Linux Yaz Kampı 2012
pfSense 2.0 Eğitimi

Çağrı Ersen
cagri.ersen@gmail.com
http://www.syslogs.org

Eğitim Hakkında

Bu eğitim pfSense 2.0 kurulumu/yapılandırması, network trafiğinin yönlendirilmesi ve filtrelenmesi, DHCP, DNS, VPN gibi temel network servislerinin çalıştırılması gibi konuların işleneceği bir eğitimdir.

Katılımcıların networking konusunda temel seviyede bilgili oldukları varsayılmaktadır.

Amaçlar

- Güvenlik duvarı prensiplerinin anlaşılması
- İnternet ve yerel ağ trafiğini yönetmek
- Temel ağ servislerini yapılandırmak
- Web trafiğinin filtrelemek ve raporlamak
- VPN ile güvenli iletişim kanalları oluşturmak
- Birden fazla WAN bağlantısı için yük dengelleme
- Trafik şekillendirme
- Ağdaki aktivitelerin takibi ve raporlanması

İçerik(1)

Bölüm 1 - Giriş

- PF: OpenBSD Packet Filter
- pfSense Nedir ?
- Neden pfSense ?
- pfSense Özellikleri
- Destek

İçerik(2)

Bölüm 2 - pfSense Kurulumu

- Donanım Seçimi
- Minimum Donanım Gereksinimleri
- Full Kurulum

İçerik(3)

Bölüm 3 - Temel Yapılandırma

- Yönetim Arayüzleri
- Genel Yapılandırma
- Ağ Arayüzlerinin Belirlenmesi
- Ağ Arayüz Ayarları
- SSH Servisinin Devreye Alınması

Bölüm 4 - Temel Servisler

- DHCP Server Yapılandırması
- DNS Forwarder
- Dynamic DNS

Bölüm 5 - Firewall

- Firewall Kural Tanımlamaları
- Alias Tanımlamaları
- Schedule Tanımlamaları
- Virtual IP Tanımlamaları

Bölüm 6 - NAT

- Port Yönlendirme
- 1:1 NAT
- Outbound NAT

İçerik(7)

Bölüm 7 - VPN

- pfSense VPN Desteği
- OpenVPN Servisi
- Pptp VPN Servisi

Bölüm 8 - Load Balancing & Failover

- Multiple WAN - Load Balancing
- Multiple WAN - Failover

Bölüm 9 - Diğer Servisler

- Paket Sistemi
- OpenNTPD
- SNMP
- Wake On LAN

Bölüm 10 - Bakım ve Monitoring

- Config Backup/Restore
- Servislerin Yönetilmesi
- E-Mail Durum Bildirilmleri
- External Syslog Sunucusuna Loglama
- RRD Grafikleri
- Sistem Loglarının Görüntülenmesi

BÖLÜM 1
GİRİŞ

NEDİR ?
NE DEĞİLDİR ?

OpenBSD Projesi

OpenBSD, güvenlik ve kararlılık odaklı olarak 1995 yılından beri geliştirilmekte olan açık kaynak kodlu bir UNIX türüdür.

Son sürümü (5.1) 1 Mayıs 2012 tarihinde piyasaya sürülmüştür.

Proje altında OpenSSH, OpenNTP gibi alt projeler de geliştirilmektedir.

Bir çok ticari güvenlik ürününde OpenBSD bileşenleri kullanılmaktadır.

OpenBSD Packet Filter

Packet Filter (Nam-ı diğer pf) OpenBSD takımı tarafından geliştirilmekte olan bir güvenlik duvarı uygulamasıdır.

Temel olarak trafik filtreleme, NAT, port yönlendirme, yük dengeleme, yük aktarma, trafik şekillendirme gibi işlevleri yerine getirir.

FreeBSD, NetBSD, DragonFlyBSD, Debian GNU/kFreeBSD gibi sistemlere port edilmiştir.

pfSense Nedir ?

pfSense, m0n0wall isimli FreeBSD işletim sistemi ve OpenBSD Packet Filter kullanan açık kaynak kodlu firewall dağıtımı temel alınarak geliştirilmiş bir başka güvenlik duvarı ve router dağıtımıdır.

Tüm yapılandırma işlemi bir web arabirimi üzerinden gerçekleştirilebilmektedir.

Paket sistemi sayesinde bir çok farklı uygulamayı da desteklemektedir.

Neden pfSense ?

- FreeBSD altyapısı
- OpenBSD PF Güvenlik Duvarı
- Geniş Özellik Listesi
- Kapsamlı Dökümantasyon
- Destek
  - Mail Listeleri
  - Forum Sayfaları (13 dilde destek)
  - IRC Kanalı
  - Ticari Destek

ÖZELLİKLER

FIREWALL

- Kaynak/Hedef IP, IP Protocol ve TCP/UDP Port bazlı filtreleme.
- Kural bazlı olarak eşzamanlı bağlantı limiti tanımlama yeteneği
- OS bazlı filtreleme yeteneği. (Linux'lar internete çıksın, Win'ler çıkamasın vs.)
- Yük dengeleme,yük dağıtma ve çoklu WAN için kural bazlı gateway seçme imkanı.(Kural bazlı routing)
- Alias tanımlamaları ile host, network ve portlar için grup oluşturabilme.
- Layer 2 seviyesinde transparan firewalling
- Paket normalleştirme. Anormal trafiği düzenler ve parçalanmış paketleri birleştirir.

ÖZELLİKLER

DURUM TABLOSU

- Kurallar öntanımlı olarak statefuldur (durum kontrolü)
- Durum tablosunun ebatı ayarlanabilir. (1state = 1KB~ RAM)
- Kural bazlı olarak:
  - Maximum tekil host bağlantı limiti
  - Host başına maximum kurulabilecek bağlantı limiti
  - Saniyede maximum yeni bağlantı sınırı
  - Durum türü belirleme
- State Type - Durum Türü
  - keep state - Stateful Kural (Default)
  - synproxy state - Gelen bağlantılar için proxy görevi görerek IP Spoof ve SYN Flood saldırılarına karşı korunmaya yardımcı olur.
  - none: Herhangi bir durum kontrolü yapılmaması içindir.

ÖZELLİKLER

Durum Tablosu Optimizasyon Seçenekleri

Pf, bağlantı durumlarının optimize edilebilmesi için 4 farklı optimizaston seçeneği sunar:

- **Normal**: Öntanımlı algoritma.
- **High Latency**: Uydu bağlantıları gibi yüksek gecikme değeri olan linklerde kullanılır. Boşta bekleyen (idle) bağlantılar normalden daha uzun sürede kapatılır.
- **Aggressive**: Idle bağlantıları normalden daha kısa sürede kapatır. Donanım kaynaklarını verimli kullanılmasını sağlar, ancak aslında kullanımda olan bağlantıların da kapatılmasına neden olabilir.
- **Conservative**: Donanıma daha fazla yüklenerek mümkün olduğunca kullanımda olan bağlantıları düşürmemeye çalışır.

ÖZELLİKLER

Network Address Translation (NAT)

- Gelişmiş port yönlendirme
- 1:1 NAT desteği
- Outbound NAT
- NAT Reflaction

ÖZELLİKLER

YEDEKLİLİK

- **CARP**: OpenBSD'nin CARP desteği ile iki ya da daha fazla pfSense yedekli olarak çalıştırılabilir. Firewallardan birisi gittiği zaman diğeri aktif duruma geçerek görevi devralır. Ayrıca yapılandırmanın tüm yedek sunucularla senkronize edilmesi sağlanır.

- **pfsync**: Durum tablosunun, yedekli çalışmak üzere yapılandırılan tüm firewall'lara replike edilmesini sağlar.

ÖZELLİKLER

YÜK DENGELEME

- **Outbound LB**: Birden fazla WAN bağlantısının eş zamanlı ortak ya da yedekli kullanılmasıdır. Kural bazlı olarak farklı ağ geçitleri seçilebilmesine olanak sağlar.

- **Inbound LB:** Gelen bağlantı isteklerini birden fazla sunucuya dağıtmak üzere kullanılır. Genellikle web ve mail servislerinde kullanılır.

ÖZELLİKLER

VPN SERVİSLERİ

- Üç farklı VPN desteği sunulur.
  - **IPsec**: Genel olarak uzak networkleri birbirine bağlamak için kullanılır. (site-to-site)
  - **OpenVPN**: Yaygın bir SSL VPN çözümüdür.
  - **PPTP**: Hemen her işletim sisteminde built-in geldiğinden dolayı sık kullanılan bir VPN servisidir.

ÖZELLİKLER

DHCP SERVER / DNS Forwarder

- pfSense öntanımlı olarak DHCP server kurulu gelir.
- Ayrıca herhangi başka bir DHCP sunucuyu kullanabilmek için DHCP Relay servisi vardır.
- DNS Forwarder desteği ile kendisine gelen DNS isteklerini çözümleme yapacak DNS sunucuya gönderir.
- Ayrıca pfsense üzerinde, alan adları için yetkili dns sunucu tanımlaması ya da spesifik hostlar için dns kayıtları oluşturulması sağlanabilir.

ÖZELLİKLER

Dynamic DNS

- Dinamik IP adresiniz değiştiğinde durumu DNS sunucuya bildirip DNS kaydınızın güncellenmesini sağlar.

- "DynDNS - DHS - DNSexit - DyNS - easyDNS - freeDNS
  HE.net - Loopia - Namecheap - No-IP - ODS.org - OpenDNS - ZoneEdit" gibi Dinamik DNS servislerini destekler.

ÖZELLİKLER

CAPTIVE PORTAL

Captive Portal internete çıkış için zorunlu kimlik denetimi sağlanmasına olanak sağlayan servistir.

Bu servis ile kullanıcılar bir URL'ye yönlendirilebilir ve internet erişimi için kullanıcı adı / şifre girmeleri ya da bir linke tıklamaları sağlanabilir.

Genelde hot spot ağlarda kullanılır.

DESTEK

Dökümantasyon

http://doc.pfsense.org/index.php/Main_Page

http://doc.pfsense.org/index.php/Tutorials

Sorun Giderme Klavuzları

http://doc.pfsense.org/index.php/Category:Troubleshooting

Eğitim Videoları

http://www.cehturkiye.com/videolar/pfsense/

DESTEK

Mail Listeleri

pfSense Support listesi: support-subscribe@pfsense.com

Listeye boş bir e-mail gönderip dönen cevabı onaylamanız yeterli.

Türkçe Liste: pfsense-tr+subscribe@googlegroups.com

Liste Arşivi:

http://dir.gmane.org/gmane.comp.security.firewalls.pfsense.support

http://marc.info/?l=pfsense-support

http://tinyurl.com/a3j3kp

DESTEK

Forum Sayfası

Arasında “Türkçe” nin bulunduğu 13 dilde destek formu,
http://forum.pfsense.com

IRC Kanalı

Freenode irc servisi üzerinde, #pfsense adında bir kanal bulunuyor.Ortalama 100 kişi sürekli aktif oluyor.Bu kanala dahil olup, sorunuzu yöneltebilirsiniz.

Ticari Destek

pfSense geliştiricilerinden direk destek alınabilecek bir mecra.
https://portal.pfsense.org/index.php/support-subscription

BÖLÜM 2
KURULUM

KURULUM

DONANIM SEÇİMİ

- Kurulum Gerektirmeyen Çalışan CD'ler
- Sabit Diskler
- Tak Çalıştır USB Aygıtlar
- Compact Flash Kartlar
- Gömülü Sistemler

KURULUM

UYUMLULUK LİSTESİ

FreeBSD 8.1 (pfSense 2.0.1)

http://www.freebsd.org/releases/8.1R/hardware.html

KURULUM

MİNİMUM DONANIM GEREKSİNİMLERİ

CPU - 100 MHz Pentium

RAM - 128 MB

Live CD

CD-ROM drive

Ayarları saklamak için USB flash sürücü.

Sabit Diske Kurulum

CD-ROM, kurulum başlangıcı için

1 GB hard disk

Gömülü Sistemler

512 MB Compact Flash card

Yönetim için Seri port

KURULUM

FULL KURULUM

Symmetric Multiprocessing Kernel

Çok çekirdekli / çok işlemcili donanımları destekler

Embedded Kernel

Gömülü anakartlar için. VGA konsolu ve klavye yok. Seri porttan yönetilir.

Developer Kernel

Debug seçeneklerinin aktif edildiği geliştirici versiyonu.

BÖLÜM 3
TEMEL YAPILANDIRMA

TEMEL YAPILANDIRMA

Yönetim Arabirimleri

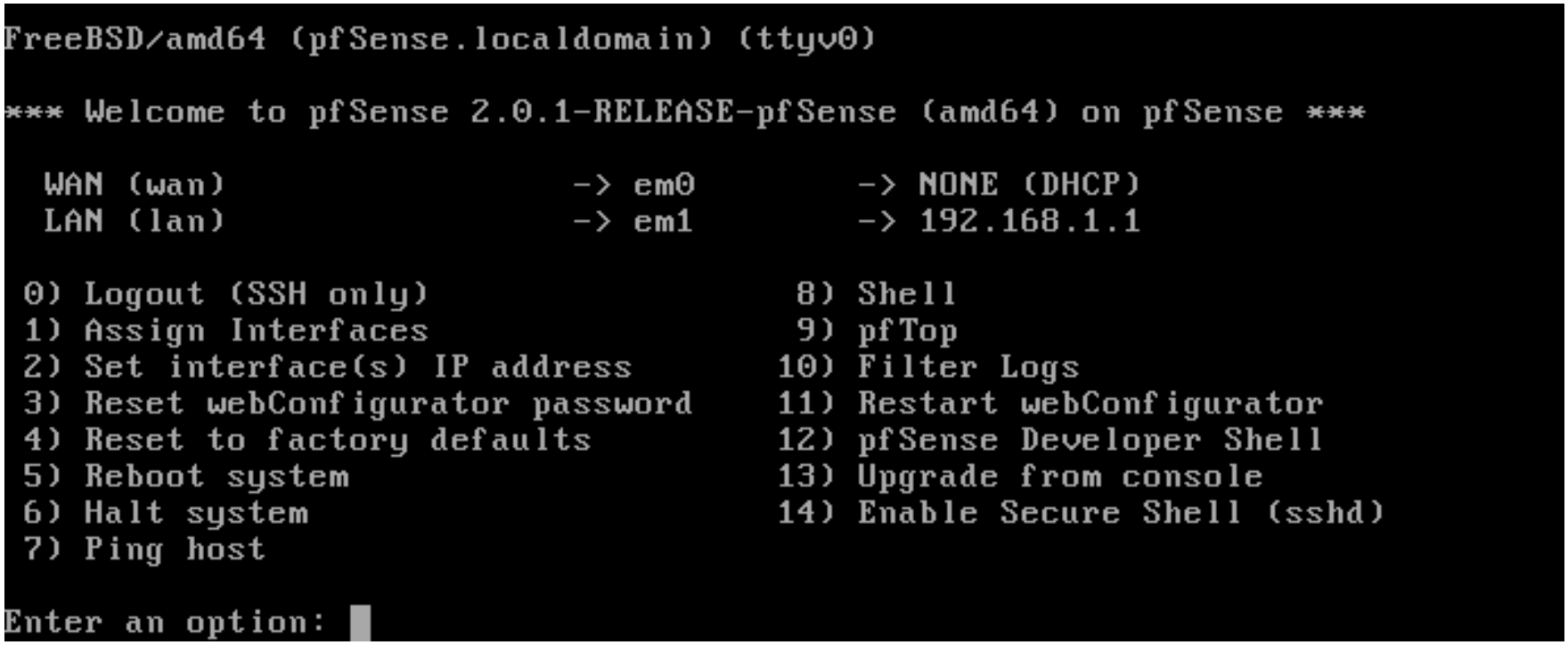
pfSense'in konsol ve web olmak üzere iki farklı yönetim arabirimi vardır.

Konsol Arabirimi: Temel ayarlar ve kurtarma operasyonları için seçenekler sunan sade bir menüdür.

Web Arabirimi: Hemen tüm sistem ayarlarının ve yönetimsel faliyetlerin yürütülebildiği web tabanlı yönetim arabirimidir.

