FirewallSuite™ Yapılandırma Rehberi

Ürünümüzü tercih ettiğiniz için teşekkür ederiz.

Bu doküman, FirewallSuite™ ilk yapılandırma aşamalarını adım adım anlatmaktadır.

Bu belge OpenOffice.org ile hazırlanmıştır.

İçindekiler Dizini

1. TEMEL KURULUM

a. Ağ Ayarları

Ağ ayarları temelde üç bölümden oluşmaktadır. Hedef ilk önce cihazın kendisinin internete bağlanabilmesidir. Cihazımızın bir ağ geçidi olacağı göz önünde bulundurulacağından dolayı en az iki ağ kartına ve bu ağ kartlarının birbirinden ayrı segmentlerde ağlar olması gerekmektedir.

Örneğin ilk ağ kartımız her zaman internet tarafına bakmalı ve Modem/Router ile aynı ağda olmalı ve ağ geçidi, bu Modem/Router ip adresi olmalıdır.

Varsayım olarak Modem/Router ağı 10.0.0.0 iç ağımız 192.168.0.0 gibi. Bu örnek olarak verilen IP adresleri sizin ağınıza göre değişiklik gösterebilir.

Öneri olarak, iç ağ IP adreslerinde herhangi bir değişiklik yapmamak için Modem/Router kısmında yapılacak ufak bir değişiklik ile cihaz ağ geçidi olarak kolaylıkla yerleştirilebilir.

Aşağıdaki örnek senaryoya göre, cihaz bir ağa ilk kez ağ geçidi olarak konumlandırılacaktır.

- Modem/Router ağımızdaki istemcilerin ağ geçididir ve IP adresi 192.168.1.250 olarak ayarlıdır. DNS olarak da bu IP adresi istemcilerde kullanılmaktadır.
- İstemcilerin IP adresleri 192.168.1.0 ağı içindedir.

Bu en çok karşılaşılan ağ yapısıdır. Cihazın bu ağa, bir ağ geçidi olarak yerleştirilebilmesi için modemimizi 10.0.0.1 olarak ayarlayarak ağdan çıkarabiliriz. Böylece artık cihazımıza 192.168.1.250 IP adresini vererek istemcilerin ağ geçidi, DNS gibi ayarlarını değiştirmek zorunda kalmamış olacağız.

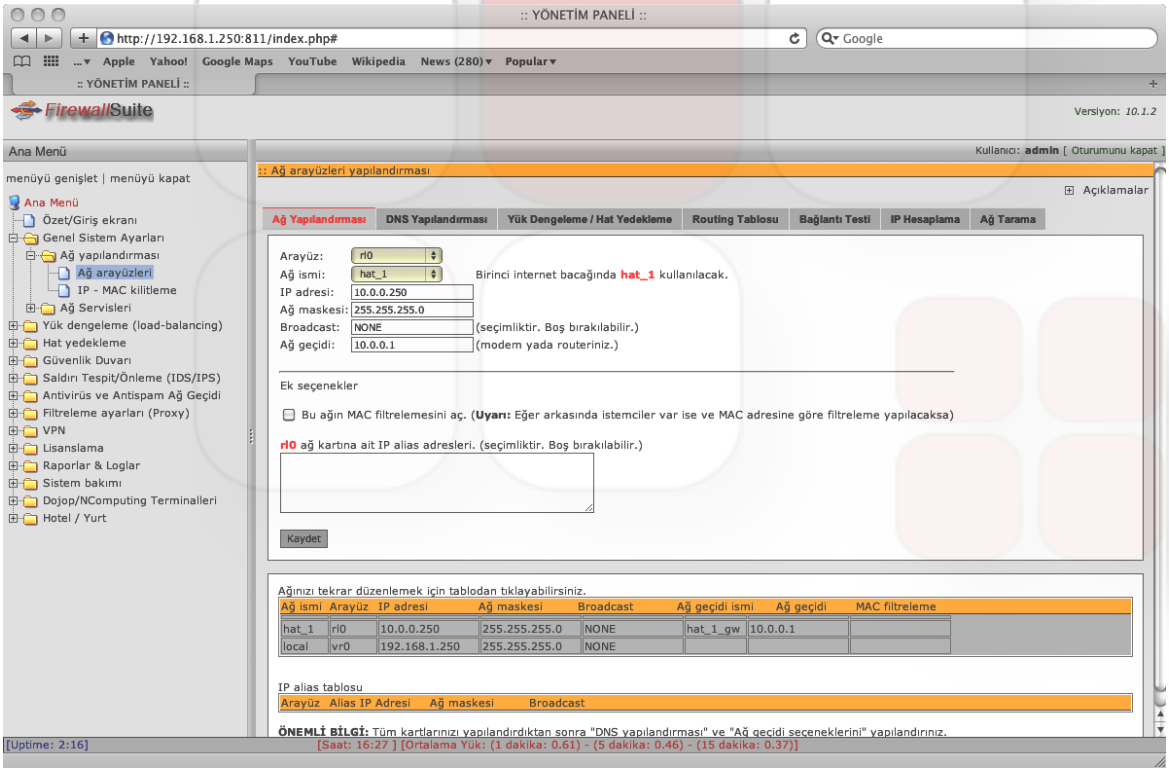
IP yapılandırırken FirewallSuite™ cihazlı olarak satın alındığında ön tanımlı olarak,

internet bacağında 10.0.0.100
iç bacağında 192.168.0.1
ağ geçidi olarak 10.0.0.1
DNS olarak ise yine 10.0.0.1 veya 8.8.8.8

IP adresleri yapılandırılmıştır.

FirewallSuite™ ürünlerinde ağ kartları kullanım kolaylığı sağlaması bakımından etiketlendirilmektedir.

İnternet bacağı her zaman birinci ağ kartıdır ve **hat_1** olarak anılır. İç ağ bacağı her zaman ikinci ağ kartıdır ve **local** olarak anılır. Sonrasında bir çok yerde ve yapılandırmada bu etiketler kullanılır.



Genel Sistem Ayarları > Ağ yapılandırması > Ağ arayüzleri

Örnek IP senaryosunda ise IP yapılandırması aşağıdaki gibi yapılandırılabilir.

b. Ağ Yapılandırması Sekmesi

Bu sekme IP adreslerinin yapılandırmasını içerir. Aşağıda örnek senaryoya göre IP adres yapılandırması yapılmıştır. İstemcilerin ağ geçidinde ve birinci DNS'lerinde 192.168.1.250 IP adresi kullanılacaktır. Hatırlatmak gerekirse bu IP adresi daha önceden Modem/Router cihazımızda yazılıydı. Ancak biz, modemi 10.0.0.0 ağına alarak interneti FirewallSuite™ cihazımıza almış olduk ve istemcilerin IP adreslerine veya ağ geçidi gibi ayarlarına dokunmamış olduk.

FirewallSuite™ cihazımızın IP adreslerini bu ekrandan aşağıdaki gibi yapılandırabiliriz.

İnternet için:

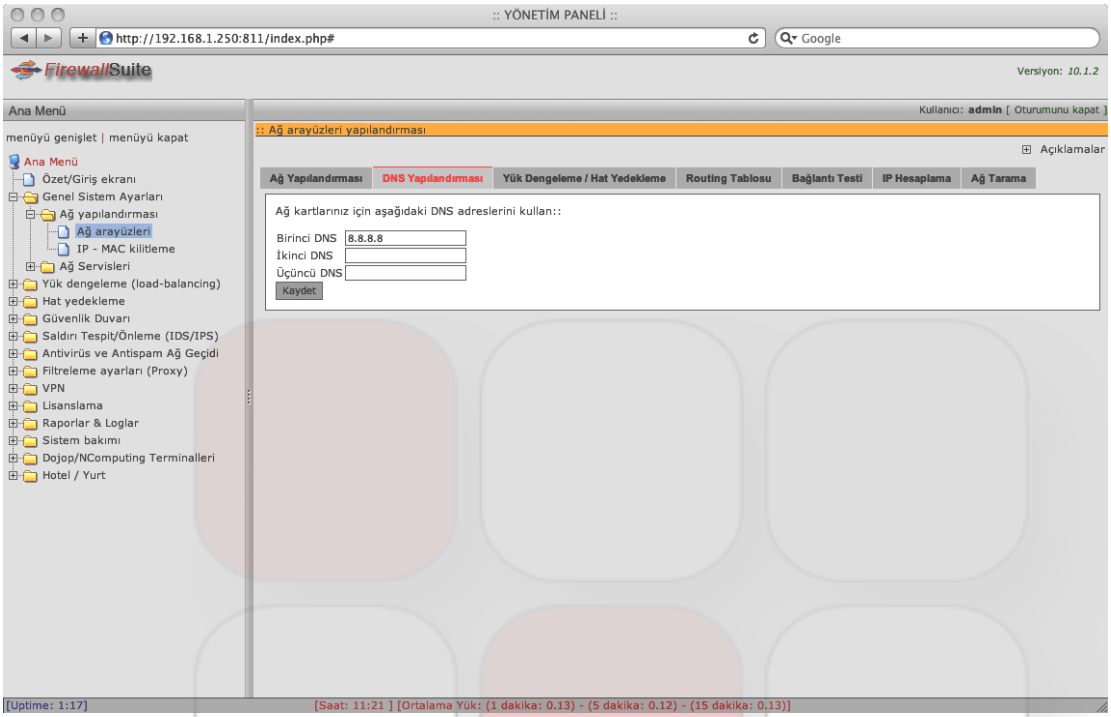
Arayüz: ilk ağ kartı
Ağ ismi: hat_1
IP adresi: 10.0.0.250
Ağ maskesi: 255.255.255.0
Broadcast: BOŞ BIRAKILIR
Ağ geçidi: 10.0.0.1

iç ağ için:

Arayüz: ikinci ağ kartı
Ağ ismi: local
IP adresi: 192.168.1.250
Ağ maskesi: BOŞ BIRAKILIR
Ağ geçidi: BOŞ BIRAKILIR
Ek seçenekler: Bu ağın MAC filtrelemesini aç işaretli

c. DNS Yapılandırması Sekmesi

Bu kısımdaki DNS FirewallSuite™ cihazımızın internet üzerindeki alan adlarını çözebilmesi için gerekli olan DNS adresidir. Genelde modem/router veya TTNET gibi servis sağlayıcıların vermiş olduğu DNS IP adresleri kullanılır.



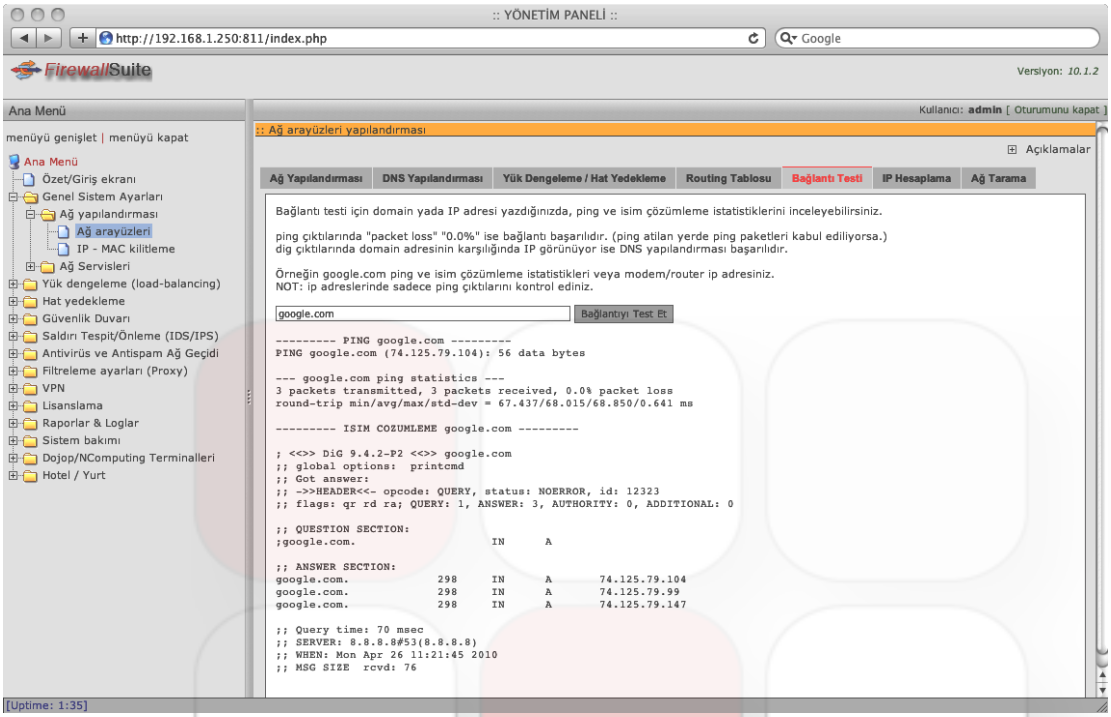
Bizim örneğimizde şu an google DNS adresi olan 8.8.8.8 verilerek konunun pekişmesi sağlanmıştır.

