + Esnek Yapılandırma
Web Erişimi Raporları	Standart	Standart	Standart	Standart	Standart
Proxy Erişimi Raporları	Yok	Yok	Opsiyonel	Standart	Standart
Anlık Web Erişimleri	Yok	Yok	Opsiyonel	Standart	Standart
Anlık Proxy Erişimleri	Yok	Yok	Opsiyonel	Standart	Standart
Bant Genişliği Monitörü	Yok	Yok	Opsiyonel	Standart	Standart
DHCP Monitörü	Yok	Yok	Opsiyonel	Standart	Standart
Trafik İstatistik(Up-Down)	Standart	Standart	Standart	Standart	Standart
Rapor Arşivi(Logları Sak.)	Standart	Standart	Standart	Standart	Standart
Gözetim ekranı	Standart	Standart	Standart	Standart	Standart
Syslog Desteği	Yok	Yok	Standart	Standart	Standart
Kayıt Formu Düzenleme	Standart	Standart	Standart	Standart	Standart
İstemci Başvuruları	Standart	Standart	Standart	Standart	Standart
Karantinalı Kullanıcılar	Yok	Yok	Opsiyonel	Standart	Standart
Rapor Yönetimi	Yok	Yok	Standart	Standart	Standart
Özel Port Yönetimi	Yok	Yok	Standart	Standart	Standart
Uzantı Filtreleme	Yok	Yok	Standart	Standart	Standart
Sayfa Yasaklama	Yok	Yok	Standart	Standart	Standart
Port Yönlendirme	Standart	Standart	Standart	Standart	Standart
Statik NAT	Yok	Standart	Opsiyonel	Standart	Standart
Routing Ayarlama	Standart	Standart	Opsiyonel	Standart	Standart
Netflow Raporlama	Yok	Yok	Opsiyonel	Standart	Standart
Network Monitor	Yok	Standart	Standart	Standart	Standart
Proxy kullanıcıları	Yok	Yok	Opsiyonel	Standart	Standart
Yönetim Paneli Erişimi	Yok	Yok	Standart	Standart	Standart
Kullanıcı Yönetimi / Radius	Yok	Yok	Standart	Standart	Standart
Yedekle/Geri Yükle	Standart	Standart	Standart	Standart	Standart
Özel Kullanıcı Kontrolü	Yok	Yok	Standart	Standart	Standart
Bant Genişliği Kontrolü	Yok	Yok	Standart	Standart	Standart
VPN Uygulaması (PPTP)	Opsiyonel	Opsiyonel	Standart	Standart	Standart
VPN (Site to Site)	Yok	Yok	Opsiyonel	Standart	Standart
VPN Oturumları	Opsiyonel	Opsiyonel	Standart	Standart	Standart
IPSEC Kriptolama	Yok	Yok	DES, 3DEC, AES	DES, 3DEC, AES	DES, 3DEC, AES
İstemci Durum/Tanımları	Standart	Standart	Standart	Standart	Standart
Performans Durumu	Standart	Standart	Standart	Standart	Standart
Yardımcı Araçlar	Standart	Standart	Standart	Standart	Standart

Tabloda verilen model ve özellikleri aşağıda tek tek açıklayalım;

**ePati Bilişim Teknolojileri San. ve Tic. Ltd. Şti.**

Tel : +90 324 361 02 33 Fax : +90 324 361 02 39 Web: <http://www.epati.com.tr> ePosta: [bilgi@epati.com.tr](mailto:bilgi@epati.com.tr)

Adres: Mersin Üniversitesi Çiftlikköy Kampusu, Teknopark İdari Binası Kat:4 No:411 MERSİN