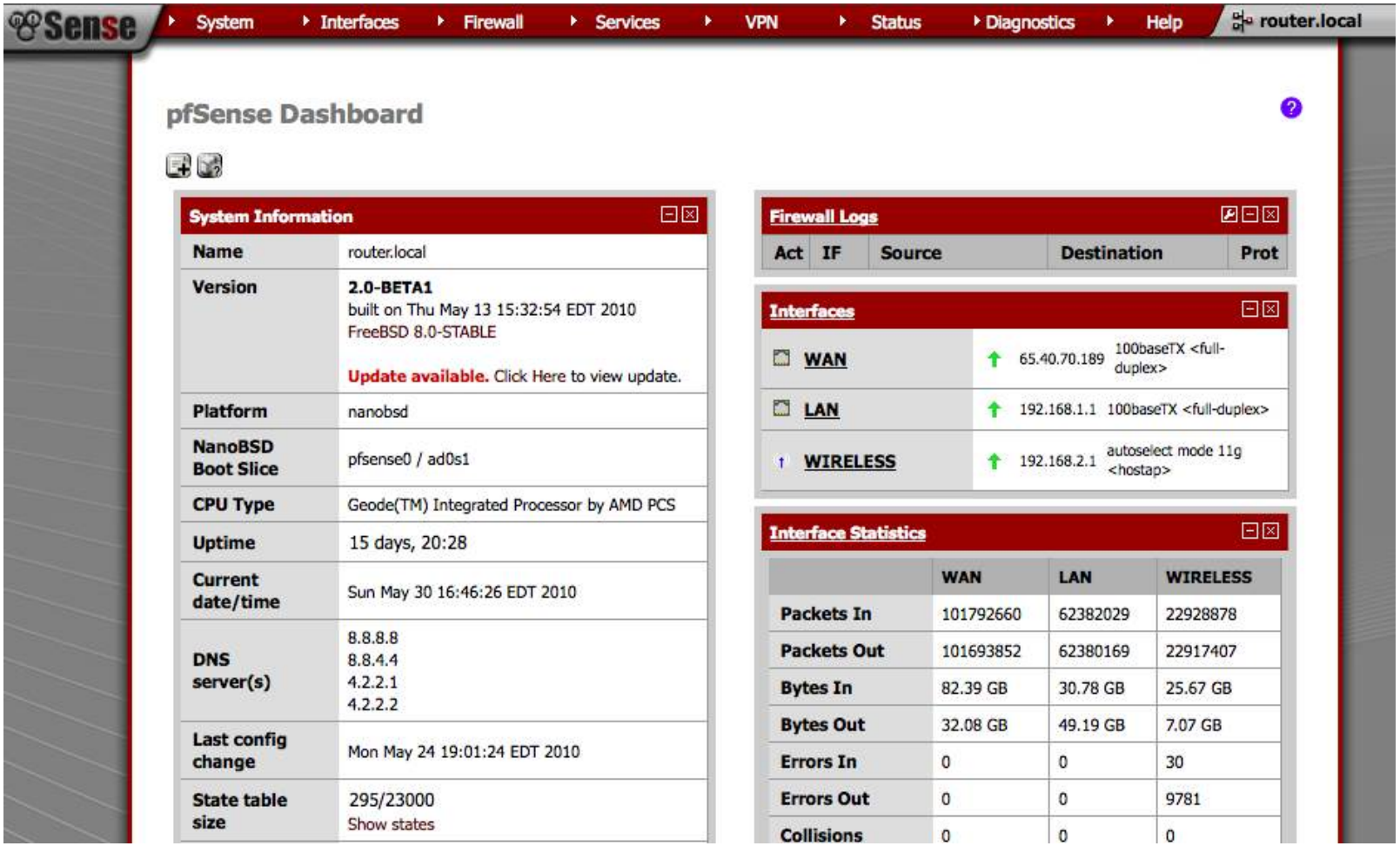
TEMEL YAPILANDIRMA

Konsol Arabirimi

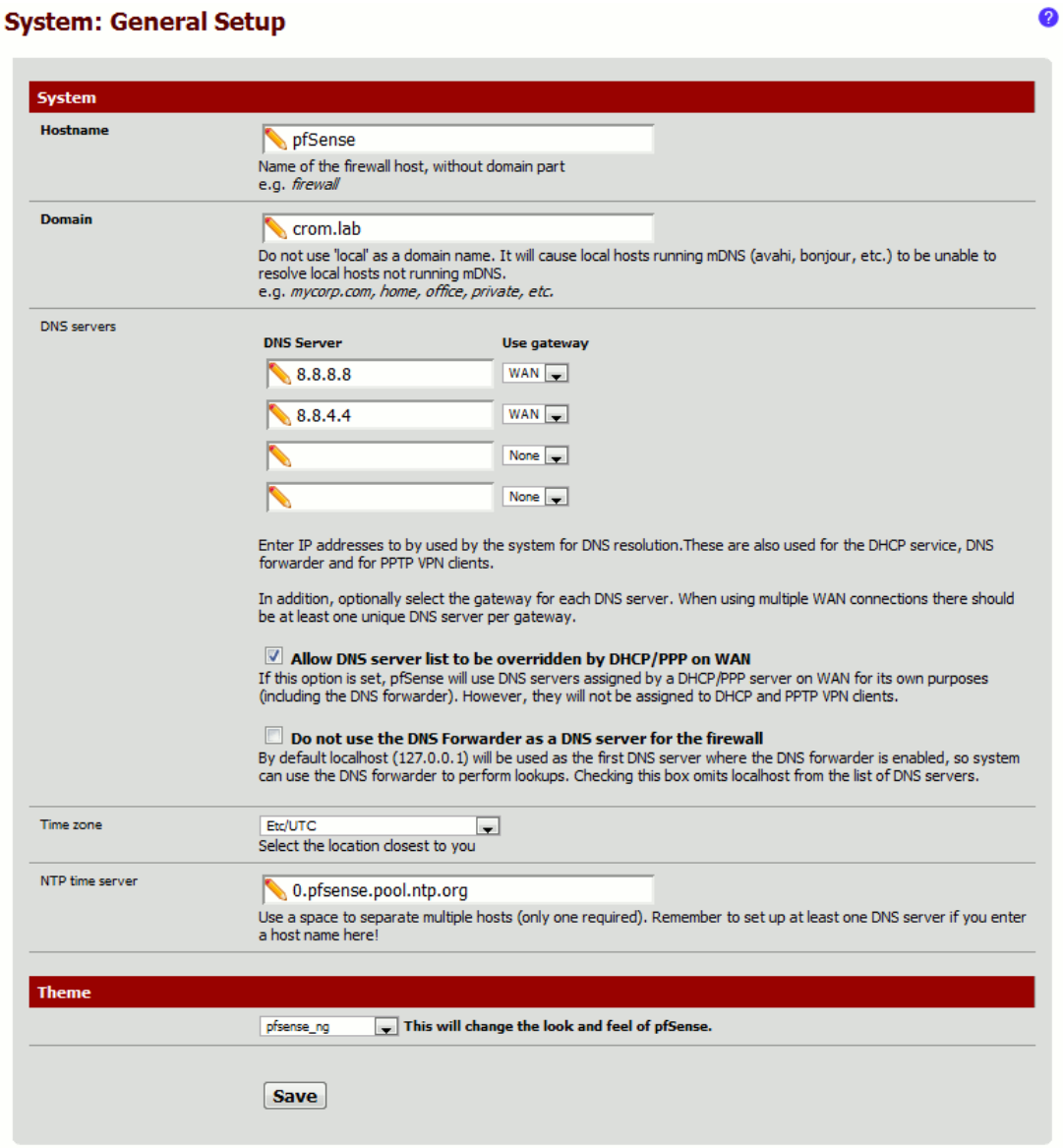


TEMEL YAPILANDIRMA

Web Arabirimi



TEMEL YAPILANDIRMA

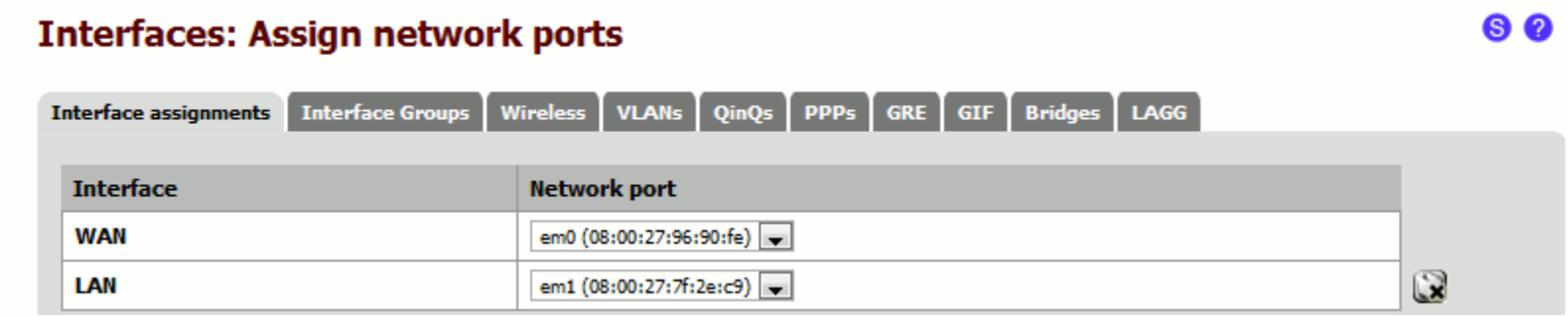


TEMEL YAPILANDIRMA

Ağ Arabirimlerinin Belirlenmesi

Arayüzler hem WebGui hem de Konsol üzerinden tanımlanabilir.

```
0) Logout (SSH only)                  8) Shell
1) Assign Interfaces                  9) pfTop
2) Set interface(s) IP address       10) Filter Logs
3) Reset webConfigurator password    11) Restart webConfigurator
4) Reset to factory defaults         12) pfSense Developer Shell
5) Reboot system                     13) Upgrade from console
6) Halt system                       14) Enable Secure Shell (sshd)
7) Ping host
```



TEMEL YAPILANDIRMA

Ağ Arayüz Ayarları

- Ağ ayarları WebGui'nin Interfaces Menüsünden yapılır.
- Menü farklı arayüz tiplerine göre değişiklik gösterebilir.
- Bir çok farklı tür tanımlama yapılabilir.
  - Static IP Yapılandırması
  - DHCP
  - PPoE/PPTP
  - Wireless

TEMEL YAPILANDIRMA

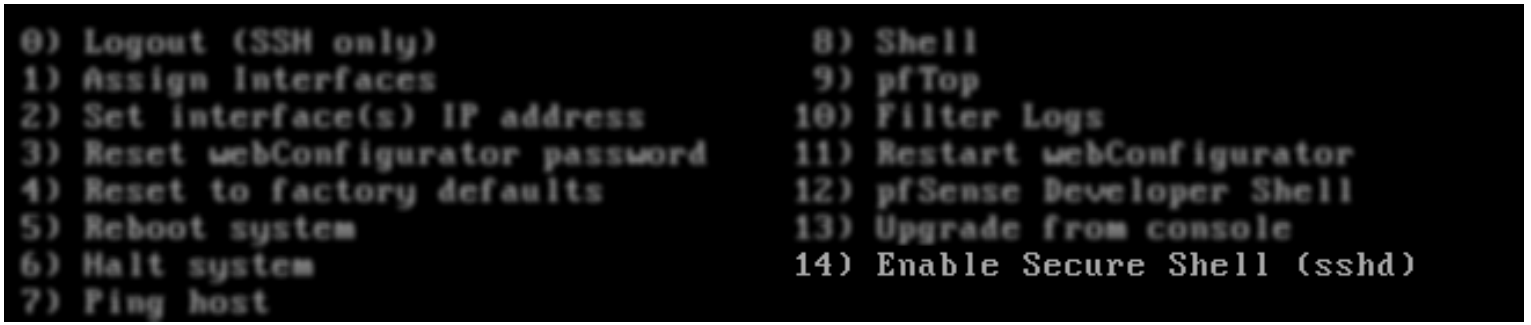
Ağ Arayüz Ayarları

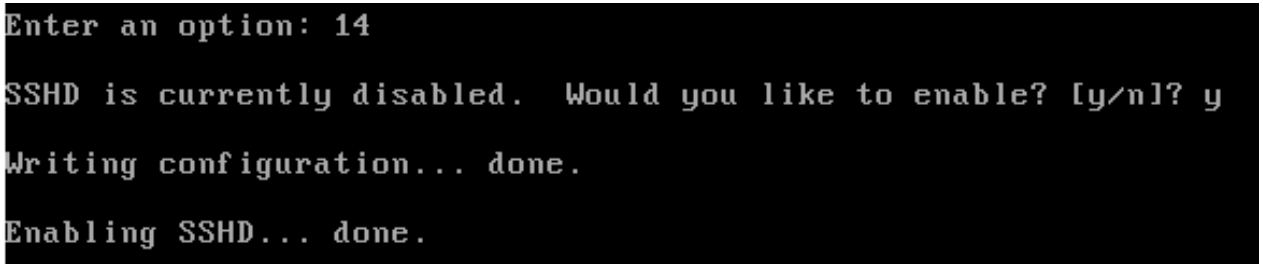
- **Static IP Yapılandırması**
  IP Adresi ve subnet mask değeri manual olarak atanır. WAN arabirimine sabit ip tanımlaması yapılırken gateway değeri de atanmalıdır.
- **DHCP**
  IP otomatik olarak ortamdaki DHCP sunucudan alınır. Ayrıca opsiyonel olarak arayüz için hostname ve alias olarak ikinci bir IP adresi girilebilir.
- **PPoE/PPTP**
  PPoE ve PPTParayüzlerine kullanıcı adı / parola, opsiyonel olarak servis adı dial-and-demand, idle timeout değerleri set edilebilir.
- **Wireless:**
  Wireless arayüzü istemcilere hizmet vermek üzere Access Point olarak kullanılabilir ya da başka bir AP'e bağlanabilir.

TEMEL YAPILANDIRMA

SSH Servisinin Devreye Alınması

SSH servisi konsol menüsünün 14 numaralı seçeneği kullanılarak devreye alınabilir:





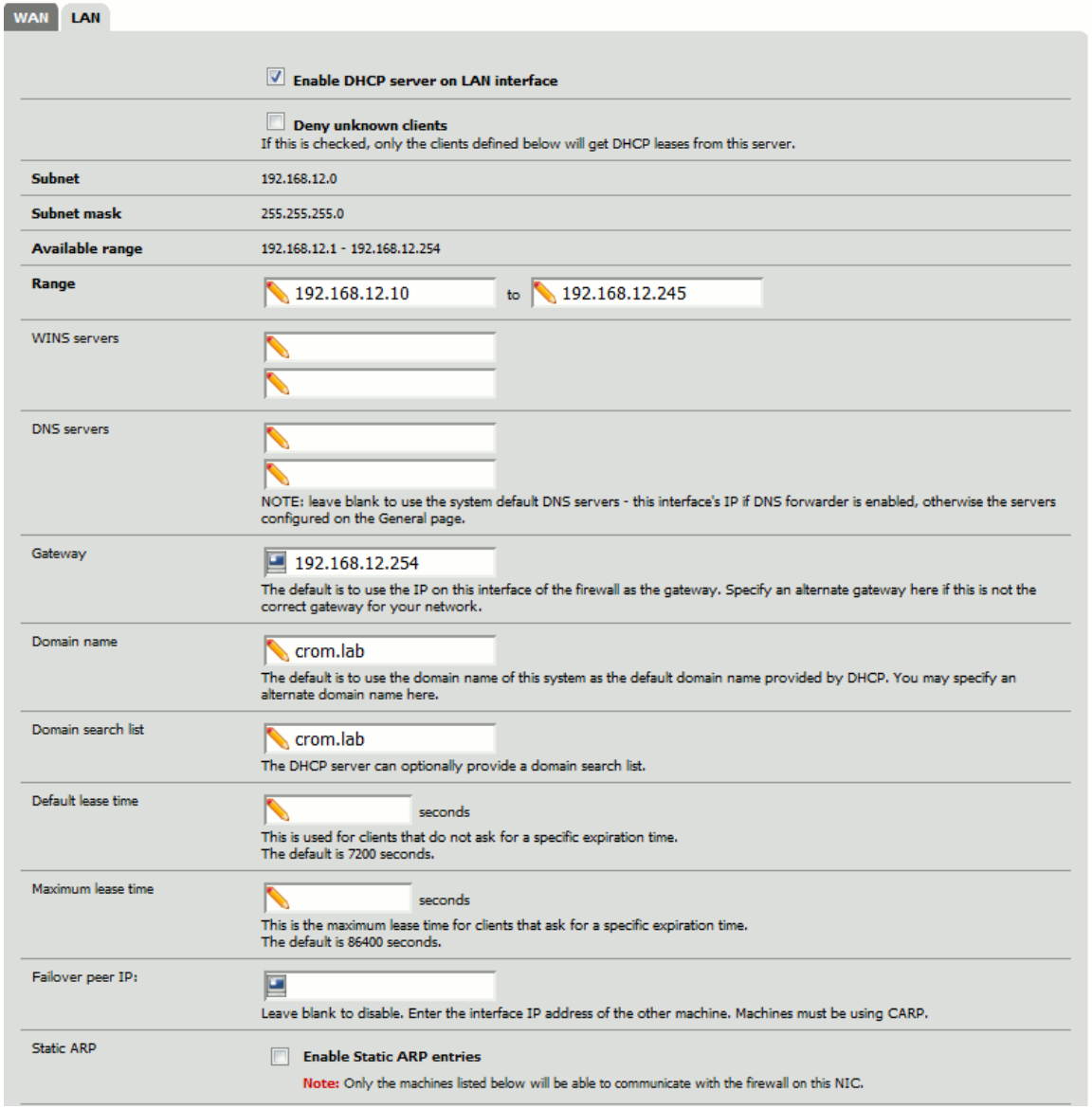
BÖLÜM 4
TEMEL SERVİSLER

TEMEL SERVİSLER

DHCP SERVER

- İstemcilere otomatik olarak IP adresi dağıtmak üzere kullanılır.
- DHCP sunucunun çalıştığı interface'in statik IP adresi olmalıdır.
- MAC adresine göre statik IP ataması yapılabilir.
- NTP server, Dynamic DNS vs. gibi bilgiler DHCP istemcilerine bildirilebilir.
- DNS ve Gateway tanımı yapılabilir.
- DHCP kira süreleri tanımlanabilir.
- DHCP kiralarını görüntüleme ve yönetme arabirimi mevcuttur.
- DHCP'de tanımlanmamış istemcilerin ağa erişimini engeller.