d. Yük Dengeleme / Hat Yedekleme Sekmesi

Bu kısımda içlerinden sadece birini seçebileceğimiz üç farklı amaca yönelik çalışma modları bulunmaktadır. Eğer tek modeminiz var ise yani yük dağıtma ya da hat yedekleme yapılmayacaksa, her zaman üçüncü seçenek olan **Tek hatlı yapı** kullanılır. IP adresi olarak Modem/Router IP adresi verilir.

e. IP Adresi Yapılandırmasının Bitirilmesi

Temel anlamda buraya kadar olan kısımda artık IP yapılandırması tamamlanmıştır. **Bağlantı testi** sekmesinden bağlantı testi yapılabilir.



f. Routing Tablosu

Diğer seçeneklerden routing tabloları isteğe bağlı olarak farklı ağlara farklı bir router'dan gidilecekse kullanılabilir. Örnek: 212.2.23.0 255.255.255.0 ağına gitmek için 10.0.0.2 router'ını kullan şeklinde belirlenebilir

2. AĞ SERVİSLERİ

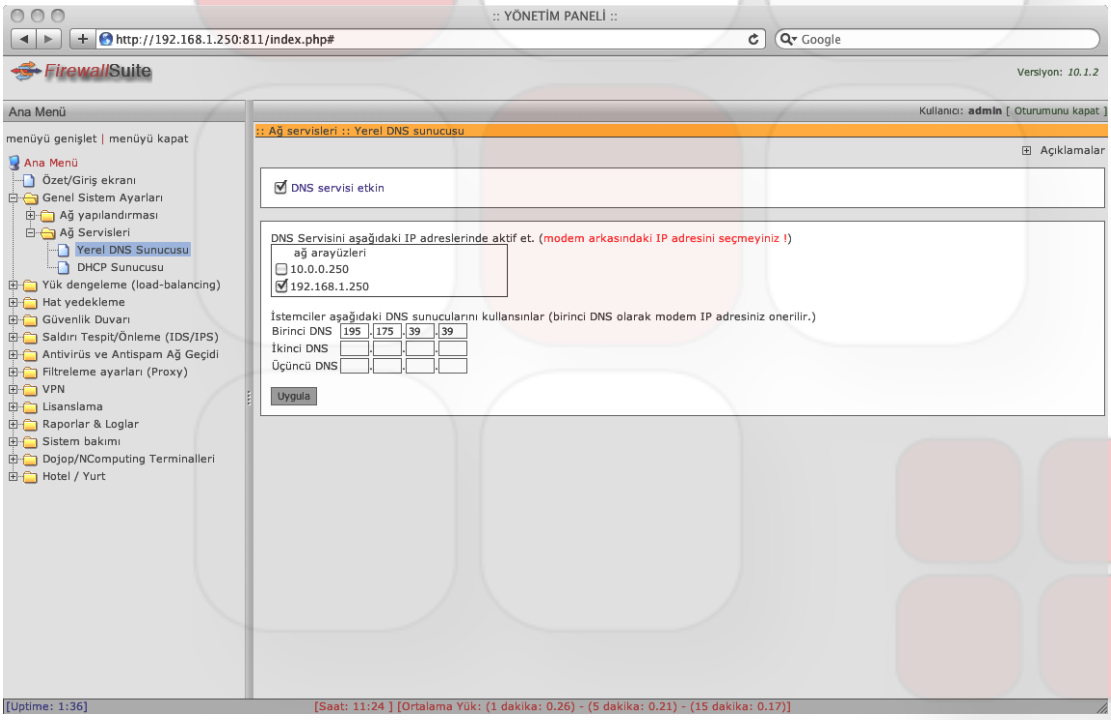
FirewallSuite™ ağ servisleri olarak, istemcilerin internet üzerindeki domainleri çözbilemesi için forwarder olarak çalışan DNS sunucusu ve iç IP dağıtımının sağlanabilmesi için DHCP sunucularını içerir.

Her iki serviste seçimliktir. Eğer bu hizmetleri sağlayan farklı cihaz yada sunucu kullanılıyorsa bu servislerin FirewallSuite™ ürününde aktif edilmesi zorunlu değildir.

a. Yerel DNS Sunucusu

FirewallSuite™ ürününde DNS sunucusu sadece forwarder olarak çalışır. Yani internet domainlerinin IP dönüşümleri için kullanılmaktadır. Eğer istemcilerinizde birinci DNS olarak FirewallSuite™ iç IP adresi yani önceki bölümdeki IP yapılandırma örneğimize göre 192.168.1.250 kullanılacak ise, DNS sunucusu etkinleştirilmelidir.

DNS sunucusunun yapılandırılması son derece kolaydır. İlk başta **DNS servisi etkin** onay kutusu işaretlenerek servisin sistem açılışında etkinleştirileceğini konusundaki ayarı yapmış bulunuyoruz.



Ağ arayüzleri: Burada iç ağımıza bakan, örneğimize göre 192.168.1.250 IP adresi seçilir.

Birinci DNS: bu kısım, servis sağlayıcınızın verdiği DNS adresi olabileceği gibi, yapıda varsa Windows DNS sunucusu da olabilir.

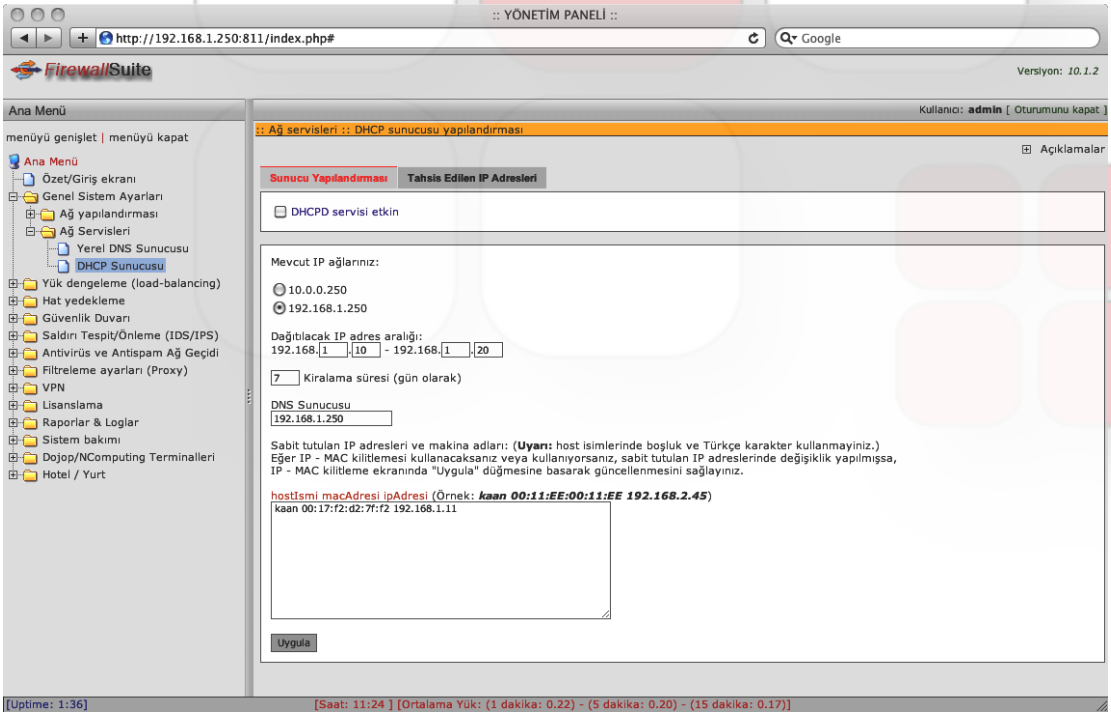
Eğer yapınızda Windows DNS hizmeti varsa, mutlaka birinci DNS adresi olarak Windows DNS sunucunuzun IP adresini vermelisiniz. Windows DNS sunucunuzun forwarder (iletici) ayarlarında ise birinci sırada servis sağlayıcınızın verdiği DNS adresi veya 8.8.8.8 gibi kullanılabilecek başka bir dış DNS olmalıdır.

Yapınızda Windows DNS sunucunuz varsa, forwarder (iletici) ayarlarında yine FirewallSuite™ IP adresini verirseniz ve FirewallSuite™ DNS kısmında Windows DNS sunucunuz var ise, DNS istekleri loop'a (kısır döngü) girebilir.

Aynı şekilde yapınızda Windows DNS sunucunuz varsa ve istemciler bu DNS'i kullanması gerekiyorsa, FirewallSuite™ DNS kısımında ise servis sağlayıcınızın DNS adresi yapılandırılmışsa ve istemcilerin birinci DNS kısmında FirewallSuite™ IP adresi yazılıysa bu sefer istemcileriniz Windows DNS servislerine erişemeyebilirler.

b. DHCP Sunucusu

İç IP'lerin dağıtımı için DHCP sunucusunu kullanabilirsiniz. Eğer ağınızda kullanmanız gereken başka bir DHCP sunucusu var ise bu servisi etkinleştirmeyiniz. Bir ağda en fazla bir adet DHCP sunucusu bulunabilir. Bu kısım yapılandırılması gerekiyorsa, ilk önce DHCPD servisi etkin onay kutusu tıklanarak bu servisin açılışta etkinleştirilmesini sağlayınız.



Seçilecek IP adresi olarak iç ağınız, örneğimize göre 192.168.1.250 olmalıdır. Böylelikle bu ağ kartının bulunduğu switch'e bağlı istemcilere IP dağıtımının yapılmasını sağlamış olur.

Dağıtılacak IP aralığı olarak, IP aralığının son iki okted'i boş bırakılmıştır. Böylelik ile ağ maskenize göre 254 host üzerinde en fazla 65535 host'a kadar IP dağıtımı sağlayabilirsiniz.

Kiralama süresi genelikle 7 gün olarak ayarlanır. Bu sayede, bir kere IP alan istemciler bir hafta boyunca istek göndermez ise IP adresi değişecektir. Bunun anlamı, 7 gün boyunca hiç açılmayan bir istemci varsa IP adresi açtığınız IP aralığı havuzuna devredilir.

DNS Sunucusu olarak, istemcilerin birinci DNS adreslerinin hangi DNS sunucusu olacağı ayarlanabilir.

Ayrıca IP adresi sabitlenmek istenirse, hostIsmi macAdresi ipAdresi biçimine uygun olarak bazı IP adresleri sabitlenebilir.

Sabitlenecek IP adreslerinin, açtığınız IP adresi aralığı havuzunda olmamalıdır.

FirewallSuite™ ürünü istenildiğinde iç IP dağıtım loglarını İletişim Daire Başkanlığı (TIB) tarafından verilen program ile (IP Log İmzalayıcı) zaman damgası (HASH) için kullanılacak log dosyasını, başkanlık tarafından verilen örneğe uygun olarak hazırlayabilmektedir.

İç IP dağıtım logları zaman damgası ile işaretlenecek ise DHCP sunucusu olarak FirewallSuite™ kullanmanız gerekmektedir.

Bununla ilgili yönergeler FirewallSuite™ yazılımında **Raporlar & Loglar > TIB (5651) Loglama** kısmında verilmiştir.

c. İstemciler İçin Filtreleme – Proxy – Firewall - Loglama

FirewallSuite™ ürünü, merkezi olarak ve kolayca istemcilerinizin internet çıkışlarının yapılandırmasını hedefler. Bu amaç ile grup mantığı ile çalışır. Örneğin 30 istemci olan bir ağda birden fazla grup açarak, her birine farklı bir anlayış ile internet hizmetlerini verebilirsiniz gibi admin tercihlerine baplı olarak kolayca tüm istemcilerinizi bir grup altında yönetebilirsiniz. Bir grup açtığınızda internet erişim haklarını merkezi bir şekilde yöneterek, firewall, proxy gibi ayarları için tekrar yapılandırma yapmak zorunda kalmazsınız.

IP yapılandırmamıza bağlı kalarak dört farklı grubun olabileceğini varsayıyoruz. Bu guruplarımız; SUNUCULAR, FINANS, GENEL ve YONETIM olacak.

Sunucularımız internete doğru çıkarken herhangi bir kısıtlamaya maruz kalmayacaklar.