### Yönetim Arabirimi

- Kullanıcı dostu, kolay ve Türkçe desteği olan bir web ara yüzünden yönetilir.
- Yönetim paneli ile içerisindeki çoğu servis kapatılıp açılabilir. LAN, WAN ayarları değiştirilebilir ve istenirse bu sunucu uzaktan kapatılabilir.
- Sistemin CPU, RAM ve Disk Durumu yönetim panelinden takip edilebilmelidir.
- Yönetim paneline erişim kısıtlanabilir ve sadece belirtilen ip'lere giriş verilebilir.
- Yönetim paneline istenildiği kadar kullanıcı açılabilir ve bu kullanıcılara istenilen menülerin gösterim hakkı verilebilmelidir. Bu sayede hangi modül ve menüleri hangi kullanıcıların kullanacağı ayarlanabilir. Sonradan bu yetkilerde azaltma veya ekleme yapılabilir.
- Kurum içinden, evden veya internet olan herhangi bir yerden vpn ile sistem web ara yüzünü görebilme imkânı. Bu işlem için işletim sistemi bağımsızdır. Herhangi bir internet browser ile bu erişim yapılabilir.
- SFTP ile uzaktan güncelleme yapılabilir.

**AntiKor – İkiz Modeli** (Cluster + Failover Desteği)sürekliliğin sağlanabilmesi amacıyla geliştirilen bu model, ikiz AntiKor'ların eş zamanlı ve ortak çalışması temeli üstüne kuruludur. Olası sorunlarda çalışması duran ikizlerden biri, yükünü diğerine bırakır. Böylece süreklilik sağlanmış olur. Ayrıca ikizler eş zamanlı çalışmaları sayesinde yük dengeleme, trafik paylaşımı gibi verim kazançları da sağlar.

**Cluster:** İkiz AntiKor'lar, internet trafiğini dengeli bir şekilde dağıtmak amacıyla kullanılırlar. Temelde, hedef adresi kontrol ederek trafiği sıralı erişim ile yönlendiren bir sistemdir. Dinamik bir yapıya sahip olan sistem trafiği hedeflere her iki AntiKor üzerinden dağıtarak yükü dengeler. Örneğin port 80 (HTTP) üzerindeki trafiği bölüşen ikizler, kendi paylarını kendi bağlantıları üzerinden göndererek yük dengesi sağlarlar. Ayrıca bu Cluster mekanizması, Failover mekanizmasını da desteklemektedir.

**Failover:** İkizlerden birinde bağlantı kaybı yaşandığı anda, diğeri trafiği bölüşmeyi bırakıp, tamamını üzerine alarak bağlantının sürekliliğini sağlar. Temel Failover yöntemlerinden biri olan bu mekanizma tamamen otomatiktir ve bağlantı kaybı yaşayan ikiz tekrar aktif duruma gelince bölüşme süreci yeniden başlar.

### AntiKor - Yedek Hat

İnternet hattı kesildiğinde yedek bir hattın kullanılmasını sağlar. Tek bir AntiKor ile çalışan bu sistem sayesinde kullanıcılar hiç fark etmeden internetin devamlılığı sağlanmış olur.

### Güvenlik Duvarı

- Güvenlik Duvarına, Layer 3 seviyesinde sınırsız kural yazılabilir.
- Statik olarak paket filtreleme, dinamik paket filtreleme (stateful inspection-stateful screening)
- FIN veya SYN/ACK flag'lı paketlerin bir oturumun devamı olmadığını kontrol edebilir.
- Antispoof özelliği ile kendi ağında olmayan ip trafiğini engelleyebilir.
- Kaynak ve hedef ip ve port bilgilerine göre kural eklenebilir ve silinebilir.
- Kurallar tek yönlü(stateless) veya çift yönlü(keep-state) yazılabilir ve sıra numarası verilebilir.
- IP, Kullanıcı, ağ bazında kural yazılıp filtrelenebilir.
- IP-MAC Eşlemesi yapılabilir.
- Paket yönlendirme desteği vardır.
- NAT(network address translating), PAT(port adres translating) yapabilir.
- PPPoE ve Routing modunda yerel ağdaki sanal bir ip ye Port yönlendirme desteği vardır.
- Routing modunda yerel ağdaki sanal bir ip ile gerçek ipye bütün portlarıyla yönlendirme yapabilir.
- Kural hitlerinin gösterebilir.
- Birden çok Protokol kullanan uygulamalar ile çalışabilir.



