6.2.3 DMZ Host

Bilgisayar ağlarında, DMZ (De-Militarized Zone) şirketin özel ağı ile dış genel ağ arasındaki tarafsız bölgeye yerleştirilmiş bir bilgisayar hostu veya küçük bir ağdır. Dış kullanıcıların şirkete ayit bir sunucuya direk erişimini engeller.

DMZ firewall a opsiyonel ve daha güvenli bir yaklaşımdır ve proxy server gibi davranır.

Küçük bir şirket için tipik bir DMZ konfigürasyonunda, ayrı bir bilgisayar (veya network terimiyle host)özel ağdaki kullanıcılardan Web sitelerine veya genel ağda erişilebilen diğer şirketlere erişim için gönderdiği istekleri alır. Fakat DMZ hostu özel networke yeniden bir oturum başlatamaz. Sadece önceden istenen paketleri iletebilir.

Şirket dışındaki genel ağ kullanıcıları sadece DMZ hosta erişebilirler. DMZ tipik olarak şirketin web sayfasına da sahip olabilir böylece bu dış dünyaya hizmet edebilir. Eğer bir dış kullanıcı DMZ hostun güvenliğine girerse web sayfaları bozulabilir fakat diğer şirket bilgileri açığa çıkmaz.

DMZ Host a tıklandığında aşağıdaki sayfa çıkar.

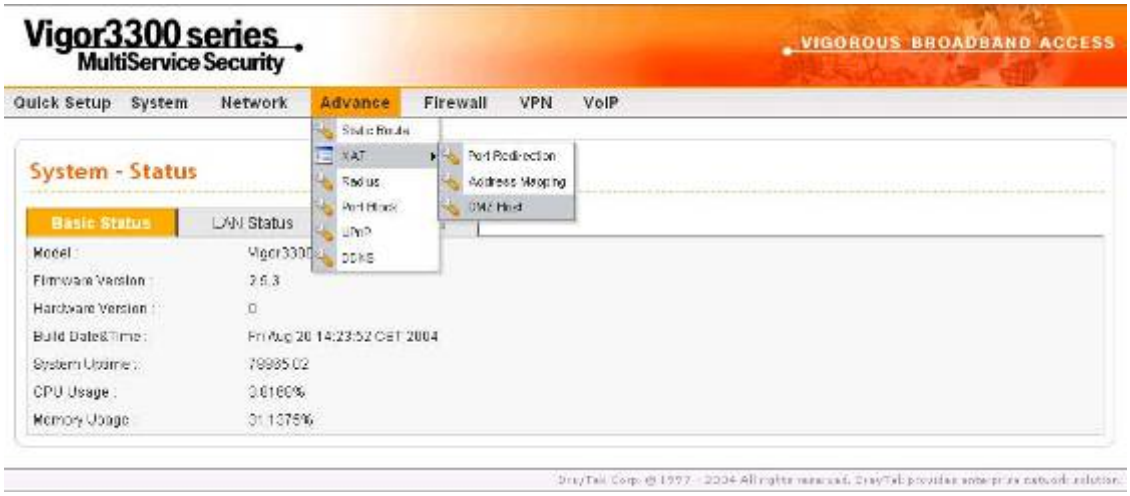


FIGURE 6-13 DMZ Host Tablosu

DMZ Host tablosuna yeni giriş yapmak için edit e tıklayın.

Aux.WAN IP – WAN konfigürasyonundaki IP Alias ayarlarından bir ip adresi seçin.

Private IP – DMZ snucusuna dışardan erişim için kabul edilecek bir ip adresi ata.

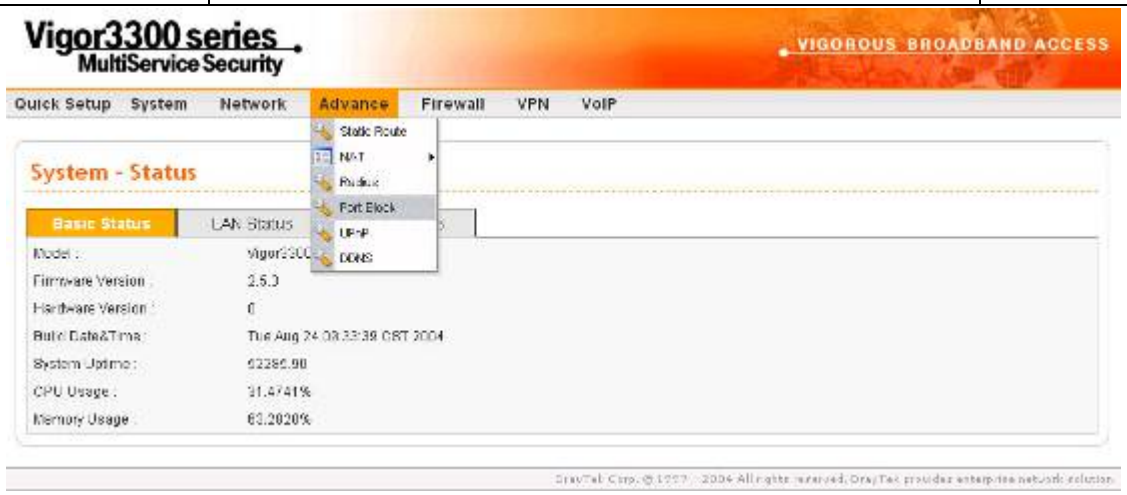
Ayarları bilitmek için applya tıklayın. Var olan bir DMZ Host tablosunu kaldırmak için delete e tıklayın.

Ayaları bitirmek için apply a tıklayın.

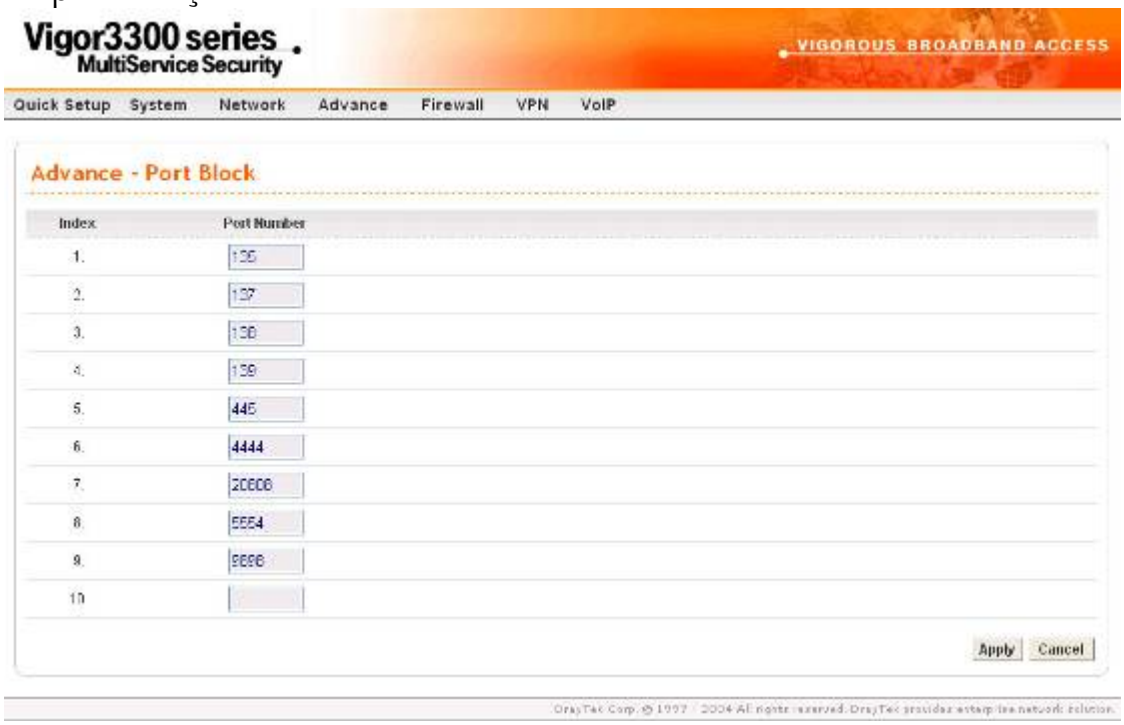
6.3 Port Blok Ayarı

Port Block fonksiyonu kullanıcıya birçok özel port numarası ayarlamasını sağlar. Eğer bu atanan port numaralarıyla paketler dışardan gelirse, bu paketler düşürülür.

Bu özelliğin avantajı bazı gereksiz paketleri veya internet üzerinden gelen saldırı paketlerinifiltrelemesidir.



Vigor3300 serisi 10 port numöarasının bloklanmasını destekler. Port Block a tıklanırsa aşağıdaki pencere açılır:



6.4 UPnP Ayarı

UPnP (Universal Plug and Play) protokolü tak ve kullan ağ cihazlarını hedefler. Bu özellik Windows'un tak ve kullan sisteminde direk bağlı PC çevre elemanlarında zaten vardır.

NAT routerları için, UpnP nin vigor3300 üzerindeki en büyük özelliği NAT 'NAT Traversal'dir. Bunun anlamı firewall içindeki uygulamalar routerın içine girmek için otomatik olarak port açar. Böyle bir mekanizma routerın üzerindeki açık portları kendisinin dağıtmasına güvenmekten daha olasıdır. Dahası kullanıcılar port haritalarını yada DMZ i manuel olarak yapmak zorunda değildirler.

UPnP özelliğiyle Vigor3300 serisi ses, video ve Windows XP üzerindeki MSN messenger mesajlaşma iletilerini de destekler.

UpnP ye tıklarsaız aşağıdaki sayfa çıkar .

UpnP fonksiyonunu enable veya disable etmek için radyo butona tıklayın.

Network Interfaces –UpnP için bir WAN interface i seçin

Ayarları bitirmek için apply a tıklayın.

Şekilde gösterildiği gibi Windows XP/Network Connections dan IP Broadband Connection on DrayTek Router a tıklayın. Bağlantı durumları ve bağlantı durumları aktive edilebilecektir.

UPnP nin NAT Traversal özelliği uygulamalarınızın multimedya özelliğini aktive eder. UpnP olmadan , port haritalamaları ayarlamalı veya bazı benzer konfigürasyonları manuel olarak

yapmalısınız. Yukarıdaki screenshotlar örneklerdir.

Figür 6-24 UPnP konfigürasyonu

Vigor3300 UPnP özelliği NAT içindeki UPnP-duyarlı uygulamaları örneğin MSN Messenger 'ın dış ip adresini keşfetmesi ve router üzerinde port haritalama konfigüre etmesi. Sonuç olarak: UPnP li bir router uygulama gereklerine göre dış portlardan gelen paketleri iç portlara yeniden yönlendirecektir.

6.5 DDNS Ayarları

Dinamik DNS fonksiyonu routera tanımlanmış DDNS sunucuya ISS veya DHCP tarafından verilen kendi WAN ip adresini online olarak güncellemesine izin verir. Router online olduktan sonra, routera erişmek veya internetten iç sanal sunuculara erişmek için routerın kayıtlı kırmızı bölge ismini kullanabilirsiniz. DDNS ISS dan sıklıkla ip adresini değiştiren dinamik ip kullanıcıları arasında daha popülerdir.

DDNS fonksiyonunu ayarlamadan önce DDNS sağlayıcıların ücretsiz alan adına üye olmanız gerekir. Router fonsiyon için üçe kadar hesap sağlar ve şu sağlayıcıları destekler: www.dynsns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic-nameserver.com. Kendi alan adınızı routera kaydettirmek için kendi web sayfalarını ziyaret etmeniz gerekir.
DDNS e tıklarsanız aşağıdaki ekran gelecektir. DDNS tablosuda değişiklik yapmak için **#number** a tıklayın.

Disable(devre dışı)veya **Enable**(aktve) için radyo butonlarını kullanın.

Interface – WAN1 den WAN4 e kadar DDNS sunucusunun bulunduğu bir interface seçin.

Server Provider –DDNS sunucusunu sağlayacak servis sağlayıcısının adını atayın.

Server Type – seçeneklerden birini seçin.– **Static**, **Dynamic** and **Custom** desteklenenseçeneklerdir.

Domain Name – erişilecek bir özel alan adı atayın.

Login Name – DDNS sunucusunda oturumu açacak bir isim atayın.

Login Password –DDNS sunucusunda oturumu açacak bir parola atayın.

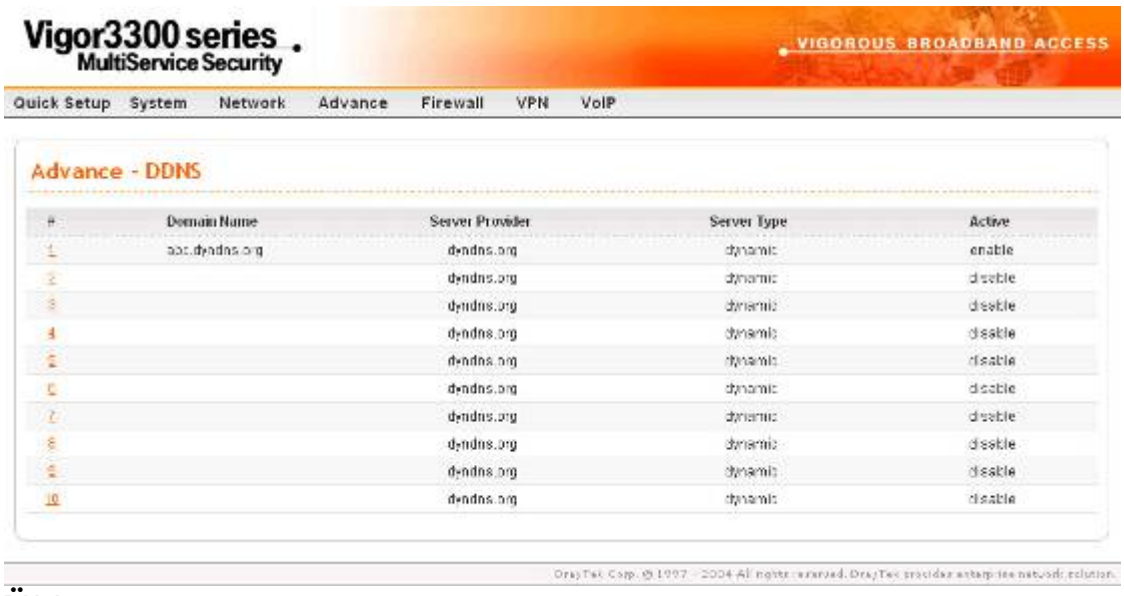
Wild Card –bu fonksiyonu aktive edin veya devre dışı bırakın.