TEMEL SERVİSLER



TEMEL SERVİSLER

Dynamic DNS	Advanced - Show Dynamic DNS
NTP servers	Advanced - Show NTP configuration
TFTP server	Advanced - Show TFTP configuration
LDAP URI	Advanced - Show LDAP configuration
Enable network booting	Advanced - Show Network booting
Additional BOOTP/DHCP Options	Advanced - Show Additional BOOTP/DHCP Options

Save

Note:
The DNS servers entered in System: General setup (or the DNS forwarder, if enabled) will be assigned to clients by the DHCP server.

The DHCP lease table can be viewed on the Status: DHCP leases page.

MAC address	IP address	Hostname	Description
08:00:27:65:d1:11	192.168.12.246	Lab02-Debian6	Lab02-Debian6 Static Lease

TEMEL SERVİSLER

Status: DHCP leases

IP address	MAC address	Hostname	Start	End	Online	Lease Type
192.168.12.12	08:00:27:8f:35:1f		2012/06/28 11:53:22	2012/06/28 13:53:22	online	active
192.168.12.102	08:00:27:aa:22:23	Lab03-FreeBSD-8	2012/06/28 11:42:29	2012/06/28 13:42:29	online	active
192.168.12.246	08:00:27:65:d1:11	Lab02-Debian6	n/a	n/a	online	static

Status: System logs: DHCP

System | Firewall | DHCP | Portal Auth | IPsec | PPP | VPN | Load Balancer | OpenVPN | OpenNTPD | Wireless | Settings

Last 50 DHCP service log entries	
Jun 28 12:11:03	dhcpd: DHCPOFFER on 192.168.12.11 to 08:00:27:65:d1:11 via em1
Jun 28 12:11:03	dhcpd: DHCPREQUEST for 192.168.12.11 (192.168.12.254) from 08:00:27:65:d1:11 via em1
Jun 28 12:11:03	dhcpd: DHCPACK on 192.168.12.11 to 08:00:27:65:d1:11 via em1
Jun 28 12:14:36	dhcpd: Internet Systems Consortium DHCP Server 4.2.3
Jun 28 12:14:36	dhcpd: Copyright 2004-2011 Internet Systems Consortium.
Jun 28 12:14:36	dhcpd: All rights reserved.
Jun 28 12:14:36	dhcpd: For info, please visit https://www.isc.org/software/dhcp/

TEMEL SERVİSLER

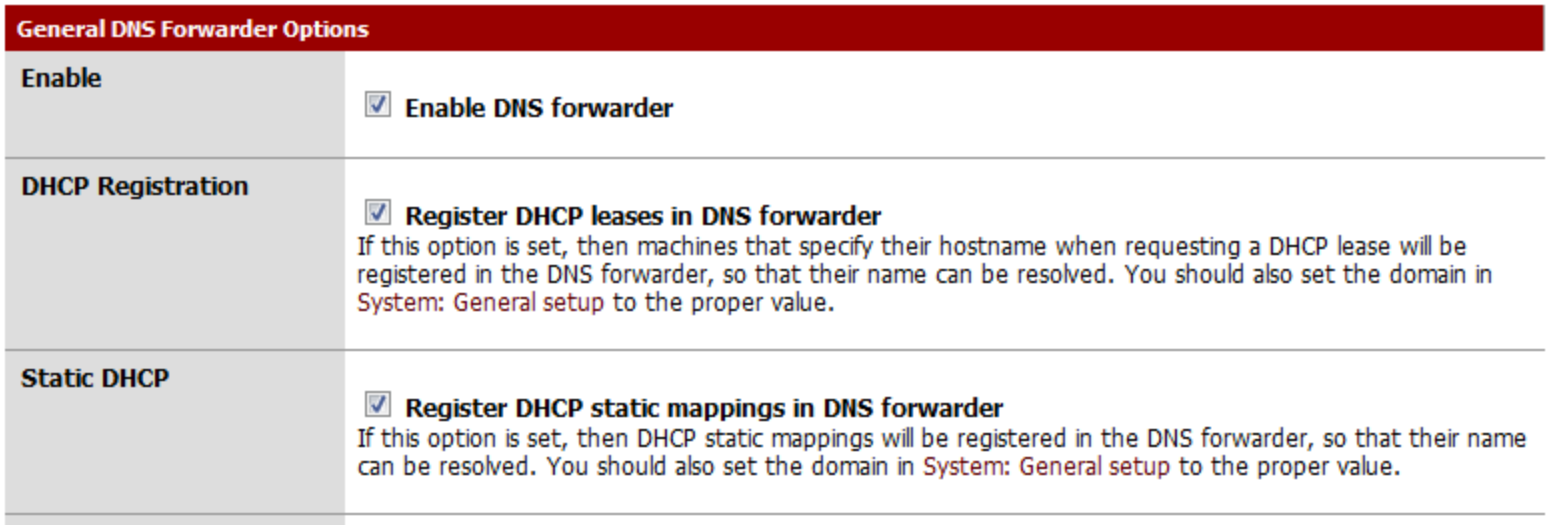
DNS Forwarder

pfSense üzerinde DNS sunucu bulunmaz, kendisine gelen istekleri "System > General Setup" kısmında tanımladığınız DNS sunuculardan çözerek istemciye cevam döndürür.

Ayrıca domainler için yetkili dns sunucuları ve ya bir host için A tipi DNS kaydı eklenebilir.

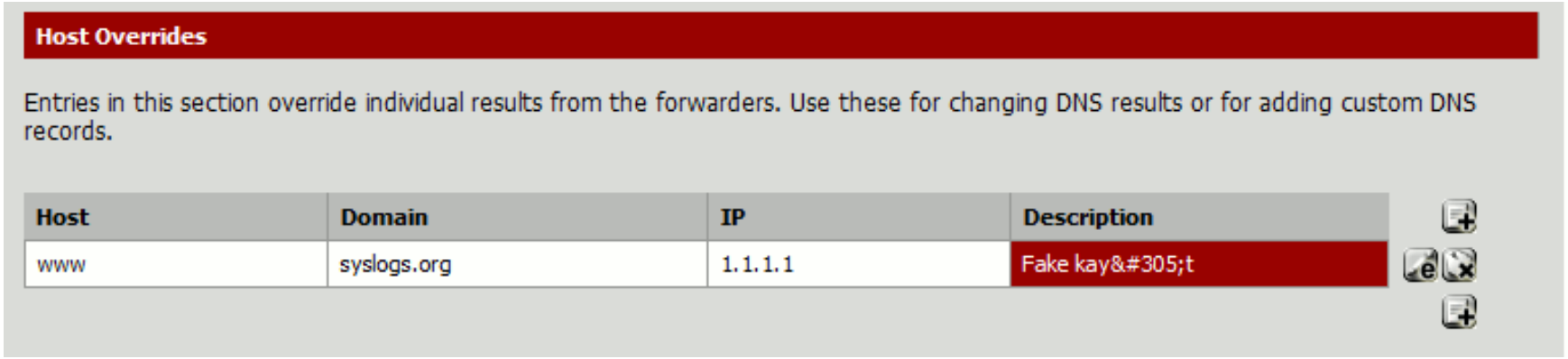
DHCP servisinden IP alan istemcilerin hostnameleri dns forwarder'a kayıt edilebilir. Böylece yerel ağdaki bilgisayar adları çözümlenebilir.

TEMEL SERVİSLER



Yukarıdaki paramerteler DNS Forwarder'ı devreye alır ve DHCP'den IP alan istemcilerin hostnamelerinin çözümlenebilmesini sağlar.

TEMEL SERVİSLER



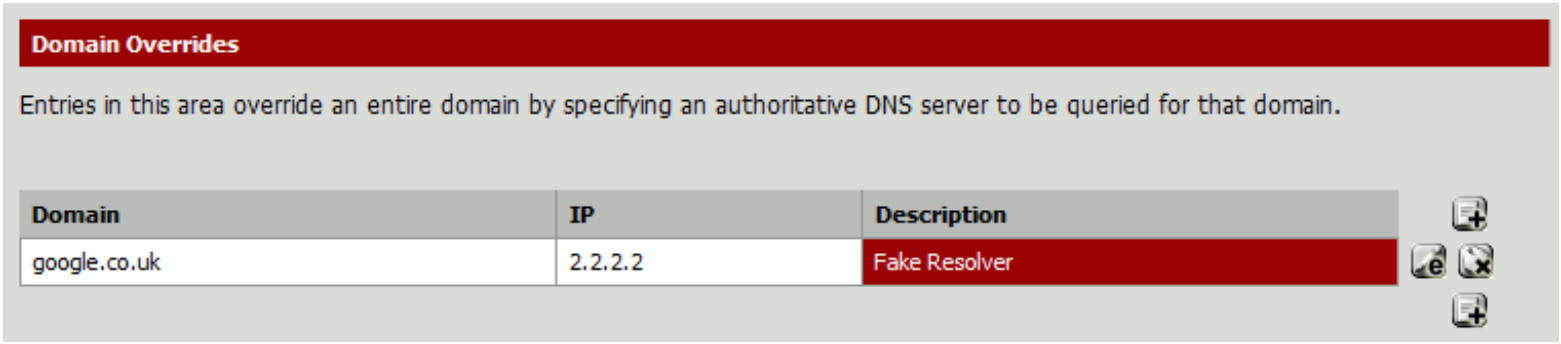
Bu kayıt www.syslogs.org adresinin 1.1.1.1 olarak çözümlenmesine neden olacaktır.

~# dig www.syslogs.org

;; ANSWER SECTION:

www.syslogs.org. 1 IN A 1.1.1.1

TEMEL SERVİSLER



Bu kayıt da google.co.uk ile ilgil sorgular için 2.2.2.2 ip'li dns sunucuda sorgulama yapacaktır

.

~# dig mx google.co.uk

192.168.0.196.8238 > 2.2.2.2.53: [udp sum ok] 32718+ MX? google.co.uk.

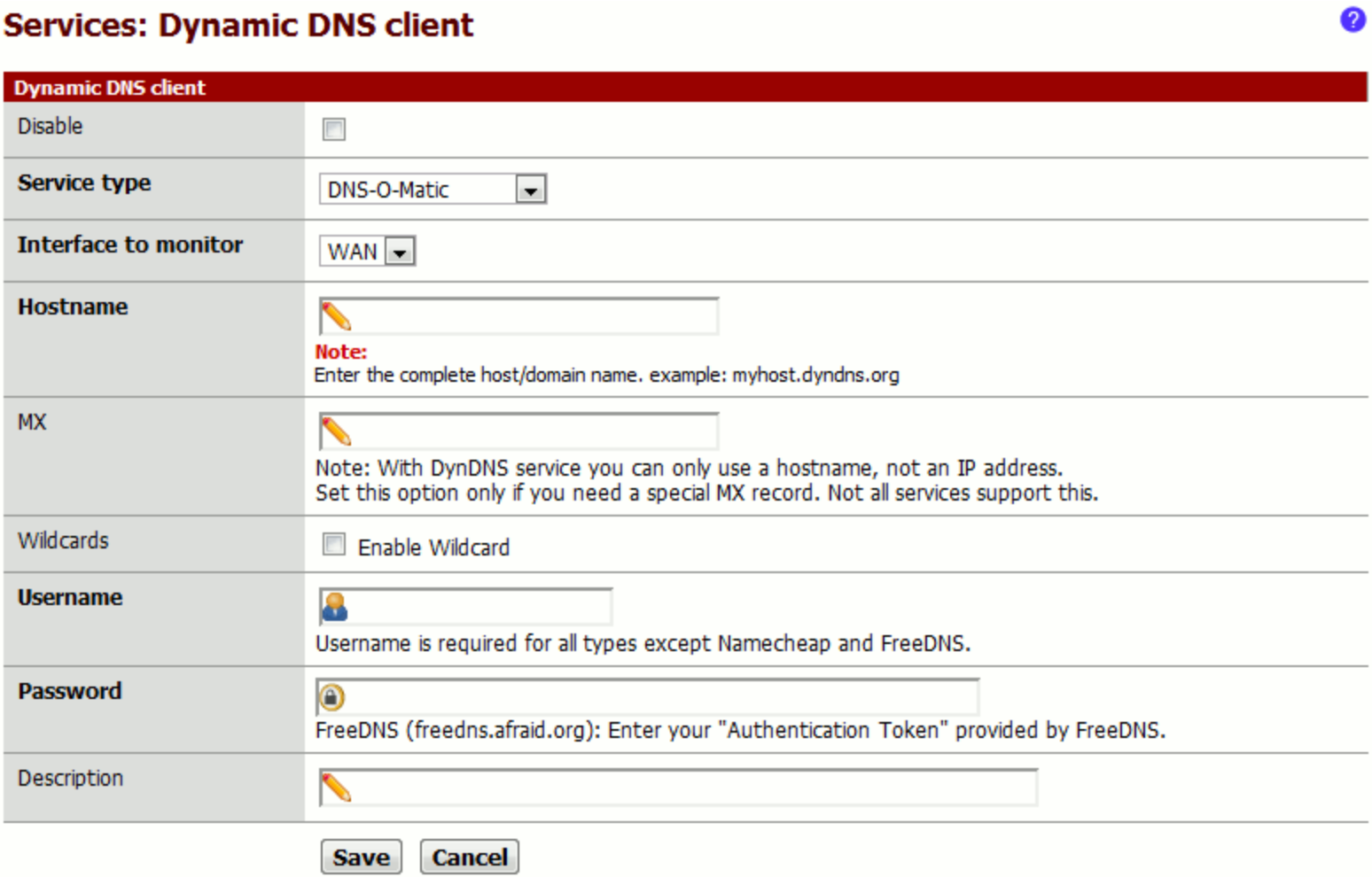
TEMEL SERVİSLER

Dynamic DNS

DynDNS servisi, Services menüsünün altında Dynamic DNS segmesinde bulunur. Bu servis dinamik ip adresiniz her değiştiğinde ilgili değişikliği DNS sunucusuna bildirip otomatik olarak DNS kaydınızın güncellenmesini sağlar.

pfSense, "DNS-O-Matic, No-IP, ODS.org, ZoneEdit, Loopia, freeDNS, DNSexit, OpenDNS, Namecheap, HE. net, DHS, DyNS, easyDNS" gibi dinamik servislerini desteklemektedir.

TEMEL SERVİSLER



BÖLÜM 5
FIREWALL

FIREWALL - MENÜ

Trafik filtreleme ile ilgili herşey Ana menüdeki "Firewall" segmesi altından yapılır.

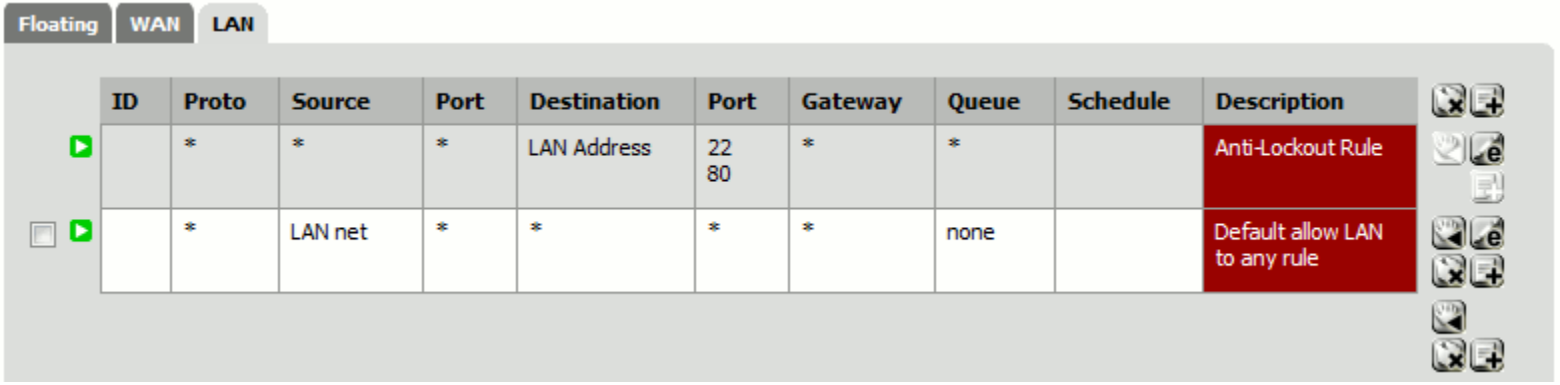
Bu menü altında:

- Host, ip, network gruplama için kullanılan Alias
- Nat ve Port yönlendirme işleri için kullanılan NAT
- Firewall kurallarını oluşturmak için kullanılan Rules
- Kuralların çalışma zamanlarının belirlendiği Schedules
- Trafik şekillendirme için kullanılan Traffic Shaper
- Genelde NAT işlerinde kullanılan sanal IP'lerin tanımlandığı Virtual IPs

alt menüleri bulunur.