### VLAN Uygulaması (IEEE 802.1Q) Modülü

#### AntiKor-P100 ve AntiKor-P200 modelleri için;

- Kurum içerisindeki yerel ağ, kurum içerisinde yönetimsel switchler (IEEE 802.1Q) özelliği sayesinde VLAN taglarını koyabilir
- Antikor ise bu tag'ları ayırarak her VLAN'a kendi içerisindeki DHCP Sunucusundan ip dağıtılabilir.
- Hem WAN tarafına hemde LAN tarafına birden fazla VLAN tanımları yapılabilir.
- Bu sayede yerel ağdaki switch'lerden gelen VLAN tag'larını ayrıştırarak farklı ağ grupları oluşturur. Bu sayede ağları birbirinden izole eder.
- Her VLAN'a DHCP ip grubu tanımlanabilir, her VLAN'e ayrı bant genişliği yapılabilir.

### DMZ Uygulaması

#### AntiKor-P200 modelleri için;

- Sunucular fiziksel olarak farklı bir switchde toplanarak hem yerel ağdan hem de internetten izole edilmelidir.
- DMZ bölgesindeki sunuculara sanal ip verilir ve Antikor'da dış dünyada görünmesi gereken ip ile eşitlenir.
- Sadece erişim verilen portlar DMZ bölgesine yönlendirilir. Erişimi olmayan portlar bloklanır.
- Kurum içinde bulunan ve hizmet veren kendi sunucularını bu DMZ bölgesine toplamalı ve sunucuların ayarlarını buna göre yapılandırılmalıdır.

### HTTP-Web Filtreleme

#### AntiKor-S100 (Ticari Amaçla İnternet Toplu Kullanım Sağlayıcıları) modeli için;

- T.İ.B. tarafından Ek-1'de belirtilen şekilde bildirilen kara liste güncellemelerini 1 gün içerisinde kullanıcılarına iletacaktır.
- T.İ.B den çekilen database'e müdahale hiçbir şekilde müdahale ettirilmeyecektir, Kullanıcı yasakları kapatamayacaktır.
- Gözetim ekranında Filtre programının açık-kapalı olduğu görülebilir.
- Antikor, bir web adresine erişimin engellenmesi durumunda, formatı T.İ.B. tarafından belirlenen uyarı sayfasını görüntüleyecektir. T.İ.B. dilediğinde uyarı sayfası üzerinde Ek-1'de belirtilen şekilde değişiklik yapabilecektir
- Güncelleme Sunucumuz Adana Maya-NET servis sağlayıcısında olup ePati Bilişim Teknolojilerine aittir.

#### AntiKor-S200, AntiKor-P100 ve AntiKor-P200 modelleri için;

#### Web Filtreleme kuralı yazabilmek için;

- Kurum içinde belirlenen politikaya göre kullanıcı grupları oluşturur ve bu grupların içine kurum içi ip'leri ekleyebilir.
- Kategoriler oluşturulur, kategoriler içerisine internet adresleri eklenebilir.
- Haftanın günleri ve saatlerine göre zaman dilimleri oluşturabilir. Bu oluşturulan grupları, kategorilere göre zaman dilimleri içerisinde yasaklayabilir.
- İçerisindeki karaliste ile konsorsiyumların tanımladığı, 5651 sayılı kanununun 8. maddesinde belirtilen ve suç teşkil eden sayfaları engelleyebilir. Sistem yöneticisi, yönetim panelinden bu sayfalara ek yapıp, çıkartabilir.

### POP3 Virüs Filtreleme

- İnternette, pop3 (mail alma - 110 nolu port) üzerinden geçen trafiği süzer. Virüsü bulduğu zaman virüsü alan kullanıcıya, bulunduğu virüsün ismini ve durum bilgisini gönderir.
- Mailin konu kısmında [AntiKor-Virus] olarak işaretlenir.
- POP3 üzerinden tarama işlemi Sistem Durumundan kapatılıp açılabilir.