Backup MX – bu fonksiyonu aktive edin veya devre dışı bırakın.

Mail Extender – bir email adresi atayın.

Not:
1 Wildcard ve Backup MX özellikleri tüm DNS sağlayıcıları tarafından desteklenmez. Web sayfalarından bununla ilgili detaylı bilgi almalısınız.
2. Backup Mx ana e-mail sunucunuz herhangi bir nedenden dolayı offline olursa ikinci bir mail sunucusu sağlar.yenidn online olduğunuzda e-mailleriniz size ulaştırılacaktır

Ayarları bitirmek için **Apply** a tıklayın.



BÖLÜM 7
Firewall Ayarları
7.1 Giriş

Vigor routerlarda **Firewall** paket filtreleme, Denial of Service (DoS) koruması ve URL (Universal Resource Locator) içerik filtreleme özelliklerini kapsar. Firewall özelliği yerel ağınızı dışardan gelecek saldırılara karşı korur. Aynı zamanda yerel kullanıcıların internet erişimini de sınırlandırabilir. Routerın dışarı bağlantı kurmasını tetikleyecek özel paketleri filtreleyebilir. Call Filter(hücre filtresi) V3300i ISDN modelinde desteklenir.

Paket filtreleme fonksiyonu iki çeşit fonsiyon içerir: Call Filter(arama filtresi) ve Data Filter(veri filtresi). Arama filtresi LAN tarafınadan dışarıya bağlantı kurmaya çalışan kulanıcılar için kulanılır. Data filtreleme WAN bağlantısı kurulduktan sonra hagi tip ip paketlerinin routerdan geçmesine izin verileceğini belirler.

Konsept olarak, dışarı giden bir paket routerdan WANa yönlendirildiği zaman,ip filtresi paketin data filtresine mi hücre filtresine mi iletileceğine karar verir. WAN bağlantısı kapalıysa, paket hücre filtresine girecektir. Pakete routerı bağlantı için tetiklemesine izin verilmezse , paket düşürülür. Değilse WAN bağlantısı kurmak için bir arama başlatır.

Routerdaki WAN linki açıksa, paket data filtresine girer. Paket çeşitinde blok ayarlandıysa,paket düşürülür. Değilse WAN inerface ine gönderilir. Alternatif olarak, WAN interface inden gelen bir paket girerse direk data filtresine girecektir. Paket çeşidi bloklanacak olarak ayarlandıysa, paket düşürülür, değilse iç LAN a gönderilir.

Firewall fonsiyonundaki ip filtreleme özelliğini aktive etmeden önce, kullanıcı filtre kurallarını içeren bir grup yaratmalıdır . ileri filtre fonksiyonları için filtre kuralları alt gruplara ayrılabilir. Bu gruplar filtre fonksiyonlarını düzenler ve işletir. Bir başlama grubu seçmeli ve sonraki grup olarak bir grup atamalı veya filtre kuralındaki diğer gruba dallandırılmalıdır. Konsept figürde gösterilmiştir.

Group 1

1. başlangış Grubunu seçin

Filtre kuralı 1-1
Filtre kuralı 1-2
Filtre kuralı 1-3

Group 3

2. paket 3-1 kuralıyla eşleşirse

Kural 1-2 daha sonra

Group 3 e dal

Filtre kuralı 3-2
Filtre kuralı 3-3

Group 2

3. Group 2 is Filter Rule 2-1 the next group Filter Rule 2-2 of Group 1 Filter Rule 2-3

.

7.2 Firewall Ayarlarına Genel Bir Bakış

Aşağıdaki bölümler firewall un nasıl konfigüre edileceğini anlatmaktadır. Web konfigürasyonunda **Firewall** a basın, **General Setup(genel ayarlar)**, **IP Filter**, **DoS** ve **URL Filter** bulacaksınız. Öncelikle en az bir grup yaratlamısınız : **IP Filter** > **Group Table**. Daha sonra **Data Filter** ı aktive edin ve **General Setup dan Start Filter Group** u seçin. **DoS** koruması DoS saldırılarını belirler ve hafifletir. **URL Filter** istenemeyen web sitelerine erişimi engeller.

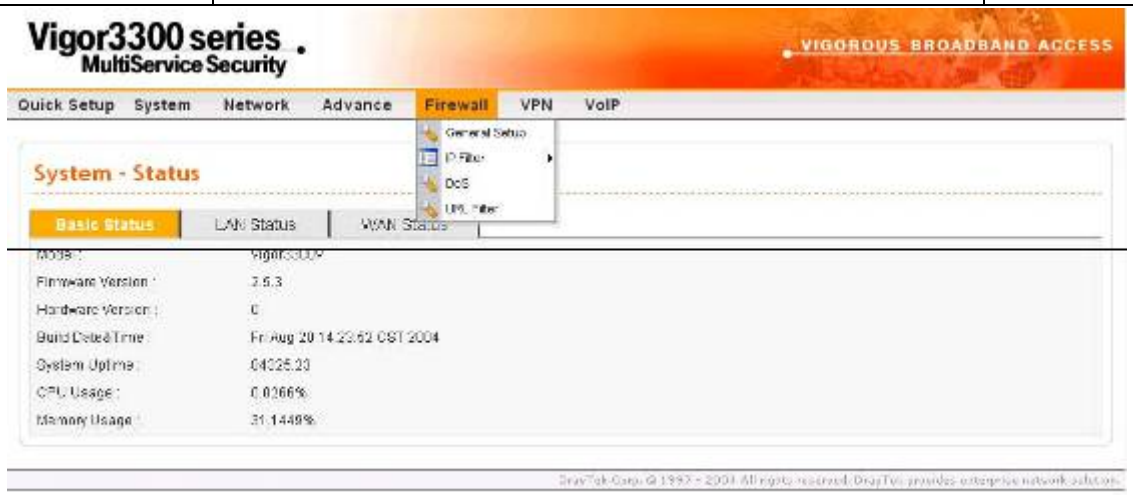
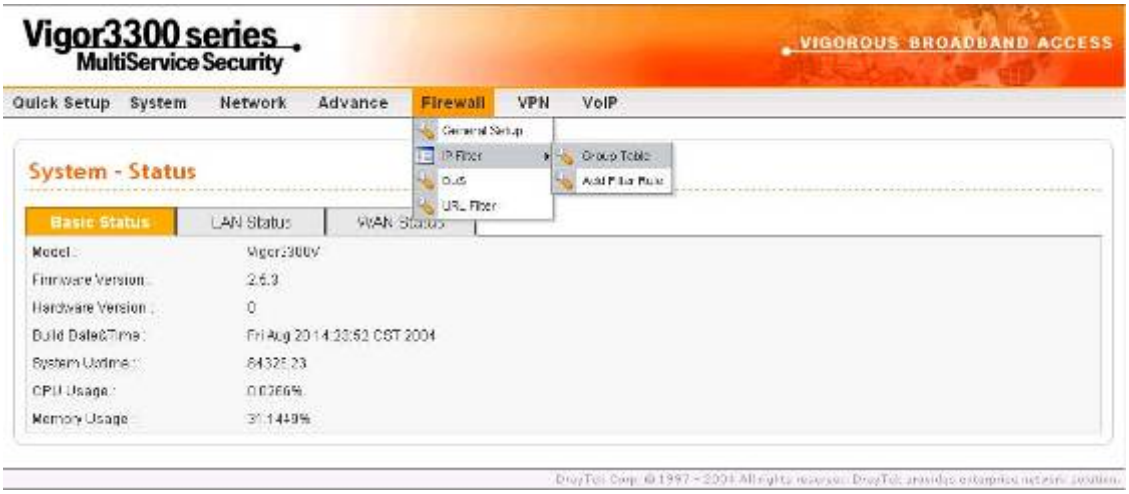


FIGURE 7-3 Firewall Location

7.3 IP Filter Kural Ayarları

Filtre kuralları ayar sayfasına girmek için **IP Filter** a tıklayın.

7.3.1 Group Tablosu Ayarları



Group Table seçeneğine tıklayın Yeni grup eklemek için **Add** e tıklayın. **Group Name(grup adı)**, **Next Group Name(sonraki grup adı)** ve **Comment(açıklama)**. Ayarları saklamak için **Apply** a tıklayın veya vazgeçmek için **Cancel** a tıklayın.

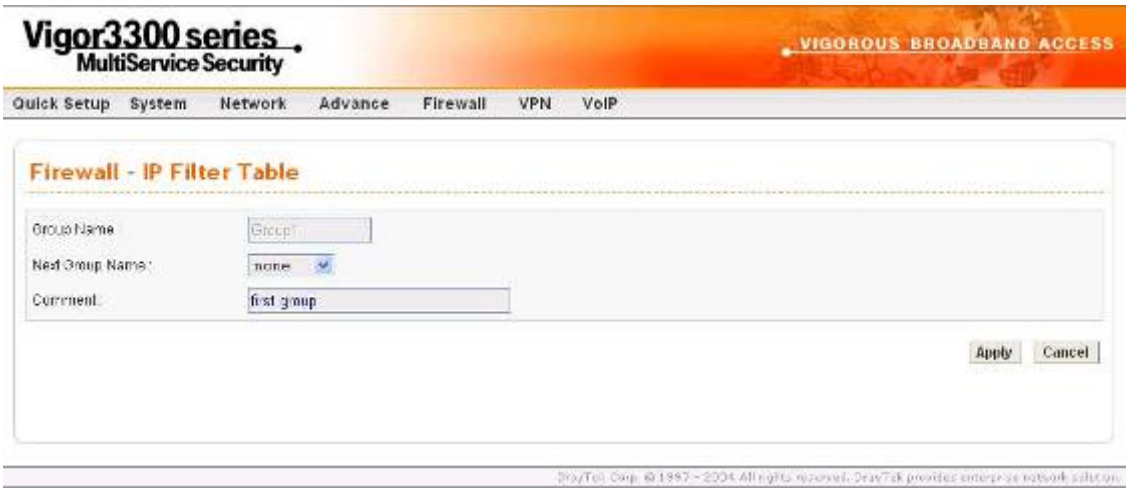
Group Name **–**ip filtreleme tablosunada bir grup tanımlayın.

Next Group Name **–**sonraki grup mevcut grupta filtrelendikten sonra yeniden filtreleneceği ip filtresini belirtir.

Comment **–**kural grubu için yorum tabloda gösterilmiştir.

Ayarları tamamlamak için **Apply** a tıklayın.

Değişiklik yapmak için **Edit** e tıklayın.



Grubu kaldırmak için **Delete** e tıklayın..

7.3.2 Filtre Kuralı Ekleyin

Firewall->IP Filter->Add Filter Rule a tıklayın.

Source IP **–**filtre kuralının uygulanacağı kaynak ip adresi.ip adresinden önce ''!'' sembolü koymak bu kuralın o ipye uygulanmasını engeller. Bu özet bir NOT operatürüne eşittir.

Subnet Mask **–**kaynak ip adresi için alt ağ maskesini belirtir.

Source Port **–**kaynak ip için port belirtir.

(Operator)

operatör kolunu port numarası ayarlarını belirtir. **Start Port** u boşsa ***Start Port*** ve ***End Port*** kolonları gözardı edilecektir. Filtre kuralı her port numarasını filtreleyecektir. **=** *:* eğer ***End Port*** boşsa, filtre kuralı port numarasını ***Start Port*** un değerine atayacaktır. Değilse, port numara değerleri ***Start Port*** ve ***End Port*** arasında değerler alacaktır. (***Start Port*** ve ***End Port*** u da içerir).

!= *: eğer* ***End Port*** boşsa, port numarası ***Start Port*** un değerine eşit değildir. Değilse port numarası ***Start Port*** ile ***End Port*** arasında değildir. (***Start Port*** ve ***End Port*** u da içerir).

>: port numarasının ***Start Port*** dan büyük olduğunu belirtir(***Start Port*** dahil*).*

< : port numarasının ***Start Port*** dan küçük olduğunu belirtir. (***Start Port****).*

Destination IP **–**bu filtre kuralının uygulanacağı hedef ip adresini belirtir. Ip adresinden önce "**!**" koymak bu ipye bu kuralın uykgulanmasını engeller. NOT operatörüne eşittir.

Destination Mask **–**hedef ip adresi için ağ maskesi

Destination Port **–**hedef ip adresi için port deperini belirtir.

Group Name **–**kullanımda olan kuralın grup adı.

Direction **–**paket akışının yönünü belirtir. **IN** gelen paketler için

OUT çıkan paketler için **Any** her iki yön için..

Protocol **–**filtre kuralındaki protokolleri belirtir.

Fragments **–**parçalanmış paket faaliyetlerini belirtir.

- **do not care:** filtre kuralında parçalanma seeçeneği lmadığını belirtir.
- **unfragment:** kuralı parçalanmamış paketlere uygular.

fragmented: kuralı parçalanmış paketlere uygular.
Active **–** fonksiyonu aktive etmek için u seçeneği kullanın.
Firewall Setup Block or Pass **–**paketler kuralla eşlenince yapılması gereken işlemi belirtir.

Block: bu kuralla eşleşen baketler anında bloklanır.