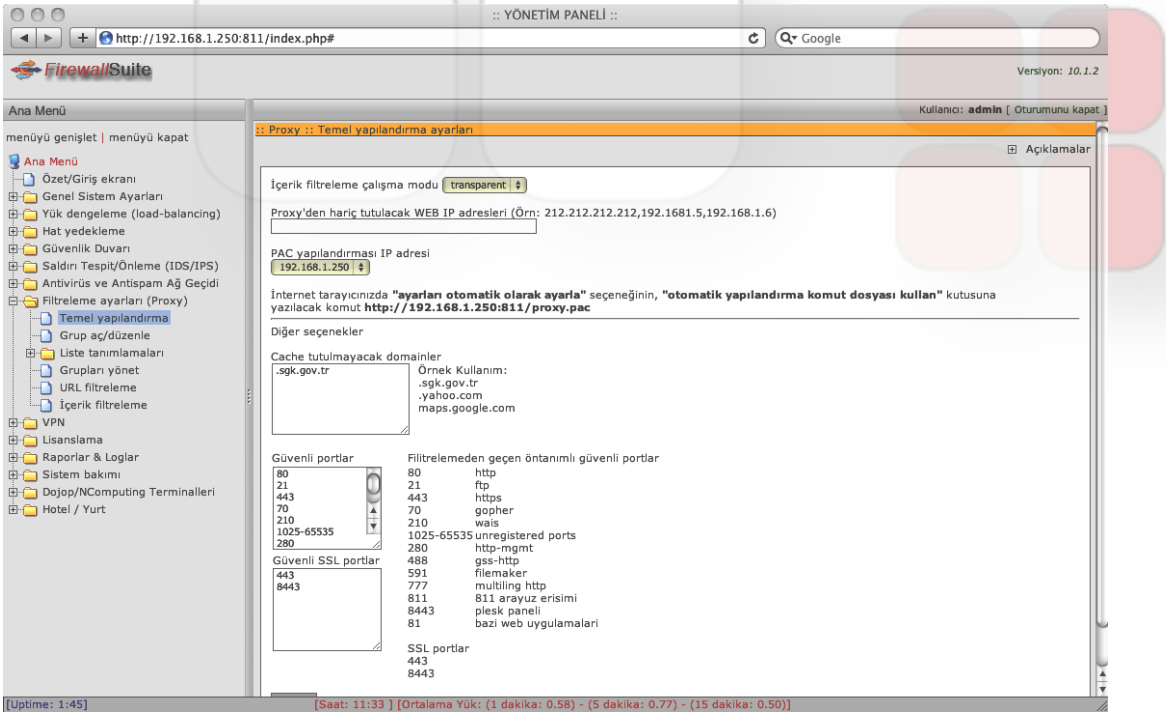
Yönetim grubu, sunuculara benzer şekilde ancak log kayıtları tutulacak.

Finans grubu sadece belirli sitelere gidebilecekler. Aynı zamanda log kayıtları tutulacak. MSN görüşmesi yapabilecek ancak MSN görüşmeleri de kayıt altına alınacak.

Genel grubu ise kısıtlı ve log kayıtları tutulacak şekilde internete çıkacaklar. Ancak MSN görüşmeleri yapamayacaklar.

d. Temel Yapılandırma

Öncelikle Filtreleme ayarları **(Proxy) > Temel yapılandırma** kısmından, PAC yapılandırması IP adresi ayarlamasında, başlangıçta örneğimiz olan iç IP adresimiz 192.168.1.250 seçilmelidir. **Kaydet** düğmesinden sonra bir sonraki adım olan, **Grup aç/düzenle** kısmından yukarıdaki gruplarımızı açabiliriz.



FirewallSuite™ transparent proxy (şeffaf proxy) teknolojilerini kullanır. Bu sayede istemcilerde proxy ayarları gibi yapılandırmalara gerek bıraktırmaz.

Yapısı gereği SSL sayfaları (bankacılık işlemleri veya benzeri gizlilik gerektiren uygulamalar) transparent (şeffaf proxy) teknolojilerde filtrelenemezler. Doğrudan istemci-sunucu mimarisinde çalışacak şekilde dizayn edilmiştirler ve FirewallSuite™ ürünü bu mimarinin gerektirdiği şeklide çalışır. Müdahale, araya girme, sızma gibi üçüncü parti yazılımları önermez ve desteklemez. Ancak proxy PAC yapılandırması özelliği ile gidilen SSL sitelerinin WEB adreslerini loglayabilir veya içerik filtreleme dışında bir yasak varsa bu adreslerin de bu kriterlere uymasını sağlayabilirsiniz.

e. Proxy PAC Yapılandırması:

Birçok internet tarayıcısında olan (İnternet Explorer, Firefox vs.) ayarları otomatik algıla seçeneği kullanılması PAC yapılandırması gereken noktalarda faydalı bir özelliktir. Seçimlik olmasına rağmen bir çok yerde kullanılan ayrıca SSL loglarının tutulmasının avantajını da getiren, proxy yapılandırması, port vs. gibi yapılandırmaları otomatik getiren bir özelliğe sahiptir. Örneğin bu ayar kullanıldığında, ağımızda bulunan bir laptop bizim ağımızdaki proxy özelliklerini alırken, dışarıya çıkarıldığında otomatik olarak devre dışı kalarak, transparent proxy gibi çalışmayı hedefler. PAC yapılandırması kullanılacağı zaman, internet gözatınızın proxy ayarlarında, ayarları otomatik algıla seçeneği etkinleştirilerek, http://192.168.1.250:811/proxy.pac yazıldığında FirewallSuite™ proxy ayarları istemci tarafından otomatik algılanarak, elle başka bir ayar yapmaya gerek bıraktırmaz.

f. Proxy'den Hariç Tutulacak WEB Adresleri:

Eğer proxy'den atlanacak dış IP adresleri varsa, yine bu kısımdaki Proxy'den hariç tutulacak WEB IP adresleri kısmında, arada boşluk olmadan, virgül ile ayırarak yazılabilir. Buraya yazılan IP adreslerindeki WEB sunucular proxy üzerinden geçirilmeden doğrudan erişimi sağlanır.

Cache olarak tutulmayacak domainler ile bazı web sayfalarının cache içinden değil ancak filtrelenerek gelmesi sağlanabilir.

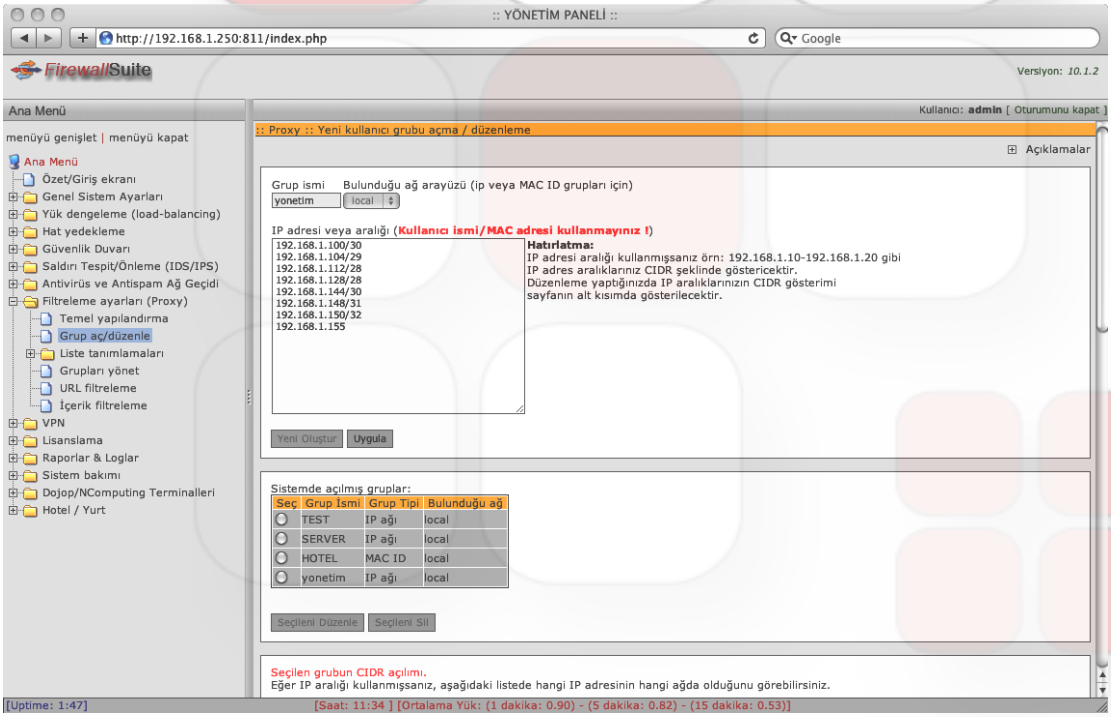
g. Grup Aç/Düzenle

Örneğimizdeki grupların açılacağı kısım burasıdır. Gruplar IP adreslerine göre veya MAC adreslerine göre açılabilir. IP adresleri 192.168.1.10-192.168.1.20 gibi aralık verileceği gibi tek tek de yazılabilir veya her iki türlü de olabilir.

Örnek:

192.168.1.10-192.168.1.20
192.168.1.24
192.168.1.55

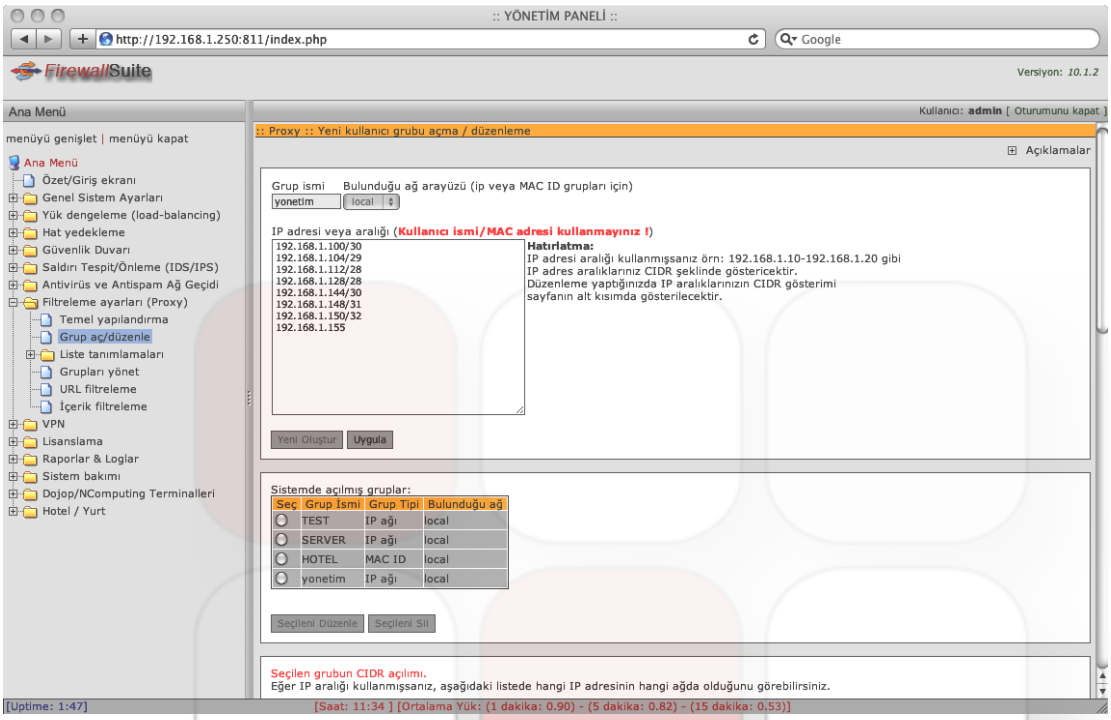
gibi.



IP aralıklarında sistem otomatik olarak aralıktaki IP adreslerini alt ağlara (CIDR) bölecektir. Grubu düzenlemek istediğinizde bu alt ağların tüm açılımını özet olarak verecektir.

MAC adreslerinde dikkat edilmesi gereken nokta, local ağın bu özelliği ağ ayarlarında açılmış olması gerekmektedir. Zaten örneğe göre ağ ayarlarında MAC adres filtrelemesini açmıştık.

Grup açılırken, ağ tipi ve bulunduğu arayüz seçilmelidir. Arayüz, normal şartlarda her zaman **local'**dir.



Her bir gurubu, gruba özgü grup ismi vererek açtığınızda, **Grupları yönet** kısmından, ilgili grup seçilerek yönetimi sağlanır.

Gruplar açıldığında, IP adresleri birbirini kapsamamalıdır. Örneğin bir grup, 192.168.1.10-192.168.1.50 aralığına sahipken, başka bir grupta bu IP aralığında herhangi bir IP adresi olmamalıdır.

h. Liste Tanımlamaları

Liste tanımlamalarında yönetici kendi kriterlerini belirtebilir. Istediği kadar liste veritabanı açıp, istediği gruplara uygulayabilir.

