FirewallSuite® 10.2.x Genel Yapıladırma Kılavuzu

FirewallSuite® ürününü tercih ettiğiniz için teşekkür ederiz.

İçindekiler Dizini

Önsöz....5
Yapılandırma Öncesi....6
FirewallSuite® Ağ Ayarlarının Yapılması....8
IP Ayarlarının Yapılması....9
DNS Yapılandırması....11
Ağ Geçidi Seçenekleri....12
DHCP Sunucusu....13
Yerel DNS Sunucusu....15
Güvenlik Duvarı....17
Port Yönlendirme....18
Filtrelemeler....20
Grup Açma....21
Gruba İnternet Erişim Haklarını Verme....22
HotSpot İnternet Erişimini Açma....23
T.C. Kimlik No ile Doğrulama....23
Gruba İnternet Erişim Haklarını Verme....24
Panel Üzerinden HotSpot Kullanıcısı Açmak....24
Diğer Ayarlar....27
Alias IP Tanımlama....27
Routing Yazmak....27
Bağlantı Testi....28
IP Hesaplama (CIDR)....29
Ağ Tarama....29
DHCP Dosyasını Temizlemek....30
Hat Yedekleme....30
Filtrelemeler....32
Bir Dış IP Adresini Proxy'den Hariç Tutmak....32
Web Filtreleme (L7)....32
Web Filtreleme (L3)....33
Sadece İzin Verilen Siteler....34
Hariç Tutulan Siteler....35
Yasaklı Dosya Uzantıları....35
Uygulama Tipi Yasaklar....36
Band Genişliği Tanımlamaları....37
Zaman Profilleri....38
Grupları Yönet....40
İnternet Çıkış İzinleri....40
Mesai Saati....41
Sadece İzin verilen siteler....41

Hariç tutulan siteler....42
Yasaklı Dosya Uzantıları....42
Uygulama Tipi Yasaklar....42
Band Genişliği Tanımlamaları....42
Domain /URL / Kelime Filtreleme....42
İçerik Filtreleme....43
Raporlar & Loglar....45
Zaman Damgası....45
Açıklamalar....46
IP LOG İmzalayıcı....46
Zaman Damgalı LOG Yedekleme Sunucusu....46
Zaman Damgalı LOG Doğrulama....46
Tubitak Zaman Damgası (UEKAE)....46
Zaman Damgası İşlem Kaydı....46
Grafikler....47
Gerçek Zamanlı İzleme....47
Anlık Band Yükü Grafikleri....48
Web Raporları....48
Web İstatistikleri....49
Sistem Bakımı....49
SSL Sertifikası Yapılandırılması....50
Şifre Değiştirme....51
Sistem Yedekleri....52
Sistem Servisleri....53
Zaman/Tarih Ayarları....53
Sistemi Yeniden Başlat/Kapat....53
Misafir / Hotel / Yurt (HotSpot)....54
Kimlik Doğrulama....54
Açıklamalar....55
Yapılandırma....55
KYS Lobi....55
T.C. Kimlik No....56
SMS....57
Veritabanı & Üye Misafir....57
Veritabanı & Konaklayan Misafir....57
Etkinlik / Konferans Salonu....57
Facebook Login....58
Sayfa / Mesaj Özelleştirme....58
E-Posta Yapılandırması....59
SMS Entegrasyonu....60
Veri Tabanı Entegrasyonu....61

Yedekleme.....61
Notlar.....62

Önsöz

Bu dokümanda, FirewallSuite® ilk yapılandırma aşamaları örnek bir senaryo ile adım adım anlatılmaktadır. Ayrıca bu yapılandırmaya dahil olmayan diğer ayarlar hakkında genel bilgiler verilmektedir. Kısaca bilgi verilen kısımlar için FirewallSuite® üzerinde kullanıma ilişkin detaylı açıklamalara yer verilmiştir.

Her bir ağ sisteminin birbirinden farklı türde ve farklı IP yapısında olabileceği unutulmamalı ve kendi ağınızda uygulama yaparken, burada anlatılanları ağınızdaki parametrelere göre yeniden değerlendirmeyi ihmal etmemelisiniz.

Belgede sözü geçen bazı özel terim ve kısaltmalar (proxy, domain, alias, routing, HTTP, URL, vb...) anlam bütünlüğünün bozulmaması adına orijinal halleri ile kullanılmıştır.

Facebook kimlik doğrulamasına ilişkin doğrulama sistemi yalnızca Facebook Inc.'in izin verdiği standartlarda çalışır.

T.C. Kimlik doğrulama sistemi kimlik doğrulamasına ilişkin doğrulama sistemi yalnızca Türkiye Cumhuriyeti Devleti'inin izin verdiği standartlarda çalışır.

TUBİTAK, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'dur.

FirewallSuite® arayüzündeki etiket ve menüler ***Eğik*** ***İtalik*** yazı ile tanımlanmıştır.

İp ucu niteliğindeki önemli noktalar kutu içine alınımştır.

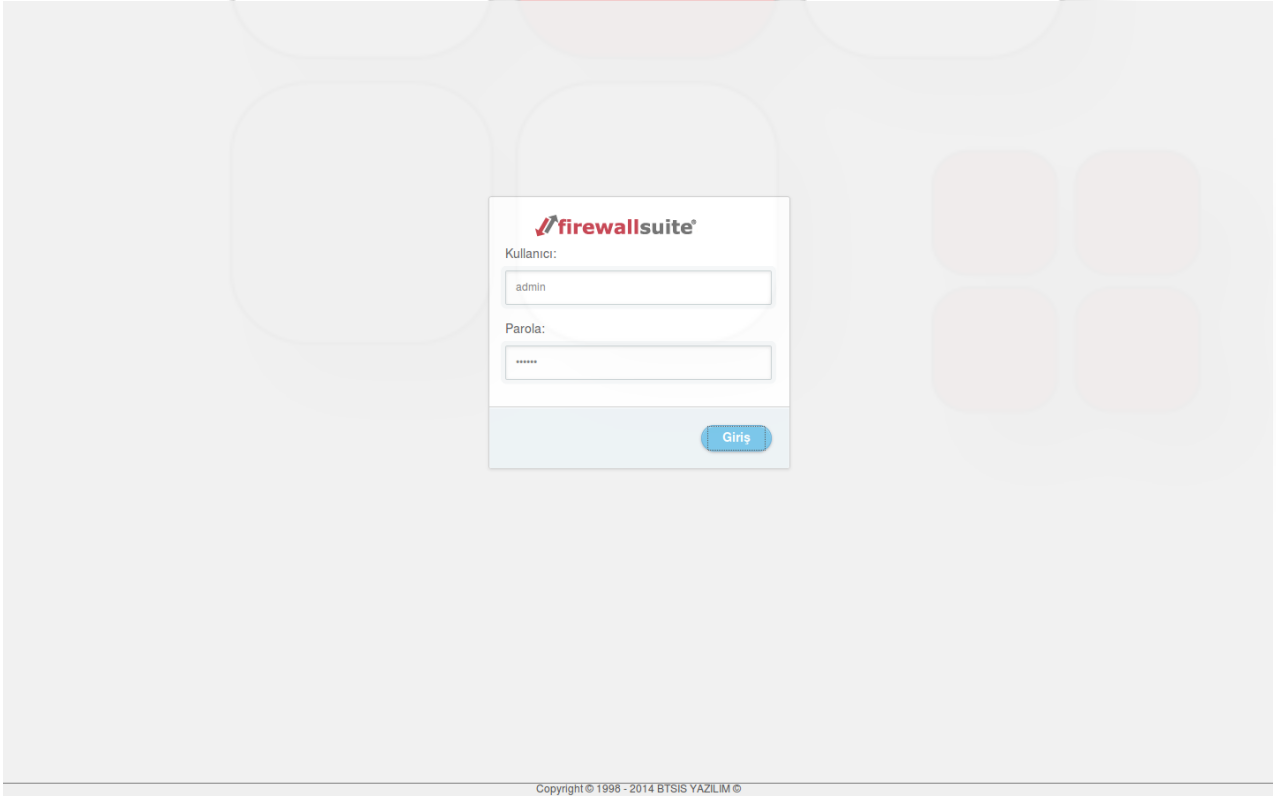
Yapılandırma Öncesi

Yapılandırma işlemine başlamadan önce kurulacak ağ topolojisinin önceden planlanmış olması gereklidir. Ağ topolojileri hizmet olarak aynı hizmetleri içermekle birlikte farklı altyapılara sahip olabilir. Bu dokümanda örnek bir senaryo anlatılmış olmakla birlikte, sahada daha farklı ve gelişmiş senaryolar da uygulanabilir.

İstemcilere internet hizmetinin verilmesi iki ana işlemden oluşmaktadır. Bunlardan ilki FirewallSuite®'in kendisine internet erişiminin sağlanması, ikinci aşamada ise iç kısımda yer alan istemcilere internet hizmetinin verilmesidir.

İstemcilere internet hizmetinin verilmesi işlemi istenilen IP veya MAC adreslerine göre planlanan grupların açılması ve bu gruplara tercih edilen yetkiler dahilinde internet erişim hizmetinin verilmesi olarak değerlendirilebilir.

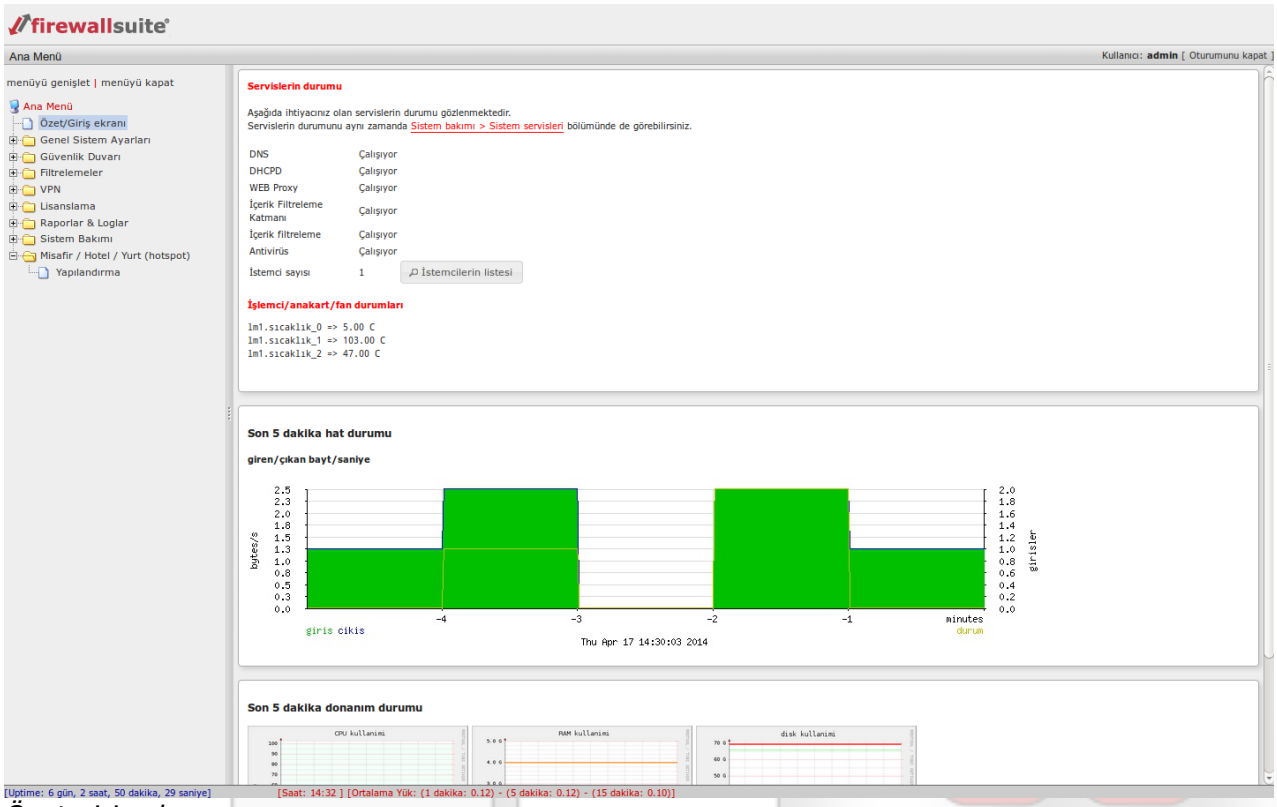
Örnek senaryoda bir adet internet girişi, bir adet personel ağı, bir adet misafir HotSpot ağı olmak üzere toplam üç farklı ağ tasarlanmıştır. Ağınızdaki IP adresleri tasarlanmış olan ağlara göre farklılık gösterebilir.



Giriş ekranı

FirewallSuite® için yapılacak işlemler için HTML tabanlı bir panelden yapılır. Erişim IP adresi kullanıcı tarafından değiştirilmiş olabileceği gibi varsayılan değer olarak

http://10.0.0.2:811



Özet giriş ekranı

adresinden erişim sağlanır. Bu erişimin ardından var sayılan kullanıcı adı **admin** ve parola **123456** şeklinde tanımlamış olmakla birlikte sistem yöneticisi tarafından değiştirilebilir. İlk yapılandırma erişimi için ilgili ağ tarafında bir IP dağıtıcı bulunmadığı için erişim sağlanacak bilgisayarın kendisine de ilgili ağ segmentinden bir IP adresinin elle verilmesi gerekir.

✦ FirewallSuite® konumlandığı ağda modem tarafına göre istemci, istemci tarafına göre de ağ geçidi konumundadır. Bu bakımdan modem tarafı ile ilgili IP ayarlamalarında modemin dinamik IP dağıtım sistemi kapatılmalı ya da dağıtım aralığı FirewallSuite®'in sabit IP adresi dışında ayarlanmalıdır.

Örnek senaryoya göre 3 ağ kartı kullanılacak bir FirewallSuite® ürünü için IP tanımlamaları aşağıdaki gibi planlanmıştır.

Modem (Gateway): 10.0.0.1

FirewallSuite® modem tarafı: 10.0.0.2

FirewallSuite® personel ağı tarafı: 192.168.10.1

FirewallSuite® misafir HotSpot ağı tarafı: 192.168.20.1

Varsayılan Sunucu: 192.168.10.2 (RDP erişimi için 3389 port yönlendirmesi yapılacak)

Tüm ağ kartları için alt ağ maskesi: 255.255.255.0

olarak planlanmıştır.

FirewallSuite® Ağ Ayarlarının Yapılması

Bu işlem farklı adımlardan oluşur. Tüm adımlar aşağıda sıra ile verilmiştir. İlk işlem ağ kartlarına IP adreslerini sıra ile tanımlama işlemidir.

Ayarlamalarımızı yaparken ağ kartlarını hat1, local, local2 gibi isimlerle adlandırılırken aynı ağ kartları sistem tarafında vr0, rl1, em0 gibi isimlerle tanımlanmıştır. Sistem tarafındaki bu isimler değişiklik gösterebilir.

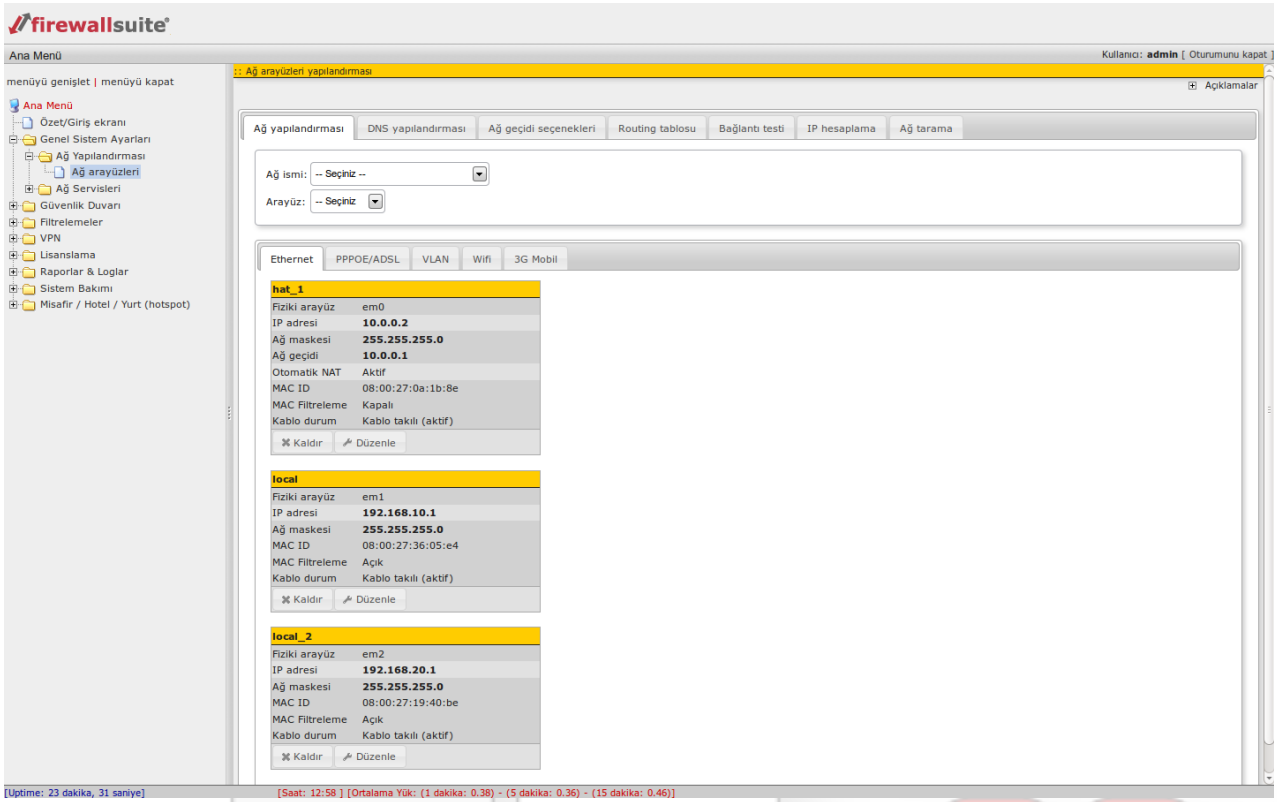
Senaryomuza göre belirlediğimiz IP adreslerini sisteme tanımlamak için sistemde var olan üç farklı ağ kartını kullanmamız gerekmektedir. Bu tanımları ağ kartlarımızın ilk ayarında bir kereye mahsus olarak kullanacağız. Ağ kartlarını IP adreslerini tanımlamak için

Ana Menü > ***Genel Sistem Ayarları*** > ***Ağ Yapılandırması*** > ***Ağ arayüzleri*** > ***Ağ yapılandırması***

menüsüne geliniz. Bu kısımda ağ ve ağ geçidi ile ilgili ayarlar bulunmaktadır.

IP Ayarlarının Yapılması

Modem (WAN) tarafındaki ağ kartı için:



Ağ Ayarlar (1)

Ağ ismi: hat_1

Arayüz: (kullanılacak ağ kartının arayüzü)

Yapılandırma: IP adresini aşağıdaki gibi yapılandır

IP adresi: 10.0.0.2

Ağ maskesi: 255.255.255.0

Broadcast: (seçimliktir. Boş bırakılabilir.)

Ağ geçidi: 10.0.0.1 (modem yada routerinizin IP adresi)

Otomatik NAT: (İşaretli olacak)

ilgili ayarları yaptıktan sonra ***Kaydet*** düğmesine basınız. Bu işleme paralel olarak modem ya da router cihazınızın DHCP otomatik IP dağıtım sistemini kapatmanız ya da 10.0.0.2 IP adresini dağıtılacak IP aralığının dışında tutmanız gerekmektedir. Aksi taktirde internet hattı tarafında doğabilecek bir çakışma yüzünden hizmette kesintiler olabilir.

Bu işlemden sonra personel ağına ait IP ayarlarını yapılandırmak için

Ağ ismi: local

Arayüz: (kullanılacak ağ kartının arayüzü)

Yapılandırma: IP adresini aşağıdaki gibi yapılandır

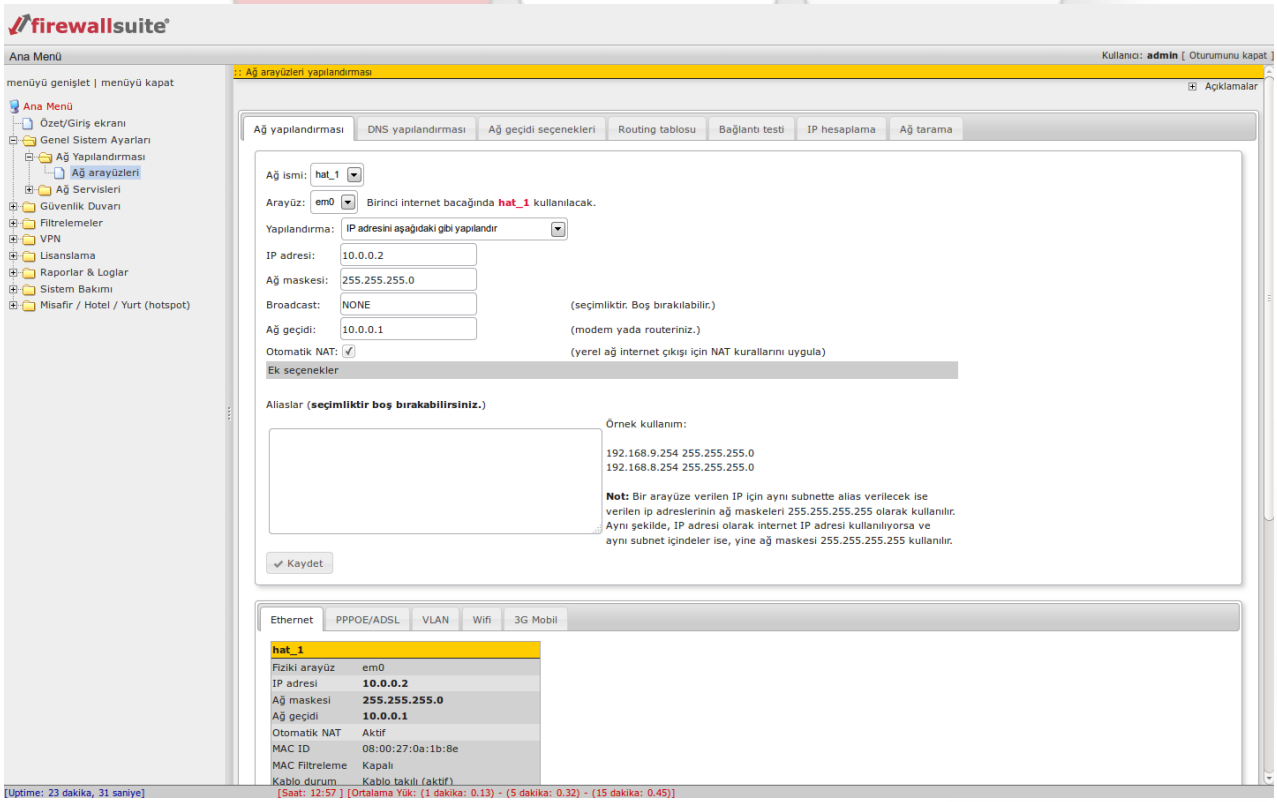
IP adresi: 192.168.10.1

Ağ maskesi: 255.255.255.0

Broadcast: (seçimliktir. Boş bırakılabilir.)

Bu ağın MAC filtrelemesini aç. (İşaretli olacak)

Kaydet düğmesine basınız.



