BİLGİ GÜVENLİĞİ
AKADEMİSİ

pfSense Firewall ve Router Eğitimi

Ozan UÇAR

ozan.ucar@bga.com.tr

Bilgi Güvenliği Akademisi
İstanbul 2012

Eğitim Hakkında

pfSense Firewall ve Router eğitimi; paket filtreleme sistemlerinin çalışma yapısı, network trafiğinin yönlendirilmesi, vpn ağlarının kurulması konularında bol teorik ve gerçek sistemler üzerinde bu işlemlerin nasıl yapıldığını uygulamalı olarak içeren bir eğitimdir.

Ülkemizdeki yer sağlayıcıları, erişim sağlayıcıları ve içerik sağlayacıları ilgilendiren 5651 kanunu ve pfSense üzerinde uygulama senaryolarını içermektedir.

Bu eğitim, FreeBSD ve TCP/IP eğitimi **değildir.**

Amaç ve Hedefler

- Güvenlik duvarları ve çalışma prensiplerinin anlaşılması
- Ağ tabanlı saldırıların tespitini ve engellenmesini sağlamak
- İnternet ve yerel ağ trafiğini yönetmek ve raporlamak
- Web trafiğinin filtrelenmesi ve raporlanmasını sağlamak
- Anlık iletişim araçlarının kontrolü
- VPN ile uzak ağları birleştirmek, güvenli iletişim kanalları oluşturmak
- Güvenli kablosuz ağlar yaratmak ve yönetmek
- Kimlik doğrulamalı sınır kapısı oluşturmak
- Yük dengeleme, yük aktarma ve yedekli çalışma stratejileri
- Trafik şekillendirme

Parola: ?

Ezber değil MANTIK !

Sertifikasyon

- Eğitim sonrası katılım sertifikası verilecektir.

Notlar

- Network şemaları www.gliffy.com adresinden oluşturulmuştur. Network şemaları özel olarak isimlendirilmiştir.
- Tüm uygulamalar, vmware sanallaştırma platformunda test edilecektir. win2k3, xp, freebsd, linux ve pfSense kuruludur.
- Cisco switch ve router gereksinimi için gns3lab kullanılmıştır.
- Ek modül ve geliştirmeler, yazılımların pfSense'e port edilmesi için FreeBSD 8.2 işletim sistemi kullanılmıştır.
- Senaryolar, gerçek dünyadan kurumsal networklerin ihtiyaçları göz önüne alınarak oluşturulmuştur.

Eğitim İçeriği

1. **OpenBSD PF Packet Filter Giriş**
2. **PF Aktif Edilmesi ve Kontrolü**
3. **pf.conf Konfigürasyon Dosyası**
4. **PF Tabanlı Firewall Dağıtımları**
5. **pfSense Giriş**
6. **Donanım**
7. **Kurulum ve Yükseltme**
8. **Konfigürasyon**
9. **Interfaces**
10. **Wireless**
11. **Servisler**
12. **Firewall**
13. **NAT (Network Address Translation)**
14. **Routing**

Eğitim İçeriği | Devam

15. **Bridging**
16. **Multiple Wan**
17. **Incoming Server Load Balancing**
18. **CARP, Redundancy Firewall, pfsync**
19. **VPN**
20. **Trafik Şekillendirme (Traffic Shaper)**
21. **Captive Portal**
22. **Sistem Monitör**
23. **Paket Sistemi**
24. **Snort**
25. **Squid**
26. **SquidGuard**
27. **HAVP Antivirus**
28. **Cron**

Eğitim İçeriği | Devam

29. BandwidhD

30. IMSpector

31. Yedekleme ve Kurtarma

32. 5651 Sayılı Kanuna Göre Log Toplama ve İmzalama

33. Geliştiriciler İçin pfSense

34. Pfsense ile Özelleştirilebilir Güvenlik Duvarı Oluşturmak

35. Uygulama Senaryoları

Zaman Yönetimi

1. Gün	2. Gün	3. Gün
09:30 – 10:15 I. Ders	09:30 – 10:15 I. Ders	09:30 – 10:15 I. Ders
10:15 – 10:30 ARA	10:15 – 10:30 ARA	10:15 – 10:30 ARA
10:30 – 11:15 II. Ders	10:30 – 11:15 II. Ders	10:30 – 11:15 II. Ders
11:15 – 11:30 ARA	11:15 – 11:30 ARA	11:15 – 11:30 ARA
11:30 – 12:15 III. Ders	11:30 – 12:15 III. Ders	11:30 – 12:15 III. Ders
12:15 – 13:15 Yemek Arası	12:15 – 13:15 Yemek Arası	12:15 – 13:15 Yemek Arası
13:14 – 14:00 IV. Ders	13:14 – 14:00 IV. Ders	13:14 – 14:00 IV. Ders
14:00 – 14:15 ARA	14:00 – 14:15 ARA	14:00 – 14:15 ARA
14:15 – 15:00 V. Ders	14:15 – 15:00 V. Ders	14:15 – 15:00 V. Ders
15:00 – 15:15 Ara	15:00 – 15:15 Ara	15:00 – 15:15 Ara
15:15 – 16:00 VI. Ders	15:15 – 16:00 VI. Ders	15:15 – 16:00 VI. Ders
16:00 – 16:15 Ara	16:00 – 16:15 Ara	16:00 – 16:15 Ara
16:15 – 17:30 VII. Ders	16:15 – 17:30 VII. Ders	16:15 – 17:30 VII. Ders

Bölüm 1:
OpenBSD Projesi

- ’95 yılında Theo De Raadt başkanlığında 4.4 BSD Lite tabanlı “Özgür” bir UNIX çeşidi...
- 2011: 16 Yaşında
- Güvenlik ve Kararlılık öncelikli bir proje
- Ne yaptığını bilen bir ekip
- Çoğu popüler güvenlik ürünlerinde bileşenleri var
  - Dhcp
  - Pf
  - ssh vs.

Bölüm 1:
OpenBSD Packet Filter

OpenBSD PF'in güvenlik duvarı olarak sağladığı özellikler piyasada bulunabilecek herhangi bir güvenlik duvarından oldukça farklıdır.

Bu yönü ile hem ticari hem de özgür yazılımlar arasında parmak ile gösterilebilecek bir konuma sahiptir.

Yedekli çalışma, yük dengeleme, yük aktarma, synproxy özellikleri ile gelişmiş bir firewall uygulamasıdır.

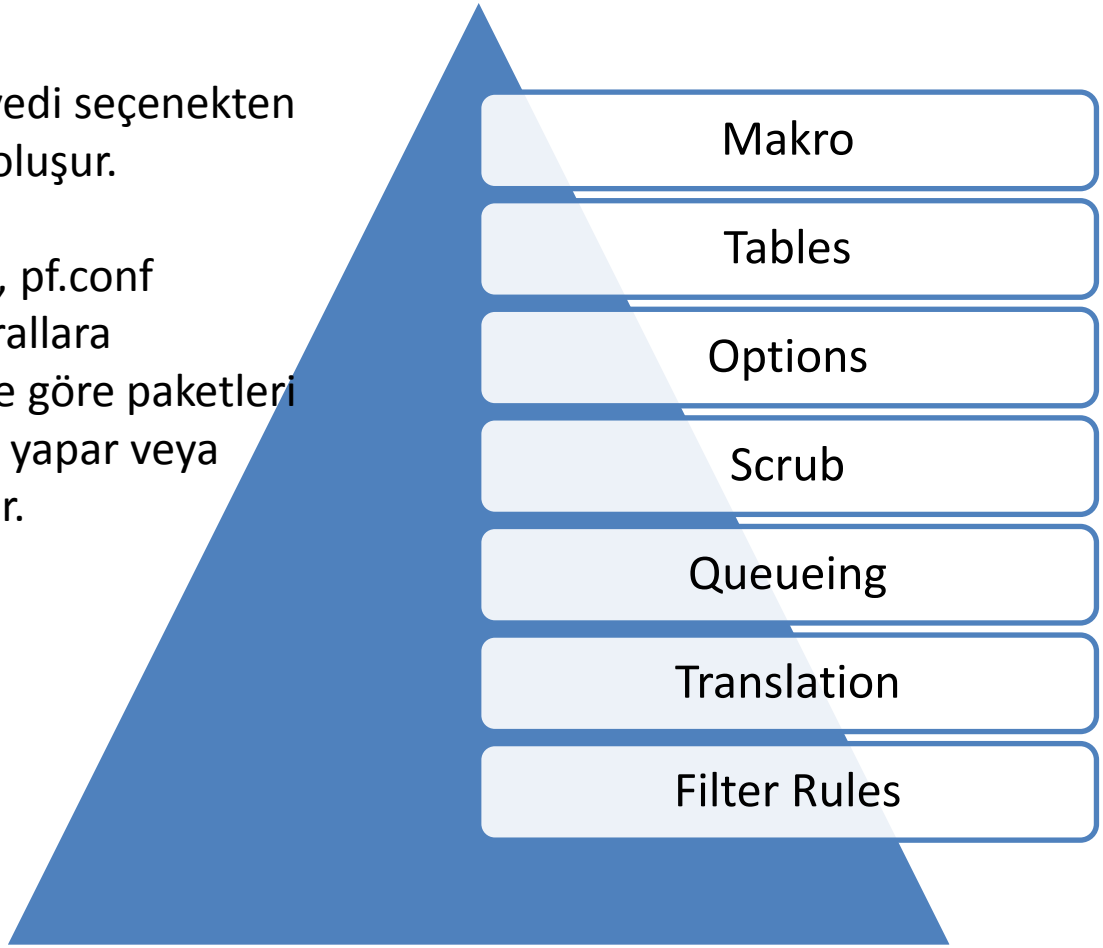
Bölüm 2:
PF Aktif Edilmesi ve Kontrolü

PF Aktif Edilmesi	PF Kontrolü
▪OpenBSD için # pf=YES > /etc/rc.conf.local ▪FreeBSD için #kldload pf #pf_enable=YES > /etc/rc.conf	**PF Kontrol Edilmesi** ▪pf kaptılması #pfctl -d ▪pf.conf yüklemek #pfctl -f /etc/pf.conf ▪Parse et, fakat yükleme #pfctl -nf /etc/pf.conf ▪Sadece NAT kurallarını yükle #pfctl -Nf /etc/pf.conf ▪Geçerli Filtreleme kurallarını listele #pfctl -sr ▪Durum tablosunu listele #pfctl –ss *Not:Daha falza bilgi için pfctl(8) man sayfasına bakınız.*

Bölüm 3:
pf.conf dosyası

pf.conf dosyası yedi seçenekten ve sıralamadan oluşur.

packet filter (pf), pf.conf dosyasındaki kurallara veya seçeneklere göre paketleri durur, değişlik yapar veya geçişine izin verir.



Bölüm 3:
pf.conf dosyası

Macro

Makroları, programlama dilindeki değişkenlere benzetebiliriz.

ext_if= “em0”

Tables

Tablolar, IP adresi gruplarıdır.

Table <spamciler> persist {1.2.3.0/24,4.5.6.0/24}

Options

PF sahip olduğu çeşitli seçenekler. Örneğin, iz sürmeleri engelle

set fingerprints file

Scrub

Paket normalleştirme. Anormal trafiği düzenler ve parçalanmış paketleri birleştirir.

scrub in all

Queueing

Trafik şekillendirme ve bandwidth yönetimi

altq on em0 cbq bandwidth 2MB queue {ssh,ftp}

Bölüm 3:
pf.conf dosyası

Translation

NAT, PAT, 1:1NAT işlemlerini tanımlar

nat on $ext_if from $lan_net to any ->($ext_if)

Filter Rules

Paket filtreleme kurallarını içerir

block in on $ext_if proto tcp from any to any port ssh

Bölüm 4:
PF Tabanlı Firewall Dağıtımları

m0n0wall

FreeBSD işletim sistemi ve PF güvenlik duvarını kullanan ilk açık kaynak kodlu güvenlik duvarı dağıtımıdır.

- **M0n0wall tabanlı bazı dağıtımlar ;**
  - pfSense
  - AskoziaPBX
  - FreeNAS

pfSense

M0n0wall temel alınarak geliştirilmiş firewall ve router dağıtımıdır.m0n0wall'dan bağımsız bir ekip tarafından geliştirilmektedir.Paket sistemi ile opensour bir çok uygulamayı desteklemektedir.

Bölüm 5:
pfSense Giriş

Neden pfSense

- FreeBSD sağlamlığını taşıyor
- OpenBSD PF güvenlik duvarı
- Kararlı ve Ne Yaptığını Bilen Bir Ekip
- Hızlı Destek
- Mail Listesi
- Forum Sayfası (13 Dilde Destek)
- IRC Kanalı
- Ticari Destek
- Yerel, Yerinde Destek
- CVS Server,CVSWeb, CVSTrack ticket desteği

Bölüm 5:
pfSense Destek ve Yardım Seçenekleri

Mail Listesi

pfSense Support Listesi, support-subscribe@pfsense.com adresine boş bir e-posta göndermeniz ve gelen onay mailini doğrulamanız yeterli.

pfsense-tr türkçe mail listesi, pfsense-tr+subscribe@googlegroups.com eposta adresine boş bir eposta göndermeniz yeterli.

Liste Arşivi
Bu liste birden fazla yerde arşivleniyor.

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

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

- **Mail-archive.com**
http://tinyurl.com/a3j3kp

Bölüm 5:
pfSense Destek ve Yardım Seçenekleri

Döküman ve Özel Dersler

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
www.cehturkiye.com/videolar/pfsense

Bölüm 5:
pfSense Destek ve Yardım Seçenekleri

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.

IRC kullanımını bilmiyorsanız, http://tr.wikipedia.org/wiki/IRC

Ticari Destek

pfSense geliştiricilerinden direkt destek alabileceğiniz ücretli bir hat. https://portal.pfsense.org/index.php/support-subscription sayfasından kayıt olup size uygun destek paketini seçmelisiniz.

Bölüm 5:
pfSense Destek ve Yardım Seçenekleri

CVS Server

Kaynak kodlar, ayar dosyaları ve script dosyalarına ulaşabilirsiniz,
http://cvs.pfsense.com/cgi-bin/cvsweb.cgi/

CVS Track

http://cvstrac.pfsense.org/

Bug'lar ve düzenlemeler hakkında rapor gönderebilirsiniz

Bug Listesi

http://redmine.pfsense.org/

Bölüm 6:
Donanım Seçimi

Desteklediği Donanımlar

Gömülü (Embedded) Sistemler

Tak çalıştır USB aygılar

Kurulum gerektirmeksizin çalışan CD'ler

CF Kartlar

Bölüm 6:
Minimum Donanım Gereksinimleri

pfSense 1.2.x sürümü için minimum donanım gereksinimleri;

CPU - 100 MHz Pentium

RAM - 128 MB

Diğer Platformlar

Live CD

CD-ROM drive

USB flash sürücü, ayarları saklamak için

Hard drive installation

CD-ROM, kurulum başlangıcı için

1 GB hard disk

Embedded

512 MB Compact Flash card

Seri port, yönetim için

Bölüm 7:
Full Kurulum

Symmetric Multiprocessing Kernel

Çok çekirdekli veya çok işlemcili donanımları destekler

~~**Uniprocessor Kernel**~~

~~Yalnızca tek çekirdekli donanımları destekler~~

Embedded Kernel

Gömülü anakartlar.VGA konsolu ve klavye kapalı,seri porttan yönetilir.

Developers Kernel

Debug seçeneklerinin aktif edildiği, geliştiriciler için

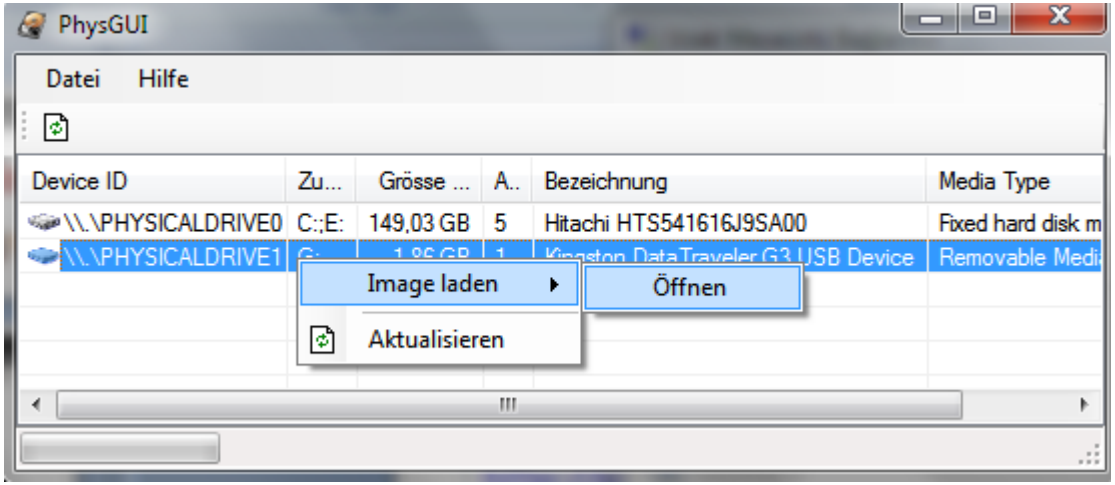
Bölüm 7:
Embedded Kurulum

Embedded iso imajları

http://pfsense.phoenixkv.net/downloads/

- Windows'dan Kurulum

physdiskwrite 0.5.2 + PhysGUI (188 KB) – .NET Framework 3.5 gerekli



Bölüm 7:
Embedded Kurulum

Embedded iso imajları

http://pfsense.phoenixkv.net/downloads/

- Linux üzerinden kurulum

 # gunzip –c pfSense-2.0.1-RELEASE-2g-i386-nanobsd.img.gz | dd of=/dev/hdX bs=16k

Not: CF kart veya IDE diskler /dev/hdX olarak isimlendirilir. USB veya SCSI diskler /dev/sdX olarak isimlendirilir.

- FreeBSD üzerinden kurulum

 # gunzip pfSense-2.0.1-RELEASE-2g-i386-nanobsd.img.gz

 # dd if=pfSense-2.0.1-RELEASE-2g-i386-nanobsd.img.gz of=/dev/adX obs=64k

Bölüm 7:
Alternatif Kurulum Teknikleri

USB dönüştürücü aygıtlar aracılığıyla IDE, SATA disklere ve CF kartlara kurulum Vmware player veya workstation sürümleri ile yapılabilir.

- vmware imajı oluşturularak aşağıdaki adımlarla full kurulum yapılır
- Yeni bir vm imajı oluştur
- Fiziksel disk ekle (usb dönüştürücü ile IDE/SATA vb. diskler eklenebilir)
- Sanal makinayı başlat
- Full veya Embedded kurulum için yönergeleri tamamla

Bölüm 7:
Kurulum Aşamalarında Sorun Giderme

Gömülü anakartlarda boot hatası alıyorsanız,

01F0 Master 044A CF Card
Phys C/H/S 7745/16/63 Log C/H/S 968/128/63
1 FreeBSD
2 FreeBSD

Boot: 1
Boot error

PC Engines ALIX.2 v0.99h
640 KB Base Memory
261120 KB Extended Memory

01F0 Master 044A CF Card
Phys C/H/S 7745/16/63 Log C/H/S 968/128/63

1 FreeBSD
2 FreeBSD

Boot: 1
Boot error

Bölüm 7:
Kurulum Aşamalarında Sorun Giderme

Gömülü anakartlarda boot hatası alıyorsanız,

BIOS Ayarları aşağıdaki gibi olmalıdır:

9 9600 baud (2) 19200 baud (3) 38400 baud (5) 57600 baud (1) 115200 baud
C CHS mode (L) LBA mode (W) HDD wait (V) HDD slave (U) UDMA enable
(M) MFGPT workaround
(P) late PCI init
R Serial console enable
(E) PXE boot enable
(X) Xmodem upload
(Q) Quit

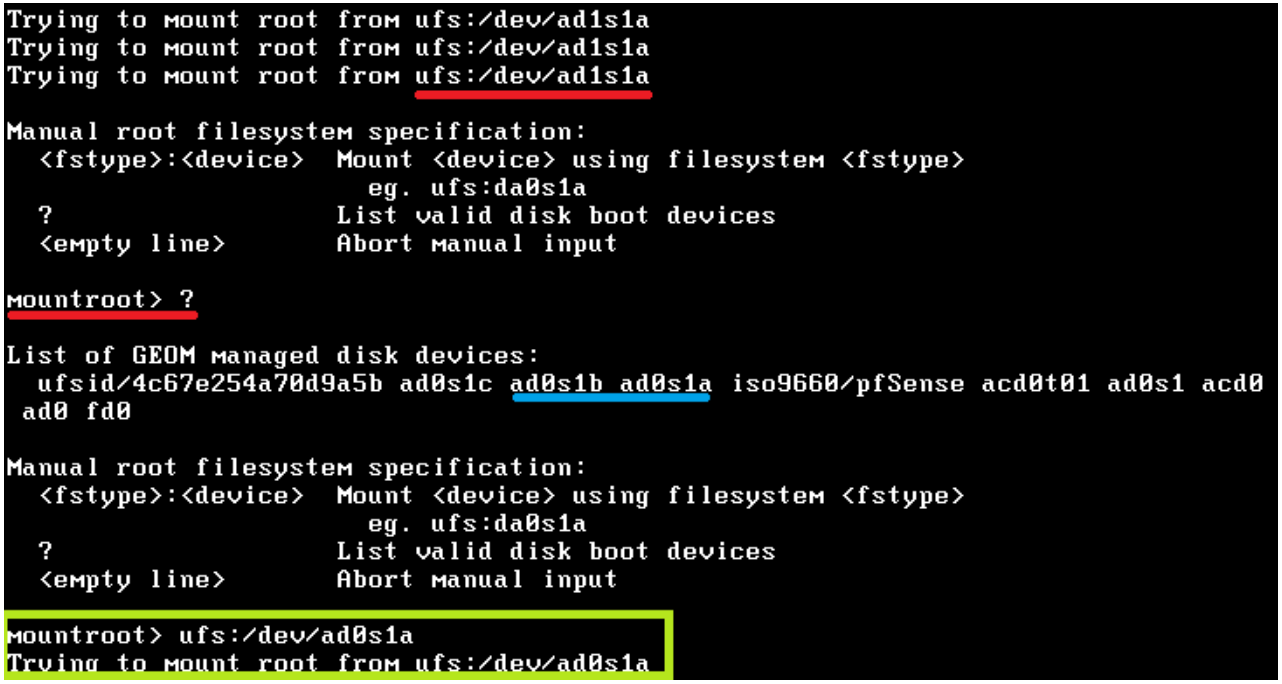
Bölüm 7:
Kurulum Aşamalarında Sorun Giderme

Disk mount problemi;

pfSense kurulu disk, bir başka donanımda farklı disk adını alabilir.

Mountroot> ? ile sistemdeki mevcut diskler listelenir ve mount edilecek disk **ufs:/dev/adXs1a** ile mount edilir.

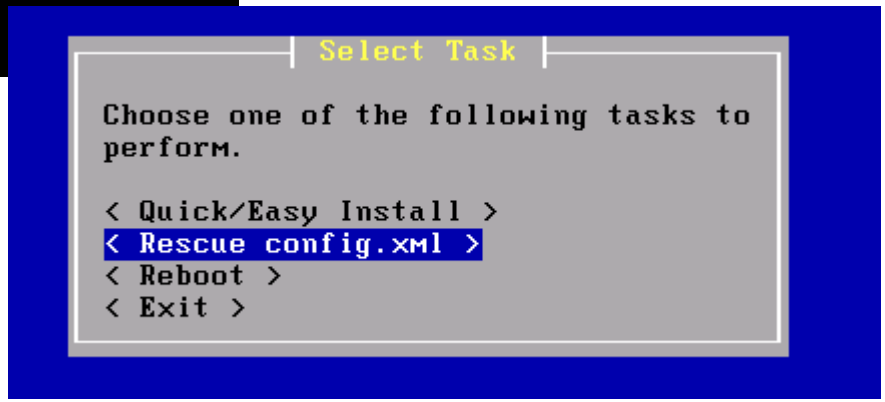
Ayarların kalıcı olması için **"/etc/fstab"** dosyasındaki disk adı düzenlenir.



Bölüm 7:
Kurtarma Operasyonu

- Config.xml kurtarma operasyonu

```
[ Press R to enter recovery mode or ]
[  press I to launch the installer  ]

(R)ecovery mode can assist by rescuing config.xml
from a broken hard disk installation, etc.

(I)nstaller may be invoked now if you do
not wish to boot into the liveCD environment at this time.

(C) continues the LiveCD bootup without further pause.

Timeout before auto boot continues (seconds): 5
```



- pfSense config.xml dosyasına erişim
- Backup config dosyalarına erişim

mount /dev/da0s1a /mnt

ls –lah /mnt/cf/conf/

Bölüm 8:
Konfigurasyon | Yönetim Arabirimleri

pfSense firewall, iki farklı yönetim arabirimine sahiptir.

Konsol arabirimi, sade bir menü yapısına sahiptir. Temel ayarlar ve kurtarma operasyonları için seçenekler sunar. FreeBSD komut satırının gücünü ve esnekliğini kullanmamız için geçiş sağlar.

Web arabirimi, işlevselliği yükse ve sade, gelişmiş bir yönetim arabirimi.Servis ve sistem ayarlarını web tabanlı yönetir.

Bölüm 8:
Konfigurasyon | Yönetim Arabirimleri

Konsole Arabirimi	Web Arabirimi
0) Logout (SSH only) 1) Assign Interfaces 2) Set LAN IP address 3) Reset webConfigurator password 4) Reset to factory defaults 5) Reboot system 6) Halt system 7) Ping host 8) Shell 9) PFtop 10) Filter Logs 11) Restart webConfigurator 12) pfSense Developer Shell 13) Upgrade from console 14) Disable Secure Shell (sshd)	System Interfaces Firewall Services VPN Status Diagnostics Help

Bölüm 8:
Konfigurasyon | Konsol Arabirimi

```
FreeBSD/i386 (pfsense.fabrikam.com) (ttyv0)

*** Welcome to pfSense 2.0-RC3-pfSense (i386) on pfsense ***

  WAN (wan)                -> em1        -> 6.6.6.106 (DHCP)
  LAN (lan)                -> em0        -> 192.168.1.1
  OPT1 (opt1)              -> em2        -> NONE

 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

Enter an option:
```

9) pfTop

```
pfTop: Up State 1-22/23, View: default, Order: none, Cache: 10000       15:59:12

PR    D SRC                  DEST                 STATE   AGE   EXP  PKTS BYTES
icmp  O 6.6.6.106:6806       6.6.6.1:0             0:0    668     9  1308 83712
udp   O 6.6.6.106:61671      188.124.15.164:123    2:2    668    34    52  3952
tcp   I 192.168.1.99:1475    192.168.1.1:443       4:4    139 86395   138 28017
udp   I 192.168.1.100:56166  192.168.0.1:138       0:1     63     0     1   211
udp   O 192.168.1.100:56166  192.168.0.1:138       1:0     63     0     1   211
udp   I 192.168.1.100:56166  192.168.204.1:138     0:1     63     0     1   211
udp   O 192.168.1.100:56166  192.168.204.1:138     1:0     63     0     1   211
udp   I 192.168.1.100:56166  192.168.142.1:138     0:1     63     0     1   211
```

Bölüm 8:
Konfigurasyon | Konsol Arabirimi

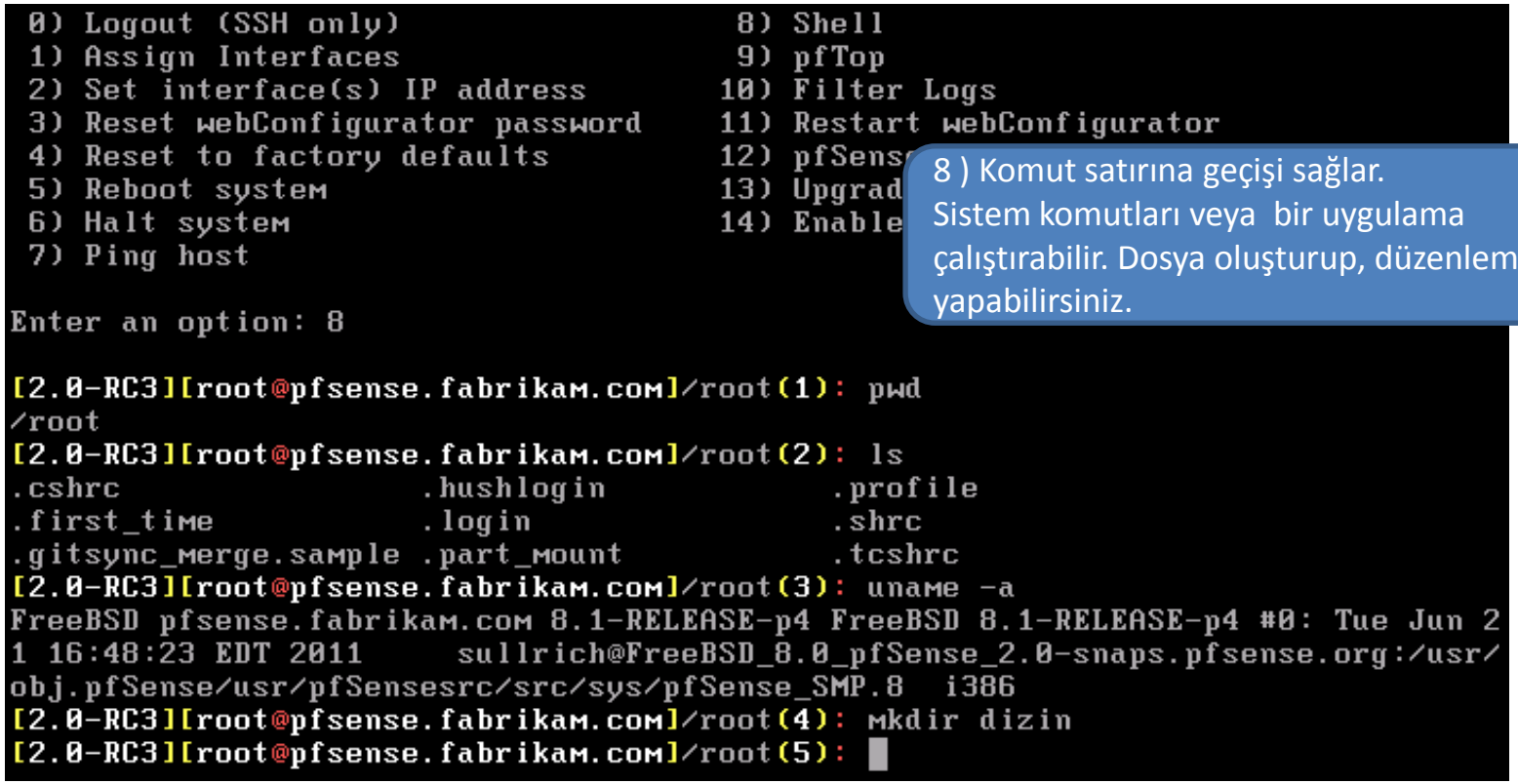
Web parolasını sıfırla

```
Enter an option: 3


The webConfigurator admin password and privileges will be reset to the default (
which is "pfsense").
Do you want to proceed [y|n]?y


The password for the webConfigurator has been reset and
the default username has been set to "admin".

Remember to set the password to something else than
the default as soon as you have logged into the webConfigurator.
Press ENTER to continue.
```

Sistem Yükseltme

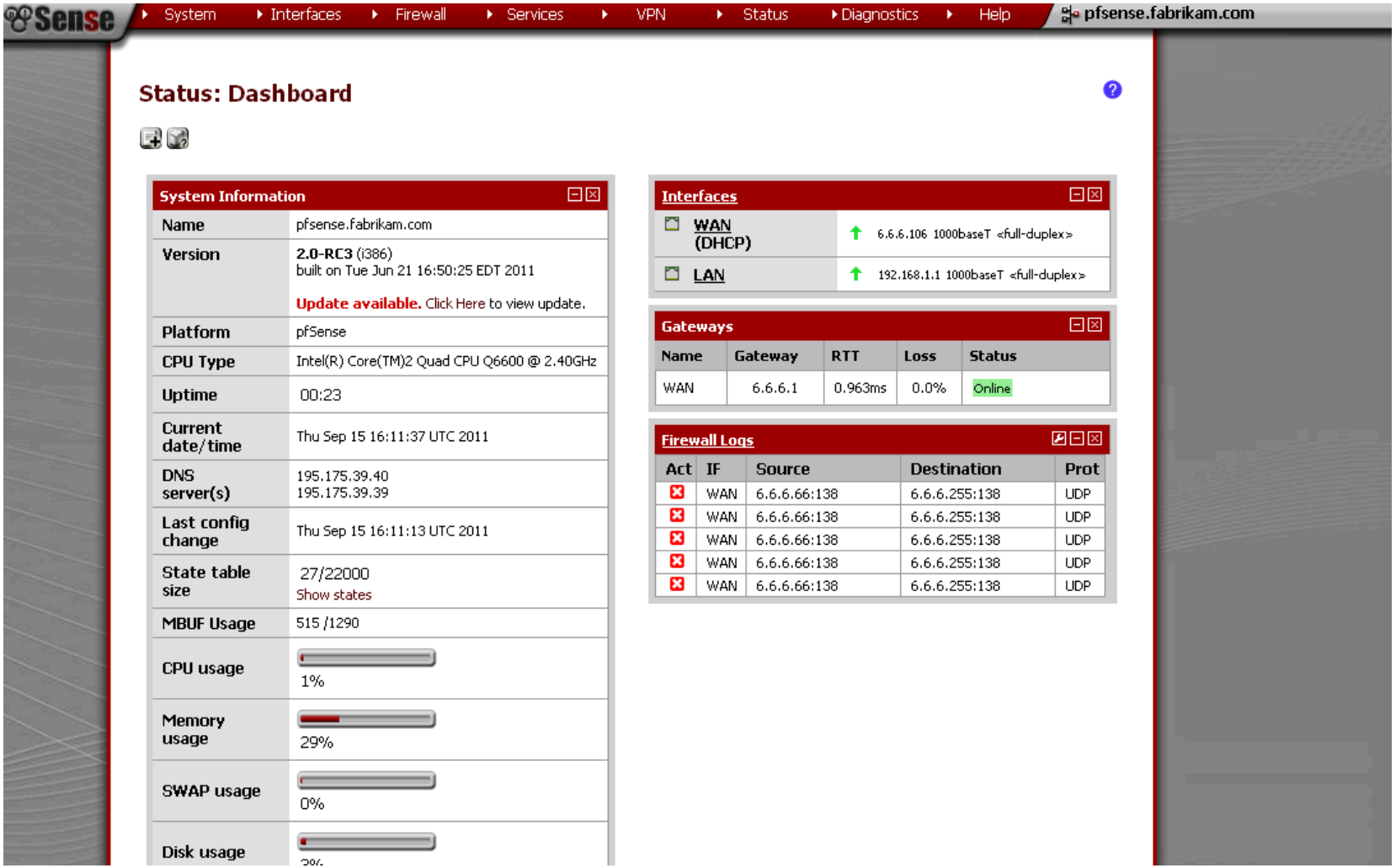
```
Enter an option: 13


Starting the pfSense console firmware update system..

1) Update from a URL
2) Update from a local file
Q) Quit

Please select an option to continue: 2

Enter the complete path to the .tgz or .img.gz update file: /tmp/update.tar.gz
```

Bölüm 8:
Konfigurasyon | Konsol Arabirimi

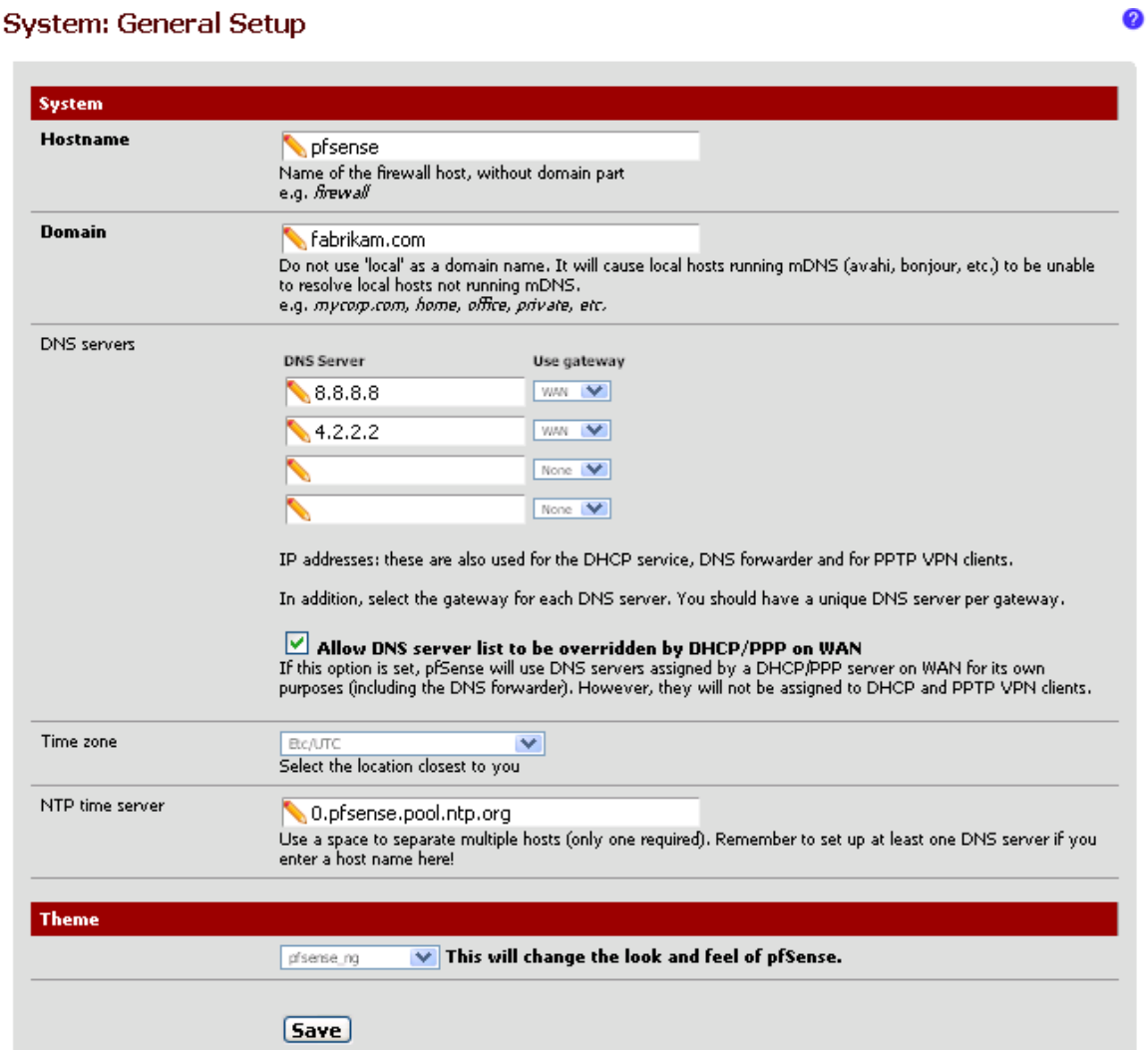


8) Komut satırına geçişi sağlar.
Sistem komutları veya bir uygulama çalıştırabilir. Dosya oluşturup, düzenlemeler yapabilirsiniz.

Bölüm 8:
Konfigurasyon | Web Arabirimi



Bölüm 8:
Konfigurasyon | Genel Ayarlar



Bölüm 9:
Ağ Ayarları

- Ağ ayarları menüsü, değişik ağ arabirimlerine göre farklılık gösterebilir.
- Herhangi bir ağ arabirimi için atanacak IP türleri;
  - Static
  - DHCP
  - PPoE/PPTP
  - Özel IP Adresleri
  - Wireless

Bölüm 9:
Ağ Ayarları | IP Türleri

- **Static**

IP adresi ve CIDR mask sabit olarak set edilir. Eğer WAN arabirimine ip atanıyorsa, gateway adreside tanımlanmalıdır.

- **DHCP**

IP adresi otomotik olarak ortamdaki bir DHCP sunucudan alınır. DHCP sunucunun hostname adresi ve ailas olarka ikinci bir ip adresi girilebilir.

- **PPoE/PPTP**

PPoE ve PPTP arabirimlerine kullanıcı adı ve parola, opsiyonel olarak servis adı, dial and demon, boş zaman aşımı değerleri ve opsiyonel olarak periyodik reset (yalnızca PPoE için) ayarları set edilir.

Bölüm 9:
Ağ Ayarları | IP Türleri

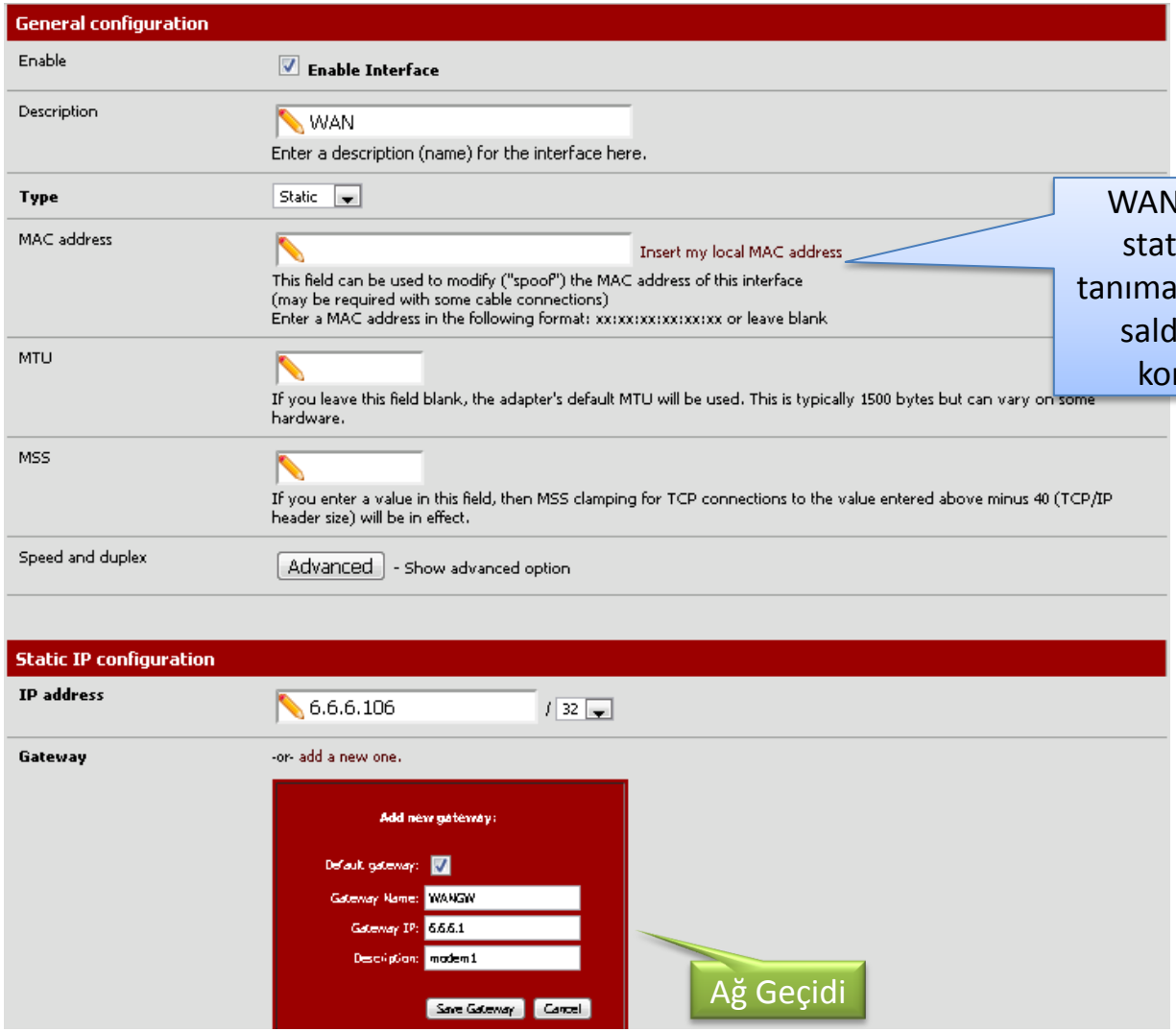
- **Özel IP Adresleri**

RFC1918 standardına göre, yerel ağlarda kullanılmak üzere ayrılmış ip adresleri ve atanmamış networkler.

- **Wireless**

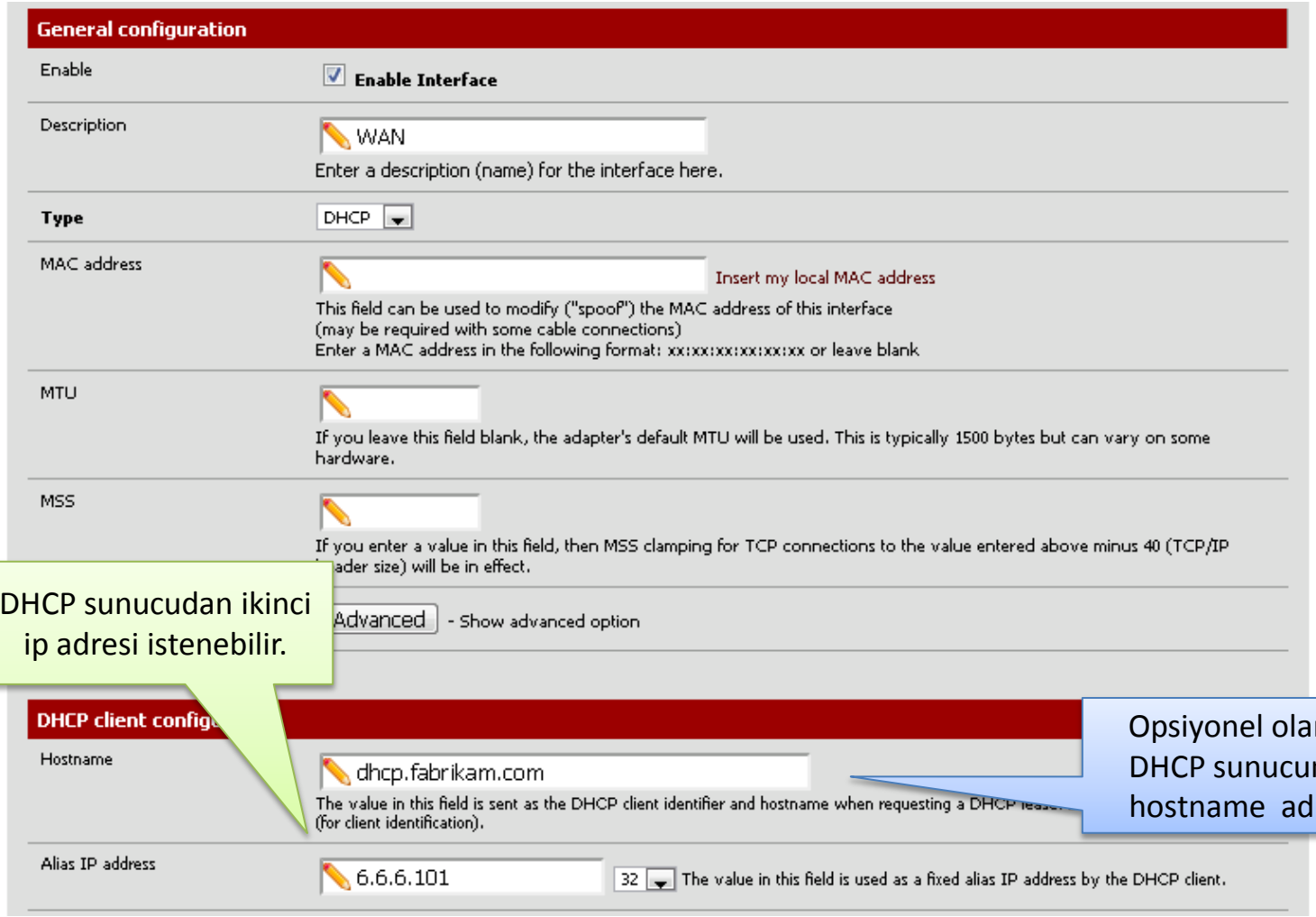
Diğerler seçeneklerden farklı olarak, SSID ve Encryption (WEP, WPA) değerleri tanımlanmalıdır.Wireless ağ arabirimi, istemcilere hizmet vermek için Access Point olarak kullanılabilir veya bir başka Access Point bağlantısı kurabilir.

Bölüm 9:
Ağ Ayarları| WAN | Static



WAN arabirimi için statik MAC kaydı tanımalamak, spoofing saldırılarına karşı koruma sağlar.

Bölüm 9:
Ağ Ayarları| WAN | DHCP



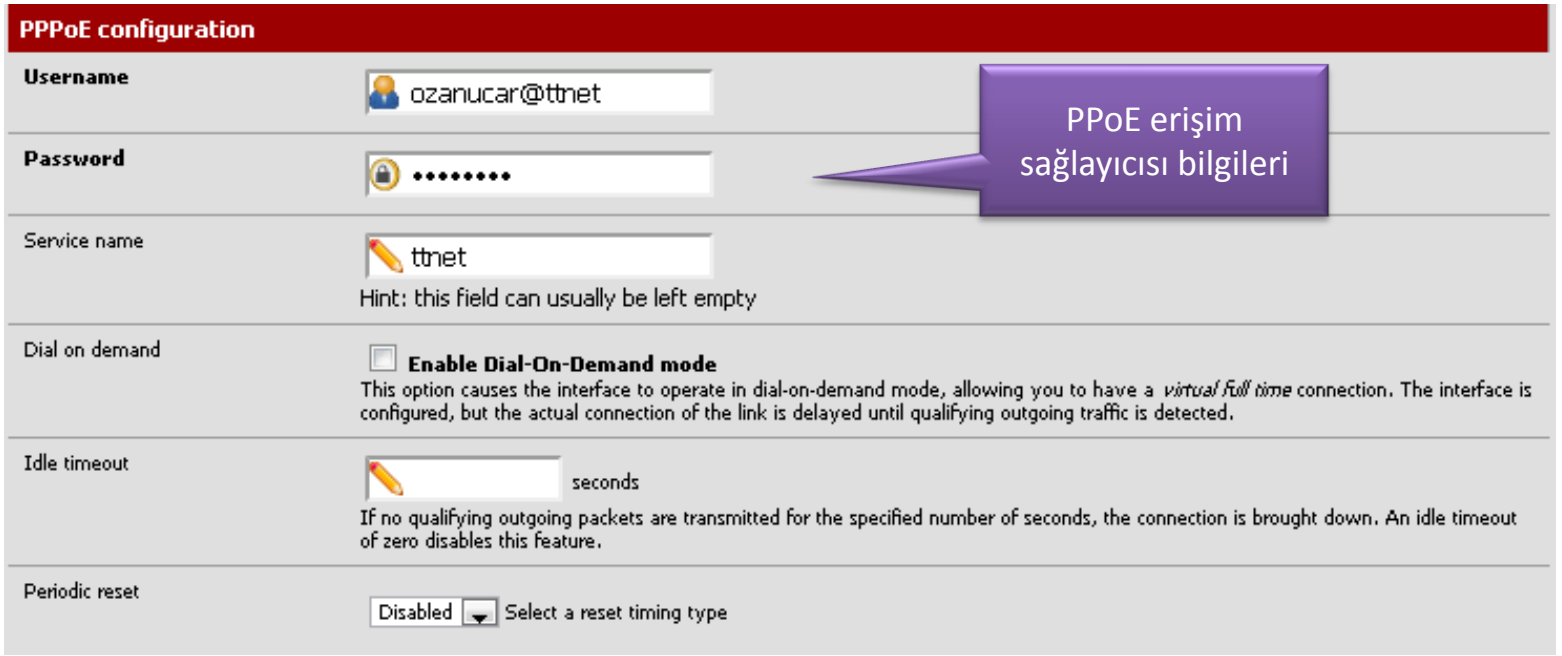
Bölüm 9:
Ağ Ayarları| WAN | DHCP Kirası

Status > Interfaces

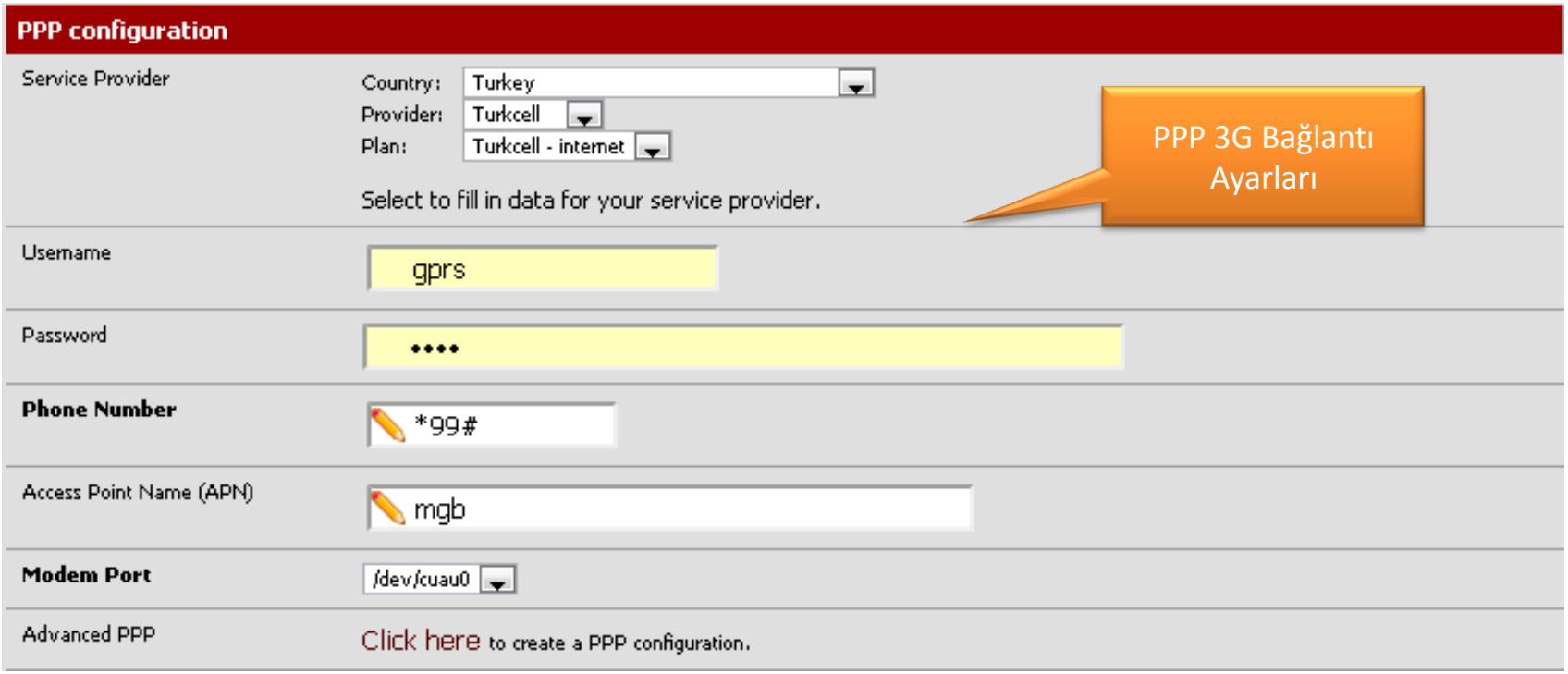
WAN interface (em1)	
Status	up
DHCP	up Release
MAC address	00:0c:29:f7:69:8b
IP address	6.6.6.106
Subnet mask	255.255.255.0
Gateway	6.6.6.1
ISP DNS servers	195.175.39.40 195.175.39.39 192.168.1.1
Media	1000baseT <full-duplex>
In/out packets	35440/35440 (5.49 MB/4.95 MB)
In/out packets (pass)	35440/39527 (5.49 MB/4.95 MB)
In/out packets (block)	0/0 (0 bytes/0 bytes)
In/out errors	0/0
Collisions	0

DHCP sunucudan alınan ağ ayarları.