FirewallSuite™ ürününde internet erişim yetkilendirmesine ilişkin 7 çeşit veritabanı açılabilir. Bunlar,

- Yasaklı siteler
- Sadece izin verilen siteler
- Hariç tutulan siteler
- Yasaklı kelimeler
- Yasaklı dosya uzantıları
- Uygulama tipi yasaklar
- Band genişliği tanımları

Listeler tamamen seçimliktir ve yöneticinin, ağına göre ihtiyaçlar ile ilgilidir. Listelerin dışında FirewallSuite™ ürününde hem dünyaca kullanılan hazır gelen URL veritabanı hemde içerik filtreleme vardır. İçerik filtreleme ile URL kontrolunen farklı olarak sayfanın tüm iç yapısı kontrol edilir.

i. Yasaklı Siteler

Domain bazında, yöneticinin kendi karar verdiği siteleri kapsar. Her bir site http:// veya www olmadan başında nokta ile başlamalıdır. Örnek,

.google.com
.yahoo.com

gibi. Bu sayede ana domain ile birlikte alt domainlerde kapsam içine girer. Ayrıca belirli bir alt domainli site varsa shop.apple.com gibi de yazılabilir. Bu durumda sadece ilgili site kapsam içine girer.

j. Sadece İzin Verilen Siteler

Bu tip veritabanı, sadece gidilebilen domainleri kapsar. Kullanımı yine **yasaklı siteler** gibidir. Bu özellik uygulanan grup sadece belirtilen sitelere gidebilir. Örneğin finsans grubu için, işletmenin çalıştığı bankalar yazıldığında sadece bankalara gidebilir. Ayrıca .com.tr .gov.tr gibi üst seviye domain desteği de vardır.

k. Hariç Tutulan Siteler

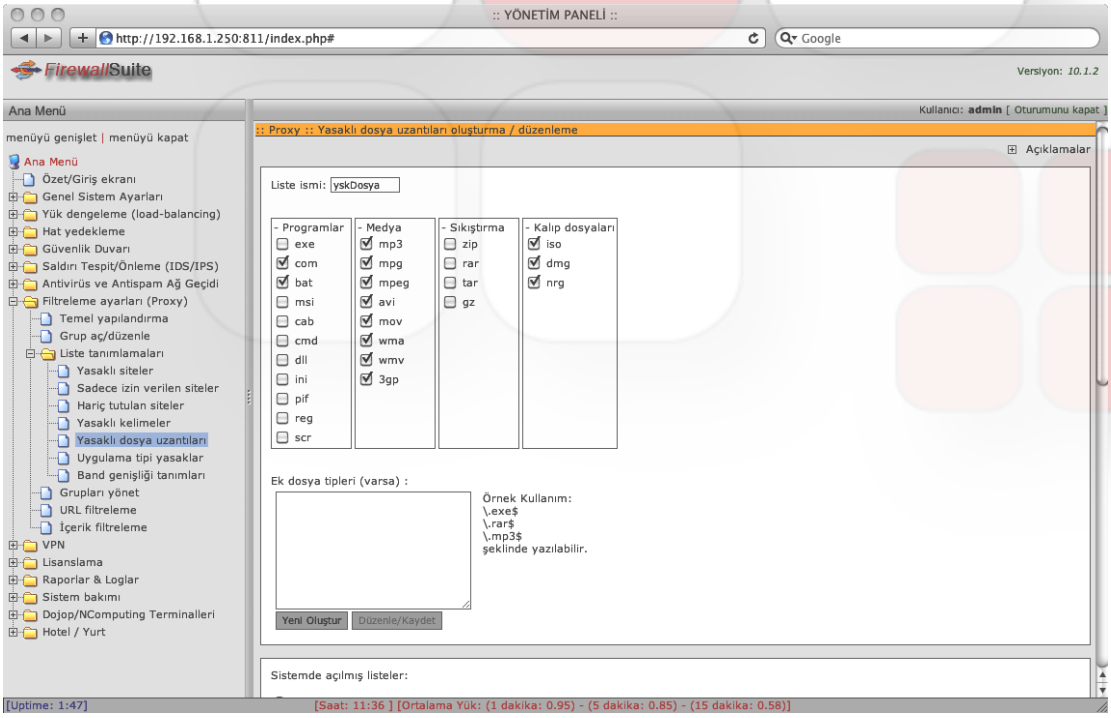
Tüm yasaklardan hariç tutulacak siteleri kapsar. Örneğin dosya indirme yasakken, güncelleme sitelerini yazdığınızda, bu tip yerlerden dosya indirme serbest bırakılır. Örneğin, antivirüs yazılımlarınızın siteleri, kullandığınız işletim sistemlerinizin siteleri gibi. Kullanım şekli yine **yasaklı siteler** ile aynıdır.

l. Yasaklı Kelimeler

URL bazında yasaklanan kelimeleri içerir. Örneğin, genelde messenger ya da tünel sitelerinin alan adlarında ya da alt domainlerinde veya bağlantılarında "messenger" veya "tunnel" kelimeleri geçmektedir. Benzeri şekilde "xxx", "porn" gibi kelimeler de uygunsuz sitelerde geçmektedir. İstenmeyen kelimeleri alt alta olacak şekilde yazıp, kendi veritabanınızı da oluşturabilirsiniz.

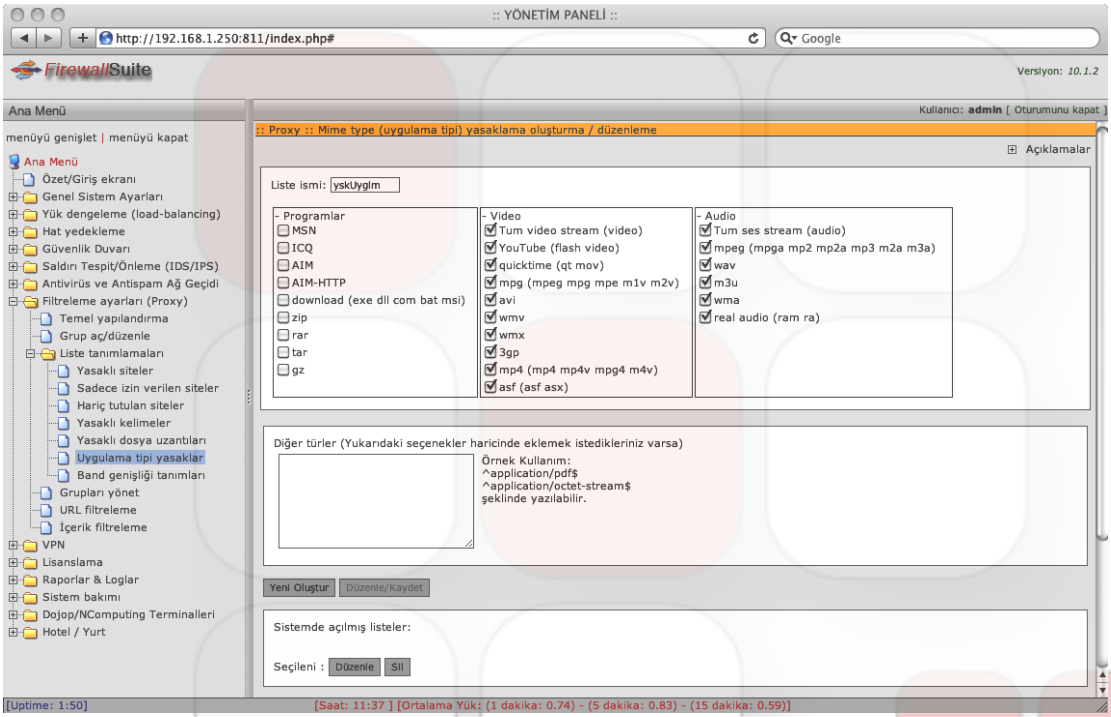
m. Yasaklı dosya uzantıları

İndirilebilir dosya tiplerinin yasaklamasını yapabilirsiniz. Ancak bu sistem sadece dosya uzantıları ile sınırlı değildir. Aynı zamanda bu dosya uzantılarını kota sınırlaması ile de destekleyebilirsiniz. Açtığınız veritabanını gruba uygularken, bu dosyaların yasaklanması mı veya dosya başına uygun görülen MB cinsinden kota miktarıda belirlenebilmektedir.



n. Uygulama Tipi Yasaklar

Uygulama tipi yasakları internet gözatıcınzın penceresinde olabilecek uygulamalardır. Örneğin video seyretme, müzik dinleme gibi. Kullanımı yasaklı dosya uzantılarına benzerdir ve kota konulabilir.

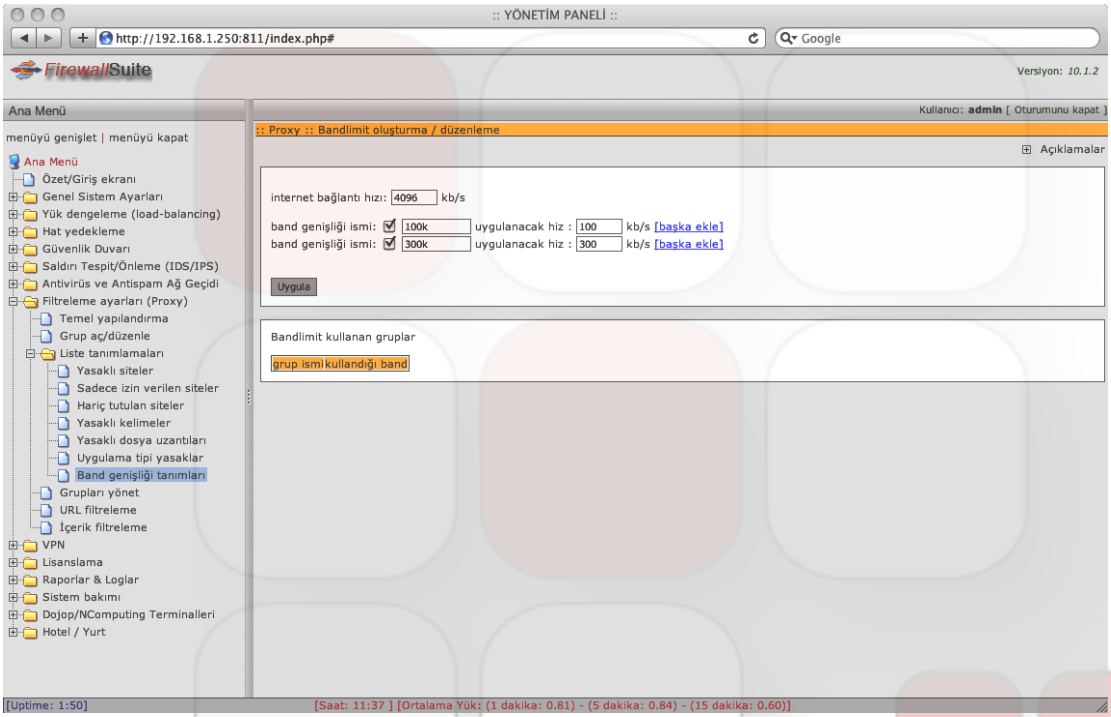


o. Band Genişliği Tanımları

Çeşitli band genişlikleri veritabanı oluşturularak, istenilen grupların internet trafiği yavaşlatılabilir veya bazı grıplar aynı zamanda serbest bırakılabilir. FirewallSuite™ toplu olarak gruplara tanımlayabileceğiniz 5 farklı band genişliği tanımlamasını destekler.

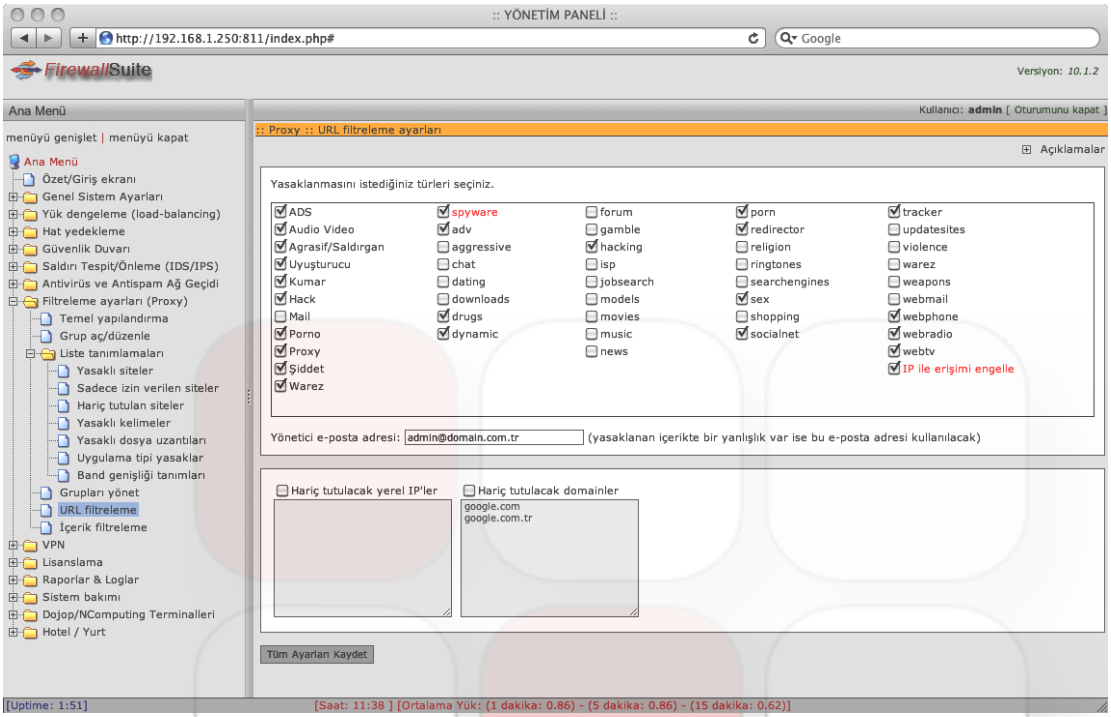
p. URL Filtreleme

URL veritabanı 45 ayrı kategoride ve toplamda 2.5 milyon, kullanıcılar tarafından şikayetler üzerine oluşturulmuş veritabanını kapsar. Aynı zamanda IP adresi ile sitelere erişimi de bu kısımdan kapatabilirsiniz.