FIREWALL - KURALLAR

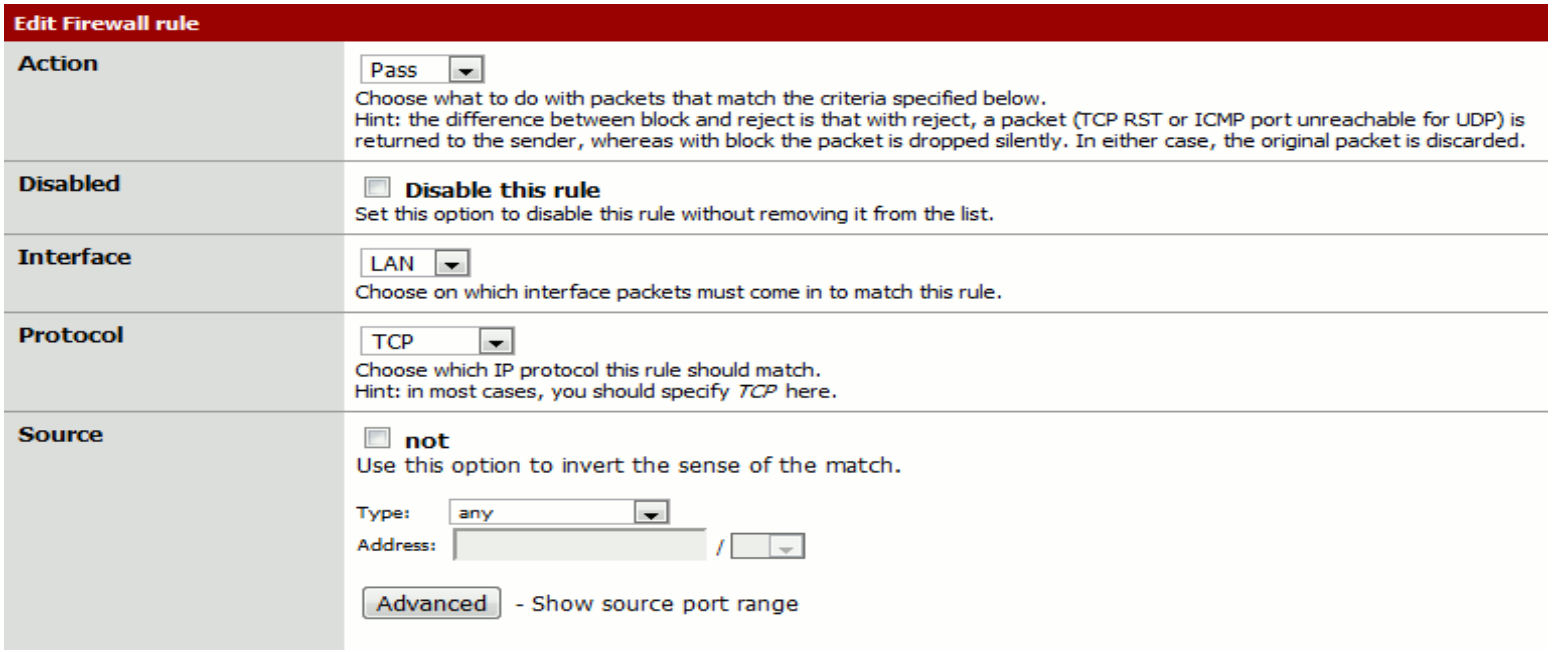
Kuralların tanımlandığu alt menü olan "Rules" bölümünde her interface için ayrı kural sayfası bulunur.



Örnek olarak LAN'dan dışarıya doğru yapılacak filtreleme kural "LAN" tabı altında oluşturulmalıdır. Aynı şekilde dışarıdan içeriye doğru olan trafik üzerindeki filtrelemeler de "WAN" tabı altında yapılmalıdır.

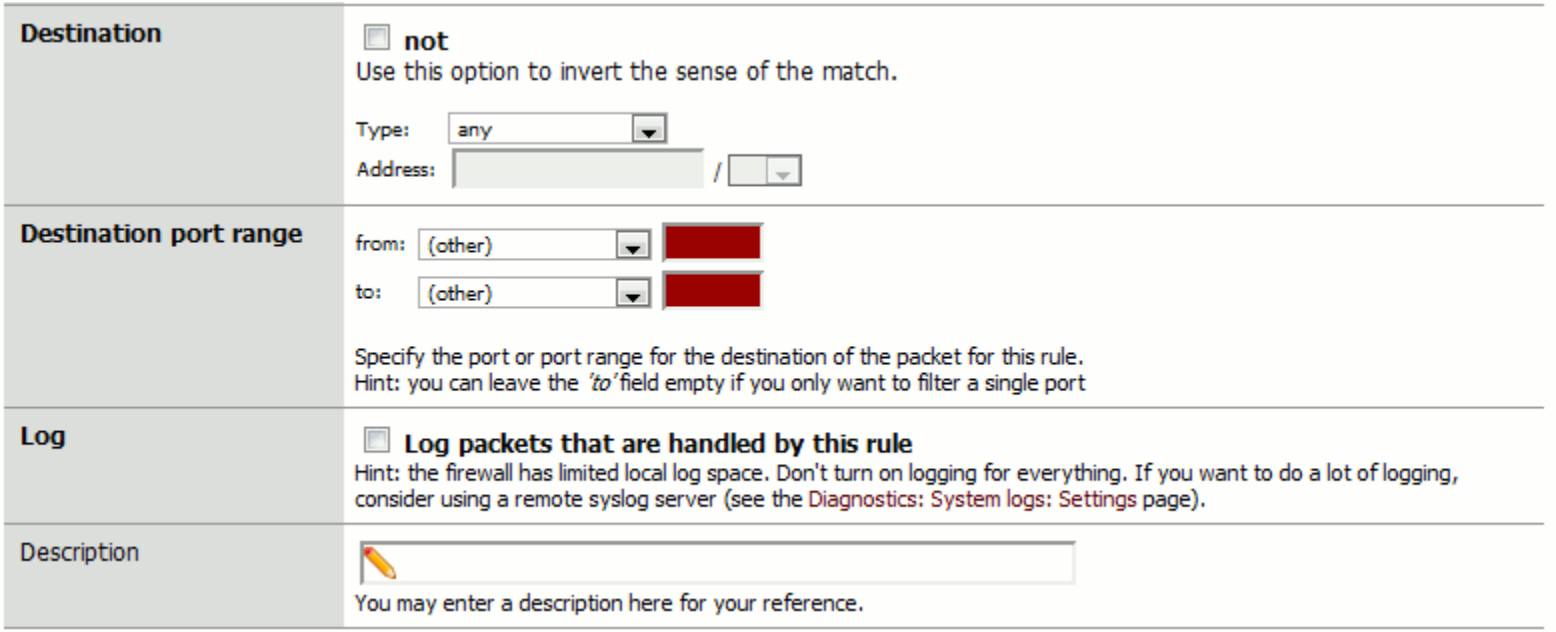
"Floating" tabı ise tüm interfacelerde yürütülecek kurallar içindir.

FIREWALL - KURALLAR



- **Action**: Pakete uygulanacak filtre kriteri.
  - Pass: Paketin geçişine izin verir.
  - Block: Paketi engeller. (drop)
  - Reject: TCP paketlerine "TCP RST", UDP için ise "ICMP port unreachable" yanıtı döndürür.
- **Disabled**: Kuralı devre dışı bırakır.
- **Interface**: Kuralın uygulanacağı arayüz.
- **Protocol**: IP protokolü.(TCP, UDP, ICMP vs.)
- **Source**: Paketin kaynağı. (IP, Alias, Subnet vs.)
  - **Source port range**: Kaynak port aralığı.

FIREWALL - KURALLAR



- **Destination**: Paketin hedefi (IP, Alias, Subnet vs.)
  - **Destination port range**: Paketin hedef port aralığı.
- **Log**: Kural için kayıt tut.
- **Description**: Kuralı tanımlayıcı açıklama satırı.

FIREWALL - KURALLAR

Advanced features	
Source OS	Advanced - Show advanced option
Diffserv Code Point	Advanced - Show advanced option
Advanced Options	Advanced - Show advanced option
TCP flags	Advanced - Show advanced option
State Type	Advanced - Show advanced option
No XMLRPC Sync	Advanced - Show advanced option
Schedule	Advanced - Show advanced option
Gateway	Advanced - Show advanced option
In/Out	Advanced - Show advanced option
Ackqueue/Queue	Advanced - Show advanced option
Layer7	Advanced - Show advanced option

FIREWALL - KURALLAR

- **Source OS**: Kuralın geçerli olacağı işletim sistemi. (Yalnızca TCP kurallar için geçerlidir.)

- **Advanced Options**: Gelişmiş PF seçenekleri.
  - Maximum state entries this rule can create: Bu kural için oluşturulabilecek maximum state (durum) girdisi.
  - Maximum number of unique source hosts: Bu hosta erişebilecek maximum tekil host (ip) adedi.
  - Maximum number of established connections per host: Her bir hostun kurabileceği max bağlantı sınırı.
  - Maximum state entries per host: Her bir host için oluşturulabilecek max state girdisi.
  - Maximum new connections / per second(s): Saniye bazlı olarak açılabilecek max yeni bağlantı sayısı.

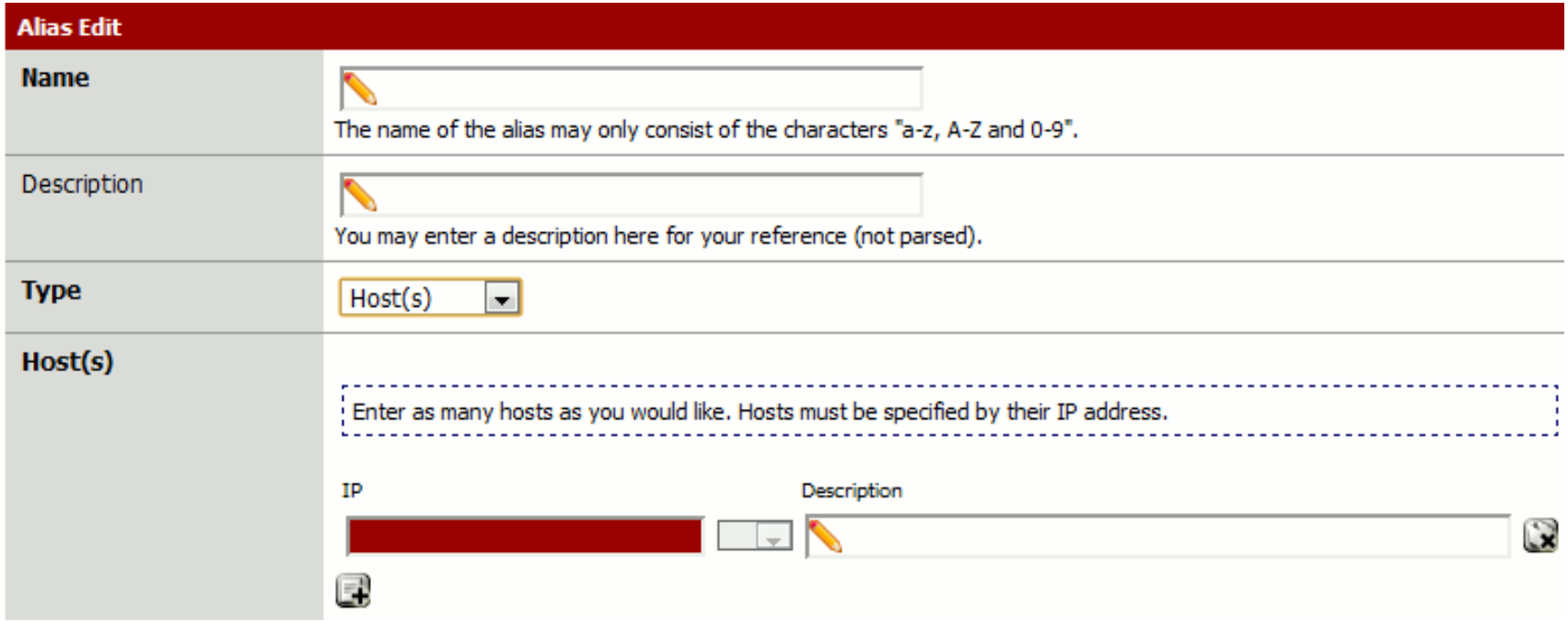
FIREWALL - KURALLAR

- **TCP Flags**: Spesifik TCP bayraklarını set etmek için kullanılır.
-
- **State Type**: Durum türü.
  - keep state: Durum kontrollü kurallar. (Default)
  - sysnproxy state: Gelen istekler için proxy görevi görür. Handshake tamamlanmadan arkadaki hosta bağlantı açmaz. Bu şekilde spoofed IPlerden gelen SYN Flood saldırılarından korunmaya yardımcı olur.
  - none: Herhangi bir durum mekanizması kullanmaz.
- **Schedule**: Kuralın aktif olacağı zaman diliminin belirlenmesi.

- **Gateway**: Birden fazla gateway olması durumunda kural için hangi gateway'in kullanılacağını set eder. (Policy based routing)

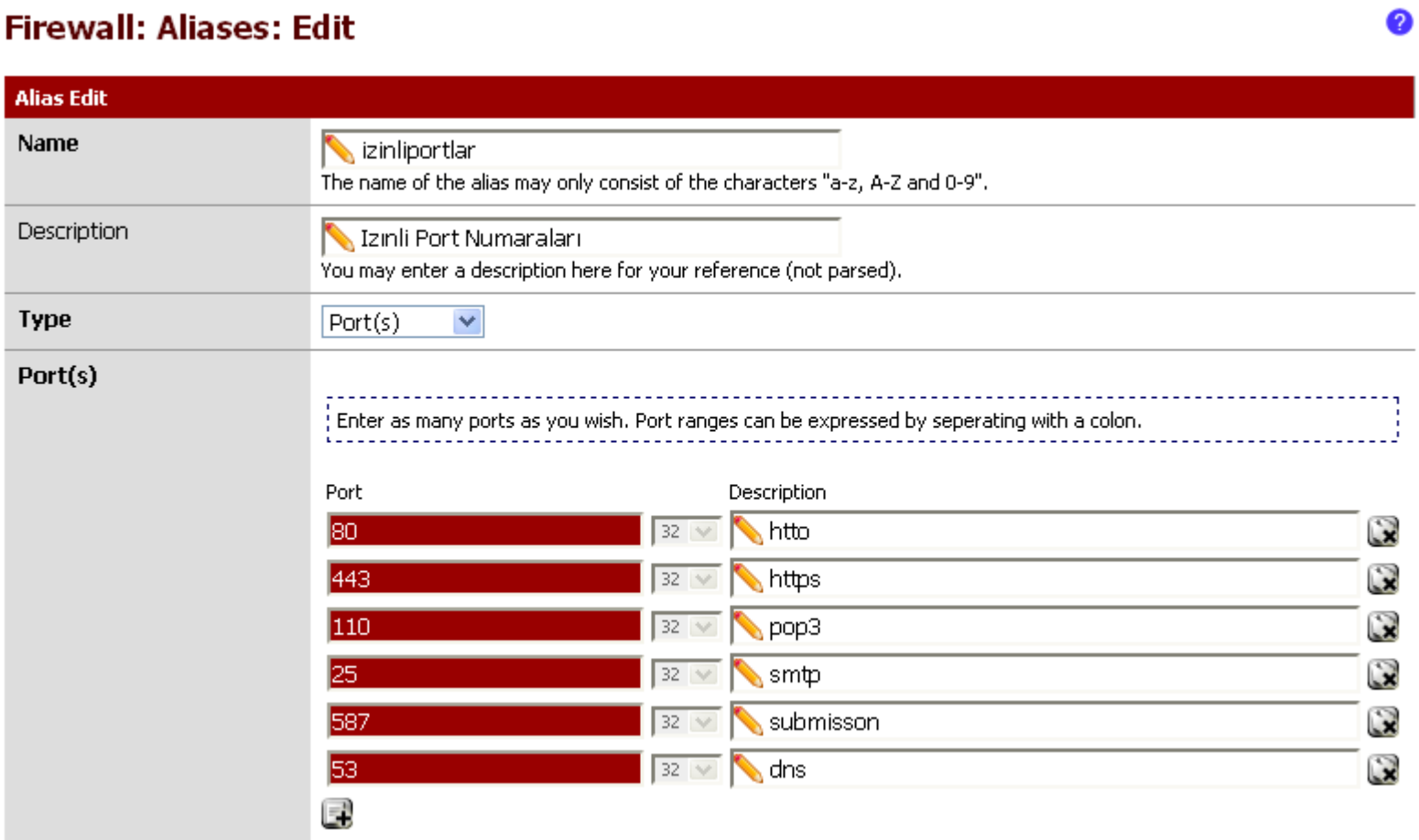
FIREWALL - ALIASES

Kurallarda kullanılmak üzere IP, port ve network adreslerini gruplandırmak için kullanılır.