Ağ ayarları (2)

Bu işlemden sonra misafir HotSpot ağına ait IP ayarlarını yapılandırmak için

Ağ ismi: local_2

Arayüz: (kullanılacak ağ kartının arayüzü)

Yapılandırma: IP adresini aşağıdaki gibi yapılandır

IP adresi: 192.168.20.1

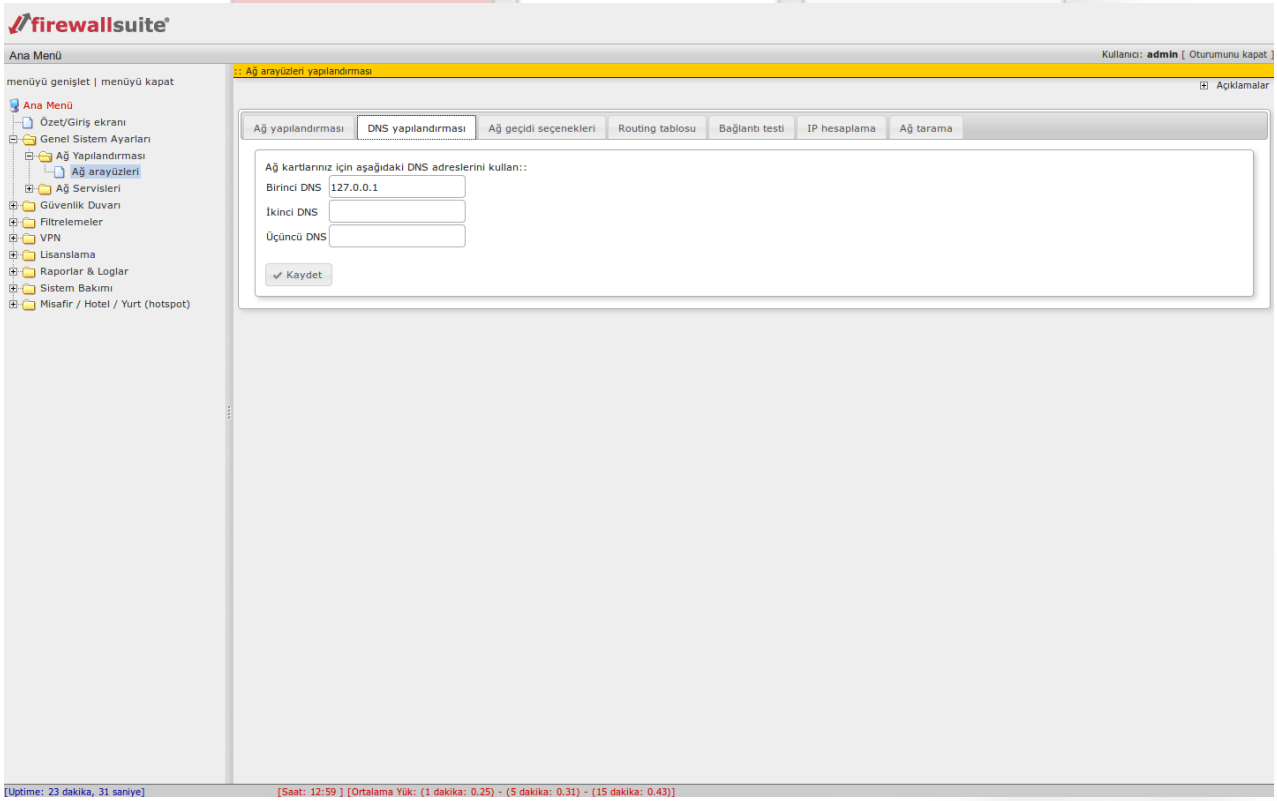
Ağ maskesi: 255.255.255.0

Broadcast: (seçimliktir. Boş bırakılabilir.)

Bu ağın MAC filtrelemesini aç. (İşaretli olacak)

Kaydet düğmesine basınız.

DNS Yapılandırması



DNS yapılandırması

DNS yapılandırması konusunda FirewallSuite® kendi içinde bir DNS servisi içerir ve bu servisin kullanılması önerilir. Ancak farklı bir DNS sunucunuz varsa bu DNS sunucunun kullanılması da mümkündür. DNS ayarları için

Ana Menü > ***Genel Sistem Ayarları*** > ***Ağ Yapılandırması*** > ***Ağ arayüzleri*** > ***DNS yapılandırması***

menüsüne geliniz. ***Birinci DNS*** 127.0.0.1 değerini giriniz

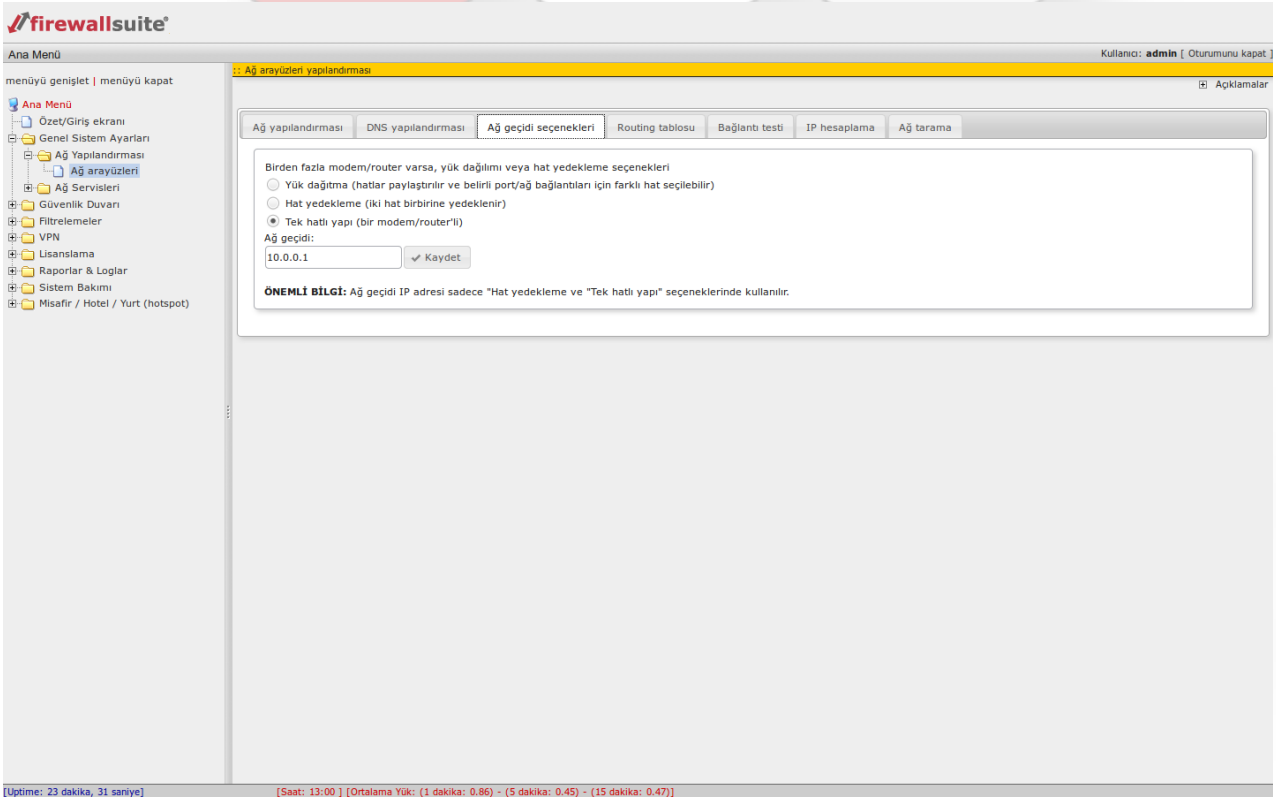
Kaydet düğmesine basınız.

Ağ Geçidi Seçenekleri

FirewallSuite® ağ geçidi noktasında birden fazla çalışma modu ile gelir. Bu modlar yük dağıtma, hat yedekleme ve tek internet hatlı yapı olarak üç farklı çalışma şeklini içerir. FirewallSuite® seçime ve ihtiyaçlara bağlı olarak bu seçeneklerden sadece biri ile çalışır. Örnek senaryomuzdaki yapımız bir internet hattı içeren yapı olduğu için bu kısımda

Tek hatlı yapı (bir modem/router'li) seçeneğini işaretleyin

Ağ geçidi: 10.0.0.1 değerini giriniz ve



Ağ geçidi seçenekleri

Kaydet düğmesine basınız.

DHCP Sunucusu

FirewallSuite® internet hizmeti sağladığı ağlar için gelişmiş DHCP özellikleri içerir. Örnek senaryomuzda bir personel bir de misafir HotSpot olarak iki farklı ağ planlanmaktadır. Bu nedenle iki yerel ağa hizmet verebilecek iki farklı DHCP sunucu tanımlanması gerekmektedir. Bunun için izlenecek adımlar

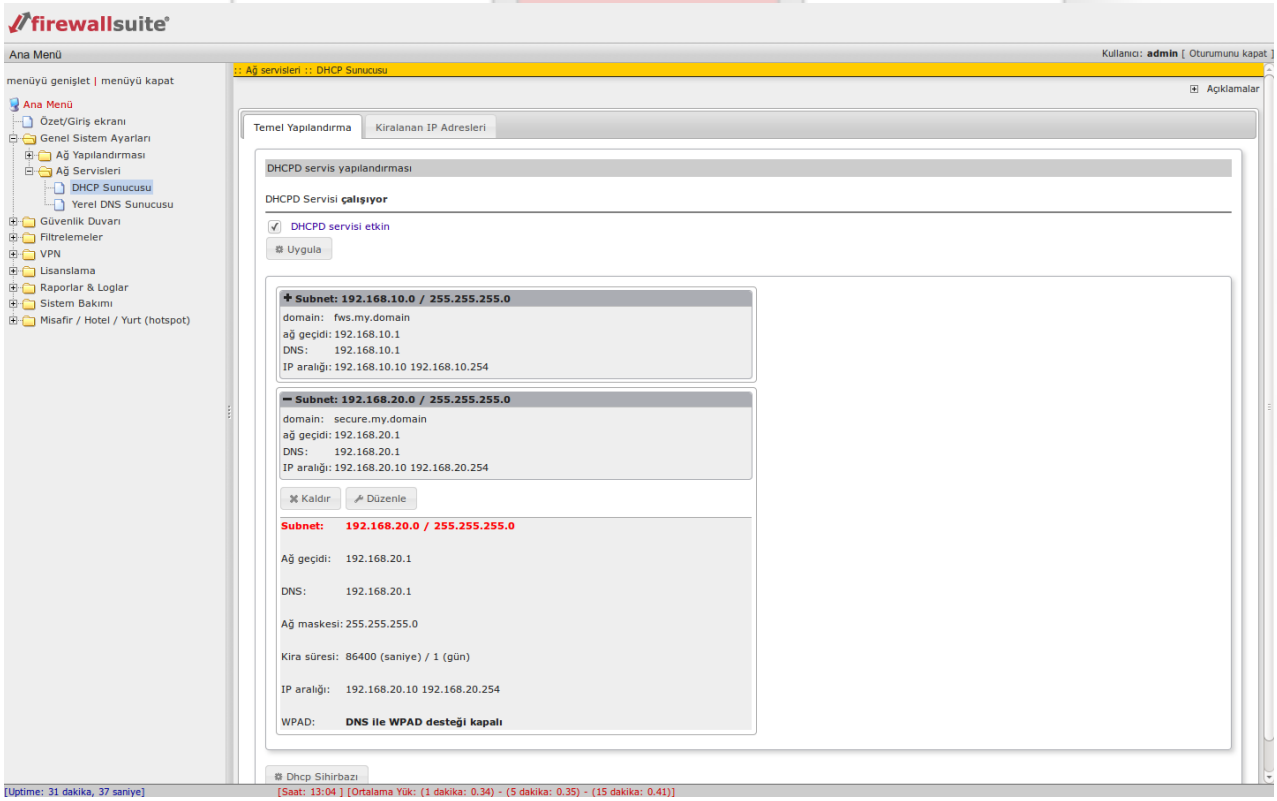
Ana Menü > ***Genel Sistem Ayarları*** > ***Ağ Yapılandırması*** > ***Ağ arayüzleri*** > ***DHCP Sunucusu***

kısmına geliniz. Bu kısımdaki ***DHCP Sihirbazı*** düğmesine basınız ve karşınıza gelen adımlara göre

IP alacak istemcilerin ağında DNS son eki için kullanılacak şirket domaini sirketim.local (gibi değer giriniz) ***İleri*** düğmesine basınız

Oluşturulacak subnet: local 192.168.10.1/255.255.255.0 (seçeneğini seçiniz) ***İleri*** düğmesine basınız

Dağıtılacak IP aralığı/aralıkları: ***Yeni aralık ekle*** linkine tıklayarak yeni aralık ekleme kısmını açınız ve aralık olarak 192.168.10.10 – 192.168.10.254 aralığını giriniz ve ***İleri*** düğmesine basınız.



DHCP Ayarları

IP adresi sabitlenen istemciler: kısmında bir ayar yapmadan ***İleri*** düğmesine basınız. (Bu kısımda MAC adresini bildiğiniz bir istemcinin, tanımlanmış DHCP havuzu dışında belirlenmiş bir IP adresini alması sağlanabilir)

İstemcilerin ağ maskesi: 255.255.255.0 değerini giriniz ve ***İleri*** düğmesine basınız.

Kullanılacak ağ geçidi: değerini ilgili ağ kartının IP adresi olan 192.168.10.1 olarak giriniz ve ***İleri*** düğmesine basınız.

İstemcilerin kullanacağı DNS adresleri: değerini ilgili ağ kartının IP adresi olan 192.168.10.1 olarak giriniz ve ***İleri*** düğmesine basınız.

Kira süresi / gün*:** değerini 7 olarak giriniz ve ***İleri düğmesine basınız. (Burada kullanılan değer isteğe bağlı olarak değişiklik gösterebilir.)

DNS ile WPAD desteğini etkinleştir. seçeneğini işaretlemeden ***İleri*** düğmesine basınız.

DHCP kurulum sihirbazı tamamlandı. Adımında ***İleri*** ve ardından ***Uygula*** düğmesine basınız.

Açılmış olan DHCP kaydı içinden üst kısımdaki artıya ***(+)*** basarak yaptığınız ayarları kontrol edebilirsiniz. Eğer yanlış bir ayar yapıldıysa açılan menüden Düzenle düğmesine basılarak ilgili ayar düzenlenip yukarıdaki adımları geçtikten sonra kaydedebilirsiniz.

Mevcut senaryomuza göre misafir HotSpot tarafını yapılandırmak için yine

Ana Menü > ***Genel Sistem Ayarları*** > ***Ağ Yapılandırması*** > ***Ağ arayüzleri*** > ***DHCP Sunucusu***

kısmına geliniz. Bu kısımdaki ***DHCP Sihirbazı*** düğmesine basınız ve karşınıza gelen adımlara göre

IP alacak istemcilerin ağında DNS son eki için kullanılacak şirket domaini **firewallsuite.sirketim.local** (gibi değer giriniz) ***İleri*** düğmesine basınız

✦ Misafir HotSpot doğrulama işlemi kendinden imzalı sertifika ile yapılabilir. Ancak yetkili SSL sertifikalı bir doğrulama üzerinde yapılacaksa buradaki alan adı ona göre tanımlanmış bir alan adı olmalı ve kurum internet sayfanızda tanımlanmış bir alt alan adı olmalıdır.

Oluşturulacak subnet: local 192.168.20.1/255.255.255.0 (seçeneğini seçiniz) ***İleri*** düğmesine basınız

Dağıtılacak IP aralığı/aralıkları: Yeni aralık ekle linkine tıklayarak yeni aralık ekleme kısmını açınız ve aralık olarak 192.168.20.10 – 192.168.20.254 aralığını giriniz ve ***İleri*** düğmesine basınız.

IP adresi sabitlenen istemciler: kısmında bir ayar yapmadan ***İleri*** düğmesine basınız. (Bu kısımda MAC adresini bildiğiniz bir istemcinin tanımlanmış DHCP havuzu içerisinde her zaman belirlenmiş bir IP adresini alması sağlanabilir)

İstemcilerin ağ maskesi: 255.255.255.0 değerini giriniz ve ***İleri*** düğmesine basınız.

Kullanılacak ağ geçidi: değerini ilgili ağ kartının IP adresi olan 192.168.20.1 olarak giriniz ve ***İleri*** düğmesine basınız.

İstemcilerin kullanacağı DNS adresleri: değerini ilgili ağ kartının IP adresi olan 192.168.20.1 olarak giriniz ve ***İleri*** düğmesine basınız.

Kira süresi / gün*:** değerini 7 olarak giriniz ve ***İleri düğmesine basınız.

DNS ile WPAD desteğini etkinleştir. Seçeneğini işaretlemeden ***İleri*** düğmesine basınız.

DHCP kurulum sihirbazı tamamlandı. Adımında ***İleri*** ve ardından ***Uygula*** düğmesine basınız.

Yerel DNS Sunucusu

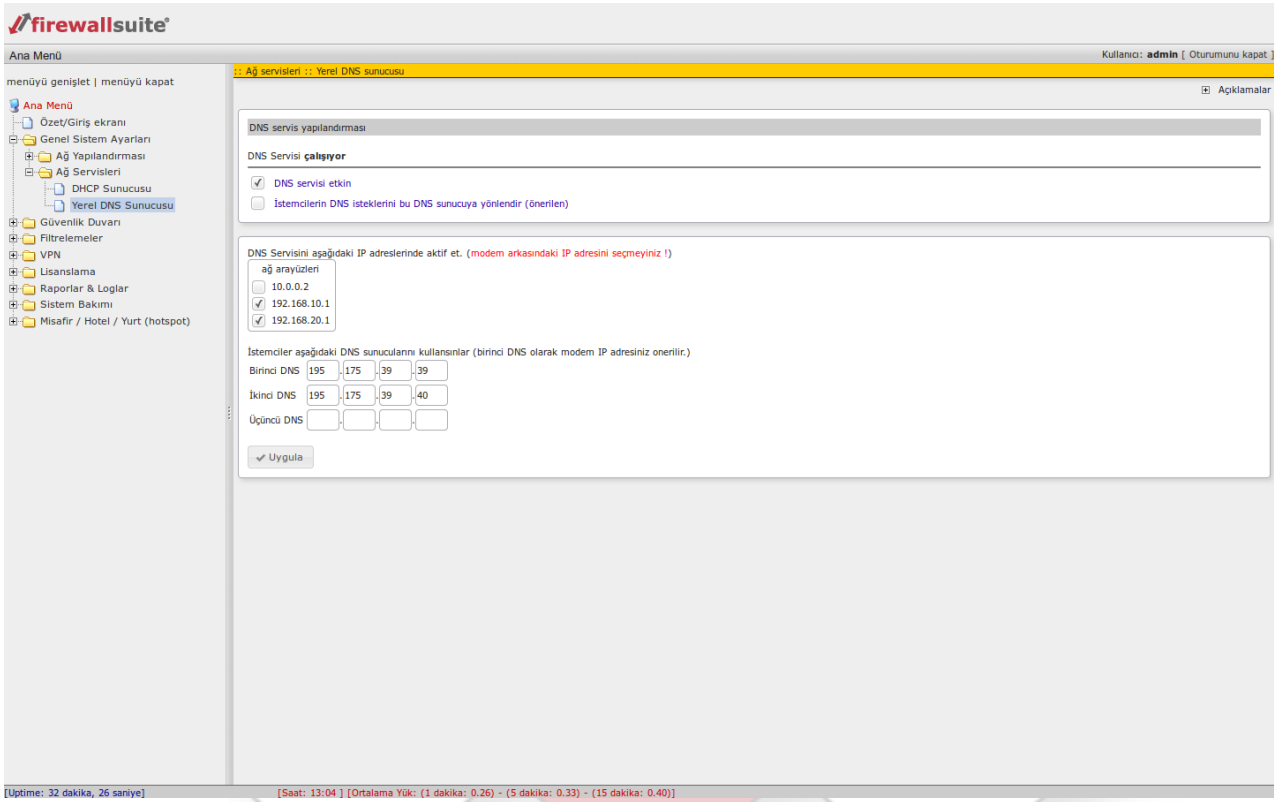
FirewallSuite® üzerinde bir DNS sunucusu ile gelir. Bu DNS sunucusunu ayarlamak için

Ana Menü > Genel Sistem Ayarları > Ağ Servisleri > Yerel DNS Sunucusu

kısmına geliniz. Burada

DNS servisi etkin onay kutusunu işaretleyiniz.

İstemcilerin DNS isteklerini bu DNS sunucuya yönlendir (önerilen) onay kutusunu işaretleyiniz. Bu seçenek ile kullanıcılar kendilerine özel DNS adresi yazsalar bile FirewallSuite® kendi üzerinde belirlenmiş olan DNS adresinden çalışmaya zorlar. Ağınızda farklı bir DNS sunucu var ise o DNS sunucuya göre planlama yapmanız gerekebilir.



Yerel DNS sunucu

DNS Servisini aşağıdaki IP adreslerinde aktif et. kısmında yer alan ***ağ arayüzleri*** için önceden belirlemiş olduğumuz local ağlarımız olan 192.168.10.1 ve 192.168.20.1 ağlarına ait onay kutularını işaretleyiniz.

İstemciler aşağıdaki DNS sunucularını kullansınlar kısmında hizmet aldığınız servis sağlayıcının DNS adreslerini giriniz (Örnek olarak Türk Telekom için ***Birinci DNS*** 195.175.39.39 ve ***İkinci DNS*** 195.175.39.40 gibi)

Uygula düğmesine basınız.

Güvenlik Duvarı

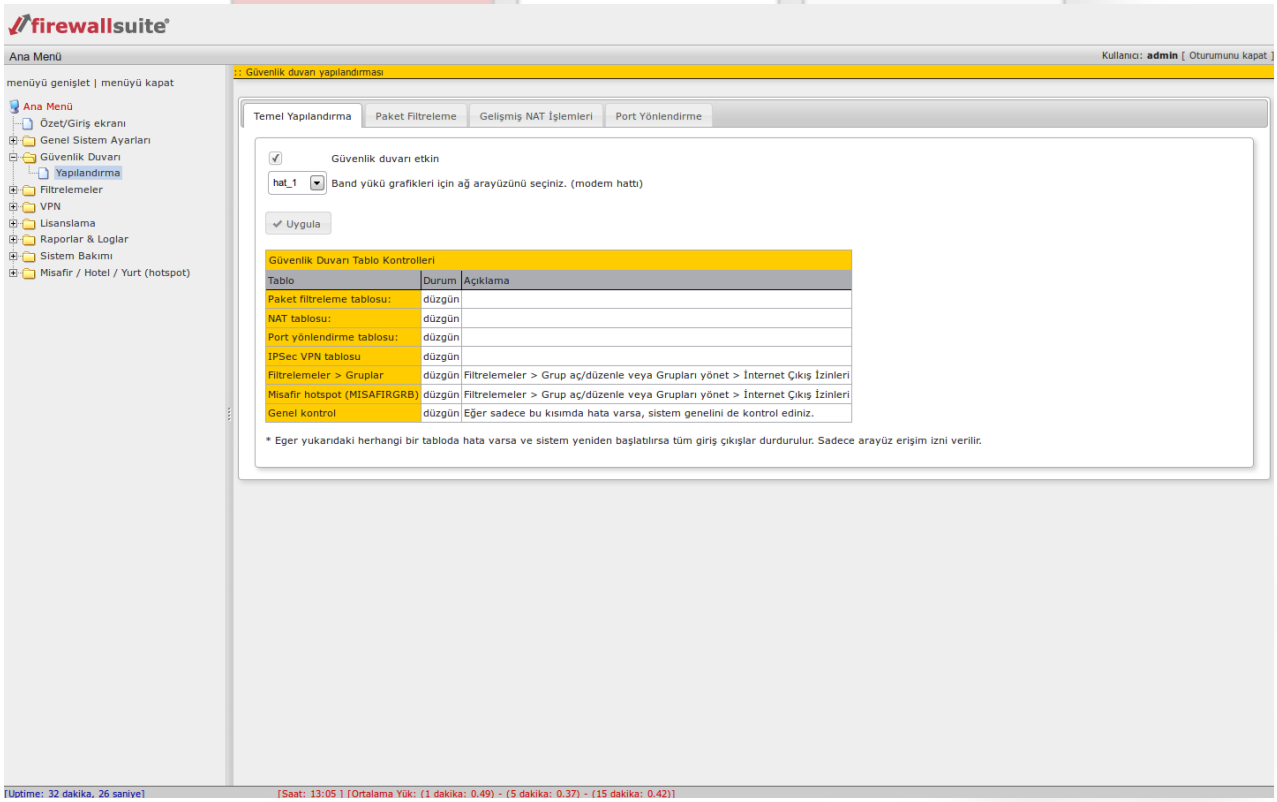
Bu yapılan işlemden sonra güvenlik duvarını aktif etmeniz gerekmektedir. Bunun için

Ana Menü > ***Genel Sistem Ayarları*** > ***Güvenlik Duvarı*** > ***Yapılandırma***

kısmına geliniz.

Güvenlik duvarı etkin onay kutusunu işaretleyiniz.