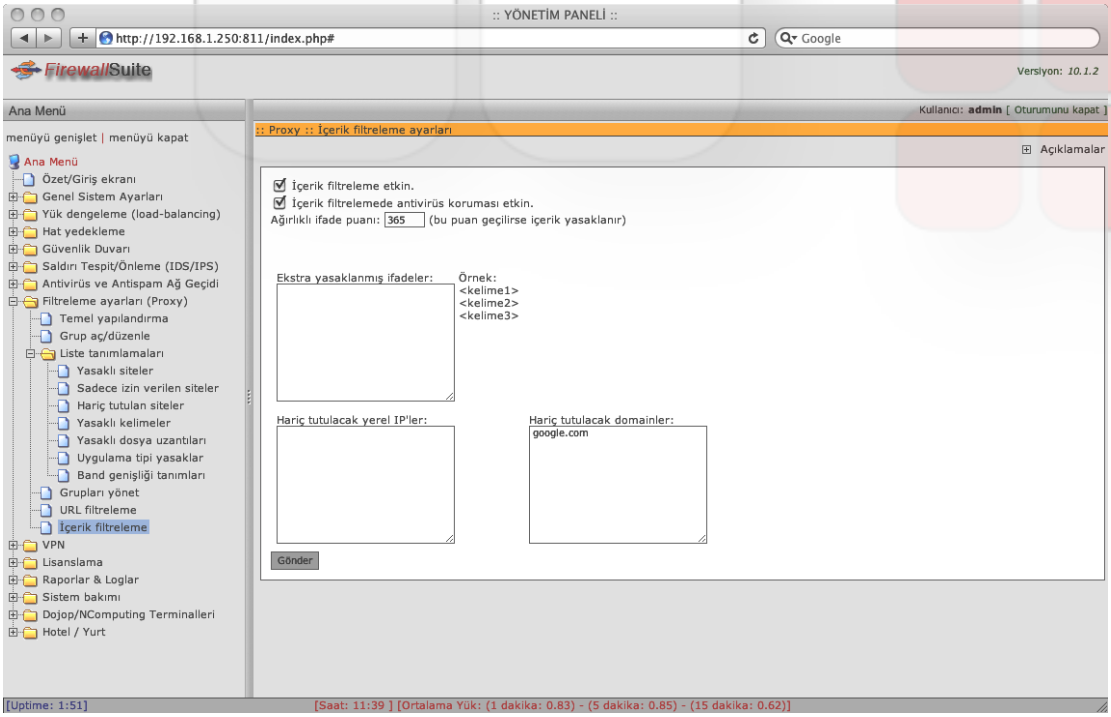


r. İçerik Filtreleme

Sayfanın tüm içeriğine bakılan kısımdır. Yine bu kısımda hariç tutulacak domain veya iç IP adresleri yapılandırmasını da yapabilirsiniz. İçerik filtreleme puantaj sistemi ile bakar ve daha çok uygunsuz yerli veya yabanci sitelere gidişi engeller. Aynı zamanda antivirüs sistemi ile de sayfa içerikleri bu kısımda kontrol ettirilebilir.



FirewallSuite™ diğer tüm yasaklama modüllerinde olduğu gibi yasaktan etkilenmesine rağmen açılması gereken bir domain adresi söz konusu olduğunda her tür yasaklama ekranı altında yer alan beyaz listeler kullanılabilir. FirewallSuite™ kara listeler içinde beyaz listeleri desteklerek kullanıcısına çok geniş opsiyonlar sunar.



s. Grupların Yönetimi

Gruplar bu kısımda merkezi olarak kolaylıkla yönetilebilir. Daha önceden açılan tüm veritabanları bu kısımda istenilen gruba atamasının yapılacağı gibi, port bazında yapılan tüm yapılandırmalar da bu kısımdan gruba uygulanır. Öntanımlı olarak tüm çıkışlar kapalıdır. İlgili grup seçildiğinde, ilk başta **WEB isteklerini PROXY arkasına al** ve **LOG tut** işaretlenerek saydam proxy bu gruba uygulanmış olur. Yine ilgili grubun MSN ve yahoo görüşmelerinin kayıt altına alınıp, alınmayacağı, internet üzerinde hangi servislerin kullanılacağı bu kısımda yapılandırılır.

Yine aynı şekilde, örneğin bir dosya indirme yasağı varsa bu kısımda, yasaklı dosya uzantılarına tıklayarak, açılan veritabanları bu kısımda seçilen gruba ataması yapılmış olunur.

Grupların yönetimi ilk yapılandırmada en son yapılan ayarlamadır. Gruba ilgili atamalar yapıldığı anda veya **WEB isteklerini PROXY arkasına al** işaretlenip, kullanabilecekleri servisler seçilip kaydedildiği anda ilgili grup internete girebilir.

Eğer açılan grupların dışında hiç bir makinenin web isteklerine ulaşmamasını istiyorsanız, Güvenlik duvarı > Paket filtreleme > Kural tablosunu göster diyerek, 80 443 portlu olan kuralı silebilirsiniz. Kural sildikten sonra Yapılandırmayı Kontrol Et düğmesine ve Yeniden Başlat düğmesine basınız. İlk düğme kural tablosunu kontrol eder, ikincisi ise bu tabloda hata yoksa uygular.

t. Kurulumun Tamamlanması

Buraya kadar olan kısımda iç ağınızın internet çıkışları tamamlanmıştır. Grupların yönetimi örneği arttırılabilir ve her bir grubunuza farklı internet verilebilir.

3. RAPOLAR / LOGLAR

FirewallSuite™ her gün sonunda, gece rapor ve analizleri oluşturmaktadır. Bir güne ilişkin rapor ertesi günü hazırlanarak izlenebilir hale gelir. Buna karşılık aktif olarak anlık hareketleri görmek istiyorsanız aynı şekilde bu izlemeleri de yapabilirsiniz.

a. TIB 5651 Loglama

İletişim Daire Başkanlığı tarafından çıkarılan 5651 kanununun yönetmeliğine göre ticari olarak interneti satan internet salonları ve benzeri yerler ve işletmesinde interneti kullandıran yerler için yapılması gerekenler belirlenmiş ve log örneği bildirilmiştir.

HASH (zaman damgası) Hakkında

İç IP dağıtım loglarına zaman damgası **Ticari amaçla internet toplu kullanım sağlayıcılarının yükümlülükleri**

4/5/2007 Tarihli ve 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve
Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun kapsamında

01.11.2007 tarihli ve 26687 sayılı Resmi Gazete'de yayımlanan İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik'in
5 inci maddesi birinci fıkrasının (e) bendine istinaden, (d) bendi gereğince, **ticari amaçla internet toplu kullanım sağlayıcılarının**
elektronik ortamda sistemlerine kaydettikleri dahili IP dağıtım loglarının doğruluğunun ve bütünlüğünün teyit edilebilmesi amacıyla
çeşitli yöntemlerle oluşturulan dahili IP dağıtım loglarının doğruluk ve bütünlüğünün korunması için, bu log dosyalarının girdi olarak
alınarak, elektronik imzasının oluşturulması ve bu dosyaların imzası ile birlikte saklanması gerekmektedir.

FirewallSuite™ kendi DHCP sunucusu üzerinde tutulan İç IP dağıtım loglarını(1) TIB tarafından yayımlanmış örneğe göre
hazırlanmakta ve TIB (Telekomünikasyon İletişim Başkanlığı)'in geliştirmiş olduğu IP Log İmzalayıcı programı(2) ile imzalamaktadır.

(1) 01.11.2007 tarihli ve 26687 sayılı Resmi Gazete'de yayımlanan İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik'in
5 inci maddesi birinci fıkrasının (d) bendi
(2) 01.11.2007 tarihli ve 26687 sayılı Resmi Gazete'de yayımlanan İnternet Toplu Kullanım Sağlayıcıları Hakkında

Yönetmelik'in
5 inci maddesi birinci fıkrasının (e) bendi
(3) 01.11.2007 tarihli ve 26687 sayılı Resmi Gazete'de yayımlanan İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik'in
5 inci maddesi birinci fıkrasının (a) bendi

Kasım 2007 PERŞEMBE **Resmî Gazete** Sayı : 26687

YÖNETMELİK

Başbakanlıktan:

İNTERNET TOPLU KULLANIM SAĞLAYICILARI HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam
MADDE 1 – (1) Bu Yönetmeliğin amacı; internet toplu kullanım sağlayıcıları ve ticari amaçla internet toplu kullanım sağlayıcılarının yükümlülükleri ve sorumlulukları ile denetimlerine ilişkin esas ve usulleri düzenlemektir.

Dayanak
MADDE 2 – (1) Bu Yönetmelik, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna dayanılarak hazırlanmıştır.

Tanımlar
MADDE 3 – (1) Bu Yönetmeliğin uygulamasında;
a) Başkanlık: Telekomünikasyon İletişim Başkanlığını,
b) Bilgi: Verilerin anlam kazanmış biçimini,
c) Erişim: Herhangi bir vasıtayla internet ortamına bağlanarak kullanım olanağı kazanılmasını,
ç) Erişim sağlayıcı: Internet toplu kullanım sağlayıcılarına ve abone olan kullanıcılarına internet ortamına erişim olanağı sağlayan işletmeciler ile gerçek veya tüzel kişileri,
d) Filtreleme yazılımı: İnternet ortamında web adresi, alan adı, IP adresi, kelime ve benzeri kriterlere göre erişimi engelleyen yazılımları,
e) İç IP Dağıtım Logları: Kendi iç ağlarında dağıtılan IP adres bilgilerini, kullanıma başlama ve bitiş tarih ve saatini ve bu IP adreslerini kullanan bilgisayarların

tekil ağ cihaz numarasını (MAC adresi) gösteren bilgileri,

f) İnternet ortamı: Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı,

g) İnternet toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan gerçek ve tüzel kişileri,

ğ) İşyeri: Ticari amaçla internet toplu kullanım sağlayıcı olarak faaliyet gösteren gerçek veya tüzel kişiler tarafından açılan ve işletilen umuma açık yeri,

h) İzin belgesi: Mülki idare amiri tarafından bu Yönetmelik kapsamındaki işyerlerinin açılıp faaliyet göstermesi için verilen izni,

ı) Kanun: 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu,

i) Mülki idare amiri: İllerde valiyi, Büyükşehir belediyesi hudutları içinde kalanlar dahil ilçelerde kaymakamı,

j) Sabit IP Adresi: Belirli bir ağa bağlı cihazların ağ üzerinden birbirlerine veri yollamak için kullandıkları, zamana, oturuma göre değişmeyen ve sistem yöneticisi tarafından belirlenip tanımlanan ve değiştirilebilen IP adresini,

k) Sorumlu müdür: İzin belgesi sahibinin işinin başında bulunmadığı zamanlarda onun yerine yetkili olan kişiyi,

l) Ticari amaçla internet toplu kullanım sağlayıcı: İnternet salonu ve benzeri umuma açık yerlerde belirli bir ücret karşılığı internet toplu kullanım sağlayıcılığı hizmeti veren veya bununla beraber bilgisayarlarda bilgi ve beceri artırıcı veya zekâ geliştirici nitelikteki oyunların oynatılmasına imkân sağlayan gerçek ve tüzel kişileri,

m) Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri,

ifade eder.

İKİNCİ BÖLÜM
Yükümlülükler ve Sorumluluklar

İnternet toplu kullanım sağlayıcılarının yükümlülükleri

MADDE 4 – (1) İnternet toplu kullanım sağlayıcılarının yükümlülükleri şunlardır:

a) Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak.

b) İç IP Dağıtım Loglarını elektronik ortamda kendi sistemlerine kaydetmek.

Ticari amaçla internet toplu kullanım sağlayıcılarının yükümlülükleri

MADDE 5 – (1) Ticarî amaçla internet toplu kullanım sağlayıcılarının yükümlülükleri şunlardır:

a) Mülki idare amirinden izin belgesi almak.

b) Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak.

c) Başkanlık tarafından onaylanan içerik filtreleme yazılımını kullanmak.

ç) Erişim sağlayıcılardan sabit IP almak ve kullanmak.

d) İç IP Dağıtım Loglarını elektronik ortamda kendi sistemlerine kaydetmek.

e) Başkanlık tarafından verilen yazılım ile, (d) bendi gereğince kaydedilen bilgileri ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydetmek ve bu verileri bir yıl süre ile saklamak.

