

Linux Yaz Kampı 2012

pfSense 2.0 Eğitimi

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

Eğitim Hakkında

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

Katılımcıların networking konusunda temel seviyede bilgili oldukları varsayılmaktadır.

Amaçlar

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

Bölüm 1 - Giriş

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

Bölüm 2 - pfSense Kurulumu

- Donanım Seçimi
- Minimum Donanım Gereksinimleri
- Full Kurulum

Bölüm 3 - Temel Yapılandırma

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

Bölüm 4 - Temel Servisler

- DHCP Server Yapılandırması
- DNS Forwarder
- Dynamic DNS

Bölüm 5 - Firewall

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

Bölüm 6 - NAT

- Port Yönlendirme
- 1:1 NAT
- Outbound NAT

Bölüm 7 - VPN

- pfSense VPN Desteği
- OpenVPN Servisi
- Pptp VPN Servisi

Bölüm 8 - Load Balancing & Failover

- Multiple WAN - Load Balancing
- Multiple WAN - Failover

Bölüm 9 - Diğer Servisler

- Paket Sistemi
- OpenNTPD
- SNMP
- Wake On LAN

Bölüm 10 - Bakım ve Monitoring

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

BÖLÜM 1

GİRİŞ

NEDİR ?
NE DEĞİLDİR ?

OpenBSD Projesi

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

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

Proje altında OpenSSH, OpenNTP gibi alt projeler de geliştirilmektedir.

Bir çok ticari güvenlik ürününde OpenBSD bileşenleri kullanılmaktadır.

OpenBSD Packet Filter

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

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

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

pfSense Nedir ?

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

Tüm yapılandırma işlemi bir web arabirimi üzerinden gerçekleştirilebilmektedir.

Paket sistemi sayesinde bir çok farklı uygulamayı da desteklemektedir.

Neden pfSense ?

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

ÖZELLİKLER

FIREWALL

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

ÖZELLİKLER

DURUM TABLOSU

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

ÖZELLİKLER

Durum Tablosu Optimizasyon Seçenekleri

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

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

ÖZELLİKLER

Network Address Translation (NAT)

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

ÖZELLİKLER

YEDEKLİLİK

- **CARP**: OpenBSD'nin CARP desteği ile iki ya da daha fazla pfSense yedekli olarak çalıştırılabilir. Firewallardan birisi gittiği zaman diğeri aktif duruma geçerek görevi devralır. Ayrıca yapılandırmanın tüm yedek sunucularla senkronize edilmesi sağlanır.
- **pfsync**: Durum tablosunun, yedekli çalışmak üzere yapılandırılan tüm firewall'lara replike edilmesini sağlar.

ÖZELLİKLER

YÜK DENGEME

- **Outbound LB**: Birden fazla WAN bağlantısının eş zamanlı ortak ya da yedekli kullanılmasıdır. Kural bazlı olarak farklı ağ geçitleri seçilebilmesine olanak sağlar.
- **Inbound LB**: Gelen bağlantı isteklerini birden fazla sunucuya dağıtmak üzere kullanılır. Genellikle web ve mail servislerinde kullanılır.

ÖZELLİKLER

VPN SERVİSLERİ

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

ÖZELLİKLER

DHCP SERVER / DNS Forwarder

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

ÖZELLİKLER

Dynamic DNS

- Dinamik IP adresiniz değiştiğinde durumu DNS sunucuya bildirip DNS kaydınızın güncellenmesini sağlar.
- "DynDNS - DHS - DNSexit - DyNS - easyDNS - freeDNS
HE.net - Loopia - Namecheap - No-IP - ODS.org - OpenDNS - ZoneEdit" gibi Dinamik DNS servislerini destekler.

ÖZELLİKLER

CAPTIVE PORTAL

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

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

Genelde hot spot ağlarda kullanılır.

DESTEK

Dökümantasyon

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

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

Sorun Giderme Klavuzları

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

Eğitim Videoları

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

DESTEK

Mail Listeleri

pfSense Support listesi: support-subscribe@pfsense.com

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

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

Liste Arşivi:

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

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

<http://tinyurl.com/a3j3kp>

DESTEK

Forum Sayfası

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

IRC Kanalı

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

Ticari Destek

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

BÖLÜM 2

KURULUM

KURULUM

DONANIM SEÇİMİ

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

KURULUM

UYUMLULUK LİSTESİ

FreeBSD 8.1 (pfSense 2.0.1)

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

KURULUM

MINIMUM DONANIM GEREKSİNİMLERİ

CPU - 100 MHz Pentium

RAM - 128 MB

Live CD

CD-ROM drive

Ayarları saklamak için USB flash sürücü.