Bölüm 9:
Ağ Ayarları| WAN | PPoE

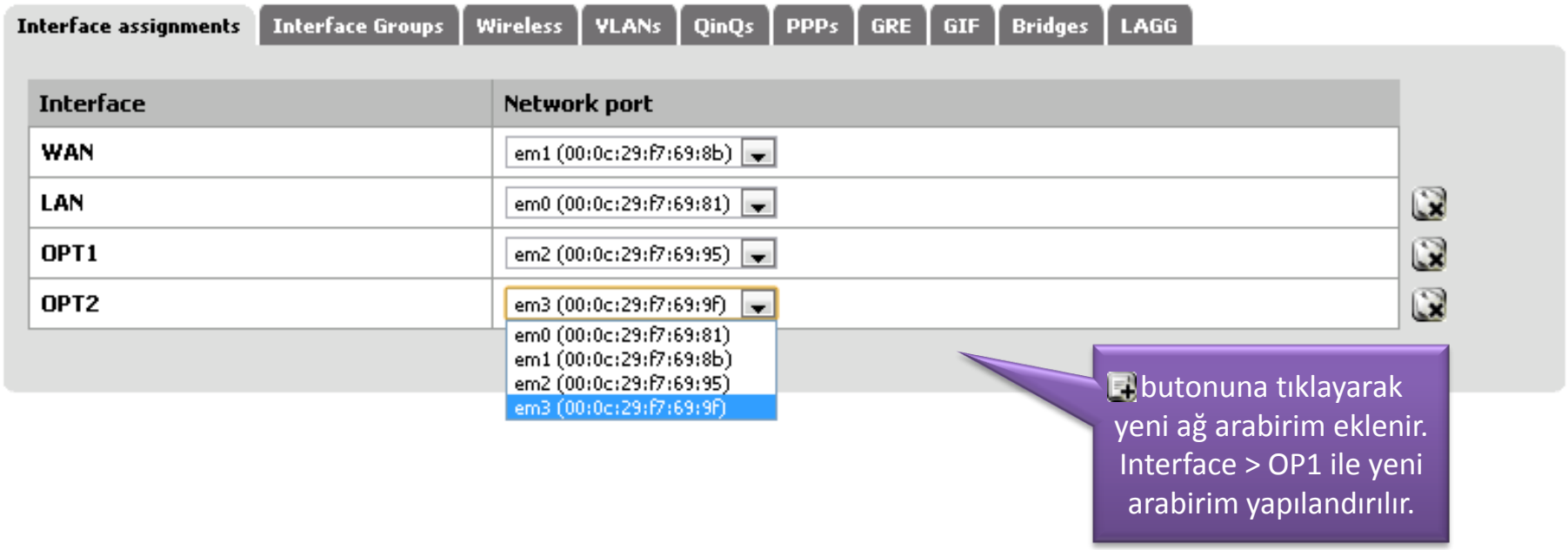


Bölüm 9:
Ağ Ayarları| WAN | PPP

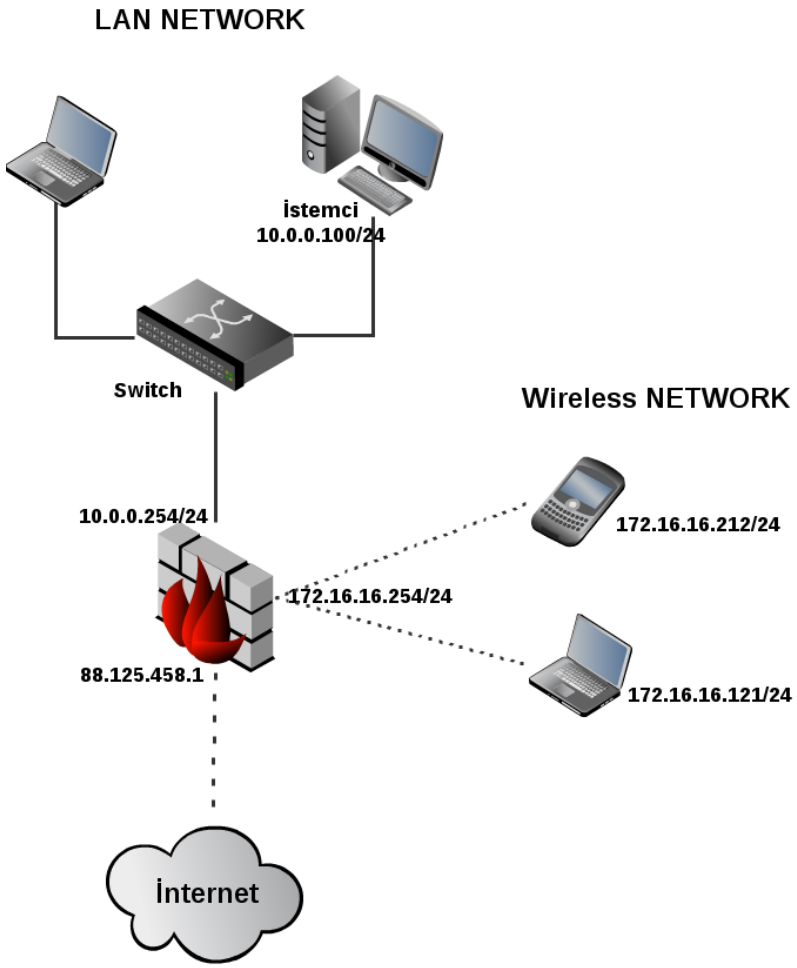


Bölüm 9:
Ağ Ayarları| Arabirim Eklemek

- Interfaces > Assign sekmesinden yeni ağ arabirimi eklenebilir ve kaldırılabilir.

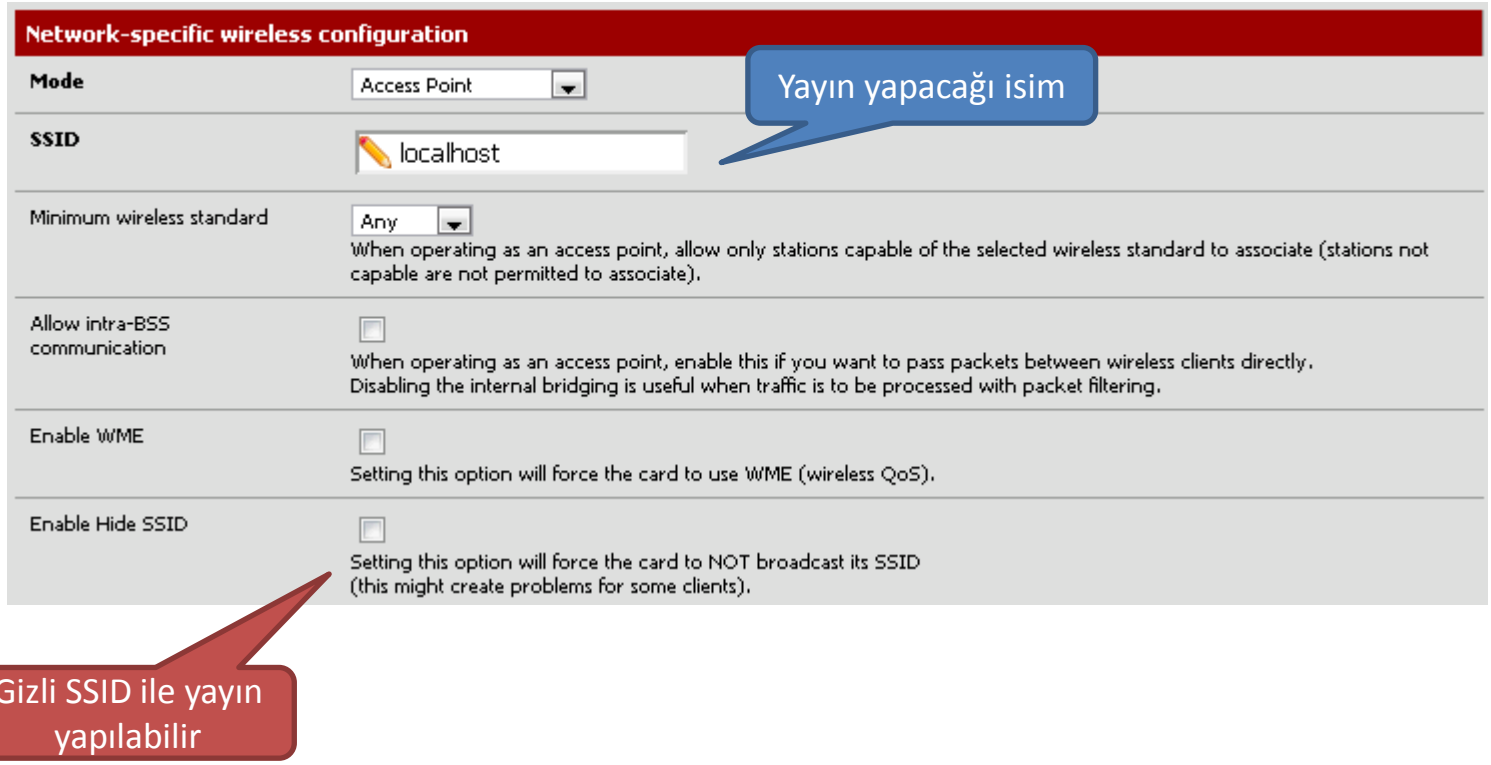


Bölüm 10:
Wireless



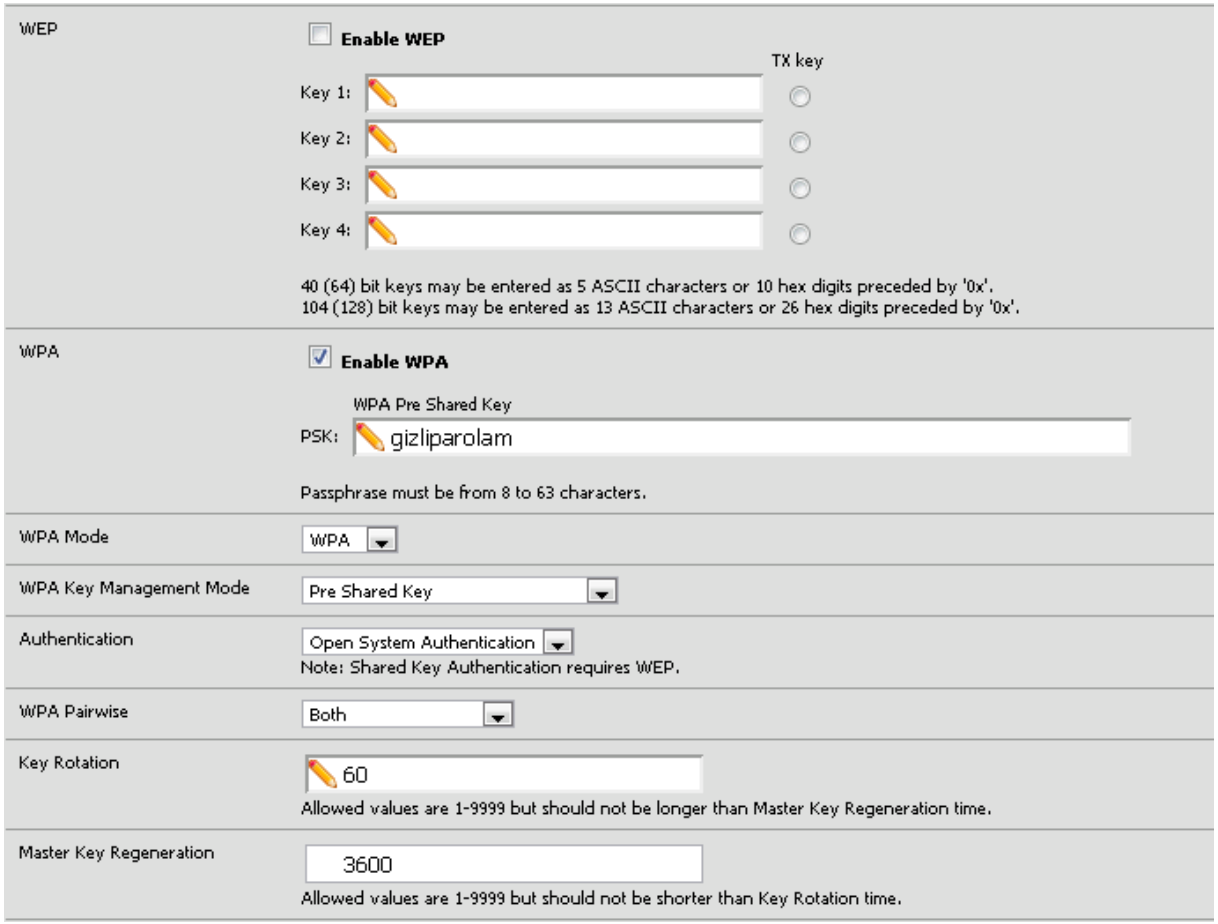
Bölüm 10:
Wireless | Arabirim Ayarları

Access Point Olarak Yapılandırmak



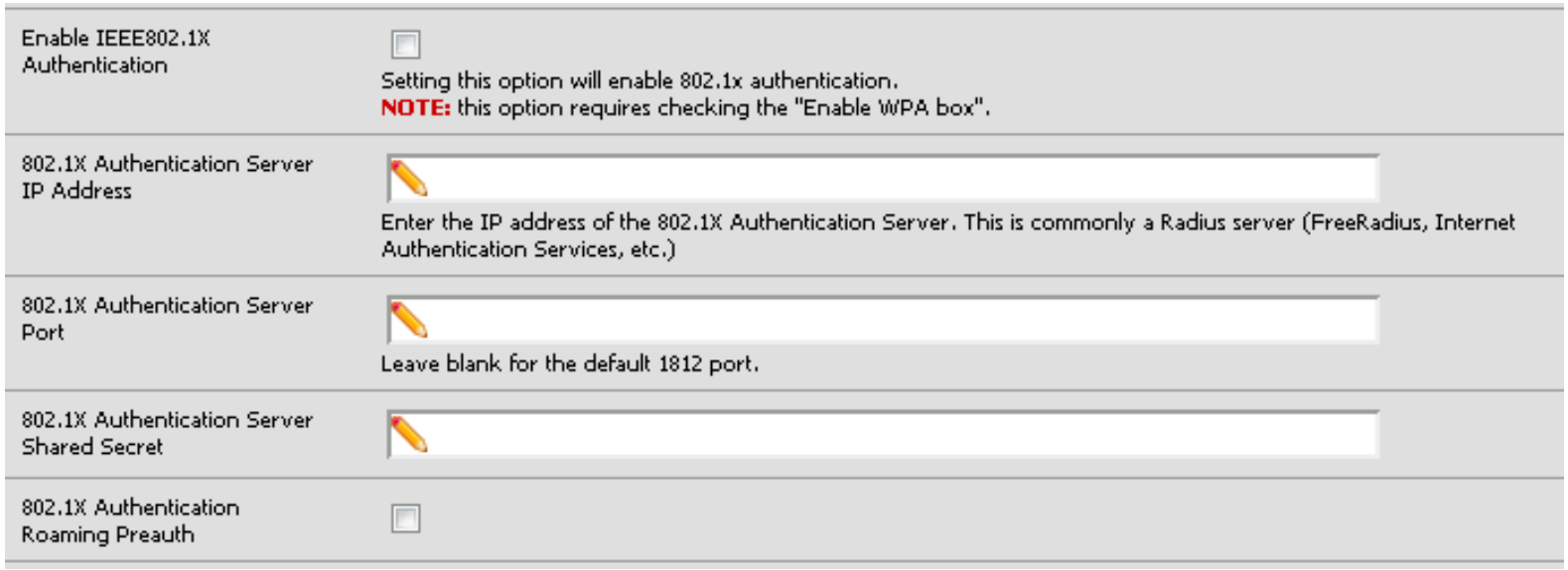
Bölüm 10:
Wireless | Arabirim Ayarları

Şifreleme Türleri



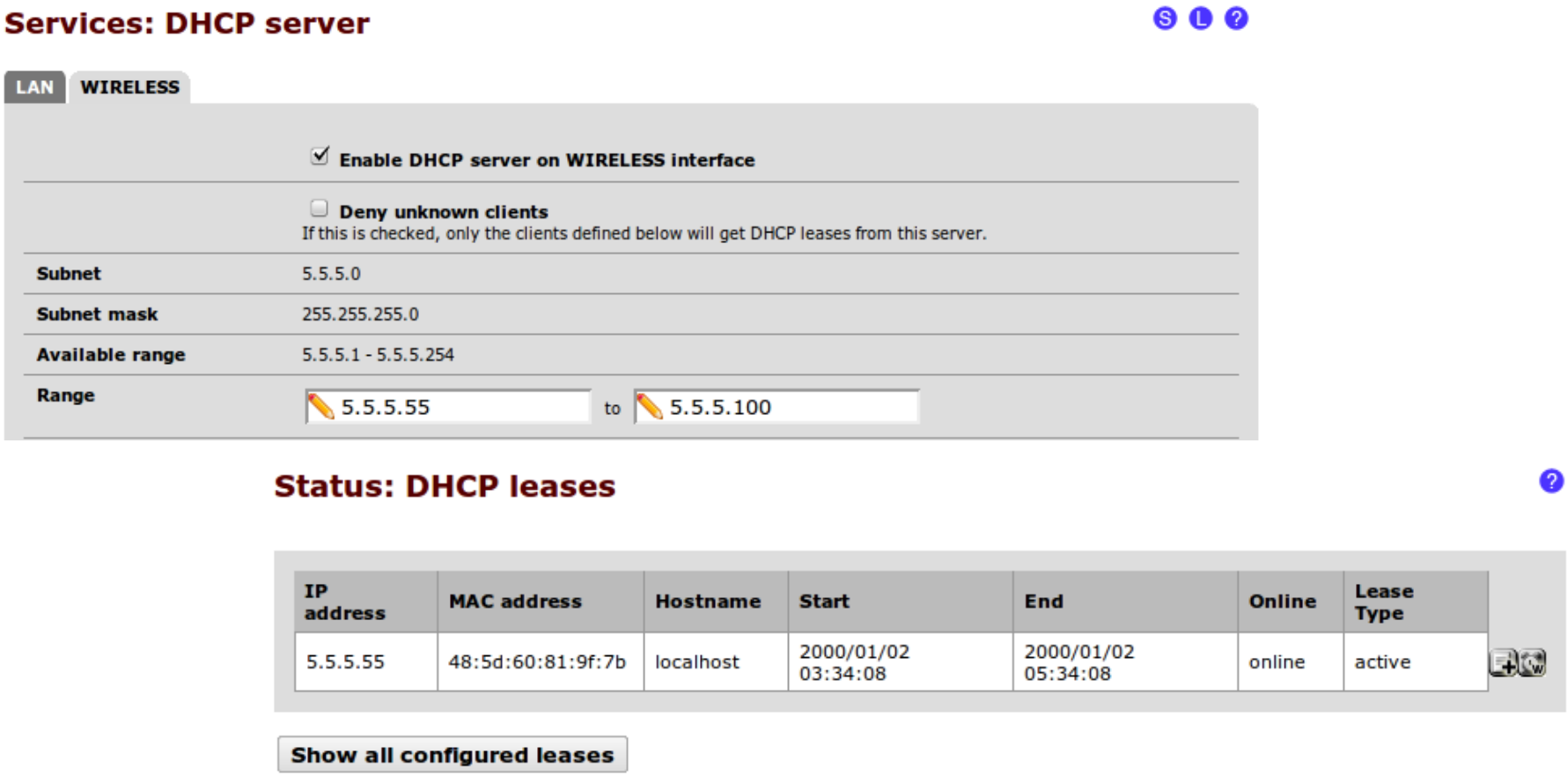
Bölüm 10:
Wireless | Arabirim Ayarları

802.1x



Bölüm 10:
Wireless | Arabirim Ayarları

Wireless ağ arabirimi için DHCPD



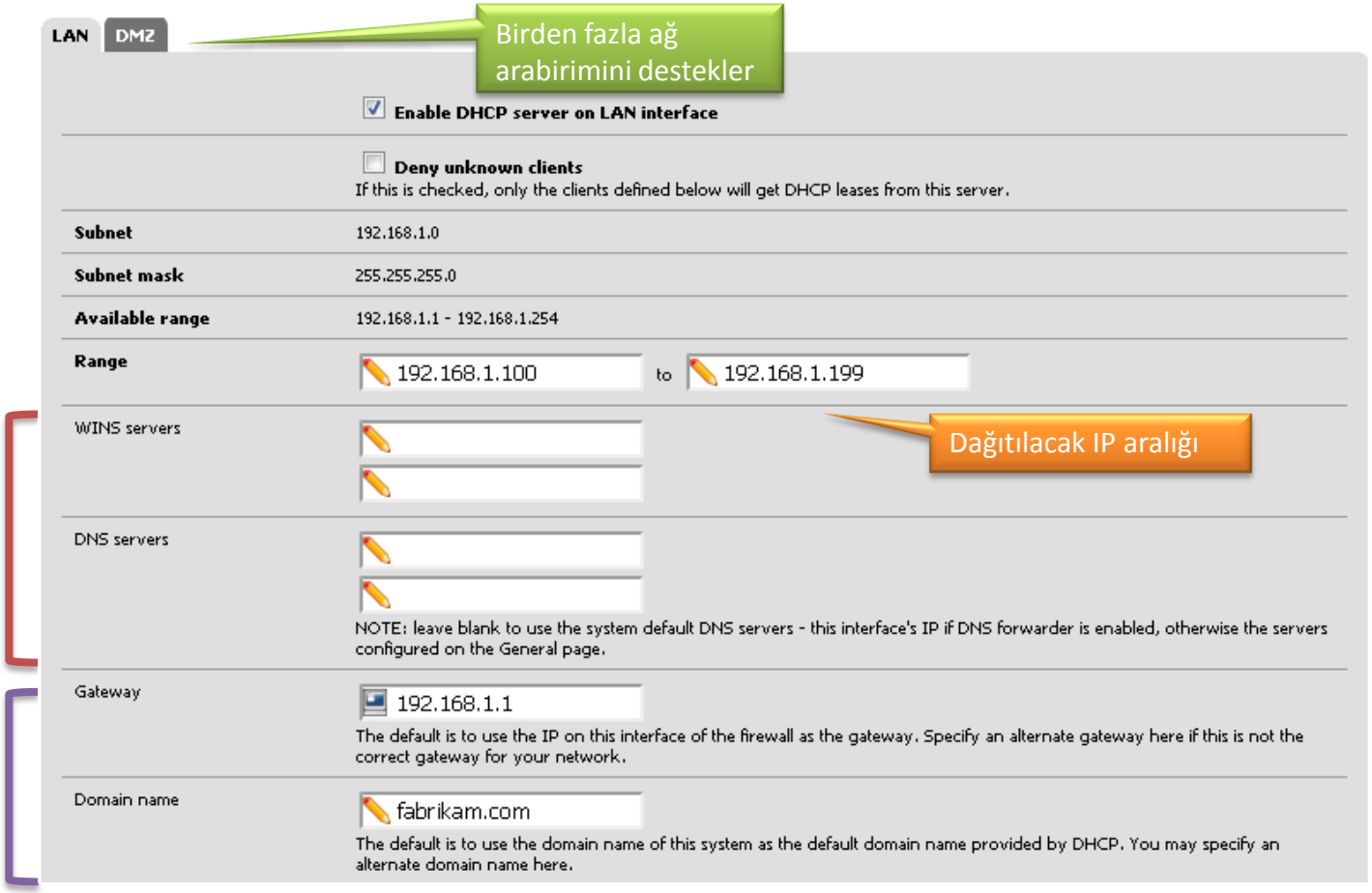
Bölüm 11:
Servisler

Captive Portal **Hizmet portalı, güvenli hotspot ağı** **DNS Forwarder** **DNS isteklerinin iletimi** **DHCP Relay** **DHCP paketlerinin aktarımı** **DHCP Server** **IP dağıtımı** **Dynamic DNS** **Dinamik DNS sunucularının kullanımı** **Load Balancer** **Yük dengeleme ve yük aktarma servisi**	**OLSRD** **Kablosuzlar arası neti dağıtmak** **PPPoE Server** **RIP** **Router Information Protocol** **SNMP** **Snmp servisinden bilgi alma** **UPnP** **OpenNTPD** **Zaman sunucusu kurulumu** **Wake on LAN** **Ağ üzerinden bilgisayar açmak**

Bölüm 11:
Services | DHCP Server

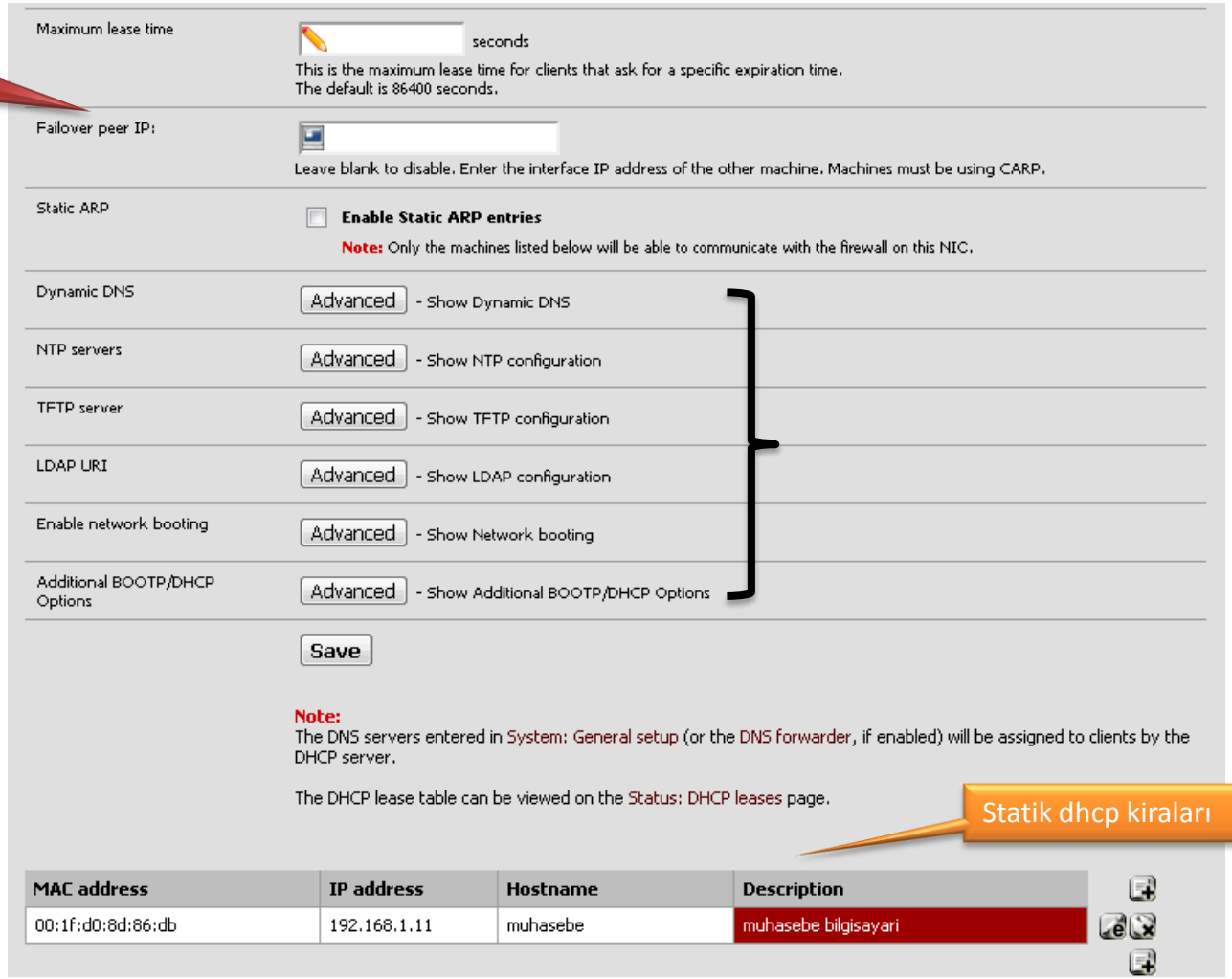
- İç ağa ip adresi dağıtmak için kullanılır.
- **DHCP sunucunun hizmet verdiği ağ arabiriminin statik ip adresine sahip olması gerekir.**
- MAC adresine göre statik ip ataması yapılabilir.
- NTP server, Dynamic DNS bilgileri dhcp istemcilerine iletilebilir.
- DNS ve Gateway tanımı yapılabilir.
- Ağ üzerinden işletim sistemi yüklemeyi sağlayabilir.
- DHCP kira süreleri tanımlanabilir.
- DHCP kiralarını görtüleme ve yönetme arabirimi mevcuttur.
- Tanımlanmamış ip aralığı ve ip-mac listesi dışındaki istemcilerin ağa erişimini engeller.Bu özelliği ile diğer dhcp sunucular'dan en büyük farkını yansıtır.

Bölüm 11:
Services | DHCP Server

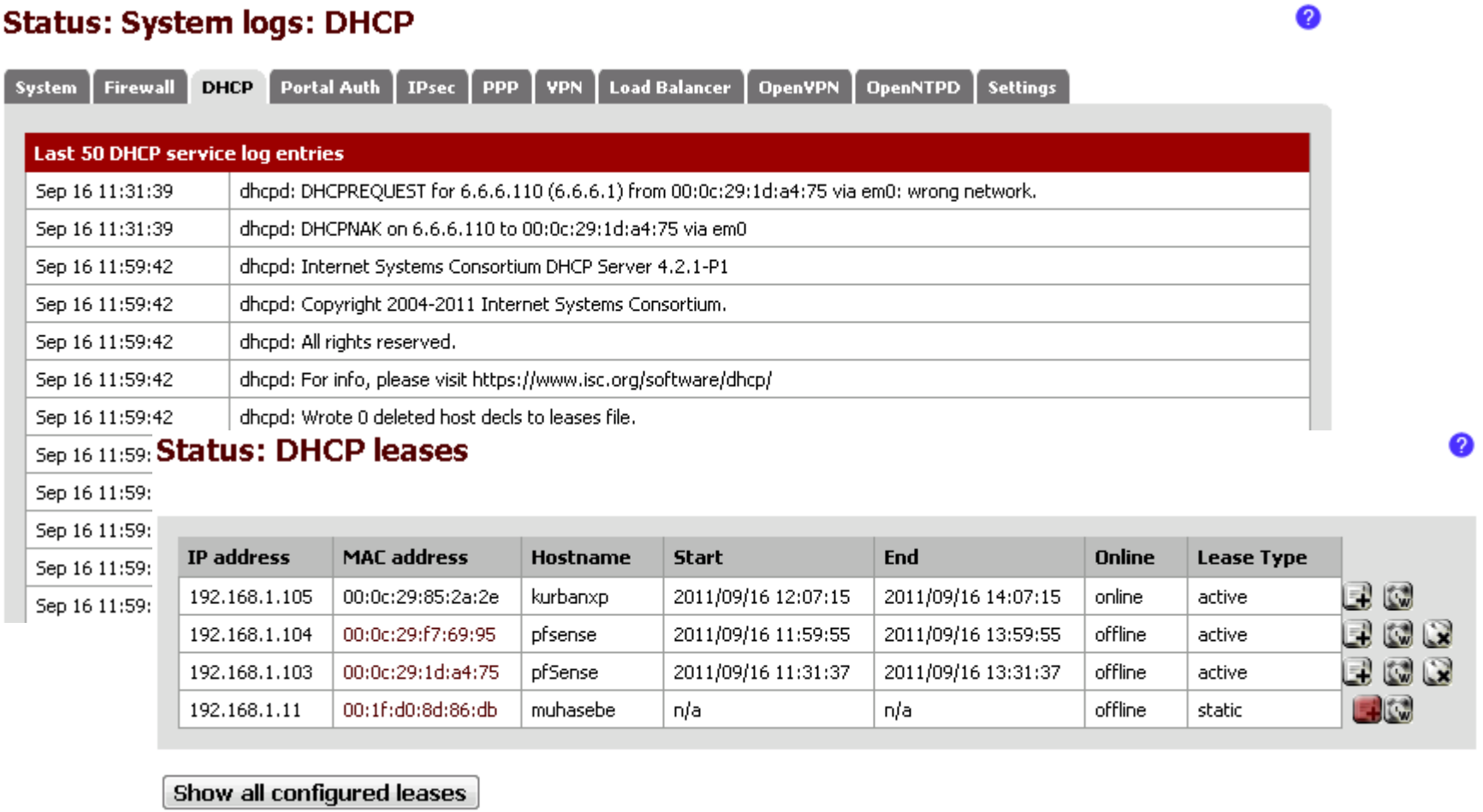


Bölüm 11:
Services | DHCP Server

Cluster yapısı için kullanılır.



Bölüm 11:
Services | DHCP Server | Kayıtların İncelenmesi



Status: System logs: DHCP

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

Last 50 DHCP service log entries

Sep 16 11:31:39	dhcpd: DHCPREQUEST for 6.6.6.110 (6.6.6.1) from 00:0c:29:1d:a4:75 via em0: wrong network.
Sep 16 11:31:39	dhcpd: DHCPNAK on 6.6.6.110 to 00:0c:29:1d:a4:75 via em0
Sep 16 11:59:42	dhcpd: Internet Systems Consortium DHCP Server 4.2.1-P1
Sep 16 11:59:42	dhcpd: Copyright 2004-2011 Internet Systems Consortium.
Sep 16 11:59:42	dhcpd: All rights reserved.
Sep 16 11:59:42	dhcpd: For info, please visit https://www.isc.org/software/dhcp/
Sep 16 11:59:42	dhcpd: Wrote 0 deleted host decls to leases file.
Sep 16 11:59:	
Sep 16 11:59:	
Sep 16 11:59:	
Sep 16 11:59:	
Sep 16 11:59:	

Status: DHCP leases

IP address	MAC address	Hostname	Start	End	Online	Lease Type
192.168.1.105	00:0c:29:85:2a:2e	kurbanxp	2011/09/16 12:07:15	2011/09/16 14:07:15	online	active
192.168.1.104	00:0c:29:f7:69:95	pfsense	2011/09/16 11:59:55	2011/09/16 13:59:55	offline	active
192.168.1.103	00:0c:29:1d:a4:75	pfSense	2011/09/16 11:31:37	2011/09/16 13:31:37	offline	active
192.168.1.11	00:1f:d0:8d:86:db	muhasebe	n/a	n/a	offline	static

Show all configured leases

Bölüm 11:
Services | DHCP Server | Sorun Giderme

DHCP servisi IP dağıtmıyor. Servis restart ettiğinizde aşağıdaki (zaten servi çalışıyor) mesajı alıyorsanız;

Oct 4 23:21:28 dhcpd: There's already a DHCP server running

Aslında dhcp servisi çalışmıyor, pid dosyası silinmemiş yeni çalışacak olan proccess bir kopyasının çalıştığını düşünüyor.

Çözüm;

 # rm /var/dhcpd/var/run/dhcpd.pid

Komut satırından veya arayüzden tekrar servisi başlatın. Servisimiz çalışıyor olacak;

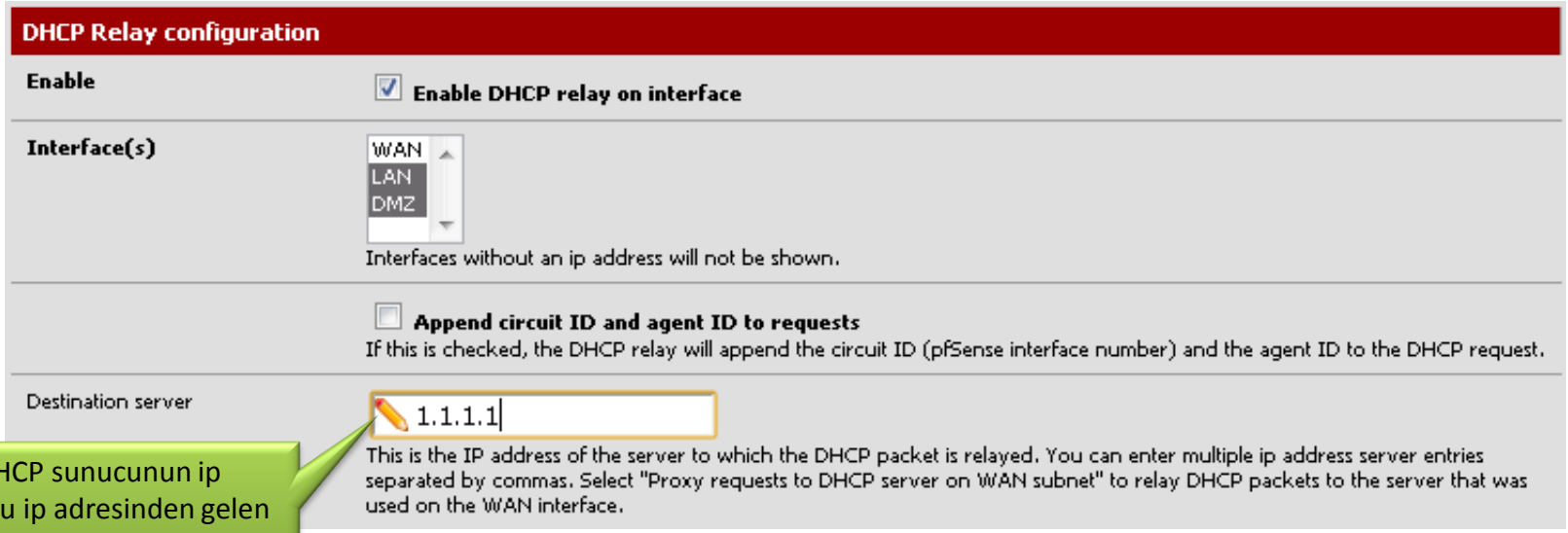
 # ps ax |grep dhcp

1433 ?? Ss 0:00.00 /usr/local/sbin/dhcpd -user dhcpd -group _dhcp -chroot /var/dhcpd -cf /var/dhcpd/etc/dhcpd.conf vr0

Bölüm 11:
Services | DHCP Relay

DHCP istekleri broadcast olarak iletirilir.Router'lar DHCP isteklerini geçirmezler. DHCP isteklerini wan ağından, lan ağına aktarması (relay) için DHCP Relay servisi kullanılır.

DHCP Broadcast'lerini yakalayarak bunları Unicast'e çevirip yetkili DHCP Server'a gönderir.



Yetkili DHCP sunucunun ip adresi. Bu ip adresinden gelen dhcp istekleri lan ağına iletilecektir.

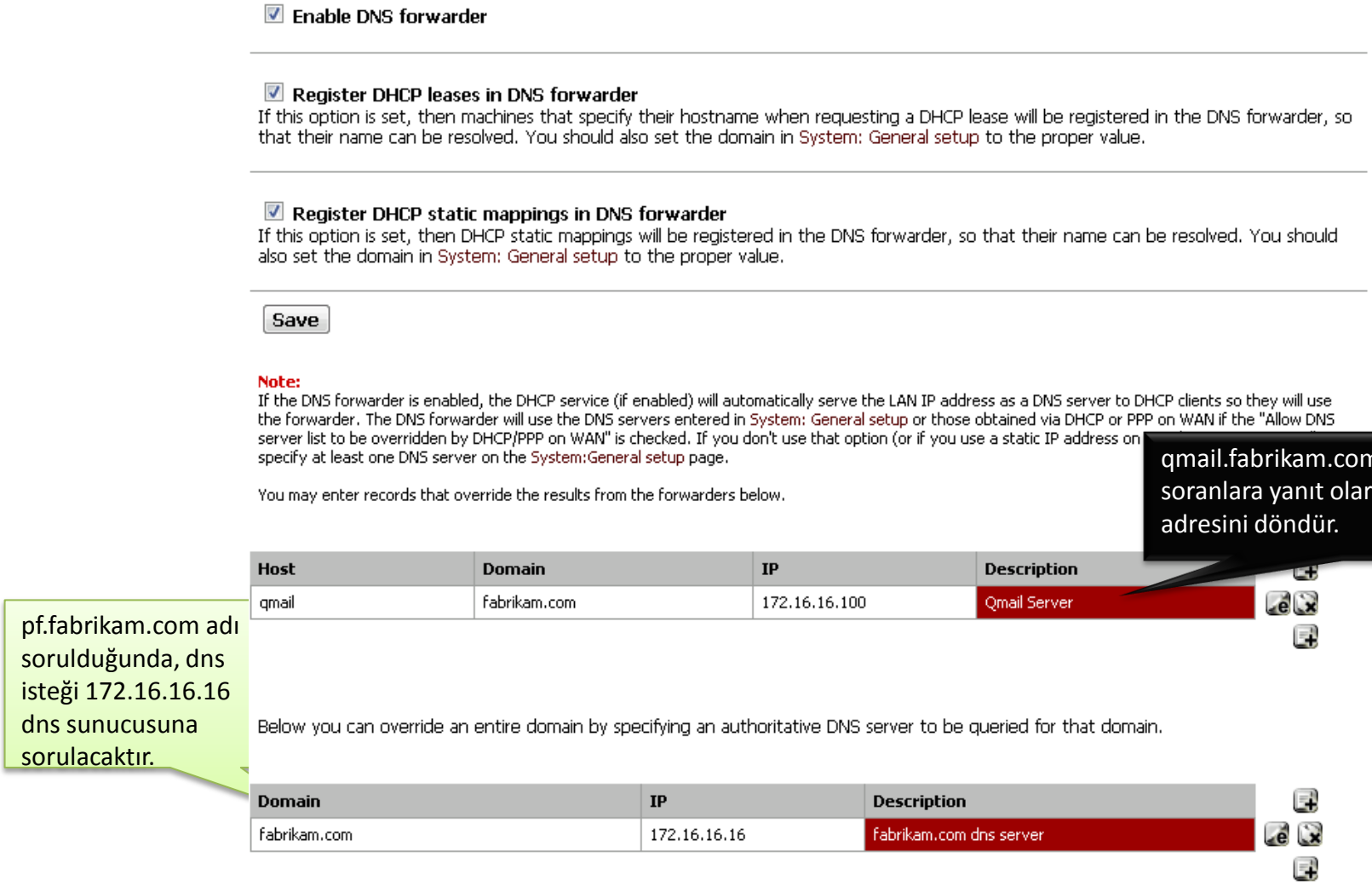
Bölüm 11:
Services | DNS Forwarder

pfSense üzerinde DNS Sunucu bulunmaz, DNS Forwarder olarak hizmet verir. Kendisine gelen dns isteklerini “**System > General Setup**” sayfasında belirttiğiniz DNS sunuculardan çözerek istemciye iletir.

Ayrıca, domainler için yetkili dns sunucuları veya bir host adresi için dns kaydı eklenebilir.

DHCP servisinden ip alan istemcilerin ip adresi ve hostnamelerini dns forwarder’a ekleyerek, yerel ağda bilgisayar adlarını çözmeyi sağlayabilirsiniz.

Bölüm 11:
Services | DNS Forwarder

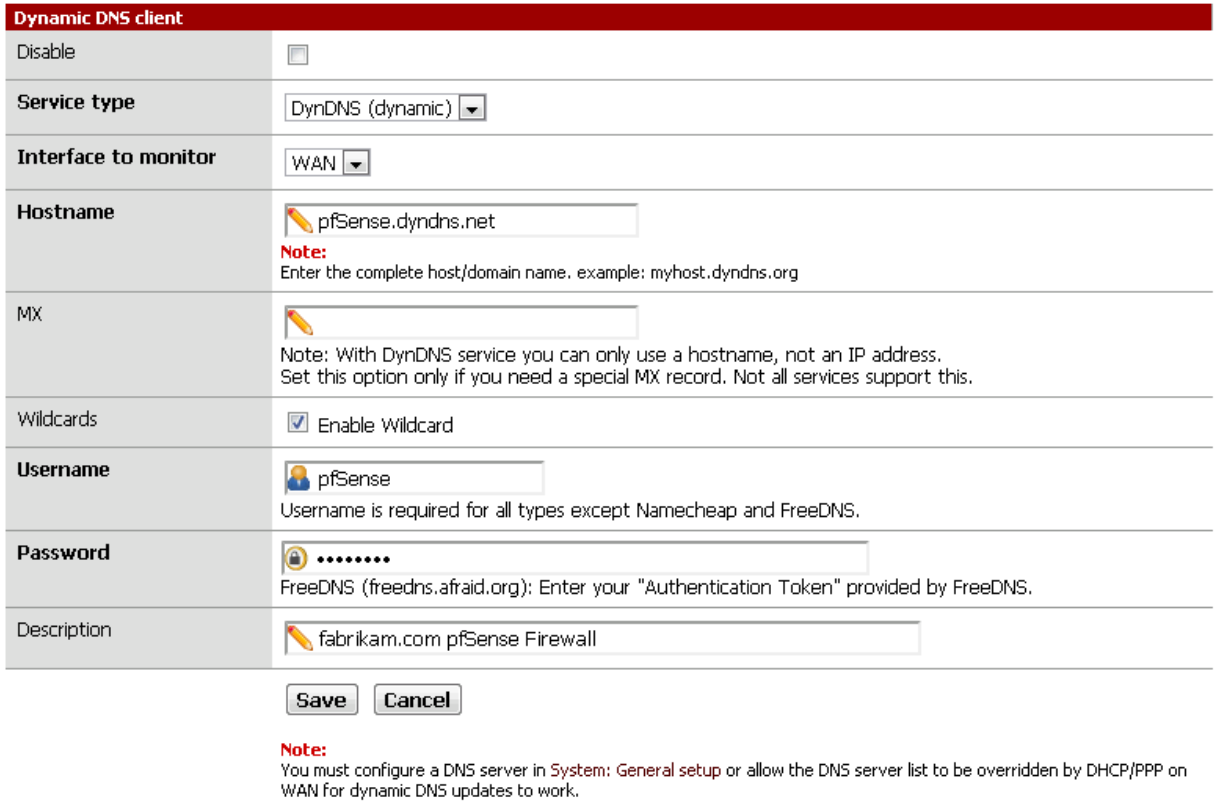


qmail.fabrikam.com alan adını soranlara yanıt olarak 172.16.16.100 ip adresini döndür.

pf.fabrikam.com adı sorulduğunda, dns isteği 172.16.16.16 dns sunucusuna sorulacaktır.

Bölüm 11:
Services | Dynamic DNS

DynDNS servisi Services > Dynamic DNS menüsünde bulunur, dinamik ip adresiniz her değiştiğinde bunu DNS sunucuya bildirip otomotik olarak DNS kaydınızı güncelleyen servistir.



Bölüm 11:
Services | SNMP

Uzak ağları , sistemleri monitor etmek için kullanılır. Bir endüstri standartıdır.

pfSense SNMP modüllerinin sağladığı bilgiler ;

MibII

Network ve ağ arabirimleri hakkında bilgi verir.Ağ arabirimlerinin durumu, donanım bilgisi, IP adresleri ve gelen/giden verinin miktarı gibi bilgiler sunar.

Netgraph

Bağlantı kurulan noktalar hakkında, bu noktaların durumları ve oluşan hatalar hakkında bilgi verir.

PF

pf kuralları, durum tablosu, ağ arabirimleri, tablolar ve ALTQ queues verileri elde etmekte kullanılır.

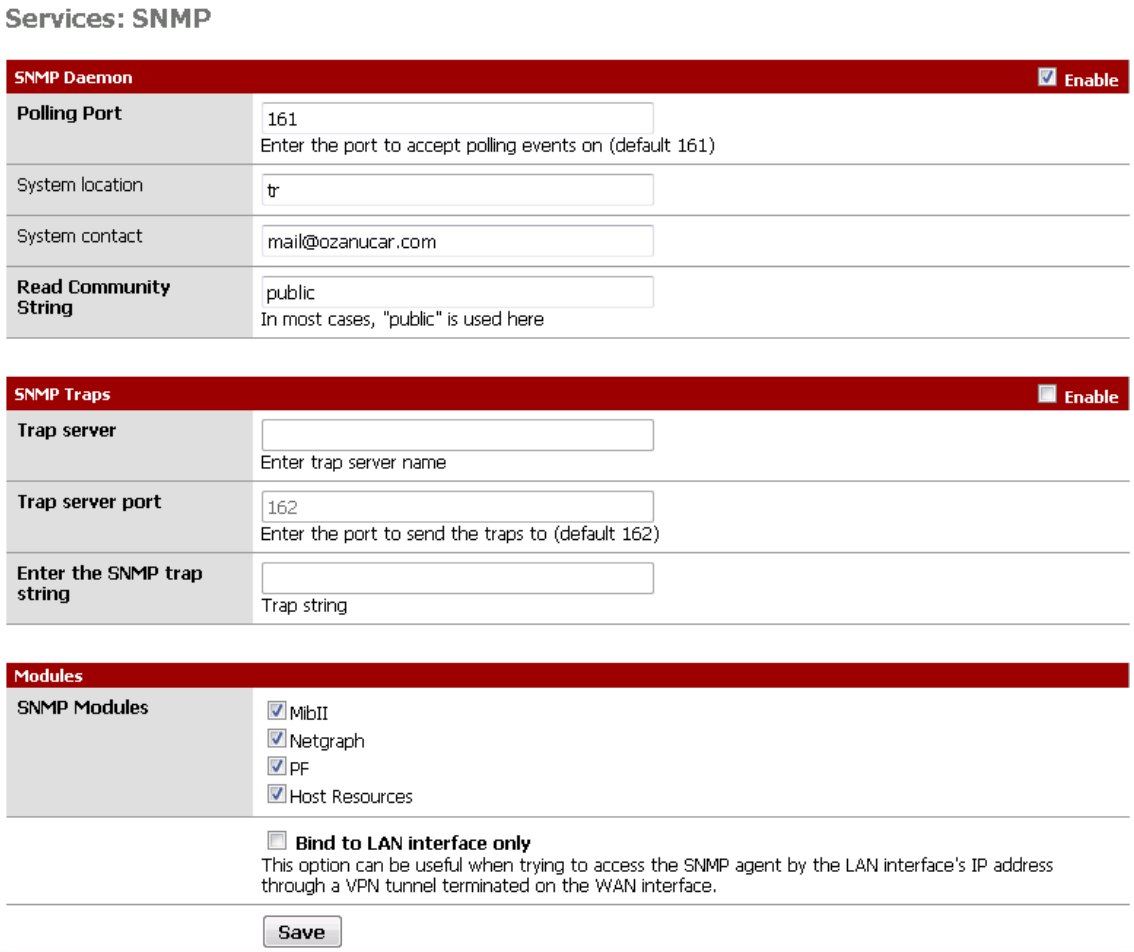
Host Resources

Sunucunun uptime,load average, processes, disk kullanımları, bağlı sistem aygıtları ve kurulu yazılımlar hakkında detay bilgi sağlar.

SNMP Araçları

Cacti, Nagios, SnmpWalk, Snmpcheck

Bölüm 11:
Services | SNMP



Bölüm 11:
Services | SNMP Araçları

Nagios = http://www.nagios.com

Current Network Status
Last Updated: Mon Mar 1 21:06:00 GMT 2010
Updated every 90 seconds
Nagios® Core™ 3.2.0 - www.nagios.org
Logged in as *monitor*

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
3	1	0	0

All Problems	All Types
1	4

Service Status Totals

Ok	Warning	Unknown	Critical
13	0	0	0

All Problems	All Types
0	13

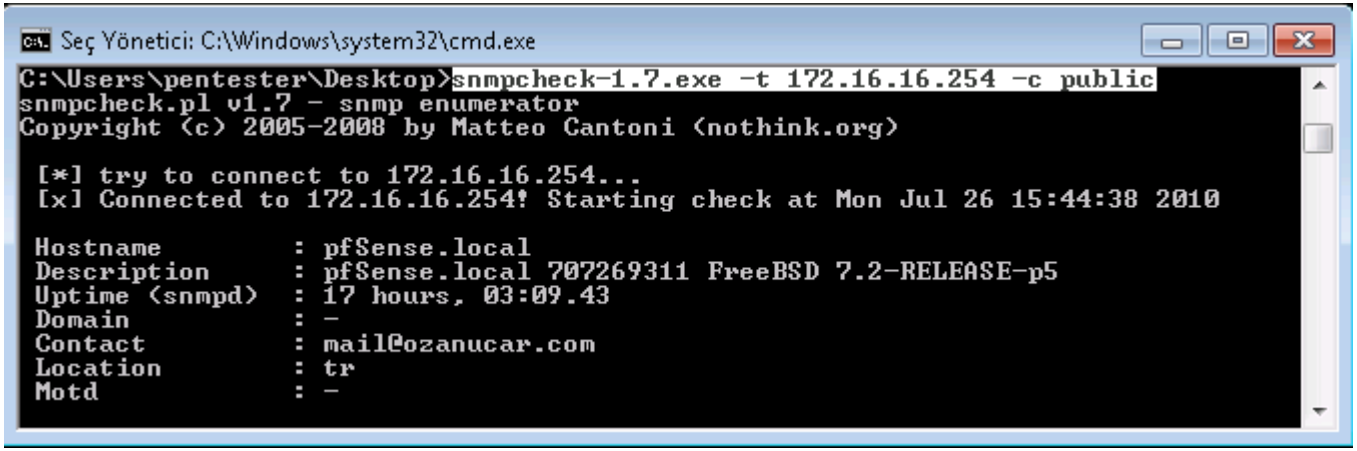
Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Aventail	HTTPS	OK	03-01-2010 10:01:58	0d 15h 44m 2s	1/3	HTTP OK: HTTP/1.1 302 Found - 717 bytes in 0.455 second response time
SNWL-LASSO	HTTP_URL	OK	03-01-2010 10:09:07	1d 3h 36m 53s	1/3	HTTP OK: HTTP/1.1 200 OK - 3267 bytes in 0.031 second response time
UK-TL-Gateway	Number of Connections	OK	03-01-2010 10:01:15	3d 4h 54m 45s	1/3	SNMP OK - 219
	PING	OK	03-01-2010 10:10:11	5d 7h 30m 49s	1/3	PING OK - Packet loss = 0%, RTA = 0.51 ms
	Uptime	OK	03-01-2010 10:01:16	5d 6h 44m 44s	1/3	SNMP OK - Timeticks: (181908487) 21 days, 1:18:04.87
localhost	Current Load	OK	03-01-2010 10:10:21	7d 10h 50m 39s	1/4	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	03-01-2010 10:08:00	7d 10h 50m 1s	1/4	USERS OK - 2 users currently logged in
	HTTP	OK	03-01-2010 10:08:00	7d 10h 49m 24s	1/4	HTTP OK: HTTP/1.1 200 OK - 452 bytes in 0.000 second response time
	PING	OK	03-01-2010 10:08:00	7d 10h 48m 46s	1/4	PING OK - Packet loss = 0%, RTA = 0.03 ms
	Root Partition	OK	03-01-2010 10:08:00	7d 10h 48m 9s	1/4	DISK OK - free space: / 9249 MB (68% inode=77%):
	SSH	OK	03-01-2010 10:08:29	7d 10h 47m 31s	1/4	SSH OK - OpenSSH_5.1p1 Debian-6ubuntu2 (protocol 2.0)
	Swap Usage	OK	03-01-2010 10:09:46	7d 10h 46m 54s	1/4	SWAP OK - 97% free (650 MB out of 675 MB)
	Total Processes	OK	03-01-2010 10:09:44	7d 10h 46m 16s	1/4	PROCS OK: 91 processes with STATE = RSZDT

13 Matching Service Entries Displayed

Bölüm 11:
Services | SNMP

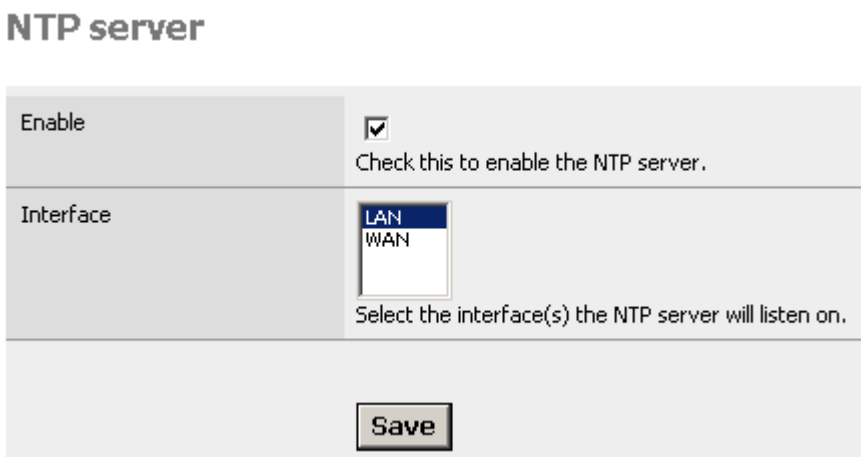
SNMP Check



Bölüm 11:
Services | OpenNTPD

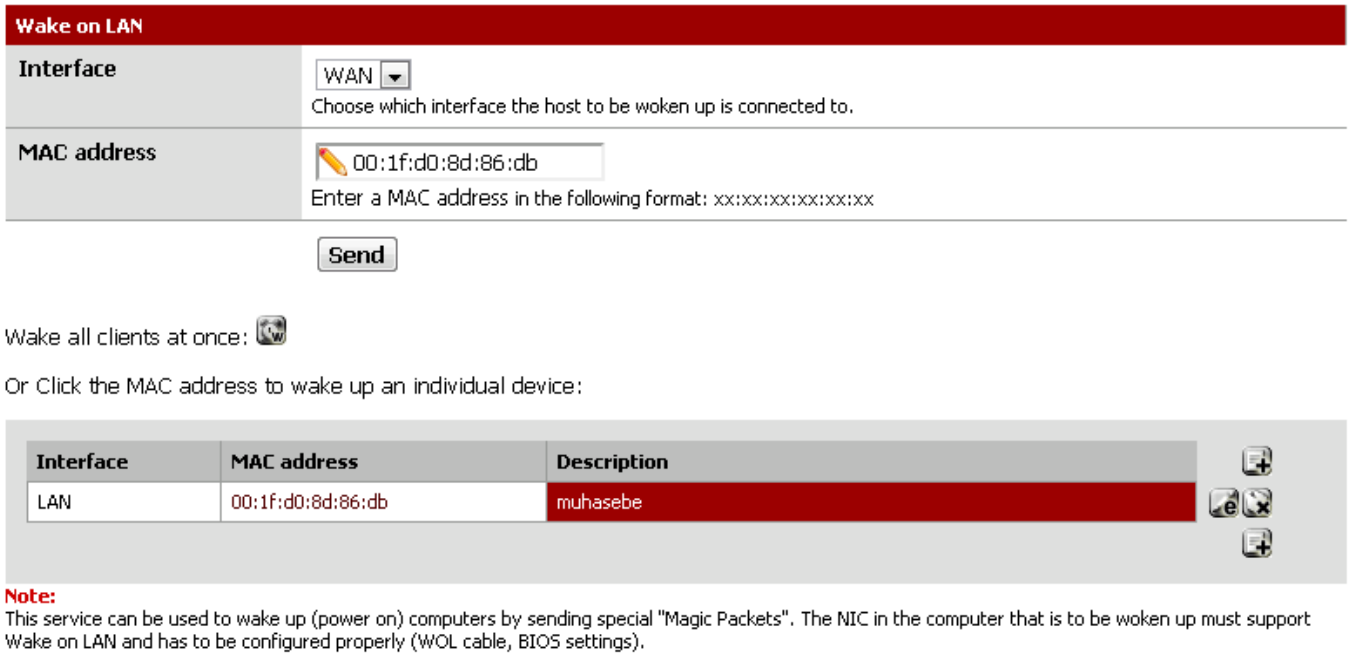
OpenNTPD, bir NTP (Network Time Protocol) servisidir.
Zaman bilgisini, ntp istemcilerine sunar.

ntp.nasa.gov misali ...