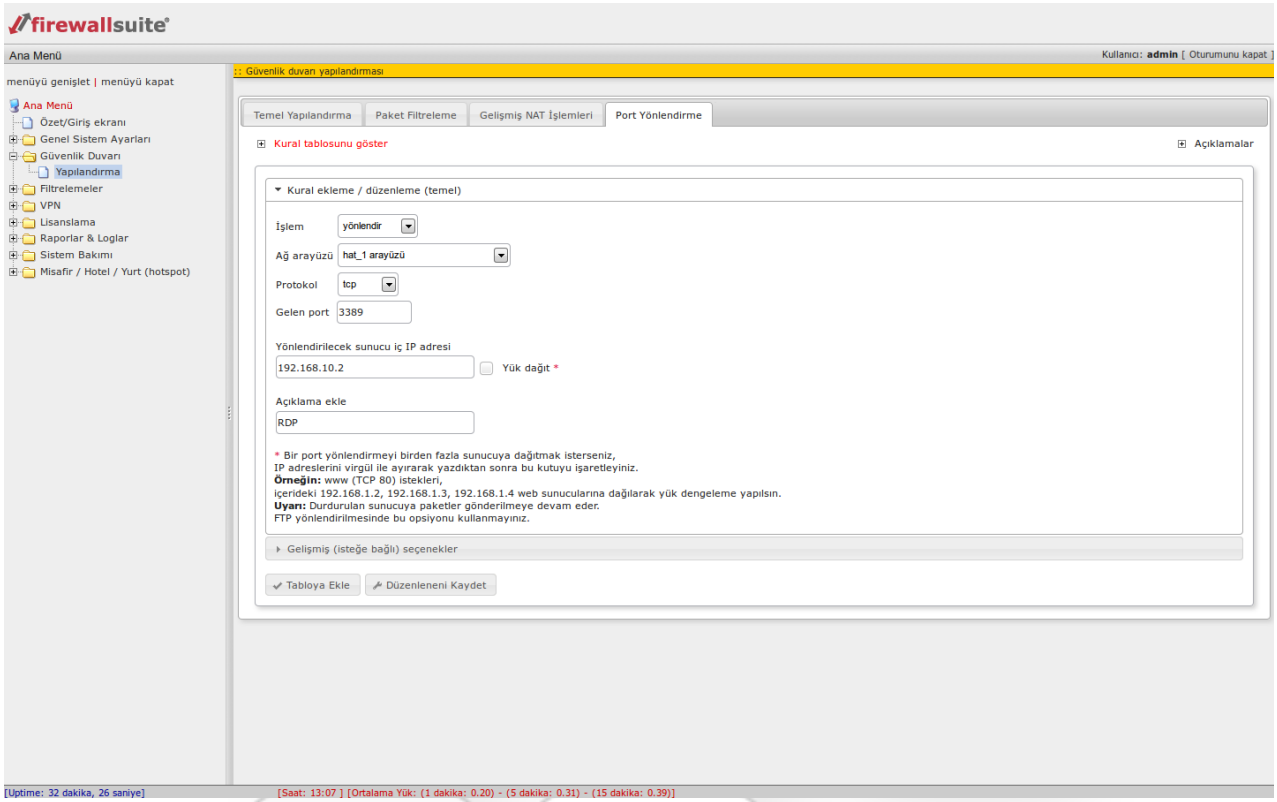
Band yükü grafikleri için ağ arayüzünü seçiniz. kısmını ***hat_1*** olarak seçiniz ve ***Uygula*** düğmesine basınız.



Güvenlik duvarı

Bu kısımda yer alan rapor ekranında güvenlik duvarı ile ilgili yapılandırmanızda bir hata olup olmadığını görebilirsiniz.

Port Yönlendirme



Port yönlendirme

Port yönlendirme işleminde yerel ağımızda bir sunucu olduğu ve bu sunucunun 192.168.10.2 IP adresine sahip olduğu tasarlanmıştır. Bu sunucu için yapılacak RDP port yönlendirme işlemi için 3389 nolu TCP portunu yönlendirme yapılacağı var sayılmıştır.

Bu işlem için

İşlem açılan kutudan **yönlendir** seçiniz.

Ağ ara yüzü açılan kutudan **hat_1 ara yüzü** seçiniz.

Protokol açılan kutudan **TCP** seçiniz. Yönlendirme yapacağınız sistemin gerekliliklerine göre TCP veya UDP seçeneklerini seçebilirsiniz.

Gelen porta 3389 yazınız. (Birden fazla port yazmanız gerekirse portlar arasında bir boşluk bırakarak yazabilirsiniz)

Yönlendirilecek sunucu iç IP adresi senaryomuza göre 192.168.10.2 sunucumuzun IP adresini yazınız.

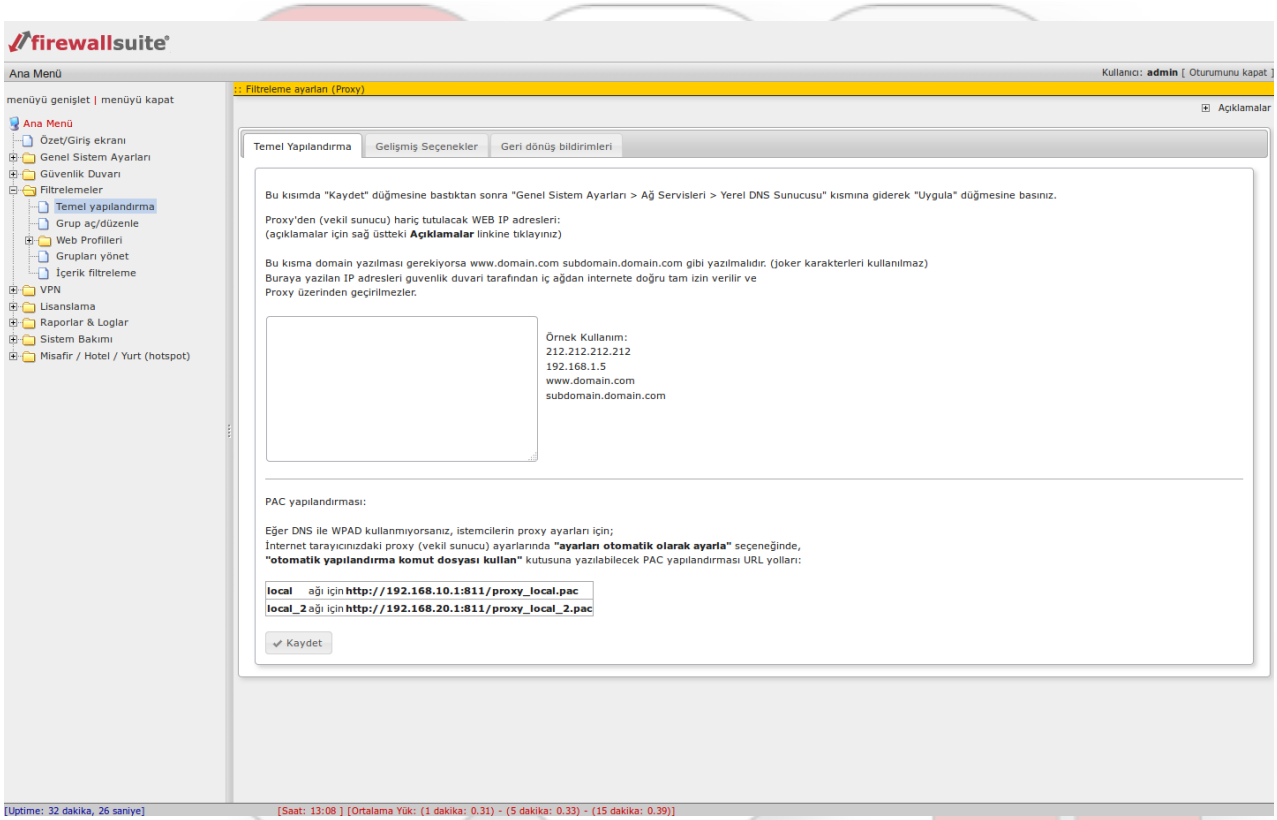
Açıklama ekle kısmına daha sonra yapılan işlemi hatırlamak için RDP gibi bir açıklama yazabilirsiniz.

Temel port yönlendirme işlemi bu kadardır.

✦ DVR cihazları gibi sistemler port yönlendirme konusunda aralık isteyebilirler. Aralık yazma işlemini iki nokta üst üste ile yazabilirsiniz. Örnek olarak 5000 ile 6000 portları arasını 5000 ve 6000 dahil olmak üzere **5000:6000** olarak yazabilirsiniz. Buna ek olarak 3389 ve 5000 ile 6000 arası gibi bir yönlendirme gerektiğinde **3389 5000:6000** şeklinde yazabilirsiniz.

Filtrelemeler

FirewallSuite® çok gelişmiş filtreleme seçenekleri sunar. Bu seçenekleri uygulamadan önce ön ayarların yapılması ve sistem üzerinde planlanan grupların açılmış olması gerekmektedir.



Filtrelemeler

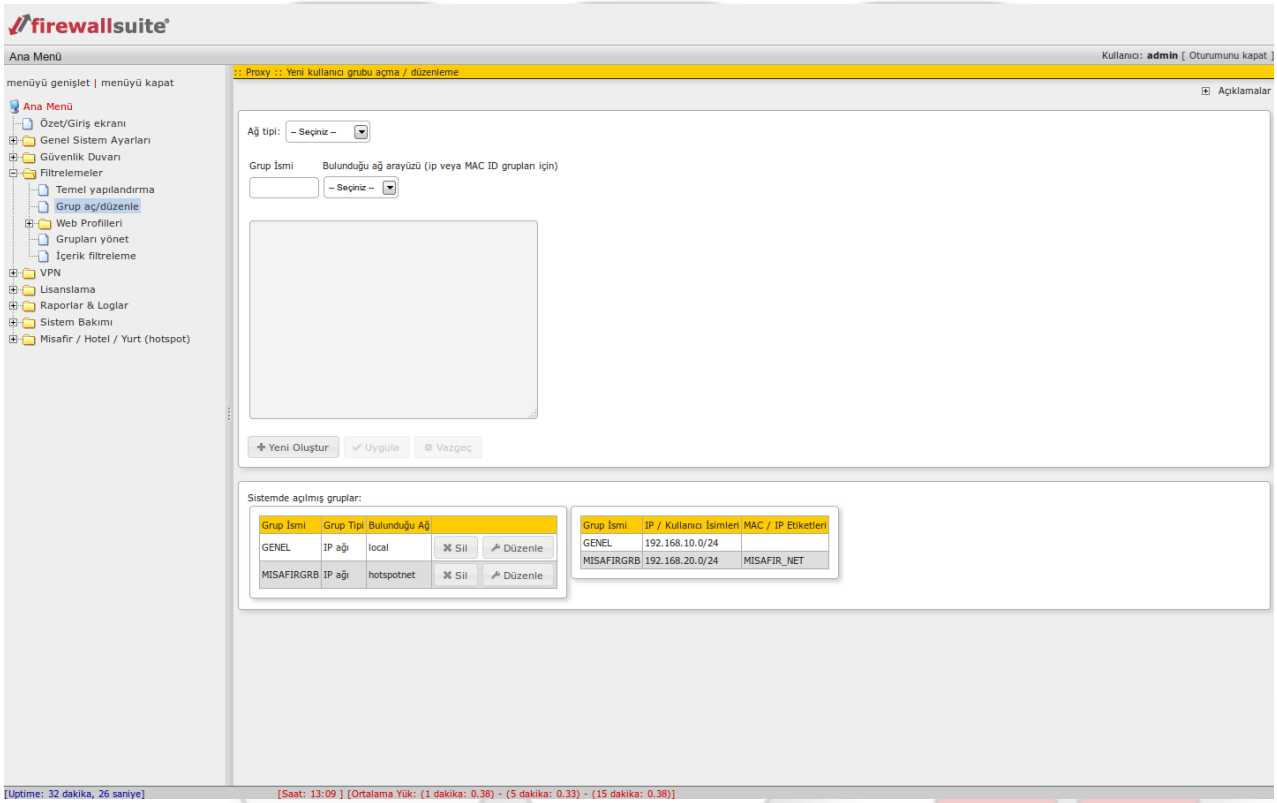
Bu işlemler için ilk olarak

Ana Menü > ***Filtrelemeler*** > ***Temel Yapılandırma***

kısmına geliniz. ***Temel yapılandırma*** sekmesi altında yer alan ***Kaydet*** düğmesine bir kere basınız. Aynı yerde bulunan ***Gelişmiş Seçenekler*** sekmesinde yer alan ***Kaydet*** düğmesine bir kere basınız.

Grup Açma

Bu işlemlerden sonra sistemde internet hizmeti alacak gruplarımızı tanımlamamız gerekmektedir. Grup tanımlama işlemini IP aralığı, MAC adresi gibi seçeneklere göre yapabilirsiniz. Örnek uygulamamızda IP adresine göre bir grup oluşturarak tanımlama yapacağız. Misafir HotSpot tarafı için grup açma işlemi sistem tarafından otomatik olarak yapılmaktadır.



Grup aç düzenle

IP tabanlı grup açmak için

Ana Menü > ***Filtrelemeler*** > **Grup aç/düzenle**

menüsüne geliniz.

Ağ tipi: açılan kutudan **IP adresi** seçiniz.

Grup İsmi kısmına **GENEL** gibi bir isim veriniz. (Vereceğiniz grup isminde Ç, Ğ, İ, Ö, Ü, ç, ğ, ı, ö, ü gibi karakterler kullanmayınız)

Bulunduğu ağ arayüzü seçeneğini **personel** grubu olması itibariyle ***local*** seçeneğini işaretleyiniz.

IP adresi veya aralığı kısmında personel tarafımıza olan IP bloğu için **192.168.10.0/24** yazınız.

Yeni Oluştur düğmesine basınız.

✦ Bu kısımda tek tek IP adreslerini alt alta yazabildiğiniz gibi bir IP bloğu yazmak istediğiniz zaman **192.168.10.1-192.168.10.254** şeklinde IP aralığı da yazabilirsiniz. Burada dikkat edilmesi gereken en önemli noktalardan biri, bir grup içine yazılan bir IP adresinin başka bir grupta bulunmamasıdır.

Gruba İnternet Erişim Haklarını Verme

Açtığımız **GENEL** grubuna internet erişiminin sağlanması için ***Ana Menü*** > ***Filtrelemeler*** > ***Grupları Yönet*** *kısmına geliniz.*

Grubu seç: açılan kutudan açmış olduğumuz **GENEL** grubunu seçiniz ve ***İnternet Çıkış İzinleri*** sekmesine geliniz.

Bu grup için tüm internet servislerine izin ver onay kutusunu işaretleyiniz.

WEB isteklerini Filtrele ve LOG tut (önerilen) onay kutusunu işaretleyiniz.

Uygula düğmesine basınız.

Normal şartlarda bu işlem ile tüm internet servislerine izin vermiş olmaktayız. İlgili gruba sadece e-posta erişimi ya da belirli porta erişim izni verecekseniz ***Bu grup için tüm internet servislerine izin ver*** onay kutusunu işaretlemeden istediğiniz protokollere uygun onay kutularını işaretleyebilir ve ya ***Diğer TCP portlar:*** ve ***Diğer UDP portlar:*** bölümüne istediğiniz port değerlerini elle girebilirsiniz. Bu kısımda birden fazla port olduğunda boşluk bırakarak yazabilirsiniz.

Bu işlemle senaryomuza göre personel ağına internet erişimi vermiş olduk.

HotSpot İnternet Erişimini Açma

FirewallSuite® misafir HotSpot tarafında birden fazla doğrulama seçeneği ile gelir. Bu seçeneklerden biri kullanılabileceği gibi istenilen birden fazla seçenek de bir arada kullanılabilir. Tüm seçenekler yetkili bir görevlinin LOBİ arayüzünden elle şifre temini destekler ancak örnek senaryomuza göre gelen misafirimiz için T.C. Kimlik doğrulamalı bir saatlik internet hizmeti tanımlayacağız.

Bu işlem için

Ana Menü > ***Misafir / Hotel / Yurt (hotspot) / Yapılandırma*** > ***Kimlik Doğrulama*** > ***Yapılandırma***

menüsüne geliniz. Bu menüden misafir HotSpot ağını temel olarak aktif etmek için

192.168.20.1 ağının onay kutusunu işaretleyin ve ardından DHCP de tanımlamış olduğunuz

secure.sirketim.local onay kutusunu işaretleyiniz.

Etkinleştirme sonrası bu sayfaya yönlendir. kısmına isteğe bağlı olarak ilk bağlantıda otomatik olarak yönlendirilmesini istediğini bir internet adresi yazınız.

Kaydet düğmesine basınız.

T.C. Kimlik No ile Doğrulama

Bir sonraki aşamada T.C. Kimlik ile girişi etkinleştirmek için ***Ana Menü*** > ***Misafir / Hotel / Yurt (hotspot) / Yapılandırma*** > ***Kimlik Doğrulama*** > ***T.C. Kimlik No*** *menüsüne geliniz.*

T.C. KİMLİK NO doğrulayarak girişi etkinleştir. onay kutusunu işaretleyiniz.

İzin verilen en fazla cihaz sayısı ile bir T.C. Kimlik No ile bağlanabilecek eş zamanlı istemci sayısını belirleyiniz.

İzin verilen internet kullanım süresi'ni 1 saat olarak belirleyiniz.

ve bu süre dolduğunda izin verilmeyen internet süresi. değerini kişi internet erişim süresini harcadıktan sonra kaç saat boyunca internete erişmesi istenmiyorsa ona göre belirleyebilirsiniz.

Kaydet düğmesine basınız.

Gruba İnternet Erişim Haklarını Verme

Bu işlem ile misafir HotSpot için T.C. Kimlik doğrulaması için izin vermiş olduk. Son işlem olarak ilgili gruba internet erişim haklarının tanımlanması gereklidir. Bunun için sistem tarafından otomatik olarak açılmış **MISAFIRGRB** grubuna internet erişiminin sağlanması için

Ana Menü > ***Filtrelemeler*** > ***Grupları Yönet***

kısmına geliniz.

Grubu seç: açılan kutudan açmış olduğumuz **MISAFIRGRB** grubunu seçiniz ve **İnternet Çıkış İzinleri** sekmesine geliniz.

Bu grup için tüm internet servislerine izin ver onay kutusunu işaretleyiniz.

WEB isteklerini Filtrele ve LOG tut (önerilen) onay kutusunu işaretleyiniz.

DNS isteklerini yerel DNS sunucusuna yönlendir (önerilen) onay kutusunu da isteğe bağlı olarak işaretleyebilirsiniz.

Uygula düğmesine basınız.

Bu işlemlerle birlikte HotSpot internet hizmetini açmış olduk.

✦ HotSpot modülü, tüm kullanıcı doğrulama işlemlerini güvenlik nedeniyle SSL şifrelemesiyle yapmaktadır. SSL sistemi için gerekli olan sertifika kendinden imzalı ya da yetkili otorite tarafından sağlanmış olabilir. Yetkili otorite tarafından sağlanmamış ya da yetkili otorite tarafından sağlanmış olmasına karşılık geçerlilik süresi dolmuş setifikalar istemci bilgisayarların internet tarayıcılarında sertifika uyarısı karşılaşmasına neden olurlar.

Panel Üzerinden HotSpot Kullanıcısı Açmak

Yetkili personel tarafından kullanıcı tanımlaması gerektiğinde Kimlik Yönetim Sitemine erişmek için http://192.168.10.1:811/KYS/ adresine erişim sağlayın. Bu kısımda kullanıcı adı **lobi** ve varsayılan şifre **123456** olarak tanımlanmıştır. Bu kısımdaki şifre değeri değiştirilebilir. Erişim yaptığınız IP adresi kendi kurulumunuza göre değişiklik gösterebilir.

Buradan bir kullanıcı açmak için

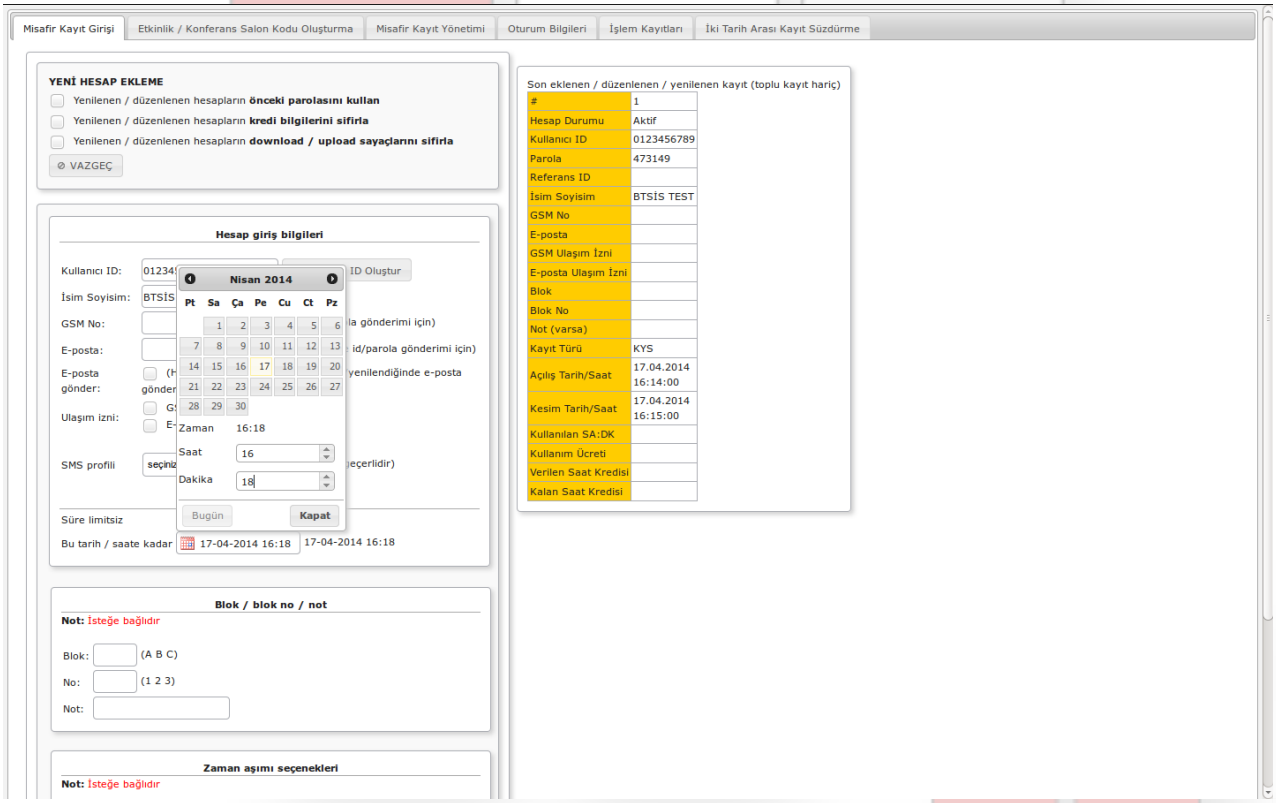
Kullanıcı ID: kısmına kişinin T.C. Kimlik numarasını yazabilirsiniz. Eğer bu şekilde bir imkan yoksa ***Rastgele ID Oluştur*** düğmesine basabilirsiniz.

İsim Soyisim: kısmına kullanıcının adını ve soyadını yazınız.

GSM No: ve ***E-Posta*** bilgilerini isteğe bağlı olarak doldurunuz.

Bu tarih / saate kadar kısmında kullanıcının alacağı internetin ne zamana kadar geçerli olacağı bilgisini giriniz.