<sup>1</sup>**23 Mayıs 2007**'de Resmi Gazetede Yayınlanan, **5651** Sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun": <http://www.tbmm.gov.tr/kanunlar/k5651.html>

### SMTP Virüs Filtreleme

- İnternette, smtp (mail gönderme - 25 nolu port) üzerinden geçen trafiği süzer.
- Virüsü bulduğu zaman virüsü atan kullanıcıya, bulunduğu virüsün ismini ve durum bilgisini gönderir.
- Mailin konu kısmında [AntiKor-Virus] olarak işaretlenir.
- SMTP üzerinden tarama işlemi Sistem Durumundan kapatılıp açılabilir.

### POP3 Spam Filtreleme

- İnternette, pop3 (mail alma - 110 nolu port) üzerinden geçen trafiği süzer.
- Mailleri derecelendirir ve puanlandırır.
- Kendi içinde 5 puanı geçen mailler, konu kısmında [AntiKor-SPAM] olarak işaretlenir. SPAM'li mail de ek olarak mailin sonuna eklenir. Kullanıcı bunun SPAM olmadığına karar verirse, eml uzantılı ekteki orijinal maili açıp bakabilir.

### Saldırı Tespit ve Önleme

- Sistem internet bağlantısının önünde Port bazlı saldırıları algılayabilir.
- Yönetim panelinden saldırı yapan IP adresleri görülebilir.
- Saldırıyı yapan ip'yi, deneme sayısını, byte cinsinden gelen paketin büyüklüğünü ve son deneme saatini gösterir.
- Durum korumalı(stateful) paket izleme yeteneği vardır.
- Protokol analizi, içerik arama ve denetleme yeteneği vardır.
- Portscan tespit edebilir. Bunlarda deneme sayısı ve byte cinsinden değeri o görünür.
- Gerçek zamanlı saldırı tespitini gösterebilme yeteneği vardır.

### URL Filtreleme ve Blacklist

- Yazılım "Telekomünikasyon İletişim Başkanlığı"na, Onaylı İçerik Filtreleme yazılımı olduğundan hem TİB'in sağladığı karalisteyi hemde Uluslar arası konsorsiyumundan alınan 3,5 milyonun üzerindeki veritabanını kullanır.
- İstenilen kategoriler Antikor S100-P100 ve P200'de filtreden çıkarılabilir.
- İstenildiği zaman Sayfa yasaklama Antikor S100-P100 ve P200'de durdurulabilir.

### Web Erişimi Raporları

Web Erişim kayıtları, yerel ağımızdaki kullanıcılarımızın trafik bilgilerini içeriğini değil, web sayfalarında kullanıcıların girdikleri web site başlıkları (URL), yaptığı downloadlar (sadece dosya adı), giriş yapılan saatler, en çok girilen siteler, yasaklanan sitelere girişimlerini görülebilir ve hangi siteye kimler girdiğini raporlayabilir. Bu bölümün çok ayrıntılı anlatımı ayrı bir doküman olan AntiKor Raporlama da bulacaksınız. ([http://www.epati.com.tr/docs/AntiKor\\_Raporlama.pdf](http://www.epati.com.tr/docs/AntiKor_Raporlama.pdf))

### Proxy Erişimi Raporları

Sitem ayarları kategorisinde "Proxy Kullanıcıları" kısmına tanımlanan kullanıcıların kaydını tutar. Rapor şekli tamamen yukarıda anlatılan Web erişim Raporları ile aynıdır. Bu sayede kullanıcılar evlerinden Antikoru Proxy olarak tanımlayıp internete buradan çıkabilir. Bu kişilerin erişimleri de burada tutulur. Bu sayede evden kurumun ip'si ile internete çıkılır.

### Anlık Web Erişimleri

AntiKor üzerinden geçen ve web sayfalarına bağlı olan kişileri gösterir. Kaç kullanıcı olduğunu, Bağlantı sayısını, anlık ve ortalama bilgilerini gösterir.

### Anlık Proxy Erişimleri

AntiKora Proxy üzerinden bağlı kullanıcıları ve web sayfalarında o anda hangi sayfalara bağlı olduğunu gösterir. Kaç kullanıcı olduğunu, Bağlantı sayısını, anlık ve ortalama bilgilerini gösterir.