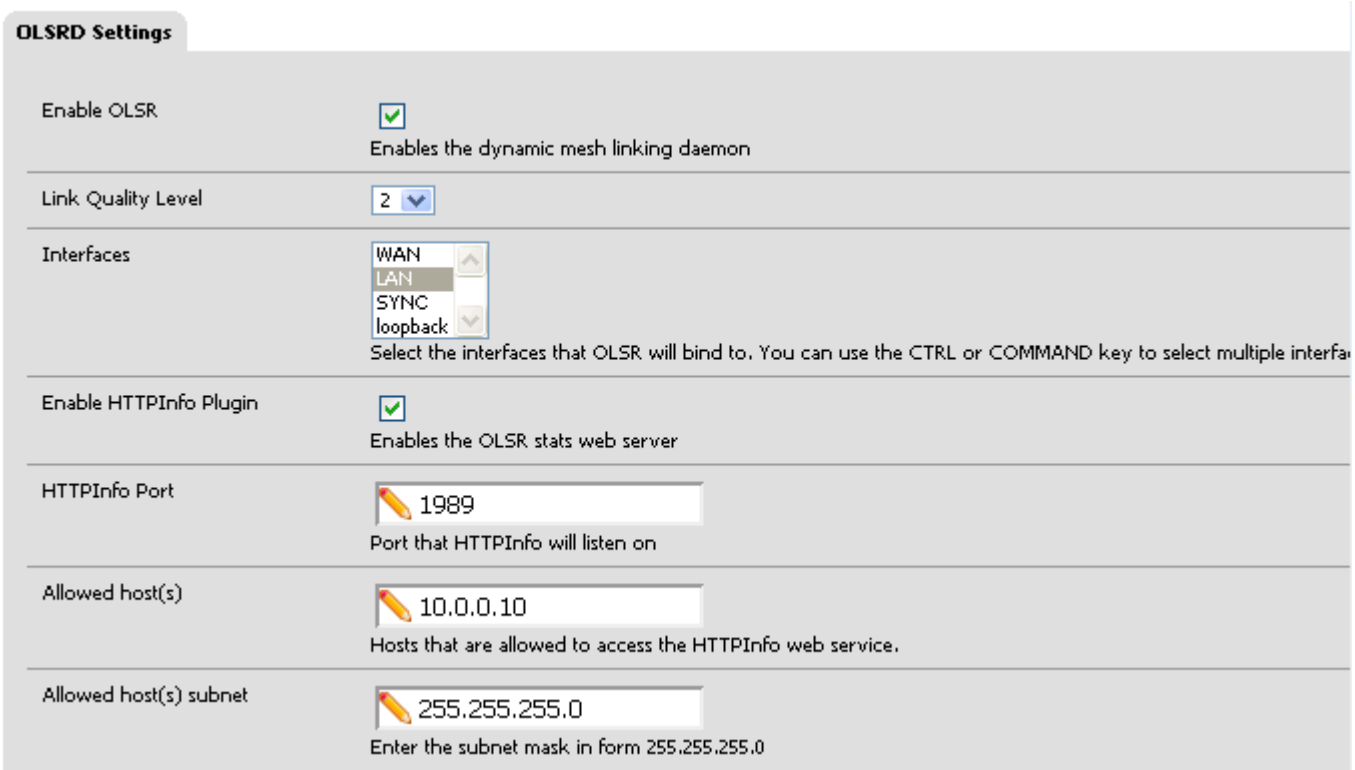
Bölüm 11:
Services | Wake on Lan

Bilgisayarı ağ üzerinden açmayı sağlar. Özel hazırlanmış bir paketi ethernet kartına göndererek kapalı bilgisayarın açılmasını sağlar.
Ağ üzerinden açılacak bilgisayarın sahip olduğu ethernet kartının "wake on lan" özelliğini desteklemesi ve BIOS ayarlarından bu özelliğin aktif olması gerekir.



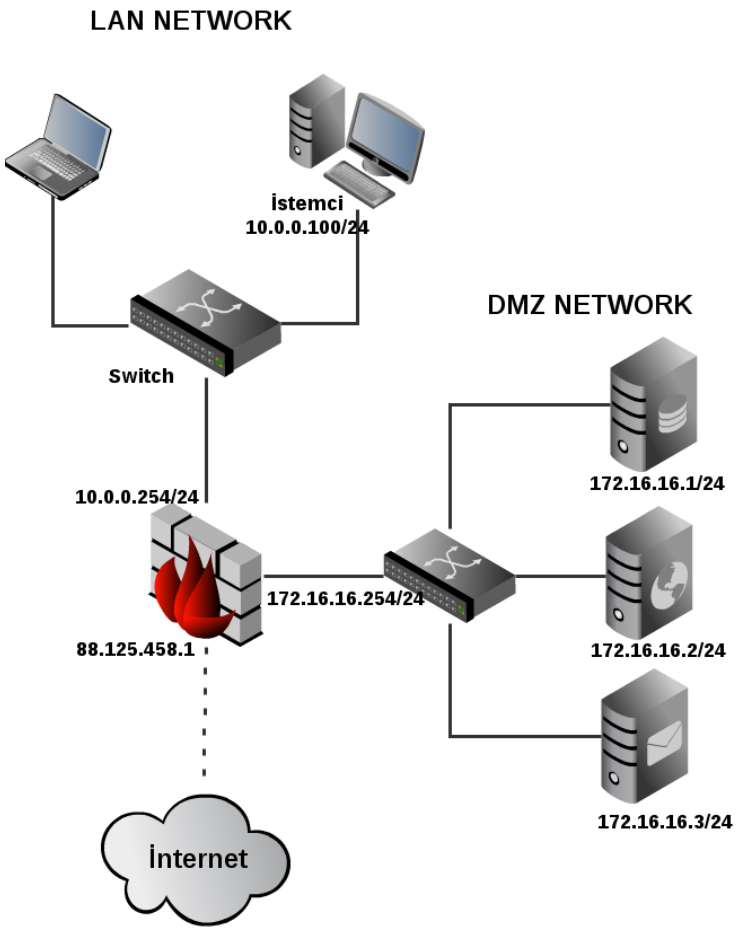
Bölüm 11:
Services | OLSRD

Kablosuz cihazlar arası kablo çekmeden atlama yaparak neti dağıtmak için kullanılır.

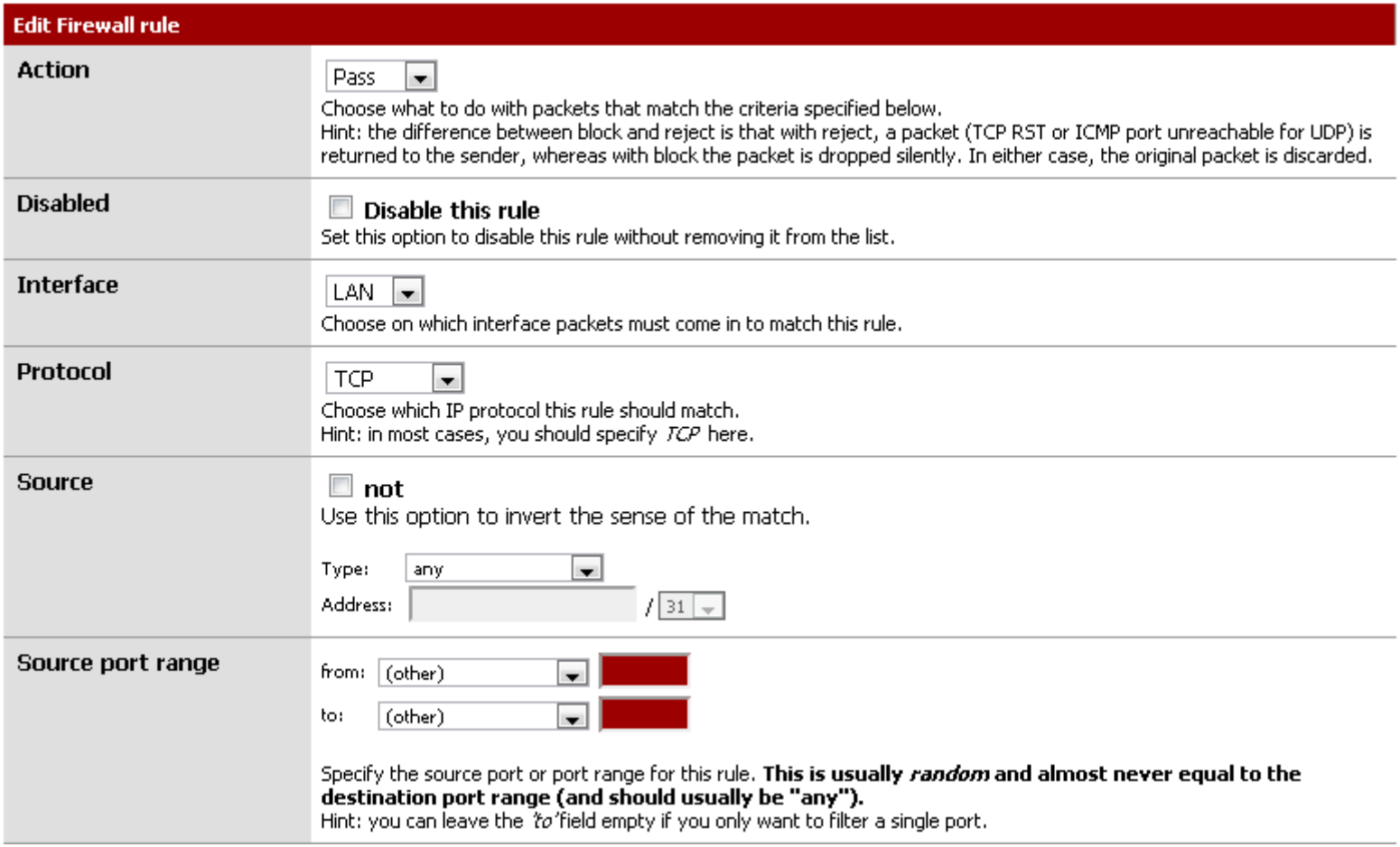


Bölüm 11:
Services | OLSRD

Bölüm 12:
Firewall



Bölüm 12:
Firewall | Rules I



Bölüm 12:
Firewall | Rules I

Action : Pakete uygulanacak kriter.

– ***Pass:*** Paketin geçişine izin ver.

–***Block:*** Paketi engelle (drop et)

–***Reject:*** TCP paketlerine TCP RST, UDP için ICMP port unreachable yanıtını döndür.

Disabled: Kuralı pasif yap.

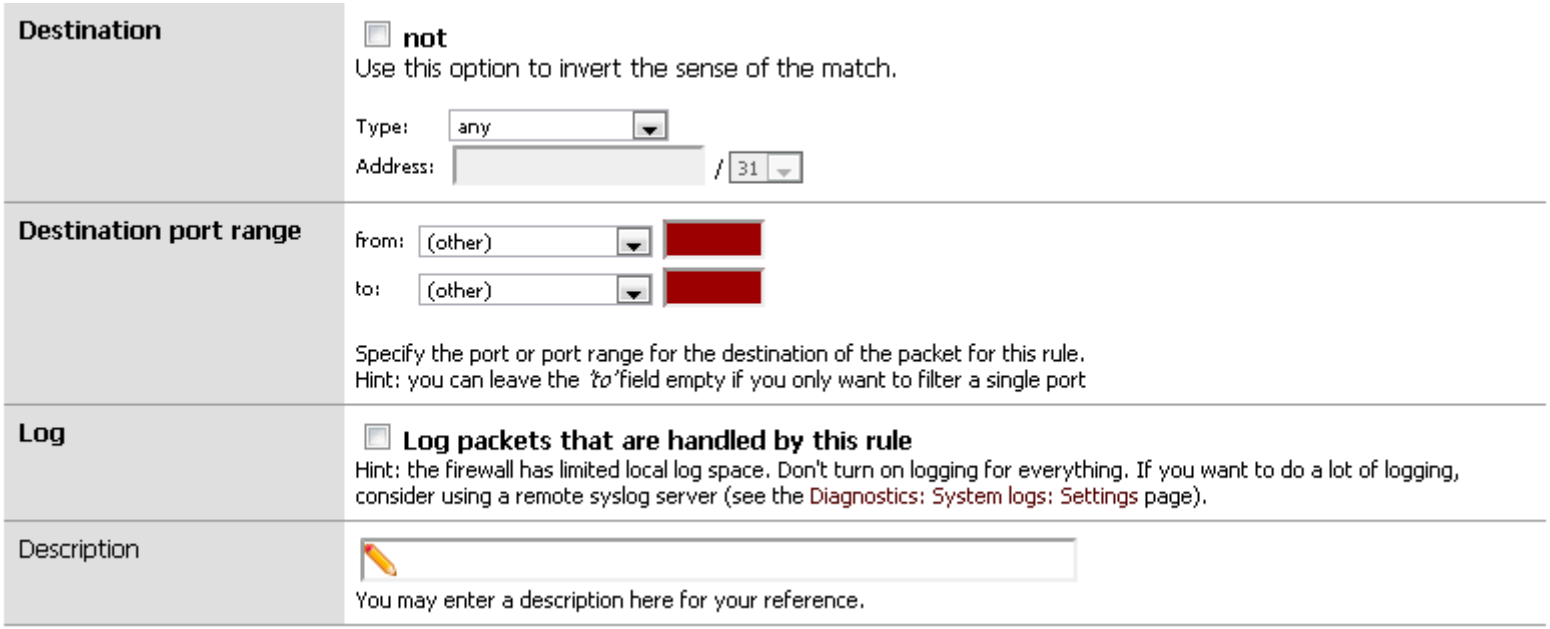
Interface: Kuralın uygunalacağı ağ arabirimi

Protocol: Kullanılacak IP protokolü

Source: Kaynak türü; IP,Network,Ağ arabirimi, Aliase, Subnet vb.

–***Source port range:*** Kaynak port aralığı

Bölüm 12:
Firewall | Rules II



Bölüm 12:
Firewall | Rules II

Destination: Hedef türü; IP,Network,Ağ arabirimi, Aliase, Subnet vs.

–***Destination port range:*** Hedef port aralığı.

Log: Kural için kayıt tut.

Description: Kuralı tanımlayan hatırlatıcı bir mesaj.

Bölüm 12:
Firewall | Rules III

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

Bölüm 12:
Firewall | Rules III

Source OS: Kuralın geçerli olacağı işletim sistemi. Yalnızca TCP kuralları için geçerli olur.

Diffserv Code Point: Bu mekanizma QOS için geliştirilmiştir. Sistemler, paketin kod noktası değerlerine göre önceliğini belirler.

Advanced Options: PF Gelişmiş Seçenekler

- ***Simultaneous client connection limit***: Eşzamanlı istemci bağlantı limit: Limiti
- ***Maximum state entries per host:*** İstemciye gelecek maksimum baglanti siniri
- ***Maximum new connections / per second:*** Eşzamanlı maksimum yeni bağlantı
- ***State Timeout in seconds:*** Saniye içinde zaman aşırımı süresi

TCP Flags: *TCP bayraklarını set etmek için kullanılır.*

State Type: Durum türü

- ***keep state:*** Tüm IP protokolleri ile çalışır.
- ***synproxy state***: Proksilerden gelen TCP bağlantıları için sunucuyu Syn Flood ve IP Spoof saldırılarına karşı korunmaya yardımcı olur.
- **none**: Bir durum mekanizması kullanma

Bölüm 12:
Firewall | Rules III

No XMLRPC Sync: *CARP yapısındaki diğer firewalla kuralın akarılmasını engeller.*

Schedule: Kuralın çalışacağı zaman, zamanlanmış görev.

Gateway: Kural tabanlı yönlendirme için hedef belirler.

In/Out: *Virtual interface'ler için trafik şekillendirme*

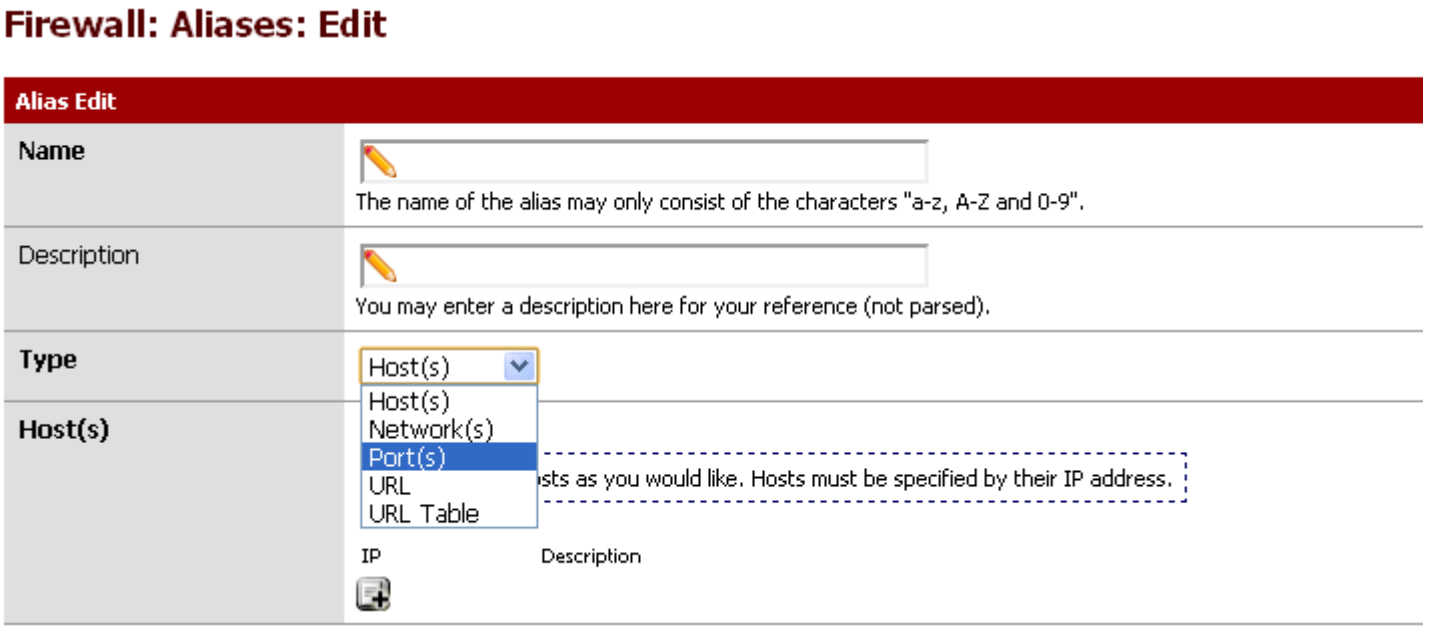
Ackqueue/Queue : *Trafik şekillendirme*

Layer 7: *Uygulama katmanında trafik şekillendirme kuralları uygular*

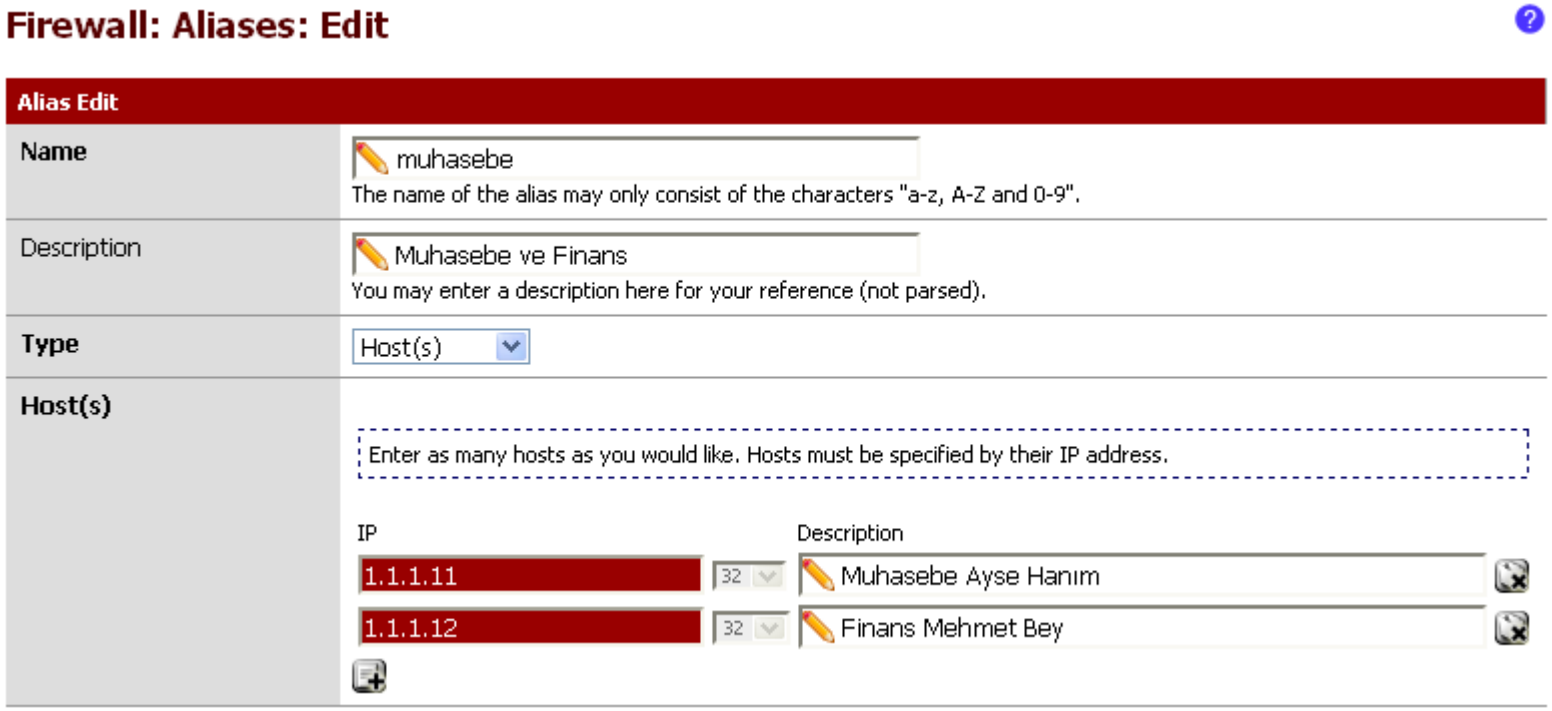
Description: Kuralı tanımlayan hatırlatıcı bir mesaj.

Bölüm 12:
Firewall | Alias

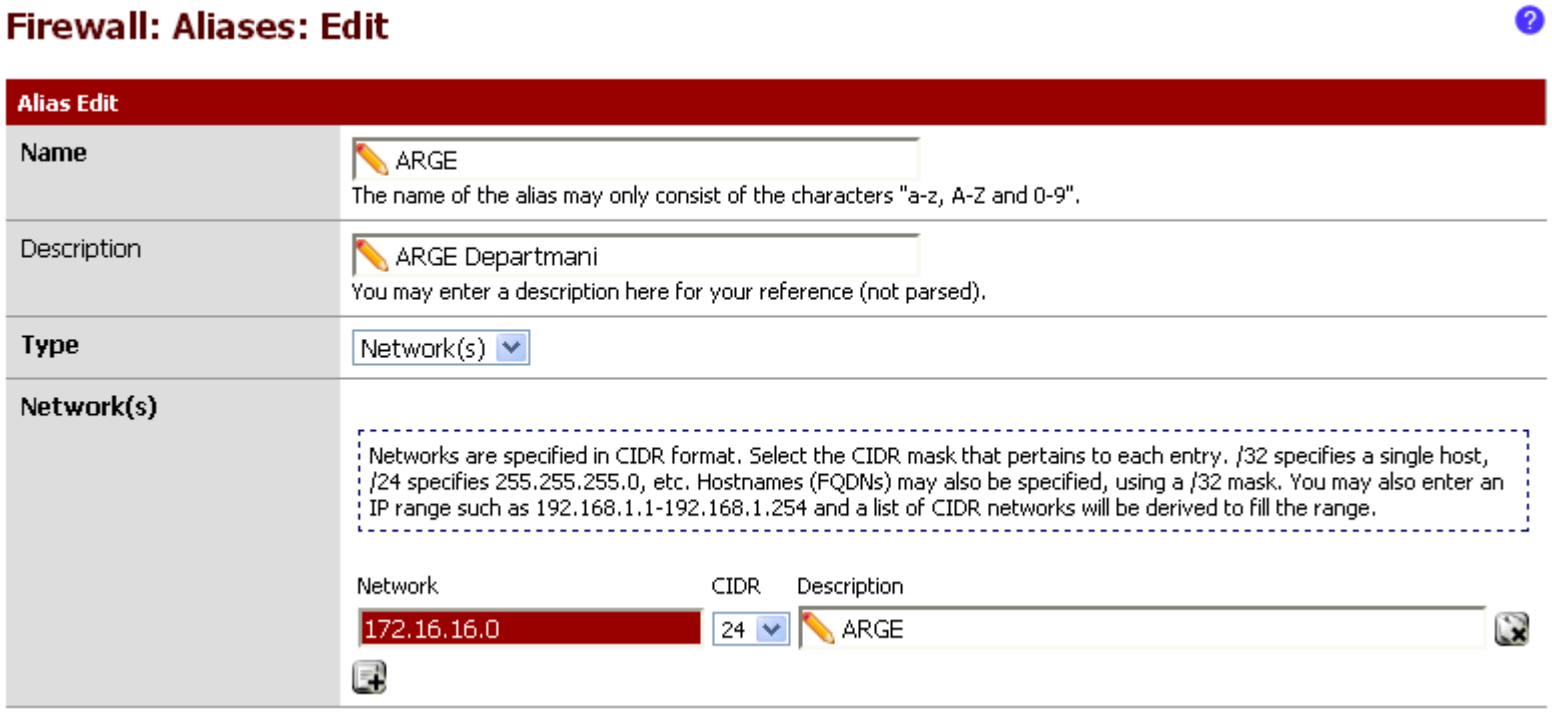
IP, port ve network adreslerini gruplamak için kullanılır. Firewall kurallarında kolaylık sağlar ve geniş ağlar , port numaraları ve kaynak/hedef ip adresleri için efor kazandırır.



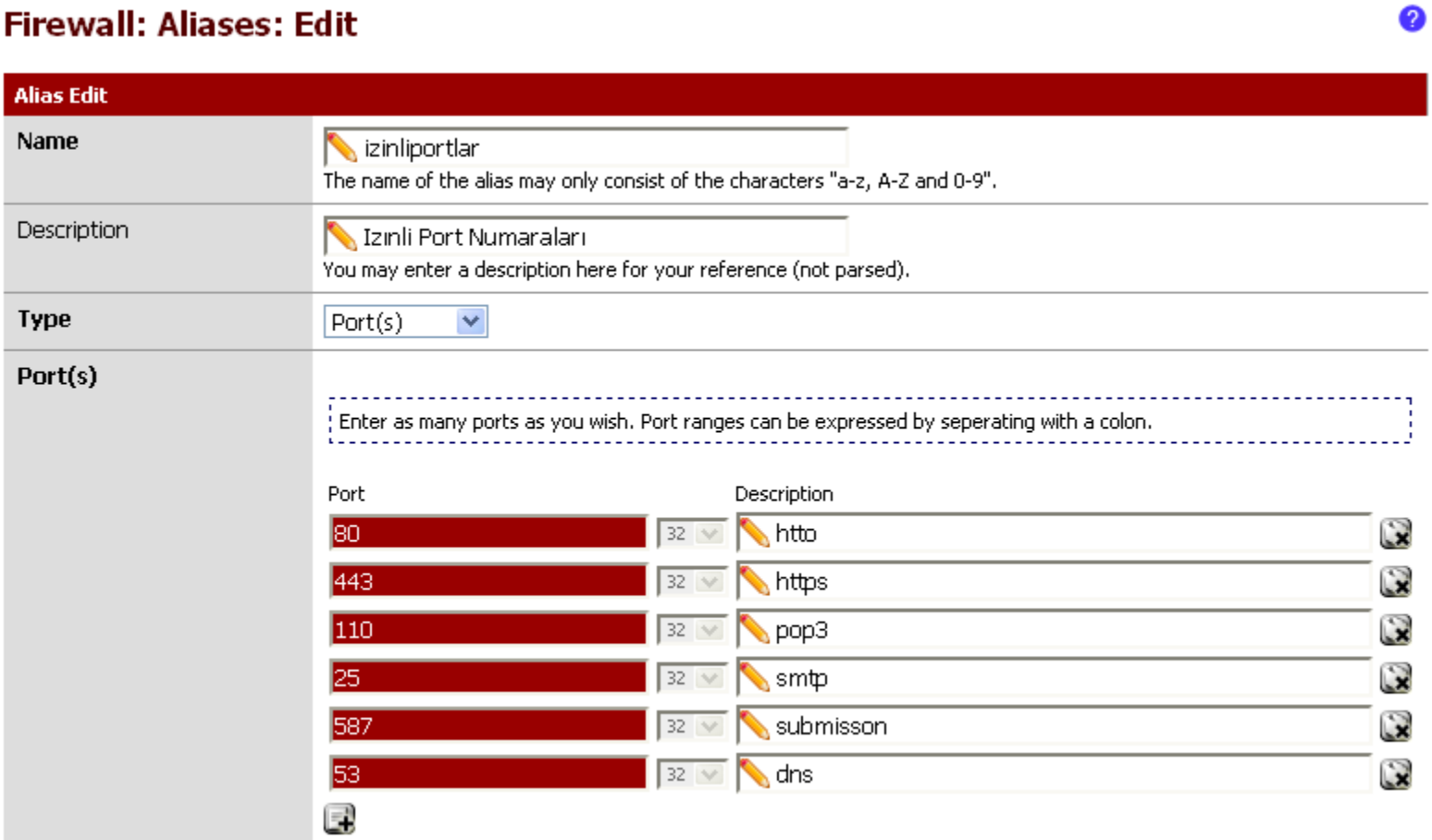
Bölüm 12:
Firewall | Alias | Host



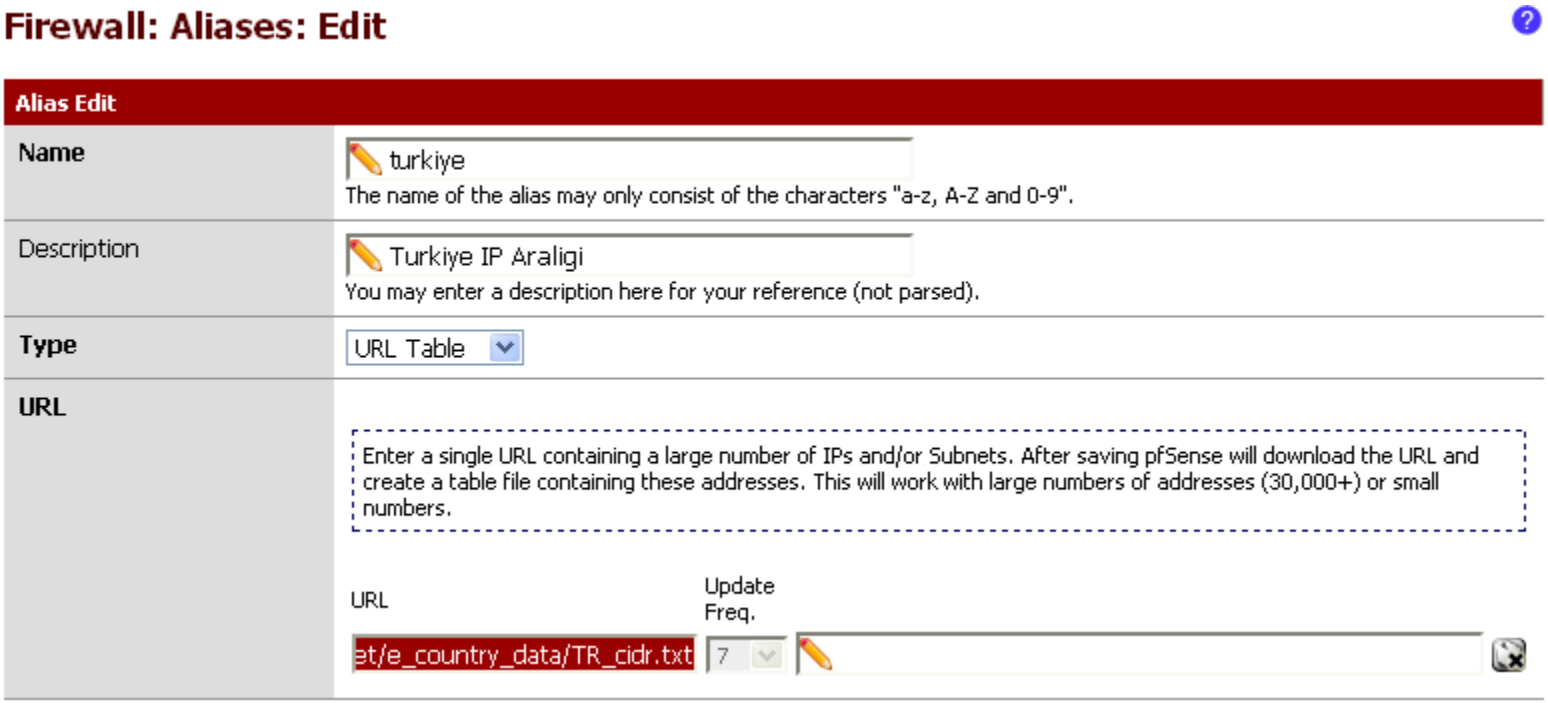
Bölüm 12:
Firewall | Alias | Network



Bölüm 12:
Firewall | Alias | Port

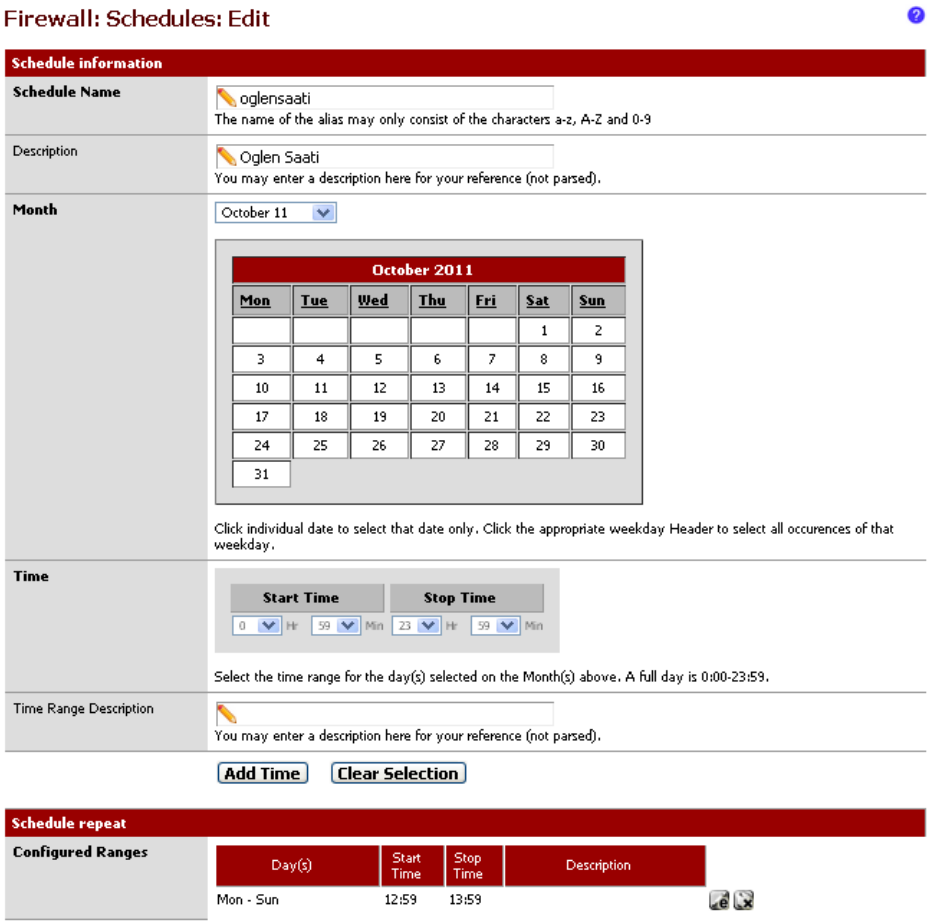


Bölüm 12:
Firewall | Alias | Urltable



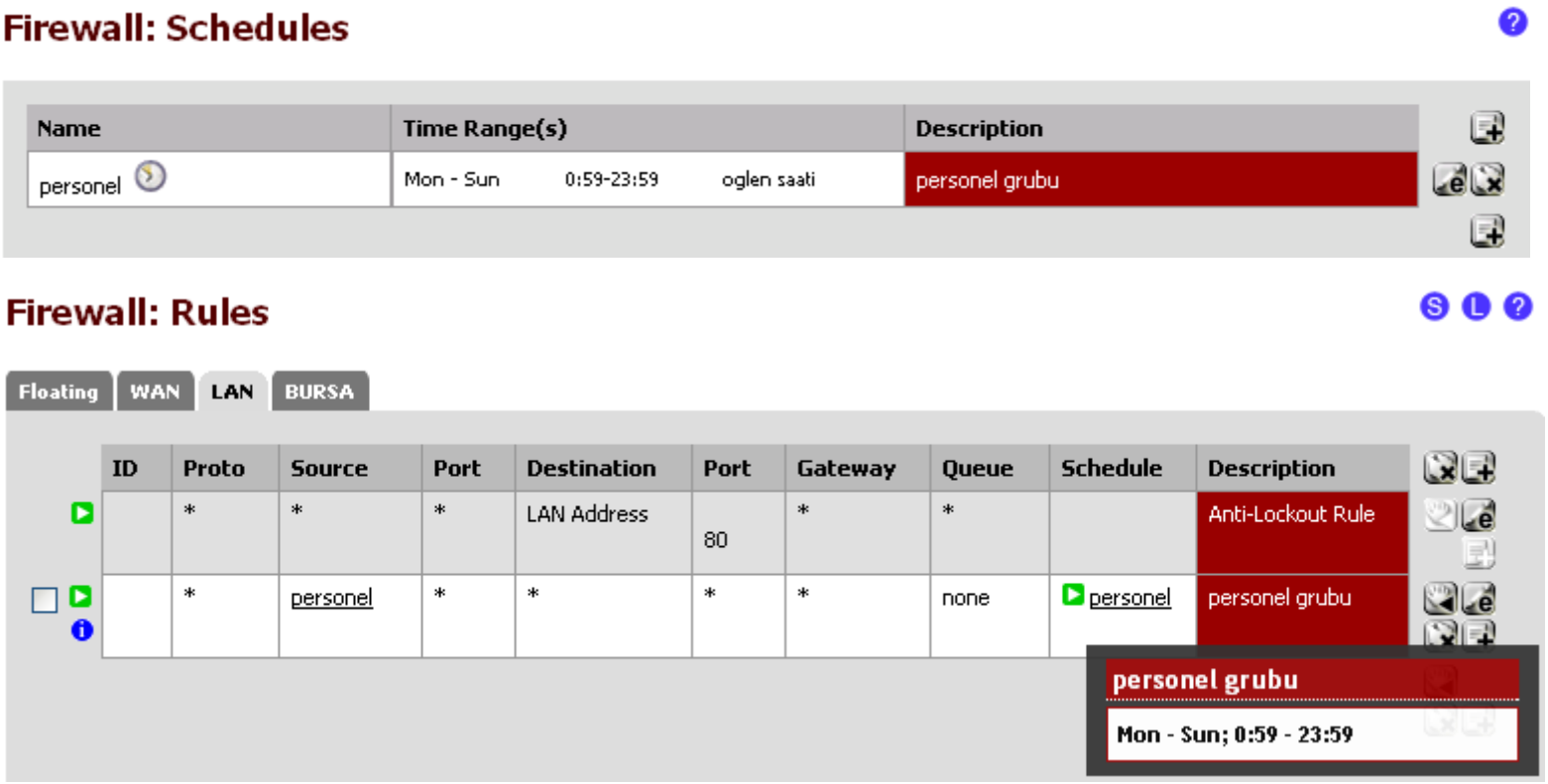
Bölüm 12:
Firewall | Schedules

Zaman bazlı firewall kuralları yazmayı sağlar.



Bölüm 12:
Firewall | Schedules | Uygulama

fabrikam.com personeli için öğlen saatleri arasında (12:59-13:59) internet açık diğer saatlerde kapalı.

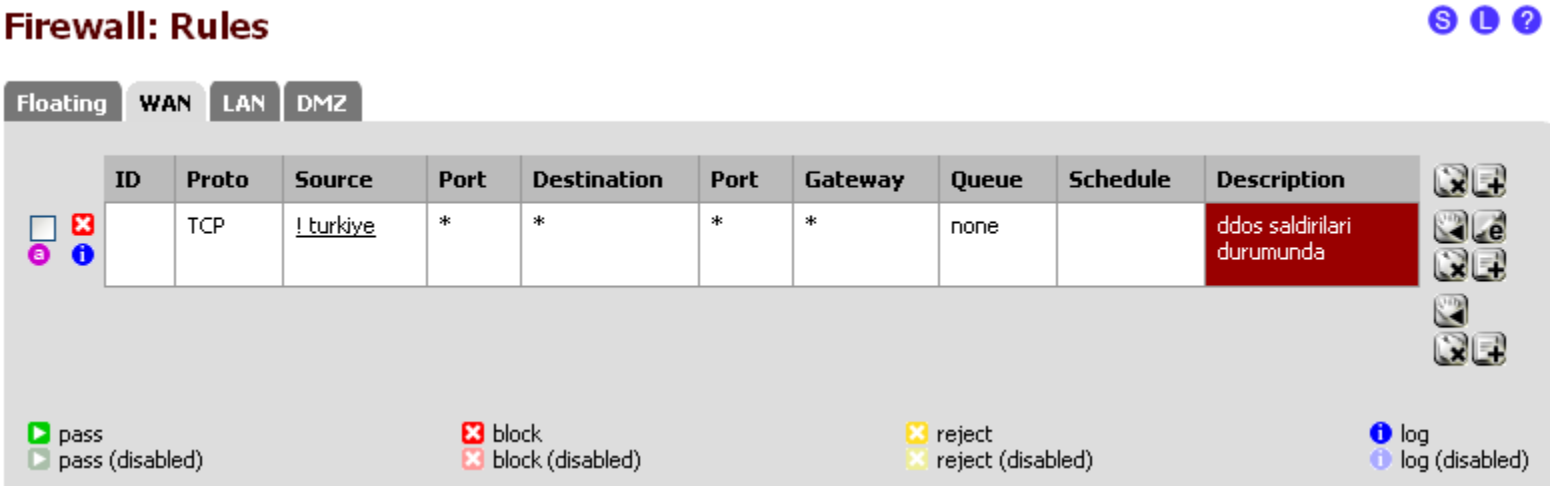


Bölüm 12:
Firewall | Rules | Uygulamalar

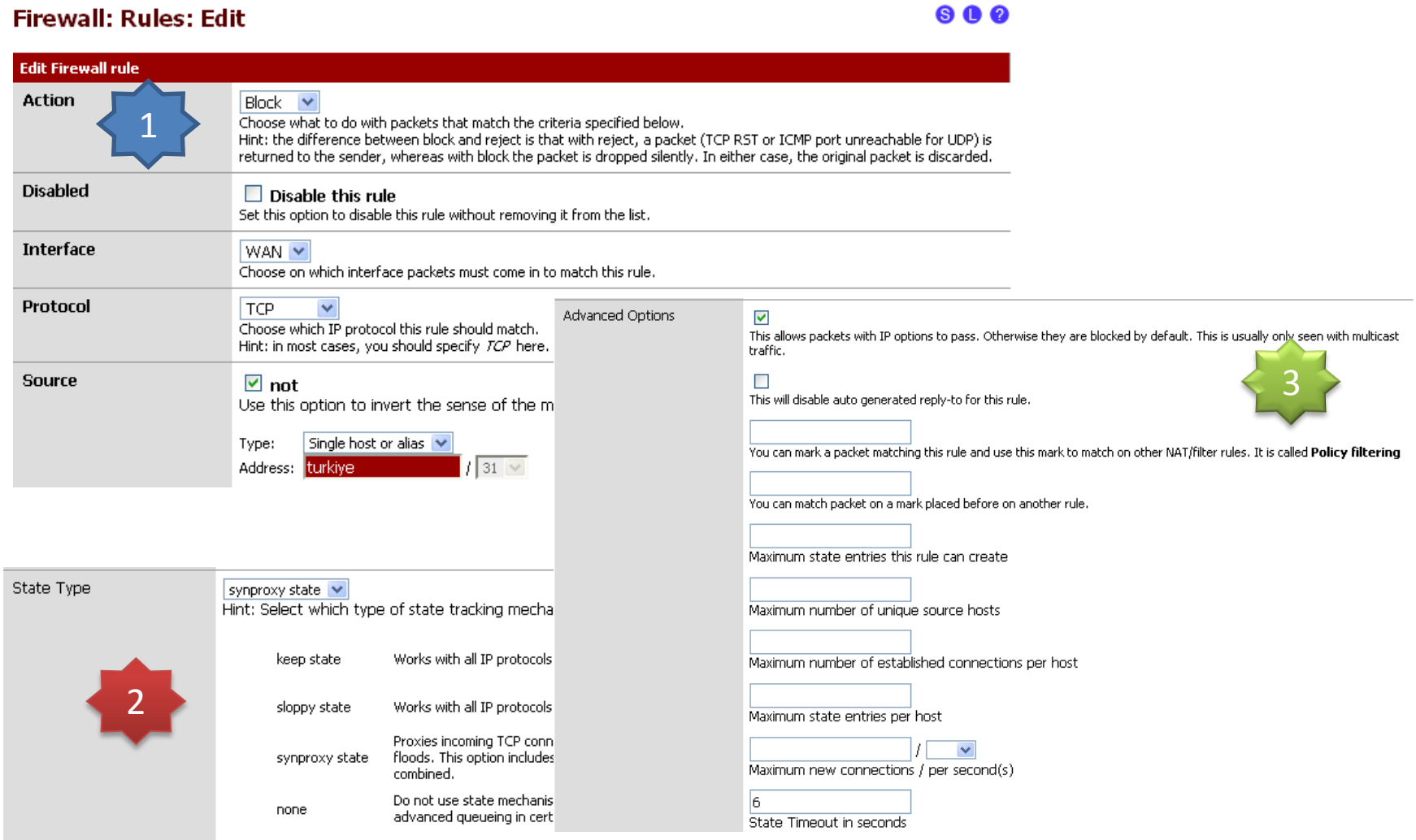
1. DDOS saldırıları durumunda, turkiye ip aralığı dışındaki paketleri engelle ve turkiye'den gelen ip adreslerine eş zamanlı maksimum bağlantı sayısını 5 olarak set et ve timeout süresini 6 saniyeye düşür. Synproxy aktif olsun.
2. Arge ve Muhasebe&Finans birimleri yalnızca izinli port'lara erişim kurabilsinler ve bağlantıları kayıt altına alınsın. Geri kalan herşey yasak.
3. 172.16.16.0/24 subnet'ine yalnızca LAN network'ünden 1.1.1.100 ip adresi erişebilsin.
4. 172.16.16.0/24 subnet'I internete yalnızca tcp 80 ve 443 portu için izinli olsun.

Bölüm 12:
Firewall | Rules | Uygulama I

1. Internetten gelebilecek DDOS saldırıları durumunda, Türkiye ip aralığı dışındaki ipleri engelle. Türkiye'den gelen ip adreslerinin eş zamanlı maksimum bağlantı sayısı 5 olsun ve bir tcp oturumun timout süresi 6 saniyeye olsun. Spoof edilmiş ip adreslerine karşı Synproxy koruması da aktif olsun.



Bölüm 12:
Firewall | Rules | Uygulama I



Bölüm 12:
Firewall | Rules | Uygulama II & III

2. Arge ve Muhasebe&Finans birimleri yalnızca izinli port'lara erişim kurabilsinler ve bağlantıları kayıt altına alınsın. Geri kalan herşey yasak.
3. 172.16.16.0/24 subnet'ine yalnızca LAN network'ünden 1.1.1.100 ip adresi erişebilsin.

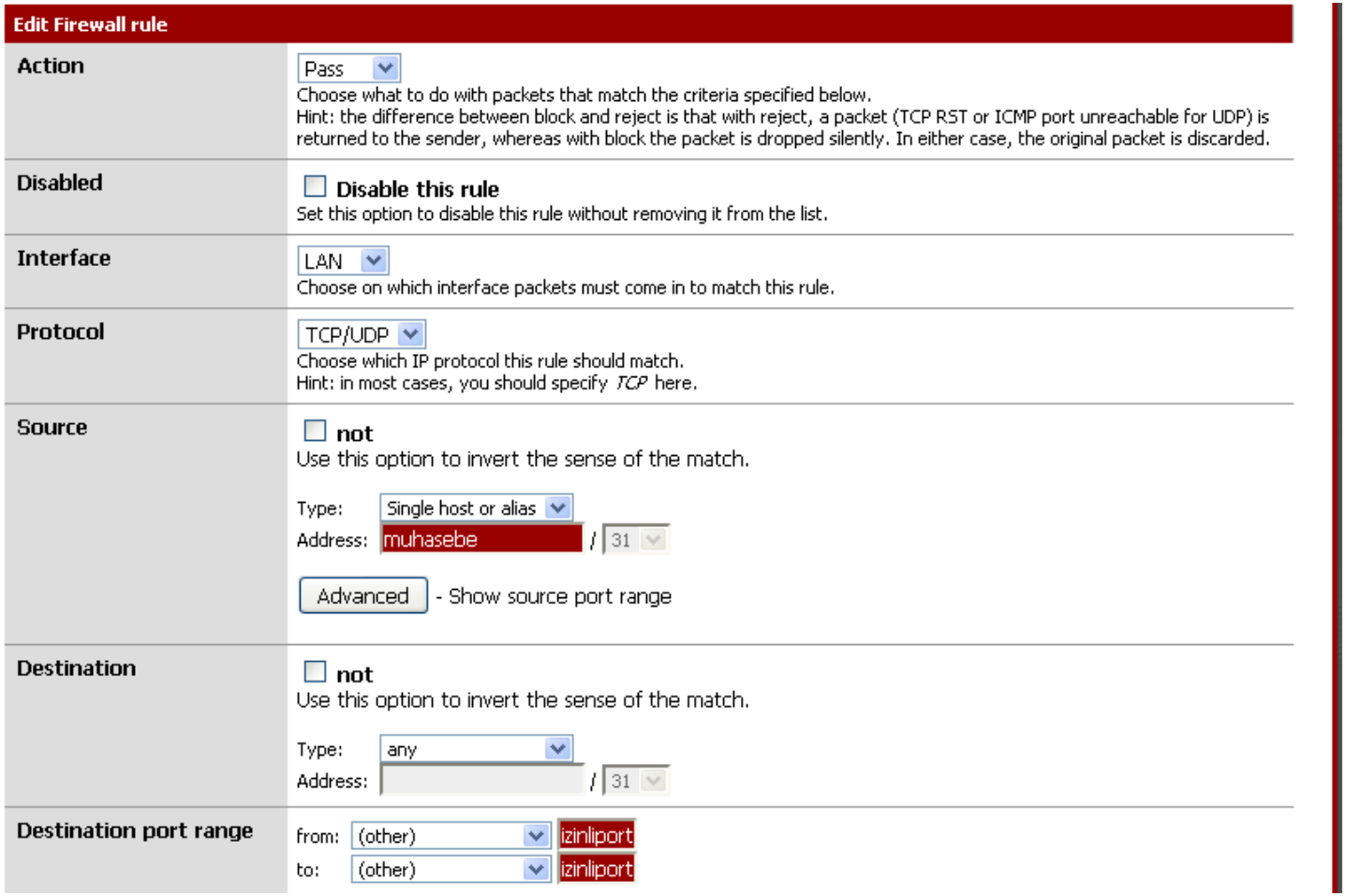
Firewall: Rules

Floating | WAN | LAN | DMZ

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
☐		TCP/UDP	muhasebe	*	*	izinliportlar	*	none		Muhasebe ve Finans
☐		*	1.1.1.100	*	ARGE	*	*	none		Accept for ARGE

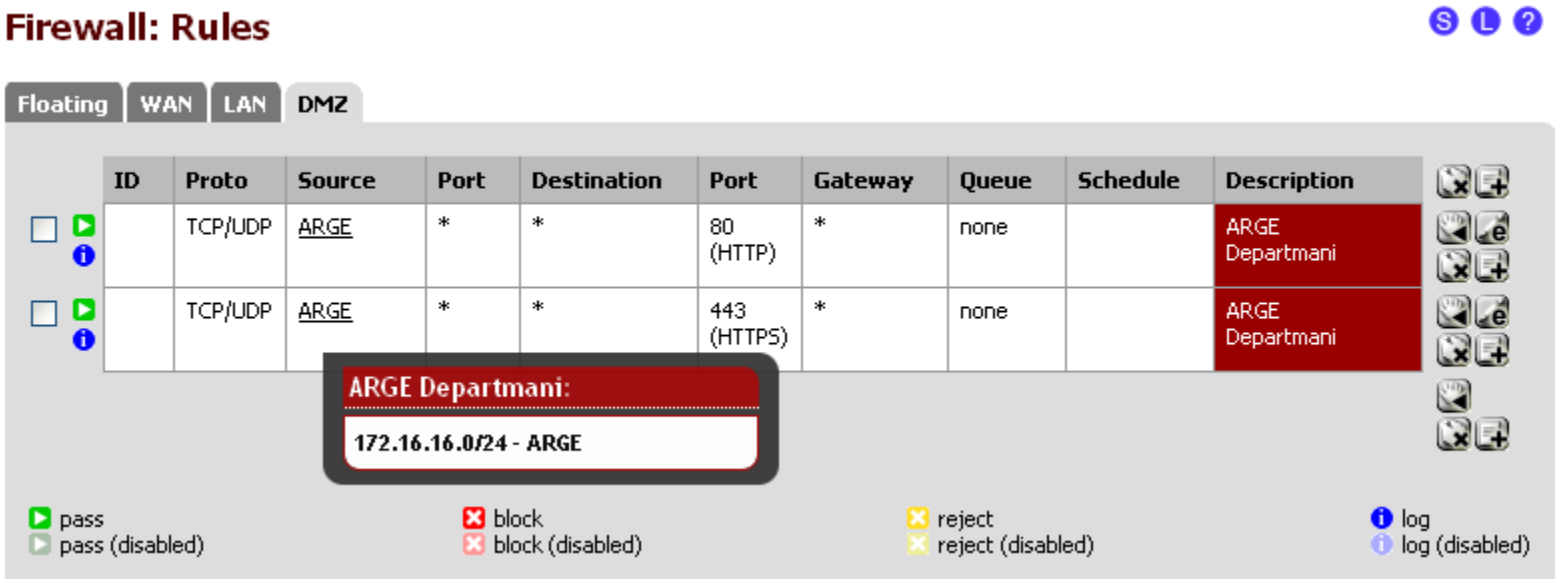
pass / pass (disabled) — block / block (disabled) — reject / reject (disabled) — log / log (disabled)

Bölüm 12:
Firewall | Rules | Uygulama II



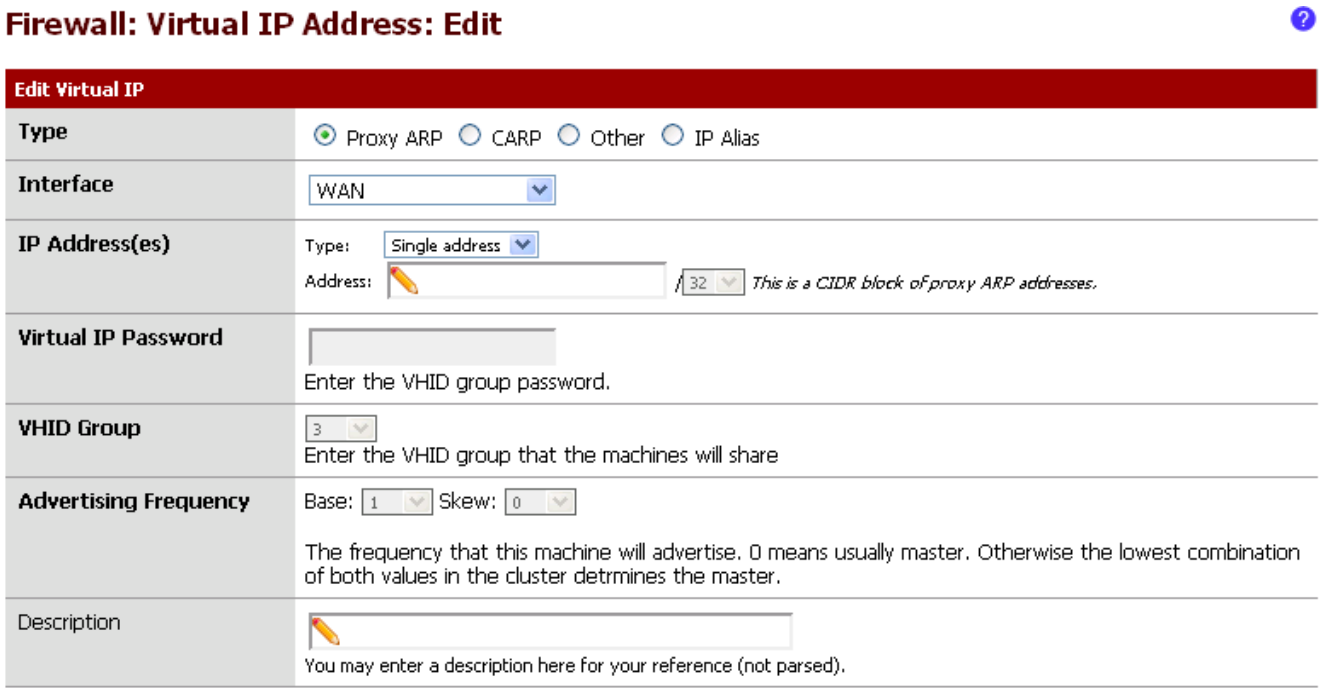
Bölüm 12:
Firewall | Rules | Uygulama IV

4. 172.16.16.0/24 subnet'I internete yalnızca tcp 80 ve 443 portu için izinli olsun.



Bölüm 12:
Firewall | Virtual IP

pfSense tarafından kullanılan sanal IP adresidir, ağ arabirimi için tanımlanan ana IP adresi değildir.Virtual IP, pfSense tarafından NAT port forwarding, Outbound NAT ve 1:1 NAT gibi yönlendirme işlemlerinde kullanılır.Ayrıca failover gibi özellikler içinde kullanılır. pfSense 2.0 ile birlikte ağ arabirimine ikinci ip adresi atama özelliğide virtual ip ile desteklenmektedir.