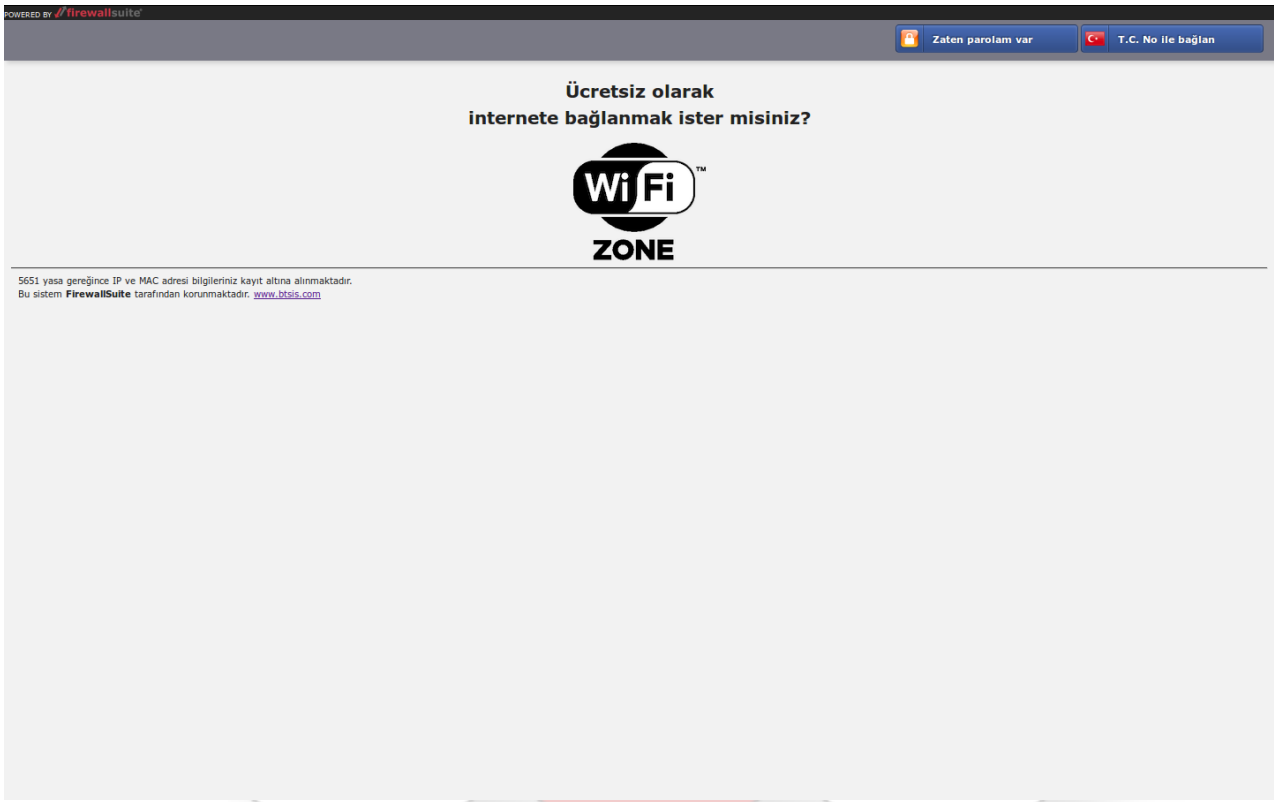
Hesabı Oluştur düğmesine basınız.



KYS Lobi erşim paneli

Normal şartlar altında oluşturduğunuz hesaba ait erişim bilgilerini bu sayfada sağ tarafta bulunan ***Kullanıcı ID*** ve ***Parola*** gibi hesap bilgilerini özet ekranlarında görebilirsiniz. Bu özet ekranı gerek elle girilen gerekse otomatik tanımlı son eklenmiş kişin bilgilerini sunar. Oluşturulmuş hesaplara ait ana listeyi görmek için yine LOBİ erişim ekranında bulunan ***Misafir Kayıt Yönetimi*** sekmesini kullanabilirsiniz. Bu ekranda son eklenen kayıtlar en üstte olacak şekilde gözükecektir.

Örnek senaryomuza göre yapılandırma yukarıdaki gibidir. Yukarıda anlatılanlar belirli bir ağ segmentine göre internet hizmetinin alınıp iç ağa verilmesi şeklindedir.



Misafir internet erişim ekranı

✦ HotSpot modülü, birden fazla kullanıcı doğrulama yönteminin bir arada çalışmasına olanak sağlar. Sistem yöneticisi uygun gördüğü kullanıcı doğrulama yöntemlerini sunabilir ve kullanıcı da bu yöntemlerden kendine uygun olanı seçebilir.

Diğer Ayarlar

Yukarıdaki kısımda FirewallSuite® ürününe internet sağlanması ve sağlanan bu internetin yerel kullanıcılara verilmesi konusuna değinilmiştir. FirewallSuite® ürününün yetenekleri yukarıda anlatılanlarla sınırlı değildir. Bundan sonraki bölümlerde yasaklamalar, misafir HotSpot ayarları kısımlarda yapılabilecek önemli ayarlar hakkında genel bilgiler verilecektir. Anlatım bütünlüğü açısından gerekli görülen yerlerde yapılan bir ayarın neden yapıldığı bilgisi öncesinde paylaşılmıştır.

Alias IP Tanımlama

FirewallSuite® ile ağ kartlarına alias IP tanımı yapılabilir. Örnek olarak local ağ kartımıza bir alias IP tanımlamak için

Ana Menü > ***Genel Sistem Ayarları*** > ***Ağ Yapılandırması*** > ***Ağ arayüzleri*** > ***Ağ yapılandırması***

sekmesine geliniz ve ***local*** olarak tanımladığımız ağ grubunun ***Düzenle*** düğmesine basınız.

Bu kısımda yer alan ***Aliaslar*** kutusuna 192.168.9.254 255.255.255.0 gibi istediğiniz IP adresi ve bir boşluk bırakarak alt ağ maskesini yazmak suretiyle bir veya daha fazla IP adresi girebilirsiniz. Yapacağınız ailas tanımlama işlemlerinin sistemde bir IP çakışması oluşturmamasına dikkat ediniz.

Routing Yazmak

FirewallSuite® ile routing yazmak son derece kolaydır. Bir tek makine için routing yazabileceğiniz gibi bir ağ içinde routing yazabilirsiniz. Örnek olarak 3 adet ağ kartımız olduğunu; Ağ geçitlerimizin 10.0.0.1 diğer ağ kartının 192.168.10.1 olduğunu ve de yerel ağımızın 192.165.0.1 olduğunu farz edelim. Normal internet çıkışları 10.0.0.1 üzerinden yapılırken örnek olarak 1.2.3.4 IP adresine erişimin 192.168.10.1 üzerinden yapılması gerektiği bir durum da

Ana Menü > ***Genel Sistem Ayarları*** > ***Ağ Yapılandırması*** > ***Ağ arayüzleri*** > ***Ağ yapılandırması*** > **Routing tablosu**

sekmesine geliniz.

Ağ/makine seçeneğini ***Makine*** olarak işaretleyiniz.

Hedef : 1.2.3.4

Ağ maskesi : 255.255.255.0

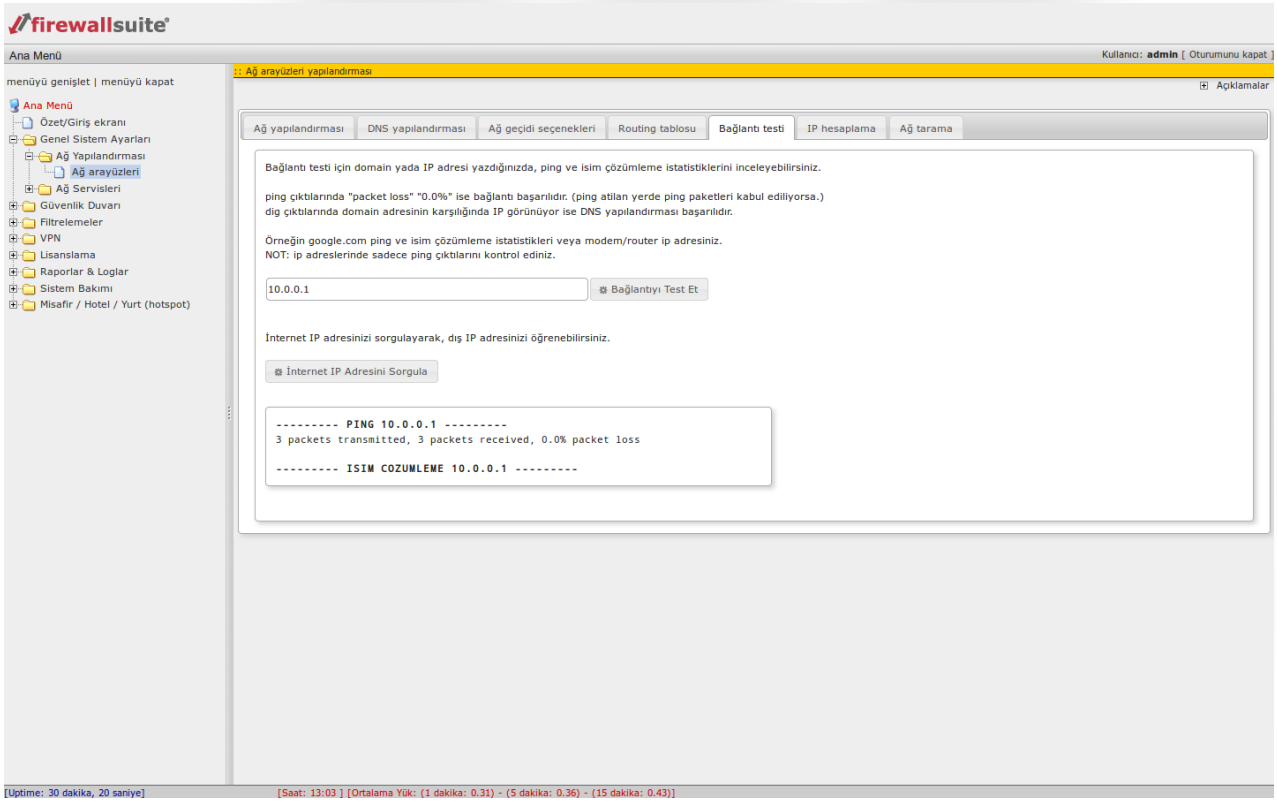
Ağ geçidi : 192.168.10.1

değerlerini giriniz ve ***Kaydet*** düğmesine basınız. Bu işlemden sonra FirewallSuite® üzerinde yapılacak her routing işleminde 1.2.3.4 IP adresine gidiş için ağ geçidi 192.168.10.1 olarak tanımlanacaktır.

Daha sonra aynı ekran içinde yer alan ***Kullanıcı tanımlı yönlendirme tablosu*** üzerinden yazılmış olan routing işlemleri yeniden düzenlenebilir ya da silinebilir.

Bağlantı Testi

FirewallSuite® ürününüzün internet hizmeti alıp almadığı konusunda kontrol yapmak istediğinizde arayüzdeki bağlantı testi bölümünü kullanabilirsiniz.



Bağlantı testi

Bunun için

Ana Menü > ***Genel Sistem Ayarları*** > ***Ağ Yapılandırması*** > ***Ağ arayüzleri*** > ***Ağ yapılandırması*** > ***Bağlantı Testi***

menüsüne geliniz. Buradaki kutuya www.google.com.tr gibi internet üzerinde aktif olduğuna emin olduğunu bir internet adresi yazarak ***Bağlantıyı Test Et*** düğmesine basınız. FirewallSuite® internet hizmeti alıyorsa ve yapılandırmalar doğruysa (ağ geçidi ve DNS gibi) kısa bir süre için alt kısımda bağlantı testi yapmış olduğunu internet adresine ilişkin IP adreslerini görmeniz gereklidir.

✦ Bu kısma modem IP adresi yazarak da Ping kaybı olup olmadığı konusunda test yapabilirsiniz.

IP Hesaplama (CIDR)

FirewallSuite® CIDR sistemine sahip IP hesaplama aracı içerir. Bu araç ile üç farklı biçimde IP hesaplama işlemi yapılabilir. Örnek olarak 192.168.0.10 IP adresine ve 255.255.255.0 alt ağ maskesine sahip olduğumuz bir durumda

Ana Menü > ***Genel Sistem Ayarları*** > ***Ağ Yapılandırması*** > ***Ağ arayüzleri*** > ***Ağ yapılandırması*** > ***IP Hesaplama***

menüsüne gelince ilgili kutuya

192.168.0.10/255.255.255.0

yazın ve ***Hesapla*** düğmesine basınız. Karşınıza çıkan

address: 192.168.0.10
netmask: 255.255.255.0 (0xffffff00)
network: 192.168.0.0 /24
broadcast: 192.168.0.255
host min: 192.168.0.1
host max: 192.168.0.254
hosts/net: 254

değerlerine göre içinde bulunduğu ağ hakkında bilgi edinebilirsiniz.

Ağ Tarama

FirewallSuite® bağlı bulunduğu ağlardaki host makinelerini tarama aracına sahiptir. Bunun için

Ana Menü > ***Genel Sistem Ayarları*** > ***Ağ Yapılandırması*** > ***Ağ arayüzleri*** > ***Ağ yapılandırması*** > ***Ağ Tarama***

menüsüne geliniz. Tarama işlemi CIDR ağ sistemine göre yapılmaktadır. Örnek olarak 192.168.10 IP adresine sahip olduğunuzu ve yerel ağ tarafında

bulunduğunuz düşünüldüğünde 192.168.10.0/24 ağını taramanız gereklidir. Bu değeri sahip olduğunuz IP adresi ve alt ağ maskesi ile FirewallSuite® IP hesaplama aracından hesaplayabilirsiniz. Aldığınız çıktı değerindeki ağ değeri bulunduğunuz ağa ilişkin tanımlamadır.

İlk olarak ilgili menü de açılan kutudan ***local*** seçeneğini işaretleyiniz ve alt kısımdaki kutuya ***192.168.10.0/24*** olan yerel ağ blok değerini giriniz ve ***Tara*** düğmesine basınız. Bu işlem ile ağınızda bulunan Host makinelerinin listesini alabilirsiniz. Bazı istemcilerdeki yerel güvenlik duvarı ya da bunun gibi yazılımlar bu bilgilerin alınmasını engelleyebilir. Ağınızda farklı IP blokları bulunabilir. Bu tip durumlarda ilgili IP bloğuna göre tarama yapabilirsiniz.

DHCP Dosyasını Temizlemek

DHCP kira dosyası yapılandırmaya veya beklenenden fazla istemci olması gibi sebeplere bağlı olarak dolabilir. Özellikle DHCP kira süresinin uzun tutulduğu noktalarda karşılaşılabilen bu durum için DHCP kira dosyasının temizlenmesi gerekebilir. Bunun için

Ana Menü > ***Genel Sistem Ayarları*** > ***Ağ Servisleri*** > ***DHCP Sunucusu*** > ***Kiralanan IP Adresleri***

menüsüne geliniz

Kira Dosyasını Temizle düğmesine basınız. Bu işlemden sonra ağdaki istemciler yeniden DHCP sunucusundan IP adresi alacaklardır.

Hat Yedekleme

FirewallSuite® iki adet internet hattı kullandığı durumlarda bu hatlardan bir tanesini diğerine otomatik olarak yedekleme özelliğine sahiptir. Bu yapılandırma için öncelikle FirewallSuite® üzerinde iki adet internet hattı bulunması gerekir. Bu hatlardan biri birinci hat, diğeri ikinci hat olarak belirlenmelidir. Birinci hat her zaman öncelikli olarak çalışır ve birinci hattın koptuğu durumlarda ikinci hat otomatik olarak devreye girer. Birinci hattın internet hizmeti açıldığı anda otomatik olarak ikinci hat kapanır ve erişimler birinci hattan devam eder.

Bu işlemi ayarlamak için öncelikle FirewallSuite® üzerinde iki adet internet hattı takılı olduğuna emin olunuz.

Ana Menü > ***Genel Sistem Ayarları*** > ***Ağ Yapılandırması*** > ***Ağ arayüzleri*** > ***Ağ geçidi seçenekleri***

menüsüne geliniz.

Hat yedekleme (iki hat birbirine yedeklenir) radyo düğmesini seçiniz.

Bu işlemden sonra aynı yerde alt kısımda açılan hat yedekleme menüsünde

Yedeklenecek ağ geçitleri (birinci koparsa ikinci devralacak) menüsünden birinci internet hattını ve ikinci internet hattını seçiniz.

Hat kontrolü için kullanılacak IP adresi (domain isimleri kullanmayınız) kısmına internetin var olup olmadığının kontrol edileceği ve internette var olduğuna emin olduğunuz bir IP adresini yazınız.

✦ Örnek olarak ns1.google.com gibi emin olduğunuz bir alan adına ait bir IP adresi yazılmalıdır.

Filtrelemeler

FirewallSuite® çok geniş filtreleme seçenekleri seçenekleri ile gelir. Bu filtreleme seçeneklerinde temel uygulama mantığı üç aşamalı olarak değerlendirilir.

1. İstenilen kullanıcı gruplarının açılması
2. Planlanan yasakların tanımlanması
3. İstenilen gruplara planlanan yasakların uygulanması

Bunun bir örneği ilk bölümde yer alan örnek kullanım senaryosunda anlatılmıştır. Bu kısımda ise ilgili menülere değinilmiştir. ***Filtrelemeler*** bölümünde yer alan ***Temel yapılandırma*** menüsünde temel yapılandırma işlemleri yapılır. Bu işlemler içerisinde istenilen IP veya domain adreslerini proxy'den (vekil sunucudan) hariç tutmak, elle yapılandırılacak istemci proxy ayarları için gerekli adreslerin tanımı, ön belleğe alınmayacak domainlerin tanımı ve yasaklama sayfaları bildirimleri gibi seçenekler bulunur.

Filtrelemeler bölümünde yer alan ***Grup aç/düzenle*** *bölümünde ise* FirewallSuite® tarafında erişim verilecek ya da erişimi yasaklanacak grupların tanımı yapılır. Bu tanımlar IP adresi, MAC adresi ya da kullanıcı adı olmak üzere üç farklı biçimde açılabilir. Yalnız HotSpot işlemi için elle grup tanımı yapılmaz. HotSpot kullanılacak yerlerde servis aktif edildiğinde ilgili grup otomatik olarak oluşturulur ve bu gruba internet erişim yetkileri elle tanımlanır.

Bir Dış IP Adresini Proxy'den Hariç Tutmak

Bazı özel durumlarda belirli IP ya da domain adreslerini proxy hizmetinden hariç tutmak gerekebilir. Bunun için

Ana Menü > Filtrelemeler > Temel Yapılandırma > Temel Yapılandırma

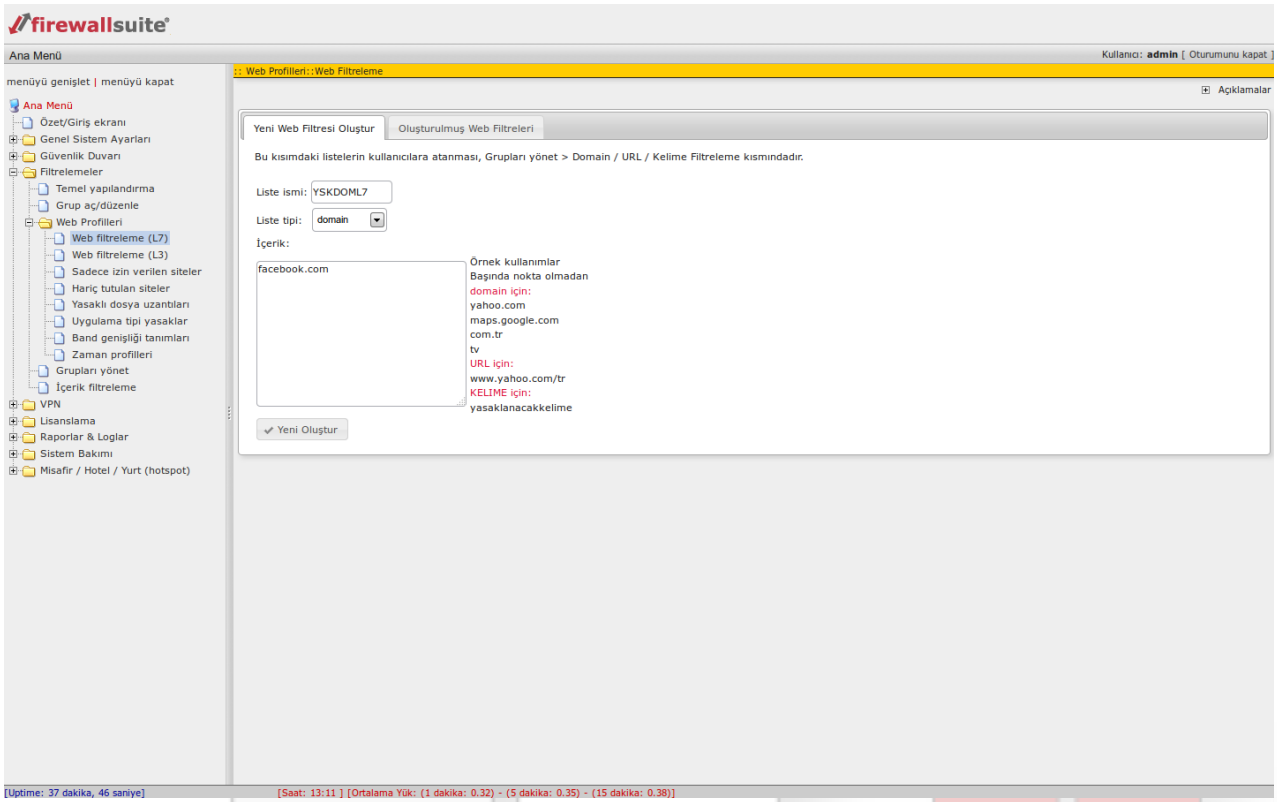
menüsüne geliniz ve proxy hizmetinden hariç tutmak istediğiniz IP ya da domain adreslerini bu kısımda ki kutucuğa yazınız. Bu kısma eklediğiniz adresler tüm yasaklama ve LOG kayıt işlemlerinden hariç tutulur. Bu yüzden gerekmedikçe bu kısma bir değer girmeniz önerilmez.

Web Filtreleme (L7)

Tüm HTTP bazlı domain, URL ve kelime yasakları bu kısımdan yapılır. Önce bir liste ismi tanımlanır. Sonrasında Liste tipi ile ne tür bir yasak yapılacağı

tanımlanır ve bu tanıma göre yasaklanması gereken değerler girilir. İşlem bittiğinde ***Yeni Oluştur*** düğmesine basılarak yasaklama tanımı yapılmış olur.

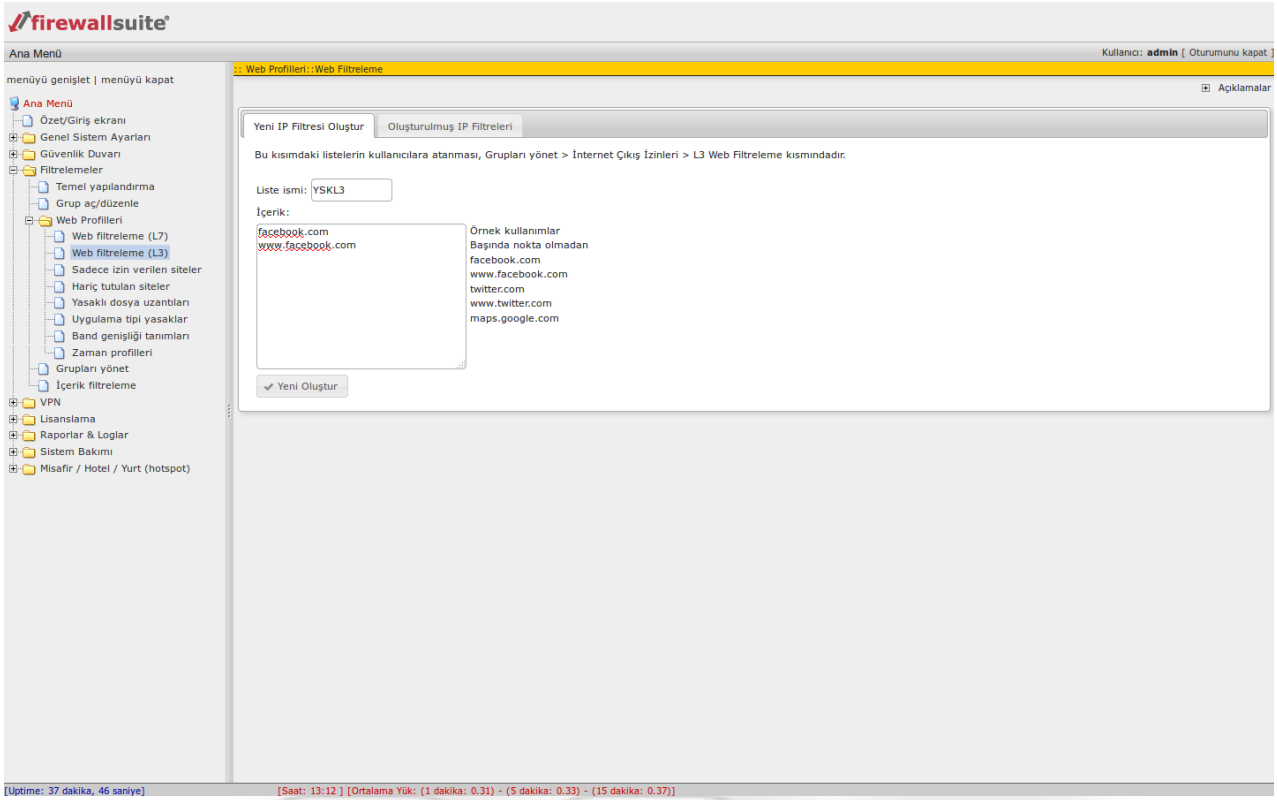
Grupları yönet > Domain / URL / Kelime Filtreleme kısmından tanımlamış yasaklama aktif edilebilir.