Sabit Diske Kurulum

CD-ROM, kurulum başlangıcı için

1 GB hard disk

Gömülü Sistemler

512 MB Compact Flash card

Yönetim için Seri port

KURULUM

FULL KURULUM

Symmetric Multiprocessing Kernel

Çok çekirdekli / çok işlemcili donanımları destekler

Embedded Kernel

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

Developer Kernel

Debug seçeneklerinin aktif edildiği geliştirici versiyonu.

BÖLÜM 3

TEMEL YAPILANDIRMA

TEMEL YAPILANDIRMA

Yönetim Arabirimleri

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

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

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

TEMEL YAPILANDIRMA

Konsol Arabirimi

```
FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.0.1-RELEASE-pfSense (amd64) on pfSense ***

  WAN (wan)                -> em0                -> NONE (DHCP)
  LAN (lan)                 -> em1                -> 192.168.1.1

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

Enter an option: █
```

TEMEL YAPILANDIRMA

Web Arabirimi

The screenshot displays the pfSense web interface. At the top is a navigation bar with the 'Sense' logo and menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The user is logged in as 'router.local'. The main content area is titled 'pfSense Dashboard' and contains four panels:

- System Information:** A table showing system details.

Name	router.local
Version	2.0-BETA1 built on Thu May 13 15:32:54 EDT 2010 FreeBSD 8.0-STABLE Update available. Click Here to view update.
Platform	nanobsd
NanoBSD Boot Slice	pfsense0 / ad0s1
CPU Type	Geode(TM) Integrated Processor by AMD PCS
Uptime	15 days, 20:28
Current date/time	Sun May 30 16:46:26 EDT 2010
DNS server(s)	8.8.8.8 8.8.4.4 4.2.2.1 4.2.2.2
Last config change	Mon May 24 19:01:24 EDT 2010
State table size	295/23000 Show states
- Firewall Logs:** A table with columns: Act, IF, Source, Destination, Prot.
- Interfaces:** A table showing network interfaces.

IF	IP Address	Speed
WAN	65.40.70.189	100baseTX <full-duplex>
LAN	192.168.1.1	100baseTX <full-duplex>
WIRELESS	192.168.2.1	autoselect mode 11g <hostap>
- Interface Statistics:** A table showing traffic statistics for WAN, LAN, and WIRELESS.

	WAN	LAN	WIRELESS
Packets In	101792660	62382029	22928878
Packets Out	101693852	62380169	22917407
Bytes In	82.39 GB	30.78 GB	25.67 GB
Bytes Out	32.08 GB	49.19 GB	7.07 GB
Errors In	0	0	30
Errors Out	0	0	9781
Collisions	0	0	0

TEMEL YAPILANDIRMA

System: General Setup



System

Hostname

pfSense

Name of the firewall host, without domain part
e.g. *firewall*

Domain

crom.lab

Do not use 'local' as a domain name. It will cause local hosts running mDNS (avahi, Bonjour, etc.) to be unable to resolve local hosts not running mDNS.
e.g. *mycorp.com, home, office, private, etc.*

DNS servers

DNS Server	Use gateway
8.8.8.8	WAN
8.8.4.4	WAN
	None
	None

Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS forwarder and for PPTP VPN clients.

In addition, optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.

☒ **Allow DNS server list to be overridden by DHCP/PPP on WAN**
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). However, they will not be assigned to DHCP and PPTP VPN clients.

☐ **Do not use the DNS Forwarder as a DNS server for the firewall**
By default localhost (127.0.0.1) will be used as the first DNS server where the DNS forwarder is enabled, so system can use the DNS forwarder to perform lookups. Checking this box omits localhost from the list of DNS servers.

Time zone

Etc/UTC

Select the location closest to you

NTP time server

0.pfsense.pool.ntp.org

Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if you enter a host name here!

Theme

pfSense_ng

This will change the look and feel of pfSense.

Save

TEMEL YAPILANDIRMA

Ağ Arabirimlerinin Belirlenmesi

Arayüzler hem WebGui hem de Konsol üzerinden tanımlanabilir.

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

Interfaces: Assign network ports



Interface assignments | Interface Groups | Wireless | VLANs | QinQs | PPPs | GRE | GIF | Bridges | LAGG

Interface	Network port
WAN	em0 (08:00:27:96:90:fe) ▼
LAN	em1 (08:00:27:7f:2e:c9) ▼



TEMEL YAPILANDIRMA

Ağ Arayüz Ayarları

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

TEMEL YAPILANDIRMA

Ağ Arayüz Ayarları

- **Static IP Yapılandırması**

IP Adresi ve subnet mask değeri manual olarak atanır. WAN arabirimine sabit ip tanımlaması yapılırken gateway değeri de atanmalıdır.