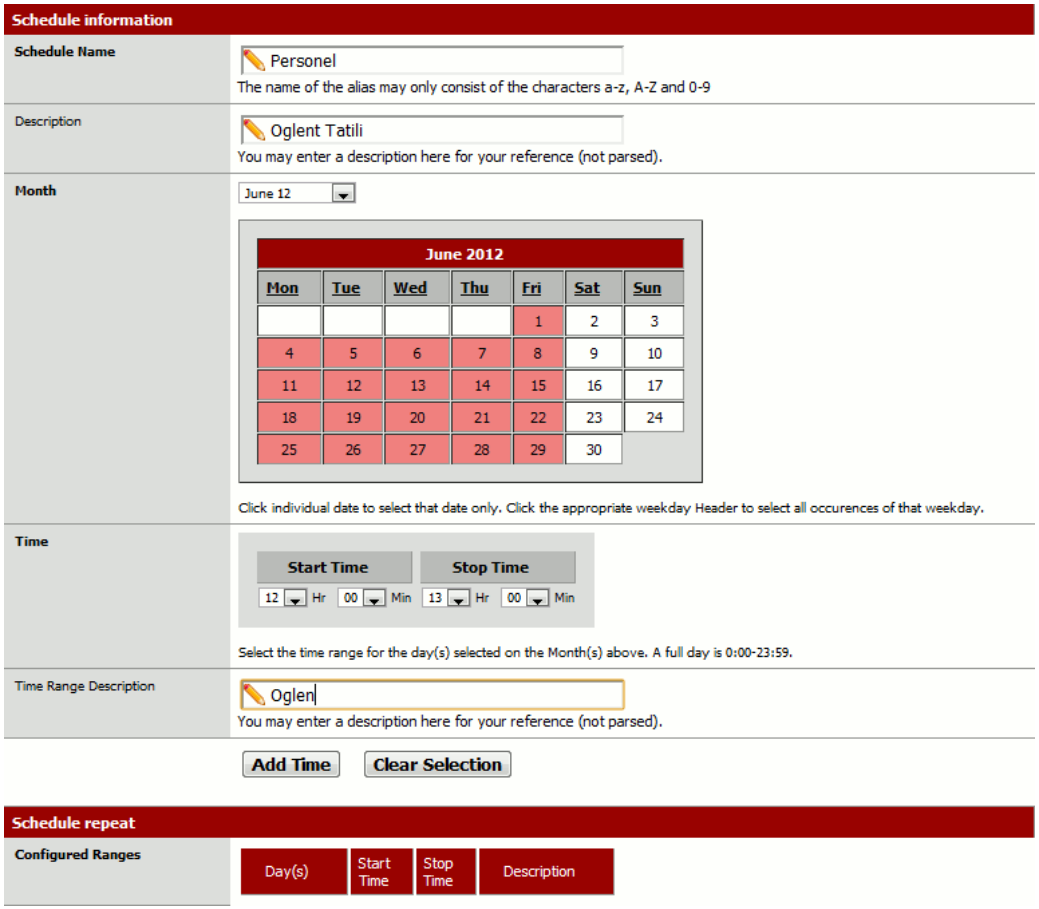
FIREWALL - ALIASES

Örnek olarak izin verilmesi istenen portlar gruplanarak tüm portlara tek bir firewall kuralı ile izin verilebilir.



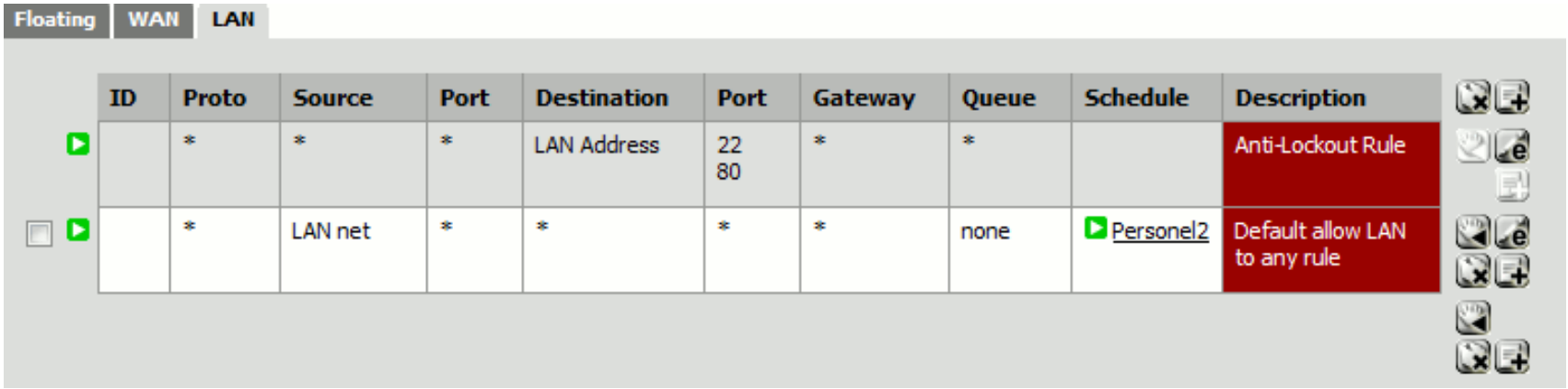
FIREWALL - SCHEDULES

Zaman bazlı firewall kuralları oluşturmak için kullanılan bir özelliktir.



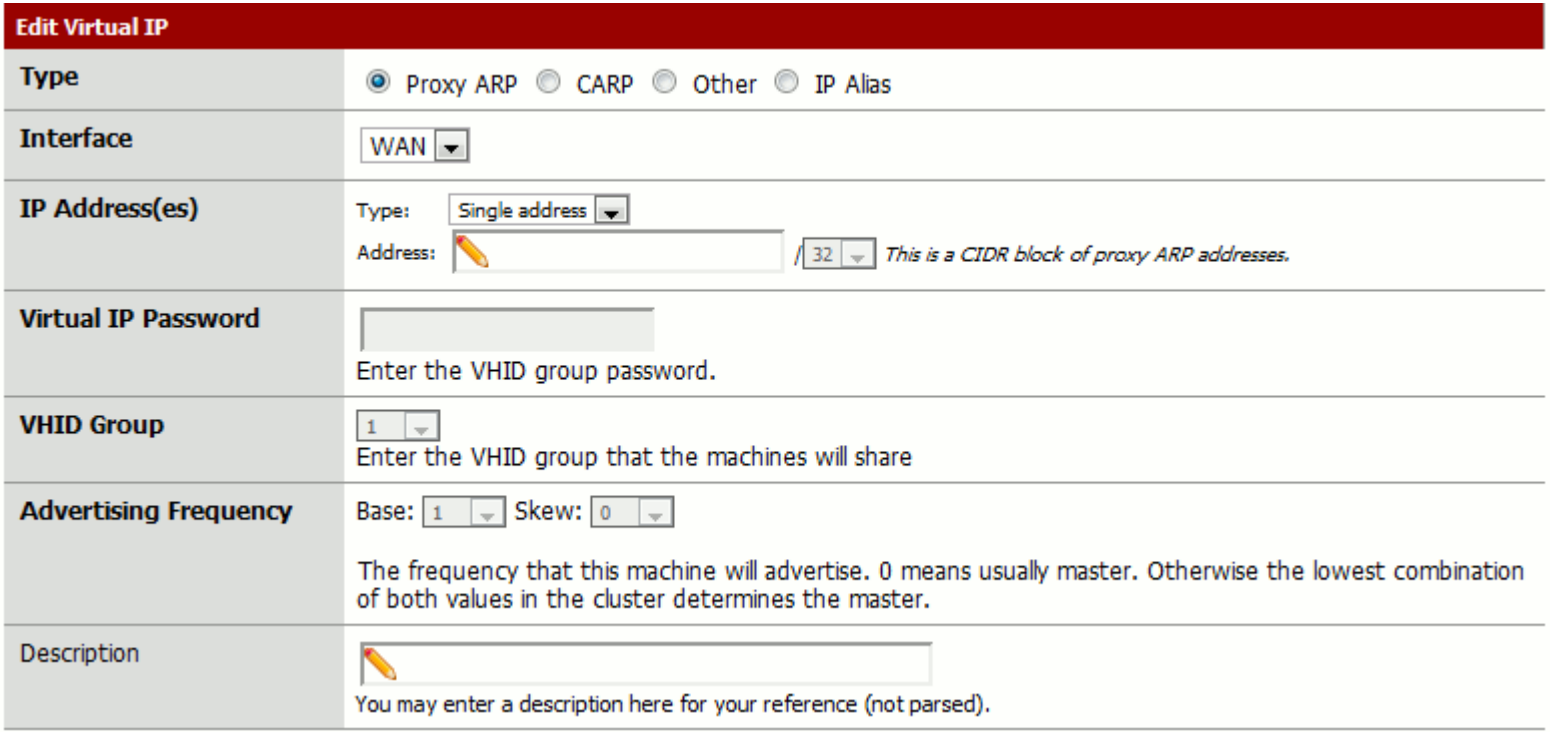
FIREWALL - SCHEDULES

Oluşturulan schedule tanımları kurallara uygulanır. Böylece ilgili kurallark spesifik zaman aralıklarında çalışmalarını sağlayabilirsiniz.



FIREWALL - VIRTUAL IPs

PfSense üzerinde kullanılan sanal IP adresleridir Özellikle NAT ve Port yönlendirme işlemleri için kullanılır. pfSense 2.0 sürümünden itibaren ağ arayüzlerine ikinci IP adresi tanımlama işlemleri de "Virtual IPs" bölümünden yapılmaktadır. Ayrıca failover pfSense (Carp) yapılandırmalarında da sanal IPler kullanılır.



FIREWALL - VIRTUAL IPs

Toplam olarak 4 farklı virtual IP tipi bulunmaktadır.

IP Alias:

- Firwall'un kendi servisleri ya da yönlendirmeler için kullanılır
- Ağ arayüzlerine ikinci IP adresi eklenmesine olanak sağlar
- pfSense 2.0 sürümünden itibaren vardır

Proxy ARP:

- Yönlendirme işlemleri için kullanılır
- Ağ arayüzü ile farklı subnette olabilir
- Ping'e yanıt vermez

FIREWALL - VIRTUAL IPs

CARP:

- Firwall'un kendi servisleri ya da yönlendirmeler için kullanılır.
- Cluster işlemleri içindir
- Ağ arabirimi ile aynı subnette olması gerekir
- Firwall'dan izin verilirse ping'e cevap verir.

OTHER:

- Sadece yönlendirme işlemleri için kullanılabilir.
- Ağ arayüzünden farklı subnette olabilir.
- Ping'e yanıt vermez.

BÖLÜM 6
Network Address Translation

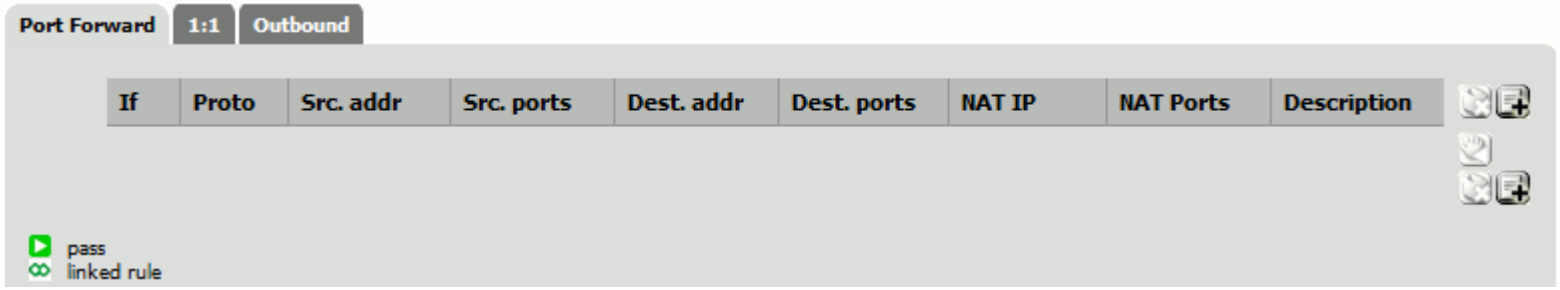
NAT

PfSense üç farklı NAT özelliği sunar:

Port Yönlendirme: Klasik port yönlendirme işleri için kullanılır. LAN'da bulunan herhangi bir servise (port) WAN üzerinden erişilebilmesine olanak sağlar.

1:1 NAT: Belirtilen IP adresine gelen trafiği bir hedef IP adresine yönlendirir. Bunun için kullanılacak internet IP'leri virtual IP (proxy arp) olarak tanımlanmalıdır.

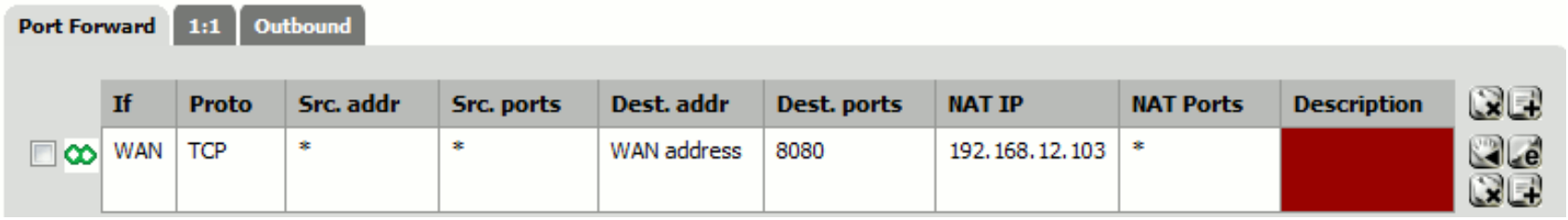
Outbound NAT: Spesifik bir hostun ya da networkün dışarıya spesifik bir IP üzerinden çıkarılması için kullanılır.



NAT - Port Yönlendirme

Senaryo 1:

WAN arayüzünden gelen ve hedef portu 8080 olan tcp trafiğini 192.168.12.103 adresine yönlendir.



If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
WAN	TCP	*	*	WAN address	8080	192.168.12.103	*	

Senaryo 2:

WAN arayüzünden gelen ve hedef portu 587 olan tcp trafiğini LAN'da bulunan 192.168.12.103 adresinin 25. portuna gönder.

WAN	TCP	*	*	WAN address	587	192.168.12.103	25 (SMTP)	

1:1 NAT

Senaryo:

WAN arayüzünden 86.19.12.103 gelen tüm trafiği 192.168.12.103 adresine yönlendir.

1- Önce ilgili dış IP için Proxy ARP türünde bir VirtualIP tanımlanır:

2- 1:1 Nat girdisi oluşturulur:

Interface	External IP	Internal IP	Destination IP	Description
WAN	86.19.12.103	192.168.12.103	*	1:1 Nat

OUTBOUND NAT

Senaryo:

192.168.12.103 host'unu internete çıkarken 86.19.12.103 olarak dönüştür

1- Önce ilgili dış IP için Proxy ARP türünde bir VirtualIP tanımlanır:

2- Outbound Nat girdisi oluşturulur:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
☐	WAN	192.168.12.103/32	*	*	*	86.19.12.103	*	NO	Outbound

BÖLÜM 7
VPN SERVİSLERİ

VPN

Uzak ağları güvenli olarak birbirine bağlamak ya da uzaktaki kullanıcıların ağa bağlamak üzere kullanılır.

pfSense tarafından aşağıdaki VPN çözümleri desteklenir.

- IPSec
- OpenVPN
- PPTP
- L2TP

VPN - IPSec

IPSec genel olarak site-to-site olarak tabir edilen farklı networkleri birbirine bağlamak üzere kullanılan VPN türüdür.

Genel senaryo şirketlerin ofislerinin, merkez ofis networküne güvenli ve kalıcı bir şekilde birbirlerine bağlanmasıdır.

UDP Port 500 ve ESP/AH protokolleri üzerinden çalışır.

IPSec ile site-to-site VPN yapabilmek birbirine bağlanacak her networkün ayrı IP subnetlerinde olmaları gerekir.