İşyerlerinin açılması

MADDE 6 – (1) Ticari amaçla internet toplu kullanım sağlayıcı olarak faaliyet göstermek isteyen gerçek ve tüzel kişiler, 14/7/2005 tarihli ve 2005/9207 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan İşyeri Açma ve Çalışma Ruhsatlarına İlişkin Yönetmelikte belirtilen usule uygun olarak işyeri açma ve çalışma ruhsatı aldıktan sonra mülki idare amirliklerine bir dilekçe ile başvurur.

(2) İşyerlerinin faaliyette bulunması için mülki idare amirleri tarafından Ek-1'de yer alan izin belgesi verilir.

(3) İşyerlerinin açılması hususundaki başvurular mülki idare amirlikleri tarafından onbeş gün içinde sonuçlandırılır.

İzin alınmadan açılan işyerleri

MADDE 7 – (1) Mülki idare amirlerince izin alınmadan açıldığı tespit edilen işyerleri, mülki idare amirlikleri tarafından sebebi bir tutanakla belirlenmek ve mühürlenmek suretiyle re'sen kapatılır.

(2) Mülki idare amirlikleri, izin alınmadan açıldığı için kapatılan işyerlerini en geç üç gün içinde elektronik ortamda veya yazılı olarak Başkanlığa bildirir.

İzin belgesi sahibi ve sorumlu müdür

MADDE 8 – (1) İzin belgesi sahibinin tüzel kişi olması durumunda, işyerini idare etmek üzere bir sorumlu müdür görevlendirilir. Gerçek kişiler de işyerinde sorumlu müdür görevlendirebilir. Sorumlu müdür mülki idare

amirliklerine bildirilerek izin belgesinde belirtilir.

(2) İzin belgesi sahibi veya sorumlu müdürlere, mülki idare amirliklerince yılda bir kez bilgilendirme eğitimi verilir. Eğitimin içeriği, Milli Eğitim Bakanlığı tarafından, İçişleri Bakanlığı, Başbakanlık Aile ve Sosyal Araştırmalar Genel Müdürlüğü ve Başkanlığın görüşü alınarak belirlenir.

İşyerlerinde uyulması gereken kurallar

MADDE 9 – (1) İşyerlerinde uyulması gereken kurallar şunlardır:

a) 12 yaşından küçükler ancak, yanlarında veli veya vasileriyle işyerlerine girebilirler.

b) 15 yaşından küçükler yanlarında veli veya vasileri olmadan saat 20.00'den sonra işyerlerine alınmazlar.

c) Tütün ve tütün mamulleri tüketim bölümü bulunmayan işyerlerinde tütün ve tütün mamulleri içilemez.

ç) İşyerlerinde 1117 sayılı Küçükleri Muzır Neşriyattan Koruma Kanununa aykırı hareket edilemez.

d) İşyerlerinde 4250 sayılı İspirto ve İspirtolu İçkiler İnhisarı Kanununun 19 uncu maddesi gereğince alkollü içecek satılması, bulundurulması veya sunulması yasaktır.

e) İşyerlerinde 5846 sayılı Fikir ve Sanat Eserleri Kanunu kapsamında korunan hakların ihlal edilmesinin önlenmesi için gerekli tedbirler alınır.

f) İşyerlerinde elektronik ve mekanik oyun alet ve makineleri bulunamaz.

g) İşyerlerindeki bilgisayarlarda uyuşturucu veya uyarıcı madde alışkanlığı, intihara yönlendirme, cinsel istismar, müstehcenlik, fuhuş, şiddet, kumar ve benzeri kötü alışkanlıkları teşvik eden ve 18 yaşından küçüklerin psikolojik ve fizyolojik gelişimine olumsuz etkisi olabilecek oyunlar oynatılamaz.

ğ) İşyerlerine giren ve çıkanların tespiti amacıyla gerekli kamera kayıt sistemi kurulur. Bu sistem aracılığıyla elde edilen kayıtlar yedi gün süreyle saklanır ve bu kayıtlar yetkili makamlar haricindeki kişi ve kuruluşlara verilemez.

ÜÇÜNCÜ BÖLÜM
Denetleme ve Cezalar

Denetleme usul ve esasları

MADDE 10 – (1) Ticari amaçla internet toplu kullanım sağlayıcılar;

a) Mülki idare amirlikleri tarafından, bu Yönetmeliğin 5 ve 9 uncu maddelerinde yer alan yükümlülükler

ve şartlar açısından denetlenir.

b) Kolluk tarafından genel güvenlik ve asayiş yönünden denetlenir ve tespit edilen mevzuata aykırı hususlar mülki idare amirliklerine gereği yapılmak üzere bildirilir.

İdari para cezaları

MADDE 11 – (1) 5 inci maddedeki yükümlülüklere aykırı hareket ettiği belirlenen ticari amaçla internet toplu kullanım sağlayıcılara, mülki idare amiri tarafından üçbin Yeni Türk Lirasından onbeşbin Yeni Türk Lirasına kadar idarî para cezası verilir.

(2) 9 uncu maddede belirtilen kurallara uymayanlara, mülki idare amiri tarafından 2559 sayılı Polis Vazife ve Salahiyet Kanununun 6 ncı maddesinin birinci fıkrasının (d) bendi uyarınca idari para cezası verilir.

(3) İdari para cezaları, 5326 sayılı Kabahatler Kanununda belirtilen usul ve esaslara göre uygulanır.

DÖRDÜNCÜ BÖLÜM
Çeşitli ve Son Hükümler

Uygulamaya ilişkin işlemler

MADDE 12 – (1) Ticari amaçla internet toplu kullanım sağlayıcılara verilen izin belgelerine ilişkin işlemler, mülki idare amirliklerinin yazı işleri müdürlükleri bünyesinde yürütülür.

(2) İzne ilişkin bilgiler otuz gün içinde mülki idare amiri tarafından Başkanlığa elektronik ortamda veya yazılı olarak bildirilir.

(3) Ticari amaçla internet toplu kullanım sağlayıcıların faaliyetlerinin herhangi bir şekilde sona ermesi halinde durum üç gün içinde mülki idare amiri tarafından Başkanlığa elektronik ortamda veya yazılı olarak bildirilir.

Başkanlığın bilgi talebi

MADDE 13 – (1) Başkanlık, Kanunla verilen görevleri dolayısıyla ticari amaçla internet toplu kullanım sağlayıcılara ilişkin gerekli gördüğü bilgileri doğrudan ticari amaçla internet toplu kullanım sağlayıcılardan veya mülki idare amirliklerinden talep edebilir.

(2) Ticari amaçla internet toplu kullanım sağlayıcılar Başkanlığın taleplerini derhal yerine getirir.

GEÇİCİ MADDE 1 – (1) Halen faaliyet icra eden ticari amaçla internet toplu kullanım sağlayıcılar, Kanunun yürürlüğe girdiği tarihten itibaren altı ay içinde alınması gereken izin belgesini temin etmekle yükümlüdürler.

Yürürlük
MADDE 14 – (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.
Yürütme
MADDE 15 – (1) Bu Yönetmelik hükümlerini Başbakan yürütür.

5651 kanunun yönetmeliğine göre, interneti ticari olarak satan veya bünyesinde kullandıran yerler, log kayıtlarını en az bir yıl süre ile saklaması gerekmekte ve koruyucu tedbirleri alması gerekmektedir. İnterneti ticari olarak satan yerler ise (internet salonları vb. belirli süreliğine internet hizmetini satan) aynı zamanda iç IP dağıtım loglarını (DHCPD) TIB tarafından verilen program ile zaman damgası ile damgalayarak saklaması gerekmektedir.

FirewallSuite™ 5651 cihazı değildir. Ancak istenildiğinde kendi üzerindeki DHCP kayıtlarını TIB tarafından verilen program ile yönetmeliğe uygun olarak zaman damgalayabilir. Aynı zamanda kayıtları bir yıl süre ile saklayabilir ve koruyucu tedbirleri alabilir. Bununla ilgili yönerge ve programlar FirewallSuite™ içerisindeki Raporlar & Loglar > TIB 5651 Loglama kısmında yeralmaktadır.

b. Grafikli Çıktılar

FirewallSuite™ kendi üzerindeki internet ve donanım kullanımını geriye dönük ve grafikli olarak saklamaktadır. Böylelikle hat ve donanım yeterlilikleri konusundaki verileri alabilirsiniz.

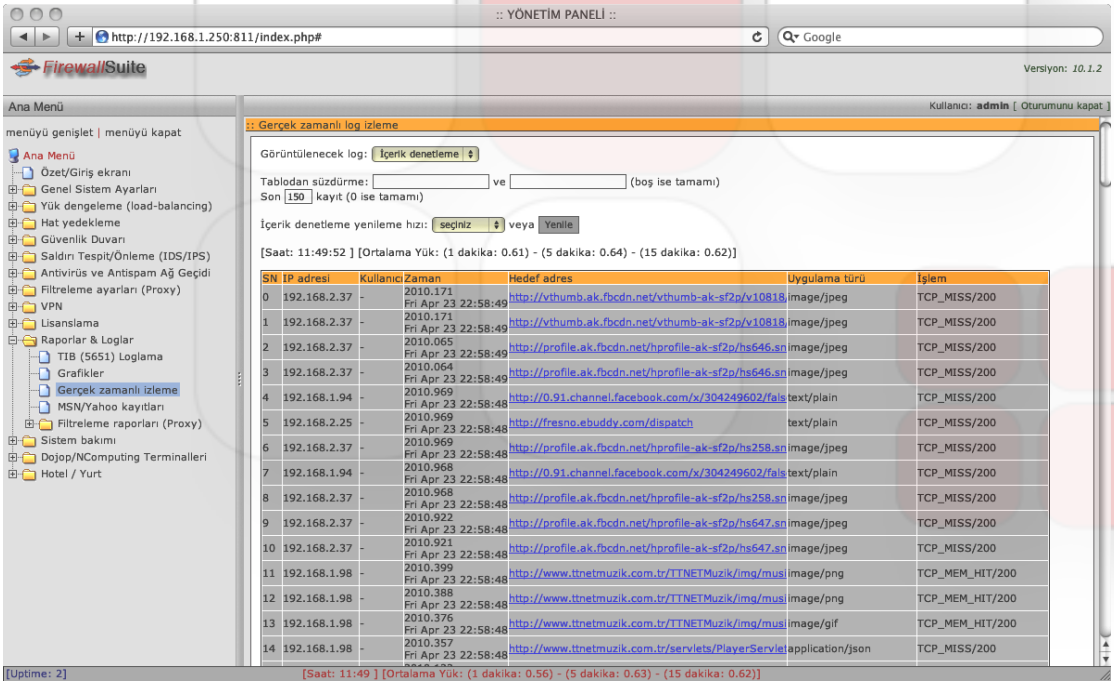
c. Anlık İzlemeler

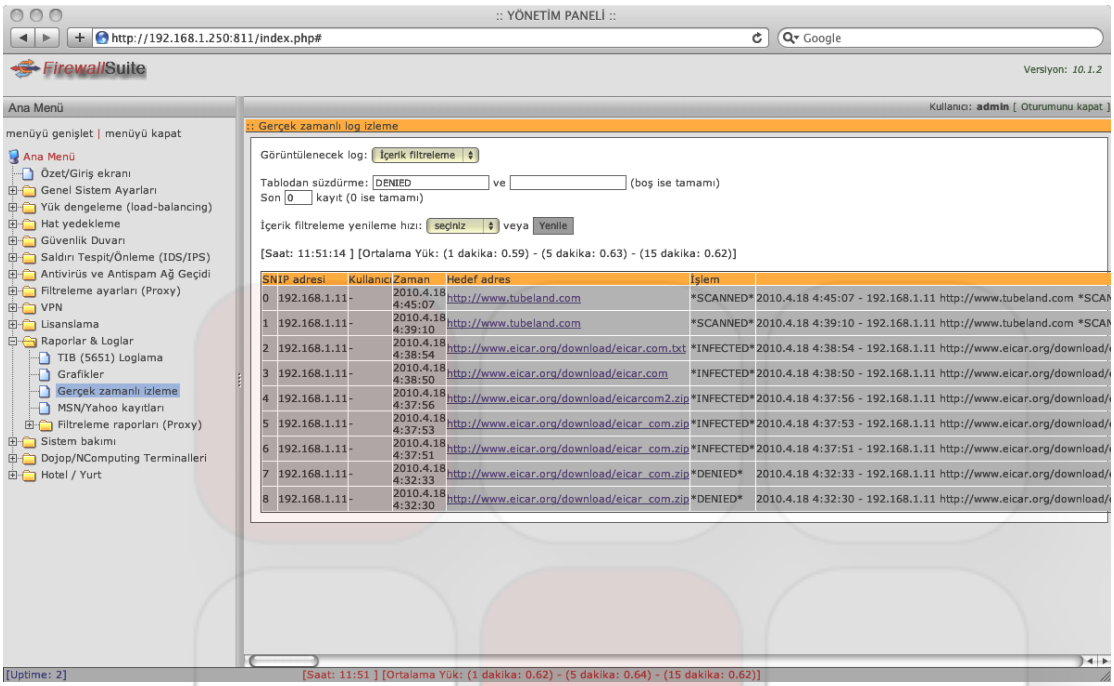
FirewallSuite™ üzerinden geçen dataların kayıtlarını anlık olarak izlenmesine olanak tanımaktadır. Hem filtreleme sisteminden geçen istemcilerin o an hangi internet üzerinde hangi sayfalara eriştiği hemde içerik filtrelemede hangi istemcilerin hangi eriştiği siteler denetleniyor ve işlem sonuçlarını anlık olarak takip edebilirsiniz.

d. Geçmişe Dönük LOG ve Analizler

FirewallSuite™ geriye dönük olarak log kayıtlarını tarihsel olarak saklar. Hangi istemci ne kadar veri indirmiş, hangi web sayfalarına ulaşmış, ne kadar zaman kalmış gibi bilgiler alınabilir. Aynı şekilde genel internet kullanımı grafikli olarak izlenebilir.