- **DHCP**

IP otomatik olarak ortamdaki DHCP sunucudan alınır. Ayrıca opsiyonel olarak arayüz için hostname ve alias olarak ikinci bir IP adresi girilebilir.

- **PPoE/PPTP**

PPoE ve PPTParayüzlerine kullanıcı adı / parola, opsiyonel olarak servis adı dial-and-demand, idle timeout değerleri set edilebilir.

- **Wireless:**

Wireless arayüzü istemcilere hizmet vermek üzere Access Point olarak kullanılabilir ya da başka bir AP'e bağlanabilir.

TEMEL YAPILANDIRMA

SSH Servisinin Devreye Alınması

SSH servisi konsol menüsünün 14 numaralı seçeneği kullanılarak devreye alınabilir:

```
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: 14
```

```
SSHD is currently disabled. Would you like to enable? [y/n]? y
```

```
Writing configuration... done.
```

```
Enabling SSHD... done.
```

BÖLÜM 4

TEMEL SERVİSLER

TEMEL SERVİSLER

DHCP SERVER

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

TEMEL SERVİSLER

WAN

LAN

☒ Enable DHCP server on LAN interface

☐ Deny unknown clients

If this is checked, only the clients defined below will get DHCP leases from this server.

Subnet	192.168.12.0
Subnet mask	255.255.255.0
Available range	192.168.12.1 - 192.168.12.254
Range	192.168.12.10 to 192.168.12.245
WINS servers	
DNS servers	NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS forwarder is enabled, otherwise the servers configured on the General page.
Gateway	192.168.12.254 The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network.
Domain name	crom.lab The default is to use the domain name of this system as the default domain name provided by DHCP. You may specify an alternate domain name here.
Domain search list	crom.lab The DHCP server can optionally provide a domain search list.
Default lease time	seconds This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum lease time	seconds This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Failover peer IP:	Leave blank to disable. Enter the interface IP address of the other machine. Machines must be using CARP.
Static ARP	☐ Enable Static ARP entries Note: Only the machines listed below will be able to communicate with the firewall on this NIC.

TEMEL SERVİSLER

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

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

The DHCP lease table can be viewed on the [Status: DHCP leases](#) page.

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



TEMEL SERVİSLER

Status: DHCP leases



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

Status: System logs: DHCP



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

Last 50 DHCP service log entries

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

TEMEL SERVİSLER

DNS Forwarder

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

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

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

TEMEL SERVİSLER

General DNS Forwarder Options	
Enable	☒ Enable DNS forwarder
DHCP Registration	☒ Register DHCP leases in DNS forwarder If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.
Static DHCP	☒ Register DHCP static mappings in DNS forwarder If this option is set, then DHCP static mappings will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.

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

TEMEL SERVİSLER

Host Overrides

Entries in this section override individual results from the forwarders. Use these for changing DNS results or for adding custom DNS records.

Host	Domain	IP	Description
www	syslogs.org	1.1.1.1	Fake kayıt

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

```
~# dig www.syslogs.org
```

```
:: ANSWER SECTION:
```

```
www.syslogs.org.      1      IN      A       1.1.1.1
```

TEMEL SERVİSLER

Domain Overrides			
Entries in this area override an entire domain by specifying an authoritative DNS server to be queried for that domain.			
Domain	IP	Description	
google.co.uk	2.2.2.2	Fake Resolver	   

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

~# dig mx google.co.uk

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

TEMEL SERVİSLER

Dynamic DNS

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

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

TEMEL SERVİSLER

Services: Dynamic DNS client



Dynamic DNS client	
Disable	☐
Service type	DNS-O-Matic
Interface to monitor	WAN
Hostname	 Note: Enter the complete host/domain name. example: myhost.dyndns.org
MX	 Note: With DynDNS service you can only use a hostname, not an IP address. Set this option only if you need a special MX record. Not all services support this.
Wildcards	☐ Enable Wildcard
Username	 Username is required for all types except Namecheap and FreeDNS.
Password	 FreeDNS (freedns.afraid.org): Enter your "Authentication Token" provided by FreeDNS.
Description	