Bölüm 12:
Firewall | Virtual IP

Virtual IP Adres Türleri

CARP

Firewall servisleri veya yönlendirmeler için kullanılır
VIP için Layer 2 trafik üretir
Clustering işlemi için kullanılabilir.
Gerçek ağ arabiriminin IP adresi ile ***aynı subnet'de olabilir.***
ICMP ping paketlerine yanıt verir, firewall tarafından izinliyse

Proxy ARP

Firewall servisleri için kullanılamaz ama yönlendirmeler için kullanılır
VIP için Layer 2 trafik üretir
Gerçek ağ arabiriminin IP adresi ile ***farklı subnet'de olabilir.***
ICMP ping paketlerine yanıt vermez

Diğer

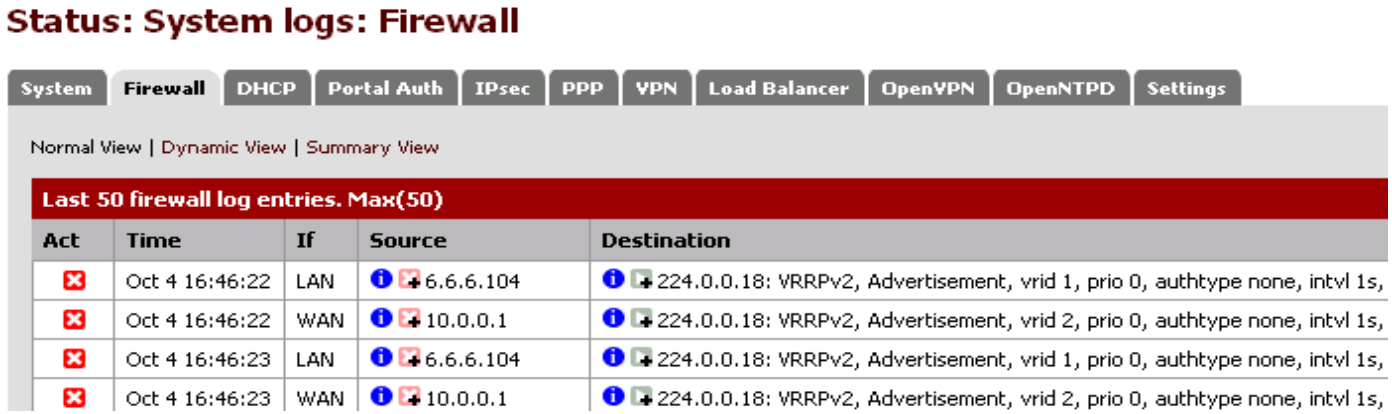
Firewall servisleri için kullanılamaz ama yönlendirmeler için kullanılır
VIP için Layer 2 trafik üretir
Gerçek ağ arabiriminin IP adresi ile ***farklı subnet'de olabilir.***
ICP ping paketlerine yanıt vermez

IP Alias

pfSense tarafından kullanılabilir, yönlendirme yapılabilir.

Bölüm 12:
Firewall | Kayıtların İzlenmesi

Firewall logları, hayati öneme sahiptir.Gelen-Giden paketleri incelemede ve sorun çözmede sıkça ihtiyaç duyulur. Diagnostics | System logs | Firewall sayfasından şu bilgiler edinilebilir;



Action: *Pakete uygulanan kriter*
Time: *Logun oluşma tarihi ve saati*
If: *Paketin geldiği ağ arabirimi*
Source: *Kaynak IP adresi ve Port numarası*
Destination: *Hedef IP adresi ve Port numarası*
Proto: *Protokol*

Bölüm 12:
Firewall | Kayıtların İzlenmesi

Arayüzde yorumlanan kayıtların yetersiz kalması durumunda veya pratik filtreleme teknikleri uygulamak için komut satırından kayıtlar izlenebilir.

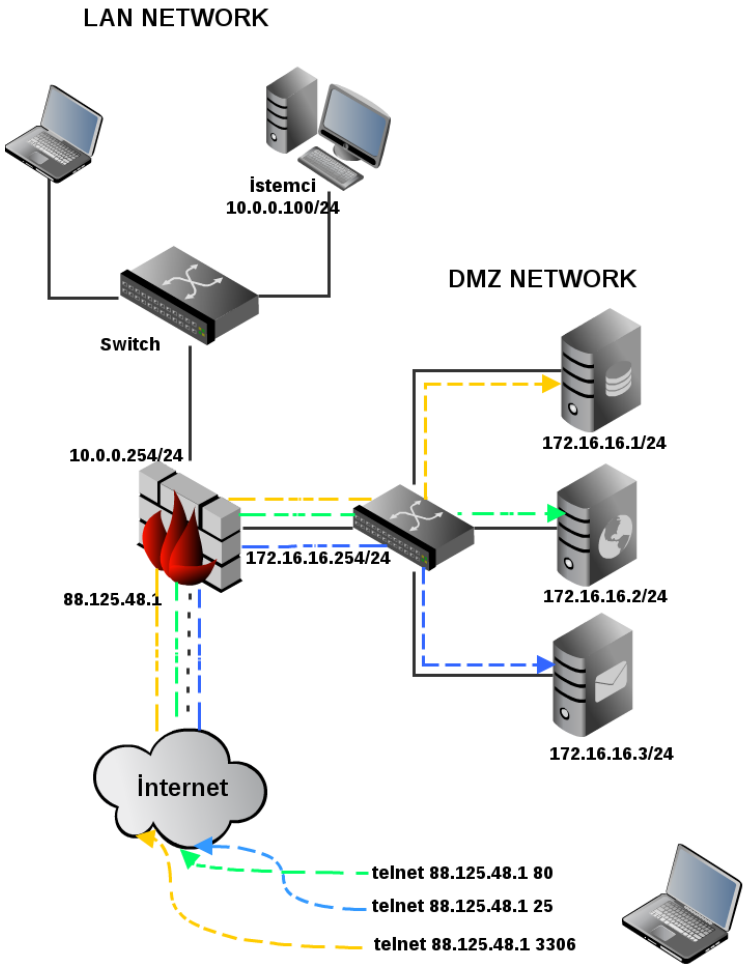
Komut Satırından Görüntüleme

clog /var/log/filter.log
clog -f /var/log/filter.log (logları canlı izlemek için)
clog /var/log/filter.log | php /usr/local/www/filterparser.php

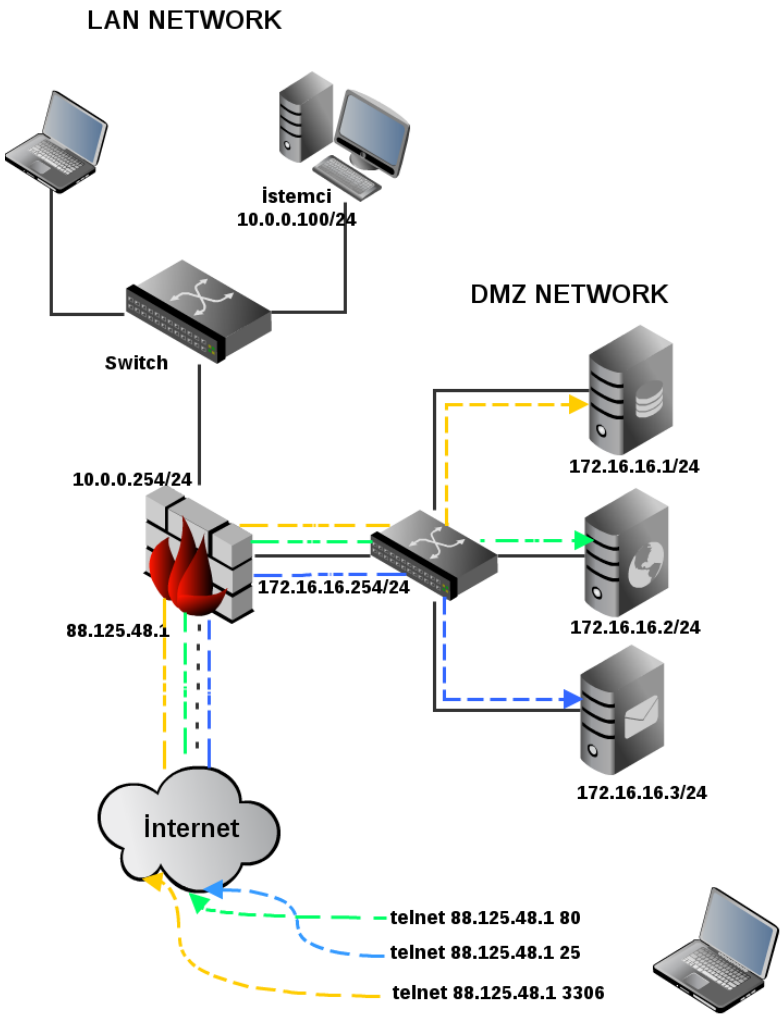
Tcpdump ile izleme

tcpdump -n -e -ttt -r /var/log/filter.log
tcpdump -n -e -ttt -i pflog0

Bölüm 13:
NAT (Network Address Translation)



Bölüm 13:
NAT | Port Forwarding | Uygulama

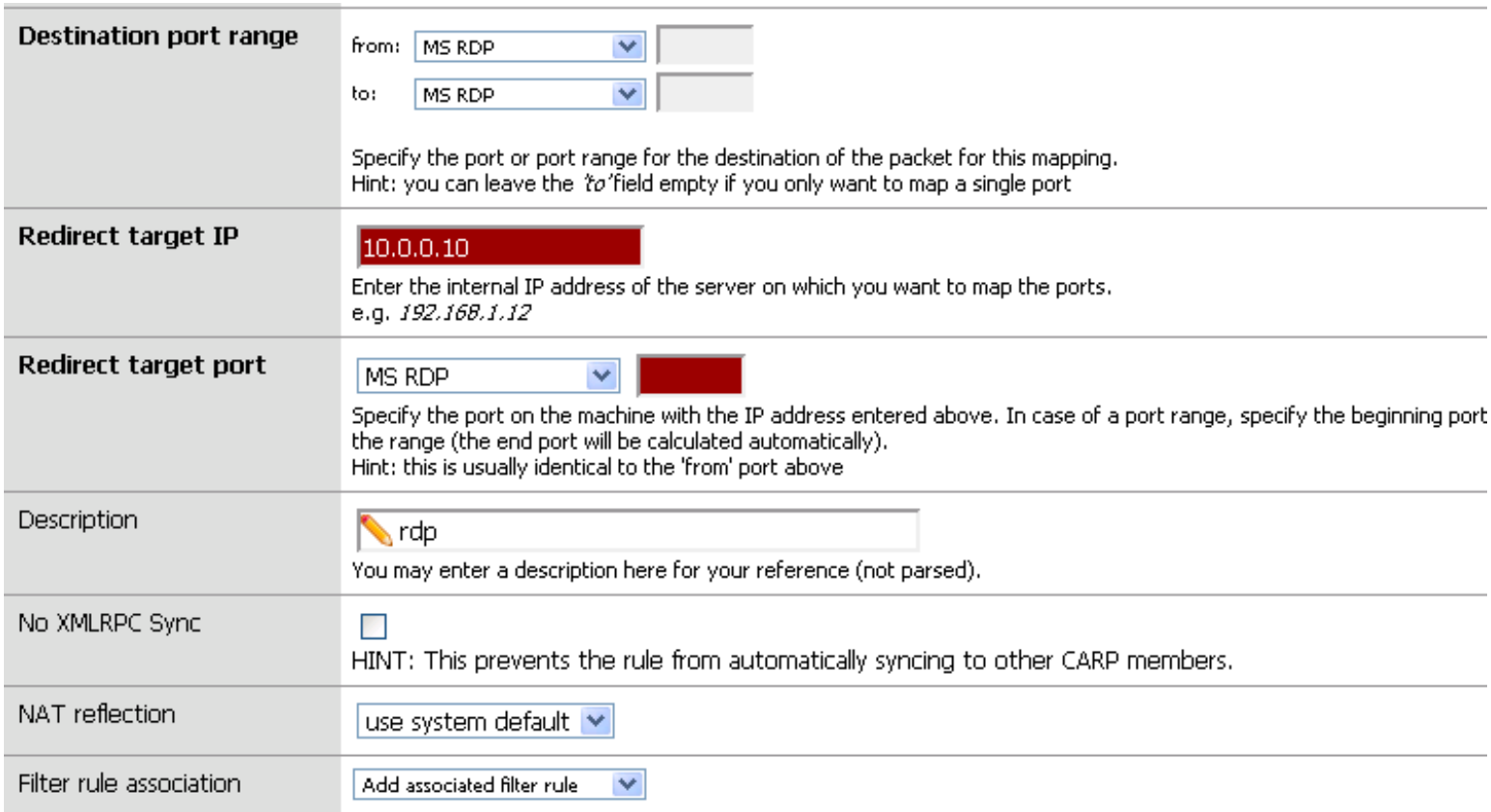


WAN arabiriminden gelen ve hedef portu 80 olan tcp trafiğini 172.16.16.2 adresinin tcp 80 portuna yönlendir.

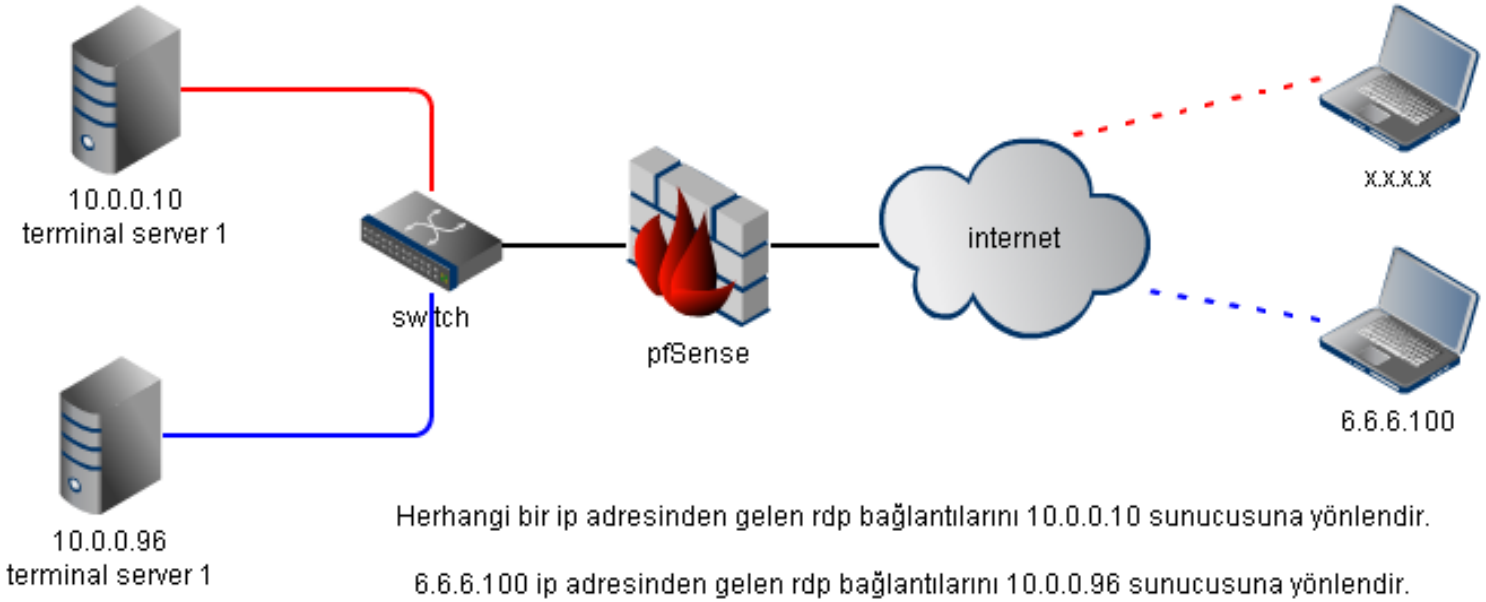
WAN arabiriminden gelen ve hedef portu 587 olan tcp trafiğini 172.16.16.3 adresinin tcp 25 portuna yönlendir.

WAN arabiriminden 85.95.238.172 ip adresi port 3389 a bağlantı isteği gönderirse onu 172.16.16.1 terminal server'a yönlendir.

Bölüm 13:
NAT | Port Forwarding

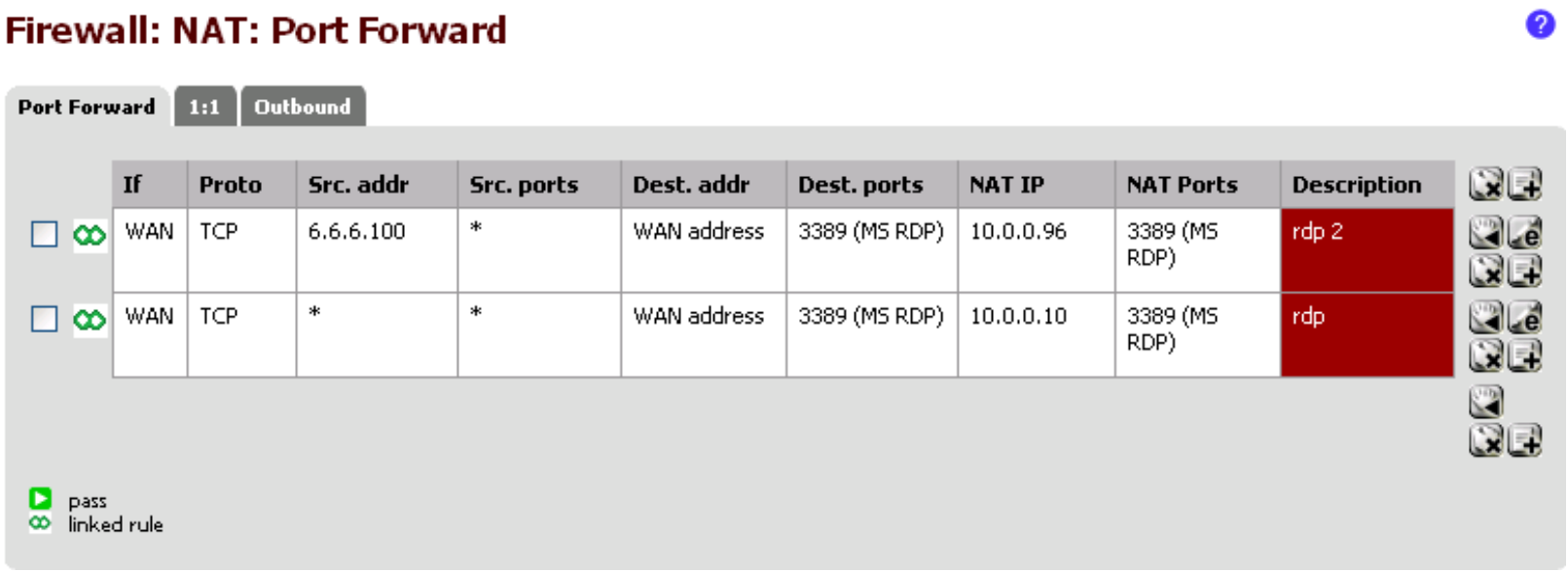


Bölüm 13:
NAT | Port Forwarding | Uygulama

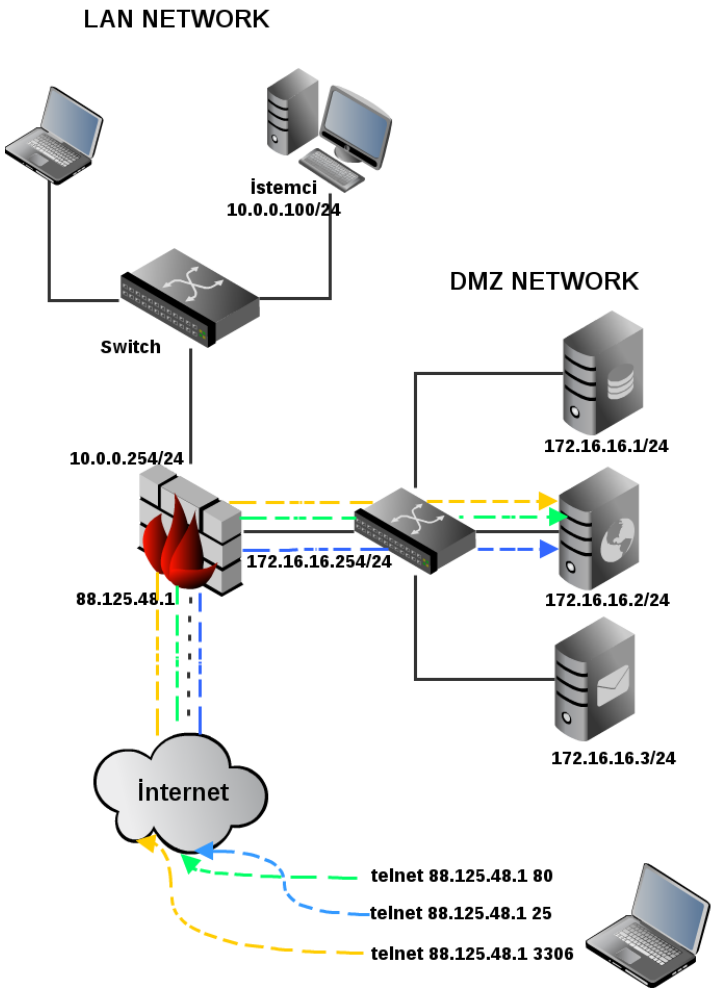


Bölüm 13:
NAT | Port Forwarding | Uygulama

- 6.6.6.100 ip adresi rdp yapmak isterse onu 10.0.0.96 ya yönlendir. Bunun dışındaki rdp bağlantılarını 10.0.0.10 sunucusuna yönlendir.



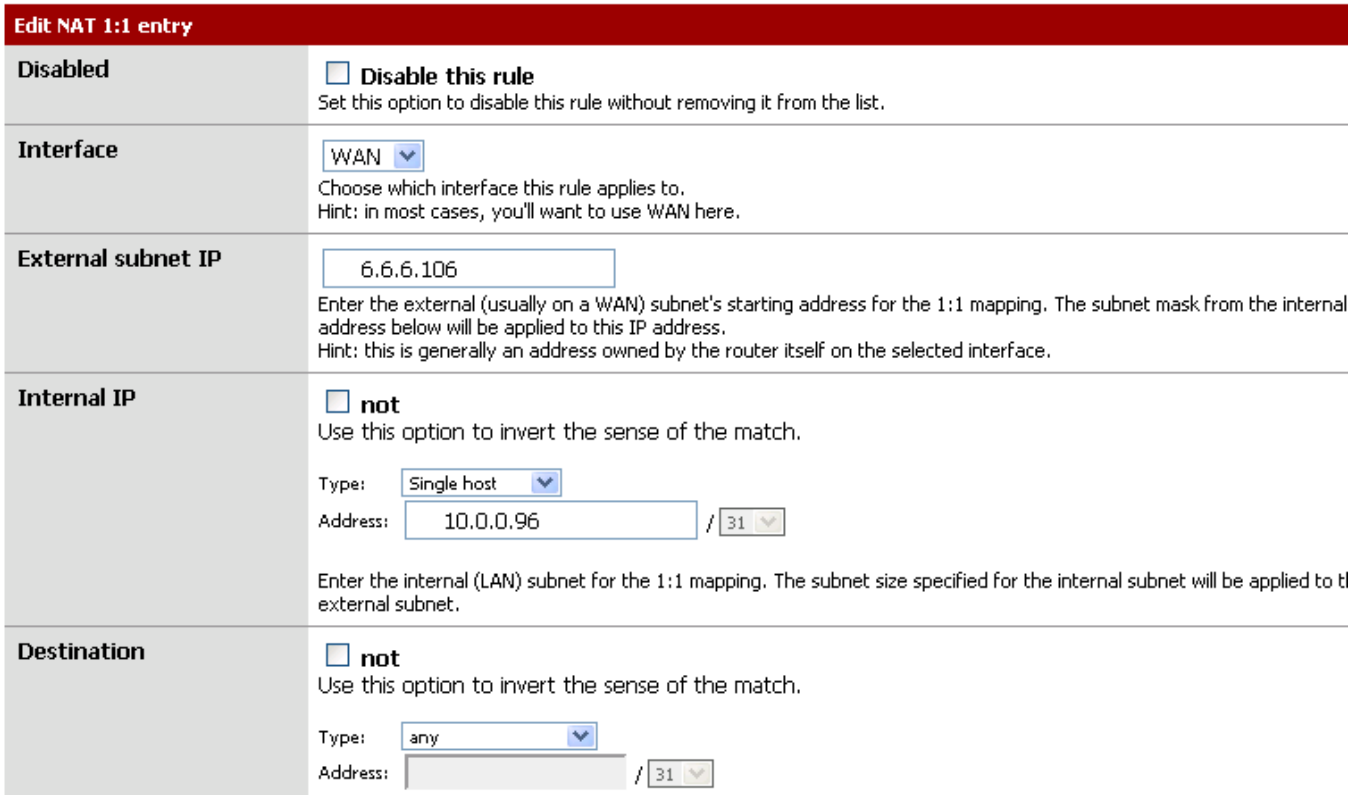
Bölüm 13:
1:1 NAT



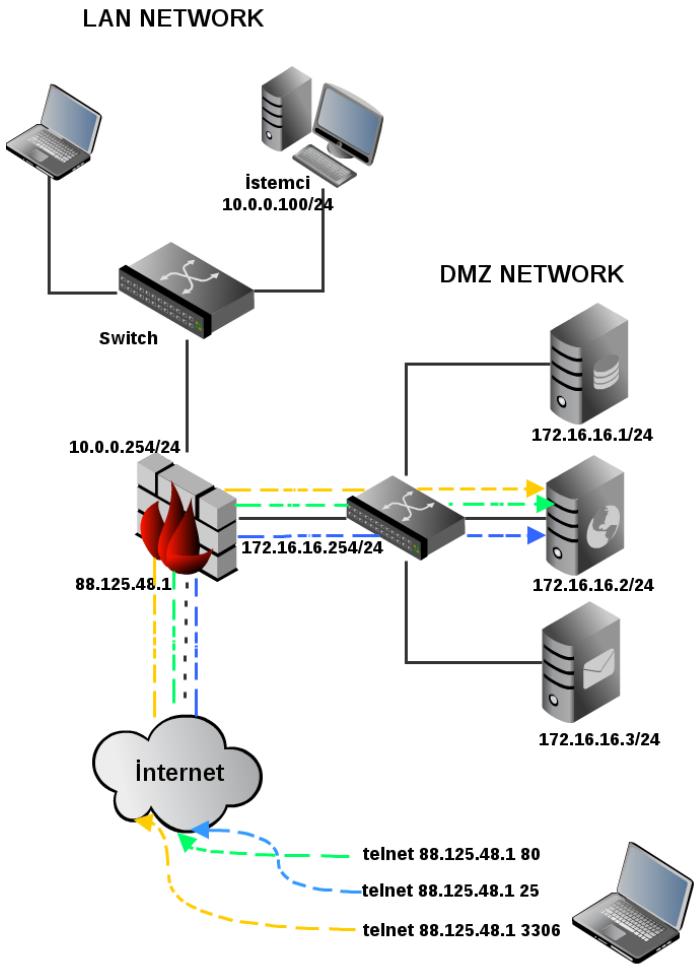
Bölüm 13:
1:1 NAT

Belirtilen IP adresine gelen bütün trafiği bir hedef ip adresine iletir.

Not:Virtual IP ile kullanacağınız internet ip'leri tanımlanmalıdır.

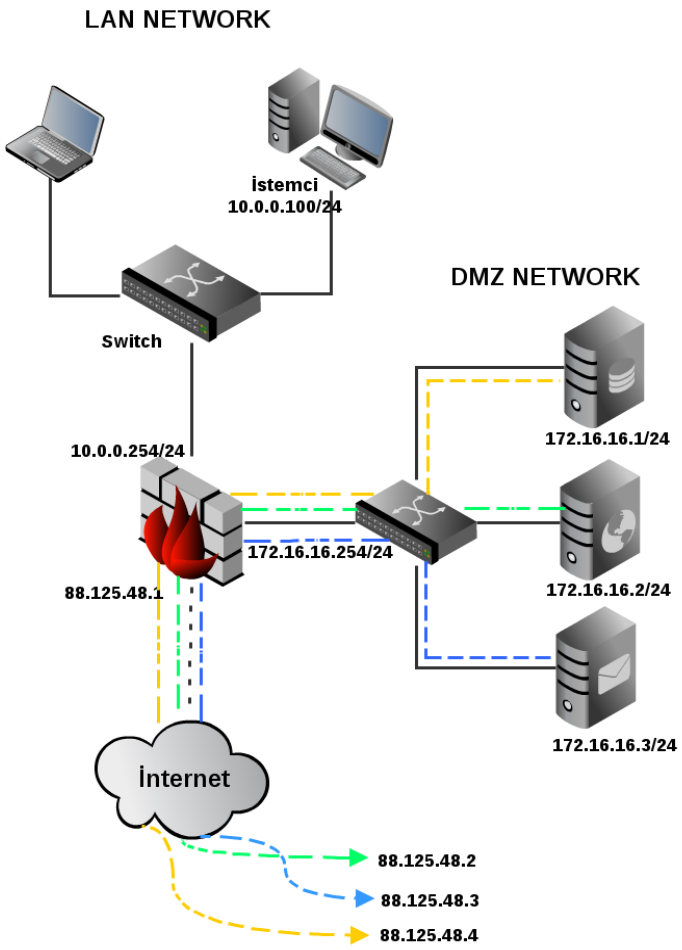


Bölüm 13:
1:1 NAT | Uygulama

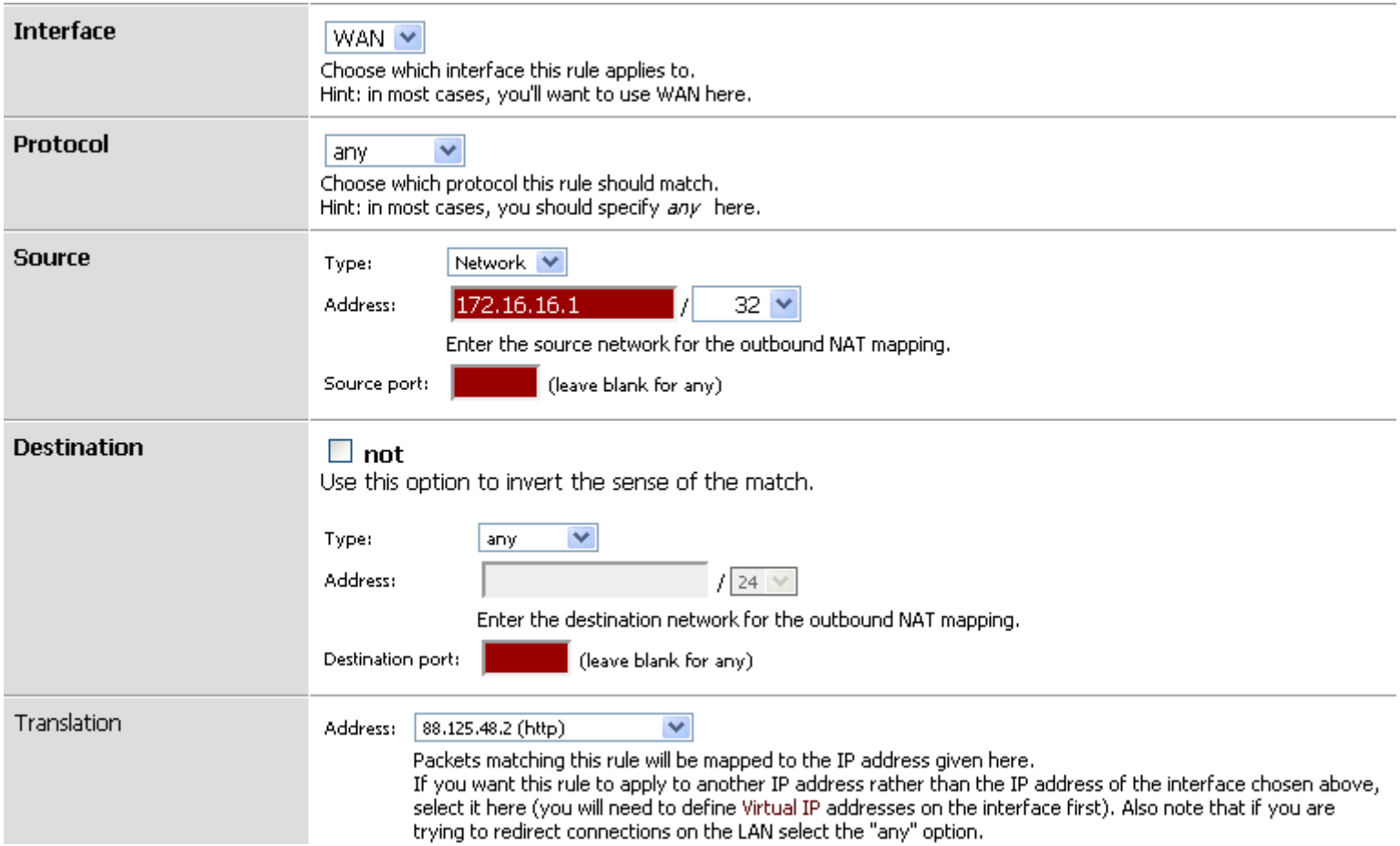


Wan arabiriminden 88.125.48.1 ip adresine gelen tüm trafiği 172.16.16.2 ip adresine bire bir yönlendir.

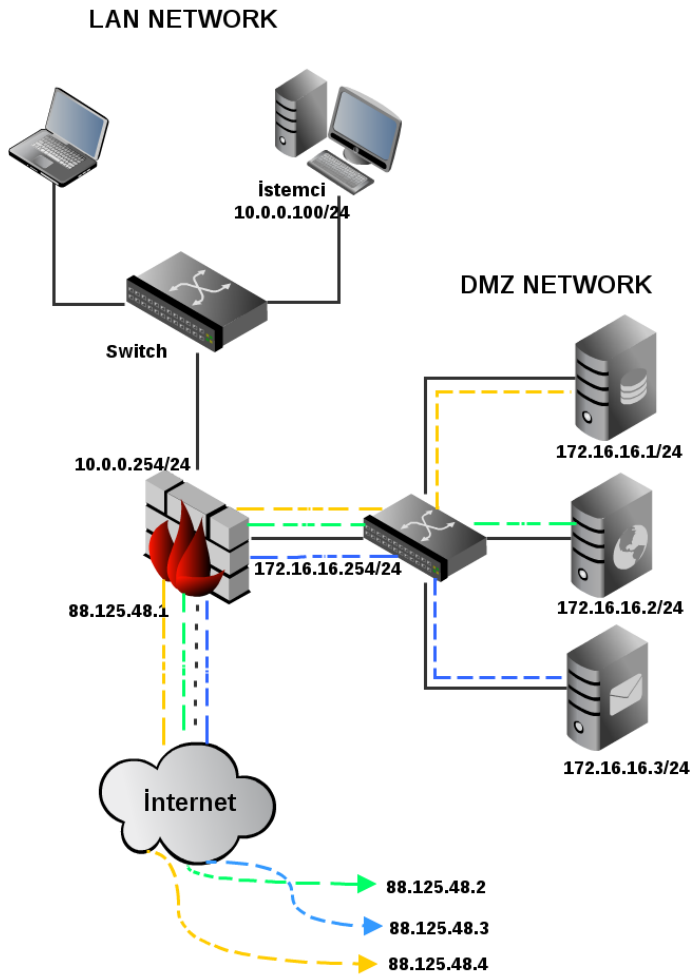
Bölüm 13:
NAT | Outbound NAT



Bölüm 13:
NAT | Outbound NAT



Bölüm 13:
NAT | Outbound NAT | Uygulama

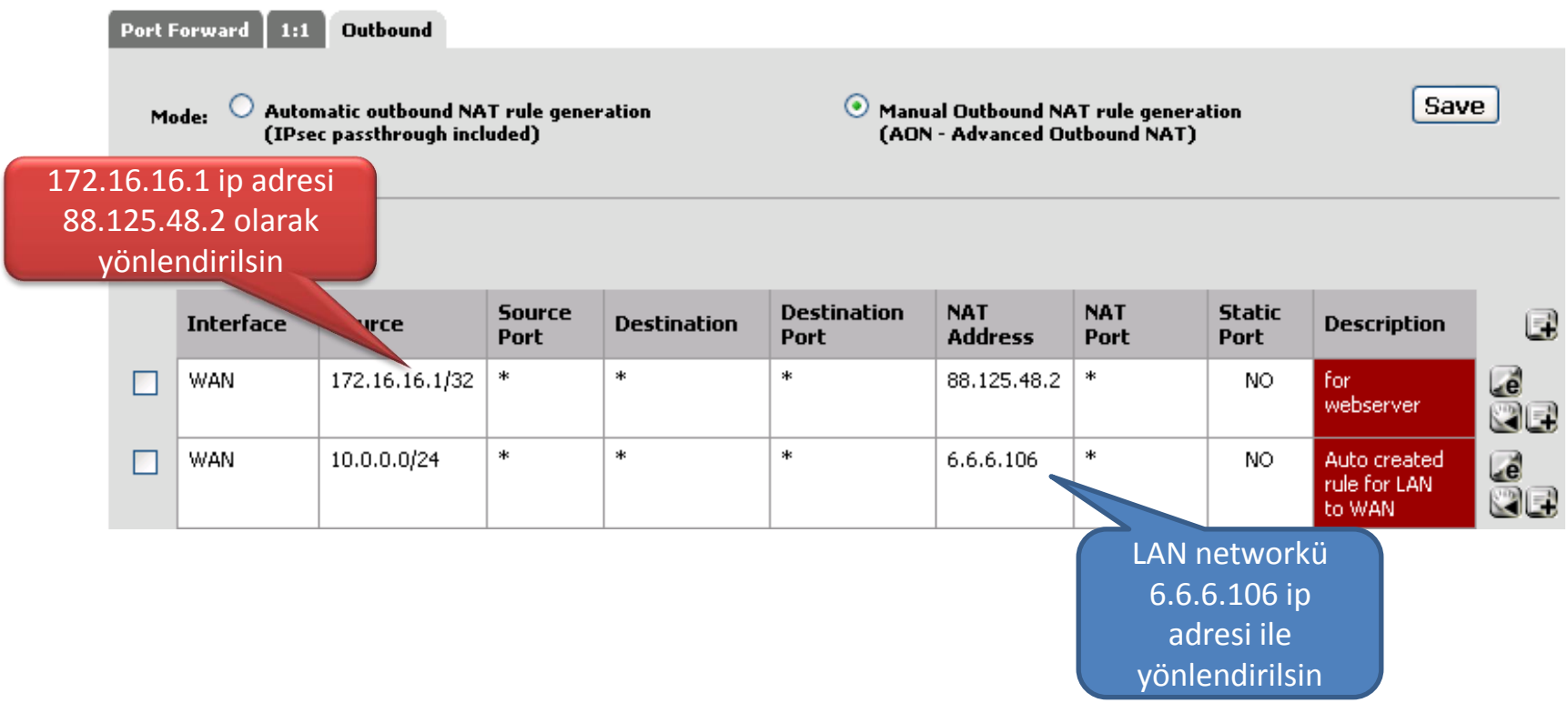


172.16.16.1 ip adresini internet'e çıkarken 88.124.48.1 olarak dönüştür.

172.16.16.2 ip adresini internet'e çıkarken 88.124.48.2 olarak dönüştür.

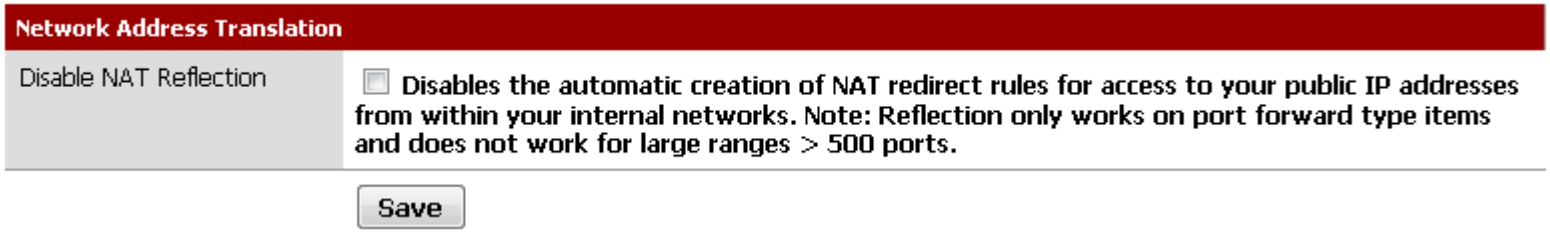
172.16.16.3 ip adresini internet'e çıkarken 88.124.48.3 olarak dönüştür.

Bölüm 13:
NAT | Outbound NAT | Uygulama



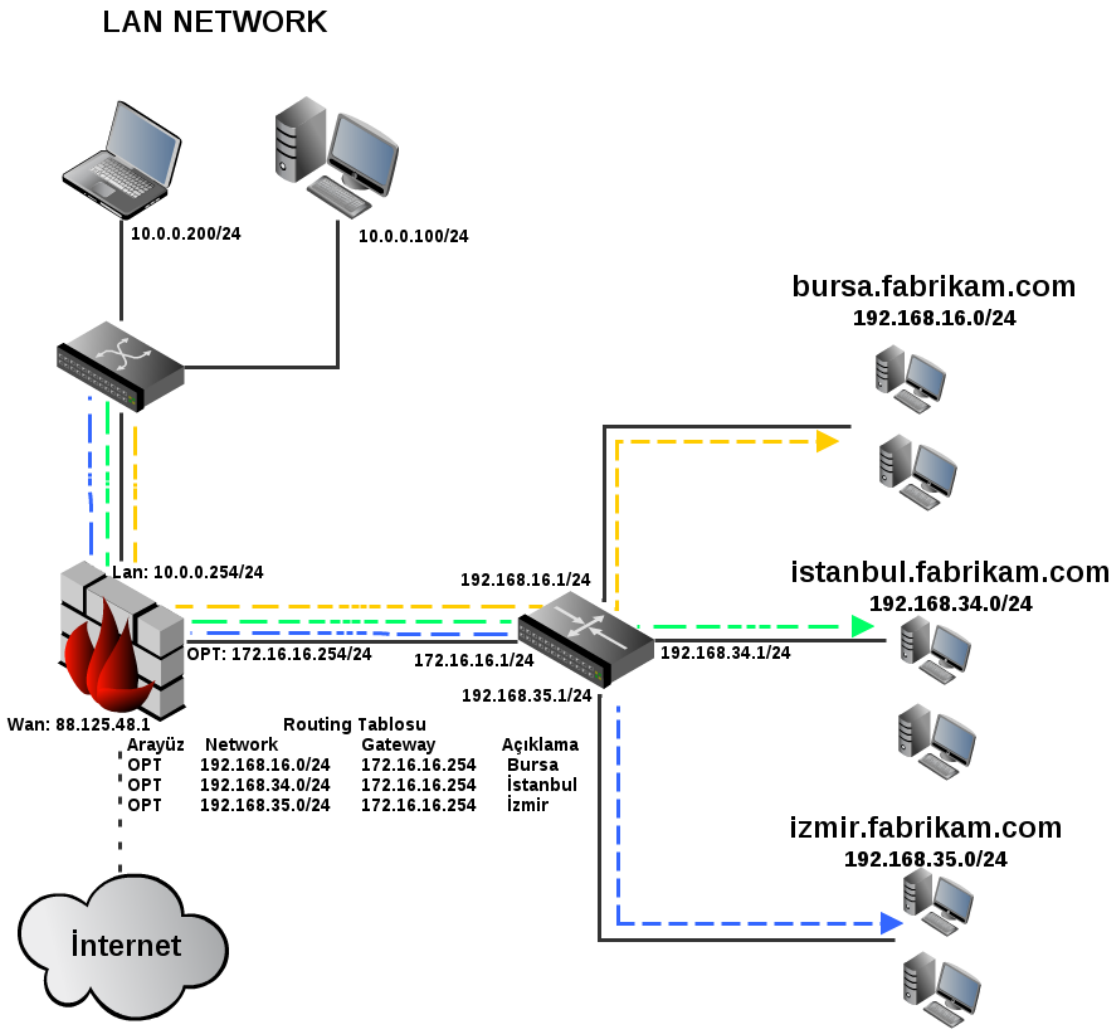
Bölüm 13:
NAT Reflection

Yerel ağda bulunan ip adresleri wan arabirimine ait ip adreslerine bağlanabilsinler !



http://doc.pfsense.org/index.php/Why_can%27t_I_access_forwarded_ports_on_my_WAN_IP_from_my_LAN/OPTx_networks%3F

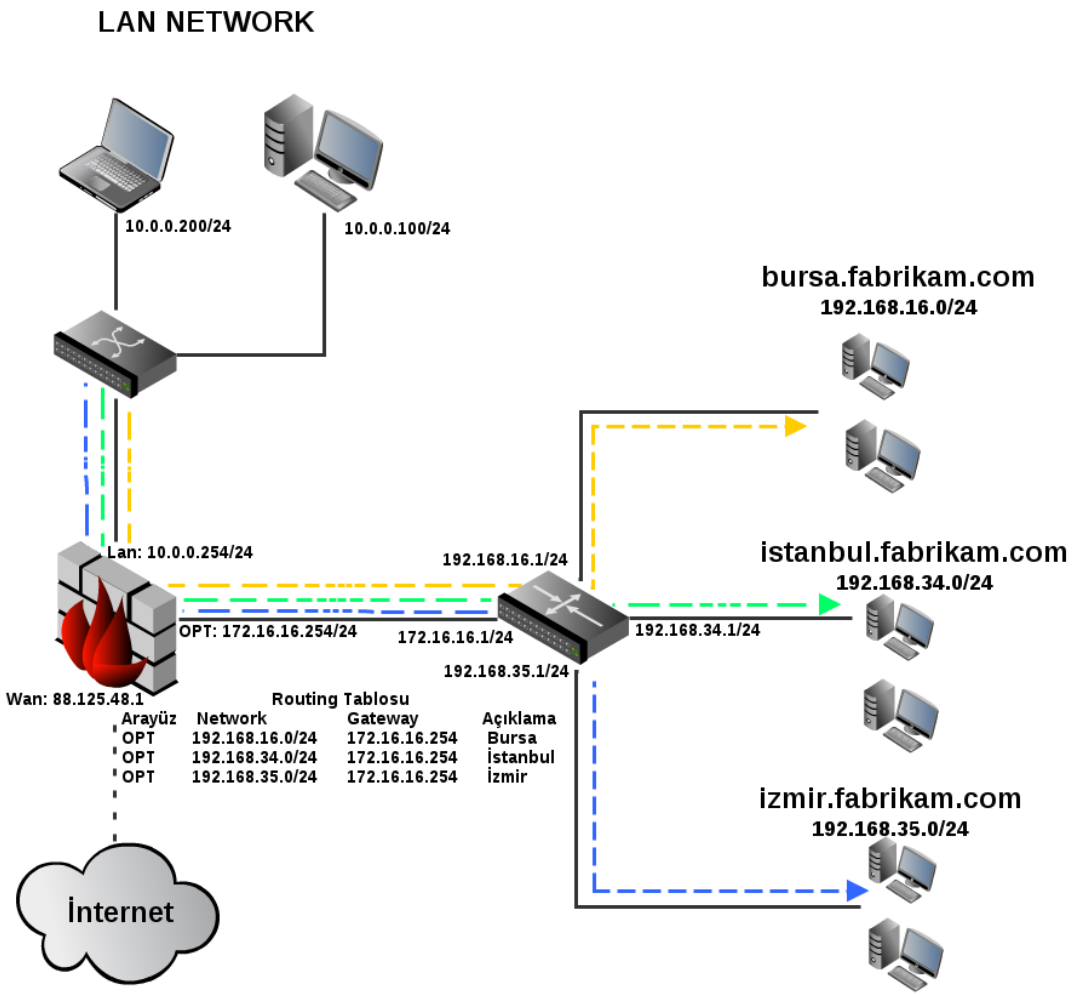
Bölüm 14:
Routing



Bölüm 14:
Routing

pfSense aynı zamanda router olarak hizmet verebilmektedir. Static route, RIP, BGP, OSPF routing protokollerini desteklemektedir.

Bölüm 14:
Routing | Static Route | Uygulama



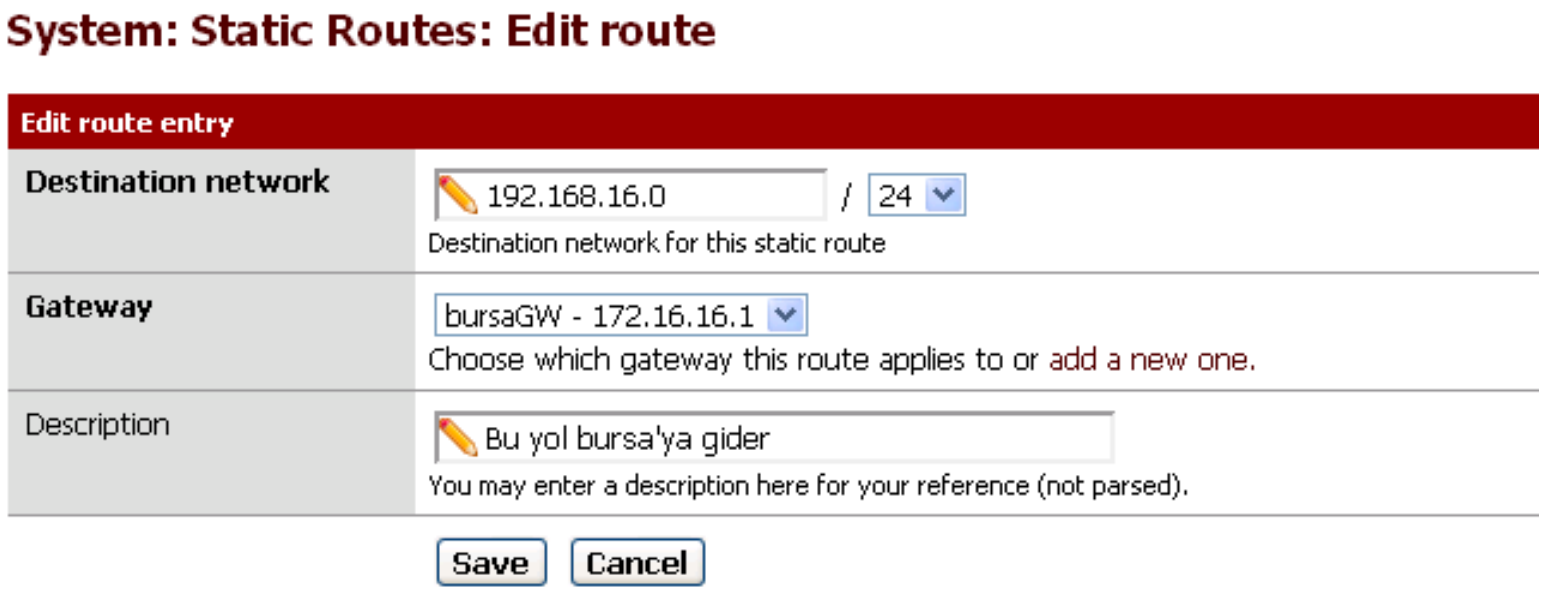
192.168.16.0/24 Bursa ağı, 172.16.16.1 router'ın arkasındadır.

192.168.34.0/24 İstanbul ağına erişmek istiyorsan paketleri 172.16.16.1 router adresine yönlendir.

192.168.35.0/24 İzmir ağını 172.16.16.1 router biliyor, paketler buraya.

Bölüm 14:
Routing | Static Route | Uygulama

192.168.16.0/24 Bursa ağı, 172.16.16.1 router'ın arkasındadır. Bursa'ya erişmek istiyorsan, paketleri bu yönlendiriciye gönder, o seni hedefe ulaştıracak.



Bölüm 14:
Routing | Route Tablosu

Diagnostics: Routing tables

Name resolution ☐ Enable
Enable this to attempt to resolve names when displaying the tables.

Show

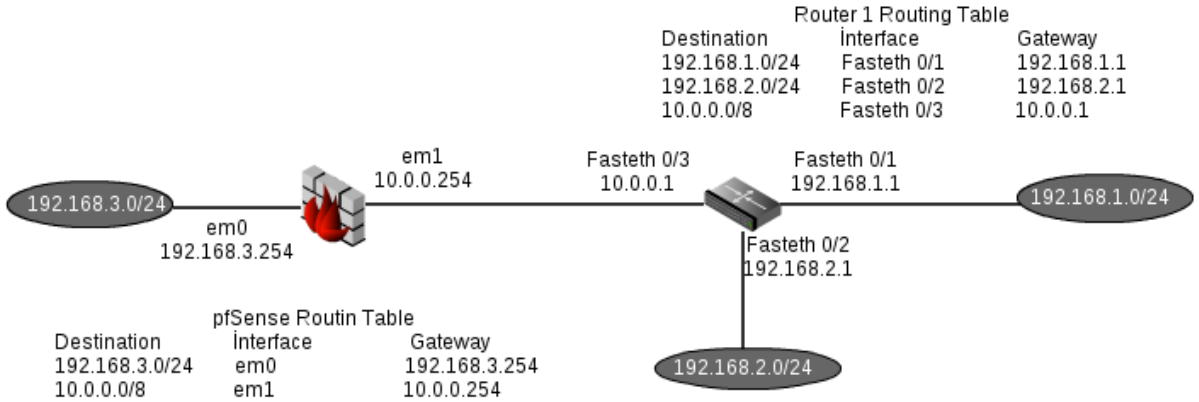
Note: By enabling name resolution, the query should take a bit longer. You can stop it at any time by clicking the Stop button in your browser.