Pass: bu kuralla eşleşen paketler anınd iletilir -

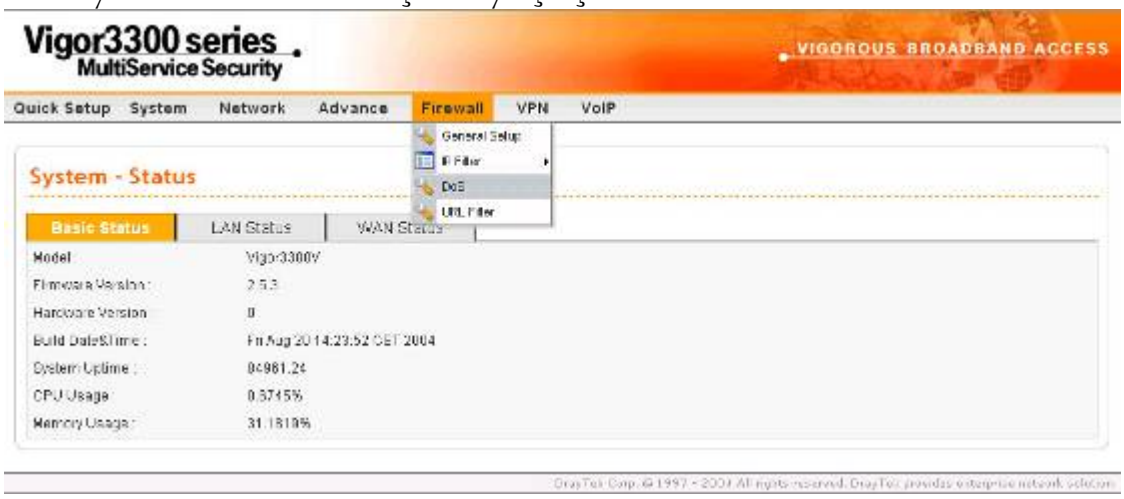
Block if no future match: herhangi bir kuralla eşleşmeyen paketler düşürülür.

Pass if no future match: hiçbir kuralla eşleşmeyen paketler geçirilir.
Next Group Name **–**sonraki grup adını seçin.Eğer **Block or Pass** deki **Block if no future match** veya **Pass if no future match** seçilirse, paket **Next Group** daki diğer kurallarla karşılaştırılır. Eğer **Block** veya **Pass** seçilirse bu gözardı edilecektir.

Not: bu kuralı aktive etmek için **Active** a tıkmayı unutmayın.

7.4 DoS Saldırıları Ayarları

DoS Koruma fonksiyonu DoS saldırılarını tespit etme ve hafifletmeye yardımcı olur. Bu saldırılar baskon şeklinde saldırılar veya zarar veici saldırılar olabilirç Baskın şeklindeki saldırılar tüm sistem kaynklarınızı kullanmaya çalışır, zarar verici saldırılar sistem veya protokolünüzün açıklarından yararlanarak sistemi felç etmeye çalışır.



DoS seçeneğine tıklarsanız:

DoS koruma motoru saldırı işaret databaseine karşı gelen her paketi inceler. Çalışma bölgesinde sistemi felç edebilecek herhangi bir paket bloklanır. DoS koruma makinası aynı zamanda network trafik davanışını da gösterir. DoS konfigürasyonunu ihlal eden herhangi bir anormal durum saldırıyı hafifletmek için ilgili fonksiyona rapor edilir. Aşağıdaki tanımlama web konfigürasyonu kullanarak DoS konfigürasyonu hakkında daha detaylı bilgi vermektedir. Ip filtrelemenin bir alt fonksiyonudur. 15 çeşit koruma fonksiyonu vardır. Varsayılan olarak DoS koruma fonksiyonu aktive edilmiştir, varsayılan sınır ve zaman dışı bazı fonksiyonlar için 300 paket/saniye ve 10 saniye olarak ayarlanmıştır. Her DoS fonksiyonu için ayrıntılı açıklama aşağıda verilmiştir:

DoS Defense –radyo butondan aktive edin veya devre dışı bırakın

Enable SYN flood defense –SYN baskın korumasını aktive etmek için kutuya tıklayın. Eğer TCP SYN paketleri kullanıcı tarafından tanımlanan sınır değerini geçerse router kullanıcı tarafından tanımlanan zaman aşımı süresi dolan kadar TCP SYN paketlerini düşürecektir. Ana avantajı router ı kaynaklarını kullanmaya çalışan TCP SYN paketlerinden korumasıdır. Varsayılan olarak sınır değeri 300 paket/saniye, zaman aşımı süresi 10saniye olarak ayarlanmıştır.

Enable UDP flood defense –Cbu fonksiyonu aktive etmek için kutuya tıklayın. UDP paketleri sınır değerini aştığı zaman router kullanıcı tarafından tanımlanan zaman aşımı süresi dolana kadar gelen tüm UDP paketlerini düşürür. Varsayılan değerleri 300 paket/saniye ve 10 saniyedir.

Enable ICMP flood defense –bu özelliği aktive etmek için kutuya tıklayın. İşleyiş UDP flood paketlerinde olduğu gibidir.

***Enable Port Scan detection* –**port tarama denetleme fonksiyonunu açmak için kutuya tıklayın. Port tarama saldırıları farklı port numaralarında paketler yollayarak buna tepki verecek boş port olup olmadığını kontrol eder. Böyle bir aktiviteden haberdar olmak için özelliği aktive etmelisiniz. Router bunu tanımlayacak ve kullanıcı arafndan tanımlanan sınır eğeri aşılırsa uyarı mesajı verecektir. Varsayılan 300 paket/ saniyedir.

***Enable Block IP options* –**bu özelliği aktive etmek için kutuya tıklayın. Datagram başlığında seçenek alanı görülen tüm ip paketleri gözardı edilir. Ip seçeneği hostların bazı önemli bilgileri(örneğin dışardan birinin analiz edip özel ağınız hakkında bilgi edinebileceği güvenlik, TCC parametreleri, internet erişim ve yönlendirme mesajları) göndermesini destekler.

***Enable Block Land* -** bu özelliği aktive etmek için kutuya tıklayın. LAN saldırısı SYN saldırısını ip hilekarlığıyla birleştirebilir(ip spoofing). Bir saldırgan tanımlayıcı kaynak ve hedef port ve ip numaraları olan paketler spoofed SYN paketleri gönderdiğinde bu saldırı türü olur.

***Enable Block Smurf* -** bu özelliği aktive etmek için kutuya tıklayın. Router broadcast adresine gönderilen her ICMP eko paketini reddeder.

***Enable Block trace route* -** bu özelliği aktive etmek için kutuya tıklayın. Router hiçbir yönlendirme izleme (trace route) paketini iletmeyecektir.

***Enable Block SYN fragment* -** bu özelliği aktive etmek için kutuya tıklayın.. SYN bayrağı olan ve daha fazla fragment biti ayarlanmış paketler düşürülür.

***Enable Block Fraggle Attack* -** bu özelliği aktive etmek için kutuya tıklayınınternetten gelen her UDP broadcast paketi bloklanacaktır.

***Enable TCP flag scan* -** bu özelliği aktive etmek için kutuya tıklayın. Anormal bayrak ayarına sahip her paket düşürülür. Bu tarama aktiviteleri: **no flag scan(bayrak tarama yok)**, **FIN without ACK scan(bilgilendirme olmadan FIN taraması), SYN FIN scan**, **Xmas scan** ve **full Xmas scan**. ***Enable Tear Drop* -** bu özelliği aktive etmek için kutuya tıklayın..bu saldırı hedef hosta gönderilen paketlerin göndericisini gerektirir böylece hedef host bir kere asıldıktan sonra paketler yeniden yapılandırılabilir. Router saldırı aktivitesi farkettiği her paketi bloklar.

***Enable Ping of Death* -**bu özelliği aktive etmek için kutuya tıklayın.. Çoğu makine maksimum uzunluğu geçen ICMP paketleri aldığı zaman olumsuz etkilenir. Bu tarz saldırıdan korunmak için router 1024 oktetten uzun ICMP paketlerini reddetmek için programlanmıştır.

***Enable Block ICMP fragment* -** bu özelliği aktive etmek için kutuya tıklayın. Fazla fragment(parçalama) biti olan paketlerdüşürülür.

Enable Block Unknown Protocol **-** bu özelliği aktive etmek için kutuya tıklayın.. bölünemeyen ip paketlerinin datagram başlığında üst katmanda çalışan protokolleri belirten bir başlık kısmı vardır. Fakat 100ün üzerinde protokol çeşidi rezerve edilmiştir ve şu an tanımlı değildir . Bu nedenle router paketlerin çeşidini tanıyabilmeli ve geri çevirebilmelidir.

Ayarları tamamlamak için apply a tıklayın.

7.5 URL Filtre Ayarı
7.5.1 Giriş

internet çok büyük bir oranda materyal barındırır ve bunların çoğu zararlı veya saldırı içerikli olabilir. Geleneksel medyadan farklı olarak internetin materyalleri URL dizilerine veya çleriklerine göre kesin olarak ayıracak araçları yoktur. Filtreleme sistemleri bazı materyallere erişimi engelleyen sistemlerdir. Bir sitenin zararlı görülmesi ve kullanıcı ekranında görüntülenmesini engellemek, çocukların ailelerinin içeriğini görmesini istemediği sayfalara erişimi engellemesiiçin URL içerik filtreleme kullanılabilir. Erişimin engellenmesinde URL içerik filtreleme yaşı küçüklere yetişkin dergilerinin satılmasını engelleyen otomatik bir sistem gibi düşünülebilir. URL içerik filtreleme aynı zamanda şirket çalışanlarının çalışma alanlarıyla ilgisiz veya yersiz internet erişiminiengellemek için kullanılır.

URL içerik filtreleme terimi URL dizilerinin içeriğinin incelenmesinden gelmektedir. Geleneksel firewalllar paketleri TCP/IP paket başlığına bağlı olarak inceleme yaparken, URL içerik filtreleme URL dizilerini veya TCP/IP paketinin yükünü yani içerdiği datayı araştırır. Routerlarda URL içerik filtreleme URL dizilerini ve TCP paketlerindeki bazı http data saklamaları araştırır.

7.5.2 URL İçerik Filtrelemeye Genel Bakış

FIGURE 7-12 URL Filtering Example

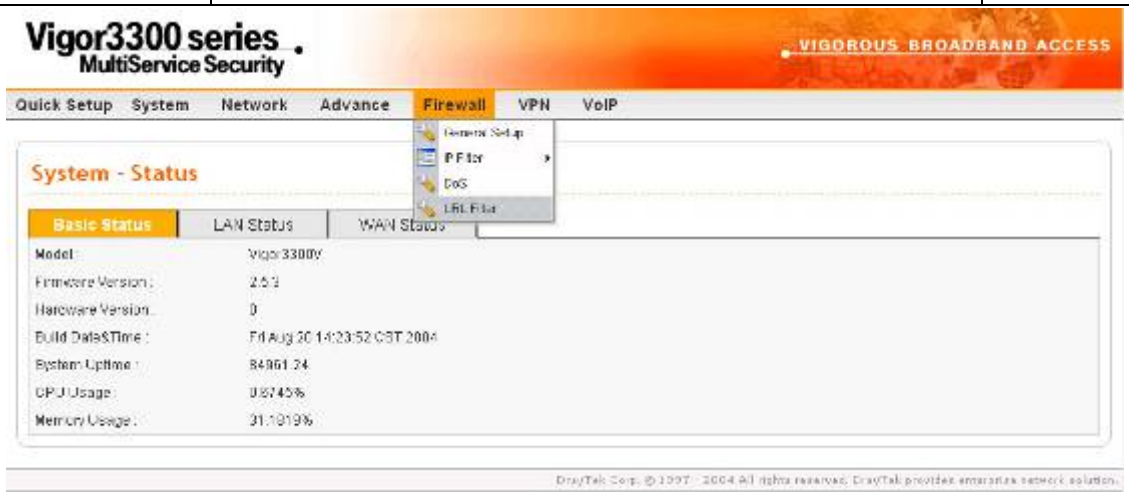
Broadband güvenlik routerlarında URL içerik filtreleme her http istemindeki URL yi anahtar kelimeye bağlı olarak araştırır. Eğer URL dizisinin içindeki bir kısım veya tamamı anahtar kelimelerle eşlenirse, router üzerinde http istemi bloklanır.

URL içerik filtreleme dizisi zararlı olarak tanımlanmış sayfalara kullanıcıların erişimini engeller. İçerik filtrelemeyi çalıştırmadan önce dikkat etmeniz gereken web tarayıcınızın ön belleğini temizlemeniz gerektiğine dikkat etmelisiniz. Böylece içerik filtreleme daha önce ziyaret ettiğiniz sayfalarda doğru olarak çalışabilir.

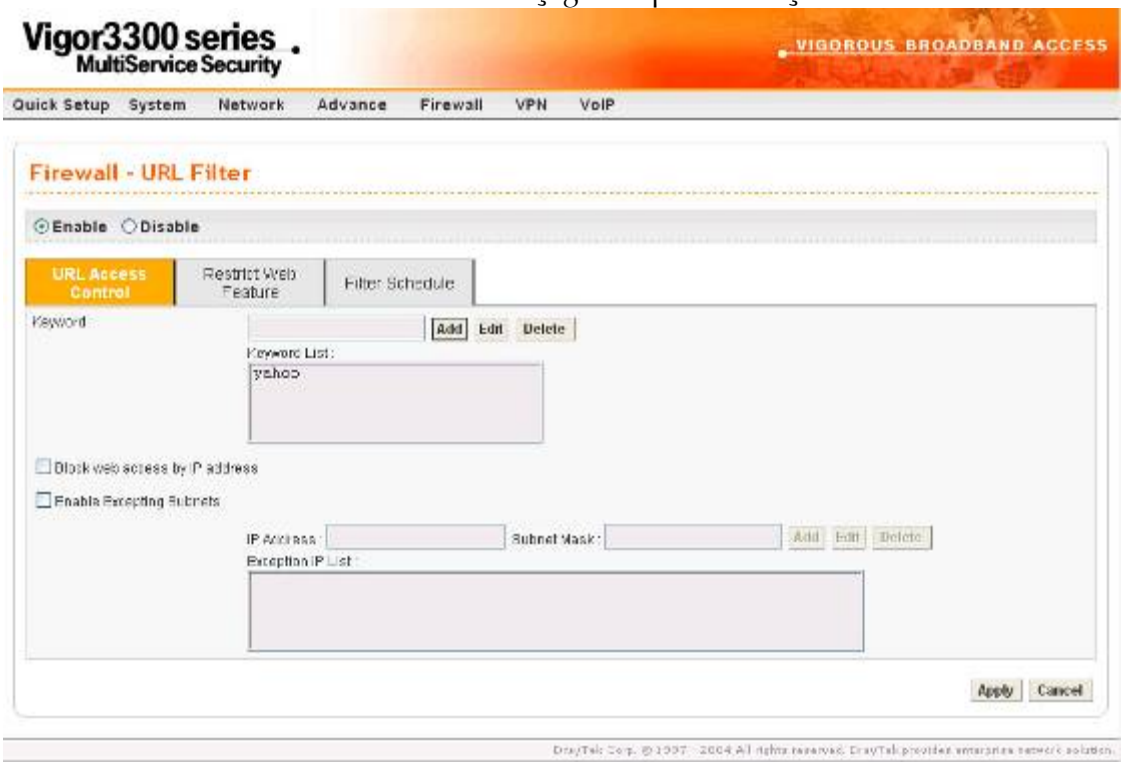
7.5.3 URL İçerik Filtreleme Konfigürasyonu

Aşağıdaki kısımda URL içerik filtrelemenin web konfigürasyonu içerdiği özel konfigürasyon bilgileri ve sahip olduğu limitler anlatılacaktır.