### BantGenişliği Monitörü

AntiKor üzerinden geçen ve download yapanların son 150sn (2.5 dk) içerisindeki gelen-giden trafiği MB cinsinden gösterir. Gelen-Giden trafiği de kendi içinde Toplam, Ortalama Hız, http, FTP, P2P ve diğer olarak ayrı ayrı gösterir.

### DHCP Monitörü

Sistemden ip alan kişilerin ip, MAC adresi, bulunduğu VLAN, Kayıtlı Bilgisayar adını, Görünen Bilgisayar Adını, Toplam Kira süresi gibi bilgileri tutar. VLAN Filtrelemesi yapılabilir yani sadece bir VLANe bakılabilir. Listeleme türünde ise Anlık, İp Adresine göre veya MAC Adresine göre Listelenebilir. Listelenirken istenirse belli tarihler arası da alınabilir.

### Trafik İstatistikleri(Up-Down)

İnternet Hattının upload ve download olarak grafiklerini çizer. Bu grafikleri de Günlük, Haftalık, Aylık ve Yıllık olarak tutar.

### Rapor Arşivi(Logları Sak.)

Her gün oluşturulan raporları, günlük olarak bu menüden bilgisayarınıza indirebilir, winrar gibi sıkıştırma Programıyla indirilen dosyayı açabilir ve html olan bu dosyayı İnternet Explorer, Firefox, v.b. gibi Programlarla inceleyebilirsiniz. Flashget gibi Programlarla da topluca indirebilir, CD lerde saklayabilirsiniz. 5651 nolu yasanın 6.b bendi gereği bu raporlar 6 ay ile 2 yıl arasında saklanmalıdır.

### Gözetim ekranı

- Gözetim Ekranı, AntiKor üzerinde işleyen Filtre Programının aktif-pasifliğini ve Sunucunun kapalı olduğunu renklerle gösterir.
- Telekomünikasyon İletişim Başkanlığının istediği bir özelliktir.
- Anlık sunucuya bağlı olan bilgisayar sayısını verir.
- Karaliste versiyonunu gösterir.

### Kayıt Formu Düzenleme

Kullanıcılarımızı Sistem Ayarları kategorisinde "LAN/VLAN Ayarlarında" kısmında yasaklamayı etkinleştirdiğimizde kullanıcıların önüne gelen formu, kendi kurumumuza göre mesajı özelleştirebiliriz.

### İstemci Başvuruları

Buradaki amaç Ağımızdaki bütün kullanıcıları kayıt altına almaktır. Bu amaçla İstemciler "LAN/VLAN Ayarları"nda "Yasakla" sekmesi aktifleştirildiğinde o VLAN'daki kullanıcıların karşısına aşağıdaki forum gelir.

Kullanıcı bu formu eksiksiz doldurduktan sonra "İstemci Başvurularına" kaydı düşer. Özellikle büyük ağlarda binlerce istemcimizin olduğu düşünülürse çok büyük kolaylıktır. İstemci hangi sayfa adresini yazarsa yazsın bu ekran karşısına çıkar. Onay verilen kişi internete çıkmaya başlar. Henüz Onay verilmeyen kişiye "Başvurunuz alınmıştır. Onay işleminden sonra internete çıkabilirsiniz" diye uyarı sayfası gelir. Burada TC Kimlik numarası doğruluğunun kontrolü vardır. Geri planda kullanıcının MAC ve ip bilgisi de otomatik alınır. Kullanıcı türünde kullanıcı Misafir olarak ağımıza başvurmuşsa her gece Raporlar oluşturulduktan sonra o kişinin kaydı silinir. Bilgisayar türünün alınmasındaki amaç ise eğer o bilgisayar Masaüstü olarak kaydedilmişse ve kullanıcı yer değiştirirse farklı ip alacaktır ve bu durumda eski kaydı otomatik olarak silinir. Ama notebook ise gezici bilgisayar olarak düşünülür ve farklı ağa geçtiğinde ikinci kayıt olarak eklenir. Bu kayıtlardan "Onay" verdiklerimiz bu listeden kalkar, Değiştir diyerek kayıtları düzeltebiliriz, Uygun kayıt bilgileri girmeyenleri ise direk silebiliriz. Bu kullanıcıların önüne tekrar kayıt formu gelir.