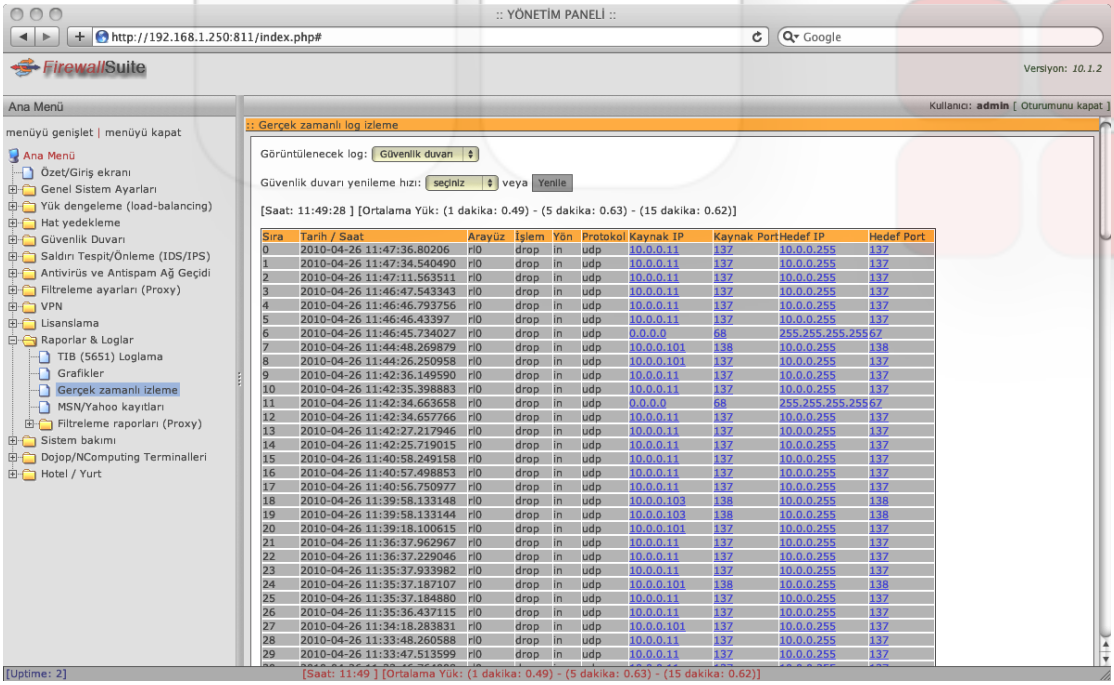
e. İçerik Denetleme





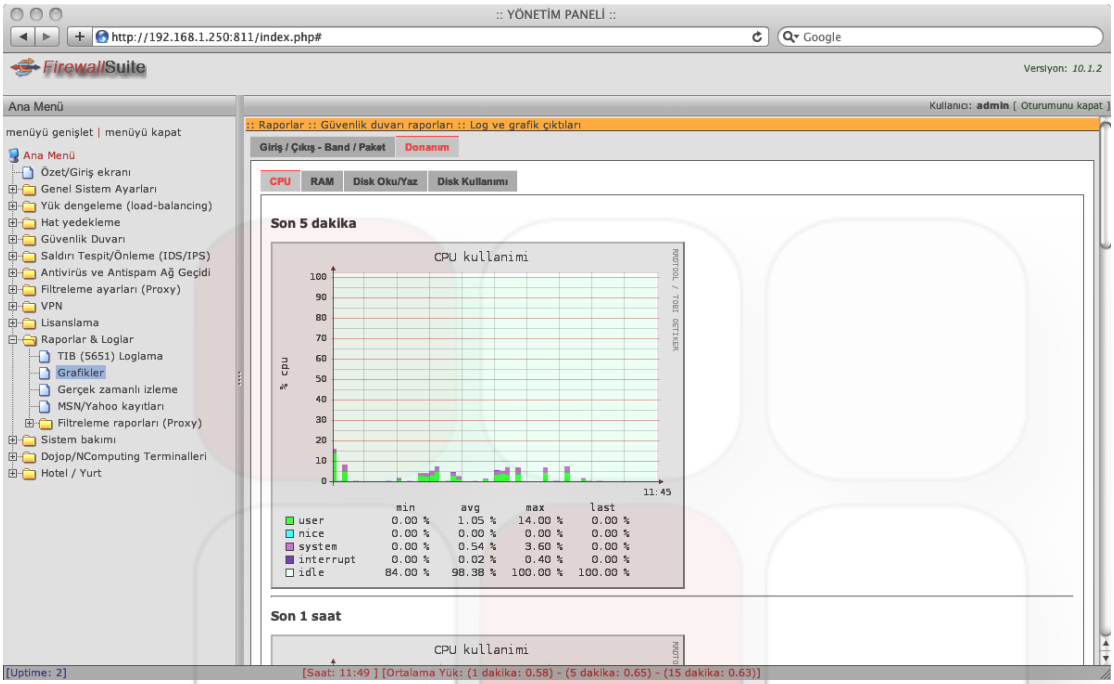
SN	IP adresi	Kullanıcı	Zaman	Hedef adres	İşlem
0	192.168.1.11	-	2010.4.18 4:45:07	http://www.tubeland.com	*SCANNED* 2010.4.18 4:45:07 - 192.168.1.11 http://www.tubeland.com *SCAN
1	192.168.1.11	-	2010.4.18 4:39:10	http://www.tubeland.com	*SCANNED* 2010.4.18 4:39:10 - 192.168.1.11 http://www.tubeland.com *SCAN
2	192.168.1.11	-	2010.4.18 4:38:54	http://www.eicar.org/download/eicar.com.txt	*INFECTED* 2010.4.18 4:38:54 - 192.168.1.11 http://www.eicar.org/download/
3	192.168.1.11	-	2010.4.18 4:38:50	http://www.eicar.org/download/eicar.com	*INFECTED* 2010.4.18 4:38:50 - 192.168.1.11 http://www.eicar.org/download/
4	192.168.1.11	-	2010.4.18 4:37:56	http://www.eicar.org/download/eicarcom2.zip	*INFECTED* 2010.4.18 4:37:56 - 192.168.1.11 http://www.eicar.org/download/
5	192.168.1.11	-	2010.4.18 4:37:53	http://www.eicar.org/download/eicar_com.zip	*INFECTED* 2010.4.18 4:37:53 - 192.168.1.11 http://www.eicar.org/download/
6	192.168.1.11	-	2010.4.18 4:37:51	http://www.eicar.org/download/eicar_com.zip	*INFECTED* 2010.4.18 4:37:51 - 192.168.1.11 http://www.eicar.org/download/
7	192.168.1.11	-	2010.4.18 4:32:33	http://www.eicar.org/download/eicar_com.zip	*DENIED* 2010.4.18 4:32:33 - 192.168.1.11 http://www.eicar.org/download/
8	192.168.1.11	-	2010.4.18 4:32:30	http://www.eicar.org/download/eicar_com.zip	*DENIED* 2010.4.18 4:32:30 - 192.168.1.11 http://www.eicar.org/download/

f. Güvenlik Duvarı

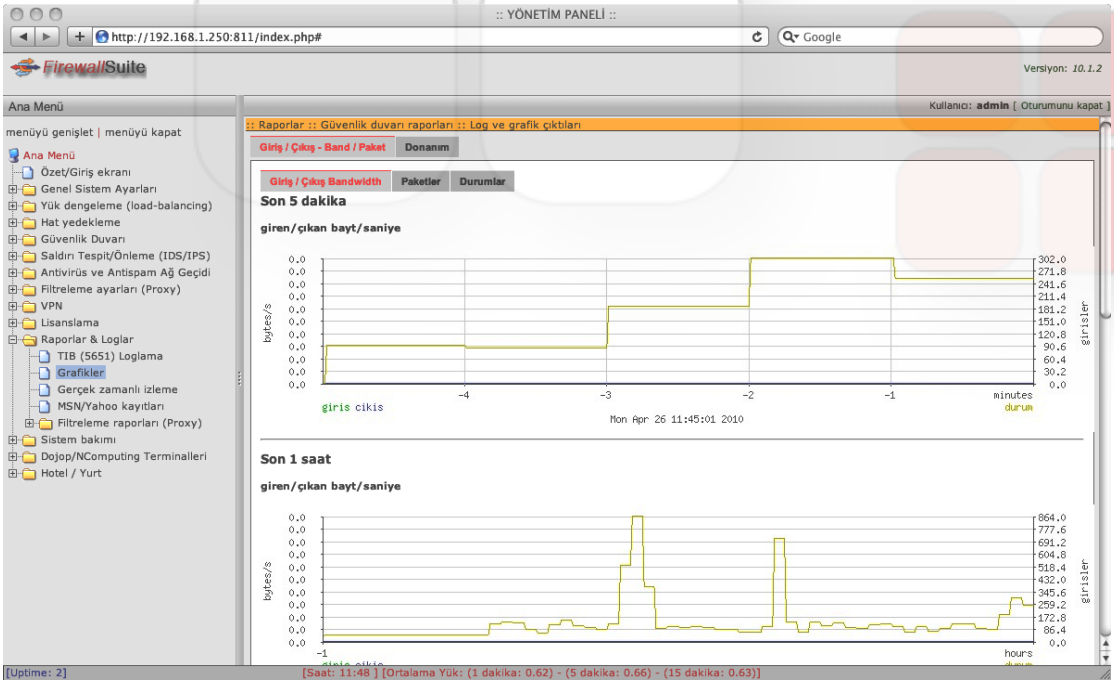


Sıra	Tarih / Saat	Arayüz	İşlem	Yön	Protokol	Kaynak IP	Kaynak Port	Hedef IP	Hedef Port
0	2010-04-26 11:47:36.80206	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
1	2010-04-26 11:47:34.540490	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
2	2010-04-26 11:47:11.563511	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
3	2010-04-26 11:46:47.543343	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
4	2010-04-26 11:46:46.793756	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
5	2010-04-26 11:46:46.43397	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
6	2010-04-26 11:46:45.734027	ri0	drop	in	udp	0.0.0.0	68	255.255.255.255	67
7	2010-04-26 11:44:48.269879	ri0	drop	in	udp	10.0.0.101	138	10.0.0.255	138
8	2010-04-26 11:44:26.250958	ri0	drop	in	udp	10.0.0.101	137	10.0.0.255	137
9	2010-04-26 11:42:36.149590	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
10	2010-04-26 11:42:35.398883	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
11	2010-04-26 11:42:34.663658	ri0	drop	in	udp	0.0.0.0	68	255.255.255.255	67
12	2010-04-26 11:42:34.657766	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
13	2010-04-26 11:42:27.217946	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
14	2010-04-26 11:42:25.719015	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
15	2010-04-26 11:40:58.249158	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
16	2010-04-26 11:40:57.498853	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
17	2010-04-26 11:40:56.750977	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
18	2010-04-26 11:39:58.133148	ri0	drop	in	udp	10.0.0.103	138	10.0.0.255	138
19	2010-04-26 11:39:58.133144	ri0	drop	in	udp	10.0.0.103	138	10.0.0.255	138
20	2010-04-26 11:39:18.100615	ri0	drop	in	udp	10.0.0.101	137	10.0.0.255	137
21	2010-04-26 11:36:37.962967	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
22	2010-04-26 11:36:37.229046	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
23	2010-04-26 11:35:37.933982	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
24	2010-04-26 11:35:37.187107	ri0	drop	in	udp	10.0.0.101	138	10.0.0.255	138
25	2010-04-26 11:35:37.184880	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
26	2010-04-26 11:35:36.437115	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
27	2010-04-26 11:34:18.283831	ri0	drop	in	udp	10.0.0.101	137	10.0.0.255	137
28	2010-04-26 11:33:48.260588	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137
29	2010-04-26 11:33:47.513599	ri0	drop	in	udp	10.0.0.11	137	10.0.0.255	137