Routerda desteklenen URL içerik filtreleme aktiviteleri URL Access Control(URL erişim kontrolü), Block web access by IP address(ip adresine göre web erişimini engelleme), Restrict Web Feature(sınırlandırılmış web özellikleri), Excepting Subnets(beklenen alt ağlar), ve Filter Schedule(filtre zaman tablosu). URL erişim kontrolü kullanıcı tarafından tanımlanan anahtar kelimelere göre URL dizisini araştırıp web sitelerine erişimi kontrol eder. Sınırlandırılmış web özelliği web sayfaları tarafından saklanmış kodları (örneğin Java Aplet, Active X cookiler,Proxy , sıkıştırılmış dosyalar, executable dosyalar)bloklar. Aynı zamanda band genişliği lullanımını kontrol etmek için web sayfalarından multimedia dosyaları indirilmesini bloklayabilir.
İp adresine göre erişim bloklaması özelliği istenmeyen sitelere doğrudan ip ile erişimin engelenmesini önlemek içindir. URL dizisi anahtar kelimelerle eşlense bile direk ip adresinden girilebileceğinden bnun önüne geçilmiş olur. Beklenen alt ağlar URL erişim kontrolünde bir grup kullanıcının URL ye erişiminin serbest olmasına izin verir. Bu gruptaki kullanıcılar bi ip adresi veya alt ağ kümsei olarak tanımlanabilir. Son olarak filtre zaman tablosu URL içerik filtrelemenin ne zaman gerçekleştirileceğini belirler.



URL Filter a tıklarsanız aşağıdaki pencere açılacaktır.



Enable URL Access Control- URL Erişim Kontrolünün Aktive Edilmesi

Keyword List (anahtar kelime listesi)-Router kullanıcılara anahtar kelime tanımlamaları için 8 çerçeve verir ve her çerçeve birçok anahtar kelime içerir. Anahtar kelime bir isim kısmi bir isim veya tüm URL dizisi olabilir. Bir çerçeve içindekibirden çok anahtar kelimeyi birbirinden ayırmak için boşluk, virgül veya noktalı virgülle birbirinden ayrılır. Her çerçeve için maksimum uzunluk 32 karakterdir. Anahtar kelimeler tanımlandıktan sonra bu anahtar kelimeyi içeren URL ye sahip web sayfaları bloklanır. Anahtarkelimeler ne kadar özelleştirilirse router o kadar yararlı çalışacaktır.

örnek –eğer URL dizisinde "sex", "fuck", "gun", or "drug" kelimeleri geçen herhangi bir sayfayı bloklamak isterseniz ,bu kelimeleri çerçevelere eklemelisiniz. Böylece sistem bu kelimeleri içeren URL leri otomatik olarak reddeder. Routerın URLsi www.backdoor.net/images/sex/p_386.htmlolan bir sayfaya erişmek istediğini düşünülürse, bağlantı kesilcektir. Fakat kullanıcı www.backdoor.net/firewall/forum/d_123.html sayfasınaulaşabilecektir. Aynı zamanda URL adresinin tamamını veya bir kısmını bloklama anahtar kelimesi olarak atayabilirsiniz.

Prevent Web Access by IP Address –direk ip adresi kullanarak webe çıkmayı yasaklar.

Enable Excepting Subnets – kullanıcılar için bazı özel ip adresleinin veya alt ağların URL erişiminde serbest olabilmesi için iki giriş vardır.bu fonksiyonu aktie etmek için kutuya tıklayınız.

Restrict Web Feature –zararlı kodlar executable objelerin içine gömülü olabilir.eğer bunlar web sayfalarından indirilirse kullanıcının sistemine zarar verebilir. Örneğin Active X bir web sayfasından indirilebilir ve çalıştırılabilir. Eğer zararlı kod içeriyorsa kullanıcının sistemine limitsiz girişe sahip labilir.

Java –java objelerini bloklamak için kutuya tıklayın. Router internetten java objelerini reddedecektir. ActiveX –Active-X özelliğini bloklamak için kutuya tıklayın. İnternetten herhangi ir Active-X objesi engellenecektir.

Compressed file – kutuya tıklandığında herhangi birisinin sıkıştırılmış dosya indirmesi engellenmiş olur. Aşağıdaki liste router tarafından bloklanan sıkıştırılmış dosyaların uzantısını

göstermektedir.

.zip .rar .arj .ace .cab .sit

Bu özelliği aktive etmek için kutuya tıklayınız.

Execute file –yukarıdaki foksiyona benzerdir. İnternetten herhangi bir türütülebilir dosya indirilmesini reddetmek için özelliği yanındaki kutudan aktive edin. Router aşağıdaki uzantıları bloklayabilir.

.exe .com .scr .pif .bas .bat .inf .reg

cookie denilen özellik Netscape taafından tanıtılan ve HTTP istek ve cevap aktivitelerine daha yakından bakabilmenizi sağlayan bir özelliktir. Çoğu web sitesi internet kullanıcılarının aktivitelerini izlemek için kullanırlar ve bu kullanıcıların özelini ihlal eder. Router bunu engeller. Aynı zamanda router tüm proxy ilişkili iletimi daha yüksek seviyede güvenlik sapğlamak için filtreleyebilir.

Cookie –cookie iletimini bloklamak için kutuya tıklayın. Router tüm web sayfalarından gelen cookieleri filtreliyecektir.

Proxy – proxy iletimini bloklamak için kutuya tıklayın. Router tüm sitelerden gelen proxy iletimini bloklayacaktır.

Multimedia - Multimedia iletimini bloklamak için kutuya tıklayın. Router tüm web sayfalarından gelen multimedia iletimini bloklar.

Filter Schedule – URL içerik filtreleme işleminin ne zaman yapılacağını belirtir. ***Always Block –*** bu özelliğe tıklarsanız router filtrelemeyi her zaman yapar. ***Block only at –***sadecde

tanımladığınız zamanlarda filtreleme yapar *H1*:*M1* den *H2*:*M2* e kadar. *H:saat M:dakika* ***Days of Week –*** haftanın hangi günlerinde URL filtreleme işleminin yapılacağını belirtin. Router kullanıcıya haftanın her günü veya haftanın belli günleri filtreleme işlemi yapacağını seçme şansı sunar. "**Everyday**" seçeneğiyle hergün filtreleme yapabilirsiniz. Veya haftanın belli günleri filtreleme yapmak için günleri kutulara tıklayarak seçmelisiniz.

7.5.4 Uyarı Mesajı

HTTP isteği reddedildiğinde, figürde görüldüğü gibi web tarayıcınızda bir uyarı mesajı görülür.

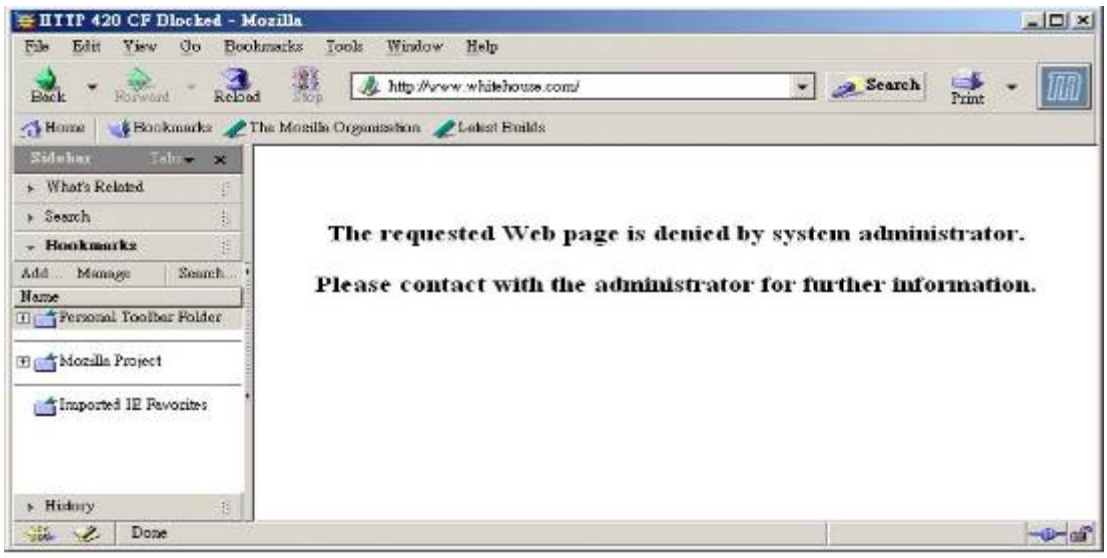


FIGURE 7-15 Warning Message

BÖLÜM: 8

VPN (Virtual Private Network-Sanal Özel Ağ) ve Uzaktan Erişim Ayarları

8.1 Giriş

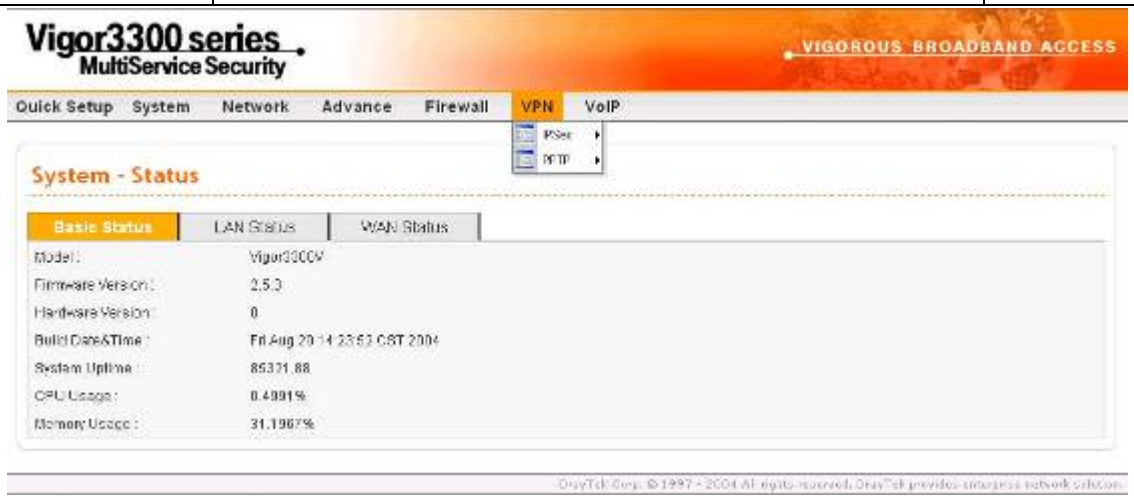
VPN internet gibi paylaşılan veya genel ağlar üzerinden bağlantı kuran özel ağın gelişmiş bi halidir. VPN size paylaşılan veya genel bir ağdan iki host arasında noktadan noktaya özel bağlantı gibi data yollanmasına izin verir.

İki çeşit VPN bağlantısı varır. Uzaktan aranığp erişilebilen (Remote Dial-In Access)VPN ve LAN dan LAN a VPN. "" işlemi uzaktan erişim noduna izin verir (bir NAT routerı veya tek kullanıcılı bilgisayar) VPN routerı arama ve uzak ağın kaynaklarına internet üzerinden erişim. LAN dan LAN a erişimişlemi iki bağımsızLANı karşılıklı paylaşım için bağlamaktır. Örneğin merkez ofis şubeye ulaşabilir v.s.

Vigor3300 broadband güvenlik routerslarındaki VPN teknolojisi kullanıcılara uyumlu VPN çözümleri sunmak için Internet Protocol Security (IPSec-internet protokol güvenliği) gibi internet endüstri standardını destekler.