IPv4

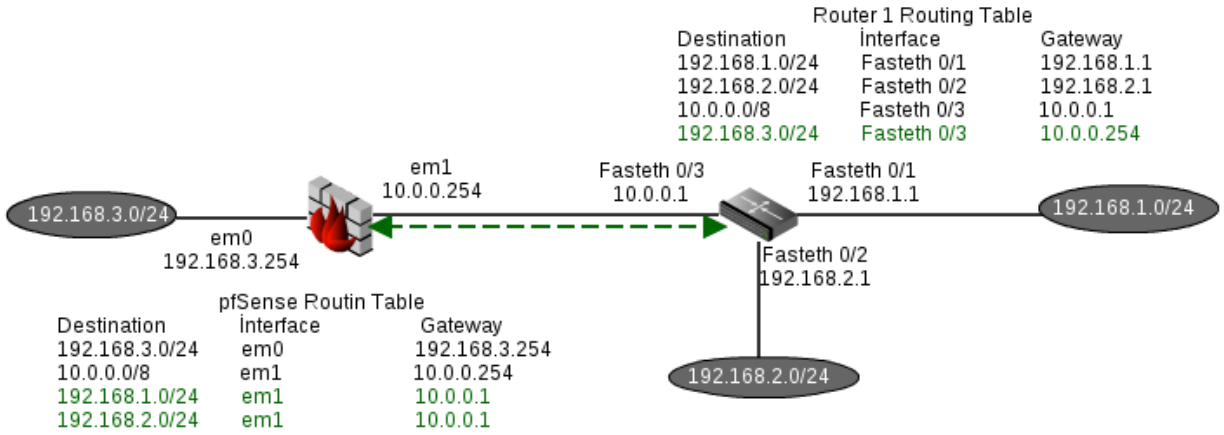
Destination	Gateway	Flags	Refs	Use	Mtu	Netif	Expire
default	172.16.16.1	UGS	0	2943	1500	em2	
6.6.6.0/24	link#2	U	0	7345	1500	em1	
6.6.6.104	link#2	UHS	0	0	16384	lo0	
6.6.6.254	link#9	UH	0	0	1500	vip1	
10.0.0.0/24	link#1	U	0	3261	1500	em0	
10.0.0.1	link#1	UHS	0	1	16384	lo0	
10.0.0.254	link#10	UH	0	0	1500	vip2	
127.0.0.1	link#5	UH	0	189	16384	lo0	
172.16.16.0/24	link#3	U	0	168	1500	em2	
172.16.16.254	link#3	UHS	0	0	16384	lo0	
192.168.16.0/24	172.16.16.1	UGS	0	0	1500	em2	

Bölüm 14:
RIP (Router Information Protokol)

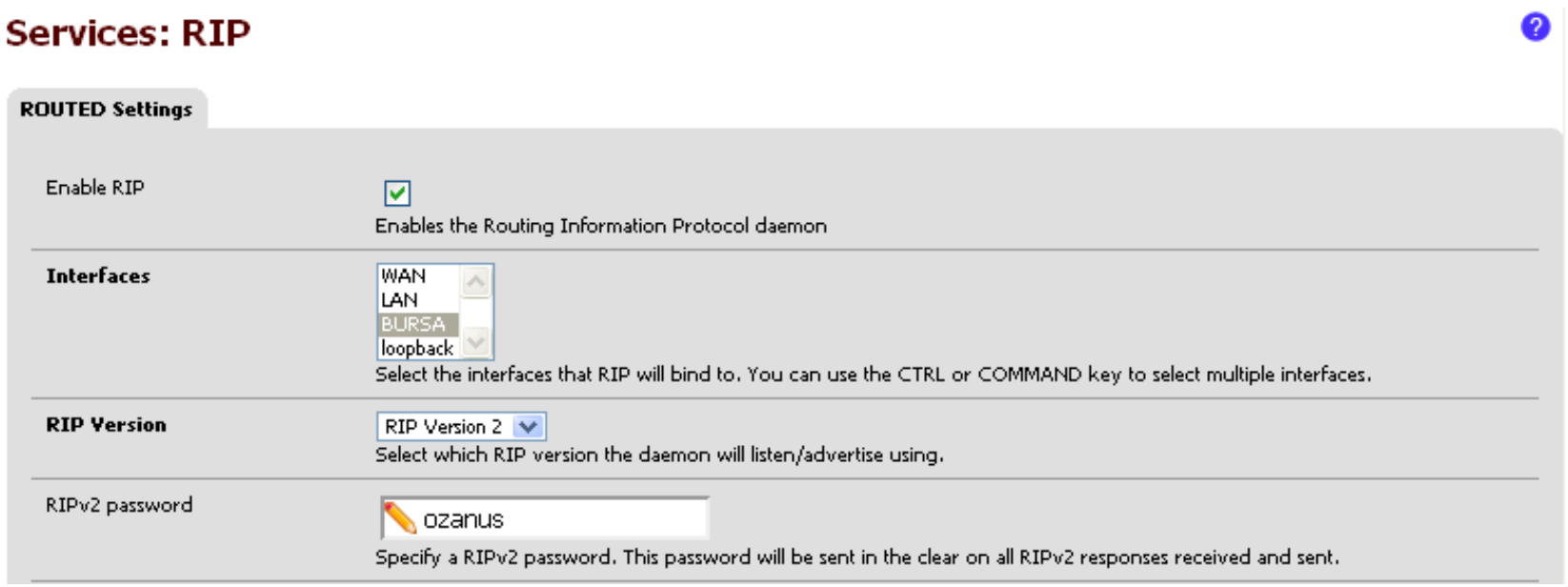
RIP Öncesi



RIP Sonrası

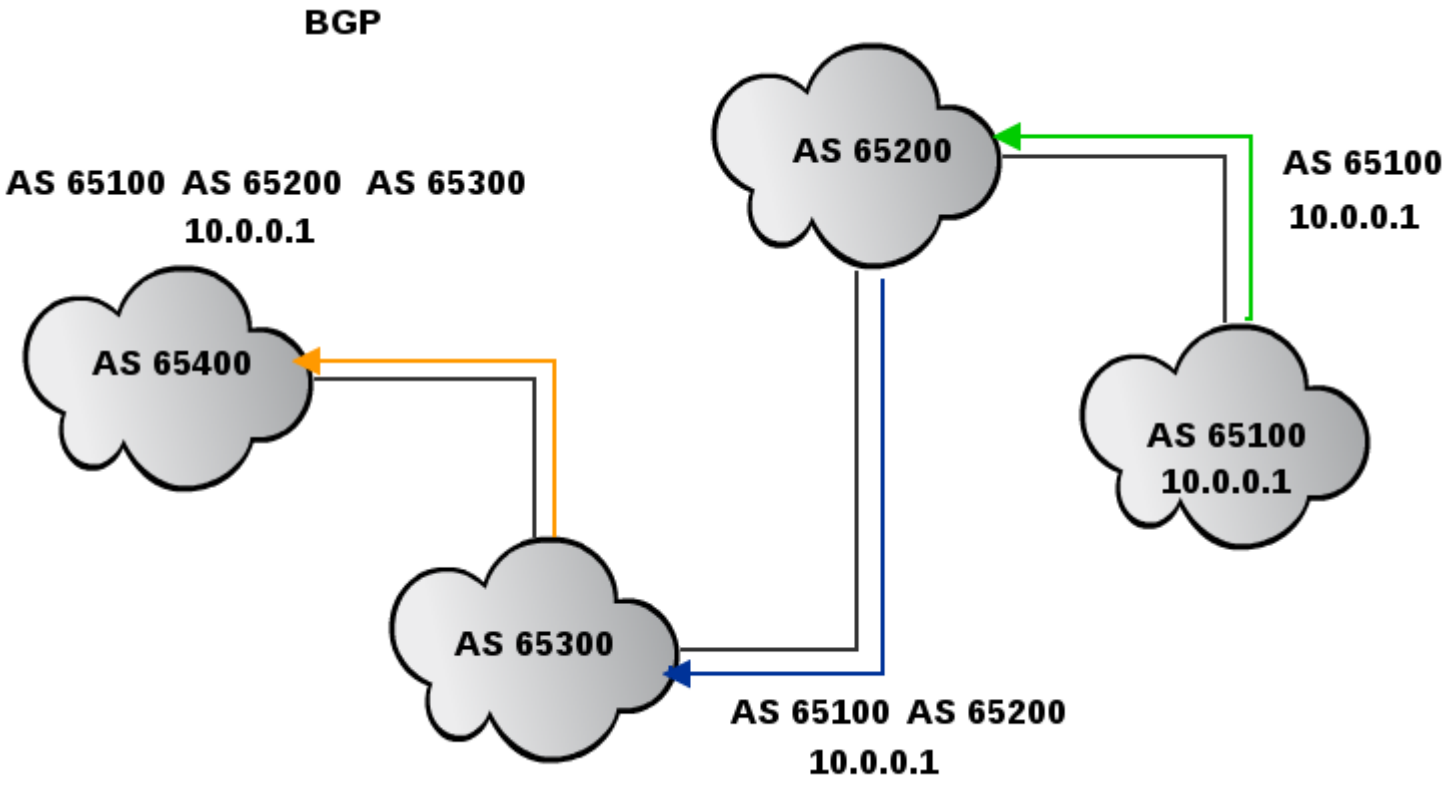


Bölüm 14:
RIP (Router Information Protokol)

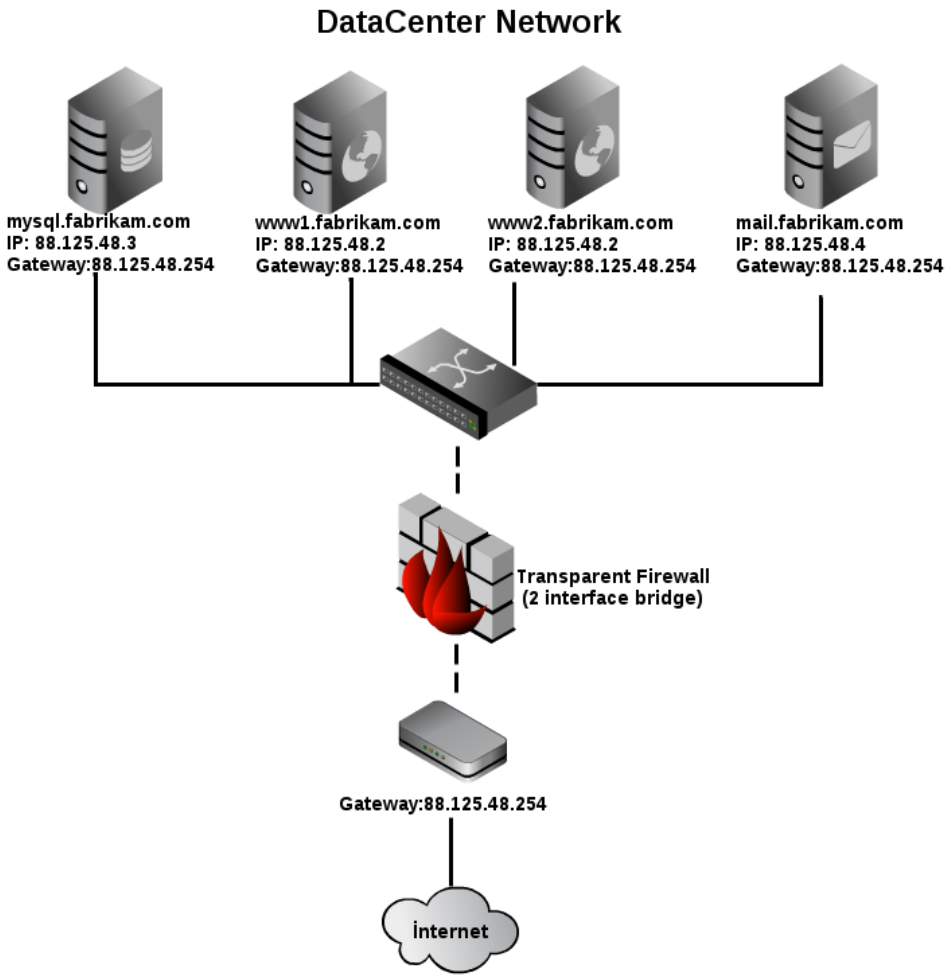


Bölüm 14:
BGP (Border Gateway Protokol)

Hosting ve datacenter ağlarında olmazsa olmazlardandır. Hedefe en kısa varış süresini hesaplar.

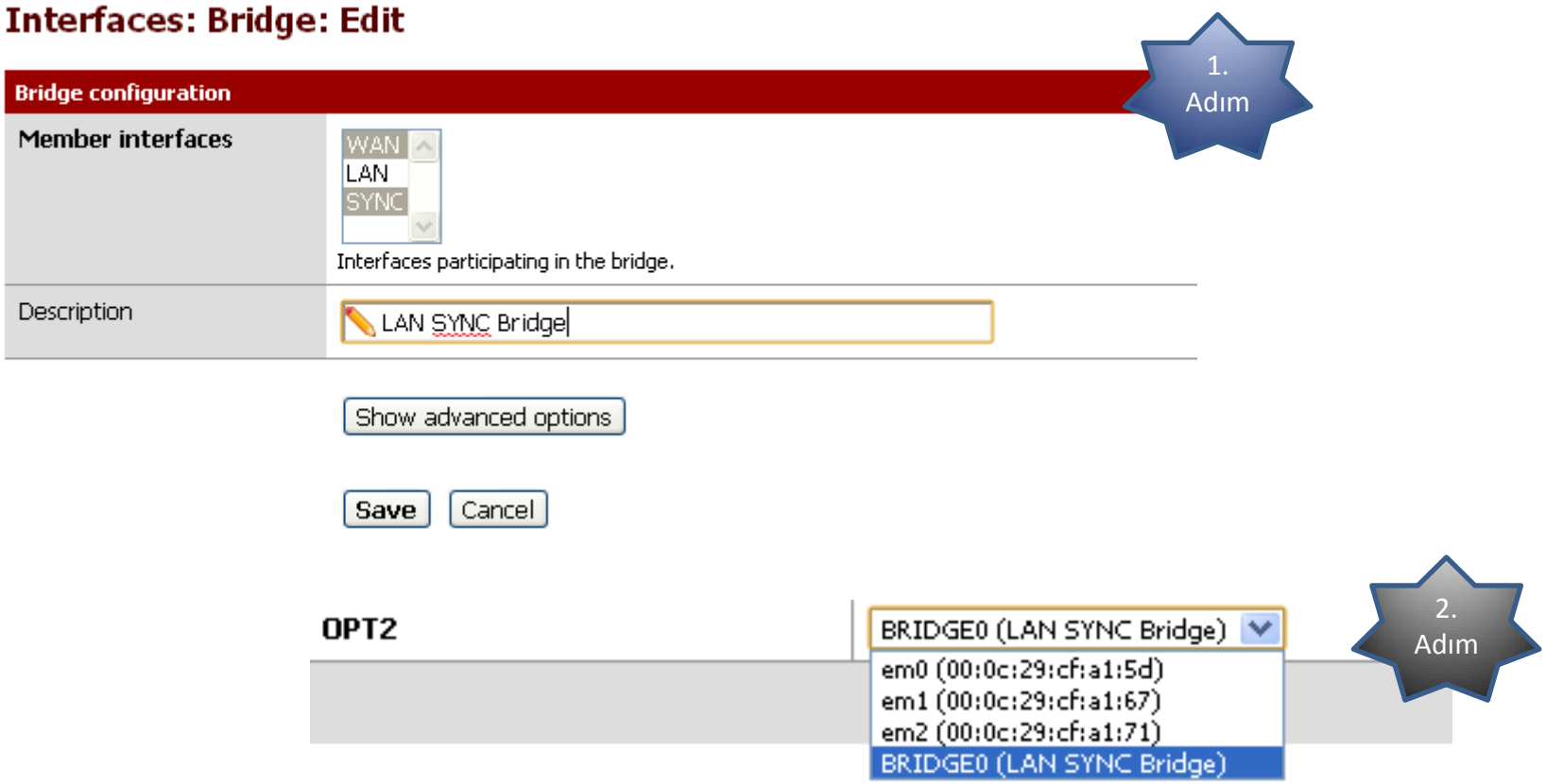


Bölüm 15:
Bridge | Layer 2 Firewall



Bölüm 15:
Bridge | Layer 2 Firewall

İki veya daha fazla ağ arabirimini tek interface olarak Layer 2 network için kullanır.



Bölüm 15:
Bridge | Layer 2 Firewall

Gelişmiş Ayarlar;

- RSTP/STP: Spanning Tree Seçenekleri
  - Protocol
  - STP Interface
  - Valid Time
  - Forward Time
  - Hello Time
  - Priority
  - Hold Count
  - Interface Priority
  - Path Cost
- Cache Size
- Cache Entry Expire Time
- Span Port
- Edge Ports
- Auto Edge Ports
- PTP Ports
- Auto PTP Ports
- Sticky Ports
- Private Ports

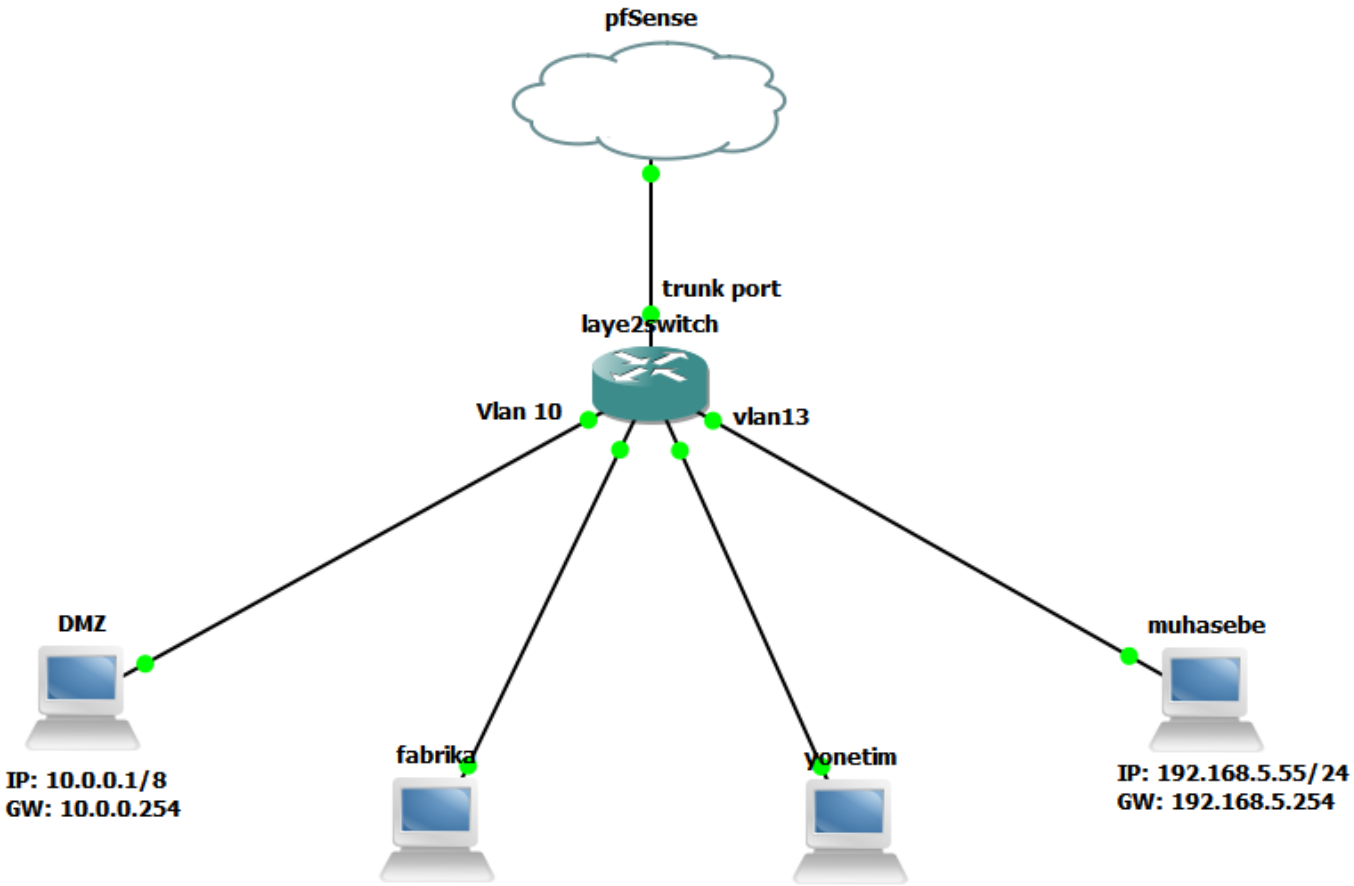
Bölüm 15:
Vlan

Sanal yerel alan ağı (VLAN), bir yerel alan ağı (LAN) üzerindeki ağ kullanıcılarının ve kaynakların mantıksal olarak gruplandırılması ve switch üzerinde port'lara atanmasıyla yapılır. VLAN kullanılmasıyla her VLAN sadece kendi broadcast'ini alacağından, broadcast trafiği azaltılarak bant genişliği artırılmış olur. VLAN tanımlamaları, bulunulan yere, bölüme, kişilere ya da hatta kullanılan uygulamaya ya da protokole göre tanımlanabilir.

VLAN'lar ağ üzerinde uygulanarak, 2. seviye anahtarlamanın getirdiği birçok problem ortadan kaldırılır. Bunları temel olarak 3 başlık altında toplayabiliriz:

1. *Broadcast Kontrol*
2. *Güvenlik*
3. *Esneklik*

Bölüm 15:
Vlan | Uygulama



Bölüm 15:
Vlan| Switch | Vlan Database

Adım 1: Vlan'ların oluşturulması;

laye2switch>**enable**

laye2switch#**vlan database**

laye2switch(vlan)#**vlan 10**

VLAN 10 added:

Name: VLAN0010

laye2switch(vlan)#**vlan 13**

VLAN 13 added:

Name: VLAN0013

laye2switch(vlan)#**vlan 14**

VLAN 14 added:

Name: VLAN0014

laye2switch(vlan)#**exit**

APPLY completed.

Exiting....

Bölüm 15:
Vlan| Switch | Interfaces

Adım 2 : Interfacelerin vlan'lara üye yapılması;

laye2switch#**configure terminal**

laye2switch(config)#**interface FastEthernet 1/0**

laye2switch(config-if)#**switchport access vlan 10**

laye2switch(config-if)#**no shutdown**

laye2switch(config-if)#

***Mar 1 00:09:13.095: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up**

***Mar 1 00:09:14.095: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up**

Bölüm 15:
Vlan|Switch | Vlan Trunk

Adım 3: Trunk port ayarı

laye2switch(config-if)#switchport mode trunk

laye2switch(config-if)#switchport tr

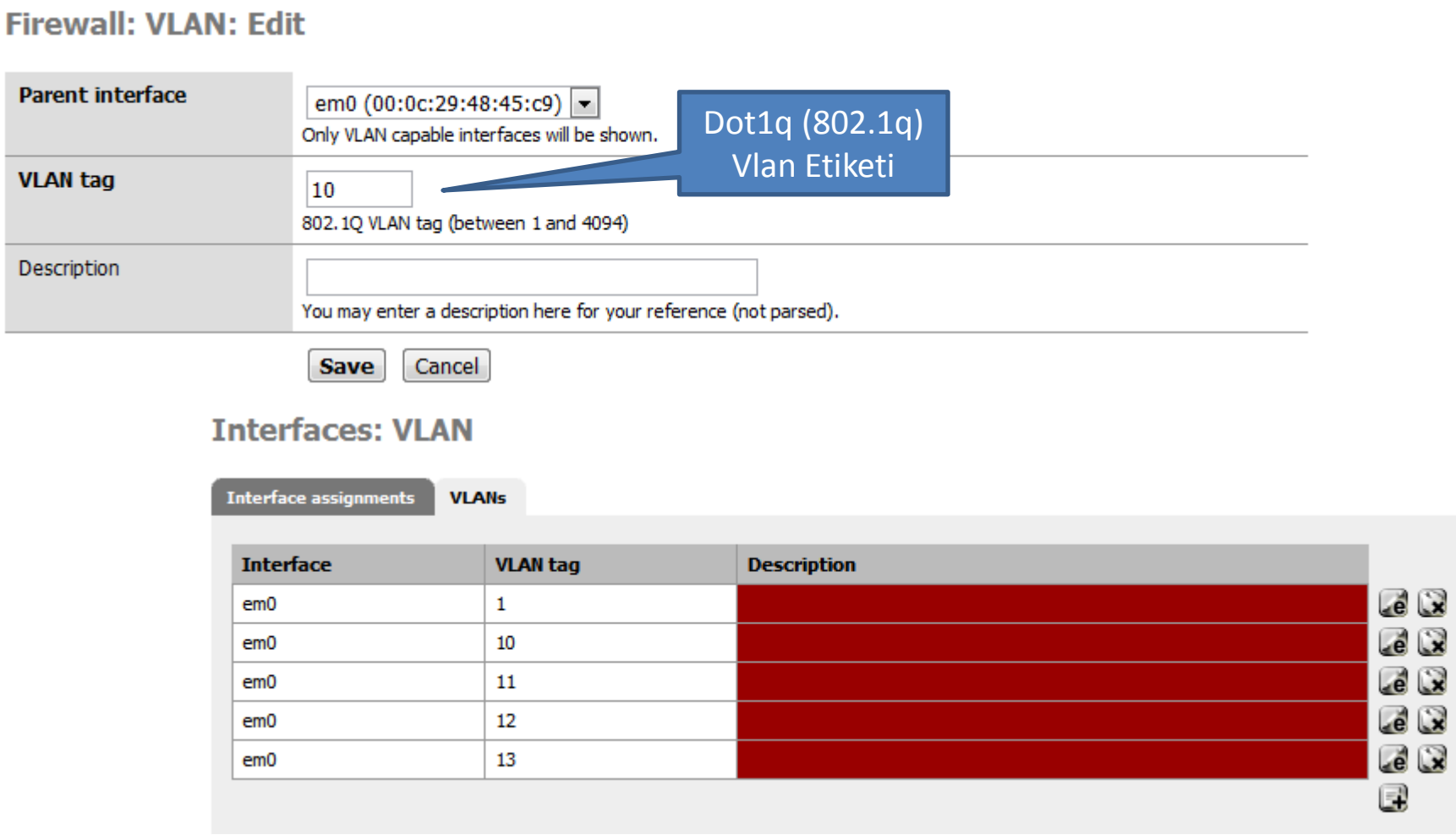
laye2switch(config-if)#switchport trunk enc

laye2switch(config-if)#switchport trunk encapsulation dot1q

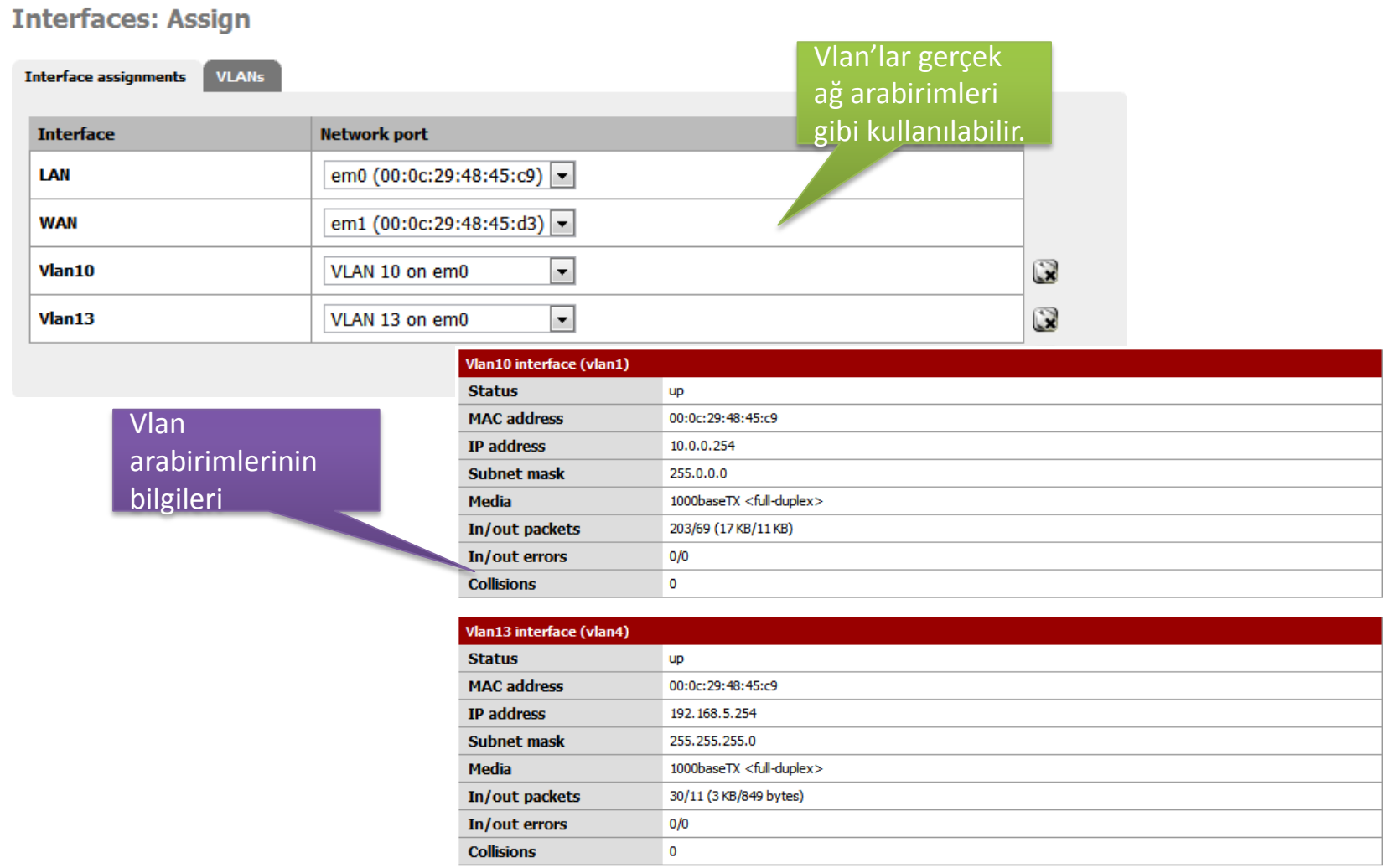
laye2switch(config-if)#no shutdown

*Mar 1 00:14:34.359: %DTP-5-TRUNKPORTON: Port Fa1/10 has become dot1q trunk

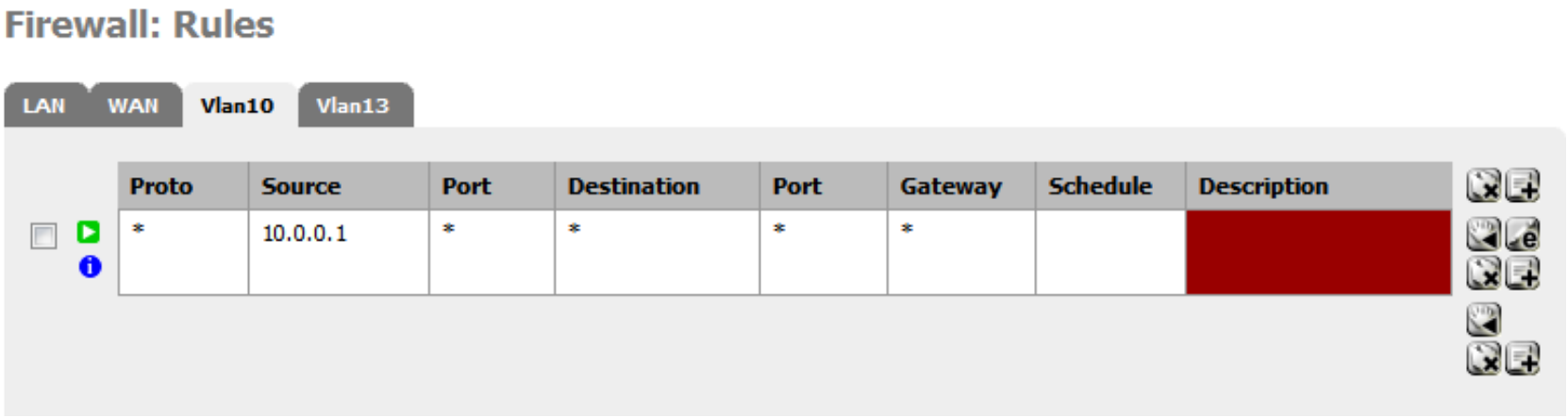
Bölüm 15:
pfSense Vlan Yapılandırması



Bölüm 15:
pfSense Vlan Yapılandırması



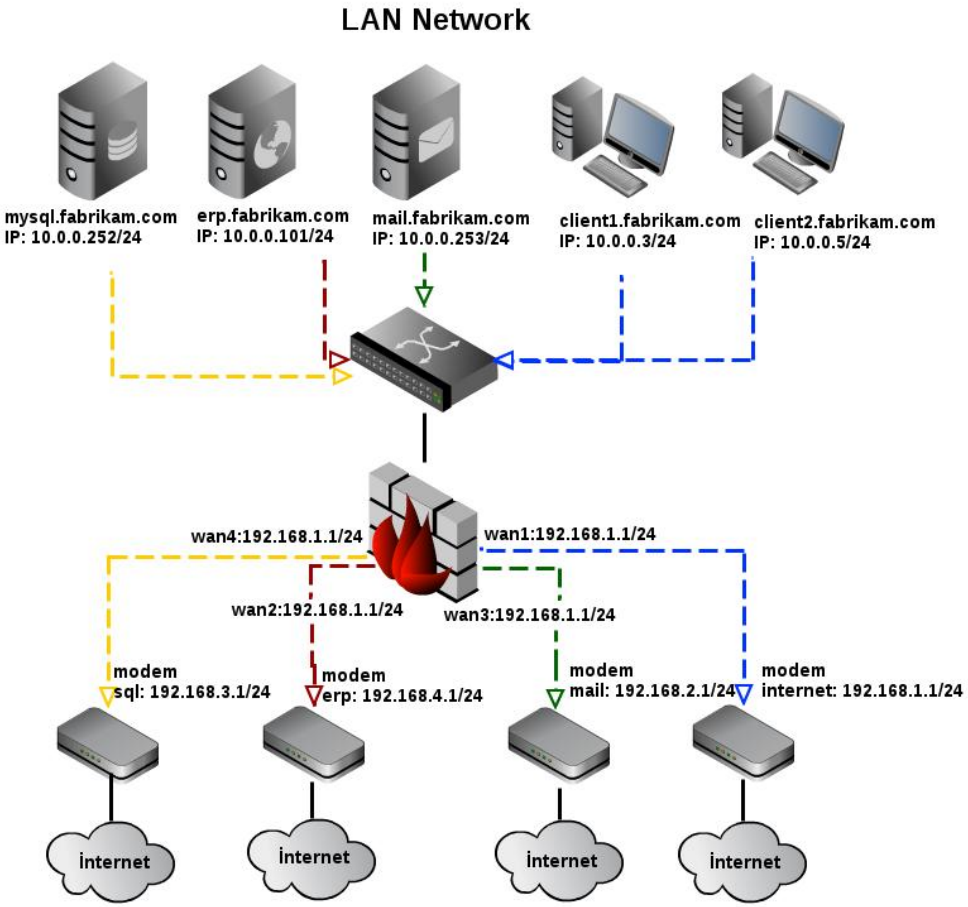
Bölüm 15:
pfSense Vlan Firewall Kuralları



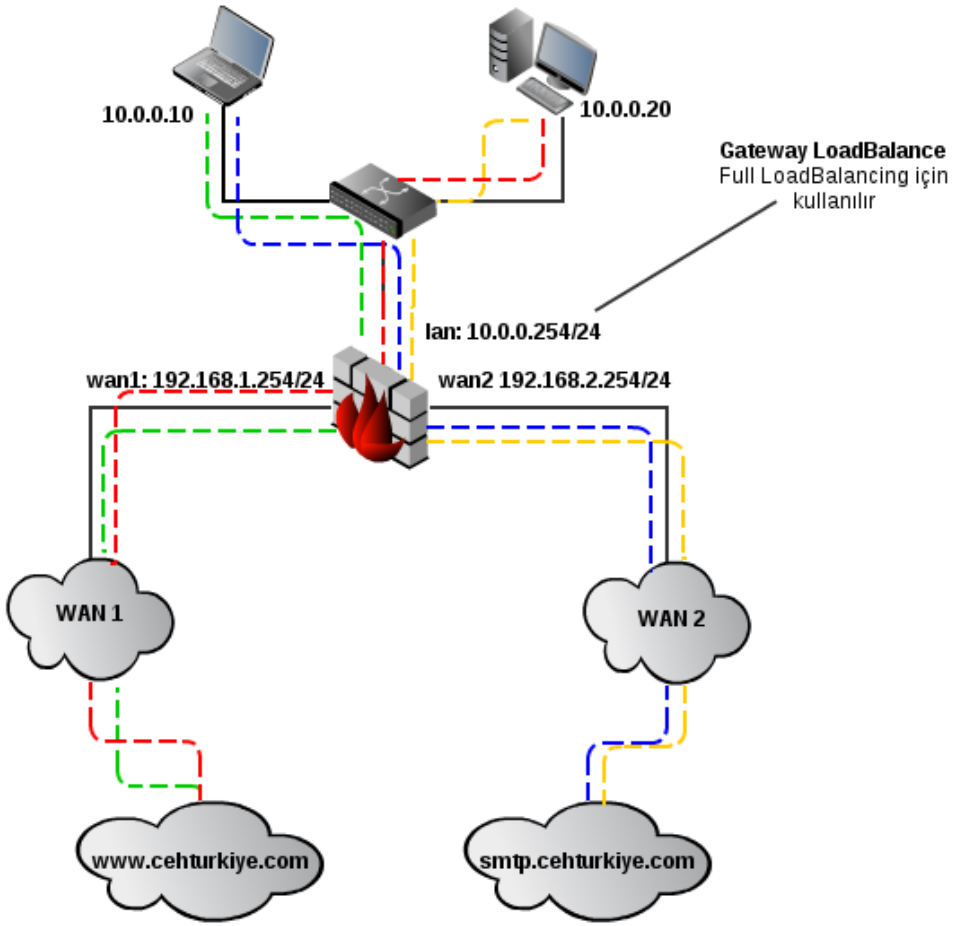
Bölüm 16:
Multiple WAN

- Multiwan ve Nat
- Policy Based Routing
- Load Balancing
- Failover
- Incoming Server Load Balancing
- Policy Routing,Load Balancing ve Failover stratejileri
- Sorun Giderme

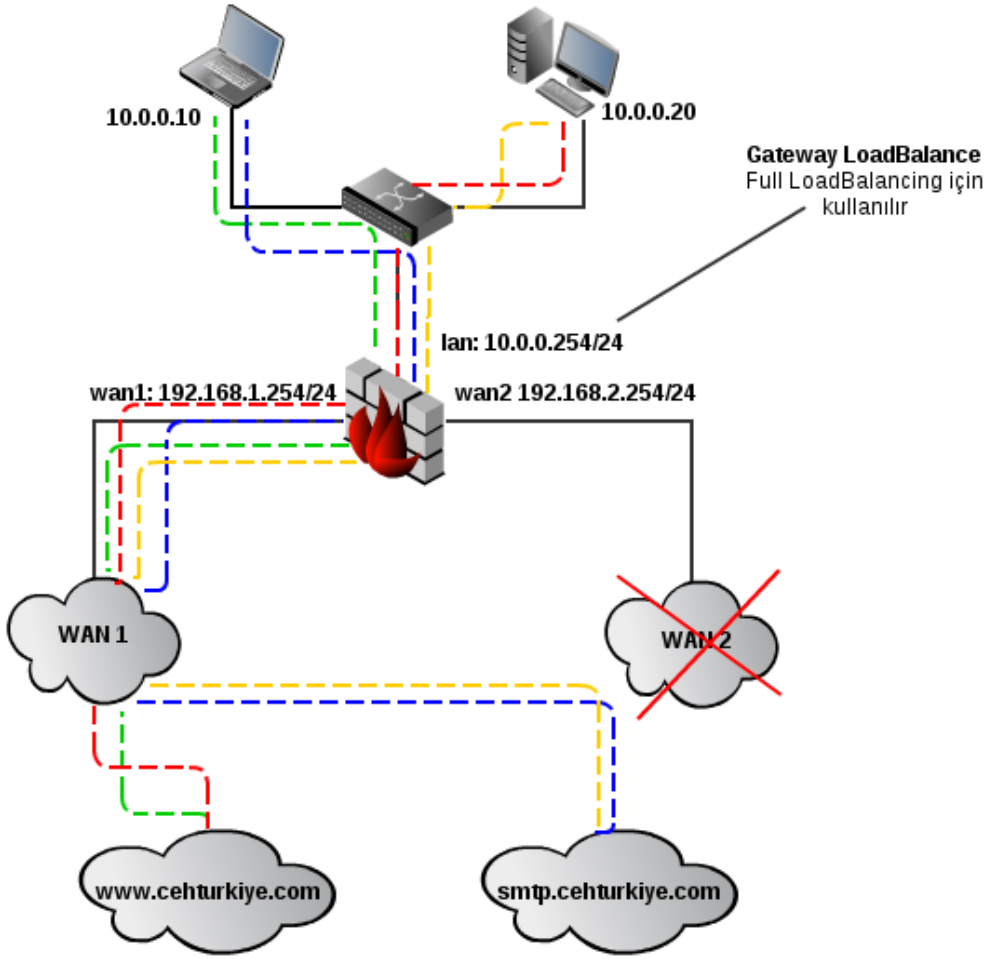
Bölüm 16:
Multiple WAN | Policy Based Routing



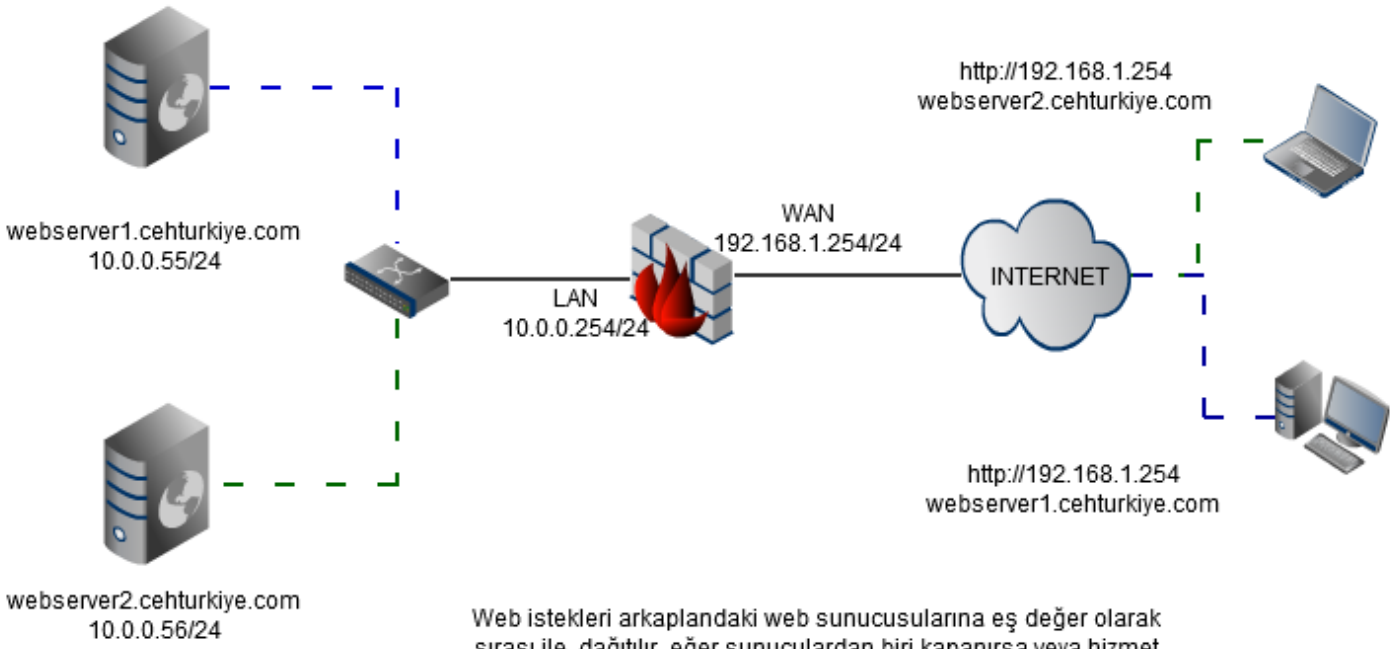
Bölüm 16:
Multiple WAN | Load Balancing



Bölüm 16:
Multiple WAN | Failover

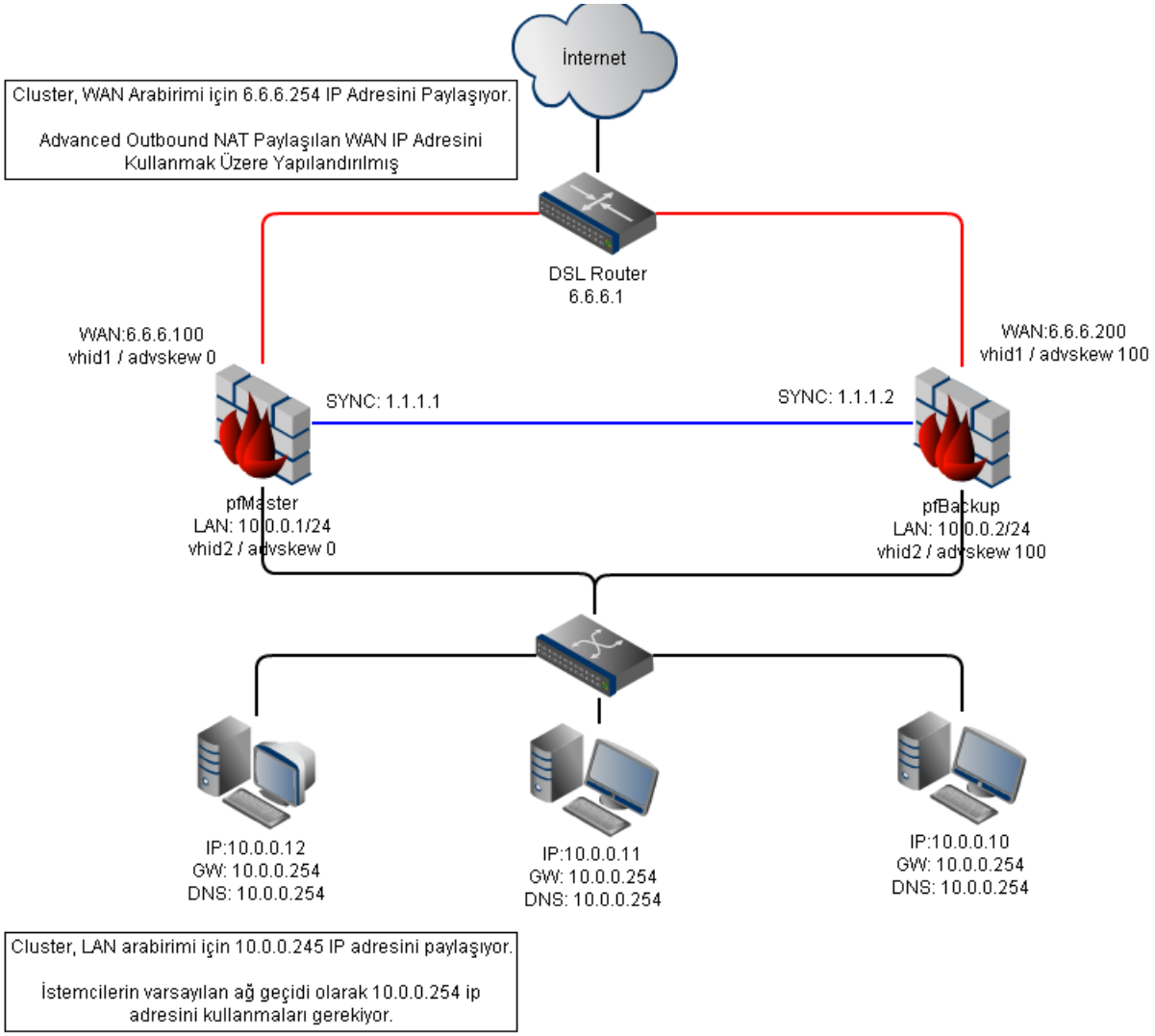


Bölüm 17:
Incoming Server Load Balancing



Web istekleri arkaplandaki web sunucusularına eş değer olarak sırası ile dağıtılır, eğer sunuculardan biri kapanırsa veya hizmet dışı kalırsa, tüm istekler ayakta kalan diğer sunucuya aktarılır.

Bölüm 18:
CARP (Cluster ARP), Redundancy Firewall, pfsync



Bölüm 18:
CARP (Cluster ARP), Redundancy Firewall, pfsync

1. Ağ arabirimleri tanımlanır
2. SYNC ağ arabirimi için tüm trafiğe izin veren firewall kuralı yazılır.
3. pfMaster : Firewall > Virtual Ips
4. pfMaster : Firewall > CARP Settings
5. Status > CARP
6. Test !

Bölüm 19:
VPN (Virtual Private Network)

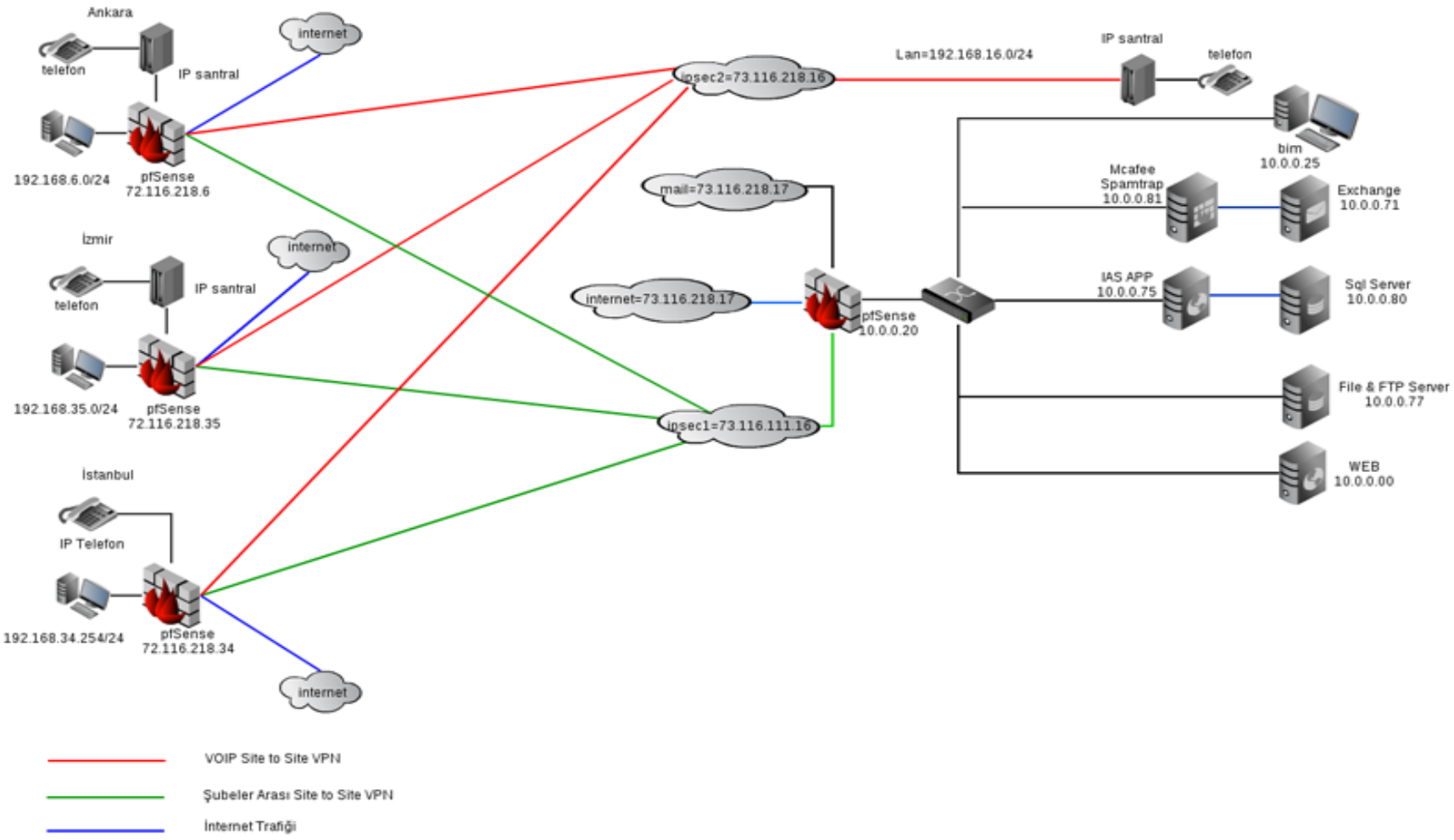
Özel sanal ağlar oluşturmak için kullanılır.
Farklı vpn türleri vardır; PPTP, L2TP, IPSEC vb.

IPSEC
UDP Port 500
ESP/AH protokollerini kullanır

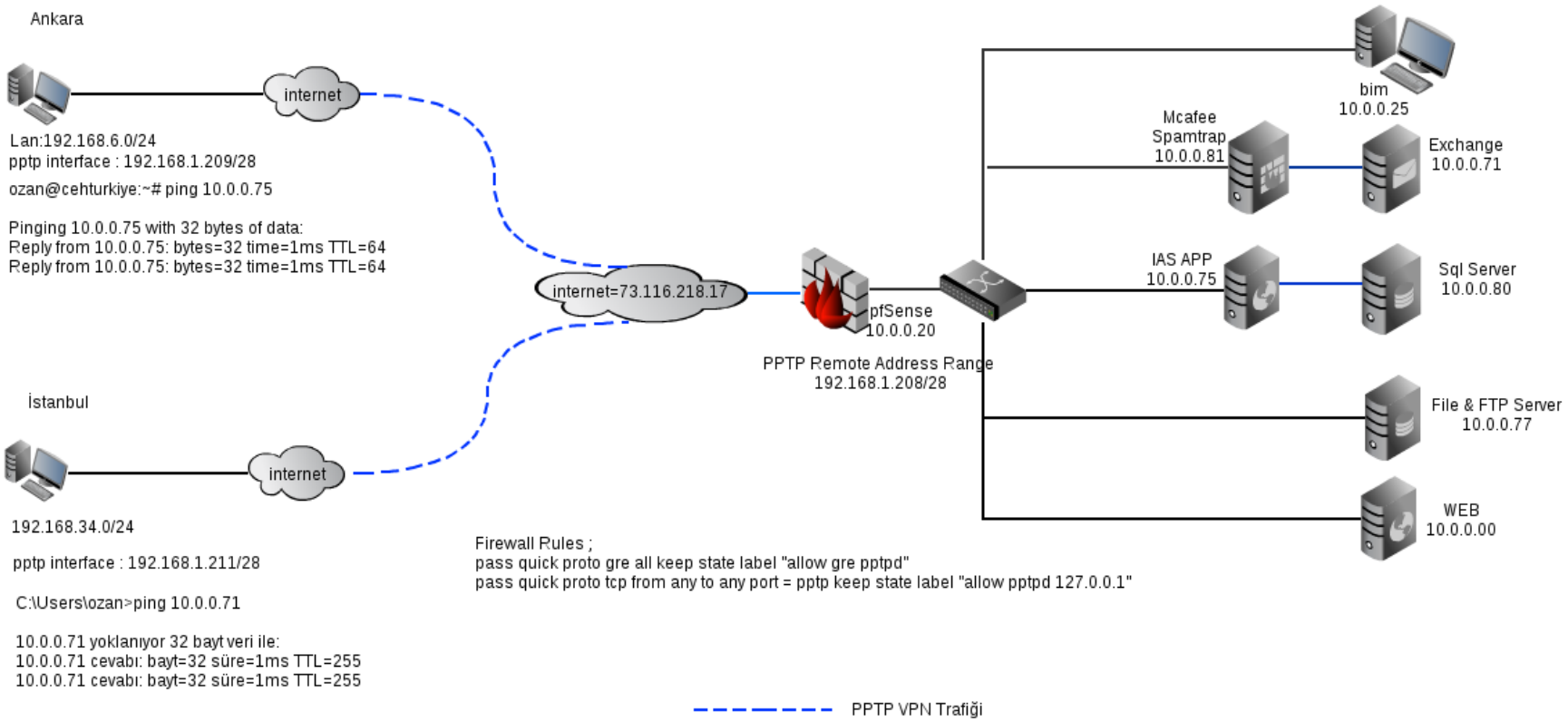
PPTP
TCP Port 1723
GRE protokolünü kullanır
Radius Auth. Destekler

OpenVPN
TCP Port 1194

Bölüm 19:
VPN | IPSEC (site2site)



Bölüm 19:
VPN | PPTP (Client2site)



Bölüm 20:
Traffic Shaper

pfsense tarafından Qos yönetimi için AltQ framework'ü kullanılıyor.

AltQ kaynak paylaşımı ve QoS kontrolü için başka mekanizmaların kullanılmasına olanak verir.

AltQ da kullanılabilir trafik zamanlayıcılar;

- Class Based Queuing (CBQ) : Sınıf tabanlı sıralama
- Priority Queuing (PRIQ): Önceliğe göre sıralama
- Hierarchical Fair Services Curve (HFSC): Yapısal adil hizmet eğrisi

AltQ sağladığı bu trafik zamanlayıcılar bir trafik biçimlendirme sihirbazı ile otomatik olarak yapılandırılabilir.

Bölüm 20:
Traffic Shaper

pfSense 2.0 ile birlikte gelen bir diğer QoS mekanizmasıda **Dummynet**'dir.

Dummynet, ipfw firewall'un bir parçasıdır ama artık pf firewall'da da kullanılabilir.

Aslen ağ protokollerini analiz için tasarlanmış olasada, günümüzde band genişliğini yönetmek içinde kullanılmaktadır.

Bölüm 20:
Traffic Shaper

Kısıtlamalar

pfSense 1.2.x sürümlerinde birden fazla WAN veya LAN için filtreleme yapılamaz.