Save

Cancel

BÖLÜM 5

FIREWALL

FIREWALL - MENÜ

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

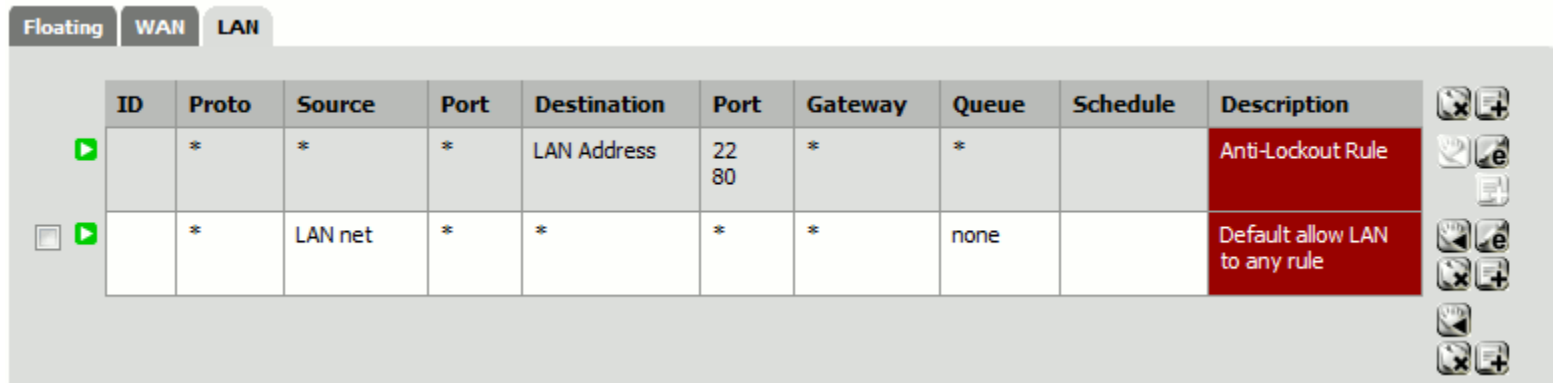
Bu menü altında:

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

alt menüleri bulunur.

FIREWALL - KURALLAR

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



ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	LAN Address	22 80	*	*		Anti-Lockout Rule
	*	LAN net	*	*	*	*	none		Default allow LAN to any rule

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

"Floating" tabı ise tüm interfacelerde yürütülecek kurallar içindir.

FIREWALL - KURALLAR

Edit Firewall rule	
Action	Pass ▾ Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	☐ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	LAN ▾ Choose on which interface packets must come in to match this rule.
Protocol	TCP ▾ Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.
Source	☐ not Use this option to invert the sense of the match. Type: any ▾ Address: / ▾ Advanced - Show source port range

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

FIREWALL - KURALLAR

Destination	☐ not Use this option to invert the sense of the match. Type: any Address: /
Destination port range	from: (other) to: (other) Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port
Log	☐ Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	 You may enter a description here for your reference.

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

FIREWALL - KURALLAR

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

FIREWALL - KURALLAR

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

FIREWALL - KURALLAR

- **TCP Flags:** Spesifik TCP bayraklarını set etmek için kullanılır.
-
- **State Type:** Durum türü.
 - keep state: Durum kontrollü kurallar. (Default)
 - sysnproxy state: Gelen istekler için proxy görevi görür. Handshake tamamlanmadan arkadaki hosta bağlantı açmaz. Bu şekilde spoofed IP'lerden gelen SYN Flood saldırılarından korunmaya yardımcı olur.
 - none: Herhangi bir durum mekanizması kullanmaz.
- **Schedule:** Kuralın aktif olacağı zaman diliminin belirlenmesi.
- **Gateway:** Birden fazla gateway olması durumunda kural için hangi gateway'in kullanılacağını set eder. (Policy based routing)

FIREWALL - ALIASES

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

Alias Edit	
Name	 The name of the alias may only consist of the characters "a-z, A-Z and 0-9".
Description	 You may enter a description here for your reference (not parsed).
Type	Host(s) 
Host(s)	Enter as many hosts as you would like. Hosts must be specified by their IP address. IP   Description   

FIREWALL - ALIASES

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

Firewall: Aliases: Edit



Alias Edit																															
Name	izinliportlar The name of the alias may only consist of the characters "a-z, A-Z and 0-9".																														
Description	İzinli Port Numaraları You may enter a description here for your reference (not parsed).																														
Type	Port(s)																														
Port(s)	Enter as many ports as you wish. Port ranges can be expressed by seperating with a colon. <table><thead><tr><th>Port</th><th></th><th>Description</th><th></th></tr></thead><tbody><tr><td>80</td><td>32 </td><td> http</td><td></td></tr><tr><td>443</td><td>32 </td><td> https</td><td></td></tr><tr><td>110</td><td>32 </td><td> pop3</td><td></td></tr><tr><td>25</td><td>32 </td><td> smtp</td><td></td></tr><tr><td>587</td><td>32 </td><td> submission</td><td></td></tr><tr><td>53</td><td>32 </td><td> dns</td><td></td></tr></tbody></table>			Port		Description		80	32	http		443	32	https		110	32	pop3		25	32	smtp		587	32	submission		53	32	dns	
Port		Description																													
80	32	http																													
443	32	https																													
110	32	pop3																													
25	32	smtp																													
587	32	submission																													
53	32	dns																													

FIREWALL - SCHEDULES

Zaman bazlı firewall kuralları oluşturmak için kullanılan bir özelliktir.