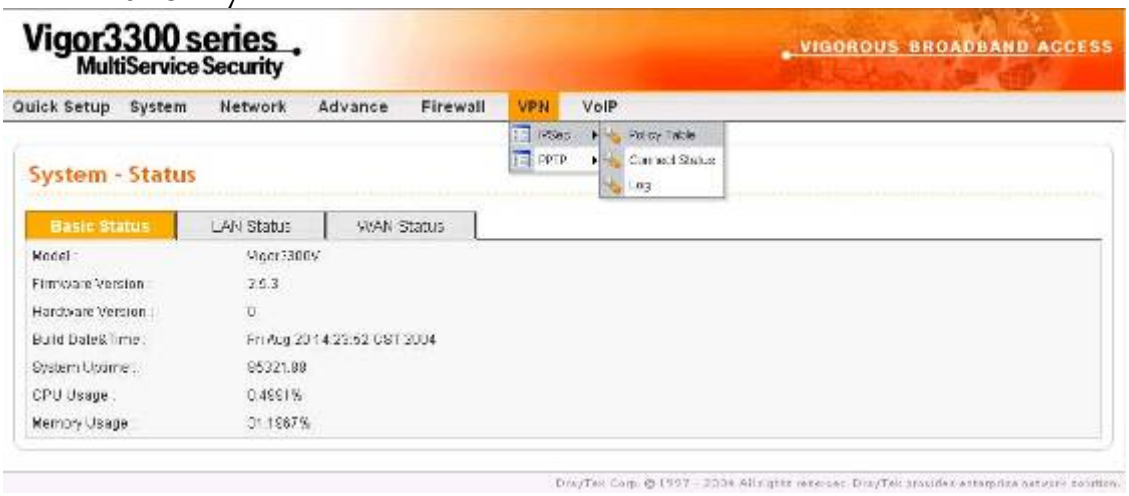
IPSec ip ağları için güvenlik mimarisidir. IPSec sistemin gereken protokolleri seçmesi servisler için kullanılacak algoritmaların belirlenmesi, ve istenilen servisleri sağlaması için kriptolanmış anahtarları aktive ederek ip katmanda güvenlik servisi sağlar. IPSec host arasındaki bir veya daha fazla yolu korumak için kullanılabilir, iki güvenlik ağ geçidi arasında veya ağ geçidi ve host arasında. IPSec erişim kontrolü connectionless integrity(bağlantısız bütünlük), veri orjinli, tekrarlanan paketlerin reddedilmesi, ve güvenlik(kodlama) sağlar. Bu hedefler iki trafik güvenlik protokolünün kullanılmasıyla sağlanır: Authentication Header (AH-kimlik doğrulama başlığı), Encapsulating Security Payload (ESP-sarma güvenlik yükü) .Kriptolanmış anahtar yönetim prosedür ve protokolleri kullanılarakyapılır.

Vigor3300 serisi anahtar yönetimi için IKE kullanarak ESP tünel modunu destekler. Internet Key Exchange (IKE-internet anahtar değişim) Protocol, ISAKMP ile birlikte kullanmak için Oakley in ve SKEME nin parçalarını ISAKMP ile konjuge olarak kullanan IPSec içindeki hibrit bir anahtar protokolüdür ve diğer AH veESP gibi güvenlik işbirlikleri için Ipsec DOI.



8.2 IPSec Grup Ayarı

8.2.1 Kural Tablosu Ayarları



VPN IPSec kuralı yaratmak için , **VPN ->IPSec->Policy Table** a tıklayın.

Yeni IPSec tüneli yaratmak için add e tıklayın.

Temel

Name –VPN bağlantısı için insanın okuyabileceği isimdir. Örneğin: "VPN1". Tüm VPN kuraları için tek lmalıdır ve beyaz karakter içeremez. Maksimum 20 karakter uzunluğunda olabilir.

PreShared Key –çift tanımı için paylaşılan bir anahtar. Boşluk karakteri içeremez ve en fazla 40 karakter uzunluğunda olmalıdır.

Security Protocol –şu anki versiyonlarda sadece ESP desteklenir.. ESP verisi kodlanacak ve kimlik denetimi yapılacaktır. Bunda NULL, DES, 3DES ve AES kodlama modları desteklenir.

Admin Status –yönetim durumudur. **Enable** seçilirse kural aktiftir ve çiftin IKE müzakeresini başlatmasını ve log mesajınıgöstermesini bekler. Eğer **Disable** seçildiyse VPN bağlantısı aktive olmaz. **Always-on** VPN bağlantısını otomatik larak aktive etmek için kullanılır.

Local Gateway (yük ağ geçidi)

WAN Interface - WAN interfacelerinden birini seçin.

IP Address –yerel ağ geçidinin genel network interfaceinin ip adresi. Aynı zamanda anahtarı varsayılan router interface adresini belirtmek için tanımlayabilirsiniz.

Subnet –lokal ağ geçidi arkasındaki alt ağdır. Varsayılan değeri 192.168.1.0/24tür.

Next Hop –sonraki sıçramanın ip adresidir. Aynı zamanda anahtarı varsayılan route interfaceinin sonraki sıçrama adresini göstermesi için varsayılan değerini tanımlayabilirsiniz.

Remote Gateway(uzak ağ geçidi)

IP Address **–**uzak istemci/ağ geçidi ip adresini belirtir. Bu alan zorunludur.0.0.0.0 ayarı dinamik atanmış ip adresi olan road-warrior için kullanılır.

Subnet **–**uzak ağ geçidinin arkasındaki alt ağdır, ayarı örneğin 192.158.2.0/24. Eğer uzak ağ geçidi ip adresi 0.0.0.0 ise, bu alan göz ardı edilebilir. Fakat bunu netlik için 0.0.0.0/32 olarak ayarlayın.

Daha ileri seçenekleri görüntülemek veya onları varsayılan değerlerinde bırakmak için Advanced a tıklayın.
IKE Phase1 group (ana mod)
Key Lifetime(anahtar yaşam süresi) –alan bağlantının IKE Phase1 anahtarının yeniden müzakere edilmeden ne kadar kalacağını belirtir. Kabul edilebilir aralık 5 den 480 dakkaya kadardır.
Proposal - proposed IKE Phase 1 müzakeresi için kriptolama ve/veya kimlik doğrulama. İzinverilebilir değerler aşağıdaki kombinasyondan gelmektedir

Encryption algorithms(kriptolama algoritmaları) **–**algoritma DES/3DES/AES olabilir.

Authentication algorithms(kimlik doğrulama algoritmaları) **-** MD5/SHA1 olabilir.

DH Group **(DH grubu)-** MODP768/MODP1024/MODP1536 olabilir.

IKE Phase 2(hızlı mod)

Key Lifetime**(anahtar yaşam süresi)-** bağlantının IKE Phase2 anahtar kanalının yeniden müzakere edilmeden önce ne kadar yaşayabileceğini gösterir. Kabul edilebilir oran 5 den 1440 dakkaya kadardır.

Proposal **–** IKE Phase 2 için kriptolama ve/veya kimlik doğrulam algoritmaları. Ayar aşağıdaki kombinasyona dayanmaktadır.

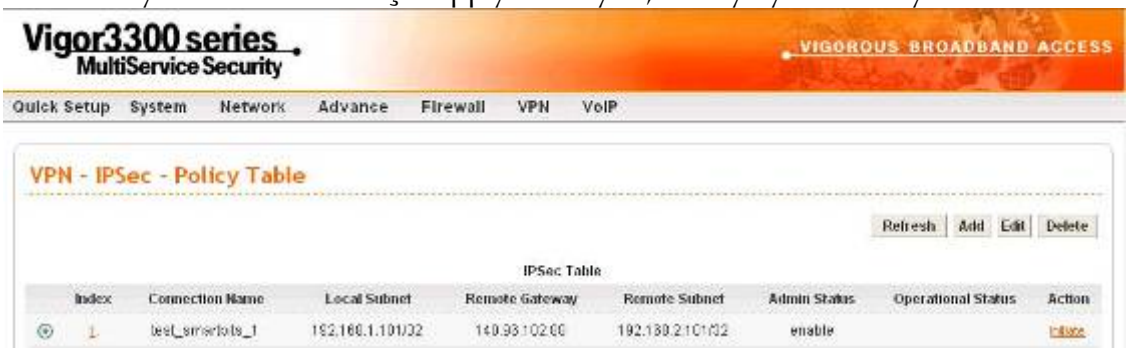
Encryption algorithms(kriptolama algoritmaları) **–**NULL/DES/3DES/AES olabilir.

Ölü Çift Belirleme Grubu

Delay(gecikme) **–**hayatta kalma zamanlayıcısıdır. Tünel boştayken periyodik bir hello mesajı iletilir. 0 değeri sistemi devre dışı bırakır. Eğer aktive edilmişse önerilen değer 30 saniyedir.

Timeout(zaman aşımı) **–**zaman aşımı zamanlayıcısıdır. Zaman aşımı değerinden sonra bilgi mesajı gelmezse çift öle olarak işaretlenir. 0 değeri sistemi devre dışı brakacaktı. Aktive için önerilen değer 120 saniyedir.

IPSec kural ayarlarını bitirmek için apply a tıklayın , tabloya yeni bir kayıt eklenecektir.



IPSec tablosundaki girişi değiştirmek için edite tıklayın.

IPSec Tablosundaki girişi kaldırmak için delete e tıklayın.

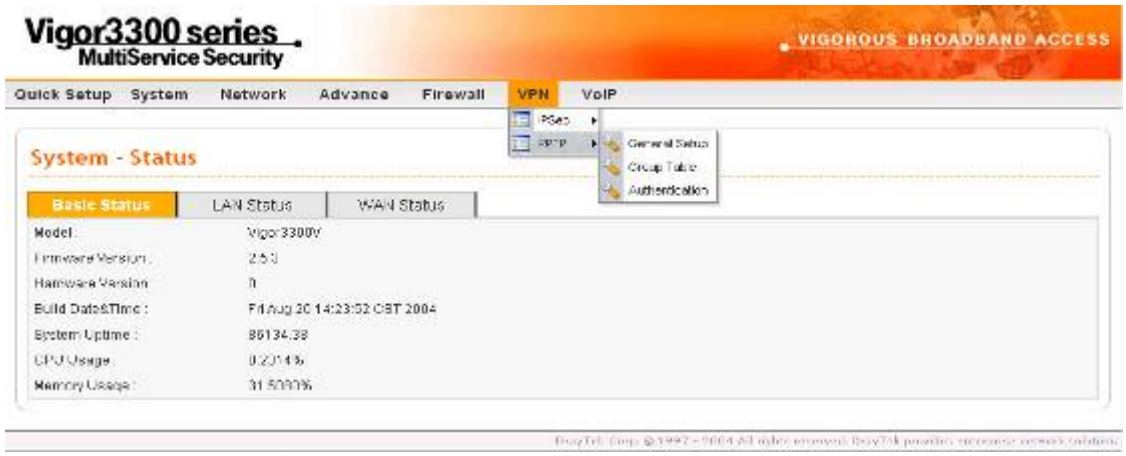
Önemli alanlar IPSec Tablosunda özetlenecektir. **Operational Status** alanı tünelin o anki statüsünü yansıtır. "up" değeri IPSec tuneli kurulmuş demektir, "down" değeri tünel olmadığını gösterir ve diğerleri tünelin özel statülerini yansıtır.

Yerel ağ geçidinin IKE belirteci olarak davranmasını istiyorsanız, örneğin ana mod mesajında ilk IKE değerini yay ; **Initiate** hiperlinkine IKE müzakeresini başlatmak için tıklayabilirsiniz. Müzakere sırasında tabloların son durumunu görmek için **Refresh** e basabilirsiniz. Eğer operasyon durumu birkaç dakkalığına "down" kalırsa yeniden denemek için **Initiate** e basabilirsiniz..
Connect Status e basınca aşağıdaki pencere açılacaktır.

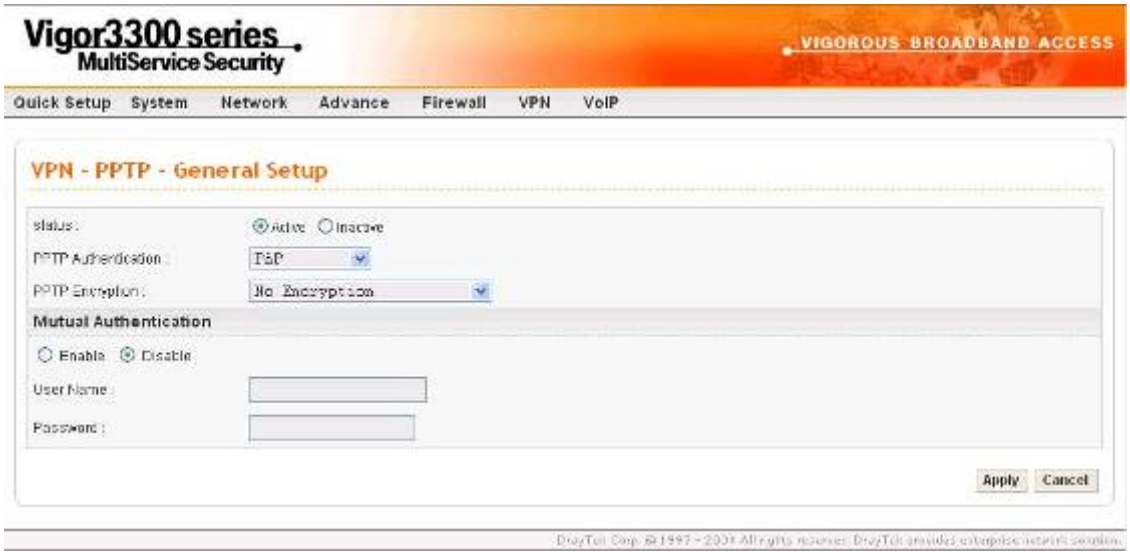
Herhangi bir anda VPN tünel statülerini görmek için **VPN > Log** e tıklayın. Kullanıcıya bağzı ayarlama problemlerinin çözümü için yeterli bilgi sağlar. Şu anki versiyonlarda, sistem en son 100 mesajı tutar. Mesajları temizlemek için clear a basabilirsiniz.

8.3 PPTP Grup Ayarı
8.3.1 Genel Ayarlar

Vigor3300 serisi VPN seçeneğinin içindeki PPTP konfigürasyonunu destekler.



VPN -> PPTP->General Setup e tıklarsanız aşağıdaki sayfa görüntülenecektir.



Status **–**fonksiyonu aktive etmek için "Active" i seçin.
PPTP Authentication(PPP kimlik doğrulama) **–**kullanıcı 4 kimlik doğrulama modundan birini seçebilir..
PPTP Encryption **(PPTP kriptolama)-**kullanıcı 3 kimlik doğrulama modundan birini seçebilir.