Sihirbaz

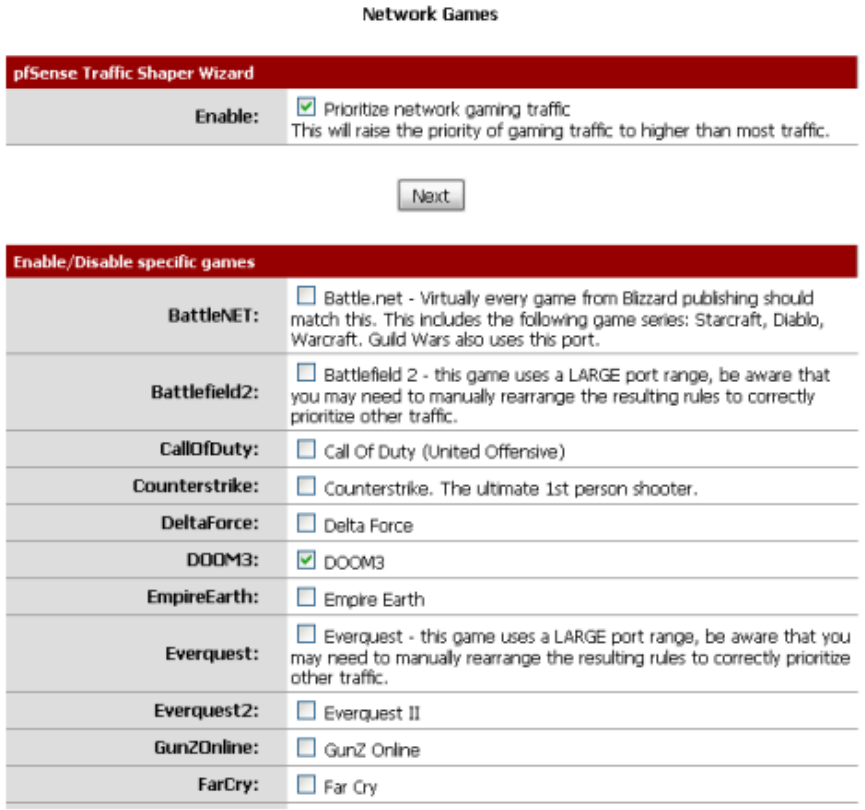
Traffic Shaper sihirbaz profilleri;

Single Lan multi Wan

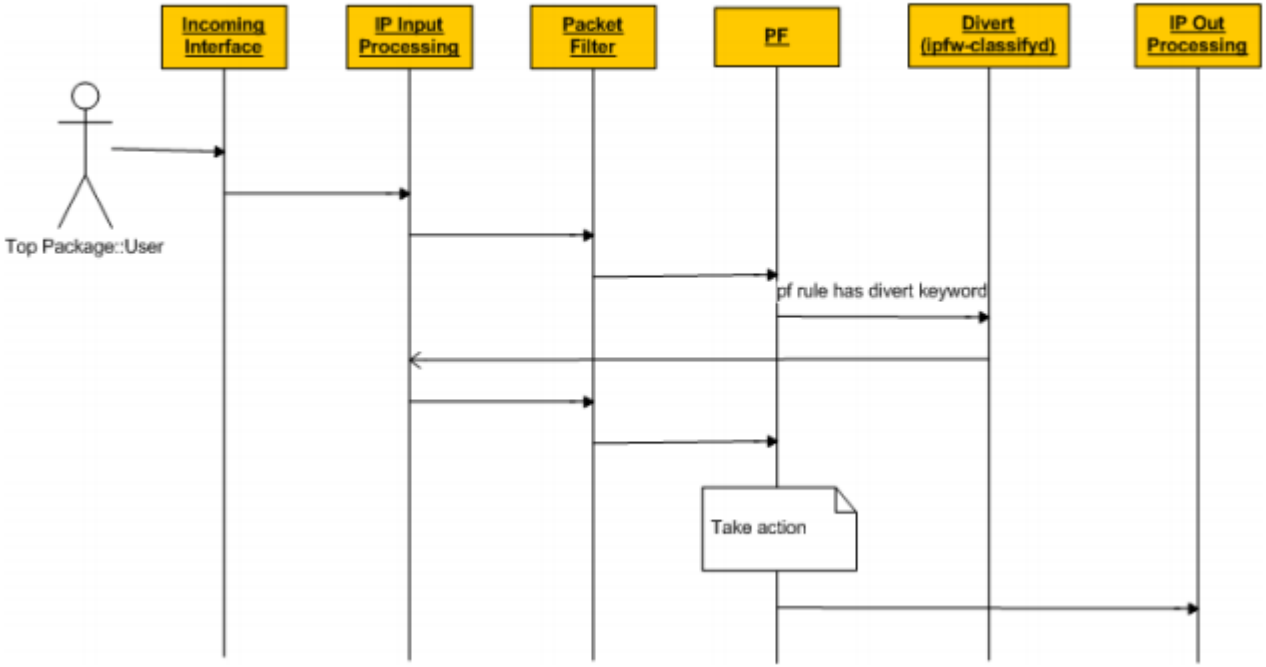
Single Wan multi Lan

Multiple Lan/Wan

Dedicated Links

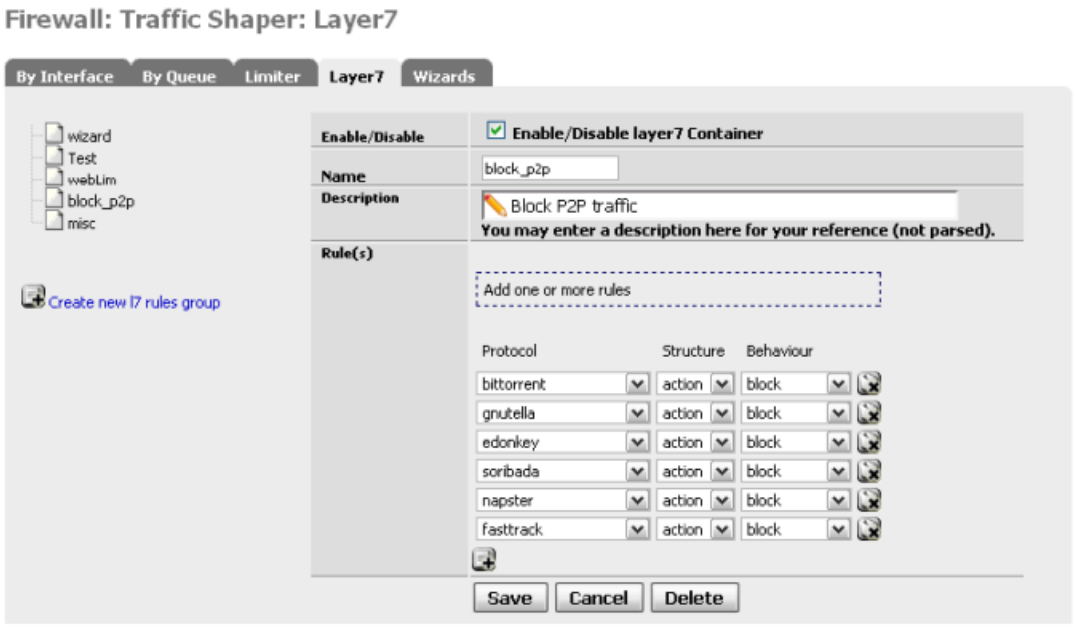


Bölüm 20:
Traffic Shaper

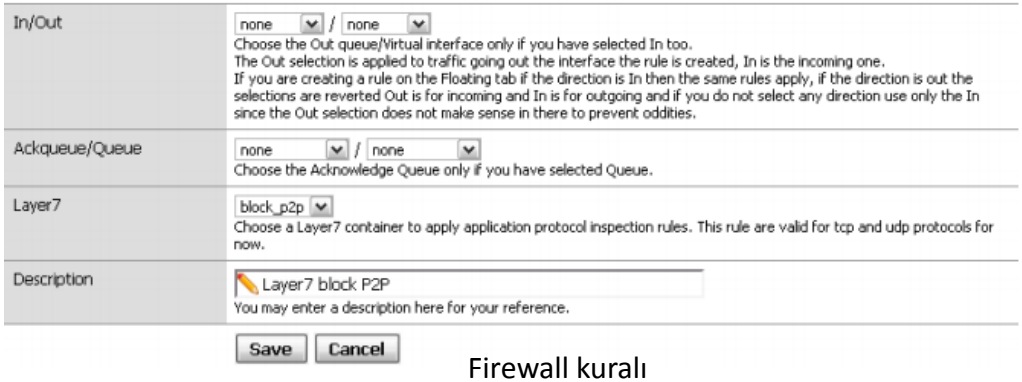


IP paketi ipfw-classifyd ye giriş-çıkış yaparken

Bölüm 20:
Traffic Shaper



Layer7 grafik arabirimi



Firewall kuralı

Bölüm 20:
Traffic Shaper

Bridge Firewall da Layer7 filtreleme için şu system ayarlarının aktif edilmesi gerekir;

net.link.bridge.pfil_member = 0

net.link.bridge.pfil_bridge = 1

Bölüm 20:
Captive Portal | Kimlik Doğrulamalı Ağ Geçidi

Bölüm 21:
Captive Portal

Genel Özellikler

Maksimum Eş Zamanlı Bağlantı

Boş Zaman Aşımı

Sabit Zaman Aşımı

Logout Popup Penceresi

Yönlendirme Adresi

Eş Zamanlı Kullanıcı Girişi

Mac Filtreleme

IP Filtreleme

Kimlik Doğrulama

- Tanımsız
- Yerel
- Radius Destekli Auth.

Bölüm 21:
Captive Portal

Genel Özellikler

Voucher Desteği

Mac Adresine Göre Trafik Limitleme

IP Adresine Göre Trafik Limitleme

Host Adına Göre Yetkilendirme

Özelleştirilebilir Giriş/Hata ve Çıkış Pencereleri

Bölüm 21:
Captive Portal | Özelleştirme

Karşılama Sayfası;

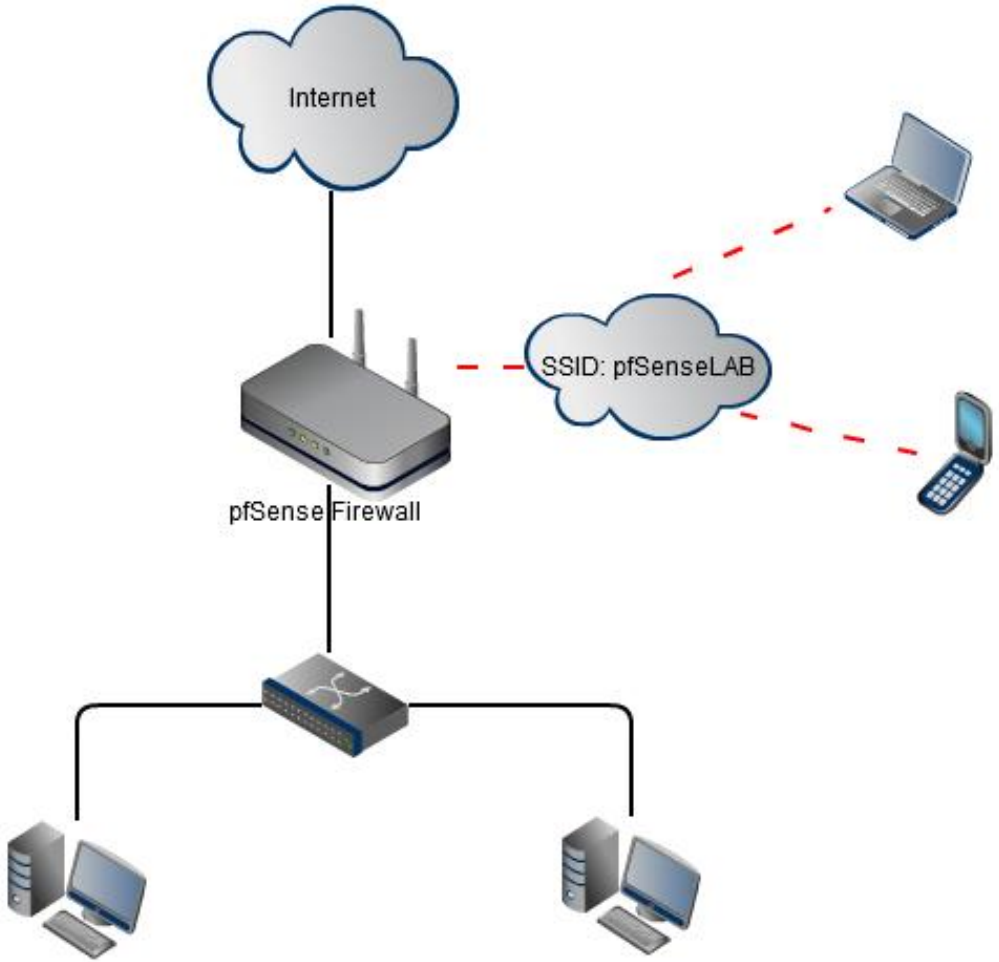
```
<html>
<head>
<title>pfSense captive portal</title>
</head>
<body>
<center>
<h2>pfSense captive portal</h2>
<p>
<form method="post" action="$PORTAL_ACTION$">
<input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
<table>
  <tr><td>Username:</td><td><input name="auth_user" type="text"></td></tr>
  <tr><td>Password:</td><td><input name="auth_pass" type="password"></td></tr>
  <tr><td> </td></tr>
  <tr>
    <td colspan="2">
      <center><input name="accept" type="submit" value="Continue"></center>
    </td>
  </tr>
</table>
</center>
</form>
</body>
</html>
```

Bölüm 21:
Captive Portal | Özelleştirme

Hata Sayfası;

```
<html>
<head>
<title>Authentication error</title>
</head>
<body>
<font color="#cc0000"><h2>Authentication error</h2></font>
<b>
Username and/or password invalid.
<br><br>
<a href="javascript:history.back()">Go back</a>
</b>
</body>
</html>
```

Bölüm 21:
Captive Portal | Güvenli Hotspot Ağı



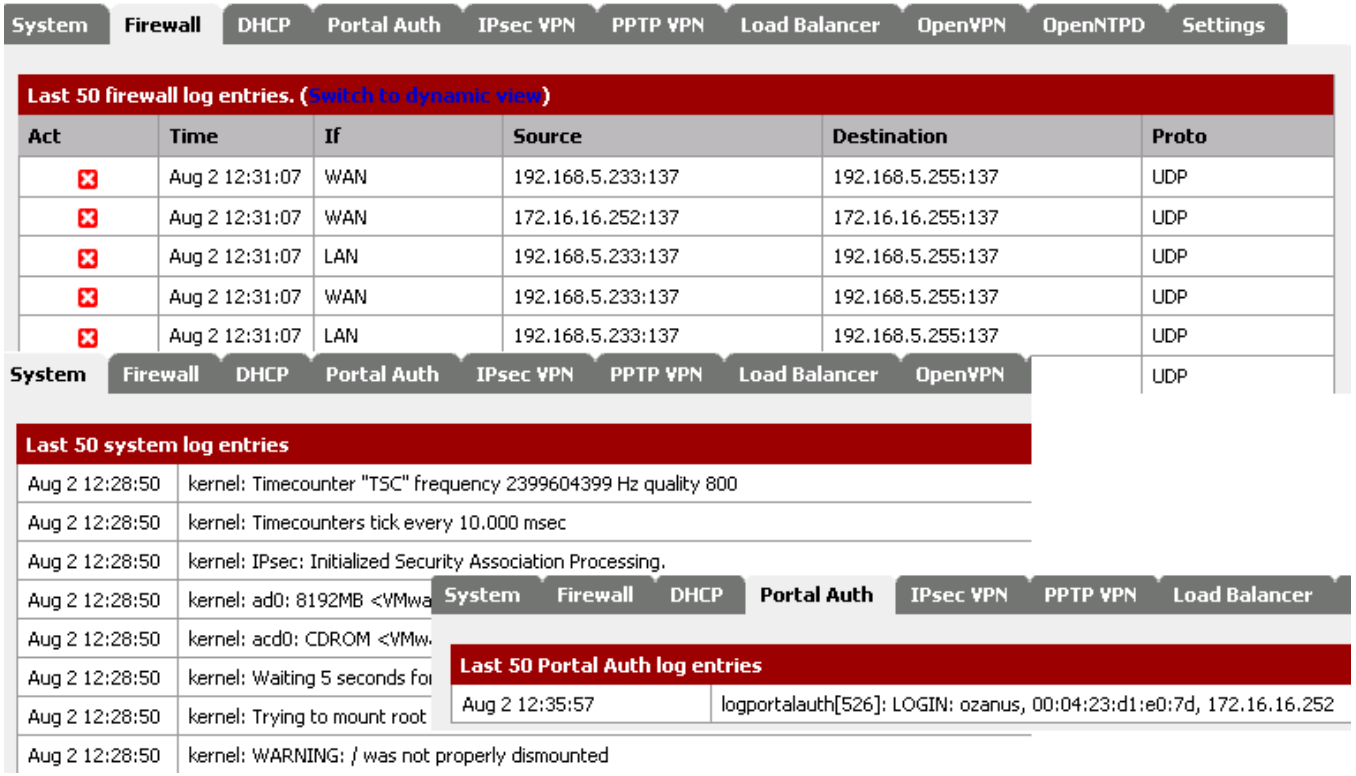
Bölüm 22:
Sistem Monitor

Sistem monitor araçları “Status“ menüsü altında bulunur. Görüntüleyeceğimiz ve izleyeceğimiz bilgiler;

- Sistem Kayıtları
- Ağ Arabirimi Durumları
- Servis Durumları
- RRD Grafikleri
- Firewall Durum Tablosu
- Sistem Kayıtlarını Uzak SyslogD yazdırmak

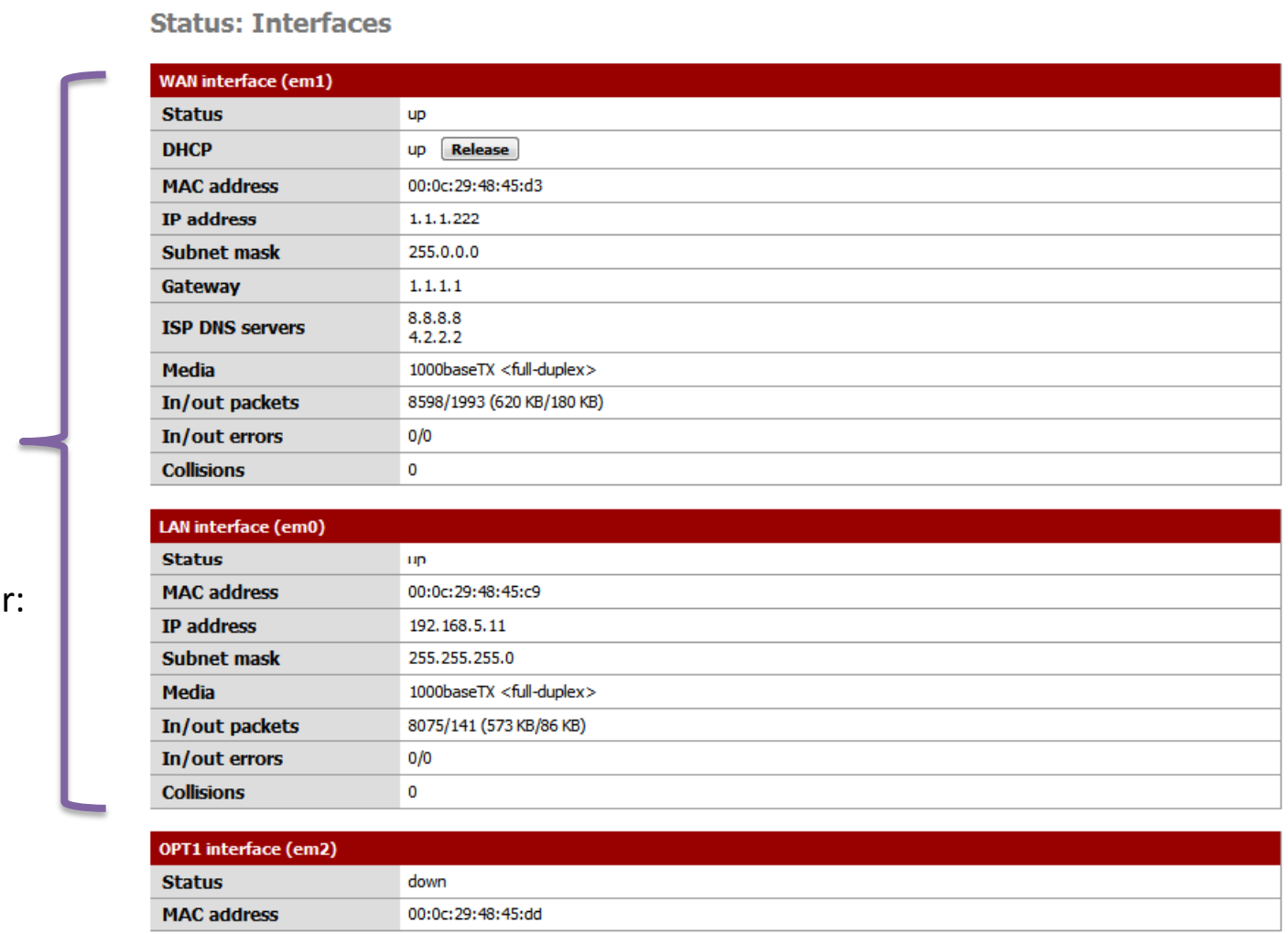
Bölüm 22:
Sistem Monitor | Sistem Kayıtları

pfSense servisleri tarafından oluşturulan kayıtlar, birşeyler düzgün çalışmıyorsa,bir hata durumunda ve/veya sistem aktivitelerini öğrenmek için ziyaret edeceğimiz ilk başvuru kaynaklarından biridir. Uyarı, bilgi ve hata mesajlarına ait kayıtlar bu sayfada yer alır.



Bölüm 22:
Sistem Monitor | Ağ Arabirimi Durumları

Wan Arabirimi Adı
Durum :
IP atama türü:
Mac Adres:
IP Adres:
Alt Ağ Maskesi:
Ağ Geçidi:
DNS Sunucular:
Ethernet Durumu:
Gelen/Giden Paketler:
Giriş/Çıkış Hataları:
Çarpışmalar:



Status: Interfaces

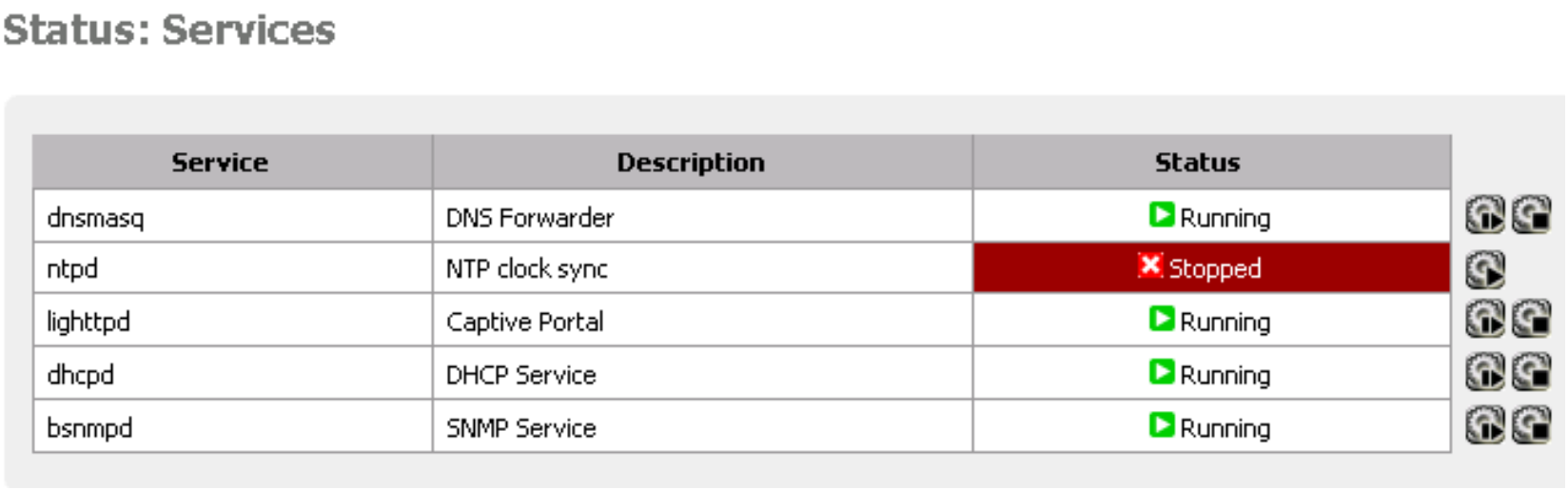
WAN interface (em1)	
Status	up
DHCP	up Release
MAC address	00:0c:29:48:45:d3
IP address	1.1.1.222
Subnet mask	255.0.0.0
Gateway	1.1.1.1
ISP DNS servers	8.8.8.8 4.2.2.2
Media	1000baseTX <full-duplex>
In/out packets	8598/1993 (620 KB/180 KB)
In/out errors	0/0
Collisions	0

LAN interface (em0)	
Status	up
MAC address	00:0c:29:48:45:c9
IP address	192.168.5.11
Subnet mask	255.255.255.0
Media	1000baseTX <full-duplex>
In/out packets	8075/141 (573 KB/86 KB)
In/out errors	0/0
Collisions	0

OPT1 interface (em2)	
Status	down
MAC address	00:0c:29:48:45:dd

Bölüm 22:
Sistem Monitor | Servis Durumları

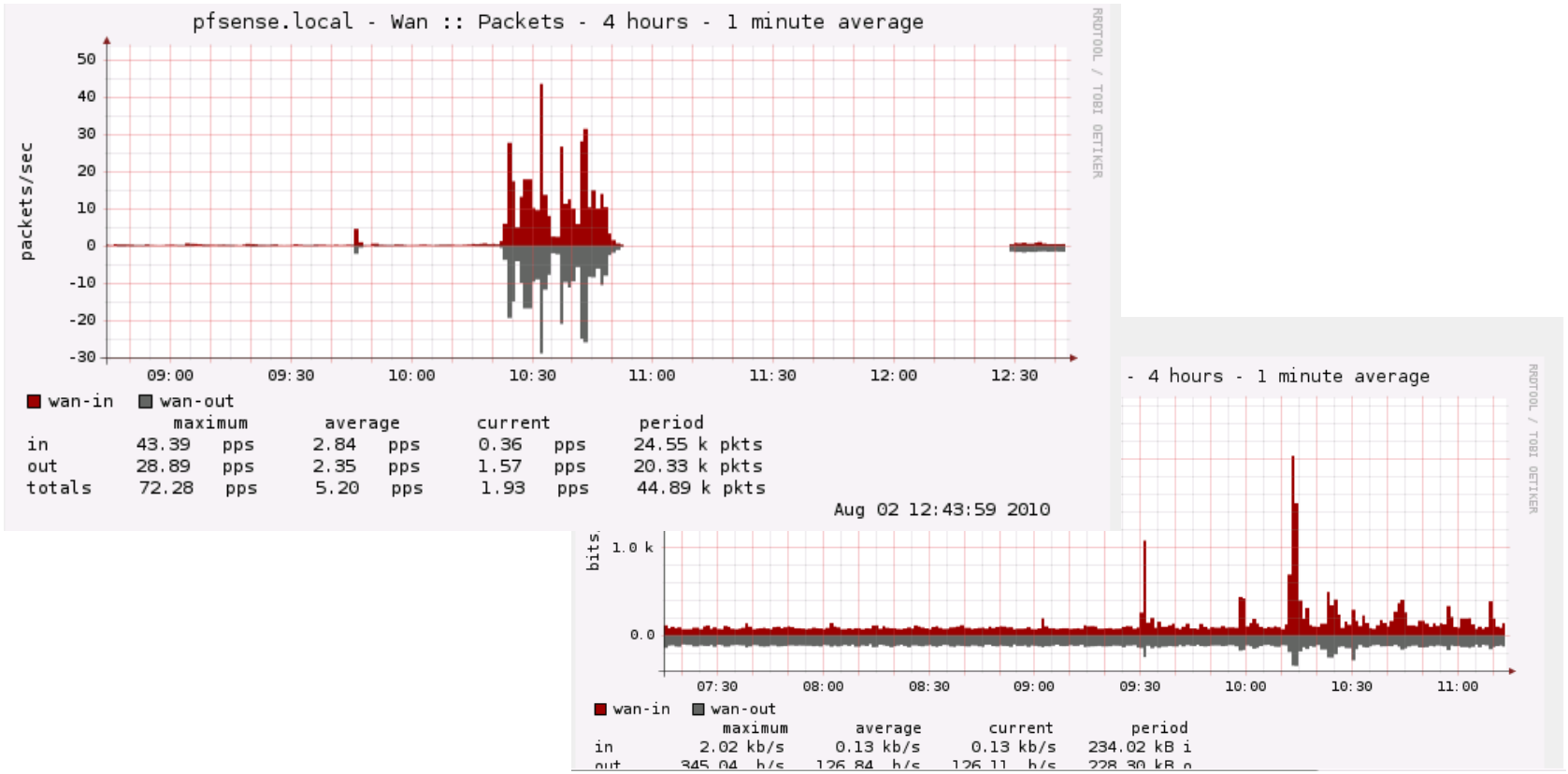
Servis durumlarını görüntülemek ve start/stop/restart işlemlerini yapmak



- Servisi restart eder.
- Servisi start eder.
- Servisi stop eder.

Bölüm 22:
Sistem Monitor | RRD Grafikleri

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



Bölüm 22:
Sistem Monitor | Firewall Durum Tablosu

Packet Filter (pf) durum tablosunu görüntüler.

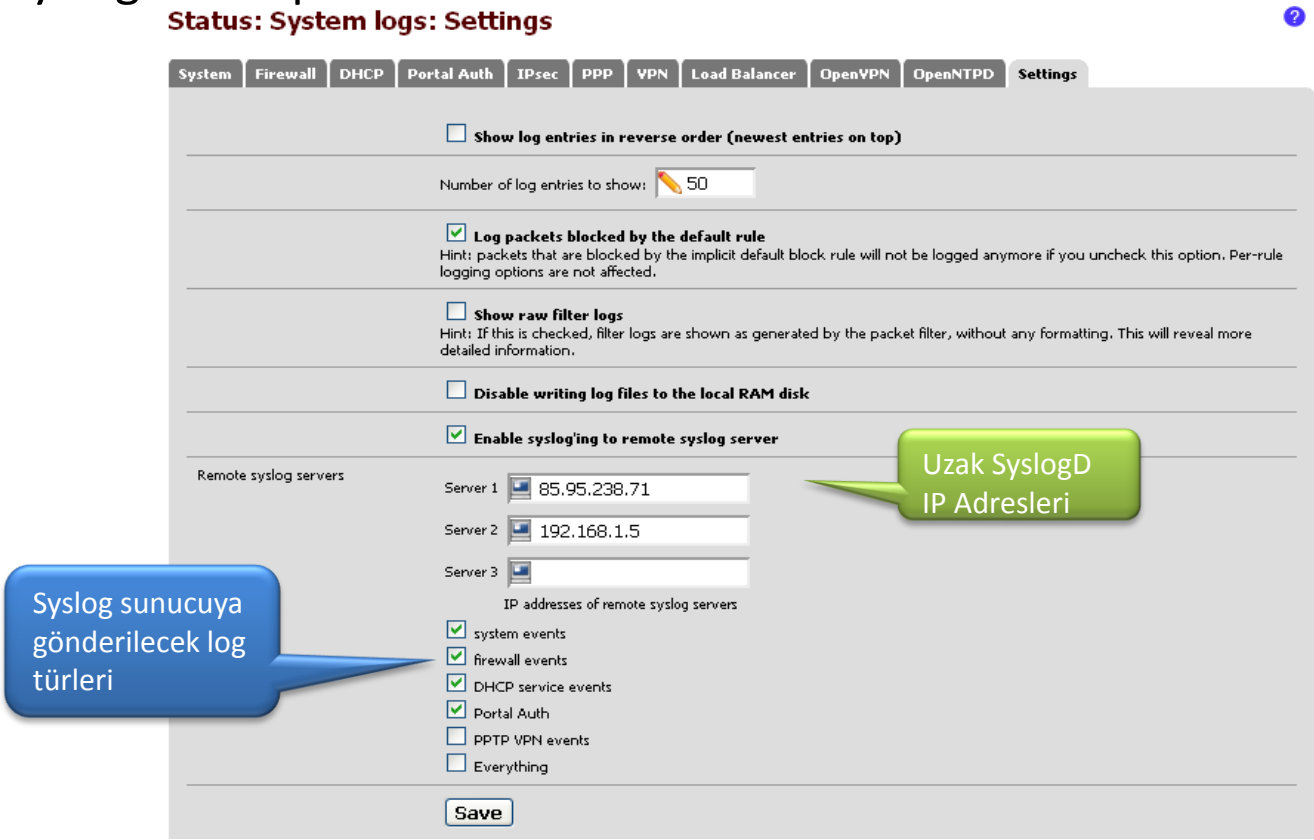
Protokol | Kaynak > Router > Hedef | Bağlanıtı Durumu

Proto	Source -> Router -> Destination	State
udp	10.0.0.254:520 -> 10.0.0.255:520	SINGLE:NO_TRAFFIC
udp	172.16.16.254:520 -> 224.0.0.9:520	SINGLE:NO_TRAFFIC
udp	192.168.5.88:123 -> 209.114.111.1:123	SINGLE:NO_TRAFFIC
udp	192.168.5.88:123 -> 66.96.98.9:123	SINGLE:NO_TRAFFIC
udp	192.168.5.88:123 -> 66.45.245.238:123	SINGLE:NO_TRAFFIC
tcp	67.192.253.140:80 <- 172.16.16.252:54004	FIN_WAIT_2:FIN_WAIT_2
udp	192.168.5.88:12348 -> 8.8.8.8:53	MULTIPLE:SINGLE
udp	192.168.5.88:54319 -> 8.8.8.8:53	MULTIPLE:SINGLE
udp	192.168.5.88:48332 -> 8.8.8.8:53	MULTIPLE:SINGLE
udp	192.168.5.88:56503 -> 8.8.8.8:53	MULTIPLE:SINGLE
udp	192.168.5.88:27159 -> 8.8.8.8:53	MULTIPLE:SINGLE
udp	192.168.5.88:29663 -> 8.8.8.8:53	MULTIPLE:SINGLE
udp	192.168.5.88:123 -> 204.15.208.61:123	SINGLE:NO_TRAFFIC
udp	192.168.5.88:123 -> 70.86.250.6:123	SINGLE:NO_TRAFFIC
udp	192.168.5.88:123 -> 169.229.70.183:123	SINGLE:NO_TRAFFIC
tcp	172.16.16.254:80 <- 172.16.16.252:54006	ESTABLISHED:ESTABLISHED

Bölüm 22:
Sistem Monitor | Uzak SyslogD

pfSense s,stem kayıtlarını geçmişe yönelik arşivlemez. Kayıtlar, saklanmak, yorumlanmak ve raporlanmak için uzak bir syslog sunucuya gönderilebilir.

NOT: SyslogD UDP port 514 kullanır.



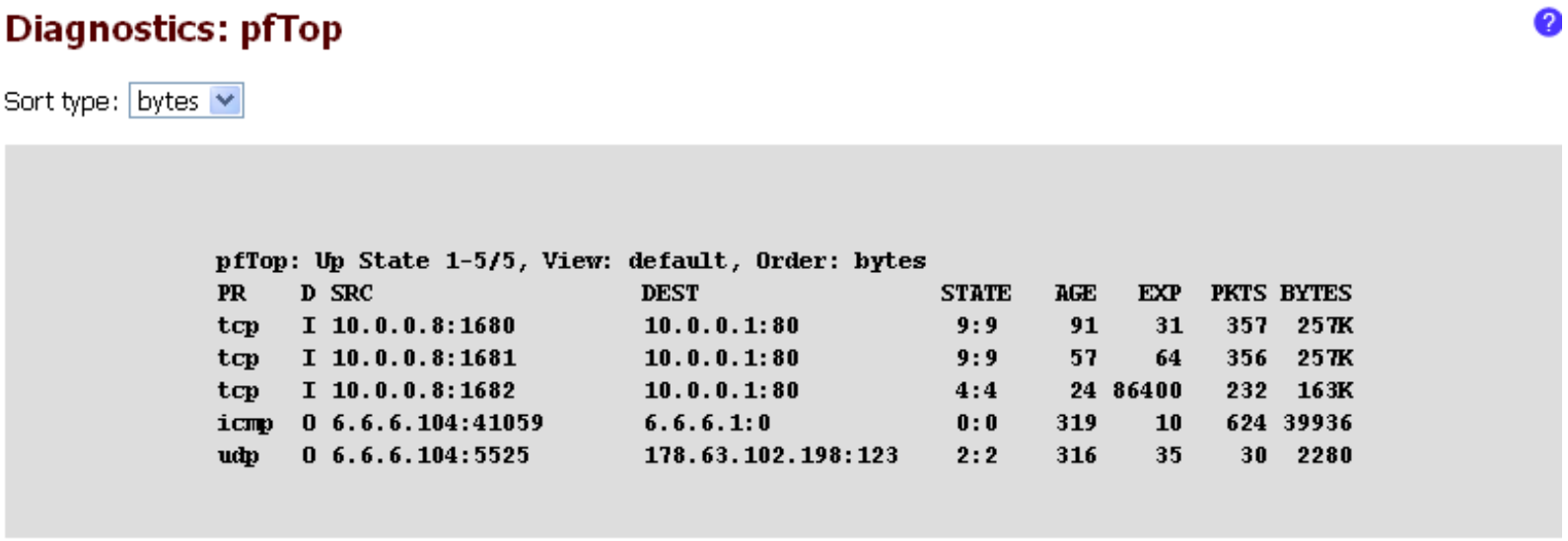
Bölüm 22:
Sistem Monitor | pfInfo

- Packet Filter istatistliğini verir

```
Status: Enabled for 0 days 00:03:08          Debug: Urgent

Hostid:   0xc799f47f
Checksum: 0x96ae4385221693ec1d3f9f2bb8b3650a

Interface Stats for em0                IPv4              IPv6
  Bytes In                            85410                 0
  Bytes Out                          755004               152
  Packets In
    Passed                              528                 0
    Blocked                              33                 0
  Packets Out
    Passed                              763                 0
    Blocked                               0                 2

State Table                          Total              Rate
  current entries                       10
  searches                            1888             10.0/s
  inserts                               23              0.1/s
  removals                              13              0.1/s
Source Tracking Table
  current entries                        0
  searches                               0              0.0/s
  inserts                                0              0.0/s
  removals                               0              0.0/s
```

Bölüm 22:
Sistem Monitor | pftop

- Aktif trafik bilgisini verir.

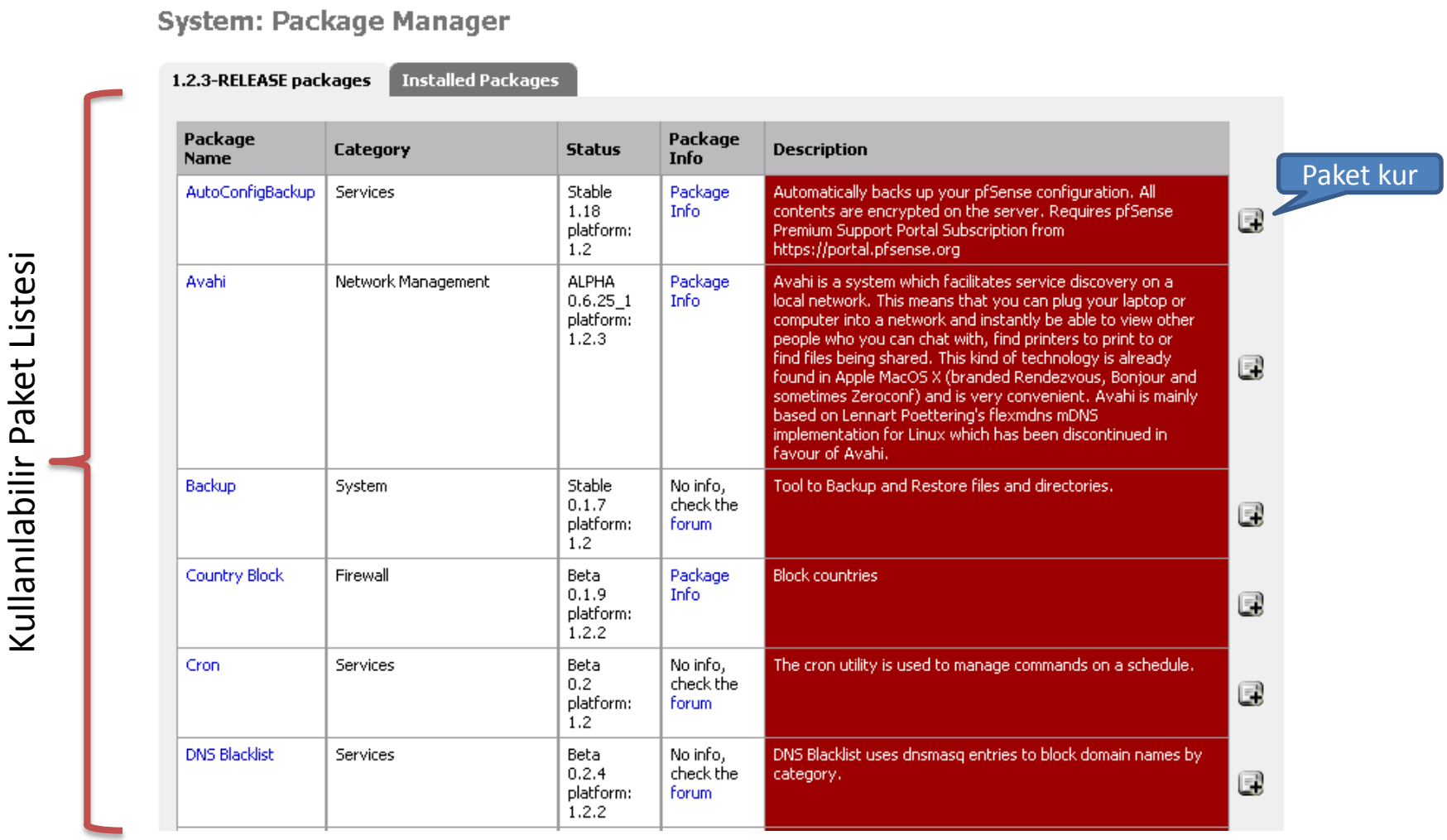


Bölüm 23:
Paket Sistemi

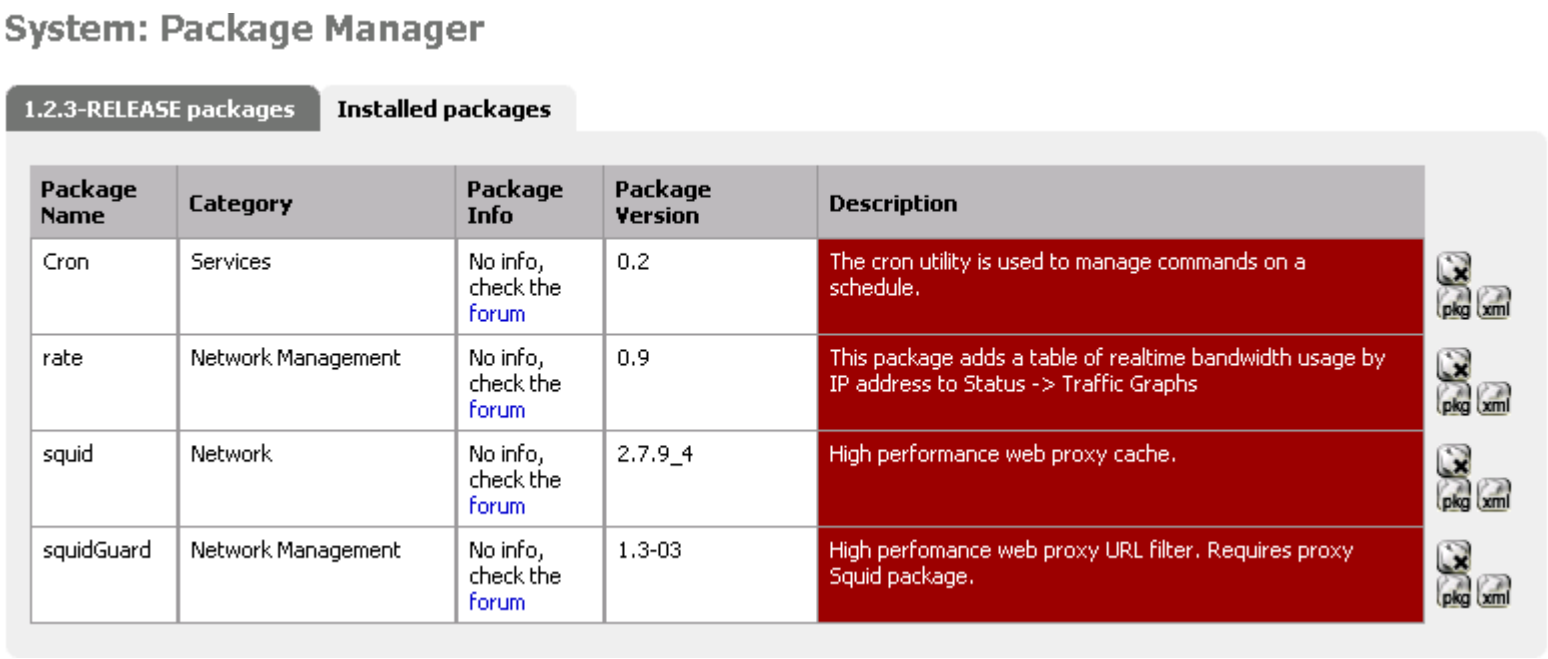
pfSense modüler yapısını paket sistemi ile sağlıyor. Ek servisler ve uygulamalar paket sisteminden kolayca yönetilebiliyor. Paket sisteminin sağladığı özellikler;

- Paket Kurulumu
- Paket Yükseltme
- Paket Kaldırma

Bölüm 23:
Paket Sistemi | Paket Kurulumu



Bölüm 23:
Paket Sistemi | Paket Yükseltme/Kaldırma



- Paketi yeniden kurmayı sağlar
- İlgili paketin web arabirimini yeniden kurar
- Kurulu paketi sistemden kaldırır

Bölüm 23:
FreeBSD Paket Sistemi

Paket deposunu tanımlamak

setenv PACKAGESITE ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-7-stable/Latest/

Kurulu paketlerin listesi;

pkg_info

FreeBSD deposundan paket kurulumu

pkg_add -rv nano

FreeBSD paketinin kurulumu

pkg_add -v dansguardian.tbz

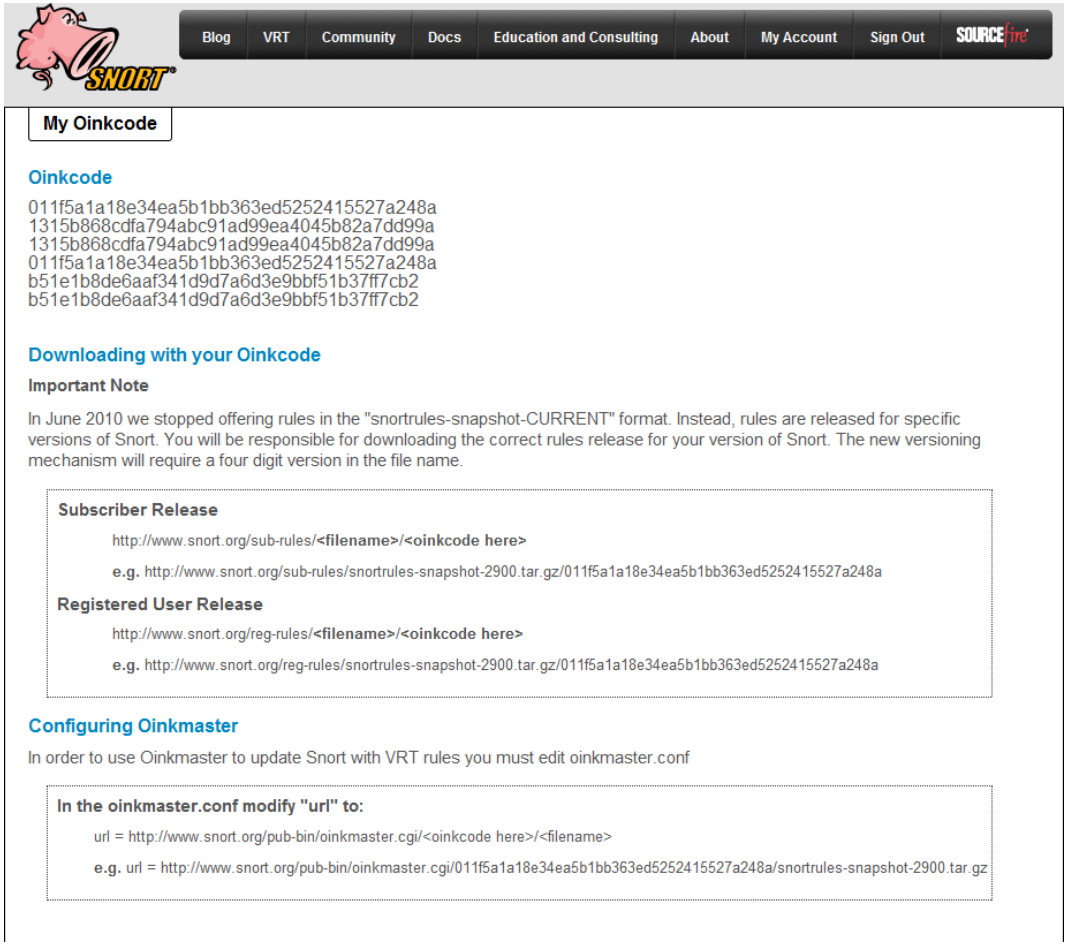
Paket kaldırmak

pkg_delete -v paket_adı

Bölüm 24:
Snort IDS/IPS

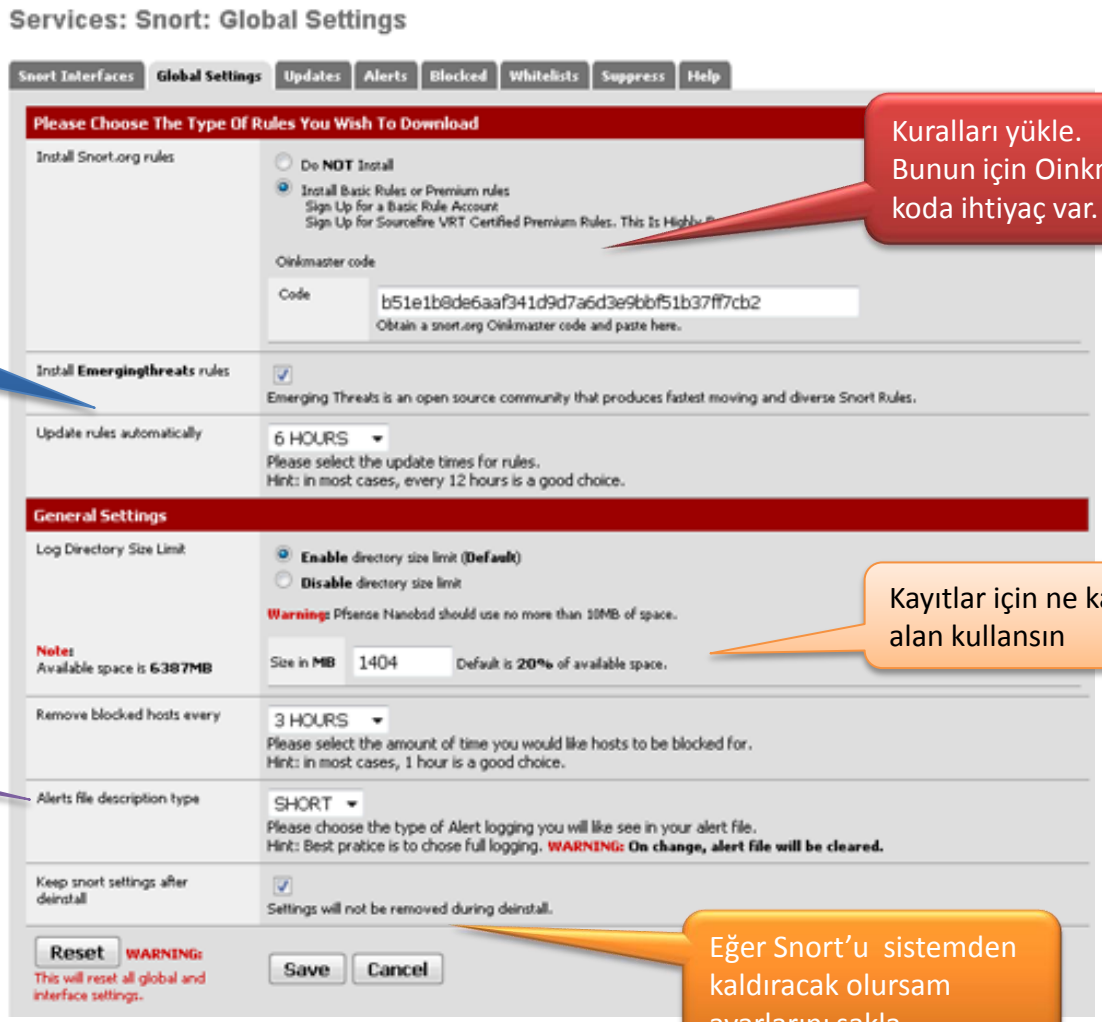
- Snort Kurulumu ve Genel Ayarlar
- Snort imzalarının yüklenmesi ve Yönetimi
- IDS olarak yapılandırmak
- IPS olarak yapılandırmak
- Barnyard Kullanımı
- Logların Mysql'e aktarılması
- Logların Yorumlanması

Bölüm 24:
Snort IDS/IPS|İmzalar



Snort imzalarını güncellemek için snort.org adresine üye olup oinkmaster code temin etmek gerekir !

Bölüm 24:
Snort IDS/IPS| Genel Ayarlar



Kuralları yükle. Bunun için Oinkmaster koda ihtiyaç var.

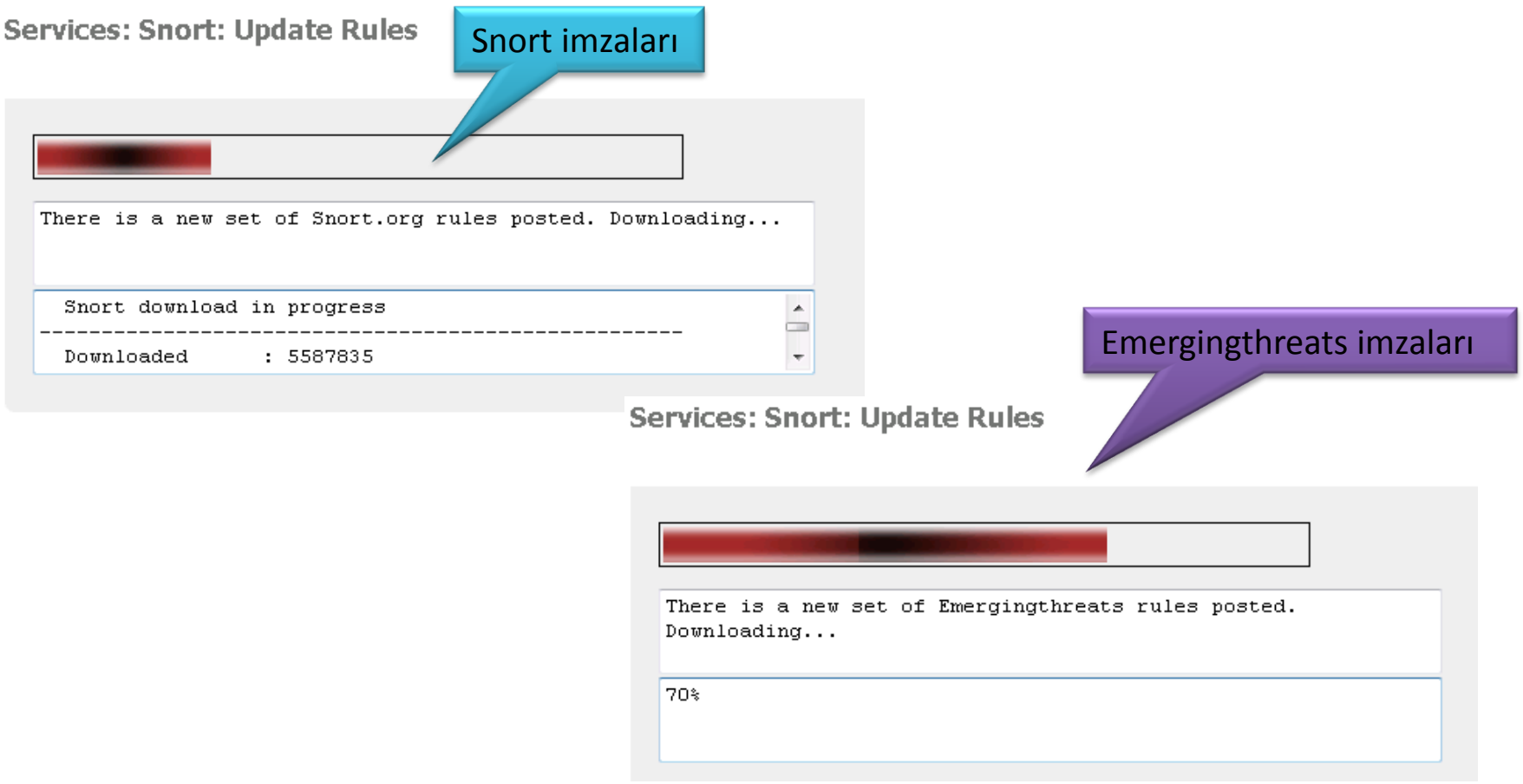
Kurallar hangi aralıklarla güncellenecek ?

Kayıtlar için ne kadar alan kullansın

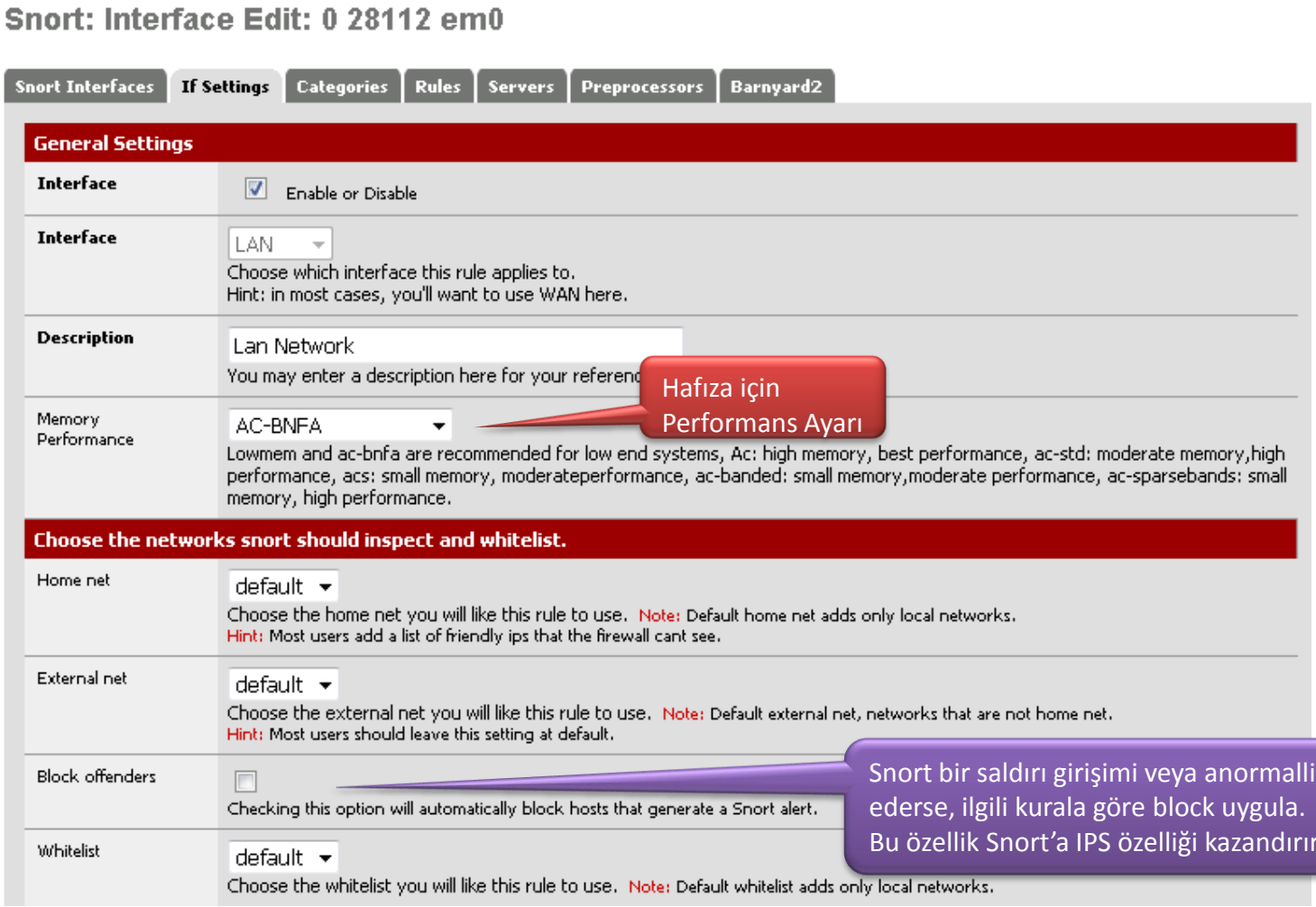
Kayıt türü

Eğer Snort'u sistemden kaldıracak olursam ayarlarını sakla.