Schedule information

Schedule Name

Personel

The name of the alias may only consist of the characters a-z, A-Z and 0-9

Description

Oglent Tatili

You may enter a description here for your reference (not parsed).

Month

June 12

June 2012

Mon	Tue	Wed	Thu	Fri	Sat	Sun
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Click individual date to select that date only. Click the appropriate weekday Header to select all occurrences of that weekday.

Time

Start Time

Stop Time

12

Hr

00

Min

13

Hr

00

Min

Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.

Time Range Description

Oglen

You may enter a description here for your reference (not parsed).

Add Time

Clear Selection

Schedule repeat

Configured Ranges

Day(s)	Start Time	Stop Time	Description
--------	------------	-----------	-------------

FIREWALL - SCHEDULES

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

Floating WAN LAN									
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	LAN Address	22 80	*	*		Anti-Lockout Rule
 	*	LAN net	*	*	*	*	none	 <u>Personel2</u>	Default allow LAN to any rule

FIREWALL - VIRTUAL IPs

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

Edit Virtual IP	
Type	☒ Proxy ARP ☐ CARP ☐ Other ☐ IP Alias
Interface	WAN
IP Address(es)	Type: Single address Address: / 32 This is a CIDR block of proxy ARP addresses.
Virtual IP Password	 Enter the VHID group password.
VHID Group	1 Enter the VHID group that the machines will share
Advertising Frequency	Base: 1 Skew: 0 The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.
Description	 You may enter a description here for your reference (not parsed).

FIREWALL - VIRTUAL IPs

Toplam olarak 4 farklı virtual IP tipi bulunmaktadır.

IP Alias:

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

Proxy ARP:

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

FIREWALL - VIRTUAL IPs

CARP:

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

OTHER:

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

BÖLÜM 6

Network Address Translation

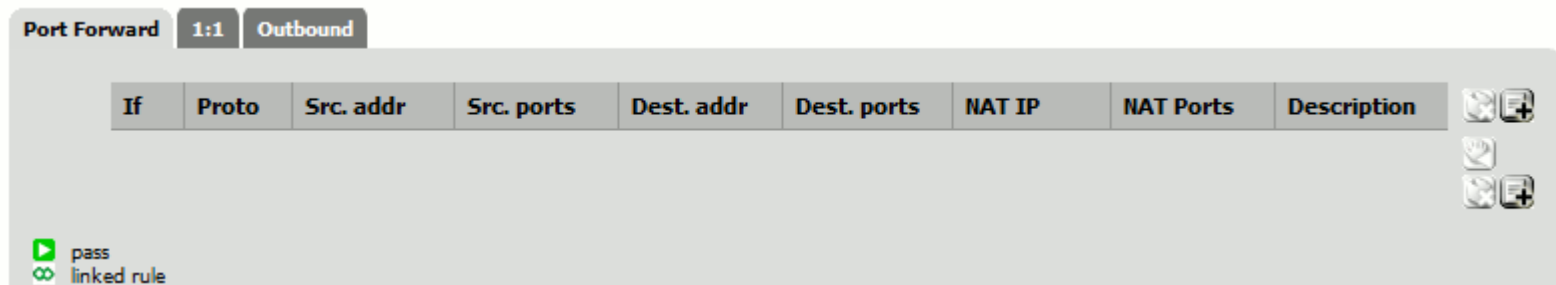
NAT

PfSense üç farklı NAT özelliği sunar:

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

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

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



NAT - Port Yönlendirme

Senaryo 1:

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

Port Forward

1:1

Outbound

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

Senaryo 2:

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

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

1:1 NAT

Senaryo:

WAN arayüzünden 86.19.12.103 gelen tüm trafiği 192.168.12.103 adresine yönlendir.

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

86.19.12.103/32	P ARP	ADSL04	e x
-----------------	-------	--------	-----

2- 1:1 Nat girdisi oluşturulur:

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

OUTBOUND NAT

Senaryo:

192.168.12.103 host'unu internete çıkarken 86.19.12.103 olarak dönüştür

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

86.19.12.103/32		ADSL04	
-----------------	---	--------	---

2- Outbound Nat girdisi oluşturulur:

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

BÖLÜM 7

VPN SERVİSLERİ

VPN

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

pfSense tarafından aşağıdaki VPN çözümleri desteklenir.

- IPSec
- OpenVPN
- PPTP
- L2TP

VPN - IPSec

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

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

UDP Port 500 ve ESP/AH protokolleri üzerinden çalışır.

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

VPN - OpenVPN

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

UDP Port 1194 kullanır. İletişim encrypt olarak sağlanır.

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

VPN - PPTP

OpenVPN benzeri bir VPN çözümüdür.

TCP port 1723 ve GRE protokolü kullanır.