VPN - OpenVPN

OpenVPN, client-to-site diye tabir edildiği şekilde internet üzerindeki kullanıcıların yerel ağa güvenli olarak dahil edilmesi için kullanılan VPN çeşididir.

UDP Port 1194 kullanır. İletişim encrypt olarak sağlanır.

Standart VPN çözümü olarak sayılabilir ancak MS işletim sistemleri tarafından öntanımlı desteklenmediğinden bu sistemlerde OpenVPN client yazılımının indirilmesi zorunluluğu vardır.

VPN - PPTP

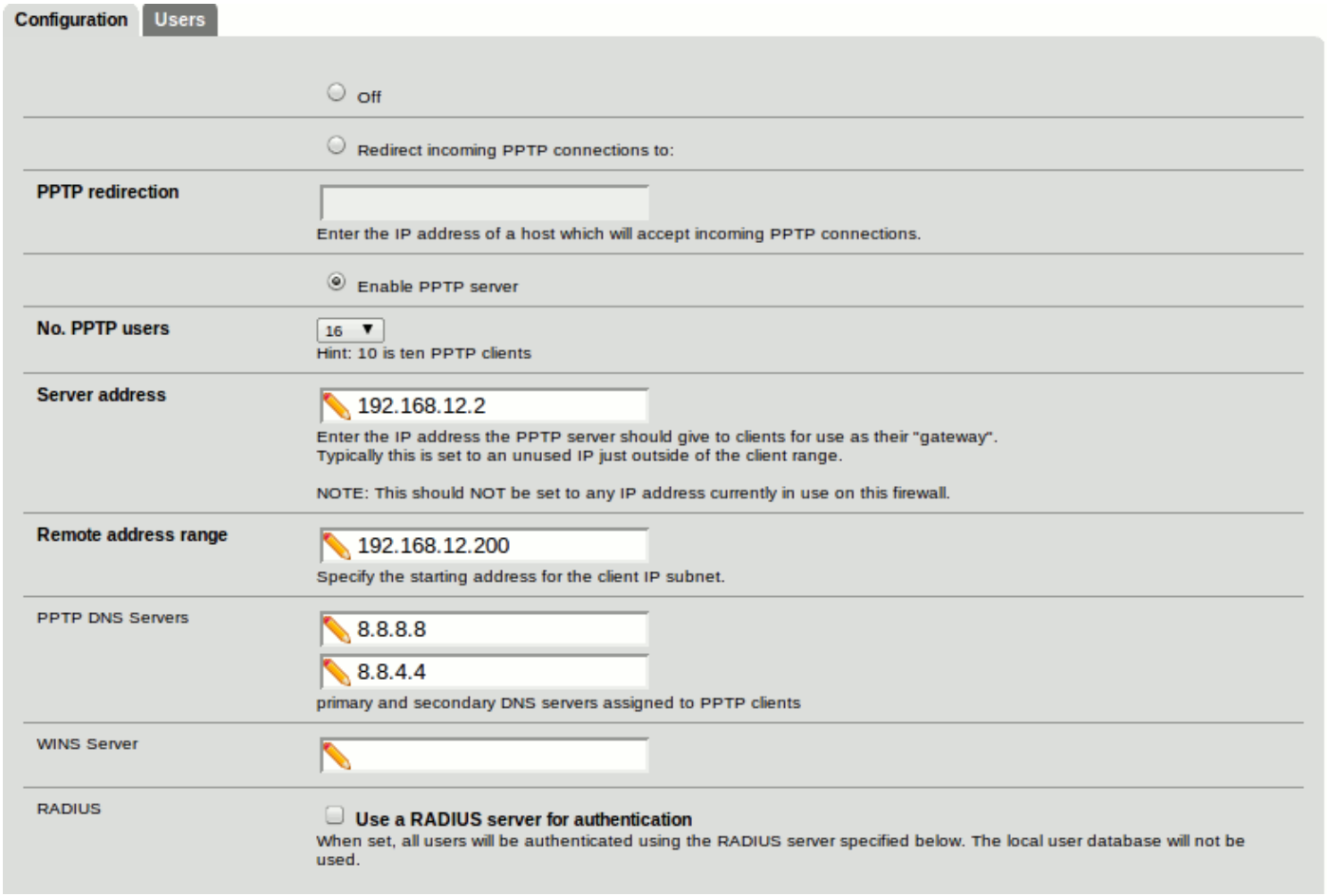
OpenVPN benzeri bir VPN çözümüdür.

TCP port 1723 ve GRE protokolü kullanır.

İletişim encrypt olarak sağlanır.

Hemen her işletim sisteminde öntanımlı olarak geldiğinden dolayı yaygın olarak kullanılan VPN teknolojisidir.

VPN - PPTP


Configuration
Users
Off
Redirect incoming PPTP connections to:
PPTP redirection
Enter the IP address of a host which will accept incoming PPTP connections.
Enable PPTP server
No. PPTP users
16
Hint: 10 is ten PPTP clients
Server address
192.168.12.2
Enter the IP address the PPTP server should give to clients for use as their "gateway".
Typically this is set to an unused IP just outside of the client range.
NOTE: This should NOT be set to any IP address currently in use on this firewall.
Remote address range
192.168.12.200
Specify the starting address for the client IP subnet.
PPTP DNS Servers
8.8.8.8
8.8.4.4
primary and secondary DNS servers assigned to PPTP clients
WINS Server
RADIUS
Use a RADIUS server for authentication
When set, all users will be authenticated using the RADIUS server specified below. The local user database will not be used.


Configuration
Users
Username
IP address
vpnuser
192.168.12.201

BÖLÜM 8
MULTIWAN
LOAD BALANCING
&
FAILOVER

LOAD BALANCING & FAILOVER

pfSense birden fazla WAN bağlantısı için hem yük dengeleme hem de hatlardan birinin gitmesi durumunda trafik akışının diğer hat üzerinden devam ettirilmesi için yük aktarma olanağı sağlamaktadır.

MultiWAN senaryolarında kural bazlı olarak routing (policy based routing) yapmak da mümkündür. Bu şekilde spesifik trafik istenen herhangi spesifik bir hattan çıkarılabilir.

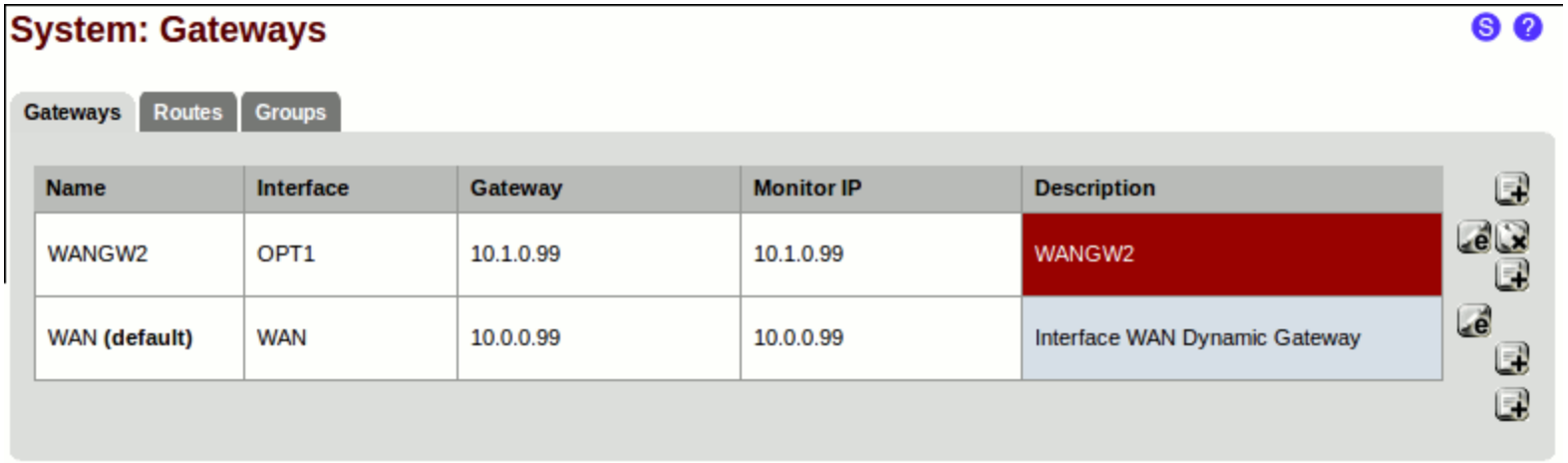
LOAD BALANCING & FAILOVER

Ayrıca, örnek olarak web gibi bellirli tipteki trafiği de birden fazla sunucuya eşit olarak dağıtabilir.

Aynı mantıkla birden fazla sunucunun yük aktarmak üzere yedekli olarak kullanılmasını da sağlayabilir.

MULTI WAN GATEWAY

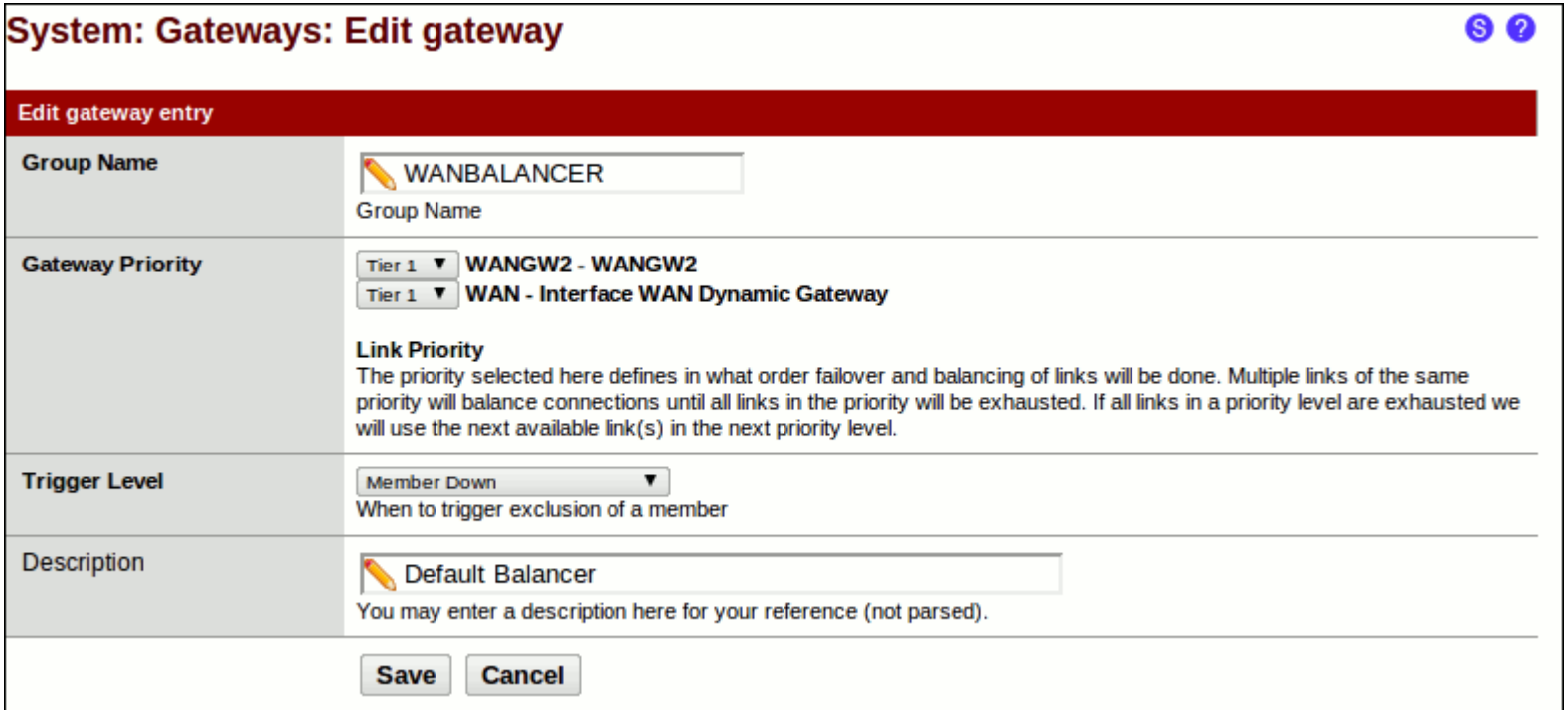
MultiWAN GW tanımlamaları "System" menusunde bulunan Routing segmentinden yapılır.



Her iki WAN hattının bağlı olduğı interface'e ait gateway'ler burada Gateways tabında tanımlanırlar.

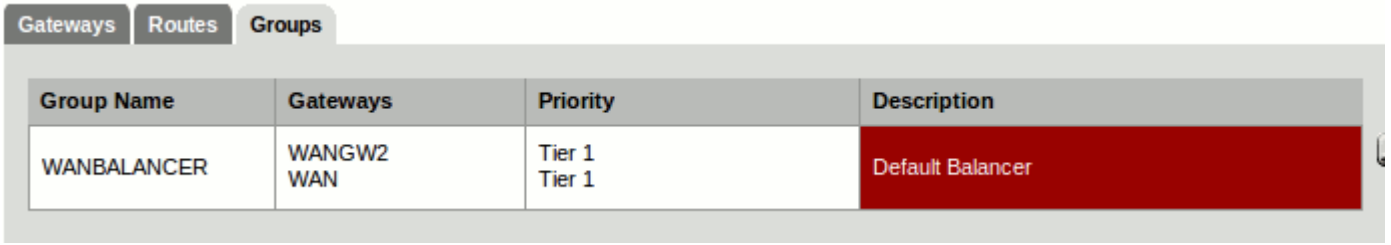
MULTI WAN / LOAD BALANCE

Her iki WAN üzerinden eşit olarak trafik geçirerek Yük Dengeleme için "Routing" menusundeki "Groups" tabı kullanılır ve her iki WAN tier1 olarak gruplanır.



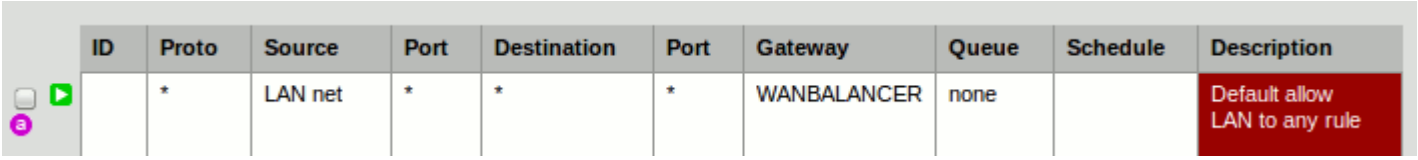
MULTI WAN / LOAD BALANCE

İki WAN gateway'inin gruplanması ile load balancer oluşturulmuş olur.



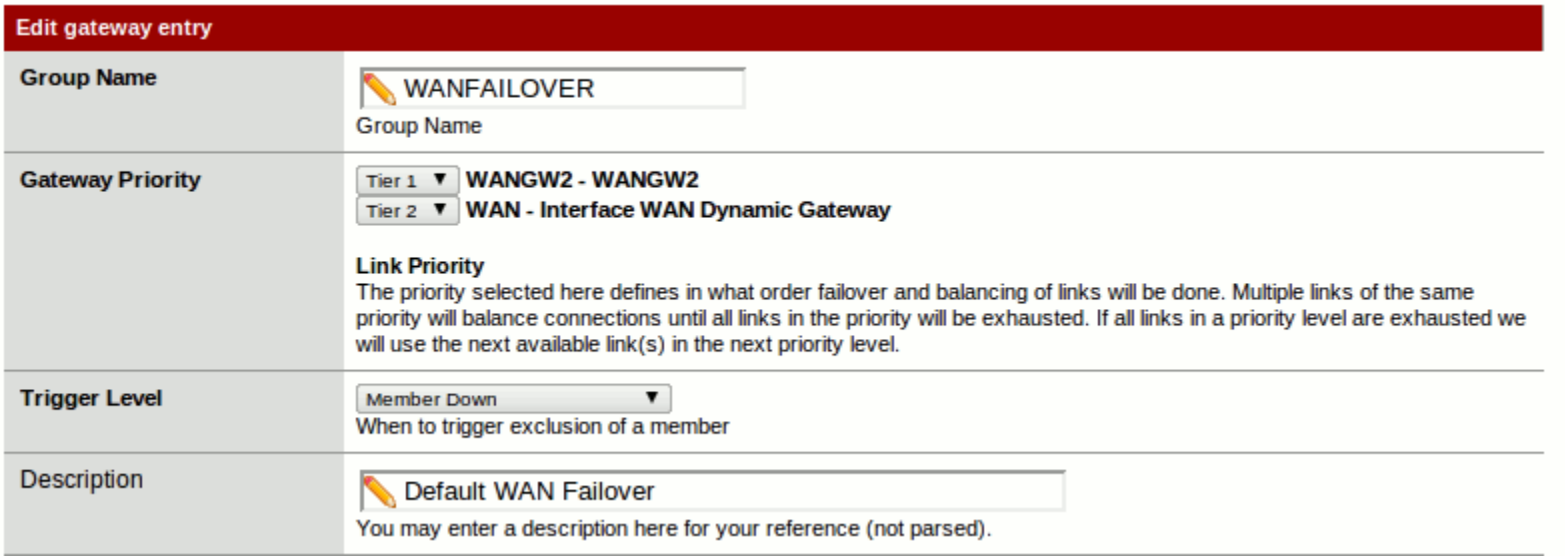
LAN tarafından oluşturulan tüm trafiğin bu balancer üzerinden geçirilmesi için ilgili firewall kuralında gateway olarak WANBALANCER isimli gateway seçilir:

Böylece ilgili kural için MULTI WAN GW kullanılacaktır.