L7 WEB filtreleme

Web Filtreleme (L3)

FirewallSuite® L3 seviyesinde filtreleme yetenekleri ile gelir. Transparan proxy teknolojileri, HTTPS paketlerine müdahale etmedikçe üzerinden geçen HTTPS paketlerinin içeriğine bakma yeteneğine sahip değildir. FirewallSuite® bu paketlerin içeriğine bakmaksızın bu paketleri kaynağından kesebilir. Örnek olarak https://www.facebook.com/ adresi durdurulmak istendiğinde HTTPS doğası gereği L7 filtre ile durdurulamamaktadır. Böyle bir durum da yeni bir L3 filtresi oluşturularak bu filtrenin içine değer olarak facebook.com ve www.facebook.com dibi değerler eklenir. Bu sistem ile HTTPS teknolojisine sahip sayfalar durdurulur. Bu engelleme işleminde kullanıcıların karşınıza herhangi bir engelleme bildirimi gelmez.



L3 WEB filtreleme

Grupları yönet > İnternet Çıkış İzinleri > L3 Web Filtreleme kısmından tanımlanan yasak aktif edilebilir.

Sadece İzin Verilen Siteler

FirewallSuite® ile istenilen bir grubun yalnızca izin verilmiş internet sitelerine erişimi sağlanabilir. Örnek olarak bir MUHASEBE grubu oluşturulduğunda bu grubun yalnızca belirli banka ve devlet sitelerine gitmesi sağlanabilir. Bunun için ilgili kısımda bir liste açılarak gidilmesine izin verilen siteler yazılır.

Grup yasaklamalarından farklı olarak ***Grupları yönet*** kısımında ilgili grup seçilerek ***İnternet Çıkış İzinleri*** sekmesinde yer alan ***Bu grup için tüm internet servislerine izin ver*** onay kutusu işaretlenmez ve buna karşılık aynı yerde bulunan ***Sadece İzin Verilen siteler*** sekmesine gelinerek oluşturulmuş listenin gruba uygulanması sağlanır.

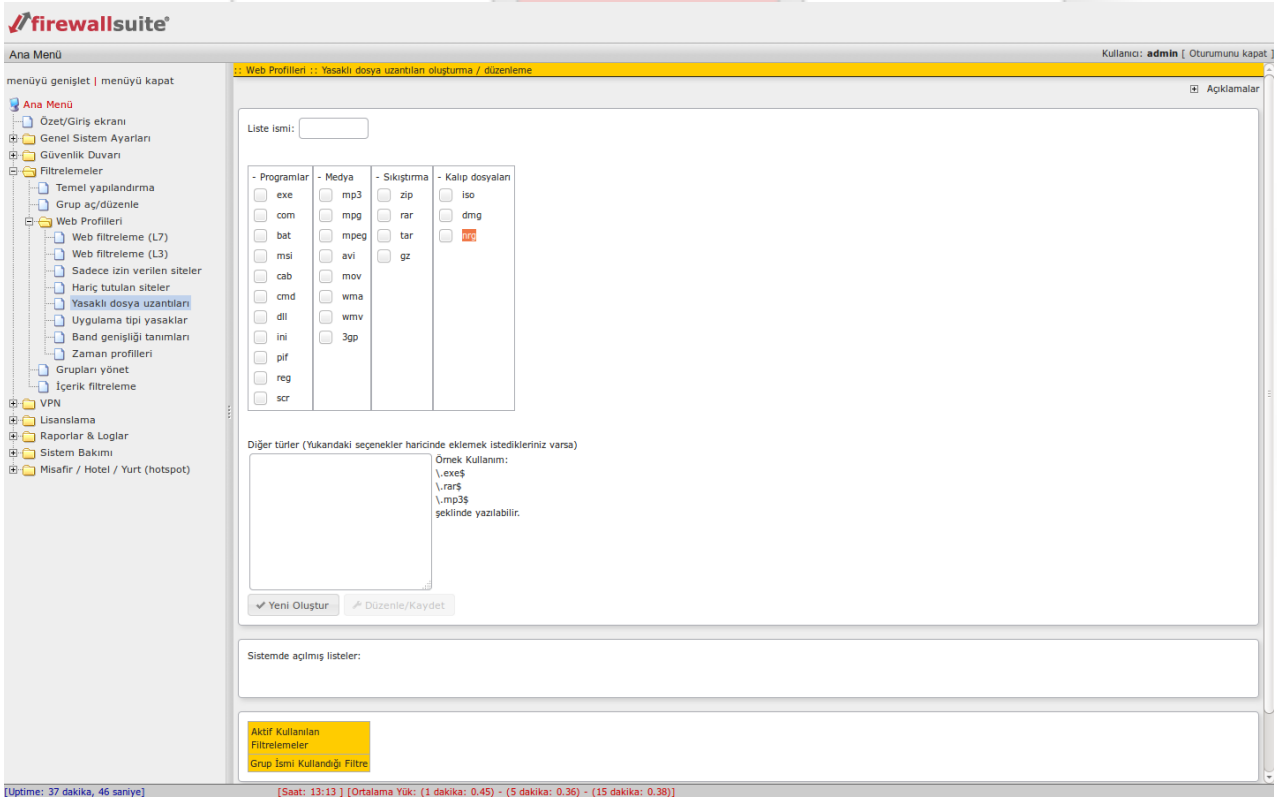
İlgili grup yalnızca izin verilen sitelere erişebilir. Bu yüzden varsayılan değer olarak elektronik posta gibi hizmetlerden yararlanamaz. Sadece izin verilen

sitelerle birlikte elektronik posta gibi hizmetlerin açılması için ***Grupları yönet*** kısmında ilgili grup seçilerek ***İnternet Çıkış İzinleri*** sekmesinde yer alan ilgili hizmetlere ait protokollerin onay kutuları işaretlenir. Bu sayede, yalnızca istenilen sitelere gidebilen ve istenilen protokollere erişen kısıtlı bir grup elde edilmiş olur.

Hariç Tutulan Siteler

Genellikle isteyerek yapılan bir yasaklama, yasaklanması istenmeyen bazı yan etkiler doğurabilir. Örnek olarak yapılan bir yasaklamanın istemciler üzerinde çeşitli antivirüs ya da güncelleme servisleri engellemesi söz konusu olabilir. Bu tip durumlarda hizmetin alındığı domainlerin yasaklardan hariç tutulması sağlanabilir. ***Hariç tutulan siteler*** bölümünde oluşturulan bir listeye (örneğin update.avira.com ya da update.microsoft.com gibi) gerekli domainler eklenerek ilgili işletim sistemleri ya da özel yazılımların güncelleme servislerinin çalışması sağlanabilir.

Yasaklı Dosya Uzantıları

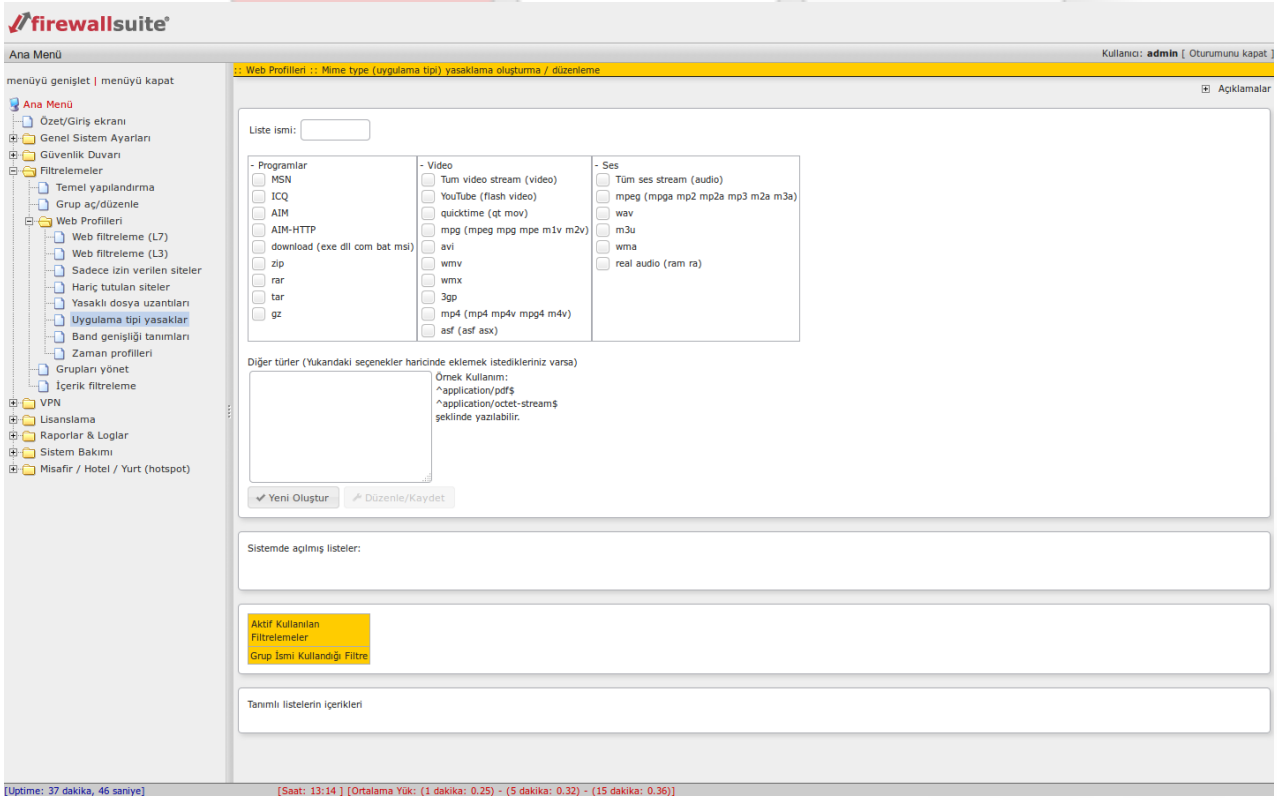


Yasaklı dosya uzantıları

Bu kısımda HTTP üzerinden indirilmesini istemediğiniz dosya uzantılarını belirleyebilirsiniz. Bu sistem yalnızca istenmeyen dosya uzantılarını engellemekle kalmaz. İstenen dosya uzantılarında bir indirme kotası belirlenebilir ve bu dosya türleri için belli bir dosya boyutundan yukarı indirme yapılması engellenebilir.

Liste ismi olarak bir isim belirlenmeli ve işlem yapılacak dosya türlerine ait onay kutuları seçilerek ***Yeni Oluştur*** düğmesine basılmalıdır. Eğer istenilen dosya türü onay kutuları içerisinde yoksa örnek olarak .img uzantılı dosya için ***\.img$*** değeri elle girilmelidir. Bu şekilde istenilen uzantılar elle girilebilir.

Uygulama Tipi Yasaklar

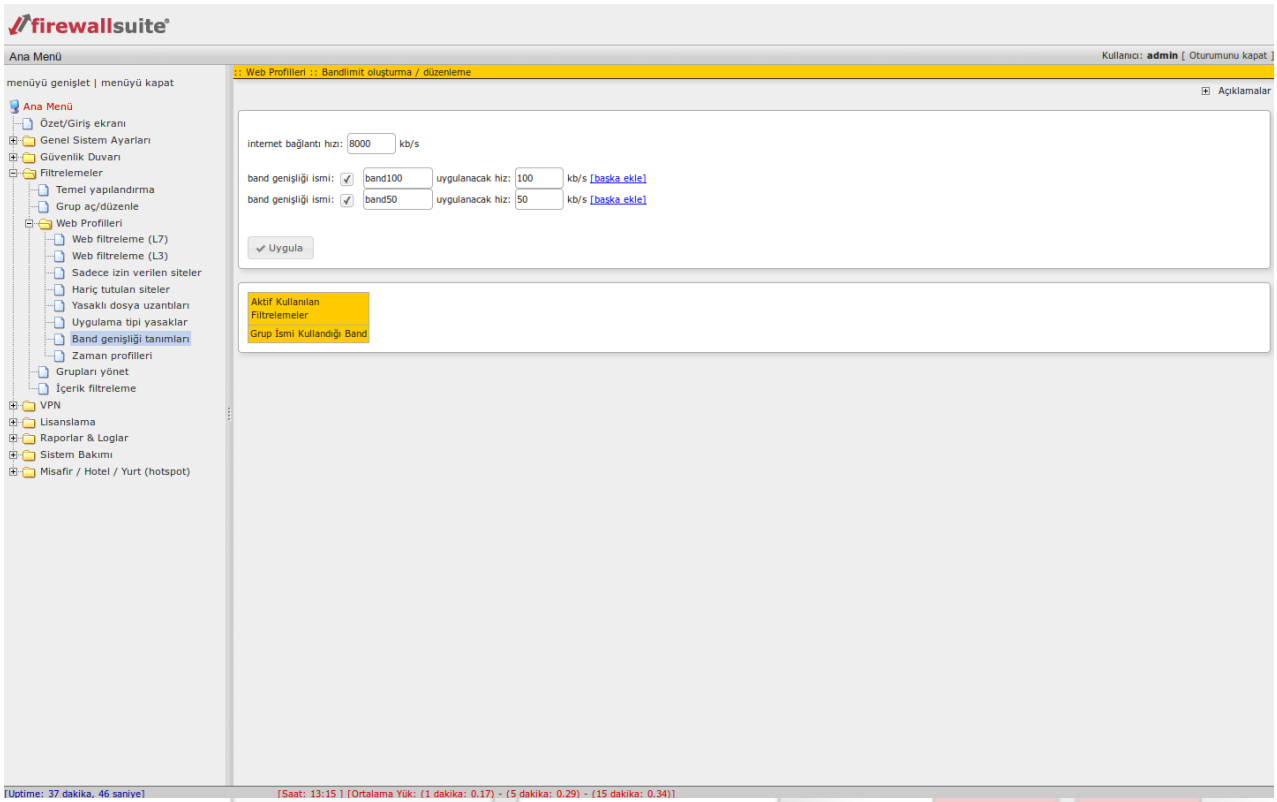


Uygulama tipi yasaklar

FirewallSuite® HTTP tabanlı uygulama tiplerine göre yasaklama özelliği içerir. Örnek olarak ilgili HTTP sitelerinin yasaklanmayıp içerisindeki video akış uygulamasının yasaklanması sayılabilir. Böyle bir işlem için ilk olarak bir liste ismi tanımlanmalıdır. Sonrasında ilgili menüde yer alan ***Video*** başlığı altındaki türlerden istenilenler seçilerek ***Yeni Oluştur*** düğmesine basılmalıdır. Eğer istenilen uygulama türü onay kutuları içerisinde yoksa örnek olarak .pdf gibi

bunun için ***^application/pdf$*** değeri elle girilmelidir. Bu şekilde istenilen uzantılar elle girilebilir.

Band Genişliği Tanımlamaları

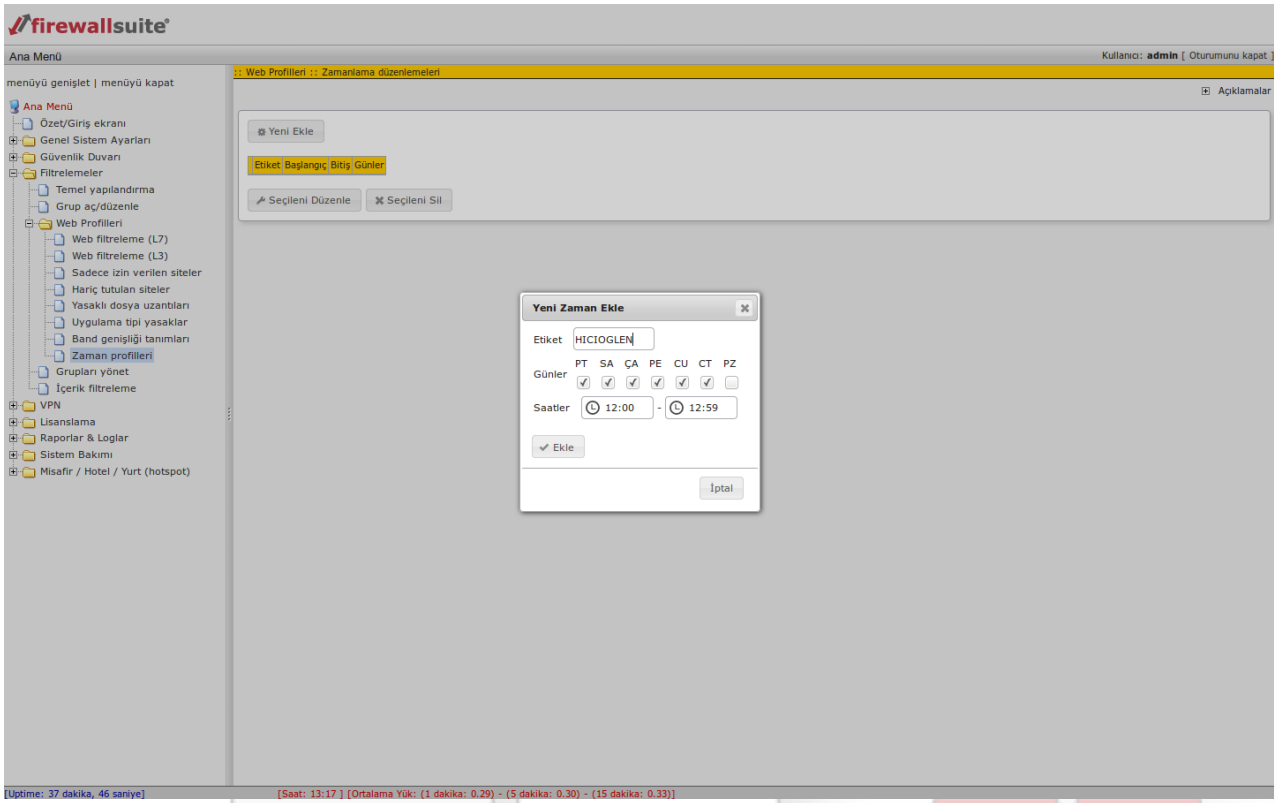


Band genişliği tanımlamaları

İstenildiğinde gruplara band genişliği tanımlaması yapılabilir. Bunun için ilk olarak ***internet bağlantı hızı: kb/s*** kutusuna toplam internet hızınızı kb/s cinsinden yazmanız gereklidir. Sonrasında ise örnek olarak 50kb/s band genişliği tanımını yapmak için ***band genişliği ismi:*** onay kutusunu işaretleyerek, BND50 gibi bir tanımlama ismi giriniz ve ***uygulanacak hız:*** değeri olarak ***50*** değerini yazınız.

Bu tanımlamaları yaparken ayarlamış olduğunuz 50 değerini birden fazla gruba uygulayabildiğiniz gibi toplam beş farklı band genişliği tanımı da yapabilirsiniz.

Zaman Profilleri



Zaman profilleri

FirewallSuite® ile çeşitli filtrelemeler ve yasaklamalar yapılmasına karşın bazı durumlarda kurum politikası gereği bazı grupların öğlen 12.00-12.59 arasında yapılan yasaklamalardan muaf tutulması istenebilir. Örnek olarak www.facebook.com erişimi, kurumunuz politikası gereği yasaklanmışken öğle arasında bir saatliğine açılması istenebilir. Örnek uygulama için ***Zaman Profilleri*** menüsünden ***Yeni Ekle*** düğmesine basınız. Karşınıza gelen ***Yeni Zaman Ekle*** diyalog kutusu içinde ***Etiket*** bir tanımlama **Serbest** gibi isim giriniz. ***Günler*** kısmında kurumun çalışma günlerine göre yasaklama yapılacak günlerin onay kutularını işaretleyiniz. ***Saatler*** kısmında da 12:00 ve 12:59 saatlerini seçiniz ve ***Ekle*** düğmesine basınız.

Bu şekilde yapılan farklı zaman tanımlamalarında belirlenmiş bir sınır bulunmamasına karşılık yapılmış bir yasaklama için yedi farklı serbest saat dilimi tanımlanabilir.

Yapılan bu serbest saat tanımlamalarını, yasaklamaları bulunan ilgili gruplarda etkinleştirmeniz gerekmektedir. Bunu yaptığınız yasaklamaya göre iki farklı yerde uygulamanız gerekebilir. Bunlardan ilki

Filtrelemeler > Grupları Yönet bölümünden işlem yapmak istediğiniz grubu seçip, o gruba ait ***Domain / URL / Kelime Filtreleme*** sekmesinde önceden tanımlamış olduğunuz saat dilimini seçmektir.

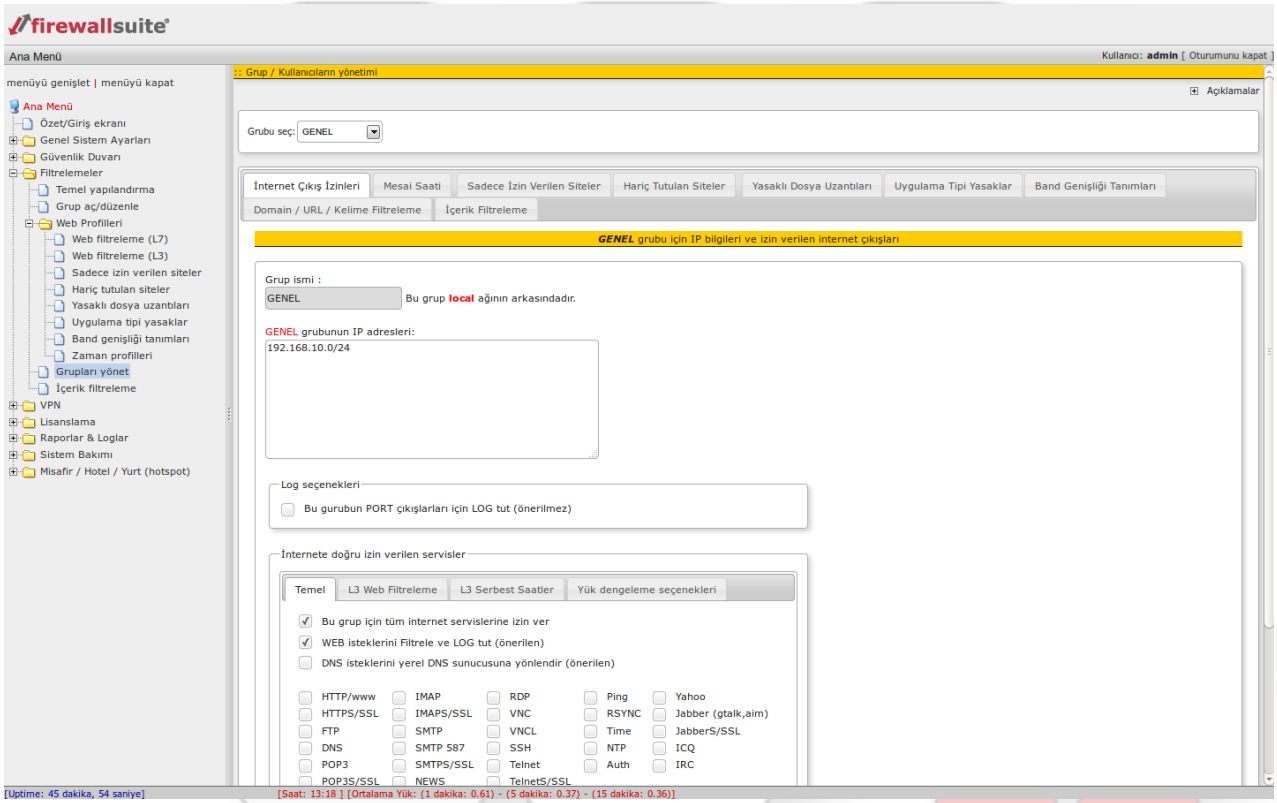
İkincisi ise

Filtrelemeler > Grupları Yönet bölümünden işlem yapmak istediğiniz grubu seçip, ***Temel*** sekmesinin alt kısmında yer alan L3 Serbest Saatler menüsünden önceden tanımlamış olduğunuz saat dilimini seçmektir.

✦ Tüm yasaklama sistemlerinin haricinde MAC ID'lerine göre yasaklı bir MAC grubu oluşturmak için **YSKMACGRB** isimli bir MAC ID grup oluşturunuz ve internet erişimi almasını istemediğiniz MAC ID adreslerini bu gruba ekleyiniz.