İletişim encrypt olarak sağlanır.

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

VPN - PPTP

Configuration **Users**

☐ Off

☐ Redirect incoming PPTP connections to:

PPTP redirection

Enter the IP address of a host which will accept incoming PPTP connections.

☒ Enable PPTP server

No. PPTP users

Hint: 10 is ten PPTP clients

Server address

Enter the IP address the PPTP server should give to clients for use as their "gateway". Typically this is set to an unused IP just outside of the client range.

NOTE: This should NOT be set to any IP address currently in use on this firewall.

Remote address range

Specify the starting address for the client IP subnet.

PPTP DNS Servers

primary and secondary DNS servers assigned to PPTP clients

WINS Server

RADIUS ☐ Use a RADIUS server for authentication

When set, all users will be authenticated using the RADIUS server specified below. The local user database will not be used.

Configuration **Users**

Username	IP address	
vpnuser	192.168.12.201	 

BÖLÜM 8

MULTIWAN

LOAD BALANCING

&

FAILOVER

LOAD BALANCING & FAILOVER

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

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

LOAD BALANCING & FAILOVER

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

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

MULTI WAN GATEWAY

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

System: Gateways S ?

Gateways Routes Groups

Name	Interface	Gateway	Monitor IP	Description
WANGW2	OPT1	10.1.0.99	10.1.0.99	WANGW2
WAN (default)	WAN	10.0.0.99	10.0.0.99	Interface WAN Dynamic Gateway

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

MULTI WAN / LOAD BALANCE

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

System: Gateways: Edit gatewayS?

Edit gateway entry

Group Name	WANBALANCER Group Name
Gateway Priority	Tier 1 ▼ WANGW2 - WANGW2 Tier 1 ▼ WAN - Interface WAN Dynamic Gateway Link Priority The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted we will use the next available link(s) in the next priority level.
Trigger Level	Member Down ▼ When to trigger exclusion of a member
Description	Default Balancer You may enter a description here for your reference (not parsed).

Save

Cancel

MULTI WAN / LOAD BALANCE

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

Gateways Routes Groups

Group Name	Gateways	Priority	Description
WANBALANCER	WANGW2 WAN	Tier 1 Tier 1	Default Balancer

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

Gateway	WANBALANCER ▼
---------	---------------

Böylece ilgili kural için MULTI WAN GW kullanılacaktır.

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	LAN net	*	*	*	WANBALANCER	none		Default allow LAN to any rule

MULTI WAN / FAILOVER

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

beli

Edit gateway entry	
Group Name	 WANFAILOVER Group Name
Gateway Priority	Tier 1 ▼ WANGW2 - WANGW2 Tier 2 ▼ WAN - Interface WAN Dynamic Gateway Link Priority The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted we will use the next available link(s) in the next priority level.
Trigger Level	Member Down ▼ When to trigger exclusion of a member
Description	 Default WAN Failover You may enter a description here for your reference (not parsed).

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

BÖLÜM 9

DiĞER SERVİSLER

PAKET SİSTEMİ

Ek servisler ve uygulamalar System > Packages menüsünden kolayca kurulabilmektedir.

System: Package Manager 

Available Packages

Installed Packages

Package Name	Category	Status	Package Info	Description	
Asterisk	Services	Beta 1.8.8.1 pkg v 0.1 platform: 2.0	Package Info	Asterisk is an open source framework for building communications applications. Asterisk turns an ordinary computer into a communications server.	
anyterm	Diagnostics	BETA 0.5 platform: 1.2.3	Package Info	Ajax Interactive Shell - Have you ever wanted SSH or telnet access to your system from an internet desert - from behind a strict firewall, from an internet cafe, or even from a mobile phone? Anyterm is a combination of a web page and a process that runs on your web server that provides this access. WARNING! We suggest using Stunnel in combination with this package!	
Avahi	Network Management	ALPHA 0.6.25_2 platform: 1.2.3	Package Info	Avahi is a system which facilitates service discovery on a local network. This means that you can plug your laptop or computer into a network and instantly be able to view other people who you can chat with, find printers to print to or find files being shared. This kind of technology is already found in Apple MacOS X (branded Rendezvous, Bonjour and sometimes Zeroconf) and is very convenient. Avahi is mainly based on Lennart Poettering's flexmdns mDNS implementation for Linux which has been discontinued in favour of Avahi.	
AutoConfigBackup	Services	Stable 1.19 platform: 1.2	Package Info	Automatically backs up your pfSense configuration. All contents are encrypted on the server. Requires pfSense Premium Support Portal Subscription from https://portal.pfsense.org	
arping	Services	Stable 2.09.1 platform: 1.0.1	Package Info	Broadcasts a who-has ARP packet on the network and prints answers.	