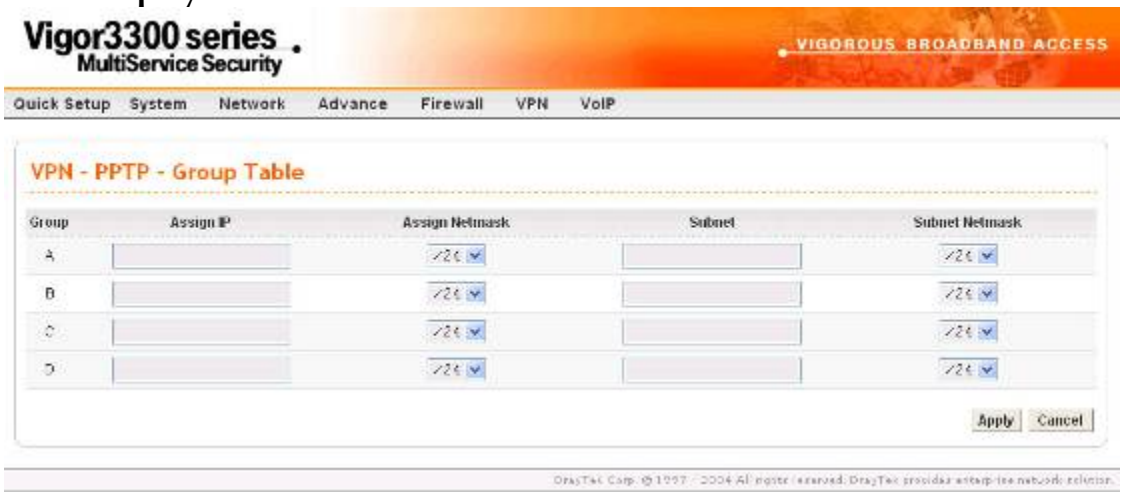
Karşılıklı Kimlik Doğrulama

Bu fonksiyon için Enable(aktive) veya Disable(devre dışı) tıklayın.

User Name(kullanıcı adı) – özel bir kullanıcı adı atayın..

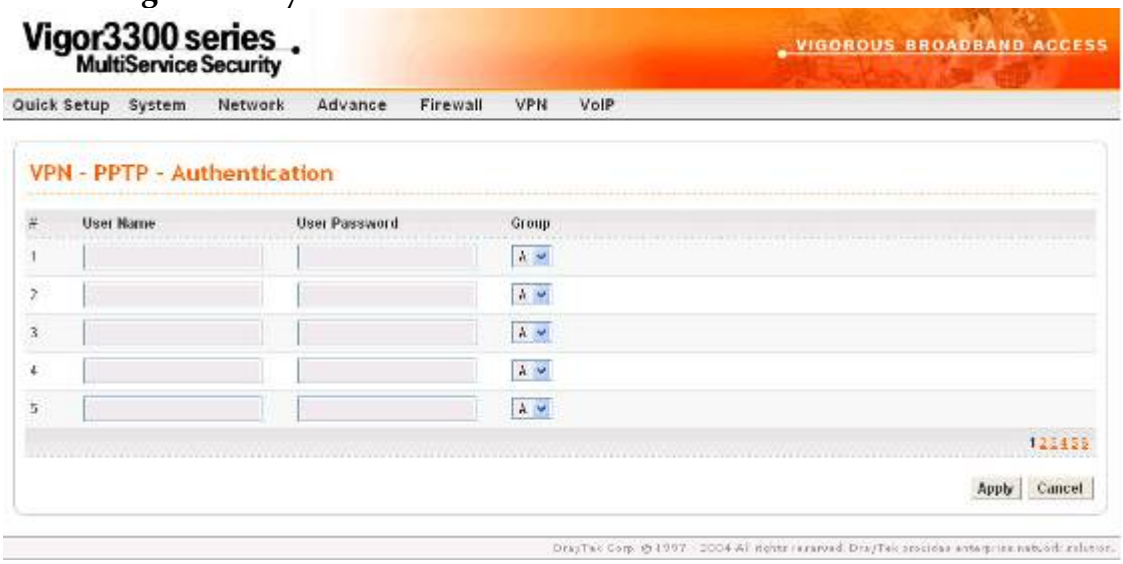
Password(şifre) – kullanıcının şifresini atayın.

8.3.2 Grup Ayarı



Kullanıcı Assign IP, Assign Netmask, Subnet ve Subnet Netmask ı 4 grupta atayabilir.

8.3.3 Kimlik Doğrulama Ayarı

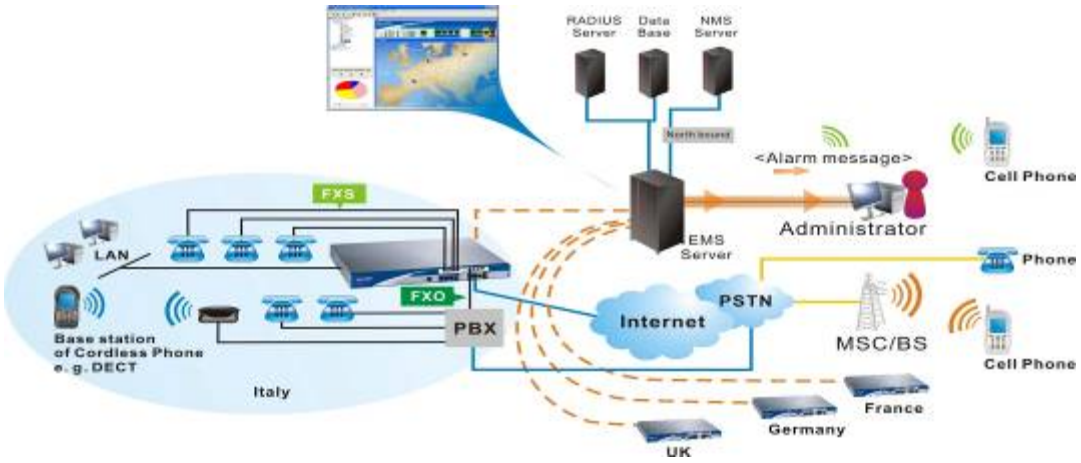


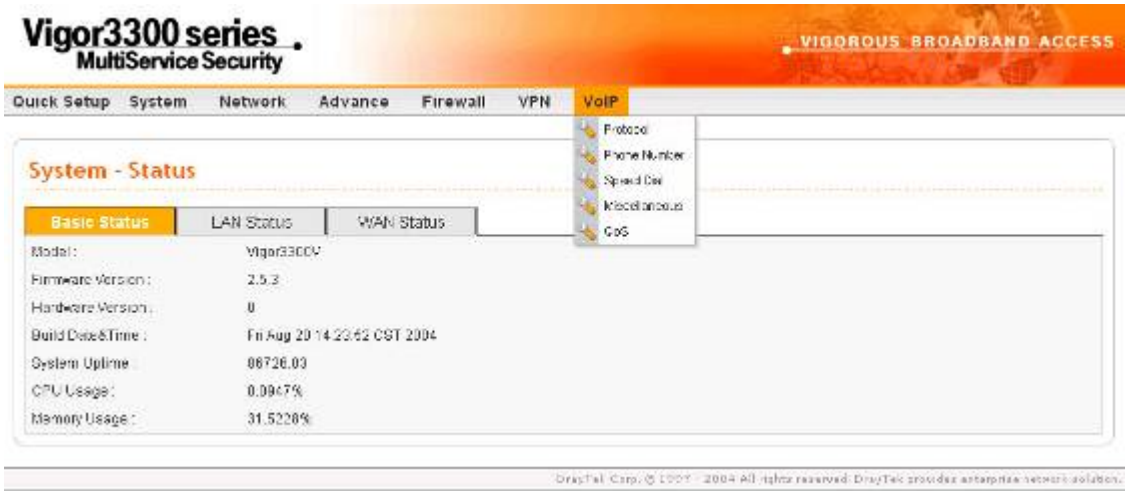
Vigor3300 serisi PPTP tablosuna en fazla 30 giriş yapılmasını destekler.

BÖLÜM:9
VoIP Ayarı

9.1 Giriş

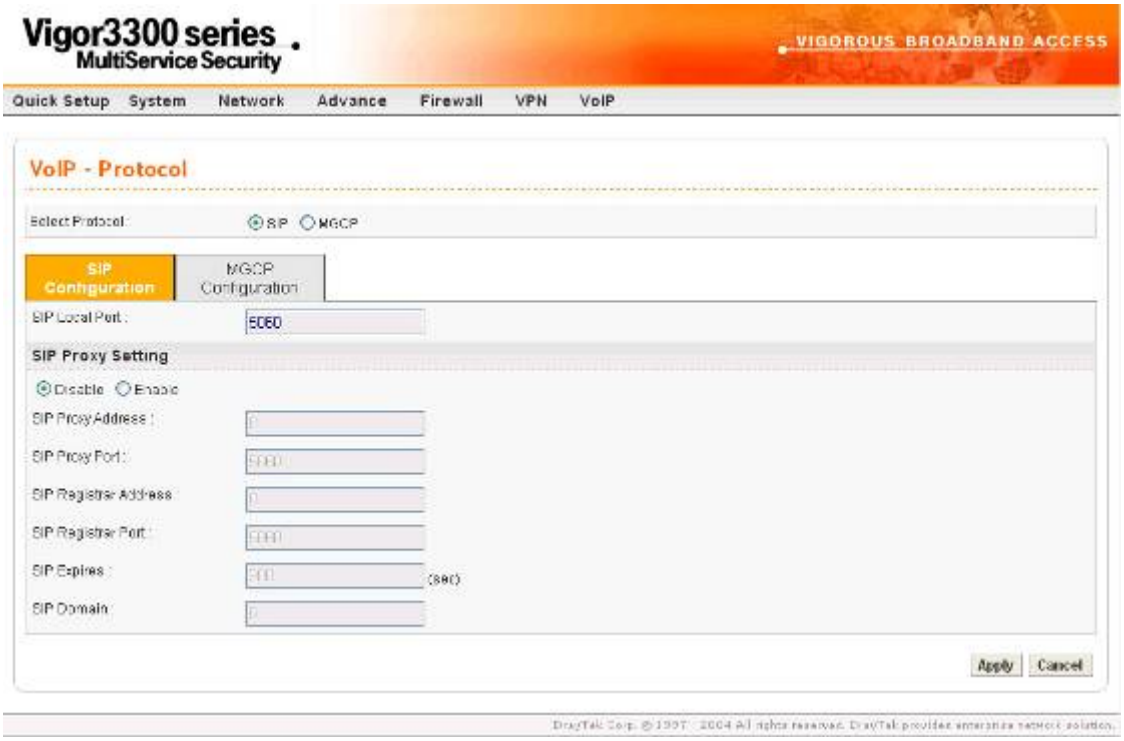
Voice over Internet Protocol (VoIP-internet protokolü üzerinden ses) düzenli (veya analog) telefon hattı yerine broadband internet bağlantısını kullanarak telefon görüşmesi yapmanızı sağlayan bir teknolojidir. Vigor3300 SME müşterileri için karlı ses seçenekleri sunmaktadır. Modül dizaynı seçmeli 4 veya 8 port FXS veya FXO olmalıdır. İkinci grup karlı ses çözümü için PABX e bağlanabilir. Hunt(av) grup özelliğiyle müşteri şirketi vigor3300la tek bir numarayla arayabilir. Vigor3300 EMS (Element Management System) ile birleşerek headquarter tarafından merkezi olarak yönetilebilir.





9.2 VoIP Protokol Ayarı

VoIP protokol ayarına tıklarsanız aşağıdaki sayfa görüntülenecektir:



Voip de iki protokol vardır. Bunlar: **SIP** ve **MGCP**.

Select Protocol(protokol seçin) **-**kullanıcılar **SIP** ve **MGCP** den birini seçebilirler. Varsayılan **SIP** dir.

9.2.1 SIP Konfigürasyonu

***SIP Local Port* – yerel SIP terminaline bir ip adresi atayın.**

SIP Proxy Ayarları

SIP Proxy Address –SIP proxy sunucusuna bir ip adresi atayın. .

SIP Proxy Port –SIP proxy sunucusuna bir port numarası atayın.

SIP Proxy Register Address –SIP register sunucusuna bir ip adresi atayın.

SIP Proxy Register Port – SIP register sunucusuna bir port numarası atayın.

SIP Expires –SIP protokolüne bir zaman aşımı değeri atayın.

SIP Domain –SIP alanına bir ip atayın.

Ayarları bitirmek için **Apply** a tıklayın.

9.2.2 MGCP Konfigürasyonu

MGCP Local Port –MGCP yerel terminalinde bir UDP port numarası atayın.

MGCP Call Agent Address – MGCP içindeki arama acentası sunucusuna bir ip adresi atayın.

MGCP Call Agent Port –Arama acentası sunucusuna bir UDP port numarası atayın.

EndPoint Name Style(bitiş noktası isim stili) –3 seçenek vardır:

aaln/#@[ip_addr]

mac_addr/#@[ip_addr]

aaln/#@mac_addr

Wild-carded RSVP –2 seçenek vardır:

her bitiş noktası kendi RSVP sini yollar

sadece bir RSVP yollar.