Grupları Yönet

Grupların açılması ve yasaklamaların belirlenmesinden sonra yapılacak son işlem, bu yasakların istenen gruplara atanması işlemidir. Bu işlem ***Grupları Yönet*** kısmından yapılır. Bu şekilde oluşturulmuş farklı yasaklamaların çapraz olarak gruplara tanımlanması sağlanarak esnek ve pratik bir yapı ile sunulur.



Grupları yönet

Grupları Yönet kısmına geldiğinizde yapılacak olan ilk işlem istisnasız olarak Grup seçme işlemidir. İlk olarak işlem yapılacak olan Grup üst kısımdaki ***Grubu seç:***

açılan kutusundan seçilir. Bundan sonra yapılan işlemler, ilgili grup seçilmişken alt kısmında yer alan sekmelerden yapılır.

İnternet Çıkış İzinleri

Açılmış olan gruplara ilişkin temel ayarların yapıldığı kısım burasıdır. İnternetin verilip verilmeyeceği, verilecekse hangi protokollere izin verileceği gibi genel ayarlar bu kısımdan yapılır.

Örnek senaryo dışında kalan işlemlerden bahsetmek gerekirse, L3 Web Filtreleme için bir liste tanımlanmışsa bu menünün altında yer alan ***L3 Web Filtreleme*** kısmından aktif edilir. Ayrıca ***Zaman profilleri*** kısmında tanımlanmış bir **Serbest Saat** varsa yine alt kısımda yer alan **L3 Serbest Saatler** menüsündeki açılan kutulardan seçilerek ilgili gruba serbest saat uygulanabilir.

Mesai Saati

Kullanıcı grupları için mesai saati tanımlaması yapabilirsiniz. Örnek olarak cumartesi günü dahil olmak üzere saat 9:00-19:00 arasında bir zaman diliminde internet hizmeti sağlanır. Bu aralık dışında kalan saatlerde internet hizmetinin verilmemesi sağlanabilir.

Sadece İzin verilen siteler

FirewallSuite® istediğiniz bir gruba sadece izin verdiğiniz bir site ya da belli başlı bir kaç siteye internet erişimi yapılmasını sağlar.

Bu işlem için öncelikle

Ana Menü > ***Filtrelemeler*** > ***Web Profilleri*** > ***Sadece izin verilen siteler***

menüsünde izin verdiğiniz site veya sitelerin tanımını yaptığınız bir listeyi oluşturmanız gerekmektedir. Bu işlemden sonra

Ana Menü > ***Filtrelemeler*** > ***Grupları Yönet***

menüsüne gelip, işlem yapmak istediğiniz grubu seçiniz. ***İnternet Çıkış İzinleri*** menüsünde

Bu grup için tüm internet servislerine izin ver seçeneğini işaretlemeden

WEB isteklerini Filtrele ve LOG tut (önerilen) seçeneğini işaretleyiniz.

DNS isteklerini yerel DNS sunucusuna yönlendir (önerilen) seçeneği isteğe ve yapılandırmaya bağlı olarak işaretlenebilir.

Normal şartlar altında bu işlem ile ilgili gruptaki kullanıcılar tanımlanmış HTML sayfalarına erişim sağlayabilirler fakat bu internet hizmetine tam anlamıyla sahip oldukları anlamına gelmez. Kullanıcı e-posta hizmeti gibi işlemler için de alt kısımda gerekli onay kutuları işaretlenebileceği gibi alt kısıma ihtiyaç duyulan TCP ve UDP portlar yazılabilir.

Hariç tutulan siteler

Yapılmış olan yasaklamalar neticesinde bazı sitelere erişim engellendiği gibi bazı sitelerden bazı dosya uzantılarını indirmekte engellenmiş olabilir. Ancak bazı sitelerin bu yasaklamaların dışında tutulması gerekebilir.

Bu menü ile ilgili yasaklamayı kaldırmadan istenilen sitelere özel olarak erişim hizmeti açılabilir. Oluşturulmuş olan hariç tutulacak site listesi bu kısımda istenilen gruplara eklenebilir.

Yasaklı Dosya Uzantıları

FirewallSuite® istemediğiniz dosya uzantılarının Web erişimini yasaklayabilir veya indirme kotası koyma imkanı sağlar. Yapılmış olan yasaklı ya da indirme kotalı dosya uzantısı listeleri bu kısımdan istenilen gruba eklenebilir.

Uygulama Tipi Yasaklar

FirewallSuite® video, ses vb. uygulamaları engelleyebilir. Bu tip uygulamalar için hazırlanmış listelerin gruba eklenmesi işlemi bu kısımdan yapılır.

Band Genişliği Tanımlamaları

Bir grup içindeki kullanıcılar için band genişliği tanımı yapılabilir. Bu tanım ile kullanıcının belirlenmiş bir hızda HTTP erişimleri yapması sağlanır. FirewallSuite® ile 5 farklı band genişliği tanımı yapılabilirken bu band genişliği tanımlamaları istenilen tüm gruplara uygulanabilir.

Domain /URL / Kelime Filtreleme

Bu kısımda birden fazla yasaklama yöntemi bir arada bulunur. Bunlar sistem tarafından kategorilere göre tanımlanmış otomatik kara listeler, kullanıcı tanımlı kara listeler olarak iki ana başlıkta incelenebilir. Kullanıcı tanımlı kara listeler domain, URL, URL içi kelime tanımı olarak üç başlıkta değerlendirilebilir.

Kullanıcı Tanımlı Domain Tarama menüsünde, kullanıcının kendi oluşturduğu yasaklı domain listeleri ilgili gruba uygulanabilir.

Kullanıcı Tanımlı URL Tarama menüsünde, kullanıcının kendi oluşturduğu yasaklı URL listeleri ilgili gruba uygulanabilir.

Sistem Tanımlı Domain Tarama menüsünde, sistem tarafından önceden eklenmiş yasaklı domain listeleri ilgili gruba uygulanabilir. Bu listeler belli kategorilere göre gruplanmıştır.

URL içi Kelime Tarama menüsünde, kullanıcının kendi oluşturduğu yasaklı

kelime listeleri ilgili gruba uygulanabilir.

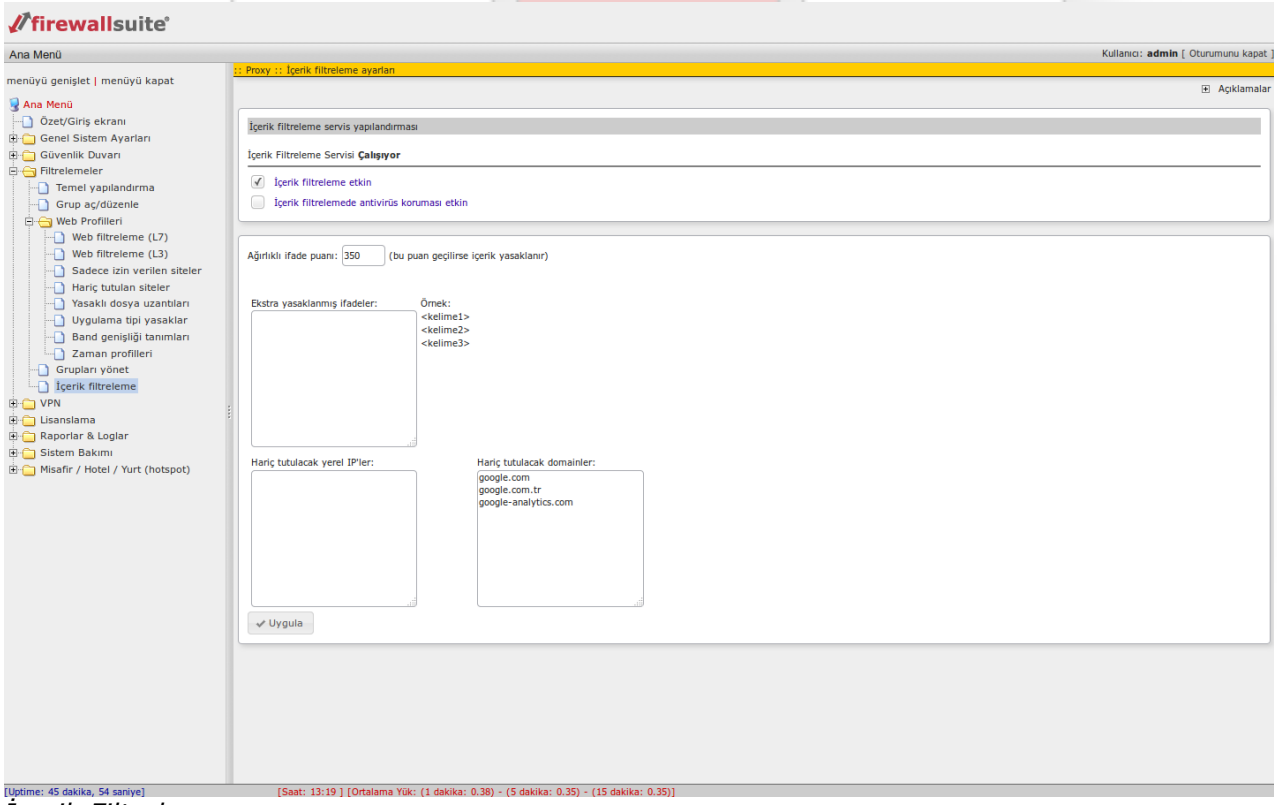
Bu uygulama işlemi, ilgili liste önündeki onay kutusunun işaretlenmesi ile uygulanır. Bu kısımdaki en önemli özelliklerden biri

Ana Menü > ***Filtrelemeler*** > ***Web Profilleri > Zaman Profilleri***

menüsünde tanımlanmış olan zaman profilleri ile bu kısımda yer alan 7 farklı serbest zaman profili içinde seçilebilir durumdadır. Bu serbest zaman profili ile yapılan yasaklamaların belirli bir zaman aralığında devre dışı kalması sağlanabilir.

İçerik Filtreleme

İçerik filtreleme sistemi tüm yasaklamalardan bağımsız olarak ayarlanmış hassasiyet derecesine ve internet sayfalarının uygunsuzluk değerine göre puanlama yaparak yasaklamaya karar veren yapay zeka sistemidir.



İçerik Filtreleme

Ana Menü > ***Filtrelemeler*** > ***İçerik Filtreleme***

menüsünden temel aktivasyon yapıldıktan sonra grupların yönetimi menüsünden ilgili grup seçilerek uygulama yapılabilir. Temel aktivasyon menüsünde hassasiyet, hassasiyet gösterilecek özel kelimeler gibi tanımlar yapılabilir.

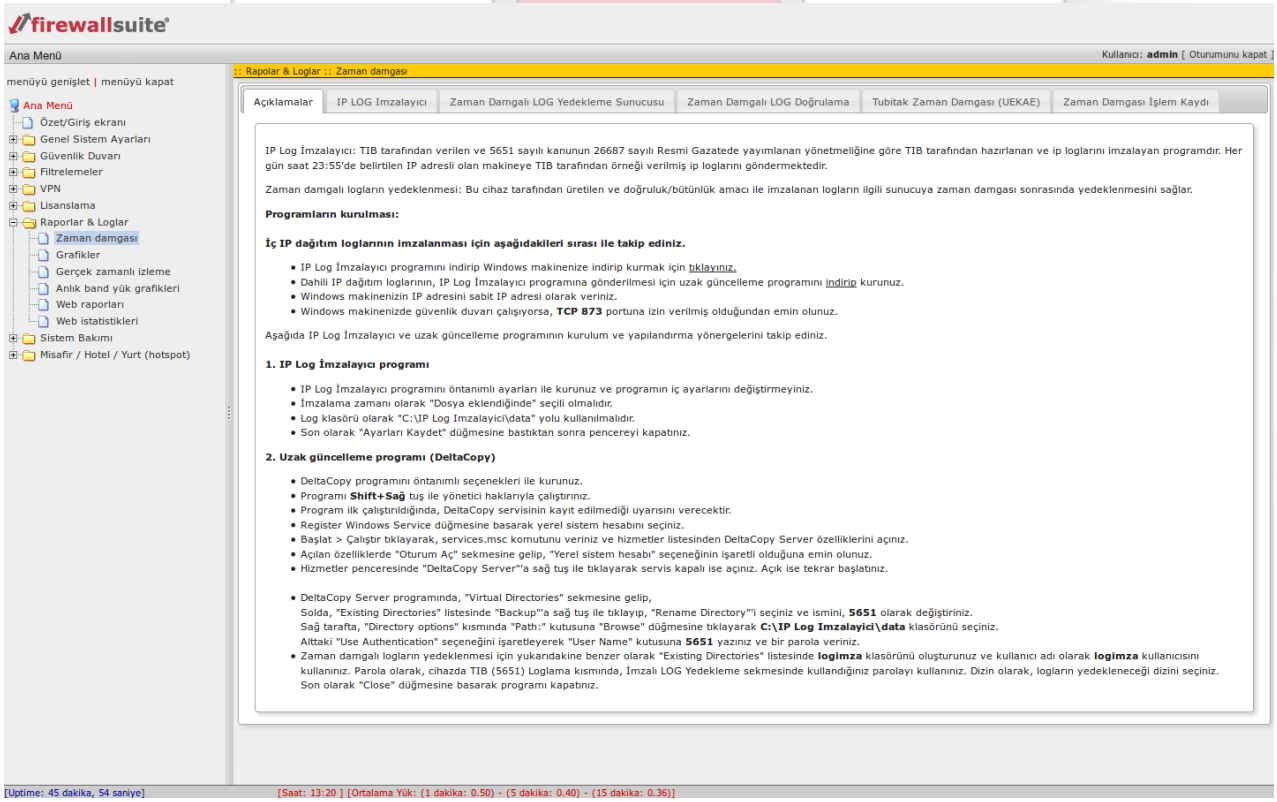
İçerik filtrelemeden etkilenen yasaklamalarda, etkilenmemesi istenen yerel IP adresleri ya da dış domainler yine içerik filtreleme temel aktivasyon menüsünden belirlenebilir. Böylelikle içerik filtreleme aktif olsa bile istenilen dış domainler ya da yerel Host IP adresleri bu yasaklamaların dışında tutulabilir.

Raporlar & Loglar

FirewallSuite® dahili LOG analiz desteği ile gelir. Kullanıcıların tüm HTTP işlemlerinin LOG'u tutulabilir. Tutulan bu LOG'lar çeşitli kriterlere göre süzdürülebilir ve LOG'lar grafik istatistikleri ile desteklenir.

Ayrıca T.İ.B. (Telekomünikasyon İletişim Başkanlığı) tarafından üretilen IP LOG İmzalayıcı program ile uyumlu olarak çalışabilmektedir. T.İ.B. tarafından örneği sunulan iç IP dağıtım LOG'larına göre çıktı üretebilir ve bu LOG'ları IP LOG İmzalayıcı programın yüklü olduğu bir sunucuya yönlendirir. IP LOG İmzalayıcı almış olduğu bu LOG'ları imzalayarak saklanmasını sağlar. Tüm bunlara ek olarak T.U.B.İ.T.A.K. (UEKAE) den temin edilen imzalarla da LOG'lar imzalanabilir. Ayrıca kendi içerisinde LOG'ları zaman damgası ile imzalayan standart bir sistem bulunmaktadır.

Zaman Damgası



Raporlar

Zaman Damgası ile LOG'ların imzalanması ve istenildiğinde bu LOG'ların dışarıdaki bir sunucuya gönderilmesi ile ilgili işlemler bu menüden yapılır.

Açıklamalar

Yapılabilecek işlemlere ait açıklamaların ve bunların nasıl yapılacağına dair bilgilerin bulunduğu sekmedir.

IP LOG İmzalayıcı

T.İ.B. tarafından sağlanan IP LOG İmzalayıcı programına yapılacak bağlantı bilgilerinin yazıldığı kısımdır.

Zaman Damgalı LOG Yedekleme Sunucusu

Zaman damgalı LOG'larınızı dışarıdaki bir noktaya yedeklemek istediğiniz de ilgili yedekleme sunucusuna ait erişim bilgilerini kaydettiğiniz bölümdür.

Zaman Damgalı LOG Doğrulama

Sistemin aldığı LOG'ların doğru bir şekilde zaman damgası uygulandığının kontrol edildiği bölümdür. Alınan LOG'lar, yapılan işlemlere göre kronolojik bir sırada üretilirler. İstenilen bir tarihe sadece tarih değerlerinin üzerine tıklanarak ulaşılabilir ve o tarihteki istenen dosyanın doğruluğu kontrol edilebildiği gibi dosya farklı kaydedilebilir.

Tubitak Zaman Damgası (UEKAE)

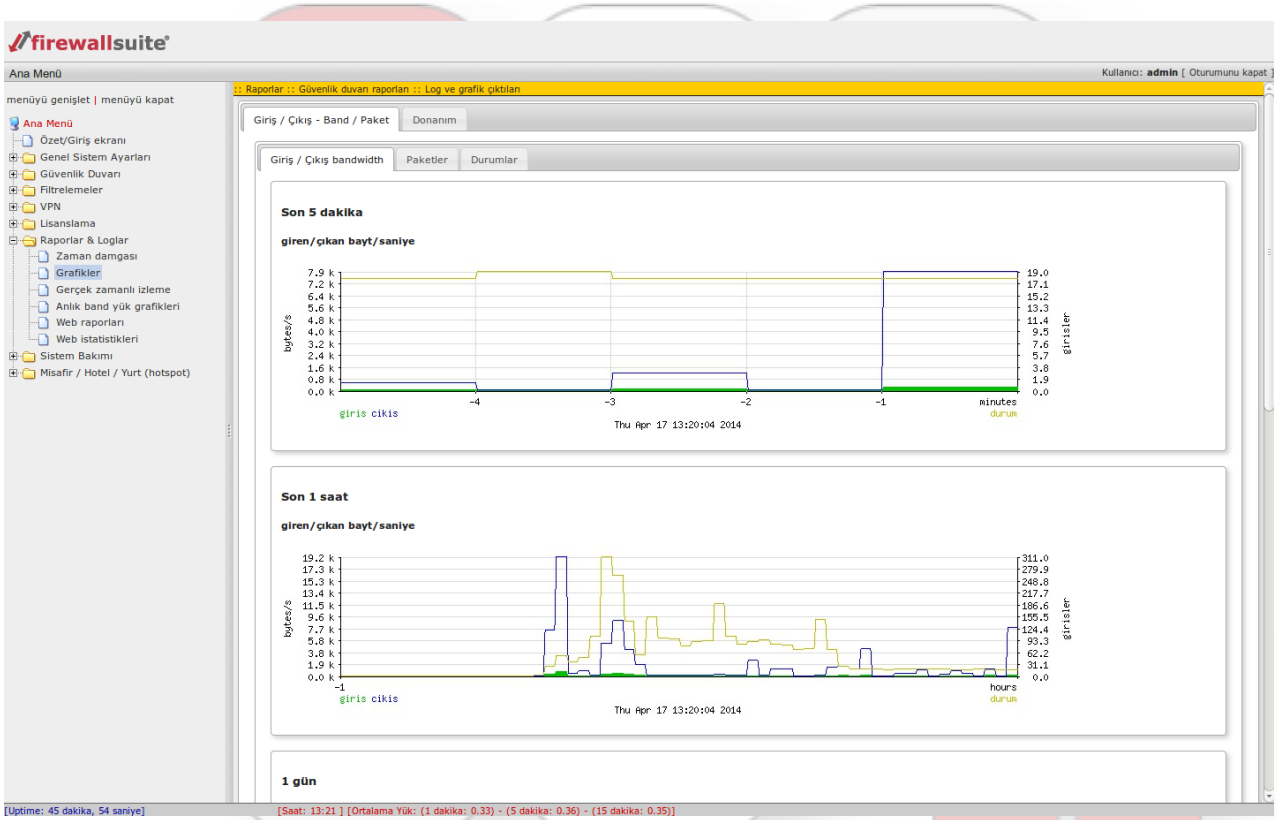
T.U.B.İ.T.A.K. (UEKAE) den temin edilen imzalara ilişkin erişim katlarının girildiği bölümdür. Bu kısma girilecek değerler ve erişim bilgileri T.U.B.İ.T.A.K. (UEKAE) tarafında sağlanır.

Zaman Damgası İşlem Kaydı

Tüm zaman damgalama işlemlerine ait işlem raporlarının tutulduğu kısımdır. Raporlar kronolojik ve tarih bilgisi ile tutulur.

Grafikler

FirewallSuite® sistem kaynaklarına ve kullanım verilerine ait gelişmiş grafik desteği sunar. Bu kısımda sistemin kullandığı işlemci gücü, bellek miktarı, disk doluluğu ve veri akışlarına ilişkin grafik değerlendirmeleri bulunur.



Garfik raporlar

Gerçek Zamanlı İzleme

Gerçek zamanlı izleme menüsünden sisteme ait LOG'lar ya da İçerik Filtreleme sistemine ait LOG'lar gerçek zamanlı olarak izlenebilir. Burada görüntülenecek LOG modülüne göre ekran tazeleme hızı ya da LOG satırı içinde belli bir ifadenin süzülmesi gibi ekstra özellikler bulunmaktadır.

Anlık Band Yükü Grafikleri

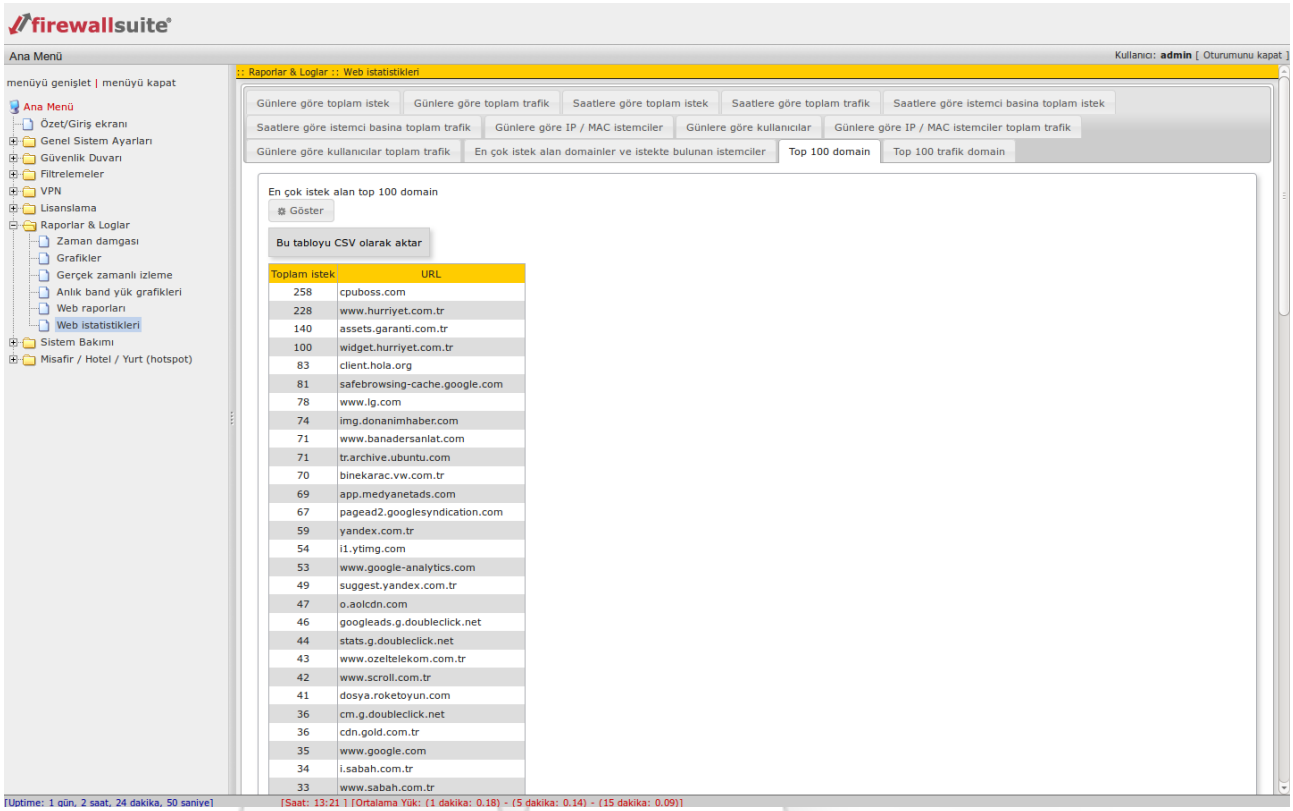
Sistem üzerindeki istemcilerin harcadıkları band yükünün anlık olarak izlenmesini sağlayan kısımdır. Bu kısımda sistemde kurulu ağlar listelenir. İlk olarak izlemek istediğiniz ağ üzerine tıklamanız gerekir. Sonra da alt kısımda listelenen IP adreslerinden herhangi birinin üzerine tıklayarak kullandığı band yükünü grafiksel olarak görebilirisiniz.