OPENNTPD

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

NTP server



Enable



Check this to enable the NTP server.

Interface

WAN
LAN
OPT1
Localhost

Select the interface(s) the NTP server will listen on.

Save

SNMP

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

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

Services: SNMP 

SNMP Daemon  Enable	
Polling Port	 161 Enter the port to accept polling events on (default 161)
System location	
System contact	 cagri.ersen@gmail.com
Read Community String	 public The community string is like a password, restricting access to querying SNMP to hosts knowing the community string. Use a strong value here to protect from unauthorized information disclosure.

Wake On LAN

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

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

Wake on LAN

Interface

WAN ▼

Choose which interface the host to be woken up is connected to.

MAC address

 0a:00:27:00:00:00

Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx

Send

Wake all clients at once: 

Or Click the MAC address to wake up an individual device:

Interface	MAC address	Description
LAN	0a:00:27:00:00:00	Ofis Bilgisayarım



Note:

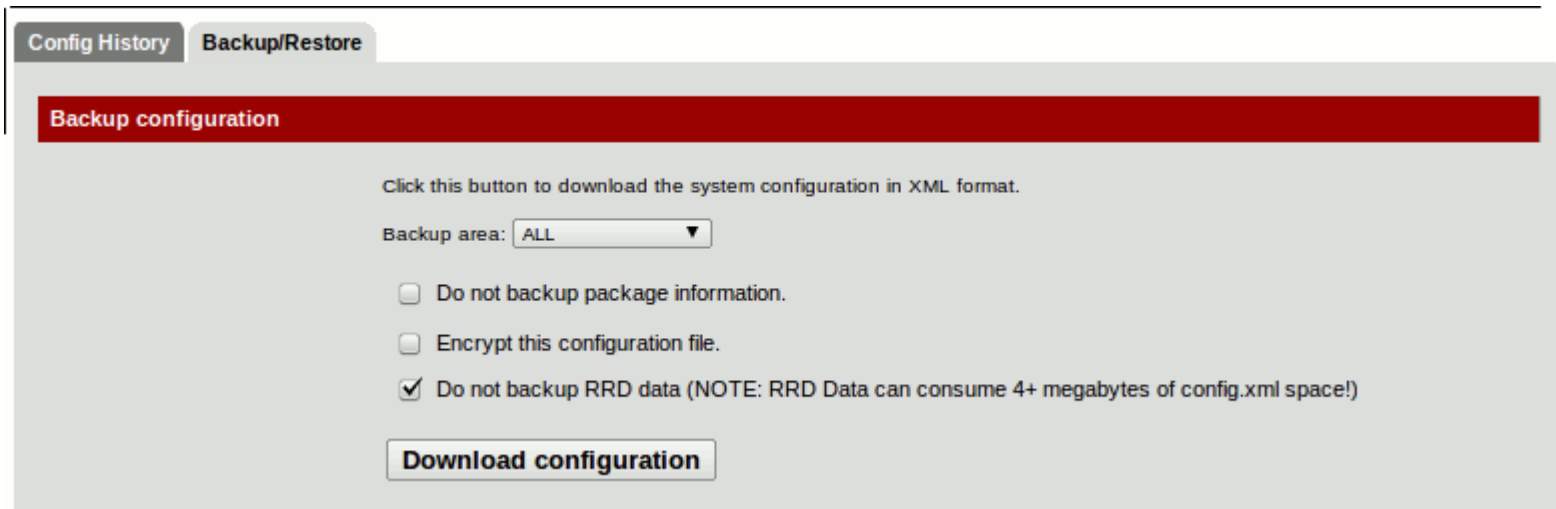
BÖLÜM 10

BAKIM VE MONITORING

BACKUP

pfSense'in bütün yapılandırma dosyaları XML tabanlıdır.

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



The screenshot shows the pfSense web interface for the Backup/Restore section. At the top, there are two tabs: "Config History" and "Backup/Restore". Below the tabs is a red header bar with the text "Backup configuration". The main content area contains the following elements:

- A text instruction: "Click this button to download the system configuration in XML format."
- A "Backup area:" label followed by a dropdown menu currently set to "ALL".
- Three checkboxes:
 - ☐ Do not backup package information.
 - ☐ Encrypt this configuration file.
 - ☒ Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)
- A "Download configuration" button at the bottom.

RESTORE

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

Restore configuration

Open a configuration XML file and click the button below to restore the configuration.

Restore area: ALL

 Choose File No file chosen

☐ Configuration file is encrypted.

Restore configuration

Note: The firewall will reboot after restoring the configuration.