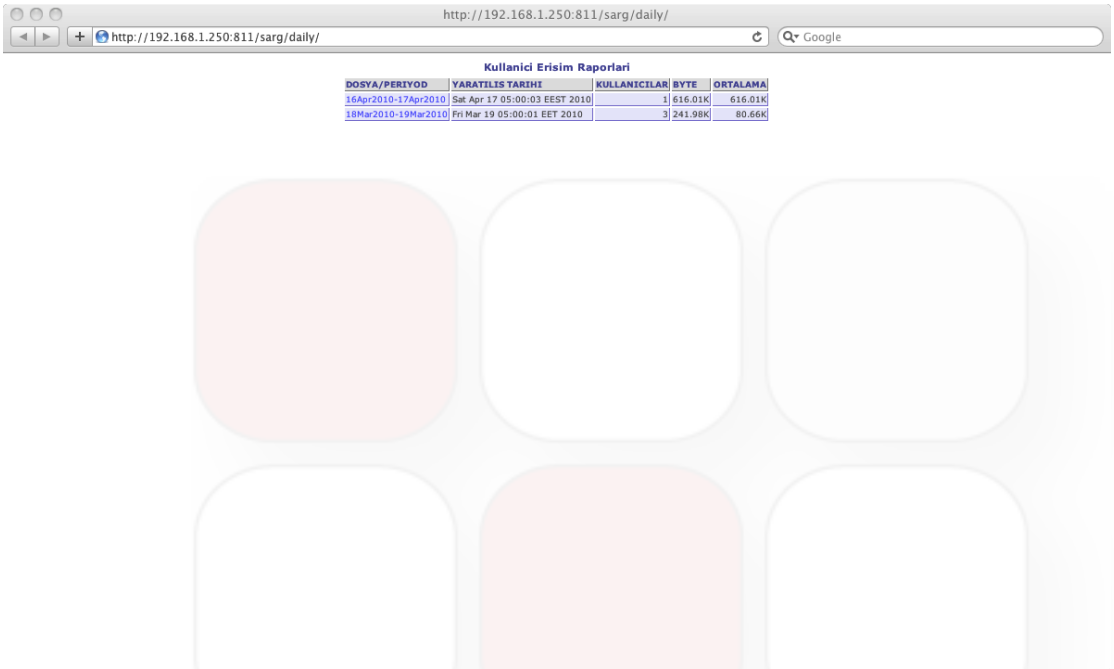
g. Donanım Yükü



h. Giriş/Çıkış Band Yükü

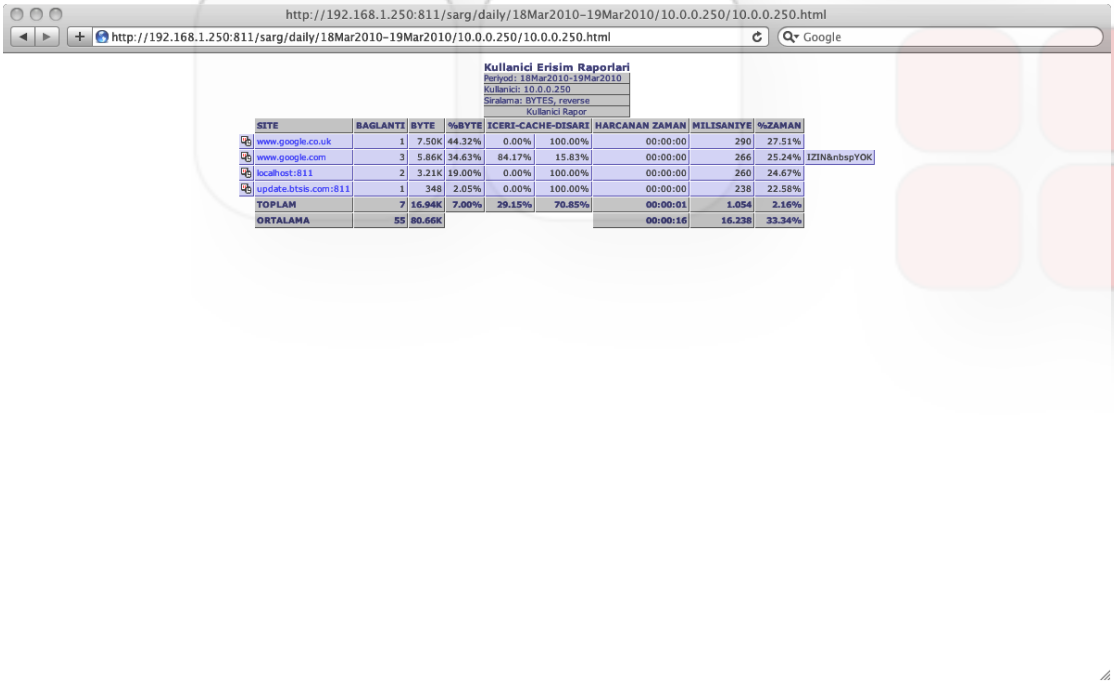


i. Günlük LOG Örneği



Kullanici Erisim Raporlari

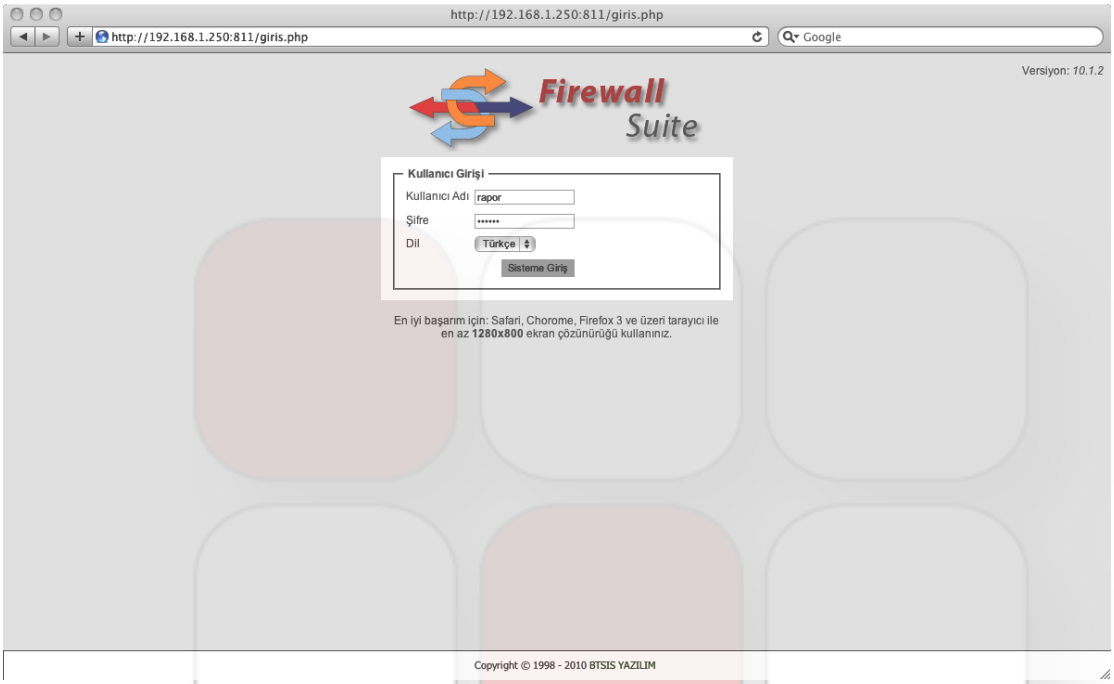
DOSYA/PERIYOD	YARATILIS TARIHI	KULLANICILAR	BYTE	ORTALAMA
16Apr2010-17Apr2010	Sat Apr 17 05:00:03 EEST 2010	1	616.01K	616.01K
18Mar2010-19Mar2010	Fri Mar 19 05:00:01 EET 2010	3	241.98K	80.66K



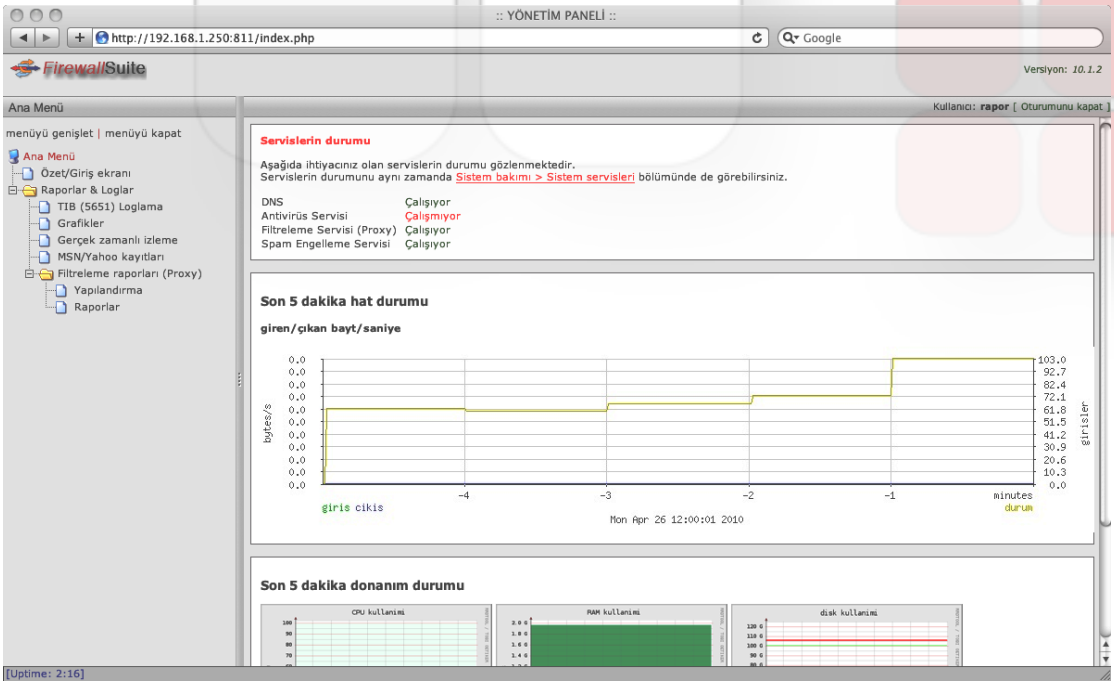
Kullanici Erisim Raporlari
Periyod: 18Mar2010-19Mar2010
Kullanici: 10.0.0.250
Siralama: BYTES, reverse
Kullanici Rapor

SITE	BAGLANTI	BYTE	%BYTE	ICERI-CACHE-DISARI		HARCANAN ZAMAN	MILISANIYE	%ZAMAN	
www.google.co.uk	1	7.50K	44.32%	0.00%	100.00%	00:00:00	290	27.51%	
www.google.com	3	5.86K	34.63%	84.17%	15.83%	00:00:00	266	25.24%	IZIN YOK
localhost:811	2	3.21K	19.00%	0.00%	100.00%	00:00:00	260	24.67%	
update.btsis.com:811	1	348	2.05%	0.00%	100.00%	00:00:00	238	22.58%	
TOPLAM	**7**	**16.94K**	**7.00%**	**29.15%**	**70.85%**	**00:00:01**	**1.054**	**2.16%**	
ORTALAMA	**55**	**80.66K**				**00:00:16**	**16.238**	**33.34%**	

j. Rapor Kullanıcısı Giriş Ekranı



k. Rapor Kullanıcısının Kısıtlanmış Arayüzü



4. SİSTEM BAKIMLARI

Sistem bakımlarında,
Şifre değiştirme,
Yedek alma,
Sistemi güncelleme,
Servislerin yönetimi,
Zaman tarih ayarları,
Sistemi yeniden başlatma/kapatma

İşlemlerini yapabilirsiniz.

5. LİSANSLAR

FirewallSuite™ BTSIS YAZILIM™'ın tescilli markasıdır.

FirewallSuite™ ürünü içerisinde kullanılan ve lisans gerektiren yazılımlar BTSIS YAZILIM adına FirewallSuite™ ürünü için lisanslıdır ve ilgili firma ve grup veya vakıfaların kendi marka ve çalışmalarına dayanır.

Alt yapıda kullanılan işletim sistemi, ilgili firma ve grup veya vakıfaların kendi marka ve çalışmalarına dayanır.

WEB arayüz teknolojilerinde kullanılan php, ajax, javascript, perl ve benzeri teknolojiler, ilgili firma ve grup veya vakıfaların kendi marka ve çalışmalarına dayanır.

Üçüncü parti kullanılan GPL ve benzeri diğer yazılımlar, ilgili firma ve grup veya vakıfaların kendi marka ve çalışmalarına dayanır.

BTSIS YAZILIM™, ürünlerinde kullandığı teknolojik metaryel ve yazılımları geliştirme hakkını gizli tutar.

Notlar