Bölüm 24:
Snort IDS/IPS|İmzalar



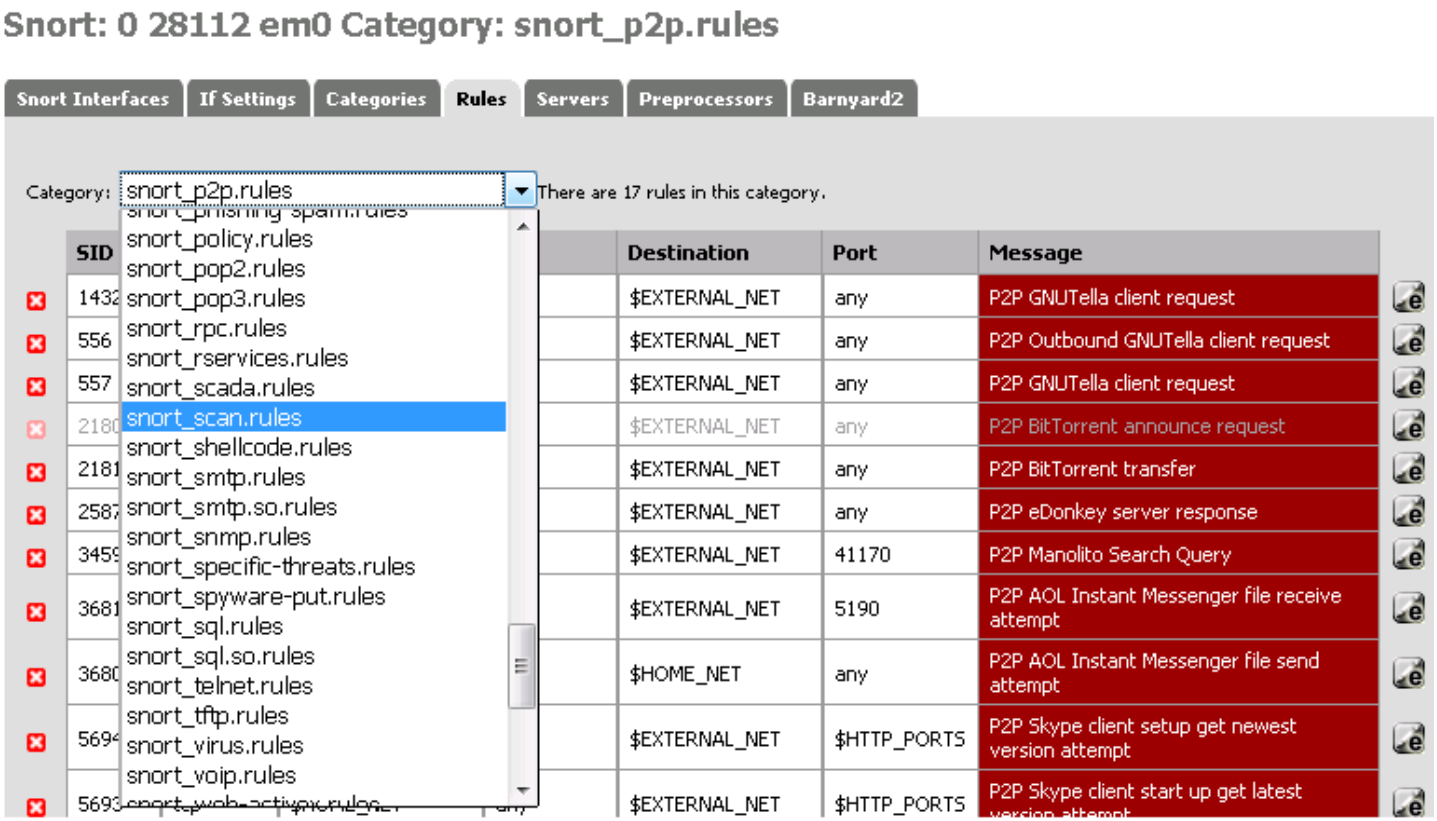
Bölüm 24:
Snort IDS/IPS| Ağ Ayarları



Bölüm 24:
Snort IDS/IPS| Kategori Yönetimi

Snort imzaları kategori bazlı tutulur. Örneğin; web tabanlı saldırılar “web-*.rules” , trojan imzaları ise “trojan.rules” olarak kategorilendirilir. Performans için ihtiyaç duyulmayan kurallar aktif edilmemelidir.

Bölüm 24:
Snort IDS/IPS| Kategori Yönetimi

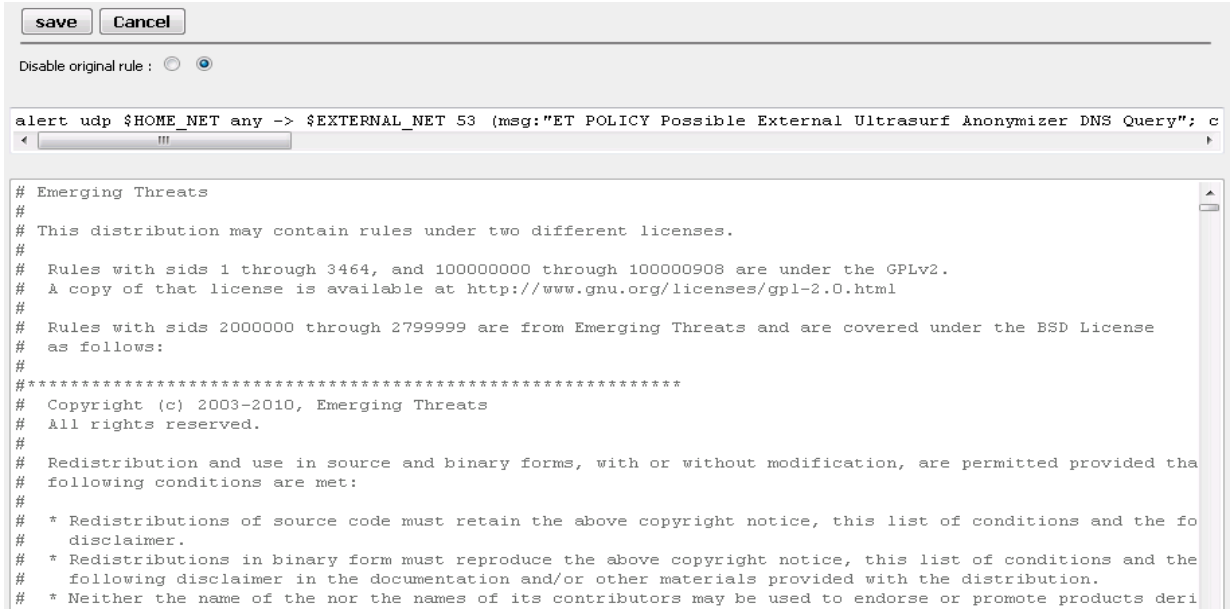


- Kural pasif durumda, tıklandığında kuralı aktif yapar
- Kural aktif durumda, tıklandığında kuralı pasif yapar
- Kuralı düzenle

Bölüm 24:
Snort IDS/IPS| Kural Yönetimi

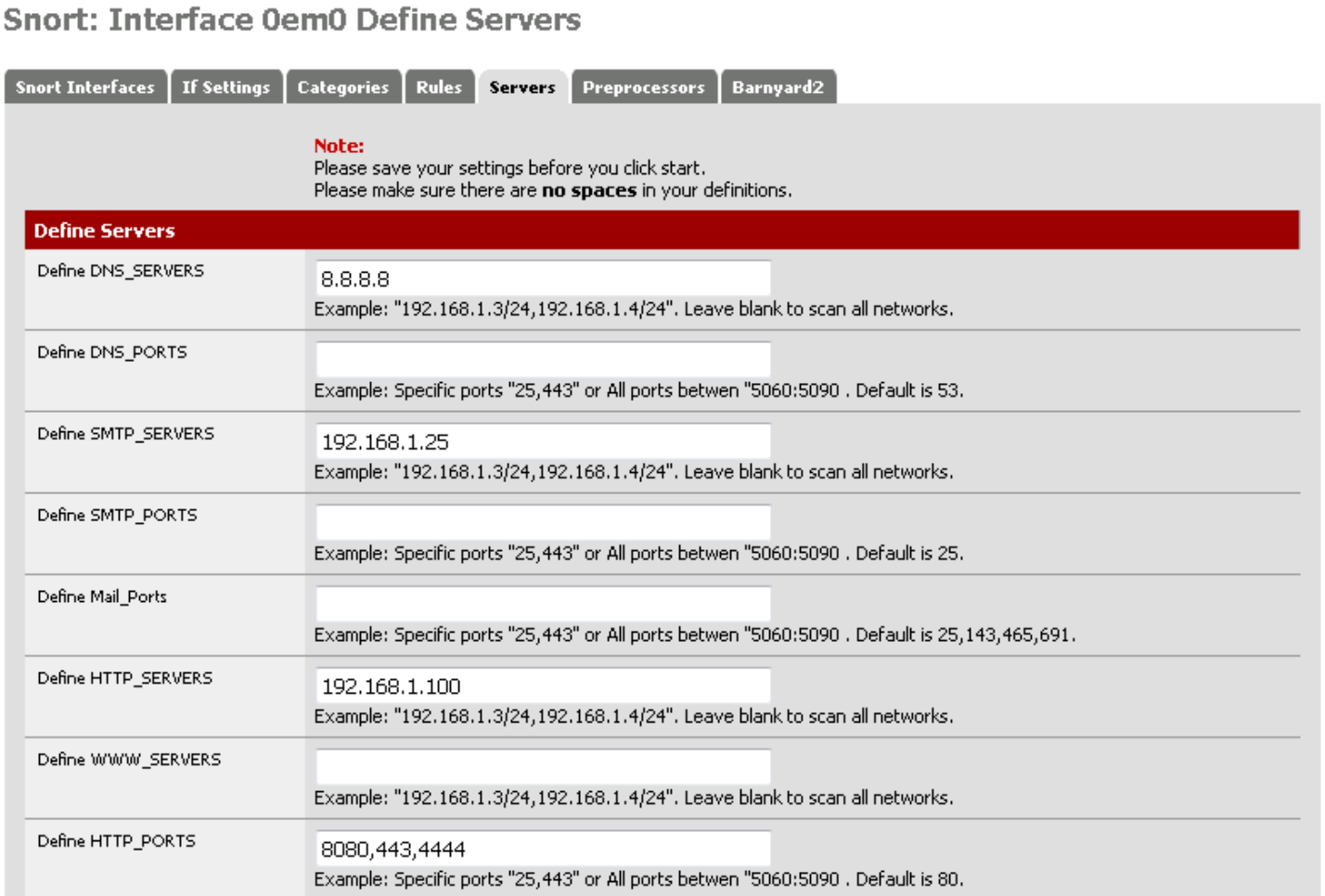
	2010797	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	ET POLICY Twitter Status Update
	2008533	udp	$HOME_NET	any	$EXTERNAL_NET	53	ET POLICY Possible External Ultrasurf Anonymizer DNS Query

UltraSurf İmzası



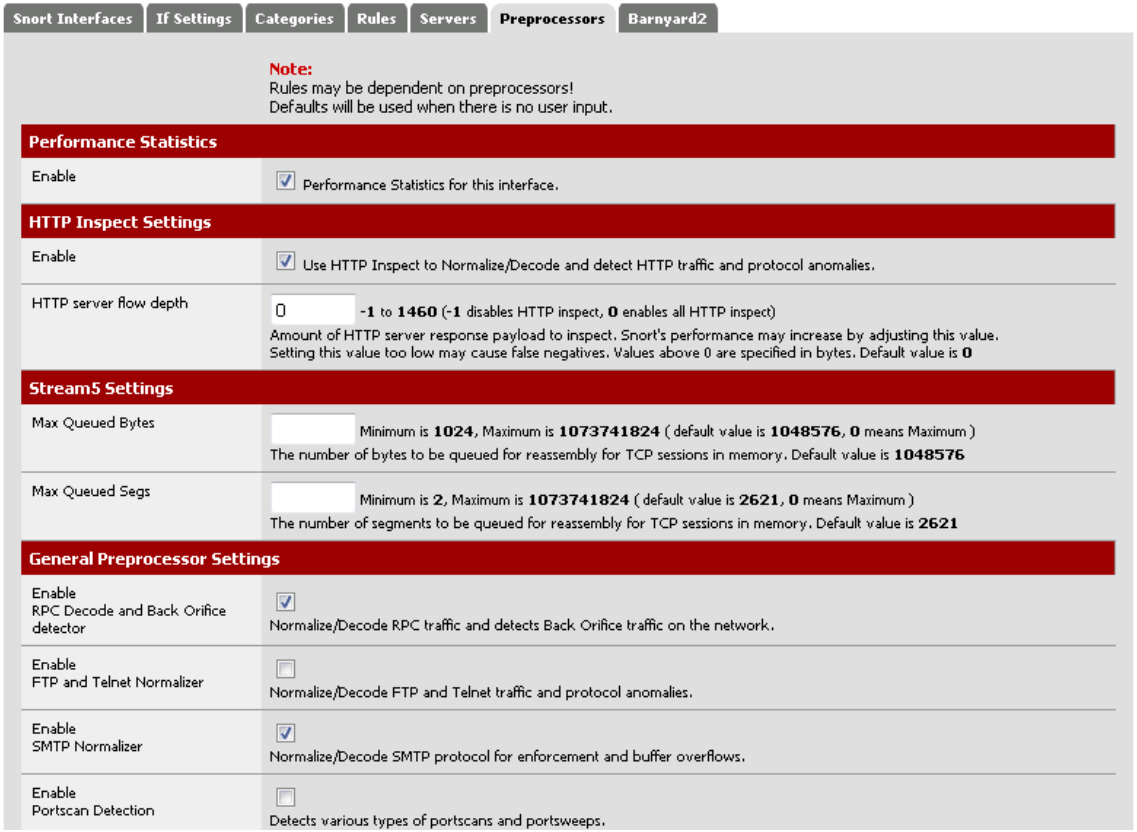
- Kural pasif durumda, tıklandığında kuralı aktif yapar
- Kural aktif durumda, tıklandığında kuralı pasif yapar
- Kuralı düzenle

Bölüm 24:
Snort IDS/IPS| Kural Yönetimi



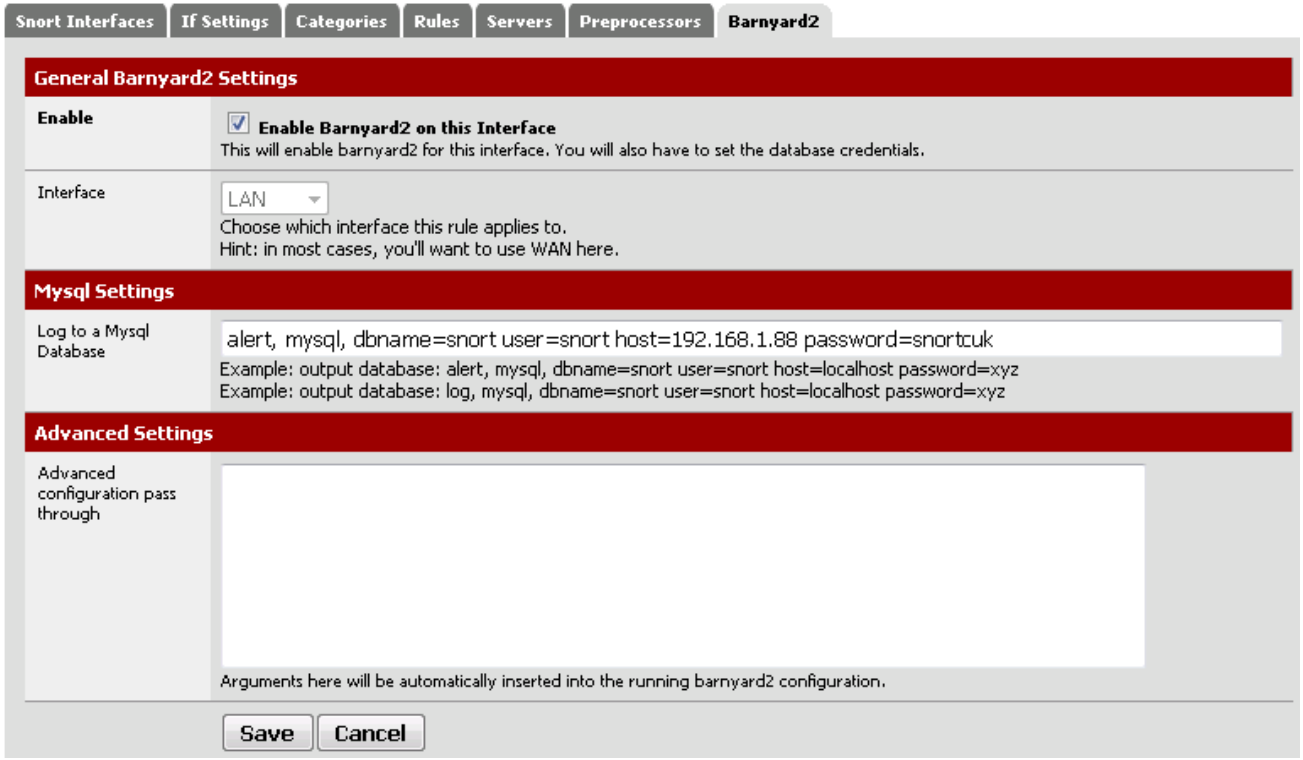
Bölüm 24:
Snort IDS/IPS | Ön İşlemciler

Ön işlemciler, tcp trafiğini analiz etmek için kullanılır. Saldırı atlatma tekniklerini (evulation) analiz edip, anormal trafiği normalleştirmek için kullanılır.
Bazı kuralların çalışması bu ön işlemcilere bağlıdır. İhtiyaca göre aktif edilmelidir.



Bölüm 24:
Snort IDS/IPS | Barnyard2

Snort tespit edilen saldırıları görüntülemeye çalışırken çok fazla zaman ve performans kaybına uğramaktadır. “barnyard2” kullanılarak bu yük Snort’un üzerinden alınır. Böylece Snort ürettiği kayıtları biçimlendirmek için zaman harcamaz ve sadece kendi işi olan saldırı tespit ve engelleme işine daha fazla zaman ayırır.

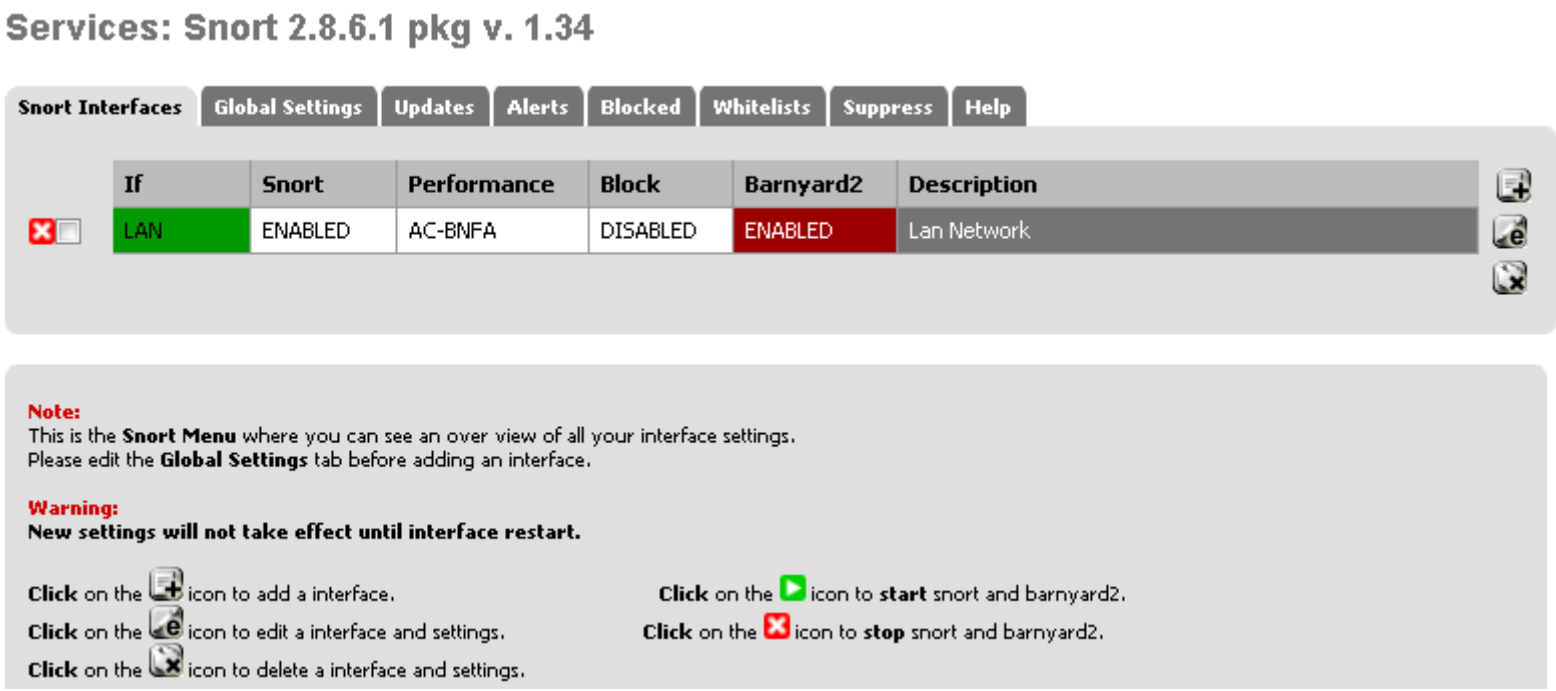


Bölüm 24:
Snort IDS/IPS | Sorun Giderme

“snort[7923]: FATAL ERROR: /usr/local/etc/snort/snort_37305_em1/rules/emerging-scan.rules(46) Please enable the HTTP Inspect preprocessor before using the http content modifiers”

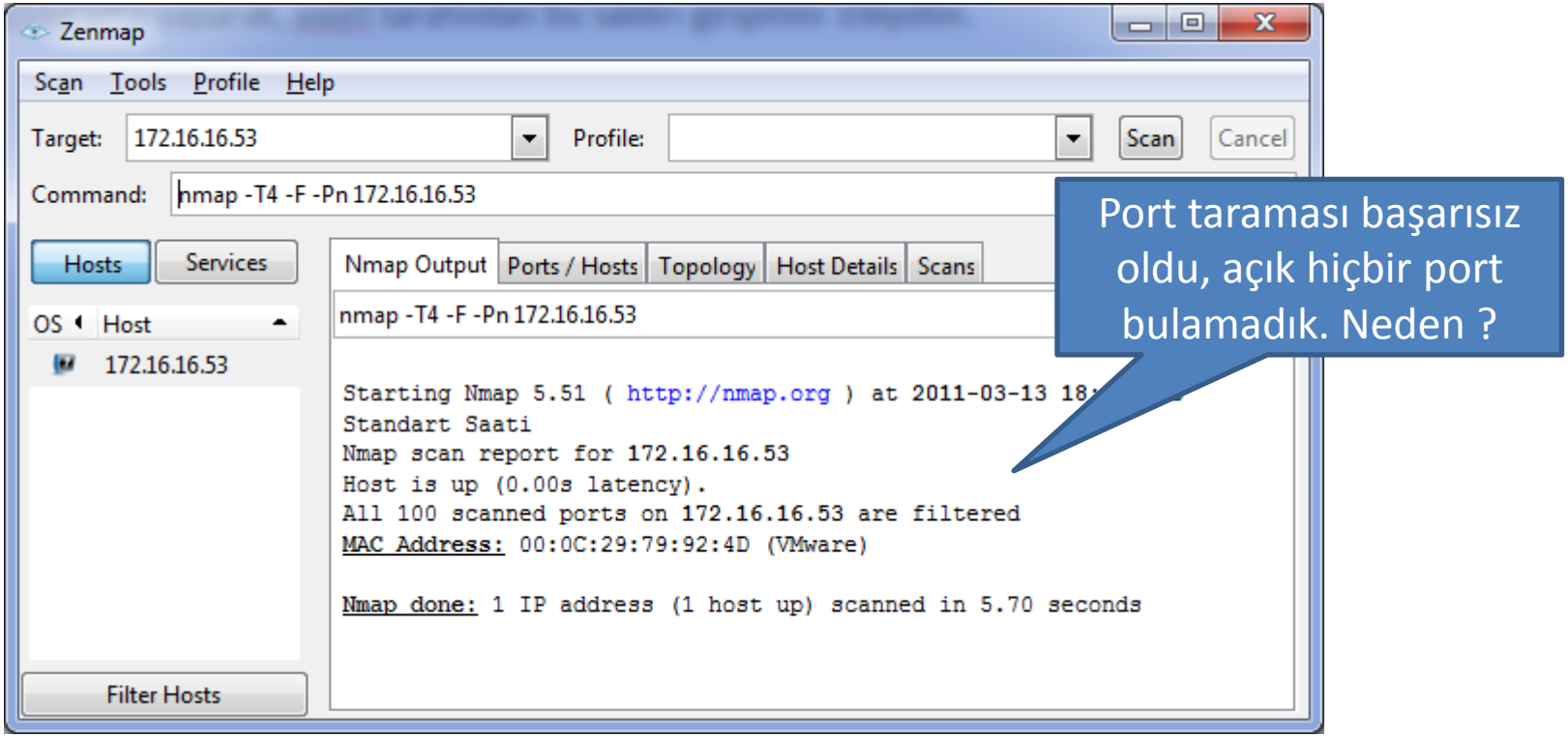
emerging-scan.rules(46) kuralını çalıştırmam için HTTP Inspect ön işlemcisine ihtiyacım var, lütfen bunu aktif et.

Bölüm 24:
Snort IDS/IPS | Son Kontrol



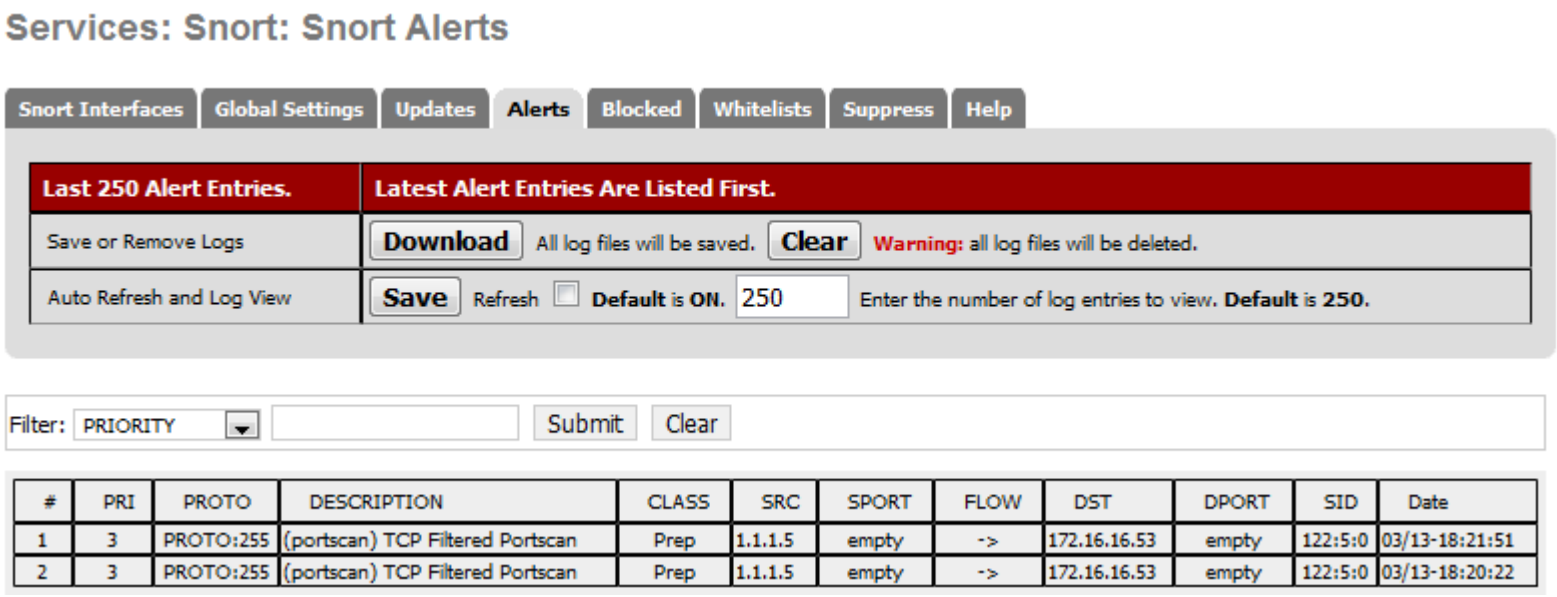
Bölüm 24:
Snort IDS/IPS | Test

Port tarama yaparak, snort tarafından bu saldırı girişimini izleyelim.



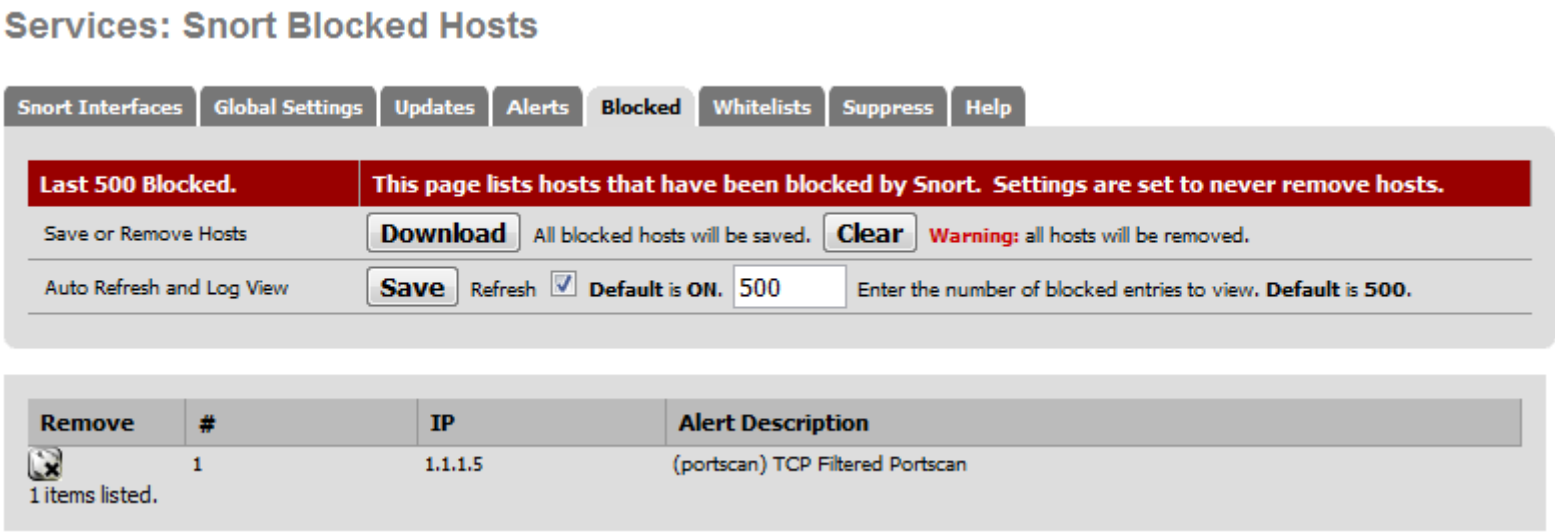
Bölüm 24:
Snort IDS/IPS | Test

Port tarama, snort tarafından bu saldırı girişimini olarak algılandı ve uyarı sayfasına kayıt düştü.



Bölüm 24:
Snort IDS/IPS | Test

Peki, yinede açık port'ları öğrenmemiz gerekmezmiydi ? Snort IDS olarak çalışsaydı EVET ! Fakat IPS özelliğide kazandırdık ve saldırı gelen ip adresini engelledi.



Bölüm 24:
Snort IDS/IPS | Test

Bilişimcilerin belası, özgürlük savaşçılarının silahı Ultrasurf.

3	1	UDP	ET POLICY Possible External Ultrasurf Anonymizer DNS Query	Potential Corporate Privacy Violation	192.168.1.8	61748	->	130.94.124.174	53	1:2008533:3	03/17-17:33:12
4	1	TCP	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted	Potential Corporate Privacy Violation	192.168.1.101	43645	->	192.168.1.1	80	1:2006380:10	03/17-17:32:26
5	1	TCP	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted	Potential Corporate Privacy Violation	192.168.1.101	43650	->	192.168.1.1	80	1:2006380:10	03/17-17:32:26
6	1	TCP	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted	Potential Corporate Privacy Violation	192.168.1.101	43646	->	192.168.1.1	80	1:2006380:10	03/17-17:32:17

Bölüm 25:
Squid

Yüksek performanslı web proxy yazılımı.

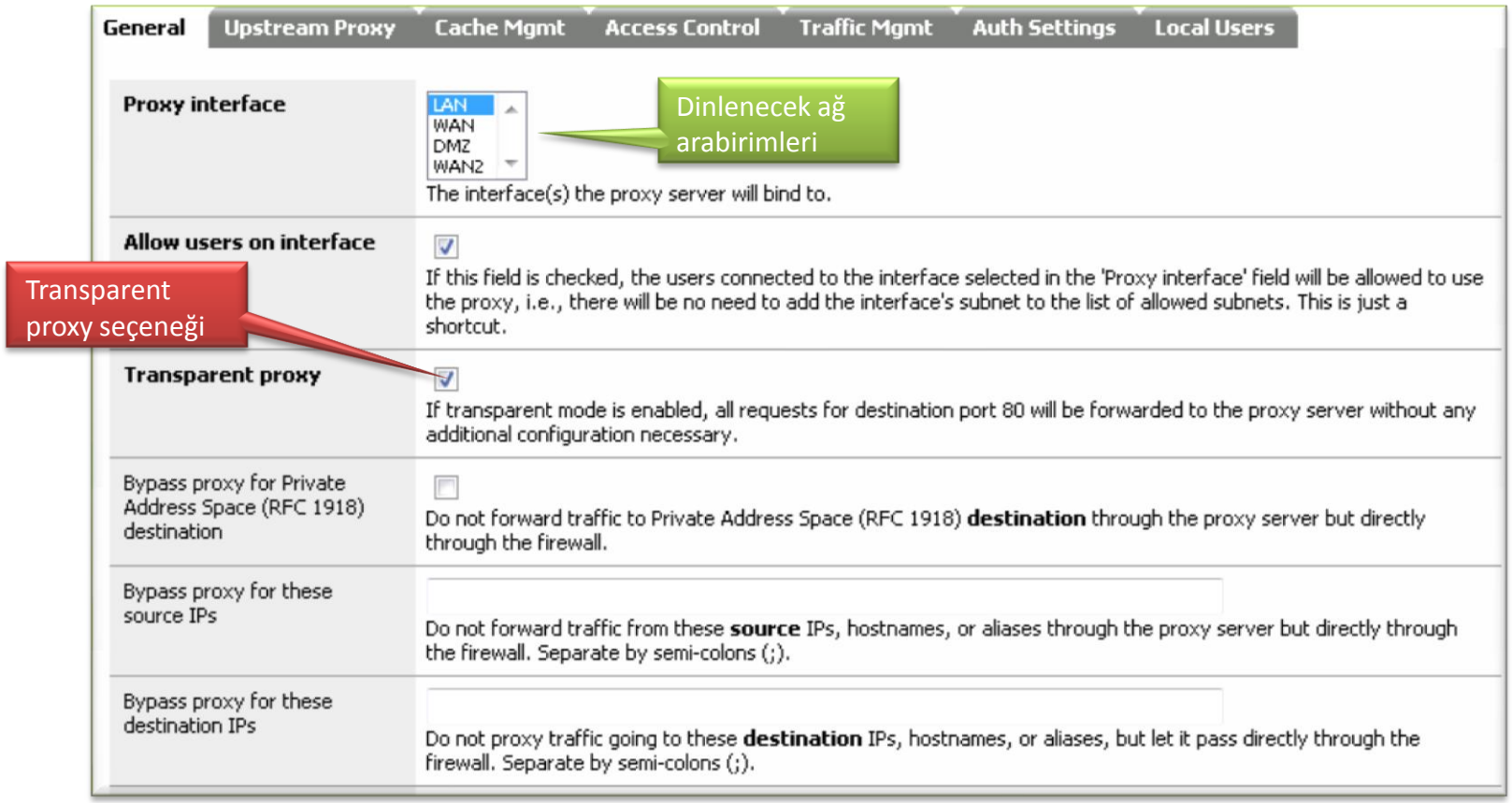
- Transparent Proxy olarak yapılandırmak
- Upstream Proxy
- Önbellek Yönetimi
- Erişim Kontrol Listeleri (ACL)
- Gelişmiş ACL Yazımı
  - MSN Block
  - UltraSurf Block
- Trafik yönetimi
- Kimlik Doğrulama
  - Yerel Kimlik Doğrulama
  - Ldap kullanarak Active Directory ile kimlik doğrulama

Bölüm 25:
Squid | Transparent Proxy

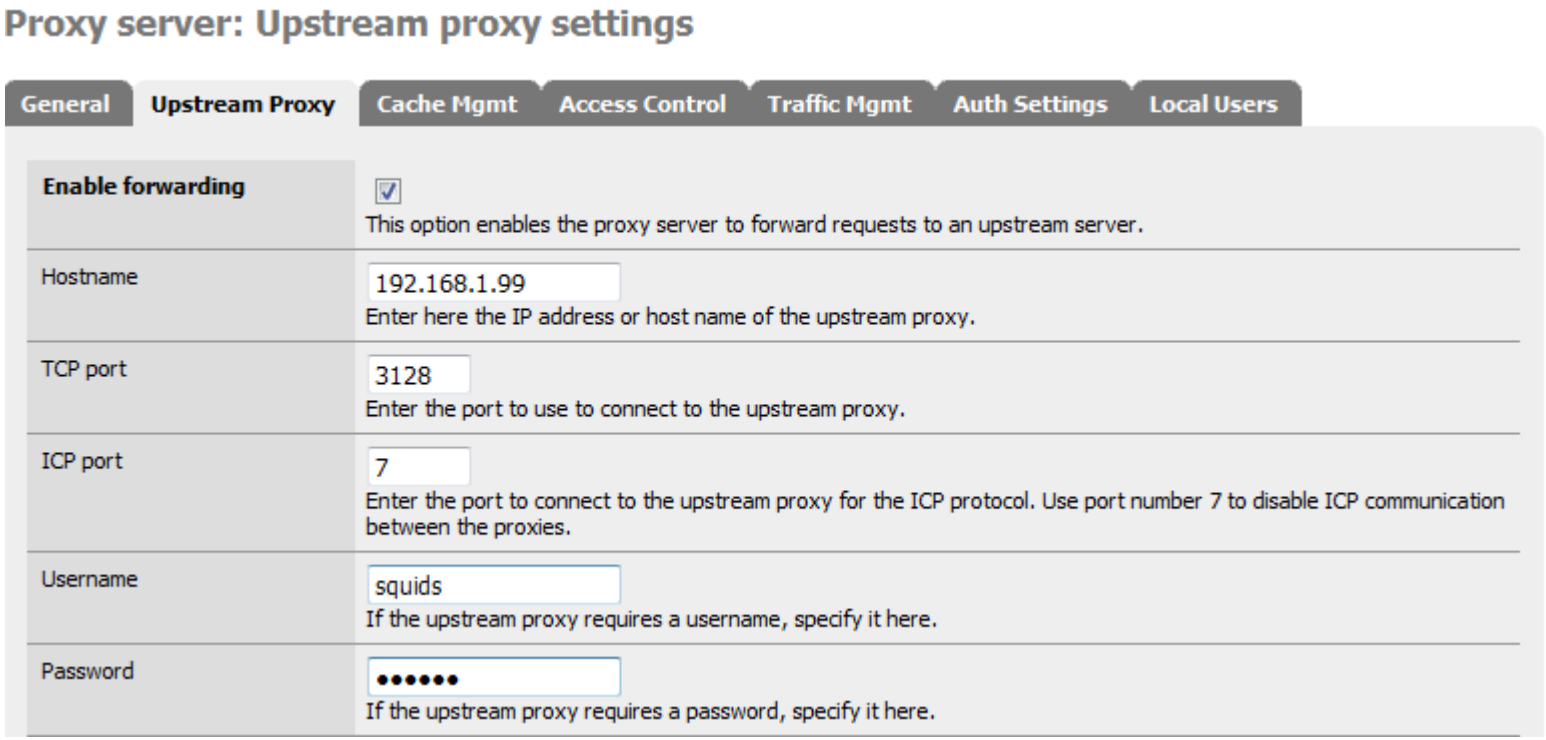
İstemcilere proxy adresi belirtmeden, hedef portu 80 olan istekleri squid'e aktarır.

 # pfctl -sn | grep http

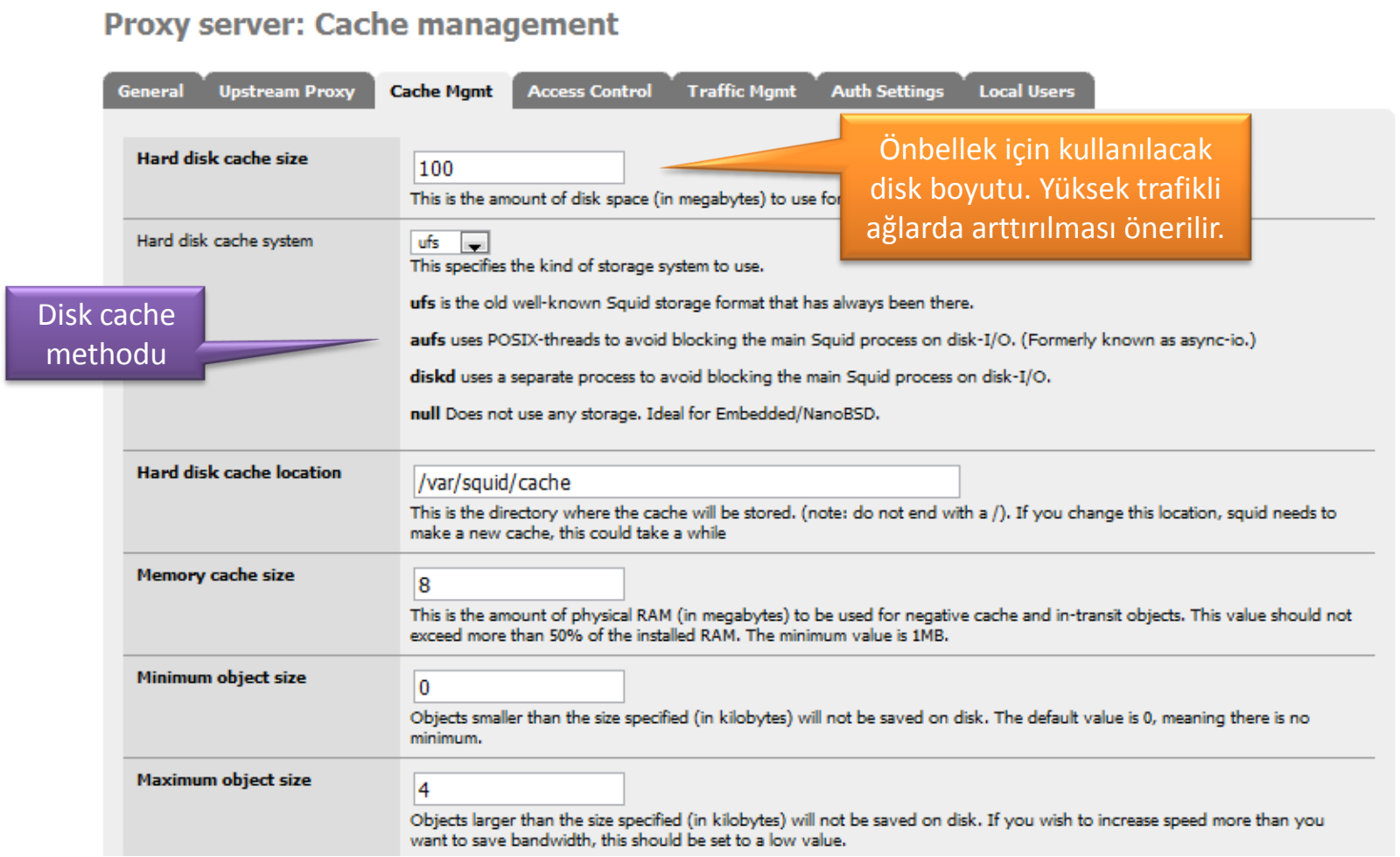
rdr on em0 inet proto tcp from any to ! (em0) port = http -> 127.0.0.1 port 80



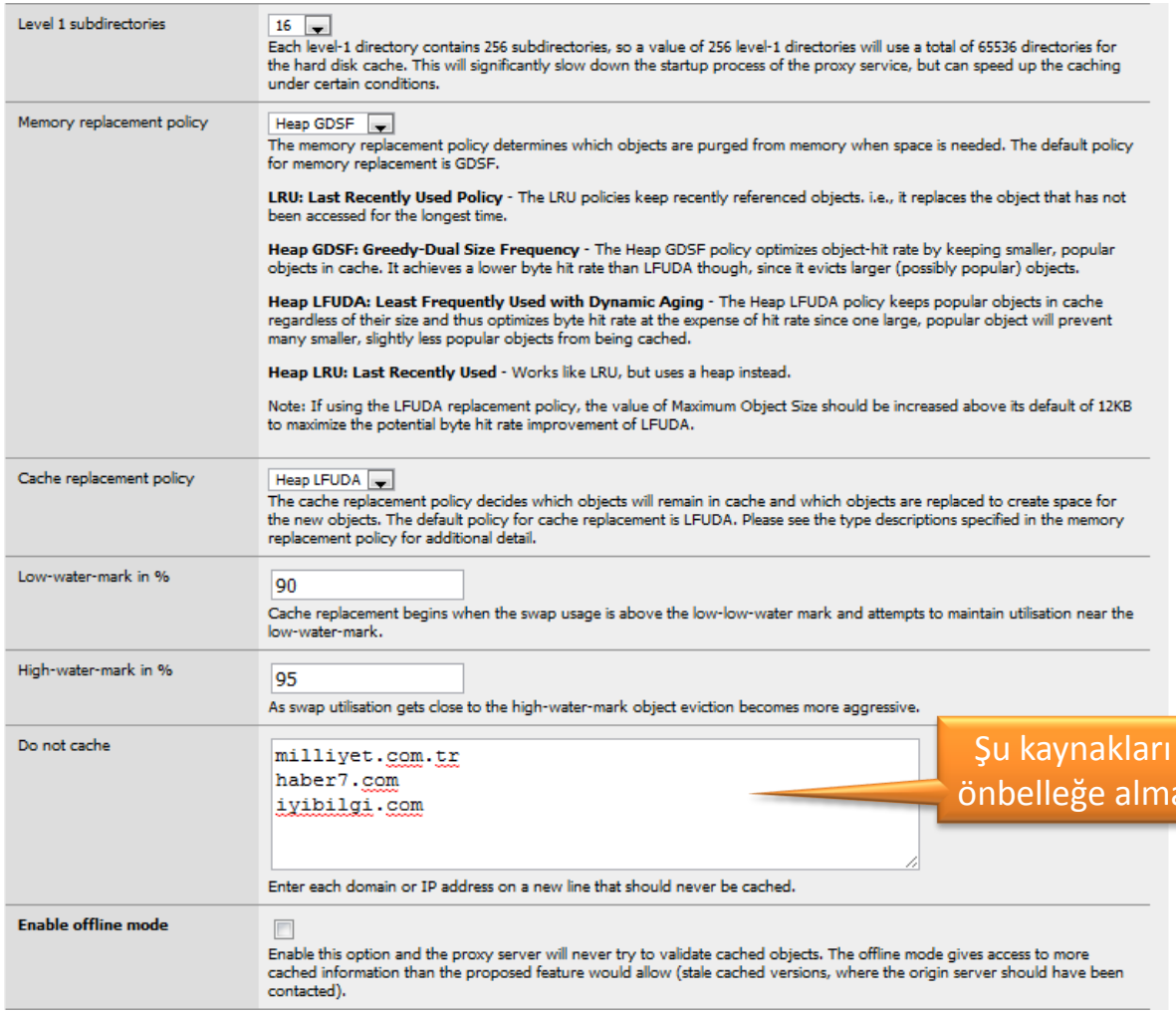
Bölüm 25:
Squid | Upstram Proxy



Bölüm 25:
Squid | Önbellek Yönetimi



Bölüm 25:
Squid | Önbellek Yönetimi



Bölüm 25:
Squid | Erişim Kontrol Listeleri (ACL)

Allowed subnets
Proxy kullanımına izin verilen ağlar.
192.168.16.0/24 gibi gibi

Unrestricted IPs
Sınırsız izne sahip ip adresleri
192.168.16.254

Banned host addresses
Proxy kullanımı yasaklı ip adresleri
192.168.16.200

Whitelist
Beyaz liste, erişim kurallarının uygulanmayacağı adresler. Hariç tutulanlar.
gmail.com
www.milliyet.com.tr

Bölüm 25:
Squid | Erişim Kontrol Listeleri (ACL)

Blacklist
Erişimi yasaklanmak istenen alan adları
facebook.com

acl safeports
Squid, güvenli port numaraları dışındaki web portlarına erişimi engeller.Ön tanımlı port numaraları, 21 70 80 210 280 443 488 563 591 631 777 901 1025-65535
Örneğin; http://www.bga.com.tr:8899 adresine ulaşmanız için “8899” port numarasını güvenli port grubuna eklemeniz gerekir.

acl sslports
SSL "CONNECT“ methodu ile bağlantı kurulmasına izin verilen sslportları. Ön tanımlı portlar 443 563.

Bölüm 25:
Squid | Gelişmiş ACL Yazımı

MSN ACL

```
acl msn1 rep_mime_type -i ^application/x-msn-messenger$
acl msndll urlpath_regex -i gateway.dll
acl msnd dstdomain messenger.msn.com gateway.messenger.hotmail.com
acl izinliler src "/etc/izinli.txt“
http_access allow izinliler msnd
http_access allow izinliler msndll
http_access allow izinliler msn1
```

Not: firewall’dan 1863 portu kapalı olmalıdır. Transparent modda filtreleme yapılabilir.

Bölüm 25:
Squid | Gelişmiş ACL Yazımı

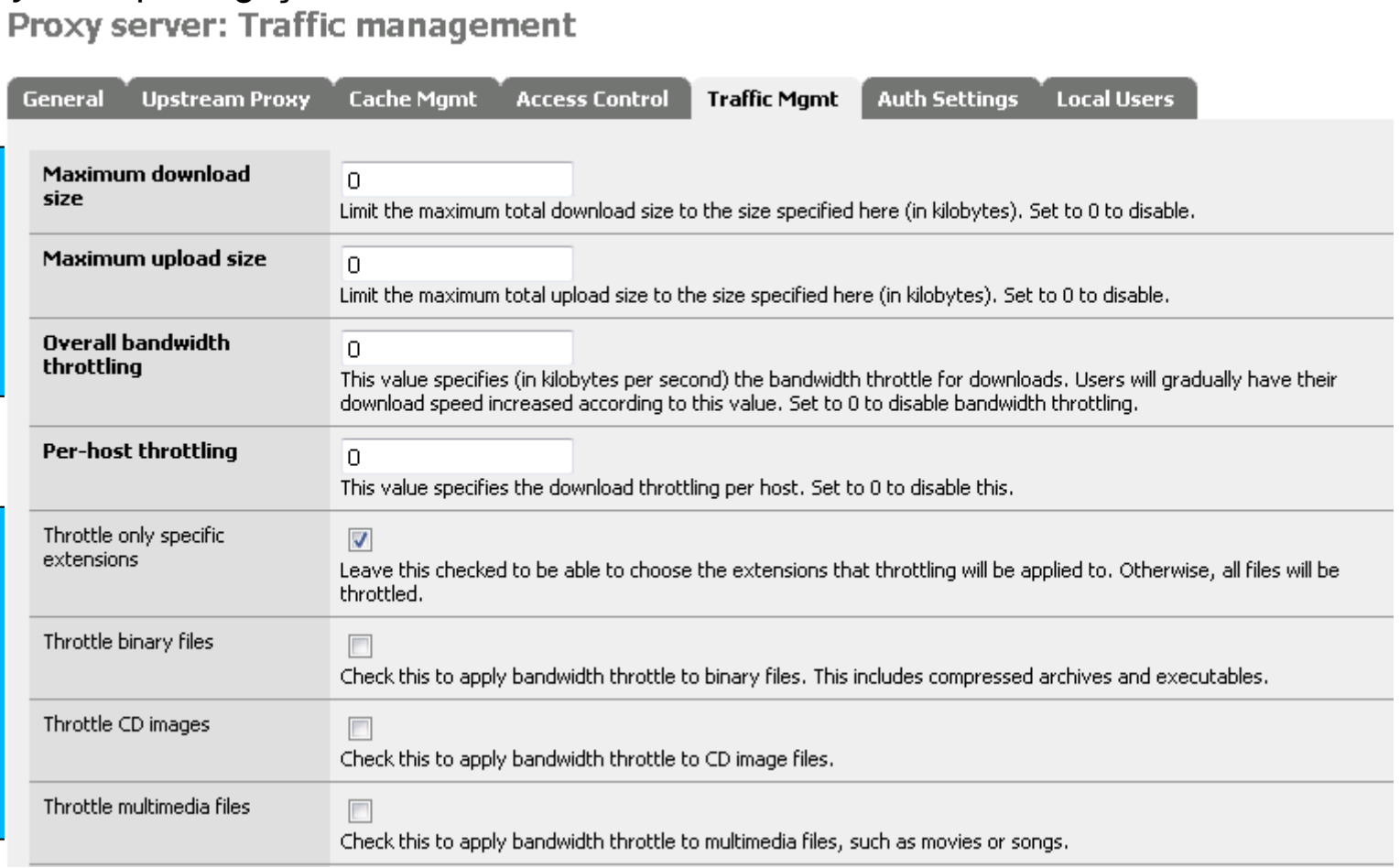
UltraSurf ACL

```
acl CONNECT method CONNECT
    acl ultra_block  url_regex ^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+
    http_access deny CONNECT ultra_block  all
```

Not: Firewall'dan 443. portunun kapalı olması gerekir. İstemcilerde proxy adresi tanımlı olmalıdır, Ultrasurf kuralı transparent squid ile çalışmaz.

Bölüm 25:
Squid | Trafik Yönetimi

Squid proxy ile http trafiği şekillendirilebilir.



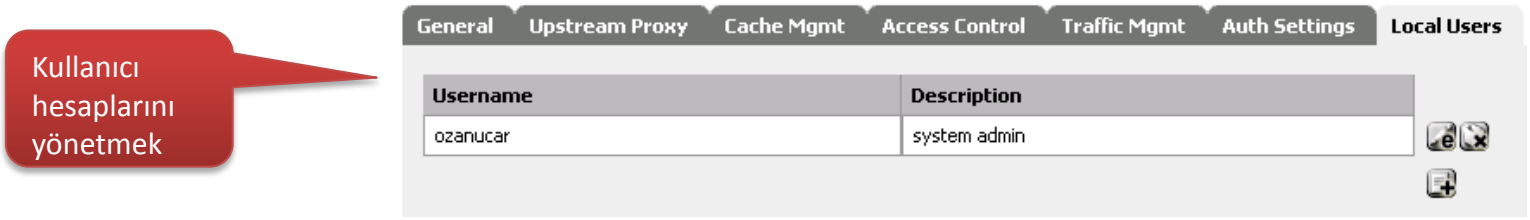
Trafik limitleri için değerler

Trafiğin set edileceği dosya türleri

Bölüm 25:
Squid | Kimlik Doğrulama | Yerel

Yerel kullanıcı veritabanını kullanarak kimlik doğrulama yapar.

Dikkat: Transparent modda kimlik doğrulama yapılamaz !