### Karantinalı İstemciler

Antikor, Layer 2 seviyesinde arp zehirlenmesi yapan ve kendini ağ geçidi imiş gibi gösterip, MAC adresini dağıtan bilgisayarları karantinaya alır. Bundan sonra o MAC adreslerine kullanılmayan bir ip bloğundan ip vererek ağın zehirlenmesinin önüne geçer. Sistem yöneticisi web yönetim panelinden o MAC adresini karantinadan çıkartmadığı sürece o bilgisayar internete çıkamaz.

Ayrıca elle de istediğimiz MAC adresini ekleyerek internete çıkmasını engelleyebiliriz.

### Rapor Yönetimi

Rapor Yönetimi AntiKor da işleyen Log'ların kapladığı alan bilgisini verir. Buradan Log'ları temizleyebilir veya güncelleyebilir. Bunlara göz atacak olursak;

- Web Erişim Raporları; Raporlar kategorisindeki "Web Erişim Raporları"ndaki Raporları sıfırlamak için kullanılır.
- Rapor Arşivi; Raporlar kategorisindeki "Rapor Arşivi"ndeki bilgisayara indirilen linkleri sıfırlamak için kullanılır.
- Trafik Raporları; Üzerinden geçen internet trafiğinin upload/download istatistiklerini sıfırlar. Bu istatistikler yeniden çizilmeye başlar.
- Saldırı Tespit Raporları; "Temizle" butonuna basıldığında saldırı yapanların ipleri temizlenir.

### Özel Port Yönetimi

AOL / ICQ, IRC, MSN, NetMeeting portlarını sistemde kapatır veya açar, Örneğin MSN portlarını Kapat dediğimizde o ağda bulunan hiç kimse msn lerini açamaz. MSN'i kapattığımızda sadece girmesini istediğimiz kişileri Sistem Ayarları kategorisinde Özel Kullanıcı tanımlarında "MSN Kullanıcıları" bölümüne girdiğimiz kişiler MSN'e girebilir.

### Uzantı Filtreleme

- Dosyaları uzantılarına göre filtreleyebilir, yasak uzantıları engelleyebilir.
- Sistem yöneticisi yönetim panelinden bu uzantılara ek yapıp, çıkarabilir.

### Sayfa Yasaklama

- Erişime engellenen sayfa için kullanıcıya uyarı verir ve kategorisine göre ayırabilir.
- Uyarı sayfasını sistem yöneticisi tarafından web yönetim panelinden değiştirebilir.

### Port Yönlendirme

Yerel ağdaki sunucularınıza internet üzerinden bağlantı kurulabilmesi için ihtiyaç duyulan portları ilgili ip adresine yönlendirme işlemidir. TCP, UDP ve GRE Protokollerini desteklemektedir.

### Statik NAT

WAN portlarının bir tanesini veya bir grubunu, yerel ağdaki herhangi bir bilgisayara yönlendirebilir. Birden fazla ip si bulunan Frame Relay / Metro Ethernet gibi internet çıkışı olanlar, birden fazla gerçek ip'ye sahipse içerdeki herhangi bir sanal ip gerçek ip ye eşitlenir.

### Routing Ayarlama

Statik route ekleyerek site-to-site vpnlerin yönlendirmeleri yapılabilir.İstenen paketler bir başka routera gönderilebilir. Özellikle birden fazla internet bağlantısı bulunan ağlarda routing yapma ihtiyacı doğacaktır.

### Netflow Raporlama

Erişim kayıtları, 5651 sayılı kanunun<sup>1</sup> 6. maddesinin b bendine göre bütün internet trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar kullanıcı bazında saklaması gerektiğinden; trafik bilgilerinin içeriğini değil, başlık(IP ve TCP/UDP header) bilgilerini tutabilir ve bu bilgileri bir toplayıcı(collector)'ya yollayabilir. Bu bilgileri gönderirken istenirse bütün bilgileri, istenirse sadece bir ip'yi, istenirse de bir network grubunu toplayıcıya gönderebilir.