9.3 VoIP Telefon Numarası Ayarı

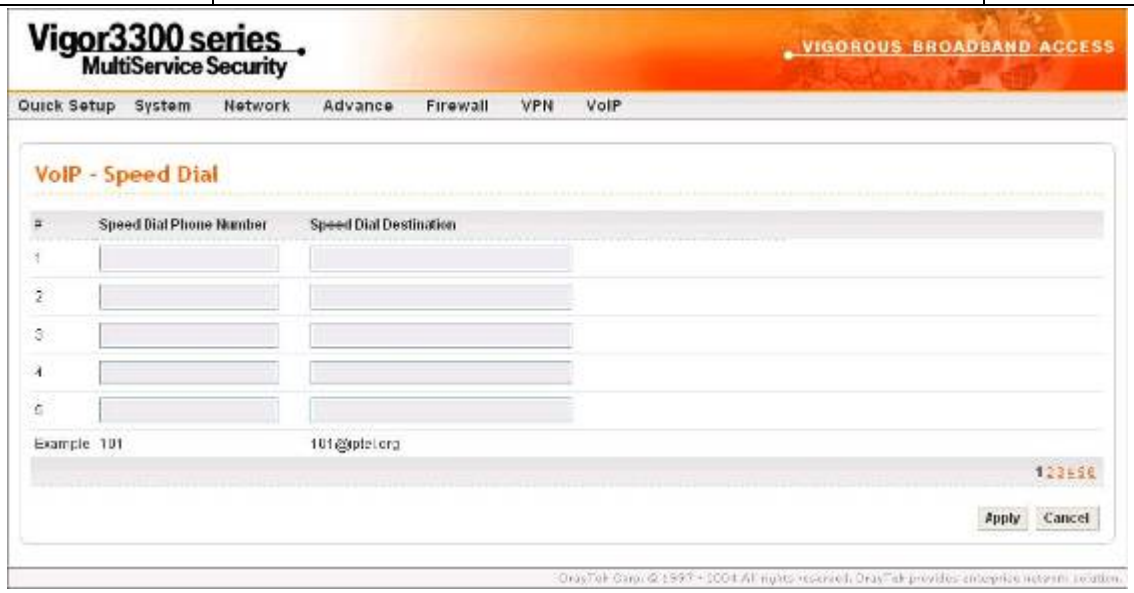
VoIP -> Phone Number a tıklarsanız aşağıdaki pencere gelecektir.

Hunt Group(av grubu) **–**ses servisi için şirkete hunt group sağlanması çok önemlidir. Kullanıcılar aynı zamanda aynı telefon numarasını arayabilir, ve Vigor3300 ses servisini sağlamak için ulaşılabilir telefonu otomatik olarak bulacaktır. Bir şirketle ilgili bir telefon numarasının hatırlanması kullanıcıya bir faydadır. Bu fonksiyonu aktive ederek, 4 veya 8 port VoIP tablodaki ilk girişi onların telefon numarası olarak kullanacaktır.
Active **–**kullanıcı bu telefon hattını **Enable** veya **Disable** edebilir.
Username **–**her telefon hattı için bir kullanıcı adı atayın.
Password –her telefon hattı için bir şifre atayın.
Display Name –diğer telefon terminalinde görünecek arayan adı atayın.
Ayarları bitirmek için apply a tıklayın.

9.4 VoIP Hızlı Arama Ayarı

Hızlı arama özelliği Vigor 3300kullanıcılarına bağzı özel müşterileri aramak için kolay bir yol sunar. Vigor 3300 en fazla 30 girişe izin verir.

VoIP -> Speed Dial a tıklarsanız aşağıdaki sayfa gelecektir.



Speed Dial Phone Number(hızlı arama telefon numarası) **–**bir arama numarası atayın.

Speed Dial Destination(hızlı arama hedefi) **–**Arma hedefine bir adres atayın.

Ayarları bitirmek için apply a tıklayın.

9.5 VoIP Çeşitli Ayarlar

Çeşiti ibaresi **Codec**, **CAS** ve **Advance** ayar parametrelerini içerir. **VoIP Miscellaneous** a tıklandığında aşağıdaki sayfa görüntülenir.

Codec(kodek)

Codec Prefer **–**VoIP iletimi için bir sıkıştırma modu seçin.

Codec Rate(kodek oranı) **–**VoIP fonksiyonunda bir oran değeri seçin.

Codec VAD –VAD (Voice Activity Detection-ses aktivite bulunması) fonksiyonu aktive edin veya devra dışı bırakın.

CAS

Country – uygulanacak bir ülke veya alan seçin.

Rx Gain –Rx fonksiyonu için bir kazanç değeri atayın.

Tx Gain –Tx fonksiyonu için bir kazanç değeri atayın.

Advance

Debug level –debug kullanımı için bir seviye seçeneği seçin.

RTP Port – RTP protokol paketi içinde bir port numarası atayın.

RTP TOS –RTP protokol paketi içine bir TOS değeri atayın.

RTP RFC2833 –RFC2833 fonksiyonunu aktive edin yada devre dışı bırakın.

Ayarları bitirmek için apply a tıklayın.

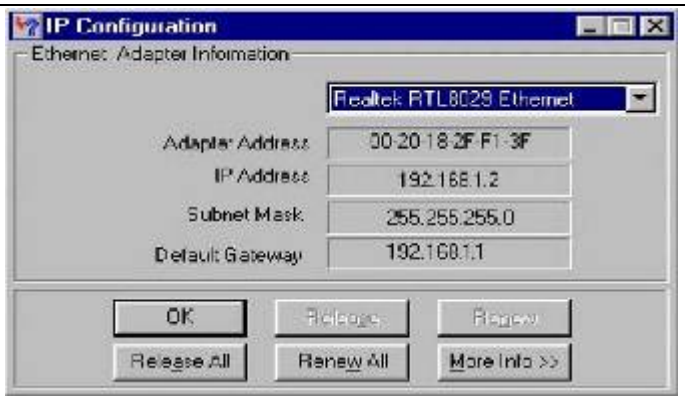
Ek A

PC Web Tarayıcısı Ayarı

Bu bölüm Vigor3300 konfigürasyonu için PC ayarını anlatmaktadır. Ayar ibareleri Vigor3300 la iletişim kurması için PC ip ayarlarını içermektedir.

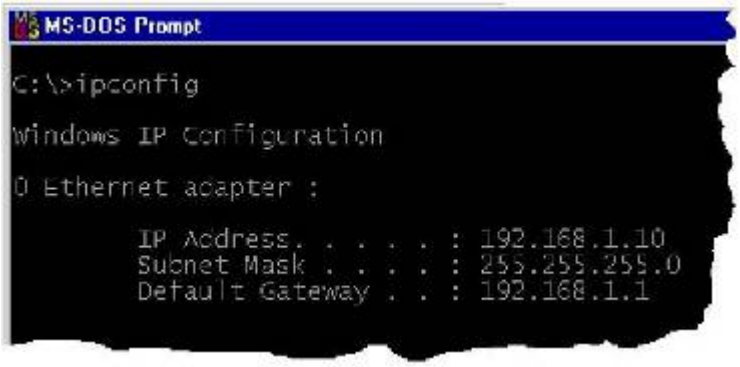
Kısım1- Vigor 3300 ile PCs/LAN iletişimi

1. PC niz router a uygun ethernet kablosuyla(RJ45)bağlanmış olmalıdır. Sonra ilgili Ethernet switch LED (1/2/3/4) leri yanacaktır (yeşil = 100Mbps, kehribar = 10Mbps). Vigor3300 un Ethernet portları hızı ve kablo konfigürasyonunu otomatik oalrak algılamaktadır. Otomatik olarak crossover/straight veya uplink/normal bağlantı olabilir.
2. ağınızdaki her cihazın tek bir eşsiz bir ip adresi olmalıdır. DHCP sunucusu buna uygun ipleri otomatik olarak verecektir. Vigor 3300 ün varsayılan ip adresi 192.168.1.1 dir ve tüm yerel Pcler aynı alt ağda birer ipye sahip olamlıdırlar. örneğin 192.168.1.10 veya 192.168.1.254.
3. PC nin ip detaylarını gerçekten Vigor 3300den aldığını winipcfg den test edin. Çalıştırmak için: Windows başlangıç-çalıştır-winipcfg ve tamama basın.
4.



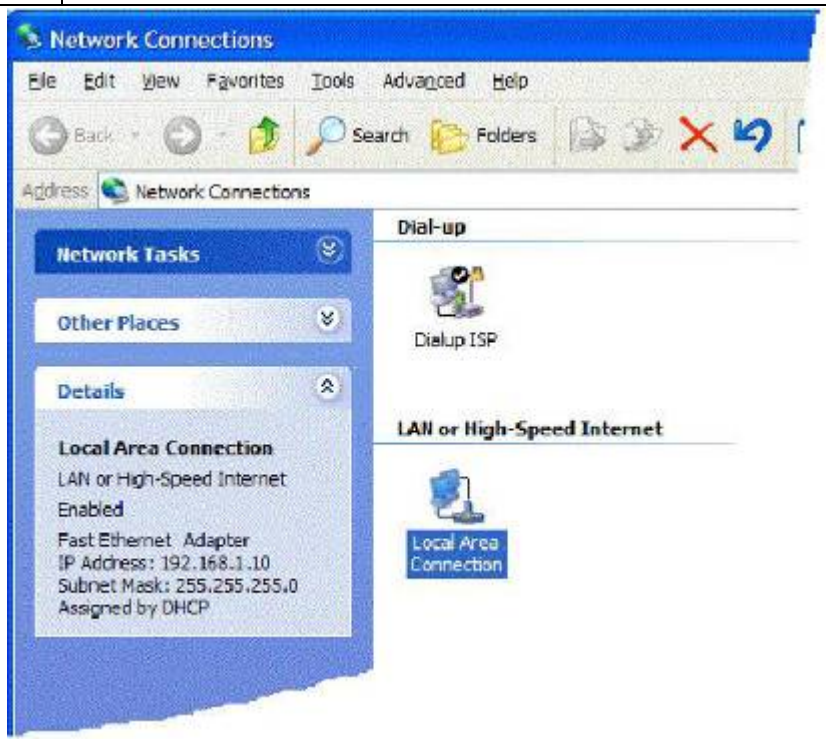
yukarıdaki örnekte Pcye 192.168.1.2 ip adresi verimiştir ve varsayılan ağ geçidi(router) 192.168.1.1dir. yukarıdaki pulldown kutudan ağ kartınızın seçildiğinden emin olun. 'Release' detayları temizler, 'Renew' yeniden alır.

winipcfg yoksa MS_DOS komut satırından **ipconfig.exe** yi deneyebilirsiniz.



Winipcfg Windows 2000 de standart olarak desteklenmez.

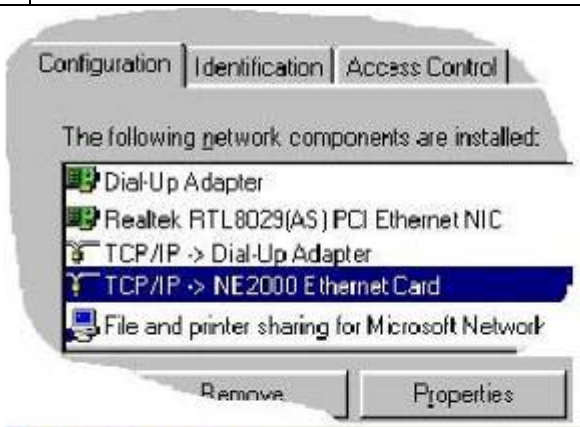
5. **Windows XP** de , PC'nizin şu anki ip adresini ağ bağlantılarını açarak kontrol edebilirsiniz. LAN bağlantılarını seçerseniz ayarlar aşağıda gösterildiği gibi ekranın solunda gelecektir. Burdan ağ bağlantısının aktive ediliğini ve ip adresinin 192.168.1.10 olduğunu görebiliyoruz.



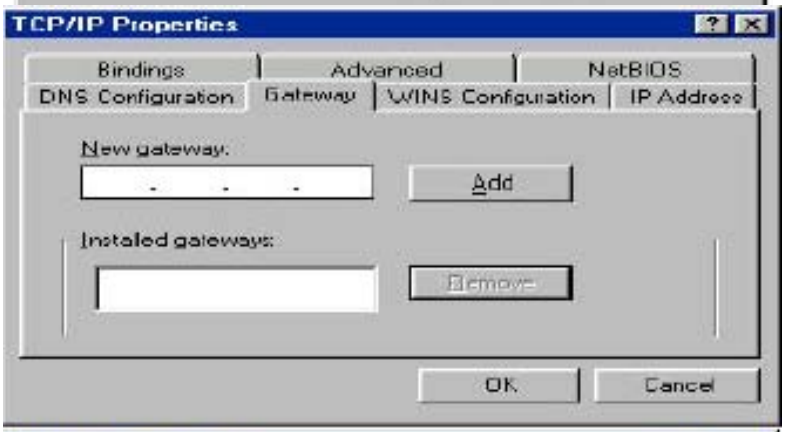
Ağ bağlantıları ikonuna sağ tıklayıp statüleri seçerek de aynı işi yapabilirsiniz.

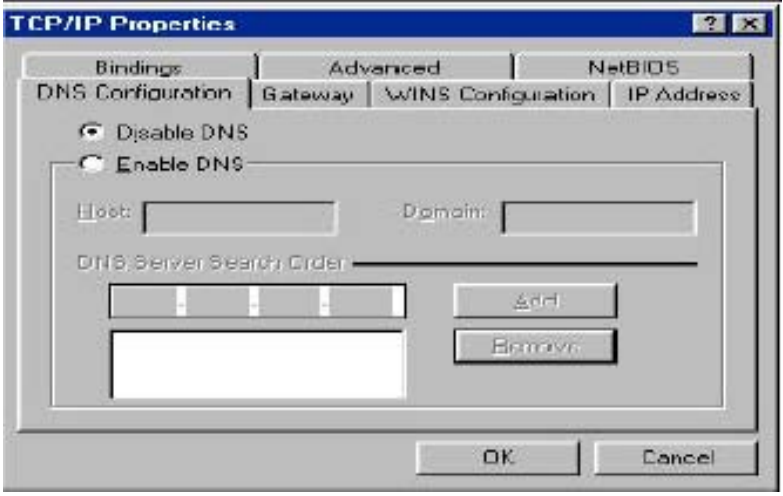
6.Eğer PC niz ip adresi almıyorsa TCP/IP ayarlarının doğru olduğunu kontrol etmeniz gerekir. Routerın DHCP fonksiyonunu kullandığını daha önce belirtmiştik. Windows98/Me Control Panel/Network, check your TCP/IP Properties den varsayılan olarak aktive edildiğini kontrol edin.

1. 7. **Windows XP** için LAN/Network kart ayarı Windows98/Me ye çok benzerdir fakat ekranlar biraz değişik görünür. Ağ kartınız bir kere yüklendiken sonra varsayılan olarak otomatik ayarlanır. Pcnizin ağ bağlantıları menüsünden ayarları doğrulayabilirsiniz.