Bölüm 25:
Squid | Kimlik Doğrulama | Ldap

Ldap ile uzak bir sistemden kimlik doğrulama yapar. Örnek: Microsoft Active Directory

Kimlik doğrulama methodu "Ldap"

Gerekli Bilgiler

Authentication method: LDAP

LDAP version: 3

Authentication server: (windows server IP adresi)

LDAP server user DN: cn=administrator,cn=Users,dc=domainadı,dc=com

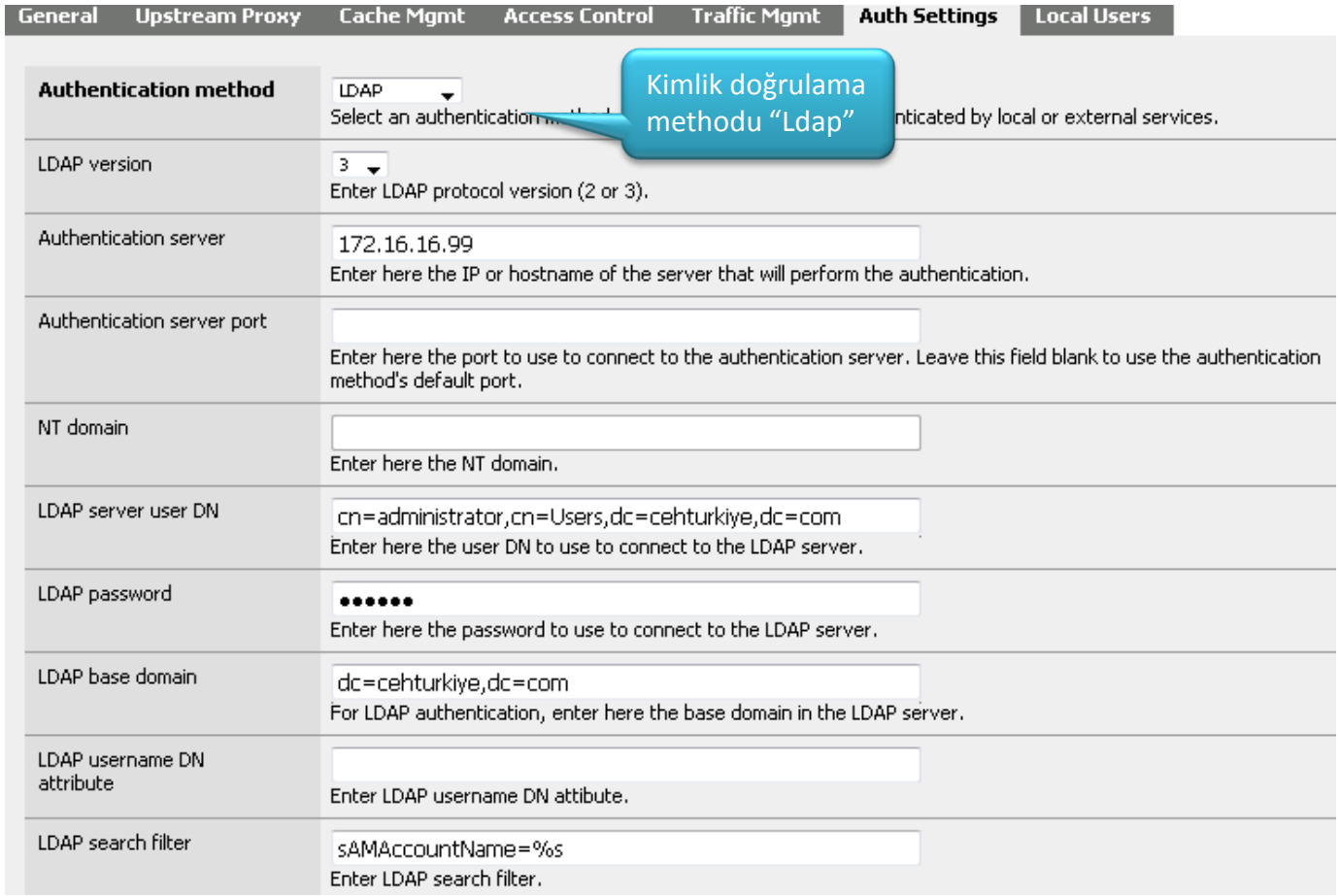
LDAP password: (administrator hesabının parolası)

LDAP base domain: dc=domainadı,dc=com

LDAP search filter: sAMAccountName=%s

Bölüm 25:
Squid | Kimlik Doğrulama | Ldap

Ldap ile uzak bir sistemden kimlik doğrulama yapar. Örnek: Microsoft Active Directory

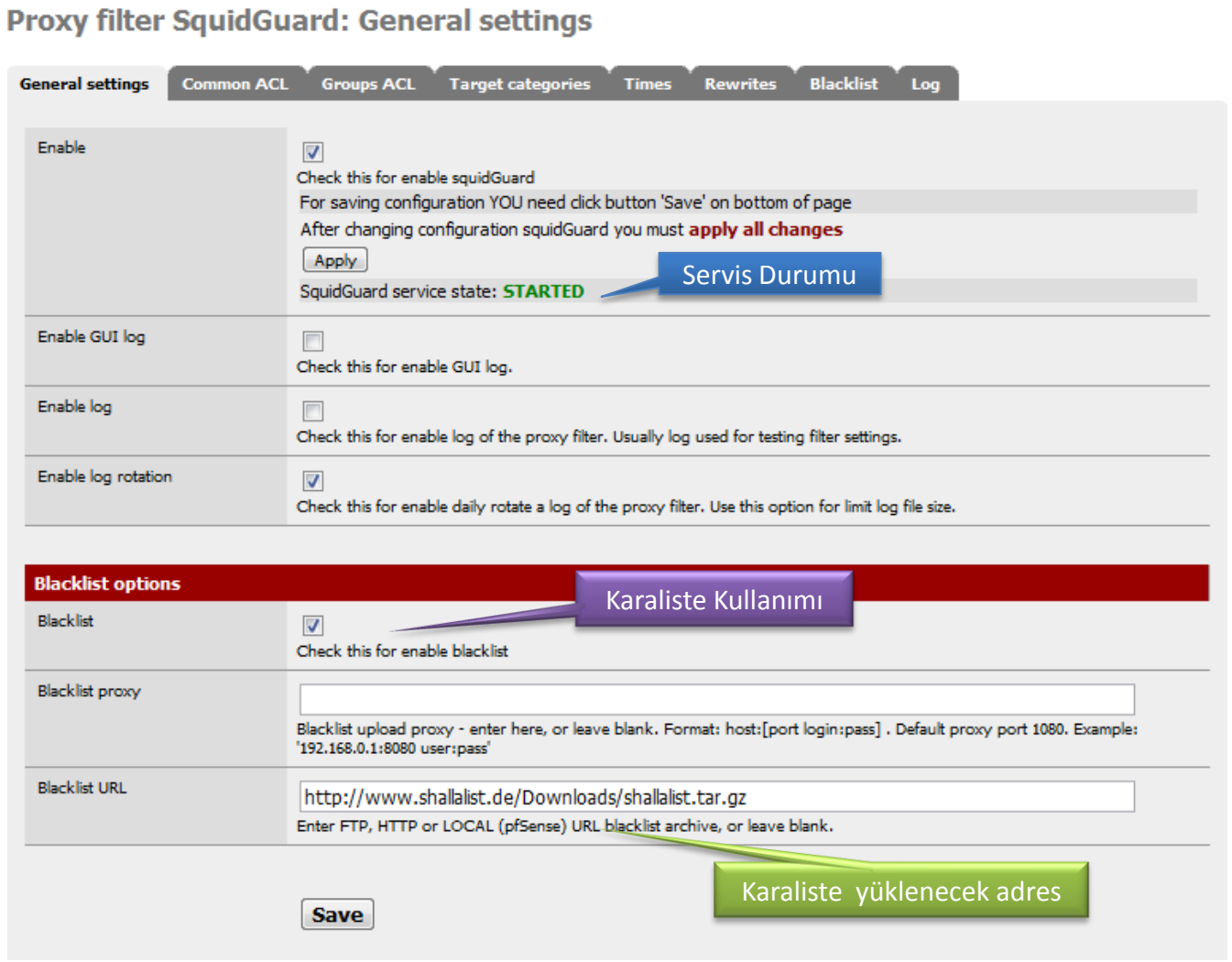


Bölüm 26:
SquidGuard

Yüksek performanslı URL Filter yazılımı. Squid e yardımcı servis.

- Genel Ayarlar
- Karaliste Güncelleme
- Kullanıcı ve Grup Bazlı URL Filtreleme
- Uzantı ve kelime bazlı kural tanımlama
- Zaman bazlı erişim kuralları tanımlama
- squidGuard kayıtlarının yorumlanması

Bölüm 26:
SquidGuard

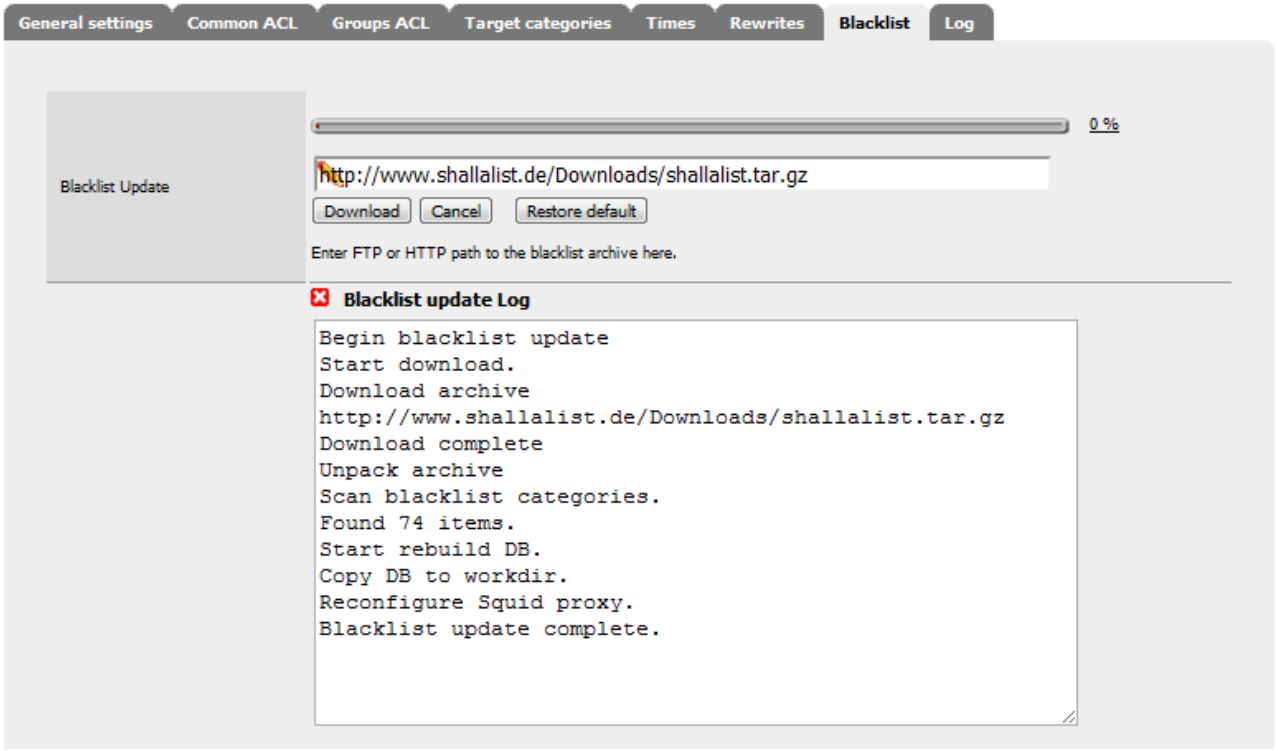


Bölüm 26:
SquidGuard | Karaliste

Sık güncellenen karaliste adresleri;

http://www.shallalist.de/

http://urlblacklist.com/



Bölüm 26:
SquidGuard | Karaliste

Yüklenen karaliste, ACL sayfalarında “Target Rules Lists” başlığı altında yer alır. İlerleyen konularda uygulamalı olarak ele alınacaktır.

Whitelist: Her durumda belirtilen kategorideki adreslere erişim serbest.Deny kuralına baskın gelir.

Deny: Belirilen kategorideki adreslere erişimi engelle. Allow kuralına baskın gelir.

Allow: Seçili kategoriye erişime izin ver. Default kuralına baskın gelir.

Bölüm 26:
SquidGuard | Hedef Kategori Ekleme

Karaliste dışında, istenilen url, domain veya bir düzenli ifadeye göre kategori oluşturulabilir. Bu kategoriler, istenilen acl tanımında kullanılır.

>> Proxy filter SquidGuard: Target categories: Edit

Domains list : Domain adresleri tanımlanır.

Örnek; 'mail.google.com yahoo.com 192.168.1.1'

Expressions: İfadeler. İfadeler pipe | işareti ile ayrılır.
Örnek; 'hack|sex|oyun|\.exe|\.tar.gz|\.php'

URLs list: URL adresleri tanımlanır.
Örnek; 'host.com/xxx 12.10.220.125/alisa'

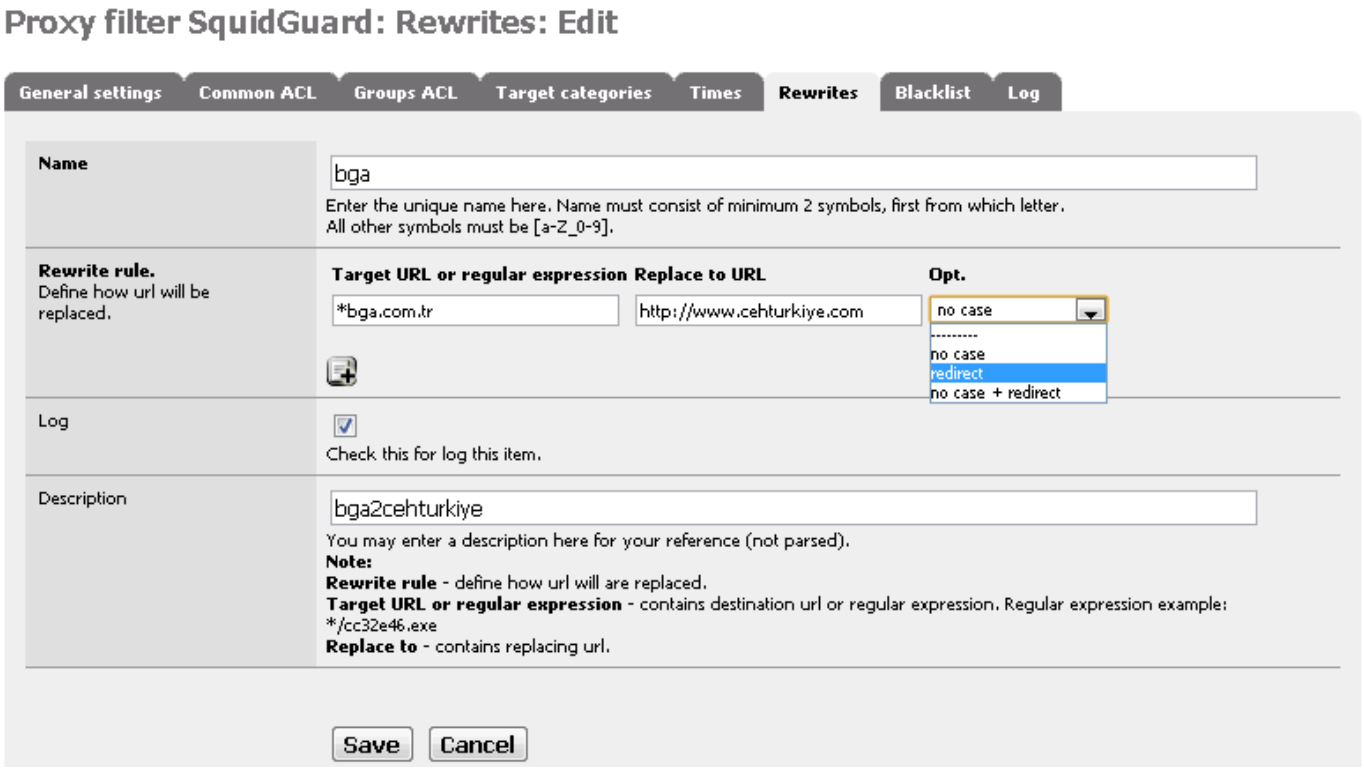
Redirect mode: Kurala uygun bir erişim olduğunda, istemcinin yönlendirme türü.
Örnek; "Bu sayfaya erişimiz engellenmiştir" gibi gibi

Bölüm 26:
SquidGuard | Hedef Kategori Ekleme

Bölüm 26:
SquidGuard | Yeniden Yönlendirme

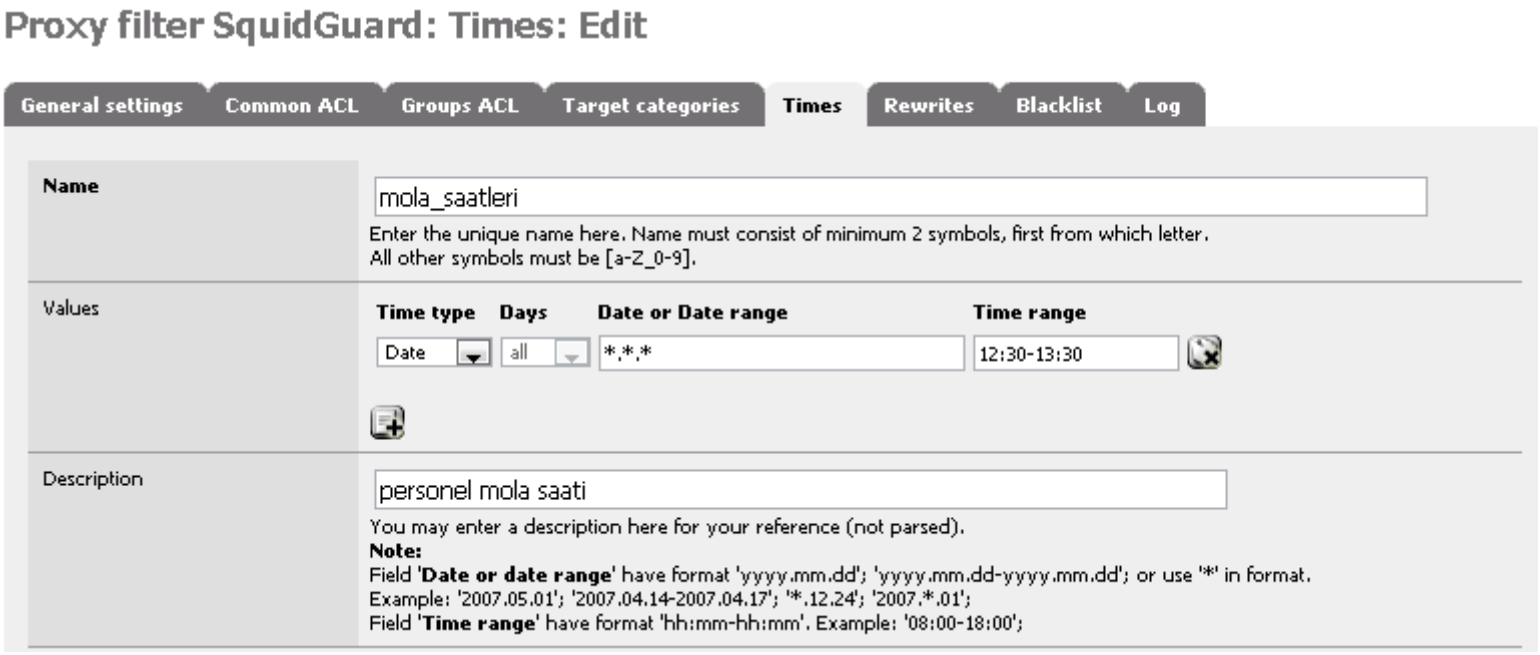
URL adresinde geçen bir ifadeyi dönüşürmek için kullanılır.

Örneğin: bga.com.tr adresine erişilmek istendiğinde cehturkiye.com olarak değiştir.



Bölüm 26:
SquidGuard | Zaman Tanımları

Oluşturulan zaman tanımları, kurallarda zamana göre filtreleme yapmak için kullanılır.



Bölüm 26:
SquidGuard | Genel ACL

“Common ACL” seçenekleri ;

Target Rules: Karalisteden seçilen hedef kategoriler.

Not to allow IP addresses in URL: URL adresi olarak bir IP adresine bağlanılmak isteniliyorsa erişime izin verme. Genelde URL filreleme servislerini atlatmak için kullanılır. http:/google.com yasaklı bir siteyse, google.com adresinin ip adresi http://74.125.87.104 yazılarak google adresine erişim kurulabilir. Dikkatli kullanılmalıdır!

Redirect mode: Erişim kısıtlandığında istemciyi yönlendirme şeklidir.

Redirect info: Yönlendirme şekline göre yazılması gereken mesaj veya url adresi

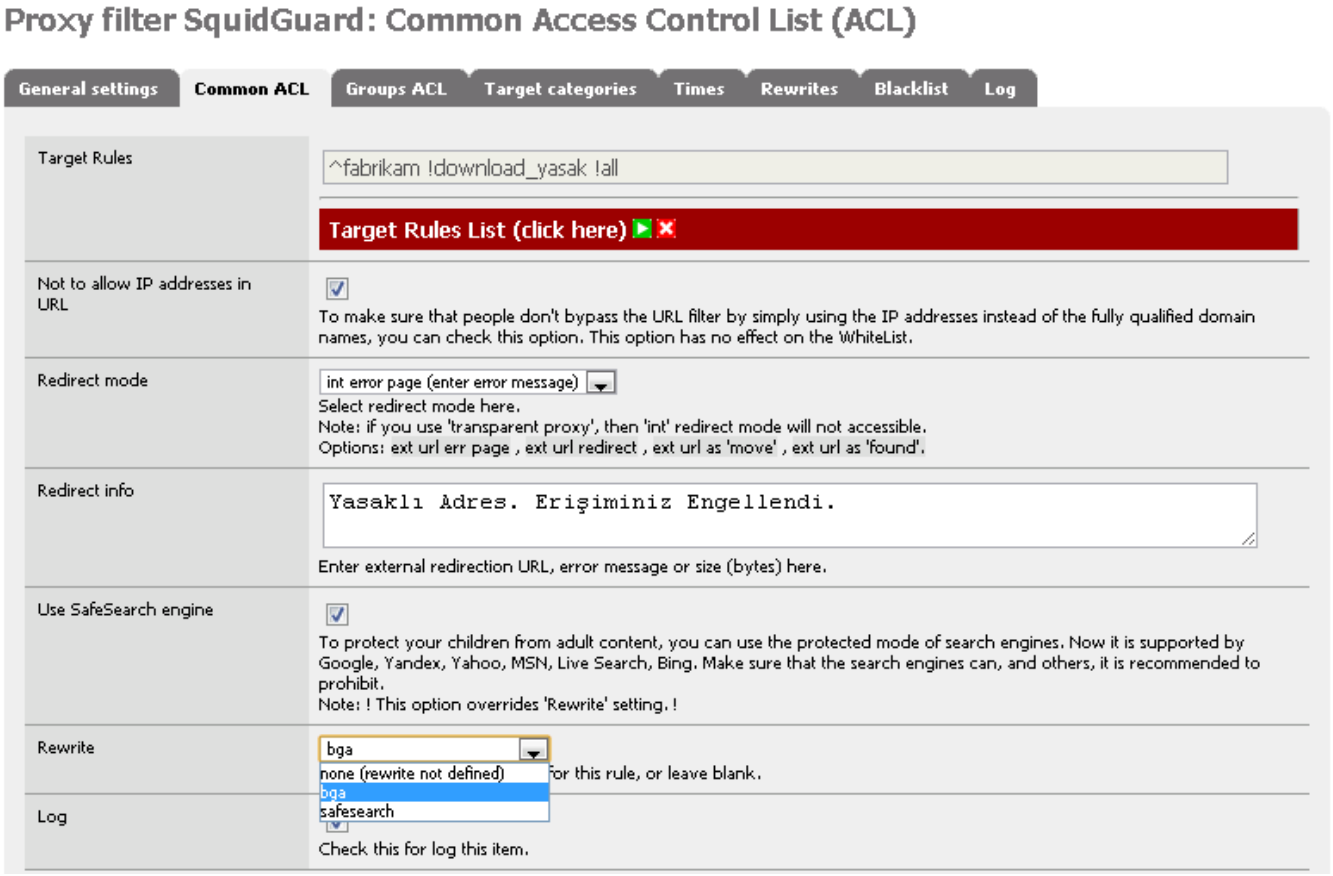
SafeSearch engine: Arama motorlarının güvenli arama özelliğini aktif eder.Örneğin, google.com adresinde porn kelimesi aratıldığında yüzlerce adres ve resim çıkmaktadır. Güvenli arama motoru etkinleştirildiğinde bu aramanın sonucunu google.com listelemeyecektir.

Rewrite: Yeniden yönlendirme hedefini bu kurala dahil et.

Log: Bu kural için kayıt tut.

Bölüm 26:
SquidGuard | Genel ACL

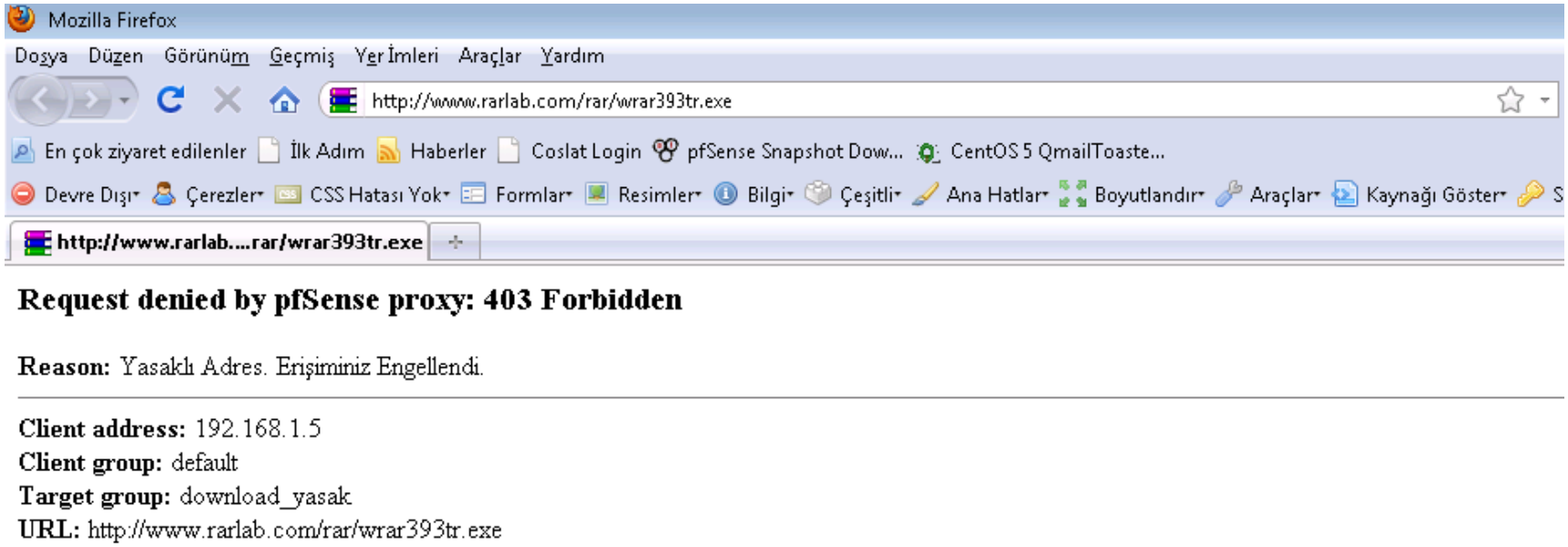
Herhangi bir kuralda tanımlı olmayan tüm kullanıcılara diğer bir deyişle varsayılan kullanıcılara “Common ACL” kuralları uygulanır.



Bölüm 26:
SquidGuard | Genel ACL | Test

Ön tanımlı tüm istemcilere “download_yasak” kuralı uygulanacakır. \.exe uzantılı bir adrese erişmek istenildiğinde, yönlendirme bilgisi olarak belirttiğimiz içerik çıkacaktır.

192.168.1.5 ip adresi, http://www.rarlab.com/rar/wrar393tr.exe url adresine erişmek istediğinde “download_yasak” hedefine göre erişimi engellendi ve ”Yasalı Adres. Erişiminiz Engellendi” mesajımız ile cevap verildi ☺



Bölüm 26:
SquidGuard | Kullanıcı/Grup Bazlı ACL

Kullanıcı ve guruplara ayrıcalıklı kurallar uygulamak için kullanılır.

Seçenekler;

Disabled: Kuralı devre dışı bırakır. Kuralı silmez, daha sonra tekrar kullanılabilir.

Name: Kural adı.

Order: Sıra. Mevcut kuralı diğer kuralların altına-üsüne taşımak için kullanılır.

Client (source): Kuralın uygulanacağı kaynak adres(ler). Örnek; IP Adresi : 10.0.0.1 yada Subnet: 10.0.0.0/24 yada ip aralığı: 192.168.1.1-192.168.1.50 yada kullanıcı adı: 'isim1'

Time: Kuralın geçerli olacağı zaman aralığı.

Target Rules: Karalisteden seçili hedef kategoriler.

Not to allow IP addresses in URL: URL adresi olarak bir IP adresine bağlanılmak isteniliyorsa erişime izin verme. Genelde URL filreleme servislerini atlatmak için kullanılır. http:/google.com yasaklı bir siteyse, google.com adresinin ip adresi http://74.125.87.104 yazılarak google adresine erişim kurulabilir. Dikkatli kullanılmalıdır!

Bölüm 26:
SquidGuard | Kullanıcı/Grup Bazlı ACL II

Redirect mode: Erişim kısıtlandığında istemciyi yönlendirme şeklidir.

Redirect info: Yönlendirme şekline göre yazılması gereken mesaj veya url adresi

SafeSearch engine: Arama motorlarının güvenli arama özelliğini aktif eder.Örneğin, google.com adresinde porn kelimesi aratıldığında yüzlerce adres ve resim çıkmaktadır. Güvenli arama motoru etkinleştirildiğinde bu aramanın sonucunu google.com listelemeyecektir.

Rewrite: Yeniden yönlendirme hedefini bu kurala dahil et.

Log: Bu kural için kayıt tut

Bölüm 26:
SquidGuard | Kullanıcı/Grup Bazlı ACL | Senaryo

Senaryo 1: Firmamın “Yönetim Birimi” var. IP aralığı 192.168.1.1-192.168.10. Bu ip aralığına herzaman herşey serbest sadece zaralı içerikli siteler yasak (hacking gibi)

Senaryo 2: Sunucu adreslerim 192.168.1.88, 192.168.1.33, 192.168.1.56. Sunucularıma herzaman herşey yasak.Yalnızca microsoft.com domainleri izinli.

Senaryo 3: Üretim grubu (192.168.1.100-192.168.1.200) yalnızca mola saatlerinde (12:30-13:30) internete çıkabilsinler bu saatler dışı herşey yasak.

Senaryo 4: Sistemimde kimlik doğrulama yapıyorum. “ozan” kullanıcı ile giriş yaptığımda herzaman herşey izinli olsun.

Bölüm 26:
SquidGuard | Kullanıcı/Grup Bazlı ACL | Senaryo

Name: uretim

Client (source): 192.168.1.100-192.168.1.200

Time: mola_saaleri

Target rules: Hedef kural setinde iki farklı alanda işlem yapmalıyız;

Target Categories: mola_saatleri geldiğinde geçerli olacak kurallar. Herşey izinli olsun istiyoruz, hacking,porn kategorileri yasak.

Target Categories for off-time: mola_saaleri dışında geçerli olacak kurallar. Herşey yasak = Default: Deny

Redirect: Mesai saatlerinde internet yasak !

Log: Kayıt tutulsun.

Bölüm 26:
SquidGuard | Kayıtların Yorumlanması

General settings | Common ACL | Groups ACL | Target categories | Times | Rewrites | Blacklist | Log

| **Blocked** | Filter GUI log | Filter log | Proxy config | Filter config |

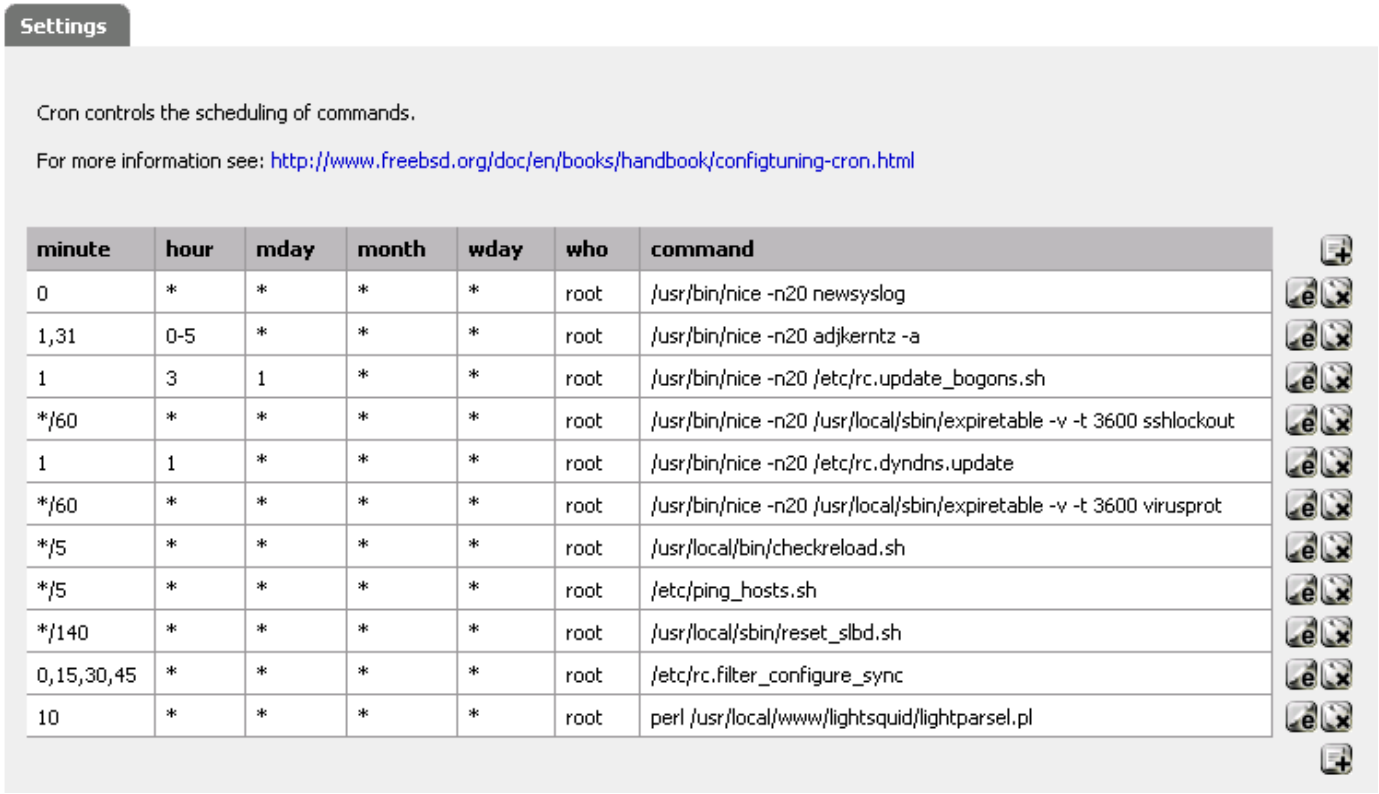
Show top 50 entries. List from the line: << 0 >>			
14.03.2011 01:14:35	192.168.1.101/-	http://www.facebook.com/	Request(uretim/none/-) - GET REDIRECT
14.03.2011 01:14:33	192.168.1.101/-	http://www.facebook.com/	Request(uretim/none/-) - GET REDIRECT
14.03.2011 01:14:33	192.168.1.101/-	http://www.facebook.com/favicon.ico	Request(uretim/none/-) - GET REDIRECT
14.03.2011 01:14:30	192.168.1.101/-	http://www.facebook.com/favicon.ico	Request(uretim/none/-) - GET REDIRECT
14.03.2011 01:14:30	192.168.1.101/-	http://www.facebook.com/favicon.ico	Request(uretim/none/-) - GET REDIRECT
14.03.2011 01:14:30	192.168.1.101/-	http://www.facebook.com/	Request(uretim/none/-) - GET REDIRECT
14.03.2011 01:13:54	192.168.1.101/-	http://www.yahoo.com/favicon.ico	Request(uretim/none/-) - GET REDIRECT
14.03.2011 01:13:51	192.168.1.101/-	http://www.yahoo.com/favicon.ico	Request(uretim/none/-) - GET REDIRECT
14.03.2011 01:13:51	192.168.1.101/-	http://www.yahoo.com/favicon.ico	Request(uretim/none/-) - GET REDIRECT
14.03.2011 01:13:51	192.168.1.101/-	http://www.yahoo.com/	Request(uretim/none/-) - GET REDIRECT
14.03.2011 01:11:18	192.168.1.101/-	http://www.google.com.tr/search?hl=tr&safe=active&q=pll&aq=f&aqi=&aql=&oq=	Request(uretim/none/-) - GET REDIRECT

Bölüm 27:
Cron

CRON, linux ve *BSD sistemlerde zamanlanmış görev tanımları oluşturmamızı sağlar. Planlanmış bir işin belirli zaman aralıklarında çalışması için cron servisine görev eklenebilir.

Cron yönetimi için “System | Packages” sayfasından “Cron” paketi kurularak web arabirimi ile cron görevlerinin yönetimini sağlayabiliriz.

Bölüm 27:
Cron Görevleri



Settings

Cron controls the scheduling of commands.

For more information see: http://www.freebsd.org/doc/en/books/handbook/configtuning-cron.html

minute	hour	mday	month	wday	who	command
0	*	*	*	*	root	/usr/bin/nice -n20 newsyslog
1,31	0-5	*	*	*	root	/usr/bin/nice -n20 adjkerntz -a
1	3	1	*	*	root	/usr/bin/nice -n20 /etc/rc.update_bogons.sh
*/60	*	*	*	*	root	/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600 sshlockout
1	1	*	*	*	root	/usr/bin/nice -n20 /etc/rc.dyndns.update
*/60	*	*	*	*	root	/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600 virusprot
*/5	*	*	*	*	root	/usr/local/bin/checkreload.sh
*/5	*	*	*	*	root	/etc/ping_hosts.sh
*/140	*	*	*	*	root	/usr/local/sbin/reset_slbd.sh
0,15,30,45	*	*	*	*	root	/etc/rc.filter_configure_sync
10	*	*	*	*	root	perl /usr/local/www/lightsquid/lightparsel.pl

- Cron'u düzenle
- Cron'u sil
- Yeni cron tanımı ekle

Bölüm 27:
Cron Görevleri

Alan Adı	İzin Verilen Değerler
Minute (dakika)	0-59
Hour (saat)	0-23
Day of month (ayın günü)	1-31
Month (ay)	1-12
Day of week (haftanın günleri)	0-7 (pazar günü için 0)
Yıldız (*) ile işaretlenmiş bir alan baştan sona (=hepsi) anlamına gelir.	

Bölüm 28:
BandwidhD

TCP, UDP, ICMP Trafiğinin İzlenmesi

Programmed by David Hinkle, Commissioned by DerbyTech wireless networking.

- Daily -- Weekly -- Monthly -- Yearly -

Pick a Subnet:
- Top20 -- 192.168.1.0 -

Top 20 IPs by Traffic - Daily

Ip and Name	Total	Total Sent	Total Received	FTP	HTTP	P2P	TCP	UDP	ICMP
Total	12.6G	671.7M	12.0G	67.6K	12.2G	8.7M	12.6G	52.7M	77.6K
192.168.1.168	7.1G	177.5M	7.0G	0	7.1G	763.4K	7.1G	18.7M	2.2K
192.168.1.89	1.2G	33.5M	1.2G	0	1.2G	0	1.2G	343.7K	0
192.168.1.60	508.2M	24.0M	484.2M	0	483.5M	37.5K	507.2M	1.1M	2.7K
192.168.1.116	488.3M	15.5M	472.8M	0	487.2M	262.8K	488.1M	240.7K	0
192.168.1.120	297.9M	14.0M	283.9M	0	286.9M	233.4K	297.4M	530.3K	192
192.168.1.67	281.6M	11.3M	270.3M	0	281.2M	7.0K	281.5M	163.1K	0
192.168.1.51	264.4M	20.1M	244.3M	0	260.8M	379.5K	261.9M	2.5M	228
192.168.1.102	229.5M	20.0M	209.5M	0	227.3M	89.6K	229.3M	202.0K	162

Bölüm 29:
IMSpector

System > Packages > IMSpector

MSN live 2011 destekli sürüm için güncelleme;

#fetch http://ozanucar.com/imspector2011.tar.gz

#tar zxvf imspector2011.tar.gz -C /

#/usr/local/sbin/imspector -c /usr/local/etc/imspector/imspector.conf –D

```
# /usr/local/sbin/imspector -c /usr/local/etc/imspector/imspector.conf -d
imspector: Protocol Plugin name: Gadu-Gadu IMSpector protocol plugin
imspector: Protocol Plugin name: Jabber IMSpector protocol plugin
imspector: Protocol Plugin name: MSN IMSpector protocol plugin
imspector: Protocol Plugin name: Yahoo IMSpector protocol plugin
imspector: ACL: List /usr/local/etc/imspector/acl.txt size: 5
imspector: ACL: Action: Allow
imspector: ACL: Local: ozan@bosgezen.com
imspector: ACL: Action: Allow
imspector: ACL: Local: kbulru@hotmail.com
imspector: ACL: Remote: ozan@bosgezen.com
imspector: ACL: Action: Allow
imspector: ACL: Local: admin@fabrikam.com
imspector: ACL: Action: Allow
imspector: ACL: Local: all
imspector: ACL: Remote: support@fabrikam.com
imspector: ACL: Action: Deny
imspector: ACL: Local: all
imspector: Filter Plugin name: ACL IMSpector filter plugin
imspector: Bad-words: Loaded 86 bad-words, replacing with '*' and blocking at 1
imspector: Filter Plugin name: Bad-words IMSpector filter plugin
imspector: Misc: Blocking all file transfers
imspector: Filter Plugin name: Misc IMSpector filter plugin
imspector: Non-HTTP port listening on 0.0.0.0:16667
```

Bölüm 30:
Yedekleme ve Kurtarma

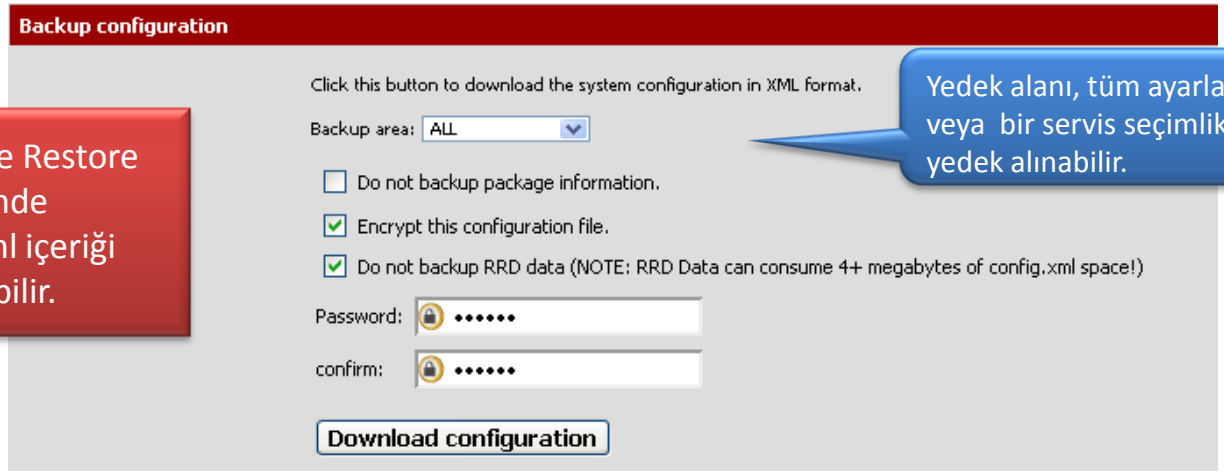
pfSense tüm ayarlarını tek bir XML dosyasında tutar.

Ayar dosyasını yedeklemek için;
Diagnostics > Backup/Restore, ve “**Download Configuration**”

Ayarları geri yüklemek için;
“Restore configuration” browse ayar dosyası

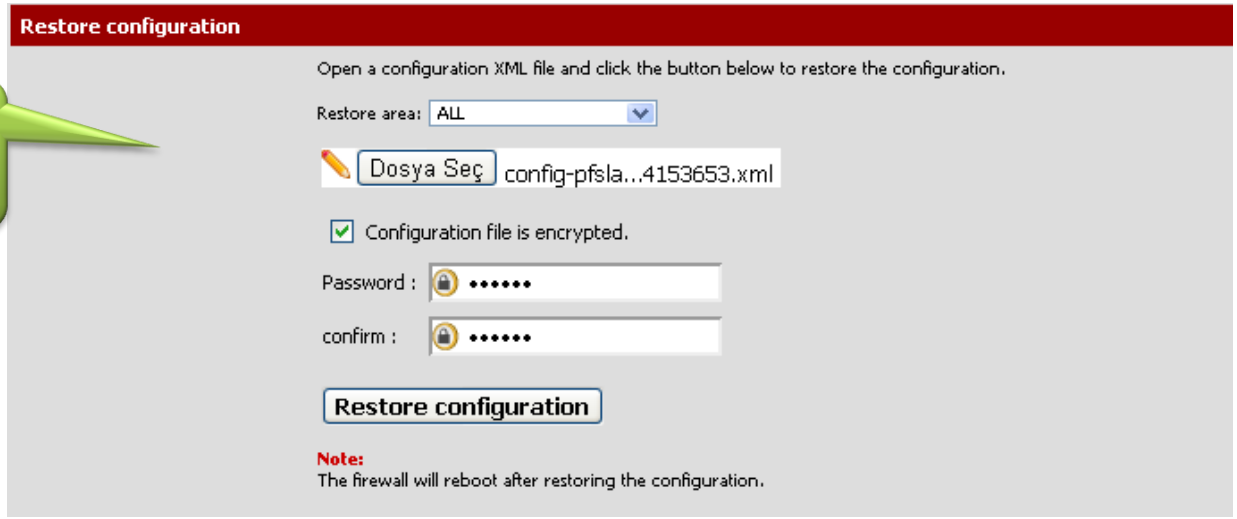
Bölüm 30:
Yedekleme ve Kurtarma

Backup ve Restore işlemlerinde config.xml içeriği şifrelenebilir.



Yedek alanı, tüm ayarlar veya bir servis seçimlik yedek alınabilir.

Geri yükleme alanı, config.xml yedek dosyası bu alandan yüklenir.



Bölüm 31:
5651 Sayılı Kanun

İnternet toplu kullanım sağlayıcılarının yükümlülükleri
MADDE 4 – (1) İnternet toplu kullanım sağlayıcılarının yükümlülükleri şunlardır:
a) Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak.
b) İç IP Dağıtım Loglarını elektronik ortamda kendi sistemlerine kaydetmek.

Erişim sağlayıcının yükümlülükleri
MADDE 15 – (1) Erişim sağlayıcı;
b) Sağladığı hizmetlere ilişkin olarak, Başkanlığın Kanunla verilen görevlerini yerine getirebilmesi için; erişim sağlayıcı trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini (hash) zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle…

Yer sağlayıcının yükümlülükleri
MADDE 16 – (1) Yer sağlayıcı;
c) Yer sağlayıcı trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini (hash) zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle…

Bölüm 31:
5651 Sayılı Kanun

Referanslar:

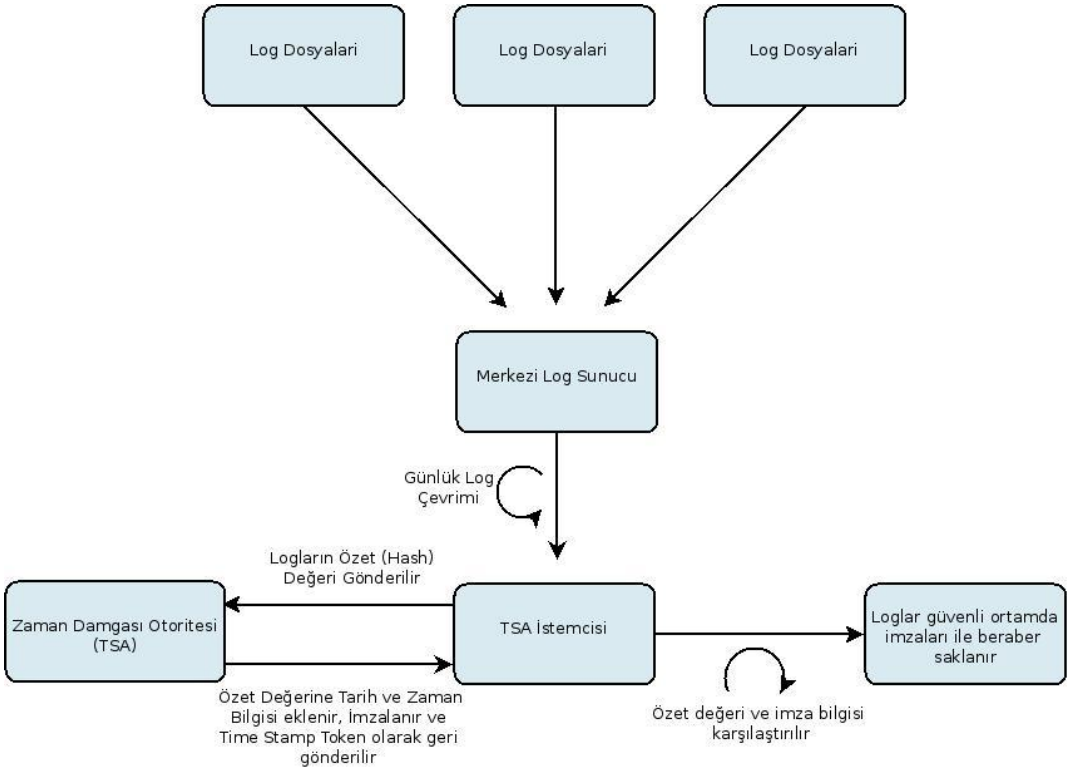
- T.C.K. 5070: “Elektronik İmza Kanunu”
- 5070 sayılı Elektronik İmza Kanunu” uyarınca yayımlanan “Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik”
- 5070 sayılı Elektronik İmza Kanunu” uyarınca yayımlanan “Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ”

Bölüm 31:
Zaman Damgası Standartlar

RFC 3161 uyumlu zaman damgası, OpenSSL ve OpenTSA yazılımları.

Bölüm 31:
Zaman Damgası

Zaman damgası, elektronik ortamda log, doküman ve sözleşme gibi elektronik verilerin, belirli bir zamandan önce var olduğunu kanıtlamak için kullanılır. Mesela bir log dosyasının, kayıt altına alındıgı tarihte orjinal haliyle var oldugunu, sonradan değiştirilmediğini ispatlamak amacıyla zaman damgasından yararlanılabilir.



Bölüm 31:
Yetkili Sertifika Otoriteleri

- Tubitak KamuSM
- Turktrust
- Globalsing

Bölüm 31:
Sniffing

Dinlediği ağ arabirimden giden-gelen trafiği anlık olarak parse eder. RFC standartlarına uygun tüm protocolleri destekler.

http://www.wireshark.org/docs/dfref/

Bölüm 31:
HTTP Sniffing

- HTTP Başlık bilgileri,istediğimiz HTTP kayıt türü;

Paketin zaman bilgisi = -e frame.time

Kaynak IP adresi = -e ip.src

Kaynak MAC adresi = -e eth.src

Hedef IP adresi = -e ip.dst

Hedef PORT numarası= -e tcp.dstport

HTTP HOST adresi = -e http.host

İstenilen URL= -e http.request.uri

HTTP Method = -e http.request.method

Ve bunların arasına birer boşluk bırakarak yaz = -E separator=’ ‘

Komut: tshark -nn -i eth0 not arp and port not 53 -d tcp.port==3128,http -R http.request –T fields -e frame.time -e ip.src -e eth.src -e ip.dst -e tcp.dstport -e http.host –e http.request.uri -e http.request.method -E separator=’ ‘

Bölüm 31:
HTTP Sniffing | Log

- HTTP Başlık bilgileri,istediğimiz HTTP kayıt türü;

Oct 11, 2010 15:15:16.111690000 192.168.5.205 aa:00:04:00:0a:04 188.124.8.106 80 www.cehturkiye.com /wp-content/themes/monochrome/comment-style.css GET

Bölüm 31:
FTP Sniffing

- FTP Başlık bilgileri,istediğimiz FTP kayıt türü;

Paketin oluşturma zamanı = -e frame.time

Kaynak IP adresi = -e ip.src

Kaynak MAC adresi = -e eth.src

Kaynak Port numarası = -e tcp.srcport

Hedef IP adresi= -e ip.dst

Hedef Port Numarası= -e tcp.dstport

FTP Komutu -e ftp.request.command -e ftp.request.arg

Yanıt Kodu(başarılı mı değil mi ?) = -e ftp.response.code -e ftp.response.arg

Ve araya bir boşluk bırakarak yaz -E separator=’ ‘

Komut: tshark -nn -i eth0 not arp and port not 53 -R ftp -T fields -e frame.time_relative -e ip.src -e eth.src -e tcp.srcport -e ip.dst -e tcp.dstport -e ftp.request.command -e ftp.request.arg -e ftp.response.code -e ftp.response.arg -E separator=’ ‘

Bölüm 31:
FTP Sniffing | Log

- FTP Başlık bilgileri,istediğimiz FTP kayıt türü;

5.464582000 89.19.25.155 00:11:bb:e0:7b:10 21 192.168.5.205 38023 220 FileZilla Server version 0.9.24 beta
5.464808000 192.168.5.205 aa:00:04:00:0a:04 38023 89.19.25.155 21 USER 123test123
5.478353000 89.19.25.155 00:11:bb:e0:7b:10 21 192.168.5.205 38023 331 Password required forozanucar.com
5.478738000 192.168.5.205 aa:00:04:00:0a:04 38023 89.19.25.155 21 PASS testtestest
5.491656000 89.19.25.155 00:11:bb:e0:7b:10 21 192.168.5.205 38023 230 Logged on
5.493490000 192.168.5.205 aa:00:04:00:0a:04 38023 89.19.25.155 21 PWD
5.506212000 89.19.25.155 00:11:bb:e0:7b:10 21 192.168.5.205 38023 257 \"/\" is current director
29.259827000 192.168.5.205 aa:00:04:00:0a:04 38026 89.19.25.155 21 PWD
29.272723000 89.19.25.155 00:11:bb:e0:7b:10 21 192.168.5.205 38026 257 \"/www\" is current directory.
29.273288000 192.168.5.205 aa:00:04:00:0a:04 38026 89.19.25.155 21 TYPE I
29.286747000 89.19.25.155 00:11:bb:e0:7b:10 21 192.168.5.205 38026 200 Type set to I
29.287069000 192.168.5.205 aa:00:04:00:0a:04 38026 89.19.25.155 21 PASV

Bölüm 31:
DHCP Sniffing

- DHCP Başlık bilgileri,istediğimiz DHCP kayıt türü;

Komut: tshark -i eth0 port not 53 -R bootp -T fields -e bootp.ip.client -e bootp.hw.mac_addr -e bootp.ip.you

Script, http://www.cehturkiye.com/tshark-http-ftp-dhcp.sh.txt

Bölüm 31:
5651 İmzalayıcı

/usr/local/ssl-1/imzaci/imzaci.sh

14 Oct 08:41:54 ntpdate[6615]: step time server 194.27.222.5 offset 0.847240 sec

Using configuration from /usr/local/ssl-1/openssl.cnf

Response has been generated.

Dogrulama tamam.

a 5651url.sign

a 5651url.sign.der

a 5651url.sign.tsq

…..

…..

Bölüm 32:
Geliştiriciler için pfSense

/usr/local/www	Web Dizini
/cf/conf/config.xml	Ayarların tutulduğu dosya
/usr/local/etc/rc.d/	Paketler ait servis ve ayar betikleri
/etc/inc/	*.inc dosyaları config.xml parser'ları
/etc/rc.d	Sistem servisleri
/usr/local/captiveportal	Captiveportal sayfaları
/usr/local/pkg/	Kurulu paketlere ait dosyalar.
/etc/inc/config.inc	pfsense ayar dosyası

Bölüm 32:
Geliştiriciler için pfSense | config.xml

pfSense tarafından tüm ayarlar (sistem ayarları, paket bilgileri vb.) config.xml dosyasında tutuluyor. Sistem açılışında bu xml dosyası parse edilip bellekte Arrey olarak tutuluyor. Bu array üzerinde işlem yaparak ayarlar değiştirilebilir.

Örnek config.xml anahtarları;

```
</interfaces>
    <staticroutes/>
    <dhcpd>
        <lan>
            <range>
                <from>192.168.1.100</from>
                <to>192.168.1.199</to>
            </range>
        </lan>
    </dhcpd>
```

Bölüm 32:
Geliştiriciler için pfSense | config.xml

Örnek bir uygulama;

Lan ağ arabirimini ve ip adresini al ardından diğer interface bilgilerini dizi olarak göster.

```
<?
include("config.inc");
$lanif=$config['interfaces']['lan']['if'];
$lanip=$config['interfaces']['lan']['ipaddr'];

print $lanif . $lanip;
echo "<br/>";

foreach($config['interfaces'] as $k=>$val){
        print "$k adresi :" . $val['ipaddr'] . "<br />";
}

?>
```

Bölüm 32:
Özelleştirilebilir Güvenlik Duvarı Oluşturmak

Neden Özelleştirme ?

pfSense alt yapısını kullanarak kendi firewall sisteminizi oluşturabilirsiniz ?

pfSense kurulumuna ek programlar, uygulamalar entegre etmek isteyebilirsiniz.

Hata, driver vb. sorunlar için yama uygulamak isteyebilirsiniz.

Geliştirdiğiniz yazılımları eklemek isteyebilirsiniz.

Özelleştirilmiş konfigurasyon yüklü kurulum oluşturabilirsiniz.

…..

Bölüm 32:
Özelleştirilebilir Güvenlik Duvarı Oluşturmak

Kurulum

FreeBSD 7.2, eğer 2.0 oluşturmak istiyorsak FreeBSD 8.0 kurulumu yapmalıyız.

1.Kabuk komutlarını çalıştırarak başlayalım

echo "WITHOUT_X11=yo" >> /etc/make.conf

echo "BATCH=yo" >> /etc/make.conf

mkdir -p /home/pfsense/pfSenseGITREPO /home/pfsense/installer /usr/pfSensesrc

2.Port ağacını indir ve GIT kur

portsnap fetch extract

cd /usr/ports/textproc/expat2 && make depends install

cd /usr/ports/devel/git && make depends install

cd /usr/ports/sysutils/fastest_cvsup/ && make depends install

rehash

Bölüm 32:
Özelleştirilebilir Güvenlik Duvarı Oluşturmak

3.GIT Reposunu temin ederek devam edelim

cd /home/pfsense && git clone http://gitweb.pfsense.org/pfsense-tools/mainline.git tools

cd /home/pfsense && git clone http://gitweb.pfsense.org/freesbie2/mainline.git freesbie2

cd /home/pfsense/tools/builder_scripts && chmod a+rx *.sh

4.Bazı portlar /usr/src içinde kaynak koda ihtiyaç duyuyor

csup -h `fastest_cvsup -c tld -q` /usr/share/examples/cvsup/standard-supfile

5.Yeni menü sistemini çalıştıralım

cd /home/pfsense/tools/builder_scripts

./menu.sh

Bölüm 32:
Özelleştirilebilir Güvenlik Duvarı Oluşturmak

6.Daha sonra menü sisteminden oluşurmak istediğiniz versiyonu seçin

Kullanılabilir versiyonlar aşağıdaki gibidir:

RELENG_1_2	**pfSense RELENG_1_2 + FreeBSD RELENG_7_2**
RELENG_2_0	pfSense HEAD (2.0) + FreeBSD RELENG_7_2
RELENG_7_2	pfSense RELENG_1_2 + FreeBSD RELENG_7_2
RELENG_8_0	pfSense HEAD + FreeBSD 8-CURRENT

Test aşaması

pfSense.iso dosyası /usr/obj.pfSense dizini altına oluşurulur. Kurulum dosyasını test edebilirsiniz.