MULTI WAN / FAILOVER

Eşit yük dengeleme yerine hatlardan birisi giderse diğerini kullanmak üzere WAN gateway gruplaması sırasında tier değerlerini değiştirerek öncelik beli

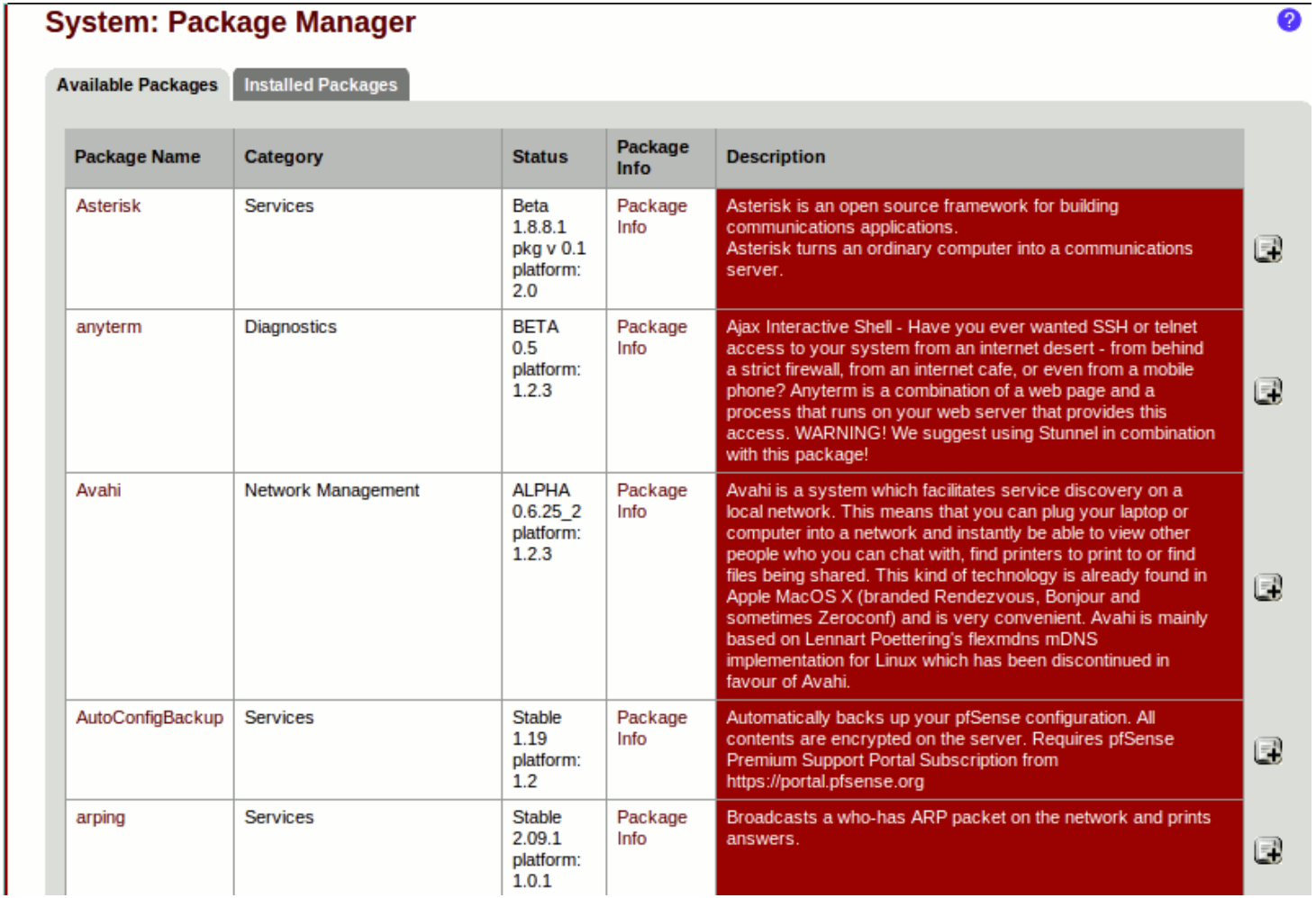


Böylece Tier 1 olan hat öncelikli kullanılır ve down olması durumunda diğer hat kullanılmaya başlanır.

BÖLÜM 9
DİĞER SERVİSLER

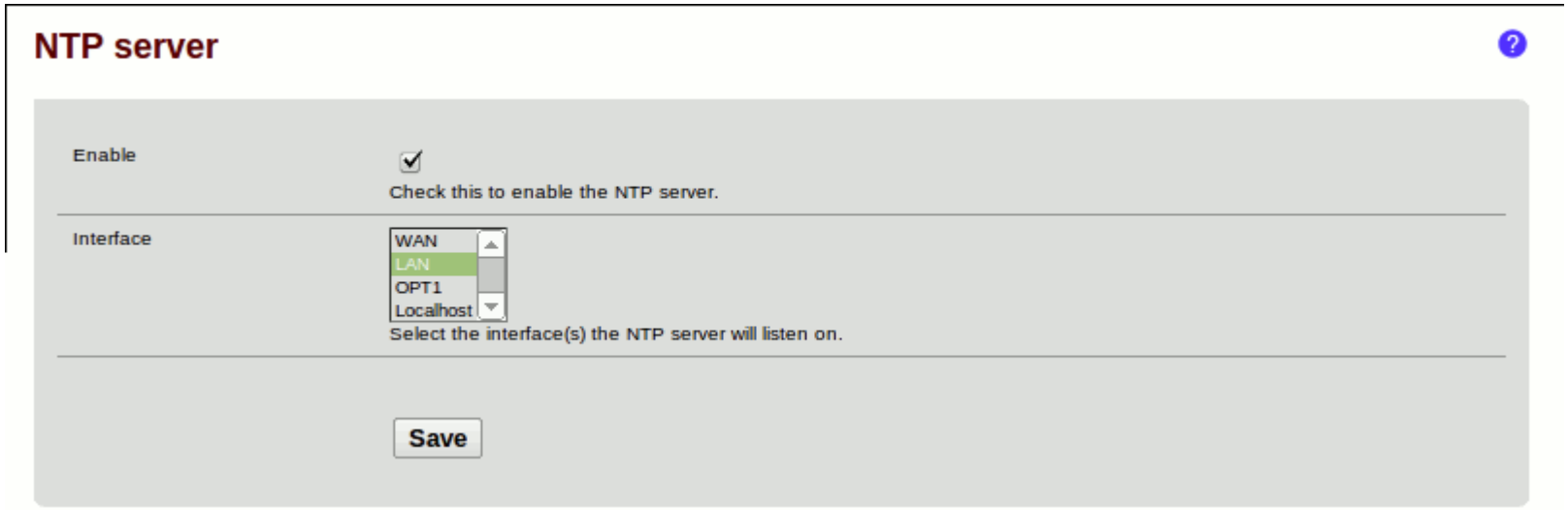
PAKET SİSTEMİ

Ek servisler ve uygulamalar System > Packages menusunden kolayca kurulabilmektedir.



OPENNTPD

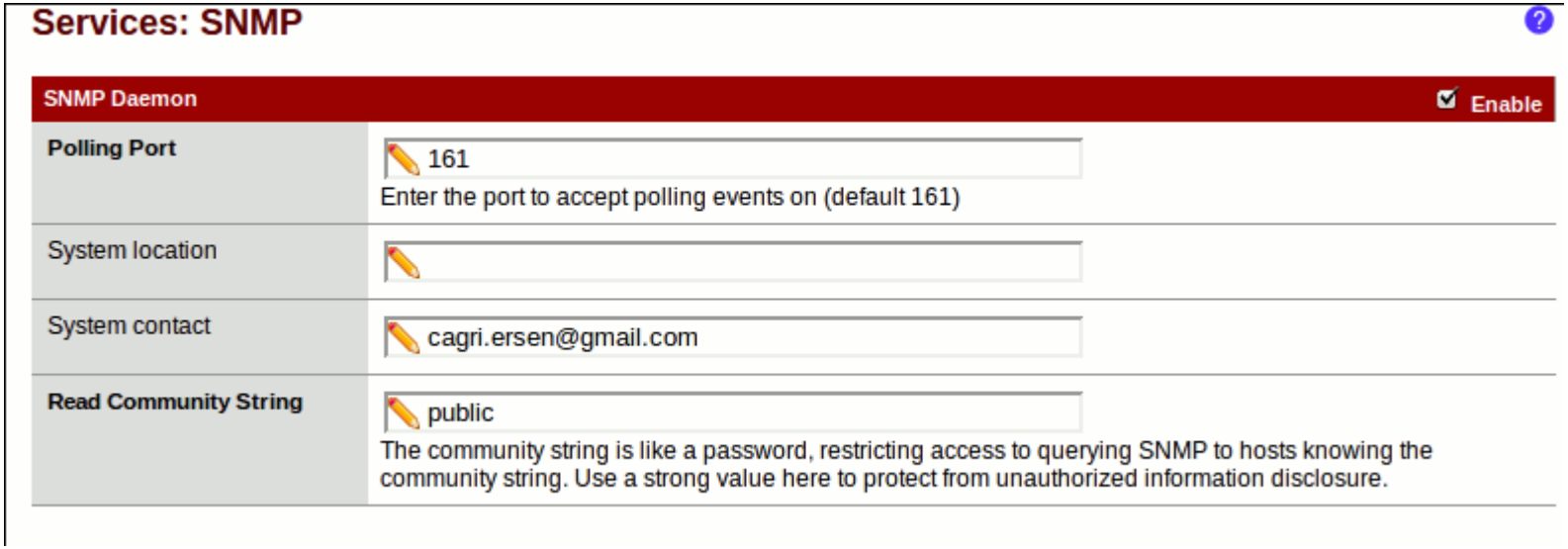
pfSense'de OpenNTPD server da bulunmaktadır. Bu nedenle ağınızdaki bilgisayarlara zaman senkronizasyon hizmeti vermeye olanak sağlar.



SNMP

pfSense'in SNMP hizmeti sistem durumunu uzaktan cacti, nagios gibi herhangi bir monitoring aracı ile monitor edebilmek mümkündür.

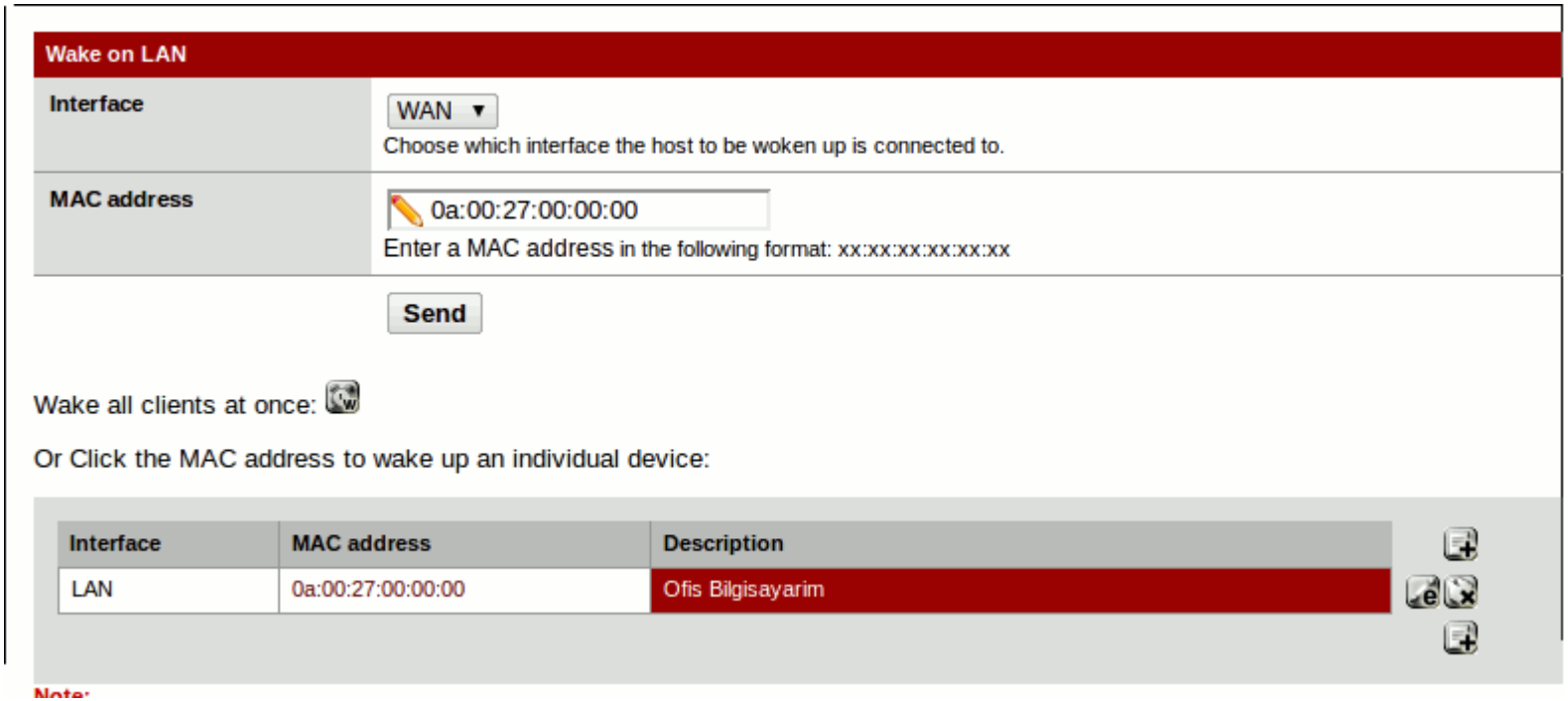
SNMP üzerinden ağ arayüzleri, sistem kaynakları, firewall kuralları hakkında istatistiki bilgiler edinilebilir.



Wake On LAN

Herhangi bir bilgisayarı ağ üzerinden açmak için kullanılan Wake On Lan hizmeti, açılacak bilgisayara "magic packet" denilen bir paket göndererek bilgisayarın açılmasını sağlamaktadır.

Bu hizmeti kullanabilmek için istemci bilgisayarın ağ kartının wake on lan desteği iolması gerekmektedir.