Configuration
Identification
Access Control
The following network components are installed:
Dial-Up Adapter
Realtek RTL8029(AS) PCI Ethernet NIC
TCP/IP -> Dial-Up Adapter
TCP/IP -> NE2000 Ethernet Card
File and printer sharing for Microsoft Network
Remove
Properties

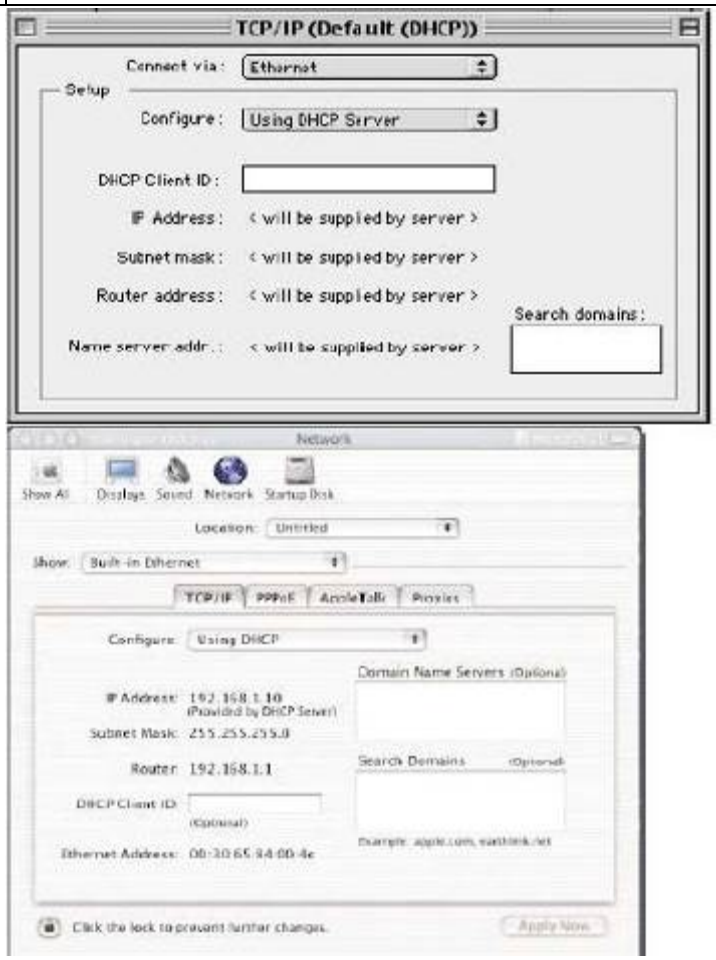

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
New gateway:
Add
Installed gateways:
Remove
OK
Cancel


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
Disable DNS
Enable DNS
Host:
Domain:
DNS Server Search Order
Add
Remove
OK
Cancel

Gösterildiği gibi TCP/IP protokolünü seçin ve özelliklere tıklayın ve ardından onu doğrulayın. Otomatik ip ve DNS alma seçilmiştir:

7. **Apple MacOS** için DHCP seçmek için, the TCP/IP kontrol paneli MacOS 8/9 and X için şunun gibi seçilmelidir:



Vigor 3300 tarafından ip adresleri bir kere atanırsa , yukarıdaki ekranda görülecektir.

8. DHCP kullanmıyorsanız o zaman Pcnize elinizle ip vermelisiniz.Bu adres routerın kendi LAN ip adresiyle aynı alt ağda olmalıdır. Eğer router 192.168.1.1 ise, diğer PCler 192.168.1.nnn değerine ayarlanmalıdır. 'nnn' 2 – 254 arası bir sayıdır. Ek olarak her PCnin 'Default Gateway' ve"DNS Server Address" olarak routerın IP adres (192.168.1.1 değiştirilmediyse.) verilmelidir. DHCP kullanıyorsanız bunların hiç birine gerek yoktur

9. Pcniz ile router arasındaki bağlantıyı test etmek için Windows 'ping' komutunu kullanın. Bu routerın geri göndereceği küçük paketler göndererek bağlantıyı test eder. MS-DOS komut satırından 'ping 19.168.1.1' girilirse milisaniyeler cinsinden cevap alınması gerekir.

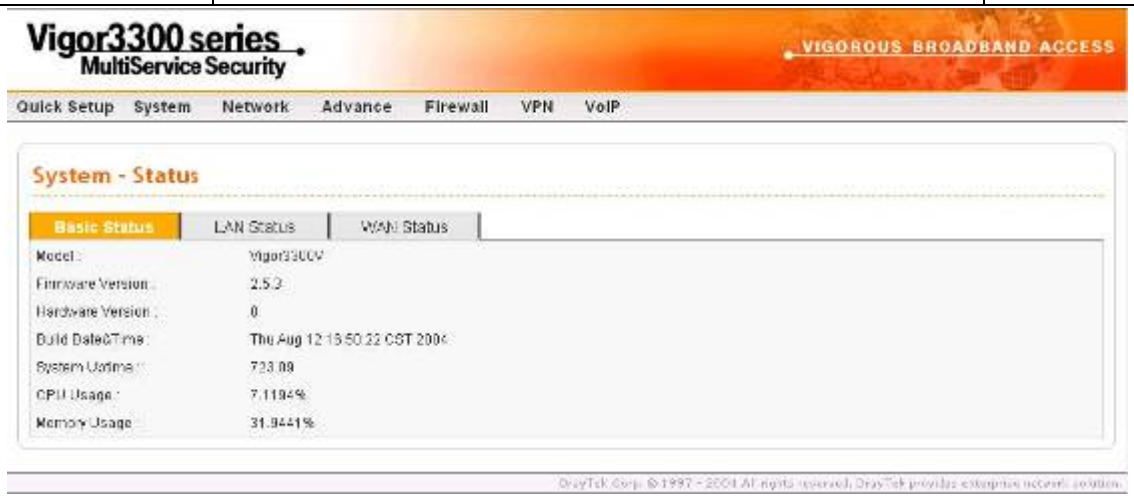
Kısım2-Web Tarayıcı Versiyonunuzu Ayarlamak

10. yukardaki doğrulamalar Pcnizin Vigor3300a konfigürasyon arayüzüne erişebilmeniz için doğru bağlandığını doğrulamak içindi. Bu routerı ayarlamak, kontrol etmek ve görüntülemek için ana metotdur. Güncellenmiş web tarayıcınızı yükleyin. (IE 6.0 veya Netscape 7.1 tercih edilir). www.microsoft.com **-resources-downloads** kısmından edinebilirsiniz. **Search for a Download** on **Product/ Technology** alanı **Internet Explore** yazılımını bulur. En yeni versiyonu bulup güncelleyebilirsiniz.

11. Bara basın ve http://192.168.1.1 olan Vigor 3300 ipsini girin.

Kullanıcı adı ve şifreyi girin. Fabrika varsayılanı kullanıcı adı: "Draytek"ve şifresi "1234"dir. Daha sonra ok e basın, aşağıdaki gibi login mesajı gelecektir

Daha sonra aşağıdaki gibi ana menü görünmelidir.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advance
Firewall
VPN
VoIP
System - Status
Basic Status
LAN Status
WAN Status
Model :
Vigor3300V
Firmware Version :
2.5.2
Hardware Version :
0
Build Date&Time :
Thu Aug 12 15:50:22 CST 200
System Uptime :
723:09
CPU Usage :
7.1194%
Memory Usage :
31.9441%

YETKİLİ SERVİSLER

SIRA NO	UNVAN	HİZMET YERİ ADRESİ	YETKİLİNİN ADI SOYADI	TEL/FAKS	VERGİ NO
1	SİMET BİL.HAB.ELEK.REK.TUR.GID.OTO.İNŞ.TEKS EML.TEM.MED.MÜH.GÜV.SİS.ORG.NAK.SAN.LTD.	ÇETİN EMEÇ BULVARI 8.CAD. 84.SK.3/1 A.ÖVEÇLER/ANKARA	SİBEL BEDİR RENKMEN	312-472 87 87 312-472 31 31	7700072424
2	BETİM BİLGİSAYAR EĞİTİM TİC.SAN.VE İNŞ.LTD.ŞTİ.	İSTEMİYE MAH.TURGUT TEMELLİ CAD EREN İŞ MERK. KAT:1 N:4 MALATYA	EMİNE YILDIRIM	422-326 01 73 422-323 67 40	1670070120
3	ASBİMSAN ELEKTRONİK BİLGİSAYAR SAN.TİC.LTD.ŞTİ	CİNNAH CAD.NO:61/1-3 ÇANKAYA/ANKARA	AHMET SITKI YAZICIOĞLU	312-441 64 55 312-441 73 33	0860039811
4	ÇÖZÜMEVİ ELEKTRONİK MEDİKAL BİLİŞİM KIRTASİYE İNŞ.GIDA SAN TİC.LTD.ŞTİ	KONUR SOKAK NO:63/5 BAKANLIKLAR-ÇANKAYA/ANKARA	NESİMİ KEÇELİOĞLU	312-419 46 15 312-419 46 17	2630285720
5	ATM BİLGİSAYAR YAZ.DON.ELEKT.İLETİŞİM VE DAN.HİZ.TİC.LTD.ŞTİ	BOĞAZ SOKAK NO:27/1 GOP/ANKARA	ABDULLAH TANSEL GEZMİŞ	312-4661476 312-4686198	1030059918
6	DEMİREZEN BİLGİSAYAR VE OTO SANAYİ TİC.LTD.ŞTİ	GAZİ MUHTARPAŞA BUL. 4.CAD SAİT SAYIN İŞ MERK ALTI NO:13 GAZİANTEP	MEHMET BULUT	242-3450911 242-3353047	2730039264
7	BÜKOM BÜRO MAKİNALARI PAZ. SAN. VE TİC A.Ş.	HALK SOKAK NO:22/1 KIZILAY / ANKARA	LEVENT SARUHAN	312-433 62 29 312-433 35 06	1920003238
8	VİZYON ELEKT.BİLİŞİM SİSTEMLERİ VE DANIŞ.SANAYİ TİCARETLTD.ŞTİ.	KOCATEPE OLGUNLAR SOK.NO:36/4 ÇANKAYA/ANKARA	AHMET BAL ALİ BAL	312-419 94 51 312-419 83 96	9250142774
9	URFANET MUHAMMET TAŞÇILAR	BAHÇELİEVLER MAH.4.SOK TAŞÇILAR APT.ALTI NO:27 ŞANLIURFA	MUHAMMET TAŞÇILAR	414-316 36 69 414-312 17 42	8260112093
10	ARNİL-NET BİLGİSYAR İLETİŞİM HZM YAZ.TURZ.SAN.TİC.LTD.ŞTİ	İMÖNÜ CAD.HÜZMEN PLAZA A BLOK NO:29/A OSMANGAZİ	SERKAN AKSOY	224-224 91 63 224-223 58 60	800048520
11	NİSAN BİLGİSAYAR LTD.ŞTİ.	MAREŞAL FEVZİ ÇAKMAK MAH. NO:16/C-16 BEŞEVLER / ANKARA	RAHMİ ŞİMŞEK	312-212 96 96 312-223 57 57	6310050405
12	ŞAHİNOĞLU BİLGİSAYAR İLETİŞİM SİSTEMLERİ KIRTASİYE SAN.VE TİC.LTD.ŞTİ	TABAKLAR MAH.AKBABA SOKAK NO:2 BOLU	TURGAY ŞAHİNOĞLU	374-212 70 86 374-217 30 49	7980462223
13	ÇİZGİ BİLG..TAN. HİZ. TİC. LTD. ŞTİ.	REŞATBEY MAH. FUZULİ CAD. EROĞLU APT. ZEMİNKAT 37/A SEYHAN/ADANA	MEHMET ALİ ALTUN	322-4577507 322-4578948	742032419
14	SHOV BİLGİSAYAR TAN.HİZ.TUR.TİC.LTD.ŞTİ.	STRAZBURG CAD.NO:40/A SIHHIYE/ANKARA	LEVİN FİGEN OKUMUŞ	312-229 87 92 312-230 20 13	7690008054
15	PROBİLİŞİM BİLGİSAYAR VE İLETİŞİM SİSTEMLERİ TİC.LTD.ŞTİ.	ÇETİN EMEÇ BULVARI 1325.SOKAK NO:10/3 A.ÖVEÇLER/ANKARA	MUSA ELMALI	312-4733585 312-4733565	8590500880
16	BİRCAN BİLGİSAYAR İNŞ.SAN.TİC.LTD.ŞTİ.	KİRİŞÇİ MAH. ŞEHİT ZAFER AK CAD. NO:4 KARAMAN	BAYRAM BİRCAN	338-2132222 338-2149382	1770052623
17	ATLANTİS BİLGİSAYAR –NEVRES SARIZ	BANKALAR CAD. 3.PARK SOK. DEVECİ İŞ MERKEZİ KAT:2 NO:38 SİVAS	NEVRES SARIZ	346-2231429 346-2220966	14729305438
18	ÖZKAN ALTAY BİLGİSAYAR ELEKTRONİK İNŞAAT VE GIDA SAN.TİC.LTD.ŞTİ.	VATAN MAH.POLAT CAD. NO:74/A YEŞİLYURT/İZMİR	ÖZKAN ALTAY	232-2452323 232-2453836	7340129856
19	PROBİL BİLGİSAYAR VE PROG.SAN.TİC.LTD.ŞTİ	ŞARKİYE MAH. KAZIM KARABEKİR CAD. NO:13 ORDU	ERCAN ÖKTENAY	452-2251920 452-2251921	7330032316
20	AHMET AYDIN-BİLGİSAYAR HASTANESİ	NUSRATİYE MAH. 119.CAD. NO:117/A MERSİN	AHMET AYDIN	324-3365559	11534346816
21	BİLGİ TEKNOLOJİLERİ BİLGİSAYAR İNTERNET VE YAZILIM HİZMETLERİ SAN.TİC.LTD.ŞTİ.	ÖVEÇLER 1.CADDE 14/A ÇANKAYA/ANKARA	EMRE YILDIRIM	312-4784446	1720116541