### Network Monitörü

Network Monitor, AntiKor da üzerinden geçen Layer2, Layer3, Web ve DNS paketlerini gösterir.

### Proxy kullanıcıları

Proxy olarak tanımlamak için İnternet Explorer da "Araçlar" menüsünden "İnternet Seçenekleri" seçilir. Karşımıza çıkan pencereden "Bağlantılar" sekmesindeki "Yerel Ağ Ayarları" butonuna basılır. Proxy Sunucusu kısmında Adres : "AntiKoron dış IP adresi", Bağlantı Portuna ise 4128 yazılır. En son olarak da "Yerel Adresler için Proxy Sunucusunu atla" seçeneği işaretlenir. Bundan sonra İnternet Explorer'dan hangi siteyi istersek bizden kullanıcı adı ve şifreyi ister. Bu kısma da Antikorda Proxy Kullanıcılarına tanımladığımız kullanıcı adı ve şifredir.

### Yönetim Paneli Erişimi

Sisteminin web yönetim arabirimine hangi ip'lerden giriş yapılacağını gösterir. İster her yerden erişim, istersek de kısıtlı erişim seçip sadece hangi iplerden erişeceğimizi girebiliriz.

### Kullanıcı Yönetimi

AntiKor üzerinde istenildiği kadar kullanıcı açılıp hangi menünün o kullanıcıya gösterileceği ayarlanabilir. Her kullanıcının şifresi Değiştir ile yeniden şifre atanabilir. Yetki Düzenle diyerek de yetkilerini artırıp eksiltebiliriz.

### Yedekle/Geri Yükle

AntiKor'daki bütün ayarlar kendi bilgisayarımıza alınıp istenildiği zaman yedekten geri dönülebilir. İndir butonuna basılarak yedek bilgisayarımıza kaydedilir. (Not:indirme yapılırken Flashget tarzı download Programlarınız varsa kapatınız.) Gözet seçeneği ile bilgisayarımıza aldığımız yedek tekrar sisteme atılabilir.

### Özel Port Yönetimi

Bilinen MSN, NetMeeting, IRC, ICQ gibi Programların portları yönetim panelinden kapatılabilir.

### Özel Kullanıcı Tanımları

Antikor'da bazı kullanıcılara özel ayrıcalık vermek isteyebiliriz. Bunların hepsini özel kullanıcı tanımlarından yaparız. Bunlar;

- ByPass'a yazılan ip'ler sisteme takılmadan geçer.
- Rapora dahil adminlere de her şey serbest olur ama rapora dahildirler.
- MSN Kullanıcılarına yazılan ip'lerin MSN leri genelde Port yasaklamada MSN yasaklı olsa dahi açılır.
- Doğrudan Erişime yazılan iplere erişim direk olur.
- Yasak kullanıcılara eklenen iplerin internet erişimi olmaz.

Bu ayarları sistem yöneticisi kendi kurumunun politikasına göre yapar.

### Bant Genişliği Kontrolü

- Kişi bazlı maksimum bant genişliği tanımlanabilir.
- İnternet trafiğinin hızı, port bazında sınırlandırılabilir.
- Tüm trafiğe ortak sınırlandırma getirilebilir.
- Sınırlandırmadan muaf olan portlar tanımlanabilir

### VPN Uygulaması (PPTP) ve VPN (Site to Site)

- X509 sertifika desteği vardır.
- AH ve ESP alt güvenlik Protokollerini kullanır.
- 3DES, AES şifreleme algoritmalarını kullanır.
- SHA1, SHA2, MD5 paket bütünlüğünü sağlar.
- IPCOMP ile veri sıkıştırma
- Windows istemcilerindeki pptp ile VPN'e bağlanmasını sağlar, ek Program kurmaya gerek yoktur.
- Point to Point VPN destekler.
- Site to Site VPN destekler. Bu şekilde AntiKor olan diğer birimleriyle yerel ağlarını birleştirebilir.
- VPN kullanıcıları yönetim panelinden tanımlanabilir.
- Üzerine kurulan VPN oturumlarını gösterebilir.