Web Raporları

Guplar menüsünde LOG tutulması için gerekli ayarlamalar yapıldıysa, ilgili kullanıcıların HTTP hareketlerinin LOG'landığı ve sistemde saklandığı kısımdır. Bu kısım kayıtlı verilere anlık olarak ulaşma imkanı sağlanır. Ayrıca belli bir tarih arasında LOG süzdürme işlemi yapılabilir. IP ya da MAC adreslerinin gitmiş olduğu domainler gibi çapraz sorgulamalar yapılabilir.

Yapılan sorgunun çıktı görüntüsü ***Bu tabloyu CSV olarak aktar*** düğmesinden dışarı alınabilir.

Web İstatistikleri



WEB istatistikleri

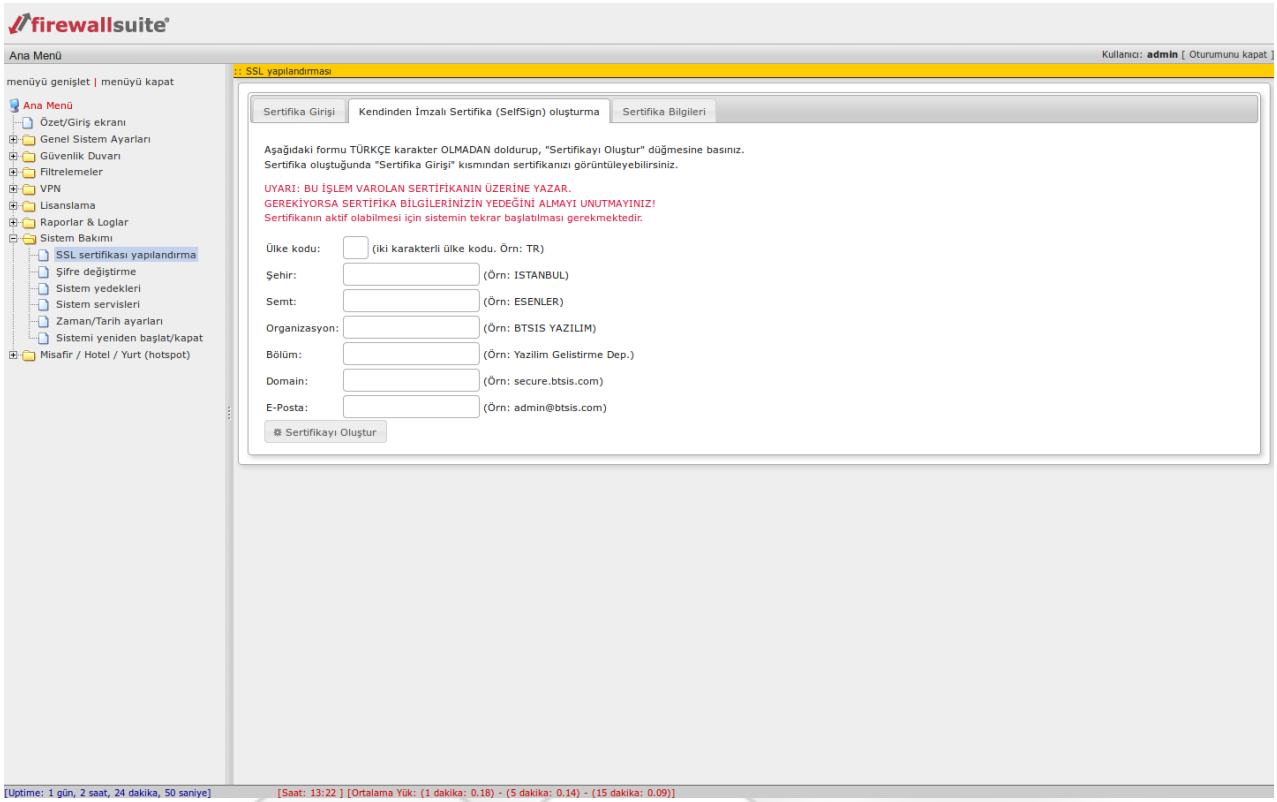
Bu kısımda tüm HTTP istatistikleri tutulur. Bu istatistikler içerisinde en çok istek gönderilen alan adları, en çok trafik yapılan alan adları gibi onüç farklı veri sunulur.

Sistem Bakımı

Sistem bakımına ilişkin tüm alt uygulamalar bu kısımda yer alır.

✦ FirewallSuite® sistem kapatma/yeniden başlatma işlemleri, doğrudan güç kaynağını kesmek yerine Sistem Bakımı bölümünden yapılmalıdır.

SSL Sertifikası Yapılandırılması

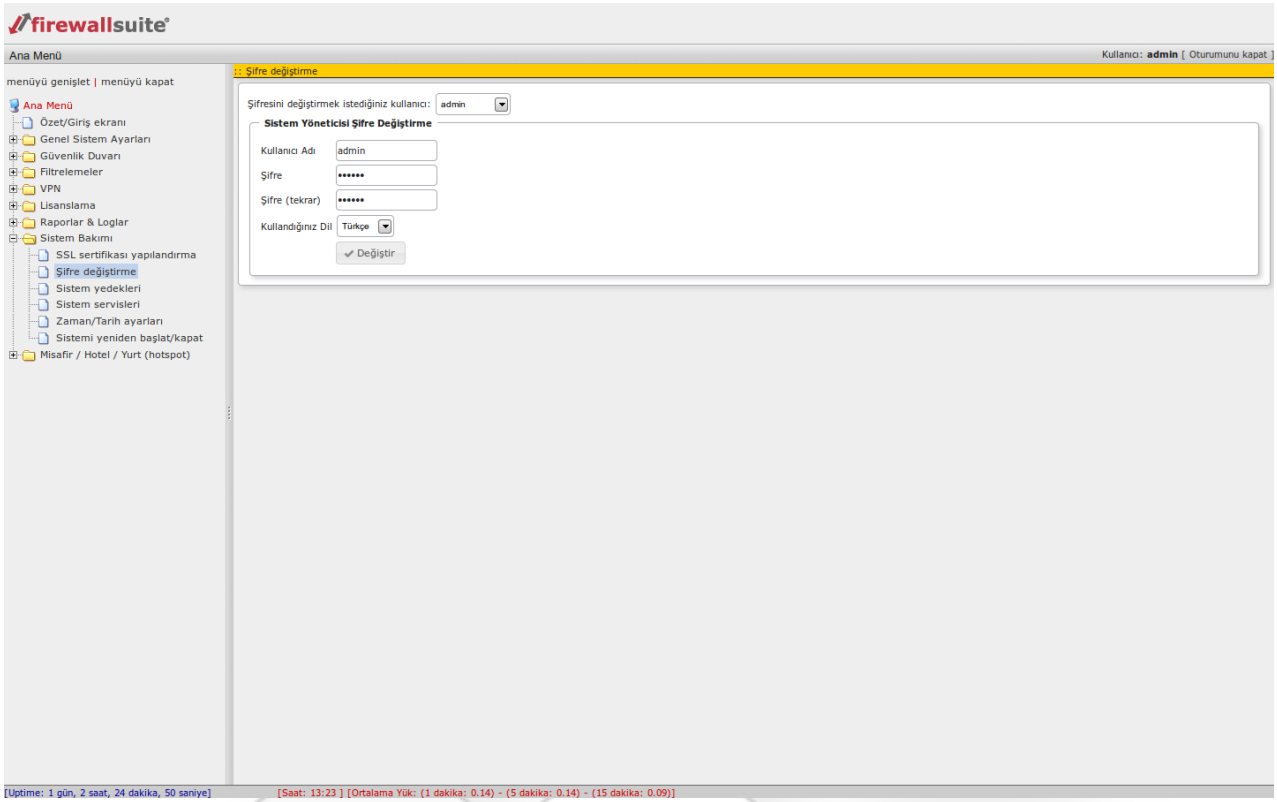


SSL yapılandırması

Yetkili otorite tarafından sağlanan SSL sertifikası yapılandırma işlemi bu kısımdan yapılır. **Kendinden İmzalı Sertifika (SelfSign) oluşturma** sekmesinden sertifika oluşturabilirsiniz. Bu sertifikanın CSR dosyası yardımıyla yetkili otoriteden imza alabileceğiniz gibi kendinden imzalı sertifika ile sistemi kullanabilirsiniz. Bu sertifika kullanım işlemi HotSpot internet paylaşım hizmetlerinde, kimlik doğrulaması için yerel ağdan iletilen bilgilerin SSL imzalı olarak taşınmasını ve üçüncü kişiler tarafından okunamamasını sağlamaktadır.

Eğer sertifikanız yetkili bir otorite tarafından imzalı değilse yine SSL sistemi çalışmasına karşın istemcilerin internet tarayıcı programlarında "bu site güvenli değil, devam etmek istiyor muzunuz?" gibi bir uyarı çıkabilir.

Şifre Değiştirme



Şifre Değiştirme

Bu kısımda FirewallSuite® paneline erişim şifrelerini değiştirebilirsiniz. Şifre değiştirebileceğiniz kullanıcılar;

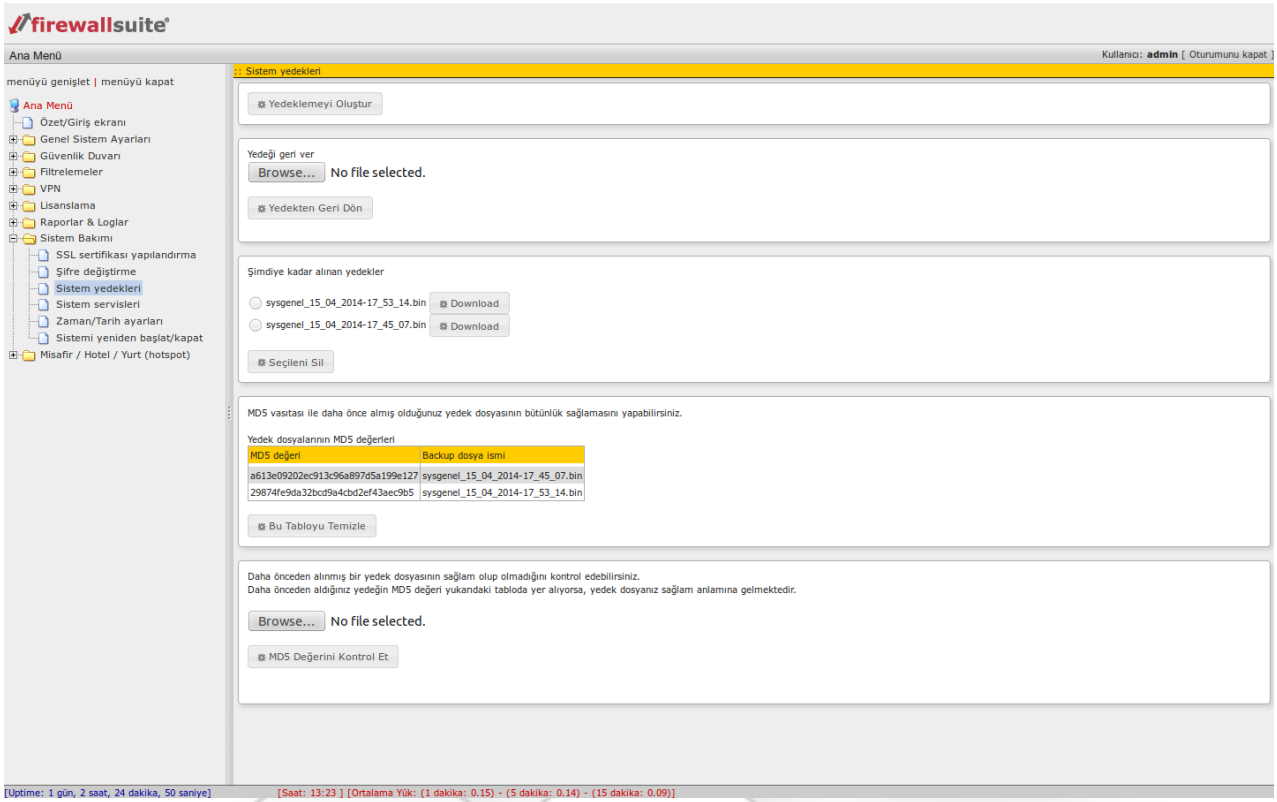
admin: Sistem Yöneticisi

lobi: Misafir interneti elle açabilen görevli kullanıcı

rapor: Yalnızca kullanıcıların HTTP erişimlerini görmekle yetkili olan kullanıcı

şeklindedir. Yalnızca **admin** kullanıcısının kullanıcı adı değişebilir.

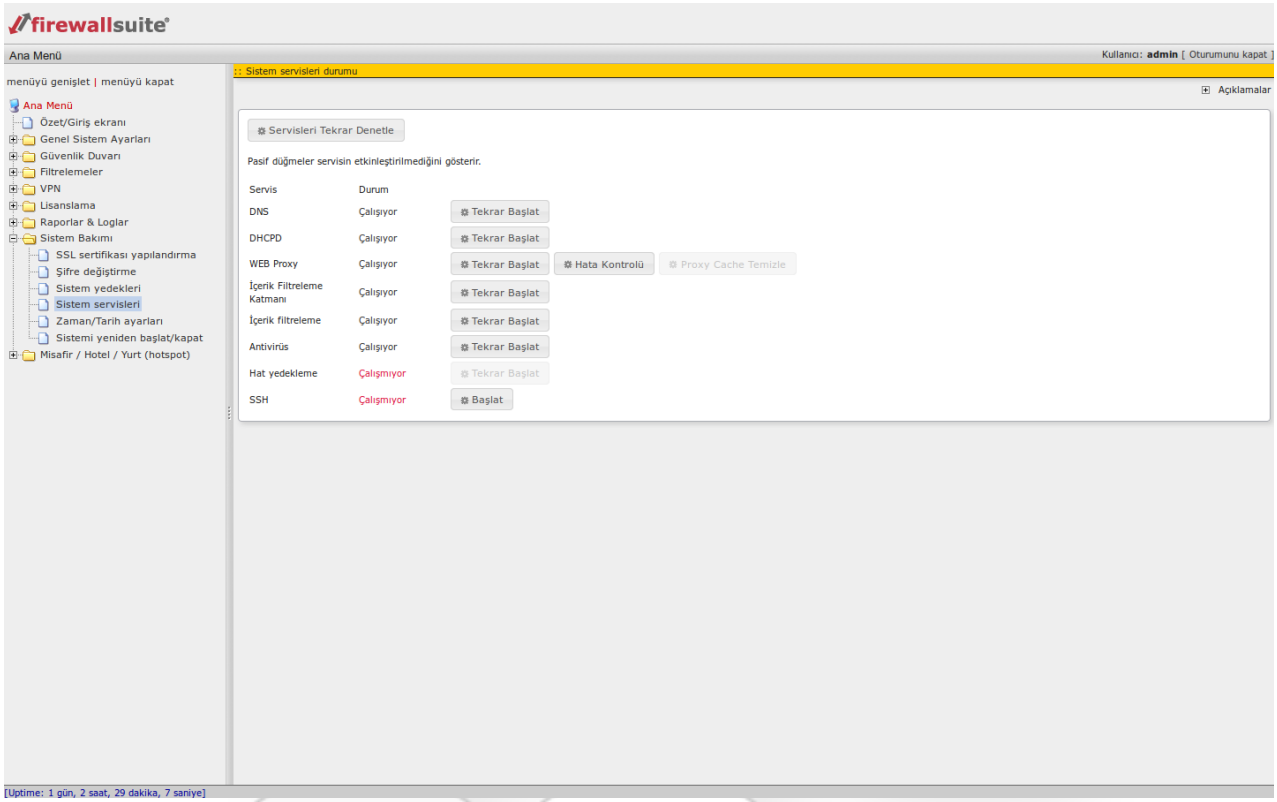
Sistem Yedekleri



Sistem Yedekleri

Çalışan sisteminizin ayar yedeklerini alabileceğiniz ve bu yedekleri tekrar geri yükleyebileceğiniz kısımdır. Yedekler geri yüklendikten sonra sistemi bir kere yeniden başlatmanız gerekir.

Sistem Servisleri



Sistem Servisleri

Çalışan sistem servislerinin izlenebildiği ve gerekli durumlarda yeniden başlatılabildiği kısımdır. Diğer servislerden farklı olarak Web Proxy menüsünde hata kontrolü ve ön bellek temizleme seçenekleri de bulunmaktadır.

Zaman/Tarih Ayarları

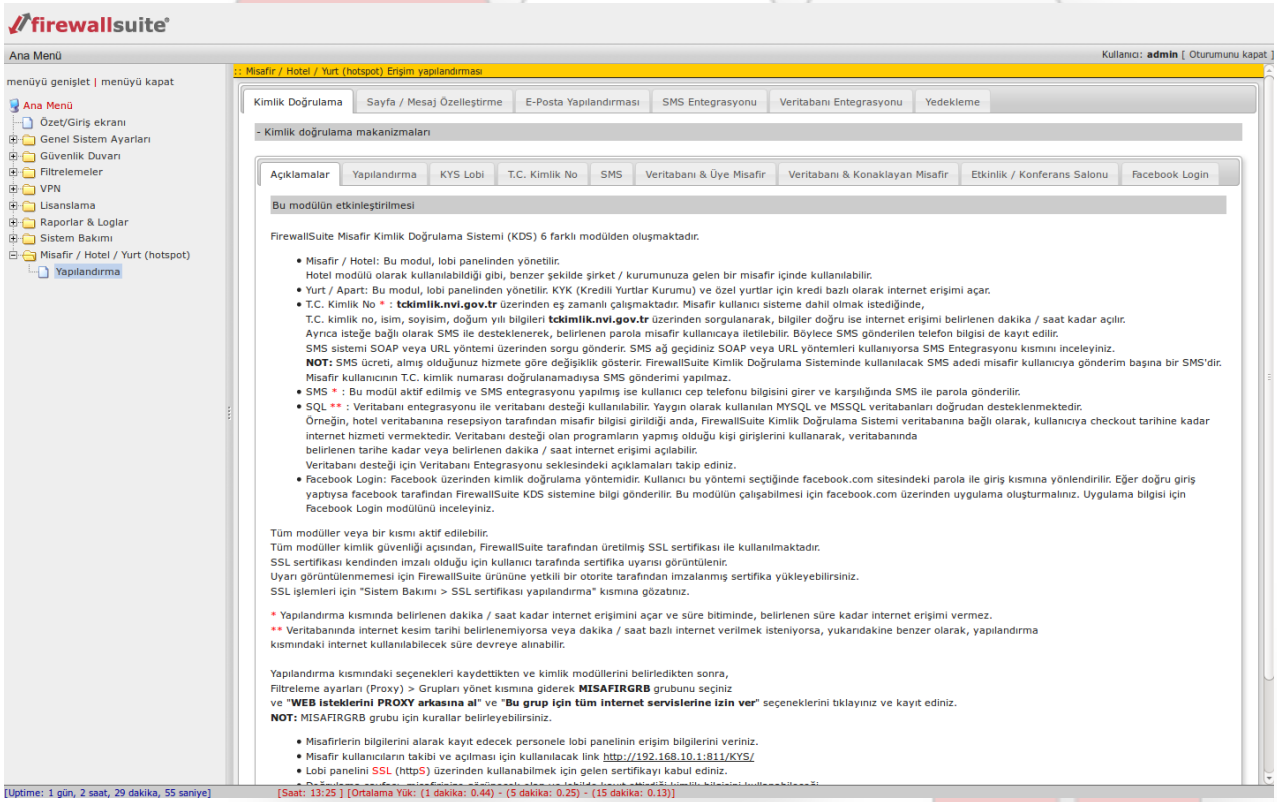
Adından da anlaşılacağı üzere sistemin tarih ve saat ayarının yapılabileceği kısımdır. Tarih ve saatin doğru olması özellikle LOG sistemi açısından çok önemlidir.

Sistemi Yeniden Başlat/Kapat

Sistemi güç kaynağından çekmeden önce kapatma işleminin yapılacağı kısımdır. Ayrıca gerekli hallerde sistemi yeniden başlatma işlemi de bu menüden yapılır.

Misafir / Hotel / Yurt (HotSpot)

Örnek senaryoda da değinildiği üzere misafir internet hizmeti ile ilgili yapılandırmaların tamamı bu kısımda yer alır. Birbirinden farklı HotSpot internet bağlantı seçenekleri düzenlenebilir. Bu seçeneklerden yalnızca biri tercih edilebileceği gibi birden fazla senaryo da bir arada kullanılabilir. Örnek olarak Facebook Login seçeneği ile T.C. Kimlik No doğrulaması seçeneği bir arada kullanılabilir.



HotSpot Yapılandırması

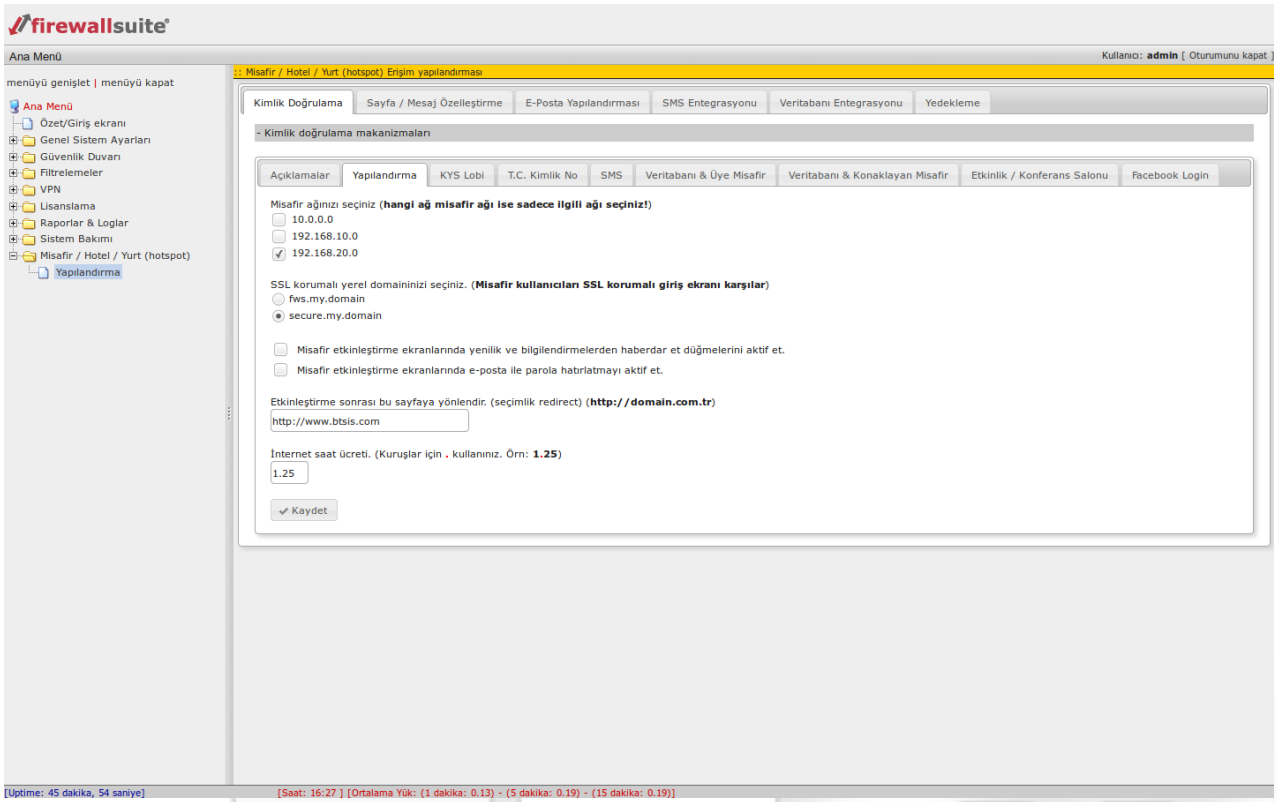
Kimlik Doğrulama

Tüm kimlik doğrulama mekanizmaları ile ilgili ayarlar bu kısımda yer alır. Birbirinden farklı doğrulama metotları olsa da tüm modüllerde internet erişim seçenekleri hemen hemen ortak özellikler içerir. Bunlar temelde doğrulama sonrası alınan şifrenin yaşam süresi, bir şifre ile bağlanabilecek eş zamanlı istemci sayısı, alınan bu internet hizmeti sona erdikten sonra ne kadar zaman internet hizmeti alınamayacağı gibi özelliklerdir.