SERVİSLERİN YÖNETİLMESİ

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

Status: Services



Service	Description	Status	
dhcpcd	DHCP Service	 Running	 
dnsmasq	DNS Forwarder	 Running	 
ntpd	NTP clock sync	 Running	 
relayd	Server load balancing daemon	 Running	 

E-MAIL DURUM BİLDİRİMLERİ

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

SMTP E-Mail

E-Mail server

This is the FQDN or IP address of the SMTP E-Mail server to which notifications will be sent.

SMTP Port of E-Mail server

☐ Enable SSL/TLS Authentication

This is the port of the SMTP E-Mail server, typically 25, 587 (submission) or 465 (smtps, tick ssl/tls checkbox)

From e-mail address

This is the e-mail address that will appear in the from field.

Notification E-Mail address

Enter the e-mail address that you would like email notifications sent to.

Notification E-Mail auth username (optional)

Enter the e-mail address username for SMTP authentication.

Notification E-Mail auth password

Enter the e-mail address password for SMTP authentication.

Save

Kayıtları Log Sunucusna Göndermek

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

The screenshot shows a web interface for configuring remote syslog servers. At the top, there is a checkbox labeled "Enable syslog'ing to remote syslog server". Below this, the section "Remote syslog servers" contains three input fields labeled "Server 1", "Server 2", and "Server 3". Underneath these fields is the text "IP addresses of remote syslog servers". At the bottom, there is a list of event types, each with an unchecked checkbox: "System events", "Firewall events", "DHCP service events", "Portal Auth events", "VPN (PPTP, IPsec, OpenVPN) events", "Gateway Monitor events", "Server Load Balancer events", and "Wireless events".

RRD Grafikleri

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

Status: RRD Graphs

System

Traffic

Packets

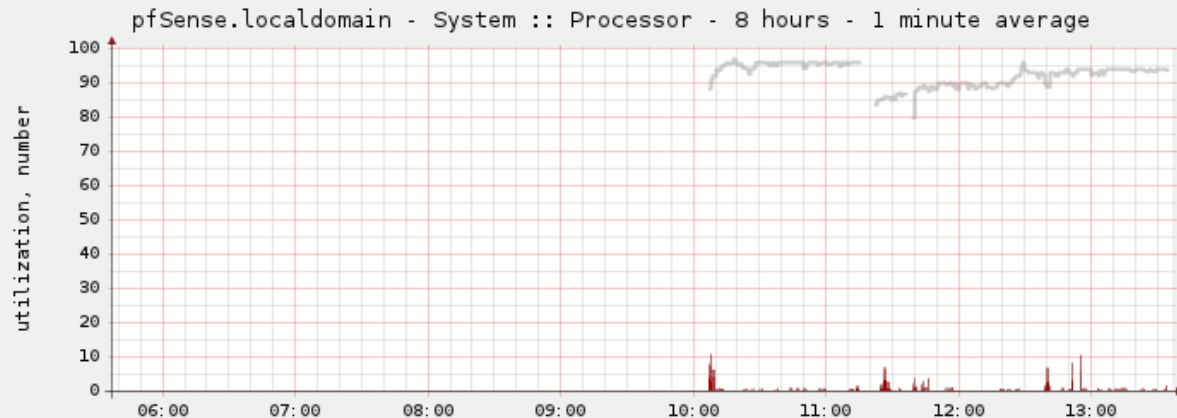
Quality

Custom

Settings

Note: Change of color and/or style may not take effect until the next refresh

Graphs: Processor Style: Inverse Period: Absolute Timespans



	minimum	average	maximum	current
User util.	0.00	117.55 m	3.66	0.00
Nice util.	0.00	111.24 m	5.85	171.79 m
System util.	0.00	303.93 m	5.13	1.13
Interrupt	0.00	30.51 m	738.02 m	0.00
Processes	79.88	92.46	97.00	93.75

Jun 30 13:36:39 2012

Sistem Loglarının Görüntülenmesi

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

Status: System logs: System	
System	Firewall DHCP Portal Auth IPsec PPP VPN Load Balancer OpenVPN OpenNTPD Wireless Settings
Last 50 system log entries	
Jun 30 12:31:31	check_reload_status: Syncing firewall
Jun 30 12:31:54	check_reload_status: Syncing firewall
Jun 30 12:31:56	check_reload_status: Reloading filter
Jun 30 12:32:16	check_reload_status: Syncing firewall
Jun 30 12:32:18	check_reload_status: Reloading filter
Jun 30 12:35:03	check_reload_status: Syncing firewall
Jun 30 12:35:05	check_reload_status: Reloading filter
Jun 30 12:35:39	check_reload_status: Syncing firewall
Jun 30 12:35:41	check_reload_status: Reloading filter
Jun 30 12:36:05	check_reload_status: Syncing firewall
Jun 30 12:36:07	check_reload_status: Reloading filter
Jun 30 12:36:25	check_reload_status: Syncing firewall