### VPN Oturumları

Sisteme VPN aracılığı ile bağlantı yapanların aktifliğini gösterir. Ayrıcabağlantı yapılan ip adresini de gösterir.

### Rapor yönetimi

İçerisinde günlük web istatistiklerini sıkıştırarak, her gece saat 12 den sonra o günün raporunu bir dosya halinde tutar, AntiKor yöneticisi bu logları bilgisayarına indirip saklayabilir, Raporlar html olduğundan istenilen günün raporlarını kendi bilgisayarında açıp bakabilir.

### İstemci Durum/Tanımları

Kurum içi internet kullananlar kayıt yaptırır. Tanımlı olmayan bilgisayarlar "Tanımlı Değil" şeklinde görünür.

### Performans Durumu

AntiKor'ın çalıştığı sunucunun CPU, Bellek ve Disk durumunu verir. Sistemdeki işlemcinin, günlük, haftalık, aylık ve yıllık durumlarını verir. Buradaki değerlere göre donanımın sizin yerel ağa yetip yetmeyeceği ortaya çıkar. Aynı durum Bellek ve Disk Durumu için de aynıdır.

### Yardımcı Araçlar

Sunucunun internet erişiminde kullanılacak araçları içinde barındırır.

TraceRoute Aracı → Belirttiğimiz ip'ye kadar internette üzerinden geçtiği ip'leri gösterir.

Ping Aracı → İnternetteki veya yerel ağdaki bir ip'yi ping eder.

DNS Sorgulama Aracı → herhangi bir domaini sorgular.

### Güç Yönetimi

Sistemin yeniden açılması ve tamamen kapatılması için kullanılır. Bu işlem uzaktan da yapılabilir.

## İletişim



**ePati Bilişim Teknolojileri**

**San. Ve Tic. Ltd. Şti.**

Telefon: +90 (324) 361 02 33

Web: <http://www.epati.com.tr>

<http://www.antikor.com.tr>

E-Posta: [bilgi@epati.com.tr](mailto:bilgi@epati.com.tr)

Adres: Mersin Üniversitesi Çiftlikköy Kampusu, Teknopark İdari Binası Kat:4 No:411 **MERSİN**

#### Harun SONUVAR

Bilgisayar Programcısı

Müşteri İlişkileri Yöneticisi

Tel.: 0 324 361 02 33 - 102

Cep : 0 507 310 94 92

e-mail: harun@ePati.com.tr

#### Serbest ZİYANAK

Bilgisayar Mühendisi

Network - Database Yöneticisi

Tel.: 0 324 361 02 33 - 101

Cep : 0 533 924 94 98

e-mail: serbest@ePati.com.tr

#### Kutluhan KİBRİT

Bilgisayar Mühendisi

Genel Koordinatör

Tel.: 0 324 361 02 33 - 106

Cep : 0 532 427 95 40

e-mail: kutluhan@ePati.com.tr

#### Nasır Can KIRIK

Bilgisayar Mühendisi

ArGe Yazılım Yöneticisi

Tel.: 0 324 361 02 33 - 104

e-mail: can@ePati.com.tr

#### Özkan KIRIK

Elektrik-Elektronik Mühendisi

Şirket Müdürü

Tel.: 0 324 361 02 33 - 105

e-mail: ozkan@ePati.com.tr

#### Serhat GÖKMEN

Bilgisayar Mühendisi

Yazılım Uzmanı

Tel.: 0 324 361 02 33 - 101

e-mail: serhat@ePati.com.tr

#### Hasan Fatih TÜRER

Bilgisayar Mühendisi

Yazılım Uzmanı

Tel.: 0 324 361 02 33 - 102

e-mail: fatih@ePati.com.tr

#### Fırat KAPAR

Bilgisayar Mühendisi

Yazılım Uzmanı

Tel.: 0 324 361 02 33 - 103

e-mail: firat@ePati.com.tr