Açıklamalar

Genel açıklamaların bulunduğu kısımdır. Yapılması istenen işlemlere ilişkin detaylı açıklamalar burada bulunur.

Yapılandırma



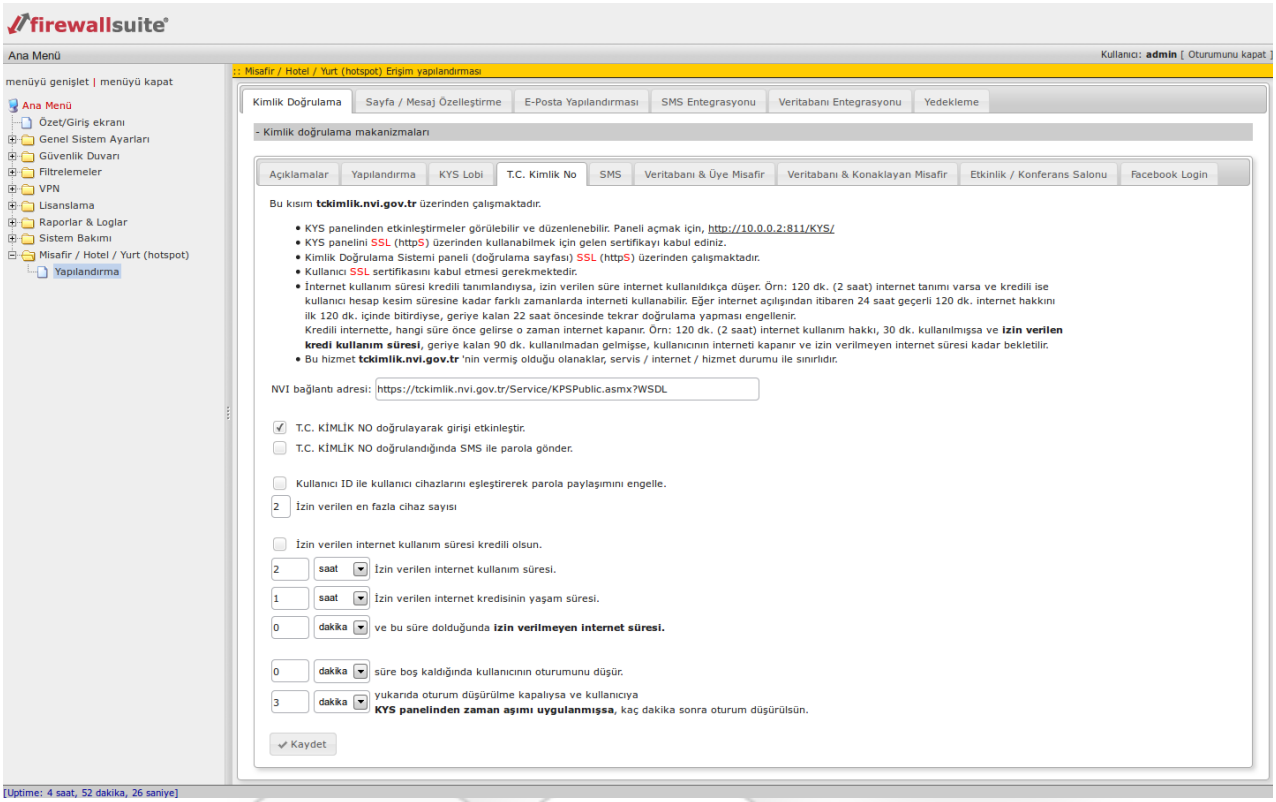
HotSpot temel yapılandırması

Bu bölümde HotSpot sisteminin aktivasyonu, hangi ağ kartında çalışacağı, hangi domain ismi üzerinden çalışacağı gibi genel ayarlar yer alır. HotSpot arayüzünün ağ kartı değiştirildiğinde ayarların buradan tekrar uygulanması gerekir.

KYS Lobi

Yetkili personelin şifre ile dağıtacağı internetin erişim seçeneklerini içerir. Diğer sistemler gibi otomatik bir sistem olmadığı için kullanıcının interneti ne kadar süre ile kullanacağı Lobide ki yetkili personel tarafından hizmet açılırken isteğe bağlı olarak belirlenebilir.

T.C. Kimlik No



HotSpot T.C. Kimlik No entegrasyonu

T.C. Kimlik No sorgusu ile internet erişimi bu kısımdan aktif edilir. Sistem https://tckimlik.nvi.gov.tr adresinden T.C. Kimlik No, ad, soyad ve doğum yılını sorgular. Bu bilgiler geçerli ise önceden tanımlanmış istemci sayısı ve süre kadar internet hizmeti sunabilir. Tanımlı erişim süresi bittiğinde kişiye önceden tanımlanmış süre kadar internet verilmemesi de yine bu kısımdan ayarlanır.

TC kimlik sorgusu ile internet erişimi için bir diğer önemli seçenek ise sistemin SMS hizmeti ile desteklenebilmesidir. Hizmeti sunan kurum, isterse şifre temini SMS üzerinden cep telefonuna göndererek de yapabilir. Bu hizmetin alınabilmesi için SMS servis sağlayıcısından SMS gönderim hakkı alınması ve sisteme bu haklar ile ilgili hesap ayarlarının girilmesi gereklidir.

SMS

SMS ile doğrulama seçeneklerinin yapıldığı kısımdır. Şifre gönderimi ile internet hizmeti sağlanması hizmetini içerir. T.C. Kimlik No sistemindeki tüm erişim seçenekleri bu kısımda da geçerlidir. Yine T.C. Kimlik No sisteminin SMS seçeneğindeki gibi SMS servis sağlayıcısından SMS gönderim hakkı alınması ve sisteme bu haklar ile ilgili hesap ayarlarının girilmesi gereklidir.

Veritabanı & Üye Misafir

Kullanıcıya ait herhangi bir dış veritabanı (MSSQL ve MySQL) entegrasyonu ile misafirlere önceden tanımlanmış süreli internet hizmeti sağlanmasını içerir. İnternet kesimi FirewallSuite® üzerinde önceden tanımlı bir değer olarak belirlenerek otomatik kesim sağlanabilir. Örnek olarak önceden tanımlanmış üyelik kartlarındaki ID'lere göre üyelere özel sınırlı süreli internet verilmesi sayılabilir.

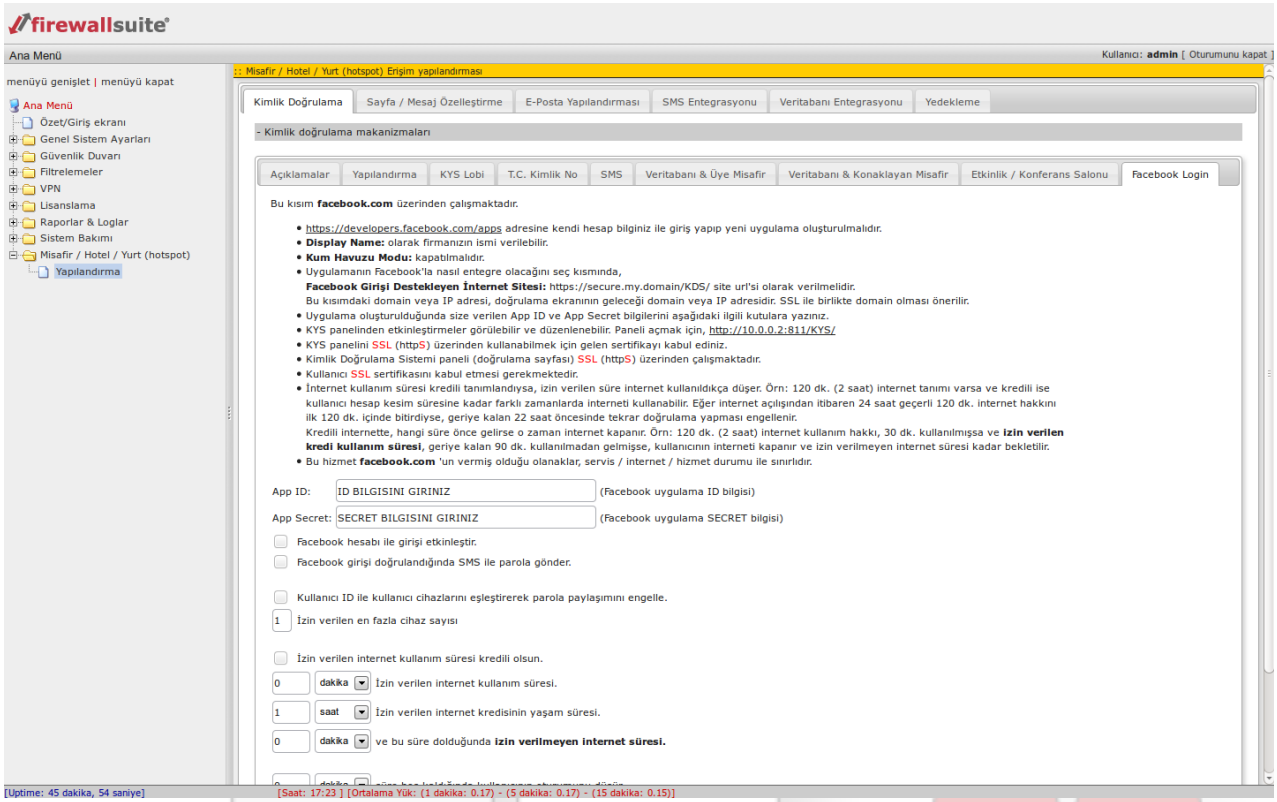
Veritabanı & Konaklayan Misafir

Kullanıcıya ait herhangi bir dış veritabanı (MSSQL ve MySQL) entegrasyonu ile misafirlerin erişim bilgilerine göre internet hizmeti sağlanması hizmetini içerir. Özellikle MSSQL ve MySQL veri tabanı kullanan otel müşteri takip programları ile otomatik olarak haberleşebilir. Veritabanı & Üye Misafir sisteminden farkı, internet kesimleri de dış veri tabanındaki kayıttan gelir. Örnek olarak otelden çıkan müşterinin hesap kesiminde otomatik olarak internet hizmetinin kesilmesi sayılabilir.

Etkinlik / Konferans Salonu

Konferans salonları için etkinlik kodu oluşturmaya yarar. Bu etkinlik kodu bir kere ayarlandığında önceden belirlenmiş zaman dilimlerinde otomatik olarak aktif olur ve sonlanır. Mevcut etkinlik kodu, ilgili konferans salonunda paylaşılarak sadece o salon içerisindekilerin bildiği bu kod ile konferans süresince internet hizmeti almaları sağlanabilir.

Facebook Login



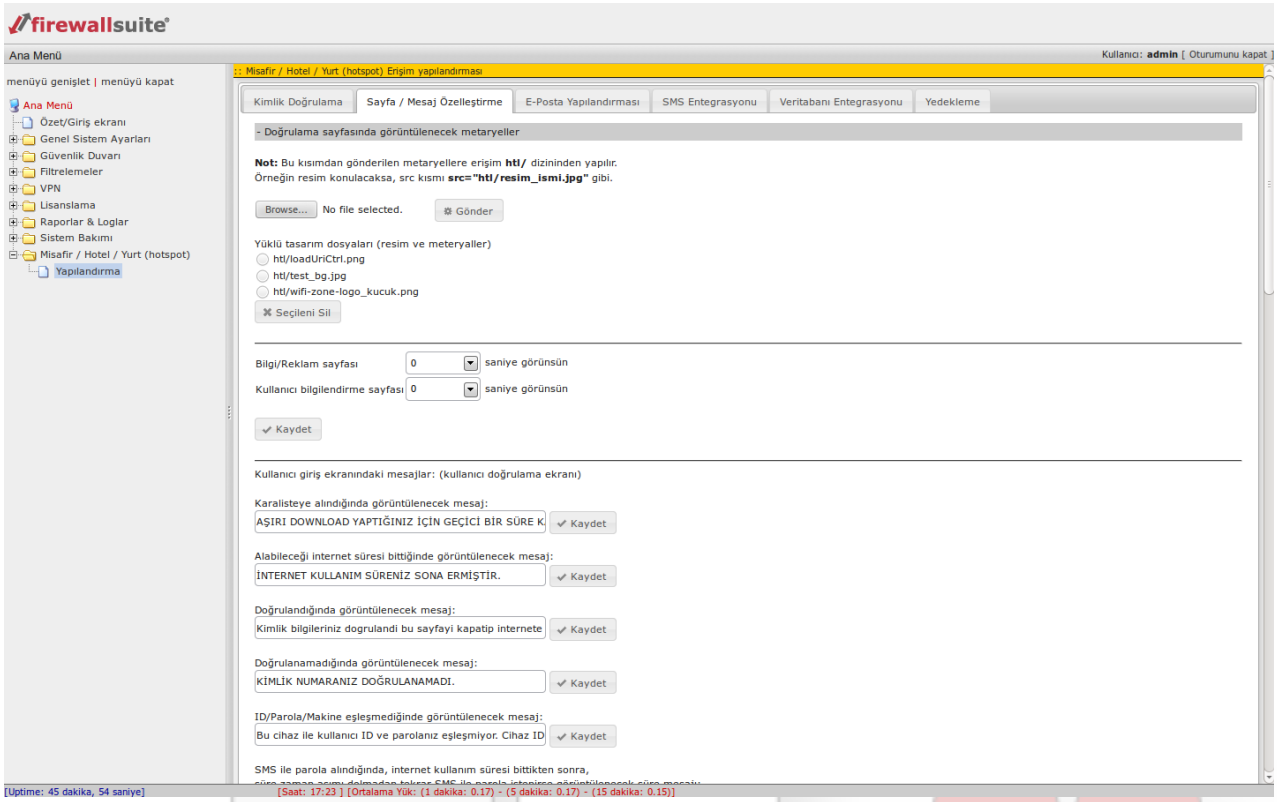
HotSpot Facebook entegrasyonu

Kullanıcı doğrulamasının Facebook hesabı üzerinden yapıldığı sistemdir ve kullanım özellikleri olarak T.C. Kimlik No doğrulama sistemindeki tüm erişim seçeneklerini içerir. Facebook doğrulama mekanizmasının çalışabilmesi için mevcut bir Facebook hesabınızın olması ve Facebook üzerinde bu hesaba ilişkin bir uygulama açılması gereklidir. Uygulama açıldıktan sonra Facebook tarafında sağlanan FirewallSuite® üzerinde yapılandırma kısmında ***App ID*** ve ***App Secret:*** değerlerinin girilmesi gereklidir.

Sayfa / Mesaj Özelleştirme

HotSpot internet kullanıcılarının internet hizmeti almadan önce karşılaşacakları sayfaların görsel düzenlemesinin yapıldığı kısımdır. Bu kısımda kurumunuzun logosu gibi görsel öğelerin bulunduğu kullanıcı doğrulama sayfası tasarlayabilirsiniz. Tasarım işlemleri HTML standardı üzerinden yapılır.

Gösterilecek sayfada bulunan resim dosyaları FirewallSuite® üzerine yüklenerek kendi içinden gelmesi sağlanır.



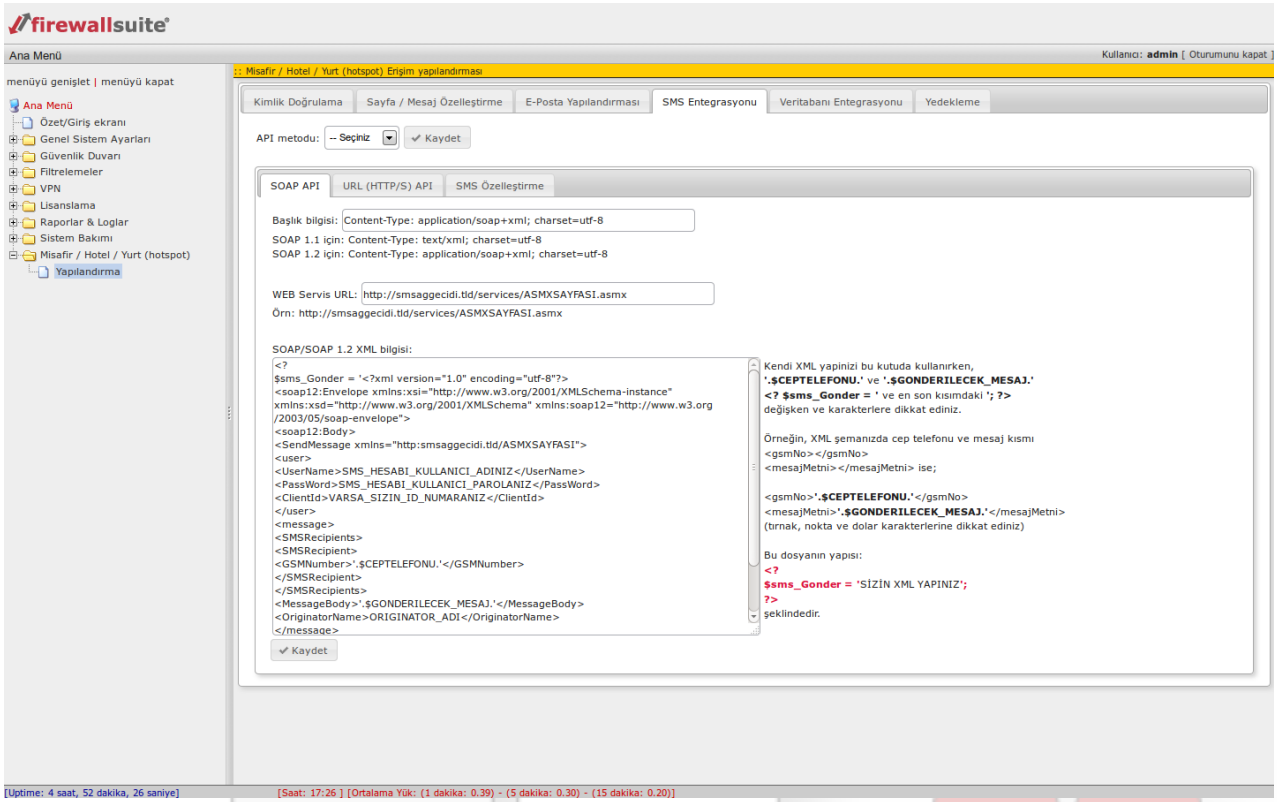
HotSpot karşılama sayfası özelleştirme

İki adet isteğe bağlı ve bir adet zorunlu doğrulama sayfası bulunur. İsteğe bağlı sayfalardan ilki doğrulama öncesi reklam ve bilgilendirme sayfasıdır. Sonra ikinci adımda doğrulama sayfası gelir ve son adımda ise yine isteğe bağlı bilgilendirme sayfası gösterilebilir. Bilgilendirme sayfalarının gösterim süreleri de bu kısımda seçilir.

E-Posta Yapılandırması

HotSpot şifre hatırlatma seçenekleri içinde elektronik posta ile şifre hatırlatma seçeneği bulunur. Eğer bu seçenek aktif edilirse sistemin şifre hatırlatma elektronik postasını atabilmesi için bu kısımda geçerli bir elektronik posta adresi ile yapılandırılmış olması gerekmektedir.

SMS Entegrasyonu



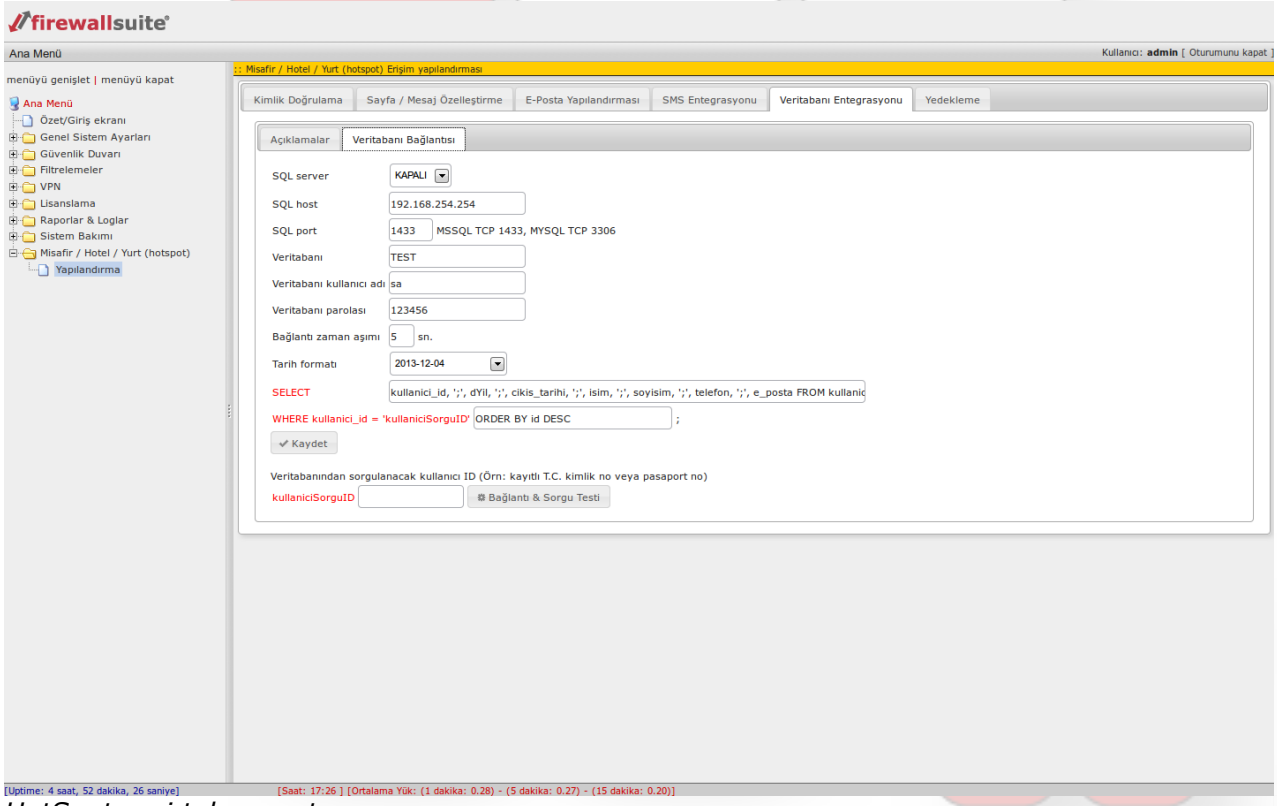
HotSpot SMS entegrasyonu

SMS ile doğrulama seçeneklerinin kullanılabilmesi için SMS servis sağlayıcısından toplu SMS hakkı alınması gereklidir. Alınan toplu SMS hizmeti ile ilgili hesap bilgilerinin girildiği ve ayarlarının yapıldığı kısımdır. Sistem SOAP ve HTTP URL olmak üzere iki farklı metodu destekler.

Hizmet satın alındıktan ve gerekli hesap bilgileri girildikten sonra FirewallSuite® SMS ile doğrulama seçeneği kullanılabilir hale gelir. Dış servise bağlı bu sistemde ***SOAP*** ve ***HTTP URL API*** düzenleme seçenekerli açık olarak gelmektedir. Hizmet satın almadan önce uyumluluk kontrolü yapmanız tavsiye edilmektedir.

Veri Tabanı Entegrasyonu

Kullanıcı veri tabanının dışarıda tutulduğu durumlarda (Otel Müşteri Takip Programı vb.) dış veri tabanına erişim ile ilgili ayarlamalar bu kısımda yapılır. FirewallSuite® MSSQL ve MySQL alt yapılı veri tabanlarını destekler. Bu veri tabanına ait sistemlerde kullanıcı doğrulaması için sorgu gönderebilir.



HotSpot veri tabanı entegrasyonu

Bu sistem özellikle otel ve benzeri platformlarda Lobi üzerinde kullanıcıya şifre sağlama gibi ekstra zaman kaybının önüne geçerek tamamen otomatik bir çözüm sunar.

Yedekleme

Sistem ayarlarından farklı olarak KYS panelinden açılmış kullanıcı veri tabanının yedeklenmesini sağlar. Alınan yedeğin sisteme verilmesi de yine bu menüden yapılır.

Notlar