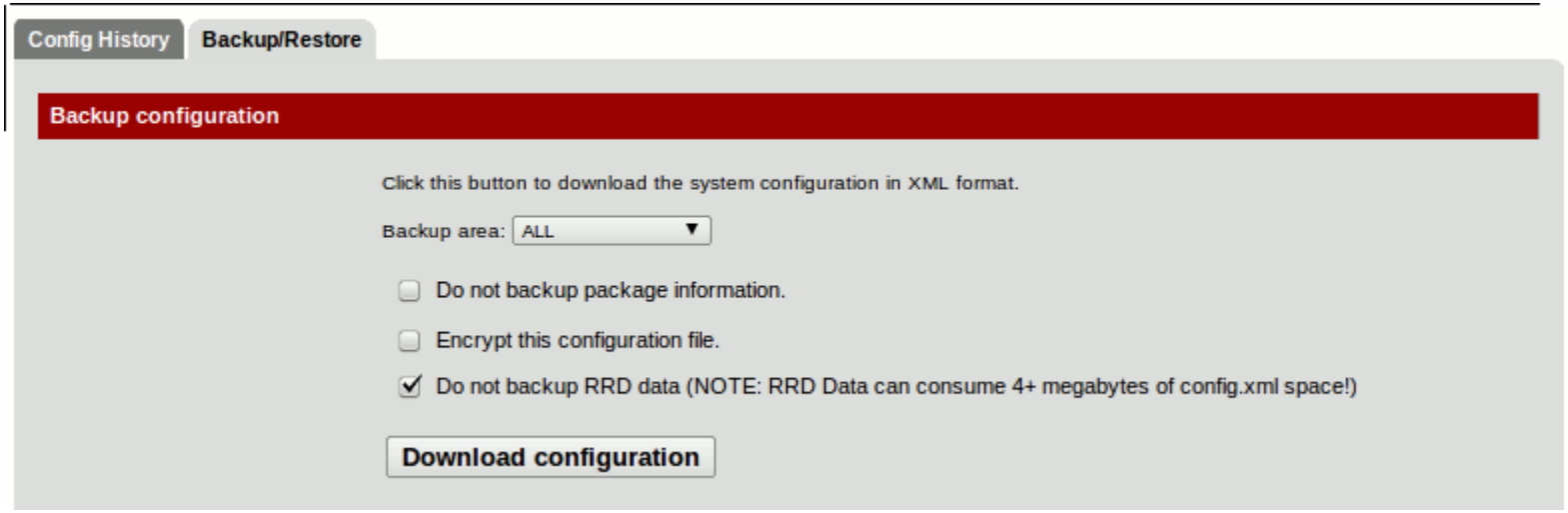


BÖLÜM 10
BAKIM VE MONITORING

BACKUP

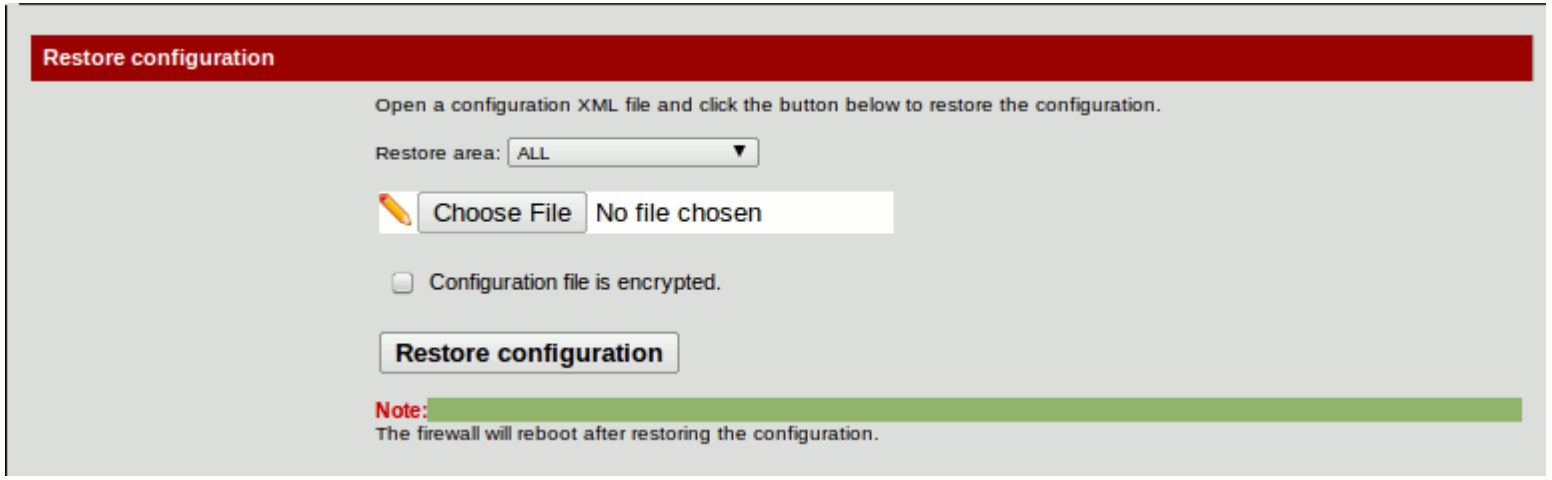
pfSense'in bütün yapılandırma dosyaları XML tabanlıdır.

Yapılandırmayı yedeklemek için "Diagnostics" menusunden "Backup/Restore" alt menüsüne gitmek ve "Download Configuration" seçeneğini kullanmak yeterlidir.



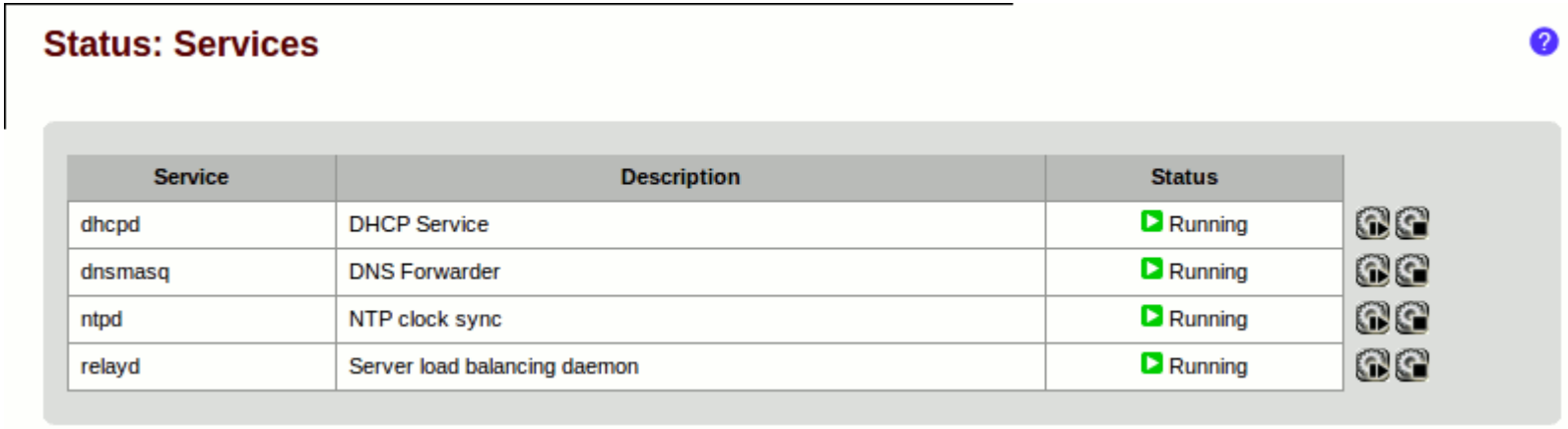
RESTORE

Yapılanıdırmayı yedekten dönmek için ise "Backup/Restore" alt menüsünde bulunan "Restore Configuration" seçeneğini kullanılmaktadır.



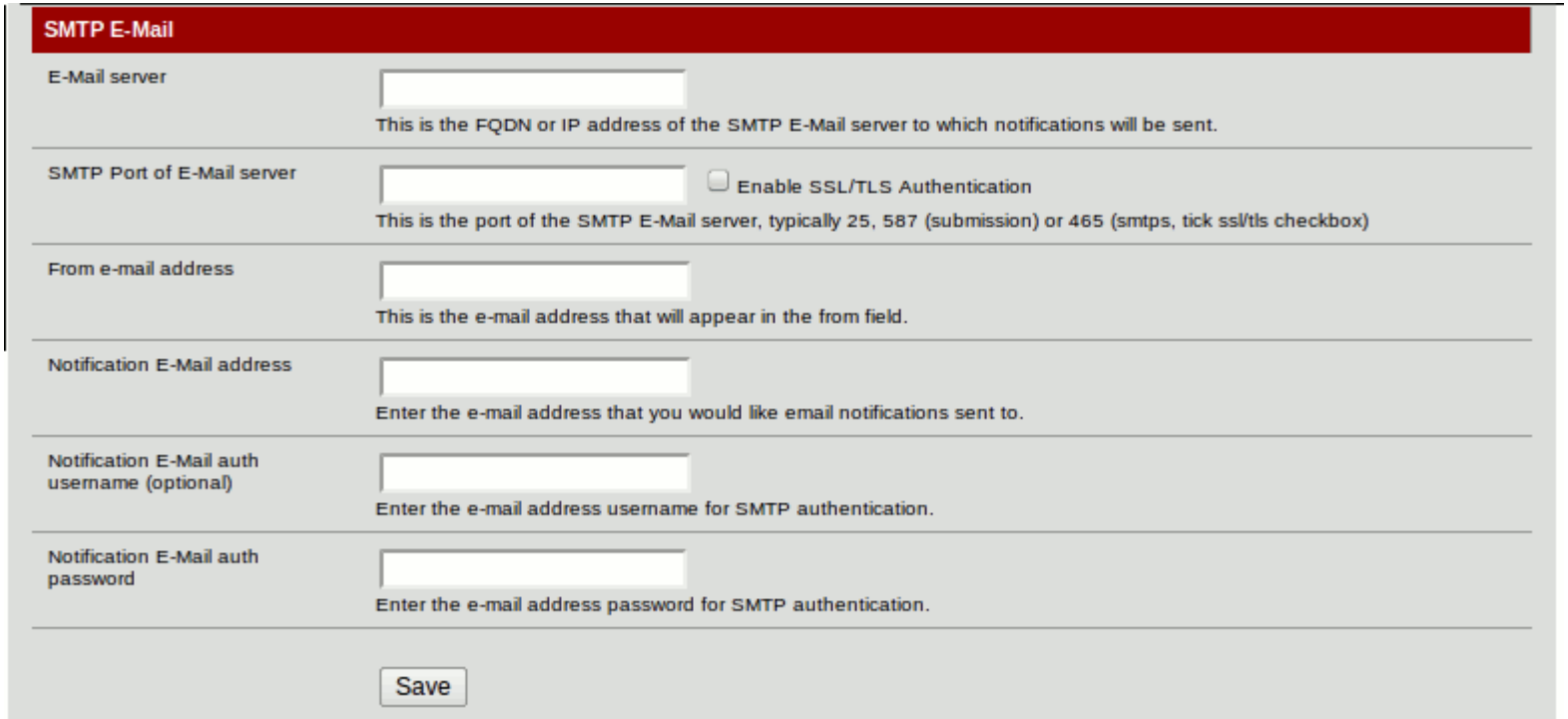
SERVİSLERİN YÖNETİLMESİ

Çalışmakta olan servislerin listesi Status Menusunde bulunan Services sekmesinde bulunur ve buradan start/stop/restart yapılabilir.



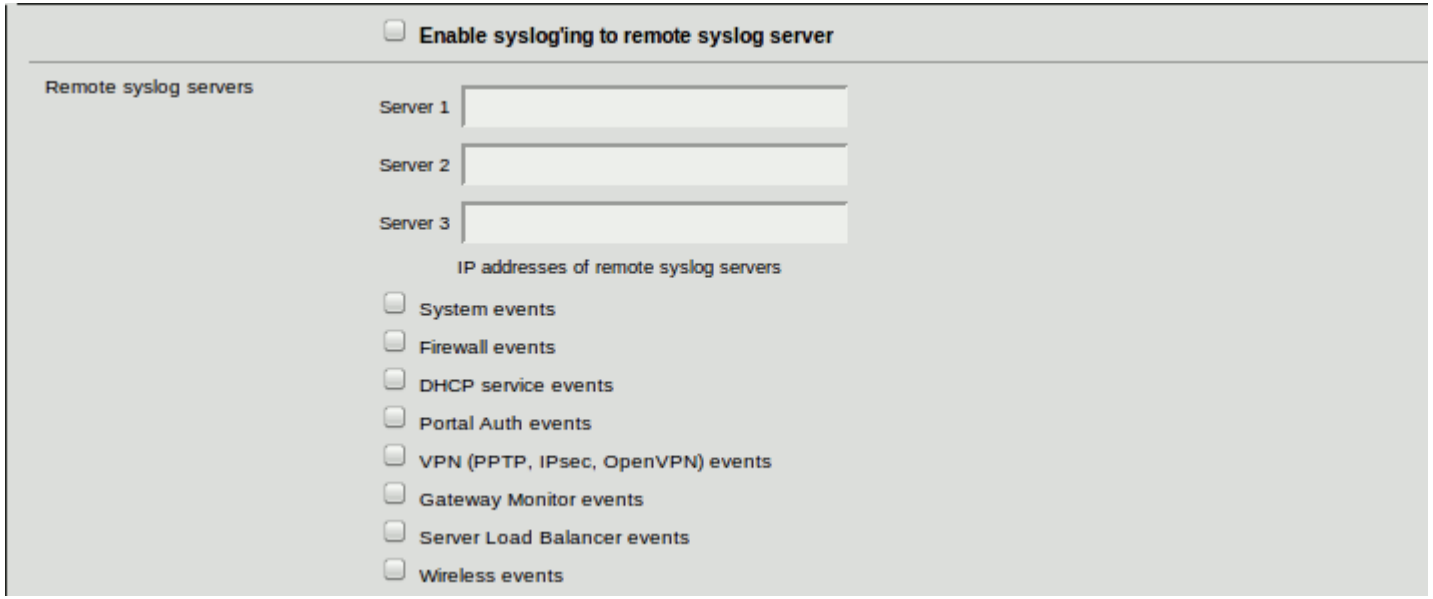
E-MAIL DURUM BİLDİRİMLERİ

Sistem durumu ile ilgili raporların e-mail ile gönderilmesi için SMTP ayarları "System > Advanced" menusunde bulunan "Notification" tabından yapılmaktadır.



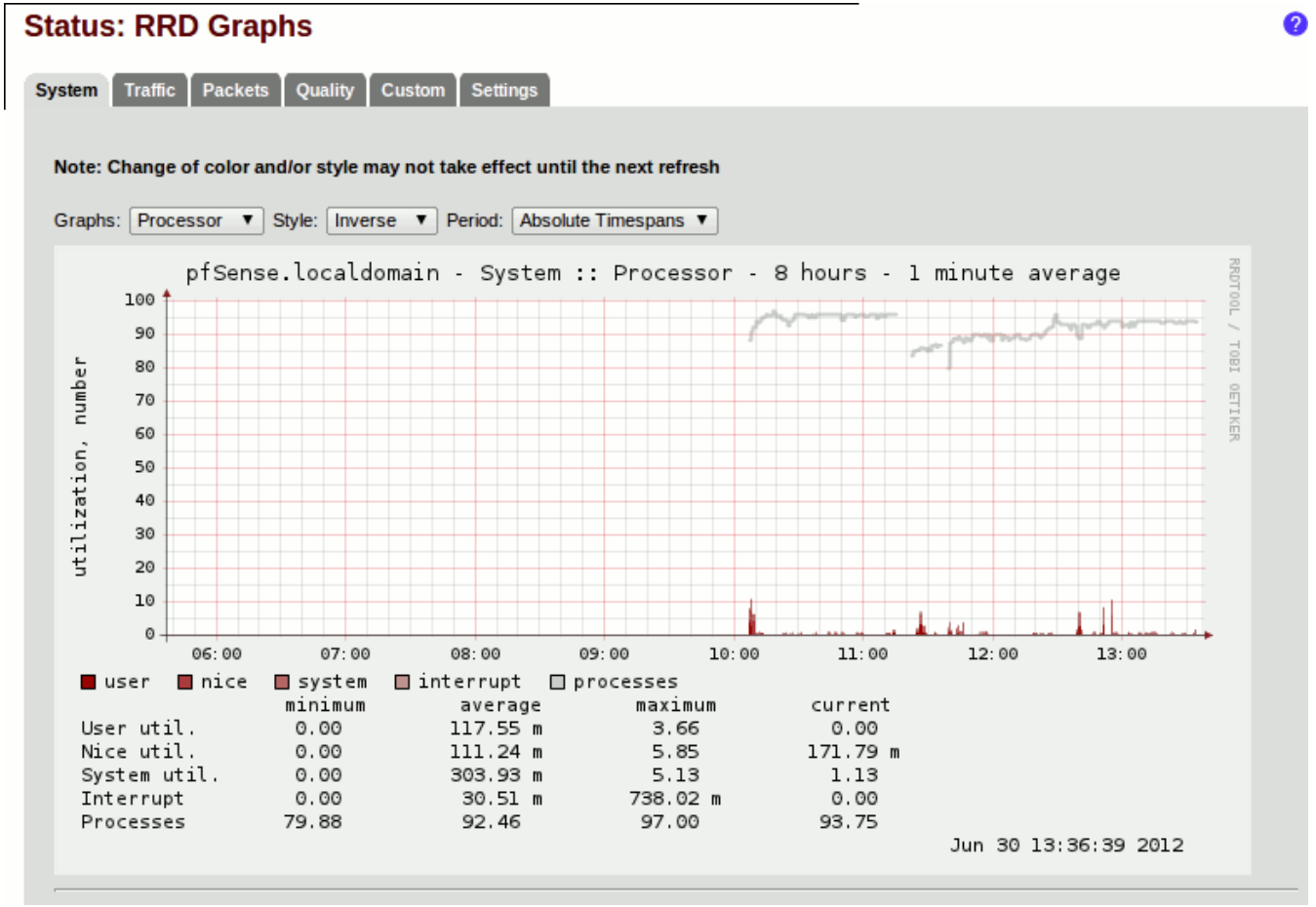
Kayıtları Log Sunucusna Göndermek

Merkezi bir log sunucunuz varsa, sistem kayıtlarını bu log sunucuya gönderebilirsiniz. İlgili ayarlar "Status > System Logs > Settings" menusunden yapılmaktadır.



RRD Grafikleri

Status menüsünden ulaşılan RRD Grafikleri, geçmişe yönelik olarak cpu,ram,trafik ve durum tablosu bilgilerini grafiksel olarak ve sayısal olarak sunar.



Sistem Loglarının Görüntülenmesi

pfSense ile ilgili her türlü log bilgisi, "Status > System Logs" menusunde bulunmaktadır.